Algebra
– Arbeitsversion –

Prof. Dr. Ina Kersten
geTEXt von Ole Riedlin

4. April 2002

Inhaltsverzeichnis

0 Worum geht es?

Gruppen Ringe Körper

Galois-Theorie

E. Galois N.H. Abel

1811 – 1832 1802 – 1829

Anwendungen

Als Anwendung der Galoistheorie erhalten wir Ergebnisse über die Auflösbarkeit von Gleichungen

$$\boxed{c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0 = 0}$$

in einer Variablen x. Die Koeffizienten $c_0, \ldots, c_n$ liegen in einem Körper K, und die Lösungen liegen in einem geeigneten Erweiterungskörper L von K. Ist $c_n \neq 0$, so heißt n der *Grad der Gleichung*. Man dividiert dann alle Koeffizienten $c_0, \ldots, c_n$ durch c_n und erhält eine Gleichung der Form:

$$x_n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$$

mit $a_0, \ldots, a_{n-1} \in K$.

0.1 Quadratische Gleichungen

Die Gleichung $x^2 + ax + b = 0$ hat bekanntlich (falls $1 + 1 \neq 0$) die Lösungen

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

0.2 Kubische Gleichungen

$$(*) \qquad x^3 + ax^2 + bx + c = 0 \quad \text{mit} \quad a, b, c \in K (\neq \mathbb{Z}/3\mathbb{Z} \text{ und } \neq \mathbb{Z}/2\mathbb{Z})$$

Mit Hilfe der *Tschirnhausen-Transformation (1683)* $x = z - \frac{a}{3}$ geht die Gleichung $(*)$ in eine Gleichung der Form $z^3 + pz + q = 0$ über (mit $p, q \in K$). Hierfür gibt es die von Cardano 1545 veröffentlichte Auflösungsformel.

Bemerkung. Für die Lösungen $x_1, x_2, x_3 \in L$ von $(*)$ gilt:

$$(x-x_1)(x-x_2)(x-x_3) = x^3 - (\underbrace{x_1+x_2+x_3}_{\in K})x^2 + (\underbrace{x_1x_2+x_1x_3+x_2x_3}_{\in K})x - \underbrace{x_1x_2x_3}_{\in K}$$

Die Koeffizienten liegen in K, wie später bewiesen wird.
Koeffizientenvergleich mit $(*)$ ergibt:

$$\boxed{x_1+x_2+x_3=-a} \qquad \boxed{x_1x_2+x_1x_3+x_2x_3=b} \qquad \boxed{x_1x_2x_3=-c}$$

0.3 Biquadratische Gleichungen

$$\boxed{x^4+ax^3+bx^2+cx+d=0 \quad \text{mit} \quad a,b,c,d \in K}$$

Spezialfall: $a=c=0$. Durch die Substitution $x^2=z$ geht dann die Gleichung in $z^2+bz+d=0$ über und läßt sich mit Hilfe von (0.1) lösen. Sonst führt die *Tschirnhausen-Transformation* $x=z-\frac{a}{4}$ auf eine Gleichung der Form $z^4+pz^2+qz+r=0$ mit $p,q,r \in K$. Hierfür gibt es die *Auflösungsformeln von Ferrari*, die Cardano 1545 veröffentlicht hat (vgl. erstes Übungsblatt).

Bemerkung. Aus der Galois-Theorie folgt, dass die Gleichung

$$x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=0$$

im allgemeinen für $n \geq 5$ nicht durch Wurzelausdrücke lösbar ist, wie dies für $n=2,3,4$ möglich ist. Man sagt, dass die allgemeine Gleichung n-ten Grades ab $n \geq 5$ nicht durch Radikale lösbar sei.

0.4 Konstruktionen mit Zirkel und Lineal

Wann ist ein geometrisches Konstruktionsproblem mit Zirkel und Lineal lösbar? Das Lineal darf nur zum Ziehen von Geraden, aber nicht zum Ablesen von Werten benutzt werden!
Sei $M \subset \mathbb{R}^2$ eine Menge mit mindestens zwei Punkten, $G(M)$ die Menge aller Geraden, die zwei Punkte von M enthalten (Stichwort: Lineal), $K(M)$ die Menge aller Kreise mit Mittelpunkt aus M, deren Radius der Abstand zweier Punkte aus M ist (Stichwort: Zirkel).
Sei $M' \supset M$ die Menge aller Punkte aus $\mathbb{R}^2$, die in M liegen oder die man durch Anwenden *einer* der folgenden Operationen aus M erhält.

(O1) Schnitt zweier Geraden aus $G(M)$

(O2) Schnitt einer Geraden aus $G(M)$ mit einem Kreis aus $K(M)$

(O3) Schnitt zweier Kreise aus $K(M)$

Setze $M_0 = M$, $M_1 = M'_0$, $M_2 = M'_1$, $\ldots$, $M_{n+1} = M'_n$, $\ldots$
und erhalte so eine Kette von Punktmengen der Ebene
$M = M_0 \subset M_1 \subset \cdots \subset M_n \subset \cdots$

Definition. Sei $M \subset \mathbb{R}^2$ eine Menge mit mindestens zwei Punkten. Die Vereinigung $\widehat{M} = \bigcup_{n=0}^{\infty} M_n$ heißt die *Menge aller aus M mit Zirkel und Lineal konstruierbaren Punkte.*

Beispiel (Konstruktion des Mittelpunktes).
Sei $M = M_0 = \{p_1, p_2\}$. Dann ist $M_1 = M'_0 = \{p_1, p_2, q_1, q_2\}$, wobei q_1, q_2 durch (O3) gewonnen sind: q_1, q_2 sind die Schnittpunkte des Kreises mit Mittelpunkt p_1 und Radius $\overline{p_1p_2}$ mit dem Kreis mit Mittelpunkt p_2 und Radius $\overline{p_1p_2}$.

Sei $M_2 = M'_1 = \{p_1, p_2, q_1, q_2, m\}$, wobei m durch die Operation (O1) konstruiert wird. Es ist m der Schnittpunkt der Geraden $\overline{q_1q_2}$ mit $\overline{p_1p_2}$ und gleichzeitig der gesuchte Mittelpunkt.

0.5 Delisches Problem der Kubusverdopplung

Zu einem vorgegebenen Würfel soll ein Würfel doppelten Volumens mit Zirkel und Lineal konstruiert werden.
Es ist $M = \{p_1, p_2\}$, wobei der Abstand a zwischen p_1, p_2 die Kantenlänge des Würfels ist. Der Würfel doppelten Volumens hat die Kantenlänge $\sqrt[3]{2}\,a$.
frage Gehört ein Punkt q, der von p_1 den Abstand $\sqrt[3]{2}\,a$ hat, zu $\widehat{M}$?
Die Antwort ist nein. Die Würfelverdopplung mit Zirkel und Lineal ist nicht möglich, wie wir sehen werden. Auch die Dreiteilung des Winkels $\frac{\pi}{3}$ ist nicht mit Zirkel und Lineal möglich, ebenso wie die Quadratur des Kreises.

Übungsaufgaben 1 – 4

Man benutze in den ersten beiden Aufgaben die folgenden Formeln und schreibe die Lösungen in der Form $a + bi$ mit reellen Zahlen a, b . (Es ist $i^2 = -1$.)

Cardano-Formeln. (Ferro (1465-1526), Tartaglia):
Die Gleichung $x^3 + px + q = 0$ mit komplexen Koeffizienten p, q hat die

Lösungen

$$x_1 = u + v\,, \qquad x_2 = -\frac{u+v}{2} + \frac{u-v}{2}\sqrt{-3}\,, \qquad x_3 = -\frac{u+v}{2} - \frac{u-v}{2}\sqrt{-3}\,,$$

wobei $u = \sqrt[3]{-\frac{q}{2} + \sqrt{D}}$ und $v = \sqrt[3]{-\frac{q}{2} - \sqrt{D}}$ mit $D = \left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2$ gilt und die komplexen dritten Wurzeln so bestimmt werden, dass $3uv = -p$ ist.

Cardano-Formeln. (Ferrari (1522-1565), Schüler von Cardano):
Die Lösungen der Gleichung $x^4+px^2+qx+r = 0$ mit komplexen Koeffizienten p, q, r sind

$$\begin{aligned} x_1 &= \tfrac{1}{2}\left(\sqrt{-y_1} + \sqrt{-y_2} + \sqrt{-y_3}\right)\,, & x_2 &= \tfrac{1}{2}\left(\sqrt{-y_1} - \sqrt{-y_2} - \sqrt{-y_3}\right)\,, \\ x_3 &= \tfrac{1}{2}\left(-\sqrt{-y_1} + \sqrt{-y_2} - \sqrt{-y_3}\right)\,, & x_4 &= \tfrac{1}{2}\left(-\sqrt{-y_1} - \sqrt{-y_2} + \sqrt{-y_3}\right)\,, \end{aligned}$$

wobei y_1, y_2, y_3 die Lösungen der *kubischen Resolvente*

$$y^3 - 2py^2 + (p^2 - 4r)y + q^2 = 0$$

sind und die Wurzeln so gewählt werden, dass $\sqrt{-y_1} \cdot \sqrt{-y_2} \cdot \sqrt{-y_3} = -q$ gilt.

Aufgabe 1. Man löse die Gleichung $x^3 + 6x + 2 = 0$.

Aufgabe 2. Man löse die Gleichung $x^4 - x + \frac{1}{2} = 0$.

Aufgabe 3. Man löse die Gleichung $x^3 - 1 = 0$ in $\mathbb{C}$ und zeige:

(a) Für jede dritte Einheitswurzel ζ gilt $\overline{\zeta} = \zeta^2 = \zeta^{-1}$.

(b) Für jede dritte Einheitswurzel $\zeta \neq 1$ gilt $1 + \zeta + \zeta^2 = 0$.

(c) Für $u, v \in \mathbb{C}$ gilt: $u^3 = v^3 \iff u = \zeta v$ mit einer dritten Einheitswurzel ζ.

Aufgabe 4. Seien $p, q \in \mathbb{R}$ und $D = \left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2$. Man ermittle in den Fällen $D = 0$, $D > 0$ und $D < 0$ jeweils, ob das Polynom $f(x) = x^3 + px + q$ mehrfache Nullstellen besitzt und welche Nullstellen von $f(x)$ reell sind.
Hinweis. Man benutze die Cardano-Formeln für kubische Gleichungen.

Teil I
Gruppen

1 Die Isomorphiesätze der Gruppentheorie

1.1 Einige Grundbegriffe

- Eine *Gruppe* ist eine Menge G mit einer Verknüpfung

$$G \times G \longrightarrow G, \ (a,b) \longmapsto ab\,,$$

derart, dass gilt:

(G1) $(ab)c = a(bc) \ \forall\, a,b,c \in G$

(G2) $\exists\, e \in G$ mit $ea = a \ \forall\, a \in G$ (*neutrales Element*)

(G3) Zu jedem $a \in G$ gibt es ein Inverses $a^{-1} \in G$ mit $a^{-1}a = e$.

Gilt zusätzlich $ab = ba \ \forall\, a,b \in G$, so heißt G *abelsch* oder *kommutativ*.
Ist G eine Gruppe, so gilt $\boxed{ae = a \ \forall\, a \in G}$ und $\boxed{aa^{-1} = e \ \forall\, a \in G}$, und e und a^{-1} sind eindeutig bestimmt (vgl. AGLA 2.2, 2.3, 10.4).

- Seien G, G' zwei Gruppen mit neutralen Elementen e von G und e' von G'. Eine Abbildung $f\colon G \longrightarrow G'$ heißt *Homomorphismus*, falls $f(ab) = f(a) \circ f(b) \ \forall\, a,b \in G$ gilt, wobei $\circ$ die Verknüpfung in G' ist. (Den Kringel lassen wir meist weg. Ist $+$ die Verknüpfung, schreiben wir $a+b$ statt ab und $-a$ statt a^{-1}.)
Ist $f\colon G \longrightarrow G'$ ein Gruppenhomomorphismus, so gilt $f(e) = e'$ und $f(a^{-1}) = (f(a))^{-1} \ \forall\, a \in G$ (vgl. AGLA 10.6, 10.7).

- Eine Teilmenge H einer Gruppe G heißt *Untergruppe* von G, falls

(i) $a,b \in H \Longrightarrow ab \in H$ (*Abgeschlossenheit*)

(ii) $a \in H \Longrightarrow a^{-1} \in H$

(iii) $e \in H$.

Eine Untergruppe ist eine Gruppe (vgl. AGLA 10.5).

- Seien G eine Gruppe, $a \in G$ fest und H eine Untergruppe von G. Dann heißt die Teilmenge $aH := \{ah \mid h \in H\}$ eine *Linksnebenklasse* (vgl. AGLA 10.9).

- Eine Untergruppe H einer Gruppe G heißt *Normalteiler* in G, falls

$$\boxed{aHa^{-1} \subset H \text{ für jedes } a \in G}.$$

Dabei ist $aHa^{-1} = \{aha^{-1} \mid h \in H\}$. Ist H Normalteiler in G, so schreibt man $H \lhd G$. Es gilt

$$\boxed{H \lhd G} \iff \boxed{aHa^{-1} = H \;\forall\, a \in G} \iff \boxed{aH = Ha \;\forall\, a \in G}$$

(Beweis in AGLA 10.17).

- Ferner gilt: $\boxed{H \lhd G} \Longrightarrow \boxed{G/H := \{aH \mid a \in G\} \text{ ist eine Gruppe.}}$
Verknüpfung $aH \cdot bH = abH$ (ist wohldefiniert).
Neutrales Element: H.

  G/H heißt *Faktorgruppe von G nach H* (vgl. AGLA 10.18).

1.2 Homomorphiesatz

Ist $f\colon G \longrightarrow G'$ ein surjektiver Gruppenhomomorphismus, so induziert f einen Isomorphismus

$$G/\operatorname{kern}(f) \xrightarrow{\sim} G', \; a \operatorname{kern}(f) \longmapsto f(a)\,.$$

Beweis. S. AGLA 10.19. □

- Es ist $\operatorname{kern}(f) := \{x \in G \mid f(x) = e'\}$ ein Normalteiler in G (vgl. AGLA 10.17).

1.3 Ein Untergruppenkriterium

Satz.
Seien U, V Untergruppen einer Gruppe G und $UV := \{uv \mid u \in U,\, v \in V\}$. Dann gilt:

$$\boxed{UV \textit{ ist Untergruppe von } G} \iff \boxed{UV = VU}$$

Beweis. „$\Longrightarrow$“: Sei UV eine Untergruppe von G. Zu zeigen: $UV = VU$.

„$\subset$“: Sei $uv \in UV$ mit $u \in U, v \in V$.
$\Longrightarrow (uv)^{-1} \in UV$, da UV Untergruppe
$\Longrightarrow (uv)^{-1} = u_1v_1$ mit $u_1 \in U$ und $v_1 \in V$
$\Longrightarrow uv = (u_1v_1)^{-1} = v_1^{-1}u_1^{-1} \in VU$.
Also ist $UV \subset VU$.

„$\supset$“: Sei $v \in V, u \in U$.
$\Longrightarrow vu = \underbrace{ev}_{\in UV} \cdot \underbrace{ue}_{\in UV} \in UV$, da UV Untergruppe.
Also ist $VU \subset UV$.

„$\Longleftarrow$“: Sei $UV = VU$. Zu zeigen: UV ist Untergruppe von G.

(1) Es ist $e = ee \in UV$.

(2) $uv \in UV \Longrightarrow (uv)^{-1} = v^{-1}u^{-1} \in VU = UV$.

(3) Seien $u_1v_1, u_2v_2 \in UV$. Zu zeigen: $u_1v_1u_2v_2 \in UV$.
Da $VU = UV$ gilt, folgt $v_1u_2 = u_3v_3$ mit $u_3 \in U, v_3 \in V$.
$\Longrightarrow u_1v_1u_2v_2 = \underbrace{u_1u_3}_{\in U} \cdot \underbrace{v_3v_2}_{\in V} \in UV$.

□

1.4 Erster Noetherscher Isomorphiesatz

Satz.
Seien U eine Untergruppe und N ein Normalteiler in einer Gruppe G. Dann gelten:

(a) UN ist eine Untergruppe von G.

(b) $U \cap N$ ist ein Normalteiler in U.

(c) Der Homomorphismus $\varphi\colon U \longrightarrow G/N\,,\ u \longmapsto uN\,$, induziert einen Gruppenisomorphismus

$$\boxed{U/(U \cap N) \xrightarrow{\ \sim\ } UN/N\,,\ u(U \cap N) \longmapsto uN}\,.$$

Beweis. (a) Es ist $UN = \bigcup_{u \in U} uN \underset{\text{da } N \triangleleft G}{=} \bigcup_{u \in U} Nu = NU$
$\Longrightarrow UN$ ist eine Untergruppe von G nach 1.3.

(b) Wir zeigen: $\operatorname{kern}\varphi = U \cap N$.

„$\subset$“: Sei $u \in \operatorname{kern}\varphi \Longrightarrow N = \varphi(u) = uN$
$\Longrightarrow u \in N \Longrightarrow u \in U \cap N$.

„$\supset$“: Sei $u \in N \cap U \Longrightarrow \varphi(u) = uN = N$
$\Longrightarrow u \in \operatorname{kern}\varphi\,$.

Also ist $U \cap N = \operatorname{kern}\varphi\,$. Hieraus folgt (b) und nach dem Homomorphiesatz auch (c). □

1.5 Das Bild eines Normalteilers

Lemma.
Ist $f: G \longrightarrow H$ ein surjektiver Homomorphismus von Gruppen und N Normalteiler in G, so ist $f(N)$ Normalteiler in H.

Beweis. Zu zeigen: $hf(n)h^{-1} \in f(N)\ \forall\, h \in H, n \in N$.
Da f surjektiv ist, folgt $h = f(g)$ mit einem $g \in G$.
$\Longrightarrow hf(n)h^{-1} = f(g)f(n)f(g)^{-1} = f(\underbrace{gng^{-1}}_{\in N \lhd G}) \in f(N)$. □

1.6 Der kanonische Restklassenhomomorphismus $G \longrightarrow G/N$

Ist N Normalteiler in einer Gruppe G, so nennt man den Homomorphismus $\pi: G \longrightarrow G/N$, $g \longmapsto gN$, *kanonisch* (oder *kanonischen Restklassenhomomorphismus*). Es ist π surjektiv.

1.7 Zweiter Noetherscher Isomorphiesatz

Satz.
Seien M, N zwei Normalteiler in einer Gruppe G, und sei $N \subset M$. Dann ist M/N Normalteiler in G/N und die Komposition

$$\varphi: G \xrightarrow[kan]{\pi} G/N \xrightarrow[kan]{} (G/N)/(M/N)$$

induziert einen Isomorphismus

$$G/M \xrightarrow{\sim} (G/N)/(M/N)\,.$$

Beweis. $\pi: G \longrightarrow G/N$ ist surjektiv, und es ist $\pi(M) = M/N$
$\underset{1.5}{\Longrightarrow} M/N \lhd G/N$. Da $\ker \varphi = M$ ist, folgt die Behauptung aus dem Homomorphiesatz 1.2. □

1.8 Übungsaufgaben 5 – 7

Aufgabe 5. Man untersuche, welche der folgenden Teilmengen Untergruppen sind:

(a) Die Menge der n-ten Einheitswurzeln in $\mathbb{C}^* := \mathbb{C} \setminus \{0\}$ bezüglich Multiplikation.

(b) Die Menge $\{1, -1, i, -i\}$ in $\mathbb{C}^*$ bezüglich Multiplikation.

(c) Das *Zentrum* $Z(G) := \{a \in G \mid ab = ba \ \forall\, b \in G\}$ in einer Gruppe G.

Aufgabe 6. Man untersuche, welche der folgenden Abbildungen Gruppenhomomorphismen sind:

(a) $f_1 \colon \mathbb{Z} \longrightarrow \mathbb{Z}\,,\ z \longmapsto 2z\,,$

(b) $f_2 \colon \mathbb{Z} \longrightarrow \mathbb{Q}^*,\ z \longmapsto z^2 + 1\,,$

(c) $f_3 \colon \mathbb{C}^* \longrightarrow \mathbb{R}^*,\ z \longmapsto |z|\,,$

(d) $f_4 \colon \mathbb{C} \longrightarrow \mathbb{R}\,,\ z \longmapsto |z|\,.$

Dabei ist die Verknüpfung in $\mathbb{Z}$, $\mathbb{R}$ und $\mathbb{C}$ jeweils die Addition sowie in $\mathbb{R}^*$, $\mathbb{Q}^*$ und $\mathbb{C}^*$ jeweils die Multiplikation.

Aufgabe 7. Seien U und V Normalteiler in einer Gruppe G, und es gelte $U \cap V = \{e\}$. Man zeige, dass $uv = vu$ für alle $u \in U$ und alle $v \in V$ gilt und dass die *Produktabbildung*

$$U \times V \longrightarrow G\,,\ (u,v) \longmapsto uv\,,$$

ein injektiver Gruppenhomomorphismus ist.

Bemerkung.
Gilt zusätzlich noch $UV = G$, so sind die Gruppen $U \times V$ und G isomorph.

2 Die Sylowschen Sätze

Sei $n \in \mathbb{N}$ und p eine Primzahl, die n teilt (Schreibweise: $p \mid n$). Dann ist $n = p^r m$, wobei $r > 0$ und m nicht mehr durch p teilbar ist (Schreibweise: $p \nmid m$).

Beispiel.

$$\begin{aligned} 60 &= 2 \cdot 2 \cdot 3 \cdot 5 \ (\textit{Primfaktorzerlegung}) \\ &= 2^2 \cdot 15 \text{ und } 2 \nmid 15 \\ &= 3 \cdot 20 \text{ und } 3 \nmid 20 \\ &= 5 \cdot 12 \text{ und } 5 \nmid 12 \end{aligned}$$

2.1 Hilfssatz über Binomialkoeffizienten

Satz.
Sei $n = p^r m$ mit $p \nmid m$ und $r > 0$, und sei $0 \le s \le r$. Dann ist die Zahl $\binom{n}{p^s}$ nicht durch p^{r-s+1} teilbar. Insbesondere ist $\binom{n}{p^r}$ nicht durch p teilbar.

Beweis. Für $s = 0$ ist $\binom{n}{1} = n$ nicht durch p^{r+1} teilbar, da $p \nmid m$.
Sei $s > 0$. Es ist

$$\binom{n}{p^s} = \frac{n!}{p^s!(n-p^s)!} = \frac{n(n-1)\cdots(n-(p^s-1))}{p^s(p^s-1)\cdots(p^s-(p^s-1))} = p^{r-s}m \prod_{k=1}^{p^s-1} \frac{n-k}{p^s-k}\,,$$

denn wegen $n = p^r m$ kann p^s gekürzt werden. Es ist $\prod_{k=1}^{p^s-1} \frac{n-k}{p^s-k} = \binom{n-1}{p^s-1} \in \mathbb{N}$.
Wegen der Eindeutigkeit der Primfaktorzerlegung ist nur noch zu zeigen:

$$p \nmid \prod_{k=1}^{p^s-1} \frac{n-k}{p^s-k}$$

Betrachte jeden Faktor $\frac{n-k}{p^s-k}$ einzeln: Schreibe $k = p^t \ell$ mit $p \nmid \ell$ und $0 \le t < s$.
Es ist $t < s$, da $k < p^s$. Daraus folgt

$$\begin{aligned} n - k &= p^r m - p^t \ell = p^t(p^{r-t}m - \ell)\,, \\ p^s - k &= p^s - p^t \ell = p^t(p^{s-t} - \ell)\,. \end{aligned}$$

Also sind $n-k$ und p^s-k beide durch p^t teilbar, aber $p^{r-t}m-\ell$ und $p^{s-t}-\ell$ sind nicht durch p teilbar, weil $p \nmid \ell$ und $s > t$. Also teilt p keinen der Faktoren $\frac{n-k}{p^s-k}$ und damit auch nicht das Produkt. $\square$

Definition.
Die *Ordnung* einer endlichen Gruppe G ist die Anzahl der Elemente von G.
Schreibweise: $|M|$ = Anzahl der Elemente einer Menge M (auch „$\#M$“ geschrieben).

2.2 Erster Sylowscher Satz

Satz.
Sei G eine endliche Gruppe der Ordnung $n = p^r m$, wobei p eine Primzahl sei, die m nicht teilt. Dann gibt es zu jedem s mit $1 \leq s \leq r$ eine Untergruppe von G der Ordnung p^s.

Beweis. Sei $M := \{T \subset G \mid |T| = p^s\}$. Dann operiert G auf M durch

$$G \times M \longrightarrow M\,,\ (g,T) \longmapsto gT\,,$$

wobei $gT = \{gt \mid t \in T\} \in M$ und gt die Verknüpfung in G ist.
Nach AGLA 10.24 ist der *Stabilisator*

$$\boxed{\mathrm{Stab}(T) := \{g \in G \mid gT = T\}}$$

eine Untergruppe von G für jedes $T \in M$, und es ist $|M| = \sum\limits_{B \text{ Bahn}} |B|$, wobei jede Bahn B die Form $B = GT := \{gT \mid g \in G\}$ mit $T \in M$ hat. Da $|M| = \binom{n}{p^s}$ gilt, und also $|M|$ nach 2.1 nicht durch p^{r-s+1} teilbar ist, gibt es ein $T \in M$ so, dass für die Bahn $B = GT$ gilt: $p^{r-s+1} \nmid |B|$. Dann ist $U := \mathrm{Stab}(T)$ die gesuchte Untergruppe.
Noch zu zeigen: $|U| = p^s$. Aus der Bahnformel (vgl. 2.3 unten) folgt

$$|GT| = \frac{|G|}{|U|} \tag{1}$$

$\Longrightarrow |GT| \leq p^{r-s}m$ nach Wahl der Bahn B
$\Longrightarrow p^{r-s}mp^s = \frac{|G|}{|U|}|U| \underset{(1)}{=} |GT| \cdot |U| \leq p^{r-s}m \cdot |U|$
$\Longrightarrow \boxed{p^s \leq |U|}$.
Sei $t \in T \Longrightarrow Ut \subset T$ nach Definition von $\mathrm{Stab}(T) = U$.
$\Longrightarrow |U| = |Ut| \leq |T| \underset{\text{da } T \in M}{=} p^s \Longrightarrow \boxed{|U| \leq p^s}$. □

2.3 Die Bahnformel

Sei G eine endliche Gruppe, die auf einer nichtleeren Menge X *operiere*, d.h. es gebe eine Abbildung

$$G \times X \longrightarrow X\,,\ (g,x) \longmapsto g \cdot x\,,$$

mit folgenden Eigenschaften:

(1) $e \cdot x = x \;\forall\, x \in X$, wobei e das neutrale Element in G sei,

(2) $(gg') \cdot x = g \cdot (g' \cdot x)\ \forall\, x \in X\ ,\ g, g' \in G\,.$

Es sei $G \cdot x := \{g \cdot x \mid g \in G\}$ die *Bahn von* $x \in X$,
und $\mathrm{Stab}(x) := \{g \in G \mid g \cdot x = x\}$ der *Stabilisator von* $x \in X$.
Dann gilt $|X| = \sum |B|$, wobei B die verschiedenen Bahnen von X durchläuft (vgl. AGLA 10.24). Ferner gilt:

Satz.
Es ist Stab(x) *eine Untergruppe von* G *(nach AGLA 10.24), und es gilt die* Bahnformel

$$|G \cdot x| = \frac{|G|}{|\mathrm{Stab}(x)|} \qquad \textit{für jedes } x \in X\,.$$

Beweis. Allgemein heißt die Anzahl der Linksnebenklassen gH, wobei H eine Untergruppe von G ist, der *Index von* H *in* G (Schreibweise: $(G : H)$). Es gilt:

$$\begin{aligned} |G \cdot x| &= (G : \mathrm{Stab}(x)) && \text{nach AGLA 10.24 (3)} \\ &= \frac{|G|}{|\mathrm{Stab}(x)|} && \text{nach der Abzählformel in AGLA 10.10.} \end{aligned}$$

□

Definition.
Sei G eine Gruppe mit neutralem Element e, und sei $a \in G$. Dann ist die *Ordnung von* a die kleinste natürliche Zahl k mit der Eigenschaft $a^k = e$ oder ∞, falls es ein solches k nicht gibt.

2.4 Satz von Cauchy

Satz.
Ist G *eine endliche Gruppe und* p *eine Primzahl, die die Ordnung von* G *teilt, dann enthält* G *ein Element der Ordnung* p*.*

Beweis. Nach dem ersten Sylowschen Satz 2.2 enthält G eine Untergruppe H der Ordnung p. Nach dem Satz von Lagrange (vgl. AGLA 10.13) teilt die Ordnung eines Elementes einer Gruppe stets die Gruppenordnung.
Da $|H| = p$ eine Primzahl ist, enthält H ein Element der Ordnung p. □

2.5 Gruppen der Ordnung 6

Satz.
Bis auf Isomorphie gibt es genau zwei Gruppen der Ordnung 6 *.*

Beweis. Sei G eine Gruppe der Ordnung $|G| = 3 \cdot 2$.
$\underset{2.4}{\Longrightarrow}$ G enthält ein Element a der Ordnung 3 und ein Element b der Ordnung 2.
$\Longrightarrow G = \{e, a, a^2, b, ab, a^2b\}$, da $|G| = 6$ und diese Elemente alle verschieden sind.

$$\begin{aligned}(\text{z.B. } & ab = a^2b \Longrightarrow b = ab \Longrightarrow e = a \text{ Widerspruch}\\ & a^2 = b \Longrightarrow a^4 = b^2 \Longrightarrow a = e, \text{ da } a^3 = b^2 = e \text{ Widerspruch})\end{aligned}$$

Es ist $ba \in G$, da G Gruppe

$$\Longrightarrow ba = ab \qquad \text{oder} \qquad ba = a^2b\,,$$

denn alle anderen Möglichkeiten führen zum Widerspruch:
$ba \neq b$, weil sonst $a = e$ wäre,
$ba \neq e$, da sonst $a = b^{-1} = b$ und also $\operatorname{ord}(a) = 2$ wäre,
$ba \neq a$, weil sonst $b = e$ wäre,
$ba \neq a^2$, weil sonst $b = a$ wäre.
Damit erhalten wir höchstens zwei Möglichkeiten, die Gruppentafel für G aufzustellen, nämlich

1. mit den Relationen $a^3 = e,\ b^2 = e,\ ba = ab$
2. mit den Relationen $a^3 = e,\ b^2 = e,\ ba = a^2b$

Da es bis auf Isomorphie mindestens zwei Gruppen der Ordnung 6 gibt, nämlich die abelsche Gruppe $\mathbb{Z}/6\mathbb{Z}$ und die Diedergruppe mit 6 Elementen, folgt die Behauptung. □

2.6 p-Gruppen

Definition.
Sei p eine Primzahl. Eine Gruppe G heißt *p-Gruppe*, falls die Ordnung eines jeden Elementes von G eine p-Potenz ist.

Satz.
Ist G eine endliche Gruppe, so gilt:
G ist eine p-Gruppe $\Longleftrightarrow$ $|G|$ ist eine p-Potenz.

Beweis. „$\Longrightarrow$“: Wenn es eine Primzahl $q \neq p$ gäbe, die $|G|$ teilt, so würde G nach 2.4 ein Element der Ordnung q enthalten und also keine p-Gruppe sein.

„$\Longleftarrow$“: folgt aus dem Satz von Lagrange (AGLA 10.13).

□

2.7 p-Sylowgruppen

Definition.
Sei G eine Gruppe der Ordnung $n = p^r m$, wobei p eine Primzahl sei, die m nicht teilt, und sei $r > 0$. Jede Untergruppe von G der Ordnung p^r heißt dann eine *p-Sylowgruppe.*

- Nach dem ersten Sylowschen Satz 2.2 gibt es zu jedem Primteiler p von $|G|$ eine p-Sylowgruppe in G (Fall $r = s$ in 2.2).
- Ist H eine p-Sylowgruppe, so ist der Index $(G : H)$ nicht durch p teilbar (denn $(G : H) = \frac{|G|}{|H|} = \frac{p^r m}{p^r} = m$ nach AGLA 10.10 und da $p \nmid m$).

2.8 Zweiter Sylowscher Satz

Satz.
Seien G eine endliche Gruppe, H eine p-Sylowgruppe in G und U eine Untergruppe von G der Ordnung p^s mit $s \geq 0$. Dann gibt es $g \in G$ so, dass $U \subset gHg^{-1}$ gilt.

Beweis. Sei $M = \{gH \mid g \in G\}$ die Menge der Linksnebenklassen von H.
$\Longrightarrow |M| = (G : H) \underset{2.7}{=} m$ mit $p \nmid m$.
Die Gruppe U operiert auf M durch

$$U \times M \longrightarrow M\,,\ (u, gH) \longmapsto ugH\,.$$

Da $p \nmid m = \sum\limits_{B \text{ Bahn}} |B|$ gilt, folgt

$$\exists \text{ Bahn } \ B := \{ugH \mid u \in U\} \text{ mit } p \nmid |B| \text{ und einem } g \in G\,.$$

Andererseits folgt aus der Bahnformel
$|B| \cdot |\mathrm{Stab}(gH)| \underset{2.3}{=} |U| = p^s \Longrightarrow |B| = 1$ nach Wahl von B.
$\Longrightarrow B := \{ugH \mid u \in U\} = \{gH\}$
$\Longrightarrow ugH = gH \quad \forall\, u \in U$
$\Longrightarrow ugH \ni uge = ug \in gH \quad \forall\, u \in U$
$\Longrightarrow u \in gHg^{-1} \quad \forall\, u \in U\,.$ $\square$

2.9 Folgerungen

Korollar.

(a) *Ist eine Untergruppe U von G eine p-Gruppe, so ist U in einer p-Sylowgruppe von G enthalten.*

(b) *Je zwei p-Sylowgruppen sind konjugiert in G*
(d.h. $\exists\, g \in G$ mit $H' = gHg^{-1}$ für p-Sylowgruppen H, H' in G).

(c) *Eine p-Sylowgruppe H ist genau dann Normalteiler in G, wenn sie die einzige p-Sylowgruppe in G ist.*

Beweis. (a) Nach 2.2 gibt es eine p-Sylowgruppe H in G.
Nach 2.8 ist $U \subset gHg^{-1}$ für ein $g \in G$. Da $|H| = |gHg^{-1}|$ gilt, ist auch gHg^{-1} eine p-Sylowgruppe in G.

(b) In 2.8 sei auch U eine p-Sylowgruppe in G. Dann folgt

$$U \subset gHg^{-1} \text{ und } |U| = \left|gHg^{-1}\right| \Longrightarrow U = gHg^{-1}.$$

(c) $H \lhd G \underset{1.1}{\Longrightarrow} gHg^{-1} = H \;\forall\, g \in G$
$\underset{(b)}{\Longrightarrow} H$ ist die einzige p-Sylowgruppe in G.
Da gHg^{-1} für alle $g \in G$ eine p-Sylowgruppe ist, gilt „$\Longleftarrow$“.

□

2.10 Der Normalisator einer Untergruppe

Satz.
Sei U eine Untergruppe einer Gruppe G. Dann heißt

$$N(U) := \{g \in G \mid gUg^{-1} = U\}$$

der Normalisator von U in G. *Es gelten:*

(i) *$N(U)$ ist eine Untergruppe von G.*

(ii) *Die Anzahl der zu U konjugierten Untergruppen ist gleich dem Index $(G : N(U))$.*

(iii) *$U \lhd N(U)$.*

(iv) *$N(U)$ ist die größte Untergruppe von G, in der U Normalteiler ist. Insbesondere gilt:*

$$\boxed{N(U) = G} \quad \Longleftrightarrow \quad \boxed{U \lhd G}.$$

Beweis. Sei $M = \{T \subset G\}$. Dann operiert G auf M durch Konjugation

$$G \times M \longrightarrow M, \; (g, T) \longmapsto gTg^{-1}$$

$\Longrightarrow N(U) = \mathrm{Stab}(U)$
$\Longrightarrow N(U)$ ist Untergruppe von G (vgl. 2.3)
$\Longrightarrow |\{gUg^{-1} \mid g \in G\}| = \frac{|G|}{|N(U)|}$ nach der Bahnformel in 2.3
$\Longrightarrow$ (ii).
Es ist $U \subset N(U)$, da $uUu^{-1} = U \;\forall\, u \in U$ gilt. (iii) und (iv) folgen nach Definition von $N(U)$ und Definition eines Normalteilers. □

2.11 Dritter Sylowscher Satz

Satz.
Sei G eine Gruppe der Ordnung $n = p^r m$, wobei $r > 0$ und p eine Primzahl sei, die m nicht teilt. Sei n_p die Anzahl der p-Sylowgruppen in G. Dann ist n_p ein Teiler von m, und $n_p - 1$ ist durch p teilbar (Schreibweise: $n_p \mid m$ und $n_p \equiv 1 \bmod p$).

Beweis. Sei H eine p-Sylowgruppe in G.
$\underset{2.9}{\Longrightarrow}$ Alle p-Sylowgruppen sind zu H konjugiert in G.
$\Longrightarrow n_p = (G : N(H))$ nach 2.10. Es gilt

$$m \underset{2.7}{=} \frac{|G|}{|H|} = \underbrace{\frac{|G|}{|N(H)|}}_{(G:N(H))} \cdot \frac{|N(H)|}{|H|} = n_p \frac{|N(H)|}{|H|} = n_p \cdot (N(H) : H)$$

$\Longrightarrow n_p \mid m$.
Sei $M = \{H_1, \ldots, H_{n_p}\}$ die Menge der p-Sylowgruppen in G,
und sei $H = H_1$. Dann operiert H auf M durch

$$H \times M \longrightarrow M\,,\ (h, H_i) \longmapsto hH_ih^{-1}\,.$$

Jedes H_i liegt in einer Bahn $\boxed{B_i = \{hH_ih^{-1} \mid h \in H\}}$ (vgl. AGLA 10.24).
Wir zeigen: Es gibt genau eine Bahn B_i mit $|B_i| = 1$ und $p \mid |B_j|$ für $j \neq i$.
Da $n_p = |M| = \sum_{B \text{ Bahn}} |B|$ gilt, folgt dann die zweite Behauptung. Es gilt:

$$|B_i| = 1 \iff B_i = \{H_i\} \iff hH_ih^{-1} = H_i \;\forall\, h \in H \iff H \subset N(H_i).$$

Sei nun $|B_i| = 1 \underset{2.10}{\Longrightarrow} H, H_i \subset N(H_i)$
$\Longrightarrow H, H_i$ sind p-Sylowgruppen in $N(H_i)$
$\Longrightarrow H_i = H$, da $H_i \lhd N(H_i)$ nach 2.10 und also H_i nach 2.9 c) die einzige p-Sylowgruppe in $N(H_i)$ ist.
Es gibt also nur eine Bahn der Länge 1, nämlich $\{H\}$. Ist B_j eine Bahn mit $|B_j| > 1$, so ist $|B_j|$ durch p teilbar, denn aus der Bahnformel 2.3 folgt

$$p^r \underset{2.7}{=} |H| \underset{2.3}{=} |B_j| \cdot \mathrm{Stab}(H_j)\,.$$

□

Satz (Lagrange).
Die Ordnung einer Untergruppe teilt die Gruppenordnung (vgl. AGLA 10.13).

Folgerung.
Jede Gruppe der Primzahlordnung p ist isomorph zur additiven Gruppe $\mathbb{Z}/p\mathbb{Z}$ (vgl. AGLA 10.14).

2.12 Gruppen der Ordnung 15

Satz.
Bis auf Isomorphie gibt es genau eine Gruppe der Ordnung 15 *,*
nämlich $\mathbb{Z}/15\mathbb{Z}$ *.*

Beweis. Sei G eine Gruppe der Ordnung $5 \cdot 3$, und seien n_5 die Anzahl der 5-Sylowgruppen und n_3 die Anzahl der 3-Sylowgruppen in G. Nach 2.11 gilt $n_5 \mid 3$, also $n_5 = 3$ oder 1, und $n_5 - 1$ ist durch 5 teilbar
$\Longrightarrow \boxed{n_5 = 1}$, da $3 < 5$
Analog: $n_3 \mid 5$, also $n_3 = 5$ oder 1, und $n_3 - 1$ ist durch 3 teilbar
$\Longrightarrow \boxed{n_3 = 1}$.
Also gibt es in G genau eine 5-Sylowgruppe U und genau eine 3-Sylowgruppe V
$\underset{2.9\text{ c)}}{\Longrightarrow} U, V$ sind Normalteiler in G
$\Longrightarrow UV$ ist Untergruppe von G (nach 1.4 a))
$\Longrightarrow UV = G$, denn $|UV|$ teilt nach dem Satz von Lagrange $5 \cdot 3 = |G|$ und es ist $|UV| > 5$.
Es ist $U \cap V = \{e\}$, da U und V beide nur $\{e\}$ als echte Untergruppe besitzen.

$$\Longrightarrow G = UV \underset{3.7}{\simeq} U \times V \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}\,.$$

Wende dieses Resultat auf die Gruppe $\mathbb{Z}/15\mathbb{Z}$ an.
Dann folgt $\mathbb{Z}/15\mathbb{Z} \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Also ist $\mathbb{Z}/15\mathbb{Z} \simeq G$ für jede Gruppe G der Ordnung 15. □

2.13 Übungsaufgaben 8 – 10

Aufgabe 8. Seien p und q zwei Primzahlen, wobei $p > q$ gelte und $p - 1$ nicht durch q teilbar sei. Man zeige, dass es bis auf Isomorphie genau eine Gruppe der Ordnung pq gibt.

Aufgabe 9. Man ermittle, wieviele Elemente der Ordnung 5 eine Gruppe der Ordnung 20 enthält.

Definition. Eine Gruppe $G \neq \{e\}$ heißt *einfach*, wenn sie keine echten Normalteiler besitzt, d.h. wenn $\{e\}$ und G die einzigen Normalteiler in G sind.

Aufgabe 10. Man beweise, dass eine Gruppe der Ordnung pq, wobei p und q Primzahlen sind, nicht einfach ist.

3 Strukturaussagen über einige Gruppen

Sei G eine endliche Gruppe.

3.1 Die Klassengleichung

Definition.
Betrachte den Spezialfall, dass G per *Konjugation* auf sich selbst operiert:

$$G \times G \longrightarrow G\,,\ (g,x) \longmapsto gxg^{-1}.$$

Die *Bahn* von $x \in G$ ist dann die *Konjugationsklasse*

$$\boxed{K(x) := \{gxg^{-1} \mid g \in G\}}$$

in G. Der *Stabilisator* von $x \in G$ ist dann der *Zentralisator*

$$\boxed{Z_x := \{g \in G \mid gxg^{-1} = x\}}\,.$$

Die Bahnformel lautet nun:

$$\boxed{|K(x)| \underset{2.3}{=} \frac{|G|}{|Z_x|}}\,.$$

(Dabei ist $\frac{|G|}{|Z_x|} \underset{\text{AGLA 10.10}}{=} (G : Z_x)$ der Index von Z_x in G.)

Klassengleichung.
Seien $K(x_1),\ldots,K(x_k)$ die verschiedenen Konjugationsklassen in G. Dann gilt:

$$\boxed{|G| = \sum_{i=1}^{k} |K(x_i)| = \sum_{i=1}^{k} (G : Z_{x_i})}\,.$$

Die Klassengleichung läßt sich auch in der Form

$$\boxed{|G| = |Z(G)| + \sum_{(G:Z_{x_i})>1} (G : Z_{x_i})}$$

schreiben, wobei $Z(G) := \{x \in G \mid gx = xg\ \forall\, g \in G\}$ das Zentrum *von G bezeichnet.*

Beweis. Nach AGLA 10.24 zerfällt G disjunkt in Bahnen, also

$$|G| = \sum_{B \text{ Bahn}} |B| = \sum_{i=1}^{k} |K(x_i)| \ .$$

Da $|K(x_i)| = (G : Z_{x_i})$ gilt, folgt auch die zweite Gleichung:
Für $x \in G$ gilt

$$x \in Z(G) \iff Z_x = G \iff 1 = (G : Z_x) = |K(x)| \iff K(x) = \{x\} \, .$$

In der Summe $|G| = \sum\limits_{i=1}^{k} |K(x_i)|$ treten also genau $|Z(G)|$ Summanden 1 auf, die übrigen Summanden sind größer 1 . □

3.2 Das Zentrum einer p-Gruppe ist nicht-trivial

Satz.
Sei p eine Primzahl, und sei $|G| = p^r$ mit $r \geq 1$.
Dann ist $|Z(G)| = p^s$ mit $s \geq 1$.

Beweis. Es ist $p^r = |G| = |Z(G)| + \sum\limits_{(G:Z_{x_i})>1} (G : Z_{x_i})$ nach 3.1
$\Longrightarrow p \mid |Z(G)|$, da p jeden Index $(G : Z_{x_i})$ teilt
(wegen $p^r = |G| = |Z_{x_i}| \cdot (G : Z_{x_i})$). □

3.3 Existenz von Normalteilern in p-Gruppen

Satz.
Sei p eine Primzahl, und sei $|G| = p^r$ mit $r \geq 1$. Dann besitzt G einen Normalteiler der Ordnung p^{r-1}.

Beweis. Induktion nach r.
Sei $r = 1 \Longrightarrow$ Behauptung, da $\{e\} \triangleleft G$.
Sei $r > 1 \Longrightarrow |Z(G)| = p^s$ mit $s \geq 1$ nach 3.2
$\Longrightarrow Z(G)$ hat eine Untergruppe N mit $|N| = p$ nach dem ersten Sylowschen Satz 2.2.
Es ist $N \triangleleft G'$ für jede Untergruppe G' von G , die N enthält,
(denn die Normalteilerbedingung

$$\boxed{gNg^{-1} \subset N \quad \forall g \in G'}$$

ist erfüllt; es gilt sogar $gxg^{-1} = x \;\forall\, x \in N$, $g \in G'$, weil $N \subset Z(G)$).
Die Faktorgruppe G/N hat die Ordnung

$$|G/N| = \frac{|G|}{|N|} = \frac{p^r}{p} = p^{r-1}.$$

Nach Induktionsvoraussetzung hat G/N einen Normalteiler $\overline{M}$ der Ordnung p^{r-2}. Sei $\pi\colon G \longrightarrow G/N\,,\ g \longmapsto gN\,,$ der kanonische Homomorphismus, und sei $M = \pi^{-1}\left(\overline{M}\right) := \{g \in G \mid \pi(g) \in \overline{M}\}$
$\Longrightarrow M \lhd G\,,$ denn M ist Untergruppe von $G\,,$ und es ist
$\pi(gxg^{-1}) = \pi(g)\pi(x)\pi(g)^{-1} \in \overline{M},$ da $\overline{M} \lhd G/N$
$\Longrightarrow gxg^{-1} \in \pi^{-1}(\overline{M}) = M \quad \forall\, g \in G\,,\ x \in M\,,$ also $M \lhd G\,.$
Es ist $N \subset M$ (da $\pi(e) = N$ das neutrale Element in $\overline{M}$ ist)
$\Longrightarrow N \lhd M$ (s. oben) und $M/N = \overline{M}\,.$ Es folgt

$$p^{r-2} = \left|\overline{M}\right| = \frac{|M|}{|N|} = \frac{|M|}{p} \Longrightarrow |M| = p^{r-1}.$$

□

3.4 Zyklische Gruppen

Definition.
Eine *zyklische* Gruppe ist eine Gruppe, die von einem Element erzeugt wird. Ist $|G| =: n < \infty$, so gilt

$$\boxed{G \text{ zyklisch}} \quad \Longleftrightarrow \quad \boxed{G \text{ enthält ein Element } a \text{ der Ordnung } n}$$

Wir schreiben dann $G = \{e, a, \ldots, a^{n-1}\}$ (vgl. AGLA 10.12).
Ferner gelten:

- Jede endliche zyklische Gruppe G ist isomorph zu $\mathbb{Z}/|G|\mathbb{Z}$ (AGLA 10.16).
- Jede Gruppe der Primzahlordnung p ist zyklisch und also isomorph zur (additiven) Gruppe $\mathbb{Z}/p\mathbb{Z}$ (AGLA 10.14).

3.5 Gruppe der Ordnung p^2

Satz.
Sei p eine Primzahl. Dann ist jede Gruppe der Ordnung p^2 kommutativ, und bis auf Isomorphie gibt es genau zwei Gruppen der Ordnung p^2, nämlich $\mathbb{Z}/p^2\mathbb{Z}$ und $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Beweis. Sei $Z(G) = \{x \in G \mid gx = xg\ \forall g \in G\}$ das Zentrum von G.
$\Longrightarrow |Z(G)| = p$ oder p^2 nach 3.2

1.Fall $|Z(G)| = p^2 \Longrightarrow G$ ist kommutativ.

2.Fall $|Z(G)| = p \Longrightarrow |G/Z(G)| = \frac{p^2}{p} = p$
$\Longrightarrow G/Z(G)$ ist zyklisch nach 3.4.
$\Longrightarrow G$ kommutativ nach Aufgabe 11.
$\Longrightarrow G = Z(G) \Longrightarrow$ Widerspruch. Dieser Fall kann also nicht eintreten.

Zeige nun die zweite Behauptung. Da die Ordnung eines jeden Elementes von G die Gruppenordnung $|G| = p^2$ teilt, sind nur zwei Fälle möglich:

1. Es gibt ein Element der Ordnung p^2 in G. Dann ist G zyklisch und $G \simeq \mathbb{Z}/p^2\mathbb{Z}$ nach 3.4

2. Jedes Element $\neq e$ aus G hat die Ordnung p. Wähle $a \in G$ mit $a \neq e$
$\Longrightarrow U = \{e, a, \ldots, a^{p-1}\}$ ist Untergruppe von G der Ordnung p (AGLA 10.12).
$\Longrightarrow U \triangleleft G$, denn in einer abelschen Gruppe ist jede Untergruppe Normalteiler.
Wähle $b \in G \setminus U$ und setze $V = \{e, b, \ldots, b^{p-1}\}$
$\Longrightarrow |V| = p$ und $V \triangleleft G$ (analog)
$\Longrightarrow UV$ ist Untergruppe von G nach 1.4(a)
$\Longrightarrow UV = G$, da $|UV| > p$ und $|UV|$ ein Teiler von $|G| = p^2$ ist.
Es ist $|U \cap V| = 1$, denn wäre $|U \cap V| = p$, so wäre $U = U \cap V = V$, was $b \notin U$ widerspräche.
$\Longrightarrow U \cap V = \{e\} \underset{3.7}{\Longrightarrow} G \simeq U \times V \underset{3.4}{\simeq} \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

□

3.6 Gruppen der Ordnung $2p$

Satz.
Sei p eine Primzahl $\neq 2$. Dann gibt es bis auf Isomorphie genau zwei Gruppen der Ordnung $2p$, nämlich die zyklische Gruppe $\mathbb{Z}/2p\mathbb{Z}$ und die (nicht abelsche) Diedergruppe D_p mit $2p$ Elementen.

Beweis. Sei $|G| = 2p$ und $p > 2$. Dann besitzt G eine p-Sylowgruppe

$$\boxed{U = \{e, a, \ldots, a^{p-1}\}}$$

nach 2.7 und 3.4. Sei n_p die Anzahl der p-Sylowgruppen in G
$\underset{2.11}{\Longrightarrow} n_p \mid 2$, also $n_p = 1$ oder 2, und $n_p - 1$ ist durch p teilbar.
$\Longrightarrow \boxed{n_p = 1} \underset{2.9}{\Longrightarrow} U \triangleleft G$.
Für die Anzahl n_2 der 2-Sylowgruppen in G gilt $n_2 \mid p$, also $n_2 = 1$ oder p (nach 2.11).

1. Fall $\boxed{n_2 = 1}$ Dann gibt es genau eine 2-Sylowgruppe $V = \{e, b\}$ in G.
$\underset{2.9(c)}{\Longrightarrow} V \lhd G$. Es ist $U \cap V = \{e\}$, (da $V = \{e, b\}$ und $b \notin U$).
$\underset{3.7}{\Longrightarrow} ab = ba$. Da $\operatorname{ord}(b) = 2$ und $\operatorname{ord}(a) = p$ ungerade ist, folgt $\operatorname{ord}(ab) = 2p = |G| \underset{3.4}{\Longrightarrow} G$ ist zyklisch.

2. Fall $\boxed{n_2 = p}$. Für jedes $x \in G \setminus U$ gilt $\operatorname{ord}(x) = 2$ oder $2p$ (denn U ist die einzige Untergruppe der Ordnung p in G).
Angenommen, es gibt ein $x \in G$ mit $\operatorname{ord}(x) = 2p$. Dann ist G zyklisch nach 3.4, also abelsch und die 2-Sylowgruppe ist Normalteiler, woraus $n_2 = 1$ nach 2.9(c) folgt im Widerspruch zu $n_2 = p$.
Also hat jedes Element aus $G \setminus U$ die Ordnung 2. Wähle $b \in G \setminus U$.
Dann ist $G = \{e, a, \ldots, a^{p-1}, b, ba, \ldots, ba^{p-1}\}$ die Diedergruppe D_p. Es ist $(ab)(ab) = e$ und also $(ab) = (ab)^{-1} = b^{-1}a^{-1} = ba^{p-1}$.

$\square$

3.7 Direkte Produkte von Normalteilern

Satz.
Seien $N_1, \ldots, N_k$ Normalteiler in einer Gruppe G. Es sei

$$\boxed{N_i \cap (N_1 \cdot N_2 \cdot \ldots \cdot N_{i-1} \cdot N_{i+1} \cdot \ldots \cdot N_k) = \{e\} \quad \forall i = 1, \ldots, k}.$$

Für $i \neq j$ gilt dann:

$$\boxed{x_i x_j = x_j x_i \quad \forall x_i \in N_i \text{ und } x_j \in N_j}$$

und die Produktabbildung

$$\pi\colon N_1 \times \cdots \times N_k \longrightarrow G,\ (x_1, \ldots, x_k) \longmapsto x_1 \cdots x_k$$

ist ein injektiver Gruppenhomomorphismus.

Beweis. Es ist

$$\begin{aligned}(x_i x_j)(x_j x_i)^{-1} &= (\underbrace{x_i x_j x_i^{-1}}_{\in N_j \lhd G}) x_j^{-1} \in N_j \\ &= x_i (\underbrace{x_j x_i^{-1} x_j^{-1}}_{\in N_i \lhd G}) \in N_i\end{aligned}$$

$$\begin{aligned}
&\Longrightarrow (x_i x_j)(x_j x_i)^{-1} \in N_i \cap N_j \subset N_i \cap N_1 \cdots N_{i-1} N_{i+1} \cdots N_k) \underset{\text{Vor.}}{=} \{e\} \\
&\Longrightarrow x_i x_j = x_j x_i \quad \text{für } i \neq j \\
&\Longrightarrow \pi((x_1, \ldots, x_k) \cdot (x_1', \ldots, x_k')) = \pi(x_1 x_1', \ldots, x_k x_k') \\
&= x_1 x_1' \cdots x_k x_k' = x_1 \cdots x_k \cdot x_1' \cdots x_k' \\
&= \pi(x_1, \ldots, x_k) \cdot \pi(x_1', \ldots, x_k')
\end{aligned}$$

Also ist π ein Homomorphismus, und π ist injektiv,
denn sei $e = \pi(x_1, \ldots, x_k) = x_1 \cdots x_k$
$\Longrightarrow x_i^{-1} = x_1 \cdots x_{i-1} x_{i+1} \cdots x_k \in N_i \cap (N_1 \cdots N_{i-1} N_{i+1} \cdots N_k) = \{e\}$
$\Longrightarrow x_i^{-1} = e \Longrightarrow x_i = e \quad \forall\, i = 1, \ldots, k$ □

Bemerkung.
Sei G eine endliche Gruppe. Unter den Voraussetzungen des Satzes ist $N_1 \times \cdots \times N_k \simeq \operatorname{bild}(\pi)$, und daher $|N_1| \cdots |N_k| = |N_1 \times \cdots \times N_k| = |\operatorname{bild}(\pi)|$.
Da $\operatorname{bild}(\pi)$ eine Untergruppe von G ist, folgt:
Wenn zusätzlich $|N_1| \cdot \ldots \cdot |N_k| = |G|$ ist, so ist π ein Isomorphismus.

3.8 Endliche abelsche Gruppen (Eine Ergänzung von Michael Adam)

Die Struktur der endlichen abelschen Gruppen kann mit den bisherigen Mitteln bestimmt werden. Das soll hier heißen, dass eine vollständige Liste von Vertretern für die Isomorphieklassen der endlichen abelschen Gruppen angegeben wird. Der Isomorphismus zu einem solchen Vertreter ist aber in der Regel nicht eindeutig bestimmt. Ich schreibe abelsche Gruppen im folgenden immer additiv.

Behauptung 1.
Jede endliche abelsche Gruppe ist Produkt ihrer Sylowgruppen.

Beweis. Sei $\#(A) = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ mit paarweise verschiedenen Primzahlen $p_1, \ldots, p_r$. Da A abelsch ist, sind alle Untergruppen Normalteiler, insbesondere die Sylowgruppen. Folglich gibt es zu jedem p_i genau eine p_i-Sylowgruppe A_i in A; es ist $\#(A_i) = p_i^{e_i}$. Weil die Ordnung eines Elementes von $A_1 \cap A_2$ sowohl $p_1^{e_1}$ als auch $p_2^{e_2}$ teilen muss und p_1 und p_2 teilerfremd sind, gilt $A_1 \cap A_2 = \{0\}$. Damit ist die Additionsabbildung $A_1 \times A_2 \to A, (a_1, a_2) \mapsto a_1 + a_2$ ein injektiver Gruppenhomomorphismus, und das Bild $A_1 + A_2$ ist insbesondere eine Untergruppe der Ordnung $p_1^{e_1} \cdot p_2^{e_2}$. Induktiv fortfahrend erhält man, dass

$$\mu : A_1 \times \cdots \times A_r \to A, \ (a_1, \ldots, a_r) \mapsto a_1 + \ldots + a_r$$

ein injektiver Gruppenhomomorphismus ist. Weil die beiden Gruppen die gleiche Ordnung haben, ist μ sogar ein Isomorphismus. □

Der zweite Schritt ist nun, abelsche p-Gruppen weiter zu zerlegen.

Behauptung 2.
Sei p eine Primzahl und A eine abelsche p-Gruppe. Dann gibt es natürliche Zahlen $e_1, \ldots, e_n$, so dass

$$A \cong \mathbb{Z}/p^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{e_n}\mathbb{Z}.$$

Die Folge $e_1, \ldots, e_n$ ist bis auf Reihenfolge eindeutig.

Wenn man die beiden Behauptungen zusammennimmt, erhält man, dass jede endliche abelsche Gruppe isomorph zu einem Produkt von Gruppen $\mathbb{Z}/p^e\mathbb{Z}$ ist für verschiedene Primzahlen p und Exponenten e. Diese Aussage könnte man **Hauptsatz über endliche abelsche Gruppen** nennen. Der Beweis von 2 und damit des Hauptsatzes erfordert keine weiteren Mittel, aber ich verschiebe ihn auf Abschnitt 10.12, wo ich als weiteren Einschub den allgemeineren Hauptsatz über endlich *erzeugte* abelsche Gruppen beweisen werde.

3.9 Übungsaufgaben 11 – 14

Aufgabe 11. Sei G eine Gruppe, und sei $Z := \{x \in G \mid gx = xg \; \forall\, g \in G\}$ das *Zentrum von G*. Man zeige:

(a) Wenn G/Z zyklisch ist, dann ist G kommutativ (und also $G = Z$).

(b) Das Zentrum einer nicht-abelschen Gruppe der Ordnung p^3 hat stets die Ordnung p. Hierbei sei p eine Primzahl.

Aufgabe 12. Man zeige, dass es bis auf Isomorphie genau eine Gruppe der Ordnung 1001 gibt.

Aufgabe 13. Man zeige, dass jede Gruppe der Ordnung 200 einen abelschen Normalteiler $\neq \{e\}$ besitzt.

Aufgabe 14. Seien p und q zwei verschiedene Primzahlen. Man zeige, dass jede Gruppe G der Ordnung p^2q eine Sylowgruppe besitzt, die Normalteiler in G ist.

4 Auflösbare Gruppen

4.1 Definition einer auflösbaren Gruppe

Definition.
Eine Gruppe G heißt *auflösbar*, wenn es eine Kette

$$G = U_k \supset U_{k-1} \supset \cdots \supset U_1 \supset U_0 = \{e\}$$

von Untergruppen $U_0, \ldots, U_k$ von G gibt mit den Eigenschaften

(1) U_{i-1} ist Normalteiler in U_i $\forall\, i = 1, \ldots, k$

(2) Die Faktorgruppen U_i/U_{i-1} sind abelsch $\forall\, i = 1, \ldots, k$

4.2 Beispiele

- Jede abelsche Gruppe G ist auflösbar (da $G = G/\{e\}$ abelsch).
  Jede nichtabelsche, einfache Gruppe ist nicht auflösbar.
  (Dabei heißt eine Gruppe einfach, wenn sie außer sich selbst und $\{e\}$ keinen Normalteiler besitzt.)

Behauptung.
Jede endliche p-Gruppe ist auflösbar (p Primzahl).

Beweis. Sei U_k eine Gruppe der Ordnung p^k mit $k > 1$. Nach 3.3 gibt es eine Kette

$$U_k \triangleright U_{k-1} \triangleright \cdots \triangleright U_1 \triangleright U_0 = \{e\}$$

mit $|U_i/U_{i-1}| = p \quad \forall\, i = 1, \ldots, k$.
$\underset{3.4}{\Longrightarrow}$ U_i/U_{i-1} ist zyklisch, also abelsch, $\forall\, i = 1, \ldots, k$. □

4.3 Untergruppen und homomorphe Bilder auflösbarer Gruppen

Satz. (a) *Jede Untergruppe einer auflösbaren Gruppe ist auflösbar.*

(b) *Sei G eine auflösbare Gruppe, und sei $f\colon G \longrightarrow G'$ ein surjektiver Homomorphismus von Gruppen. Dann ist G' auflösbar. Insbesondere ist G/N auflösbar für jeden Normalteiler N in G.*

(c) *Ist N Normalteiler in einer Gruppe G und sind N und G/N auflösbar, so ist G auflösbar.*

Beweis. (a) Sei $U \subset G$ eine Untergruppe. Mit Hilfe einer Kette aus 4.1 erhält man eine Kette

$$U = U \cap U_k \supset U \cap U_{k-1} \supset \cdots \supset U \cap U_1 \supset U \cap U_0 = \{e\}$$

Da $U_{i-1} \lhd U_i \Longrightarrow U \cap U_{i-1} \lhd U \cap U_i$ für $i = 1, \ldots, k$. Nach dem ersten Noetherschen Isomorphiesatz 1.4 gilt:

$$(U \cap U_i)/(U \cap U_{i-1}) = (U \cap U_i)/(U \cap U_i \cap U_{i-1}) \underset{1.4}{\simeq} (U \cap U_i)U_{i-1}/U_{i-1}$$

Die letzte Gruppe ist als Untergruppe von $\underbrace{U_i/U_{i-1}}_{\text{abelsch nach Voraussetzung}}$ abelsch.

(b) Sei eine Kette von Untergruppen von G wie in 4.1 gegeben. Dann ist $G' = f(U_k) \supset f(U_{k-1}) \supset \cdots \supset f(U_1) \supset f(U_0) = \{e\}$ eine Kette von Untergruppen von G'. Nach 1.5 ist $f(U_{i-1})$ Normalteiler in $f(U_i)$, und f induziert einen surjektiven Homomorphismus

$$U_i/U_{i-1} \longrightarrow f(U_i)/f(U_{i-1}).$$

Da U_i/U_{i-1} abelsch, ist auch $f(U_i)/f(U_{i-1})$ abelsch.
Da der kanonische Homomorphismus $G \longrightarrow G/N, g \longmapsto gN$, surjektiv ist, folgt die zweite Behauptung in (b).

(c) Nach Voraussetzung gibt es zwei Ketten

$$N = N_k \rhd N_{k-1} \rhd \cdots \rhd N_1 \rhd N_0 = \{e\} \text{ und}$$
$$G/N = U_\ell/N \rhd U_{\ell-1}/N \rhd \cdots \rhd U_1/N \rhd U_0/N = \{N\},$$

wobei die Faktorgruppen N_i/N_{i-1} und $(U_i/N)/(U_{i-1}/N) \underset{1.7}{\simeq} U_i/U_{i-1}$ abelsch sind.

$$\Longrightarrow G = U_\ell \supset U_{\ell-1} \supset \cdots \supset U_1 \supset U_0 = N_k \supset N_{k-1} \supset \cdots \supset N_0 = \{e\}$$

erfüllt (1) und (2) in 4.1.

□

4.4 Verfeinerung von Normalreihen

Definition. Eine Kette $G = U_k \supset U_{k-1} \supset \cdots \supset U_1 \supset U_0 = \{e\}$ von Untergruppen $U_0, \ldots, U_k$ einer Gruppe G heißt *Normalreihe von* G, wenn U_{i-1} Normalteiler in U_i ist $\forall\, i = 1, \ldots, k$. Eine Gruppe ist also genau dann gemäß 4.1 auflösbar, wenn sie eine Normalreihe mit abelschen Faktorgruppen besitzt.

Satz. *Sei G eine endliche auflösbare Gruppe, und sei*

$$G = U_k \supsetneqq U_{k-1} \supsetneqq \cdots \supsetneqq U_1 \supsetneqq U_0 = \{e\}$$

irgendeine Normalreihe von G mit abelschen Faktorgruppen. Dann läßt sich diese Normalreihe zu einer Normalreihe verfeinern, deren Faktorgruppen von Primzahlordnung sind.

Beweis. Ist eine der Faktorgruppen U_i/U_{i-1} nicht von Primzahlordnung, so wähle $\bar{a} \in U_i/U_{i-1}$ mit $\bar{a} \neq e$ und gehe zu einer geeigneten Potenz $\bar{b} = \bar{a}^j$ über, wobei $\bar{b}$ Primzahlordnung hat.
$\Longrightarrow$ $\bar{b}$ erzeugt eine Untergruppe $\bar{H} \subsetneqq U_i/U_{i-1}$ von Primzahlordnung. Da U_i/U_{i-1} abelsch ist, gilt $\bar{H} \triangleleft U_i/U_{i-1}$.
Sei $H = \pi^{-1}(\bar{H})$, wobei $\pi\colon U_i \longrightarrow U_i/U_{i-1}$ kanonisch.
$\Longrightarrow$ $H \triangleleft U_i$ und $U_i \supsetneqq H \supsetneqq U_{i-1}$.
Füge H in die Normalreihe von G ein. Dann erhält man eine neue Normalreihe, deren Faktorgruppen abelsch sind, denn H/U_{i-1} ist als Untergruppe von U_i/U_{i-1} abelsch, und $U_i/H \underset{1.7}{\simeq} (U_i/U_{i-1})/(H/U_{i-1})$ ist abelsch. Da G endlich ist, kommt man durch Wiederholung dieses Verfahrens nach endlich vielen Schritten zu einer Normalreihe, deren sämtliche Faktorgruppen von Primzahlordnung sind. □

Bemerkung. Die Voraussetzung im Satz, daß alle Faktorgruppen abelsch seien, ist entbehrlich, wenn man noch den *Hauptsatz von Schreier über Normalreihen* anwendet, der hier ohne Beweis erwähnt sei:

Satz. *Je zwei Normalreihen*

$$\begin{aligned} G &= U_k \supset U_{k-1} \supset U_{k-2} \supset \cdots \supset U_1 \supset U_0 = \{e\} \\ G &= V_m \supset V_{m-1} \supset V_{m-2} \supset \cdots \supset V_1 \supset V_0 = \{e\} \end{aligned}$$

einer Gruppe G besitzen isomorphe Verfeinerungen

$$\begin{aligned} &G \supset \cdots \supset U_{k-1} \supset \cdots \supset U_{k-2} \supset \cdots \supset \{e\} \\ \simeq\ &G \supset \cdots \supset V_{m-1} \supset \cdots \supset V_{m-2} \supset \cdots \supset \{e\} \end{aligned}$$

Dabei heißen zwei Normalreihen isomorph*, wenn alle Faktorgruppen der einen Reihe zu den Faktorgruppen der anderen Reihe isomorph sind, wobei es aber nicht auf die Reihenfolge ankommt.*

Ist zum Beispiel $\langle a \rangle$ eine zyklische Gruppe der Ordnung 6, so sind die Normalreihen

$$\langle a \rangle \supset \langle a^2 \rangle \supset \{e\} \text{ und } \langle a \rangle \supset \langle a^3 \rangle \supset \{e\}$$

isomorph.

4.5 Kommutatorgruppen

Definition. Sei G eine Gruppe. Dann heißt

$$\boxed{[a,b] := aba^{-1}b^{-1} \text{ mit } a,b \in G}$$

der *Kommutator von a und b*. Es ist $ab = [a,b] \cdot ba$. Das Produkt von zwei Kommutatoren ist im allgemeinen kein Kommutator mehr, aber es gilt

$$\boxed{[a,b]^{-1} = [b,a] \quad \forall a,b \in G}$$

Die von allen Kommutatoren $[a,b]$ mit $a,b \in G$ erzeugte Untergruppe von G heißt die *Kommutatorgruppe von G*. Sie besteht aus allen (endlichen) Produkten von Kommutatoren aus G und wird als $[G,G]$ geschrieben.

Bemerkung. Es ist $[G,G]$ Normalteiler in G und $G/[G,G]$ abelsch. Es ist $[G,G]$ sogar der kleinste Normalteiler unter allen Normalteilern N in G, für die $G/[G,G]$ abelsch ist.

Beweis. Benutze $\boxed{ab = ag^{-1}gb}$ und $\boxed{(gag^{-1})^{-1} = ga^{-1}g^{-1} \quad \forall\, a,g \in G}$.
Es folgt:

$$g[a,b]g^{-1} = gaba^{-1}b^{-1}g^{-1} = gag^{-1}gbg^{-1}ga^{-1}g^{-1}gb^{-1}g^{-1} = [gag^{-1}, gbg^{-1}]$$

Da $[G,G]$ aus Produkten von Kommutatoren besteht, folgt
$g[G,G]g^{-1} \subset [G,G]\,\forall\, g \in G$ und also $[G,G] \lhd G$.
Ist $N \lhd G$ und G/N abelsch, so folgt $[a,b] \in N\ \forall\, a,b \in G \Longrightarrow [G,G] \subset N$. $\square$

4.6 Beispiele

1. Es gilt: G abelsch $\Longleftrightarrow [G,G] = \{e\}$

2. G nicht-abelsche, einfache Gruppe. Dann ist $[G,G] = G$

3. Seien K ein Körper, $B_n(K)$ die Gruppe der oberen Dreiecksmatrizen in $GL_n(K)$ und $U_n(K)$ die Untergruppe der oberen Dreiecksmatrizen mit Diagonalelementen, die alle 1 sind. Dann gilt

$$\boxed{U_n(K) = [B_n(K), B_n(K)]}$$

Insbesondere gilt: $U_n(K) \lhd B_n(K)$

Für $n = 2$ sieht man dies wie folgt ein:
Seien

$$B := \left\{ \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \in \mathrm{M}_{2\times 2}(K) \mid xz \neq 0 \right\} \text{ und}$$
$$U := \left\{ \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \mid y \in K \right\}$$

Behauptung. $U = [B, B]$.

Beweis. "$\subset$" Sei $u = \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} \in U$. Dann rechnet man nach, daß für $b = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ gilt: $u = [u, b]$, also $u \in [B, B]$.

"$\supset$" Es genügt zu zeigen, daß alle Kommutatoren $[a, b]$ mit $a, b \in B$ in U liegen.
Sei $a = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$ und $b = \begin{pmatrix} x' & y' \\ 0 & z' \end{pmatrix} \in B$.

$$\Longrightarrow a^{-1} = \frac{1}{xz} \begin{pmatrix} z & -y \\ 0 & x \end{pmatrix} \in U \quad \text{und}$$
$$[a, b] = aba^{-1}b^{-1} = \underbrace{\begin{pmatrix} xx' & * \\ 0 & zz' \end{pmatrix}}_{ab} \underbrace{\frac{1}{xz} \cdot \frac{1}{x'z'} \begin{pmatrix} zz' & * \\ 0 & xx' \end{pmatrix}}_{a^{-1}b^{-1}} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \in U$$

□

Bemerkung. Die Gruppe $B_n(K)$ ist auflösbar für alle $n \geq 2$:
Ist $n = 2 \Longrightarrow U$ abelsch $\Longrightarrow B \supset U \supset \{e\}$ ist Normalreihe mit abelschen Faktorgruppen $\Longrightarrow B$ ist auflösbar.
Ist $n > 2$, so zeigt man dass $U_n(K)$ auflösbar ist. Da $B_n(K)/U_n(K)$ abelsch ist, folgt dann, dass $B_n(K)$ auflösbar ist (vgl. 4.3(c)).

4.7 Iterierte Kommutatorgruppen

Definition. Sei G eine Gruppe. Definiere die *i-te iterierte Kommutatorgruppe* induktiv durch

$$D^0(G) = G,\ D^1(G) = [G, G], \ldots,\ D^{i+1}(G) = [D^i(G), D^i(G)]$$

Man erhält dann eine Kette von Untergruppen

$$G = D^0(G) \supset D^1(G) \supset \cdots \supset D^i(G) \supset \cdots$$

wobei $D^{i+1}(G) \lhd D^i(G)$ gilt und $D^i(G)/D^{i+1}(G)$ abelsch ist $\forall\, i \geq 0$ (vgl. 4.5).

4.8 Kriterium für Auflösbarkeit mittels Kommutatoren

Satz. *Eine Gruppe G ist genau dann auflösbar, wenn es ein $k \geq 0$ gibt mit $D^k(G) = \{e\}$.*

Beweis. Ist $D^k(G) = \{e\}$ für ein $k \geq 0$, so ist die Kette in 4.7 eine Normalreihe mit abelschen Faktorgruppen und also D auflösbar.
Ist umgekehrt eine Normalreihe

$$G = U_k \supset U_{k-1} \supset \cdots \supset U_1 \supset U_0 = \{e\}$$

mit abelschen Faktorgruppen vorgegeben, so zeige mit Induktion:
$D^i(G) \subset U_{k-i}$ für $i = 0, \ldots, k$ und insbesondere $D^k(G) \subset U_0 = \{e\}$.
Für $i = 0$ ist $D^0(G) = U_k = G$.
Es gelte $D^i(G) \subset U_{k-i}$ für $i < k \Longrightarrow D^i(G) \subset U_{k-(i+1)}$, da $U_{k-i}/U_{k-(i+1)}$ abelsch (vgl. 4.5).
$\Longrightarrow D^{i+1}(G) \subset [D^i(G), D^i(G)] \subset U_{k-(i+1)}$ □

4.9 Übungsaufgabe 15

Aufgabe 15. Seien p und q zwei Primzahlen. Man zeige, dass Gruppen der folgenden Ordnungen auflösbar sind:

(1) $p^2 q$,

(2) $p^r q$, wobei $p > q$ und $r \in \mathbb{N}$,

(3) 100.

5 Exkurs über Permutationsgruppen

Sei M eine nicht-leere Menge. Dann bildet die Menge aller bijektiven Abbildungen $M \longrightarrow M$ bezüglich Hintereinanderausführung von Abbildungen eine Gruppe, genannt *symmetrische Gruppe* oder *Permutationsgruppe von M*. Das neutrale Element ist die *Identität* $\mathrm{id}\colon M \longrightarrow M, x \longmapsto x$.
Ist speziell $M = \{1, 2, \ldots, n\}$, so heißt diese Gruppe die *symmetrische Gruppe S_n*. Es ist $|S_n| = n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (n-1) \cdot n$.
Ist $\pi\colon \{1, \ldots, n\} \to \{1, \ldots, n\}$ bijektiv, so schreibt man

$$\pi = \begin{pmatrix} 1 & 2 & \cdots & n \\ \pi(1) & \pi(2) & \cdots & \pi(n) \end{pmatrix}$$

und nennt π eine *Permutation*.

Beispiel.

$$\begin{aligned}
n = 3: \quad \sigma &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \text{ und } \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \\
\Rightarrow \sigma^2 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \Rightarrow \sigma^3 = \sigma\sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \mathrm{id} \\
\Rightarrow \tau^2 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \mathrm{id} \text{ und } \sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \tau\sigma^2 \\
\text{und } \sigma^2\tau &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \tau\sigma \\
\Rightarrow S_3 &= \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \right. \\
&\quad \left. \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\} \\
&= \{\mathrm{id}, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}
\end{aligned}$$

5.1 Zyklen

Sei $r \in \mathbb{N},\ r \geq 2$.

- Eine Permutation $\pi \in S_n$ heißt ein *r-Zyklus*, wenn es paarweise verschiedene Zahlen $x_1, \ldots, x_r \in \{1, 2, \ldots, n\}$ gibt mit

  $$\pi(x_i) = x_{i+1} \text{ für } 1 \leq i < r \text{ und } \pi(x_r) = x_1$$

  sowie $\pi(x) = x$ für $x \in \{1, \ldots, n\} \setminus \{x_1, \ldots, x_r\}$

- Ist π ein r-Zyklus, so schreibt man $\pi = (x_1, x_2, \dots, x_r)$. Es ist dann $\pi = (x_1, \pi(x_1), \pi^2(x_1), \dots, \pi^{r-1}(x_1))$ und $\pi^r(x_1) = x_1$.
- Zwei Zyklen $(x_1, \dots, x_r)$ und $(y_1, \dots, y_s)$ heißen *disjunkt*, wenn $\{x_1, \dots, x_r\} \cap \{y_1, \dots, y_s\} = \emptyset$.
- Ein 2-Zyklus heißt *Transposition.*

Beispiel.

$n = 3 \Longrightarrow \sigma = (1,3,2), \sigma^2 = (1,2,3), \tau = (1,2), \sigma\tau = (2,3), \sigma^2\tau = (1,3)$.

5.2 Kanonische Zyklenzerlegung einer Permutation

Satz. *Sei $n \geq 2$. Dann gelten:*

(i) *Es ist $\pi_1\pi_2 = \pi_2\pi_1$ für disjunkte Zyklen π_1, π_2.*

(ii) *Jede Permutation $\pi \in S_n \setminus \{\mathrm{id}\}$ läßt sich eindeutig (bis auf die Reihenfolge der Faktoren) als Produkt von paarweise disjunkten Zyklen schreiben.*

(iii) *Jede Permutation $\pi \in S_n$ ist ein Produkt von Transpositionen.*

Beweis. (i) Klar.

(ii) Sei U die von π erzeugte Untergruppe in S_n.
(also $U = \langle\pi\rangle := \{\mathrm{id}, \pi, \pi^2, \dots, \pi^{k-1}\}$ mit $k = \mathrm{ord}(\pi)$, vgl. AGLA 10.12). Dann operiert U auf $M = \{1, \dots, n\}$ durch

$$U \times M \longrightarrow M,\ (\pi^j, x) \longmapsto \pi^j(x)$$

Jede Bahn hat die Form $B = B(x) = \{x, \pi(x), \dots, \pi^{r-1}(x)\}$, wobei $r \in \mathbb{N}$ und $\pi^r(x) = x$. (Ist $j > r$, so ist $j = mr + r'$ mit $0 \leq r' < r$. $\Longrightarrow \pi^j(x) = \pi^{r'}(x) \in B(x)$.)

$\Longrightarrow \pi_B := (x, \pi(x), \dots, \pi^{r-1}(x))$ definiert einen r-Zyklus mit $r = |B|$.
Seien $B_1, \dots, B_\ell$ die Bahnen mit $|B_i| \geq 2$ für $i = 1, \dots, \ell$.
$\Longrightarrow \pi = \pi_{B_1} \cdots \pi_{B_\ell}$ ist ein Produkt von disjunkten Zyklen.

Eindeutigkeit. Seien $\pi_1 \dots \pi_\ell = \pi'_1 \dots \pi'_\ell$ zwei Zyklenzerlegungen von π.
Zu jedem Zyklus $\pi_i = (x_1, \dots, x_{r_i})$ gehört die Bahn $B_i := \{x_1, \dots, x_{r_i}\}$.
Analog gehört zu π'_j die Bahn B'_j. Wähle $x \in M$ mit $\pi(x) \neq x$.
$\Longrightarrow$ Es gibt eindeutig bestimmte Indizes i, j mit $x \in B_i$ und
$x \in B'_j \underset{\text{AGLA 10.24}}{\Longrightarrow} B_i = B'_j \Longrightarrow \pi_i = \pi'_j$
Wegen (i) kann man $\pi_i = \pi'_j$ kürzen und kommt mit einem Induktionsargument zur Eindeutigkeitsaussage.

(iii) Jeder r-Zyklus $(x_1, \ldots, x_n) \in S_n$ läßt sich zerlegen in $(x_1, \ldots, x_r) = (x_1, x_2)(x_2, x_3) \ldots (x_{r-1}, x_r)$. Also folgt (iii) aus (ii) für $\pi \neq \mathrm{id}$. Es ist $\mathrm{id} = (1, 2)(1, 2)$.

□

Beispiel.

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 5 & 7 & 1 & 6 & 4 \end{pmatrix} \in S_7$$

hat die kanonische Zyklenzerlegung

$$\pi = (1, 2, 3, 5)(4, 7)$$

5.3 Das Vorzeichen einer Permutation

Definition. Das *Vorzeichen* oder *Signum* einer Permutation $\pi \in S_n$ ist definiert durch

$$\mathrm{sign}(\pi) := \prod_{1 \leq i < j \leq n} \frac{\pi(i) - \pi(j)}{i - j}$$

Es ist $\mathrm{sign}(\pi) = \pm 1$. Im Fall $\mathrm{sign}(\pi) = 1$ heißt π eine *gerade Permutation* und im Fall $\mathrm{sign}(\pi) = -1$ eine *ungerade Permutation*. Eine Transposition ist stets ungerade.

Beispiel. $n = 3$

$$\begin{aligned} \tau = (1, 2) &\Longrightarrow \mathrm{sign}(\tau) = \frac{2-1}{1-2} \cdot \frac{2-3}{1-3} \cdot \frac{1-2}{2-3} = -1 \\ \sigma = (2, 1, 3) &\Longrightarrow \mathrm{sign}(\sigma) = \frac{3-1}{1-2} \cdot \frac{3-2}{1-3} \cdot \frac{1-2}{2-3} = 1 \end{aligned}$$

und es ist $\sigma = (2, 1, 3) = (2, 1)(1, 3)$ ein Produkt von zwei Transpositionen, also von einer geraden Anzahl von Transpositionen.

Satz. *Für* $n \geq 2$ *ist* $\mathrm{sign}\colon S_n \to \{1, -1\} \subset \mathbb{R}^*$ *ein Gruppenhomomorphismus, und es gilt* $\mathrm{sign}(\pi) = (-1)^m$, *falls* π *ein Produkt von* m *Transpositionen ist.*

Beweis. Für $\pi, \sigma \in S_n$ ist

$$\begin{aligned} \mathrm{sign}(\pi\sigma) &= \prod_{1 \leq i < j \leq n} \frac{\pi\sigma(i) - \pi\sigma(j)}{i - j} \\ &= \prod_{i<j} \frac{\pi\sigma(i) - \pi\sigma(j)}{\sigma(i) - \sigma(j)} \cdot \prod_{i<j} \frac{\sigma(i) - \sigma(j)}{i - j} = \mathrm{sign}(\pi)\,\mathrm{sign}(\sigma)\,, \end{aligned}$$

denn $\operatorname{sign}(\pi)$ unterscheidet sich von dem ersten Produkt nur durch die Reihenfolge der Faktoren.
Ist $\pi = \tau_1 \cdots \tau_m$ ein Produkt von m Transpositionen, so folgt
$\operatorname{sign}(\pi) = \operatorname{sign}(\tau_1) \cdot \ldots \cdot \operatorname{sign}(\tau_m) = (-1)^m$. □

Korollar. *Ist $\pi \in S_n$ ein r-Zyklus, so ist* $\operatorname{sign}(\pi) = (-1)^{r-1}$.

Beweis. Sei $\pi = (x_1, \ldots, x_r)$ ein r-Zyklus.
$\Longrightarrow \pi = (x_1, x_2)(x_2, x_3) \ldots (x_{r-1}, x_r)$
$\Longrightarrow \operatorname{sign}(\pi) = (-1)^{r-1}$. □

5.4 Die alternierende Gruppe

Sei A_n die Menge aller geraden Permutationen in S_n. Dann ist A_n der Kern des Homomorphismus $\operatorname{sign}\colon S_n \longrightarrow \{1, -1\}$ und also A_n ein Normalteiler in S_n (vgl. AGLA 10.17).
Sei $n \geq 2$. Da sign surjektiv ist, folgt

$$(S_n : A_n) = \frac{|S_n|}{|A_n|} = |\{1, -1\}| = 2 \quad \text{(vgl. 1.2 und AGLA 10.10 (3))},$$

also $|A_n| = \frac{n!}{2}$.

Beispiel. • $A_3 = \{\mathrm{id}, (2,1,3), (1,2,3)\}$
$\Longrightarrow A_3 = \{\mathrm{id}, \sigma, \sigma^2\} \simeq \mathbb{Z}/3\mathbb{Z}$
$\Longrightarrow A_3$ ist einfach.

- Die *Kleinsche Vierergruppe* $V_4 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ läßt sich schreiben als $V_4 = \{\mathrm{id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$, also $V_4 \subset A_4 \subset S_4$. Es ist V_4 Normalteiler in A_4 (nach Aufgabe 19).
  $\Longrightarrow A_4$ ist nicht einfach.

5.5 Einfachheit der alternierenden Gruppe für $n \neq 4$

Lemma 1. *Für $n \geq 3$ besteht A_n aus allen Permutationen $\pi \in S_n$, die sich als Produkt von 3-Zyklen schreiben lassen.*

Beweis. Seien $x_1, x_2, x_3 \in \{1, \ldots, n\}$ paarweise verschieden. Dann gilt

$$(x_1, x_2)(x_2, x_3) = (x_1, x_2, x_3)\,.$$

$\Longrightarrow$ Jeder 3-Zyklus und damit jedes Produkt von 3-Zyklen ist in A_n. Sind x_1, x_2, x_3, x_4 paarweise verschieden in $\{1, \ldots, n\}$, so gilt

$$(x_1, x_2)(x_3, x_4) = (x_1, x_3, x_2)(x_1, x_3, x_4).$$

Insgesamt folgt, dass jedes Produkt einer geraden Anzahl von Transpositionen, also jedes Element von A_n, ein Produkt von 3-Zyklen ist. □

Lemma 2. *Für $n \geq 5$ sind alle 3-Zyklen konjugiert in A_n.*

Beweis. Sei (x_1, x_2, x_3) ein 3-Zyklus in A_n. Es genügt zu zeigen, dass es ein $\pi \in A_n$ gibt mit $\pi(1,2,3)\pi^{-1} = (x_1, x_2, x_3)$. Da $n \geq 5$, gibt es zwei Zahlen $x_4, x_5 \in \{1, \ldots, n\}$, so dass $x_1, \ldots, x_5$ paarweise verschieden sind.
$\Longrightarrow$ Entweder ist $\pi := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \ldots & n \\ x_1 & x_2 & x_3 & x_4 & x_5 & \ldots & x_n \end{pmatrix}$ oder
$\pi' := (x_4, x_5) \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \ldots & n \\ x_1 & x_2 & x_3 & x_4 & x_5 & \ldots & x_n \end{pmatrix}$ in A_n nach Satz 5.3. Es ist

$$\begin{aligned} \pi(1,2,3)\pi^{-1} &= (\pi(1), \pi(2), \pi(3)) \quad \text{(vgl. Aufgabe 18 c))} \\ &= (x_1, x_2, x_3) = (\pi'(1), \pi'(2), \pi'(3)) = \pi'(1,2,3)\pi'^{-1} \end{aligned}$$

$\Longrightarrow (x_1, x_2, x_3)$ sind zu $(1,2,3)$ in A_n konjugiert. □

Satz. *Für $n \geq 5$ ist A_n eine einfache Gruppe.*

Beweis. Sei $N \lhd A_n$ und $N \neq \{\mathrm{id}\}$. Zu zeigen: $N = A_n$. Dazu genügt es, zu zeigen, daß N einen 3-Zyklus $z = (z_1, z_2, z_3)$ enthält, denn dann folgt $\pi z \pi^{-1} \in N \ \forall \pi \in A_n$, da $N \lhd A_n$, und mit den Lemmata 1,2 folgt dann $N = A_n$.
Sei $\sigma \in N$. Benutze die Zyklenzerlegung 5.2 von σ.

1.Fall: In der Zyklenzerlegung von σ gibt es einen Zyklus $(x_1, x_2, x_3, \ldots, x_r)$ mit $r \geq 4$. Setze $\tau = (x_1, x_2, x_3)$. Dann folgt

$$\begin{aligned} N \ni \underbrace{\sigma}_{\in N} \underbrace{\tau \sigma^{-1} \tau^{-1}}_{\in N \lhd A_n} &= \sigma(x_1, x_2, x_3)\sigma^{-1}\tau^{-1} = (\sigma(x_1), \sigma(x_2), \sigma(x_3))\tau^{-1} \\ &= (x_2, x_3, x_4)(x_3, x_2, x_1) = (x_1, x_4, x_2) \end{aligned}$$

2.Fall In der Zyklenzerlegung von σ kommen nur Transpositionen und mindestens ein 3-Zyklus vor. Ist σ selbst kein 3-Zyklus, so folgt $\sigma = (x_1, x_2, x_3)(x_4, x_5) \cdots$. Setze $\tau = (x_1, x_2, x_4)$, so folgt wie oben

$$\begin{aligned} N \ni \sigma\tau\sigma^{-1}\tau^{-1} &= (\sigma(x_1), \sigma(x_2), \sigma(x_4))(x_4, x_2, x_1) \\ &= (x_2, x_3, x_5)(x_4, x_2, x_1) = (x_1, x_4, x_3, x_5, x_2) \end{aligned}$$

$\Longrightarrow N$ enthält einen 5-Zyklus $\Longrightarrow N$ enthält einen 3-Zyklus wie in Fall 1.

3.Fall σ ist ein Produkt von disjunkten Transpositionen. Da σ gerade ist, ist σ keine Transposition.
Sei $\sigma = (x_1, x_2)(x_3, x_4)\cdots$. Setze $\tau = (x_2, x_3, x_4)$

$$\begin{aligned} N \ni \sigma\tau\sigma^{-1}\tau^{-1} &= (\sigma(x_2), \sigma(x_3), \sigma(x_4))(x_4, x_3, x_2) \\ &= (x_1, x_4, x_3)(x_4, x_3, x_2) = (x_1, x_4)(x_2, x_3) =: \pi_1 \end{aligned}$$

Setze $\varrho = (x_1, x_4, x_5)$

$$\begin{aligned} N \ni \varrho(x_1, x_4)\varrho^{-1}\varrho(x_2, x_3)\varrho^{-1} &= (\varrho(x_1), \varrho(x_4))(\varrho(x_2), \varrho(x_3)) \\ &= (x_4, x_5)(x_2, x_3) =: \pi_2 \end{aligned}$$

$$\Longrightarrow N \ni \pi_1 \cdot \pi_2 = (x_1, x_4)(x_4, x_5) = (x_1, x_4, x_5).$$

□

Bemerkung. Es ist $|A_5| = \frac{5!}{2} = 60$, und A_5 ist die kleinste nicht-abelsche einfache Gruppe.

5.6 Die symmetrische Gruppe ist ab $n = 5$ nicht auflösbar

Satz. *Die symmetrische Gruppe S_n ist für $n \leq 4$ auflösbar und für alle $n \geq 5$ nicht auflösbar.*

Beweis. Man hat folgende Normalreihen:

$$S_2 \supset \{\mathrm{id}\}, \qquad S_3 \supset A_3 \supset \{\mathrm{id}\}, \text{ und } S_4 \supset A_4 \supset V_4 \supset \{\mathrm{id}\}.$$

Alle Faktorgruppen sind abelsch, denn

$$S_3/A_3 \simeq \mathbb{Z}/2\mathbb{Z} \simeq S_4/A_4 \text{ und } A_3 \simeq \mathbb{Z}/3\mathbb{Z} \simeq A_4/V_4$$

$$(\text{wegen } (S_n : A_n) \underset{5.4}{=} 2 \text{ und } |A_3| = 3 = \frac{12}{4} = \frac{|A_4|}{|V_4|}).$$

Wäre S_n für $n \geq 5$ auflösbar, so wäre auch die Untergruppe A_n auflösbar (vgl. 4.3). Da A_n für $n \geq 5$ nicht abelsch ist, wäre dann A_n nicht einfach im Widerspruch zu Satz 5.5. □

5.7 Bemerkung über Transpositionen

Nach 5.2(iii) ist jede Permutation $\pi \in S_n$ ein Produkt von Transpositionen (x, y) mit $x, y \in \{1, \ldots, n\}$. Da

$$(x, y) = (1, y)(1, x)(1, y) \text{ für } x, y \in \{2, \ldots, n\}$$

gilt, wird S_n sogar von den Transpositionen $(1, x)$ mit $x \in \{2, \ldots, n\}$ erzeugt. Man schreibt

$$\boxed{S_n = \langle\, (1, x) \mid x \in \{2, \ldots, n\}\,\rangle}$$

5.8 Übungsaufgaben 16 – 19

Aufgabe 16. Es sei $\pi \in S_{15}$ die Permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 1 & 3 & 5 & 7 & 9 & 11 & 13 & 15 & 2 & 4 & 6 & 8 & 10 & 12 & 14 \end{pmatrix}.$$

(a) Man bestimme die kanonische Zyklenzerlegung von π.

(b) Man stelle π als Produkt von Transpositionen dar.

(c) Man berechne das Vorzeichen von π.

Aufgabe 17. Man berechne in S_5 die Potenzen π^i für $0 \leq i \leq 5$ von

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix} (2,3).$$

Aufgabe 18. Sei $\sigma = (x_1, \ldots, x_r)$ ein r-Zyklus in S_n. Man zeige:

(a) Die Ordnung von σ ist gleich r.

(b) Es ist $\sigma^{-1} = (x_r, x_{r-1}, \ldots, x_1)$.

(c) Es gilt $\pi\sigma\pi^{-1} = (\pi(x_1), \ldots, \pi(x_r))$ für jede Permutation $\pi \in S_n$.

Aufgabe 19. Man zeige, dass die Gruppe $V_4 = \{\mathrm{id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ ein Normalteiler in S_4 ist.

Teil II
Ringe

6 Grundbegriffe der Ringtheorie

6.1 Definition eines Ringes

Definition. Eine Menge R, die mit zwei Verknüpfungen

$$\begin{aligned} +\colon R &\longrightarrow R, (a,b) \longmapsto a+b, \\ \cdot\colon R &\longrightarrow R, (a,b) \longmapsto ab, \end{aligned}$$

versehen sei, heißt *Ring*, wenn gelten:

1. R ist bezüglich $+$ eine abelsche Gruppe (mit neutralem Element 0).

2. $(a+b)c = ac+bc$ und $a(b+c) = ab+ac \quad \forall a,b,c \in R$.

3. $(ab)c = a(bc) \quad \forall a,b,c \in R$.

4. Es gibt ein *Einselement* $e \in R$ mit $ea = a = ae$ für alle $a \in R$
(Wir schreiben meist 1 oder 1_R statt e).

Ein Ring R heißt *kommutativ*, falls $ab = ba \quad \forall a,b \in R$ gilt.

6.2 Einheiten und Nullteiler

Definition. Sei R ein Ring, und sei

$$\boxed{R^* := \{a \in R \mid \exists\, b \in R \text{ mit } ab = 1 = ba\}}$$

die Menge der *multiplikativ invertierbaren Elemente* oder *Einheiten* in R. Dann ist R^* bezüglich Multiplikation eine Gruppe, die *Einheitengruppe von* R. Ein Element $a \in R$ heißt *Nullteiler*, falls es ein $b \in R \setminus \{0\}$ gibt mit $ab = 0$ oder $ba = 0$.
Ein kommutativer Ring $R \neq \{0\}$ heißt *nullteilerfrei* oder *Integritätsring* oder *Integritätsbereich*, falls 0 der einzige Nullteiler in R ist.

6.3 Beispiele

1. $\mathbb{Z}$ ist ein Integritätsring mit Einheitengruppe $\mathbb{Z}^* = \{1, -1\}$.

2. Jeder Körper K ist ein Integritätsring mit Einheitengruppe $K^* = K \setminus \{0\}$.

3. Ein *Schiefkörper* ist ein Ring $R \neq \{0\}$, in dem jedes Element $\neq 0$ invertierbar ist. Es ist dann $R^* = R \setminus \{0\}$. Es ist

$$\mathbb{H} := \left\{ \begin{pmatrix} z & u \\ -\bar{u} & \bar{z} \end{pmatrix} \in \mathrm{M}_{2\times 2}(\mathbb{C}) \right\}$$

ein Schiefkörper bezüglich Matrizenmultiplikation und -addition (Dabei bedeutet $\bar{z}$ die zu z konjugiert komplexe Zahl). Man rechnet leicht nach, dass mit $a, b \in \mathbb{H}$ auch $a + b$ und ab aus $\mathbb{H}$ sind.

Für $a = \begin{pmatrix} z & u \\ -\bar{u} & \bar{z} \end{pmatrix}$ ist $\det(a) = z\bar{z} + u\bar{u} \neq 0$, falls $a \neq 0$, und

$$a^{-1} = \frac{1}{\det(a)} \begin{pmatrix} \bar{z} & -u \\ \bar{u} & z \end{pmatrix} \in \mathbb{H}.$$

Für $a = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ und $b = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ gilt $ab = -ba$.

Der *Quaternionenschiefkörper* $\mathbb{H}$ ist also nicht kommutativ (Hamilton 1844).

4. Für $n \geq 2$ bildet die Menge $\mathrm{M}_{n\times n}(K)$ der $(n \times n)$-Matrizen mit Einträgen aus einem Körper K bezüglich Matrizenaddition und -multiplikation einen Ring, der nicht kommutativ ist und Nullteiler $\neq 0$ besitzt.

(z.B. $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$)

Es ist $(\mathrm{M}_{n\times n}(K))^* = \mathrm{GL}_n(K) = \{x \in \mathrm{M}_{n\times n}(K) \mid \det(x) \neq 0\}$.

5. Ist V ein K-Vektorraum, so ist

$$\mathrm{End}_K(V) = \{f : V \to V \mid f \text{ ist } K\text{-linear}\}$$

ein Ring bezüglich

$$\begin{aligned} f + g &: V \longrightarrow V,\ v \longmapsto f(v) + g(v) \\ f \circ g &: V \longrightarrow V,\ v \longmapsto f(g(v)). \end{aligned}$$

Dabei ist $v \longmapsto 0$ das Nullelement und $\mathrm{id}: v \longmapsto v$ das Einselement.

6. Ist $M \neq \emptyset$ eine Menge und ist R ein Ring, so ist die Menge aller Abbildungen $M \to R$ ein Ring mit

$$f + g \colon M \longrightarrow R,\ x \longmapsto f(x) + g(x)$$
$$f \cdot g \colon M \longrightarrow R,\ x \longmapsto f(x)g(x)$$

für Abbildungen $f, g \colon M \longrightarrow R$. Dabei ist $x \longmapsto 0$ das Nullelement und $x \longmapsto 1$ das Einselement.

6.4 Unterringe

Definition. Sei S ein Ring. Eine Teilmenge $R \subset S$ heißt *Unterring von* S, wenn R bezüglich Addition eine Untergruppe ist, und wenn $1 \in R$, und $ab \in R$ für alle $a, b \in R$ gilt. Es ist R dann ein Ring, und S heißt *Ringerweiterung von* R.

Beispiele.
- $\mathbb{Z}$ ist ein Unterring von $\mathbb{Q}$.
- $\mathbb{Q}$ ist ein Unterring von $\mathbb{R}$.

6.5 Ideale

Ideale spielen in der Ringtheorie eine ähnlich wichtige Rolle wie Normalteiler in der Gruppentheorie.

Definition. Sei R ein Ring. Eine additive Untergruppe $\mathfrak{I}$ von R heißt *Linksideal*, wenn

$$\boxed{rx \in \mathfrak{I}\ \forall r \in R, x \in \mathfrak{I}}$$

Rechtsideal, wenn

$$\boxed{xr \in \mathfrak{I}\ \forall r \in R, x \in \mathfrak{I}}$$

und *zweiseitiges Ideal* oder kurz *Ideal*, wenn $\mathfrak{I}$ sowohl Links- als auch Rechtsideal ist.

Bemerkung. Ist R kommutativ, so ist jedes Linksideal ein Ideal und jedes Rechtsideal ebenfalls. Man unterscheidet dann nicht zwischen Links- und Rechtsidealen.

Beispiele. 1. Sei $\mathfrak{I} = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \in \mathrm{M}_{2\times 2}(\mathbb{R}) \right\}$. Dann ist $\mathfrak{I}$ ein Linksideal in $\mathrm{M}_{2\times 2}(\mathbb{R})$, denn $\mathfrak{I}$ ist additive Untergruppe und für $r = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \in \mathrm{M}_{2\times 2}(\mathbb{R})$ ist $r \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} a_1 a + a_2 b & 0 \\ a_3 a + a_4 b & 0 \end{pmatrix} \in \mathfrak{I}$.
Aber $\mathfrak{I}$ ist kein Rechtsideal in $\mathrm{M}_{2\times 2}(\mathbb{R})$, denn z.B. für $a \neq 0$ und $r = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ ist $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} r = \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} \notin \mathfrak{I}$.

2. Sei $\mathfrak{J} = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in \mathrm{M}_{2\times 2}(\mathbb{R}) \right\}$. Dann ist $\mathfrak{J}$ ein Rechtsideal, aber kein Linksideal.

6.6 Summe, Produkt und Durchschnitt von Idealen

Seien $\mathfrak{I}, \mathfrak{J}$ zwei Ideale in einem Ring R. Dann erhält man damit folgende weitere Ideale

$$\begin{aligned} \mathfrak{I} + \mathfrak{J} &:= \{x + y \mid x \in \mathfrak{I}, y \in \mathfrak{J}\} \\ \mathfrak{I} \cdot \mathfrak{J} &:= \{\sum_{\text{endl.}} x_i y_i \mid x_i \in \mathfrak{I}, y_i \in \mathfrak{J}\} \\ \mathfrak{I} \cap \mathfrak{J} &:= \{x \in R \mid x \in \mathfrak{I} \text{ und } x \in \mathfrak{J}\}. \end{aligned}$$

Es gilt stets $\mathfrak{I}\mathfrak{J} \subset \mathfrak{I} \cap \mathfrak{J}$ (vgl. Aufgabe 22).
Analog kann man das Produkt von endlich vielen Idealen bilden, sowie Summe und Durchschnitt beliebig vieler Ideale. Das Summenideal hat dann die Form

$$\sum_{j\in I} \mathfrak{I} = \left\{ \sum_{j\in I} x_j \mid x_j = 0 \text{ bis auf endlich viele } j \right\}$$

(Hierbei sei I eine Indexmenge)

6.7 Erzeugung von Idealen

Sei R ein Ring. Jedes Element $a \in R$ erzeugt ein Linksideal

$$\boxed{Ra = \{ra \mid r \in R\}}$$

Jede Familie $(a_i \mid i \in I)$ erzeugt ein Linksideal

$$\sum_{i\in I} Ra_i = \left\{ \sum_{\text{endlich}} r_i a_i \mid r_i \in R \right\}$$

und ein Ideal

$$\sum_{i\in I} Ra_iR = \Big\{ \sum_{\text{endlich}} r_ia_is_i \mid r_i, s_i \in R \Big\}$$

- Sei R ein kommutativer Ring. Dann heißt ein Ideal $\mathfrak{I}$ *endlich erzeugt*, wenn es endlich viele Elemente $a_1, \ldots, a_n \in R$ gibt, so dass

  $$\mathfrak{I} = \{r_1a_1 + \cdots + r_na_n \mid r_1, \ldots, r_n \in R\}$$

  gilt. Man schreibt dann $\boxed{\mathfrak{I} = (a_1, \ldots, a_n)}$

- R heißt *noethersch*, falls jedes Ideal in R endlich erzeugt ist.

6.8 Hauptidealringe

Sei R ein kommutativer Ring. Ein Ideal $\mathfrak{I}$, das von einem Element erzeugt wird, heißt *Hauptideal*. Es ist dann

$$\boxed{\mathfrak{I} = (a) = \{ra \mid r \in R\}}$$

mit einem $a \in R$. Ein Integritätsring, in dem jedes Ideal Hauptideal ist, heißt *Hauptidealring*. Ein Hauptidealring ist stets noethersch.

Beispiel. Jeder Körper K ist ein Hauptidealring, denn K besitzt als einzige Ideale die beiden Hauptideale (0) und $(1) = K$.

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

Beweis. Nach AGLA 10.5.5 hat jede Untergruppe von $\mathbb{Z}$ die Gestalt $n\mathbb{Z}$ mit einem $n \in \mathbb{Z}$. Da jedes Ideal in $\mathbb{Z}$ insbesondere eine Untergruppe von $\mathbb{Z}$ ist (bezüglich Addition), folgt die Behauptung. $\square$

Schreibweisen für Hauptideale in R sind auch $(a) = Ra = aR$.

6.9 Ringhomomorphismen

Seien R und R' zwei Ringe. Dann heißt eine Abbildung $f\colon R \to R'$ ein Homomorphismus, falls gelten:

$$\begin{aligned} f(x+y) &= f(x) + f(y) \\ f(xy) &= f(x)f(y) \quad \forall\, x, y \in R \\ \text{und } f(1_R) &= 1_{R'} \end{aligned}$$

Satz. *Ist $f\colon R \to R'$ ein Homomorphismus von Ringen, so ist*

$$\operatorname{kern}(f) := \{x \in R \mid f(x) = 0\}$$

ein Ideal in R, und $\operatorname{bild}(f)$ *ist ein Unterring.*

Beweis. $\operatorname{kern}(f)$ ist eine additive Untergruppe von R.
Seien $r \in R$ und $x \in \operatorname{kern}(f)$.
$\Longrightarrow f(rx) = f(r)\underbrace{f(x)}_{=0} = 0$
$\Longrightarrow rx \in \operatorname{kern}(f)$.
Analog $xr \in \operatorname{kern}(f)$. □

Folgerung. Sei K ein Körper und sei R ein Ring $\neq \{0\}$. Dann ist jeder Homomorphismus $f\colon K \to R$ injektiv.

Beweis. Da $f(1) = 1 \neq 0$ gilt, ist f nicht die Nullabbildung $x \longmapsto 0$
$\Longrightarrow \operatorname{kern}(f) = (0)$, da K als Körper keine weiteren echten Ideale enthält. □

6.10 Quotientenringe

Sei R ein kommutativer Ring.

Definition. Eine Teilmenge $S \subset R \setminus \{0\}$ heißt *multiplikativ abgeschlossen*, wenn $1 \in S$ und wenn $\forall\, s, s' \in S$ auch $ss' \in S$ gilt.

Beispiele. für multiplikativ abgeschlossene Mengen:

1. R^* = Menge der invertierbaren Elemente in R.
2. Die Potenzen $r^n, n \geq 0$, eines Elementes $r \in R \setminus \{0\}$.
3. Die Menge der Nichtnullteiler in R.
4. $R \setminus \{0\}$, falls R ein Integritätsring ist.

Sei S eine multiplikativ abgeschlossene Menge in R. Dann konstruiert man wie folgt einen Quotientenring:

$$S^{-1}R := \left\{\frac{r}{s} \mid r \in R, s \in S\right\}$$

Definiere für $(r, s), (r', s') \in R \times S$ eine Relation

$$\boxed{(r, s) \sim (r', s')} \quad \Longleftrightarrow \quad \boxed{\exists\, t \in S \text{ mit } t(rs' - sr') = 0}\,.$$

Ist R ein Integritätsring, so kommt man ohne das $t \in S$ aus, und die Relation besagt $\frac{r}{s} = \frac{r'}{s'}$, so wie wir es von den rationalen Zahlen her gewohnt sind. Wir zeigen nun, dass die Relation eine Äquivalenzrelation ist.
Es gilt offensichtlich $(r,s) \sim (r,s)$ und: $(r,s) \sim (r',s') \Longrightarrow (r',s') \sim (r,s)$.
Sei nun $(a,s) \sim (b,u)$ und $(b,u) \sim (c,v)$ mit $a,b,c \in R,\ s,u,v \in S$. Dann gibt es $t,t' \in S$ mit

$$t(au - sb) = 0 \quad \text{und} \quad t'(bv - uc) = 0\,.$$

Multipliziert man die linke Gleichung mit $t'v$, die rechte mit ts und addiert beide Gleichungen, so heben sich die Summanden mit dem Faktor b weg, und wir erhalten $tt'u(av - sc) = 0$, woraus $(a,s) \sim (c,v)$ folgt.

Sei $\frac{r}{s} := \big\{(r',s') \in R \times S \mid (r',s') \sim (r,s)\big\}$ die Äquivalenzklasse von $(r,s) \in R \times S$, und sei $S^{-1}R = \Big\{\frac{r}{s} \mid r \in R, s \in S\Big\}$. Definiere $\frac{r}{s} + \frac{r'}{s'} = \frac{rs'+r's}{ss'}$ und $\frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}$ und zeige, daß Summe und Produkt dadurch wohldefiniert sind, und daß $S^{-1}R$ ein kommutativer Ring ist. Man nennt $S^{-1}R$ den *Quotientenring von R bezüglich S.*

Satz. *Die kanonische Abbildung* $\iota\colon R \longrightarrow S^{-1}R,\ r \longmapsto \frac{r}{1}$ *ist ein Ringhomomorphismus mit* $\operatorname{kern}(\iota) = \{r \in R \mid sr = 0$ *für ein* $s \in S\}$.

Beweis. Die Homomorphie ist ersichtlich. Sei $r \in \operatorname{kern}(\iota)$.
$\Longrightarrow \iota(r) = \frac{r}{1} = \frac{0}{1} \Longrightarrow (r,1) \sim (0,1) \Longrightarrow \exists\, t \in S$ mit $0 = t(r \cdot 1 - 1 \cdot 0) = tr$.
Ist umgekehrt $sr = 0$ für ein $s \in S$, so ist $\frac{r}{1} = \frac{sr}{s} = \frac{0}{s} = \frac{0}{1}$ und also $r \in \operatorname{kern}(\iota)$. □

Universelle Eigenschaft des Quotientenrings. *Sei $g : R \longrightarrow R'$ ein Homomorphismus von kommutativen Ringen so, dass $g(s)$ eine Einheit für jedes $s \in S$ ist. Dann gibt es genau einen Ringhomomorphismus $h : S^{-1}R \longrightarrow R'$ mit $g = h \circ \iota$.*

Beweis. Wir setzen $h(\frac{r}{s}) := \frac{g(r)}{g(s)}$ für $r \in R,\ s \in S$. Ist $\frac{r}{s} = \frac{r'}{s'}$, so gibt es ein $t \in S$ mit $t(rs' - sr') = 0$, also mit $g(t)\Big(g(r)g(s') - g(s)g(r')\Big) = 0$. Da $g(t)$ eine Einheit ist, folgt $\frac{g(r)}{g(s)} = \frac{g(r')}{g(s')}$, und h ist also wohldefiniert. Da g ein Ringhomomorphismus ist, ist auch h ein solcher. Sei nun $h' : S^{-1}R \longrightarrow R'$ ein weiterer Ringhomomorphismus mit $g = h' \circ \iota$. Dann gilt $h(\frac{r}{1}) = g(r) = h'(\frac{r}{1})$ für alle $r \in R$. Es folgt

$$h(\frac{r}{s}) = h(\frac{r}{1}) \cdot h(\frac{s^{-1}}{1}) = g(r) \cdot g(s^{-1}) = h'(\frac{r}{1}) \cdot h'(\frac{s^{-1}}{1}) = h'(\frac{r}{s})\,.$$

□

6.11 Quotientenkörper

Sei R ein Integritätsring (wie in 6.2 definiert). Dann ist der kanonische Homomorphismus $R \longrightarrow S^{-1}R$ injektiv für jede multiplikativ abgeschlossene Menge S in R nach Satz 6.10. Ist speziell $S = R\backslash\{0\}$, so ist $S^{-1}R$ ein Körper, genannt *Quotientenkörper*.

Beispiel. $\mathbb{Q}$ ist der Quotientenkörper von $\mathbb{Z}$.

Definition. Ist K ein Körper, dann nennt man den Quotientenkörper des Polynomrings $K[X]$ den *Körper der rationalen Funktionen in einer Unbestimmten über* K und schreibt $K(X)$ dafür.

6.12 Polynomringe

Sei R ein kommutativer Ring, und sei P die Menge aller Folgen (a_i), wobei $a_i \in R$ mit $i \in \mathbb{N} \cup \{0\}$ und $a_i \neq 0$ für nur endlich viele i gelte. Definiere in P eine Addition und Multiplikation

$$\boxed{(a_i) + (b_i) := (a_i + b_i) \text{ und } (a_i)(b_i) := \left(\sum_{j=0}^{i} a_j b_{i-j}\right)}\,.$$

Dann ist P ein kommutativer Ring mit Einselement $(1, 0, 0, \ldots)$. Setze $X = (0, 1, 0, \ldots)$. Dann ist $X^2 = (0, 0, 1, 0, \ldots)$ und allgemein
$X^n = (0, \ldots, 0, 1, 0, \ldots)$ mit einer Eins an der $(n+1)$-ten Stelle. Es ist

$$R \longrightarrow P,\ a \longmapsto (a, 0, \ldots)$$

ein injektiver Ringhomomorphismus. Identifiziere die Elemente $a \in R$ mit ihrem Bild $(a, 0, \ldots)$. Dann folgt:

$$\boxed{(a_0, a_1, a_2, \ldots, a_n, 0, \ldots) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n}\,,$$

wobei $a_i = 0$ für $i > n$ gilt. Man erhält so P als Polynomring

$$\boxed{R[X] = \left\{\sum_{i=0}^{n} a_i X^i \mid a_i \in R; n \in \mathbb{N} \cup \{0\}\right\}}$$

mit der Addition

$$\boxed{\sum_{i=0}^{n} a_i X^i + \sum_{j=0}^{m} b_j X^j = \sum_{i=0}^{\max(n,m)} (a_i + b_i) X^i}$$

und der Multiplikation:

$$\boxed{\left(\sum_{i=0}^{n} a_i X^i\right)\left(\sum_{j=0}^{m} b_j X^j\right) = \sum_{i=0}^{n+m}\left(\sum_{j=0}^{i} a_j b_{i-j}\right) X^i}\,.$$

In Kapitel 21 wird die obige Konstruktion verallgemeinert, um den Polynomring in beliebig vielen Unbstimmten zu definieren. Dort wird auch die *universelle* Eigenschaft des Polynomrings gezeigt, die dann seine Eindeutigkeit (bis auf einen Isomorphismus) garantiert.

6.13 Der Grad eines Polynoms

Definition. Sei R ein kommutativer Ring, und sei

$$\boxed{f = a_0 + a_1 X + \cdots + a_n X^n \in R[X]}$$

ein *Polynom*. Dann ist der *Grad von f* definiert als

$$\operatorname{grad}(f) := \max\{i \mid a_i \neq 0\}\,.$$

Das konstante Polynom $a_0 \neq 0$ hat den Grad 0, und man setzt $\operatorname{grad}(0) = -\infty$. Ist $\operatorname{grad}(f) = n$, so heißt a_n der *Leitkoeffizient* und $a_n X^n$ heißt der *Leitterm von f*.

Gradformeln. *Für Polynome $f, g \in R[X]$ gilt*

a) $\operatorname{grad}(f+g) \leq \max(\operatorname{grad}(f), \operatorname{grad}(g))$

b) $\operatorname{grad}(f \cdot g) \leq \operatorname{grad}(f) + \operatorname{grad}(g)$

c) $\boxed{R \textit{ Integritätsring}} \quad \Longrightarrow \quad \boxed{\operatorname{grad}(fg) = \operatorname{grad}(f) + \operatorname{grad}(g)}$

Beweis. Für $f = 0$ oder $g = 0$ sind die Formeln erfüllt. Seien $n := \operatorname{grad}(f)$ und $k := \operatorname{grad}(g)$ beide ≥ 0, und seien

$$f = \sum_{i=0}^{n} a_i X^i \quad \text{und} \quad g = \sum_{j=0}^{k} a_j X^j$$
$$\Longrightarrow a_i + b_i = 0 \text{ für } i > \max(n, k)$$

nach Definition der Addition in 6.12. $\Longrightarrow$ a).
Ferner ist $\sum_{j=0}^{i} a_j b_{i-j} = 0$ für $i > n + k$ nach Definition der Multiplikation in 6.12 $\Longrightarrow$ b)
Da $\operatorname{grad}(f) = n \Longrightarrow a_n \neq 0$, und da $\operatorname{grad}(g) = k \Longrightarrow b_k \neq 0$.
Ist R Integritätsring, folgt $a_n b_k \neq 0 \Longrightarrow$ c) □

Folgerung. Sei R ein Integritätsring. Dann ist $R[X]$ ein Integritätsring, und es ist
$(R[X])^* = R^*$.

Beweis. Sind f, g beide $\neq 0$

$$\Longrightarrow \mathrm{grad}(fg) = \underbrace{\mathrm{grad}(f)}_{\geq 0} + \underbrace{\mathrm{grad}(g)}_{\geq 0} \geq 0$$
$$\Longrightarrow fg \neq 0$$

Ist f invertierbar

$$\Longrightarrow 0 = \mathrm{grad}(1) = \mathrm{grad}(ff^{-1}) = \underbrace{\mathrm{grad}(f)}_{\geq 0} + \underbrace{\mathrm{grad}(f^{-1})}_{\geq 0}$$
$$\Longrightarrow \mathrm{grad}(f) = 0 \Longrightarrow f \in R^*$$

□

6.14 Hilbertscher Basissatz

Definition. Sei R ein kommutativer Ring. Dann heißt R *noethersch*, wenn jedes Ideal in R endlich erzeugt ist.

Satz. *Wenn R noethersch ist, dann ist auch der Polynomring $R[X]$ noethersch.*

Beweis. Angenommen, es gibt ein Ideal $\mathfrak{J}$ in $R[X]$, das nicht endlich erzeugt ist. Wähle $f_1 \neq 0$ vom kleinsten Grad in $\mathfrak{J}$ und induktiv eine Folge $f_1, \ldots, f_j, \ldots$ in $\mathfrak{J} \setminus \{0\}$, so daß

$$(*) \qquad \boxed{f_{j+1} \text{ vom kleinsten Grad in } \mathfrak{J} \setminus (f_1, \ldots, f_j)}$$

gilt. Sei b_j der Leitkoeffizient von f_j. Dann erhält man eine Kette von Idealen

$$(b_1) \subset (b_1, b_2) \subset \cdots \subset (b_1, \ldots, b_i) \subset \cdots$$

in R, und es ist $\mathfrak{J} := \bigcup\limits_j (b_1, \ldots, b_j)$ ein Ideal in R, und $\mathfrak{J}$ ist endlich erzeugt, da R noethersch ist.
$\Longrightarrow \exists n \in \mathbb{N}$, so daß $(b_1, \ldots, b_n)$ ein Erzeugendensystem von $\mathfrak{J}$ enthält.
$\Longrightarrow \mathfrak{J} = (b_1, \ldots, b_n)$

$\Longrightarrow \mathfrak{I} \ni b_{n+1} = r_1 b_1 + \cdots + r_n b_n$ mit $r_1, \ldots, r_n \in R$.

$$\begin{aligned}
\text{Sei } g &= \sum_{i=1}^{n} r_i f_i X^{\mathrm{grad}(f_{n+1})-\mathrm{grad}(f_i)} \\
&= r_1 b_1 X^{\mathrm{grad}(f_{n+1})} + \text{ Polynom kleineren Grades} \\
&+ r_2 b_2 X^{\mathrm{grad}(f_{n+1})} + \text{ Polynom kleineren Grades} \\
&+ \cdots \\
&+ r_n b_n X^{\mathrm{grad}(f_{n+1})} + \text{ Polynom kleineren Grades} \\
&= \underbrace{b_{n+1} X^{\mathrm{grad}(f_{n+1})}}_{\text{Leitterm von } f_{n+1}} + \text{ Polynom kleineren Grades}
\end{aligned}$$

$\Longrightarrow \mathrm{grad}(f_{n+1} - g) < \mathrm{grad}(f_{n+1})$
Dies ist ein Widerspruch zu $(*)$, da $g \in (f_1, \ldots, f_n)$ und also
$f_{n+1} - g \in \mathfrak{I} \setminus (f_1, \ldots, f_n)$ gilt. □

6.15 Übungsaufgaben 20 – 22

Aufgabe 20. Sei K ein Körper.

(1) Man zeige, dass die Matrizen der Form $\left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right)$ einen kommutativen Unterring R von $\mathrm{M}_{2\times 2}(K)$ bilden.

(2) Man bestimme die Einheiten und Nullteiler in R.

Aufgabe 21. Es seien R und S zwei Ringe, und es sei $f\colon R \longrightarrow S$ eine Abbildung, die

$$f(x+y) = f(x) + f(y) \text{ und } f(xy) = f(x)f(y)$$

für alle $x, y \in R$ erfüllt. Man zeige, dass $f(1)$ Einselement in $\mathrm{bild}(f)$ ist, aber dass $f(1)$ nicht notwendig Einselement in S ist.

Aufgabe 22. Man zeige

(a) Für Hauptideale (a) und (b) in einem kommutativen Ring gilt: $(a)(b) = (ab)$.

(b) Für Ideale $\mathfrak{I}$ und $\mathfrak{J}$ in einem Ring gilt: $\mathfrak{I}\mathfrak{J} \subset \mathfrak{I} \cap \mathfrak{J}$. Man kontruiere ein Beispiel, in dem $\mathfrak{I}\mathfrak{J} \neq \mathfrak{I} \cap \mathfrak{J}$ gilt.

7 Restklassenringe

7.1 Kongruenzen

Definition. Sei $m \in \mathbb{N}$ vorgegeben. Zwei Zahlen $a, b \in \mathbb{Z}$ heißen *kongruent modulo* m, wenn sie bei Division durch m densselben Rest r mit $0 \leq r < m$ ergeben. Man schreibt dann

$$\boxed{a \equiv b \bmod m}\,.$$

Beispiele.

- $m = 21 \Longrightarrow 54 \equiv 33 \equiv 12 \bmod 21$, da
$$\begin{aligned} 54 &= 2 \cdot 21 + 12 \\ 33 &= 1 \cdot 21 + 12 \\ 12 &= 0 \cdot 21 + 12 \end{aligned}$$
- $m = 5 \Longrightarrow 11 \equiv 6 \equiv 1 \bmod 5$, da
$$\begin{aligned} 11 &= 2 \cdot 5 + 1 \\ 6 &= 1 \cdot 5 + 1 \\ 1 &= 0 \cdot 5 + 1 \end{aligned}$$
- $m = 5 \Longrightarrow -7 \equiv 3 \bmod 5$, da $-7 = -2 \cdot 5 + 3$ und $3 = 0 \cdot 5 + 3$
- Definiere
$$\begin{aligned} \bar{1} &:= \{a \in \mathbb{Z} \mid a \equiv 1 \bmod 5\} = \{\ldots, -9, -4, 1, 6, 11, \ldots\} \\ \bar{2} &:= \{a \in \mathbb{Z} \mid a \equiv 2 \bmod 5\} = \{\ldots, -8, -3, 2, 7, 12, \ldots\} \\ \bar{3} &:= \{a \in \mathbb{Z} \mid a \equiv 3 \bmod 5\} = \{\ldots, -7, -2, 3, 8, 13, \ldots\} \\ \bar{4} &:= \{a \in \mathbb{Z} \mid a \equiv 4 \bmod 5\} = \{\ldots, -6, -1, 4, 9, 14, \ldots\} \\ \bar{0} &:= \{a \in \mathbb{Z} \mid a \equiv 0 \bmod 5\} = \{0, \pm 5, \pm 10, \pm 15, \ldots\} \end{aligned}$$
Für jedes $r \in \mathbb{Z}$ mit $0 \leq r < 5$ gilt
$$\bar{r} = a + 5\mathbb{Z} =: \bar{a} \quad \forall\, a \in \bar{r}$$
- Für jedes $m \in \mathbb{N}$ erhält man analog den *Restklassenring*
$$\mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{m-1}\}$$
mit $\bar{r} = \{a \in \mathbb{Z} \mid a \equiv r \bmod m\} = a + m\mathbb{Z} =: \bar{a} \quad \forall\, a \in \bar{r}$
und $r = 0, 1, \ldots, m-1$.
Es gilt $\bar{a} + \bar{b} = \overline{a+b}$ und $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$ (z.B. $m = 5 \Longrightarrow \bar{3} + \bar{4} = \bar{7} = \bar{2}$).
- Uhren messen Stunden modulo 12 oder modulo 24.

7.2 Rechnen mit Restklassen

Definition. Sei $\mathfrak{I}$ ein Ideal in einem Ring R. Für $a \in R$ sei

$$\boxed{a + \mathfrak{I} := \{a + x \mid x \in \mathfrak{I}\}}$$

die *Restklasse von a bezüglich* $\mathfrak{I}$.

Lemma. *Für $a, b \in R$ gilt:*

$$\boxed{a + \mathfrak{I} = b + \mathfrak{I}} \Longleftrightarrow \boxed{a - b \in \mathfrak{I}}$$

Beweis. "$\Rightarrow$" $a = a + 0 = b + x$ mit $x \in \mathfrak{I}$
$\Longrightarrow a - b = x \in \mathfrak{I}$

"$\Leftarrow$" $a - b =: x \in \mathfrak{I} \Longrightarrow a = b + x \in b + \mathfrak{I}$
$\Longrightarrow a + y = b + \underbrace{x + y}_{\in \mathfrak{I}} \in b + \mathfrak{I} \quad \forall y \in \mathfrak{I}$
$\Longrightarrow a + \mathfrak{I} \subset b + \mathfrak{I}$
Ist $a - b =: x \in \mathfrak{I} \Longrightarrow b - a = -x \in \mathfrak{I} \Longrightarrow b + \mathfrak{I} \subset a + \mathfrak{I}$ analog.

□

Definition. Zwei Elemente $a, b \in R$ heißen *kongruent modulo* $\mathfrak{I}$, falls $\boxed{a - b \in \mathfrak{I}}$ gilt. Man schreibt $\boxed{a \equiv b \bmod \mathfrak{I}}$.

Satz. *Die Menge $R/\mathfrak{I} := \{a + \mathfrak{I} \mid a \in R\}$ bildet einen Ring bezüglich*

$$\boxed{a + \mathfrak{I} + b + \mathfrak{I} := a + b + \mathfrak{I}} \text{ und } \boxed{(a + \mathfrak{I}) \cdot (b + \mathfrak{I}) = a \cdot b + \mathfrak{I}} \quad \forall a, b \in R.$$

Nullelement ist $\mathfrak{I}$, und Einselement ist $1+\mathfrak{I}$. Ist R kommutativ, so auch $R/\mathfrak{I}$.

Beweis. Wie leicht zu sehen ist, übertragen sich die Ringeigenschaften von R auf $R/\mathfrak{I}$. Zu zeigen ist die Wohldefiniertheit der Verknüpfungen.
Sei $a + \mathfrak{I} = \tilde{a} + \mathfrak{I}$. Dann ist $a - \tilde{a} \in \mathfrak{I}$. nach dem Lemma. Bezüglich Addition folgt $(a + b) - (\tilde{a} + b) \in \mathfrak{I}$. Also $a + b + \mathfrak{I} = \tilde{a} + b + \mathfrak{I}$ nach dem Lemma. Bezüglich Multiplikation folgt $(a - \tilde{a})b \in \mathfrak{I}$, da $\mathfrak{I}$ Rechtsideal. Mit dem Lemma folgt $ab + \mathfrak{I} = \tilde{a}b + \mathfrak{I}$.
Analog zeigt man, daß die Verknüpfungen nicht von der Wahl des Repräsentanten $\tilde{b} \in b + \mathfrak{I}$ abhängen. Bezüglich Multiplikation benutzt man dann, dass $\mathfrak{I}$ Linksideal ist. □

Definition. Der Ring $R/\mathfrak{I}$ heißt *Restklassenring* oder *Faktorring* von R modulo $\mathfrak{I}$.

Bemerkung. Es gelten:

1. $\mathfrak{I} = R \Longrightarrow R/\mathfrak{I} = \{\mathfrak{I}\}$.
2. $\mathfrak{I} = (0) \Longrightarrow R/\mathfrak{I} = R$.

7.3 Ideale im Restklassenring

Satz. *Seien R ein Ring, $\mathfrak{I} \neq R$ ein Ideal in R, und*

$$\pi\colon R \longrightarrow R/\mathfrak{I},\ r \longmapsto r+\mathfrak{I},$$

die kanonische Abbildung. *Dann ist π ein surjektiver Ringhomomorphismus, und man hat eine Bijektion*

$$\{\textit{Ideale in } R/\mathfrak{I}\} \xrightarrow{\sim} \{\textit{Ideale } \mathfrak{J} \textit{ in } R \textit{ mit } \mathfrak{J} \supset \mathfrak{I}\},\ \mathfrak{a} \longmapsto \pi^{-1}(\mathfrak{a}).$$

Beweis. Es ist $\pi^{-1}(\mathfrak{a}) = \{v \in R \mid \pi(v) \in \mathfrak{a}\}$ ein Ideal in R, da π ein Homomorphismus ist (vgl. Satz 7.2). Da π surjektiv ist, ist $\pi(\pi^{-1}(\mathfrak{a})) = \mathfrak{a}$. Für jedes Ideal $\mathfrak{J}$ mit $\mathfrak{J} \supset \mathfrak{I}$ gilt $\pi^{-1}(\pi(\mathfrak{J})) = \pi^{-1}(\mathfrak{J}/\mathfrak{I}) = \mathfrak{J}$. □

7.4 Primideale und maximale Ideale

Definition. Sei R ein kommutativer Ring. Das Ideal $\mathfrak{J}$ in R heißt *Primideal*, wenn die Menge $R \setminus \mathfrak{J}$ *multiplikativ abgeschlossen* ist. Mit anderen Worten:

$$\boxed{\mathfrak{J} \text{ Primideal in } R} :\Longleftrightarrow \boxed{\mathfrak{J} \neq R \text{ und für } a,b \in R \text{ mit } ab \in \mathfrak{J} \text{ gilt } a \in \mathfrak{J} \text{ oder } b \in \mathfrak{J}}$$

Ein Ideal $\mathfrak{m}$ in R heißt *maximales Ideal*, wenn $\mathfrak{m} \neq R$ und wenn es kein Ideal $\mathfrak{I}$ in R gibt mit $\mathfrak{m} \subsetneqq \mathfrak{I} \subsetneqq R$.

Satz. *Sei $\mathfrak{I}$ ein Ideal in R. Dann gelten:*

(1) *$\mathfrak{I}$ Primideal $\Longleftrightarrow$ $R/\mathfrak{I}$ Integritätsring.*

(2) *$\mathfrak{I}$ maximales Ideal $\Longleftrightarrow$ $R/\mathfrak{I}$ Körper.*

(3) *Jedes maximale Ideal ist Primideal.*

(4) *(0) ist Primideal $\Longleftrightarrow$ R ist Integritätsring.*

Beweis. Es ist $\mathfrak{I}$ das Nullelement in $R/\mathfrak{I}$.

(1) "$\Rightarrow$" Sind zwei Restklassen $a+\mathfrak{I}$ und $b+\mathfrak{I}$ beide $\neq \mathfrak{I}$, so gilt $a, b \notin \mathfrak{I}$, also $ab \notin \mathfrak{I}$, da $\mathfrak{I}$ Primideal. Es folgt $ab+\mathfrak{I} = (a+\mathfrak{I})(b+\mathfrak{I}) \neq \mathfrak{I}$.

"$\Leftarrow$" Sind $a+\mathfrak{I}$ und $b+\mathfrak{I}$ beide $\neq \mathfrak{I}$, so folgt $ab+\mathfrak{I} = (a+\mathfrak{I})(b+\mathfrak{I})$, da $R/\mathfrak{I}$ Integritätsring. $\underset{7.2}{\Longrightarrow}$ $ab \notin \mathfrak{I}$.

(2) "⇒" Seien $\mathfrak{I}$ ein maximales Ideal in R und $a \in R/\mathfrak{I}$.
Zu zeigen: $a + \mathfrak{I}$ invertierbar. Sei $\mathfrak{J} = Ra + \mathfrak{I}$
$\Longrightarrow \mathfrak{J} = R$, da $a \notin \mathfrak{I}$ und $\mathfrak{I}$ maximal.
$\Longrightarrow 1 \in \mathfrak{J} \Longrightarrow \exists r \in R$ und $x \in \mathfrak{I}$ mit
$1 = ra + x \Longrightarrow (r + \mathfrak{I})(a + \mathfrak{I}) = ra + \mathfrak{I} = 1 + \mathfrak{I}$, da $x \in \mathfrak{I}$.

"⇐" Sei $R/\mathfrak{I}$ Körper $\Longrightarrow \mathfrak{I} \neq R$, und $R/\mathfrak{I}$ besitzt als einzige Ideale sich selbst und das Nullideal. Mit 7.3 folgt, daß R das einzige Ideal ist mit $\mathfrak{I} \subsetneq R$.

(3) folgt aus (1) und (2), und (4) folgt aus (1), (da $R/(0) = R$).

□

7.5 Das Zornsche Lemma

Definition. Seien M eine Menge und $H \subset M \times M$. Statt $(x, y) \in H$ schreiben wir $x \leq y$ und sprechen von einer *Relation* $\leq$. Dann heißt M *halbgeordnet (partiell geordnet)* bezüglich $\leq$, wenn für $x, y, z \in M$ gilt:

1. $x \leq x$

2. $x \leq y$ und $y \leq z \Longrightarrow x \leq z$

3. $x \leq y$ und $y \leq x \Longrightarrow x = y$

   M heißt *geordnet* oder *Kette*, falls zusätzlich gilt:

4. $x, y \in M \Longrightarrow x \leq y$ oder $y \leq x$.

Sei M halbgeordnet bezüglich $\leq$. Ein Element $a \in M$ heißt *obere Schranke* einer (bezüglich $\leq$) geordneten Menge $N \subset M$, wenn $x \leq a \quad \forall\, x \in N$ gilt. Ein Element $a \in M$ heißt *maximal*, wenn aus $a \leq x$ für $x \in M$ stets $a = x$ folgt.

Lemma von Zorn. *Sei M eine nicht-leere, halbgeordnete Menge. Jede geordnete Teilmenge von M besitze eine obere Schranke. Dann besitzt M ein* maximales *Element.*

(vgl. M. Zorn, A remark on methods in transfinite algebra, Bull. Amer. Math. Soc. (1935) 667-670)

7.6 Existenz maximaler Ideale

Satz. *Sei R ein kommutativer Ring und $\mathfrak{I} \neq R$ ein Ideal in R. Dann gibt es ein maximales Ideal $\mathfrak{m}$ in R mit $\mathfrak{I} \subset \mathfrak{m}$. Insbesondere besitzt jeder kommutative Ring $\neq \{0\}$ ein maximales Ideal.*

Beweis. Sei $M := \{\text{Ideale } \mathfrak{J} \text{ in } R \mid \mathfrak{J} \neq R \text{ und } \mathfrak{I} \subset \mathfrak{J}\}$. Dann ist M bezüglich $\subset$ halbgeordnet. Da $\mathfrak{I} \in M \Longrightarrow M \neq \emptyset$. Sei $N \neq \emptyset$ eine geordnete Teilmenge von M. Dann ist $\mathfrak{J} = \bigcup_{\mathfrak{a} \in N} \mathfrak{a}$ ein Ideal in R mit $\mathfrak{I} \subset \mathfrak{J}$. Wäre $\mathfrak{J} = R$, so wäre $1 \in \mathfrak{J}$, also $1 \in \mathfrak{a}$ für ein $\mathfrak{a} \in N$, was $\mathfrak{a} \neq R$ widerspräche. Es folgt $\mathfrak{J} \in M$, und $\mathfrak{J}$ ist obere Schranke von N. Nach 7.5 besitzt M ein maximales Element, und dies ist das gesuchte Ideal. Anwendung auf $\mathfrak{I} = 0$ ergibt die zweite Behauptung. □

7.7 Der Homomorphiesatz für Ringe

Definition. Ein bijektiver Ringhomomorphismus heißt *Isomorphismus* (und dessen Umkehrabbildung ist auch ein Isomorphismus).

Homomorphiesatz. *Ist $f\colon R \longrightarrow R'$ ein surjektiver Homomorphismus von Ringen, dann induziert f einen Isomorphismus*

$$\bar{f}\colon R/\operatorname{kern}(f) \longrightarrow R', r + \operatorname{kern}(f) \longmapsto f(r).$$

Beweis. **Wohldefiniertheit:** $r + \operatorname{kern}(f) = \tilde{r} + \operatorname{kern}(f)$
$\underset{7.2}{\Longrightarrow} r - \tilde{r} \in \operatorname{kern}(f) \Longrightarrow f(r) = f(\tilde{r})$.

Homomorphie: folgt, weil f Homomorphismus.

Injektivität: $\bar{f}(r + \operatorname{kern}(f)) = f(r) = 0$
$\Longleftrightarrow r \in \operatorname{kern}(f) \Longleftrightarrow r + \operatorname{kern}(f) = 0 + \operatorname{kern}(f)$

Surjektivität: Klar, da f surjektiv.

□

7.8 Chinesischer Restsatz

- Das kartesische Produkt von endlich vielen Ringen ist stets ein Ring bezüglich komponentenweiser Addition und Multiplikation.
- Zwei Ideale $\mathfrak{I}, \mathfrak{J}$ in einem Ring R heißen *teilerfremd*, wenn $\mathfrak{I} + \mathfrak{J} = R$ gilt.

Lemma. *Sind $\mathfrak{J}_1, \ldots, \mathfrak{J}_n$ paarweise teilerfremde Ideale in einem Ring R, so ist*
$\mathfrak{J}_k + \bigcap\limits_{j \neq k} \mathfrak{J}_j = R$ *für jedes* $k = 1, \ldots, n$.

Beweis. Sei $k \in \{1, \ldots, n\}$. Dann gibt es zu jedem $j \neq k$ Elemente $a_j \in \mathfrak{J}_k$ und $b_j \in \mathfrak{J}_j$ mit $a_j + b_j = 1$, (denn $\mathfrak{J}_k + \mathfrak{J}_j = R$ nach Voraussetzung). Es folgt

$$1 = \prod_{j \neq k} (a_j + b_j) \in (\mathfrak{J}_k + \prod_{j \neq k} \mathfrak{J}_j) \underset{\text{Aufgabe 22}}{\subset} \mathfrak{J}_k + \bigcap_{j \neq k} \mathfrak{J}_j$$

und damit die Behauptung, da $(1) = R$. □

Chinesischer Restsatz. *Sei R ein Ring, und seien $\mathfrak{J}_1, \ldots, \mathfrak{J}_n$ paarweise teilerfremde Ideale in R. Dann ist der Homomorphismus*

$$f\colon R \longrightarrow R/\mathfrak{J}_1 \times \cdots \times R/\mathfrak{J}_n, \ r \longmapsto (r + \mathfrak{J}_1, \ldots, r + \mathfrak{J}_n)$$

surjektiv mit $\operatorname{kern}(f) = \bigcap\limits_{j=1}^{n} \mathfrak{J}_j$. *Insbesondere induziert f einen Isomorphismus*

$$R/\bigcap_{j=1}^{n} \mathfrak{J}_j \xrightarrow{\sim} R/\mathfrak{J}_1 \times \cdots \times R/\mathfrak{J}_n.$$

Beweis. Nach dem Lemma gibt es zu jedem $k \in \{1, \ldots, n\}$ Elemente $c_k \in \mathfrak{J}_k$ und $d_k \in \bigcap\limits_{j \neq k} \mathfrak{J}_j$ (also $d_k \in \mathfrak{J}_j \quad \forall j \neq k$) mit $c_k + d_k = 1$ (also mit $d_k - 1 \in \mathfrak{J}_k$).

$$\underset{7.2}{\Longrightarrow} \boxed{d_k + \mathfrak{J}_k = 1 + \mathfrak{J}_k} \text{ und } \boxed{d_k + \mathfrak{J}_j = \mathfrak{J}_j \text{ für } j \neq k}$$

Sei nun $(r_1 + \mathfrak{J}_1, \ldots, r_n + \mathfrak{J}_n) \in R/\mathfrak{J}_1 \times \cdots \times R/\mathfrak{J}_n$. Setze $r = r_1 d_1 + \cdots + r_n d_n$. Dann folgt

$$f(r) \underset{\text{Def}}{=} (r + \mathfrak{J}_1, \ldots, r + \mathfrak{J}_n) = (r_1 + \mathfrak{J}_1, \ldots, r_n + \mathfrak{J}_n)$$

Also ist f surjektiv. Die Aussage über den Kern ist ersichtlich, und die letzte Behauptung folgt aus dem Homomorphiesatz 7.7. □

Korollar. *Für beliebige Elemente $r_1, \ldots, r_n \in R$ und paarweise teilerfremde Ideale $\mathfrak{J}_1, \ldots, \mathfrak{J}_n$ ist das Kongruenzensystem*

$$x \equiv r_1 \bmod \mathfrak{J}_1, \ldots, x \equiv r_n \bmod \mathfrak{J}_n$$

immer lösbar, und ist r eine Lösung, so ist die Menge $r + \bigcap\limits_{j=1}^{n} \mathfrak{J}_j$ *die Menge aller Lösungen.*

7.9 Übungsaufgaben 23 – 27

Aufgabe 23. Sei R ein kommutativer Ring. Man zeige, dass die folgenden drei Bedingungen äquivalent sind:

(1) R ist noethersch.

(2) Jede Kette $\mathfrak{I}_1 \subset \mathfrak{I}_2 \subset \cdots \subset \mathfrak{I}_m \subset \cdots$ von Idealen in R wird stationär, d.h. es gibt ein $n \in \mathbb{N}$ mit $\mathfrak{I}_{n+k} = \mathfrak{I}_n$ für alle $k \in \mathbb{N}$.

(3) Jede nichtleere Menge M von Idealen in R besitzt ein maximales Element (das ist ein Ideal $\mathfrak{I} \in M$ mit der Eigenschaft: $\mathfrak{J} \in M$ und $\mathfrak{J} \supset \mathfrak{I} \Longrightarrow \mathfrak{I} = \mathfrak{J}$).

Bemerkung. Hieraus folgt, dass in einem noetherschen Ring jedes Ideal $\mathfrak{I} \neq R$ in einem maximalen Ideal enthalten ist. Der Nachweis gelingt hier also, ohne das Lemma von Zorn zu benutzen.

Aufgabe 24. Seien $\mathfrak{I}$ und $\mathfrak{J}$ zwei teilerfremde Ideale in einem kommutativen Ring R. Man zeige, dass dann $\mathfrak{I}\mathfrak{J} = \mathfrak{I} \cap \mathfrak{J}$ gilt.

Aufgabe 25. Seien R ein kommutativer Ring, $\mathfrak{I}$ ein Ideal in R und $a \in R$. Man zeige, dass die Restklasse $a + \mathfrak{I}$ genau dann eine Einheit in $R/\mathfrak{I}$ ist, wenn die beiden Ideale (a) und $\mathfrak{I}$ teilerfremd sind.

Aufgabe 26. Man löse in $\mathbb{Z}$ das Kongruenzensystem $x \equiv 6 \bmod 5$, $x \equiv 5 \bmod 6$,
$x \equiv 7 \bmod 7$ gemäß dem unten angegebenen Verfahren.

Verfahren zur Lösung von Kongruenzensystemen. *Der Beweis des Chinesischen Restsatzes 8.12 liefert ein praktisches Verfahren zur Lösung von Kongruenzsystemen der Form*

$$x \equiv a_1 \bmod m_1\,,\ x \equiv a_2 \bmod m_2\,,\ \ldots,\ x \equiv a_n \bmod m_n\,,$$

wenn die Zahlen $m_1, \ldots, m_n \in \mathbb{N}$ paarweise teilerfremd sind.

1. Schritt: Berechne $M_1 := \prod_{j=2}^{n} m_j\,, \ldots,\ M_k := \prod_{j \neq k} m_j\,, \ldots,\ M_n := \prod_{j=1}^{n-1} m_j\,.$

2. Schritt: Bestimme $x_1, \ldots, x_n$ mit $x_1 M_1 \equiv 1 \bmod m_1, \ldots, x_n M_n \equiv 1 \bmod m_n$.
Es ist dann $d_k := x_k M_k \in \prod_{j \neq k} (m_j) = \bigcap_{j \neq k} (m_j)$ und $d_k - 1 \in (m_k)$ für jedes $k \in \{1, \ldots, n\}$.

3. Schritt: *Berechne* $r := r_1 d_1 + \cdots + r_n d_n$ *mit* $d_k = x_k M_k$ *und* $r_k \equiv a_k \bmod m_k$.

4. Schritt: *Prüfe, dass tatsächlich* $r \equiv a_1 \bmod m_1, \ldots, \; r \equiv a_n \bmod m_n$ *gilt und damit* r *die modulo* $m = m_1 \cdot \ldots \cdot m_n$ *eindeutig bestimmte Lösung ist.*

Beispiel. Man löse das Kongruenzsystem $x \equiv 2 \bmod 7$, $x \equiv 4 \bmod 8$, $x \equiv 10 \bmod 9$.

1. Schritt: Berechne $M_1 := 8 \cdot 9 = 72$, $M_2 := 7 \cdot 9 = 63$, $M_3 := 7 \cdot 8 = 56$.

2. Schritt: Die Zahlen $x_1 = 4 \;\; x_2 = -1$ und $x_3 = -4$ erfüllen
$x_1 M_1 \equiv 1 \bmod 7 \;\; x_2 M_2 \equiv 1 \bmod 8$ und $x_3 M_3 \equiv 1 \bmod 9$.

3. Schritt: Berechne $r := 2 \cdot 288 - 4 \cdot 63 - 1 \cdot 224 = 576 - 476 = 100$.

4. Schritt: Es ist $r = 100$ tatsächlich die modulo $7 \cdot 8 \cdot 9 = 504$ eindeutig bestimmte Lösung, denn $100 \equiv 2 \bmod 7$, $100 \equiv 4 \bmod 8$ und $100 \equiv 1 \equiv 10 \bmod 9$.

Aufgabe 27. Sei $f\colon R \longrightarrow S$ ein Homomorphismus von kommutativen Ringen $\neq \{0\}$. Man entscheide jeweils, ob das Bild $f(\mathfrak{I})$ eines Ideals $\mathfrak{I}$ in R und das Urbild $f^{-1}(\mathfrak{J})$ eines Ideals $\mathfrak{J}$ in S wieder ein Ideal ist. Man untersuche dann jeweils, ob sich dabei die Eigenschaft, Primideal bzw. maximales Ideal zu sein, vererbt. Was ändert sich, wenn f als surjektiv vorausgesetzt wird?

8 Teilbarkeit in kommutativen Ringen

Sei R ein kommutativer Ring.

8.1 Division mit Rest im Polynomring

Satz. *Sei $h = c_0 + c_1X + \cdots + c_mX^m \in R[X]$ ein Polynom mit $c_m \in R^*$. Dann gibt es zu jedem Polynom $f \neq 0$ in $R[X]$ eindeutig bestimmte Polynome $g, r \in R[X]$ mit*

$$\boxed{f = gh + r \text{ und } \operatorname{grad}(r) < m \text{ oder } r = 0}$$

Beweis. **Existenz:** Ist $\operatorname{grad}(f) < m$, setze $g = 0$ und $f = r$.
Sei nun $f = a_0 + a_1X + \cdots + a_nX^n$ vom Grad $n \geq m$. Führe Induktion nach n durch.
$n = 0 \Longrightarrow h = c_0 \in R^*$. Setze $g = c_0^{-1}f$ und $r = 0$.
Sei $n > 0 \Longrightarrow f - f_0h$ mit $f_0 = a_nc_m^{-1}X^{n-m}$ hat Grad $< n$.
$\Longrightarrow f - f_0h = gh + r$ mit $\operatorname{grad}(r) < m$ nach Induktionsvoraussetzung
$\Longrightarrow f = (g + f_0)h + r$.

Eindeutigkeit: Da $c_m \in R^*$ ist, gilt $\operatorname{grad}(fh) = \operatorname{grad}(f) + \operatorname{grad}(h)$ für jedes Polynom $f \neq 0$ in $R[X]$.
Sei $gh + r = g'h + r'$ mit $\operatorname{grad}(r) < m$ und $\operatorname{grad}(r') < m$
$\Longrightarrow (g - g')h = r' - r$ mit $\operatorname{grad}(r - r') < m$ nach 6.13 a).
Ist $g = g' \Longrightarrow r' = r$. Ist $g \neq g'$
$\Longrightarrow 0 \leq \operatorname{grad}(g - g') + \underbrace{\operatorname{grad}(h)}_{m} = \operatorname{grad}(r' - r) < m$
$\Longrightarrow$ Widerspruch.

□

8.2 Nullstellen und Linearfaktoren

Lemma. *Besitzt $f \in R[X]$ eine Nullstelle x in R und ist $f \neq 0$, so gibt es ein $g \in R[X]$ mit*

$$\boxed{f = (X - x)g \text{ und } \operatorname{grad}(g) = \operatorname{grad}(f) - 1}$$

Beweis. Nach 8.1 gibt es $g, r \in R[X]$ mit $f = g(X - x) + r$
und $\operatorname{grad}(r) < \operatorname{grad}(X - x) = 1$ oder $r = 0 \Longrightarrow r \in R$.
$\Longrightarrow 0 = f(x) = g(x)(\underbrace{x - x}_{0}) + r = r$
$\Longrightarrow \operatorname{grad}(f) = \operatorname{grad}(g(X - x)) = \operatorname{grad}(g) + 1$ □

Satz. *Sei R ein Integritätsring. Dann hat jedes Polynom in $R[X]$ vom Grad $n \geq 0$ höchstens n Nullstellen in R.*

Beweis. Induktion nach n:
Sei $n = 0$. Ist $f \in R[X]$ vom Grad 0
$\Longrightarrow f = a \in R$ mit $a \neq 0$
$\Longrightarrow f$ hat keine Nullstelle.
Sei $n > 0$, und sei $f \in R[X]$ vom Grad n. Wenn f eine Nullstelle x in R hat, ist $f = (X - x)g$ mit $\mathrm{grad}(g) = n - 1$ (nach Lemma). Besitzt f eine weitere Nullstelle $y \neq x$ in R, so ist y auch Nullstelle von g, denn es ist

$$0 = f(y) = \underbrace{(y - x)}_{\neq 0}\, g(y), \text{ also } g(y) = 0,$$

da R Integritätsring. Nach Induktionsvoraussetzung besitzt g höchstens $n-1$ Nullstellen, also f höchstens n. □

8.3 Euklidische Ringe

Definition. Ein Integritätsring R heißt *euklidisch*, wenn es eine Abbildung

$$\delta \colon R \setminus \{0\} \longrightarrow \mathbb{N} \cup \{0\}$$

gibt mit der Eigenschaft:
Zu je zwei Elementen $a, b \in R$ mit $a \neq 0$ und $\delta(a) \leq \delta(b)$ gibt es Elemente $q, r \in R$ mit

$$\boxed{b = qa + r \text{ und } \delta(r) < \delta(a) \text{ oder } r = 0}\,.$$

Man nennt ein solches δ *Gradabbildung*.

Beispiele. 1. $\mathbb{Z}$: Man setze $\delta(a) = |a|$.

2. $K[X]$, wobei K Körper. Dies folgt aus 8.1. Setze $\delta(f) = \mathrm{grad}(f)$.

Satz. *Jeder euklidische Ring ist Hauptidealring.*

Beweis. Sei $\mathfrak{I} \neq (0)$ ein Ideal in R. Wähle unter den Elementen aus $\mathfrak{I} \setminus \{0\}$ ein a mit minimalem Wert $\delta(a)$. Für jedes $b \in \mathfrak{I}$ ist $b = qa + r$ mit $\delta(r) < \delta(a)$ oder $r = 0$. Es folgt $r = b - qa \in \mathfrak{I}$. Da $\delta(a)$ minimal ist, folgt $r = 0$ und also $b = qa$. Damit ist $\mathfrak{I} \subset (a)$ gezeigt. Da $a \in \mathfrak{I}$, ist $\mathfrak{I} = (a)$. □

8.4 ggT und kgV

Sei R ein Integritätsring.

Definition. (1) Ein Element $a \in R$ heißt *Teiler von* $b \in R$, falls es ein $x \in R$ gibt mit $b = xa$. Wir schreiben dann $a \mid b$ und sagen „a teilt b“.

(2) Ein Element $d \in R$ heißt *größter gemeinsamer Teiler von* $a_1, \dots, a_n \in R$, wenn

(i) $d \mid a_i$ für $i = 1, \dots, n$

(ii) Ist $a \in R$ und gilt $a \mid a_i$ für $i = 1, \dots, n \quad \Longrightarrow a \mid d$

Sind (i) und (ii) erfüllt, schreiben wir

$$\boxed{d = \operatorname{ggT}(a_1, \dots, a_n)}$$

(3) Ein Element $v \in R$ heißt *kleinstes gemeinsames Vielfaches von* $a_1, \dots, a_n$, wenn gilt

(i) $a_i \mid v$ für $i = 1, \dots, n$

(ii) Ist $a \in R$ und gilt $a_i \mid a$ für alle $i = 1, \dots, n \quad \Longrightarrow v \mid a$.

Wir schreiben dann

$$\boxed{v = \operatorname{kgV}(a_1, \dots, a_n)}$$

Bemerkung. Falls existent, sind $\operatorname{ggT}(a_1, \dots, a_n)$ und $\operatorname{kgV}(a_1, \dots, a_n)$ bis auf Multiplikation mit Einheiten eindeutig bestimmt.

Satz. *Seien $a_1, \dots, a_n \in R$. Dann gelten:*

(a) *Ist das von $a_1, \dots, a_n$ erzeugte Ideal $(a_1, \dots, a_n)$ ein Hauptideal (d), so ist $d = \operatorname{ggT}(a_1, \dots, a_n)$.*

(b) *Ist $(a_1) \cap \dots \cap (a_n)$ ein Hauptideal (v), so gilt $v = \operatorname{kgV}(a_1, \dots, a_n)$.*

(c) *Sei R ein Hauptidealring. Dann existiert der größte gemeinsame Teiler $\operatorname{ggT}(a_1, \dots, a_n) =: d$, und es gibt $r_1, \dots, r_n \in R$ mit*

$$\boxed{r_1 a_1 + \dots + r_n a_n = d}$$

Sind $a, b \in R$ teilerfremd, *d.h. $\operatorname{ggT}(a, b) = 1$, so folgt $(a)(b) = (a) \cap (b)$.*

Beweis. (a) (i) $(a_1, \dots, a_n) = (d) \Longrightarrow a_i \in (d)\ \forall i \Longrightarrow d \mid a_i\ \forall i$

(ii) Es gelte $a \mid a_i \; \forall i$. Da $d \in (a_1, \ldots, a_n)$
$\Longrightarrow \exists\, r_1, \ldots, r_n \in R$ mit $d = r_1 a_1 + \cdots + r_n a_n$
$\Longrightarrow a \mid d$.

(b) (i) $\bigcap\limits_i (a_i) = (v) \Longrightarrow v \in (a_i) \; \forall i \Longrightarrow a_i \mid v \; \forall i$

(ii) $a_i \mid a \forall i \Longrightarrow a \in (a_i) \; \forall i \Longrightarrow a \in \bigcap\limits_i (a_i) = (v) \Longrightarrow v \mid a$.

(c) Die erste Behauptung folgt aus (a). Es gilt also

$$\boxed{\mathrm{ggT}(a,b) = 1} \quad \Longrightarrow \quad \boxed{\exists\, r, s \in R \text{ mit } ra + sb = 1}$$
$$\Longrightarrow 1 \in (a) + (b) \Longrightarrow (a) + (b) = R$$
$$\underset{\text{Aufgabe 24}}{\Longrightarrow} (a)(b) = (a) \cap (b)$$

□

8.5 Irreduzible Elemente und Primelemente

Definition. Sei R ein Integritätsring, und sei $p \neq 0$ eine Nichteinheit in R. Dann heißt p *irreduzibel*, wenn für jede Zerlegung $p = ab$ mit $a, b \in R$ stets folgt $a \in R^*$ oder $b \in R^*$, und p heißt *Primelement*, wenn das Hauptideal (p) ein *Primideal* ist (d.h. falls aus $p \mid ab$ für $a, b \in R$ stets folgt $p \mid a$ oder $p \mid b$).

Satz. *Es gilt stets:*

$$\boxed{p \textit{ Primelement}} \quad \Longrightarrow \quad \boxed{p \textit{ irreduzibel}}$$

Ist R ein Hauptidealring, so sind äquivalent:

(i) *p irreduzibel*

(ii) *(p) maximales Ideal*

(iii) *p Primelement*

Beweis. Sei p ein Primelement, und sei $p = ab \Longrightarrow p \mid a$ oder $p \mid b$.
Wenn $p \mid a$ gilt $\Longrightarrow \exists\, r \in R$ mit $a = pr$.
$\Longrightarrow p = ab = prb \Longrightarrow p(1 - rb) = 0$.
$\Longrightarrow rb = 1$, da $p \neq 0$ und R Integritätsring $\Longrightarrow b \in R^*$.
Analog falls $p \mid b$.

Sei nun R ein Hauptidealring.

$(i) \Rightarrow (ii)$ Sei $\mathfrak{I} = (a)$ ein Ideal in R mit $(p) \subset (a) \subset R \Longrightarrow p \in (a)$
$\Longrightarrow p = ab$ mit $b \in R$
$\Longrightarrow a \in R^*$ oder $b \in R^*$, da p irreduzibel.
Ist $a \in R^* \Longrightarrow (a) = R$
Ist $b \in R^* \Longrightarrow a = b^{-1}p \in (p) \Longrightarrow (p) = (a)$

$(ii) \Rightarrow (iii)$ Nach 7.4.3 ist jedes maximale Ideal ein Primideal. Also ist (p) ein Primideal.

$(iii) \Rightarrow (i)$ Ist oben schon allgemein gezeigt.

□

$$\boxed{R \text{ euklidisch}} \underset{\underbrace{\not\Leftarrow}_{\text{i.a.}}}{\overset{}{\underset{8.3}{\Longrightarrow}}} \boxed{R \text{ Hauptidealring}} \underset{\underbrace{\not\Leftarrow}_{\text{i.a.}}}{\overset{}{\underset{8.10}{\Longrightarrow}}} \boxed{R \text{ faktoriell}}$$

8.6 Beispiel

Sei $R = \mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$. Dann ist 2 irreduzibel in R.

Beweis. Sei $2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$ mit $a, b, c, d \in \mathbb{Z}$.
$\Longrightarrow 2 = \bar{2} = (a - b\sqrt{-5})(c - d\sqrt{-5})$
$\Longrightarrow 4 = 2 \cdot \bar{2} = (a^2 + 5b^2)(c^2 + 5d^2) \in \mathbb{Z}$.
Da $a^2 + 5b^2 = 2$ mit $a, b \in \mathbb{Z}$ nicht lösbar ist, genügt es wegen der eindeutigen Primfaktorzerlegung in $\mathbb{Z}$, den Fall

$$a^2 + 5b^2 = 4 \quad \text{und} \quad c^2 + 5d^2 = 1$$

zu betrachten. Es folgt $c = \pm 1$ und $d = 0$ und $b = 0$ und $a = \pm 2$. □

Es ist aber 2 kein Primelement in R, denn
$(2) \ni 3 \cdot 2 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ und $1 \pm \sqrt{-5} \neq (a + b\sqrt{-5}) \cdot 2 \quad \forall\, a, b \in \mathbb{Z}$,
also ist keiner der beiden Faktoren $1 \pm \sqrt{-5}$ in (2).
Mit Satz 8.5 folgt: $\mathbb{Z}[\sqrt{-5}]$ ist kein Hauptidealring. In $\mathbb{Z}[\sqrt{-5}]$ gibt es keine eindeutige Zerlegbarkeit in Produkte von irreduziblen Elementen

$$6 = \underset{irr.}{3} \cdot \underset{irr.}{2} = (1 + \underset{irr.}{\sqrt{-5}})(1 - \underset{irr.}{\sqrt{-5}})$$

(vgl. Aufgabe 29).

8.7 Assoziierte Elemente

Definition. Zwei Elemente a, b in einem Integritätsring R heißen *assoziiert*, wenn $a = \varepsilon b$ mit $\varepsilon \in R^*$.

Bemerkung.

$$\boxed{a \text{ assoziiert } b} \iff \boxed{(a) = (b)} \iff \boxed{a \mid b \text{ und } b \mid a}$$

Beweis. 1. $a = \varepsilon b \Longrightarrow a \in (b)$ und $b = \varepsilon^{-1} a \in (a) \Longrightarrow (a) = (b)$

2. $(a) = (b) \Longrightarrow a \mid b$ und $b \mid a$ nach Definition 8.4

3. $a \mid b$ und $b \mid a \Longrightarrow \exists r, s \in R$ mit $b = sa$ und $a = rb = rsa$
Ist $a = 0 \Longrightarrow b = 0 \Longrightarrow a = 1 \cdot b$.
Ist $a \neq 0 \Longrightarrow 1 = rs$ (da R Integritätsring und $\underbrace{a}_{\neq 0}(1 - rs) = 0$)
$\Longrightarrow r \in R^* \Longrightarrow a$ assoziiert b.

□

8.8 Eindeutigkeit von Primfaktorzerlegungen

Satz. *Sei R ein Integritätsring. Wenn $p_1 \cdots p_m = q_1 \cdots q_n$ mit Primelementen $p_1, \ldots, p_m, q_1, \ldots, q_n$ in R gilt, ist $n = m$, und nach eventueller Umnumerierung ist p_i assoziiert zu q_i $\forall\, i = 1, \ldots, n$.*

Beweis. $p_1 \mid q_1 \cdots q_n \Longrightarrow p_1 \mid q_j$ für ein j, da p_1 Primelement. Numeriere die q_j so um, daß $p_1 \mid q_1$ gilt. Dann ist $p_1 = \varepsilon_1 q_1$ mit $\varepsilon_1 \in R^*$, da q_1 irreduzibel ist nach Satz 8.5.
$\Longrightarrow \varepsilon_1 q_1 p_2 \cdots p_m = q_1 \cdots q_n$
$\Longrightarrow \varepsilon_1 p_2 \cdots p_m = q_2 \cdots q_n$,
da R Integritätsring. Setze dieses Verfahren induktiv fort. □

8.9 Primfaktorzerlegung in Hauptidealringen

Satz. *Sei R ein Hauptidealring, und sei $a \neq 0$ eine Nichteinheit in R. Dann besitzt a eine Zerlegung $a = p_1 \cdots p_n$ mit Primelementen $p_1, \ldots, p_n \in R$. Bis auf Assoziiertheit und Reihenfolge ist diese Zerlegung eindeutig.*

Beweis. Sei M die Menge aller Hauptideale (x) in R, wobei $x \neq 0$ Nichteinheit und x keine Zerlegung in Primelemente besitzt.
Zu zeigen: $M = \emptyset$. Ist $M \neq \emptyset \underset{\text{Aufgabe 23}}{\Longrightarrow} M$ besitzt ein maximales Element (x), da R als Hauptidealring noethersch. Es ist $x = x_1 x_2$ mit Nichteinheiten

$x_1, x_2 \in R$ (denn sonst wäre x irreduzibel, also Primelement nach Satz 8.5 und also $x \notin M$).

$$\Longrightarrow (x) \subsetneq (x_1) \quad \text{und} \quad (x) \subsetneq (x_2)$$

(denn wäre $x_1 \in (x)$, also $x_1 = rx = rx_1x_2$, so wäre $1 = rx_2$ und also x_2 Einheit).
Da (x) maximal $\Longrightarrow x_1, x_2 \notin M$
$\Longrightarrow x_1, x_2$ haben Zerlegung in Primelemente
$\Longrightarrow x = x_1x_2$ hat Zerlegung in Primelemente
Dies ist ein Widerspruch zu $x \in M$. $\Longrightarrow M = \emptyset$.
Die Eindeutigkeitsaussage folgt aus 8.8. □

8.10 Faktorielle Ringe

Definition. Ein Integritätsring R heißt *faktoriell* oder *ZEP-Ring*, falls sich jede Nichteinheit $\neq 0$ in R als ein (endliches) Produkt von Primelementen schreiben läßt.

Bemerkung. Ist R faktoriell, so ist jedes irreduzible Element Primelement.

Beweis. Sei $r \in R$ irreduzibel und $r = p_1 \cdots p_n$ eine Zerlegung in R mit Primelementen $p_1, \ldots, p_n \Longrightarrow n = 1$, da r irreduzibel. □

Beispiele. Jeder Hauptidealring ist faktoriell (nach 8.9), insbesondere sind $\mathbb{Z}$ und $K[X]$, wobei K Körper, faktoriell (vgl. 8.3) und $\mathbb{Z}[\sqrt{-5}]$ ist nicht faktoriell (vgl. 8.6).

Satz. *Sei R ein Integritätsring. Dann gilt:*
R ist genau dann faktoriell, wenn sich jede Nichteinheit $x \neq 0$ in R (bis auf Assoziiertheit und Reihenfolge) eindeutig als (endliches) Produkt von irreduziblen Elementen schreiben läßt.

Beweis. "$\Rightarrow$" Es ist $x = p_1 \cdots p_n$ mit Primelementen $p_1, \ldots, p_n$ nach Definition. Nach 8.8 folgt die Eindeutigkeit der Zerlegung, und nach 8.5 sind die p_i irreduzibel.

"$\Leftarrow$" Es genügt zu zeigen, daß jedes irreduzible Element ein Primelement ist.
Sei $p \in R$ irreduzibel, und es gelte $p \mid ab$ mit $a, b \in R$. Zu zeigen: $p \mid a$ oder $p \mid b$.

1. Fall: $a \in R^* \Longrightarrow p \mid b$, denn $ab = rp$ mit $r \in R \Longrightarrow b = a^{-1}rp$.
2. Fall: $b \in R^* \Longrightarrow p \mid a$ analog.

Seien a, b Nichteinheiten, $a = p_1 \cdots p_m$ und $b = q_1 \cdots q_n$ Zerlegungen in irreduzible Elemente.
$\Longrightarrow p \mid p_1 \cdots p_m q_1 \cdots q_n$ (da $p \mid ab$)
$\Longrightarrow p$ ist assoziiert zu einem p_i oder einem q_j wegen der Eindeutigkeit der Zerlegung von $ab \Longrightarrow p \mid a$ oder $p \mid b$.

$\square$

8.11 Existenz von ggT und kgV in faktoriellen Ringen

Sei R faktoriell und $a_1, \ldots, a_n \in R \setminus \{0\}$. Dann gibt es paarweise nicht-assoziierte Primelemente $p_1, \ldots, p_m$ und Zahlen $r_1(a_i), \ldots, r_m(a_i)$, so daß

$$a_i = \varepsilon_i p_1^{r_1(a_i)} \cdots p_m^{r_m(a_i)} \text{ mit } \varepsilon_i \in R^* \text{ für } i = 1, \ldots, n.$$

Setze $r_j = \min(r_j(a_i) \mid i = 1, \ldots, n)$ und $s_j = \max(r_j(a_i) \mid i = 1, \ldots, n)$. Bis auf Assoziiertheit ist dann

$$\boxed{\mathrm{ggT}(a_1, \ldots, a_n) = p_1^{r_1} \cdots p_m^{r_m}} \quad \text{und} \quad \boxed{\mathrm{kgV}(a_1, \ldots, a_n) = p_1^{s_1} \cdots p_m^{s_m}}$$

8.12 Spezielle Version des Chinesischen Restsatzes

Satz. *Sei R ein Hauptidealring, und sei $a = \varepsilon p_1^{n_1} \cdots p_m^{n_m}$ eine Primfaktorzerlegung in R mit einer Einheit ε und paarweise nicht assoziierten Primelementen $p_1, \ldots, p_m$. Dann sind die Ideale $(p_1^{n_1}), \ldots, (p_m^{n_m})$ paarweise teilerfremd, und es gilt $a = \mathrm{kgV}(p_1^{n_1}, \ldots, p_m^{n_m})$ und $(a) = \bigcap_{i=1}^m (p_i^{n_i})$. Insbesondere gibt es einen kanonischen Isomorphismus*

$$\boxed{R/(a) \xrightarrow{\sim} R/(p_1^{n_1}) \times \cdots \times R/(p_m^{n_m})}$$

Beweis. Dies folgt aus dem Chinesischen Restsatz 7.8 und der idealtheoretischen Charakterisierung von ggT und kgV in Satz 8.4. $\square$

Beispiel. $\mathbb{Z}/(15) \simeq \mathbb{Z}/(3) \times \mathbb{Z}/(5)$

8.13 Beispiele für Körper

Satz. (a) *Für jede Primzahl $p \in \mathbb{N}$ gilt:*

$$\boxed{p \text{ Primzahl}} \quad \Longleftrightarrow \quad \boxed{\mathbb{Z}/p\mathbb{Z} \text{ Körper}}$$

(b) *Für jedes nicht-konstante Polynom $f \in K[X]$, wobei K Körper, gilt*

$$\boxed{f \text{ irreduzibel}} \quad \Longleftrightarrow \quad \boxed{K[X]/(f) \text{ ist Körper}}$$

Beweis. "$\Rightarrow$" Nach 8.5 sind (p) und (f) maximale Ideale $\Longrightarrow$ Behauptung nach 7.4.

"$\Leftarrow$" Sei $R = \mathbb{Z}$ oder $K[X]$ und $a = p$ oder f. Ist a wie in 8.12 zerlegt in mindestens zwei Primfaktoren, so ist $R/(a)$ kein Körper, denn z.B. $(1, 0, \ldots, 0) \notin R^*$.

□

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

8.14 Übungsaufgaben 28 – 30

Aufgabe 28. (1) Es sei $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Man bestimme den größten gemeinsamen Teiler der Polynome $f = X^5 + X^4 + X^3 + X^2 + X + 1$ und $g = X^4 - X^3 - X + 1$ in $\mathbb{F}_2[X]$.

(2) Man zeige, dass die Polynome $X^3 + 2X^2 - X - 1$ und $X^2 + X - 3$ keine gemeinsame Nullstelle in $\mathbb{C}$ besitzen, ohne Nullstellen zu berechnen.

Aufgabe 29. Es sei $R := \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$.

(1) Man zeige, dass 3 und $1 \pm \sqrt{-5}$ irreduzibel in R sind und dass 3 kein Primelement in R ist.

(2) Man bestimme alle Einheiten in R.

Aufgabe 30. Sei R ein Integritätsring. Man zeige, dass die folgenden Bedingungen äquivalent sind:

(1) R ist faktoriell.

(2) Jede Nichteinheit $\neq 0$ in R wird von einem Primelement geteilt, und jede aufsteigende Kette von Hauptidealen in R wird stationär.

9 Primfaktorzerlegung in Polynomringen

9.1 Hilfssatz über Primelemente

Hilfssatz. *Sei p eine Nichteinheit $\neq 0$ in einem Integritätsring R. Dann gilt:*

$$\boxed{p \text{ Primelement in } R} \iff \boxed{p \text{ Primelement in } R[X]}$$

Beweis. "$\Rightarrow$" Da pR nach Voraussetzung Primideal ist, sind $\overline{R} := R/pR$ und dann auch $\overline{R}[X]$ Integritätsringe (vgl. 7.4 und 6.13). Da der surjektive Ringhomomorphismus

$$\boxed{\psi\colon R[X] \longrightarrow \bar{R}[X],\ \sum_{i=0}^{n} a_i X^i \longmapsto \sum_{i=0}^{n} \bar{a}_i X^i \text{ mit } \bar{a}_i \equiv a_i \bmod pR,}$$

$\operatorname{kern}(\psi) = pR[X]$ erfüllt, impliziert der Homomorphiesatz 7.7, daß auch $R[X]/pR[X]$ ein Integritätsring ist und also p Primelement in $R[X]$ ist (vgl. 7.4).

"$\Leftarrow$" Zu zeigen: $p \mid ab$ mit $a, b \in R \Longrightarrow p \mid a$ oder $p \mid b$.
Dies gilt aber nach Voraussetzung sogar für $a, b \in R[X]$.

□

9.2 Primitive Polynome

Definition. Sei R faktoriell. Ein Polynom $f = a_n X^n + \cdots + a_1 X + a_0 \in R[X] \setminus \{0\}$ heißt *primitiv*, wenn $\underbrace{\operatorname{ggT}(a_0, \ldots, a_n)}_{\text{existiert nach 8.11}} \in R^*$ ist.

Beispiele. 1. f *normiert*, d.h. $a_n = 1$, $\Longrightarrow f$ primitiv.

2. $\boxed{f \text{ irreduzibel, } \operatorname{grad}(f) > 0} \Longrightarrow \boxed{f \text{ primitiv}}$.
denn: $a \mid a_i \ \forall i \underset{6.13}{\Longrightarrow} f = ag$ mit $\operatorname{grad}(g) > 0 \underset{6.13}{\Longrightarrow} g$ Nichteinheit $\Longrightarrow a \in R^*$, da f irreduzibel.

Lemma von Gauß. *Sei R faktoriell, und seien $f, g \in R[X]$ primitiv. Dann ist auch $f \cdot g$ primitiv.*

Beweis. Wenn fg nicht primitiv ist, dann gibt es ein Primelement $p \in R$, das alle Koeffizienten von fg teilt (da R faktoriell).
$\Longrightarrow p$ Primelement in $R[X]$ nach 9.1
$\Longrightarrow p \mid f$ oder $p \mid g$
$\Longrightarrow f$ oder g nicht primitiv.

□

9.3 Übergang zum Quotientenkörper von R

Ziel zu zeigen: R faktoriell $\Longrightarrow R[X]$ faktoriell
Man geht zum Quotientenkörper K von R über und nutzt aus, daß $K[X]$ faktoriell ist. Der folgende Satz beschreibt den Weg von $K[X]$ zurück zu $R[X]$.

Satz. *Seien R faktoriell, K der Quotientenkörper von R und $f \in R[X]$ mit $f \neq 0$. Dann gelten:*

(a) *Ist $f = q_1 \cdot \ldots \cdot q_n$ mit $q_1, \ldots, q_n \in K[X]$, so gibt es $\lambda_1, \ldots, \lambda_n \in K^*$ und primitive $p_1, \ldots, p_n \in R[X]$ mit*

(1) $q_1 = \lambda_1 p_1, \ldots, q_n = \lambda_n p_n$

(2) $\lambda_1 \cdot \ldots \cdot \lambda_n =: \lambda \in R$

(b) *Ist $p \in R[X]$ und p primitiv, so gilt*

$$\boxed{p \mid f \text{ in } K[X]} \quad \Longrightarrow \quad \boxed{p \mid f \text{ in } R[X]}$$

(c) $\boxed{f \text{ nicht konstant und irreduzibel in } R[X]} \quad \Longrightarrow \quad \boxed{f \text{ irreduzibel in } K[X]}$

Beweis. (a) Sei $i \in \{1, \ldots, n\}$, und sei m_i das Produkt der Nenner der Koeffizienten von $q_i \Longrightarrow m_i q_i \in R[X]$. Klammert man $d_i :=$ ggT (Koeffizienten von $m_i q_i$) aus, folgt

$$(*) \qquad \boxed{m_i q_i = d_i p_i}$$

mit primitivem $p_i \in R[X]$. Setze $\lambda_i = \frac{d_i}{m_i} \Longrightarrow$ (1).
Ist $n = 1 \Longrightarrow q_1 = f \in R[X] \Longrightarrow m_1 = 1 \Longrightarrow \lambda_1 = d_1 \in R$.
Sei $n > 1$. Da $f = q_1 \cdots q_n \Longrightarrow m_1 \cdots m_n f = d_1 \cdots d_n p_1 \cdots p_n$ nach $(*)$.
Sei $d_f = \text{ggT}(\text{Koeffizienten von } f)$
$\Longrightarrow m_1 \cdots m_n d_f = d_1 \cdots d_n d_{p_1 \cdots p_n} \cdot \varepsilon' = d_1 \cdots d_n \cdot \varepsilon$ mit $\varepsilon, \varepsilon' \in R^*$, da $p_1 \cdots p_n$ nach 9.2 primitiv ist.
Es folgt $R \ni d_f \varepsilon^{-1} = \lambda_1 \cdots \lambda_n \Longrightarrow$ (2).

(b) Wende (a) für $n = 2$ an und setze $q_1 := p \Longrightarrow m_1 = 1$ (da $p \in R[X]$) und $\lambda_1 = d_1 \in R^*$, (da p primitiv nach Voraussetzung)
Wenn $q_1 \mid f$ in $K[X]$ gilt $\Longrightarrow f = q_1 q_2$ mit $q_2 \in K[X]$
$\underset{\text{(a)}}{\Longrightarrow} \lambda_2 = \lambda_1^{-1} \cdot \underbrace{\lambda_1 \cdot \lambda_2}_{\in R} \in R$ und $q_2 = \lambda_2 p_2 \in R[X]$.

(c) Falls f nicht irreduzibel in $K[X]$ ist $\Longrightarrow f = q_1 q_2$, wobei $q_1, q_2 \in K[X]$ nicht konstant sind (da $(K[X])^* = K^*$)
$\Longrightarrow f = \lambda p_1 p_2$ mit nicht konstanten $p_i = \frac{1}{\lambda_i} q_i \in R[X]$ und $\lambda \in R$
$\Longrightarrow f$ nicht irreduzibel in $R[X]$.

□

9.4 Satz von Gauß

Satz. *Ist R faktoriell, so ist auch $R[X]$ faktoriell.*

Beweis. Sei $f \in R[X]$ eine Nichteinheit $\neq 0$. Zu zeigen: $f = p_1 \cdots p_n$ mit Primelementen $p_1, \dots, p_n \in R[X]$.

(I) $f \in R \Longrightarrow f = p_1 \cdots p_n \in R$ mit Primelementen $p_1, \dots, p_n \in R$, da R faktoriell. Nach 9.1 sind $p_1, \dots, p_n$ Primelemente in $R[X]$.

(II) Sei $\operatorname{grad}(f) > 0$, und sei K der Quotientenkörper von R. Da $K[X]$ nach 8.10 faktoriell ist, folgt $f = q_1 \cdots q_n$ mit Primelementen $q_1, \dots, q_n \in K[X]$. Nach 9.3(1) gilt $q_1 = \lambda_1 p_1, \dots, q_n = \lambda_n p_n$ mit primitiven $p_1, \dots, p_n \in R[X]$ und $\lambda_1, \dots, \lambda_n \in K^*$.
$\underset{9.3}{\Longrightarrow} f = \lambda p_1 \cdots p_n$ mit $\lambda := \lambda_1 \cdots \lambda_n \in R$.
Zerlege λ wie unter (I) in ein Produkt von Primelementen aus $R[X]$ und zeige, daß p_i Primelement in $R[X]$ für $i = 1, \dots, n$ ist.
Es gelte $p_i \mid gh$ mit $g, h \in R[X]$.
$\Longrightarrow p_i \mid g$ oder $p_i \mid h$ in $K[X]$, da mit $q_i = \lambda_i p_i$ auch p_i Primelement in $K[X]$.
$\Longrightarrow p_i \mid g$ oder $p_i \mid h$ in $R[X]$ nach 9.3(b)
$\Longrightarrow p_i$ Primelement in $R[X]$.

□

9.5 Folgerung für Polynomringe in mehreren Unbestimmten

Korollar. *Ist R faktoriell, so ist auch der Polynomring $R[X_1, \dots, X_n]$ faktoriell.*

Beweis. Dies folgt durch Induktion aus 9.4. □

9.6 Umkehrung des Satzes von Gauß

Sei R ein Integritätsring.

Satz.

$$\boxed{R[X] \textit{ faktoriell}} \iff \boxed{R \textit{ faktoriell}}$$

Beweis. "$\Rightarrow$" Sei $a \neq 0$ eine Nichteinheit in R. Da $R[X]$ faktoriell, folgt $a = p_1 \dots p_n$ mit Primelementen $p_1, \dots, p_n \in R[X]$
$\underset{6.13}{\Longrightarrow} 0 = \operatorname{grad}(a) = \sum_{j=1}^{n} \underbrace{\operatorname{grad}(p_i)}_{\geq 0}$
$\Longrightarrow \operatorname{grad}(p_i) = 0 \quad \forall\, i \Longrightarrow p_i \in R$.
und p_i ist Primelement in R nach 9.1 $\forall\, i$.

"$\Leftarrow$" folgt aus 9.4.

□

9.7 Wann ist ein Polynomring ein Hauptidealring?

Sei R ein Integritätsring.

Bemerkung.

$$\boxed{R[X] \text{ Hauptidealring}} \iff \boxed{R \text{ Körper}}$$

Beweis. "$\Rightarrow$" Für den surjektiven Ringhomomorphismus

$$\varphi\colon R[X] \longrightarrow R, f \longmapsto f(0)$$

gilt $\operatorname{kern}(\varphi) = (X)$.
$\underset{7.7}{\Longrightarrow} R[X]/(X) \simeq R$
$\Longrightarrow R[X]/(X)$ ist Integritätsring, da R ein solcher ist
$\Longrightarrow (X)$ ist Primideal in $R[X]$ nach 7.4 und daher ein maximales Ideal in $R[X]$ (nach 8.5, da $R[X]$ Hauptidealring)
$\Longrightarrow R \simeq R[X]/(X)$ ist Körper nach 7.4.

"$\Leftarrow$" folgt aus 8.3.

□

Folgerung. Es ist $\mathbb{Z}[X]$ ein faktorieller Ring (nach 8.10 und 9.4), aber $\mathbb{Z}[X]$ ist kein Hauptidealring.

9.8 Eisensteinsches Irreduzibilitätskriterium

Satz. *Seien R ein faktorieller Ring, K sein Quotientenkörper und $f = a_nX^n + \dots + a_1X + a_o \in R[X]$ ein Polynom vom Grad $n > 0$. Es gebe ein Primelement $p \in R$ mit*

$$(*) \qquad \boxed{p \mid a_i \textit{ für } i = 0, \dots, n-1,\ p \nmid a_n \textit{ und } p^2 \nmid a_0}$$

- *Dann ist f irreduzibel in $K[X]$.*
- *Ist f primitiv, so ist f sogar irreduzibel in $R[X]$.*

Beweis. Sei $\boxed{f = gh}$ mit $g = \sum_{i=0}^{k} b_i X^i$ und $h = \sum_{i=0}^{\ell} c_i X^i$, wobei $b_k \neq 0$ und $c_\ell \neq 0$ gelte.
Nach Voraussetzung ist $f \neq 0$ und f Nichteinheit. Da $a_0 = b_0 c_0$ und $p \mid a_0 \Longrightarrow p \mid b_0$ oder $p \mid c_0$ (denn p ist Primelement).
Da $p^2 \nmid a_0$ gilt, kann p nicht beide, b_0 und c_0, teilen.
Es gelte etwa: $\boxed{p \mid b_0}$ und $\boxed{p \nmid c_0}$. Da $p \nmid a_n = b_k c_\ell \Longrightarrow p \nmid b_k$.
Sei m der kleinste Index mit $p \nmid b_m$, also mit $p \mid b_i$ für $i = 0, \dots, m-1$. Nach Definition der Multiplikation in $R[X]$ gilt

$$a_m = \underbrace{b_0 c_m + b_1 c_{m-1} + \cdots + b_{m-1} c_1}_{\text{durch } p \text{ teilbar}} + b_m c_0 \quad (\text{mit } c_i = 0 \text{ für } i > \ell)$$

Da $p \nmid b_m c_0$ und $p \mid a_i$ für $i < n \Longrightarrow m = n$. Wegen $m \leq k = \operatorname{grad}(g) \leq n \Longrightarrow \operatorname{grad}(g) = n$
$\Longrightarrow \operatorname{grad}(h) = 0$ (da $n = \operatorname{grad}(f) \underset{6.13}{=} \underbrace{\operatorname{grad}(g)}_{n} + \operatorname{grad}(h)$)
$\Longrightarrow h = c_0 \in R \setminus \{0\}$ und $h \mid d := \operatorname{ggT}(a_0, \dots, a_n)$

- Ist f primitiv $\Longrightarrow h \in R^* \Longrightarrow f$ irreduzibel in $R[X]$.
- Ist f nicht primitiv $\Longrightarrow a_i = d\tilde{a}_i$, wobei $\tilde{a}_i \in R$ für $i = 0, \dots, n$ und $\tilde{f} := \sum_{i=0}^{n} \tilde{a}_i X^i$ primitiv ist.
  Wegen $p \nmid a_n \Longrightarrow p \nmid d \Longrightarrow p \mid \tilde{a}_i$ für $i = 0, \dots, n-1$ und $p \nmid \tilde{a}_n$ und $p^2 \nmid \tilde{a}_0$ (da p Primelement).
  Wie oben gezeigt, ist $\tilde{f}$ irreduzibel in $R[X]$ und also nach 9.3(c) in $K[X]$.
  Da $d \in K^* \Longrightarrow f = d\tilde{f}$ irreduzibel in $K[X]$.

□

9.9 Beispiel für ein Eisensteinpolynom

Definition. Ein Polynom aus $R[X]$ mit den Eigenschaften $(*)$ aus Satz 9.8 heißt *Eisensteinpolynom.*

Beispiel. Sei p eine Primzahl und $n \in \mathbb{N}$. Dann ist $X^n - p$ ein Eisensteinpolynom und also irreduzibel in $\mathbb{Q}[X]$.

- Die reelle Zahl $\sqrt[n]{p}$ ist also nicht rational, falls $n > 1$.

9.10 Polynome von kleinem Grad

Bemerkung. Sei R ein faktorieller Ring. Dann ist ein Polynom $f \in R[X]$ vom Grad 2 oder 3 irreduzibel in $R[X]$, wenn f keinen Teiler vom Grad 0 oder 1 besitzt.
Hat $f \in R[X]$ den Grad 4 oder 5, so ist f irreduzibel in $R[X]$, wenn f keinen Teiler vom Grad 0, 1 oder 2 hat.

9.11 Substitutionsmethode zum Nachweis von Irreduzibilität

Ist $\varphi\colon R \longrightarrow S$ ein Homomorphismus von kommutativen Ringen, so ist

$$\varphi_s\colon R[X] \longrightarrow S, \ \sum a_i X^i \longmapsto \sum \varphi(a_i) \cdot s^i \,,$$

ein Ringhomomorphismus für $s \in S$.
Spezialfall $S = R[X]$ und $\varphi\colon R \longrightarrow R[X]$, $r \longmapsto r \cdot 1$.
Dann ist $\varphi_{X-a}\colon R[X] \longrightarrow R[X]$, $\sum a_i X^i \longmapsto \sum a_i (X-a)^i$, ein Ringhomomorphismus für jedes $a \in R$. Man schreibt $X \longmapsto X - a$. Vermöge $X \longmapsto X + a$ sieht man, daß φ_{X-a} ein Isomorphismus ist. Zum Nachweis der Irreduzibilität von $f \in R[X]$ genügt es also zu zeigen, daß $\varphi_{X-a}(f)$ irreduzibel ist für passendes $a \in R$.

9.12 Das p-te Kreisteilungspolynom

Sei p eine Primzahl. Dann heißt

$$f = X^{p-1} + X^{p-2} + \cdots + X + 1 \in \mathbb{Z}[X]$$

das *p-te Kreisteilungspolynom*. Es ist irreduzibel über $\mathbb{Q}$. In $\mathbb{Z}[X]$ gilt

$$\boxed{(X-1)f = X^p - 1}\,.$$

Sei $\Psi = \varphi_{X+1}\colon X \longmapsto X + 1$
$\Longrightarrow X\Psi(f) = (X+1)^p - 1 = \left(\sum\limits_{i=0}^{p} \binom{p}{i} X^i\right) - 1$
$= \sum\limits_{i=1}^{p} \binom{p}{i} X^i \Longrightarrow \Psi(f) = \sum\limits_{i=1}^{p} \binom{p}{i} X^{i-1}$
ist ein Eisensteinpolynom, denn $p \mid \binom{p}{i}$ für $i = 1, \ldots, p-1$, $p \nmid \binom{p}{p} = 1$, $p^2 \nmid \binom{p}{1} = p$.
$\underset{9.8,\ 9.11}{\Longrightarrow}$ $\Psi(f)$, und damit f, ist irreduzibel in $\mathbb{Q}[X]$.

9.13 Reduktionssatz

Seien R ein faktorieller Ring, K sein Quotientenkörper, $\bar{R} = R/\mathfrak{J}$ mit einem Primideal $\mathfrak{J}$ in R, und sei $R[X] \longrightarrow \bar{R}[X]$, $f \longmapsto \bar{f}$, der kanonische Homomorphismus, bei dem die Koeffizienten jeweils modulo $\mathfrak{J}$ reduziert werden, also:

$$f = \sum a_i X^i \Longrightarrow \bar{f} = \sum \bar{a}_i X^i \text{ mit } \bar{a}_i \equiv a_i \bmod \mathfrak{J}\,.$$

Satz. *Sei* $f = \sum\limits_{i=0}^{n} a_i X^i \in R[X]$ *nichtkonstant und* $a_n \notin \mathfrak{J}$. *Dann gilt*

$$\boxed{\bar{f} \textit{ irreduzibel in } \bar{R}[X]} \quad \Longrightarrow \quad \boxed{f \textit{ irreduzibel in } K[X]}$$

Beweis. Sei $d = \mathrm{ggT}(a_0, \ldots, a_n) \Longrightarrow f = df_0$ mit primitivem $f_0 \in R[X]$. Es genügt zu zeigen, daß f_0 irreduzibel in $R[X]$ ist, denn dann folgt die Behauptung aus 9.3(c). Da $a_n \notin \mathfrak{J} \Longrightarrow \mathrm{grad}(\bar{f}) = \mathrm{grad}(f) \underset{6.13}{=} \mathrm{grad}(f_0) \Longrightarrow \bar{f} = \bar{d}\bar{f}_0$ mit $\bar{d} \in \bar{R}^*$, da $\bar{f}$ irreduzibel. $\Longrightarrow \bar{f}_0$ irreduzibel und $\mathrm{grad}(\bar{f}_0) = \mathrm{grad}(f_0)$.
Angenommen, f_0 nicht irreduzibel in $R[X]$.
$\Longrightarrow f_0 = gh$ mit nichtkonstanten $g, h \in R[X]$, da f_0 primitiv.
$\Longrightarrow \bar{f}_0 = \bar{g}\bar{h}$ und $\mathrm{grad}(g) + \mathrm{grad}(h) = \mathrm{grad}(f_0) = \mathrm{grad}(\bar{f}_0) = \underbrace{\mathrm{grad}(\bar{g})}_{\leq \mathrm{grad}(g)} + \underbrace{\mathrm{grad}(\bar{h})}_{\leq \mathrm{grad}(h)}$
$\Longrightarrow \mathrm{grad}(\bar{g}) = \mathrm{grad}(g)$ und $\mathrm{grad}(\bar{h}) = \mathrm{grad}(h)$
$\Longrightarrow \bar{f}_0$ nicht irreduzibel. Widerspruch. □

9.14 Beispiel zum Reduktionssatz

Man untersuche, ob das Polynom

$$X^5 - X^2 + 10X + 1 \in \mathbb{Z}[X]$$

irreduzibel ist in $\mathbb{Q}[X]$. Sei $\mathfrak{J} = 2\mathbb{Z}$ und $\mathbb{F}_2 = \mathbb{Z}/\mathfrak{J}$.

$$\Longrightarrow \quad \boxed{\bar{f} = X^5 + X^2 + \bar{1} \in \mathbb{F}_2[X]}$$

Prüfe nun, ob $\bar{f}$ von einem Polynom vom Grad 1 oder 2 geteilt wird. Da $\bar{f}$ keine Nullstelle in $\mathbb{F}_2$ besitzt, hat $\bar{f}$ keinen Teiler von Grad 1. Die quadratischen Polynome $X^2 + X$, $X^2 + \bar{1}$, X^2 haben jeweils eine Nullstelle in $\mathbb{F}_2$ und können daher kein Teiler von $\bar{f}$ sein. Durch Division mit Rest erhält man

$$\bar{f} = (X^3 + X^2)(X^2 + X + \bar{1}) + \bar{1} \Longrightarrow (X^2 + X + \bar{1}) \nmid \bar{f}$$

$\underset{9.10}{\Longrightarrow} \bar{f}$ ist irreduzibel in $\mathbb{F}_2[X] \underset{9.13}{\Longrightarrow} f$ irreduzibel in $\mathbb{Q}[X]$.

9.15 Übungsaufgaben 31 – 33

Aufgabe 31. Der folgende Beweis, dass es unendlich viele Primzahlen gibt, stammt von Euklid: Sind $p_1, \dots, p_k$ Primzahlen, so muss jeder Primfaktor von $n = 1 + p_1 \cdot p_2 \cdot \ldots \cdot p_k$ von allen p_i verschieden sein; die Liste $p_1, \dots, p_k$ ist also nicht vollständig. Man verwende diese Beweisidee, um zu zeigen, dass der Polynomring $K[X]$ für jeden Körper K unendlich viele Primideale besitzt.

Aufgabe 32. Man zeige, dass folgende Polynome in $\mathbb{Q}[X]$ irreduzibel sind:

(a) $2X^4 + 200X^3 + 2000X^2 + 20000X + 20\,,$

(b) $X^4 + 3X^3 + X^2 - 2X + 1\,.$

Aufgabe 33. Man untersuche die folgenden Polynome in $\mathbb{Q}[X]$ auf Irreduzibilität:

(a) $X^5 + 7X^3 + 4X^2 + 6X + 1\,,$

(b) $X^4 - 4X^3 + 6X^2 - 4X - 9999\,.$

10 R-Moduln

Sei R ein Ring.

10.1 Links- und Rechtsmoduln

Definition. 1) Eine abelsche Gruppe M, versehen mit einer Skalarmultiplikation

$$R \times M \longrightarrow M, \ (r, m) \longmapsto rm\,,$$

heißt *R-Modul*, wenn für alle $r_1, r_2, r \in R$ und $m_1, m_2, m \in M$ gilt:

$$(*) \qquad \begin{aligned} r(m_1 + m_2) &= rm_1 + rm_2 \\ (r_1 + r_2)m &= r_1 m + r_2 m \\ r_1(r_2 m) &= (r_1 r_2)m \\ 1m &= m \end{aligned}$$

2) Eine abelsche Gruppe M mit einer Abbildung $M \times R \longrightarrow M, \ (m, r) \longmapsto mr\,,$ heißt *R-Rechtsmodul*, wenn die zu $(*)$ analogen Eigenschaften gelten.

Beispiel. R ist ein R-Modul (mit Multiplikation in R).

10.2 Beispiele für R-Moduln

1) R.

2) Jedes Linksideal in R.

3) Jeder K-Vektorraum, wenn $R = K$ Körper.

4) Jede abelsche Gruppe G ist ein $\mathbb{Z}$-Modul, wobei gilt:

$$nx = \underbrace{x + \cdots + x}_{n \text{ Summanden}} \in G \text{ und}$$
$$(-n)x = -(nx) \text{ für } x \in G, n \in \mathbb{N}\,.$$

10.3 R-Modulhomomorphismen

Definition. Eine Abbildung $\varphi\colon M \longrightarrow M'$ mit R-Moduln M, M' heißt *R-Modulhomomorphismus* oder *R-linear*, wenn

$$\begin{aligned} &\varphi(m + m') = \varphi(m) + \varphi(m') \\ &\text{und } \varphi(rm) = r\varphi(m) \quad \forall\, m, m' \in M, r \in R \end{aligned}$$

gilt. Es ist
$$\mathrm{End}_R\, M := \{\varphi\colon M \longrightarrow M,\ \varphi \text{ ist } R\text{-linear}\}$$
eine R-Algebra mit

$$\begin{aligned}(\varphi+\psi)(m) &:= \varphi(m)+\psi(m)\\ (\varphi\circ\psi)(m) &:= \varphi(\psi(m))\\ (r\varphi)(m) &:= r\varphi(m)\end{aligned}$$

für alle $m \in M, r \in R, \varphi, \psi \in \mathrm{End}_R\, M$ (vgl. AGLA 10.21).

10.4 Untermoduln

Definition. Eine additive Untergruppe N eines R-Moduls M heißt *Untermodul*, wenn $rn \in N\ \forall\, n \in N, r \in R$ gilt.

Satz. *Ist $\varphi\colon M \longrightarrow M'$ eine R-lineare Abbildung, so sind*

$$\begin{aligned}\mathrm{kern}(\varphi) &:= \{m \in M \mid \varphi(m) = 0\} \textit{ bzw.}\\ \mathrm{bild}(\varphi) &:= \{\varphi(m) \mid m \in M\}\end{aligned}$$

Untermoduln von M bzw. M', und φ induziert einen Isomorphismus

$$M/\,\mathrm{kern}(\varphi) \xrightarrow{\ \sim\ } \mathrm{bild}(\varphi),\ m + \mathrm{kern}(\varphi) \longmapsto \varphi(m)\,.$$

10.5 Erzeugendensysteme

Definition. Sei M ein R-Modul. Eine Familie $(m_i)_{i\in I}$ (wobei I eine Indexmenge bezeichnet) heißt *Erzeugendensystem* (bzw. *Basis*), wenn sich jedes $m \in M$ schreiben (bzw. eindeutig schreiben) läßt als $m = \sum_{i\in I} r_i m_i$, wobei $r_i \in R$, und nur endlich viele $r_i \neq 0$ sind.

Besitzt M ein endliches Erzeugendensystem, so heißt M *endlich erzeugt* über R. Besitzt M eine Basis, so heißt M ein *freier R-Modul.* Im allgemeinen sind R-Moduln nicht frei.

10.6 Beispiele für freie Moduln

1) $R^n = R \times \cdots \times R$ ist freier R-Modul (Addition und Skalarmultiplikation komponentenweise). Eine Basis ist die Standardbasis.

2) Für jede Menge $Y \neq \emptyset$ gibt es den freien $\mathbb{Z}$-Modul $\mathbb{Z}^Y$ mit Basis Y. Es ist $\mathbb{Z}^Y := \{f\colon Y \longrightarrow \mathbb{Z} \mid f(y) \neq 0 \text{ für nur endlich viele } y\}$
Addition: $(f+\tilde f)(x) := f(x) + \tilde f(x)\,,$

Skalarmultiplikation: $(nf)(x) := n \cdot f(x)\ \forall\, x \in Y, n \in \mathbb{Z}$,
Basis: $\left\{ f_y \colon Y \longrightarrow \mathbb{Z} \mid f_y = \begin{cases} 1 & \text{für } x = y \\ 0 & \text{für } x \neq y \end{cases} \right\}$
Die Abbildung $Y \longrightarrow \{f_y \mid y \in Y\}$, $y \longmapsto f_y$, ist eine Bijektion. Schreibe daher y statt f_y.

10.7 Definition des Tensorprodukts

Sei R ein Ring, M ein R-Rechtsmodul und P ein R-Linksmodul (d.h. P ein R-Modul). Sei U der Untermodul von $\mathbb{Z}^{M \times P}$, der von allen Elementen der Form

$$\begin{gathered} (m+m', p) - (m,p) - (m', p)\,, \\ (m, p+p') - (m,p) - (m,p') \text{ und} \\ (mr, p) - (m, rp) \end{gathered}$$

mit $r \in R$, $m, m' \in M$ und $p, p' \in P$ erzeugt wird.

Definition. Der $\mathbb{Z}$-Modul $\mathbb{Z}^{M \times P}/U =: M \otimes_R P$ heißt das *Tensorprodukt von M und P über R*. Für $m \in M$ und $p \in P$ bezeichnet $m \otimes p$ die Restklasse $(m,p) + U$ in $M \otimes_R P$. Nach Definition gilt dann:

(a) $(m+m') \otimes p = m \otimes p + m' \otimes p$
$m \otimes (p+p') = m \otimes p + m \otimes p'$
$mr \otimes p = m \otimes rp \quad \forall\, m, m' \in M, p, p' \in P, r \in R$

(b) Jedes $z \in M \otimes_R P$ kann geschrieben werden als

$$z = \sum_{i=1}^{n} m_i \otimes p_i \text{ mit } m_i \in M, p_i \in P \text{ und } n \in \mathbb{N}$$

Die Darstellung ist im allgemeinen *nicht* eindeutig.

(c) Ist R kommutativ, so ist $M \otimes_R P$ ein R-Modul vermöge

$$r(m \otimes p) = mr \otimes p = m \otimes rp$$

für alle $r \in R$, $m \in M$, $p \in P$.

10.8 Universelle Eigenschaft des Tensorproduktes

Satz. *Sei V ein $\mathbb{Z}$-Modul. Jede bilineare Abbildung $\gamma\colon M \times P \longrightarrow V$ mit*

$$(1) \qquad \boxed{\gamma(mr,p) = \gamma(m,rp)\ \forall\, m \in M, p \in P, r \in R}$$

induziert einen eindeutig bestimmten Homomorphismus

$$g\colon M \otimes_R P \longrightarrow V \ \text{ mit } g(m \otimes p) = \gamma(m,p)$$

Folgendes Digramm ist also kommutativ:

$$\begin{tikzcd}
M \times P \arrow[rr, "\gamma"] \arrow[dr, "kan"'] & & V \\
& M \otimes_R P \arrow[ur, "\exists!\, g"'] &
\end{tikzcd}$$

Beweis. Setze γ fort zu

$$\gamma'\colon \mathbb{Z}^{M\times P} \longrightarrow V,\ \sum_i z_i(m_i,p_i) \longmapsto \sum_i z_i\gamma(m_i,p_i)$$

mit $z_i \in \mathbb{Z}$, $m_i \in M$, $p_i \in P$
$\Longrightarrow \gamma$ ist $\mathbb{Z}$-linear, und es gilt $\gamma'(u) = 0\ \forall\, u \in U$, da γ bilinear und (1) erfüllt.
$\Longrightarrow \gamma'$ induziert $g\colon M \otimes_R P \longrightarrow V$ mit $g(m \otimes p) = \gamma(m,p)\ \forall m \in M, p \in P$, und γ ist hierdurch eindeutig bestimmt. □

10.9 Folgerungen

Mit Hilfe der universellen Eigenschaft lassen sich leicht Homomorphismen $M \otimes_R P \longrightarrow V$ konstruieren.

Satz. *Es gibt kanonische $\mathbb{Z}$-Modulisomorphismen*

$$\begin{aligned} M \otimes_R R &\longrightarrow M,\ m \otimes r \longmapsto mr \ \text{ und} \\ R \otimes_R P &\longrightarrow P,\ \ r \otimes p \longmapsto rp\,. \end{aligned}$$

Ist R kommutativ, so sind diese R-linear.

Beweis. Die bilineare Abbildung

$$\gamma\colon M \times R \longrightarrow M,\ (m,r) \longmapsto mr\,,$$

erfüllt (1). Nach 10.8 gibt es genau eine $\mathbb{Z}$-lineare Abbildung $g\colon M \otimes_R R \longrightarrow M$ mit $g(m \otimes r) = mr\ \forall\, m \in M, r \in R$. Die Abbildung ist bijektiv mit Umkehrabbildung $M \longrightarrow M \otimes_R R,\ m \longmapsto m \otimes 1$. □

10.10 Das Tensorprodukt von direkten Summen

Seien I, J Indexmengen. Die direkte Summe

$$M := \bigoplus_{i \in I} M_i \text{ von } R\text{-Rechtsmoduln}$$

besteht aus Familien (m_i), wobei $m_i \neq 0$ für nur endlich viele $i \in I$. Addition und Skalarmultiplikation wird in M komponentenweise definiert. Analog erhält man die direkte Summe $\bigoplus_{j \in J} P_j$ von R-Linksmoduln P_j.

Satz. *Es gibt einen kanonischen $\mathbb{Z}$-Modulisomorphismus*

$$\begin{aligned} \Big(\bigoplus_{i \in I} M_i\Big) \otimes_R \Big(\bigoplus_{j \in J} P_j\Big) &\longrightarrow \bigoplus_{(i,j) \in I \times J} (M_i \otimes_R P_j), \\ (m_i) \otimes (p_j) &\longmapsto (m_i \otimes p_j)\,. \end{aligned}$$

Dieser ist R-linear, falls R kommutativ ist.

Beweis. Konstruktion der Abbildung und ihrer Umkehrabbildung analog wie in 10.9. □

10.11 Tensorprodukt mit einem freien Modul

Satz. *(1) Ist M ein freier R-Rechtsmodul mit Basis $\{m_i \mid i \in I\}$, so läßt sich jedes $z \in M \otimes_R P$ schreiben als*

$$z = \sum_i m_i \otimes p_i$$

mit eindeutig bestimmten $p_i \in P$ (die fast alle 0 sind).

(2) Ist R kommutativ, und ist M ein R-Modul mit Basis $\{m_1, \ldots, m_n\}$, so ist $M \simeq R^n$, und jede Basis von M hat n Elemente (n heißt dann Rang*).*

(3) Seien V, W zwei K-Vektorräume, $\{v_1, \ldots, v_n\}$ eine Basis von V und $\{w_1, \ldots, w_m\}$ eine Basis von W.
Dann ist $\{v_i \otimes w_j \mid i = 1, \ldots, n,\ j = 1, \ldots, m\}$ eine Basis von $V \otimes_K W$.
Insbesondere gilt

$$\dim_K(V \otimes_K W) = (\dim_K V) \cdot (\dim_K W)\,.$$

Beweis. (1) Es ist $M \otimes_R P \simeq \Big(\bigoplus_i m_i R\Big) \otimes_R P \underset{10.10}{\simeq} \bigoplus_i (m_i R) \otimes_R P \underset{10.9}{\simeq} \bigoplus_i P$, da $m_i R \simeq R$.

(2) Nach 7.7 gibt es ein maximales Ideal $\mathfrak{m}$ in R. Mit $P = R/\mathfrak{m}$ folgt wie in (1), daß $M \otimes_R (R/\mathfrak{m})^n$ ist. Da $R/\mathfrak{m}$ ein Körper ist (vgl. 7.4), folgt aus dem entsprechenden Satz für Vektorräume die Behauptung (vgl. AGLA 3.8).

(3) folgt mit Hilfe von (1).

□

10.12 Der Hauptsatz über endlich erzeugte abelsche Gruppen (Eine Ergänzung von Michael Adam)

Die Vorlesungszeit war zu knapp, um den folgenden grundlegenden Satz zu beweisen:

Hauptsatz über endlich erzeugte abelsche Gruppen. *Jede endlich erzeugte abelsche Gruppe ist zu einer Gruppe der Form*

$$\mathbb{Z}^r \oplus (\mathbb{Z}/p_1^{e_1}\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/p_n^{e_n}\mathbb{Z})$$

isomorph, wobei $r \in \mathbb{Z}_{\geq 0}$ ist, die p_i Primzahlen sind (nicht notwendigerweise verschieden) und $e_i \in \mathbb{N}$.

Dieser Satz ist der Spezialfall für den Ring $\mathbb{Z}$ des allgemeineren Hauptsatzes für endlich erzeugte Moduln über Hauptidealringen. (Erinnerung: Abelsche Gruppen sind „das gleiche“ wie $\mathbb{Z}$-Moduln.) Weil sich die Gestalt des endlichen Teils in diesem Fall als relativ leichte Folgerung aus den Sylowsätzen ergibt, möchte ich hier als Ergänzung zur Vorlesung einen Beweis vorführen. Er gliedert sich in zwei größere Schritte:

1. Zerlegung in freien und endlichen Anteil: $A \cong \mathbb{Z}^r \oplus A_{\text{tors}}$. Dabei ist A_{tors} die Untergruppe von A der Elemente endlicher Ordnung.

2. Die Strukturaussage für den endlichen Anteil A_{tors}. Dies könnte auch „Hauptsatz über endliche abelsche Gruppen“ genannt werden.

Die beiden Teile des Beweises sind unabhängig voneinander. **Wer also nur an endlichen abelschen Gruppen interessiert ist, kann auch direkt Abschnitt 10.12.2 lesen.**
Der Isomorphismus aus dem Hauptsatz ist nicht eindeutig. Aussagen über die Eindeutigkeit der Darstellung werden in Abschnitt 10.12.3 gemacht.

10.12.1 Die Zerlegung in endlichen und freien Anteil

Dieser Schritt geht ganz genauso für Moduln über beliebigen Hauptidealringen. Ich schreibe auch meist „$\mathbb{Z}$-Modul“ statt „abelsche Gruppe“. Weil ich noch einige generelle Aussagen über freie Moduln bringen muss, ist dieser Abschnitt etwas länglich (aber nicht schwierig – der endliche Anteil ist zumindest ohne die Sylow-Sätze deutlich schwieriger).
Sei A eine endlich erzeugte abelsche Gruppe. Es bezeichne A_{tors} die Teilmenge von A der Elemente endlicher Ordnung (*Torsionselemente*[1]); dies ist eine Untergruppe, die *Torsionsuntergruppe* von A. Jetzt soll gezeigt werden, dass A/A_{tors} ein freier $\mathbb{Z}$-Modul ist und $A \cong A_{\text{tors}} \oplus (A/A_{\text{tors}})$. Der Beweis wird in mehrere separate Behauptungen unterteilt.

Behauptung 3. *Sei A ein endlich erzeugter $\mathbb{Z}$-Modul. Dann ist A/A_{tors} torsionsfrei, besitzt also keine Elemente endlicher Ordnung ausser* 0.

Beweis. Das ist „philosophisch“ klar, weil man ja die Torsion aus A herausgeteilt hat. Der richtige Beweis ist auch nicht schwer:
Sei $a \in A$ derart, dass $n \cdot \bar{a} = 0$ in A/A_{tors} für ein $n \in \mathbb{N}$. Das heißt $n \cdot a \in A_{\text{tors}}$. Aber wenn $n \cdot a$ von endlicher Ordnung ist, dann auch a. Folglich ist $a \in A_{\text{tors}}$ und somit $\bar{a} = 0$ in A/A_{tors}. □

Behauptung 4. *Endlich erzeugte torsionsfreie $\mathbb{Z}$-Moduln sind frei.*

Zum Beweis benötige ich zwei Tatsachen über freie Moduln: Erstens wurde schon bewiesen, dass alle Basen eines endlich erzeugten freien $\mathbb{Z}$-Moduls die gleiche Mächtigkeit[2] haben. (Sie wird *Rang* von A genannt.) Die zweite Aussage beschäftigt sich mit Untermoduln von freien Moduln:

Behauptung 5. *Jeder Untermodul B eines endlich erzeugten freien $\mathbb{Z}$-Moduls A ist wieder frei, und* $\operatorname{rang}(B) \leq \operatorname{rang}(A)$.

Beweis. Sei A ein endlich erzeugter freier $\mathbb{Z}$-Modul und $B \subset A$ ein Untermodul. Sei $x_1, \ldots, x_n$ eine Basis von A. Der Beweis wird per Induktion über den Rang n von A geführt.

1. Sei $n = 1$. Dann ist also $B \subset \mathbb{Z}x_1$. Die Menge I der $n \in \mathbb{Z}$ mit $n \cdot x_1 \in B$ bildet ein Ideal in $\mathbb{Z}$, also gibt es ein $a \in \mathbb{Z}$ mit $I = \mathbb{Z} \cdot a$. Damit ist $B = \mathbb{Z}ax_1$ frei vom Rang 0 oder 1, je nachdem, ob $a = 0$ oder $a \neq 0$.

[1] Allgemein heißt ein Element m eines R-Moduls M *Torsionselement*, wenn es ein $r \in R \setminus \{0\}$ gibt mit $r \cdot m = 0$.

[2] Die *Mächtigkeit* oder *Kardinalität* einer Menge ist die Anzahl ihrer Elemente. Dies aber nicht nur für endliche Mengen - die Mächtigkeit der natürlichen Zahlen (abzählbar) zum Beispiel heißt $\aleph_0$ (Aleph null).

2. Für den Induktionsschritt sei $n \geq 1$. Setze $A_1 := \mathbb{Z}x_2 \oplus \cdots \oplus \mathbb{Z}x_n \subset A$. Dann ist A_1 frei vom Rang $n-1$, und nach Induktion ist $B_1 = B \cap A_1$ frei vom Rang $\leq n-1$. Nun betrachte die Projektion $p_1 : A \to \mathbb{Z}x_1$ mit Kern A_1. Ist $p_1(B) = \{0\}$, so ist $B = B_1$ frei vom Rang $\leq n-1$, und wir sind fertig. Anderenfalls ist $p_1(B) = \mathbb{Z}ax_1$ mit einem $a \in \mathbb{Z} \setminus \{0\}$. Wähle ein $y_1 \in B$ mit $p_1(y_1) = ax_1$. Dann gilt $B = \mathbb{Z}y_1 \oplus B_1$:
   (a) Es ist $B_1 \cap \mathbb{Z}y_1 = \{0\}$, denn $ny_1 \in B_1$ bedeutet $0 = p_1(ny_1) = nax_1$, also $n = 0$.
   (b) Es ist $B = \mathbb{Z}y_1 \oplus B_1$: Sei $b \in B$. Sei $p_1(b) = nax_1$. Dann ist $b = ny_1 + (b - ny_1)$ mit $b - ny_1 \in \mathrm{kern}(p_1) = B_1$.

   Damit ist B frei vom Rang $= 1 + \mathrm{rang}(B_1) \leq n$.

$\square$

Beweis von Behauptung 4. Sei also A ein endlich erzeugter, torsionsfreier $\mathbb{Z}$-Modul. Sei $\{a_1, \ldots, a_n\}$ ein Erzeugendensystem für A, und sei $\{b_1, \ldots, b_m\} \subset \{a_1, \ldots, a_n\}$ maximal linear unabhängig. Dann ist

$$B = \langle b_1, \ldots, b_m \rangle = \mathbb{Z}b_1 \oplus \cdots \oplus \mathbb{Z}b_m \subset A$$

ein freier Untermodul. Wir wollen zeigen, dass es ein $r \in \mathbb{Z} \setminus \{0\}$ gibt, so dass $r \cdot A \subset B$. Dann sind wir fertig, denn weil A torsionsfrei ist, ist die Abbildung $A \to A, a \mapsto r \cdot a$ injektiv, d. h. A ist als $\mathbb{Z}$-Modul isomorph zu rA, und dieser ist als Untermodul des freien Moduls B nach Behauptung 5 ein freier Modul.
Weil $\{b_1, \ldots, b_m\} \subset \{a_1, \ldots, a_n\}$ maximal linear unabhängig gewählt war, gibt es für jedes $i \in \{1, \ldots, n\}$ ein $r_i \in \mathbb{Z} \setminus \{0\}$, so dass $r_i \cdot a_i \in B$. (Ist $a_i = b_j$ für ein j, so setze $r_i = 1$, sonst benutze die lineare Abhängigkeit von $\{a_i, b_1, \ldots, b_m\}$.) Damit ist $r_1 \cdot r_2 \cdot \ldots \cdot r_n \cdot a_i \in B$ für jedes i. Mit $r := r_1 \cdot r_2 \cdot \ldots \cdot r_n$ gilt also $r \cdot A \subset B$. $\square$

Nun wissen wir also, dass für eine endlich erzeugte abelsche Gruppe A der Modul A/A_{tors} frei ist. Wir müssen noch zeigen, dass $A \cong (A/A_{\mathrm{tors}}) \oplus A_{\mathrm{tors}}$ gilt.

Behauptung 6. *Sei A ein endlich erzeugter $\mathbb{Z}$-Modul. Sei $\{x_1, \ldots, x_n\}$ eine Basis von A/A_{tors}, und seien $a_i \in A$ derart, dass $\pi(a_i) = x_i$ unter der kanonischen Abbildung $\pi : A \to A/A_{\mathrm{tors}}$. Dann ist $\{a_1, \ldots, a_n\}$ linear unabhängig, die Einschränkung von π auf $\mathbb{Z}a_1 \oplus \cdots \oplus \mathbb{Z}a_n$ ist ein Isomorphismus $\mathbb{Z}a_1 \oplus \cdots \oplus \mathbb{Z}a_n \xrightarrow{\sim} A/A_{\mathrm{tors}}$, und es gilt*

$$A = A_{\mathrm{tors}} \oplus (\mathbb{Z}a_1 \oplus \cdots \oplus \mathbb{Z}a_n) \cong A_{\mathrm{tors}} \oplus (A/A_{\mathrm{tors}}).$$

Beweis. Sei $r_1a_1 + \dots r_na_n = 0$. Dann ist

$$0 = \pi(r_1a_1 + \cdots + r_na_n) = r_1x_1 + \cdots + r_nx_n.$$

Folglich sind alle $r_i = 0$, weil die x_i linear unabhängig sind. Also ist $\{a_1, \dots, a_n\}$ linear unabhängig. Dass die π durch Einschränkung einen Isomorphismus von $A' = \mathbb{Z}a_1 \oplus \cdots \oplus \mathbb{Z}a_n$ nach A/A_{tors} induziert, ist damit klar. Es ist noch zu zeigen, dass $A = A_{\text{tors}} \oplus A'$ ist.

1. Es ist $A_{\text{tors}} \cap A' = \{0\}$, weil A' frei ist und A_{tors} nur aus Torsionselementen besteht.

2. Sei $a \in A$. Sei $\pi(a) = r_1x_1 + \cdots + r_nx_n$. Dann ist $a' = r_1a_1 + \cdots + r_na_n \in A'$ und $a - a' \in \text{kern}(\pi) = A_{\text{tors}}$. Somit ist $A = A_{\text{tors}} + A'$.

□

10.12.2 Die Struktur des endlichen Anteils

In Abschnitt 3.8 ist bereits gezeigt worden, dass jede endliche abelsche Gruppe Produkt ihrer Sylowgruppen ist. Um den Hauptsatz zu beweisen, müssen nun nur noch die einzelnen Sylowgruppen untersucht werden.

Behauptung 7. *Sei p eine Primzahl und A eine abelsche p-Gruppe. Dann gibt es natürliche Zahlen $e_1, \dots, e_n$, so dass*

$$A \cong \mathbb{Z}/p^{e_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{e_n}\mathbb{Z}.$$

Beweis. Wir beweisen die Behauptung durch Induktion über die Gruppenordnung. Ist $\#(A) = p$ (oder 0), so ist die Behauptung wahr. Für den Induktionsschritt sei $a_1 \in A$ ein Element maximaler Ordnung p^{e_1}. Ist $A = \langle a_1 \rangle$, so sind wir fertig; ansonsten ist nach Induktionsvoraussetzung $A/\langle a_1 \rangle \cong \langle \bar{a}_2 \rangle \oplus \cdots \oplus \langle \bar{a}_n \rangle$ mit Elementen $\bar{a}_i$ der Ordnung p^{e_i}.
Behauptung: Es gibt Vertreter a_i von $\bar{a}_i$ mit $\text{ord}(a_i) = \text{ord}(\bar{a}_i) = p^{e_i}$.
Um das zu beweisen, sei allgemein $\bar{a} \in A/\langle a_1 \rangle$ ein Element von Ordnung p^r und $a \in A$ irgendein Vertreter. Dann ist $p^r a \in \langle a_1 \rangle$, etwa $p^r a = p^s \cdot m \cdot a_1$ mit $p \nmid m$. Dann ist $\text{ord}(a) = p^{r+(r_1-s)}$. Auf Grund der Maximalität der Ordnung von a_1 folgt $r + r_1 - s \leq r_1$ also $r \leq s$. Daher ist $p^r(a - p^{s-r} \cdot m \cdot a_1) = 0$, und folglich ist $a - p^{s-r} \cdot m \cdot a_1$ ein Vertreter von $\bar{a}$ der Ordnung p^r.
Seien nun also a_i Vertreter von $\bar{a}_i$ mit $\text{ord}(a_i) = \text{ord}(\bar{a}_i)$. Dann gilt

$$A = \langle a_1 \rangle \oplus \cdots \oplus \langle a_n \rangle,$$

denn:

1. Es ist $\langle a_1\rangle \cap \langle a_2,\ldots,a_n\rangle = \{0\}$: Sei $a = m_2a_2 + \cdots + m_na_n \in \langle a_1\rangle$. Dann ist $a \bmod \langle a_1\rangle = m_2\bar{a}_2 + \cdots + m_n\bar{a}_n = 0$, und das bedeutet $m_2 = \cdots = m_n = 0$, weil ja $A/\langle a_1\rangle = \langle\bar{a}_2\rangle \oplus \cdots \oplus \langle\bar{a}_n\rangle$. Also ist $a = 0$.

2. Es ist $A = \langle a_1\rangle + \cdots + \langle a_n\rangle$: Sei $a \in A$. Sei $a \bmod \langle a_1\rangle = m_2\bar{a}_2 + \cdots + m_n\bar{a}_n$. Dann ist $a - (m_2a_2 + \cdots + m_na_n) \in \langle a_1\rangle$, etwa $= m_1a_1$, und damit ist $a = m_1a_1 + m_2a_2 + \cdots + m_na_n \in \langle a_1\rangle + \cdots + \langle a_n\rangle$.

Da $\langle a_i\rangle \cong \mathbb{Z}/p^{e_i}\mathbb{Z}$, ist damit alles gezeigt. □

Bemerkung. Man kann den Beweis wie folgt auch mit einer etwas anderen Induktion führen, die etwas konstruktiver ist. Dazu wählt man zunächst wieder $a_1 \in A$ von maximaler Ordnung p^{e_1}; dann wählt man $\bar{a}_2 \in A/\langle a_1\rangle$ von maximaler Ordnung p^{e_2} und wählt wie oben einen Vertreter a_2 der gleichen Ordnung. Dann gilt $\langle a_1\rangle \cap \langle a_2\rangle = \{0\}$, und somit $\langle a_1, a_2\rangle \cong \langle a_1\rangle \oplus \langle a_2\rangle$. Man wählt dann weiter $\bar{a}_3 \in A/\langle a_1, a_2\rangle$ von maximaler Ordnung p^{e_3}, eine Vertreter a_3 von gleicher Ordnung, und induktiv $\bar{a}_i \in A/\langle a_1,\ldots,a_{i-1}\rangle$ von maximaler Ordnung p^{e_i} sowie einen Vertreter a_i der gleichen Ordnung. Dabei geht das Finden des Vertreters im Prinzip genauso wie oben, nur werden die Notationen (und auch die Argumente) aufwendiger. Dann gilt jeweils $\langle a_1,\ldots,a_{i-1}\rangle \cong \langle a_1\rangle \oplus \cdots \oplus \langle a_{i-1}\rangle$ und $\langle a_1,\ldots,a_{i-1}\rangle \cap \langle a_i\rangle = \{0\}$, und man folgert $\langle a_1,\ldots,a_i\rangle \cong \langle a_1\rangle \oplus \cdots \oplus \langle a_i\rangle$. Weil A endlich ist, muss dieser Prozess abbrechen, d. h. irgendwann gilt $A = \langle a_1,\ldots,a_n\rangle$, und man ist fertig. ◊

10.12.3 Über die Eindeutigkeit der Darstellung

Schließlich soll noch die Eindeutigkeit der Summenzerlegung

$$A \cong \mathbb{Z}^r \oplus (\mathbb{Z}/p_1^{e_1}\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/p_n^{e_n}\mathbb{Z})$$

aus dem Hauptsatz diskutiert werden.

- Der freie Summand $\mathbb{Z}^r$ ist nicht eindeutig bestimmt, wohl aber die Zahl r, der *Rang* von A: Es ist der Rang des freien Moduls A/A_{tors}.

- Die einzelnen endlichen Summanden sind nicht eindeutig bestimmt, wohl aber die Summe aller endlichen Summanden: Dies ist die Untergruppe A_{tors} der Elemente endlicher Ordnung von A.

- In A_{tors} ist die Summe A_p aller Summanden, deren Ordnung Potenz einer festen Primzahl p ist, eindeutig bestimmt: Dies ist die p-Sylowgruppe von A_{tors}.

- Ist $A_p = \mathbb{Z}/p^{e_{p,1}}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{e_{p,n_p}}\mathbb{Z}$ mit $e_{p,1} \geq e_{p,2} \geq \cdots \geq e_{p,n_p}$, so ist die Untergruppe $\mathbb{Z}/p^{e_{p,1}} \oplus \cdots \oplus \mathbb{Z}/p^{e_{p,i}}$ eindentig bestimmt: Dies ist die von den Elementen von Ordnung mindestens p^{e_i} erzeugte Untergruppe. Daraus ergibt sich, dass die Folge $e_{p,1}, \ldots, e_{p,n_p}$ eindeutig bestimmt ist. A_p ist durch die Folge $e_{p,1}, \ldots, e_{p,n_p}$ bis auf Isomorphie festgelegt.

Schreibt man genauer als oben

$$\begin{aligned}(1)\quad A \cong \mathbb{Z}^r \oplus (\mathbb{Z}/p_1^{e_{p_1,1}}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_1^{e_{p_1,n_{p_1}}}\mathbb{Z}) \oplus \cdots \\ \cdots \oplus (\mathbb{Z}/p_m^{e_{p_m,1}}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_m^{e_{p_m,n_{p_m}}}\mathbb{Z})\end{aligned}$$

mit $e_{p_i,1} \geq e_{p_i,2} \geq \cdots \geq e_{p_i,n_{p_i}}$, so ist also die Folge

$$r, (e_{p_1,1}, \ldots, e_{p_1,n_{p_1}}), \ldots, (e_{p_m,1}, \ldots, e_{p_m,n_{p_m}})$$

eindeutig bestimmt, und diese legt andersherum A bis auf Isomorphie fest.

10.13 Übungsaufgabe 34

Seien R ein kommutativer Ring und M ein R-Modul. Man nennt n Elemente $m_1, \ldots, m_n \in M$ *linear abhängig*, wenn es in M eine Linearkombination $r_1m_1 + \cdots + r_nm_n = 0$ gibt, bei der mindestens einer der Koeffizienten $r_1, \cdots r_n \in R$ ungleich 0 ist.
Eine Teilmenge $S \subset M$ mit n Elementen heißt *Erzeugendensystem von M der Länge n*, wenn sich jedes Element aus M als Linearkombination der Elemente aus S darstellen läßt. Ein Erzeugendensystem S von M heißt *minimal*, wenn jede echte Teilmenge von S kein Erzeugendensystem von M ist.

Aufgabe 34. (a) Sei K ein Körper und V ein K-Vektorraum. Dann gilt nach AGLA 3.2:
Je n Vektoren $v_1, \ldots, v_n \in V$ sind genau dann linear abhängig, wenn einer der Vektoren $v_1, \ldots, v_n$ eine Linearkombination der übrigen ist.
Man entscheide, wie weit dieser Satz richtig bleibt, wenn die Vektoren $v_1, \ldots, v_n \in V$ durch Elemente $m_1, \ldots, m_n \in M$ mit einem R-Modul M ersetzt werden.

(b) Man zeige, dass $\mathbb{Z} = \mathbb{Z}2 + \mathbb{Z}3$ gilt, und folgere daraus, dass $\mathbb{Z}$ als $\mathbb{Z}$-Modul minimale Erzeugendensysteme verschiedener Länge besitzt.

Teil III
Körper

11 Grundbegriffe der Körpertheorie

11.1 Wiederholung der Definition eines Körpers

Definition. Ein *Körper* K ist eine Menge, die mit zwei Verknüpfungen (genannt Addition und Multiplikation),

$$K \times K \longrightarrow K, \; (a,b) \longmapsto a+b,$$
$$K \times K \longrightarrow K, \; (a,b) \longmapsto a \cdot b,$$

versehen ist so, dass K bezüglich Addition und $K^* := K \setminus \{0\}$ bezüglich Multiplikation abelsche Gruppen sind und das Distributivgesetz

$$(a+b)c = ac + bc \quad \forall\, a,b,c \in K$$

gilt.

- Insbesondere ist ein jeder Körper ein kommutativer Ring (vgl. 6.1).

11.2 Teilkörper und Körpererweiterungen

Definition. Ein *Teilkörper* eines Körpers K ist ein Unterring von K, der ein Körper ist (vgl. 6.4 für die Definition eines Unterrings). Eine *Körpererweiterung L von K* ist ein Körper L, der K als Teilkörper enthält.

Beispiele.
- $\mathbb{Q}$ ist ein Teilkörper von $\mathbb{R}$ und von $\mathbb{C}$, und $\mathbb{C}$ ist eine Körpererweiterung sowohl von $\mathbb{Q}$ als auch von $\mathbb{R}$.
- Der Durchschnitt von Teilkörpern von K ist ein Teilkörper von K.

11.3 Erzeugung und Adjunktion

Sei M eine Teilmenge eines Körpers L.

Definition. (1) Der von M erzeugte Teilkörper von L ist der Durchschnitt aller Teilkörper von L, die M enthalten.

(2) Ist K ein Teilkörper von L, so bezeichnet $K(M)$ den von $K \cup M$ erzeugten Teilkörper. Wir sagen, daß $K(M)$ aus K *durch Adjunktion von M* entstehe.

(3) Ist $M = \{x_1, \dots, x_n\}$ eine endliche Menge, so heißt $K(M) =: K(x_1, \dots, x_n)$ *endlich erzeugt über* K.

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

11.4 Isomorphismen und K-Isomorphismen

Definition.

- Seien L, L' zwei Körper. Eine bijektive Abbildung $\varphi\colon L \longrightarrow L'$ heißt *Isomorphismus*, falls

$$\varphi(a+b) = \varphi(a) + \varphi(b) \text{ und } \varphi(ab) = \varphi(a)\varphi(b) \quad \forall\, a, b \in L$$

  gilt. Es ist dann $\varphi(0) = 0$ und $\varphi(1) = 1$.

- Seien L und L' Körpererweiterungen eines Körpers K. Dann heißt ein Isomorphismus $\varphi\colon L \longrightarrow L'$ ein *K-Isomorphismus*, falls $\varphi(a) = a\ \forall\, a \in K$ gilt.

- L und L' heißen *isomorph* (bzw. *K-isomorph*), wenn es einen Isomorphismus (bzw. K-Isomorphismus) $L \longrightarrow L'$ gibt. Schreibweise: $L \simeq L'$ bzw. $L \underset{K}{\simeq} L'$.

Satz. *Sei $\varphi\colon L \longrightarrow L'$ ein K-Isomorphismus, und sei $f \in K[X]$. Ist $x \in L$ eine Nullstelle von f, so ist $y = \varphi(x)$ ebenfalls eine Nullstelle von f.*

Beweis. Es ist $f = a_nX^n + \dots + a_1X + a_0$ mit $a_0, \dots, a_n \in K$. Da x Nullstelle von f ist, folgt

$$0 = \varphi(0) = \varphi(a_nx^n + \dots + a_1x + a_0) = a_ny^n + \dots + a_1y + a_0\,,$$

da φ ein K-Isomorphismus ist.
$\Longrightarrow$ y ist Nullstelle von f. □

11.5 Die Charakteristik eines Integritätsrings

Sei K ein Integritätsring. Dann induziert der Ringhomomorphismus

$$\varphi\colon \mathbb{Z} \longrightarrow K,\ n \longmapsto n \cdot 1\,,$$

einen Ringisomorphismus

$$\mathbb{Z}/\operatorname{kern}(\varphi) \xrightarrow{\sim} \operatorname{bild}(\varphi)$$

nach Homomorphiesatz 7.7. Da K Integritätsring
$\Longrightarrow$ $\mathbb{Z}/\operatorname{kern}(\varphi)$ Integritätsring

$\underset{7.4}{\Longrightarrow}$ kern(φ) ist Primideal in $\mathbb{Z}$.
$\underset{8.5}{\Longrightarrow}$ kern$(\varphi) = (0)$ oder (p) mit einer Primzahl p (denn $\mathbb{Z}$ ist Hauptidealring nach 6.8).
Die *Charakteristik von K* ist definiert als

$$(2) \qquad \operatorname{char}(K) = \begin{cases} 0 & \text{falls } \operatorname{kern}(\varphi) = (0), \\ p > 0 & \text{falls } \operatorname{kern}(\varphi) = (p) \text{ mit einer Primzahl } p. \end{cases}$$

Beispiele. 1. Sei $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \Longrightarrow \operatorname{char}(\mathbb{F}_p) = p$

2. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ haben die Charakteristik 0.

11.6 Primkörper

Definition. Der *Primkörper eines Körpers K* ist definiert als Durchschnitt aller Teilkörper von K.

Satz. *Sei P der Primkörper eines Körpers K. Dann gelten:*

(i) $\operatorname{char}(K) = p > 0 \Longleftrightarrow P \simeq \mathbb{F}_p$ *mit einer Primzahl* p.

(ii) $\operatorname{char}(K) = 0 \Longleftrightarrow P \simeq \mathbb{Q}$.

Bis auf Isomorphie gibt es also nur die Primkörper $\mathbb{F}_p$ mit einer Primzahl p und $\mathbb{Q}$.

Beweis. Sei $\varphi\colon \mathbb{Z} \longrightarrow K$, $n \longmapsto n \cdot 1$
$\Longrightarrow \varphi(n) = \underbrace{1 + \cdots + 1}_{n \text{ Summanden}} \in P \; \forall n \in \mathbb{N}$
$\Longrightarrow \quad \boxed{\operatorname{bild}(\varphi) \subset P}$

"$\Rightarrow$" (i) $\operatorname{char}(K) = p > 0 \Longrightarrow \operatorname{kern}(\varphi) = p\mathbb{Z}$ mit einer Primzahl p.
$\Longrightarrow \mathbb{Z}/p\mathbb{Z} \underset{7.7}{\simeq} \operatorname{bild}(\varphi)$ ist ein Körper nach 8.13.
Also folgt $\operatorname{bild}(\varphi) = P$, da P als Primkörper in jedem Teilkörper von K enthalten ist.

(ii) $\operatorname{char}(K) = 0 \Longrightarrow \operatorname{kern}(\varphi) = 0 \Longrightarrow \operatorname{bild}(\varphi) \simeq \mathbb{Z}$
Sei Q der Quotientenkörper von $\operatorname{bild}(\varphi)$, wie in 6.10, 6.11 konstruiert. $\Longrightarrow Q \simeq \mathbb{Q}$
Man prüft leicht nach, daß $\varphi_0\colon Q \longrightarrow P$, $\frac{n}{m} \longmapsto \varphi(n)\varphi(m)^{-1}$, ein wohldefinierter Ringhomomorphismus, und also nach Folgerung 6.9 injektiv ist.
$\Longrightarrow Q \simeq \underbrace{\operatorname{bild}(\varphi_0)}_{\text{Körper}} \subset P$
$\Longrightarrow Q \simeq P$ nach Definition von P.

"$\Leftarrow$" Es ist $\mathrm{char}(P) = \mathrm{char}(K)$.
$\Longrightarrow$ Behauptung, da $\mathrm{char}(\mathbb{F}_p) = p$ und $\mathrm{char}(\mathbb{Q}) = 0$.

□

11.7 Der Grad einer Körpererweiterung

Sei K ein Körper und L eine Körpererweiterung von K. Dann ist L insbesondere ein K-Vektorraum. Als Addition nimmt man die Addition in L und als Skalarmultiplikation λx mit $\lambda \in K$, $x \in L$ die Multiplikation in L.

Definition. Der *Grad von L über K* ist definiert als die Dimension von L als K-Vektorraum. Man schreibt: $\dim_K L = [L : K]$.

Beispiel. $[\mathbb{C} : \mathbb{R}] = 2$

Gradsatz. *Sind $K \subset L \subset M$ Körpererweiterungen, so gilt $[M : K] = [M : L] \cdot [L : K]$.*

Beweis. Zu zeigen: $\dim_K M = (\dim_L M) \cdot (\dim_K L)$.
Sei $\{v_1, \ldots, v_n\}$ eine Basis von L über K, und $\{w_1, \ldots, w_m\}$ eine Basis von M über L. Zeige, daß die $m \cdot n$ Produkte $v_j \cdot w_i$ für $i = 1, \ldots, n$, $j = 1, \ldots, m$ eine Basis von M über K bilden.
Jedes $w \in M$ ist darstellbar als $w = \lambda_1 w_1 + \cdots + \lambda_m w_m$ mit $\lambda_1, \ldots, \lambda_m \in L$, und es ist $\lambda_i = \mu_{i1} v_1 + \cdots + \mu_{in} v_n$ mit $\mu_{i1}, \ldots, \mu_{in} \in K$ für $i = 1, \ldots, m$.
Es folgt $w = \sum\limits_{i=1}^{m} \sum\limits_{j=1}^{n} \mu_{ij} v_j w_i$, also bilden die $v_j w_i$ ein Erzeugendensystem von M über K.
Ist $w = 0$, folgt $\sum\limits_{j=1}^{n} \mu_{ij} v_j = 0 \; \forall\, i$, da $w_1, \ldots, w_m$ linear unabhängig über L sind.
$\Longrightarrow \mu_{ij} = 0 \; \forall\, i, j$, da $v_1, \ldots, v_n$ linear unabhängig über K sind.
Die gleiche Argumentation geht durch, wenn M oder L oder beide unendlichdimensional sind. □

11.8 Algebraische und transzendente Elemente über *K*

Definition. Sei L eine Körpererweiterung eines Körpers K. Ein Element $x \in L$ heißt *algebraisch über K*, falls x Nullstelle eines Polynoms $f \in K[X] \setminus \{0\}$ ist und anderenfalls *transzendent über K*. Mit Hilfe des *Einsetzungshomomorphismus*

$$\varphi_x \colon K[X] \longrightarrow L, \; f = \sum a_i X^i \longmapsto \sum a_i x^i =: f(x)$$

für $x \in L$ kann man die Definition auch so formulieren:
Es ist $x \in L$ *algebraisch über* K, wenn $\operatorname{kern}(\varphi_x) \neq (0)$ und *transzendent über* K, wenn $\operatorname{kern}(\varphi_x) = (0)$.

11.9 Das Minimalpolynom

Sei L eine Körpererweiterung eines Körpers K, und sei $x \in L$ algebraisch über K, also $(0) \neq \operatorname{kern}(\varphi_x) \underset{9.7}{=} (f)$ mit

$$f = a_n X^n + \cdots + a_1 X + a_0 \text{ und } a_n \neq 0\,.$$

Nach 8.7 ist f bis auf einen Faktor aus $(K[X])^* \underset{6.13}{=} K^*$ eindeutig bestimmt.
Normiere f, d.h. setze $\boxed{m_x := a_n^{-1} f}$.
Dann ist m_x das eindeutig bestimmte, normierte Polynom aus $K[X] \setminus \{0\}$ kleinsten Grades, das x als Nullstelle hat. m_x heißt *Minimalpolynom von x über K*.
Es gelten:

(1) $\operatorname{kern}(\varphi_x) = (m_x)$

(2) m_x ist irreduzibel in $K[X]$ (denn $K[X]/(m_x) \underset{7.7}{\simeq} \operatorname{bild}(\varphi_x) \subset L \Longrightarrow m_x$ ist irreduzibel nach 7.4, 8.5)

(3) Ist $f \in K[X]$ normiert, irreduzibel mit $f(x) = 0 \Longrightarrow f = m_x$.

11.10 Satz über den Grad des Minimalpolynoms

Sei L eine Körpererweiterung von K.

Satz. *Sei $x \in L$ algebraisch über K. Sei $n = \operatorname{grad}(m_x)$ der Grad des Minimalpolynoms m_x von x. Dann induziert der Einsetzungshomomorphismus*

$$\varphi_x\colon K[X] \longrightarrow L,\ f \longmapsto f(x)\,,$$

einen Isomorphismus

$$K[X]/(m_x) \xrightarrow{\sim} K(x)$$

und $\{1, x, \ldots, x^{n-1}\}$ ist eine Basis von $K(x)$ als K-Vektorraum. Insbesondere gilt:

$$\boxed{[K(x) : K] = \operatorname{grad}(m_x)}$$

Beweis. Nach 11.9 ist $(m_x) = \mathrm{kern}(\varphi_x)$, und m_x ist irreduzibel.
$\underset{8.13}{\Longrightarrow}$ $K[X]/(m_x) \underset{7.7}{\simeq} \mathrm{bild}(\varphi_x)$ ist ein Körper. Da $x \in \mathrm{bild}(\varphi_x) \subset K(x)$ und $K(x)$ nach 11.3 der kleinste Teilkörper von L ist, der K und x enthält, folgt $\mathrm{bild}(\varphi_x) = K(x)$.
Sei $\lambda_0 \cdot 1 + \lambda_1 x + \cdots + \lambda_{n-1}x^{n-1} = 0$ mit $\lambda_0, \ldots, \lambda_{n-1} \in K$. Ist $\lambda_i \neq 0$ für ein i, so wähle i maximal mit $\lambda_i \neq 0$.
Dann ist $X^i + \cdots + \frac{\lambda_1}{\lambda_i}X + \frac{\lambda_0}{\lambda_i}$ normiert, hat x als Nullstelle und einen Grad $< n$. Widerspruch zur Minimalität von $n = \mathrm{grad}(m_x)$. Also sind $1, x, \ldots, x^{n-1}$ linear unabhängig. Ist $f(x) \in K(x)$, so ergibt Division mit Rest (vgl. 8.1), daß $f = qm_x + r$ mit $r = 0$ oder $\mathrm{grad}(r) < n$ in $K[X]$ gilt. Daher ist $f(x) = q(x) \cdot \underbrace{m_x(x)}_{=0} + r(x) = r(x)$ eine Linearkombination von $1, x, \ldots, x^{n-1}$. □

11.11 Beispiele

(1) Es ist $X^2 + 1$ irreduzibel über $\mathbb{Q}$, also $\mathbb{Q}[X]/(X^2+1) \simeq \mathbb{Q}(i)$ und $\{1, i\}$ ist Basis von $\mathbb{Q}(i)$ über $\mathbb{Q}$ nach 11.10.

(2) Man bestimme den Grad $[L : \mathbb{Q}]$, wobei $L = \mathbb{Q}(\sqrt[3]{2}, \zeta)$ (und $\sqrt[3]{2} \in \mathbb{R}$) und ζ Nullstelle von $f = X^2 + X + 1$ in $\mathbb{C}$ ist.
Nach 9.9 und 9.12 sind $X^3 - 2$ und f irreduzibel in $\mathbb{Q}[X]$.
$\underset{11.10}{\Longrightarrow}$ $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ und $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$. Betrachte

$$\begin{tikzcd}
 & L \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt[3]{2}) \arrow[dr, dash, "3"'] & & \mathbb{Q}(\zeta) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Nach Gradsatz 11.7 folgt $[L : \mathbb{Q}] \leq 6$ sowie $3 \mid [L : \mathbb{Q}]$ und $2 \mid [L : \mathbb{Q}]$
$\Longrightarrow [L : \mathbb{Q}] = 6$
Sei $x = \sqrt[3]{2} \underset{11.10}{\Longrightarrow} \mathbb{Q}(\zeta x) \simeq \mathbb{Q}(x)$, da $\zeta^3 = 1$ und also $m_x = m_{\zeta x}$.

(3) Man bestimme das Minimalpolynom m_x von $x = \sqrt{2 + \sqrt[3]{2}}$ über $\mathbb{Q}$. Es ist
$x^2 = 2 + \sqrt[3]{2} \Longrightarrow x^2 - 2 = \sqrt[3]{2}$
$\Longrightarrow (x^2-2)^3 = 2 \Longrightarrow x^6 - 6x^4 + 12x^2 - 8 = 2$
$\Longrightarrow \quad \boxed{m_x = X^6 - 6X^4 + 12X^2 - 10}$,
denn dieses Polynom ist nach Eisenstein mit $p = 2$ irreduzibel in $\mathbb{Q}[X]$

und hat x als Nullstelle (vgl. 11.9).
Folgerung: $[\mathbb{Q}(x) : \mathbb{Q}] = 6$ nach 11.10.

11.12 Eine Charakterisierung algebraischer Elemente

Satz. *Seien $K \subset L$ Körper, und sei $x \in L$. Dann gilt:*

$$\boxed{x \text{ algebraisch über } K} \iff \boxed{[K(x) : K] < \infty}$$

Beweis. "$\Rightarrow$" Es ist $[K(x) : K] = \operatorname{grad}(m_x)$ nach 11.10.

"$\Leftarrow$" Sei $\dim_K K(x) =: n < \infty$
$\Longrightarrow$ die $n+1$ Vektoren $1, x, \ldots, x^n$ sind linear abhängig
$\Longrightarrow \exists\, \lambda_0, \ldots, \lambda_n \in K$, die nicht alle Null sind, mit $\sum_{i=0}^{n} \lambda_i x^i = 0$
$\Longrightarrow f := \sum\limits_{i=0}^{n} \lambda_i X^i \neq 0$ und $f(x) = 0 \Longrightarrow x$ algebraisch.

$\square$

11.13 Einfache Körpererweiterungen

Definition. Eine Körpererweiterung L von K heißt *einfach*, wenn sie von einem Element erzeugt wird, wenn also $L = K(u)$ mit einem $u \in L$ gilt. Die einfachen algebraischen Körpererweiterungen sind durch 11.10 klassifiziert.

11.14 Einfache transzendente Körpererweiterungen

Satz. *Sei $K(u)$ eine Körpererweiterung von K, wobei u transzendent über K sei. Dann gelten:*

(1) *$K(u) \simeq K(X)$, wobei $K(X)$ der Quotientenkörper von $K[X]$ sei.*

(2) $[K(u) : K] = \infty$

(3) *u^2 ist transzendent, und es gilt $K(u^2) \subsetneq K(u)$*

Beweis. (1) folgt aus der Definition eines transzendenten Elementes (vgl. 11.8). Danach gilt für den Einsetzungshomomorphismus

$$\varphi_u \colon K[X] \longrightarrow K(u)\,,$$

dass $\operatorname{kern}(\varphi_u) = (0)$ ist. Hieraus folgt, dass der Quotientenkörper $K(X)$ isomorph zum Quotientenkörper von $\operatorname{bild}(\varphi_u) = \left\{ \sum\limits_{\text{endl.}} a_i u^i \mid a_i \in K \right\}$ ist.

(2) folgt aus 11.12.

(3) $1, u, \dots, u^m, \dots$ sind linear unabhängig $\forall\, m \in \mathbb{N}$.
Sei $f = \sum_{i=0}^{n} a_i X^i \in K[X]$ mit $f(u^2) = \sum_{i=0}^{n} a_i u^{2i} = 0 \Longrightarrow a_i = 0 \;\forall\, i$
$\Longrightarrow f = 0 \Longrightarrow u^2$ ist transzendent über K.
Es ist $K(u^2) \subset K(u)$.
Angenommen, $u \in K(u^2)$. Wende (1) auf u^2 an.
$\Longrightarrow u = \frac{f(u^2)}{g(u^2)}$ mit $f, g \in K[X]$ und $g(u^2) \neq 0 \Longrightarrow ug(u^2) = f(u^2)$.
Rechts stehen Linearkombinationen mit geraden Potenzen, links mit ungeraden.
$\Longrightarrow f(u^2) = 0 \Longrightarrow u = 0$. Widerspruch.

□

Fazit. Bis auf Isomorphie gibt es nur eine einfache transzendente Körpererweiterung von K, nämlich $K(X)$, aber eine einfache transzendente Körpererweiterung $K(u)$ von K hat unendlich viele Zwischenkörper.

$$K(u) \supsetneq K(u^2) \supsetneq \cdots \supsetneq K(u^{2n}) \supsetneq \cdots \supsetneq K$$

11.15 Übungsaufgaben 35 – 37

Aufgabe 35. Sei P der Primkörper eines Körpers K. Man zeige, dass jeder Isomorphismus $\sigma\colon K \longrightarrow K$ ein P-Isomorphismus ist. (Zu zeigen ist: $\sigma(a) = a$ für alle $a \in P$.)

Aufgabe 36. Seien p, q Primzahlen und $L = \mathbb{Q}(\sqrt{p}, \sqrt[3]{q})$. Man zeige, dass $[L : \mathbb{Q}] = 6$ ist und das $L = \mathbb{Q}(x)$ mit $x = \sqrt{p} \cdot \sqrt[3]{q}$ gilt. Man bestimme das Minimalpolynom von x über $\mathbb{Q}$.

Aufgabe 37. Man bestimme den Grad von $\mathbb{Q}(\sqrt{2}, i)$ über $\mathbb{Q}$ und das Minimalpolynom von $x = i + \sqrt{2}$ über $\mathbb{Q}$.

12 Algebraische Körpererweiterungen

Sei K ein Körper und L eine Körpererweiterung von K.

12.1 Definition

1) L heißt *endlich über* K, falls $[L : K] := \dim_K L < \infty$.

2) L heißt *algebraisch über* K, falls jedes Element aus L *algebraisch über* K ist, und andernfalls *transzendent über* K.

12.2 Endliche Körpererweiterungen sind algebraisch

Satz.

$$\boxed{L \text{ endlich über } K} \quad \Longrightarrow \quad \boxed{L \text{ algebraisch über } K}$$

Beweis. Sei $[L : K] = n < \infty$, und sei $x \in L$. Dann ist $[K(x) : K]$ nach dem Gradsatz in 11.7 ein Teiler von n und also $< \infty$. Mit 11.12 folgt, daß x algebraisch über K ist. □

Die Umkehrung von 12.2 ist i.a. falsch, vgl. Aufgabe 38.

12.3 Charakterisierung endlicher Körpererweiterungen

Satz. *Es sind äquivalent:*

(i) *L ist endlich über K.*

(ii) *Es gibt endlich viele über K algebraische Elemente $x_1, \dots, x_n \in L$ mit $L = K(x_1, \dots, x_n)$.*

Beweis. "$(i) \Rightarrow (ii)$" Jede Basis $\{x_1, \dots, x_n\}$ von L als K-Vektorraum erfüllt die Behauptung.

"$(ii) \Rightarrow (i)$" Induktion nach n:

Ist $L = K(x_1)$ und ist x_1 algebraisch über $K \underset{11.12}{\Longrightarrow} [L : K] < \infty$.

Sei $L = K(x_1, \dots, x_n)$ mit algebraischen $x_1, \dots, x_n \in L$.

$$\underset{11.7}{\Longrightarrow} [L : K] = \underbrace{[K(x_1, \dots, x_{n-1})(x_n) : K(x_1, \dots, x_{n-1})]}_{<\infty \text{ nach } 11.12} \cdot$$

$$\cdot \underbrace{[K(x_1, \dots, x_{n-1}) : K]}_{<\infty \text{ nach Ind.vor.}} < \infty.$$

□

12.4 Charakterisierung algebraischer Körpererweiterungen

Satz. *Es sind äquivalent:*

(i) *L ist algebraisch über K.*

(ii) *L wird über K von algebraischen Elementen erzeugt.*

Beweis. "$(i) \Rightarrow (ii)$" Klar nach Definition 12.1.

"$(ii) \Rightarrow (i)$" folgt mit Hilfe von 12.3 und 12.1.

□

12.5 Der algebraische Abschluß von K in L

Sei weiterhin L eine Körpererweiterung von K.

Satz. *Die Menge $\overline{K}$ aller über K algebraischen Elemente aus L ist ein Teilkörper von L.*

Beweis. Seien $x, y \in L$ algebraisch über K.
$\Longrightarrow K(x, y)$ ist algebraisch über K nach 12.4.
$\Longrightarrow$ Die Elemente $x + y$, xy, $-x$ und x^{-1} (mit $x \neq 0$) sind alle algebraisch über K, da sie in $K(x, y)$ liegen. □

Bemerkung. Die Körpererweiterung $\overline{K}$ heißt *algebraischer Abschluß von K in L.* Man nennt $\overline{\mathbb{Q}} \subset \mathbb{C}$ den *Körper der algebraischen Zahlen.* Dieser wird in der algebraischen Zahlentheorie studiert.

12.6 Die Eigenschaft „algebraisch" ist transitiv

Satz. *Seien $K \subset L \subset M$ Körpererweiterungen. Ist L algebraisch über K, und ist $x \in M$ algebraisch über L, so ist x algebraisch über K.*
Insbesondere sind äquivalent:

(i) *M über L algebraisch und L über K algebraisch*

(ii) *M ist algebraisch über K.*

Beweis. Sei L algebraisch über K und x algebraisch über L. Dann gibt es eine Gleichung

$$a_n x^n + \cdots + a_1 x + a_0 = 0 \text{ mit } a_0, \ldots, a_n \in L$$

$\Longrightarrow x$ ist algebraisch über $K' = K(a_0, \ldots, a_n) \Longrightarrow [K'(x) : K'] < \infty$ nach 11.12. Es ist auch $[K' : K] < \infty$ nach 12.3, da L algebraisch über K.

$\Longrightarrow [K'(x):K] \underset{11.7}{=} \underbrace{[K'(x):K']}_{<\infty}\underbrace{[K':K]}_{<\infty} < \infty$

$\Longrightarrow x$ ist algebraisch über K nach 12.2. Mit Definition 12.1 folgt auch die behauptete Äquivalenz. □

12.7 Existenz von Nullstellen in Körpererweiterungen

Satz (Kronecker). *Sei $p \in K[X]$ irreduzibel. Dann gibt es eine einfache Körpererweiterung $K(x) = L$ von K so, dass $p(x) = 0$ und $[L:K] = \mathrm{grad}(p)$ gilt.*

Beweis. Nach 8.13 ist $L := K[X]/(p)$ ein Körper, und der Homomorphismus

$$\psi\colon K \longrightarrow L,\ a \longmapsto a + (p)\,,$$

ist injektiv nach Folgerung 6.9. Wir können also K mit $\mathrm{bild}(\psi)$ identifizieren, und so wird L zu einer Körpererweiterung von K. Sei $x := X + (p)$ und $p = a_nX^n + \cdots + a_1X + a_0$ mit $a_0, \ldots, a_n \in K$.

$$\begin{aligned}\Longrightarrow p(x) &= \left(\sum_{i=0}^{n} a_iX^i\right) + (p) \text{ nach Satz 7.2}\\ &= p + (p) = 0 + (p) \text{ nach Lemma 7.2}\\ \Longrightarrow p(x) &= 0 \text{ in } L\,.\end{aligned}$$

Da p irreduzibel ist, folgt $(p) = (m_x)$ und also $L \simeq K(x)$ nach 11.10. Weiter folgt $\mathrm{grad}(p) \underset{11.9}{=} \mathrm{grad}(m_x) \underset{11.10}{=} [L:K]$. □

12.8 Existenz eines Zerfällungskörpers

Sei $f \in K[X]$ nicht konstant.

Definition. Eine Körpererweiterung L von K heißt *Zerfällungskörper von f*, wenn es Elemente $x_1, \ldots, x_m \in L$ und $c \in K$ mit

1. $f = c(X - x_1)\cdots(X - x_m)$ („alle Nullstellen von f sind in L“)
2. $L = K(x_1, \ldots, x_m)$ („L wird von den Nullstellen von f erzeugt“)

Satz. *Ist $f \in K[X]$ von Grad $n > 0$, so besitzt f einen Zerfällungskörper L mit $[L:K] \leq n!$.*

Beweis. Induktion nach n.
$n = 1 \Longrightarrow f := cX + b$ mit $c, b \in K$, $c \neq 0$
$\Longrightarrow L = K$ ist Zerfällungskörper mit $[L : K] = 1$,
$n > 1$: Es ist $f = q \cdot p$ mit irreduziblem $p \in K[X]$.
$\underset{12.7}{\Longrightarrow} \exists$ Körper $L_1 = K(x_1)$ mit $p(x_1) = 0$, also $f(x_1) = 0$ und $[L_1 : K] = \operatorname{grad}(p) \leq n$.
In $L_1[X]$ ist $f = (X - x_1)g$ mit $\operatorname{grad}(g) = n - 1$ nach 8.2.
Nach Induktionsvoraussetzung besitzt g einen Zerfällungskörper $L = L_1(x_2, \ldots, x_m)$ mit $[L : L_1] \leq (n-1)!$
Es folgt $f = c(X - x_1)(X - x_2) \cdots (X - x_m)$, wobei $c \in K$ der Leitkoeffizient von f ist, und

$$[L : K] \underset{11.7}{=} \underbrace{[L : L_1]}_{\leq (n-1)!} \underbrace{[L_1 : K]}_{\leq n} \leq n(n-1)! = n!$$

□

12.9 Algebraische Differenziation und mehrfache Nullstellen

Definition. Sei $f = a_n X^n + \cdots + a_1 X + a_0 \in K[X]$. Bilde die *Ableitung*

$$\boxed{f' := n a_{n-1} X^{n-1} + \cdots + 2a_2 X + a_1}$$

Regeln. *Für $f, g \in K[X]$ und $\lambda, \mu \in K$ gelten:*

(1) $(\lambda f + \mu g)' = \lambda f' + \mu g'$ *("Linearität")*

(2) $(fg)' = f'g + fg'$ *("Produktregel")*

Beweis. (1) folgt aus der Definition der Ableitung.

(2) Wegen (1) genügt es, den Fall $g = X^m$ zu betrachten.

$$\begin{aligned}\Longrightarrow (fg)' = (fX^m)' = \left(\sum_i a_i X^{i+m}\right)' &= \sum_i (i+m) a_i X^{i+m-1} \\ &= \left(\sum_i i a_i X^{i-1}\right) X^m + \left(\sum_i a_i X^i\right) m X^{m-1} \\ &= f'g + fg'\end{aligned}$$

□

Satz. *Seien $f \in K[X] \setminus \{0\}$ und L ein Zerfällungskörper von f. Dann sind für $x \in L$ äquivalent:*

(1) *x ist mehrfache Nullstelle von f (d.h. $(X-x)^2 \mid f$ in $L[X]$).*

(2) *x ist Nullstelle von f und f'.*

(3) *x ist Nullstelle von $\mathrm{ggT}(f, f')$.*

Beweis. Sei x Nullstelle von f mit *Vielfachheit* m. Dann gilt: $f = (X-x)^m g$ mit $g \in L[X]$ und $g(x) \neq 0$ sowie $f' = m(X-x)^{m-1}g + (X-x)^m g'$ nach Produktregel. Es folgt $f'(x) = 0 \Longleftrightarrow m \geq 2$, also (1) $\Leftrightarrow$ (2).
Die Äquivalenz (2) $\Leftrightarrow$ (3) ist offensichtlich. □

Korollar. *Sei $f \in K[X]$ irreduzibel. Dann besitzt f genau dann eine mehrfache Nullstelle in L, wenn $f' = 0$ ist. Ist $\mathrm{char}(K) = 0$, so besitzt f keine mehrfache Nullstelle in L.*

Beweis. Wenn $f \mid f'$ gilt, folgt $f' = 0$ (da sonst $\mathrm{grad}(f') \geq \mathrm{grad}(f)$ gelten würde). Es folgt $f' = 0 \Longleftrightarrow f \mid f' \Longleftrightarrow \mathrm{ggT}(f, f') = f \underset{f \text{ irr}}{\Longleftrightarrow} \mathrm{ggT}(f, f')$ nicht konstant $\underset{\text{Satz}}{\Longleftrightarrow} f$ hat eine mehrfache Nullstelle in L.
Ist $\mathrm{char}(K) = 0 \Longrightarrow f' \neq 0$. □

12.10 Übungsaufgaben 38 – 42

Aufgabe 38. Sei $a_n \in \mathbb{R}$ eine Nullstelle des Polynoms $X^n - 2 \in \mathbb{Q}[X]$, und sei
$L = \mathbb{Q}(\{a_n \mid n \in \mathbb{N}\})$. Man zeige, dass L über $\mathbb{Q}$ algebraisch ist und dass $[L : \mathbb{Q}] = \infty$ gilt.

Aufgabe 39. (a) Man zeige für Körpererweiterungen $K \subset K' \subset L$ mit $[L : K] = [L : K'] < \infty$, dass $K' = K$ gilt.

(b) Man belege mit einem Beispiel, dass in der obigen Behauptung notwendig $K \subset K' \subset L$ vorausgesetzt werden muss, d.h. aus $[L : K] = [L : K']$ folgt nicht zwingend $K' = K$.

Aufgabe 40. Sei L eine Körpererweiterung eines Körpers K von Primzahlgrad p. Man zeige:

(a) Es ist $L = K(x)$ für jedes $x \in L \setminus K$.

(b) Ist p ungerade, so gilt auch $L = K(x^2)$ für jedes $x \in L \setminus K$.

Aufgabe 41. Sei $L \subset \mathbb{C}$ ein Zerfällungskörper von $f = X^4 - 3 \in \mathbb{Q}[X]$.

(a) Man zeige, dass L über $\mathbb{Q}$ von i und einer Nullstelle x von f erzeugt wird.

(b) Man zeige, dass $[L : \mathbb{Q}] = 8$ gilt.

(c) Man bestimme drei Nullstellen x_1, x_2, x_3 von f so, dass $\mathbb{Q}(x_1, x_2)$ nicht isomorph zu $\mathbb{Q}(x_1, x_3)$ ist.

Aufgabe 42. Man untersuche, ob die Polynome

$$X^5 + 5X + 5\,, \quad X^5 + 6X^3 + 3X + 4 \quad \text{und} \quad X^4 - 5X^3 + 6X^2 + 4X - 8$$

aus $\mathbb{Q}[X]$ mehrfache Nullstellen in $\mathbb{C}$ besitzen und bestimme dieselben gegebenenfalls.

13 Normale Körpererweiterungen

Betrachte folgende Situation

$$\begin{tikzcd} L \arrow[r, dashed, "\sim", "\psi"'] \arrow[d, dash] & \tilde{L} \arrow[d, dash] \\ K \arrow[r, "\sim", "\varphi"'] & \tilde{K} \end{tikzcd}$$

Dabei seien L und $\tilde{L}$ Körpererweiterungen von K bzw. $\tilde{K}$ und φ ein Isomorphismus von Körpern.

Definition. Ein Isomorphismus $\psi\colon L \longrightarrow \tilde{L}$ heißt *Fortsetzung von* φ, wenn $\psi(a) = \varphi(a)\ \forall\, a \in K$ gilt. Man schreibt dann auch $\psi|_K = \varphi$.

13.1 Ein Fortsetzungslemma

Seien K und $\tilde{K}$ Körper, und sei $\varphi\colon K \longrightarrow \tilde{K}$ ein Isomorphismus. Dann induziert φ einen Ringisomorphismus

$$K[X] \longrightarrow \tilde{K}[X],\ f = \sum_i a_i X^i \longmapsto \sum_i \varphi(a_i) X^i =: \tilde{f}$$

Lemma. *Seien $p \in K[X]$ irreduzibel, x Nullstelle von p in einem Erweiterungskörper L von K und $\tilde{x}$ Nullstelle von $\tilde{p}$ in einem Erweiterungskörper $\tilde{L}$ von $\tilde{K}$. Dann gibt es einen Isomorphismus*

$$\boxed{\psi\colon K(x) \xrightarrow{\sim} \tilde{K}(\tilde{x}) \text{ mit } \psi(x) = \tilde{x} \text{ und } \psi(a) = \varphi(a)\ \forall\, a \in K}$$

Beweis. Der obige Ringisomorphismus induziert einen Isomorphismus von Körpern

$$K[X]/(p) \xrightarrow{\sim} \tilde{K}[X]/(\tilde{p})\,,$$

und der gesuchte Isomorphismus ψ ergibt sich aus 11.9, 11.10 als Kompositum

$$K(x) \xrightarrow[11.10]{\sim} K[X]/(p) \xrightarrow{\sim} \tilde{K}[X]/(\tilde{p}) \xrightarrow[11.10]{\sim} \tilde{K}(\tilde{x})$$

$\square$

13.2 Folgerung

Satz. *Seien $p \in K[X]$ irreduzibel und x, y Nullstellen von p in Erweiterungskörpern von K. Dann gibt es einen K-Isomorphismus*

$$\psi\colon K(x) \xrightarrow{\sim} K(y)$$

mit $\psi(x) = y$.

Beweis. Wende 13.1 mit $\varphi = \mathrm{id}$ und $\tilde{x} = y$ an. □

13.3 Fortsetzung von Isomorphismen auf Zerfällungskörper

Satz. *Seien $\varphi\colon K \xrightarrow{\sim} \tilde{K}$ ein Isomorphismus von Körpern, $f \in K[X]$ nicht konstant und L bzw. $\tilde{L}$ Zerfällungskörper von f bzw. von dem zu f gehörigen Polynom $\tilde{f} \in \tilde{K}[X]$. Dann gibt es einen Isomorphismus*

$$\psi\colon L \longrightarrow \tilde{L} \textit{ mit } \psi(a) = \varphi(a)\ \forall\, a \in K\,.$$

Beweis. Induktion nach dem Grad von L (dieser ist $< \infty$ nach 12.8).
Ist $[L : K] = 1 \Longrightarrow L = K$ und $\tilde{L} = \tilde{K}$. Setze $\psi = \varphi$.
Sei $[L : K] > 1$. Wähle irreduziblen Faktor p von f vom Grad > 1 und eine Nullstelle x von p mit $[L : K(x)] < [L : K]$ (ist möglich nach Gradsatz 11.7).
Nach 13.1 hat φ eine Fortsetzung

$$\psi\colon K(x) \xrightarrow{\sim} \tilde{K}(\tilde{x})\,.$$

Da L auch Zerfällungskörper von f über $K(x)$ und $\tilde{L}$ Zerfällungskörper von $\tilde{f}$ über $\tilde{K}(\tilde{x})$ ist, hat ψ nach Induktionsvoraussetzung eine Fortsetzung $\psi_1\colon L \xrightarrow{\sim} \tilde{L}$, und es gilt $\psi_1(a) = \psi(a) = \varphi(a)\ \forall\, a \in K$. □

13.4 Eindeutigkeit des Zerfällungskörpers

Korollar. *Ein nicht konstantes Polynom $f \in K[X]$ besitzt bis auf K-Isomorphie genau einen Zerfällungskörper.*

Beweis. Die Existenz wurde in 12.8 gezeigt. Die Eindeutigkeit folgt aus 13.3 für $\varphi = \mathrm{id}$. □

13.5 Definition einer normalen Erweiterung

Definition. Eine algebraische Körpererweiterung L von K heißt *normal*, wenn jedes irreduzible Polynom aus $K[X]$, das in L eine Nullstelle hat, in $L[X]$ ganz in Linearfaktoren zerfällt.

13.6 Charakterisierung endlicher normaler Erweiterungen

Satz. *Sei* $[L : K] < \infty$. *Dann gilt:*

$$\boxed{L \text{ normal über } K} \iff \boxed{L \text{ ist Zerfällungskörper eines Polynoms } f \in K[X]}$$

Beweis. L ist algebraisch, da $[L : K] < \infty$, vgl. 12.2.

"$\Rightarrow$" Sei $\{x_1, \ldots, x_n\}$ eine Basis von L als K-Vektorraum. Dann ist $L = K(x_1, \ldots, x_n)$, und jedes x_i ist Nullstelle seines Minimalpolynom $m_i \in K[X]$. Nach 13.5 zerfällt daher jedes m_i und daher auch $f := m_1 \cdots m_n$ in Linearfaktoren in $L[X]$.

"$\Leftarrow$" Sei L Zerfällungskörper von $f \in K[X]$. Sei $p \in K[X]$ irrduzibel mit $p(x) = 0$ für ein $x \in L$. Zu zeigen: Jede weitere Nullstelle von p liegt in L. Nach 13.2 gibt es einen K-Isomorphismus

$$\varphi \colon K(x) \xrightarrow{\sim} K(y)\,.$$

Es ist $L = L(x)$ Zerfällungskörper von f über $K(x)$, und $L(y)$ ist Zerfällungskörper von f über $K(y)$.

$\underset{13.3}{\Longrightarrow} \exists$ Isomorphismus $\psi \colon L \xrightarrow{\sim} L(y)$ mit $\psi(a) = \varphi(a)\ \forall\, a \in K$

$\Longrightarrow \psi$ ist K-linear und $\dim_K L = \dim_K L(y)$.

Da $L \subset L(y) \Longrightarrow L = L(y) \Longrightarrow y \in L$.

□

13.7 Beispiele

1. $[L : K] = 2 \Longrightarrow L$ normal über K.
2. $\mathbb{Q}(\sqrt[3]{2})$ ist nicht normal über $\mathbb{Q}$, aber $\mathbb{Q}(\sqrt[3]{2}, \zeta)$ enthält alle Nullstellen von $X^3 - 2$, ist also normal über $\mathbb{Q}$. (Es ist $\zeta^3 = 1$, vgl. 11.11(2))

13.8 Einbettung in eine normale Erweiterung

Satz. *Zu jeder endlichen Körpererweiterung K' von K gibt es eine endliche normale Körpererweiterung von K, die K' enthält.*

Beweis. Wähle eine Basis $\{x_1, \ldots, x_r\}$ von K' als K-Vektorraum und setze $f = m_1 \cdots m_r$, wobei $m_i \in K[X]$ das Minimalpolynom von x_i sei für $i = 1, \ldots, r$.

Der Zerfällungskörper von f ist nach 13.6 normal, enthält K' und ist nach 12.8 endlich über K. □

13.9 Der Satz vom primitiven Element

Definition. Ein über K algebraisches Element x heißt *separabel über* K, falls sein Minimalpolnom $m_x \in K[X]$ keine mehrfachen Nullstellen in einem Zerfällungskörper besitzt.

Satz. *Ist x separabel und y algebraisch über K, so gibt es ein $u \in K(x,y)$ mit*

$$\boxed{K(u) = K(x,y)}.$$

Beweis. Ist $|K| < \infty \underset{12.3}{\Longrightarrow} |K(x,y)| < \infty \underset{14.2}{\Longrightarrow}$ Behauptung.
Der Körper K besitze also unendlich viele Elemente. Sei m_x bzw. m_y das Minimalpolynom von x bzw. y. Nach 13.8 und 13.1 gibt es eine Körpererweiterung $L \supset K(x,y)$ von K, in der alle Nullstellen $x, x_2, \dots, x_k$ von m_x und alle Nullstellen $y = y_1, y_2, \dots, y_n$ von m_y liegen. Da $|K| = \infty$ gilt, gibt es ein $c \in K$ mit

(1) $$c \neq \frac{y_j - y}{x - x_i} \ \forall\, i = 2, \dots, k, \ j = 1, \dots, n$$

Sei $u := cx + y \Longrightarrow K \subset K(u) \subset K(x,y) \subset L$. Zeige $x \in K(u)$. Dann folgt $\boxed{y = u - cx \in K(u)}$ und also $K(x,y) = K(u)$.
Es ist $m_y = \sum\limits_{j=0}^{n} a_j X^j$ mit $a_j \in K$ und $a_n = 1$.
Setze $h := \sum\limits_{j=0}^{n} a_j (u - cX)^j$ in $K(u)[X]$ (mit denselben a_j wie in m_y)
$\Longrightarrow h(x) = m_y(y) = 0$, also ist x Nullstelle von h in L und
$h(x_i) = m_y(u - cx_i) \neq 0 \ \forall i = 2, \dots, k$ (denn es ist
$u - cx_i = \underbrace{cx + y}_{u} - cx_i \underset{(1)}{\neq} y_j \ \forall\, i = 2, \dots, k, \ j = 1, \dots, n$ nach (1))
Es folgt

(2) $$\boxed{\mathrm{ggT}(m_x, h) = (X - x)}$$

in $L[X]$ (denn x ist separabel und $m_x = (X - x)(X - x_2) \cdots (X - x_k)$ in $L[X]$)
Betrachtet man $d := \mathrm{ggT}(m_x, h)$ in $K(u)[X]$, so folgt $d = X - x$ und also $x \in K(u)$ (denn $d \mid m_x$ und $d \mid h \underset{(2)}{\Longrightarrow} d \mid (X - x) \Longrightarrow d = 1$ oder $d = X - x$
Ist $d = 1 \underset{8.4(c)}{\Longrightarrow} 1 = rm_x + sh$ mit $r, s \in K(u)[X]$
Da $(X - x) \mid m_x$ und $(X - x) \mid h$ in $L[X]$
$\Longrightarrow (X - x) \mid 1$, Widerspruch). □

13.10 Korollar

Sind $x_1, \ldots, x_n$ separabel über K und ist y algebraisch über K, so gibt es ein $u \in K(x_1, \ldots, x_n)$ mit $K(u) = K(x_1, \ldots, x_n, y)$.

Beweis. folgt durch Induktion aus 13.9. □

13.11 Übungsaufgabe 43

Aufgabe 43. Seien $x = i\sqrt{5}$ und $y = (1+i)\sqrt[4]{5}$. Man zeige:

(a) $\mathbb{Q}(x)$ ist normal über $\mathbb{Q}$.

(b) $\mathbb{Q}(y)$ ist normal über $\mathbb{Q}(x)$.

(c) $\mathbb{Q}(y)$ ist nicht normal über $\mathbb{Q}$.

14 Endliche Körper

Definition. Ein *endlicher Körper* ist ein Körper mit endlich vielen Elementen. Ein solcher wird auch *Galoisfeld* genannt. Schreibweise: $K = \mathbb{F}_q$, wobei $q = |K|$ die Anzahl der Elemente des endlichen Körpers K ist.

14.1 Lemma über die Ordnung von Gruppenelementen

Lemma. *Sei G eine Gruppe, und seien $a, b \in G$. Dann gilt*

(1) $$\boxed{\operatorname{ord}(a) = m} \quad \Longrightarrow \quad \boxed{\operatorname{ord}(a^k) = \frac{m}{\operatorname{ggT}(k,m)} \forall\, k \in \mathbb{Z}}$$

Ist G abelsch, so gelten für $m := \operatorname{ord}(a)$ und $n := \operatorname{ord}(b)$

(2) $$\boxed{\operatorname{ggT}(m,n) = 1} \quad \Longrightarrow \quad \boxed{\operatorname{ord}(ab) = mn}$$

(3) $$\exists c \in G \textit{ mit } \operatorname{ord}(c) = \operatorname{kgV}(m,n)$$

Beweis. (1) Sei $d = \operatorname{ggT}(k,m) \Longrightarrow \boxed{m = dm'}$ und $k = dk'$ mit $\operatorname{ggT}(k', m') = 1$. Für $s := \operatorname{ord}(a^k)$ ist zu zeigen : $\boxed{s = m'}$.
Es ist $(a^k)^{m'} = a^{m'dk'} = a^{mk} = e$. Also $\boxed{s \leq m'}$.
Andererseits ist $e = (a^k)^s = a^{ks}$ und $ks = qm + r$ mit $q \in \mathbb{Z}$ und $0 \leq r < m \Longrightarrow e = a^{mq+r} = \underbrace{a^{mq}}_{e} a^r = a^r \Longrightarrow r = 0$ (da $\operatorname{ord}(a) = m$ gilt und m also minimal ist mit $a^m = e$)
$\Longrightarrow ks = mq \mid \cdot\frac{1}{d} \Longrightarrow k's = m'q$
$\Longrightarrow m' \mid k's \Longrightarrow m' \mid s$, da $\operatorname{ggT}(k', m') = 1$
$\Longrightarrow \boxed{m' \leq s}$

(2) Sei $t := \operatorname{ord}(ab)$. Zu zeigen $t = mn$. Es ist $(ab)^{mn} = (a^m)^n (b^n)^m = e \Longrightarrow t \leq mn$.
Andererseits ist $a^{nt} = a^{nt} \underbrace{b^{nt}}_{e} = (ab)^{nt} = e \Longrightarrow m \mid nt$
(denn $nt = qm + r \Longrightarrow r = 0$ analog wie im Beweis von (1))
$\Longrightarrow m \mid t$, da $\operatorname{ggT}(m,n) = 1$
Es folgt $mn \mid t$, also $mn \leq t$.

(3) Wähle Primfaktorzerlegung $\operatorname{kgV}(mn) = p_1^{n_1} \cdot \ldots \cdot p_r^{n_r}$. Es sei m_0 das Produkt der Faktoren $p_i^{n_i}$, die m teilen, und n_0 das Produkt der Faktoren $p_i^{n_i}$, die m nicht teilen
$\Longrightarrow \operatorname{kgV}(m,n) = m_0 n_0$, wobei $\operatorname{ggT}(m_0, n_0) = 1$, sowie $m_0 \mid m$ und

$n_0 \mid n$, also $m = m'm_0$ und $n = n'n_0$.
$\Longrightarrow \operatorname{ord}(a^{m'}) \underset{(1)}{=} \frac{m}{\operatorname{ggT}(m',m)} = m_0$ und $\operatorname{ord}(b^{n'}) = n_0$
$\Longrightarrow \operatorname{ord}(a^{m'}b^{n'}) \underset{(2)}{=} m_0 n_0 = \operatorname{kgV}(m,n)$.

□

14.2 Die multiplikative Gruppe eines Galoisfeldes ist zyklisch

Wir beweisen allgemeiner

Satz. *Sei K ein Körper, und sei H eine endliche Untergruppe von K^*. Dann ist H zyklisch.*

Beweis. Sei $a \in H$ ein Element maximaler Ordnung m, und sei
$H_m := \{h \in H \mid \operatorname{ord}(h) \mid m\}$. Dann gilt $|H_m| \leq m$, da jedes $h \in H$ Nullstelle des Polynoms $X^m - 1 \in K[X]$ ist (vgl. Satz 8.2).
Da $a \in H_m$ ist, gilt $m \leq |H_m|$. Also ist $|H_m| = m$ und H_m ist die von a erzeugte zyklische Untergruppe von H (vgl. AGLA 10.12).
Wenn es ein $b \in H \setminus H_m$ gäbe, so gäbe es auch ein $c \in H$ mit $\operatorname{ord}(c) \underset{14.1}{=} \operatorname{kgV}(\operatorname{ord}(b), m) > m$ im Widerspruch zur Maximalität von m. □

14.3 Satz über die Anzahl der Elemente eines Galoisfeldes

Satz. *Sei K ein endlicher Körper. Dann ist* $\operatorname{char}(K) = p > 0$, *und es gilt* $|K| = p^n$, *wobei n der Grad von K über seinem Primkörper ist.*

Beweis. Nach 11.6 gilt für den Primkörper P von L, daß $P \simeq \mathbb{Z}/p\mathbb{Z}$ mit einer Primzahl p oder $P \simeq \mathbb{Q}$ gilt. Da $|K| < \infty$ ist, kommt $\mathbb{Q}$ nicht in Frage, und also ist $\operatorname{char}(K) = p$.
Sei $n = [K : P] := \dim_P K$ und sei $\{x_1, \ldots, x_n\}$ eine Basis von K als P-Vektorraum. Dann ist jedes $x \in K$ darstellbar als $x = \lambda_1 x_1 + \cdots + \lambda_n x_n$ mit eindeutig bestimmten $\lambda_1, \ldots, \lambda_n \in P$. Da $|P| = p$ gilt, sind für jeden Koeffizienten p Werte möglich. Es gibt daher p^n Linearkombinationen der Form $\lambda_1 x_1 + \cdots + \lambda_n x_n$, also gilt $|K| = p^n$. □

14.4 Existenz und Eindeutigkeit eines Galoisfeldes mit q Elementen

Satz. *Sei p eine Primzahl, und sei $n \in \mathbb{N}$. Dann gibt es bis auf Isomorphie genau ein Galoisfeld K mit $q = p^n$ Elementen. Die Elemente von K sind die*

Nullstellen des Polynoms $X^q - X \in \mathbb{F}_p[X]$.

Beweis. Existenz: Sei $P = \mathbb{Z}/p\mathbb{Z}$, und sei K die Menge aller Nullstellen von $f = X^q - X \in P[X]$ in einem Zerfällungskörper L von f (vgl. 12.8). Dann ist K ein Körper, denn $0, 1 \in K$, und für $x, y \in K$ gilt $x^{p^n} = x$ und $y^{p^n} = y$ und also $(x+y)^{p^n} = x^{p^n} + y^{p^n} = x + y$ (da $\operatorname{char}(K) = p$), $(-x)^{p^n} = (-1)^{p^n} x^{p^n} = -x$ da $-x = x$, falls $p = 2$ und $(-1)^{p^n} = -1$, falls $p \neq 2$ sowie $\left(\frac{x}{y}\right)^{p^n} = \frac{x^{p^n}}{y^{p^n}} = \frac{x}{y}$, falls $y \neq 0$.
Da $f = X^q - X$ höchstens q Nullstellen in K hat, gilt $|K| \leq q$. Es ist $f' = qX^{q-1} - 1 = -1$ (da $q \equiv 0 \bmod p$), also hat f keine mehrfachen Nullstellen (vgl. Satz 12.9).
$\underset{8.2}{\Longrightarrow}$ f zerfällt in $K[X]$ in q verschiedene Linearfaktoren $\Longrightarrow |K| = q$.

Eindeutigkeit: Sei $\tilde{K}$ ein weiterer Körper mit $|\tilde{K}| = q$. Dann ist der Primkörper $\tilde{P}$ von $\tilde{K}$ isomorph zu P (vgl. 14.3 und 11.6).
Da $\tilde{K}^*$ nach 14.2 zyklisch von der Ordnung $q - 1$ ist, gilt $x^{q-1} = 1 \ \forall x \in \tilde{K}^*$ und damit $x^q = x \ \forall x \in \tilde{K}$. Also sind K und $\tilde{K}$ beide Zerfällungskörper von $X^q - X$. Nach 13.3 folgt $\tilde{K} \simeq K$.

□

Beispiel. $\mathbb{F}_4 \simeq \mathbb{F}_2[X]/(X^2 + X + 1)$
Eine Basis über $\mathbb{F}_2$ ist $\{1, x\}$, wobei x Nullstelle von $X^2 + X + 1$, vgl. 11.10.

14.5 Kleiner Satz von Fermat

Satz. *Sei p eine Primzahl, und sei $a \in \mathbb{Z}$ mit $a \not\equiv 0 \bmod p$.*
Dann ist $a^{p-1} \equiv 1 \bmod p$.

Beweis. Wende 14.4 mit $K = \mathbb{Z}/p\mathbb{Z}$ an. Dann ist jede Restklasse $\bar{a} = a \bmod p$ Nullstelle von $X^p - X$. Für $\bar{a} \neq \bar{0}$ gilt also $\bar{a}^{p-1} - \bar{1} = \bar{0}$. □

14.6 Satz von Wilson

Satz. *Für jede Primzahl p gilt:*

$$(p-1)! \equiv -1 \bmod p\,.$$

Beweis. Nach 14.4 gilt:
$X^{p-1} - \bar{1} = (X - \bar{1})(X - \bar{2}) \cdots (X - (\overline{p-1}))$ in $\mathbb{Z}/p\mathbb{Z}[X]$.
Setzt man $X = \bar{p}$ ein, erhält man $\overline{-1} = (\overline{p-1})!$. □

14.7 Übungsaufgaben 44 – 48

Aufgabe 44. Man stelle die Additions- und Multiplikationstafeln für $\mathbb{Z}/4\mathbb{Z}$ und für $\mathbb{F}_4$ auf und vergleiche sie.

Aufgabe 45. (a) Man bestimme den Zerfällungskörper des Polynoms $X^6 + 1 \in \mathbb{F}_2[X]$.

(b) Man zerlege das Polynom $X^9 - X$ in $\mathbb{F}_3[X]$ in irreduzible Faktoren.

(c) Man zerlege das Polynom $X^4 + X + 1$ in $\mathbb{F}_4[X]$ in irreduzible Faktoren.

Aufgabe 46. Man ermittle die Ordnungen der folgenden Gruppen.

(a) Der Gruppe $\mathrm{GL}_2(\mathbb{F}_q)$ der invertierbaren 2×2-Matrizen über $\mathbb{F}_q$.

(b) Der Gruppe $\mathrm{SL}_2(\mathbb{F}_q)$ der 2×2-Matrizen über $\mathbb{F}_q$ mit Determinante 1.

(c) Des Zentrums von $\mathrm{SL}_2(\mathbb{F}_q)$.

Aufgabe 47. Sei K ein Körper, und sei $m \in K$. Man zeige:

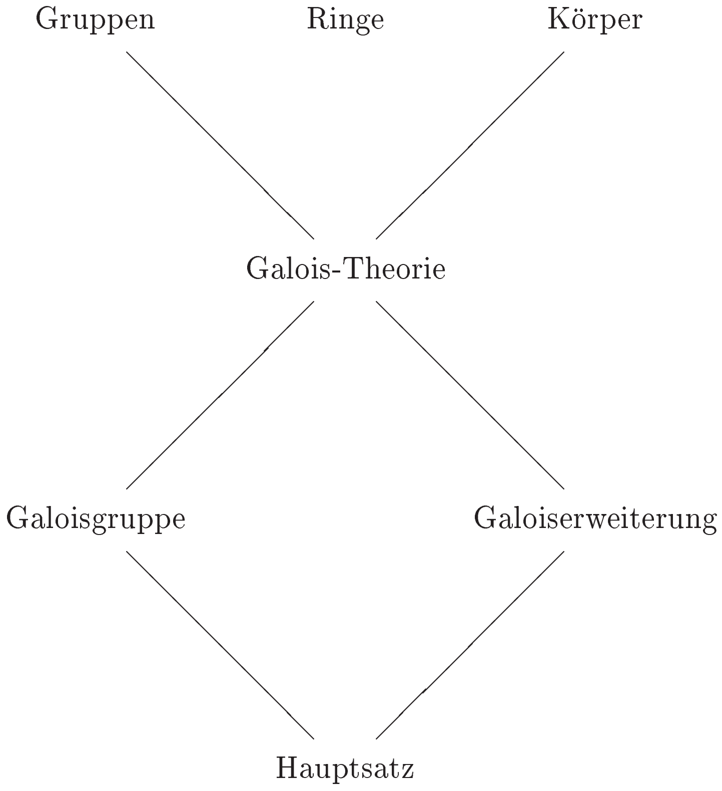
(a) Die Matrizen der Form $\begin{pmatrix} a & b \\ mb & a \end{pmatrix}$ bilden einen kommutativen Unterring L_m von $\mathrm{M}_{2\times 2}(K)$.

(b) L_m ist genau dann ein Körper, wenn m kein Quadrat in K ist.

(c) Ist L_m ein Körper und $K = \mathbb{F}_p$ mit einer ungeraden Primzahl p, so gilt $L_m \simeq \mathbb{F}_{p^2}$.

Aufgabe 48. Man bestimme die Ordnungen der Gruppen $\mathrm{GL}_3(\mathbb{F}_2)$ und $\mathrm{SL}_3(\mathbb{F}_2)$.

Teil IV
Galoistheorie



15 Galoiserweiterungen

15.1 Der Fixkörper

Definition. Ein *Automorphismus eines Körpers* L ist ein Isomorphismus $L \xrightarrow{\sim} L$. Die Menge aller Automorphismen von L bildet bezüglich Hintereinanderausführung eine Gruppe $\mathrm{Aut}(L)$. Für jede Untergruppe G von $\mathrm{Aut}(L)$ ist die Menge

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

ein Teilkörper von L, genannt *Fixkörper von* G.

15.2 Die Wirkung einer endlichen Automorphismengruppe

Jede Untergruppe G von $\mathrm{Aut}(L)$ operiert auf L durch

$$G \times L \longrightarrow L,\ (\sigma, x) \longmapsto \sigma(x)\ .$$

Ist G endlich, so ist die Bahn

$$B(x) := \{\sigma(x) \mid \sigma \in G\}$$

endlich, und es gilt $|B(x)| \leq |G|$, z.B. $B(a) = \{a\}\ \forall\, a \in L^G$.

Satz. *Sei L ein Körper und G eine endliche Untergruppe von $\mathrm{Aut}(L)$. Dann ist jedes $x \in L$ algebraisch über dem Fixkörper $K := L^G$.*
Ist $B(x) = \{x =: x_1, \ldots, x_r\}$ die Bahn von $x \in L$, so ist $[K(x) : K] = r$, und das Minimalpolynom von x über K ist

$$m_x = (X - x_1) \cdot \ldots \cdot (X - x_r)\,.$$

Insbesondere teilt der Grad $[K(x) : K]$ die Ordnung von G, und x ist separabel über K.

Beweis. Jedes $\tau \in G$ induziert einen Ringisomorphismus

$$\bar{\tau}\colon L[X] \longrightarrow L[X],\ \sum_i y_i X^i \longmapsto \sum_i \tau(y_i) X^i$$

Sei $f := (X - x_1) \cdots (X - x_r)$ in $L[X]$
$\Longrightarrow \bar{\tau}(f) = f\ \forall\, \tau \in G$ (denn $\tau(\sigma(x)) = (\tau\sigma)(x) \in B(x)\ \forall\, \sigma, \tau \in G$, also vertauscht $\bar{\tau}$ nur die Faktoren)
$\Longrightarrow f \in K[X]$, da $K = L^G$
$\Longrightarrow x$ ist algebraisch über K (da Nullstelle von f)
Sei $m_x \in K[X]$ das Minimalpolynom von x
$\underset{11.4}{\Longrightarrow}$ mit $x = x_1$ sind auch $x_2, \ldots, x_r$ Nullstellen von m_x (da $K = L^G$ und also jedes $\sigma \in G$ ein K-Automorphismus ist)
$\Longrightarrow f \mid m_x \Longrightarrow f = m_x$ (da m_x irreduzibel (vgl. 11.9) und f, m_x beide normiert sind)
$\Longrightarrow r = \mathrm{grad}(m_x) \underset{11.10}{=} [K(x) : K]$
Nach der Bahnformel 2.3 ist die Bahnlänge r ein Teiler von $|G|$. Da die Nullstellen $x_1, \ldots, x_r$ von m_x paarweise verschieden sind, ist x separabel über K (vgl. Definition 13.9). $\square$

15.3 Beispiel

Sei $L = \mathbb{Q}(i, \sqrt{2}) \subset \mathbb{C}$, und sei $x = i + \sqrt{2}$. Man berechne das Minimalpolynom $m_x \in \mathbb{Q}[X]$.
Seien $\sigma, \tau \in \operatorname{Aut}(L)$ definiert durch $\sigma(a) = a \ \forall\, a \in \mathbb{Q}$, sowie $\sigma(i) = -i$, $\sigma(\sqrt{2}) = \sqrt{2}$ und $\tau(i) = i$, $\tau(\sqrt{2}) = -\sqrt{2}$.
Dann ist $G := \{\mathrm{id}, \sigma, \tau, \sigma\tau\}$ die Kleinsche Vierergruppe ($\sigma^2 = \mathrm{id} = \tau^2$ und $\sigma\tau = \tau\sigma$).
Die Bahn von $x = i + \sqrt{2}$ ist
$\{x_1 = i + \sqrt{2}, x_2 = \underbrace{-i + \sqrt{2}}_{\sigma(x)}, x_3 = \underbrace{i - \sqrt{2}}_{\tau(x)}, x_4 = \underbrace{-i - \sqrt{2}}_{\sigma\tau(x)}\}$
$\underset{15.2}{\Longrightarrow} m_x = (X - x_1)(X - x_2)(X - x_3)(X - x_4) = X^4 - 2X^2 + 9$ (und $L = \mathbb{Q}(x)$).
Es ist

$$\begin{aligned}
-(\text{Koeffizient von } X^3) &= x_1 + x_2 + x_3 + x_4 = 0\,, \\
\text{Absolutglied} &= \underbrace{x_1x_2}_{3}\underbrace{x_3x_4}_{3} = 9\,, \\
-(\text{Koeffizient von } X) &= \underbrace{x_1x_2x_3}_{3x_3} + \underbrace{x_1x_2x_4}_{3x_4} + \underbrace{x_1x_3x_4}_{3x_1} + \underbrace{x_2x_3x_4}_{3x_2} \\
&= -6\sqrt{2} + 6\sqrt{2} = 0\,, \\
\text{Koeffizient von } X^2 &= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 \\
&= 3 - 3 - (1 + 2i\sqrt{2}) - (1 - 2i\sqrt{2}) - 3 + 3 = -2\,.
\end{aligned}$$

15.4 Der Grad über dem Fixkörper

Satz. *Sei G eine endliche Gruppe von Automorphismen eines Körpers L, und sei $K := L^G$ ihr Fixkörper. Dann ist $[L : K] = |G|$.*

Beweis. Nach 15.2 gilt $[K(x) : K] \leq |G|$ für jedes $x \in L$. Wähle $x \in L$ mit maximalem Grad $[K(x) : K]$. Zeige zunächst $L = K(x)$.
Sei $y \in L$ beliebig $\underset{15.2}{\Longrightarrow}$ y separabel über K
$\underset{13.9}{\Longrightarrow} \exists u \in L$ mit $K(x, y) = K(u) \Longrightarrow [K(u) : K] \leq [K(x) : K]$ nach Wahl von x
$\underset{11.10}{\Longrightarrow} K(x) = K(u)$, da $K(x) \subset K(u)$.
$\Longrightarrow y \in K(x)$ (für jedes $y \in L$). Es folgt $\boxed{L = K(x)}$.
Sei B die Bahn von x unter G.

$$\Longrightarrow \boxed{|B| \cdot |\operatorname{Stab}(x)| = |G|} \text{ nach Bahnformel 2.3}$$

Ist $\sigma \in \operatorname{Stab}(x) := \{\tau \in G \mid \tau(x) = x\}$
$\Longrightarrow \sigma(y) = y \ \forall\, y \in L$ (denn $K = L^G$ und $y = \lambda_0 + \lambda_1 x + \cdots + \lambda_{n-1}x^{n-1}$ mit

$\lambda_0, \dots, \lambda_{n-1} \in K$ nach 11.10)
$\Longrightarrow \sigma = \mathrm{id} \Longrightarrow |\,\mathrm{Stab}(x)| = 1$
$\Longrightarrow [L:K] \underset{15.2}{=} |B| \underset{2.3}{=} |G|$. □

15.5 Die Galoisgruppe einer Körpererweiterung

Definition. Sei L eine Körpererweiterung eines Körpers K. Dann heißt die Gruppe

$$G(L/K) := \mathrm{Aut}_K\, L := \{\sigma \in \mathrm{Aut}(L) \mid \sigma(a) = a \;\forall\, a \in K\}$$

die *Galoisgruppe von L über K.*

Bemerkung. Ist L Zerfällungskörper eines Polynoms $f \in K[X]$ und ist $M = \{x_1, \dots, x_r\}$ die Menge der verschiedenen Nullstellen von f, so operiert $G := G(L/K)$ auf M, und der Gruppenhomomorphismus

$$G(L/K) \longrightarrow S(M) := \{M \xrightarrow{\text{bij.}} M\} \simeq S_r,\; \sigma \longmapsto \sigma|_M\,,$$

ist injektiv.

Beweis. Die Operation geschieht durch

$$G(L/K) \times M \longrightarrow M,\; (\sigma, y) \longmapsto \sigma(y)\,,$$

denn mit y ist auch $\sigma(y)$ Nullstelle von f nach 11.4.
Ist $\sigma|_M = \mathrm{id} \Longrightarrow \sigma(x_j) = x_j \;\forall j = 1, \dots, r$.
Da auch $\sigma(a) = a \;\forall\, a \in K$ gilt und $L = K(x_1, \dots, x_r)$ ist, folgt $\sigma = \mathrm{id}$. □

Beispiel. $G(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, \sigma\}$ mit $\sigma(i) = -i$ und also $\sigma(-i) = i$. Es ist $f = X^2 + 1$ und $M = \{i, -i\}$ die Menge der Nullstellen von f.

15.6 Satz über die Ordnung der Galoisgruppe

Satz. *Sei L endlich über K. Dann ist die Galoisgruppe $G := G(L/K)$ endlich, und es ist $|G|$ ein Teiler von $[L:K] := \dim_K L$. Ferner gilt:*

$$\boxed{|G| = [L:K]} \quad \Longleftrightarrow \quad \boxed{L^G = K}$$

Beweis. Nach Definition 15.1 ist $L^G := \{a \in L \mid \sigma(a) = a \;\forall\, \sigma \in G\}$
$\Longrightarrow K \subset L^G \subset L \Longrightarrow [L:K] \underset{11.7}{=} [L:L^G][L^G:K] = |G| \cdot [L^G:K]$ nach 15.4, wenn $|G| < \infty$.
Hieraus folgt die zweite Behauptung und die Äquivalenz.

Noch zu zeigen: G ist endlich. Da $\dim_K L < \infty$ ist, ist L algebraisch über K nach 12.2. Seien $\{x_1, \ldots, x_r\}$ eine Basis von L als K-Vektorraum,
$f = m_{x_1} \cdots m_{x_r} \in K[X]$ das Produkt der Minimalpolynome und $\overline{L}$ ein Zerfällungskörper von f. Dann ist $L \subset \overline{L}$, und jedes $\sigma \in G$ hat nach 13.3 eine Fortsetzung zu einem $\bar{\sigma} \in G(\overline{L}/K)$. Es folgt $|G| \leq |G(\overline{L}/K)| \underset{15.5}{<} \infty$. □

15.7 Definition einer Galoiserweiterung

Definition. Sei L eine endliche Körpererweiterung eines Körpers K, und sei $G := G(L/K)$ die Galoisgruppe von L über K. Dann ist $|G|$ ein Teiler von $[L : K]$ nach 15.6, und L heißt *Galoiserweiterung von* K oder *galoissch über* K, falls
$|G| = [L : K]$ gilt.

Beispiel. $\mathbb{C}$ ist galoissch über $\mathbb{R}$, denn $|G(\mathbb{C}/\mathbb{R})| = 2$ nach 15.5 und $[\mathbb{C} : \mathbb{R}] = 2$, da $\{1, i\}$ Basis von $\mathbb{C}$ als $\mathbb{R}$-Vektorraum.

15.8 Charakterisierung von Galoiserweiterungen

Definition. 1. Eine Körpererweiterung L von K heißt *separabel* (vgl. 13.9), wenn jedes Element aus L separabel über K ist.

2. Ein Polynom $f \in K[X]$ heißt *separabel*, wenn jeder irreduzible Faktor von f keine mehrfachen Nullstellen in einem Zerfällungskörper von f besitzt.

Satz. *Für eine endliche Körpererweiterung L eines Körpers K sind äquivalent:*

(1) *L ist galoissch über K.*

(2) $L^{G(L/K)} = K$.

(3) *L ist normal und separabel.*

(4) *L ist Zerfällungskörper eines separablen Polynoms aus $K[X]$.*

Beweis. (1) $\Leftrightarrow$ (2) wurde in 15.6 gezeigt.

(2) $\Rightarrow$ (3) Nach 15.2 ist jedes $x \in L$ separabel über $L^{G(L/K)} \underset{(2)}{=} K \Longrightarrow L$ ist separabel über K.
Sei $p \in K[X]$ irreduzibel und sei $x \in L$ eine Nullstelle von p.
$\underset{15.2}{\Longrightarrow} p = cm_x$ (mit $c \in K$) zerfällt in $L[X]$ in Linearfaktoren
$\underset{13.5}{\Longrightarrow} L$ normal über K.

(3) ⇒ (4) Da L über K normal $\underset{13.6}{\Longrightarrow}$ L ist Zerfällungskörper eines Polynoms $f \in K[X]$.
Da L separabel über $K \Longrightarrow f$ ist separabel (denn jeder normierte irreduzible Faktor von f ist Minimalpolynom aller seiner Nullstellen).

(4) ⇒ (2) Sei $G := G(L/K)$, und sei L Zerfällungskörper eines separablen Polynoms $f \in K[X]$. Es gilt $K \subset L^G \subset L$.
Zeige: $L^G \subset K$ durch Induktion nach der Anzahl n der nicht in K liegenden Nullstellen von f.
$n = 0 \Longrightarrow K = L^G = L$.
Sei nun $x \in L \setminus K$ eine Nullstelle von f. Das Minimalpolynom m_x ist ein irreduzibler Faktor von f, hat also lauter verschiedene Nullstellen $x, x_2, \ldots, x_r \in L$. Es folgt $r = \operatorname{grad}(m_x) = [K(x) : K] > 1$ nach 11.10. Nach 13.2 gibt es zu jedem $i = 2, \ldots, r$ einen K-Isomorphismus $\psi_i\colon K(x) \longrightarrow K(x_i)$ mit $\psi_i(x) = x_i$, und nach 13.3 gibt es dazu jeweils ein $\sigma_i \in G$ mit $\sigma_i(x) = x_i$. Es ist $G(L/K(x)) \subset G$, also

$$L^G \subset L^{G(L/K(x))} \subset K(x)$$

nach Induktionsvoraussetzung (denn betrachtet man f als Polynom in $K(x)[X]$, so bleibt f separabel und L ist Zerfällungskörper von f).
Sei nun $y \in L^G$. Zu zeigen: $y \in K$. Es ist $y = \lambda_0 + \lambda_1 x + \cdots + \lambda_{r-1} x^{r-1}$ mit $\lambda_0, \ldots, \lambda_{r-1} \in K$ nach 11.10 und da $y \in K(x)$
$\underset{y \in L^G}{\Longrightarrow} y = \sigma_2(y) = \lambda_0 + \lambda_1 x_2 + \cdots + \lambda_{r-1} x_2^{r-1}, \ldots,$
$y = \sigma_r(y) = \lambda_0 + \lambda_1 x_r + \cdots + \lambda_{r-1} x_r^{r-1}$
$\Longrightarrow h := y - \lambda_0 + \lambda_1 X + \cdots + \lambda_{r-1} X^{r-1} \in L^G[X]$ hat r verschiedene Nullstellen $x, x_2, \ldots, x_r$ und ist vom Grad $< r \Longrightarrow h = 0$
$\Longrightarrow y = \lambda_0 \in K$.

□

15.9 Folgerung

Satz. *Jede endliche separable Körpererweiterung von K läßt sich in eine Galoiserweiterung von K einbetten.*

Beweis. Sei L endlich-separabel über K.
$\underset{13.9}{\Longrightarrow} L = K(u)$ mit einem separablen $u \in L$
$\underset{15.8}{\Longrightarrow}$ Der Zerfällungskörper von m_u ist galoissch über K. □

15.10 Übungsaufgaben 40 – 50

Aufgabe 49. Man bestimme für folgende Körper L die Galoisgruppe $G(L/\mathbb{Q})$.

(a) $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.

(b) $L = \mathbb{Q}(\sqrt[3]{2})$.

Aufgabe 50. Für $a \in \mathbb{Q}$ sei L_a der Zerfällungskörper des Polynoms $X^3 - a$. Man bestimme die Galoisgruppe $G(L_a/\mathbb{Q})$ in Abhängigkeit von a.

16 Hauptsatz der Galoistheorie

Definition. Sei K ein Körper und L eine endliche Körpererweiterung von K. Ein *Zwischenkörper* Z ist ein Teilkörper von L mit $K \subset Z \subset L$.

Wenn L galoisch über K ist, liefert der Hauptsatz eine Übersicht über alle Zwischenkörper: Diese entsprechen eineindeutig den Untergruppen der Galoisgruppe $G(L/K) := \operatorname{Aut}_K L$.

16.1 Hauptsatz

Satz. *Sei L eine Galoiserweiterung eines Körpers K mit Galoisgruppe $G := G(L/K)$. Dann ist L galoissch über jedem Zwischenkörper, und man hat eine Bijektion von Mengen*

$$\begin{aligned} \{\textit{Zwischenkörper}\} &\xrightarrow{\sim} \{\textit{Untergruppen von } G\}, \\ Z &\longmapsto G(L/Z) = \{\sigma \in \operatorname{Aut}(L) \mid \sigma(z) = z \;\forall\, z \in Z\} \end{aligned}$$

mit Umkehrabbildung

$$\begin{aligned} \{\textit{Untergruppen von } G\} &\xrightarrow{\sim} \{\textit{Zwischenkörper}\}, \\ H &\longmapsto L^H := \{z \in L \mid \sigma(z) = z \;\forall\, \sigma \in H\} \end{aligned}$$

Dabei gelten

(1) $\quad [Z : K] = \dfrac{|G|}{|G(L/Z)|}$

(2) $\quad Z \subset Z' \Longrightarrow G(L/Z') \subset G(L/Z) \quad$ *und* $\quad H \subset H' \Longrightarrow L^{H'} \subset L^H$.

Beweis. L ist galoissch über K.
$\Longrightarrow$ L ist Zerfällungskörper eines separablen Polynoms aus $K[X] \subset Z[X]$.
$\Longrightarrow$ L ist Zerfällungskörper eines separablen Polynoms aus $Z[X]$.
$\Longrightarrow$ L ist galoissch über Z.
Zeige, daß die Abbildungen

$$Z \overset{\varphi}{\longmapsto} G(L/Z) \text{ und } H \xrightarrow{\psi} L^H$$

invers zueinander sind. Es ist
$\psi(\varphi(Z)) = L^{G(L/Z)} = Z$ nach 15.8.2, da L galoissch über Z
$\varphi(\psi(H)) = G(L/L^H) = H$, denn
$|H| \underset{15.4}{=} [L : L^H] \underset{15.7}{=} |G(L/L^H)|$, da L galoissch über L^H.
Da $H \subset G(L/L^H)$, folgt $H = G(L/L^H)$.

(1) Es ist $|G| \underset{15.7}{=} [L:K] \underset{11.7}{=} [L:Z][Z:K] \underset{15.7}{=} |G(L/Z)| \cdot [Z:K]$

(2) Klar nach Definition.

$\square$

16.2 Beispiel

$L = \mathbb{Q}(\sqrt[3]{2}, \zeta)$ mit $\zeta^2 + \zeta + 1 = 0$ und $\zeta^3 = 1$
$\underset{11.11}{\Longrightarrow} [L : \mathbb{Q}] = 6$ und L ist Zerfällungskörper von $f = X^3 - 2 \in \mathbb{Q}[X]$, denn $X^3 - 2 = (X - \sqrt[3]{2})(X - \zeta\sqrt[3]{2})(X - \zeta^2\sqrt[3]{2})$
$\underset{15.8}{\Longrightarrow} L$ ist galoissch über $\mathbb{Q} \Longrightarrow |G(L/\mathbb{Q})| = 6$
$\Longrightarrow G \simeq S_3$ nach 15.5.
Betrachte

$$\begin{tikzcd}
& L \arrow[dl, dash, "\text{gal}"', "3"] \arrow[dr, dash, "2"', "\text{gal}"] & \\
\mathbb{Q}(\zeta) \arrow[dr, dash, "2", "\text{gal}"'] & & \mathbb{Q}(\sqrt[3]{2}) \arrow[dl, dash, "3"', "\text{nicht galoissch, da nicht normal}"] \\
& \mathbb{Q} &
\end{tikzcd}$$

Setze $\sigma(\sqrt[3]{2}) = \zeta\sqrt[3]{2}$, $\sigma(\zeta) = \zeta$
$\Longrightarrow \sigma^2(\sqrt[3]{2}) = \zeta^2\sqrt[3]{2}$ und $\sigma^3 = \mathrm{id}$
$\Longrightarrow G(L/\mathbb{Q}(\zeta)) = \{\mathrm{id}, \sigma, \sigma^2\}$

16.3 Wann ist ein Zwischenkörper galoissch über K?

Seien $K \subset Z \subset L$ endliche Körpererweiterungen, wobei L galoissch über K sei. Dann ist L galoissch über Z nach 16.1, aber Z ist i.a. nicht galoissch über K.

$$K \overset{?}{\hookrightarrow} Z \overset{\text{gal}}{\hookrightarrow} L$$

Sei $G := G(L/K)$ die Galoisgruppe von L über K.

Lemma. *Für jedes $\sigma \in G$ ist $\sigma(Z)$ ein Zwischenkörper, und es gilt*

$$\boxed{G(L/\sigma(Z)) = \sigma G(L/Z)\sigma^{-1} \quad \forall\, \sigma \in G}$$

Beweis. Für $\sigma, \tau \in G$ gilt

$$\begin{aligned}\tau \in G(L/\sigma(Z)) &\Longleftrightarrow \tau(\sigma(z)) = \sigma(z)\ \forall z \in Z\\ &\Longleftrightarrow \sigma^{-1} \circ \tau \circ \sigma \in G(L/Z)\\ &\Longleftrightarrow \tau \in \sigma G(L/Z)\sigma^{-1}\end{aligned}$$

□

Satz. *Äquivalent sind*

(a) Z ist galoissch über K.

(b) $\sigma(Z) = Z \quad \forall\, \sigma \in G$.

(c) $G(L/Z)$ ist Normalteiler in G.

Ferner gilt: Ist (b) erfüllt, so gibt es einen Gruppenhomomorphismus

$$G \longrightarrow G(Z/K),\ \sigma \longmapsto \sigma|_Z\,,$$

und dieser induziert einen Isomorphismus

$$G/G(L/Z) \simeq G(Z/K)\,.$$

Beweis. **"(b)⇔(c)"** Es gilt $\sigma(Z) = Z\ \forall\, \sigma \in G$
$\underset{16.1}{\Longleftrightarrow} G(L/\sigma(Z)) = G(L/Z)\ \forall\, \sigma \in G$
$\underset{\text{Lemma}}{\Longleftrightarrow} G(L/Z) \triangleleft G$

"(a)⇒(b)" Sei Z galoissch über K.
$\underset{15.8}{\Longrightarrow} Z$ ist Zerfällungskörper eines separablen Polynoms $f \in K[X]$.
$\Longrightarrow Z = K(M)$, wobei M die Menge der Nullstellen von f ist (vgl. Definition 12.8)
Ist $x \in M \Longrightarrow \sigma(x) \in M\ \forall\, \sigma \in G$ nach Satz 11.4.
$\Longrightarrow \sigma(Z) \subset Z\ \forall\, \sigma \in G$ und also auch $Z \subset \sigma^{-1}(Z)\ \forall\, \sigma \in G$
$\Longrightarrow \sigma(Z) = Z$.

"(b)⇒(a)" Sei $\sigma(Z) = Z\ \forall\, \sigma \in G$
$\Longrightarrow \exists$ Homomorphismus $\varphi\colon G \longrightarrow G(Z/K),\ \sigma \longmapsto \sigma|_Z$ mit $\operatorname{kern}(\varphi) = G(L/Z)$
$\Longrightarrow [Z:K] \underset{16.1}{=} \frac{|G|}{|G(L/Z)|} \underset{1.2}{=} |\operatorname{bild}(\varphi)| \le |G(Z/K)|$
Da andererseits $|G(Z/K)| \le [Z:K]$ nach 15.6 gilt, folgt $|G(Z/K)| = [Z:K]$
$\Longrightarrow$ (a) nach Definition 15.7
Ferner folgt $\operatorname{bild}(\varphi) = G(Z/K)$.

□

16.4 Beispiel

Sei $L = \mathbb{Q}(x, \zeta)$ mit $x = \sqrt[3]{2} \in \mathbb{R}$ und einer dritten Einheitswurzel $\zeta \in \mathbb{C} \setminus \mathbb{R}$, also $\zeta^2 + \zeta + 1 = 0$ und $\zeta^3 = 1$ wie in 16.2. Es ist $G(L/\mathbb{Q}) = \{\mathrm{id}, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$, wobei $\sigma(x) = \zeta x$, $\sigma(\zeta) = \zeta$ und $\tau(x) = x$ und $\tau(\zeta) = \zeta^2$. Man erhält die Zwischenkörper

$$\begin{tikzcd}
 & & & L \arrow[dlll, dash, "3"'] \arrow[dl, dash, "2"] \arrow[dr, dash, "2"'] \arrow[drrr, dash, "2"] & & & \\
\mathbb{Q}(\zeta) & & \mathbb{Q}(x) & & \mathbb{Q}(\zeta x) & & \mathbb{Q}(\zeta^2 x) \\
 & & & \mathbb{Q} \arrow[ulll, dash, "2"] \arrow[ul, dash, "3"'] \arrow[ur, dash, "3"] \arrow[urrr, dash, "3"'] & & &
\end{tikzcd}$$

Es ist $\mathbb{Q}(\zeta)$ galoissch über $\mathbb{Q}$, denn $X^2 + X + 1 = (X - \zeta)(X - \zeta^2)$, (vgl. 15.8).
Aber die drei anderen echten Zwischenkörper sind nicht galoissch über $\mathbb{Q}$, da sie nicht normal über $\mathbb{Q}$ sind.
Sie erfüllen 16.3(b) nicht, denn

$$\sigma(\mathbb{Q}(x)) = \mathbb{Q}(\zeta x) \neq \mathbb{Q}(x) \subset \mathbb{R}$$

Es ist $\sigma(\zeta^2 x) = \zeta^2 \zeta x = x$ und $\sigma\tau(\zeta x) = x$, also $\sigma(\mathbb{Q}(\zeta^2 x)) = \mathbb{Q}(x) \neq \mathbb{Q}(\zeta^2 x)$ und $\sigma\tau(\mathbb{Q}(\zeta x)) = \mathbb{Q}(x) \neq \mathbb{Q}(\zeta x)$.
Sie erfüllen 16.3(c) nicht, weil die Galois-Gruppe $G(L/Z)$ für $Z = \mathbb{Q}(\zeta^2 x)$ jeweils eine 2-Sylowgruppe in G ist, also G drei Sylowgruppen besitzt.
$\Longrightarrow G(L/Z)$ ist kein Normalteiler in G nach 2.9(c).

16.5 Abelsche und zyklische Galoiserweiterungen

Definition. Sei L eine endliche Körpererweiterung eines Körpers K. Dann heißt L *abelsch*, wenn L galoissch über K ist und die Galoisgruppe $G(L/K)$ abelsch ist, und L heißt *zyklisch*, wenn L galoissch über K ist und die Galoisgruppe $G(L/K)$ zyklisch ist.

Beispiele. 1) Ist $L = \mathbb{Q}(\sqrt[3]{2}, \zeta)$ wie in 16.2, 16.4, so ist $G(L/\mathbb{Q}) \simeq S_3$, und also L nicht abelsch (und erst recht nicht zyklisch). Aber L ist zyklisch über $\mathbb{Q}(\zeta)$, da $G(L/\mathbb{Q}(\zeta)) \simeq \mathbb{Z}/3\mathbb{Z}$ nach 16.2.

2) Sei $L = \mathbb{Q}(i, \sqrt{2})$ wie in 15.3. Dann ist L abelsch, aber nicht zyklisch über $\mathbb{Q}$, da $G(L/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

3) Ist L eine Körpererweiterung vom Grad 2 über $\mathbb{Q}$, so ist L zyklisch, da $G(L/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$.

16.6 Die Zwischenkörper einer zyklischen Körpererweiterung

Bemerkung. Sei L zyklisch vom Grad n über einem Körper K. Dann entsprechen die Zwischenkörper genau den (positiven) Teilern von n. Ist m Teiler von n, so gibt es genau einen Zwischenkörper Z mit $[L : Z] = m$. Es ist L zyklisch über Z und Z zyklisch über K mit $[Z : K] = \frac{n}{m}$.

Beweis. Dies folgt mit Hilfe des folgenden Satzes aus dem Hauptsatz 16.1 und 16.3. □

Satz. *Sei $G = \{\sigma, \ldots, \sigma^{n-1}, \sigma^n = e\}$ eine zyklische Gruppe der Ordnung n. Dann gibt es eine Bijektion von Mengen*

$$\psi\colon \{m \in \mathbb{N} \mid m \text{ Teiler von } n\} \xrightarrow{\sim} \{\text{Untergruppen von } G\},\ m \longmapsto H_m\,,$$

wobei H_m die von $\sigma^{n/m}$ erzeugte (zyklische) Untergruppe von G ist. Es ist $|H_m| = m$.

Beweis. $m \mid n \Longrightarrow n = km$ mit $k \in \mathbb{N}$.
$\Longrightarrow k = \frac{n}{m}$ und $\operatorname{ord}(\sigma^k) \underset{14.1}{=} \frac{n}{\operatorname{ggT}(k,n)} = \frac{n}{k} = m$.
$\Longrightarrow \psi$ ist injektiv.
Wir zeigen nun, daß jede Untergruppe H der additiven Gruppe $\mathbb{Z}/n\mathbb{Z}$ zyklisch ist und von $\frac{n}{|H|} + n\mathbb{Z}$ erzeugt wird. Daraus folgt, daß ψ surjektiv ist, da es einen Isomorphismus $\mathbb{Z}/n\mathbb{Z} \longmapsto G,\ H + n\mathbb{Z} \longmapsto \sigma^k$, gibt (vgl. AGLA 10.16).
Sei H eine beliebige Untergruppe von $\mathbb{Z}/n\mathbb{Z}$. Dann ist $|H|$ ein Teiler von n nach AGLA 10.13.
Sei $\pi\colon \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z},\ a \longmapsto a + n\mathbb{Z} \Longrightarrow \pi^{-1}(H)$ ist eine Untergruppe von $\mathbb{Z}$, die $n\mathbb{Z}$ enthält.
$\Longrightarrow \pi^{-1}(H) = \ell\mathbb{Z}$ mit einem $\ell \in \mathbb{N}$, weil jede Untergruppe von $\mathbb{Z}$ so aussieht (vgl. AGLA 10.5.5).
$\Longrightarrow H \underset{\pi \text{ surj.}}{=} \pi(\pi^{-1}(H)) = \ell\mathbb{Z}/n\mathbb{Z}$ ist zyklisch (als Bild der zyklischen Gruppe $\ell\mathbb{Z}$) und wird von $\ell + n\mathbb{Z}$ erzeugt.
Aus dem zweiten Noetherschen Isomorphiesatz 1.7 folgt

$$|(\mathbb{Z}/n\mathbb{Z})/(\ell\mathbb{Z}/n\mathbb{Z})| = |\mathbb{Z}/\ell\mathbb{Z}|\,.$$

Das ergibt $\frac{n}{|H|} = \ell$ nach der Abzählformel (AGLA 10.10). □

16.7 Der Frobenius-Homomorphismus

Satz. *Sei K ein endlicher Körper und $|K| = q$ die Anzahl der Elemente von K. Dann ist jede endliche Erweiterung L von K zyklisch, und die Galoisgruppe $G(L/K)$ wird vom* Frobenius-Homomorphismus

$$\sigma_q \colon L \longrightarrow L,\ x \longmapsto x^q\,,$$

erzeugt.

Beweis. Nach 14.3 ist $q = p^n$, wobei die Primzahl p die Charakteristik von K und $n \in \mathbb{N}$ der Grad von K über dem Primkörper ist. Es folgt

$$\sigma_q(x+y) = (x+y)^q = x^q + y^q = \sigma_q(x) + \sigma_q(y)$$

Da σ_q auch multiplikativ ist, und $\sigma_q(1) = 1$ ist, ist σ_q nach 6.9 ein injektiver Homomorphismus und daher auch surjektiv, da $|L| < \infty$. Sei G die von σ_q erzeugte Untergruppe von $\mathrm{Aut}(L)$.
$\Longrightarrow L^G = K$, da K nach 14.4 genau aus den Elementen $a \in L$ mit $a^q = a$ besteht.
$\underset{15.2}{\Longrightarrow}$ L ist separabel über K und normal über K.
$\underset{15.8}{\Longrightarrow}$ L ist galoissch über K.
$\Longrightarrow |G| \underset{15.4}{=} [L:K] \underset{15.7}{=} |G(L/K)| \Longrightarrow G = G(L/K)$. □

16.8 Vollkommene Körper

Definition. Ein Körper K heißt *vollkommen* oder *perfekt*, wenn jedes irreduzible Polynom $f \in K[X]$ separabel ist.

Bemerkung. Ist K vollkommen, so ist jede algebraische Körpererweiterung von K separabel.

Beispiel. 1) Körper der Charakteristik 0 sind vollkommen (vgl. 12.9).

2) Endliche Körper sind vollkommen.

Beweis. Sei K ein endlicher Körper, $f \in K[X]$ irreduzibel und L Zerfällungskörper von f.
$\underset{16.7}{\Longrightarrow}$ L galoissch über K, da auch L endlich
$\underset{15.8}{\Longrightarrow}$ L ist separabel über $K \Longrightarrow f$ ist separabel. □

16.9 Bemerkung über Zwischenkörper

(a) Jede endliche separable Körpererweiterung eines Körpers K besitzt nur endlich viele Zwischenkörper (Ist $\mathrm{char}(K) = 0$, so ist die Voraussetzung der Separabilität immer erfüllt).

Beweis. Nach 15.9 läßt sich jede endliche separable Körpererweiterung in eine Galoiserweiterung einbetten. □

(b) Ist L eine Galoiserweiterung von K, so gilt:
In der (inklusionsumkehrenden) Galoiskorrespondenz 16.1 entspricht der Körper L der Gruppe $G(L/L) = \{\mathrm{id}\}$ und der Körper K der Galoisgruppe $G(L/K)$.

16.10 Übungsaufgaben 51 – 53

Aufgabe 51. Sei $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

(a) Man zeige, dass L galoissch über $\mathbb{Q}$ ist.

(b) Man bestimme die Galoisgruppe $G(L/\mathbb{Q})$.

(c) Man bestimme alle Zwischenkörper.

(d) Man bestimme das Minimalpolynom m_x in $\mathbb{Q}[X]$ von $x := \sqrt{2} + \sqrt{3}$.

Aufgabe 52. Man bestimme jeweils den Zerfällungskörper des Polynoms

(a) $X^3 - 1$

(b) $X^4 - 5X^2 + 6$

(c) $X^6 - 8$

sowie jeweils seinen Grad über $\mathbb{Q}$.

Aufgabe 53. Sei K ein Körper der Charakteristik $p > 0$. Man zeige, dass K genau dann vollkommen ist, wenn der *Frobenius-Homomorphismus* $K \longrightarrow K,\ x \longmapsto x^p$, surjektiv ist.

Teil V
Anwendungen und Ergänzungen

17 Kreisteilungskörper

Sei K ein Körper, und sei $n \in \mathbb{N}$.

17.1 Einheitswurzeln

Definition. Sei L ein Zerfällungskörper des Polynoms $X^n - 1 \in K[X]$. Die Nullstellen dieses Polynoms heißen *n-te Einheitswurzeln über K* und L heißt *n-ter Einheitswurzelkörper über K*. Falls $K = \mathbb{Q}$ ist, heißt L auch *n-ter Kreisteilungskörper*.

Satz. *1) Die n-ten Einheitswurzeln über K bilden eine Untergruppe U_n von L^*.*

2) Gilt $\operatorname{char}(K) \nmid n$*, so ist U_n zyklisch von der Ordnung n.*

3) Ist $\operatorname{char}(K) = p > 0$ *und $p \mid n$, so ist $n = p^r m$ mit $r > 0$ und $p \nmid m$, und es gilt $U_n = U_m$.*
(Bei der Betrachtung der Gruppe U_n kann man sich also auf den Fall $\operatorname{char}(K) \nmid n$ beschränken.)

Beweis. 1) Ist offensichtlich.

2) U_n ist zyklisch nach 14.2. Gilt $\operatorname{char}(K) \nmid n$, so haben $X^n - 1$ und $(X^n - 1)' = nX^{n-1}$ keine gemeinsamen Nullstellen. Daher sind die n-ten Einheitswurzeln nach Satz 12.9 alle verschieden, und es folgt $|U_n| = n$.

3) Das Polynom $X^m - 1$ hat, wie in 2) gezeigt, keine mehrfachen Nullstellen. Es ist $X^n - 1 = (X^m - 1)^{p^r}$, da $\operatorname{char}(K) = p$. Die Nullstellen von $X^n - 1$ stimmen also mit den Nullstellen von $X^m - 1$ überein. Es folgt $U_n = U_m$.

□

17.2 Die Eulersche φ-Funktion

Definition. Für $n \in \mathbb{N}$ sei $\varphi(n)$ die Anzahl der zu n teilerfremden Zahlen aus $\{1, \ldots, n\}$. Die Funktion

$$\varphi\colon \mathbb{N} \longrightarrow \mathbb{N} \cup \{0\},\ n \longmapsto \varphi(n)$$

heißt *Eulersche φ-Funktion.*

Satz. *(1) Es ist $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$, denn für $m, n \in \mathbb{N}$ gilt*

$$\boxed{m + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^*} \quad \Longleftrightarrow \quad \boxed{\mathrm{ggT}(m,n) = 1}$$

(2) Seien $m, n \in \mathbb{N}$ und $\mathrm{ggT}(m,n) = 1 \Longrightarrow \varphi(mn) = \varphi(n)\varphi(m)$.

(3) Für jede Primzahl p und $r \in \mathbb{N}$ ist $\varphi(p^r) = p^{r-1}(p-1)$.

(4) Ist $n > 1$ und $n = p_1^{r_1} \cdot \cdots \cdot p_k^{r_k}$ mit $r_1, \ldots, r_k \in \mathbb{N}$ und paarweise verschiedenen Primzahlen $p_1, \ldots, p_k$, so ist

$$\varphi(n) = \prod_{i=1}^{k} p_i^{r_i - 1}(p_i - 1)$$

Beweis. (1) Nach Satz 6.8 ist $\mathbb{Z}$ ein Hauptidealring und nach Satz 8.4 wird das Ideal $m\mathbb{Z} + n\mathbb{Z}$ in $\mathbb{Z}$ von $d := \mathrm{ggT}(m,n)$ erzeugt. Es folgt
$d = 1 \underset{8.4}{\Longleftrightarrow} m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z} \underset{\text{Aufgabe 25}}{\Longleftrightarrow} (m + n\mathbb{Z}) \in (\mathbb{Z}/n\mathbb{Z})^*$

(2) Sei $\mathrm{ggT}(m,n) = 1$. Zerlege m und n in ein Produkt von Primzahlpotenzen, dann folgt aus dem Chinesischen Restsatz 8.12 und Aufgabe 24, daß

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

gilt. Dies induziert einen Isomorphismus der Einheitsgruppen

$$(\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^* \simeq (\mathbb{Z}/mn\mathbb{Z})^*\,.$$

Mit Hilfe von (1) folgt hieraus (2).

(3) Die p^{r-1} Zahlen $p, 2p, \ldots, p^{r-1}p$ sind genau die Zahlen aus $\{1, \ldots, p^r\}$, die nicht teilerfremd zu p^r sind. Es folgt $\varphi(p^r) = p^r - p^{r-1}$.

(4) folgt aus ((3)) und ((2)).

□

17.3 Primitive n-te Einheitswurzeln

Definition. Es gelte $\mathrm{char}(K) \nmid n$. Dann heißt jedes erzeugende Element der Gruppe U_n der n-ten Einheitswurzeln in L eine *primitive n-te Einheitswurzel* (vgl. 17.1).
Sei L der n-te Einheitswurzelkörper über K, wobei $\mathrm{char}(K) \nmid n$ gelte. Die Gruppe U_n der n-ten Einheitswurzeln in L^* ist zyklisch von der Ordnung n (vgl. 17.1), und jedes erzeugende Element heißt *primitive n-te Einheitswurzel.*

Bemerkung. Sei ζ_n eine primitive n-te Einheitswurzel in L. Dann gelten:

(1) $L = K(\zeta_n)$.

(2) Für $k \in \mathbb{N}$ gilt:

$$\boxed{\zeta_n^k \text{ primitiv}} \underset{\text{Def.}}{\Longleftrightarrow} \boxed{\mathrm{ord}(\zeta_n^k) = n} \underset{14.1}{\Longleftrightarrow} \boxed{\mathrm{ggT}(k,n) = 1}$$

(3) Es gibt genau $\varphi(n)$ primitive n-te Einheitswurzeln in L (Dies folgt aus (2) und der Definition von $\varphi(n)$ in 17.2).

Beispiel. Ist $n = p$ eine Primzahl ($\neq \mathrm{char}(K)$), so ist jede p-te Einheitswurzel $\neq 1$ in L primitiv (vgl. 17.2.3).

17.4 Der n-te Einheitswurzelkörper ist abelsch

Satz. *Es gelte* $\mathrm{char}(K) \nmid n$. *Dann ist der n-te Einheitswurzelkörper galoissch über K, und die Galoisgruppe $G(L/K)$ ist isomorph zu einer Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^*$, also insbesondere abelsch.*

Beweis. Da $|U_n| = n$ nach 17.1
$\Longrightarrow X^n - 1 \in K[X]$ ist separabel.
$\underset{15.8}{\Longrightarrow}$ L ist galoissch über K.
Sei ζ eine primitive n-te Einheitswurzel in L. Dann ist auch $\sigma(\zeta)$ eine solche für $\sigma \in G(L/K)$ (denn mit ζ ist auch $\sigma(\zeta)$ Nullstelle von $X^n - 1$ nach Satz 11.4, und die Ordnung von ζ bleibt unter σ erhalten).
$\underset{17.3}{\Longrightarrow}$ $\boxed{\sigma(\zeta) = \zeta^{k_\sigma} \text{ mit } \mathrm{ggT}(k,n) = 1}$ für jedes $\sigma \in G(L/K)$
$\underset{17.2}{\Longrightarrow}$ Es gibt eine Abbildung $\psi\colon G(L/K) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*$, $\sigma \longmapsto k_\sigma + n\mathbb{Z}$
Man kann dabei $k_\sigma \in \{1, \ldots, n\}$ wählen. Es ist ψ ein Homomorphismus, denn für $\sigma, \tau \in G(L/K)$ ist $(\tau \circ \sigma)(\zeta) = \tau(\zeta^{k_\sigma}) = \tau(\zeta)^{k_\sigma} = \zeta^{k_\tau k_\sigma}$, also $\psi(\tau \circ \sigma) = k_\tau k_\sigma + n\mathbb{Z} \underset{7.2}{=} (k_\tau + n\mathbb{Z})(k_\sigma + n\mathbb{Z}) = \psi(\tau)\psi(\sigma)$.
Es ist ψ injektiv, denn ist $k_\sigma = 1$, so ist $\sigma = \mathrm{id}$, da $L = K(\zeta)$ und $\sigma(a) = a \;\forall\, a \in K$ gilt. $\square$

17.5 Das n-te Kreisteilungspolynom

Definition. Es gelte $\mathrm{char}(K) \nmid n$. Sei L der n-te Einheitswurzelkörper über K, und seien $\zeta^{(1)}, \dots, \zeta^{(\varphi(n))}$ die primitiven n-ten Einheitswurzeln in L. Das *n-te Kreisteilungspolynom* ist definiert als

$$\boxed{\Phi_n := (X - \zeta^{(1)}) \cdot \ldots \cdot (X - \zeta^{(m)})} \quad \text{mit } m := \varphi(n)\,.$$

Satz. *(1)* $X^n - 1 = \prod_{d \mid n} \Phi_d\,.$

(2) $\Phi_n \in K[X]$ *und* $\Phi_n \in \mathbb{Z}[X]$*, falls* $K = \mathbb{Q}\,.$

Beweis. (1) Nach 17.1 ist $|U_n| = n$, also $X^n - 1 = \prod_{\zeta \in U_n} (X - \zeta)$. Ist $\zeta \in U_n$ und $\mathrm{ord}(\zeta) = d \Longrightarrow d \mid n$, und ζ ist eine primitive d-te Einheitswurzel.

(2) Es ist $\Phi_1 = X - 1$. Sei $n > 1$, und sei die Behauptung für alle echten Teiler von n schon bewiesen.
$\Longrightarrow X^n - 1 = \Phi_n \cdot g$, wobei g ein normiertes Polynom aus $K[X]$ (bzw. $\mathbb{Z}[X]$, falls $K = \mathbb{Q}$)
$\underset{(1)}{\Longrightarrow} (X^n - 1) : g = \Phi_n \in K[X]$ (bzw. $\mathbb{Z}[X]$).

□

Bemerkung. Mit Hilfe von (1) kann man Φ_n berechnen:

$$\begin{aligned}
\Phi_1 &= X - 1\,,\\
\Phi_2 &= \frac{X^2 - 1}{X - 1} = X + 1\,,\\
\Phi_3 &\underset{9.13}{=} X^2 + X + 1\,,\\
\Phi_4 &= \frac{X^4 - 1}{\Phi_1 \cdot \Phi_2} = X^2 + 1\,,\\
\Phi_5 &\underset{9.12}{=} X^4 + X^3 + X^2 + X + 1\,, \ldots
\end{aligned}$$

Für große n treten auch Koeffizienten $\neq \pm 1$ auf.

17.6 Die Galoisgruppe des n-ten Kreisteilungskörpers

Satz. *Ist* $K = \mathbb{Q}$*, so gelten:*

(1) Das n-te Kreisteilungspolynom ist irreduzibel in $\mathbb{Q}[X]$.

(2) *Der n-te Kreisteilungskörper $L = \mathbb{Q}(\zeta_n)$ ist abelsch, und es ist $G(L/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$.*

Beweis. (1) Es ist $\Phi_n \in \mathbb{Z}[X]$ normiert (vgl. 17.5). Sei $\pi \in \mathbb{Z}[X]$ ein normierter irreduzibler Teiler von Φ_n, und sei ζ eine Nullstelle von π. Dann ist ζ auch Nullstelle von Φ_n und also eine primitive n-te Einheitswurzel in L. Wir zeigen:

$$(*) \qquad \pi(\zeta^k) = 0 \text{ für jedes } k \in \{1, \ldots, n\} \text{ mit } \operatorname{ggT}(k, n) = 1$$

Aus $(*)$ folgt $\operatorname{grad}(\pi) \underset{17.2}{=} \varphi(n) \underset{17.3}{=} \operatorname{grad}(\Phi_n)$, und also $\Phi_n = \pi$. Hieraus folgt, daß Φ_n irreduzibel in $\mathbb{Z}[X]$ ist und also nach 9.3(c) auch in $\mathbb{Q}[X]$. Zum Nachweis von $(*)$ genügt es, $\pi(\zeta)^p = 0$ für jeden Primteiler p von k zu zeigen, wie man mit Induktion einsieht.
Sei also p eine Primzahl mit $p \mid k$.
$\Longrightarrow p \nmid n$, da $\operatorname{ggT}(k, n) = 1$.
Angenommen, $\pi(\zeta^p) \neq 0$. Da $\pi \mid \Phi_n$ und $\Phi_n \mid (X^n - 1)$, folgt

$$\boxed{X^n - 1 = \pi g \text{ mit einem normierten } g \in \mathbb{Z}[X]}$$

Es folgt $g(\zeta^p) = 0$, da $\pi(\zeta^p) \neq 0$
$\Longrightarrow$ $g(X^p)$ hat ζ als Nullstelle, wobei $g = \sum a_i X^i$ mit $a_i \in \mathbb{Z}$ und $g(X^p) = \sum a_i (X^p)^i$
$\underset{11.9}{\Longrightarrow}$ $\pi \mid g(X^p)$ (da π irreduzibel in $\mathbb{Q}[X]$ nach 9.3(c) und also $\pi = m_\zeta$ gilt)
$\Longrightarrow g(X^p) = \pi \cdot h$ mit $h \in \mathbb{Z}[X]$
$\Longrightarrow \overline{g}(X^p) = \overline{\pi} \cdot \overline{h}$ in $\mathbb{F}_p[X]$, wobei $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ und $\mathbb{Z}[X] \longrightarrow \mathbb{F}_p[X],\ f \longmapsto \overline{f}$, gilt.
$\Longrightarrow \overline{g}^p = \overline{\pi}\overline{h}$, (da $\overline{g}^p = \left(\sum \overline{a_i} X^i\right)^p = \sum \overline{a_i}^p X^{ip} = \overline{g}(X^p)$, denn $\overline{a_i}^p = \overline{a_i}$ nach 14.5)
$\Longrightarrow$ Jede Nullstelle von $\overline{\pi}$ ist Nullstelle von $\overline{g}^p$ und also von $\overline{g}$ (in einem Zerfällungskörper von $\overline{g}$)
$\Longrightarrow X^n - \overline{1} = \overline{\pi}\overline{g}$ hat eine doppelte Nullstelle im Widerspruch zu 17.1, da $\operatorname{char}(\mathbb{F}_p) = p \nmid n$.

(2) Es gilt

$$|G(L/\mathbb{Q})| \underset{15.7}{=} [L : \mathbb{Q}] \underset{11.10}{=} \operatorname{grad}(\Phi_n) \underset{17.2}{=} |(\mathbb{Z}/n\mathbb{Z})^*|$$

Da $G(L/\mathbb{Q})$ isomorph ist zu einer Untergruppe von $(\mathbb{Z}/n\mathbb{Z})^*$, folgt (2). $\square$

17.7 Endliche Schiefkörper sind kommutativ

Satz (Wedderburn 1905). *Jeder endliche Schiefkörper ist kommutativ.*

Beweis. von Witt (1931) mit Hilfe von 17.5 und der Klassengleichung 3.1 (vgl. Kopie des Originals). □

17.8 Kroneckers Jugendtraum

Jede abelsche Körpererweiterung von $\mathbb{Q}$ ist in einem Kreisteilungskörper $\mathbb{Q}(\zeta_n)$ mit passendem $n \in \mathbb{N}$ enthalten.
Dies ist der Satz von *Kronecker-Weber* aus der algebraischen Zahlentheorie (1853 von Kronecker vermutet und 1886 von H. Weber bewiesen).

17.9 Übungsaufgabe 54

Aufgabe 54. Für $n \geq 3$ sei $\zeta = \zeta_n$ eine primitive n-te Einheitswurzel. Man zeige:

$$\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1}) = 2\,.$$

18 Auflösbarkeit von Gleichungen durch Radikale

Sei K ein Körper.

18.1 Die Galoisgruppe eines Polynoms

Definition. Sei $f \in K[X]$ ein separables Polynom. Dann ist der Zerfällungskörper L von f galoissch über K nach 15.8. Man nennt dann die Galoisgruppe $G(L/K)$ die *Galoisgruppe des Polynoms* f oder auch die *Galoisgruppe der Gleichung* $f = 0$.

Bemerkung. Ist f irreduzibel, so operiert die Galoisgruppe $G(f)$ transitiv auf der Menge der Nullstellen von f (d.h. zu je zwei Nullstellen x, y von f gibt es ein $\sigma \in G(f)$ mit $\sigma(x) = y$).

Beweis. Nach 13.2 gibt es einen K-Isomorphismus $\psi\colon K(x) \longrightarrow K(y)$ mit $\psi(x) = y$, und dieser hat nach 13.3 eine Forsetzung zu einem $\sigma \in G(f)$. $\square$

Beispiel. $f = X^3 - 2 \in \mathbb{Q}[X] \Longrightarrow L = \mathbb{Q}(\sqrt[3]{2}, \zeta) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$, wobei ζ Nullstelle von X^2+X+1, also $\zeta = -\frac{1}{2}+\frac{1}{2}\cdot\sqrt{-3} = e^{\frac{2\pi i}{3}}$ (und $\zeta^2 = -\frac{1}{2}-\frac{1}{2}\cdot\sqrt{3}$) $\Longrightarrow G(f) := G(L/\mathbb{Q}) \simeq S_3$ nach 16.2, 16.4.

18.2 Definition der Auflösbarkeit durch Radikale

Definition. 1) Eine Körpererweiterung L von K heißt *Radikalerweiterung*, wenn es einen Körperturm

$$K = K_1 \subset K_2 \subset \cdots \subset K_n = L$$

gibt, so daß $K_{i+1} = K_i(x_i)$ und x_i Nullstelle eines Polynoms $X^{n_i} - a_i \in K_i[X]$ ist (d.h. K_{i+1} entsteht aus K_i durch Adjunktion einer n_i-ten Wurzel eines Elementes aus K_i). Man nennt x_i dann ein *Radikal.*

2) Sei $f \in K[X]$. Dann heißt die Gleichung $f = 0$ *durch Radikale auflösbar*, wenn es eine Radikalerweiterung von K gibt, die eine Nullstelle von f enthält.

18.3 Die Galoisgruppe einer reinen Gleichung

Definition. Es gelte $\operatorname{char}(K) \nmid n$. Dann nennt man eine Gleichung der Form $\boxed{X^n - a = 0}$ mit $a \in K^*$ eine *reine Gleichung.*

Satz. *Die n-ten Einheitswurzeln seien in K enthalten. Dann gilt:*

(i) Die Galoisgruppe des Polynoms $f = X^n - a$ mit $a \in K^*$ ist zyklisch.

(ii) Zu jeder zyklischen Körpererweiterung L von K vom Grad n gibt es ein $x \in L$ mit $L = K(x)$ und $x^n \in K$.

Beweis. (i) Sei L der Zerfällungskörper von f und ζ eine primitive n-te Einheitswurzel in K. Sei $x \in L$ Nullstelle von f, so ist $\{x, \zeta x, \dots, \zeta^{n-1}x\}$ die Menge aller Nullstellen von f. Also ist $L = K(x)$.
Für jedes $\sigma \in G(L/K)$ gilt $\sigma(x) = \zeta^{k_\sigma}x$, und hierdurch ist σ eindeutig bestimmt. Daher gibt es eine injektive Abbildung

$$\psi\colon G(L/K) \longrightarrow \mathbb{Z}/n\mathbb{Z},\ \sigma \longmapsto k_\sigma + n\mathbb{Z}\,.$$

Für $\sigma, \tau \in G(L/K)$ gilt $(\sigma \circ \tau)(x) = \sigma(\zeta^{k_\tau}x) = \zeta^{k_\tau}\sigma(x) = \zeta^{k_\tau + k_\sigma}x$ und also $\psi(\sigma \circ \tau) = k_\sigma + k_\tau + n\mathbb{Z} \underset{7.2}{=} k_\sigma + n\mathbb{Z} + k_\tau + n\mathbb{Z} = \psi(\sigma) + \psi(\tau)$.
Da die additive Gruppe $\mathbb{Z}/n\mathbb{Z}$ zyklisch ist, ist auch die Untergruppe $\psi(G(L/K)$ von $\mathbb{Z}/n\mathbb{Z}$ zyklisch (vgl. 16.6). Da ψ injektiv ist, folgt (i).

(ii) Sei σ ein erzeugendes Element von $G(L/K)$, und sei ζ eine primitive n-te Einheitswurzel in K. Die Automorphismen $\mathrm{id}, \sigma, \dots, \sigma^{n-1}$ sind linear unabhängig über L nach 18.4 unten. Es gibt also ein $y \in L$, so daß die *Lagrangesche Resolvente* $x := y + \zeta\sigma(y) + \zeta^2\sigma^2(y) + \cdots + \zeta^{n-1}\sigma^{n-1}(y) \neq 0$ ist. Es folgt

$$(*) \qquad \sigma(x) = \sigma(y) + \zeta\sigma^2(y) + \zeta^2\sigma^3(y) + \cdots + \zeta^{n-2}\sigma^{n-1}(y) + \zeta^{n-1}y$$

und daher $\sigma(x^n) = \sigma(x)^n \underset{(*)}{=} x^n\ \forall\, \sigma \in G(L/K)$ (da $G(L/K)$ zyklisch)
Es folgt $x^n \in L^{G(L/K)} \underset{15.8}{=} K$.
Da $\sigma^k(x) \underset{(*)}{=} \zeta^{-k}x$ gilt für $k = 0, 1, \dots, n-1$, folgt $[K(X) : K] \leq n$
$\underset{16.6}{\Longrightarrow} L = K(x)$.

□

18.4 Lineare Unabhängigkeit von Charakteren

Sei L ein Körper und G eine (multiplikative) Gruppe.

Definition. Ein *Charakter von G in L* ist ein Gruppenhomomorphismus $G \longrightarrow L^*$.

Beispiel. Jedes $\sigma \in \mathrm{Aut}(L)$ definiert einen Charakter $\sigma\colon L^* \longrightarrow L^*$.

Satz. *Seien $\sigma_1, \dots, \sigma_n$ paarweise verschiedene Charaktere von G in L, und seien $\lambda_1, \dots, \lambda_n \in L$ gegeben mit*

$$(*) \qquad \lambda_1\sigma_1(x) + \cdots + \lambda_n\sigma_n(x) = 0 \;\forall\, x \in G\,.$$

Dann folgt $\lambda_1 = \cdots = \lambda_n = 0$.

Beweis. durch Induktion nach n.
$n = 1$: Ist $\lambda_1\sigma_1(x) = 0 \;\forall\, x \in G$, so ist $\lambda_1 = 0$, da $\sigma_1(x) \in L^*$.
Sei $n > 1$, und die Behauptung sei für $n-1$ Charaktere bewiesen. Wähle $y \in G$ mit $\sigma_1(y) \neq \sigma_n(y)$ und multipliziere $(*)$ mit $\sigma_n(y)$. Dann folgt

$$\lambda_1\sigma_n(y)\sigma_1(x) + \cdots + \lambda_n\sigma_n(y)\sigma_n(x) = 0$$

Setze in $(*)$ statt x das Element yx ein. Dann folgt

$$\lambda_1\sigma_1(y)\sigma_1(x) + \cdots + \lambda_n\sigma_n(y)\sigma_n(x) = 0$$

Subtraktion ergibt

$$\lambda_1(\underbrace{\sigma_n(y) - \sigma_1(y)}_{\neq 0 \text{ nach Wahl von } y})\sigma_1(x) + \cdots + \lambda_{n-1}(\sigma_n(y) - \sigma_{n-1}(y))\sigma_{n-1}(x) = 0 \;\forall\, x \in G$$

Also folgt $\lambda_1 = 0$ nach Induktionsvoraussetzung. Wende nun die Induktionsvoraussetzung auf $(*)$ an.
$\Longrightarrow \lambda_2 = \cdots = \lambda_n = 0$. □

18.5 Das Kompositum von Zwischenkörpern

Sei L eine Körpererweiterung eines Körpers K.

Definition. Das *Kompositum* Z_1Z_2 zweier Zwischenkörper Z_1, Z_2 ist definiert als der von der Vereinigung $Z_1 \cup Z_2$ erzeugte Teilkörper von L.

Lemma. *Für Zwischenkörper Z_1, Z_2, Z und $Z_1 \subset Z_2$ gilt:*

$$\boxed{Z_2 \text{ galoissch über } Z_1} \quad \Longrightarrow \quad \boxed{ZZ_2 \text{ galoissch über } ZZ_1}$$

Die Galoisgruppe $G(ZZ_2/ZZ_1)$ ist dann isomorph zu einer Untergruppe von $G(Z_2/Z_1)$.

Beweis. Nach 15.8 ist Z_2 Zerfällungskörper eines separablen Polynoms $f \in Z_1[X]$. Sei M die Menge der Nullstellen von f.
$\Longrightarrow Z_2 = Z_1(M) \Longrightarrow ZZ_2 = ZZ_1(M)$
$\underset{15.8}{\Longrightarrow} ZZ_2$ ist galoissch über ZZ_1 (da endlich nach 12.3 und normal über ZZ_1 und da f separabel über ZZ_1)
Der Homomorphismus $G(ZZ_2/ZZ_1) \longrightarrow G(Z_2/Z_1)$, $\sigma \longmapsto \sigma|_{Z_2}$, ist injektiv, da σ durch die Wirkung auf M eindeutig bestimmt ist (vgl. 15.5). □

18.6 Gleichungen mit auflösbarer Galoisgruppe

Satz. *Sei K ein Körper, $f \in K[X]$ irreduzibel und separabel. Die Galoisgruppe $G(f)$ sei auflösbar, und es gelte* $\mathrm{char}(K) \nmid |G(f)|$. *Dann ist die Gleichung $f = 0$ durch Radikale lösbar, und alle Lösungen von f sind Radikale.*

Beweis. Sei L Zerfällungskörper von f, also $G(f) \underset{18.1}{=} G(L/K)$. Da $G(f)$ auflösbar ist, gibt es nach Satz 4.4 eine Kette von Untergruppen

$$G(f) = U_k \subset U_{k-1} \subset \cdots \subset U_1 \subset U_0 = \{\mathrm{id}\},$$

wobei $U_{i-1} \triangleleft U_i$ und U_i/U_{i-1} (zyklisch) von Primzahlordnung p_i ist für $i = 0, \ldots, k$. Nach dem Hauptsatz 16.1 und 16.3 gibt es hierzu einen Körperturm

$$K = Z_0 \subset Z_1 \subset \cdots \subset Z_k = L,$$

wobei Z_i zyklisch vom Grad p_i ist für $i = 1, \ldots, k$.
Es folgt $n := [L : K] = p_1 \cdot \ldots \cdot p_k$.
Da $\mathrm{char}(K) \nmid n$ nach Voraussetzung gilt
$\Longrightarrow \mathrm{char}(K) \nmid p_i \ \forall\, i = 1, \ldots, k$
$\Longrightarrow$ Der n-te Einheitswurzelkörper K' von K enthält die p_i-ten Einheitswurzeln. Da in dem Körperturm

$$K' = K'Z_0 \subset K'Z_1 \subset \cdots \subset K'Z_k = K'L =: L'$$

die Erweiterungen $K'Z_i$ alle zyklisch über $K'Z_{i-1}$ sind nach 18.5, gibt es Elemente $x_i \in K'Z_i$ und $n_i \in \mathbb{N}$ mit $x_i^{n_i} \in K'Z_{i-1}$ für $i = 1, \ldots, k$ (nach 18.3(ii)) $\Longrightarrow L'$ ist Radikalerweiterung von K'. Da K' Radikalerweiterung von K ist, ist L' auch eine solche über K. Alle Nullstellen von f liegen in L', sind also Radikale. □

18.7 Durch Radikale auflösbare Gleichungen

Satz. *Sei K ein Körper der Charakteristik 0, und sei $f \in K[X]$ irreduzibel. Die Gleichung $f = 0$ sei durch Radikale auflösbar. Dann ist die Galoisgruppe $G(f)$ auflösbar.*

Beweis. Nach Voraussetzung gibt es eine Radikalerweiterung R von K, in der f eine Nullstelle besitzt. Es gibt also einen Körperturm $K = R_0 \subset R_1 \subset \cdots \subset R_k = R$, wobei $R_{i+1} = R_i(x_i)$ mit $x_i^{n_i} \in R_i$ und $n_i \in \mathbb{N}$ gilt für alle $i = 0, \ldots, k-1$ (vgl. Definition 18.2). Sei $n = n_0 \cdot \ldots \cdot n_{k-1}$, und sei K' der n-te Einheitswurzelkörper über K. Dann ist K' abelsch über K nach 17.4, und man erhält einen Körperturm

$$K \underset{\text{abelsch}}{\subset} K' = KR_0 \underset{\text{zyklisch}}{\subset} K'R_1 \subset \cdots \subset K'R_k =: R',$$

in dem KR_i zyklisch über $K'R_{i-1}$ ist $\forall\, i = 1,\dots,k$ nach 18.3(i).
Bette R' gemäß 15.8 in eine Galoiserweiterung N von K ein. Jedes $\sigma \in G(N/K)$ definiert dann einen Körperturm

$$K \underset{\text{abelsch}}{\subset} \sigma(K'R_0) \underset{\text{zyklisch}}{\subset} \sigma(K'R_1) \underset{\text{zyklisch}}{\subset} \dots \underset{\text{zyklisch}}{\subset} \sigma(K'R_k)\,.$$

Sei Z_i das Kompositum aller $\sigma(K'R_i)$ mit $\sigma \in G(N/K)$ für $i = 0,\dots,k$. Dann ist Z_0 abelsch über K, und Z_i ist zyklisch über Z_{i-1} für alle $i = 1,\dots,k$ nach 18.5 (und 16.9). Man erhält dann einen Körperturm

$$K \underset{\text{abelsch}}{\subset} Z_0 \underset{\text{zyklisch}}{\subset} Z_1 \underset{\text{abelsch}}{\subset} \dots \underset{\text{abelsch}}{\subset} Z_k =: L\,, (\subset N)$$

wobei zusätzlich noch L galoissch über K ist nach 16.3 "(b) $\Longrightarrow$ (a)".
Hierzu gehört nach dem Hauptsatz 16.1 und nach 16.3 ein Gruppenturm

$$G(L/K) \rhd G(L/Z_0) \rhd G(L/Z_1) \rhd \cdots \rhd G(L/Z_k) = \{\mathrm{id}\}\,.$$

Dies sind jeweils Normalteiler nach 16.3. Die Faktorgruppen sind alle abelsch (denn $G(L/Z_{i-1})/G(L/Z_i) \underset{16.3}{\simeq} G(Z_i/Z_{i-1})$ ist zyklisch und
$G(L/K)/G(L/Z_0) \underset{16.3}{\simeq} G(Z_0/K)$ ist abelsch (vgl. Definition 16.5)).
Also ist $G(L/K)$ auflösbar nach Definition 4.1. Es gilt $R \supset L \Longrightarrow L$ enthält eine Nullstelle von f.
$\underset{13.5}{\Longrightarrow}$ L enthält einen Zerfällungskörper Z von f (da L normal über K und f irreduzibel).
$\underset{16.3}{\Longrightarrow}$ $G(L/Z) \lhd G(L/K)$ (da Z galoissch über K, vgl. 15.8 und 16.8) und $G(Z/K) \simeq G(L/K)/G(L/Z)$
$\underset{4.3}{\Longrightarrow}$ $G(f) \underset{\text{Def}}{=} G(Z/K)$ ist auflösbar, da $G(L/K)$ auflösbar. □

18.8 Nicht auflösbare Gleichungen vom Grad p

Satz. *Sei p eine Primzahl, und sei $f \in \mathbb{Q}[X]$ ein irreduzibles Polynom vom Grad p, das in $\mathbb{C}$ genau zwei nicht-reelle Nullstellen besitze. Dann ist die Galoisgruppe $G(f)$ isomorph zur symmetrischen Gruppe S_p, und die Gleichung $f = 0$ ist nicht durch Radikale auflösbar, falls $p \geq 5$.*

Beweis. Sei L Zerfällungskörper von f. Dann ist die Galoisgruppe $G(f) := G(L/K)$ isomorph zu einer Untergruppe G von S_p nach 15.5.
Ist x eine Nullstelle von f
$\underset{11.10}{\Longrightarrow}$ $[\mathbb{Q}(x) : \mathbb{Q}] = p$, da f irreduzibel
$\Longrightarrow p \mid [L : \mathbb{Q}] \underset{15.7}{=} |G|$

$\underset{2.4}{\Longrightarrow}$ G enthält ein Element σ der Ordnung p (Satz von Cauchy)
$\Longrightarrow$ σ ist ein p-Zyklus (überlegt man sich mit Hilfe von 5.2, wonach σ ein Produkt von paarweise vertauschbaren Zyklen ist).
Seien $x_1, \dots, x_p$ die Nullstellen von f (diese sind nach Korollar 12.9 alle verschieden), und seien x_1, x_2 die beiden Nullstellen aus $\mathbb{C} \setminus \mathbb{R}$. Dann entspricht der komplexen Konjugation die Transposition $(1, 2)$.
Indem man σ gegebenenfalls durch eine geeignete Potenz ersetzt, kann man $\sigma = (1, \dots, p)$ annehmen. Es folgt
$G \ni \sigma\tau\sigma^{-1} = (\sigma(1), \sigma(2)) = (2, 3)$
$G \ni \sigma(2, 3)\sigma^{-1} = (3, 4)$ usw. (vgl. Aufgabe 18 c).
Für jedes $n \in \{1, \dots, p\}$ ist also $(n, n+1) \in G$.
Da $(1, n)(n, n+1)(1, n) = (1, n+1)$ gilt, folgt $G \ni (1, n)\ \forall\, n = 2, \dots, p$.
$\underset{5.7}{\Longrightarrow}$ $G \simeq S_p$. Da S_p für $p \geq 5$ nicht auflösbar ist nach 5.6, ist f nicht durch Radikale auflösbar für $p \geq 5$. □

18.9 Beispiel

Sei $f = X^5 - 4X + 2 \in \mathbb{Q}[X]$. Dann ist f irreduzibel nach Eisenstein mit $p = 2$ und f hat genau drei reelle Nullstellen, denn $f' = 5X^4 - 4$ hat genau zwei Nullstellen $\pm\sqrt[4]{\frac{4}{5}}$ in $\mathbb{R}$. Also hat f höchstens drei Nullstellen in $\mathbb{R}$ nach dem Satz von Rolle.
Es ist $f(-2) < 0, f(0) > 0, f(1) < 0, f(2) > 0$. Also hat f mindestens 3 reelle Nullstellen nach dem Zwischenwertsatz. Nach 18.8 ist $f = X^5 - 4X + 2 \in \mathbb{Q}[X]$ nicht durch Radikale auflösbar.

18.10 Klausur

Aufgabe 1. Man zeige, dass es bis auf Isomorphie genau eine Gruppe der Ordnung 1295 gibt.

Aufgabe 2. Man zeige, dass jede Gruppe der Ordnung 441 auflösbar ist.

Aufgabe 3. Man bestimme die Gruppe $G := (\mathbb{Z}/8\mathbb{Z})^*$ der Einheiten in dem Ring $\mathbb{Z}/8\mathbb{Z}$ und ermittle, ob G zyklisch ist.

Aufgabe 4. Sei L der Zerfällungskörper des Polynoms $X^4 - 10X^2 + 21 \in \mathbb{Q}[X]$. Man bestimme die Galoisgruppe $G(L/\mathbb{Q})$ und alle Zwischenkörper.

Aufgabe 5. Man bestimme den Grad $[L : \mathbb{Q}]$ und ermittle, ob der Körper L galoissch über $\mathbb{Q}$ ist, in den folgenden Fällen:

(a) $L = \mathbb{Q}(i, \sqrt[3]{5}, \zeta)$,

(b) $L = \mathbb{Q}(i, \sqrt[3]{5})$.

Es ist hierbei $\sqrt[3]{5} \in \mathbb{R}$, $i^2 = -1$ und ζ eine dritte Einheitswurzel $\neq 1$ in $\mathbb{C}$.

Aufgabe 6. (a) Man ermittle, ob das Polynom $X^5 + 55X^4 + 121X + 33$ irreduzibel in $\mathbb{Q}[X]$ ist.

(b) Man zerlege das Polynom $X^4 + 1 \in \mathbb{R}[X]$ in $\mathbb{C}[X]$ in Linearfaktoren. (Gesucht ist eine Zerlegung $X^4 + 1 = (X - x_1)(X - x_2)(X - x_3)(X - x_4)$, bei der die Zahlen x_1, x_2, x_3, x_4 jeweils in der Form $a + bi$ mit $a, b \in \mathbb{R}$ zu schreiben sind.)

19 Symmetrische Funktionen

In diesem Abschnitt kommen Polynomringe $R[Y_1, \dots, Y_n]$ in n Unbestimmten $Y_1, \dots, Y_n$ über einem kommutativen Ring R vor. Wer noch nicht mit solchen Polynomringen vertraut ist, sollte zunächst 21.3 und 21.6 lesen, wo der Polynomring in beliebig vielen Unbestimmten über R eingeführt und seine universelle Eigenschaft bewiesen wird.
Sind $y_1, \dots, y_n$ Elemente aus einer kommutativen Ringerweiterung R' von R, so gibt es einen eindeutig bestimmten Ringhomomorphismus

$$\Phi : R[Y_1, \dots, Y_n] \longrightarrow R'$$

mit $\Phi(Y_i) = y_i$ für alle $i = 1, \dots, n$ und $\Phi(r) = r$ für alle $r \in R$, wie aus 21.6 folgt. Es ist dann $\mathrm{bild}(\Phi)$ ein Unterring von R' und diesen bezeichnen wir mit $R[y_1, \dots, y_n]$.

Sei K ein Körper.

19.1 Rationaler Funktionenkörper

Definition. Der Quotientenkörper $F := K(X_1, \dots, X_n)$ des Polynomrings $K[X_1, \dots, X_n]$ in n Unbestimmten heißt *Körper der rationalen Funktionen in den Unbestimmten* $X_1, \dots, X_n$.

Bemerkung. (1) Es ist $[F : K] = \infty$ (da schon die Potenzen $X_1^i \in \mathbb{N} \cup \{0\}$ linear unabhängig sind).

(2) Die Galoisgruppe $G(F/K)$ besitzt eine zur symmetrischen Gruppe S_n isomorphe Untergruppe S_n^*, denn jede Permutation $\pi \in S_n$ induziert einen Isomorphismus

$$\begin{aligned} \pi^*\colon K[X_1, \dots, X_n] &\longrightarrow K[X_1, \dots, X_n], \\ f(X_1, \dots, X_n) &\longmapsto f(X_{\pi(1)}, \dots, X_{\pi(n)}), \end{aligned}$$

und also einen K-Automorphismus

$$\pi^*\colon F \longrightarrow F \text{ mit } \pi^*\left(\frac{g}{h}\right) = \frac{\pi^*(g)}{\pi^*(h)}$$

für $g, h \in K(X_1, \dots, X_n)$, $h \neq 0$. Dies ist wohldefiniert, und $(\pi^*)^{-1}$ wird durch π^{-1} induziert.

(3) Die Elemente des Fixkörpers

$$F^{S_n^*} := \{f \in F \mid \pi^*(f) = f \ \forall \pi \in S_n\}$$

heißen *symmetrische Funktionen* (weil sie festbleiben unter der Wirkung der symmetrischen Gruppe).

Eine symmetrische Funktion $f \in F^{S_n^*} \cap K[X_1, \ldots, X_n]$ nennt man auch ein *symmetrisches Polynom*.

19.2 Elementarsymmetrische Funktionen

Beispiele für symmetrische Funktionen sind die *elementar symmetrischen Funktionen*:

$$s_0 := 1, \quad s_1 := X_1 + \cdots + X_n \text{ (Spur)}$$
$$s_2 := X_1X_2 + \cdots + X_1X_n + X_2X_3 + \cdots + X_2X_n + \cdots + X_{n-1}X_n = \sum_{i<j} X_iX_j$$

...

$$s_m := \sum_{i_1<i_2<\cdots<i_m} X_{i_1} \cdot \ldots \cdot X_{i_m}$$
$$s_n := X_1 \cdot \ldots \cdot X_n \text{ (Norm)}$$

Bemerkung. Sei $g = (X - X_1) \cdot \ldots \cdot (X - X_n) \in K(X_1, \ldots, X_n)[X]$. Dann erhält man durch Ausmultiplizieren und Ordnen nach Potenzen von X, daß

$$\boxed{g = \sum_{i=0}^{n} (-1)^i s_i X^{n-i}}$$

gilt (vgl. Beispiel 15.3 für $n = 4$ mit x_i statt X_i).

19.3 Hauptsatz über symmetrische Funktionen

Satz. *Sei K ein Körper, $F = K(X_1, \ldots, X_n)$ der Körper der rationalen Funktionen in den Unbestimmten $X_1, \ldots, X_n$, und sei Z der Teilkörper der symmetrischen Funktionen. Dann gelten:*

(a) $Z = K(s_1, \ldots, s_n)$, wobei $s_1, \ldots, s_n$ die elementarsymmetrischen Funktionen sind.

(b) F ist Zerfällungskörper des Polynoms

$$g := \sum_{i=0}^{n} (-1)^i s_i X^{n-i} \in Z[X] \,.$$

(c) *F ist galoissch über Z mit Galois-Gruppe $G(F/Z) \simeq S_n$, insbesondere ist $[F : Z] = n!$.*

(d) *Jedes symmetrische Polynom läßt sich als polynomialer Ausdruck in den elementarsymmetrischen Funktionen darstellen, und diese Darstellung ist eindeutig.*

Beweis. Sei $Z_0 = K(s_1, \ldots, s_n)$. Nach 19.2 gelten $Z_0 \subset Z \subset F$ und $F := K(X_1, \ldots, X_n) = Z_0(X_1, \ldots, X_n)$ ist Zerfällungskörper des (separablen) Polynoms $g \in Z_0[X]$. Also ist f galoissch über Z_0 nach 15.8. Nach Definition 19.1(3) ist $Z = F^{S_n^*}$ mit $S_n^* \simeq S_n$. Es folgt $[F : Z_0] \leq n! = |S_n^*| \underset{15.4}{=} [F : Z]$ und daher $[Z : Z_0] \leq 1$ nach Gradsatz. Es folgt $Z = Z_0$ und $G(F/Z) = S_n^*$ (vgl. 15.8).
Damit sind (a), (b) und (c) bewiesen. Wir zeigen nun (d). Da die elementarsymmetrischen Funktionen s_i nach Definition 19.2 Polynome sind, erhalten wir $R := K[s_1, \ldots, s_n]$ als Unterring von $K[X_1, \ldots, X_n]$. Wir haben zu zeigen, dass jedes symmetrische Polynom aus $K[X_1, \ldots, X_n]$ bereits in R liegt. Aus (b) folgt, dass X_1 eine Nullstelle von $g = \sum_{i=0}^{n} (-1)^i s_i X^{n-i}$ ist. Da $f = qg + r$ mit $\mathrm{grad}(r) < n$ oder $r = 0$ für jedes $f \in R[X]$ nach 8.1 gilt, folgt $f(X_1) = r(X_1)$, und also ist $\{1, X_1, \ldots, X_1^{n-1}\}$ ein Erzeugendensystem von $R[X_1]$ als R-Modul. Dividieren wir g durch $X - X_1$, so erhalten wir ein normiertes Polynom vom Grad $n-1$ aus $R[X] \subset R[X_1][X]$ mit der Nullstelle X_2 , und es folgt analog, dass $\{1, X_2, \ldots, X_2^{n-2}\}$ ein Erzeugendensystem von $R[X_1, X_2]$ als $R[X_1]$-Modul ist. Die Produkte $X_1^{m_1} \cdot X_2^{m_2}$ mit $0 \leq m_1 \leq n-1$ und $0 \leq m_2 \leq n-2$ bilden dann ein Erzeugendensystem von $R[X_1, X_2]$ als R-Modul, (dies geht analog wie beim Gradsatz 11.7).
Induktiv erhalten wir also, dass die $n!$ *Monome* $X_1^{m_1} \cdot \ldots \cdot X_n^{m_n}$ mit $0 \leq m_i \leq n - i$ für $i = 1, \ldots, n$ ein Erzeugendensystem von $K[X_1, \ldots, X_n] = R[X_1, \ldots, X_n]$ als R-Modul bilden. Sie bilden dann auch ein Erzeugendensystem von $F = K(X_1, \ldots, X_n)$ als Z-Vektorraum. (Dies kann man so begründen: F besitzt nach (c) eine Basis $\{v_i = \frac{g_i}{h_i} \mid g_i , h_i \in K[X_1, \ldots, X_n], h_i \neq 0,\ i = 1, \ldots, n!\}$ über Z. Es sei h das Produkt der Nenner h_i und $\lambda := \prod_{\pi \in S_n} \pi^*(h)$ die *Norm* von h, dann ist λ im Fixkörper $Z = F^{S_n^*}$ und durch jedes h_i teilbar. Die Elemente λv_i , $i = 1, \ldots, n!$, bilden also eine Basis von F über Z, die in $K[X_1, \ldots, X_n]$ liegt und also in den besagten Monomen ausdrückbar ist.) Aus (c) folgt, dass diese Monome sogar eine Basis von F über $Z \overset{(a)}{=} K(s_1, \ldots, s_n)$ bilden, und daher bilden sie auch eine Basis von $K[X_1, \ldots, X_n]$ als R-Modul. Sei nun f ein symmetrisches Polynom, dann ist $f \in K[X_1, \ldots, X_n] \cap Z$ und also $f \in R$.
Der Nachweis der Eindeutigkeit der Darstellung von f als polynomialer Ausdruck in $s_1, \ldots, s_n$ ergibt sich beim Beweis des nächsten Satzes automatisch,

vgl. die Bemerkung in 19.4. $\square$

19.4 Die allgemeine Gleichung n-ten Grades

Definition. Sei $K(u_1, \dots, u_n)$ der Körper der rationalen Funktionen in den Unbestimmten $u_1, \dots, u_n$ über einem Körper K. Das Polynom

$$f := X^n + u_1 X^{n-1} + \cdots + u_{n-1}X + u_n \in K(u_1, \dots, u_n)[X]$$

heißt *allgemeines Polynom n-ten Grades über K*, und die Gleichung $f = 0$ heißt *allgemeine Gleichung n-ten Grades über K*
(Die Koeffizienten sind hierbei Unbestimmte. Durch *Spezialisieren* $u_i \longrightarrow a_i$ mit $a_i \in K$ für $i = 1, \dots, n$ erhält man daraus ein Polynom aus $K[X]$).

Satz. *Die Galoisgruppe $G(f)$ der allgemeinen Gleichung n-ten Grades ist zur symmetrischen Gruppe S_n isomorph.*

Beweis. Seien $v_1, \dots, v_n$ die Nullstellen von f, und sei L Zerfällungskörper von f über $K(u_1, \dots, u_n)$.
$\underset{19.2}{\Longrightarrow} f = (X - v_1) \cdot \ldots \cdot (X - v_n) = \sum\limits_{i=0}^{n} (-1)^i s_i(v_1, \dots, v_n) X^{n-i}$
$\underset{\text{Koeffizientenvergleich}}{\Longrightarrow} u_i = (-1)^i s_i(v_1, \dots, v_n) \in K(v_1, \dots, v_n)$
$\Longrightarrow L = K(v_1, \dots, v_n)$
Wir zeigen:

$$\begin{array}{ccc} F := K(X_1, \dots, X_n) & \xrightarrow{\sim} & K(v_1, \dots, v_n) = L \\ \Big| \, n! & & \Big| \\ Z := K(s_1, \dots, s_n) & \xrightarrow{\sim} & K(u_1, \dots, u_n) \end{array}$$

Dann folgt $G(f) \simeq G(F/Z) \underset{19.3}{\simeq} S_n$.
Für den Ringhomomorphismus

$$\boxed{\psi\colon K[X_1, \dots, X_n] \longrightarrow L \text{ mit } \psi(X_i) = u_i \ \forall\, i}$$

gilt $\psi((-1)^i s_i) = u_i$. Dann induziert ψ einen Isomorphismus
$\varphi\colon K[s_1, \dots, s_n] \xrightarrow{\sim} \underset{\text{Polynomring}}{K[u_1, \dots, u_n]}$ mit Umkehrabbildung $u_i \longmapsto (-1)^i s_i$.
Hieraus folgt, daß ψ injektiv ist.
Ist $g \neq 0$ im $\operatorname{kern}(\varphi)$, so ist $x := \prod\limits_{\pi \in S_n} \pi^*(g) \neq 0$ und $\sigma(x) = x \ \forall\, \sigma \in S_n^* = G(F/Z)$
Also ist $x \in Z$ nach 15.8, und also $0 \neq x \in \operatorname{kern}(\varphi)$.
Widerspruch, da φ injektiv. Daher induziert ψ einen Isomorphismus $F \simeq L$ und φ einen Isomorphismus $Z \simeq K(u_1, \dots, u_n)$. $\square$

Bemerkung. Aus dem Beweis geht hervor, dass der Ring $K[s_1, \ldots, s_n]$ isomorph zum Polynomring in n Unbestimmten über K ist. Insbesondere folgt hieraus, dass sich jedes symmetrische Polynom in n Unbestimmten *eindeutig* darstellen läßt als Polynom in den elementarsymmetrischen Funktionen $s_1, \ldots, s_n$, wie in Satz 19.3(d) behauptet.

Korollar. *Sei* $\operatorname{char}(K) = 0$. *Dann ist die allgemeine Gleichung* n*-ten Grades über* K *für* $n = 2, 3, 4$ *durch Radikale auflösbar und für* $n \geq 5$ *nicht durch Radikale auflösbar.*

Beweis. Sei $f = 0$ besagte Gleichung. Dann ist $G(f) \simeq S_n$ nach dem Satz. Da S_n für $n \leq 4$ auflösbar ist, und für $n \geq 5$ nicht auflösbar ist nach 5.6, folgt die Behauptung aus 18.7. □

19.5 Realisierung endlicher Gruppen als Galoisgruppen

Satz. *Sei* G *eine endliche Gruppe der Ordnung* n. *Dann ist* G *isomorph zu einer Untergruppe der symmetrischen Gruppe* S_n, *und es gibt Körper* $Z \subset F$, *so daß* F *galoissch über* Z *ist mit Galoisgruppe* $G(F/Z) \simeq G$.

- *Jede endliche Gruppe läßt sich also als Galoisgruppe einer Galoiserweiterung realisieren.*

Beweis. Definiere $t_\sigma \colon G \longrightarrow G,\ \tau \longmapsto \sigma\tau$. Dann ist

$$\psi \colon G \longrightarrow G(f) \simeq S_n,\ \sigma \longmapsto t_\sigma\,,$$

ein injektiver Gruppenhomomorphismus, denn $t_{\rho\sigma}(\tau) = \rho\sigma\tau = t_\rho(\sigma\tau) = (t_\rho \circ t_\sigma)(\tau)\ \forall\, \tau \in G$, und also $\psi(\rho\sigma) = \psi(\rho) \circ \psi(\sigma)\ \forall\, \rho, \sigma \in G$. Ist $t_\sigma = t_\rho$, folgt $\sigma = t_\sigma(\mathrm{id}) = t_\rho(\mathrm{id}) = \rho$, also ist ψ injektiv.
Ist K ein Körper, so ist der rationale Funktionenkörper $K(X_1, \ldots, X_n)$ galoissch über $Z_0 := K(s_1, \ldots, s_n)$ mit Galoisgruppe $G(F/Z_0) \simeq S_n$ nach 19.3. Also ist G isomorph zu einer Untergruppe H von $G(F/Z_0)$, und F ist galoissch über $Z := F^H$ mit Gruppe $H \simeq G$ nach 16.1. □

19.6 Das Umkehrproblem der Galoistheorie

Es sei ein Grundkörper K fest vorgegeben. Welche endlichen Gruppen lassen sich dann als Galoisgruppen einer Galoiserweiterung von K realisieren? Anders gesagt: Gegeben ein Körper K und eine endliche Gruppe G. Gibt es dann eine Galoiserweiterung L von K mit $G(L/K) \simeq G$? Dies ist ein aktuelles Forschungsgebiet, vgl. Malle, G., Matzat, B.H.: Inverse Galois theorie, Springer-Verlag 1999)

19.7 Die Diskriminante eines Polynoms

Definition. Sei K ein Körper, und sei

$$f = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in K[X]$$

ein normiertes Polynom. Seien $x_1, \ldots, x_n$ die Nullstellen von f in einem Zerfällungskörper L von f. Dann heißt

$$\triangle(f) := \prod_{i<j}(x_i - x_j)^2 = (-1)^{n(n-1)/2} \prod_{i \neq j}(x_i - x_j)$$

die *Diskriminante von* f. Sie ist symmetrisch in $x_1, \ldots, x_n$ und kann daher nach 19.3(d) als polynomialer Ausdruck in den $s_i(x_1, \ldots, x_n)$ geschrieben werden. In L[X] gilt

$$f = (X - x_1) \cdot \ldots \cdot (X - x_n) \overset{19.2}{=} \sum_{i=0}^{n}(-1)^i s_i(x_1, \ldots, x_n)X^{n-i}$$

und also $a_i = (-1)^i\, s_i(x_1, \ldots, x_n) \in K$ für $i = 1, \ldots, n$, wie man durch Koeffizientenvergleich in $L[X]$ sieht. Die Diskriminante $\triangle(f)$ ist also ein polynomialer Ausdruck in den Koeffizienten $a_1, \ldots, a_n$. Sie kann auch berechnet werden, wenn man die Nullstellen von f nicht kennt. Für $n = 2$ gilt zum Beispiel $\triangle(f) = a_1^2 - 4a_0$, und für das Polynom $f = X^3 + a_1X + a_0$ ist $\triangle(f) = -4a_1^3 - 27a_0^2$.
Es ist $\sqrt{\triangle(f)} \in L$, und $Z := K(\sqrt{\triangle(f)})$ ist ein Zwischenkörper vom Grad $[Z : K] \leq 2$.
Ferner gilt $\triangle(f) = 0$ genau dann, wenn f eine mehrfache Nullstelle besitzt.

Bemerkung. Wenn $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in K[X]$ separabel ist, so ist der Zerfällungskörper L von f nach 15.8 galoissch über K, und man sieht sofort, dass die Elemente $s_i(x_1, \ldots, x_n) \in L$ in K liegen, denn sie liegen im Fixkörper $L^{G(L/K)} \overset{15.8}{=} K$. Die Automorphismen der Galoisgruppe permutieren ja nur die Nullstellen $x_1, \ldots, x_n$ von f nach 15.5 und lassen daher alle in $x_1, \ldots, x_n$ symmetrischen Ausdrücke wie zum Beispiel $x_1 + \cdots + x_n$ fest.

19.8 Spur und Norm

Sei L eine Galoiserweiterung eines Körpers K. Dann heißt die additive Abbildung

$$\mathrm{Spur}_{L/K} \colon L \longrightarrow K\,,\ x \longmapsto \sum_{\sigma \in G(L/K)} \sigma(x)\,,$$

die *Spur von* L *über* K. Es ist $\mathrm{Spur}_{L/K}(x) \in K$ für jedes $x \in L$, da $\mathrm{Spur}_{L/K}(x) \in L^{G(L/K)} \underset{15.8}{=} K$ gilt. Oft benutzt wird auch die folgende Eigenschaft der Spur:

Behauptung. Es gibt ein $y \in L$ mit $\mathrm{Spur}_{L/K}(y) \neq 0$.

Beweis. Wäre $\sum_\sigma \sigma(x) = 0$ für alle $x \in L$, so wären die Charaktere $\sigma|_{L^*} : L^* \longrightarrow L^*$ linear abhängig, was Satz 18.4 widerspräche. □

Die multiplikative Abbildung

$$N_{L/K} \colon L^* \longrightarrow K^* , \ x \longmapsto \prod_{\sigma \in G(L/K)} \sigma(x) ,$$

nennt man *Norm von L über K*. Ist $[L : K] = n$, so gilt $N_{L/K}(a) = a^n$ und $\mathrm{Spur}_{L/K}(a) = na$ für jedes $a \in K$.

20 Konstruierbarkeit mit Zirkel und Lineal

Wir identifizieren $\mathbb{R}^2$ mit dem Körper $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$ der komplexen Zahlen. Für $z = a + bi$ mit $a, b \in \mathbb{R}$ setzen wir wie üblich

$$|z| = \sqrt{a^2 + b^2} \qquad \text{und} \qquad \bar{z} = a - bi$$

und nennen $a =: \mathrm{Re}(z)$ den *Realteil* und $b =: \mathrm{Im}(z)$ den *Imaginärteil* von z.

Sei M eine Teilmenge von $\mathbb{C}$, die mindestens zwei Punkte enthalte, (mit *Punkten* sind hier Elemente von $\mathbb{C}$ gemeint). Wie in 0.4 definiert, sei dann $\widehat{M}$ die Menge der *aus M mit Zirkel und Lineal konstruierbaren Punkte* in $\mathbb{C}$.

20.1 Konstruktion von Senkrechten und Parallelen

Bemerkung. Es seien g eine Gerade in $\mathbb{C}$, die mindestens zwei Punkte aus $\widehat{M}$ enthalte, $p \in \widehat{M}$ ein Punkt, der nicht auf g liege, und $g^\perp$ die zu g senkrechte Gerade durch p. Dann gelten:

(i) Der Schnittpunkt von g und $g^\perp$ liegt in $\widehat{M}$. Man sagt dazu auch: Der Fußpunkt des Lotes von p auf die Gerade g ist mit Zirkel und Lineal aus M konstruierbar.

(ii) Die Parallele von g durch p ist die Verbindungsgerade zweier Punkte aus $\widehat{M}$.

Beweis. (i): Wir wählen einen Punkt $q \in \widehat{M}$, der auf g aber nicht auf $g^\perp$ liegt, und schlagen einen Kreis um p vom Radius $\overline{pq} := |p - q|$. Dieser Kreis schneidet g in q und in einem weiteren Punkt q'. Es ist $q' \in \widehat{M}$, (da q' durch Operation (2) in 0.4 gewonnen wird). Schlägt man nun

Kreise vom Radius $\overline{pq}$ um q und um q', so liegen die beiden Schnittpunkte dieser Kreise auf $g^\perp$ und sind in $\widehat{M}$, (da sie durch Operation (3) in 0.4 gewonnen werden). Der Schnittpunkt von g und $g^\perp$ liegt dann in $\widehat{M}$, (da er durch Operation (1) in 0.4 gewonnen wird).

(ii): Es sei s der Schnittpunkt von g und $g^\perp$, also $s \in \widehat{M}$ nach (i). Der Kreis vom Radius $\overline{sp}$ um p schneidet $g^\perp$ in s und in einem weiteren Punkt s'. Es ist $s' \in \widehat{M}$, (da s' durch Operation (2) in 0.4 gewonnen wird). Schlägt man nun Kreise vom Radius $\overline{ss'}$ um s und um s', so liegen die Schnittpunkte dieser beiden Kreise auf der Parallelen von g durch p. Sie sind in $\widehat{M}$, (da sie durch Operation (3) in 0.4 gewonnen werden).

□

20.2 Lemma über konstruierbare Punkte

Lemma. *Es gelte $\{0,1\} \subset M \subset \mathbb{C}$. Dann hat die Menge $\widehat{M}$ aller aus M mit Zirkel und Lineal konstruierbaren Punkte die folgenden Eigenschaften und bildet insbesondere einen Teilkörper von $\mathbb{C}$.*

(1) $i \in \widehat{M}$.

(2) $z \in \widehat{M} \implies |z|,\ \mathrm{Re}(z),\ \mathrm{Im}(z),\ \bar{z} \in \widehat{M}$

(3) $z_1, z_2 \in \widehat{M} \implies z_1 + z_2 \in \widehat{M}$ *und* $-z_2 \in \widehat{M}$

(4) $z_1, z_2 \in \widehat{M},\ z_2 \neq 0, \implies z_1 z_2 \in \widehat{M}$ *und* $z_2^{-1} \in \widehat{M}$.

Beweis. Die reelle Gerade $\mathbb{R}$ enthält die Punkte $0, 1 \in M$.

(1): Es ist -1 ein Schnittpunkt von $\mathbb{R}$ mit dem *Einheitskreis* $\mathbb{E}$ vom Radius 1 um 0, und daher gilt $-1 \in \widehat{M}$ gemäß der Operation (2) in Abschnitt 04. Der Abstand zwischen -1 und 1 ist 2, und daher sind die beiden Schnittpunkte der Kreise vom Radius 2 um 1 und um -1 in $\widehat{M}$ gemäß Operation (3) in 0.4. Die Verbindungsgerade dieser Schnittpunkte ist die imaginäre Achse. Schneidet man diese mit $\mathbb{E}$, so erhält man $i \in \widehat{M}$.

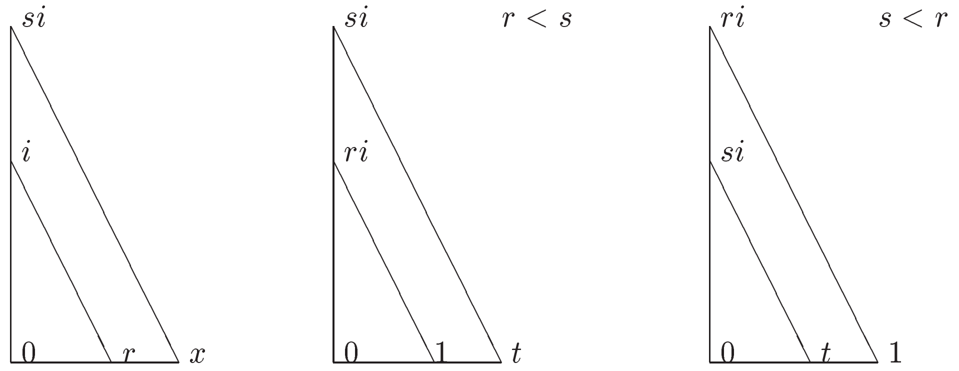
(2): Es ist $|z|$ ein Schnittpunkt der reellen Achse mit dem Kreis um 0 vom Radius $|z|$. Also ist mit z auch $|z| \in \widehat{M}$. Schreiben wir $z = a + bi$ mit $a = \mathrm{Re}(z)$ und $b = \mathrm{Im}(z)$, so ist a der Fußpunkt des Lotes von z auf $\mathbb{R}$, und daher gilt $a \in \widehat{M}$ nach 20.1. Es ist $\bar{z}$ ein Schnittpunkt des Kreises um a vom Radius $\overline{az}$ mit der Geraden durch z und a, also gilt $\bar{z} \in \widehat{M}$. Wegen (1) erfüllt auch die imaginäre Achse $\mathbb{R}i$ die Voraussetzung an die Gerade g in 20.1, und daher ist $bi \in \widehat{M}$ als Fußpunkt des Lotes von z auf $\mathbb{R}i$. Es ist dann auch $b \in \widehat{M}$ als Schnittpunkt des Kreises um 0 vom Radius $|bi| = |b|$ mit $\mathbb{R}$.

(3): Sind z_1 und z_2 linear unabhängig, so schlage man einen Kreis um z_1 mit Radius $|z_2|$ und einen Kreis um z_2 mit Radius $|z_1|$. Einer der Schnittpunkte der beiden Kreise ist dann Eckpunkt des von z_1 und z_2 aufgespannten Parallelogramms und also gleich $z_1 + z_2$. Hieraus folgt $z_1 + z_2 \in \widehat{M}$. Sind z_1 und z_2 linear abhängig und ist $z_2 \neq 0$, so erhält man $z_1 + z_2$ als Schnittpunkt der Geraden durch 0 und z_2 mit dem Kreis vom Radius $|z_2|$ um z_1. Also ist dann ebenfalls $z_1 + z_2 \in \widehat{M}$. Speziell für $z_1 = 0$ ist $-z_2$ ein Schnittpunkt und liegt daher in $\widehat{M}$.

(4): Nach Definition der Multiplikation in $\mathbb{C}$ ist $z_1 z_2 = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1)i$ für $z_1 = a_1 + b_1 i$ und $z_2 = a_2 + b_2 i$ mit $a_1, a_2, b_1, b_2 \in \mathbb{R}$. Um $z_1 z_2 \in \widehat{M}$ zu zeigen, ist nach (2) und (3) nur noch zu zeigen, dass $rs \in \widehat{M}$ gilt für alle positiven reellen $r, s \in \widehat{M}$.

Mit s liegt auch si in $\widehat{M}$, wie man erkennt, wenn man einen Kreis vom Radius s um 0 schlägt.

Wir betrachten, wie im linken Dreieck illustriert, die Parallele durch si von der Geraden durch i und r. Deren Schnittpunkt x mit $\mathbb{R}$ liegt in $\widehat{M}$, wie aus 20.1 (ii) folgt.



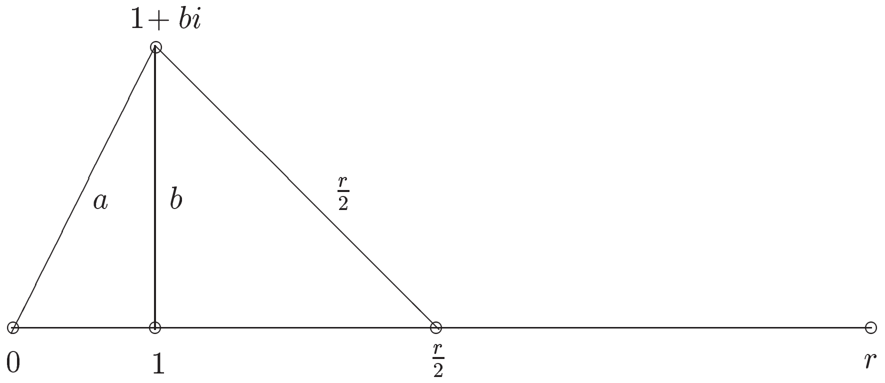
Nach dem Strahlensatz gilt $\dfrac{x}{r} = \dfrac{|si|}{|i|} = \dfrac{s}{1}$ und also $x = rs \in \widehat{M}$.

Um $z_2^{-1} \in \widehat{M}$ zu zeigen, genügt es nach dem Vorangegangenen $r^{-1} \in \widehat{M}$ für alle positiven reellen $r \in \widehat{M}$ zu zeigen, denn es ist $z_2^{-1} = \overline{z_2} \cdot |z_2|^{-2}$. Dies folgt analog aus 20.1 (ii) und dem Strahlensatz. Wie durch die beiden rechten Dreiecke veranschaulicht, gilt danach $\dfrac{s}{r} = \dfrac{t}{1}$ und also $\dfrac{s}{r} \in \widehat{M}$ für alle positiven reellen $r, s \in \widehat{M}$. $\square$

20.3 Wurzeln konstruierbarer Punkte

Satz. *Es gelte* $\{0,1\} \subset M \subset \mathbb{C}$. *Dann ist der Körper* $\widehat{M}$ *der aus* M *mit Zirkel und Lineal konstrierbaren Punkte* quadratisch abgeschlossen, *d. h. zu jedem Punkt* $z \in \widehat{M}$ *gehört auch der Punkt* $\sqrt{z}$ *zu* $\widehat{M}$. *(Dabei bezeichnet* $\sqrt{z}$ *eine komplexe Zahl* w *mit* $w^2 = z$.*)*

Beweis. Nach 20.2 sind $r := |z|$ sowie $\frac{r}{2}$ und r^{-1} in $\widehat{M}$. Wir stellen $z \neq 0$ in der Form $z = r(\cos\varphi + i\sin\varphi)$ dar, wobei $r > 0$ und $-\pi < \varphi \leq \pi$ gilt. Es ist $\sqrt{z} = \pm\sqrt{r}\,(\cos\frac{\varphi}{2} + i\sin\frac{\varphi}{2})$. Da man die Winkelhalbierende stets mit Zirkel und Lineal konstruieren kann, ist nur noch zu zeigen, dass $\sqrt{r}$ in $\widehat{M}$ liegt. Wir betrachten zunächst den Fall $r > 1$. Sei $1 + bi$ mit $b \in \mathbb{R}$ einer der Schnittpunkte des Kreises vom Radius $\frac{r}{2}$ um $\frac{r}{2}$ mit der Parallelen durch 1 zur imaginären Achse. Dann ist $1 + bi \in \widehat{M}$, (nach 20.2, 20.1 und 0.4), und also gilt auch $a := \sqrt{1+b^2} = |1 + bi| \in \widehat{M}$ nach 20.2.



Nach dem Satz von Pythargoras ist $(\frac{r}{2} - 1)^2 + b^2 = (\frac{r}{2})^2$. Hieraus folgt $1 + b^2 = r$ und also $\sqrt{r} = a \in \widehat{M}$. Im Fall $r < 1$ zeigt man analog $\sqrt{r^{-1}} \in \widehat{M}$, woraus dann $\sqrt{r} \in \widehat{M}$ nach 20.2 folgt. $\square$

20.4 Algebraische Formulierung der Konstruierbarkeit

Es sei weiterhin M eine Menge mit $\{0,1\} \subset M \subset \mathbb{C}$ und $\widehat{M}$ der Teilkörper von $\mathbb{C}$ aller aus M mit Zirkel und Lineal konstruierbaren Punkte, (vgl. 20.2). Es ist dann $\mathbb{Q}$ ein Teilkörper von $\widehat{M}$, (denn $\mathbb{Q}$ ist als Primkörper von $\mathbb{C}$ in jedem Teilkörper von $\mathbb{C}$ enthalten, vgl. 11.6).

Wir setzen $\overline{M} := \{\bar{z} \mid z \in M\}$. Dann ist auch der Körper $\mathbb{Q}(M \cup \overline{M})$ ein Teilkörper von $\widehat{M}$ nach 20.2 (2). Wir zeigen, dass jeder Punkt $z \in \widehat{M}$ in einer Galoiserweiterung dieses Körpers von 2-Potenzgrad enthalten ist. Deren Galoisgruppe ist auflösbar, und wir erhalten dadurch Aussagen über die Lösbarkeit einiger Konstruktionsprobleme.

Satz. *Sei $\{0,1\} \subset M \subset \mathbb{C}$, und sei $K_0 = \mathbb{Q}(M \cup \overline{M})$. Für $z \in \mathbb{C}$ sind dann äquivalent:*

(i) Es gilt $z \in \widehat{M}$.

(ii) Es gibt Körpererweiterungen $K_0 \subset K_1 \subset \cdots \subset K_n \subset \mathbb{C}$ mit $z \in K_n$ und $[K_i : K_{i-1}] = 2$ für $i = 1, \ldots, n$.

(iii) Es ist z enthalten in einer Galoiserweiterung L von K_0, für die $[L : K_0]$ eine Potenz von 2 ist.

Beweis. Für einen Teilkörper K von $\mathbb{C}$ sei $\mathcal{G}(K)$ die Menge aller Geraden, die mindestens zwei Punkte von K enthalten, und sei $\mathcal{K}(K)$ die Menge aller Kreise mit Mittelpunkt aus K, deren Radius der Abstand zweier Punkte aus K sind.
(i) $\Longrightarrow$ (ii): Sei K ein Teilkörper von $\mathbb{C}$, der zu jedem $w \in K$ auch die konjugiert komplexe Zahl $\bar{w}$ enthält. Gemäß der Definition in 0.4 der Konstruierbarkeit mit Zirkel und Lineal betrachten wir folgende drei Fälle:

(a) Es ist z ein Schnittpunkt zweier Geraden aus $\mathcal{G}(K)$.

(b) Es ist z ein Schnittpunkt eines Kreises aus $\mathcal{K}(K)$ mit einer Geraden aus $\mathcal{G}(K)$.

(c) Es ist z ein Schnittpunkt zweier Kreise aus $\mathcal{K}(K)$

Wir zeigen, dass in jedem dieser Fälle z in einer Körpererweiterung vom Grad ≤ 2 von K enthalten ist. Durch Induktion folgt daraus die Aussage (ii).
Im Fall (a) gibt es $\lambda, \lambda' \in \mathbb{R}$ und $z_1, z_2, z_1', z_2' \in K$ derart, dass $z_1 + \lambda z_2 = z = z_1' + \lambda' z_2'$ gilt. Da $z_1 \pm \overline{z_1} \in K$ und $z_1 = a_1 + b_1 i$ mit $a_1, b_1 \in \mathbb{R}$ gilt, sind a_1 und $b_1 i$ in K. Analoges gilt für z_2, z_1', z_2', und wir erhalten ein lineares Gleichungssystem in λ, λ' der Form

$$\begin{aligned} a_1 + \lambda a_2 &= a_1' + \lambda' a_2' \\ b_1 i + \lambda b_2 i &= b_1' i + \lambda' b_2' i \end{aligned}$$

mit Koeffizienten $a_k, a_k', b_k i, b_k' i \in K$ für $k = 1, 2$. Es folgt dann $\lambda, \lambda' \in K$ und also auch $z = z_1 + \lambda z_2 \in K$.

Im Fall (b) habe der Kreis den Mittelpunkt $z_3 = a_3 + b_3 i$ und Radius r. Der Schnittpunkt $z = z_1 + \lambda z_2$ dieses Kreises mit einer Geraden aus $\mathcal{G}(K)$ erfüllt die Gleichung

$$(\lambda a_2 + a_1 - a_3)^2 - (\lambda b_2 i + b_1 i - b_3 i)^2 = r^2 .$$

Dies ist entweder eine lineare oder eine quadratische Gleichung in λ. Im ersten Fall folgt $\lambda \in K$ und daher $z \in K$. Im zweiten Fall erhält man eine Gleichung der Form $\lambda^2 + p\lambda + q$ mit $p, q \in K$, und es folgt $\lambda = -\frac{p}{2} \pm \sqrt{w}$ mit $w = \frac{p^2}{4} - q$. Hieraus folgt $z \in K(\sqrt{w})$.

Im Fall (c) seien die beiden (verschiedenen) Kreise durch die Gleichungen

$$\begin{aligned} (a - a_1)^2 - (bi - b_1 i)^2 &= r^2 \\ (a - a_2)^2 - (bi - b_2 i)^2 &= s^2 \end{aligned}$$

gegeben. Subtraktion ergibt $xa + ybi = t$ mit $x, y, t \in K$ und $(x, y) \neq (0, 0)$. Weil die Mittelpunkte der beiden Kreise verschieden sind, beschreibt diese Gleichung eine Gerade aus $\mathcal{G}(K)$, die die Kreise in z schneidet. Wir können nun wie im Fall (b) schließen.

(ii) $\Longrightarrow$ (i): Da $\widehat{M}$ nach 20.2, 20.3 ein quadratisch abgeschlossener Teilkörper von $\mathbb{C}$ ist, gilt diese Implikation.

(ii) $\Longrightarrow$ (iii): Seien $\sigma_1, \ldots, \sigma_m \in G(N/K)$, wobei N eine Galoiserweiterung von K sei, die K_n enthalte, die verschiedenen K-Homomorphismen von K_n in $\mathbb{C}$
Nach 15.9 kann K_n in eine Galoiserweiterung N von K eingebettet werden. Sei $G(N/K) = \{\sigma_1, \ldots \sigma_m\}$ ihre Galoisgruppe, und sei L das Kompositum der Körper $\sigma_1(K_n), \ldots, \sigma_m(K_n)$. Dann ist L galoissch über K_0 nach 16.3, und L entsteht aus K_0 durch sukzessives Ziehen von Quadratwurzeln, weil dies für K_n und alle $\sigma_j(K_n)$ mit $j = 1, \ldots, m$ gilt. Also ist der Grad von L über K_0 eine Potenz von 2, und es ist $z \in L_n \subset L$.

(iii) $\Longrightarrow$ (ii): Die Galoisgruppe $G(L/K_0)$ ist nach 3.3 eine Normalreihe mit Faktorgruppen der Ordnung 2. Dieser Normalreihe entspricht nach dem Hauptsatz der Galoistheorie 16.1 ein Körperturm wie in (ii) verlangt. □

20.5 Konstruierbare Punkte haben 2-Potenzgrad

Korollar. *Sei $\{0,1\} \subset M \subset \mathbb{C}$, und sei $K_0 = \mathbb{Q}(M \cup \overline{M})$. Dann ist der Körper $\widehat{M}$ aller aus M mit Zirkel und Lineal konstruierbaren Punkte eine algebraische Körpererweiterung von K_0, und für jedes $z \in \widehat{M}$ ist der Grad $[K_0(z) : K_0]$ eine Potenz von 2.*

Beweis. Dies folgt unmittelbar aus Satz 20.4 und dem Gradsatz 11.7. □

20.6 Delisches Problem der Würfelverdoppelung

Kann man das Volumen eines Würfels durch Konstruktion mit Zirkel und Lineal verdoppeln? Betrachten wir einen Würfel der Kantenlänge 1, so hat der Würfel doppelten Volumens die Kantenlänge $\sqrt[3]{2}$, und der Punkt $\sqrt[3]{2}$ ist aus $M = \{0, 1\}$ mit Zirkel und Lineal zu konstruieren. Dies ist aber nach 20.5 nicht möglich, da $\mathbb{Q}(\sqrt[3]{2})$ den Grad 3 über $\mathbb{Q}$ hat. Das Delische Problem der Würfelverdoppelung ist also nicht lösbar.

20.7 Problem der Quadratur des Kreises

Kann man einen Kreis, der durch Mittelpunkt und Radius gegeben ist, durch Konstruktion mit Zirkel und Lineal in ein Quadrat gleichen Flächeninhalts verwandeln? Der Flächeninhalt des Kreises um 0 vom Radius 1 ist gleich π. Das Quadrat mit dem Flächeninhalt π hat die Seitenlänge $\sqrt{\pi}$. Da π transzendent über $\mathbb{Q}$ ist (wie Lindemann 1882 in der Zeitschrift *Mathematische Annalen* bewiesen hat) und $\widehat{\{0,1\}}$ nach 20.5 eine algebraische Körpererweiterung von $\mathbb{Q}$ ist, ist also das Problem der Quadratur des Kreises nicht lösbar.

20.8 Problem der Winkeldreiteilung

Kann man zu einem Winkel α den Winkel $\frac{\alpha}{3}$ mit Zirkel und Lineal konstruieren? Dieses Problem ist im allgemeinen nicht lösbar.

Beispiele. (1) Der Winkel $\frac{\pi}{3} \mathrel{\widehat{=}} 60°$ läßt sich nicht mit Zirkel und Lineal dritteln.

(2) Der Winkel $\frac{\pi}{2} \mathrel{\widehat{=}} 90°$ hingegen ist mit Zirkel und Lineal zu dritteln.

Beweis. (1) Aus der Konstruierbarkeit des Winkels von 20° würde die Konstruierbarkeit des Winkels von 40° folgen, und also müsste die primitive 9-te Einheitswurzel $\zeta_9 = e^{2\pi i/9}$ konstruierbar sein.
Es ist aber $[\mathbb{Q}(\zeta_9) : \mathbb{Q}] = \varphi(9) = 6$ nach 17.6 und 17.2 und also keine 2-Potenz im Widerspruch zu 20.5.

(2) Der Punkt $z = \cos\frac{\pi}{6} + i\sin\frac{\pi}{6}$ ist aus $M = \{0, 1\}$ mit Zirkel und Lineal konstruierbar, denn es ist $z = \pm\frac{1}{2}\sqrt{3} + \frac{i}{2}$ und also Nullstelle des quadratischen Polynoms $X^2 - iX - 1 \in \mathbb{Q}(i)[X]$. Da $i \in \widehat{M}$ gilt nach 20.2, folgt $z \in \widehat{M}$ aus 20.4 “(ii) ⇒ (i)”.

□

20.9 Problem der Konstruierbarkeit von regelmäßigen n-Ecken

Lemma. *Sei $n \in \mathbb{N}, n \geq 3$. Das regelmäßige n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn $\varphi(n)$ eine Potenz von 2 ist. (Dabei bezeichnet φ die Eulersche φ-Funktion, vgl. 17.2).*

Beweis. Das regelmäßige n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn die primitive n-te Einheitswurzel $\zeta_n = e^{2\pi i/n}$ in $\widehat{M}$ liegt für $M = \{0, 1\}$. Es ist $Q(\zeta_n)$ galoissch über $\mathbb{Q}$ vom Grad $\varphi(n)$ nach 17.6 und 17.2. Ist $\zeta_n \in \widehat{M}$, so ist $\varphi(n)$ eine Potenz von 2 nach 20.5. Ist umgekehrt $\varphi(n)$ als Potenz von 2 vorausgesetzt, so folgt $\zeta_n = e^{2\pi i/n} \in \widehat{M}$ aus 20.4 "(iii) $\Rightarrow$ (i)". □

Bemerkung. Eine Zahl F_ℓ heißt *Fermatsche Zahl*, wenn sie von der Form $2^{2^\ell} + 1$ ist; zum Beispiel sind $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ Primzahlen und werden daher *Fermatsche Primzahlen* genannt, aber man weiß, dass die Fermatsche Zahl F_ℓ für $5 \leq \ell \leq 16$ keine Primzahl ist.

Satz. *Sei $n \in \mathbb{N}, n \geq 3$. Das regelmäßige n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn es ein $m \in \mathbb{Z}, m \geq 0$, und paarweise verschiedene Fermatsche Primzahlen $p_1, \dots, p_s$ gibt mit $n = 2^m \cdot p_1 \cdot \dots \cdot p_s$ oder $n = 2^m$.*

Beweis. Sei $n = 2^m \cdot p_1^{m_1} \cdot \dots \cdot p_s^{m_s}$ die Primzahlzerlegung von n mit paarweise verschiedenen Primzahlen $p_1 \neq 2, \dots, p_s \neq 2$ und $m_1, \dots, m_s > 0$. Wie in 17.2 gezeigt wurde, ist dann

$$\varphi(n) = \begin{cases} 2^{m-1} \cdot p_1^{m_1-1}(p_1-1) \cdot \ \dots \ \cdot p_s^{m_s-1}(p_s-1) & \text{falls } m > 0 \\ \\ p_1^{m_1-1}(p_1-1) \cdot \ \dots \ \cdot p_s^{m_s-1}(p_s-1) & \text{falls } m = 0 \end{cases}$$

Also ist $\varphi(n)$ genau dann eine Potenz von 2, wenn $m_1 = \dots = m_k = 1$ gilt und $p_1, \dots, p_s$ Fermatsche Primzahlen sind, denn ist p eine Primzahl und $p-1$ eine Potenz von 2, etwa $p = (2^{2^\ell})^k + 1$, mit ungeradem $k \in \mathbb{N}$, dann muss $k = 1$ gelten, weil man andernfalls die Primzahl p echt zerlegen könnte in $p = \left(2^{2^\ell} + 1\right)\left((2^{2^\ell})^{k-1} - \dots + 1\right)$. Der Satz folgt nun aus dem Lemma. □

21 Algebraischer Abschluss eines Körpers

Wir sind bei der Herleitung der Galoistheorie mit dem Begriff des Zerfällungskörpers eines Polynoms ausgekommen. In einigen Algebra-Büchern wird dabei auch noch der algebraische Abschluss eines Körpers hinzugezogen, weil man mit diesem in vielen Teilen der Mathematik sowieso arbeiten muss. Wir werden nun in diesem letzten Paragraphen der Vorlesung den algebraischen Abschluss eines Körpers definieren und seine Existenz und Eindeutigkeit beweisen.

Es sei K ein beliebiger Körper. Ist zudem eine Körpererweiterung L von K vorgegeben, so kann man leicht den *algebraischen Abschluss* $\overline{K}$ *von* K *in* L bestimmen, so wie wir es in 12.5 auch schon getan haben. Ist aber L nicht gegeben, so besteht die Schwierigkeit darin, eine geeignete Körpererweiterung überhaupt erst einmal zu finden. Dazu werden wir in 21.3 den Polynomring $K[\mathfrak{X}]$ mit einem System $\mathfrak{X}$ von beliebig vielen Unbestimmten definieren und damit in 21.4 den algebraischen Abschluss nach einer Methode von Emil Artin konstruieren.

21.1 Algebraisch abgeschlossene Körper

Definition. Ein Körper L heißt *algebraisch abgeschlossen*, wenn jedes nicht konstante Polynom aus $L[X]$ eine Nullstelle in L besitzt.

Beispiele.

1. Der Körper $\mathbb{C}$ ist algebraisch abgeschlossen, wie in der Vorlesung *Funktionentheorie* bewiesen wird.

2. Sei L eine Körpererweiterung eines Körpers K. Wenn L algebraisch abgeschlossen ist, so ist auch der oben erwähnte algebraische Abschluss $\overline{K}$ von K in L algebraisch abgeschlossen.

   Beweis. Sei $f \in \overline{K}[X]$ ein nicht konstantes Polynom. Dann hat f eine Nullstelle x in L; diese ist algebraisch über $\overline{K}$ und also auch über K nach 12.6. Es folgt $x \in \overline{K}$. □

3. Der in 12.5 definierte Körper $\overline{\mathbb{Q}}$ der algebraischen Zahlen ist algebraisch abgeschlossen, wie aus 2. folgt.

Satz. *Für einen Körper K sind folgende Aussagen äquivalent.*

(i) *K ist algebraisch abgeschlossen.*

(ii) *Die irreduziblen Polynome in $K[X]$ sind die Polynome vom Grad* 1.

(iii) *Jedes Polynom $f \neq 0$ in $K[X]$ besitzt eine Darstellung*

$$f = c(X - x_1)^{k_1} \cdot \ldots \cdot (X - x_n)^{k_n}$$

mit $c \in K$, paarweise verschiedenen $x_1, \ldots, x_n \in K$ und $k_1, \ldots, k_n \in \mathbb{N}$.

(iv) *Für jede algebraische Körpererweiterung L von K gilt $L = K$.*

Beweis. (i) $\Longrightarrow$ (ii): Sei f irreduzibel und also nicht konstant. Dann besitzt f nach (i) eine Nullstelle x in K. Nach Lemma 8.2 ist $f = (X - x)g$ mit $\text{grad}(g) = grad(f) - 1$. Da f irreduzibel ist, folgt $\text{grad}(g) = 0$ und $\text{grad}(f) = 1$, vgl. 6.13.

(ii) $\Longrightarrow$ (iii): Dies gilt, weil $K[X]$ faktoriell ist, vgl. 8.10.

(iii) $\Longrightarrow$ (iv): Sei L algebraisch über K und $x \in L$. Da das Minimalpolynom m_x von x irreduzibel und normiert ist, gilt $m_x = X - x$ nach (iii). Es folgt $x \in K$.

(iv) $\Longrightarrow$ (i): Sei $f \in K[X]$ nicht konstant. Dann gilt $L = K$ für den Zerfällungskörper L von f nach (iv). Folglich sind die Nullstellen von f in K. $\square$

21.2 Definition des algebraischen Abschlusses

Eine Körpererweiterung $\overline{K}$ eines Körpers K heißt *algebraischer Abschluss* von K, wenn erstens $\overline{K}$ algebraisch über K ist und wenn zweitens $\overline{K}$ algebraisch abgeschlossen ist.

21.3 Polynomringe in beliebig vielen Unbestimmten

Sei H eine abelsche Halbgruppe, also eine Menge mit einer assoziativen, kommutativen Verknüpfung $H \times H \longrightarrow H$, $(h, h') \mapsto h + h'$, und einem neutralen Element 0, zum Beispiel $H = \mathbb{N}_0$ mit $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$.

Für eine nicht leere Menge I definieren wir H^I als eine Menge von Abbildungen

$$H^I = \{\varphi : I \to H \mid \varphi(i) \neq 0 \text{ für nur endlich viele } i \in I\}.$$

Es ist dann H^I eine Halbgruppe; die Addition ist definiert durch $(\varphi + \varphi')(i) := \varphi(i) + \varphi'(i)$ für alle $i \in I$. Üblicherweise identifiziert man φ mit seinem Bild $\varphi(I)$ und erhält H^I als Menge aller *Familien* $(h_i)_{i \in I}$ mit *Komponenten* $h_i \in H$ und $h_i \neq 0$ für nur endlich viele $i \in I$. Die Addition geschieht dann komponentenweise.

Sei R ein kommutativer Ring, und sei M eine abelsche Halbgruppe. Dann ist die Halbgruppe R^M eine additive abelsche Gruppe, und wir definieren eine Multiplikation auf R^M durch

$$(a_m)_{m\in M} \cdot (b_m)_{m\in M} := \left(\sum_{k+\ell=m} a_k\, b_\ell\right)_{m\in M} .$$

Damit ist R^M ein kommutativer Ring. Für $m \in M$ sei $X^m := (\delta_{m,n})_{n\in M}$, wobei $\delta_{m,n}$ das *Kronecker-Symbol* sei, also $\delta_{m,n} = 0$ für $m \neq n$ und $\delta_{m,n} = 1$ für $m = n$ gelte. Die Elemente von R^M können dann in der Form $\sum_{m\in M} a_m X^m$ geschrieben werden mit eindeutig bestimmten Koeffizienten $a_m \in R$, die fast alle 0 sind. Addition und Multiplikation lesen sich dann so:

$$\sum_{m\in M} a_m X^m + \sum_{m\in M} b_m X^m = \sum_{m\in M} (a_m + b_m) X^m$$

$$\text{und} \quad \sum_{k\in M} a_k X^k \cdot \sum_{\ell\in M} b_\ell X^\ell = \sum_{m\in M} \left(\sum_{k+\ell=m} a_k b_\ell\right) X^m .$$

Es ist X^0 das Einselement von R^M, und vermöge der Identifikation von $a \in R$ mit aX^0 wird R als Unterring von R^M aufgefaßt. Wir nennen R^M einen *Polynomring*.

Wir betrachten nun den Spezialfall $M = \mathbb{N}_0^I$ mit $I = \{1, \ldots, n\}$. Dann gilt $m = (m_1, \ldots, m_n)$ mit $m_1, \ldots, m_n \in \mathbb{N}_0$ für jedes $m \in M$. Sei $X_i = X^{(0,\ldots,0,1,0,\ldots,0)}$, wobei die 1 an der i-ten Stelle stehe, für $i = 1, \ldots, n$. Das *Monom* X^m schreibt sich dann als $X^m = X_1^{m_1} \cdot \ldots \cdot X_n^{m_n}$ und der Koeffizient a_m als $a_m = a_{m_1\ldots m_n}$ für $m \in M$. Wir schreiben dann $R[X_1, \ldots, X_n]$ anstelle von R^M und nennen $R[X_1, \ldots, X_n]$ den *Polynomring in n Unbestimmten* $X_1, \ldots, X_n$.

Speziell für $n = 1$, also $M = \mathbb{N}_0$, ist $X_1 = X^1 = (0, 1, 0, \ldots)$. Wir setzen dann $X := X^1$ und erhalten den in 6.12 eingeführten Polynomring $R[X]$ in einer Unbestimmten X .

Ist allgemein $M = \mathbb{N}_0^I$ mit einer nicht leeren Menge I, so setzen wir $X_i = X^{(0,\ldots,0,1,0\ldots)}$, wobei die 1 an der i-ten Stelle stehe, für $i \in I$. Wir schreiben dann für den Ring R^M auch $R[\mathfrak{X}]$ mit $\mathfrak{X} = (X_i)_{i\in I}$ und nennen $R[\mathfrak{X}]$ den *Polynomring in den Unbestimmten* X_i , $i \in I$. Die Elemente von $R[\mathfrak{X}]$ sind dann definitionsgemäß jeweils Polynome in endlich vielen Unbestimmten $X_{i_1}, \ldots, X_{i_n}$, wobei $\{i_1, \ldots, i_n\}$ die endlichen Teilmengen von I durchlaufen, $n \in \mathbb{N}$.

21.4 Existenz des algebraischen Abschlusses

Satz. *Sei K ein Körper. Dann gibt es einen algebraischen Abschluss $\overline{K}$ von K.*

Beweis. Jedem Polynom $f \in K[X]$ vom Grad ≥ 1 ordnen wir eine Unbestimmte X_f zu. Dann betrachten wir den Polynomring $K[\mathfrak{X}]$ in den sämtlichen Unbestimmten X_f. Es sei $\mathfrak{I}$ das von allen Polynomen $f(X_f)$ erzeugte Ideal in $K[\mathfrak{X}]$, wobei $f(X_f)$ aus f entsteht, indem man in f die Unbestimmte X durch X_f ersetzt.

Wir zeigen zunächst, dass $\mathfrak{I}$ ein echtes Ideal in $K[\mathfrak{X}]$ ist. Andernfalls wäre $1 \in \mathfrak{I}$, und es gäbe eine Gleichung der Form

$$\sum_{i=1}^{n} g_i\, f_i(X_{f_i}) = 1$$

mit $g_1, \ldots, g_n \in K[\mathfrak{X}]$ und $f_1(X_{f_1}), \ldots, f_n(X_{f_n}) \in \mathfrak{I}$. Ausgehend vom Zerfällungskörper von $f_1 \in K[X]$ konstruieren wir dann induktiv eine Körpererweiterung von K, in der jedes Polynom $f_i \in K[X]$ eine Nullstelle x_i besitzt, $(i = 1, \ldots, n)$. Setzen wir x_i für X_{f_i} in die obige Gleichung ein, erhalten wir den Widerspruch $0 = 1$.

Nach 7.6 ist nun $\mathfrak{I}$ in einem maximalen Ideal $\mathfrak{M}$ von $K[\mathfrak{X}]$ enthalten, und $L_1 := K[\mathfrak{X}]/\mathfrak{M}$ ist ein Körper nach 7.4. Vermöge der kanonischen Homomorphismen $K \hookrightarrow K[\mathfrak{X}] \to L_1$ können wir L_1 als Körpererweiterung von K auffassen, (vgl. Folgerung 6.9). Es ist dann die Restklasse $X_f + \mathfrak{M} \in L_1$ eine Nullstelle von $f \in K[X]$, (dies sieht man analog wie beim Beweis des Satzes von Kronecker 12.7 ein).

Durch Wiederholung dieses Verfahrens erhalten wir induktiv einen Körperturm $K = L_0 \subset L_1 \subset L_2 \subset \ldots$ mit der Eigenschaft, dass jedes nicht konstante Polynom aus $L_n[X]$ eine Nullstelle in L_{n+1} besitzt. Der Körper $L := \bigcup_{n=0}^{\infty} L_n$ ist dann algebraisch abgeschlossen, denn ist $f \in L[X]$ ein nicht konstantes Polynom, so gibt es ein n so, dass $f \in L_n[X]$ ist, (weil f nur endlich viele Koeffizienten $\neq 0$ hat), und also f eine Nullstelle in $L_{n+1} \subset L$ besitzt. Der algebraische Abschluss $\overline{K}$ von K in L ist algebraisch über K gemäß 12.5 und algebraisch abgeschlossen nach 21.1.2. $\square$

21.5 Eindeutigkeit des algebraischen Abschlusses

Satz. *Sei K ein Körper, und sei $\overline{K}$ ein algebraischer Abschluss von K. Dann lässt sich jede algebraische Körpererweiterung K' von K in $\overline{K}$ einbetten, und je zwei algebraische Abschlüsse von K sind K-isomorph.*

Beweis. Wir zeigen mit Hilfe des Zornschen Lemmas 7.5 und des Fortsetzungslemmas 13.1, dass die Inklusion $\iota : K \hookrightarrow \overline{K}$ eine Fortsetzung zu einem Homomorphismus $K' \longrightarrow \overline{K}$ besitzt.

Sei M die Menge aller Paare (Z, σ) mit einem Zwischenkörper $K \subset Z \subset K'$ und einer Fortsetzung von ι zu einem Homomorphimus $\sigma : Z \longrightarrow \overline{K}$. Dann ist M halbgeordnet bezüglich der Relation $(Z, \sigma) \leq (Z', \sigma')$, bei der $Z \subset Z'$ gelte und $\sigma' : Z' \longrightarrow \overline{K}$ eine Fortsetzung von σ sei. Es ist $M \neq \emptyset$, da (K, ι) zu M gehört. Sei $N = \{(Z_i, \sigma_i)_{i \in J}\}$ (mit einer Indexmenge J) eine geordnete Teilmenge von M. Setzen wir $\tilde{L} := \bigcup_{i \in J} Z_i$ und $\tilde{\sigma}(x) := \sigma_i(x)$ für $x \in Z_i$, so erhalten wir eine wohldefinierte Fortsetzung $\tilde{\sigma} : \tilde{L} \longrightarrow \overline{K}$ von ι, und das Paar $(\tilde{L}, \tilde{\sigma})$ ist eine obere Schranke für N. Nach dem Zornschen Lemma 7.5 besitzt M ein maximales Element (L, σ). Es ist $L = K'$, denn andernfalls gäbe es ein $x \in K' \setminus L$ und nach 13.1 (da x algebraisch über K ist) eine Fortsetzung $L(x) \longrightarrow \overline{K}$ von σ im Widerspruch zur Maximalität von (L, σ).

Wir haben also eine Fortsetzung $\sigma : K' \longrightarrow \overline{K}$ von ι gefunden, und diese ist injektiv nach Folgerung 6.9.

Ist K' ein algebraischer Abschluss von K, so ist mit K' auch $\sigma(K')$ algebraisch abgeschlossen, und nach 12.6 ist $\overline{K}$ algebraisch über $\sigma(K')$. Mit 21.1 "(i) $\Longrightarrow$ (iv)" folgt $\overline{K} = \sigma(K')$, und also ist σ dann auch surjektv. $\square$

21.6 Universelle Eigenschaft des Polynomrings

Sei R ein kommutativer Ring, und sei M eine abelsche Halbgruppe. Wir bezeichnen mit R' stets einen kommutativen Ring und nennen eine Abbildung $\sigma : M \longrightarrow R'$ mit $\sigma(m + m') = \sigma(m) \cdot \sigma(m')$ für alle $m, m' \in M$ einen *Morphismus*. Der in 21.3 definierte Polynomring R^M hat dann die folgende *universelle Eigenschaft*.

Satz. *Zu jedem Ringhomomorphismus $\varphi : R \longrightarrow R'$ und zu jedem Morphismus $\sigma : M \longrightarrow R'$ gibt es genau einen Ringhomomorphismus $\Phi : R^M \longrightarrow R'$ mit $\Phi|_R = \varphi$ und $\Phi(X^m) = \sigma(m)$ für alle $m \in M$.*

Beweis. Jedes Element aus R^M hat die Form $\sum_{m \in M} a_m X^m$ mit eindeutig bestimmten Koeffizienten $a_m \in R$, die fast alle 0 sind, vgl. 21.3. Wir setzen

$$\Phi(\sum a_m X^m) = \sum \varphi(a_m)\sigma(m)$$

und erhalten dadurch einen Ringhomomorphismus $\Phi : R^M \longrightarrow R'$. Ist nun $\Phi' : R^M \longrightarrow R'$ irgendein Ringhomomorphismus mit $\Phi'|_R = \varphi$ und $\Phi'(X^m) = \sigma(m)$ für alle $m \in M$, so folgt

$$\Phi'(\sum a_m X^m) = \sum \Phi'(a_m X^m) = \sum \Phi'(a_m)\Phi'(X^m) = \Phi(\sum a_m X^m)$$

und damit $\Phi = \Phi'$. $\square$

Das folgende Korollar zeigt, dass der Polynomring bis auf einen einzigen Isomorphismus durch seine universelle Eigenschaft eindeutig bestimmt ist. Insbesondere haben wir dadurch die Möglichkeit im Fall $M = \mathbb{N}_0^n$ den Polynomring R^M in n Unbestimmten $X_1, \ldots, X_n$ auch als Polynomring $\tilde{R}[X_n]$ in *einer* Unbestimmten über dem Ring $\tilde{R} := R[X_1, \ldots, X_{n-1}]$ zu interpretieren.

Korollar. *Sei S eine kommutative Ringerweiterung von R, und sei $\iota : M \longrightarrow S$ ein Morphismus. Der Ring S habe die universelle Eigenschaft:* Zu jedem Ringhomomomorphismus $\psi : R \longrightarrow R'$ und zu jedem Morphismus $\tau : M \longrightarrow R'$ gibt es genau einen Ringhomomorphismus $\Psi : S \longrightarrow R'$ mit $\Psi|_R = \psi$ und $\Psi \circ \iota = \tau$. Dann gibt es genau einen Ringisomorphismus $\Phi : R^M \xrightarrow{\sim} S$ mit $\Phi|_R = \mathrm{id}$ und $\Phi(X^m) = \iota(m)$ für alle $m \in M$.

Beweis. Zur Inklusion $R \hookrightarrow S$ und zu $\iota : M \longrightarrow S$ gibt es nach dem Satz genau einen Ringhomomorphismus $\Phi : R^M \longrightarrow S$ mit $\Phi|_R = \mathrm{id}$ und $\Phi(X^m) = \iota(m)$ für alle $m \in M$. Wegen der universellen Eigenschaft von S gibt es zur Inklusion $R \hookrightarrow R^M$ und zum Morphismus $M \longrightarrow R^M$, $m \mapsto X^m$, genau einen Ringhomomorphismus $\Psi : S \longrightarrow R^M$ mit $\Psi|_R = \mathrm{id}$ und $\Psi(\iota(m)) = X^m$ für alle $m \in M$. Dann sind $\Phi \circ \Psi : S \longrightarrow S$ und die Identität $\mathrm{id}_S : S \longrightarrow S$ zwei Ringhomomorphismen, deren Einschränkung auf R jeweils die Identität ergibt und die beide $\iota(m)$ für jedes $m \in M$ festlassen. Nach Voraussetzung kann es aber nur einen solchen Ringhomomorphismus geben, und es folgt $\Phi \circ \Psi = \mathrm{id}_S$. Da $\Psi \circ \Phi : R^M \longrightarrow R^M$ und $\mathrm{id}_{R^M} : R^M \longrightarrow R^M$ zwei Ringhomomorphismen sind, deren Einschränkung auf R jeweils die Identität ergibt und die beide X^m für jedes $m \in M$ festlassen, folgt aus dem Satz, dass $\Psi \circ \Phi = \mathrm{id}_{R^M}$ gilt. $\square$

22 Index