Friedrich-Schiller-Universität Jena
Mathematisches Institut

Algebra 1
Wintersemester 2008/09

David J. Green
Stand: 12. Februar 2009

Inhaltsverzeichnis

1 Einleitung

Gruppen, Ringe, Körper.

- Ein Körper: die Skalare in einem Vektorraum. Additive Gruppe, kommutative Multiplikation, $1 \neq 0$, Existenz von Multiplikativen Inversen.

  Es gibt mehr Körper, als nur die – etwa $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_p$ – die man bereits kennt.

- Unlösbarkeit der klassischen Probleme:
  - Verdopplung des Würfels
  - Dreiteilung eines beliebigen Winkels
  - Quadratur des Kreises (vorausgesetzt: π transzendent)

- Galois-Theorie: Die Unlösbarkeit der quintischen Gleichung durch Radikale. Die Galois-Korrespondenz zwischen Körpern und Gruppen. Die Galoisgruppe eines Polynoms, etwa S_5 für $x^5 - 80x + 5$.

- Noch ein Beweis des Fundamentalsatzes der Algebra.

- Ein kleines bisschen Zahlentheorie (faktorielle Ringe).

Mehr zu Galoistheorie

- Quadratische Gleichung $x^2 + px + q = 0$. Substituiere $y = x + \frac{p}{2}$, also $y^2 = x^2 + px + \frac{p^2}{4}$, also $y^2 = \frac{p^2}{4} - q$, daher $y = \pm\sqrt{\frac{p^2}{4} - q}$ und $x = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}$.

  Zutaten für die Lösung: p, q und die Wurzel-Funktion.

- Kubische Gleichung $x^3 + ax^2 + bx + c = 0$: hier gibt es auch eine – allerdings deutlich kompliziertere – Lösungsformel. Zutaten: $a, b, c, \sqrt{}, \sqrt[3]{}$. Man sagt: jede kubische Gleichung ist durch Radikale lösbar.

- Auch für die allgemeine quartische Gleichung $x^4 + ax^3 + bx^2 + cx + d = 0$ gibt es eine (sehr komplizierte) Lösungsformel mit Radikale $\sqrt{}$, $\sqrt[3]{}$.

- Bei der quintischen Gleichung $x^5 + ax^4 + bx^3 + cx^2 + dx + e = 0$ sieht es anders aus. Es gibt keine allgemeine Lösungsformel durch Radikale, also keine Formel, die sich aus den Zutaten $a, b, c, d, e, \sqrt{}, \sqrt[3]{}, \sqrt[5]{}, \ldots$ zusammensetzt (Abel 1824; Ruffini 1799, mit Lücken).

  E. Galois (1832): Erkennungsprinzip, ob eine *gegebene* quintische Gleichung durch Radikale lösbar ist.

  Beispiele $x^5 - 5x^3 + 4x = 0$ lösbar durch Radikale: die Lösungen sind $0, \pm 1, \pm 2$. Dagegen lässt sich keine Lösung von $x^5 - 80x + 5 = 0$ durch Radikale ausdrücken.

Der Zugang von Galois

Es geht darum, welche Permutationen der Lösungen zulässig sind.

Fundamentalsatz der Algebra: die beiden quintischen Polynome oben haben je fünf Nullstellen in $\mathbb{C}$ (gezählt mit Vielfachheit).

Bemerkung Analysis: α ist eine *wiederholte* Nullstelle des Polynoms f genau dann wenn $\mathrm{ggT}(f, f') \neq 1$ ist.

Hat das Polynom f lauter reelle Koeffizienten, und ist $z \in \mathbb{C}$ eine Nullstelle von f, so ist auch $\bar{z}$ eine Nullstelle. Also operiert die komplexe Konjugation als eine Permutation der Menge der Nullstellen.

Um zu prüfen, wieviele Nullstellen von der komplexen Konjugation verändert werden, macht man eine Kurvendiskussion[1], um die Anzahl der reellen Nullstellen zu bestimmen.

Manchmal kann man auch andere Permutationen der Nullstellen durch sogenannten *Körperautomorphismen* bewirken. Die *Galoisgruppe* des Polynoms ist die Gruppe aller solchen Polynome.

Beispiele Für $f = X^2 - 1 = (X - 1)(X + 1)$ mit Nullstellen ± 1 sind keine nichttriviale Permutationen erlaubt: Automorphismen dürfen nichts in $\mathbb{Q}$ verändern.

Dagegen bei $f = (X^2 + 1)(X^2 + 4)$ bewirkt die komplexe Konjugation die Permutation $i \leftrightarrow -i$, $2i \leftrightarrow -2i$. Es gibt aber keinen Automorphismus mit $i \mapsto 2i$, denn i ist Nullstelle von $X^2 + 1$, $2i$ dagegen nicht.

$f(x) = x^5 - 80x + 5$ hat genau drei reelle Nullstellen (Kurvendiskussion), also operiert die komplexe Konjugation als eine *Transposition*: zwei Nullstellen werden miteinander vertauscht, die anderen bleiben unverändert. Da das Polynom außerdem *irreduzibel* ist, und sein Grad eine Primzahl ist, werden wir in §9.6 folgern, dass die Galoisgruppe die volle symmetrische Gruppe S_5 ist. Da die Gruppe S_5 nicht *auflösbar* ist, ist dieses Polynom also nicht durch Radikale lösbar.

Wie man eine kubische Polynom löst

Durch den Variablenwechsel $y = x + \frac{a}{3}$ reduziert man die kubische Gleichung $x^3 + ax^2 + bx + c = 0$ auf dem Fall $a = 0$, also beschäftigen wir uns mit der Gleichung

$$x^3 - px + q = 0\,.$$

Seien $\alpha, \beta, \gamma \in \mathbb{C}$ die drei Nullstellen. Setzen wir

$$\Delta = (\beta - \alpha)(\gamma - \beta)(\gamma - \alpha) \qquad\qquad D = \Delta^2\,.$$

[1] Kann durchaus in der mündlichen Prüfung vorkommen!

Dann ist die *Diskriminante* D symmetrisch in α, β, γ, d.h. jede Permutation der drei Nullstellen lässt D unverändert. Aus dem Hauptsatz der Galoistheorie – die sogenannte Galoiskorrespondenz – folgt, dass D sich durch p, q auszudrücken sein muss. Im Anhang §A.5 zeigen wir: es ist

$$D = 4p^3 - 27q^2 \,.$$

Somit können wir $\Delta = \pm\sqrt{D}$ berechnen.

Sei $\omega = \exp\left(\frac{2\pi i}{3}\right) = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Dann ist ω eine kubische Einheitswurzel; $\omega^2 = \bar{\omega}$; und $\omega + om\bar{e}ga = -1$. Es ist

$$\begin{aligned} 2(\alpha - \omega\beta)^3 &= (2\alpha^3 + 3\alpha^2\beta - 3\alpha\beta^2 - 2\beta^3) - 3i\sqrt{3}(\alpha^2\beta + \alpha\beta^2) \\ &= \Delta - 3i\sqrt{3}q \,. \end{aligned}$$

Also $\alpha - \omega\beta = \sqrt[3]{\frac{\Delta - 3i\sqrt{3}q}{2}}$. Analog kann man $\alpha - \omega^2\beta$ berechnen – Vorsicht aber bei der Wahl der kubischen Wurzel, es muss $(\alpha - \omega\beta)(\alpha - \omega^2\beta) = p$ gelten. Dann kann man α, β berechnen.

Hier sieht $\alpha - \omega\beta$ etwas aus der Luft gegriffen. Mehr zur sogenannten Lagrange-Resolvente im §11.1.

Weitere Themen

- Der Hauptsatz der Galoistheorie ist die *Galoiskorrespondenz* zwischen Körpern und Gruppen.

  Hier vielleicht das Bild der Zwischenkörper für $X^3 - 2$?

- $x^3 - 2 = 0$ hat genau eine reelle Nullstelle $\sqrt[3]{2}$. Die weiteren Nullstellen lassen sich also nicht durch rationale Zahlen und $\sqrt[3]{2}$ ausdrücken.

- Sei $\theta \in \mathbb{C}$ eine Nullstelle von $f(x) = x^3 - 3x + 1$. Dann ist auch $\theta^2 - 2$ eine Nullstelle.

  Beachten Sie: wäre $\theta = \theta^2 - 2$, dann $\theta \in \{2, -1\}$. Keine dieser beiden Werte ist eine Nullstelle von f.

- In $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ hat 6 zwei verschiedene vollständige Faktorisierungen:

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

  Nachweis der Vollständigkeit und der Inäquivalenz mittels der Norm $N(a + b\sqrt{-5}) = a^2 + 5b^2$, multiplikativ.

- Sei $\alpha = \sqrt{2} + \sqrt{3}$. Dann $(\alpha - \sqrt{2})^2 = 3$, also $2\sqrt{2}\alpha = \alpha^2 - 1$, also

  $$\alpha^4 - 10\alpha^2 + 1 = 0 \,.$$

  Man sagt, dass $\sqrt{2} + \sqrt{3}$ eine *algebraische Zahl* ist, denn Nullstelle eines Polynoms.

2 Gruppentheorie

2.1 Gruppen

Definition Eine *Gruppe* G besteht aus einer Menge G und einer Abbildung $\mu\colon G \times G \to G$, $(g,h) \mapsto gh$, die folgende Axiome erfüllt:

(G1) Assoziativität: $(gh)k = g(hk)$ für alle $g, h, k \in G$;

(G2) Neutrales Element: Es gibt ein $e \in G$ mit: $\forall g \in G \quad eg = ge = g$;

(G3) Existenz von Inversen: Zu jedem $g \in G$ gibt es ein $g' \in G$ mit $gg' = g'g = e$.

Gilt $gh = hg$ für alle $g, h \in G$, so heißt G *abelsch*.

Bezeichnung Die *Gruppenordnung* $|G|$ ist die Anzahl der Elemente der Gruppe. Meistens schreibt man x^{-1} statt x'; manchmal schreibt man 1 statt e. Bei manchen abelschen Gruppen schreibt man $g + h$ statt gh; dementsprechend schreibt man dann 0 für e, und $-g$ für g'. Eine solche Gruppe nennt man eine *additive* Gruppe.

Bemerkung Man zeigt (vgl. Übungsserie Nr. 1), dass das neutrale Element und die Inversen *eindeutig* definiert sind.

Beispiele

a) $\mathbb{Z}$ ist eine additive Gruppe; jeder Körper ist eine Gruppe bzgl. Addition, jeder Vektorraum auch.

b) Ist k ein Körper, so ist $k^* := k \setminus \{0\}$ eine abelsche Gruppe bzgl. Multiplikation. Beispiele: $\mathbb{C}^*, \mathbb{R}^*$.

c) Auch der Einheitskreis $S^1 := \{z \in \mathbb{C} \mid |z| = 1\}$ ist eine abelsche Gruppe bzgl. Multiplikation.

d) Für $n \geq 2$ ist $C_n := \{\exp\left(\frac{2\pi i r}{n}\right) \mid 0 \leq r \leq n-1\}$ eine endliche abelsche Gruppe, mit $|G| = n$. Insbesondere ist $C_2 = \{+1, -1\}$. Die Gruppenoperation ist Multiplikation.

e) Für $n \geq 3$ ist die Isometriegruppe (Symmetriegruppe) des regulären n-Ecks eine nichtabelsche Gruppe bzgl. Verknüpfung: die Diedergruppe D_n.

   Beispiel D_4: ρ = Drehung durch $\frac{\pi}{2}$; σ = Spiegelung in die x-Achse. Dann $\rho\sigma \neq \sigma\rho$. Es ist $|D_4| = 8$ und $D_4 = \{\mathrm{Id}, \rho, \rho^2, \rho^3, \sigma, \rho\sigma, \rho^2\sigma, \rho^3\sigma\}$.

f) Sei k ein Körper und $n \geq 1$. Die allgemeine lineare Gruppe $GL_n(k)$ besteht aus den invertierbaren $(n \times n)$-Matrizen mit Einträgen aus k, bzgl. Matrixmultiplikation. Nichtabelsch für $n \geq 2$.

g) Zahlreiche weitere Matrixgruppen, darunter die speziell lineare Gruppe $SL_n(k) := \{A \in GL_n(k) \mid \det(A) = 1\}$, die orthogonale Gruppe $O(n) = \{A \in GL_n(\mathbb{R}) \mid A^T = A^{-1}\}$, die unitäre Gruppe $U(n) = \{A \in GL_n(\mathbb{C}) \mid \overline{A^T} = A^{-1}\}$, die speziell orthogonale Gruppe $SO(n) := SL_n(\mathbb{R}) \cap O(n)$, und die speziell unitäre Gruppe $SU(n) := SL_n(\mathbb{C}) \cap U(n)$.

h) Die symmetrische Gruppe $S(X)$ aller Permutationen der Menge X, inbesondere $S_n = S(\{1, 2, \ldots, n\})$. Operation: Verknüpfung $\sigma\tau(x) = \sigma(\tau(x))$. Es ist $|S_n| = n!$. Zwei Schreibweisen für Permutationen:

   i) $\sigma \in S_n$ als $\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$ schreiben.

   ii) Die *Zerlegung in disjunkten Zykeln* sagt mehr über die Permutation aus. Ist $r \geq 2$ und sind $a_1, \ldots, a_r \in X$ paarweise verschieden, so heißt die Permutation σ gegeben durch „$\sigma(a_i) = a_{i+1}$, $\sigma(a_r) = a_1$ und $\sigma(x) = x$ sonst“ der *r-Zykel* $(a_1\ a_2\ \ldots\ a_n)$. Jede Permutation lässt sich als Produkt von disjunkten Zykeln schreiben[2], diese Zerlegung ist im wesentlichen eindeutig.

   Beispiele: $(1\ 2\ 4) = (2\ 4\ 1) = (4\ 1\ 2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$.

   $(1\ 2\ 5)(3\ 4\ 6)$ disjunkt
   $(1\ 2\ 5)(3\ 4\ 5)$ nicht disjunkt, $= (1\ 2\ 5\ 3\ 4)$.

i) $\mathbb{Z}/n\mathbb{Z}$ für $n \geq 2$: die Restklassen der ganzen Zahlen modulo n. Es ist $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], [2], \ldots, [n-1]\} = \{[r] \mid r \in \mathbb{Z}\}$, wobei $[r]$ die Äquivalenzklasse von r bzgl. der Relation „$r \sim s \Leftrightarrow n$ teilt $s - r$“ ist. Additive Gruppe: $[r] + [s] = [r + s]$. Man rechnet nach, dass diese Addition repräsentantenunabhängig und somit wohldefiniert ist.

2.2 Untergruppen

Definition Sei G eine Gruppe und $H \subseteq G$ eine Teilmenge. Man nennt H eine *Untergruppe* von G, falls H selbst eine Gruppe ist, und zwar bezüglich der gleichen Multiplikation wie G. Bezeichnung: $H \leq G$.

Beispiele $C_n \leq S^1 \leq \mathbb{C}^*$; $\mathbb{C}^* \not\leq \mathbb{C}$.

Hilfslemma Sei G eine Gruppe und $H \subseteq G$ eine Teilmenge. Genau dann ist $H \leq G$, wenn gilt: $H \neq \emptyset$, und für alle $h, k \in H$ ist $h \cdot k^{-1} \in H$.

Beweis. Jede Untergruppe hat diese Eigenschaften. Hat umgekehrt H diese Eigenschaften, so gibt es ein $h \in H$, weshalb $e = hh^{-1} \in H$. Für jedes $h \in H$ ist dann $h^{-1} = eh^{-1} \in H$, also für alles $h, k \in H$ ist $hk = h(k^{-1})^{-1} \in H$. ∎

[2]Vorausgesetzt, die Menge X ist endlich.

2.3 Erzeuger und zyklische Gruppen

Lemma 2.1 *Sei G eine Gruppe.*

a) Sei $(H_i)_{i\in I}$ eine nichtleere Familie von Untergruppen von G; dann ist auch die Schnittmenge $H := \bigcap_{i\in I} H_i$ eine Untergruppe.

b) Sei $X \subseteq G$ eine Teilmenge. Dann gilt

$$\bigcap\{H \leq G \mid X \subseteq H\} = \{x_1^{n_1} x_2^{n_2} \cdots x_r^{n_r} \mid r \geq 0,\, x_i \in X,\, n_i \in \mathbb{Z}\}\,. \qquad (*)$$

Diese Untergruppe heißt $\langle X\rangle$, die durch X erzeugte *Untergruppe von G. Sie ist die kleinste Untergruppe, die die Menge X enthält.*

Beweis. a) Man wendet das Hilfslemma an.

b) Eine Untergruppe enthält X immer, nämlich G selber. Nach dem ersten Teil ist die linke Seite von (*) eine Untergruppe. Nach Konstruktion ist dies die kleinste Untergruppe, die X enthält. Die rechte Seite wiederum enthält X (Fall $r = n_1 = 1$) und ist nach Konstruktion in jeder Untergruppe enthalten, die X enthält. Es reicht also zu zeigen, dass die rechte Seite eine Untergruppe ist. Sie enthält e (Fall $r = 0$); und für Elemente $h = x_1^{n_1} \cdots x_r^{n_r}$, $k = y_1^{m_1} \cdots y_s^{m_s}$ der rechten Seite ist $hk^{-1} = x_1^{n_1} \cdots x_r^{n_r} y_s^{-m_s} \cdots y_1^{-m_1}$, was auch zur rechten Seite gehört. ∎

Beispiele Wegen $D_4 = \{\mathrm{Id}, \rho, \rho^2, \rho^3, \sigma, \rho\sigma, \rho^2\sigma, \rho^3\sigma\}$ wird D_4 von ρ, σ erzeugt. Es ist $\mathbb{Z}/3\mathbb{Z} = \{[0], [1], [1]+[1]\}$, daher ist $\mathbb{Z}/3\mathbb{Z} = \langle[1]\rangle$. Es ist $\mathbb{Z} = \langle 1\rangle \neq \langle 2\rangle$, denn $3 \neq \langle 2\rangle$.

Bezeichnung Eine Gruppe G heißt *zyklisch*, wenn es ein $g \in G$ gibt mit $G = \langle G\rangle$. Die Gruppen $\mathbb{Z}, C_n, \mathbb{Z}/n\mathbb{Z}$ sind zyklisch, die Gruppe D_4 dagegen nicht.

Beispiel Es ist $S_3 = \langle(1\ 2), (1\ 3)\rangle$, denn

$$\begin{aligned} S_3 &= \{\mathrm{Id}, (1\ 2), (1\ 3), (1\ 2\ 3), (1\ 3\ 2), (2\ 3)\} \\ &= \{\mathrm{Id}, (1\ 2), (1\ 3), (1\ 3)(1\ 2), (1\ 2)(1\ 3), (1\ 2)(1\ 3)(1\ 2)\}\,. \end{aligned}$$

Dies kann man aber auch mit dem Satz von Lagrange zeigen.

2.4 Nebenklassen und der Satz von Lagrange

Lemma 2.2 *Es sei $H \leq G$.*

a) Die Relation $\sim$ auf G gegeben durch „$x \sim y \;\Leftrightarrow\; \exists h \in H\ y = xh$“ ist eine Äquivalenzrelation.

Bezeichnung*: Die Äquivalenzklasse von $g \in G$ ist die Menge $gH = \{gh \mid h \in H\}$, die* Linksnebenklasse *von g.*

b) Alle Äquivalenzklassen sind gleich groß: $|gH| = |H|$.

Beweis. a) Reflexiv: $xe = x$; symmetrisch: $y = xh \Leftrightarrow x = yh^{-1}$; transitiv: ist $y = xh_1$ und $z = yh_2$, dann $z = xh_1h_2$.

b) Folgt aus dem ersten Teil. ∎

Bezeichnung Die Menge der Linksnebenklassen ist $G/H := \{gH \mid g \in G\}$. Der *Index* $|G : H|$ von H in G ist deren Anzahl $|G : H| := |G/H|$.

Beispiel Es gibt auch *Rechtsnebenklassen* $Hg = \{hg \mid h \in H\}$. Für $G = S_3$, $g = (1\ 2)$ und $H = \langle(1\ 3)\rangle = \{\mathrm{Id}, (1\ 3)\}$ ist $gH = \{(1\ 2), (1\ 3\ 2)\}$ und $Hg = \{(1\ 2), (1\ 2\ 3)\}$, also $gH \neq Hg$.

Der Satz von Lagrange *Sei G eine endliche Gruppe und $H \leq G$ eine Untergruppe. Dann gilt $|G : H| \cdot |H| = |G|$. Insbesondere ist $|G|$ durch $|H|$ teilbar.*

Beweis. G ist die disjunkte Vereinigung von $|G : H|$ Nebenklassen. Jede Nebenklasse enthält $|H|$ Elemente. ∎

Beispiele Sei H eine Untergruppe des S_4. Wegen $|S_4| = 24$ besagt Lagrange, dass $|H|$ ein Element der Liste $1, 2, 3, 4, 6, 8, 12, 24$ ist. Man kann nachweisen, dass jede Ordnung vorkommt: so hat etwa $\langle(1\ 2\ 3\ 4), (1\ 4)(2\ 3)\rangle$ die Ordnung 8.

Natürlich ist 120 durch 15 teilbar, trotzdem kann man zeigen, dass S_5 keine Untergruppe der Ordnung 15 hat.

2.5 Die Ordnung eines Gruppenelements

Definition Sei G eine Gruppe und $g \in G$. Die *Ordnung* $o(g)$ des Elements g ist per Definition die Ordnung der zyklischen Untergruppe $\langle g\rangle$:

$$o(g) = |\langle g\rangle| \ .$$

Beispiel Es ist $\langle(1\ 2\ 3)\rangle = \{\mathrm{Id}, (1\ 2\ 3), (1\ 3\ 2)\}$. Somit hat $(1\ 2\ 3)$ die Ordnung 3. Allgemeiner hat ein r-Zykel die Ordnung r.

Lemma 2.3 *a) Ist $g \in G$ ein Element der Ordnung n, so ist $n \mid |G|$ und $\langle g\rangle = \{e, g, g^2, \ldots, g^{n-1}\}$. Es ist $o(g) =$ das kleinste $r \geq 1$ mit $g^r = e$.*

b) Eine endliche Gruppe G der Ordnung n ist genau dann zyklisch, wenn es ein $g \in G$ gibt mit $o(g) = n$.

c) Ist p eine Primzahl, so ist jede Gruppe der Ordnung p zyklisch.

Beweis. a) Wegen Lagrange ist $n \mid |G|$. Sei $r \geq 1$ die kleinste Zahl derart, dass die Liste $e, g, g^2, \ldots, g^r$ eine Wiederholung enthält: $g^r = g^s$ für ein $0 \leq s < r$. Multipliziert man mit g^{r-s}, so erhält man $e = g^{r-s}$ und deshalb $s = 0$: es ist $g^r = e$ die erste Wiederholung. Dann ist aber $g^{-1} = g^{r-1}$, weshalb $\{e, g, \ldots, g^{r-1}\}$ eine Untergruppe von G ist, die kleinste Untergruppe, die g enthält. Also $r = n$ und $\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}$.

b) Folgt aus dem ersten Teil.

c) Sei $|G| = p$ und $g \in G$ mit $g \neq e$. Nach dem ersten Teil ist $o(g) = 1$ oder p; und $o(g) \neq 1$ wegen $g \neq e$. Also $o(g) = p$ und $G = \langle g \rangle$. ∎

Beispiel Es ist $|S_3| = 6$. Sei $K = \langle (1\ 2) \rangle$ und $H = \langle (1\ 2), (1\ 3) \rangle$. Es ist $|K| = o(1\ 2) = 2$. Nach Lagrange gilt $2 \mid |H| \mid 6$. Wegen $(1\ 3) \notin K$ ist $|H| \neq 2$. Übrig bleibt nur $|H| = 6$, also $H = S_3$.

2.6 Homomorphismen

Definition Seien G, H Gruppen. Eine Abbildung $f\colon G \to H$ heißt ein *Homomorphismus*, falls $f(g_1 g_2) = f(g_1) f(g_2)$ gilt für alle $g_1, g_2 \in G$. Hieraus folgen $f(e_G) = e_H$ und $f(g^{-1}) = f(g)^{-1}$.

Beispiele a) $f\colon (\mathbb{C}, +) \to (\mathbb{C}^*, \cdot)$, $z \mapsto \exp(2\pi i z)$.

b) $f\colon GL_n(k) \to k^*$, $A \mapsto \det(A)$.

c) $f\colon (\mathbb{Z}, +) \to (C_n, \cdot)$, $r \mapsto \exp\left(\frac{2\pi i r}{n}\right)$.

d) Ist G eine beliebige Gruppe, so ist die Identitätsabbildung $\mathrm{Id}\colon G \to G$, $g \mapsto g$ ein Homomorphismus. Sind $f\colon G \to H$ und $g\colon H \to K$ Homomorphismen, so ist auch $g \circ f\colon G \to K$ ein Homomorphismus.

e) Die Signatur einer Permutation $\varepsilon\colon S_n \to \{1, -1\}$. Bekannt aus der LAAG1. Wiederholung im Anhang §A.1.

Hilfslemma Ist $f\colon G \to H$ ein bijektiver Homomorphismus, so ist auch die Umkehrabbildung $f^{-1}\colon H \to G$ ein Homomorphismus.

Bezeichnung Ein bijektiver Homomorphismus heißt ein *Isomorphismus*. Gibt es einen Isomorphismus $f\colon G \to H$, so heißen die Gruppen G, H *isomorph*. Isomorphie ist eine Äquivalenzrelation.

Beispiel C_n und $\mathbb{Z}/n\mathbb{Z}$ sind isomorph. Ein Isomorphismus $f\colon \mathbb{Z}/n\mathbb{Z} \to C_n$ ist $f([r]) = \exp\left(\frac{2\pi i r}{n}\right)$.

2.7 Kern und Bild

Definition Sei $f\colon G \to H$. Man setzt

$$\mathrm{Bild}(f) = \{f(g) \mid g \in G\} \subseteq H \qquad \mathrm{Kern}(f) = \{g \in G \mid f(g) = e_H\}\,.$$

Lemma 2.4 *a) Es ist* $\mathrm{Bild}(f) \leq H$ *und* $\mathrm{Kern}(f) \leq G$.

b) Ferner gilt: ist $g \in G$ *und* $k \in \mathrm{Kern}(f)$, *dann auch* $gkg^{-1} \in \mathrm{Kern}(f)$.

c) Die Abbildung f *ist genau dann injektiv, wenn* $\mathrm{Kern}(f) = \{e_G\}$ *gilt.*

Beweis. a) f Homomorphismus, also $e_H = f(e_G)$, und $f(g_1)f(g_2)^{-1} = f(g_1 g_2^{-1}) \in \mathrm{Bild}(f)$. Also $\mathrm{Bild}(f) \leq H$. Es ist $e_G \in \mathrm{Kern}(f)$, und sind $g_1, g_2 \in \mathrm{Kern}(f)$ dann $f(g_1 g_2^{-1}) = f(g_1)f(g_2)^{-1} = e_H$. Also $\mathrm{Kern}(f) \leq G$.

b) $f(gkg^{-1}) = f(g)f(k)f(g)^{-1} = f(g)f(g)^{-1} = e_H$.

c) Ist $f(g) = f(g')$, dann $f(g^{-1}g') = e_H$, also $g = g'$. ∎

2.8 Normalteiler

In der Lineare Algebra ist jeder Unterraum der Kern einer geeigneten linearen Abbildung. In der Gruppentheorie dagegen, gibt es wegen Lemma 2.4 b) Untergruppen, die nicht Kerne sind. Etwa $\{\mathrm{Id}, (1\ 2)\} \leq S_3$, denn $(1\ 3)(1\ 2)(1\ 3)^{-1} = (2\ 3)$.

Definition Sei G eine Gruppe und $H \leq G$. Gilt $ghg^{-1} \in H$ für alle $g \in G$ und $h \in H$, so heißt H ein *Normalteiler* von G, Bezeichnung $H \lhd G$.

Beispiele Lemma 2.4 b) besagt also $\mathrm{Kern}(f) \lhd G$. Es ist $\{\mathrm{Id}, (1\ 2)\} \not\lhd S_3$. Ist G abelsch, so ist jede Untergruppe normal. Es ist $SL_n(k) \lhd GL_n(k)$.

Hilfslemma Sei G eine Gruppe und $H \leq G$. Die folgenden Aussagen sind äquivalent:

a) Für jedes $g \in G$ ist $gH = Hg$.

b) Für jedes $g \in G$ ist $gHg^{-1} = H$, wobei $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$.

c) $H \lhd G$.

Beweis. c) besagt $gHg^{-1} \subseteq H$ für jedes $g \in G$. a) $\Leftrightarrow$ b): multipliziert man $gH = Hg$ von rechts mit g^{-1}, so erhält man $gHg^{-1} = H$. b) $\Rightarrow$ c) ist klar. c) $\Rightarrow$ b): Da $g^{-1} \in G$ ist, ist auch $g^{-1}H(g^{-1})^{-1} \subseteq H$ für alle g, d.h. $g^{-1}Hg \subseteq H$. Also $g(g^{-1}Hg)g^{-1} \subseteq gHg^{-1}$, d.h. $(gg^{-1})H(gg^{-1}) \subseteq gHg^{-1}$, d.h. $H \subseteq gHg^{-1}$. ∎

2.9 Die Quotientengruppe

Satz 2.5 *Sei $H \lhd G$ ein Normalteiler. Mit der Multiplikation $g_1H \cdot g_2H := g_1g_2H$ wird die Menge G/H der Linksnebenklassen zu einer Gruppe, die* Quotientengruppe *G/H. Es ist $|G/H| = |G : H| = \frac{|G|}{|H|}$. Ferner ist die kanonische Projektion $p\colon G \to G/H$, $g \mapsto gH$ ein surjektiver Gruppenhomomorphismus mit Kern H.*

Beweis. Multiplikation repräsentantenunabhängig: Seien $g_1, g_1', g_2, g_2' \in G$ mit $g_1H = g_1'H$ und $g_2 = g_2'H$. Zu zeigen ist $g_1'H \cdot g_2'H = g_1H \cdot g_2H$, d.h. $g_1'g_2'H = g_1g_2H$. Wegen $g_1H = g_1'H$ und $g_2 = g_2'H$ gibt es $h_1, h_2 \in H$ mit $g_1' = g_1h_1$ und $g_2' = g_2h_2$. Also $g_1'g_2' = g_1h_1g_2h_2$. Wir wollen h_1, g_2 miteinander vertauschen. Es ist $h_1g_2 \in Hg_2$. Da $H \lhd G$ ist, ist $Hg_2 = g_2H$. Also gibt es ein $h' \in H$ mit $h_1g_2 = g_2h'$. Also $g_1'g_2' = g_1g_2h'h_2$ und deshalb $g_1'g_2'H = g_1g_2H$.

Die Multiplikation ist also wohldefiniert. Die Gruppenaxiome folgen jetzt, da sie bereits in G gelten. Die Aussage zur Ordnung $|G/H|$ folgt aus dem Satz von Lagrange. Die Abbildung p ist offensichtlich surjektiv; ein Homomorphismus ist sie, da $p(g_1g_2) = g_1g_2H = g_1Hg_2H = p(g_1)p(g_2)$ ist; und der Kern ist H denn $p(g) = eH$ genau dann wenn $gH = eH$, d.h. $g \in H$ ist. ∎

Beispiel Die zyklische Gruppe $\mathbb{Z}/n\mathbb{Z}$ ist per Konstruktion eine Quotientengruppe; wir schrieben $[r]$ für $r + n\mathbb{Z}$.

Warnbeispiel Sei $H \leq S_3$ die Untergruppe $\langle(1\ 2)\rangle = \{\mathrm{Id}, (1\ 2)\}$. Dann $(1\ 3)H \cdot (2\ 3)H = (1\ 3)(2\ 3)H = (1\ 3\ 2)H = \{(2\ 3), (1\ 3\ 2)\}$. Aber $(1\ 3)H = \{(1\ 3), (1\ 2\ 3)\} = (1\ 2\ 3)H$, und $(1\ 2\ 3)H \cdot (2\ 3)H = (1\ 2\ 3)(2\ 3)H = (1\ 2)H = \{\mathrm{Id}, (1\ 2)\}$. Ist $H \not\lhd G$, so ist die Multiplikation auf G/H nicht wohldefiniert.

2.10 Die Isomorphiesätze

Der Homomorphiesatz ist der richtige Weg, Quotientengruppen zu verstehen.

Der Homomorphiesatz *Ein Gruppenhomomorphismus $f\colon G \to H$ induziert einen Isomorphismus $\bar{f}\colon G/\operatorname{Kern}(f) \to \operatorname{Bild}(f)$. Insbesondere gilt: ist f surjektiv, so ist die Quotientengruppe $G/\operatorname{Kern}(f)$ isomorph zu H.*

Beweis. Setzen wir $K := \operatorname{Kern}(f)$. Nach Lemma 2.4 ist $\operatorname{Bild}(f) \leq H$ und $K \lhd G$. Nach Satz 2.5 existiert die Quotientengruppe G/K. Definieren wir $\bar{f}\colon G/K \mapsto \operatorname{Bild}(f)$ durch $\bar{f}(gK) := f(g)$. Ist $gK = g'K$, so gibt es $k \in K$ mit $g' = gk$. Also $f(g') = f(g)f(k) = f(g)$, denn $K = \operatorname{Kern}(f)$. Somit ist $\bar{f}(gK) = \bar{f}(g'K)$, d.h. $\bar{f}$ ist wohldefiniert. Ferner ist $\bar{f}$ ein Homomorphismus, denn

$$\bar{f}(gK \cdot g'K) = \bar{f}(gg'K) = f(gg') = f(g)f(g') = \bar{f}(gK)\bar{f}(g'K)\,.$$

Für jedes $h = f(g)$ aus $\operatorname{Bild}(f)$ ist $h = \bar{f}(gK)$, somit ist $\bar{f}$ surjektiv. Ist $\bar{f}(gK) = e_H$, dann $f(g) = e_H$, also $g \in \operatorname{Kern}(f)$ und $gK = eK$. Somit ist $\bar{f}$ auch injektiv und somit ein Isomorphismus. ∎

Beispiele Für $n \geq 2$ ist die Signatur $\varepsilon\colon S_n \to C_2 = \{1, -1\}$ surjektiv. Der Kern ist die *alternierende Gruppe* A_n, daher ist $S_n/A_n \cong C_2$.

Die Determinante ist ein surjektiver Homomorphismus $GL_n(k) \to k^*$, und der Kern ist $SL_n(k)$. Somit ist $GL_n(k)/SL_n(k) \cong k^*$.

Der 1. Isomorphiesatz *Sei G eine Gruppe, $H \leq G$ eine Untergruppe und $K \lhd G$ ein Normalteiler. Dann ist $HK := \{hk \mid h \in H, k \in K\}$ eine Untergruppe von G, $H \cap K$ ist ein Normalteiler von H, und es gibt einen Isomorphismus $HK/K \cong H/(H \cap K)$.*

Beweis. HK eine Untergruppe: $e = ee \in HK$; $(hk)(h'k')^{-1} = (hh'^{-1})k'' \in HK$ für $k'' = h'(kk'^{-1})h'^{-1} \in K$, da $K \lhd G$. Es ist $K \leq HK$, also $K \lhd HK$. Für $h \in H$ ist $h(H \cap K)h^{-1}$ eine Teilmenge von H, da $H \cap K \subseteq H$; und $h(H \cap K)h^{-1}$ eine Teilmenge von K, da $H \cap K \subseteq K$ und $K \lhd G$. Also $H \cap K \lhd G$.

Betrachten wir nun die Abbildung $f\colon H \to HK/K$, gegeben durch $f(h) = hK$. Dies ist ein Homomorphismus. Es ist surjektiv: $hkK = f(h)$. Der Kern von f ist $H \cap K$, denn $hK = eK$ genau dann, wenn $h \in K$. Nach dem Homomorphiesatz also ist $H/(H \cap K)$ isomorph zu HK/K. ∎

Beispiel Sei $G = S_4$; sei $H = \{\sigma \in S_4 \mid \sigma(4) = 4\}$, eine Kopie von S_3; und sei $K = \{\mathrm{Id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \leq S_4$. Wegen

$$\sigma \cdot (a\,b)(c\,d) \cdot \sigma^{-1} = (\sigma(a)\,\sigma(b))(\sigma(c)\,\sigma(d))$$

ist $K \lhd S_4$. Offensichtlich ist $K \cap H = \{\mathrm{Id}\}$. Nach dem 1. Isomorphiesatz also ist $HK \leq S_4$ und $HK/K \cong H/(H \cap K)$, d.h. $HK/K \cong S_3$. Also ist $|HK| = |K| \cdot |S_3|$ wegen Lagrange, d.h. $|HK| = 4 \cdot 6 = 24 = |S_4|$. Also $HK = S_4$, und $S_4/K \cong S_3$.

Der 2. Isomorphiesatz (Eine Kürzungsregel) *Sei G eine Gruppe und H, K zwei Normalteiler von G mit $K \subseteq H$. Dann $H/K \lhd G/K$, und es gibt einen Isomorphismus $(G/K)/(H/K) \cong G/H$.*

Beweis. Es ist $K \lhd H$. Da H/K selbst eine Gruppe ist bzgl. der gleichen Multiplikation wie G/K, ist $H/K \leq G/K$. Sei $f\colon G/K \to G/H$ die Abbildung $f(gK) = gH$. Dieses f ist wohldefiniert: ist $gK = g'K$ dann gibt es ein $k \in K$ mit $g' = gk$. Da $K \subseteq H$ ist, ist $k \in H$, also $g'H = gH$. Ferner ist f ein Homomorphismus: $f(g_1Kg_2K) = f(g_1g_2K) = g_1g_2H = g_1Hg_2H = f(g_1K)f(g_2K)$. Außerdem ist f surjektiv, denn $gH = f(gK)$. Schließlich ist $\mathrm{Kern}(f) = H/K$, denn $gH = eH$ genau dann, wenn $g \in H$ ist, d.h. wenn $gK \in H/K$ ist. Die Behauptung folgt aus dem homomorphiesatz. ∎

3 Ringe und Ideale

3.1 Ringe

Definition Ein *Ring* besteht aus einer Menge R zusammen mit einer Addition $R \times R \to R$, $(r, s) \mapsto r + s$ und einer Multiplikation $R \times R$, $(r, s) \mapsto rs$, die die folgenden Axiomen erfüllen:

(R1) $(R, +)$ ist eine additive Gruppe, mit neutralem Element 0;

(R2) Die Multiplikation ist assoziativ: $(rs)t = r(st)$;

(R3) Distributivgesetze: $r(s + t) = rs + rt$ und $(r + s)t = rt + st$;

(R4) Neutrales Element $1 \in R$ mit $1 \cdot r = r \cdot 1$ für alle $r \in R$.

Gilt auch $rs = sr$ für alle $r, s \in R$, so heißt R ein *kommutativer* Ring.

Eine Abbildung $f\colon R \to S$ zwischen zwei Ringen heißt ein *Ringhomomorphismus*, falls $f(r + s) = f(r) + f(s)$, $f(rs) = f(r)f(s)$ und $f(1_R) = 1_S$ gelten.

Beispiele a) $\mathbb{Z}$, jeder Körper.

b) Sei R ein kommutativer Ring und $n \geq 1$. Der Ring $M_n(R)$ der $(n \times n)$-Matrizen mit Einträgen aus R. Die Determinante $\det\colon M_n(R) \to R$ ist ein Ringhomomorphismus.

c) Der Nullring $R = \{0\}$ mit $1 = 0$.

d) Die Quaternionen $\mathbb{H}$, siehe Anhang §A.3: nicht-kommutativ, erfüllen aber sonst alle Voraussetzungen für einen Körper.

e) $R = C^0(\mathbb{R})$: alle stetige Funktionen auf $\mathbb{R}$, mit Addition und Multiplikation punktweise, d.h. $(f + g)(x) = f(x) + g(x)$, $(fg)(x) = f(x)g(x)$.

f) Die *Gaußschen Zahlen* $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$.

g) $\mathbb{Z}/n\mathbb{Z}$ ist ein Ring, mit Multiplikation $[r] \cdot [s] = [rs]$ und Einselement $[1]$. Die Abbildung $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $r \mapsto [r]$ ist ein Ringhomomorphismus.

h) Die Abbildung $\mathbb{R} \to M_2(\mathbb{R})$, $x \mapsto \left(\begin{smallmatrix} x & 0 \\ 0 & 0 \end{smallmatrix}\right)$ ist additiv und multiplikativ, aber trotzdem kein Ringhomomorphismus, denn das Bild von 1 ist $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \neq E_2$.

i) **Polynomringe:** Sei R ein kommutativer Ring. Elemente des Polynomrings $R[X]$ über R in einem Unbestimmten X sind formale R-lineare Kombinationen $p = \sum_{i=0}^{n} r_i X^i$ mit $r_i \in R$. „Formal“ bedeutet, dass zwei solche Ausdrucke nur dann gleich sind, wenn alle Koeffizienten gleich sind. Addition und Multiplikation sind wie für Polynome üblich. Ist $r_n \neq 0$, so heißt n der *Grad* von p. Das Einselement ist 1 vom Grad 0.

Ist $a \in R$, so ist die Auswertung in $X = a$ ein Ringhomomorphismus $e_a \colon R[X] \to R$, $p \mapsto p(a) = \sum_{i=0}^{n} r_i a^i$.

j) Allgemeiner betrachtet man den Polynomring $R[X_1, \ldots, X_n]$. Dieser kann man induktiv als $R[X_1, \ldots, X_{n-1}][X_n]$ konstruieren. Sehen Sie aber auch Anhang §A.2.

3.2 Ideale: die Struktur des Kerns

Lemma 3.1 *Sei $f \colon R \to S$ ein Ringhomomorphismus. Dann ist* $\mathrm{Kern}(f)$ *eine Untergruppe der additiven Gruppe $(R, +)$. Ferner gilt: ist $r \in R$ und $k \in \mathrm{Kern}(f)$, dann $rk, kr \in \mathrm{Kern}(f)$.*

Außerdem gilt: $\mathrm{Bild}(f)$ *ist ein* Unterring *von S, d.h. selbst ein Ring, und die Inklusion in S ist ein Ringhomomorphismus.* ∎

Definition Sei R ein Ring. Eine Teilmenge $I \subseteq R$ heißt ein *Ideal* in R, Bezeichnung $I \lhd R$, falls I eine Untergruppe der additiven Gruppe $(R, +)$ ist, und außerdem $ri, ir \in I$ gilt für alle $r \in R$, $i \in I$. Ist R kommutativ, so reichen natürlich $I \leq R$ und $ri \in I$.

Beispiele $n\mathbb{Z} \lhd \mathbb{Z}$; $\{p \in \mathbb{Q}[X] \mid p(3) = p(-1) = 0\} \lhd \mathbb{Q}[X]$; $\{0\} \lhd R$, $R \lhd R$. Ist $I \lhd R$ und $I \neq R$, so heißt I ein *echtes* Ideal.

Lemma 3.2 *Ist I ein Ideal in R, so wird die Quotientengruppe zum* Quotientenring R/I *durch die Multiplikation $(r + I)(s + I) = rs + I$. Die kanonische Projektion $p \colon R \to R/I$, $r \mapsto r + I$ ist ein Ringhomomorphismus mit Kern I.*

Beweis. Ist $r' + I = r + I$ und $s' + I = s + I$, so gibt es $i, j \in I$ mit $r' = r + i$, $s' = s + j$. Dann

$$r's' = (r + i)(s + j) = rs + (rj + is + ij)\,,$$

und $rj + is + ij \in I$, also $r's' + I = rs + I$. Das heißt, die Multiplikation ist repräsentantenunabhängig. ∎

Bemerkung Das Ideal $I \lhd R$ ist genau dann echt, wenn $1 \notin R$ ist.

Isomorphiesätze für Ringe:

Homomorphiesatz *Ein Ringhomomorphismus $f \colon R \to S$ induziert einen Isomorphismus $\bar{f} \colon R/\mathrm{Kern}(f) \to \mathrm{Bild}(f)$. Insbesondere gilt: ist f surjektiv, so ist der Quotientenring $R/\mathrm{Kern}(f)$ isomorph zu S.*

1. Isomorphiesatz *Sei R ein Ring, $S \subseteq R$ ein Unterring und $I \lhd R$ ein Ideal. Dann ist $S + I := \{s + i \mid s \in S, i \in I\}$ ein Unterring von R, $S \cap I$ ist ein Ideal in S, und es gibt einen Ringisomorphismus $(S + I)/I \cong S/(S \cap I)$.*

2. Isomorphiesatz *Sei R ein Ring und I, J zwei Ideal in R mit $J \subseteq I$. Dann $I/J \lhd R/J$, und es gibt einen Ringisomorphismus $(R/J)/(I/J) \cong R/I$.*

Beweis. Homomorpiesatz: $\bar{f}(rr'+I) = f(rr') = f(r)f(r') = \bar{f}(r+I)\bar{f}(r'+I)$, also ist $\bar{f}$ ein Ringhomomorphismus. Der Rest lässt sich jetzt nachrechnen. ∎

3.3 Erzeuger für Ideale

Lemma 3.3 *Sei R ein Ring.*

a) Der Durchschnitte einer beliebigen nichtleeren Familie von Ideale in R ist selbst ein Ideal in R.

b) Sei $T \subseteq R$ eine Teilmenge. Dann sind $\bigcap\{I \lhd R \mid T \subseteq I\}$ und

$$\{r_1 t_1 r_1' + r_2 t_2 r_2' + \cdots + r_n t_n r_n' \mid n \geq 0,\ t_i \in T,\ r_i, r_i' \in R\}$$

die gleiche Menge. Diese Menge ist ein Ideal, genannt (T), das durch T erzeugte *Ideal in R. Es ist das kleinste Ideal, das die Menge T enthält.*

Beweis. Analog zum Beweis von Lemma 2.1. ∎

Bemerkung Von nun an wird R fast immer kommutativ sein. In diesem Fall muss man nur $I \leq (R, +)$ und $ri \in I$ für $r \in R$, $i \in I$ prüfen, um sicherzustellen, dass I ein Ideal ist. Und

$$(T) = \{r_1 t_1 + r_2 t_2 + \cdots + r_n t_n \mid n \geq 0,\ r_i \in R,\ t_i \in T\}\,.$$

Beispiel In $\mathbb{Z}[X, Y]$ sind $I = (5, 3X, Y - 7X)$, $J = (5, X, Y)$ und $K = (5, 3X, Y-7X, X^3-2Y^2)$ das gleiche Ideal. Es ist $I \subseteq K \subseteq J$, denn jeder Erzeuger von K liegt in J. Wegen $X = 2\cdot 3X - X\cdot 5$ ist $X \in I$. Wegen $Y = (Y-7X)+7\cdot X$ ist also $Y \in I$. Also $J \subseteq I$ und deshalb $I = J = K$. Dagegen ist $X - 2 \notin I$, denn jedes Polynom in I hat ein durch 5 teilbares Absolutglied.

3.4 Integritätsbereiche und Quotientenkörper

Die wichtigen Ringe $\mathbb{Z}$, $\mathbb{Z}[i]$ und $\mathbb{Z}[\sqrt{-5}]$ sind Unterringe des $\mathbb{C}$. Nicht jeder kommutativer Ring kann ein Unterring eines Körpers sein.

Definition Ein kommutativer Ring R heißt ein *Integritätsbereich* (*ID*, englisch „Integral Domain“) falls $1 \neq 0$ und der Ring nullteilerfrei ist, d.h. aus $ab = 0$ folgt $a = 0$ oder $b = 0$.

Beispiele $\mathbb{Z}$; jeder Unterring eines Körpers; $\mathbb{C}[X]$; $\mathbb{Z}[i]$.

Lemma 3.4 *Sei R ein kommutativer Ring.*

a) Ist R ein ID, dann gilt $\operatorname{grad}(fg) = \operatorname{grad}(f) + \operatorname{grad}(g)$ *für Polynome* $f, g \in R[X]$, *wobei* $\operatorname{grad}(0) := -\infty$.

b) $R[X]$ ist genau dann ein Integritätsbereich, wenn R selbst einer ist.

Beweis. a) Sei $f = aX^n +$ Terme vom kleinerem Grad und $g = bX^m +$ Terme vom kleinerem Grad, mit $a, b \neq 0$. Dann $ab \neq 0$, also $fg = abX^{n+m} +$ Terme vom kleinerem Grad.

b) Ist $R[X]$ ein ID, dann R auch, denn R ist ein Unterring von $R[X]$. Die andere Richtung folgt aus dem ersten Teil. ∎

Das Polynom $X^3 - 3X + 1$ hat keine Nullstellen in $\mathbb{Q}$. Wie zeigt man das? Da $\mathbb{Q}$ der *Quotientenkörper* von $\mathbb{Z}$ ist, besagt das Gauß-Lemma, dass jede rationale Nullstelle in $\mathbb{Z}$ liegt. Man rechnet leicht nach, dass es davon keine gibt.

Den Körper $\mathbb{Q}$ der rationalen Zahlen konstruiert man aus den ganzen Zahlen als Brüche. So konstruiert man auch die rationalen Funktionen $\mathbb{C}(X)$ aus den Polynomen $\mathbb{C}[X]$. Diese Konstruktion kann man außerdem z.B. auf den Gaußschen Zahlen $\mathbb{Z}[i]$ anwenden.

Lemma 3.5 *Sei R ein ID. Sei $\sim$ die folgende Relation auf der Menge $M = \{(r, s) \in R \times R \mid s \neq 0\}$:*

$$(r, s) \sim (a, b) \quad \Longleftrightarrow \quad br = as\,.$$

Dann:

a) $\sim$ ist eine Äquivalenzrelation auf M. Die Äquivalenzklasse von (r, s) bezeichnen wir mit $\frac{r}{s}$.

b) Indem man $\frac{r}{s} + \frac{a}{b} := \frac{br+as}{bs}$ und $\frac{r}{s} \cdot \frac{a}{b} := \frac{ra}{sb}$ setzt, wird die Menge der Äquivalenzklassen zu einem Körper, mit Einselement $\frac{1}{1}$ und Nullelement $\frac{0}{1}$.

c) Dieser Körper heißt $Q(R)$, der Quotientenkörper *von R. Er enthält in $\{\frac{r}{1} \mid r \in R\}$ einen Unterring, der eine Kopie von R ist.*

Beweis. a) Reflexiv, symmetrisch: klar. Transitiv: Angenommrn $(r, s) \sim (a, b)$ und $(a, b) \sim (c, d)$. Dann $br = as$ und $ad = bc$. Also $bdr = ads = bcs$, also $b(dr - cs) = 0$, also $dr = cs$ und $(r, s) \sim (c, d)$, denn b ist kein Nullteiler.

b) Repräsentantenunabhängigkeit: ist $\frac{r}{s} = \frac{r'}{s'}$ und $\frac{a}{b} = \frac{a'}{b'}$, dann

$$b's'(br + as) - bs(b'r' + a's') = bb'(s'r - sr') + ss'(b'a - ba') = 0\,,$$

und

$$b's'ar - bsa'r' = s'r(b'a - ba') + ba'(s'r - sr') = 0\,,$$

weshalb $\frac{b'r'+a's'}{b's'} = \frac{br+as}{bs}$ und $\frac{a'r'}{b's'} = \frac{ar}{bs}$. Die Ringaxiome lassen sich jetzt prüfen. Eins- und Nullelemente sind wie behauptet. Ist $\frac{r}{s} \neq \frac{0}{1}$ dann $r \neq 0$, daher ist $\frac{s}{r} \in Q(R)$ das multiplikative Inverse zu $\frac{r}{s}$.

c) Folgt. ∎

3.5 Maximale Ideale und Primideale

Diskussion: Entstehungsgeschichte von Idealen als ideale Zahlen, Primidealen als ideale Primzahlen, in Ringen wie $\mathbb{Z}[i]$ und $\mathbb{Z}[\sqrt{-5}]$. So lässt sich 2 in $R = \mathbb{Z}[\sqrt{-5}]$ nicht weiter faktorisieren, trotzdem ist 2 nicht prim in dem Sinne, dass aus $2 \mid (1+\sqrt{-5})(1-\sqrt{-5})$ folgen würde, dass 2 eins aus $1 \pm \sqrt{-5}$ teilt. Andererseits hat das Ideal $I = (2, 1+\sqrt{-5})$ diese Primzahl-Eigenschaft, im folgenden Sinne: ist $ab \in I$, dann $a \in I$ oder $b \in I$. Begründung erst nach Lemma 3.6.

Definition Sei R ein kommutativer Ring und $I \lhd R$ ein echtes Ideal.

a) I heißt ein *maximales* Ideal, wenn es – außer I und R selbst – kein Ideal $J \lhd R$ gibt mit $I \subseteq J \subseteq R$.

b) I heißt ein *Primideal*, wenn gilt: sind $a, b \in R$ mit $ab \in I$, so liegt mindestens eins von a, b in I.

Beispiele Das Ideal $(X-1) \lhd \mathbb{Z}[X]$ ist prim aber nicht maximal. Das Ideal $(2, X-1) \lhd \mathbb{Z}[X]$ ist prim und maximal. Das Ideal $6\mathbb{Z} \lhd \mathbb{Z}$ ist weder prim noch maximal.

Hilfslemma Jedes maximale Ideal ist prim.

Beweis. Sei $I \lhd R$ ein maximales Ideal, und sei $a \neq I$. Dann $(I, a) = R$, also gibt es $r \in R$ und $i \in I$ mit $1 = ra + i$. Nun sei $b \in R$ mit $ab \in I$. Dann $b = rab + ib \in I$. ∎

Lemma 3.6 *Sei R ein kommutativer Ring und $I \lhd R$ ein Ideal.*

a) Genau dann ist I ein maximales Ideal, wenn der Quotientenring R/I ein Körper ist.

b) Genau dann ist I ein Primideal, wenn der Quotientenring R/I ein Integritätsbereich ist.

Beweis. Zuerst: genau dann ist I ein echtes Ideal, wenn $1 \neq 0$ in R/I gilt – was bei Körpern und IDs der Fall ist.

a) Angenommen I ist maximal und $a \neq I$. Zu zeigen ist: $a + I \in R/I$ ist invertierbar. Wie im Hilfslemma gibt es $r \in R$, $i \in I$ mit $ra + i = 1$. Also $r + I = (a+I)^{-1}$. Nun nehmen wir an, R/I ist ein Körper und $J \lhd R$ erfüllt $J \supsetneq I$. Sei also $a \in J \setminus I$. Dann gibt es ein $b \in R$ mit $(a+I)(b+I) = 1 + I$, also gibt es ein $i \in I$ mit $ab + i = 1$, also $J = R$.

b) Angenommen I ist prim und $(a + I)(b + I) = 0 + I$. Dann $ab \in I$, also $a + I = 0 + I$ oder $b + I = 0 + I$, d.h. R/I ist ein ID. Dieses Argument kann man auch umdrehen. ∎

3.6 Existenz von maximalen Idealen: das Zornsche Lemma

Irgendwann im Mathematik-Studium muss man sich mit dem Zornschen Lemma befassen. Für uns ist dieser Zeitpunkt jetzt gekommen, denn wir wollen zeigen, dass jedes maximale Ideal in einem maximalen Ideal enthalten ist, und benötigen das Zornsche Lemma hierfür. Zuerst müssen wir etwas Terminologie einführen.

Definition Eine Relation $\leq$ auf einer Menge X heißt eine *Teilordnung*, wenn sie reflexiv, transitiv und antisymmetrisch ist. Das letztere heißt, dass

$$(x \leq y) \wedge (y \leq x) \Longrightarrow x = y\,.$$

Sie heißt eine *Ordnung*, wenn x, y vergleichbar sind für alle $x, y \in X$, d.h. wenn mindestens eins aus $x \leq y$, $y \leq x$ gilt.

Ein Element $x \in X$ heißt *maximal*, falls aus $y \geq x$ immer $y = x$ folgt.

Sei $\leq$ eine Teilordnung auf X. Eine *Kette* ist eine Teilmenge $K \leq X$ derart, dass die Einschränkung von $\leq$ eine Ordnung auf K ist. Ist $x \in X$ derart, dass $x \geq y$ für alle $y \in K$, so heißt x eine *obere Schranke* der Kette K.

Beispiele a) Sei M eine Menge. Inklusion ist eine Teilordnung auf der Menge $X = \mathscr{P}(M)$ der Teilmengen von M. Für $M = \{1, 2, 3\}$ sind $x = \{1, 2\}$ und $y = \{2, 3\}$ nicht vergleichbar. Das einzige maximale Element ist M selbst.

b) Mit der üblichen Ordnung auf $X = \mathbb{R}$ ist $\mathbb{Q}$ eine Kette ohne obere Schranke; und 3 ist eine obere Schranke der Kette $(-\infty, 0)$.

c) Sei $X = \{a, b, c\}$ mit der folgenden Teilordnung: $a \leq b$, $a \leq c$, und b, c sind nicht vergleichbar. Dann b, c sind zwei maximale Elemente; und $\{a, b\}$, $\{a, c\}$ sind zwei Ketten.

Das Zornsche Lemma *Sei $(X, \leq)$ eine teilweise geordnete nichtleere Menge. Hat jede nichtleere Kette in X eine obere Schranke, so enthält X ein maximales Element.*

Das Zornsche Lemma ist äquivalent zum Auswahlaxiom der Mengenlehre. Im Anhang §A.4 beweisen wir das Zornsche Lemma unter Verwendung des Auswahlaxioms. Es ist dagegen relativ leicht, das Auswahlaxiom aus dem Zornschen Lemma zu folgern.

Lemma 3.7 *Sei R ein kommutativer Ring.*

a) Jedes echte Ideal $I \lhd R$ ist in einem maximalen Ideal enthalten.

b) Ist die Teilmenge $S \subseteq R$ multiplikativ abgeschlossen *– d.h. ist $1 \in S$ und gilt $s, s' \in S \;\Rightarrow\; ss' \in S$ –, und ist $I \lhd R$ ein Ideal mit $I \cap S = \emptyset$, dann gibt es ein Primideal $P \lhd R$ mit $I \subseteq P$ und $P \cap S = \emptyset$.*

Beweis. Der Begriff „I ist ein Ideal mit $I \cap S = \emptyset$“ ist eine Verallgemeinerung des Begriffs „I ist ein echtes Ideal“, denn dies ist der Fall $S = \{1\}$. Fangen wir also mit Teil b) an. Sei X die Menge

$$X = \{J \lhd R \mid I \subseteq J \text{ und } J \cap S = \emptyset\}\,.$$

Inklusion ist eine Teilordnung auf X. Es ist $I \in X$, also $X \neq \emptyset$. Ist K eine nichtleere Kette in R, so sei $J_0 := \bigcup\{J \mid J \in K\}$. Für jedes $J \in K$ ist dann $J \subseteq J_0$. Somit ist J_0 eine obere Schranke für K, falls $J_0 \in X$. Für den Beweis benötigen wir das Zornsche Lemma (s. Anhang §A.4). Es ist $I \subseteq J_0$, da $I \subseteq J$ für jedes $J \in K$. Ist $s \in J_0 \cap S$, so gibt es ein $J \in K$ mit $s \in J$, wegen $J_0 = \bigcup\{J \mid J \in K\}$. Aber $s \notin J$, wegen $J \in X$. Ein Widerspruch, daher $J_0 \cap S = \emptyset$. Ferner ist J_0 ein Ideal, denn sind $x, y \in J_0$ dann gibt es $J, J' \in K$ mit $x \in J$ und $y \in J'$, ferner ist entweder $J \subseteq J'$ oder $J' \subseteq J$, da K eine Kette. Also oBdA $x, y \in J$, weswegen $x \pm y, rx \in J \subseteq J_0$. Somit ist $J_0 \in X$ und jede nichtleere Kette hat eine obere Schranke.

Nach dem Zornschen Lemma also enthält X ein maximales Element $P \lhd R$. Im Fall $S = \{1\}$ ist P dann maximal im idealtheoretischen Sinne, also ist Teil a) bewiesen. Für b) bleibt noch zu zeigen, dass P für beliebiges S ein Primideal ist. Wegen $1 \in S$ ist P ein echtes Ideal. Angenommen nicht prim: dann gibt es $a, b \in R \setminus P$ mit $ab \in P$. Da die Ideale (P, a) und (P, b) echt größer als P sind, liegen Sie nicht in X. Nach Definition von X gelten $(P, a) \cap S \neq \emptyset$, weshalb es $p \in P$, $r \in R$ und $s \in S$ gibt mit $p + ar = s$. Analog gibt es $p' \in P$, $r' \in R$ und $s' \in S$ mit $p' + br' = s'$. Wir multiplizieren beide Gleichungen:

$$pp' + pbr' + p'ar + abrr' = ss'\,.$$

Die rechte Seite liegt in S, die rechte Seite – wegen $p, p', ab \in P$ – liegt in P. Dies ist ein Widerspruch zu $P \in X$. Somit ist P doch ein Primideal. ∎

4 Faktorisierung und Irreduzibilitätskriterien

4.1 Irreduzible Elemente, Primelemente

Hier ist der Ring R immer kommutativ und meistens ein ID.

Warum gilt 5 als eine Primzahl? Zwei mögliche Antworten:

a) Die einzige Faktorisierungen $5 = a \cdot b$ sind $5 \cdot 1$ und $5 = 1 \cdot 5$;

b) Ist $n \cdot m$ durch 5 teilbar, dann auch m oder n.

In $\mathbb{Z}$ sind beide Definitionen gleichbedeutend, für uns ist eher a) die eigentliche Definition. Im allgemein ist aber b) eine stärkere Aussage als a), wie man anhand der Faktorisierungen $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$ erkennt. Ferner müssen wir uns fragen, welche Bedeutung die Faktorisierung $5 = (-1) \cdot (-5)$ hat.

Definition Sei R ein kommutativer Ring.

a) $e \in R$ heißt eine *Einheit*, falls $\frac{1}{e}$ existiert in R. Die Einheiten in R bilden eine multiplikative Gruppe $R^* := \{e \in R \mid e \text{ eine Einheit}\}$.

b) Elemente $x, y \in R$ heißen *assoziiert*, falls es eine Einheit e gibt mit $y = xe$. Assoziiert sein ist eine Äquivalenzrelation, Bezeichnung $x \sim y$.

Beispiele k Körper: $k^* = k \setminus \{0\}$, wie gewohnt. $\mathbb{Z}^* = \{1, 1\}$, $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$. In $R = \mathbb{Z}/4\mathbb{Z}[X]$ ist $\bar{1} + \bar{2}X$ eine Einheit ($\bar{r} := r + 4\mathbb{Z}$), denn $(\bar{1} + \bar{2}X)^2 = \bar{1}$.

Lemma 4.1 *Da R ein ID ist, ist $(R[X])^* = R^*$. Jede Einheit des Polynomrings $R[X]$ liegt im Grad 0.*

Beweis. Da R ein ID ist, gilt $\text{grad}(fg) = \text{grad}(f) + \text{grad}(g)$. ∎

Definition Sei R ein kommutativer Ring.

a) Ist $p \in R$ weder 0 noch eine Einheit, so heißt p *irreduzibel*, falls aus $p = ab$ immer folgt, dass a oder b eine Einheit ist.

b) Ist $p \in R$ weder 0 noch eine Einheit, so heißt p *prim*, falls aus $p \mid ab$ immer folgt, dass $p \mid a$ oder $p|b$ ist.

Beispiel In $R = \mathbb{Z}[\sqrt{-5}]$ ist $R^* = \{1, -1\}$. Es ist $1 + \sqrt{-5}$ irreduzibel aber nicht prim.

Lemma 4.2 *Ist R ein ID, so gilt prim $\Rightarrow$ irreduzibel.*

Beweis. Angenommen p ist prim und $p = ab$. Dann oBdA $p \mid a$, also gibt es $c \in R$ mit $a = pc$. Dann $p = ab = pcb$, also $p(cb - 1) = 0$. Da R ein ID ist und $p \neq 0$ ist, folgt, dass $cb = 1$, also ist $b \in R^*$. ∎

Hilfslemma Ist R ein ID, so ist $X - a \in R[X]$ irreduzibel für jedes $a \in R$.

Beweis. Ist $X - a = fg$, so ist wegen der Gradformel oBdA $\text{grad}(f) = 1$, $\text{grad}(g) = 0$. Also $f = bX + c$, $g = d$ mit $b, c, d \in R$. Daher ist $fg = bdX + cd = X - a$, also ist $bd = 1$, weshalb $g = d$ eine Einheit ist. ∎

Beispiel In $\mathbb{Z}[X]$ ist aber auch $2X + 1$ irreduzibel: das wäre der Fall $bd = 2$, $cd = 1$; und auch in diesem Fall muss d eine Einheit sein.

4.2 Ein erstes Irreduzibilitätskriterium

Lemma 4.3 *Sei R ein ID und $p \in R[X]$ ein normiertes Polynom vom Grad 2 oder 3. Dann gilt: p irreduzibel $\Leftrightarrow$ p hat keine Nullstelle in R.*

Beweis. Da $X - a$ normiert ist, gibt es (Polynomdivision) ein $q \in R[X]$ mit $p(X) = (X - a)q(X) + b$ für ein $b \in R$. Setzt man $X = a$ ein, so hat man $b = p(a)$. Ist also $a \in R$ eine Nullstelle von p, so ist p durch $X - a$ teilbar, und wegen der Gradformel ist weder $X - a$ noch $q(X)$ in R, d.h. keiner der beiden ist eine Einheit. Gibt es also eine Nullstelle, dann ist p reduzibel.

Angenommen umgekehrt $p = fg$ ist irreduzibel. Da p normiert ist, ist jedes Element von R, das p teilt, eine Einheit. Zu prüfen bleibt also nur der Fall $\text{grad}(f) = 2$, $\text{grad}(g) = 1$. Es ist also $f = cX^2 + dX + e$, $g = rX + s$. Da p normiert ist, ist $cr = 1$. Ersetzen wir also f durch rf und g durch cg, so ist oBdA g normiert vom Grad 1: es ist p durch $g = X - a$ teilbar, also $p(a) = 0$. ∎

Beispiel $X^3 - 2X + 3$ ist irreduzibel in $\mathbb{Z}[X]$, da es keine Nullstellen in $\mathbb{Z}$ gibt.

Warnbeispiel $(X^2 + 1)(X^2 + 4)$ hat zwar keine Nullstellen in $\mathbb{Z}$, ist aber offensichtlich reduzibel in $\mathbb{Z}[X]$. Es kommt also auf Grad 2 oder 3 an.

4.3 Hauptidealringe

Definition Ein ID R heißt ein *Hauptidealring* (HIR), falls gilt: zu jedem Ideal $I \lhd R$ gibt es ein $a \in R$ mit $I = (a)$.

Beispiele Sei k ein beliebiger Körper. Die einzigen Ideale in k sind $\{0\} = (0)$ und $R = (1)$. Daher ist k ein HIR. Später sehen wir, dass $\mathbb{Z}$, $k[X]$ und $\mathbb{Z}[i]$ auch HIRinge sind. Dagegen sind $\mathbb{Z}[\sqrt{-5}]$, $\mathbb{Z}[X]$ und $\mathbb{C}[X, Y]$ keine HIRinge.

Hilfslemma Sei R ein ID und $x, y \in R$.

a) $(x) = \{rx \mid r \in R\}$.

b) $(x) = (y) \Leftrightarrow x \sim y$.

c) (x) ein Primideal $\Leftrightarrow$ x ein Primelement, oder $x = 0$.

Beweis. a) Klar, sogar in jedem kommutativen Ring.

b) Wegen $x \in (y)$ und $y \in (x)$ gibt es $a, b \in R$ mit $x = ay$, $y = bx$. Also $(ab-1)x = (ab-1)y = 0$. Also $ab = 1$ oder $x = y = 0$. In beiden Fällen folgt: $x \sim y$. Ist umgekehrt $x \sim y$, dann gibt es eine Einheit e mit $y = ex$ und $x = \frac{1}{e}y$. Also $y \in (x)$ und $x \in (y)$.

c) Da R ein ID ist, ist (0) ein Primideal. Ist x eine Einheit, so ist $(x) = R$, was kein Primideal ist. Sei also x weder Null noch eine Einheit. Es ist $x \mid y$ genau dann, wenn $y \in (x)$ ist; das Ergebnis folgt, indem man die beiden Definitionen miteinander vergleicht. ∎

Lemma 4.4 *Ist R ein HIR und $x \in R$, dann gilt: x irred $\Leftrightarrow$ x prim.*

Beweis. „⇐“: Lemma 4.2 „⇒“: Angenommen $x \mid ab$. Dann gibt es $c \in R$ mit $(x, a) = (c) = \{cr \mid r \in R\}$. Aus $x \in (c)$ folgt $x = cy$ für ein $y \in R$. Nach Annahme ist entweder c oder y eine Einheit. Ist y eine Einheit, dann $x \sim c$, weshalb $(c) = (x)$ und daher $a \in (x)$, d.h. $x \mid a$. Ist dagegen c eine Einheit, dann $(c) = R$ und daher $1 \in (x, a)$, d.h. es gibt $s, t \in R$ mit $rx + sa = 1$. Daher $rxb + sab = b$, weshalb $x \mid b$, denn x teilt die linke Seite. ∎

4.4 Der Begriff faktorieller Ring

Satz 4.5 *Sei R ein HIR und $x \in R$ weder 0 noch eine Einheit. Dann lässt sich x als ein Produkt $x = p_1 p_2 \cdots p_n$ von Primelementen schreiben.*

Lemma 4.6 *Sei R ein HIR und $\mathcal{I}$ eine nichtleere Menge von Idealen in R. Dann enthält $\mathcal{I}$ maximale Elemente. (D.h. Elemente, die maximal in $\mathcal{I}$ sind: sie werden häufig keine maximale Ideale sein.)*

Beweis. Wenn nicht, dann gibt es eine Abbildung $\alpha \colon \mathcal{I} \to \mathcal{I}$ derart, dass $I \subsetneq \alpha(I)$ ist für jedes $I \in \mathcal{I}$. Nun wählen wir ein $I \in \mathcal{I}$ aus und definieren eine Folge $I_0, I_1, I_2, \ldots$ in $\mathcal{I}$ durch $I_0 = I$, $I_{n+1} = \alpha(I_n)$. Dann $I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \ldots$. Sei $J := \bigcup_{n \geq 0} I_n$. Dann ist J ein Ideal (vgl. Beweis von Lemma 3.7). Da R ein HIR ist, ist $J = (a)$ für ein $a \in R$. Nach Konstruktion von J gibt es ein n mit $a \in I_n$ und daher $J \subseteq I_n$. Also $J \subseteq I_n \subsetneq I_{n+1} \subseteq J$, ein Widerspruch. ∎

Beweis von Satz 4.5. Sei $\mathcal{I} = \{I \lhd R \mid I \text{ echt}, x \in I\}$. Es ist $(x) \in \mathcal{I}$, also nach Lemma 4.6 gibt es ein I maximal in $\mathcal{I}$. Nach Konstruktion von $\mathcal{I}$ ist I ein maximales Ideal, daher ein Primideal. Aber R ist ein HIR, daher ist $I = (p)$ für ein $p \in R$. Also ist p ein Primelement, und $p \mid x$.

Nun sei $\mathcal{J} = \{(y) \mid x = yp_1 \cdots p_n \text{ mit } y \in R, n \geq 1 \text{ und } p_i \text{ prim}\}$. Nach dem ersten Teil ist $\mathcal{J}$ nicht leer. Nun sei (y) maximal in $\mathcal{J}$. Nach dem ersten Teil gilt $y = zq$ für q prim, falls y keine Einheit ist. Dann aber wäre $(y) \subsetneq (z) \in \mathcal{J}$, Widerspruch. Also ist y eine Einheit und $x = yp_1 \cdots p_n$ mit $n \geq 1$. Indem man p_1 durch das Primelement yp_1 ersetzt, erreicht man $x = p_1 p_2 \cdots p_n$. ∎

Definition Ein ID R heißt ein *faktorieller Ring*, falls jedes $x \in R$, dass weder 0 noch eine Einheit ist, sich als ein Produkt von Primelementen schreiben lässt.

Bemerkung Auf Englisch: „unique factorization domain“, oder einfach UFD.

Beispiele Nach Satz 4.5 ist jeder HIR faktoriell. Also ist jeder Körper k faktoriell, zusammen mit $\mathbb{Z}$, $\mathbb{Z}[i]$ und $k[X]$. Die Ringe $\mathbb{Z}[X]$, $\mathbb{C}[X, Y, Z]$ sind keine HIRinge, wohl aber – nach einem Satz von Gauß – faktoriell.

Hilfslemma Sei R faktoriell und $x \in R$. Dann: x irred $\Leftrightarrow$ x prim.

Beweis. In einem ID sind Primelemente irreduzibel. Sei also x irreduzibel. Da R faktoriell ist, hat x eine Primfaktorisierung $x = p_1 p_2 \cdots p_n$. Da x irreduzibel ist, und kein p_i eine Einheit ist, gilt $n = 1$, und $x = p_1$ ist prim. ∎

4.5 Euklidische Ringe

Wir zeigen, dass $\mathbb{Z}$, $k[X]$ und $\mathbb{Z}[i]$ HIRinge sind.

Definition Ein ID R heißt ein *euklidischer Ring*, wenn es eine Abbildung $N\colon R \setminus \{0\} \to \mathbb{N}_0$ gibt mit der folgenden „Division mit Rest“-Eigenschaft:

$$\forall f, g \in R \text{ mit } g \neq 0 \; \exists\, q, r \in R \; f = qg + r, \text{ und } r = 0 \text{ oder } N(r) < N(g).$$

Bemerkung N nennt man Norm. Allerdings hat „Norm“ in der algebraischen Zahlentheorie eine zweite, häufigere Bedeutung.

Lemma 4.7 *$\mathbb{Z}$, $k[X]$ und $\mathbb{Z}[i]$ sind euklidische Ringe, wobei k ein beliebiger Körper ist.*

Beweis. $\mathbb{Z}$: man setzt $N(n) = |n|$. Division mit Rest ist wohlbekannt. $k[X]$: man setzt $N(f) = \operatorname{grad}(f)$. Auch Polynomdivision mit Rest ist uns gut bekannt. $\mathbb{Z}[i]$: Hier müssen wir was tun. Definiere $N\colon \mathbb{Z}[i] \to \mathbb{N}_0$ durch $N(a + ib) = |a + ib|^2 = a^2 + b^2$. Sei $z = a + ib$, $w = c + id$ mit $w \neq 0$. Dann $\frac{z}{w} = x + iy$ mit $x, y \in \mathbb{Q}$. Wähle $m, n \in \mathbb{Z}$ mit $|x - m|, |y - n| \leq \frac{1}{2}$. Sei $q = m + in$. Dann $z - qw = w(\frac{z}{w} - q) = w((x - m) + i(y - n))$ und daher $|z - qw|^2 = |w|^2 \cdot ((x - m)^2 + (y - n)^2) \leq \frac{1}{2} |w|^2 < |w|^2$. Also $N(z - qw) < N(w)$. ∎

Lemma 4.8 *Euklidische Ringe sind HIRinge.*

Beweis. Sei $\{0\} \neq I \lhd R$ ein Ideal. Wähle $a \in I \setminus \{0\}$ mit $N(a) = \min\{N(r) \mid r \in I \setminus \{0\}\}$. Zu zeigen ist $I = (a)$. Klar ist $(a) \subseteq I$. Nun sei $b \in I$. Da R euklidisch ist, gibt es $q, r \in R$ mit $b = qa + r$. Daher ist $r = b - qa$ Element von I. Nach der „Division mit Rest"-Eigenschaft ist ferner $r = 0$, oder $N(r) < N(a)$. Nach Wahl von a bleibt nur die Möglichkeit $r = 0$. Also $b = qa \in (a)$. ∎

Bemerkung Endlich haben wir nachgewiesen: $\mathbb{Z}, k[X], \mathbb{Z}[i]$ sind HIRinge und daher faktoriell.

4.6 ggT und kgV in faktoriellen Ringen

Faktorielle Ringe sind Ringe, wo Primfaktorisierung so funktioniert, wie man es erwartet.

Definition Sei R ein ID und $r_1, \ldots, r_n \in R$.

a) $a \in R$ heißt ein ggT von $r_1, \ldots, r_n$, wenn erstens: $a \mid r_i$ gilt für jedes i, und zweitens: gilt auch $b \mid r_i$ für jedes i, dann $b \mid a$.

b) $a \in R$ heißt ein kgV von $r_1, \ldots, r_n$, wenn erstens: $r_i \mid a$ gilt für jedes i, und zweitens: gilt auch $r_i \mid b$ für jedes i, dann $a \mid b$.

Hilfslemma Sofern sie existieren, sind ggT und kgV jeweils bis auf Assoziiertheit eindeutig. Daher schreibt man auch $a = \mathrm{ggT}(r_1, \ldots, r_n)$, bzw. $a = \mathrm{kgV}(r_1, \ldots, r_n)$.

Beweis. Selber nachrechnen! ∎

Übungsaufgabe (freiwillig) Man konstruiere ein Beispiel, wo ggT und/oder kgV nicht existieren.

Wie wir sehen werden, existieren in einem faktoriellen Ring alle ggTs und kgVs.

Bemerkung Es ist $\mathrm{ggT}(r_1, \ldots, r_n) = \mathrm{ggT}(\mathrm{ggT}(r_1, r_2), r_3, \ldots, r_n)$, also reicht es nachzuweisen, dass $\mathrm{ggT}(r, s)$ existiert für alle $r, s \in R$. Ähnliches gilt für kgV.

Lemma 4.9 *Sei R ein faktorieller Ring.*

a) Sei $x \neq 0$, $x \notin R^*$. Die Primfaktorisierung von x ist in wesentlichen eindeutig: Ist

$$x = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$$

mit $n, m \geq 1$ und p_i, q_j prim, dann ist $n = m$, und es gibt eine Permutation $\sigma \in S_n$ mit $\forall\, i\ p_i \sim q_{\sigma(i)}$. (Dies gilt sogar in jedem ID.)

b) *Sei $p \in R$ ein Primelement. Die* p-adische Bewertung *ν_p, gegeben durch $\nu_p(\text{Einheit}) = 0$ und $\nu_p(p_1 \cdots p_n) :=$ Anzahl der i mit $p_i \sim p$, ist eine wohldefinierte Abbildung $\nu_p \colon R \setminus \{0\} \to \mathbb{N}_0$.*

c) *Jedes $y \in R \setminus \{0\}$ lässt sich schreiben als $y = up_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$, mit $u \in R^*$, $m \geq 0$, $e_i \in \mathbb{N}_1$ und $p_1, \ldots, p_m$ paarweise nichtassoziierte Primelemente.*

Beweis. a) Induktion über n. Damit die Induktion funktioniert, sollte die zweite Faktorisierung $x = uq_1 \cdots q_m$ sein, mit $u \in R^*$. Ist $n = 1$, dann ist x prim, daher $m = 1$ und $p_1 = x = uq_1$, also $p_1 \sim q_1$. Ist $n \geq 2$, dann $p_n \mid x$, also $p_n \mid uq_1 \cdots q_m$, also $\exists j \colon p_n \mid q_j$, denn p_n ist prim (und teilt keine Einheit). Nachdem wir die q_j ggf. umnummeriert haben, ist $j = m$ und $p_n \mid q_m$, also gibt es r mit $q_m = rp_n$. Da q_m prim und daher irreduzibel ist, ist $r \in R^*$. Also $p_n \sim q_m$, und $p_1 \cdots p_{n-1} = \frac{x}{p_n} = urq_1 \cdots q_{m-1}$. Jetzt greift die Induktionsannahme, denn $ur \in R^*$.

b) Folgt aus dem ersten Teil.

c) x Einheit: $m = 0$, $u = x$. x keine Einheit: da R faktoriell ist, hat x eine Primfaktorisierung $x = p_1 \cdots p_n$. Nachdem wir ggf. umnummeriert haben, sind $p_1, \ldots, p_m$ paarweise nichtassoziiert, und für jedes $j \geq m + 1$ gibt es $i \leq m$ mit $p_j \sim p_i$. Also $p_j = u_j p_i$ für eine bestimmte Einheit u_j. ∎

Beispiele a) $R = \mathbb{Z}$: Es ist

$$-360 = (-2)\cdot 2\cdot 2\cdot 3\cdot 3\cdot 5 = 2\cdot 5\cdot 2\cdot 3\cdot (-3)\cdot 2 = (-5)\cdot 3\cdot (-2)\cdot (-3)\cdot (-2)\cdot (-2)$$

(drei Primfaktorisierungen). Es ist $\nu_2(-360) = 3 = \nu_{-2}(-360)$; $\nu_3(-360) = 2$; $\nu_5(-360) = 1$; und $\nu_7(-360) = \nu_{41}(-360) = 0$. Zwei Faktorisierungen im Sinne von Teil c) sind

$$-360 = (-1) \cdot 2^3 \cdot 3^2 \cdot 5^1 = 1 \cdot 2^3 \cdot (-3)^2 \cdot (-5)^1 .$$

b) $R = \mathbb{Q}[X]$: Sei $f(X) = X^4 - X^3 - X - 1$. Es ist $f(X) = (X^3 - 1)(X - 1)$. Eine Primfaktorisierung ist $f(X) = (X - 1)(X - 1)(X^2 + X + 1)$, eine andere ist $f(X) = (2 - 2X) \cdot (\frac{1}{2} - \frac{X}{2}) \cdot (X^2 + X + 1)$. Es ist $\nu_{X-1}(f) = 2$, $\nu_{X^2+X+1}(f) = 1$ und $\nu_X(f) = \nu_{X^2-X+1}(f) = 0$. Eine Faktorisierung im Sinne von Teil c) ist $f = 1 \cdot (X - 1)^2 \cdot (X^2 + X + 1)$, aber eine andere ist $f = \frac{1}{4} \cdot (2 - 2X)^2 \cdot (X^2 + X + 1)$.

Die p-adische Bewertung kann sehr nützlich bei Teilbarkeitsfragen sein: man kann die Teilbarkeit getrennt für jedes Primelement prüfen.

Lemma 4.10 *Sei R ein faktorieller Ring, und $\mathbb{P} = \{[p] \mid p \text{ prim in } R\}$ die Menge der Äquivalenzklassen von Primelementen bgzl. Assoziiertheit.*

a) Es ist $\nu_p(rs) = \nu_p(r) + \nu_p(s)$ für $r, s \in R \setminus \{0\}$.

b) Es ist $\nu_p(r) \neq 0$ für nur endlich viele $[p] \in \mathbb{P}$. Ist x ein Produkt von n Primelementen ($n = 0$ falls $x \in R^*$), so gilt

$$\sum_{[p]\in\mathbb{P}} \nu_p(r) = n\,.$$

c) Es ist $r \mid s$ genau dann, wenn $\nu_p(r) \leq \nu_p(s)$ gilt für jedes $[p] \in \mathbb{P}$.

d) Fortsetzung auf dem Quotientenkörper $Q(R)$:
Indem man $\nu_p(\frac{r}{s}) := \nu_p(r) - \nu_p(s)$ setzt, erhält man einen wohldefinierten Gruppenhomomorphismus $\nu_p\colon (Q(R)^*, \cdot) \to (\mathbb{Z}, +)$.

e) Für $x \in Q(R)^*$ gelten:

$$x \in R \iff \forall [p] \in \mathbb{P}\colon \nu_p(x) \geq 0\,; \quad x \in R^* \iff \forall [p] \in \mathbb{P}\colon \nu_p(x) = 0\,.$$

Beweis. Vorne weg: ist $p \sim q$, dann $\nu_p(x) = \nu_q(x)$ für alle x, nach Definition der Bewertung.

a) Sind $r = p_1 \cdots p_n$ und $s = q_1 \cdots q_m$ Primfaktorisierungen, so ist auch $rs = p_1 \cdots p_n q_1 \cdots q_m$.

b) Für $x = u p_1^{e_1} \cdots p_m^{e_m}$ – vgl. Lemma 4.9 c) – ist $\nu_{p_i}(x) = e_i$, und $\nu_p(x) = 0$ falls $[p]$ kein $[p_i]$.

c) $s = rt \;\Rightarrow\; \nu_p(s) = \nu_p(r) + \nu_p(t) \geq \nu_p(r)$. Umgekehrt sei $s = u p_1^{e_1} \cdots p_m^{e_m}$. Wegen $\nu_p(r) \leq \nu_p(s)$ für alle $[p] \in \mathbb{P}$ muss r die Gestalt $r = v p_1^{d_1} \cdots p_m^{d_m}$ haben, mit $v \in R^*$ und $0 \leq d_i \leq e_i$ für alle i. Also $r \mid s$.

d) Ist $\frac{r}{s} = \frac{r'}{s'}$, dann $rs' = r's$. Wende ν_p an, und verwende a).

e) Die erste Aussage folgt aus c) und d). Zweite Aussage: $x \in R^*$ genau dann, wenn x, x^{-1} beide in R liegen. ∎

Beispiel Warum ist 12 kein Teiler von 18? Weil $\nu_2(12) = 2$ größer ist als $\nu_2(18) = 1$. Warum ist $\frac{25}{15}$ keine ganze Zahl? Weil $\nu_3(\frac{25}{15}) = \nu_3(25) - \nu_3(15) = 0 - 1 < 0$. Es hilft nichts, dass $\nu_5(\frac{25}{15}) = 2 - 1 > 0$ ist.

Lemma 4.11 *Sei R ein faktorieller Ring, und $r, s \in R$. Dann existieren* $\mathrm{ggT}(r, s)$ *und* $\mathrm{kgV}(r, s)$.

Beweis. Es ist $\mathrm{ggT}(r, 0) = r$ und $\mathrm{kgV}(r, 0) = 0$, also oBdA $r, s \in R \setminus \{0\}$. Nach Lemma 4.9 c) gibt es Faktorisierungen

$$x = u p_1^{a_1} \cdots p_m^{a_m} \qquad\qquad y = v p_1^{b_1} \cdots p_m^{b_m}$$

mit $u, v \in R^*$; $p_1, \ldots, p_m$ paarweise nichtassoziierte Primelementen; und $a_i, b_i \in \mathbb{N}_0$. Sei $c_i := \min(a_i, b_i)$, $d_i := \max(a_i, b_i)$. Nach Lemma 4.10 c) ist $p_1^{c_1} \cdots p_m^{c_m}$ der ggT, und $p_1^{d_1} \cdots p_m^{d_m}$ das kgV. ∎

4.7 Das Irreduzibilitätskriterium von Eisenstein

Beispiel Das Polynom $2X - 2$ ist irreduzibel in $\mathbb{Q}[X]$ (da dort zu $X - 1$ assoziiert), aber wegen $2X - 2 = 2 \cdot (X - 1)$ reduzibel in $\mathbb{Z}[X]$. Das liegt daran, dass die Koeffizienten des Polynoms $2X - 2$ einen gemeinsamen Teiler haben.

Definition Sei R faktoriell und $0 \neq f \in R[X]$. Der *Inhalt* von f ist der ggT der Koeffizienten von f. Das heißt,

$$\text{Inhalt}(a_n X^n + \cdots + a_1 X + a_0 = \text{ggT}(a_0, a_1, \ldots, a_n)\,.$$

Beispiel $R = \mathbb{Z}$: Es ist $\text{Inhalt}(12X^5 - 18X + 30) = \text{ggT}(12, 18, 30) = 6$. Es ist $\text{Inhalt}(6X^2 + 15X + 10) = \text{ggT}(6, 15, 10) = 1$. Ist $f(X)$ normiert, so ist $\text{Inhalt}(f) = 1$. $2 \in \mathbb{Z}[X]$ ist irreduzibel und hat Inhalt 2.

Hilfslemma Sei R ein faktorieller Ring, und $f \in R[X]$ mit $\text{grad}(f) \geq 1$. Ist $\text{Inhalt}(f) \neq 1$, so ist f reduzibel. Ist dagegen $\text{Inhalt}(f) = 1$ und $f = gh$ mit $\text{grad}(g) = 0$, so ist g eine Einheit.

Beweis. 1. Teil: $f = \text{Inhalt}(f) \cdot \frac{f}{\text{Inhalt}(f)}$. 2. Teil: Ist g keine Einheit, dann hat es einen Primteiler p. Dann teilt p jeden Koeffizienten von f, also $p \mid \text{Inhalt}(f)$. ∎

Das Eisenstein-Irreduzibilitätskriterium *Sei R ein faktorieller Ring, und $f = a_n X^n + \cdot + a_1 X + a_0 \in R[X]$ ein Polynom mit* $\text{Inhalt}(f) = 1$ *(etwa, weil f normiert) und* $\text{grad}(f) \geq 1$.

Angenommen, es gibt ein Primelement $p \in R$ derart, dass $p \nmid a_n$, $p \mid a_i$ für alle $0 \leq i \leq n - 1$, und $p^2 \nmid a_0$. Dann ist f irreduzibel in $R[X]$.

Bemerkung Wegen $p \nmid a_n$ ist $a_n \neq 0$ und daher $\text{grad}(f) = 0$. Die Teilbarkeitsbedingungen kann man auch mittels der Bewertung ν_p ausdrücken: $\nu_p(a_n) = 0$; $\nu_p(a_i) \geq 1$ für $1 \leq i \leq n - 1$; $\nu_p(a_0) = 1$.

Beispiel So sind in $\mathbb{Z}[X]$ die Polynome $X^7 - 50X + 20$ und $3X^5 - 2X - 2$ irreduzibel (Eisenstein für $p = 5$ bzw. für $p = 2$). Dagegen können wir mittels Eisenstein nichts über $X^5 - 16X + 20$ sagen.

Beweis. Angenommen $f = gh$, mit g, h beide $\notin R[X]^* = R^*$. Da f Inhalt 1 hat, haben g, h beide Grad ≥ 1 (Hilfslemma). Also $g = b_r X^r + \cdots + b_0$, $h = c_s X^s + \cdots + c_0$ mit $r + s = n$ und $r, s \geq 1$. Wegen $b_r c_s = a_n$ ist weder b_r noch c_s durch p teilbar. Sei $i_0 = \min\{i \in \{0, \ldots, r\} \mid p \nmid b_i\}$ und $j_0 = \min\{j \in \{0, \ldots, s\} \mid p \nmid c_j\}$. Sei $m = i_0 + j_0$. Dann

$$a_m = \sum_{i=0}^{m} b_i c_{m-i} = b_{i_0} c_{j_0} + \sum_{i<i_0} b_i c_{m-i} + \sum_{j<j_0} b_{m-j} c_j\,.$$

Es ist dann $p \nmid a_m$, denn $p \nmid b_{i_0} c_{j_0}$, aber $p \mid b_i$ für $i < i_0$ und $p \mid c_j$ für $j < j_0$. Nach Annahme ist also $m = n$ und daher $i_0 = r$, $j_0 = s$. Fazit: $p \mid b_0$ und $p \mid c_0$, also $p^2 \mid b_0 c_0 = a_0$. Widerspruch. ∎

4.8 Das Gauß-Lemma

Wir wollen den folgenden Satz beweisen:

Satz („Gauß-Kriterium“[3]) *Sei R ein faktorieller Ring und $f \in R[X]$ ein Polynom vom Grad ≥ 1. Dann gilt:*

$$f \text{ irreduzibel in } R[X] \iff \operatorname{Inhalt}(f) = 1, \text{ und } f \text{ irreduzibel in } Q(R)[X].$$

Beispiel Die Polynome $X^3 - 3X + 1$ und $X^{17} - 9X^{11} + 27X^4 - 30X + 15$ sind irreduzibel in $\mathbb{Q}[X]$, insbesondere haben sie in $\mathbb{Q}$ keine Nullstellen: denn beide sind in $\mathbb{Z}[X]$ irreduzibel, da das erste hat keine Nullstelle, und das zweite erfüllt Eisenstein mit $p = 3$.

Das Gauß-Lemma *Sei R ein faktorieller Ring und $f, g \in R[X]$. Dann*

$$\operatorname{Inhalt}(fg) = \operatorname{Inhalt}(f) \operatorname{Inhalt}(g)\,.$$

Beweis. Ist $r = \operatorname{Inhalt}(f)$, dann $f_1 := \frac{f}{r}$ liegt in $R[X]$, und es ist $\operatorname{Inhalt}(f_1) = 1$ und $fg = r \cdot f_1 g$. Also oBdA $\operatorname{Inhalt}(f) = \operatorname{Inhalt}(g) = 1$, und es ist zu zeigen: $\operatorname{Inhalt}(fg) = 1$.

Sei $p \in R$ ein Primelement, dann ist $(p) \lhd R$ ein Primideal. Also ist der Quotientenring $S := R/(p)$ ein ID. Betrachten wir den sog. *Reduktionshomomorphismus* $R[X] \to S[X]$, $f = \sum_{i=0}^n a_i X^i \to \bar{f} := \sum_{i=0}^n \bar{a}_i X^i$, wobei $\bar{a} := a + (p) \in S$ für $a \in R$. Diese Abbildung ist ein Homomorphismus, d.h. $\overline{fg} = \bar{f} \cdot \bar{g}$. Nun, wegen $\operatorname{Inhalt}(f) = 1$ gibt es einen Koeffizienten a_i von f mit $p \nmid a_i$, also $\bar{a}_i \neq 0$ und daher $\bar{f} \neq 0$. Analog ist auch $\bar{g} \neq 0$. Da S ein ID ist, ist auch $S[X]$ ein ID, und daher $\overline{fg} = \bar{f} \cdot \bar{g} \neq 0$. Also hat auch fg einen Koeffizienten c_k mit $p \nmid c_k$, weshalb $p \nmid \operatorname{Inhalt}(fg)$. Da p ein beliebiges Primelement ist, ist $\operatorname{Inhalt}(fg) = 1$. ∎

Korollar 4.12 *Sei R ein faktorieller Ring und $f, g \in Q(R)[X]$ Polynome mit $fg \in R[X]$. Dann gibt es $0 \neq q \in Q(R)$ mit $qf, \frac{1}{q} g \in R[X]$.*

Beweis. Sei $h := fg \in R[X]$. Sei r das kgV der Nenner der Koeffizienten von f: dann ist $rf \in R[X]$. Analog finden wir $0 \neq s \in R$ mit $sg \in R[X]$. Sei $t = \operatorname{Inhalt}(rf)$, $u = \operatorname{Inhalt}(sg)$. Also $rf \cdot sg = rsh$, weshalb nach dem Gauß-Lemma gilt

$$tu = \operatorname{Inhalt}(rsh) = rs \operatorname{Inhalt}(h)\,.$$

Sei $x = \frac{r}{t}$. Dann $xf \in R[X]$ und $\operatorname{Inhalt}(xf) = 1$, denn $rf \in R[X]$ und $t = \operatorname{Inhalt}(rf)$. Dann $h = xf \cdot \frac{1}{x} g$. Ferner, $\frac{1}{x} = \frac{t}{r} = \frac{s}{u} \operatorname{Inhalt}(h)$; und $\frac{s}{u} g \in R[X]$ gilt analog. Also für $x = \frac{r}{t}$ sind $xf, \frac{1}{x} g \in R[X]$. Ferner ist $\operatorname{Inhalt}(xf) = 1$. ∎

[3] „Gauß-Kriterium“ ist mein privater Name. Meistens nennt man diesen Satz das „Gauss-Lemma“, denn er ist die Hauptanwendung des untenstehenden Gauß-Lemmas.

Korollar 4.13 *Sei R faktoriell und $f, h \in R[X]$ Polynome mit* $\mathrm{Inhalt}(f) = 1$ *und $f \mid h$ in $Q(R)[X]$. Dann liegt $\frac{h}{f}$ in $R[X]$, weshalb h auch in $R[X]$ durch f teilbar ist.*

Beweis. Sei $g = \frac{h}{f} \in Q(R)[X]$. Nach Korollar 4.12 gibt es $x \in Q(R)$ mit $xf, \frac{1}{x}g \in R[X]$; und nach dessen Beweis kann man außerdem $\mathrm{Inhalt}(xf) = 1$ verlangen. Da $\mathrm{Inhalt}(f) = 1$ ist, folgt $x = 1$ und daher $g \in R[X]$. ∎

Beweis des Gauß-Kriteriums. Ist f reduzibel in $R[X]$, dann erst recht in $Q[X]$ – es sei denn, ein Faktor hat Grad 0, was genau dann möglich ist, wenn $\mathrm{Inhalt}(f) = 1$ ist. Nun angenommen f ist irreduzibel in $R[X]$. Keine echte Faktoren im Grad 0, also $\mathrm{Inhalt}(f) = 1$. Angenommen f reduzibel in $Q(R)[X]$, d.h. $f = gh$ mit $g, h \in Q(R)[X]$. Aber nach Korollar 4.12 sind oBdA $g, h \in R[X]$, ein Widerspruch. ∎

Satz 4.14 (Gauß) *Ist R faktoriell, dann auch $R[X]$.*

Beweis. R ist ein ID, also $R[X]$ auch. Jedes $f \in R[X]$ lässt sich als ein Produkt von irreduziblen Elementen schreiben: gilt für Grad 0 da R faktoriell, daher auch für $\mathrm{Inhalt}(f)$; und ist $\mathrm{Inhalt}(f) = 1$, so hat jeder Faktor kleineren Grad. Zu zeigen ist also: jedes irreduzible Element ist prim. Fall Grad 0: ist $r \in R$ prim, und ist $r \mid fg$, dann $r \mid \mathrm{Inhalt}(fg)$, daher (Gauß-Lemma) $r \mid \mathrm{Inhalt}(f)\,\mathrm{Inhalt}(g)$, daher oBdA $r \mid \mathrm{Inhalt}(f)$, also $r \mid f$. Ist $\mathrm{grad}(f) \geq 1$ und f irreduzibel, dann $\mathrm{Inhalt}(f) = 1$ und f irreduzibel im faktoriellen Ring $Q(R)[X]$, daher prim dort. Aus $f \mid gh$ in $R[X]$ folgt also oBdA $f \mid g$ in $Q(R)[X]$. Wegen $\mathrm{Inhalt}(f) = 1$ folgt also $f \mid g$ in $R[X]$ (Korollar 4.13). ∎

Beispiel $\mathbb{Z}[X, Y]$, $\mathbb{C}[X_1, X_2, X_3, X_4]$ sind keine Hauptidealringe, schon aber faktoriell.

5 Körpererweiterungen

5.1 Der Erweiterungsbegriff

Hilfslemma Seien K, L Körper und $f\colon K \to L$ ein Ringhomomorphismus. Dann ist f injektiv.

Beweis. Ist $0 \neq x \in K$, dann $1_L = f(1_K) = f(x \cdot \frac{1}{x}) = f(x) \cdot f(\frac{1}{x})$. Also $f(x) \neq 0$. ∎

Definition Ist K ein Körper und $k \subseteq K$ ein Unterring, der selbst ein Körper ist, so heißt K ein *Erweiterungskörper* von k, und man spricht von der *Körpererweiterung* K/k. Abkürzung: KE für Körpererweiterung.

Anders gesagt: es sind k, K Körper; k ist Teilmenge von K; und die Inklusion ist ein (Ring-)Homomorphismus.

Beispiele $\mathbb{C}/\mathbb{R}$, $\mathbb{Q}(i)/\mathbb{Q}$, $\mathbb{R}/\mathbb{Q}$, $\mathbb{C}/\mathbb{Q}$; und $\mathbb{F}_4/\mathbb{F}_2$, wobei $\mathbb{F}_4 = \{\bar{0}, \bar{1}, w, w + \bar{1}\}$ mit $w + w = \bar{0}$ und $w^2 = w + \bar{1}$.

Bemerkung Ist V ein Vektorraum und $U \subseteq V$ ein Untervektorraum, so stellt man sich V als das feste Referenzobjekt, dagegen betrachtet man U als variabel. Bei einer Körpererweiterung K/k dagegen betrachtet man k als das feste Referenzobjekt, und K als variabel.

5.2 Erweiterungsgrad

Definition Ist K/k eine KE, so ist K ein k-Vektorraum. Der *Erweiterungsgrad* $[K : k]$ ist per Definition die Dimension dieses Vektorraums:

$$[K : k] := \dim_k(K)\,.$$

Ist $[K : k] < \infty$, so heißt die KE K/k *endlich*.

Bezeichnung Sind K/k, K/L zwei KEen, und ist $L \supseteq k$, so heißt L ein *Zwischenkörper* der Erweiterung K/k. In diesem Fall ist auch L/k eine KE.

Meistens schreibt man einfach „Sei $k \subseteq L \subseteq K$ ein Zwischenkörper …“. Beispiel: $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

Lemma 5.1 *Sei K/k eine KE und $k \subseteq L \subseteq K$ ein Zwischenkörper. Dann gilt*

$$[K : k] = [K : L] \cdot [L : k]\,.$$

Insbesondere ist $[K : k] < \infty$ genau dann, wenn $[K : L]$, $[L : k]$ beide $< \infty$ sind.

Beweis. Ist $a_1, \ldots, a_\ell$ eine k-Basis von K, so ist $L \subseteq K$ und daher $\dim_k(L) \leq \ell$; und die a_i bilden ein L-Erzeugenensystem von K, daher $\dim_L(K) \leq \ell$. Sei also $b_1, \ldots, b_m$ eine L-Basis von K, und $c_1, \ldots, c_n$ eine k-Basis von L. Es reicht zu zeigen, dass die $b_i c_j$ eine k-Basis von K sind.

Erzeugendensystem: drücke $\alpha \in K$ als L-lineare Kombination der b_i aus, drücke dann jeden Koeffizient $\lambda_i \in L$ als k-lineare Kombination der c_j aus. Linear unabhängig: Ist $\sum_{i,j} \mu_{ij} b_i c_j = 0$ für $\mu_{ij} \in k$, dann $\sum_j \mu_{ij} c_j = 0$ für jedes i (L-lineare Unabhängigkeit der b_i, also $\mu_{ij} = 0$ für alle i, j (lineare Unabhängigkeit der c_j). ∎

Beispiel $K = \mathbb{Q}(i, \sqrt{2}) = \{a + bi + c\sqrt{2} + di\sqrt{2} \mid a, b, c, d \in \mathbb{Q}\}$ ist ein Körper: Ring weist man leicht nach; wegen $\frac{1}{x+yi} = \frac{x-yi}{x^2+y^2}$ kann man jeden Bruch so umformen, dass der Nenner den Gestalt $p+q\sqrt{2}$ hat; multipliziert man dann oben und unten mit $p - q\sqrt{2}$, so ist der Bruch als Linearkombination von $1, \sqrt{2}, i, i\sqrt{2}$ ausgedrückt. Es ist $[K : \mathbb{Q}] \leq 4$ wegen dieses Erzeugendensystems. Für $L = \mathbb{Q}(\sqrt{2})$ ist $[L : \mathbb{Q}] > 1$, da $\sqrt{2} \notin \mathbb{Q}$; und $[K : L] > 1$, da $i \notin L$. Also $[K : L] = [L : \mathbb{Q}] = 2$ und $[K : \mathbb{Q}] = 4$. Eine $\mathbb{Q}$-Basis von K ist wie oben; $1, \sqrt{2}$ ist eine $\mathbb{Q}$-Basis von L; und $1, i$ ist eine L-Basis von $\mathbb{Q}$.

5.3 Algebraische Elemente

Definition Sei K/k eine KE. Ein Element $\alpha \in K$ heißt *algebraisch* über k, falls es ein Polynom $0 \neq f \in k[X]$ gibt mit $f(\alpha) = 0$. Man darf verlangen, dass f normiert ist.

Man nennt α *transzendent* über k, wenn es nicht algebraisch ist. Ist jedes $\alpha \in K$ algebraisch über k, so heißt die KE K/k algebraisch.

Beispiele $\alpha = \sqrt{2}+\sqrt{3}$ ist algebraisch über $\mathbb{Q}$, da Nullstelle von X^4-10X^2+1. Jedes $\alpha \in k$ ist algebraisch über k, da Nullstelle von $X - \alpha$. Die Erweiterung $\mathbb{C}/\mathbb{R}$ ist algebraisch, da $a + bi$ Nullstelle von $X^2 - 2aX + a^2 + b^2$ ist – später lernen wir aber, dieses einfacher nachzuweisen.

Die Erweiterung $\mathbb{R}/\mathbb{Q}$ ist nicht algebraisch. Entweder zeigt man nichtkonstruktiv, dass es aus Mächtigkeitsgründen transzendente Elemente geben muss; oder man zeigt, dass e bzw. π transzendent ist (Hermite bzw. Lindemann).

Bezeichnung Sei K/k eine KE und $T \subseteq K$ eine Teilmenge. Mit $k(T)$ bezeichnet man den durch T erzeugten Zwischenkörper $k \subseteq k(T) \subseteq K$: der kleinste Zwischenkörper, der T enthält.

Man weist nämlich leicht nach, dass die Schnittmenge aller Zwischenkörper L mit $T \subseteq L$ selbst ein Zwischenkörper ist, also existiert $k(T)$.

Beispiel Für $n \in \mathbb{Z}$ hatten wir bisher $\mathbb{Q}(\sqrt{n})$ als $\{a+b\sqrt{n} \mid a, b \in \mathbb{Q}\}$ definiert; dies wird jetzt zu einer (wahren) Gleichung, es ist nicht mehr die Definition. Auch haben wir oben gezeigt, dass $\mathbb{Q}(i, \sqrt{2})$ eine $\mathbb{Q}$-Basis $1, \sqrt{2}, i, i\sqrt{2}$ hat.

5.4 Das Minimalpolynom eines algebraischen Elements

Satz 5.2 *Sei K/k eine KE und $\alpha \in K$ algebraisch über k. Dann:*

a) Es gibt genau ein normiertes irreduzibles Polynom in $k[X]$, die eine Nullstelle in α hat. Dieses Polynom nennt man das Minimalpolynom m_α *von α.*

b) Sei $f \in k[X]$. Es ist $f(\alpha) = 0$ genau dann, wenn $m_\alpha \mid f$ gilt.

c) Sei $n = \operatorname{grad}(m_\alpha)$. Dann ist $[k(\alpha) : k] = n$, und $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ ist eine k-Basis von $k(\alpha)$.

Beweis. $k[X]$ ist ein Hauptidealring und daher faktoriell. Sei $g \in k[X]$ ein Polynom vom Grad ≥ 1 mit $g(\alpha) = 0$. Dann muss mindestens ein irreduzibler Faktor von g eine Nullstelle in α haben. Die Menge aller Polynome $g \in k[X]$ mit Nullstelle in α bildet ein Ideal, daher ein Hauptideal. Da dieses Hauptideal ein irreduzibles Polynom enthält, muss es durch dieses Polynom erzeugt sein. Zwei Erzeuger eines Hauptideals in einem ID sind assoziiert. Also ist der normierte Erzeuger eindeutig und irreduzibel.

Offensichtlich liegen $1, \ldots, \alpha^{n-1}$ und deren k-Linearkombinationen in $k(\alpha)$. Wären diese n Elemente k-linear abhängig, so hätten wir ein Polynom vom Grad $< n$ mit Nullstelle in α: geht nicht. Jede Linearkombination hat die Gestalt $h(\alpha)$ mit $h \in k[X]$ von Grad $\leq n-1$, also $\operatorname{ggT}(h, m_\alpha) = 1$ (für $h \neq 0$), also ($k[X]$ HIR) gibt es $p, q \in k[X]$ mit $ph + qm_\alpha = 1$. Durch Polynomdivision durch m_α können wir außerdem $\operatorname{grad}(p) \leq n-1$ sicherstellen. Also $\frac{1}{h(\alpha)} = p(\alpha)$ ist eine Linearkombination von $1, \ldots, \alpha^{n-1}$. ∎

Beispiel Es ist $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$: Sei $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $L = \mathbb{Q}(\sqrt{2})$. Dann $[L : \mathbb{Q}] = 2$, da $\sqrt{2}$ hat Minimalpolynom $X^2 - 2$ über $\mathbb{Q}$. Zu zeigen ist jetzt $[K : L] = 2$. Da $K = L(\sqrt{3})$ ist, und $\sqrt{3}$ Nullstelle von $X^2 - 3 \in L[X]$ ist, müssen wir zeigen, dass $X^2 - 3$ irreduzibel in $L[X]$ ist. Wenn nicht, dann ist $\sqrt{3} \in L$. Dann wäre $\sqrt{3} = a + b\sqrt{2}$: dies geht aber nicht. (Nachrechnen!) Also $[K : L] = 2$ und $[K : \mathbb{Q}] = 4$. Eine $\mathbb{Q}$-Basis von L ist $1, \sqrt{2}$; eine L-Basis von K ist $1, \sqrt{3}$; also nach Lemma 5.1 ist $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ eine $\mathbb{Q}$-Basis von K.

Beispiel Ferner ist $\sqrt[3]{2} \notin \mathbb{Q}(\sqrt{2}, \sqrt{3})$: denn sonst wäre $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$, aber $3 = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$ ist kein Teiler von $4 = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$.

Korollar 5.3 *Sei K/k eine KE, und sei $\alpha \in K$. Die folgenden drei Aussagen sind äquivalent:*

a) α ist algebraisch über k;

b) Die KE $k(\alpha)/k$ ist endlich;

c) Es gibt einen Zwischenkörper $k \subseteq L \subseteq K$ mit $\alpha \in L$ und L/k endlich.

Beweis. a) $\Rightarrow$ b) folgt aus dem Satz. Mit $L = k(\alpha)$ folgt c) aus b). Gilt c), so liegen alle Potenzen von α im endlich dimensionalen k-Vektorraum L, daher muss es eine lineare Abhängigkeit geben: also ist α algebraisch. ∎

Hilfslemma Sei K/k eine KE.

a) Ist $\alpha \in K$ algebraisch über k, und ist $k \subseteq L \subseteq K$ ein Zwischenkörper, so ist α auch über L algebraisch.

b) Ist $S = S_1 \cup S_2 \subseteq K$, so ist $k(S) = k(S_1)(S_2)$.

Beweis. a) Ist $f(\alpha) = 0$ und $f \in k[X]$, dann $f \in L[X]$ auch.

b) $k(S_1)(S_2)$ enthält $k(S_1)$ und S_2, also k, S_1 und S_2, also k, S, also $k(S)$. Umgekehrt: $k(S)$ entält k, S_1, S_2; also $k(S_1)$ und S_2; also $k(S_1)(S_2)$. ∎

Lemma 5.4 *a) Sind $\alpha_1, \ldots, \alpha_n \in K$ algebraisch über k, dann ist die KE $k(\alpha_1, \ldots, \alpha_n)/k$ endlich.*

b) Jede endliche KE ist algebraisch.

c) Seien α, β algebraisch über k. Dann sind auch $\alpha \pm \beta$, $\alpha\beta$, $\frac{\alpha}{\beta}$ algebraisch.

Beweis. a) Induktion über n; Induktionsanfang $n = 0$ klar. Wegen Hilfslemma a) ist α_n algebraisch über $L := k(\alpha_1, \ldots, \alpha_{n-1})$. Wegen Hilfslemma b) ist $k(\alpha_1, \ldots, \alpha_n) = L(\alpha_n)$. Induktionsannahme: $[L : k] < \infty$. Korollar 5.3: $[L(\alpha_n) : L] < \infty$. Also Lemma 5.1: $[L : k] < \infty$.

b) Folgt aus Korollar 5.3, c) $\Rightarrow$ a).

c) Die angegebenen Elemente liegen alle in $k(\alpha, \beta)$. Nach den ersten beiden Teilen ist $k(\alpha, \beta)/k$ endlich und daher algebraisch. ∎

Beispiel Daher können wir feststellen, dass $\frac{2-\sqrt{3}+3i}{19-\sqrt{17}}$ algebraisch ist, ohne ein konkretes Polynom ausrechnen zu müssen.

Lemma 5.5 *Sei K/k eine KE.*

a) Ist $k \subseteq L \subseteq K$ ein Zwischenkörper mit L/k algebraisch, und ist $\alpha \in K$ algebraisch über L, dann ist α auch über k algebraisch.

b) Sei $S \subseteq K$ eine Teilmenge. Ist jedes $\alpha \in S$ algebraisch über k, dann ist die Erweiterung $k(S)/k$ algebraisch.

c) Die Menge $L := \{\alpha \in K \mid \alpha$ algebraisch über $k\}$ ist ein Zwischenkörper $k \subseteq L \subseteq K$, und L/k ist algebraisch.

Beweis. a) Sei $f(X) = X^n + a_{n-1}X^n - 1 + \cdots + a_0 \in L[X]$ ein Polynom mit $f(\alpha) = 0$. Sei $M = k(a_0, a_1, \ldots, a_{n-1})$. Dann ist $f \in M[X]$, daher ist α algebraisch über M, und $M(\alpha)/M$ ist endlich. Da jedes a_i algebraisch über k ist, ist M/k endlich. Also ist $M(\alpha)/k$ endlich, weshalb α über k algebraisch ist.

b) Ist $T \subseteq S$ endlich, so ist $k(T)/k$ algebraisch nach Lemma 5.4 a). Es reicht also zu zeigen, dass $k(S) = L$ ist, wobei $L := \bigcup\{k(T) \mid T \subseteq S \text{ endlich}\}$. Offensichtlich gilt $k(S) \supseteq L$; und L enthält k, S. Es reicht also, zu zeigen, dass L ein Körper ist. Wegen $k \subseteq L$ ist $0, 1 \in L$. Nun seien $\alpha, \beta \in L$, also gibt es $T_1, T_2 \subseteq S$ endlich mit $\alpha \in k(T_1)$, $\beta \in k(T_2)$. Sei $T = T_1 \cup T_2$, eine endliche Teilmenge von S: dann $\alpha, \beta \in k(T)$, daher liegen $\alpha \pm \beta$, $\alpha\beta$ und $\frac{\alpha}{\beta}$ in $k(T) \subseteq L$. Also ist L ein Körper.

c) Da jedes $\alpha \in L$ algebraisch ist, ist $k(L)/k$ algebraisch. Nach Definition von L folgt $k(L) \subseteq L$, also $L = k(L)$. ∎

Beispiel Man setzt $\mathbb{A} := \{\alpha \in \mathbb{C} \mid \alpha \text{ algebraisch über } \mathbb{Q}\}$. Dann ist $\mathbb{A}$ ein Körper, genannt der Körper der *algebraischen Zahlen*. Nach c) ist $\mathbb{A}/\mathbb{Q}$ algebraisch. Es ist trotzdem $[\mathbb{A} : \mathbb{Q}] = \infty$, denn $\sqrt[n]{2} \in \mathbb{A}$, also $[\mathbb{A} : \mathbb{Q}] \geq [\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$.

Später zeigen wir: $\mathbb{A}$ ist abzählbar; und der Fundamentalsatz der Algebra gilt auch dann, wenn man $\mathbb{C}$ durch $\mathbb{A}$ ersetzt.

5.5 Das Kronecker-Verfahren

Beispiel Das Polynom $X^3 + X + 1 \in \mathbb{F}_2[X]$ ist irreduzibel, da keine Nullstelle in $\mathbb{F}_2$. Gibt es eine KE $K/\mathbb{F}_2$ derart, dass $X^3 + X + 1$ eine Nullstelle $\alpha \in K$ hat?

Der Vergleich mit der Enstehungsgeschichte der komplexen Zahlen legt es nahe, dass wir uns einfach eine solche Zahl α denken. Dann können wir oBdA $K = \mathbb{F}_2(\alpha)$ nehmen. Nach Satz 5.2 ist dann $[K : \mathbb{F}_2] = 3$. Das Problem: Wir haben die Existenz von K bereits vorausgesetzt. Um die Existenz von K sicherzustellen, benötigen wir den folgenden Satz.

Satz 5.6 (Kronecker) *Sei k ein Körper und $f \in k[X]$ ein irreduzibles Polynom. Dann gibt es eine KE K/k und ein $\alpha \in K$ derart, dass $f(\alpha) = 0$ gilt.*

Folglich ist f das Minimalpolynom $f = m_\alpha$ von α (vorausgesetzt: f normiert). Wir konstruieren K so, dass $K = k(\alpha)$ ist und daher $[K : k] = \operatorname{grad}(f)$.

Beweis. Nach Satz 5.2 müsste dann $f = m_\alpha$ sein.

$k[X]$ ist ein HIR, daher faktoriell. Also ist f prim, und $(f) \lhd k[X]$ ein Primideal. In einem HIR sind Primideale $\neq \{0\}$ maximale Ideale. Also ist $K := k[X]/(f)$ ein Körper. Sei $\alpha := X + (f) \in K$. Indem wir $a \in k$ mit $a + (f) \in K$ identifizieren, können wir K als einen Erweiterungskörper von k betrachten. Offensichtlich ist dann $K = k(\alpha)$. Nun, $\alpha^2 = (X + (f))^2 = X^2 + (f)$, analog ist $g(\alpha) = g(X) + (f)$

für jedes $g \in k[X]$. Insbesondere ist $f(\alpha) = f(X) + (f) = 0 + (f)$. Das heißt, α ist Nullstelle von f. ∎

Beispiel Das Polynom $X^3 + X + 1 \in \mathbb{F}_2[X]$ ist wie gesagt irreduzibel, da keine Nullstelle in $\mathbb{F}_2$. Nach Kronecker gibt es einen Erweiterungskörper K mit $[K : \mathbb{F}_2] = 3$, und ein $\alpha \in K$ mit $\alpha^3 + \alpha + 1 = 0$. Wegen $|\mathbb{F}_2| = 2$ und $\dim_{\mathbb{F}_2}(K) = 3$ folgt $|K| = 8$. Quadrieren wir die Gleichung $\alpha^3 + \alpha + 1 = 0$, erhalten wir $\alpha^6 + \alpha^2 + 1 = 0$, wegen $2 = 0$. Also ist auch $\alpha^2 \in K$ eine Nullstelle. Daher auch $\alpha^4 = \alpha^2 + \alpha$. Da $1, \alpha, \alpha^2$ linear unabhängig über $\mathbb{F}_2$ sind (Satz 5.2), sind diese drei Nullstellen paarweise verschieden, und daher zerfällt $X^3 + X + 1$ in $K[X]$ als ein Produkt

$$X^3 + X + 1 = (X - \alpha)(X - \alpha^2)(X - \alpha^2 - \alpha)$$

von linearen Faktoren: denn der Grad ist drei, und jedes der drei linearen Faktoren muss in der Primfaktorzerlegung vorkommen.

Zum Vergleich: für $K = \mathbb{Q}(\sqrt[3]{2})$ ist

$$X^3 - 2 = (X - \sqrt[3]{2})(X^2 + \sqrt[3]{2}X + \sqrt[3]{4})$$

die Primfaktorzerlegung in $K[X]$ von $X^3 - 2$.

Korollar 5.7 *Sei k ein Körper, und seien $f_1, \ldots, f_n \in k[X]$ Polynome vom Grad ≥ 1. Es gibt eine endliche Körpererweiterung K/k derart, dass jedes der f_i mindestens eine Nullstelle in K hat.*

Beweis. Induktion über n. Klar für $n = 0$. Nun sei $n \geq 1$, und sei L/k eine endliche Erweiterung derart, dass $f_1, \ldots, f_{n-1}$ jeweils mindestens eine Nullstelle in L haben. Wegen $\text{grad}(f_n) \geq 1$ und $L[X]$ faktoriell, gibt es ein irreduzibles Polynom $g \in L[X]$ mit $g \mid f_n$. Nach Kronecker hat L eine endliche Erweiterung K/L derart, dass g – und daher auch f_n – eine Nullstelle in K hat. Mit K/L und L/k ist auch K/k endlich. ∎

5.6 Der algebraische Abschluss

Hilfslemma Für einen Körper k sind die folgenden drei Aussagen äquivalent:

a) Jedes Polynom $f \in k[X]$ vom Grad ≥ 1 hat mindestens eine Nullstelle in k;

b) Jedes (normierte) Polynom $f \in k[X]$ vom Grad ≥ 1 zerfällt in $k[X]$ als ein Produkt von linearen Faktoren

$$f(X) = \prod_{i=1}^{n} (X - a_i)\,,$$

wobei $a_i \in k$ gilt für jedes i.

c) Die einzigen irreduziblen Polynome in $k[X]$ sind die der Gestalt $X - a$ für $a \in k$.

Beweis. b) $\Rightarrow$ a): jedes a_i ist eine Nullstelle. a) $\Rightarrow$ b): Induktion über $n = \text{grad}(f)$: ist a eine Nullstelle, dann $f(X) = (X - a)g(X)$ für ein $g \in k[X]$ mit $\text{grad}(g) = n - 1$. b) $\Leftrightarrow$ c) ist klar. ∎

Definition Sei k ein Körper.

a) Ein Erweiterungskörper K von k heißt ein *algebraischer Abschluss* von k, wenn K/k algebraisch ist, und außerdem jedes (normierte) Polynom $f \in k[X]$ in $K[X]$ als Produkt von linearen Faktoren zerfällt.

b) k heißt *algebraisch abgeschlossen*, wenn es sein eigener algebraischer Abschluss ist, d.h. falls jedes Polynom $f \in k[X]$ vom Grad ≥ 1 mindestens eine Nullstelle in k hat.

Beispiel Der Fundamentalsatz der Algebra besagt, dass $\mathbb{C}$ algebraisch abgeschlossen. Wegen $\mathbb{C} = \mathbb{R}(i)$ ist $\mathbb{C}$ ein algebraischer Abschluss von $\mathbb{R}$. Da $e \in \mathbb{C}$ transzendent ist, ist $\mathbb{C}$ zu groß, als dass es ein algebraischer Abschluss von $\mathbb{Q}$ sein könnte.

Lemma 5.8 *Sei K/k eine KE.*

a) Ist K ein algebraischer Abschluss von k, so ist K algebraisch abgeschlossen[4]*.*

b) Ist K algebraisch abgeschlossen, so ist $L := \{\alpha \in K \mid \alpha \text{ algebraisch über } k\}$ ein algebraischer Abschluss von k.

c) Ist K ein algebraischer Abschluss von k und L ein Zwischenkörper $k \subseteq L \subseteq K$, so ist K auch ein algebraischer Abschluss von L.

Beweis. a) Ist K nicht algebraisch abgeschlossen, so gibt es ein (normiertes) irreduzibles Polynom $f \in K[X]$ vom Grad $n \geq 2$. Nach Kronecker gibt es einen Erweiterungskörper $M = K(\alpha)$ mit $f(\alpha) = 0$ und $\alpha \notin K$. Da K/k algebraisch ist, besagt Lemma 5.5 a), dass α über k algebraisch ist. Sei $g \in k[X]$ das Minimalpolynom. Da K ein algebraischer Abschluss ist, zerfällt g in $K[X]$ als ein Produkt von linearen Faktoren. Wegen $g(\alpha) = 0$ muss einer dieser linearen Faktoren $X - \alpha$ sein, also $\alpha \in K$. Widerspruch.

b) Schon gesehen: L ist Körper, und L/k algebraisch. Sei $X - \alpha \in K[X]$ ein linearer Faktor von $f(X) \in k[X]$, dann ist $f(\alpha) = 0$, daher α algebraisch über k, daher $\alpha \in L$. Zerfällt $f \in k[X]$ daher in $K[X]$ als Produkt von linearen Faktoren, so liegen diese linearen Faktoren bereits in $L[X]$.

[4]Vgl.: Wenn ich die Tür zumache, dann ist die Tür zu.

c) S. Übungsserie Nr. 7. ∎

Beispiel Wegen $\mathbb{A} := \{\alpha \in \mathbb{C} \mid \alpha \text{ algebraisch über } \mathbb{Q}\}$ ist $\mathbb{A}$ algebraisch abgeschlossen und der algebraischer Abschluss von $\mathbb{Q}$.

Lemma 5.9 *$\mathbb{A}$ ist abzählbar. Somit ist fast jede komplexe Zahl transzendent.*

Beweis. Jedes $\alpha \in \mathbb{A}$ ist Nullstelle eines normierten Polynoms $f \in \mathbb{Q}[X]$. Die Menge der normierten Polynome vom Grad n steht in Bijektion mit $\mathbb{Q}^n$: man packt die Koeffizienten in einem n-Tupel. Jedes solche Polynom hat höchstens n verschiedene Nullstellen in $\mathbb{C}$. Da $\mathbb{Q}^n \times \{1, \ldots, n\}$ abzählbar ist, sind nur abzählbar viele komplexe Zahlen Nullstelle eines Polynoms von diesem Grad n. Es gibt nur abzählbar viele Grade n, also ist $\mathbb{A}$ abzählbar. ∎

5.7 Existenz algebraisch abgeschlossener Körper

Satz 5.10 *Jeder Körper hat einen algebraischen Abschluss.*

Beweis. Es gibt zwei Beweismethoden. Beide sind lang. Eine setzt mehr Mengenlehre voraus, als wir bisher hatten. Wir wählen die andere, die den Nachteil hat, dass die Details sich besonders gut unter den Teppich verstecken lassen. Der Beweis gliedert sich in mehreren Schritten. In den ersten Schritten geben wir ein Verfahren, das zu jedem Körper k einen Erweiterungskörper $K(k)$ konstruiert derart, dass jedes Polynom $f \in k[X]$ vom Grad ≥ 1 mindestens eine Nullstelle in $K(k)$ hat. Sei k ein Körper.

Schritt 1 Das Ideal I.

Sei $F = \{f \in k[X] \mid \text{grad}(f) \geq 1\}$. Betrachten wir den Polynomring $R = k[X_f \mid f \in F]$, deren Unbestimmten durch die Elemente von F indiziert sind. Wegen $k \subseteq R$ macht $g(r)$ Sinn für jedes $g \in k[X]$ und für jedes $r \in R$. Insbesondere macht $f(X_f)$ Sinn für jedes $f \in F$. Sei $I \lhd R$ das Ideal $I = (f(X_f) \mid f \in F)$.

Schritt 2 I ist ein echtes Ideal.

Wenn nicht, dann gibt es $r_1, \ldots, r_n \in R$ und $f_1, \ldots, f_n \in F$ mit

$$\sum_{j=1}^{n} r_j f_j(X_{f_j}) = 1\,. \qquad (*)$$

Beachte, dass jedes $r \in R$ ein Polynom in *endlich viele* der X_f ist, die Koeffizienten sind aus k. Also gibt es $f_{n+1}, \ldots, f_m$ derart, dass jedes r_j in $k[X_{f_1}, \ldots, X_{f_m}]$ liegt. Nach Korollar 5.7 also gibt es eine endliche Erweiterung L/k und Elemente $\alpha_1, \ldots, \alpha_m \in L$ derart, dass $f_j(\alpha_j) = 0$ gilt für jedes $1 \leq j \leq m$. Da R ein Polynomring ist, dürfen wir in Gleichung (*) jedes X_{f_j} durch α_j ersetzen. Wegen $f_j(\alpha_j)$ wird die linke Seite Null. Widerspruch. Also ist I doch ein echtes Ideal.

Schritt 3 Die Erweiterung $K(k)/k$.

Nach Lemma 3.7 gibt es ein maximales Ideal $P \lhd R$ mit $I \subseteq P$. Nach Lemma 3.6 ist der Quotientenring $K(k) := R/P$ ein Körper. Der Ringhomomorphismus $\phi\colon k \to K(k)$, $\phi(a) = a + P$ ist ein Homomorphismus zwischen Körpern und daher injektiv. Indem wir k mit seinem Bild unter ϕ identifizieren, dürfen wir $K(k)$ als einen Erweiterungskörper von k betrachten.

Schritt 4 Jedes $f \in F$ hat eine Nullstelle in $K(k)$.

Für $f \in F$ sei $\alpha_f = X_f + P \in K(k)$. Dann $f(\alpha_f) = 0$, vgl. Kronecker-Beweis.

Schritt 5 Jetzt $k \mapsto K(k)$ iterieren.

Jedes Polynom $f \in k[X]$ hat eine Nullstelle in $K(k)[X]$: unklar ist aber, ob zwingend daraus folgt, dass f als Produkt von linearen Faktoren zerfällt. Wegen dieser Problematik benutzt man einen Trick: man betrachtet den Erweiterungskörper $K^2(k)$ von $K(k)$, dort hat auch jedes Polynom in $K(k)[X]$ mindestens eine Nullstelle; dann betrachtet man den Erweiterungskörper $K^3(k)$ von $K^2(k)$, usw. Es ist

$$k \subseteq K(k) \subseteq K^2(k) \subseteq K^3(k) \subseteq \cdots . \qquad (**)$$

Sei also $K = \bigcup_{n\geq 0} K^n(k)$. Dann ist K ein Körper, und eine Erweiterung von k.

Schritt 6 K algebraisch abgeschlossen, also fertig.

Nach Lemma 5.8 b) gilt: ist K algebraisch abgeschlossen, dann hat k einen algebraischen Abschluss. Sei $f \in K[X]$ mit $\operatorname{grad}(f) = 1$. Zuu zeigen ist: f hat eine Nullstelle in K. Da K die aufsteigende Vereinigung der $K^n(k)$ ist, und f nur endlich viele Koeffizienten hat, gibt es ein n mit $f \in K^n(k)[X]$. Nach Konstruktion von $K^{n+1}(k)$ hat also f eine Nullstelle in $K^{n+1}(k) \subseteq K$.

Schritt 7 (**) ist eine Notlüge, aber reparierbar.

Um $K(k)$ als Erweiterungskörper von k zu erhalten, ersetzen wir k durch seine Kopie $\phi(k)$. Kein Problem, wenn man nur endlich oft iteriert: aber schon bedenklich in unserem Fall. Die richtige Version von (**) ist, dass wir injektive Homomorphismen

$$k \to K(k) \to K^2(k) \to K^3(k) \to \cdots$$

haben. Wie sollen wir jetzt K bilden?

Eine Lösung: wir betrachten die disjunkte Vereinigung $V = \biguplus_{n\geq 0} K^n(k)$ und die Äquivalenzrelation

$$x \in K^n(k) \ \sim\ y \in K^m(k) \quad \Longleftrightarrow \quad x, y \text{ haben das gleiche Bild in } K^\ell(k)$$

für $\ell = \max(m, n)$. (Transitivität ist OK, da jeder Homomorphismus injektiv). Dann kann man jeden $K(k)$ in die Menge der Äquivalenzklassen einbetten: so kann man doch die Vereinigung bilden. ∎

Es gibt mehr Körper, als man denkt

Inzwischen kennen wir einige Verfahren, um neue Körper herzustellen:

- Am Anfang waren $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$.
- Ist R ein kommutativer Ring und $I \lhd R$ ein maximales Ideal, so ist der Quotientenring R/I ein Körper. Insbesondere für $R = \mathbb{R}$ und $I = p\mathbb{Z}$ (p eine Primzahl) enthält man den endlichen Körper $\mathbb{F}_p$.
- Jeder Integritätsbereich R hat einen Quotientenkörper $Q(R)$. So ensteht $\mathbb{Q}$ aus $\mathbb{Z}$. Ist R ein Polynomring $R = k[X_1, \ldots, X_n]$ über einen Körper k, so erhält man den Körper der *rationalen Funktionen* $k(X_1, \ldots, X_n)$.
- Kronecker: ist k ein Körper und $f \in k[X]$ irreduzibel, so erhält man einen Erweiterungskörper K mit $[K : k] = \text{grad}(f)$ derart, dass f in K eine Nullstelle hat. Mit $f = X^2 + 1$ entsteht so $\mathbb{C}$ aus $\mathbb{R}$. Mit $f = X^2 + X + 1$ entsteht $\mathbb{F}_4$ aus $\mathbb{F}_2$. Das Verfahren lässt sich auch iterieren.
- Ist K/k eine Körperweiterung, so ist $L = \{\alpha \in K \mid \alpha \text{ algebraisch über } k\}$ ein Körper, und L/k ist algebraisch. So entsteht $\mathbb{A}$ aus $\mathbb{C}/\mathbb{Q}$.
- Jeder Körper hat einen algebraischen Abschluss. Auch so entsteht $\mathbb{A}$ aus $\mathbb{Q}$. Der algebraische Abschluss von $\mathbb{C}(X)$ wird größer als $\mathbb{C}$ sein.

6 Zirkel und Lineal: Die Unlösbarkeit klassischer Probleme

Nach den alten Griechen ist die wertvollste Geometrie die, die nur vom Zirkel und vom (unmarkierten) Lineal Gebrauch macht. Trotz intensiver Suche gelang es ihnen nicht, die folgenden drei Probleme zu lösen. Dies liegt daran, dass diese drei Probleme unlösbar sind – was erst im 19. Jahrhundert nachgewiesen wurde.

- **Das delische Problem: die Würfelverdopplung** Gauß behauptete die Unlösbarkeit; Wantzel veröffentlichte 1837 den ersten Beweis.
- **Die Dreiteilung eines beliebigen Winkels** Gauß behauptete die Unlösbarkeit; Wantzel veröffentlichte 1837 den ersten Beweis. Wichtig ist das Wort „beliebig“: die Dreiteilung mancher Winkel – $\frac{\pi}{2}$ etwa – ist möglich.
- **Die Quadratur des Kreises** Erstmalige Erwähnung 1650 v. Chr. im Papyrus Rhind. Die Unlösbarkeit wurde erst 1880 endgültig nachgewiesen, als Lindemann zeigte, dass π transzendent ist.

In der Neuzeit gilt die Quadratur des Kreises als das bedeutendste der drei Probleme, in der Antike war es aber das delische Problem. Mehr zur Geschichte:
`http://www-groups.dcs.st-and.ac.uk/~history/Indexes/Greeks.html`

6.1 Eine moderne Formulierung

Sei M eine endliche Menge von Punkten der Ebene. Jede Gerade, die mindestens zwei Punkte aus M enthält, nennen wir eine Gerade in M. Sind P und Q_1, Q_2 Punkte aus M, so nennt man den Kreis um P mit Radius $|Q_1Q_2|$ einen Kreis in M. Es gibt drei mögliche Wege, die Punktmenge M zu vergössern:

Schritt M1: Man fügt den Schnittpunkt zweier Geraden in M hinzu;

Schritt M2: Man fügt die beiden Schnittpunkten von zwei Kreisen in M hinzu;

Schritt M3: Man fügt die beiden Schnittpunkten von einer Gerade und einem Kreis in M hinzu.

Indem wir *eine* dieser drei Operationen *einmal* ausführen, erhalten wir eine neue Punktmenge $M' \supseteq M$. Durch iterieren erhalten wir eine Folge von Mengen

$$M, M', M'', \ldots, M^{(n)}, \ldots .$$

Dann lauten die drei Unlösbarkeitsaussagen so:

Würfelverdopplung: $M = \{(0,0),(1,0)\}$. Egal wie wir die zulässigen Operationen ausführen: $(\sqrt[3]{2}, 0)$ liegt in keinem $M^{(n)}$.

Winkeldreiteilung: $M = \{(0,0),(1,0),(\cos\alpha,\sin\alpha)\}$. Mit z.B. $\alpha = \frac{\pi}{3}$ liegt der Punkt $(\cos\frac{\alpha}{3},\sin\frac{\alpha}{3})$ in keinem $M^{(n)}$.

Quadratur des Kreises: $M = \{(0,0),(1,0)\}$. Kein $M^{(n)}$ enthält $(\sqrt{\pi},0)$.

Bemerkung Für die Würfelverdopplung ist eigentlich zu zeigen: kein $M^{(n)}$ enthält Punkt P,Q mit $|PQ| = \sqrt[3]{2}$. Gebe es aber solche Punkte, so könnte man $(\sqrt[3]{2},0) \in M^{(n+1)}$ organisieren, denn die x-Achse ist bereits eine Gerade in M, und der Kreis um $(0,0)$ mit Radius $\sqrt[3]{2}$ wäre dann ein Kreis in $M^{(n)}$.

6.2 Eine Körpererweiterungen-Formulierung

Für eine solche Punktmenge $M = \{(x_1,y_1),\ldots,(x_m,y_m)\}$ schreiben wir K für den Körper $K = \mathbb{Q}(x_1,y_1,\ldots,x_m,y_m)$: es ist also K der kleinste Körper, der die x- und y-Koordinaten von jedem Punkt aus M enthält.

Lemma 6.1 *Es ist $[K' : K] \in \{1,2\}$. Daher ist jedes $[K^{(n)} : K]$ eine Zweierpotenz.*

Beweis. Der zweiter Teil folgt aus dem ersten. Kommen wir zum ersten Teil. Die Gerade durch $P = (p,q)$ und $R = (r,s)$ hat Geradengleichung $ax + by = c$ für (a,b,c) eine Lösung zum Gleichungssystem

$$ap + bq - c = 0$$
$$ar + bs - c = 0$$

Indem wir $a = 1$ – oder $a = 0$ und $b = 1$ – verlangen, stellen wir sicher, dass a,b,c in $\mathbb{Q}(p,q,r,s)$ liegen. Umgekehrt enthält die Gerade mit Gleichung $ax + by = c$ mit $(\frac{c}{a},0)$ und $(0,\frac{c}{b})$ mindestens zwei Punkte, deren Koordinaten alle in $\mathbb{Q}(a,b,c)$ liegen – auch wenn $ab = 0$ findet man leicht zwei solche Punkte.

Schritt M1: die Geraden haben die Gleichungen $ax + by = c$, $a'x + b'y = c'$ mit $a,b,c,a',b',c' \in K$. Der Schnittpunkt $P = (p,q)$ ist die einzige Lösung. Es ist also $p,q \in K$, daher in diesem Fall $K' = K$.

Schritt M2: $X = (x,y)$ liegt genau dann auf der Gerade durch $A = (a,b)$ und $C = (c,d)$, falls es $t \in \mathbb{R}$ gibt mit $x = ta+(1-t)c$, $y = tb+(1-t)d$. Es liegt genau dann auf dem Kreis um $P = (p,q)$ mit Radius r, wenn $(x-p)^2 + (y-q)^2 = r^2$ gilt. Die Schnittpunkte des Kreises mit der Gerade sind dann für t eine Lösung von

$$(ta + (1-t)c - p)^2 + (tb + (1-t)d - q)^2 = r^2\,.$$

Das heißt, für t Lösung einer quadratischen Gleichung mit Koeffizienten aus $\mathbb{Q}(a,c,p,b,d,q,r^2)$. Da r der Abstand zwischen zwei Punkte aus M ist, ist auch $r \in K$, also sind die Koeffizenten der quadratischen Gleichung alle in K. Bei

einer quadratischen Gleichung gilt: jeder Körper, der eine Nullstelle enthält, enthält auch die andere. Also gibt es L mit $[L : K] \in \{1, 2\}$ und L enthält beide Nullstellen: der Fall $[L : K] = 1$ ist der Fall, wo die Nullstellen bereits in K liegen. Setzen wir die beiden Werten von t in $x = ta + (1-t)c$, $y = tb + (1-t)d$, so erhalten wir die beiden Schnittpunkten, und es ist $K' = L$.

Schritt M3: Zu lösen ist jetzt das Gleichungssystem

$$(x-a)^2 + (y-b)^2 = r^2$$
$$(x-c)^2 + (y-d)^2 = s^2$$

mit $a, b, c, d, r^2, s^2 \in K$. Zieht man die zweite Gleichung von der ersten ab, so erhält man die Geradengleichung

$$2(c-a)x + 2(d-b)y = r^2 + c^2 - s^2 - a^2$$

mit Koeffizienten aus K. Wie oben angemerkt, hat diese Geradengleichung eine Parameterform

$$x = ta' + (1-t)c' \qquad\qquad y = tb' + (1-t)d'$$

mit $a', b', c', d' \in K$, obwhol (a', b'), (c', d') nicht in M liegen müssen. Mit dieser Parameterform sind wir jetzt in der Situation von M2. ∎

Satz: Unlösbarkeit der klassischen Probleme *Mit Zirkel und Lineal sind die Würfelverdopplung, die Dreiteilung des Winkels $\frac{\pi}{3}$ und – die Transzendenz von π vorausgesetzt – die Quadratur des Kreises unmöglich.*

Beweis. **Würfelverdopplung:** Für $K = \mathbb{Q}$ ist zu zeigen: kein $K^{(n)}$ enthält $\sqrt[3]{2}$.

Nach Lemma 6.1 ist $[K^{(n)} : \mathbb{Q}]$ eine Zweierpotenz. Wäre $\sqrt[3]{2} \in K^{(n)}$, dann $\mathbb{Q}(\sqrt[3]{2}) \subseteq K^{(n)}$. Wegen $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ und $[M : k] = [M : L][L : k]$ müsste dann $[K^{(n)} : \mathbb{Q}]$ durch 3 teilbar sein, Widerspruch.

Winkeldreiteilung: Es ist $K = \mathbb{Q}(\sin\alpha, \cos\alpha)$. Mit $\alpha = \frac{\pi}{3}$ ist $K = \mathbb{Q}(\sqrt{3})$, also ist $[K : \mathbb{Q}] = 2$, und jedes $[K^{(n)} : \mathbb{Q}]$ ist eine Zweierpotenz. Sei $\beta = \cos\frac{\pi}{9}$ und $\gamma = \frac{1}{\beta}$. Es reicht zu zeigen, dass das Minimalpolynom von γ über $\mathbb{Q}$ Grad 3 hat, dann ist $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 3$, weshalb γ und deshalb β in keinem $K^{(n)}$ enthalten sein kann.

Bekanntlich ist $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$, also mit $\theta = \frac{\pi}{9}$ ist $\frac{1}{2} = 4\beta^3 - 3\beta$, also $8\beta^3 - 6\beta - 1 = 0$, also $\gamma^3 + 6\gamma^2 - 8 = 0$. Mit der Substitution $\gamma = \delta - 1$ erhalten wir $\delta^3 + 3\delta^2 - 9\delta - 3 = 0$. Nach Eisenstein ($p = 3$) und Gauß ist $X^3 + 3X^2 - 9X - 3 \in \mathbb{Q}[X]$ irreduzibel, daher $X^3 + 6X - 8$ auch. Also ist $X^3 + 6X - 8$ das Minimalpolynom von γ. Wie behauptet, hat das Minimalpolynom von γ Grad 3.

Quadratur des Kreises: Es ist $K = \mathbb{Q}$, daher ist jeder $K^{(n)}$ eine endliche Erweiterung von $\mathbb{Q}$. Da aber π transzendent ist, liegt es in keiner endlichen Erweiterung von $\mathbb{Q}$. Jeder Körper, der $\sqrt{\pi}$ enthält, enthält auch π. ∎

7 Normale und separable Erweiterungen

7.1 Der Zerfällungskörper

Bezeichnung Sei k ein Körper, sei $0 \neq f \in k[X]$ ein Polynom, und sei $a \in k$ eine Nullstelle von f. Dann kommt das irreduzible Polynom $X - a$ in der Primfaktorzerlegung von $f \in k[X]$ vor, und zwar mit Vielfachheit $\nu_{X-a}(f)$. Diese Vielfachheit nennen wir die Vielfachheit $\nu_a(f)$ von a als Nullstelle von f. Für $n = \nu_a(f)$ ist dann $f = (X-a)^n g$ mit $g \in k[X]$ und $g(a) \neq 0$.

Hilfslemma Sei $f \in k[X]$ mit $\operatorname{grad}(f) = n \geq 1$. Dann

$$\sum_{a \in k} \nu_a(f) \leq n\,.$$

Das heißt, auch gezählt mit Vielfachheiten gibt es höchstens n Nullstellen von f.

Beweis. Die Primfaktorzerlegung ist eindeutig. Aus Gradgründen kann es höchstens n Faktoren geben. ∎

Definition Sei K/k eine Körpererweiterung und $f \in k[X]$ ein Polynom mit $\operatorname{grad}(f) \geq 1$. Genau dann heißt K ein *Zerfällungskörper* von f über k, wenn jedes die beiden folgenden Bedingungen gelten:

(Z1) In $K[X]$ zerfällt f als einProdukt von linearen Faktoren;

(Z2) Kein echter Zwischenkörper $k \subseteq L \subsetneq K$ erfüllt (Z1).

Beispiel $\mathbb{C}$ ist nicht der Zerfällungskörper von X^2+1 über $\mathbb{Q}$, da es nicht (Z2) erfüllt; dagegen ist $\mathbb{Q}(i)$ der Zerfällungskörper.

Lemma 7.1 *Sei $f \in k[X]$ ein Polynom. Dann f hat einen Zerfällungskörper K, und es ist $[K : k] \leq n!$*

Beweis. OBdA ist f normiert. Sei L ein algebraischer Abschluss von k. Seien $\alpha_1, \ldots, \alpha_m \in L$ die Nullstellen (mit Vielfachheiten) von f; dann ist $m = n$, da L algebraisch abgeschlossen ist, und $f = \prod_{r=1}^{n}(X - \alpha_r)$. Diese Faktorisierung gilt bereits in $K[X]$ für $K = k(\alpha_1, \ldots, \alpha_n)$. Dann ist jedes α_r algebraisch, also ist K/k endlich; und offensichtlich ist K der kleinste Körper, wo eine solche Faktorisierung möglich ist. Also ist K Zerfällungskörper.

Gradaussage: Wir zeigen $[K : k] \leq n!$ per Induktion über n. Fall $n = 1$ klar. Es ist $[k(\alpha_1) : k] \leq n$, da das Minimalpolynom von α_1 ein Faktor von f ist. Und K ist auch Zerfällungskörper des Polynoms $\frac{f}{X-\alpha_1} \in k(\alpha_1)[X]$, also Induktionsannahme anwenden. ∎

Bemerkung Ganz allgemein gilt: zerfällt $f \in k[X]$ in $K[X]$ als $f = \prod_{r=1}^{n}(X - \alpha_r)$, so ist $k(\alpha_1, \ldots, \alpha_r)$ Zerfällungskörper.

Beispiel $\mathbb{Q}(\sqrt[3]{2})$ ist nicht Zerfällungskörper von $X^3 - 2 \in \mathbb{Q}[X]$, da es nur 1 statt 3 Nullstellen enthält. Die weiteren Lösungen sind $\omega\sqrt[3]{2}$ und $\omega^2\sqrt[3]{2}$ für $\omega = \frac{1}{2}(-1 + \sqrt{-3})$, eine kubische Einheitswurzel. Als Quotient von zwei Nullstellen liegt auch ω im Zerfällungskörper, daher $\sqrt{-3}$ auch. Der Zerfällungskörper ist $\mathbb{Q}(\sqrt[3]{2}, \omega)$, mit Erweiterungsgrad 6 über $\mathbb{Q}$: kann höchstens $6 = 3!$ sein; wegen $\sqrt[3]{2}$ durch 3 teilbar; wegen ω mit Minimalpolynom $X^2 + X + 1$ durch 2 teilbar.

Beispiel $X^4 - 2 \in \mathbb{Q}[X]$ ist irreduzibel. Die Nullstellen sind $\pm\sqrt[4]{2}$ und $\pm i\sqrt[4]{2}$, also ist $\mathbb{Q}(\sqrt[4]{2}, i)$ der Zerfällungskörper. Erweiterungsgrad des Zerfällungskörpers ist 8, nicht $4! = 24$: denn $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ da $X^4 - 2$ irreduzibel; und wegen $\mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R}$ ist $X^2 + 1$ irreduzibel in $\mathbb{Q}(\sqrt[4]{2})[X]$, daher $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] = 2$.

7.2 Erweiterungen und Morphismen

Bisher sind wir stillschweigend davon ausgegangen, dass jede algebraische Erweiterung von $\mathbb{Q}$ ein Teilkörper von $\mathbb{C}$ ist. Wir werden jetzt sehen, dass dies gerechtfertigt ist. Gleichzeitig machen wir die ersten Schritte auf dem Weg, der zum Erkenntnis führt, dass die Automorphismen, die eine Körpererweiterung zulässt, ein sehr wichtiges Merkmal dieser Erweiterung sind.

Zur Erinnerung: jeder Ringhomomorphismus zwischen zwei Körpern ist injektiv.

Satz 7.2 *Sei L/k eine algebraische Erweiterung und K ein algeraisch abgeschlossener Körper. Dann: jeder Homomorphismus $\phi\colon k \to K$ lässt sich zu einem Homomorphismus $\Phi\colon L \to K$ mit $\Phi|_k = \phi$ fortsetzen.*

Für den Beweis und auch an einigen anderen Stellen benötigen wir das folgende Lemma:

Lemma 7.3 *Sei $\phi\colon k \to k_1$ ein Isomorphismus von Körpern. Seien L/k und L_1/k_1 Körpererweiterungen; sei $\alpha \in L$ algebraisch mit Minimalpolynom $f \in k[X]$; und sei $\beta \in L_1$ eine Nullstelle des Polynoms $\phi(f) \in k_1[X]$. Dann hat ϕ genau eine Fortsetzung $\Phi\colon k(\alpha) \to k_1(\beta)$, die $\Phi|_k = \phi$ und $\Phi(\alpha) = \beta$ erfüllt.*

Hier ist $\phi(f) \in k_1[X]$ das Polynom das entsteht, wenn man ϕ auf den Koeffizienten von f anwendet.

Beweis. Da ϕ ein Isomorphismus ist, ist $\phi(f)$ irreduzibel, denn f ist irreduzibel. Daher ist $k(\alpha) \cong k[X]/(f)$, mit $\alpha \leftrightarrow X + (f)$; und $k_1(\beta) \cong k_1[X]/(\phi(f))$, $\beta \leftrightarrow X + (\phi(f))$. Ferner induziert ϕ ein Isomorphismus $k[X]/(f) \to k_1[X]/(\phi(f))$, $g + (f) \mapsto \phi(g) + (\phi(f))$. Also existiert Φ. Da $k(\alpha)$ eine k-Basis hat, die aus Potenzen von α besteht, ist Φ auch eindeutig. ∎

Beweis von Satz 7.2. Sei $\mathcal{F}$ die Menge aller Paare (M, ψ), wobei $k \subseteq M \subseteq L$ ein Zwischenkörper ist, und $\psi\colon M \to K$ ein Homomorphismus ist, der ϕ fortsetzt. Betrachten wir die Teilordnung auf $\mathcal{F}$ gegeben durch $(M, \psi) \leq (M', \psi')$ falls $M \subseteq M'$ ist und dazu $\psi'|_M = \psi$. Wir werden zeigen, dass $\mathcal{F}$ ein maximales Element (M_0, ψ_0) enthält; und dass $M_0 = L$ gilt für jedes maximale Element.

Es ist $\mathcal{F} \neq \emptyset$, denn $(k, \phi) \in \mathcal{F}$. Ist $[L : k] < \infty$, dann ist $[L : k]$ eine obere Schranke für $[M : k]$, daher existieren maximale Elemente. Ist $[L : k]$ unendlich, so benutzen wir das Zornsche Lemma. Ist $(M_i, \psi_i)_{i \in I}$ eine Kette in $\mathcal{F}$, so zeigt man leicht, dass $(M, \psi) \in \mathcal{F}$ eine obere Schranke ist, für $M = \bigcup_{i \in I} M_i$ und $\psi|_{M_i} = \psi_i$ für alle i. Nach dem Zornschen Lemma existiert also ein maximales Element.

Sei also (M, ψ) maximal in $\mathcal{F}$. Zu zeigen ist $M = L$. Angenommen also $\alpha \in L \setminus M$. Da L/k algebraisch ist, ist α algebraisch über M. Sei $f \in M[X]$ das Minimalpolynom. Da K algebraisch abgeschlossen ist, hat $\psi(f)$ eine Nullstelle $\beta \in K$. Nach Lemma 7.3 lässt sich ψ zu einem Homomorphismus $\psi'\colon M(\alpha) \to K$ fortsezten. Also $(M(\alpha), \psi') \in \mathcal{F}$, ein Widerspruch zur Maximalität von (M, ψ). Fazit: $M = L$. ∎

Beispiel Sei k eine algebraische Erweiterung von $\mathbb{Q}$. Dann gibt es $\phi\colon k \to \mathbb{C}$ Mit $\phi(a) = a$ für alle $a \in \mathbb{Q}$. Daher ist k zum Teilkörper $\phi(k)$ des $\mathbb{C}$ isomorph.

Lemma 7.4 *Seien L, K zwei Erweiterungskörper von k. Sei $\phi\colon L \to K$ ein Homomorphismus mit $\phi|_k = \mathrm{Id}_k$. Sei $\alpha \in L$ eine Nullstelle von $f \in k[X]$. Dann ist auch $\phi(\alpha) \in K$ eine Nullstelle von f.*

Beweis. Es ist $0 = \phi(f(\alpha)) = \phi(f)(\phi(\alpha)) = f(\phi(\alpha))$. ∎

Beispiel Sei $\phi\colon \mathbb{Q}(i) \to \mathbb{C}$ ein Homomorphismus. Aus $\phi(1) = 1$ folgt $\phi(n) = n$, $\phi(\frac{1}{n}) = \frac{1}{n}$ und daher $\phi(a) = a$ für jedes $a \in \mathbb{Q}$. Nach Lemma 7.4 muss $\phi(i)$ eine Nullstelle von $X^2 + 1$ sein, d.h. $\phi(i) = \pm i$.

Lemma 7.5 *Sei L/k eine algebraische Erweiterung und $\phi\colon L \to L$ ein Homomorphismus mit $\phi|_k = \mathrm{Id}_k$. Dann ist ϕ ein Automorphismus von L.*

Beweis. Wir müssen Surjektivität nachweisen. Sei $\alpha \in L$. Sei $f \in k[X]$ das Minimalpolynom von α. Seien $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_r$ die verschiedenen Nullstellen von f in L: es ist dann $r \leq \mathrm{grad}(f) < \infty$. Für jedes i ist $f(\phi(\alpha_i)) = 0$ nach Lemma 7.4, also ist jedes $\phi(\alpha_i)$ ein α_j. Da ϕ injektiv ist, permutiert es daher die α_i. Also gibt es ein α_i mit $\phi(\alpha_i) = \alpha_1 = \alpha$. ∎

Korollar 7.6 *Bis auf Isomorphie ist der algebraischer Abschluss von k eindeutig.*

Beweis. Seien L, K zwei algebraische Abschlüsse von k. Nach Satz 7.2 gibt es Homomorphismen $\phi\colon L \to K$ und $\psi\colon K \to L$ mit $\phi|_k = \psi|_k = \mathrm{Id}_k$. Nach Lemma 7.5 ist $\phi \circ \psi$ ein Isomorphismus und daher surjektiv. Also ist ϕ surjetkiv und daher ein Isomorphismus. ∎

Korollar 7.7 *Für jedes Polynom $f \in k[X]$ ist der Zerfällungskörper bis auf Isomorphismus eindeutig. Daher ist die Anzahl der Nullstellen in jedem Zerfällungskörper gleich. Mehr noch: für jedes $d \geq 1$ ist die Anzahl der Nullstellen mit Vielfachheit d in jedem Zerfällungskörper gleich. Ist f irreduzibel, so haben alle Nullstellen die gleiche Vielfachheit.*

Beweis. Seien K, L zwei Zerfällungskörper. Sei $\bar{K}$ bzw. $\bar{L}$ ein algebraischer Abschluss von K bzw. von L. Nach Lemma 5.5 a) sind $\bar{K}, \bar{L}$ algebraische Abschlüsse von k. Nach Satz 7.2 gibt es also Homomorphismen $\phi\colon K \to \bar{L}$ und $\psi\colon L \to \bar{K}$ mit $\phi|_k = \psi|_k = \mathrm{Id}_k$. Sind $\alpha_1, \ldots, \alpha_r \in K$ die verschiedenen Nullstellen von f, dann ist nach Lemma 7.4 jedes $\phi(\alpha_i)$ eine Nullstelle von f in $\bar{L}$ und daher ein Element aus L. Da $K = k(\alpha_1, \ldots, \alpha_r)$ ist, ist daher $\mathrm{Bild}(\phi) \subseteq L$ und analog $\mathrm{Bild}(\psi) \subseteq K$. Wie im Beweis von Korollar 7.6 folgt jetzt: ϕ, ψ sind Isomorphismen. Folglich ist die Anzahl der Nullstellen mit Vielfachheit d gleich in beiden Körpern.

Nun sei f irreduzibel, und $\alpha, \beta \in K$ zwei Nullstellen von f. Nach Lemma 7.3 gibt es einen Homomorphismus $\phi\colon k(\alpha) \to k(\beta)$ mit $\phi|_k = \mathrm{Id}_k$ und $\phi(\alpha) = \beta$. Satz 7.2: es gibt $\Phi\colon K \to \bar{K}$ mit $\Phi|_{k(\alpha)} = \phi$. Wie oben folgt dann $\Phi(K) = K$. Wegen $\Phi(\alpha) = \beta$ haben beide Nullstellen die gleiche Vielfachheit. ∎

Beispiel $\mathbb{Q}(i)$ ist ein Zerfällungskörper von $f = X^4 + X^2 = X^2(X^2 + 1)$. Die Nullstelle 0 hat Vielfachheit 2; die Nullstellen $\pm i$ haben jeweils Vielfachheit 1.

Wichtiges Beispiel (Vgl. Begriff „(in)separabel“.) Sei p eine Primzahl und $k = \mathbb{F}_p(t)$, der Quotientenkörper des faktoriellen Rings $R = \mathbb{F}_p[t]$. Sei $f \in k[X]$ das Polynom $f = X^p - t$. Nach Eisenstein ist f irreduzibel in $R[X]$, da $t \in R$ irreduzibel ist. Nach dem Gauß-Kriterium ist also f irreduzibel in $k[X]$.

Sei K ein Zerfällungskörper von f über k. Sei $\alpha \in K$ eine Nullstelle von f, also $\alpha^p = t$. Wegen $\binom{p}{r} \equiv 0 \pmod{p}$ für alle $1 \leq r \leq p-1$ gilt $(X - \alpha)^p = X^p - \alpha^p = X^p - t = f$. Also ist

$$f(X) = (X - \alpha)^p$$

die Primfaktorzerlegung von f in $K[X]$: es ist eine Nullstelle nur, und diese hat Vielfachheit p.

Hilfslemma Seien $f, g\colon K \to L$ zwei Körperhomomorphismen. Angenommen es ist $K = k(S)$, und ferner $f|_k = g|_k$, $f|_S = g|_S$. Dann $f = g$.

Beweis. Sei $M = \{x \in K \mid f(x) = g(x)\}$. Dann $k \cup S \subseteq M$. Außerdem ist $0, 1 \in M$ (wegen $k \subseteq M$); und M ist abgeschlossen bzgl. Multiplikation, Addition, Subtraktion und Division. Also ist M ein Körper. Wegen $k \cup S \subseteq M \subseteq K = k(S)$ folgt dann $M = K$, d.h. $f = g$. ∎

Beispiel Wieviele Homomorphismen $\phi\colon \mathbb{Q}(i) \to \mathbb{C}$ gibt es? Wir wissen $\phi|_{\mathbb{Q}} = \mathrm{Id}$; und dass $\phi(i) = \pm i$. Es gibt also höchstens zwei solche Homomorphismen. Können wir beide Werte von $\phi(i)$ realisieren? Ja, mit $\phi_+(\alpha) = \alpha$ für alle $\alpha \in \mathbb{Q}(i)$ – diese Abbildung ϕ_+ hiert heißt die *Inklusion* von $\mathbb{Q}(i)$ in $\mathbb{C}$. Eine zweite Abbildung ist $\phi_-(\alpha) = \bar{\alpha}$ (komplexe Konjugation).

Beispiel Wie viele Homomorphismen $f\colon \mathbb{Q}(\sqrt{5}) \to \mathbb{C}$ gibt es? Wir wissen $\phi|_{\mathbb{Q}} = \mathrm{Id}$; und dass $\phi(\sqrt{5}) = \pm\sqrt{5}$. Es gibt also höchstens zwei solche Homomorphismen. Können wir beide Werte von $\phi(\sqrt{5})$ realisieren? Ja, wegen Lemma 7.3. Die beiden Abbildungen sind $\phi(a+b\sqrt{5}) = a+b\sqrt{5}$ und $\phi(a+b\sqrt{5}) = a-b\sqrt{5}$.

7.3 Normale Erweiterungen

Bezeichnung Sei K/k eine KE. Man schreibt $\mathrm{Aut}(K/k)$ für die Automorphismengruppe

$$\mathrm{Aut}(K/k) := \{\phi\colon K \to K \mid \phi \text{ Automorphismus}, \phi|_k = \mathrm{Id}\}\,.$$

Beispiel Zur Erinnerung: Ein Automorphismus von K ist ein Isomorphismus von K nach sich selbst. Es ist $\mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \{\mathrm{Id}, \tau\}$, wobei τ die komplexe Konjugation ist.

Lemma 7.8 *Sei L/k eine algebraische KE, und sei K ein algebraischer Abschluss von k mit $L \subseteq K$. Dann sind folgende drei Aussagen äquivalent:*

a) Jedes irreduzible Polynom $f \in k[X]$, das eine Nullstelle in L hat, zerfällt in $L[X]$ als ein Produkt von linearen Faktoren.

b) L ist der Zerfällungskörper einer Menge *F von Polynomen aus $k[X]$. Das heißt, jedes $f \in F \subseteq k[X]$ zerfällt in $L[X]$ als ein Produkt von linearen Faktoren; und dies gilt in keinem echten Zwischenkörper $k \subseteq M \subsetneq L$.*

c) Es ist $\phi(L) = L$ für jedes $\phi \in \mathrm{Aut}(K/k)$.

Beachten Sie: K kommt nur in c) vor.

Beweis. a) $\Rightarrow$ b): Sei $F = \{m_\alpha \mid \alpha \in L\} \subseteq k[X]$. Einerseits ist jedes $\alpha \in L$ Nullstelle eines dieses Polynoms, also liegt L im Zerfällungskörper; andererseits hat jedes dieser irreduziblen Polynome eine Nullstelle in L und zerfällt daher in $L[X]$ als Produkt von linearen Faktoren.

b) $\Rightarrow$ c): Es ist $L = k(S)$ für $S = \{\alpha \in K \mid \exists f \in F\ f(\alpha) = 0\}$. Sei $\phi \in \mathrm{Aut}(K/k)$, und seien $\alpha \in S$, $f \in F$ mit $f(\alpha) = 0$. Nach Lemma 7.4 ist auch $\phi(\alpha)$ eine Nullstelle von f, daher $\phi(S) \subseteq S$ und daher $\phi(L) \subseteq L$. Nach Lemma 7.5 folgt $\phi(L) = L$.

c) $\Rightarrow$ a): Sei $f \in k[X]$ ein irreduzibles Polynom mit einer Nullstelle $\alpha \in L$. Sei $\beta \in K$ eine weitere Nullstelle von f. Zu zeigen ist: $\beta \in L$. Nach Lemma 7.3 gibt es einen Homomorphismus $\phi\colon k(\alpha) \to K$ mit $\phi|_k = \mathrm{Id}$ und $\phi(\alpha) = \beta$. Nach Satz 7.2 hat ϕ eine Fortsetzung $\Phi\colon K \to K$. Nach Lemma 7.5 ist $\Phi \in \mathrm{Aut}(K/k)$. Nach Voraussetzung ist also $\Phi(L) = L$, daher $\beta \in L$. ∎

Definition Eine algebraische Erweiterung, die die äquivalente Bedingungen von Lemma 7.8 erfüllt, heißt *normal*.

Beispiel Die Erweiterungen $\mathbb{C}/\mathbb{R}$ und $\mathbb{Q}(i)/\mathbb{Q}$ sind normal, da Zerfällungskörper von X^2+1. Die Erweiterung $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ ist nicht normal, denn mit $\sqrt[4]{2}$ ist eine Nullstelle des irreduziblen Polynoms $X^4 - 2$ vorhanden, aber die Primfaktorzerlegung in $\mathbb{Q}(\sqrt[4]{2})[X]$ ist $X^4 - 2 = (X - \sqrt[4]{2})(X + \sqrt[4]{2})(X^2 + \sqrt{2})$. Die Erweiterung $\mathbb{A}/\mathbb{Q}$ ist eine unendliche normale Erweiterung.

Bemerkung Ist $F = \{f_1, \ldots, f_n\}$ endlich, so ist der Zerfällungskörper von F der Zerfällungskörper des Polynoms $f = \prod_{r=1}^{n} f_r$. Ist L/k endlich, so sei $\alpha_1, \ldots, \alpha_n$ eine k-Basis von L, und sei $f_r \in k[X]$ das Minimalpolynom von α_r. Dann ist L enthalten im Zerfällungskörper von F. Daher kann man in Lemma 7.8 die Bedingung b) durch „L/k ist Zerfällungskörper eines Polynoms $f \in k[X]$“ ersetzen, falls L/k endlich ist.

Beispiel 7.9 Sei $p_1, p_2, p_3, \ldots$ irgendeine Aufzählung der Primzahlen. Sei L der Zerfällungskörper $\mathbb{Q} \subseteq L \subseteq \mathbb{C}$ der Menge $F = \{X^2 - p_i \mid i \geq 1\} \subseteq \mathbb{Q}[X]\}$. Dann ist $L \subseteq \mathbb{R}$ eine normale Erweiterung von $\mathbb{Q}$. Wir zeigen, dass $L/\mathbb{Q}$ eine unendliche Erweiterung ist, indem wir zeigen:

$$[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) : \mathbb{Q}] = 2^n\,. \tag{7.10}$$

Induktion über n. Induktionsannahme: $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) : \mathbb{Q}] = 2^n$; und sind $p, q_1, \ldots, q_m$ für $m \geq 0$ paarweise verschiedene Primzahlen $\notin \{p_1, \ldots, p_n\}$, dann liegt $\sqrt{p/(q_1 \cdots q_m)} \notin \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$.

Induktionsanfang $n = 0$: $\sqrt{p/(q_1 \cdots q_m)} \notin \mathbb{Q}$, da $q_1 \cdots q_m X^2 - p$ irreduzibel nach Eisenstein und Gauß.

Induktionsschritt: Wegen $\sqrt{p_{n+1}} \notin M := \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$ ist

$$[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n+1}}) : \mathbb{Q}] = [M(\sqrt{p_{n+1}}) : M][M : \mathbb{Q}] = 2^{n+1}\,.$$

Ist $\sqrt{p/(q_1 \cdots q_m)} \in M(\sqrt{p_{n+1}})$, dann $\sqrt{p/(q_1 \cdots q_m)} = a + b\sqrt{p_{n+1}}$, mit $a, b \in M$. Also $p/(q_1 \cdots q_m) = a^2 + p_{n+1}b^2 + 2ab\sqrt{p_{n+1}}$. Wegen $\sqrt{p_{n+1}} \notin M$ ist dann $2ab = 0$. Nach der Induktionsannahme sind $p/(q_1 \cdots q_m) = a^2$ und $p/(q_1 \cdots q_m) = p_{n+1}b^2$ unlösbar für $a, b \in M$. Fertig.

7.4 Die Anzahl der Morphismen

Lemma 7.11 *Sei L/k eine endliche Erweiterung, sei K algebraisch abgeschlossen, und sei $\phi\colon k \to K$ ein Homomorphismus. Dann*

$$|\{\Phi\colon L \to K \mid \Phi|_k = \phi\}| \leq [L:k]\,.$$

Zusatz: Gilt Gleichheit für L/k, dann auch für M/k und L/M für jeden Zwischenkörper $k \subseteq M \subseteq L$.

Beweis. Induktion über $[L:k]$. Klar für $[L:k] = 1$. Sei also $\alpha \in L \setminus k$. Sei $M = k(\alpha)$. Sei $f = \phi(m_\alpha) \in K[X]$. Nach der Beweismethode von Lemma 7.4 ist $\psi(\alpha)$ eine Nullstelle von f, für jede Fortsetzung $\psi\colon M \to K$ von ϕ. Nach Lemma 7.3 gibt es ein solches ψ für jede Nullstelle β von f. Die Anzahl der Nullstellen – mit Vielfachheit – ist $\operatorname{grad}(f) = [M:k]$. Somit gibt es höchtens $[M:k]$ Fortsetzungen ψ. Nach der Induktionsannahme hat jedes ψ höchstens $[L:M]$ Fortsetzungen Φ.

Zusatz: Es gibt höchstens $[M:k]$ Fortsetzungen $\psi\colon M \to K$ von ϕ, und höchstens $[L:M]$ Fortsetzungen Φ von jedem ψ. ∎

Überlegung Sei L/k eine endliche Erweiterung, und K ein algebraischer Abschluss von k mit $L \subseteq K$. Nach dem obigen Lemma ist also

$$|\mathrm{Aut}(L/k)| \leq |\{\phi\colon L \to K \mid \phi|_k = \mathrm{Id}\}| \leq [L:k]\,. \tag{7.12}$$

Nach Satz 7.2 lässt sich jeder Homomorphismus $\phi\colon L \to K$ mit $\phi|_k = \mathrm{Id}$ sich zu einem $\Phi \in \mathrm{Aut}(K/k)$ fortsetzen. Also gilt Gleichheit bei der ersten Ungleichung genau dann, wenn L/k normal ist.

Definition Eine endliche Körpererweiterung L/k heißt *Galois*, falls

$$|\mathrm{Aut}(L/k)| = [L:k]$$

gilt. Bei einer Galoiserweiterung heißt $\mathrm{Gal}(L/k) := \mathrm{Aut}(L/k)$ die *Galoisgruppe* der Erweiterung.

Bemerkung Nach der obigen Überlegung ist jede Galoiserweiterung normal.

Lemma 7.13 *Sei L/k eine endliche Erweiterung und $f \in k[X]$ ein Polynom mit $L = k(T)$ für T die Nullstellenmenge $T = \{\alpha \in L \mid f(\alpha) = 0\}$ von f in L. Dann: Jedes $\phi \in \mathrm{Aut}(L/k)$ permutiert T; und die Abbildung $\mathrm{Aut}(L/k) \to S(T)$, $\phi \mapsto \phi|_T$ ist ein injektiver Gruppenhomomorphismus.*

Also um $\mathrm{Aut}(L/k)$ zu bestimmen, muss man nur ermitteln, welche Permutationen durch Automorphismen induziert werden.

Beweis. Lemma 7.4: ϕ permutiert die Nullstellen. Wegen $L = k(T)$ bestimmt die Permutation den Automorphismus (Hilfslemma nach Korollar 7.7). ∎

Gleich wollen wir ein paar Beispiele behandeln. Das nächste Lemma wird sich dabei als hilfreich erweisen.

Lemma 7.14 *Sei L der Zerfällungskörper des irreduziblen Polynoms $f \in k[X]$. Seien $\alpha, \beta \in L$ zwei Nullstellen von f. Dann gibt es ein $\phi \in \mathrm{Aut}(L/k)$ mit $\phi(\alpha) = \beta$.*

Beweis. Sei K ein algebraischer Abschluss von k mit $L \subseteq K$. Nach Lemma 7.3 gibt es $\psi\colon k(\alpha) \to k(\beta)$ mit $\psi|_k = \mathrm{Id}$ und $\psi(\alpha) = \beta$. Nach Satz 7.2 gibt es also $\Phi\colon K \to K$ mit $\Phi|_{k(\alpha)} = \psi$. Nach Lemma 7.5 ist $\Phi \in \mathrm{Aut}(K/k)$. Da L/k normal ist, ist $\Phi(L) = L$. Fertig mit $\phi = \Phi|_L$. ∎

Beispiele a) $\mathrm{Aut}(\mathbb{C}/\mathbb{R})$ enthält Id und die komplexe Konjugation. Wegen $[\mathbb{C} : \mathbb{R}] = 2$ kann es nach Gleichung (7.12) keine weiteren Automorphismen geben, und die Erweiterung ist Galois. Nach dem gleichen Argument ist auch $\mathbb{Q}(i)/\mathbb{Q}$ Galois.

b) Der Zerfällungskörper von $X^2 - 5 \in \mathbb{Q}[X]$ ist $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$. Nach Lemma 7.14 gibt es $\phi \in \mathrm{Aut}(\mathbb{Q}(\sqrt{5})/\mathbb{Q})$ mit $\phi(\sqrt{5}) = -\sqrt{5}$, daher $\phi \neq \mathrm{Id}$. Also ist $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ Galois, da der Erweiterungsgrad zwei beträgt.

c) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ ist nicht Galois, da nicht normal.

d) $X^3 - 2 \in \mathbb{Q}[X]$ ist irreduzibel. Der Zerfällungskörper $L = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ hat Erweiterungsgrad 6 und enthält drei Nullstellen. Wegen $3! = 6$ ist die Erweiterung also genau dann Galois, wenn jede Permutation der drei Nullstellen durch einen Automorphismus induziert wird. Komplexe Konjugation ist ein Automorphismus; diese vertauscht die beiden nichtreellen Nullstellen. Nach dem Satz von Lagrange gilt daher: entweder kommen alle Permutationen vor, oder die komplexe Konjugation erzeugt die Automorphismengruppe $\mathrm{Aut}(L/\mathbb{Q})$. Nach Lemma 7.14 gibt es einen Automorphismus, der die reelle Nullstelle $\sqrt[3]{2}$ auf eins der nichtreellen abbildet. Also kommen alle Permutationen vor, und die Erweiterung ist Galois. Die Galoisgruppe ist isomorph zu S_3.

e) *(Vgl. Wichtiges Beispiel nach Korollar 7.7)*
Sei p eine Primzahl. Sei $k = \mathbb{F}_p(t)$, und sei L der Zerfällungskörper des irreduziblen Polynoms $f = X^p - t \in k[X]$. Dann ist $L = k(\alpha)$ für α eine Nullstelle von f, und $f = (X - \alpha)^p$, d.h. α ist die einzige Nullstelle. Die einzige Permutation der Menge $\{\alpha\}$ ist die Identität, daher ist $\mathrm{Aut}(L/k) = \{\mathrm{Id}\}$, obwohl $[L : k] = p$ ist. Die Erweiterung ist also normal aber nicht Galois.

f) Sei L der Zerfällungskörper von $X^4 - 2 \in \mathbb{Q}[X]$. Es ist $L = \mathbb{Q}(\sqrt[4]{[2]}, i)$, denn die Nullstellen sind $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$. Es ist $[L : \mathbb{Q}] = 8$, denn $i \notin \mathbb{Q}(\sqrt[4]{2})$ und $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$. Mit $M = \mathbb{Q}(i)$ bedeutet dies, dass $[M(\sqrt[4]{2}) : M] = [L : M] = [L : \mathbb{Q}]/[M : \mathbb{Q}] = 4$, daher ist auch $X^2 - 4$ das Minimalpolynom von $\sqrt[4]{2}$ über M. Es ist $|\mathrm{Aut}(M/qq)| = 2$ (komplexe Konjugation). Sei $\phi \in \mathrm{Aut}(M/k)$. Sei α eine Nullstelle von $X^4 - 2$. Nach Lemma 7.3 gibt es genau ein $\Phi\colon L \to \mathbb{A}$ mit $\Phi(\sqrt[4]{2}) = \alpha$ und $\Phi|_M = \phi$. Da $L/\mathbb{Q}$ normal ist, ist $\mathrm{Bild}(\Phi) = L$, d.h. $\Phi \in \mathrm{Aut}(L/\mathbb{Q})$. Mit zwei Möglichkeiten für ϕ und vier für α erhalten wir somit acht verschiedene Automorphismen. Also ist $K/\mathbb{Q}$ Galois.

Sei $\rho \in \mathrm{Gal}(L/\mathbb{Q})$ der Automorphismus mit $\rho(i) = i$ und $\rho(\sqrt[4]{2}) = i\sqrt[4]{2}$. Sei $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ die komplexe Konjugation. Seien $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ die Nullstellen $\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}$. Dann operiert ρ als der 4-Zykel $(\alpha_1\ \alpha_2\ \alpha_3\ \alpha_4)$, und σ operiert als die Transposition $(\alpha_2\ \alpha_4)$. Diese beide Permutationen erzeugen die Diedergruppe D_4, die Isometriegruppe des Quadrats. Diese Gruppe hat acht Elemente. Also ist $\mathrm{Gal}(L/k)$ diese Diedergruppe.

Bemerkung Die sogenannte *absolute* Galoisgruppe $\mathrm{Aut}(\mathbb{A}/\mathbb{Q})$ besitzt eine faszinierende Komplexität und ist ein aktueller Forschungsgegenstand in der Zahlentheorie.

7.5 Separable Erweiterungen

Wir erinnern uns an Gleichung (7.12):

$$|\mathrm{Aut}(L/k)| \leq |\{\phi\colon L \to K \mid \phi|_k = \mathrm{Id}\}| \leq [L : k]\,.$$

Die endliche Erweieterung L/k ist genau dann normal bzw. Galois, wenn Gleichheit gilt in der ersten Ungleichung bzw. in beiden Ungleichungen.

Definition Sei L/k eine endliche Körpererweiterung, und K ein algebraischer Abschluss von k mit $L \subseteq K$. Die Erweiterung L/k heißt *separabel*, wenn $|\{\phi\colon L \to K \mid \phi|_k = \mathrm{Id}\}| = [L : k]$ gilt.

Bemerkung Eine Erweiterung ist also genau dann Galois, wenn sie normal und separabel ist.

Beispiele Die Erweiterungen $\mathbb{C}/\mathbb{R}$, $\mathbb{Q}(i)/\mathbb{Q}$, $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$, $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})/\mathbb{Q}$ und $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ sind separabel, da Galois. Der Zerfällungskörper von $X^p - t$ über $\mathbb{F}_p(t)$ ist normal aber nicht Galois, also nicht separabel.

Die Erweiterungen $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ und $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ sind nicht normal, aber doch separabel: denn das irreduzible Polynom $X^3 - 2 \in \mathbb{Q}[X]$ bzw. $X^4 - 2 \in \mathbb{Q}[X]$ hat drei bzw. vier verschiedene Nullstellen, was nach Lemma 7.3 zu drei bzw. vier verschiedene Morphismen nach $\mathbb{A}$ führt.

Es gibt aber einen anderen Weg, Separabilität festzustellen.

Lemma 7.15 *Sei L/k eine endliche KE, und $k \subseteq M \subseteq L$ ein Zwischenkörper. Genau dann ist L/k separabel, wenn L/M und M/k separabel sind.*

Beweis. Sei $K \supseteq L$ ein algebraischer Abschluss von k. Jedes $\psi\colon M \to K$ mit $\psi|_k = \mathrm{Id}$ lässt sich nach Satz 7.2 und Lemma 7.5 zu einem Automorphismus $\Phi = \Phi_\psi \in \mathrm{Aut}(K/k)$ mit $\Phi|_M = \psi$ fortsetzen. Daher gibt es eine Bijektion

$$\begin{aligned}\{\phi\colon L \to K \mid \phi|_M = \psi\} &\leftrightarrow \{\chi\colon L \to K \mid \chi|_M = \mathrm{Id}\}\\ \phi &\mapsto \Phi_\psi^{-1} \circ \phi\end{aligned}$$

Somit hat jedes $\psi\colon M \to K$ die gleiche Anzahl A_0 an Fortsetzungen $\phi\colon L \to K$; und daher

$$\begin{aligned}\left|\{L \xrightarrow{\phi} K \mid \phi|_k = \mathrm{Id}\}\right| &= \left|\{M \xrightarrow{\psi} K \mid \psi|_k = \mathrm{Id}\}\right| \cdot A_0\\ &= \left|\{M \xrightarrow{\psi} K \mid \psi|_k = \mathrm{Id}\}\right| \cdot \left|\{L \xrightarrow{\phi} K \mid \phi|_M = \mathrm{Id}\}\right| .\end{aligned}$$

Das Ergebnis folgt dann aus der Ungleichung

$$\left|\{L \xrightarrow{\phi} K \mid \phi|_k = \mathrm{Id}\}\right| \leq [L : k]$$

und den entsprechenden Ungleichungen für L/M, M/k. ∎

Bezeichnung Eine KE K/k heißt *einfach*, wenn es ein $\alpha \in K$ gibt derart, dass $K = k(\alpha)$ ist. Ein solches α heißt ein *primitives* Element.

Beispiel Die Erweiterung $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ ist einfach, denn $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Daher ist $\sqrt{2} + \sqrt{3}$ ein primitives Element.

Bemerkung Der Satz vom primitiven Element besagt, dass jede endliche Erweiterung von $\mathbb{Q}$ einfach ist, und sogar jede separable endliche Erweiterung. Der Beweis benutzt den Hauptsatz der Galoistheorie.

7.6 Separable Polynome

Definition Ein irreduzibles Polynom $f \in k[X]$ heißt *separabel*, falls es im Zerfällungskörper keine wiederholten Nullstellen hat.

Wir werden ein beliebiges Polynom $f \in k[X]$ separabel nennen, falls jedes irreduzible Faktor separabel ist[5].

Beispiel $X^p - t \in \mathbb{F}_p(t)[X]$ ist das einzige inseparable Polynom, das wir bisher gesehen haben. Vorsicht: separabel in $L[X]$, falls L der Zerfällungskörper ist.

[5]Für uns ist also X^2 separabel; für manche Autoren dagegen nicht.

Lemma 7.16 *Sei L/k eine KE und $\alpha \in L$ algebraisch über k. Dann sind folgende beiden Aussagen äquivalent:*

a) Die KE $k(\alpha)/k$ ist separabel.

b) Das Minimalpolynom $m_\alpha \in k[X]$ von α ist separabel.

Beweis. Sei $K \supseteq k(\alpha)$ ein algebraischer Abschluss von k. Nach Lemma 7.3 stimmt $\left|\{k(\alpha) \xrightarrow{\phi} K \mid \phi|_k = \mathrm{Id}\}\right|$ mit der Anzahl der Nullstellen von m_α überein. Der Grad von m_α ist $[k(\alpha) : k]$, d.h. mit Vielfachheiten gezählt gibt es genau $[k(\alpha) : k]$ Nullstellen. Es sind also genau dann $[k(\alpha) : k]$ Morphismen ϕ, wenn es keine wiederholten Nullstellen gibt. ∎

Korollar 7.17 *Sei L/k eine endliche Erweiterung.*

a) L/k separabel $\Leftrightarrow$ jedes $\alpha \in L$ hat ein separables Minimalpolynom $m_\alpha \in k[X]$.

b) Ist $L = k(\alpha_1, \ldots, \alpha_n)$, dann: L/k separabel $\Leftrightarrow$ jedes α_i hat Genau dann ist L/k separabel, wenn jedes α_i ein separables Minimalpolynom über k hat.

Beweis. Ist L/k separabel, dann auch jedes $k(\alpha)/k$ für $\alpha \in L$ (Lemma 7.15). Also jedes m_α separabel (Lemma 7.16). Also gilt $\Rightarrow$ in a) und in b).

$\Leftarrow$ in b): Induktion über n, nichts zu tun für $n = 0$. Sei $M = k(\alpha_1, \ldots, \alpha_{n-1})$. Nach Induktionsannahme ist M/k separabel. Nach Lemma 7.15 müssen wir zeigen: L/M ist separabel. Es ist $L = M(\alpha)$ für $\alpha = \alpha_n$. Das Minimalpolynom $f \in M[X]$ von α über M teilt das Minimalpolynom $m_\alpha \in k[X]$. Da m_α keine wiederholten Nullstellen hat, hat auch f keine. Nach Lemma 7.16 ist also L/M separabel.

$\Leftarrow$ in a): folgt aus b), denn ist $\alpha_1, \ldots, \alpha_r$ eine k-Basis von L, dann $L = k(\alpha_1, \ldots, \alpha_r)$. ∎

7.7 Die formale Ableitung

Die Analysis hilft, mehrfache Nullstellen zu erkennen. Ist a eine mehrfache Nullstelle von $f \in \mathbb{R}[X]$, so ist $(X - a)^2 \mid f$, weshalb $(X - a) \mid f'$, daher ist $\mathrm{ggT}(f, f') \neq 1$, denn der ggT hat eine Nullstelle in a. Mit der formalen Ableitung können wir diesen Ansatz auch dort verwenden, wo die Analysis nicht anwendbar ist. Etwa für endliche Körper.

Definition Sei k ein beliebiger Körper. Die *formale Ableitung* $D\colon k[X] \to k[X]$ ist die k-lineare Abbildung gegeben durch $D(X^n) = nX^{n-1}$ für jedes $n \geq 0$.

Lemma 7.18 *Die formale Ableitung erfüllt die Leibniz-Regel $D(fg) = D(f) \cdot g + f \cdot D(g)$.*

Beweis. Wegen Linearität muss man nur den Fall $f = X^r$, $g = X^s$ behandeln. Dies ist leicht. ∎

Lemma 7.19 *Sei k ein Körper und $f \in k[X]$ ein Polynom. Genau dann hat f eine wiederholte Nullstelle, wenn* $\mathrm{ggT}(f, D(f)) \neq 1$ *gilt.*

Beweis. Sei L ein Zerfällungskörper von f. Sei $\alpha \in L$ eine Nullstelle von f. Ist α eine wiederholte Nullstelle, dann $f = (X-\alpha)^2 g$ und daher $D(f) = (X-\alpha)(2g + (X-\alpha)D(g))$, weshalb $X - \alpha$ den ggT teilt. Ist dagegen der ggT $\neq 1$, so hat er eine Nullstelle $\beta \neq 1$. Dann $f = (X-\beta)h$, daher $0 = D(f)(\beta) = h(\beta)$, also $(X-\beta) \mid h$ und daher $(X-\beta)^2 \mid f$. ∎

Korollar 7.20 *Ein irreduzibles Polynom $f \in k[X]$ ist genau dann separabel, wenn $D(f) \neq 0$ ist. Ist k ein Teilkörper von $\mathbb{C}$, so ist jedes Polynom $f \in k[X]$ separabel.*

Beweis. Jedes lineare Polynom ist irreduzibel und separabel. Ist $\mathrm{grad}(f) \geq 2$ und $\mathrm{ggT}(f, D(f)) \neq 1$, dann ist f selbst der ggT. Dies kann aus Gradgründen nur dann der Fall sein, wenn $D(f) = 0$ ist. Ist $k \subseteq \mathbb{C}$, dann $D(f) = f'$, also $D(f) \neq 0$ falls $\mathrm{grad}(f) \geq 1$. ∎

Beispiel $f = X^p - t \in \mathbb{F}_p(t)[X]$ ist bekanntlich irreduzibel und inseparabel. Es ist tatsächlich $D(f) = pX^{p-1} = 0$.

Definition Die *Charakteristik* $\mathrm{char}(k)$ eines Körpers k ist die kleinste Zahl $n \geq 1$ derart, dass die n-fache Summe $1 + 1 + \cdots + 1$ den Wert 0 hat; bzw. $\mathrm{char}(n) = 0$, falls es kein solches n gibt.

Lemma 7.21 *Sei k ein Körper.*

a) *Die Charakteristik ist entweder Null oder eine Primzahl. Ist L/k eine KE, so ist* $\mathrm{char}(L) = \mathrm{char}(k)$. *Allgemeiner gilt: ist $\phi\colon k \to K$ ein Homomorphismus zwischen Körpern, so ist* $\mathrm{char}(K) = \mathrm{char}(k)$.

b) *Ist* $\mathrm{char}(k) = 0$, *so ist jedes Polynom $f \in k[X]$ separabel.*

c) *Ist* $\mathrm{char}(k) = p > 0$, *so ist ein irreduzibles Polynom $f \in k[X]$ genau dann inseparabel, wenn es ein $g \in k[X]$ gibt mit $f(X) = g(X^p)$.*

Beweis. a) ist relativ klar. Zu b): Ist $\mathrm{char}(k) = 0$ und f irreduzibel, dann $\mathrm{grad}(D(f)) = \mathrm{grad}(f) - 1$, also $D(f) \neq 0$. Zu c): Ist $\mathrm{char}(k) = p$, dann $D(X^n) = 0$ genau dann, wenn $p \mid n$. ∎

Beispiel Jeder Teilkörper des $\mathbb{C}$ hat Charakteristik 0, das gleiche gilt für $\mathbb{C}(t)$. Es ist $\mathrm{char}\,\mathbb{F}_p = \mathrm{char}\,\mathbb{F}_p(t) = p$.

Beispiel Das Polynom $f = X^9 + t^2X^6 + tX^3 - t \in \mathbb{F}_3(t)[X]$ ist irreduzibel (Eisenstein, Gauß) und daher inseparabel ($g = X^3 + t^2X^2 + tX - t$).

Lemma 7.22 *Sei k ein endlicher Körper. Dann ist jedes Polynom $f \in k[X]$ und jede endliche Erweiterung L/k separabel.*

Beweis. Fall $k = \mathbb{F}_p$: Für jedes $a \in k$ ist $a^p = a$, also ist $g(X^p) = (g(X))^p$ für jedes $f \in \mathbb{F}_p[X]$, daher reduzibel. Nach Korollar 7.17 ist auch L/k separabel.

Allgemeiner Fall: sei $p = \mathrm{char}(k) > 0$. Dann ist $\mathbb{F}_p$ ein Teilkörper von k, und $k/\mathbb{F}_p$ ist endlich. Ist L/k endlich, dann auch $L/\mathbb{F}_p$. Gerade gezeigt: $L/\mathbb{F}_p$ separabel. Daher auch L/k separabel (Lemma 7.15). Daher jedes Polynom separabel (Lemma 7.16). ∎

8 Galoiserweiterungen

Ziele: die vier Charakterisierungen einer Galoiserweiterung; der Hauptsatz der Galoistheorie.

8.1 Lineare Unabhängigkeit von Automorphismen

Lemma 8.1 *Seien k, K zwei Körper, und $\phi_1, \ldots, \phi_n \colon k \to K$ paarweis verschiedene Homomorphismen. Dann: als Abbildungen von k nach K sind $\phi_1, \ldots, \phi_n$ linear unabhängig (über K).*

Beweis. Wenn nicht, dann sei

$$\forall x \in k \ \sum_{i=1}^{n} \lambda_i \phi_i(x) = 0$$

ein Gegenbeispiel mit n so klein wie möglich, und oBdA $\lambda_1 \neq 0$. Offensichtlich muss $n \geq 2$ sein. Nach Annahme gibt es $x_0 \in k$ mit $\phi_n(x_0) \neq \phi_1(x_0)$. Also

$$\forall x \in k \ \sum_{i=1}^{n} \lambda_i \phi_n(x_0) \phi_i(x) = 0 \,.$$

Wegen $\phi_i(x_0 x) = \phi_n(x_0)\phi_n(x)$ gilt außerdem

$$\forall x \in k \ \sum_{i=1}^{n} \lambda_i \phi_i(x_0) \phi_i(x) = 0 \,.$$

Zieht man die erste von der zweiten Gleichung ab, so erhält man

$$\sum_{i=1}^{n-1} \lambda_i (\phi_i(x_0) - \phi_n(x_0)) \phi_i(x) = 0 \,.$$

Wegen $\lambda_1(\phi_1(x_0) - \phi_n(x_n)) \neq 0$ ist dies ein Widerspruch zur Minimalität von n. ∎

Bezeichnung Sei K ein Körper und $G \leq \mathrm{Aut}(K)$ eine Gruppe von Automorphismen. Mit $\mathrm{Fix}(G)$ bezeichnet man die Teilmenge

$$\mathrm{Fix}(G) = \{a \in K \mid \sigma(a) = a \forall \sigma \in G\} \,.$$

Diese Teilmenge ist offensichtlich ein Teilkörper von K, der *Fixkörper* von G.

Lemma 8.2 *Sei K ein Körper und $G \leq \mathrm{Aut}(K)$ eine endliche Gruppe von Automorphismen. Dann $[K : \mathrm{Fix}(G)] = |G|$.*

Beweis. Sei $k = \mathrm{Fix}(G)$, und sei $\omega_1, \ldots, \omega_r$ eine k-Basis von K, und sei $G = \{\sigma_1, \ldots, \sigma_n\}$, mit $\sigma_1 = \mathrm{Id}$. Zu zeigen ist: $r = n$.

Fall $r < n$: Das Gleichungssystem $\sum_{i=1}^{n} \lambda_i \sigma_i(\omega_j) = 0$ $(1 \leq j \leq r)$ ist lösbar, mit nicht alle $\lambda_i = 0$. Also $\sum_{i=1}^{n} \lambda_i \sigma_i(x) = 0$ für alle $x \in K$. Widerspruch zu Lemma 8.1.

Fall $r > n$: Hier benutzen wir nur die k-lineare Unabhängigkeit der ω_j, d.h. auch der Fall $[K : k] = \infty$ wird miterfasst. Es gibt $\mu_1, \ldots, \mu_r \in K$ mit

$$\sum_{j=1}^{r} \mu_j \sigma_i(\omega_j) = 0 \quad \text{für alle } 1 \leq i \leq n. \tag{8.3}$$

OBdA sind $\mu_1, \ldots, \mu_s \neq 0$; $\mu_j = 0$ für $j > s$; und s ist so klein wie möglich. OBdA ist dann $\mu_s = 1$. Also

$$\sigma_i(\omega_s) + \sum_{j=1}^{s-1} \mu_j \sigma_i(\omega_j) = 0 \quad \text{für alle } 1 \leq i \leq n. \tag{8.4}$$

Für $i = 1$ ist $\sigma_1 = \mathrm{Id}$, also $\sum_{j=1}^{r} \mu_j \omega_j = 0$. Wegen der linearen Unabhängigkeit der ω_j ist mindestens eins der $\mu_j \notin k$, also oBdA $\mu_1 \notin k$. Es gibt also $\tau \in G$ mit $\tau(\mu_1) \neq \mu_1$. Wenden wir τ auf (8.4): da jedes $\tau\sigma_i$ ein $\sigma_{i'}$ ist, gilt

$$\sigma_i(\omega_s) + \sum_{j=1}^{s-1} \tau(\mu_j) \sigma_i(\omega_j) = 0 \quad \text{für alle } 1 \leq i \leq n. \tag{8.5}$$

Wir ziehen (8.4) von (8.5) ab. Da $\mu_s = \tau(\mu_s) = 1$ ist, ist

$$\sum_{j=1}^{s-1} (\tau(\mu_j) - \mu_j) \sigma_i(\omega_j) = 0 \quad \text{für alle } 1 \leq i \leq n.$$

Wegen $\tau(\mu_1) - \mu_1 \neq 0$ widerspricht dies der Minimalität von s. ∎

8.2 Die vier Charakterisierungen einer Galoiserweiterung

Satz 8.6 *Für eine endliche Körpererweiterung L/k sind die folgenden vier Aussagen äquivalent:*

a) L/k *ist Galois, d.h.* $|\mathrm{Aut}(L/k)| = [L : k]$.

b) $\mathrm{Fix}(\mathrm{Aut}(L/k)) = k$.

c) L/k *ist normal und separabel.*

d) L *ist Zerfällungskörper eines separablen Polynoms* $f \in k[X]$.

Beweis. Die Äquivalenz von a) und c) hatten wir schon, direkt nach der Definition von „separable Erweiterung“; s. auch Ungleichung (7.12). Wegen dieser Ungleichung ist $|\mathrm{Aut}(L/k)| \leq [L : k]$; also sind a) und b) äquivalent, denn $k \subseteq \mathrm{Fix}(\mathrm{Aut}(L/k))$, und $[L : \mathrm{Fix}(\mathrm{Aut}(L/k))] = |Aut(L/k)|$ nach Lemma 8.2.

Als letztes behandeln wir die Äquivalenz von c) und d). Ist $L = k(\alpha_1, \ldots, \alpha_r)$ normal und separabel, so ist es der Zerfällungskörper des separablen Polynoms $f = \prod_{i=1}^{r} m_{\alpha_i}$. Ist L Zerfällungskörper des separablen Polynoms $f \in k[X]$, so ist L/k normal; und $L = k(\alpha_1, \ldots, \alpha_r)$ mit $f(\alpha_i) = 0$ für alle i, daher ist jedes m_{α_i} separabel, nach Korollar 7.17. ∎

Definition Sei $f \in k[X]$ ein separables Polynom. Sei L der Zerfällungskörper von f. Nach dem Satz ist L/k Galois. Die Galoisgruppe $\mathrm{Gal}(L/k)$ nennt man die Galoisgruppe des separablen Polynoms f.

Beispiel Das separable Polynom $X^4 - 2 \in \mathbb{Q}[X]$ hat Galoisgruppe D_4.

8.3 Die Galois-Korrepondenz: Der Hauptsatz der Galoistheorie

Hauptsatz *Die endliche Erweiterung K/k sei Galois. Dann gibt es eine bijektive Korrespondenz – die* Galois-Korrespondenz *– zwischen den Mengen*

$$\{\textit{Untergruppen } H \leq \mathrm{Gal}(K/k)\} \longleftrightarrow \{\textit{Zwischenkörper } k \subseteq L \subseteq K\}$$

gegeben durch die Bijektionen $H \mapsto \mathrm{Fix}(H)$ und $L \mapsto \mathrm{Aut}(K/L)$, die invers zueinander sind. Weitere Eigenschaften dieser Korrespondenz:

a) Für $H \leftrightarrow L$ ist $[K : L] = |H|$ und $[L : k] = |G : H|$.

b) Die Korrespondenz kehrt Inklusionen um: ist $H_1 \leftrightarrow L_1$ und $H_2 \leftrightarrow L_2$, dann

$$H_1 \leq H_2 \iff L_2 \subseteq L_1 .$$

c) Für $H \leftrightarrow L$ gilt: K/L ist immer Galois, und L/k ist immer separabel. Genau dann ist L/k normal (und daher Galois), wenn $H \lhd \mathrm{Gal}(K/k)$ ist. In diesem Fall ist $\mathrm{Gal}(L/k) \cong \mathrm{Gal}(K/k)/\mathrm{Gal}(K/L)$.

Beweis. Lemma 7.15: K/L und L/k separabel für jeden Zwischenkörper L. Da K/k normal ist, ist K Zerfällungskörper von einem $f \in k[X]$, daher K Zerfällungskörper von $f \in L[X]$, daher K/L normal. Also K/L Galois und L/k separabel.

Für jedes L ist $L = \mathrm{Fix}\,\mathrm{Aut}(K/L)$ wegen K/L Galois (vierfache Charakterisierung). Für $H \leq \mathrm{Gal}(K/k)$ ist $[K : \mathrm{Fix}(H)] = |H|$ nach Lemma 8.2. Wie gerade überlegt ist $K/\mathrm{Fix}(H)$ Galois, also $|\mathrm{Aut}(K/\mathrm{Fix}\,H)| = [K : \mathrm{Fix}\,H] = |H|$. Wegen

$H \leq \mathrm{Aut}(K/\operatorname{Fix} H)$ gilt dann $H = \mathrm{Aut}(K(\operatorname{Fix} H)$. Dies weist die Korrespondenz nach. Für a) haben wir $[K : \operatorname{Fix} H] = |H|$ schon, die andere Gleichung folgt. Zu b): ist $H_1 \leq H_2$, dann $\operatorname{Fix} H_1 \supseteq \operatorname{Fix} H_2$; ist $L_2 \subseteq L_1$ und $\phi \in \mathrm{Aut}(K/L_1)$, dann $\phi \in \mathrm{Aut}(K/L_2)$.

Übrig bleibt c). Schon hatten wir K/L Galois, L/k separabel. Sei $\bar{K} \supseteq K$ ein algebraischer Abschluss von k. Satz 7.2 und Lemma 7.5: Jedes $\phi \in \mathrm{Aut}(K/k)$ setzt sich zu $\Phi \in \mathrm{Aut}(\bar{K}/k)$ fort. Ist daher $\phi(L) \neq L$, dann $\Phi(L) \neq L$ und daher L nicht normal. Umgekehrt ist $\Phi|_K \in \mathrm{Aut}(K/k)$ für jedes $\Phi \in \mathrm{Aut}(\bar{K}/k)$, da K/k normal. Also

$$L/k \text{ normal} \iff \phi(L) = L \text{ für jedes } \phi \in \mathrm{Aut}(K/k)\,.$$

Sei $H = \mathrm{Aut}(K/L)$. Ist $\alpha \in L$, $\phi(L) = L$ und $\psi \in H$, dann $\psi\phi(\alpha) = \psi(\alpha)$, also $\phi^{-1}\psi\phi(\alpha) = \alpha$, d.h. $\phi^{-1}\psi\phi \in H$. Ist also L/k normal, dann $H \lhd \mathrm{Gal}(K/L)$. Ist L/k nicht normal, dann gibt es $\phi \in \mathrm{Gal}(K/k)$ und $\alpha \in L$ mit $\phi(\alpha) \notin L$. Wegen $L = \operatorname{Fix} H$ gibt es dann $\psi \in H$ mit $\psi\phi(\alpha) \neq \phi(\alpha)$, also $\phi^{-1}\psi\phi(\alpha) \neq \alpha$, also $\phi^{-1}\psi\phi \notin \mathrm{Aut}(K/L) = H$, also $H \not\lhd \mathrm{Gal}(K/k)$.

Ist L/k normal, so ist (s. oben) $\Phi \mapsto \Phi|_L$ ein Gruppenhomomorphismus $\mathrm{Aut}(K/k) \to \mathrm{Aut}(L/k)$. Der Kern ist $\mathrm{Aut}(K/L)$. Der Homomorphismus ist surjektiv, da jedes $\phi \in \mathrm{Aut}(L/k)$ setzt sich zu $\Psi \in \mathrm{Aut}(\bar{K}/k)$ fort, und $\Psi(K) = K$ da K normal. Also Homomorphiesatz anwenden. ∎

Korollar 8.7 *Ist die endliche Erweiterung L/k separabel, so gibt es nur endlich viele Zwischenkörper.*

Beweis. Sei $L = k(\alpha_1, \ldots, \alpha_r)$. Da L/k separabel ist, ist auch jedes $m_{\alpha_i} \in k[X]$ separabel. Sei $K \supseteq L$ der Zerfällungskörper von $f \in k[X]$ gegeben durch $f = \prod_{i=1}^{r} m_{\alpha_i}$. Dann ist f separabel, daher K/k Galois. Nach dem Hauptsatz hat sogar K/k nur endlich viele Zwischenkörper, da $\mathrm{Aut}(K/k)$ endlich ist und daher nur endlich viele Untergruppen hat. ∎

8.4 Erste Beispiele

Beispiel Der Zerfällungskörper von $X^3 - 2 \in \mathbb{Q}[X]$.

Beispiel Der Zerfällungskörper von $X^4 - 2 \in \mathbb{Q}[X]$.

Es ist $K = \mathbb{Q}(\sqrt[4]{2}, i)$. Wir sahen schon: $K/\mathbb{Q}$ ist Galois, und $\mathrm{Gal}(K/\mathbb{Q}) \cong D_4$, erzeugt von ρ, σ mit $\rho^4 = \sigma^2 = \mathrm{Id}$, $\sigma\rho\sigma = \rho^{-1}$, und

$$\begin{aligned} \rho(\sqrt[4]{2}) &= i\sqrt[4]{2} & \qquad \sigma(\sqrt[4]{2}) &= \sqrt[4]{2} \\ \rho(i) &= i & \qquad \sigma(i) &= -i\,. \end{aligned}$$

Sei $\alpha = \frac{1+i}{\sqrt{2}} \in K$. Es ist $\alpha^2 = i$, $\sigma(\alpha) = -i\alpha$ und $\rho(\alpha) = -\alpha$. Beachten Sie, dass $\alpha\sqrt[4]{2}$ eine Nullstelle von $X^4 + 2$ ist. Die Untergruppen H von $\mathrm{Gal}(K/\mathbb{Q}) \cong D_4$ sind:

- $H = \{Id\}$, Ordnung 1. Normalteiler. $\operatorname{Fix} H = K$.
- $H = \langle \rho^2 \rangle$, Ordnung 2. Normalteiler. $\operatorname{Fix} H = \mathbb{Q}(\sqrt{2}, i)$.
- $H = \langle \sigma \rangle$, Ordnung 2. Kein Normalteiler. $\operatorname{Fix} H = \mathbb{Q}(\sqrt[4]{2})$.
- $H = \langle \sigma\rho \rangle$, Ordnung 2. Kein Normalteiler. $\operatorname{Fix} H = \mathbb{Q}(\alpha\sqrt[4]{2})$.
- $H = \langle \sigma\rho^2 \rangle$, Ordnung 2. Kein Normalteiler. $\operatorname{Fix} H = \mathbb{Q}(i\sqrt[4]{2})$.
- $H = \langle \sigma\rho^3 \rangle$, Ordnung 2. Kein Normalteiler. $\operatorname{Fix} H = \mathbb{Q}(i\alpha\sqrt[4]{2})$.
- $H = \langle \rho \rangle$, zyklisch, Ordnung 4. Normalteiler. $\operatorname{Fix} H = \mathbb{Q}(i)$.
- $H = \langle \rho^2, \sigma \rangle$, Ordnung 4, $C_2 \times C_2$. Normalteiler. $\operatorname{Fix} H = \mathbb{Q}(\sqrt{2})$.
- $H = \langle \rho^2, \sigma\rho \rangle$, Ordnung 4, $C_2 \times C_2$. Normalteiler. $\operatorname{Fix} H = \mathbb{Q}(i\sqrt{2})$.
- $H = \langle \rho, \sigma \rangle$, Ordnung 8, D_4. Normalteiler. $\operatorname{Fix} H = \mathbb{Q}$.

8.5 Endliche Körper

Satz 8.8 *Sei p eine Primzahl und $q = p^m$ eine p-Potenz. Dann:*

a) Der Zerfällungskörper $=: \mathbb{F}_q$ von $X^q - X \in \mathbb{F}_p[X]$ enthält genau q Elemente. Jedes dieser Elemente ist eine Nullstelle von $X^q - X$.

b) Umgekehrt gilt: jeder endlicher Körper ist ein $\mathbb{F}_q$.

c) Die Galoisgruppe $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ *ist zyklisch der Ordnung m. Sie wird erzeugt durch den* Frobenius-Automorphismus $F(a) := a^p$.

Beweis. Für $f = X^q - X$ ist $D(f) = -1$, daher $\mathrm{ggT}(f, D(f)) = 1$ und f hat keine wiederholte Nullstellen. Daher hat f genau q verschiedene Nullstellen. Sind a, b Nullstellen, so sind auch $a \pm b$, ab und a/b. Ferner ist 1 eine Nullstelle. Also bilden die Nullstellen einen Körper.

Ist dagegen k ein endlicher Körper, dann $\mathrm{char}(k) = p$ für ein p, also ist $\mathbb{F}_p$ ein Teilkörper von k. Also ist k ein $\mathbb{F}_p$-Vektorraum, daher $|k| = q = p^m$ für ein m. Nach Lagrange ist $a^{q-1} = 1$ für jedes $a \in k^*$. Also $a^q = a$ für jedes a. Somit besteht k aus lauter Nullstellen zu $X^q - X$, und mehr als q darf es nicht geben, also ist k der Zerfällungskörper.

Wegen $p \mid \binom{p}{r}$ für $1 \le r \le p-1$ ist F ein Automorphismus. Wegen $a^q = a$ ist $F^m = \mathrm{Id}$. Wäre $F^r = \mathrm{Id}$ für ein $r < m$, so hätte $X^{p^r} - X$ jedes Element von $\mathbb{F}_q$ als Nullstelle, d.h. mehr Nullstellen als p^r, was aber nicht geht. Also $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) = \{\mathrm{Id}, F, F^2, \ldots, F^{m-1}\}$. ∎

8.6 Der Satz vom primitiven Element

Satz vom primitiven Element *Jede separable endliche Erweiterung L/k enthält ein primitives Element.*

Beweis. 1. Fall, k unendlich: Nach Induktion ist oBdA $L = k(\alpha, \beta)$ erzeugt durch zwei Elementen. Nach Korollar 8.7 gibt es nur endlich viele Zwischenkörper $k \subseteq M \subseteq L$. Also gibt es $\lambda \neq \mu \in k$ mit $k(\alpha + \lambda\beta) = k(\alpha + \mu\beta) =: M$. Dann ist M/k einfach. Aber $\beta = \frac{(\alpha+\mu\beta)-(\alpha+\lambda\beta)}{\mu-\lambda}$ und $\alpha = (\alpha + \lambda\beta) - \lambda\beta$ liegen beide in M, also $M = L$.

2. Fall, k endlich: Es ist $L = \mathbb{F}_q$ für ein $q = p^m$. Jeder Teilkörper ist ein $\mathbb{F}_{p^r}$ mit $r < m$, und der Zerfällungskörper von $X^{p^r} - X$. Also gibt es pro p^r höchstens ein Teilkörper mit p^r Elemente. Wegen $p + p^2 + \cdots + p^{r-1} < p^r$ ist die Vereinigung aller Teilkörper eine echte Teilmenge von L. Also ist $L/\mathbb{F}_p$ einfach, daher auch L/k. ∎

Beispiel Wir zeigen, dass $\mathbb{Q}(i, \sqrt{2}, \sqrt{5}, \sqrt{13}) = \mathbb{Q}(\alpha)$ ist für $\alpha = i + \sqrt{2} + \sqrt{5} + \sqrt{13}$.

Schreiben wir $L = \mathbb{Q}(i, \sqrt{2}, \sqrt{5}, \sqrt{13})$. Sei $b_1 = -1$, $b_2 = 2$, $b_3 = 5$ und $b_4 = 13$. Sei $M_i = \mathbb{Q}(\sqrt{b_1}, \ldots, \widehat{\sqrt{b_i}}, \ldots, \sqrt{b_4})$, dann ist $L = M_i(\sqrt{b_i})$. Aus Beispiel 7.9 wissen wir: $[M_1 : \mathbb{Q}] = 8$, daher $[L : \mathbb{Q}] = 16$. Es folgt, dass $i, \sqrt{2}, \sqrt{5}, \sqrt{13}$ linear unabhängig über $\mathbb{Q}$ sind. Ferner gibt es wegen $[L : M_i] = 2$ für jedes $1 \leq i \leq 4$ ein $\tau_i \in \mathrm{Aut}(L/\mathbb{Q})$ mit $\tau_i|_{M_i} = \mathrm{Id}$ und $\tau_i(\sqrt{b_i}) = -\sqrt{b_i}$. Für $e_1, \ldots, e_4 \in \{0, 1\}$ ist daher

$$\tau_1^{e_1}\tau_2^{e_2}\tau_3^{e_3}\tau_4^{e_4}(i + \sqrt{2} + \sqrt{5} + \sqrt{13}) = (-1)^{e_1}i + (-1)^{e_2}\sqrt{2} + (-1)^{e_3}\sqrt{5} + (-1)^{e_4}\sqrt{13}\,.$$

Mit 16 Elementen ist also $\{\tau_1^{e_1}\tau_2^{e_2}\tau_3^{e_3}\tau_4^{e_4} \mid e_i \in \{0, 1\}\}$ ganz $\mathrm{Gal}(L/\mathbb{Q})$. Folglich ist $\sigma(\alpha) = \alpha$ nur für $\sigma = \mathrm{Id}$. Nach der Galoiskorrespondenz ist jeder Zwischenkörper ein Fixkörper, daher gibt es keinen echten Zwischenkörper, der α enthält. Das heißt, $L = \mathbb{Q}(\alpha)$.

Lemma 8.9 *Sei α ein Element der Galoiserweiterung K/k. Die Elemente der Menge $T = \{\sigma(\alpha) \mid \sigma \in \mathrm{Gal}(K/k)\}$ heißen die* Galois-Konjugierten *von α. Es ist*

$$m_\alpha(X) = \prod_{\beta \in T}(X - \beta)\,.$$

Beispiele a) $K/k = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{2}/\mathbb{Q}$, der Zerfällungskörper von $X^3 - 2$: Die Konjugierten von $\sqrt[3]{2}$ sind $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$ und $\omega^2\sqrt[3]{2}$. Die Konjugierten von $\sqrt{-3}$ sind $\pm\sqrt{-3}$.

b) $K/k = \mathbb{Q}(\sqrt{3}, \sqrt{7})/\mathbb{Q}$. Die Konjugierten von $\sqrt{3} + \sqrt{7}$ sind $\pm\sqrt{3} \pm \sqrt{7}$ (unabhängige Vorzeichen).

Beweis. Einerseits ist jedes $\beta = \sigma(\alpha)$ eine Nullstelle von $m_\alpha(X)$, wegen Lemma 7.4. Andererseits ist jede Nullstelle von $m_\alpha(X)$ ein $\sigma(\alpha)$, wegen Lemma 7.3, Satz 7.2 und Lemma 7.5. ∎

Beispiel Betrachten wir den endlichen Körper $\mathbb{F}_q$ für $q = p^m$. Ist $\alpha \in \mathbb{F}_q$, so gibt es einen $d \mid m$ mit $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^d}$. Daher ist $m_\alpha \in \mathbb{F}_p[X]$ vom Grad d. Ist umgekehrt $f \in \mathbb{F}_p[X]$ normiert und irreduzibel von Grad $d \mid m$, so ist der Zerfällungskörper von f der Körper $\mathbb{F}_{p^d} \subseteq \mathbb{F}_q$. Daher gilt:

> $X^q - X$ faktorisiert in $\mathbb{F}_p[X]$ als das Produkt aller normierten irreduziblen Polynome, dessen Grad m teilt. Wegen des Satzes vom primitiven Element kommen Faktoren vom Grad m immer vor.

Einige Beispiele (für $p = 2$ bzw. für $p = 3$):

$$
\begin{aligned}
&X^2 - X = X(X+1)\\
&X^4 - X = X(X+1)(X^2+X+1)\\
&X^8 - X = X(X+1)(X^3+X+1)(X^3+X^2+1)\\
&X^3 - X = X(X-1)(X+1)\\
&X^9 - X = X(X-1)(X+1)(X^2+1)(X^2+X-1)(X^2-X-1)
\end{aligned}
$$

8.7 Kreisteilungskörper

Hier behandeln wir den Zerfällungskörper von $X^m - 1 \in \mathbb{Q}[X]$ für $m \geq 2$. Dies wird erzeugt durch die $m$ten Einheitswurzeln. Zur Erinnerung: ist R ein Ring, so bezeichnen wir mit R^* die Gruppe der Einheiten in R.

Definition Die Eulersche ϕ-Funktion $\phi\colon \mathbb{N}_1 \to \mathbb{N}_0$ ist gegeben durch

$$\phi(m) := |(\mathbb{Z}/m\mathbb{Z})^*| \ .$$

Es ist $\phi(1) = 1$. Für $m \geq 2$ ist $\phi(m)$ die Anzahl der $0 < r < m$ mit $\mathrm{ggT}(r, m) = 1$.

Für $m \geq 1$ sei $\zeta_m := \exp\left(\frac{2\pi i}{m}\right) \in \mathbb{C}$. Dann sind die m Zahlen $1, \zeta_m, \zeta_m^2, \ldots, \zeta_m^{m-1}$ paarweise verschieden, und Nullstellen von $X^m - 1$. Daher ist $\mathbb{Q}(\zeta_m)$ der Zerfällungskörper von $X^m - 1$. Man nennt $\mathbb{Q}(\zeta_m)$ einen *Kreisteilungskörper*. Für $0 \leq r < m$ ist $\mathbb{Q}(\zeta_m^r) \subseteq \mathbb{Q}(\zeta_m)$, mit Gleichheit genau dann, wenn $\mathrm{ggT}(r, m) = 1$ ist. Daher sind die ζ_m^r mit $\mathrm{ggT}(r, m) = 1$ die *primitiven* $m$ten Einheitswurzeln. Das Polynom

$$\Phi_m(X) = \prod_{\mathrm{ggT}(r,m)=1} (X - \zeta_m^r)$$

heißt das $m$te *Kreisteilungspolynom*. Es ist $\mathrm{grad}(\Phi_m) = \phi(m)$.

Lemma 8.10 *Φ_m ist normiert und liegt in $\mathbb{Z}[X]$. Es ist*

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

Es ist $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \phi(m)$, und $\Phi_m(X)$ ist das Minimalpolynom von ζ_m.

Beweis. Die Faktorisierung von $X^m - 1$: Wahr für $m = 1$. Es ist $X^m - 1 = \prod_{r=0}^{m-1}(X - \zeta_m^r)$. Ist $\mathrm{ggT}(r, m) = 1$, so ist $(X - \zeta_m^r)$ Faktor von $\Phi_m(X)$. Ist $\mathrm{ggT}(r, m) = s > 1$, so hat ζ_m^r Ordnung d für $d = \frac{m}{s}$, daher ist $(X - \zeta_m^r)$ ein Faktor von $\Phi_d(X)$. Umgekehrt kommt jeder Faktor vor.

Φ_m ist nach Konstruktion normiert. Nach Induktion über m liegt es zuerst in $\mathbb{Q}[X]$ und dann wegen Gauß in $\mathbb{Z}[X]$.

Für den Rest reicht es, die Irreduzibilität von Φ_m nachzuweisen. Ist Φ_m nicht irreduzibel, so gilt $\Phi_m(X) = f(X)g(X)$, wobei $f \in \mathbb{Q}[X]$ das Minimalpolynom von ζ_m ist. Wegen Gauß sind f, g normierte Polynome in $\mathbb{Z}[X]$. Sei p eine Primzahl mit $\mathrm{ggT}(p, m) = 1$, und angenommen ζ ist eine Nullstelle von f mit $f(\zeta^p) \neq 0$. Dann ist $g(\zeta^p) = 0$, denn auch ζ^p ist eine Nullstelle von Φ_m. Also ist $g(X^p)$ durch $f(X)$ teilbar, d.h. durch das Minimalpolynom von ζ. Also $g(X^p) = f(X)h(X)$ mit $h \in \mathbb{Z}[X]$ normiert. Reduzieren wir jetzt mod p: seien $\bar{f}, \bar{g}, \bar{h} \in \mathbb{F}_p[X]$ die Polynome, deren Koeffizienten die Restklassen der Koeffizienten von f, g, h sind. Dann $\bar{g}(X^p) = \bar{f}(X)\bar{h}(X)$, d.h. $\bar{g}(X)^p = \bar{f}(X)\bar{h}(X)$. Somit haben $\bar{f}, \bar{g}$ einen gemeinsamen Faktor und daher eine gemeinsame Nullstelle. Somit hat $X^m - 1$ eine wiederholte Nullstelle in Charakteristik p. Widerspruch, denn wegen $\mathrm{ggT}(p, m) = 1$ ist $\mathrm{ggT}(D(X^m - 1), X^m - 1) = 1$.

Also ζ^p ist Nullstelle von f für jede Primzahl p mit $\mathrm{ggT}(p, m) = 1$ und jede Nullstelle ζ von f. Ist $\mathrm{ggT}(r, m) = 1$, so kommen nur Primzahlen dieser Art in der Faktorisierung von r vor, also Induktion über die Anzahl der Primfaktoren: ζ_m^r ist eine Nullstelle von f. Somit hat f den gleichen Grad $\phi(m)$ wie $\Phi_m(X)$. Also $f = \Phi_m$. ∎

Beispiel

$$\begin{aligned}
\Phi_1(X) &= X - 1 & X - 1 &= \Phi_1 \\
\Phi_2(X) &= X + 1 & X^2 - 1 &= \Phi_1\Phi_2 \\
\Phi_3(X) &= X^2 + X + 1 & X^3 - 1 &= \Phi_1\Phi_3 \\
\Phi_4(X) &= X^2 + 1 & X^4 - 1 &= \Phi_1\Phi_2\Phi_4 \\
\Phi_5(X) &= X^4 + X^3 + X^2 + X + 1 & X^5 - 1 &= \Phi_1\Phi_5 \\
\Phi_6(X) &= X^2 - X + 1 & X^6 - 1 &= \Phi_1\Phi_2\Phi_3\Phi_6
\end{aligned}$$

Definition Eine endliche Körpererweiterung K/k heißt *abelsch*, falls sie Galois ist, und außerdem die Galoisgruppe $\mathrm{Gal}(K/k)$ eine abelsche Gruppe ist.

Beispiel $\mathbb{F}_q/\mathbb{F}_p$ hat zyklische Galoisgruppe und ist daher abelsch. Der Zerfällungskörper von $X^3 - 2 \in \mathbb{Q}[X]$ ist nicht abelsch.

Bezeichnung Kreisteilungspolynome werden auch *zyklotomisch* genannt.

Lemma 8.11 *Jeder Kreisteilungskörper $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ ist abelsch.*

Beweis. Galois wissen wir. Sind σ, τ zwei Automorphismen, so gibt es $r, s \in \mathbb{Z}$ mit $\mathrm{ggT}(r, m) = \mathrm{ggT}(s, m) = 1$ und $\sigma(\zeta_m) = \zeta_m^r$, $\tau(\zeta_m) = \zeta_m^s$. Dann $\sigma\tau, \tau\sigma$ bilden ζ_m auf ζ_m^{rs} ab. Da ζ_m die Erweiterung erzeugt, gilt daher $\sigma\tau = \tau\sigma$. ∎

Beispiel $\mathrm{Gal}(\mathbb{Q}(\zeta_{12})/\mathbb{Q})$ ist abelsch aber nicht zyklisch. Die primitivane 12ten Einheitswurzeln sind $\zeta_{12}, \zeta_{12}^5, \zeta_{12}^7, \zeta_{12}^{11}$. Daher ist $\operatorname{grad} \Phi_{12} = 4$, weshalb die Erweiterung Grad 4 hat, und $|\mathrm{Gal}(\mathbb{Q}(\zeta_{12})/\mathbb{Q})| = 4$ ist. Die Galoisgruppe ist daher $\{\mathrm{Id}, \rho, \sigma, \tau\}$ mit

$$\rho(\zeta_{12}) = \zeta_{12}^5 \qquad \sigma(\zeta_{12}) = \zeta_{12}^7 \qquad \tau(\zeta_{12}) = \zeta_{12}^{11}\,.$$

Da $5^2 = 25$, $7^2 = 49$ und $11^2 = 121$ alle $\equiv 1 \pmod{12}$ sind, folgt $\rho^2 = \sigma^2 = \tau^2 = \mathrm{Id}$. Daher ist die Galoisgruppe nicht zyklisch, sondern isomorph zu $C_2 \times C_2$.

9 Fortsetzung der Gruppentheorie

9.1 Lösbarkeit durch Radikale

Wir leiten die Beziehung zwischen Lösbarkeit durch Radikale und Auflösbarkeit der Galoisgruppe her.

Beispiel $\mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})/\mathbb{Q}$ ist nicht abelsch, denn die Galoisgruppe ist S_3. Für den Zwischenkörper $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{-3}) \subseteq \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ dagegen sind beide Teilerweiterungen abelsch.

Es gibt eine allgemeine Formel für die Nullstellen eines kubischen Polynoms $X^3 + aX^2 + bX + c \in \mathbb{Q}[X]$. In dieser Formel kommen vor u.a.

- Die 3. Einheitswurzel $\omega = \exp\left(\frac{2\pi i}{3}\right)$;
- $\sqrt{D}$ für ein $D \in \mathbb{Q}$;
- $\sqrt[3]{E}$ für ein $E \in \mathbb{Q}(\sqrt{D})$.

Allgemeiner sagen wir:

Bezeichnung Eine algebraische Zahl $\alpha \in \mathbb{A}$ *lässt sich durch Radikale ausdrücken*, wenn es einen Turm $\mathbb{Q} = k_0 \subseteq k_1 \subseteq \cdots \subseteq k_n$ von Körpererweiterungen gibt derart, dass $\alpha \in k_n$ ist, und für $1 \leq r \leq n$ ist

- entweder $k_r = k_{r-1}(\sqrt[m_r]{D_r})$ für ein $D_r \in k_{r-1}$;
- oder $k_r = k_{r-1}(\zeta_{m_r})$ (primitive Einheitswurzel).

Beispiele Die Nullstellen von $x^2 + px + q = 0$ lassen sich durch Radikale ausdrücken: es ist $n = 1$ und $k_1 = \mathbb{Q}(\sqrt{p^2 - 4q})$. Auch die Nullstellen eines beliebigen kubischen Polynoms aus $\mathbb{Q}[X]$ lassen sich durch Radikale ausdrücken.

Die Zahl $\alpha = \sqrt[4]{2} - \zeta_3 \sqrt[5]{\sqrt{3} + 1}$ lässt sich durch Radikale ausdrücken. Ein Turm von Erweiterungen ist:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{3}, \zeta_3) \subseteq \mathbb{Q}(\sqrt{3}, \zeta_3, \sqrt[4]{2}) \subseteq \mathbb{Q}(\sqrt{3}, \zeta_3, \sqrt[4]{2}, \sqrt[5]{\sqrt{3} + 1})\,.$$

Vereinfachende Überlegung Sei m das kgV *aller* m_r. Dann oBdA $k_1 = \mathbb{Q}(\zeta_m)$, also nach Lemma 8.11 ist $k_1/\mathbb{Q}$ abelsch. Für $r \geq 2$ ist dann $k_r = k_{r-1}(\sqrt[m_r]{D_r})$, mit $m_r \mid m$ und daher $\zeta_{m_r} \in k_1 \subseteq k_{r-1}$. Nach dem Hilfslemma unten ist also auck k_r/k_{r-1} abelsch.

Hilfslemma Sei k ein Erweiterungskörper von $\mathbb{Q}$ mit $\zeta_m \in k$, und sei $D \in k$. Dann ist $k(\sqrt[m]{D})/k$ abelsch.

Beweis. Galois: denn die Nullstellen von $X^m - D$ sind die $\zeta_m^s \sqrt[m]{D}$. Abelsch: jeder Automorphismus $\sigma \in \mathrm{Aut}(k(\sqrt[m]{D})/k)$ fixiert ζ_m und wird eindeutig bestimmt durch die Exponente $s = s(\sigma)$ in $\sigma(\sqrt[m]{D}) = \zeta_m^s \sqrt[m]{D}$, also $s(\sigma\tau) = s(\sigma) + s(\tau) = s(\tau\sigma)$. ∎

Also können wir durch die Wahl von k_1 sicherstellen, dass k_r/k_{r-1} abelsch ist für jedes $1 \leq r \leq n$. Noch schöner wäre es, wenn außerdem $k_n/\mathbb{Q}$ Galois wäre.

Lemma 9.1 *Sei $k/\mathbb{Q}$ Galois mit $\zeta_m \in k$. Sei $D \in k$. Dann gibt es eine KE. K/k derart, dass*

- *$K/\mathbb{Q}$ Galois ist;*
- *$X^m - D$ zerfällt in $K[X]$ als ein Produkt von linearen Faktoren; und*
- *es gibt einen Turm $k = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_s = K$ derart, dass jede KE L_r/L_{r-1} abelsch ist.*

Beweis. Sei $\alpha \in \mathbb{A}$ eine Nullstelle von $X^m - D$. Wegen $\zeta_m \in k$ liegt jede Nullstelle von $X^m - D$ bereits in $k(\alpha)$. Sei $f \in \mathbb{Q}[X]$ das Minimalpolynom von α über $\mathbb{Q}$; sei $g \in \mathbb{Q}[X]$ ein Polynom, dessen Zerfällungskörper k ist (vierfache Charakterisierung!); und sei K der Zerfällungskörper über $\mathbb{Q}$ von fg. Dann ist $K/\mathbb{Q}$ Galois, und $k(\alpha) \subseteq K$, also sind die ersten beiden Bedingungen erfüllt. Nach dem Hilfslemma ist $k(\alpha)/k$ abelsch, also oBdA $L_1 = k(\alpha)$. Nun angenommen wir haben $L_{r-1} \subsetneq K$ für $r \geq 2$. Da K der Zerfällungskörper über k von f ist, gibt es eine Nullstelle β von f mit $\beta \notin L_{r-1}$. Da α, β zwei Nullstellen des irreduziblen Polynoms $f \in \mathbb{Q}[X]$ sind, gibt es ein $\sigma \in \mathrm{Aut}(K/\mathbb{Q})$ derart, dass $\sigma(\alpha) = \beta$. Da $k/\mathbb{Q}$ normal ist, ist $\sigma(k) = k$, also liegt $D' := \sigma(D)$ in k, daher ist β eine Nullstelle von $X^m - D' \in k[X] \subseteq L_{r-1}[X]$. Mit $L_r = L_{r-1}(\beta)$ ist dann L_r/L_{r-1} abelsch, und $\beta \in L_r$. Durch iterieren erreichen wir am Ende K. ∎

Bemerkung Lassen sich α, β beide durch Radikale ausdrücken, so gibt es Türme $\mathbb{Q} = k_0 \subseteq \cdots \subseteq k_n$ und $\mathbb{Q} = K_0 \subseteq K_N$ mit $\alpha \in k_n$ und $\beta \in K_N$, und außerdem ist jedes $k_r = k_{r-1}(x_r)$, $K_s = K_{s-1}(y_s)$ mit jedem x_r, y_s entweder eine Einheitswurzel oder ein $\sqrt[m]{D}$.

Indem man für $1 \leq s \leq N$ den Körper k_{n+s} definiert durch $k_{n+s} = k_{n+s-1}(y_s)$, so ist $K_s \subseteq k_{n+s}$. Daher ist $\mathbb{Q} = k_0 \subseteq \cdots \subseteq k_{n+N}$ ein ähnlich gebauter Turm mit $\alpha, \beta \in k_{n+N}$. Analog kann man für $\alpha_1, \ldots, \alpha_t$, die sich durch Radikale ausdrücken lassen, einen solchen Turm konstruieren derart, dass $\alpha_1, \ldots, \alpha_t$ alle im letzten Körper liegen. Indem man die Prozedere aus der vereinfachende Überlegung anwendet, stellt man zudem sicher, dass jede Teilerweiterung im Turm abelsch ist.

Satz 9.2 *Seien $\alpha_1, \ldots, \alpha_t \in \mathbb{A}$ algebraische Zahlen, die sich durch Radikale ausdrücken lassen. Dann gibt es eine KE $M/\mathbb{Q}$ derart, dass*

- $\alpha_1, \ldots, \alpha_t \in M$;
- $M/\mathbb{Q}$ *ist Galois; und*
- *es gibt einen Turm* $\mathbb{Q} = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_t = M$ *von Zwischenkörper derart, dass* M_r/M_{r-1} *abelsch ist für jedes* $1 \leq r \leq t$.

Bemerkung Mit etwas Arbeit kann man die Sonderrolle der Einheitswurzeln beseitigen, und auch die umgekehrte Aussage zeigen: gibt es ein solches M, so lässt sich jedes α_i durch Radikale ausdrücken.

Beweis. Bisher wissen wir, dass es einen Turm $\mathbb{Q} = k_0 \subseteq k_1 \subseteq \cdots \subseteq k_n$ gibt, mit k_r/k_{r-1} abelsch für alle $r \geq 1$; $\alpha_1, \ldots, \alpha_t \in k_n$; $k_1 = \mathbb{Q}(\zeta_m)$; und für $r \geq 2$ ist $k_r = k_{r-1}(\sqrt[m_r]{D_r})$ mit $m_r \mid m$, $D_r \in k_{r-1}$. Sei $K_0 = \mathbb{Q}$, $K_1 = k_1$. Für $2 \leq r \leq n$ sei K_r das K aus Lemma 9.1 zu $k = K_{r-1}$ und $X^m - D = X^{m_r} - D_r$. Nach Induktion ist $k/\mathbb{Q}$ Galois, also auch $K_r/\mathbb{Q}$. Also ist $M = K_n$ Galois über $\mathbb{Q}$; jedes α_i liegt in M; und die L_i aus dem Lemma zwischen K_{r-1} und K_r stellen die abelschen Erweiterungen für die Enzelschritte bereit. ∎

9.2 Normalreihen und Auflösbare Gruppen

Definition Sei G eine Gruppe.

- Eine Kette
$$\{e\} = G_0 \leq G_1 \leq G_2 \leq \cdots \leq G_n = G$$
von Untergruppen heißt einer *Normalreihe* der *Länge* n, falls $G_{r-1} \lhd G_r$ ist für jedes $1 \leq r \neq n$. Die G_r/G_{r-1} heißen die *Faktorgruppen* dieser Normalreihe.
- Eine Normalreihe heißt *auflösbar*, falls jede Faktorgruppe abelsch ist.
- Eine Gruppe heißt *auflösbar*, falls sie eine auflösbare Reihe hat.

Beispiel S_3 ist auflösbar, denn $1 \lhd A_3 \lhd S_3$ ist eine auflösbare Reihe.

Korollar 9.3 *Seien* $\alpha_1, \ldots, \alpha_t \in \mathbb{A}$ *algebraische Zahlen, die sich durch Radikale ausdrücken lassen. Dann gibt es eine Galoiserweiterung* $K/\mathbb{Q}$ *mit* $\alpha_1, \ldots, \alpha_t \in K$ *derart, dass* $\mathrm{Gal}(K/k)$ *auflösbar ist.* ∎

Strategie Wir werden sehen, dass A_5 und S_5 nicht auflösbar sind. Ferner werden wir sehen, dass die Galoisgruppe eines irreduziblen Polynoms $f \in \mathbb{Q}[X]$ auflösbar sein muss, wenn das Polynom sich durch Radikale lösen lässt. Somit ist z.B. $x^5 - 80x + 5 = 0$ nicht durch Radikale lösbar.

Lemma 9.4 *Sei* G *eine endliche auflösbare Gruppe. Dann: jede Untergruppe von* G *ist auflösbar, und jede Quotientengruppe von* G *ist auflösbar.*

Bemerkung Ist $N \lhd G$ derart, dass N auflösbar und G/N abelsch ist, dann ist auch G auflösbar.

Beweis. Induktion über $|G|$, klar für $|G| = 1$. Nun sei $|G| > 1$, und sei

$$\{e\} = G_0 \leq G_1 \leq G_2 \leq \cdots \leq G_n = G$$

eine auflösbare Reihe für G. OBdA ist $K := G_{n-1}$ ein *echter* Normalteiler von G.

Untergruppen $H \leq G$: Nach dem ersten Isomorphiesatz ist $H \cap K \lhd H$, und $H/(H \cap K) \cong HK/K \leq G/K$. Also ist $H/(H \cap K)$ abelsch, denn G/K ist abelsch; und $H \cap K$ ist auflösbar, da eine Untergruppe von K. Nach der Bemerkung oben also ist H auflösbar.

Normalteiler $N \lhd G$: Es ist $NK/N \cong K/(K \cap N)$ (1. Isomorphiesatz), daher NK/N auflösbar (Induktionsannahme). Es ist $G/NK \cong (G/K)/(NK/K)$ (2. Isomorphiesatz), also G/NK abelsch wegen G/K abelsch. Nach der Bemerkung oben ist daher G/N auflösbar. ∎

Korollar 9.5 *Sei $f \in \mathbb{Q}[X]$ ein Polynom und L der Zerfällungskörper von f über $\mathbb{Q}$. Lässt sich jede Nullstelle von f durch Radikale ausdrücken, so ist* Gal(L/k) *auflösbar. Das gleiche gilt, falls f irreduzibel ist und* eine *Nullstelle hat, die sich durch Radikale ausdrücken lässt.*

Beweis. Lässt sich jede Nullstelle durch Radikale ausdrücken, so gibt es nach Korollar 9.3 eine auflösbare Erweiterung $K/\mathbb{Q}$ mit $L \subseteq K$. Dann Gal$(L/\mathbb{Q})$ eine Quotientengruppe von Gal$(K/\mathbb{Q})$ nach der Galoiskorrespondenz, also Gal$(K/\mathbb{Q})$ auflösbar.

Ist f irreduzibel und α eine Nullstelle, die sich durch Radikale ausdrücken lässt, dann erhält man $K/\mathbb{Q}$ normal, also *aller* Nullstellen in K. ∎

9.3 Permutationen

Bemerkung Die Zerlegung einer Permutation in disjunkten Zyklen setzen wir als bekannt voraus. Wegen der Eindeutigkeit dieser Zerlegung hat jede Permutation $\sigma \in S_n$ einen wohldefinierten *Typ* $2^{n_2}3^{n_3}4^{n_4}5^{n_5}6^{n_6}\ldots$, wobei n_r die Anzahl von r-Zyklen in der Zerlegung von σ ist. Vorsicht: der Typ 4^1 von (1 3 2 4) und der Typ 2^2 von (1 4)(2 3) sind nicht gleich, d.h. der Typ ist nicht auszumultiplizieren.

Beispiel Der Typ von (1 2)(3 4 5)(6 7)(8 9 10 11 12) ist $2^2 3^1 5^1$.

Bemerkung Bekanntlich ist $|S_n| = n!$.

Lemma 9.6 *a) Jeder r-Zykel ist ein Produkt von $r-1$ Transpositionen.*

b) Jede Permutation $\sigma \in S_n$ ist ein Produkt von Transpositionen.

c) Die $n-1$ Transpositionen $(1\ 2)$, $(1\ 3)$, $(1\ 4)$, $\ldots$, $(1\ n)$ erzeugen S_n.

d) Die $n-1$ Transpositionen $(1\ 2)$, $(2\ 3)$, $(3\ 4)$, $\ldots$, $(n-1\ n)$ erzeugen auch S_n.

e) Die Transposition $(1\ 2)$ und der n-Zykel $(1\ 2\ \ldots\ n)$ erzeugen S_n.

Beweis. a) Induktion über r, da $(a_1\ a_2\ \ldots\ a_r) = (a_1\ a_r)(a_1\ a_2\ \ldots\ a_{r-1})$.

b) Folgt aus a, da jede Permutation ein Produkt von disjunkten Zykeln.

c) Für $1 < a < b$ gilt $(a\ b) = (1\ a)(1\ b)(1\ a)$.

d) Für $2 \le r \le n-1$ gilt $(1\ r+1) = (r\ r+1)(1\ r)(r\ r+1)$.

e) Für $2 \le r \le n-1$ gilt $(r\ r+1) = (1\ 2\ \ldots\ n)(r-1\ r)(1\ 2\ \ldots\ n)^{-1}$. ∎

Aus der LAAG1 wissen wir:

Definition Die *Signatur* $\varepsilon(\sigma)$ einer Permutation $\sigma \in S_n$ wird definiert durch

$$\varepsilon(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(j) - \sigma(i)}{j - i} \in \{1, -1\}\,.$$

Bekanntlich ist die Signatur ein Gruppenhomomorphismus $\varepsilon\colon S_n \to C_2$ (s. Lemma A.1 für einen Beweis). Aus Lemma 9.6 erhalten wir dann:

Lemma 9.7 *Ist σ ein Produkt von N Transpositionen, so ist $\varepsilon(\sigma) = (-1)^N$. Jeder r-Zykel hat Signatur $(-1)^{r-1}$.*

Beweis. Folgt aus Lemma 9.6, sofern wir zeigen: jede Transposition hat Signatur -1. Definition der Signatur: $\varepsilon(\tau) = -1$ für $\tau = (r\ r+1)$. Beweis von Lemma 9.6 d): $\varepsilon(\tau) = -1$ für $\tau = (1\ a)$. Beweis von Lemma 9.6 c): $\varepsilon(\tau) = -1$ für jede Transposition. ∎

Definition Sei σ eine Permutation. Ist $\varepsilon(\sigma) = 1$, so heißt σ *gerade*; ist $\varepsilon(\sigma) = -1$, so heißt σ *ungerade*. Die *alternierende* Gruppe A_n ist die Menge der geraden Permutationen, d.h. der Kern von $\varepsilon\colon S_n \to C_2$, daher $A_n \lhd S_n$.

Bemerkung Nach Lemma 9.6 ist jede Permutation σ ein Produkt von Transpositionen. Nach Lemm 9.7 gilt: ist σ ein Produkt von N Permutationen, so ist N gerade, falls σ gerade ist, und N ist ungerade, falls σ ungerade ist. Also für $n \ge 2$ ist $|S_n\colon A_n| = 2$ und $|A_n| = \frac{1}{2}n!$.

9.4 Gruppenoperationen

Definition Sei G eine Gruppe und X eine Menge. Eine (Links-)Operation von G auf X besteht aus einer Abbildung $\rho\colon G \times X \to X$, $(g, x) \mapsto gx$, mit den folgenden Eigenschaften:

(O1) Assoziativität: $g(hx) = (gh)x$ für alle $g, h \in G$, $x \in X$.

(O2) Normierung: $ex = x$ für alle $x \in X$.

Beispiele a) Die Diedergruppe D_n operiert auf dem regulären n-Eck.

b) Jede Gruppe operiert auf sich selbst durch Konjugation: G ist beliebig, $X = G$ und $\rho(g, x) = gxg^{-1}$.

c) Die allgemeine lineare Gruppe $GL_n(k) = \{A \in M_n(k) \mid \det(A) \neq 0\}$ operiert auf k^n durch $\rho(A, v) = A \cdot v$.

d) Die symmetrische Gruppe S_n operiert auf $\{1, \ldots, n\}$ durch $\rho(\sigma, r) = \sigma(r)$.

e) $\mathrm{Aut}(K/k)$ operiert auf K durch $\rho(\sigma, \alpha) = \sigma(\alpha)$.

Definition Die Gruppe G operiere auf der Menge X.

a) Der *Stabilisator* $G_x = \mathrm{Stab}_G(x)$ eines Elements $x \in X$ ist

$$G_x := \{g \in G \mid gx = x\}\,.$$

b) Die *Bahn* $Gx = \mathrm{Bahn}_G(x)$ ist $Gx := \{gx \mid g \in G\}$. Die Anzahl der Elemente einer Bahn heißt die *Länge*.

Lemma 9.8 *a) Für jedes $x \in X$ ist $\mathrm{Stab}_G(x) \leq G$.*

b) Die Relation $y \in \mathrm{Bahn}_G(x)$ ist eine Äquivalenzrelation auf X, deren Äquivalenzklassen die Bahnen der Operation sind.

Beweis. a) Es ist $ex = x$, also $e \in \mathrm{Stab}_G(x)$. Ist $gx = x$, dann $g^{-1}x = x$. Ist $gx = x$ und $hx = x$, dann $(gh)x = g(hx) = gx = x$.

b) Reflexiv, da $ex = x$. Symmetrisch, da $y = gx$ genau dann, wenn $x = g^{-1}y$. Transitiv, da aus $y = gx$ und $z = hy$ folgt $z = (hg)x$. ∎

Lemma 9.9 (Die Bahnengleichung) *Für jedes $x \in X$ gilt:*

$$|\mathrm{Stab}_G(x)| \cdot |\mathrm{Bahn}_G(x)| = |G|\,.$$

Beweis. Sei $H = \mathrm{Stab}_G(x) \leq G$. Nach Lagrange ist $|G| = |H| \cdot |G : H|$. Sei $f\colon G \to X$ die Abbildung $g \mapsto gx$. Dann $\mathrm{Bild}(f) = \mathrm{Bahn}_G(x)$. Es ist $f(g) = f(g')$ genau dann, wenn $gH = g'H$, also gilt $|\mathrm{Bahn}_G(X)| = |G : H|$. ∎

Bahnen bezüglich Konjugation heißen *Konjugationsklassen.*

Lemma 9.10 *Sei G eine Gruppe und $H \leq G$.*

a) $H \lhd G \Leftrightarrow$ H eine Vereinigung von Konjugationsklassen.

b) Für $\sigma, \pi \in S_n$ berechnet man $\pi\sigma\pi^{-1}$ aus der disjunkten Zykel-Zerlegung von σ, indem man π auf jedem Zykeleintrag anwendet.

c) Zwei Permutationen $\sigma, \tau \in S_n$ liegen genau dann in der gleichen Konjugationsklasse, wenn sie vom gleichen Typ sind.

Beweis. a) Genau dann ist $H \lhd G$, wenn $ghg^{-1} \in H$ ist für alle $g \in G$, $h \in H$. b), c): selber nachrechnen. ∎

9.5 A_5 ist nicht auflösbar

Lemma 9.11 *In der alternierenden Gruppe A_5 gibt es genau 5 Konjugationsklassen:*

- *Das neutrale Element;*
- *Alle 3-Zykel (20 Stück);*
- *Alle Permutationen vom Typ 2^2, d.h. vom Typ $(a\ b)(c\ d)$ (15 Stück)*
- *Zwei verschiedene Konjugationsklassen von je zwölf 5-Zykeln. Ist σ ein 5-Zykel, so ist $\sigma \sim \sigma^{-1}$, $\sigma \nsim \sigma^2$.*

Bezeichnung Der Zentralisator $C_G(g)$ eines Elements $g \in G$ ist $C_G(g) = \{h \in G \mid hg = gh\}$. Dies ist der Stabilisator $\mathrm{Stab}_G(g)$ bzgl. der Konjugationsoperation. Also $C_G(g) \leq G$, und

$$|G| = |\text{Konjugationsklasse von } g| \cdot |C_G(g)| \ .$$

Beweis. Ist $\sigma \in A_5$ ein 3-Zykel, so gibt es $\pi \in S_5$ mit $\pi(1\ 2\ 3)\pi^{-1} = \sigma$. Das gleiche gilt, wenn man π durch $\pi(4\ 5)$ ersetzt. Eins von diesen beiden ist gerade. Das gleiche gilt mit $\sigma = (a\ b)(c\ d)$, $(1\ 2)(3\ 4)$ und $\pi(1\ 2)$.

Es gibt 24 5-Zykel in S_5. Alle sind dort konjugiert, also ist $|C_{S_5}(\sigma)| = 5$ für $\sigma \in S_5$ ein 5-Zykel. Also $C_{S_5}(\sigma) = \langle\sigma\rangle \leq A_5$. Folglich hat die Konjugationsklasse von σ in A_5 die Länge 12.

Für $\sigma = (a\ b\ c\ d\ e)$ ist $\pi\sigma\pi^{-1} = \sigma^{-1}$ für $\pi = (b\ e)(c\ d) \in A_5$, und $\pi\sigma\pi^{-1} = (a\ c\ e\ b\ d) = \sigma^2$ für $\pi = (b\ c\ e\ d) \notin A_5$. Der Zentralisator liegt in A_5, also ist $\sigma \nsim \sigma^2$ in A_5. ∎

Definition Eine Gruppe G heißt *einfach*, wenn es genau zwei Normalteiler gibt: $\{e\}$ und G selbst.

Beispiel C_p

Satz 9.12 *Die Gruppe A_5 ist einfach.*

Beweis. Jeder Normalteiler ist eine Vereinigung von Konjugationsklassen, und die Summe deren Länge teilt $60 = |A_5|$. Die Klasse $\{\mathrm{Id}\}$ ist immer dabei. Rein zahnlenmäßig bedeutet also Lemma 9.11, dass $\{\mathrm{Id}\}$ und A_5 selber die einzigen Normalteiler sind. ∎

Korollar 9.13 *A_5, S_5 sind nicht auflösbar. Hat das irreduzible Polynom $f \in \mathbb{Q}[X]$ Galoisgruppe A_5 oder S_5, so lassen sich die Nullstellen nicht durch Radikale ausdrücken.*

Beweis. A_5 ist einfach und nichtabelsch, also nicht auflösbar. Wenn S_5 auflösbar wäre, so müsste auch A_5 auflösbar sein. ∎

9.6 Ein nicht lösbares quintisches Polynom

Lemma 9.14 (Der Satz von Cauchy) *Sei p eine Primzahl und G eine endliche Gruppe mit $p \mid |G|$. Dann enthält G mindestens ein Element der Ordnung p.*

Dieses Lemma beweisen wir im nächten Kapitel, als Korollar der Sylow-Sätze.

Korollar 9.15 *Sei p eine Primzahl und $H \leq S_p$ eine Untergruppe, die eine Transposition enthält und deren Ordnung durch p teilbar ist. Dann ist $H = S_p$.*

Beweis. Nach Cauchy enthält H ein Element σ der Ordnung p. Da p eine Primzahl ist, muss σ ein p-Zykel sein. OBdA ist die Transposition $\tau = (1\ 2)$. Indem man σ durch eine Potenz ersetzt, ist $\sigma(1) = 2$. OBdA ist $\sigma = (1\ 2\ 3\ \ldots\ p)$. Wegen $\sigma, \tau \in H$ ist daher $H = S_p$, wegen Lemma 9.6 e). ∎

Beispiel Das Polynom $f(X) = X^5 - 80X + 5 \in \mathbb{Q}[X]$ lässt sich nicht durch Radikale lösen.

Irreduzibel in $\mathbb{Z}[X]$ (Eisenstein, $p = 5$), daher auch in $\mathbb{Q}[X]$ (Gauß). Kurvendiskussion: es ist $f'(X) = 5(X^4 - 16)$, mit (reellen) Nullstellen in $X = \pm 2$. Es ist $f(-2) = 133$ und $f(2) = -123$, daher (wegen Grad 5) genau drei reelle Nullstellen, daher zwei komplexe. Also operiert die komplexe Konjugation als eine Transposition auf der Menge der 5 Nullstellen. Die Galoisgruppe permutiert diese fünf Nullstellen. Da f irreduzibel vom Grad 5 ist, teilt 5 den Erweiterungsgrad des Zerfällungskörpers und daher die Ordnung der Galoisgruppe. Da 5 eine Primzahl ist, ist daher die Galoisgruppe S_5, also ist das Polynom nicht durch Radikale lösbar.

10 p-Gruppen und die Sylow-Sätze

Definition Sei p eine Primzahl. Ist G eine endliche Gruppe mit $|G| = p^n$ für ein $n \geq 0$, so heißt G eine (endliche) *p-Gruppe*.

10.1 Sylowgruppen

Definition Sei G eine endliche Gruppe und p eine Primzahl. Dann gibt es eindeutig definierte r, n mit $|G| = p^r \cdot m$ und $\mathrm{ggT}(p, m) = 1$.

Eine *p-Sylowgruppe* von G ist eine Untergruppe $S \leq G$ mit $|S| = p^r$. Die Menge der p-Sylowgruppen bezeichnet man mit $\mathrm{Syl}_p(G)$.

Bemerkung Eine p-Sylowgruppe ist also eine Untergruppe, die eine p-Gruppe ist und dessen Index teilerfremd zu p ist.

Beispiel Eine 3-Sylowgruppe von S_4 ist $\langle(1\ 2\ 3)\rangle$. Nummeriert man die vier Ecken eines quadrats mit $1, 2, 3, 4$, so erhält man $D_4 \leq S_4$, eine 2-Sylowgruppe.

Die Sylow-Sätze *Sei G eine endliche Gruppe und p eine Primzahl. Dann:*

1. Sylow-Satz $\mathrm{Syl}_p(G) \neq \emptyset$.

2. Sylow-Satz *Für* $n_p(G) := \left|\mathrm{Syl}_p(G)\right|$ *ist* $n_p(G) \equiv 1 \pmod{p}$.

3. Sylow-Satz *G operiert transitiv auf* $\mathrm{Syl}_p(G)$ *mittels Konjugation.*

4. Sylow-Satz *Ist $P \leq G$ eine p-Gruppe, so gibt es ein $T \in \mathrm{Syl}_p(G)$ mit $P \leq T$.*

Bemerkung

a) Die ersten drei Sätze wurden 1872 von P. Ludwig Sylow bewiesen. Inzwischen zählt man auch den vierten zu den Sylow-Sätzen.

b) Die moderne Beweismethode stammt von H. Wielandt (1959).

c) Zwar würde der 1. Sylow-Satz aus dem 2. folgen – der Beweis des 2. setzt aber den 1. voraus.

d) Eine Operation von G auf X heißt *transitiv*, wenn es genau eine Bahn gibt.

In den Beweisen setzen wir durchgehend voraus: $|G| = p^r \cdot m$, mit $\mathrm{ggT}(p, m) = 1$.

Beweis des 1. Sylow-Satzes. Induktion über m. Ist $m = 1$ dann $G \in \mathrm{Syl}_p(G)$. Nun sei $m > 1$.

Sei Ω die Menge aller p^r-elementigen Teilmengen von G. Beachten Sie, dass die Zahl $N = |\Omega| = \binom{p^r \cdot m}{p^r}$ teilerfremd zu p ist, da $\mathrm{ggT}(p, m) = 1$.

G operiert auf Ω, durch $g * T = \{gt \mid t \in T\}$. Da die Summe der Bahnlängen $|\Omega|$ ist, muss es ein $T \in \Omega$ geben, dessen Bahnlänge nicht durch p teilbar ist.

Sei $H = \mathrm{Stab}_G(T) \leq G$. Bahnengleichung: $|G : H| =$ Bahnlänge von T, also $|H| = p^r \cdot n$ mit $n \leq m$. Für jedes $t \in T$ ist $G * t = G$; und $|G| > |T|$ wegen $m \geq 1$. Also ist $\mathrm{Bahn}_G(T) = \{T\}$ unmöglich, d.h. $n < m$. Nach Induktionsannahme ist $\mathrm{Syl}_p(H) \neq \emptyset$. Aber $\mathrm{Syl}_p(H) \subseteq \mathrm{Syl}_p(G)$. ∎

Beweis von Lemma 9.14, d.h. des Satzes von Cauchy. G ist eine Gruppe mit $p \mid |G|$, hat also eine p-Sylowgruppe S mit $|S| = p^r$, $r \geq 1$. Sei also $e \neq g \in S$, dann $o(g) = p^s$ mit $1 \leq s \leq r$. Dann $g^{p^{s-1}} \in S \leq G$ hat Ordnung p. ∎

Satz 10.1 *Sei $S \in \mathrm{Syl}_p(G)$ und sei $P \leq G$ eine p-Untergruppe. Dann gibt es $g \in G$ mit $P \leq gSg^{-1}$.*

Beweis. Sei Ω wie im Beweis des 1. Sylow-Satzes, und sei $X = \mathrm{Bahn}_G(S) \subseteq \Omega$. Dann $\mathrm{Stab}_G(S) = S$, also $p \nmid |X|$. Betrachten wir die Operation von P auf X. Jede Bahnlänge teilt $|P|$, also eine p-Potenz. Also gibt es eine Bahn der Länge 1: d.h. es gibt $g \in G$ mit $\forall h \in P\ hgS = gS$. Also $P \leq gSg^{-1}$. ∎

Beweis der 3. und 4. Sylow-Sätze. Der 4. Satz folgt sofort aus Satz 10.1, denn auch $gSg^{-1} \in \mathrm{Syl}_p(G)$. Für den 3.: Ist $P \in \mathrm{Syl}_p(G)$, dann aus $P \leq gSg^{-1}$ folgt $P = gSg^{-1}$. ∎

Beweis des 2. Sylow-Satzes. Sei $S \in \mathrm{Syl}_p(G)$. Auf $X = \mathrm{Syl}_p(G)$ operiert S durch Konjugation. Eine Bahn ist $\{S\}$. Nun sei $S \neq T \in \mathrm{Syl}_p(G)$. Die Länge der Bahn von T teilt p^r, ist also eine p-Potenz. Reicht also zu zeigen: Bahnlänge kann nicht 1 sein, d.h. $\{T\}$ kann nicht eine Bahn sein.

Angenommen, $\{T\}$ ist eine Bahn. Dann $ST = TS$, also ist $ST \leq G$ und $T \lhd ST$. Ferner ist $|ST| = |ST : T|\,|T|$, und wegen des 1. Isomorphiesatzes ist $|ST : T| = |S : S \cap T|$, eine p-Potenz $\neq 1$, denn $S \neq T$. Ein Widerspruch also zu $T \in \mathrm{Syl}_p(G)$. ∎

Besonders in Verbindung mit dem folgenden Lemma ist der 2. Sylow-Satz sehr nützlich.

Lemma 10.2 *Ist $|G| = p^r \cdot m$ mit $\mathrm{ggT}(p, m) = 1$, dann $n_p(G) \mid m$.*

Beweis. 3. Sylow-Satz: G operiert transitiv auf $\mathrm{Syl}_p(G)$. Sei $S \in \mathrm{Syl}_p(G)$: dann $S \leq \mathrm{Stab}_G(S)$, und $|Bahn_G(S)| = n_p(G)$. Also (Bahnengleichung und Lagrange) $n_p(G) = |G : \mathrm{Stab}_G(S)| \mid |G_S| = m$. ∎

Beispiel Jedes Gruppe der Ordnung 35 ist zyklisch.

Begründung: Es ist $35 = 5 \cdot 7$. Jedes $g \in G$ hat Ordnung 1, 5, 7 oder 35. Zu zeigen ist: es gibt g mit $o(g) = 35$. Nur e hat Ordnung 1. Hat g Ordnung 7, so ist $\langle g \rangle$ eine 7-Sylowgruppe. Lemma 10.2: $n_7(G) \mid 5$. Zweiter Sylow-Satz: $n_7 \in \{1, 8, 15, \ldots\}$. Also $n_7(G) = 1$, und es gibt nur 6 Elemente der Ordnung 7: die sechs Elemente $\neq e$ der einzigen 7-Sylowgruppe. Wegen $n_5 \mid 7$ und $n_5 \in \{1, 6, 11, \ldots\}$ gibt es analog nur 4 Elemente der Ordnung 5. Also gibt es Elemente mit Ordnung 35, daher ist G zyklisch.

Beispiel Ist K/k eine Galoiserweiterung mit Grad 3500, so gibt es genau einen Zwischenkörper $k \subseteq L \subseteq K$ mit $[L : k] = 28$. Ferner ist dieses L/k Galois.

Begründung: es ist $3500 = 5^3 \cdot 28$. Ist also S eine 5-Sylowgruppe von $G = \mathrm{Gal}(K/k)$, dann ist $|G : S| = 28$. Galoiskorrespondenz: mit $L := \mathrm{Fix}(S)$ ist $[L : k] = 28$. Umgekehrt gilt: ist $[L : k] = 28$, dann $L = \mathrm{Fix}(H)$ für $H \leq H$ mit $|H| = 5^3$, d.h. $H \in \mathrm{Syl}_5(G)$. Lemma 10.2: $n_5(G) \mid 28$; zweiter Sylow-Satz: $n_5 \in \{1, 6, 11, 16, \ldots\}$. Also $n_5(G) = 1$, daher sind S, L eindeutig. Ferner ist $S \lhd G$, denn jedes gSg^{-1} ist eine 5-Sylowgruppe und daher $= S$. Galoiskorrespondenz: L/k normal und daher Galois.

10.2 Mehr über p-Gruppen

Definition Das *Zentrum* $Z(G)$ einer Gruppe G ist die Teilmenge

$$Z(G) := \{g \in G \mid hg = gh \; \forall \, h \in G\} \, .$$

Lemma 10.3 *$Z(G) \lhd G$.*

Beweis. $e \in Z(G)$; $g, h \in Z(G) \;\Rightarrow\; gh^{-1} \in Z(G)$; $g \in Z(G)$, $h \in G \;\Rightarrow\; hgh^{-1} = g \in Z(G)$. ∎

Lemma 10.4 *Sei G eine nichttriviale p-Gruppe. Dann ist das Zentrum $Z(G)$ nicht trivial: $Z(G) > \{e\}$.*

Beweis. Es ist $|G| = p^n$ mit p prim und $n \geq 1$. Betrachten wir die Operation von G auf sich selbst durch Konjugation. Die Summe der Bahnlängen beträgt $|G| = p^n$ und ist durch p teilbar. Jede Bahnlänge teilt p^n wegen der Bahnengleichung, und ist daher entweder 1 oder durch p teilbar. Es folgt, dass die Anzahl der Bahnen, deren Länge 1 beträgt, durch p teilbar sein muss. Eine solche Bahn ist $\{e\}$. Somit gibt es mindestens $p \geq 2$ solche Bahnen. Aber $g \in Z(G)$ genau dann, wenn $\{g\}$ eine Bahn ist. ∎

Lemma 10.5 *Sei G eine nichttriviale p-Gruppe. Dann gibt es $H \lhd G$ mit $|G : H| = p$.*

Beweis. Induktion über $|G|$, für $|G| = p$ ist $H = \{e\}$. Ist $|G| \geq p^2$, dann $Z(G) > \{e\}$, also (Cauchy) $\exists g \in Z(G) \;\; o(g) = p$. Dann $\langle g \rangle \lhd G$, und mit $Q = G/\langle g \rangle$ ist $|Q| = |G|/p \geq p$. Induktionsannahme: $\exists K \lhd Q \;\; |Q : K| = p$. Fertig mit $H = \{h \in G \mid h\langle g \rangle \in K\}$. ∎

Korollar 10.6 *Sei p eine Primzahl und G eine Gruppe der Ordnung $p^r \cdot m$. Dann Für jedes $0 \leq s \leq r$ gibt es mindestens eine Untergruppe $P \leq G$ mit $|P| = p^s$.*

Beweis. 1. Sylow-Satz: OBdA ist $|G| = p^r$. Mit $P = \{e\}$ und $P = G$ werden die Ordnungen p^0, p^r angenommen. Der Rest folgt per Induktion über r, wegen Lemma 10.5. ∎

Beispiel Ist K/k Galois mit Grad 3500, so gibt es Zwischenkörper L mit $|L:k| = 140$ und mit $|L:k| = 700$, da es Untergruppen P mit $|P| = 5$ und mit $|P| = 25$ gibt.

10.3 Der Fundamentalsatz der Algebra

Die Galois-Theorie liefert einen Alternativ-Beweis dafür, dass $\mathbb{C}$ algebraisch abgeschlossen ist, der nur ein wenig Analysis benutzt. Zwar haben wir häufig genug diese bekannte Tatsache benutzt: sie ging aber nicht im Beweis der Galois-Korrespondenz ein, und wir haben außerdem gesehen, dass jeder Körper – also auch $\mathbb{C}$ – einen algebraischen Abschluss hat.

Fundamentalsatz der Algebra $\mathbb{C}$ *ist algebraisch abgeschlossen.*

Bemerkung Wir benutzen nur zwei Tatsachen aus der Analysis:

- Ist $f \in \mathbb{R}[X]$ mit $\operatorname{grad}(f)$ ungerade, dann hat f eine reelle Nullstelle.
- Für jedes $z \in \mathbb{C}$ hat $X^2 - z$ eine Nullstelle in $\mathbb{C}$: ist $z = re^{i\theta}$, so ist $\sqrt{r}e^{i\frac{\theta}{2}}$ eine.

Beweis. Angenommen nicht. Sei K ein algebraischer Abschluss von $\mathbb{C}$, und sei $\alpha \in K \setminus \mathbb{C}$. Dann ist α algebraisch über $\mathbb{C}$ und daher auch über $\mathbb{R}$. Sei $L \subseteq K$ der Zerfällungskörper über $\mathbb{R}$ des Minimalpolynoms von α in $\mathbb{R}[X]$. Sei $S \leq G := \operatorname{Gal}(L/\mathbb{R})$ eine 2-Sylowgruppe, und sei $M = \operatorname{Fix}(S)$. Dann $[M:\mathbb{R}] = |G:S|$ ist ungerade. Satz vom primitiven Element: es gibt $\beta \in M$ mit $M = \mathbb{R}(\beta)$. Dann für $m_\beta \in \mathbb{R}[X]$ ist $\operatorname{grad} m_\beta = [M:\mathbb{R}]$, ungerade. Analysis: m_β hat eine Nullstelle in $\mathbb{R}$. Also $m_\beta = X - \beta$, denn irreduzibel mit Nullstelle. Also $M = \mathbb{R}$, $[L:\mathbb{R}]$ ist eine Zweierpotenz, und G ist eine 2-Gruppe.

Wegen $\alpha \notin \mathbb{R}$ ist $2 \mid |G|$. Jede p-Gruppe hat einen Normalteiler mit Index p, also gibt es $N \lhd G$ mit $|G:N| = 2$. Daher $\operatorname{Fix}(N)/\mathbb{R}$ ist normal mit Grad 2, d.h. der Zerfällungskörper von einem irreduziblen Grad 2 Polynom aus $\mathbb{R}[X]$. Quadratische Ergänzung: es ist $\operatorname{Fix}(N) = \mathbb{C}$. Also $\mathbb{C} \subseteq L$, und $L/\mathbb{C}$ ist Galois mit Galoisgruppe N. Wegen $\alpha \notin \mathbb{C} = \operatorname{Fix}(N)$ ist auch N eine nichttriviale 2-Gruppe. Daher gibt es $R \lhd N$ mit Index 2, dann ist $\operatorname{Fix}(R)/\mathbb{C}$ normal vom Grad 2, daher Zerfällungskörper eines irreduziblen Grad 2 Polynoms aus $\mathbb{C}[X]$. Quadratische Ergänzung: ein solches Polynom gibt es nicht, Widerspruch. ∎

11 Zyklische Erweiterungen und weitere Themen

11.1 Zyklische Erweiterungen

Bezeichnung Eine Körpererweiterung K/k heißt *zyklisch*, wenn sie Galois mit zyklischer Galoisgruppe ist.

Beispiel Also ist jede zyklische Erweiterung abelsch; $\mathbb{Q}(\zeta_{12})/\mathbb{Q}$ ist abelsch aber nicht zyklisch; $\mathbb{F}_q/\mathbb{F}_p$ ist zyklisch für jedes $q = p^m$.

Lemma 11.1 *Sei p eine Primzahl, $k \subseteq \mathbb{C}$ ein Körper mit $\zeta_p \in k$, und K/k eine zyklische Erweiterung vom Grad p. Dann gibt es ein $D \in k$ mit $K = k(\sqrt[p]{D})$.*

Beweis. Sei $\zeta = \zeta_p$. Wähle σ mit $\mathrm{Gal}(K/k) = \langle\sigma\rangle$. Für $\alpha \in K$ definiert man die *Lagrange-Resolvente* $R(\alpha)$ durch[6]

$$R(\alpha) = \sum_{r=0}^{p-1} \zeta^r \sigma^r(\alpha)\,.$$

Wegen Lemma 8.1 sind die σ^r linear unabhängig über K, wir können also α mit $R(\alpha) \neq 0$ wählen. Wegen $\zeta \in k$ ist $\sigma(\zeta) = \zeta$ und daher $\sigma(R(\alpha)) = \zeta^{-1}R(\alpha)$, weshalb $D := R(\alpha)^p \in \mathrm{Fix}(\sigma) = k$. Ferner ist $K = k(\beta)$ für $\beta = R(\alpha) = \sqrt[p]{D}$, denn $[K : k]$ ist prim und $\beta \notin k$ wegen $\sigma(\beta) = \zeta^{-1}\beta \neq \beta$. ∎

11.2 Kompositionsreihen

Definition Eine Normalreihe $1 = G_0 \leq G_1 \leq \cdots \leq G_n = G$ heißt eine *Kompositionsreihe* von G, falls jede Faktorgruppe G_r/G_{r-1} einfach ist.

Beispiel $1 \leq A_3 \leq S_3$ ist sowohl eine Kompositionsreihe als auch eine auflösbare Reihe von S_3. Die einzige Kompositionsreihe von A_5 ist $1 \leq A_5$. Eine Kompositionsreihe von S_5 ist $1 \leq A_5 \leq S_5$.

Hilfssatz Ist G abelsch und einfach, dann $G \cong C_p$ für eine Primzahl p.

Beweis. Sei $e \neq g \in G$, dann $\langle g\rangle = G$, da ein Normalteiler. Also $G \cong \mathbb{Z}$, oder $G \cong C_n$ für ein $n \geq 2$. Wegen $2\mathbb{Z} \lneq \mathbb{Z}$ ist $\mathbb{Z}$ nicht einfach. Ist $G = C_n$ mit n keine Primzahl, dann sei p eine Primzahl mit $p \mid n$. Dann $\langle g^p\rangle \lneq G$, ein Widerspruch. ∎

Lemma 11.2 *Jede endliche Gruppe G hat eine Kompositionsreihe. Mehr noch: jede Normalreihe von G lässt sich zu einer Kompositionsreihe verfeinern.*

[6] Der Name ist standard, die Bezeichnung ist meine.

Beweis. Jede Gruppe hat die Normalreihe $\{e\} \leq G$. Induktion über $|G|$, klar für G einfach, also insbesondere für $|G| = p$, eine Primzahl. Nun sei $1 = G_0 \leq \cdots \leq G_n = G$ eine Normalreihe. OBdA keine Wiederholungen. Ist $n = 1$, dann fertig falls G einfach; und wenn nicht, dann füge ein $H \lhd G$ dazwischen: $1 \leq H \leq G$, mit $H \notin \{1, G\}$. Ab jetzt ist $n \geq 2$, und keine Wiederholungen. Nach Induktionsannahme hat jedes G_r/G_{r-1} eine Kompositionsreihe $1 = Q_0 \leq Q_1 \leq \cdots \leq Q_s = G_r/G_{r-1}$. Sei $G_{r-1} \leq H_i \leq G_r$ die Gruppe mit $H_i/G_{r-1} = Q_i$, dann $H_i/H_{i-1} \cong Q_i/Q_{i-1}$, daher ist jede Faktorgruppe in der Teil-Normalreihe $G_{r-1} = H_0 \leq H_1 \leq \cdots \leq H_s = G_r$ einfach. Fertig, nachdem man alle diese Teril-Verfeinerungen zusammengesteckt hat. ∎

Korollar 11.3 *Jede auflösbare endliche Gruppe hat eine Normalreihe, die sowohl auflösbar als auch eine Kompositionsreihe ist.*

Beweis. Man verfeinere eine auflösbare Reihe. ∎

11.3 Zusammengesetzte Erweiterungen

Definition Seien L, M zwei Zwischenkörper der Erweiterung K/k. Mit LM bezeichnet man den kleinsten Zwischenkörper, der L und M erhält. Es ist also $LM = L(M) = M(L)$.

Lemma 11.4 *a) Ist L/k normal bzw. separabel bzw. Galois, dann LM/M auch.*

b) Sind $L/k, M/k$ beide normal bzw. separabel bzw. Galois, dann LM/k auch.

c) Ist L/k Galois, dann $[LM : M] = [L : L \cap M]$ und $\mathrm{Gal}(LM/M) \cong \mathrm{Gal}(L/L \cap M)$.

Beweis. a) Ist $L = k(\alpha_1, \ldots, \alpha_r)$, dann $LM = M(\alpha_1, \ldots, \alpha_r)$. Also klar.

b) Ist $L = k(\alpha_1, \ldots, \alpha_r)$ und $M = k(\beta_1, \ldots, \beta_s)$, dann $LM = k(\alpha_i, \beta_j)$. Also klar.

c) Für $\sigma \in \mathrm{Gal}(LM/M)$ ist $\sigma(L) = L$, da L/k normal. Sei $\phi\colon \mathrm{Gal}(LM/M) \to \mathrm{Gal}(L/k)$ die Einschränkungsabbildung $\phi(\sigma) = \sigma|_L$. Ist $\sigma|_L = \mathrm{Id}$, dann ist $\sigma = \mathrm{Id}$, denn auch $\sigma|_M = \mathrm{Id}$. Also ϕ ist injektiv. Sei $H = \mathrm{Bild}(\phi) \leq \mathrm{Gal}(L/k)$.

Einerseits ist $L \cap M \subseteq \mathrm{Fix}(H)$, denn jedes $\tau \in H$ ist $\tau = \sigma|_H$ für ein $\sigma \in \mathrm{Gal}(LM/M)$. Andererseits: Ist $\beta \in L \setminus L \cap M$, dann gibt es $\sigma \in \mathrm{Gal}(LM/M)$ mit $\sigma(\beta) \neq \beta$, also $\tau(\beta) \neq \beta$ für $\tau = \sigma|_L \in H$. Also $\mathrm{Fix}\, H = L \cap M$, weshalb ϕ ein Isomorphismus ist zwischen $\mathrm{Gal}(LM/M)$ und $\mathrm{Gal}(L/L \cap M)$. ∎

11.4 Lösbarkeit durch Radikale wieder

Satz 11.5 *Sei $f \in \mathbb{Q}[X]$ ein Polynom. Genau dann ist f durch Radikale lösbar, wenn seine Galoisgruppe G auflösbar ist.*

Beweis. Gemeint ist, dass jede Nullstelle von f sich durch Radikale ausdrücken lässt. Dass G auflösbar sein muss, sahen wir in Korollar 9.5. Sei also G auflösbar und $1 = G_0 \leq \cdots \leq G_n = G$ eine auflösbare Kompositionsreihe (Korollar 11.3). Sei $L_r = \mathrm{Fix}(G_r)$, also $\mathbb{Q} = L_n \subseteq \cdots \subseteq L_0 = L$, für L der Zerfällungskörper von f. Sei $k = \mathbb{Q}(\zeta_{|G|})$, und sei $K_r = L_r k$: also $k = K_n \subseteq \cdots K_0 = K$, und $L \subseteq K$, $L_r \subseteq K_r$. Bekanntlich ist $k/\mathbb{Q}$ Galois.

Es ist $K_r = kL_r$, daher K_r/L_r Galois. Wegen der Normalreihe ist L_{r-1}/L_r Galois. Es ist $K_{r-1} = K_r L_{r-1}$. Nach Lemma 11.4 ist also K_{r-1}/K_r Galois und

$$[K_{r-1} : K_r] = [K_r L_{r-1} : K_r] = [L_{r-1} : L_{r-1} \cap K_r] \,.$$

Wegen $L_r \subseteq K_r \cap L_{r-1}$ ist daher $[K_{r-1} : K_r]$ ein Teiler von der Primzahl $[L_{r-1} : L_r]$. Nach Lemma 11.1 lässt sich jedes Element von K durch Radikale ausdrücken. ∎

Beispiel Jedes Polynom $f \in \mathbb{Q}[X]$ vom Grad 4 ist durch Radikale lösbar.

Denn die Galoisgruppe ist eine Untergruppe von S_4, und daher auflösbar, denn S_4 ist auflösbar:

$$1 \leq V \leq A_4 \leq S_4 \,,$$

wobei $V \cong C_2 \times C_2$ besteht aus Id und allen 3 Permutationen vom Typ 2^2.

Anmerkung: Einheitswurzeln Im Beweis von Satz 11.5 brauchen wir eigentlich nur ζ_p für jede Primzahl p, die $|\mathrm{Gal}(f)|$ teilt. Insbesondere können wir $f = \Phi_d$ lösen, mit Radikalen und mit den ζ_p für Primzahlen p mit $p \mid \phi(d) < d$: denn $\mathbb{Q}(\zeta_d)/\mathbb{Q}$ ist abelsch, daher auflösbar. Per Induktion können wir die Sonderrolle der Einheitswurzeln also beseitigen. Die Induktion fängt an mit $\zeta_1 = 1$ und $\zeta_2 = -1$, beide $\in \mathbb{Q}$.

11.5 Der Satz von Jordan–Hölder

Satz 11.6 (Jordan–Hölder) *Sei G eine endliche Gruppe. Die Länge der Kompositionsreihe ist eindeutig bestimmt; bis auf die Reihenfolge sind auch die Faktorgruppen eindeutig bestimmt.*

Beweis. Induktion über G. Klar für $G = 1$, und für G einfach. Nun sei $1 = G_0 \leq G_1 \leq \cdots \leq G_n = G$ eine Kompositionsreihe für G, und sei $N \lhd G$ ein Normalteiler mit G/N einfach. Sei $r = \min\{s \mid G_s \not\leq N\}$. Nun, ist $G_{s+1}N = G$ und $G_s \lhd G_{s+1}$, dann $N \leq G_s N \lhd G$, weshalb entweder $G_s N = N$ und $G_s \leq N$,

oder $G_sN = G$. Es ist daher $G_sN = G$ für jedes $s \geq r$, und $G_s \leq N$ für jedes $s \leq r-1$.

Wegen G_r/G_{r-1} einfach und $G_{r-1} \leq N \cap G_r \lhd G_r$ ist $N \cap G_r = G_{r-1}$. Also $G_r/G_{r-1} = G_r/(N \cap G_r) \cong G_rN/N = G/N$.

Für $s \geq r$ ist $G_s/(N \cap G_s) \cong G_sN/N = G/N$. Ferner ist $G_s(N \cap G_{s+1})/(N \cap G_{s+1}) \cong G_s/(N \cap G_s) \cong G/N$, also $G_{s+1} = G_s(N \cap G_{s+1})$, und daher $G_{s+1}/G_s \cong G_s(N \cap G_{s+1})/G_s \cong (N \cap G_{s+1})/(N \cap G_s)$. Also ist $G_r/G_{r-1} \cong G/N$, und

$$1 = G_0 \leq \cdot \leq G_{r-1} = N \cap G_r \leq N \cap G_{r+1} \leq N \cap G_n = N$$

eine Kompositionsreihe von N mit den Faktorgruppen $G_1/G_0, \ldots, G_{r-1}/G_{r-1}$, $G_{r+1}/G_r, \ldots, G_n/G_{n-1}$. Fertig nach Induktion über n. ∎

11.6 Die Diskriminante

Sei k ein Körper mit $\mathrm{char}(k) \neq 2$. Sei $f \in k[X]$ ein Polynom ohne wiederholte Nullstellen (und daher separabel). Sei K der Zerfällungskörper von f über k, und seien $\alpha_1, \ldots, \alpha_n$ die Nullstellen von f – also $n = \mathrm{grad}(f)$.

Bezeichnung Wir setzen

$$\Delta = \prod_{i<j} (\alpha_j - \alpha_i) \qquad\qquad D = \Delta^2 .$$

Man nennt D die *Diskriminante* des Polynoms f.

K/k ist Galois, da Zerfällungskörper eines separablen Polynoms. Es ist $K = k(\alpha_1, \ldots, \alpha_n)$ und jedes $\sigma \in G := \mathrm{Gal}(f)$ permutiert die α_i, daher dürfen wir G als eine Untergruppe von S_n betrachten.

Lemma 11.7 *a) Für jedes $\sigma \in G$ ist $\sigma(\Delta) = \varepsilon(\sigma)\Delta$. Das heißt,*

$$\sigma(\Delta) = \begin{cases} \Delta & \sigma \text{ gerade} \\ -\Delta & \sigma \text{ ungerade} \end{cases} .$$

b) $D \in k$.

c) $G \leq A_n \Leftrightarrow \sqrt{D}$ existiert in k.

Beweis. a) Folgt unmittelbar aus der Definition der Signatur $\varepsilon(\sigma)$. b) Folgt aus a) und der Galoiskorrespondenz. c) Folgt aus a) und b). ∎

Eigentlich zeigt Lemma 11.7 c) einen Weg, zu prüfen ob $G \leq A_n$ ist. Allerdings ist die Berechnung der Diskriminante D langwierig.

Lemma 11.8 *Für beliebiges $p, q \in k$ hat das kubische Polynom $X^3 - pX + q \in k[X]$ Diskriminante $D = 4p^3 - 27q^2$.*

Siehe den Anhang §A.5 für den Beweis dieses Lemmas.

Beispiel Wir haben schon gesehen, dass $f = X^3 - 3X + 1 \in \mathbb{Q}[X]$ irreduzibel mit Galoisgruppe A_3 ist. Dementsprechend ist die Diskriminante $D = 4 \cdot 3^3 - 27 \cdot 1^2 = 81 = 9^2$. Also $\Delta = \pm 9 \in \mathbb{Q}$.

Beispiel $f = X^3 - 12X + 3 \in \mathbb{Q}[X]$ ist irreduzibel (Eisenstein, Gauß), daher $3 \mid |\mathrm{Gal}(g)|$, also $A_3 \leq \mathrm{Gal}(f)$. Die Diskriminante ist $D = 4 \cdot 12^3 - 27 \cdot 3^2 = 3^3(4^4 - 3^2) = 3^3 m$ mit $\mathrm{ggT}(m, 3) = 1$. Also $\Delta = \sqrt{D} \notin \mathbb{Q}$, daher $\mathrm{Gal}(f) \not\leq A_3$, daher $\mathrm{Gal}(f) = S_3$.

Prüfen wir jetzt die reellen Nullstellen von f: es ist $f' = 3(X^2 - 4)$, daher $f'(\pm 2) = 0$. Es ist $f'' = 6X$, also lokales Minimum in $X = 2$, lokales Maximum in $X = -2$. Es ist $f(-2) = -8 + 24 + 3 > 0$, $f(2) = 8 - 24 + 3 < 0$, daher sind alle drei Nullstellen reell.

Dies ist unser erstes Beispiel eines kubischen Polynoms, das sowohl lauter reelle Nullstellen hat, als auch Galoisgruppe S_3.

A Anhang

A.1 Die Signatur ist ein Gruppenhomomorphismus

Definition Sei $\sigma \in S_n$. Die Signatur $\varepsilon(\sigma)$ wird durch $\varepsilon(\sigma) = (-1)^m$ definiert, wobei m die Anzahl der Paare i, j ist, die $1 \leq i < j \leq n$ und $\sigma(i) > \sigma(j)$ erfüllen.

Lemma A.1 *Die Signatur ist ein Gruppenhomomorphismus* $\varepsilon\colon S_n \to \{+1, -1\}$*, eine Gruppe bzgl. Multiplikation.*

Beweis. Es ist

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}\,,$$

denn für $i < j$ gilt

$$\frac{\sigma(j) - \sigma(i)}{j - i} = \begin{cases} +1 & \text{falls } \sigma(j) > \sigma(i); \\ -1 & \text{falls } \sigma(j) < \sigma(i); \end{cases}$$

Nun, $\frac{\sigma(j)-\sigma(i)}{j-i} = \frac{\sigma(i)-\sigma(j)}{i-j}$. Also $\varepsilon(\sigma)$ ist

- das Produkt über alle 2-elementige Teilmengen $\{i, j\} \subseteq \{1, 2, \ldots, n\}$
- des gemeinsamen Werts $\frac{\sigma(j)-\sigma(i)}{j-i} = \frac{\sigma(i)-\sigma(j)}{i-j}$.

Ist also $\pi \in S_n$ eine beliebige Permutation, dann ist

$$\prod_{1 \leq i < j \leq n} \frac{\sigma(\pi(j)) - \sigma(\pi(i))}{\pi(j) - \pi(i)} = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}\,,$$

denn auf der linken Seite werden die 2-elementigen Teilmengen einfach in einer anderen Reihenfolge durchgearbeitet. Somit ist

$$\begin{aligned} \varepsilon(\sigma\pi) &= \prod_{1 \leq i < j \leq n} \frac{\sigma(\pi(j)) - \sigma(\pi(i))}{j - i} \\ &= \left(\prod_{1 \leq i < j \leq n} \frac{\sigma(\pi(j)) - \sigma(\pi(i))}{\pi(j) - \pi(i)} \right) \left(\prod_{1 \leq i < j \leq n} \frac{\pi(j) - \pi(i)}{j - i} \right) \\ &= \varepsilon(\sigma)\varepsilon(\pi)\,. \end{aligned}$$

∎

A.2 Polynome in beliebig vielen Unbestimmten

Sei $(X_i)_{i\in I}$ eine beliebige Familie von Unbestimmten. Ein *Monom* in $(X_i)_{i\in I}$ ist ein Ausdruck der Art $X_{i_1}^{e_1}\cdots X_{i_n}^{e_n}$ mit $n \geq 0$, $\{i_1,\ldots,i_n\} \subseteq I$ und $e_1,\ldots,e_n \in \mathbb{N}_0$. Etwas genauer: ein Monom ist ein Produkt $\prod_{i\in I} X_i^{e_i}$, wobei $e_i \in \mathbb{N}_0$, und nur für endlich viele $i \in I$ ist $e_i > 0$. Ein Polynom in diesen Unbestimmten ist eine R-lineare Kombination von Unbestimmten, daher kommen in einem Polynom nur endlich viele Unbestimmten vor. Zwei Polynome sind genau dann gleich, wenn sie in jedem Monom den gleichen Koeffizienten haben. Monome werden multipliziert durch

$$\left(\prod_{i\in I} X_i^{d_i}\right)\cdot\left(\prod_{i\in I} X_i^{e_i}\right) = \prod_{i\in I} X_i^{d_i+e_i}\,,$$

und Polynome werden wie üblich mittels des Distributivgesetzes multipliziert. So bilden die Polynome in $(X_i)_{i\in I}$ mit Koeffizienten im kommutativen Ring R einen Ring, den Polynomring $R[X_i \mid i \in I]$. Das Einselement ist das Monom mit $e_i = 0$ für alle i. Ist $(r_i)_{i\in I}$ eine durch I indizierte Familie von Elementen aus R, so gibt es genau einen R-linearen Ringhomomorphismus $f\colon R[X_i \mid i \in I] \to R$ mit $f(x_i) = r_i$ für alle i.

A.3 Die Quaternionen

Die Quaternionen $\mathbb{H}$ sind ein Schiefkörper, d.h. wie ein Körper, aber nicht kommutativ. Man kann $\mathbb{H}$ als ein 4-dimensionaler $\mathbb{R}$-Vektorraum mit Basis $1, i, j, k$ auffassen, wobei die Multiplikation $\mathbb{R}$-bilinear ist, d.h. linear in beiden Argumenten; $i^2 = j^2 = k^2 = -1$; $ij = k$, $jk = i$, $ki = j$; und $ji = -k$, $kj = -i$, $ik = -j$.

Für die Assoziativität der Multiplikation ist es aber besser $\mathbb{H}$ als den 2-dimensionalen $\mathbb{C}$-Vektorraum aller Matrizen der Art $\begin{pmatrix} z & w \\ -\bar{w} & \bar{z}\end{pmatrix}$ zu betrachten, mit der für Matrizen üblichen Addition und Multiplikation. Übersetzung:

$$1 \leftrightarrow \begin{pmatrix}1&0\\0&1\end{pmatrix} \qquad i \leftrightarrow \begin{pmatrix}i&0\\0&-i\end{pmatrix} \qquad j \leftrightarrow \begin{pmatrix}0&1\\-1&0\end{pmatrix} \qquad k \leftrightarrow \begin{pmatrix}0&i\\i&0\end{pmatrix}.$$

Dies kann man auch schreiben als $\mathbb{H} = \{z + \omega j \mid z, \omega \in \mathbb{C}\}$, wobei $j^2 = -1$ und $jz = \bar{z}j$. Die Quaternionen bilden einen nichtkommutativen Ring mit $1 \neq 0$.

Die invertierbaren Quaternionen $\mathbb{H}^* = \mathbb{H}\setminus\{0\}$ bilden eine nichtabelsche Gruppe bezüglich Multiplikation. Es ist

$$\frac{1}{a+bi+cj+dk} = \frac{a-bi-cj-dk}{a^2+b^2+c^2+d^2}\,.$$

Die Teilmenge $\{\pm 1, \pm i, \pm j, \pm k\}$ ist eine achtelementige Untergruppe, die man die Quaternionengruppe Q_8 nennt. Sie hat die gleiche Anzahl von Elementen wie D_4, beide Gruppen sind nichtabelsch, aber trotzdem sind sie nicht isomorph.

A.4 Das Zornsche Lemma

Gegen Ende von Kapitel 3 wurde das Zornsche Lemma ohne Beweis aufgeführt. Den Beweis liefern wir jetzt nach. Das Zornsche Lemma ist die folgende Aussage:

Das Zornsche Lemma *Sei $(X, \leq)$ eine teilweise geordnete nichtleere Menge. Hat jede nichtleere Kette in X eine obere Schranke, so enthält X ein maximales Element.*

Zuerst wiederholen wir aber die Begriffserklärungen.

Definition Eine Relation $\leq$ auf einer Menge X heißt eine *Teilordnung*, wenn sie reflexiv, transitiv und antisymmetrisch ist. Das letztere heißt, dass

$$(x \leq y) \wedge (y \leq x) \Longrightarrow x = y\,.$$

Sie heißt eine *Ordnung*, wenn x, y vergleichbar sind für alle $x, y \in X$, d.h. wenn mindestens eins aus $x \leq y$, $y \leq x$ gilt.

Ein Element $x \in X$ heißt *maximal*, falls aus $y \geq x$ immer $y = x$ folgt.

Sei $\leq$ eine Teilordnung auf X. Eine *Kette* ist eine Teilmenge $K \leq X$ derart, dass die Einschränkung von $\leq$ eine Ordnung auf K ist. Ist $x \in X$ derart, dass $x \geq y$ für alle $y \in K$, so heißt x eine *obere Schranke* der Kette K.

Beweis des Zornschen Lemmas. Ist $(X, \leq)$ ein Gegenbeispiel, dann gibt es zu jedem $x \in X$ ein $y \in X$ mit $x < y$. Sei $K \subseteq X$ eine Kette und $x_0 \in X$ eine obere Schranke für K. Sei $y \in X$ mit $y > x_0$. Dann ist y eine echte obere Schranke für K, d.h. $x < y$ für alle $x \in K$. Nach dem Auswahlaxiom gibt es eine Abbildung $u\colon \{K \subseteq X \mid K \text{ Kette}\} \to X$ derart, dass $u(K)$ eine echte obere Schranke für K ist für jede Kette K. Wir verwenden u, um eine Kette ohne obere Schranke zu konstruieren: ein Widerspruch.

Nennen wir eine Teilmenge $A \subseteq K$ ein Anfangsstück von K, falls für alle $x \in A$ und $y \in K$ mit $y \leq x$ gilt $y \in A$. Eine Kette nennen wir ausgezeichnet, falls für jedes Anfangsstück $A \neq K$ auch $A \cup \{u(A)\}$ ein Anfangsstück von K ist. Somit sind u.a. $\emptyset$, $\{u(\emptyset)\}$ und $\{u(\emptyset), u(\{u(\emptyset)\})\}$ ausgezeichnete Ketten.

Lemma A.2 *Sei K eine Kette in X.*

a) Sei C ein Anfangsstück von K. Dann jedes Anfangsstück A von C ist gleichzeitig ein Anfangsstück von K.

b) Jedes Anfangsstück $C \subseteq K$ ist eine ausgezeichnete Kette.

c) Eine beliebige Vereinigung von Anfangsstücken von K ist ein Anfangsstück von K.

Beweis. a) Sei $x \in A$ und $y \in K$ mit $y \leq x$. Wegen $A \subseteq C$ gilt $x \in C$. Da $C \subseteq K$ ein Anfangsstück ist, folgt $y \in C$. Da $A \subseteq C$ ein Anfangsstück ist, folgt jetzt $y \in A$.

b) Sei $A \subsetneq C$ ein echtes Anfangsstück. Dann ist A auch ein echtes Anfangsstück von K. Da K ausgezeichnet ist, ist $A' := A \cup \{u(A)\}$ ein Anfangsstück von K. Wegen $A \subsetneq C$ gibt es ein $y \in C \setminus A$. Ist $u(A) \leq y$, dann $u(A) \in C$, da $C \subseteq K$ ein Anfangsstück. Ist $y < u(A)$, dann $y \in A$, denn A' ist ein Anfangsstück von K. Dies ist ein Widerspruch. Somit liegen $u(A)$ und A' in C. Nun sei $x \in A'$ und $z \in C$ mit $z \leq x$. Dann $z \in A'$, denn A' ist ein Anfangsstück von K.

c) Sei $(C_i)_{i \in I}$ eine Familie von Anfangsstücken von K, sei $x \in \bigcup_{i \in I} C_i$, und sei $y \in K$ mit $y \leq x$. Dann gibt es ein $j \in I$ mit $x \in C_j$. Da C_j ein Anfangsstück ist, und $y \leq x$ gilt, liegt $y \in C_j$, weshalb $y \in \bigcup_{i \in I} C_i$. ∎

Lemma A.3 *Sind A, B zwei ausgezeichnete Ketten in X, so ist A ein Anfangsstück von B – oder umgekehrt.*

Beweis. Sei $C = \bigcup\{D \subseteq X \mid D \text{ ein Anfangsstück von } A \text{ und von } B\}$. Nach Lemma A.2 ist C selbst ein Anfangsstück von A und von B. Liegt $u(C)$ in $A \cap B$, so ist $C \cup \{u(C)\}$ ein Anfangsstück der beiden ausgezeichneten Ketten A, B, ein Widerspruch zur Definition von C. Ist $u(C) \notin A$, dann $A = C$, denn A ist ausgezeichnet. In diesem Fall ist dann $A = C \subseteq B$. Ist umgekehrt $u(C) \notin B$, dann $B = C \subseteq A$. ∎

Lemma A.4 *Eine beliebige Vereinigung von ausgezeichneten Ketten in X ist eine ausgezeichnete Kette in X.*

Beweis. Sei $(K_i)_{i \in I}$ eine solche Familie, und sei K die Vereinigung $K = \bigcup_{i \in I} K_i$. Wegen Lemma A.3 ist K eine Kette, denn sind $x, y \in K$ dann $\exists i, j \in I$ mit $a \in K_i$, $b \in K_j$. Dann ist $K' := K_i \cup K_j$ eins aus K_i, K_j und deshalb eine Kette. Also x, y sind vergleichbar.

Außerdem ist jedes K_i ein Anfangsstück von K: denn ist $x \in K_i$ und $y \in K$ mit $y \leq x$, dann gibt es ein $j \in I$ mit $y \in K_j$. Wegen Lemma A.3 gilt: entweder ist K_j ein Anfangsstück von K_i, oder K_i ist ein Anfangsstück von K_j. In beiden Fällen folgt: $y \in K_i$.

Sei also $C \subsetneq K$ ein echtes Anfangsstück. Da C echt ist, gibt es ein $z \in K \setminus C$. Dann gibt es ein $j \in I$ mit $z \in K_j$. Wie gerade gesehen, ist K_j ein Anfangsstück der Kette K. Ist $x \in C$, dann $x < z$: sonst wäre $z \in C$, denn C ist ein Anfangsstück von K. Somit gilt $C \subsetneq K_j$, denn K_j ist auch ein Anfangsstück von K. Da K_j ausgezeichnet ist, ist $C' := C \cup \{u(C)\}$ ein weiteres Anfangsstück von K_j. Nach Lemma A.2 ist C' auch ein Anfangsstück von K. Somit ist K ausgezeichnet. ∎

Jetzt können wir den Beweis des Zornschen Lemmas abschließen. Sei K die Vereinigung *aller* ausgezeichneten Ketten in X. Nach Lemma A.4 ist K selbst eine ausgezeichnete Kette in X. Dann ist aber auch $K \cup \{u(K)\}$ eine ausgezeichnete Kette, was der Konstruktion von K widerspricht. ∎

A.5 Die Diskriminante eines kubischen Polynoms

Lemma 11.8 *Seien p, q beliebig. Dann: das Polynom $f = X^3 - pX + q$ hat Diskriminante $4p^3 - 27q^2$.*

Beweis. Seien α, β, γ die Nullstellen von f. Dann $f = (X-\alpha)(X-\beta)(X-\gamma)$, also gilt – wie bekannt –

$$\alpha + \beta + \gamma = 0 \qquad \alpha\beta + \beta\gamma + \gamma\alpha = -p \qquad \alpha\beta\gamma = -q\,.$$

Wir substituieren also $\gamma = -\alpha - \beta$ und erhalten

$$p = \alpha^2 + \alpha\beta + \beta^2 \qquad q = \alpha^2\beta + \alpha\beta^2\,.$$

Nun, es ist

$$\begin{aligned}\Delta &= (\beta - \alpha)(\gamma - \beta)(\alpha - \gamma)\\ &= (\alpha - \beta)(\alpha + 2\beta)(2\alpha + \beta)\\ &= (\alpha - \beta)(2p + 3\alpha\beta)\,.\end{aligned}$$

Nun, $(\alpha - \beta)^2 = p - 3\alpha\beta$, und daher

$$\begin{aligned}D = \Delta^2 &= (p - 3\alpha\beta)(4p^2 + 12p\alpha\beta + 9\alpha^2\beta^2)\\ &= 4p^3 - 27p\alpha^2\beta^2 - 27\alpha^3\beta^3\\ &= 4p^3 - 27q^2\,,\end{aligned}$$

denn $q^2 = \alpha^2\beta^2 p + \alpha^3\beta^3$. ∎

Bemerkung Multipliziert man aus, so erhält man

$$\Delta = 2\alpha^3 + 3\alpha^2\beta - 3\alpha\beta^2 - 2\beta^3\,.$$