ALGEBRA I – GALOIS-THEORIE

OLAF M. SCHNÜRER

Inhaltsverzeichnis

Einleitung

Algebra bedeutet „Rechnen mit Gleichungen“.

Date: 17. Dezember 2018.

Skript zur Vorlesung „Algebra I – Galois-Theorie im Sommersemester 2012 an der Universität Bonn.

Lösung algebraischer Gleichungen. Gegeben: Eine Gleichung

$$x^n + a_{n-1}x^{n-1} + \dots a_1 x + a_0 = 0 \tag{0.1}$$

mit Koefizienten $a_i \in \mathbb{Q}$. Eine solche Gleichung heißt **algebraische Gleichung vom Grad** n. (Könnte andere Koeffizienten zulassen, rationale/reelle/komplexe Zahlen, in endlichem Körper.)

Gesucht: Lösungen dieser Gleichung.

Was ist eine Lösung? Wo liegen Lösungen? (heute klar, historisch war es ein weiter Weg)

(a) Grad 1: Lineare Algebra: $x = -a_0$.

(b) Grad 2:

$$x = -\frac{a_1}{2} \pm \sqrt{\frac{a_1^2}{4} - a_0} \tag{0.2}$$

(Pausenaufgabe.) Im wesentlichen den Babyloniern bekannt (ab ca. Ende 3. Jahrtausend v. Chr.), geometrische Methoden. Verbessert durch griechische und arabische Mathematiker. Obige Formel erst Beginn des 16. Jahrhunderts: negative Zahlen als Lösung akzeptiert, Wurzelzeichen.

(c) Grad 3 und 4: Explizite Formeln, die wir kennenlernen werden. Scipione del Ferro, Tartaglia, Lodovico Ferrari, Gerolamo Cardano, veröffentlicht 1545. (erst Geheimwissen: gelehrte Wettkämpfe, entscheiden über Berufungen und Gehalt).

(d) Fundamentalsatz der Algebra (d'Alembert 1746, Euler 1749. Lagrange 1772, Gauß 1799 (Doktorarbeit)): Jedes nichtkonstante Polynom n-ten Grades in $\mathbb{C}[X]$ hat genau n komplexe Nullstellen (mit Vielfachheit gezählt). (Dies klärt, wo man Lösungen suchen muß.)

(e) Grad ≥ 5: Satz von Abel-Ruffini (1824): Obige Gleichung im allgemeinen nicht „durch Radikale auflösbar“, also Lösungen nicht durch Addition, Subtraktion, Multiplikation, Division und Wurzelziehen aus Koeffizienten (und rationalen Zahlen) darstellbar.

(f) Eleganter Zugang und Präzisierung durch Évariste Galois 1830-32, Verbindung zur Gruppentheorie. Ausgearbeitet von Liouville, Dedekind, Kronecker... (algebraische Körpererweiterungen, Galois-Theorie).

Die obige Gleichung ist durch Radikale auflösbar genau dann, wenn eine gewisse (Galois-)Gruppe auflösbar ist.

Anwendungen: Konstruktionen mit Zirkel und Lineal. Ist eng verknüpft mit obigem Problem, vgl. geometrische Lösung der Babylonier.

Elementare Resultate über Körpererweiterungen (plus Transzendenz von π) erlauben die Lösung der drei klassischen Probleme der antiken Mathematik:

- Verdopplung des Würfels (Delisches Problem): Nicht möglich.
- Winkeldreiteilung: Nicht möglich (im allgemeinen).

- Quadratur des Kreises: Nicht möglich, da π nicht algebraisch über $\mathbb{Q}$ (Ferdinand von Lindemann, 1882).

Verwandtes Resultat: Gauß 1796 (19-jährig): Das regelmäßige n-Eck ist genau dann konstruierbar, wenn $n = 2^m p_1 p_2 \dots p_r$ für ein $m \in \mathbb{N}$ und paarweise verschieden Fermatsche Primzahlen $p_1, p_2, \dots, p_r$. (Eine Primzahl p ist Fermatsch genau dann, wenn sie ungerade ist und $p-1$ eine Zweierpotenz ist. Die ersten Fermatschen Primzahlen sind 3, 5, 17, 257, 65537.)

Referenzen. Vor allem: Bosch: Algebra.

Unsere Quellen sind [Bos] (Bosch: Algebra); Soergel Algebra Skript; Rapoports Vorlesungsnotizen; daneben [Jan] (Jantzen, Schwermer: Algebra); [Lor92] Lorenz: Einführung in die Algebra; [FS78] Fischer, Sacher: Einführung in die Algebra.

Konventionen und Erinnerungen. $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.

Ringe sind assoziativ, kommutativ und unitär, falls nicht explizit anders erwähnt. Oft sagen wir Morphismus statt Homomorphismus, etwa Morphismus von Ringen oder Ringmorphismus. Ist $\varphi : R \to S$ ein Morphismus von Ringen, so nehmen wir stets an, dass $\varphi(1) = 1$.

Ist R ein Ring, so schreiben wir $R^\times$ für die (multiplikative) Gruppe der Einheiten in R.

Erinnerung: Ein Ring R ist ein Körper genau dann, wenn er nicht der Nullring ist und $R^\times = R - \{0\}$.

Morphismus von Körpern := Morphismus von Ringen zwischen Körpern.

Ein Körper K hat genau zwei Ideale: $\{0\}$ und K. Insbesondere ist jeder Morphismus von Körpern injektiv.

Beispiele für Körper: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p := \mathbb{Z}/(p)$ (p Primzahl).

keine Körper: $\mathbb{Z}$, $K[X]$ (wobei K ein Körper).

Erinnerung Lokalisierung und Quotientenkörper: Ist R ein Ring und $S \subset R$ eine multiplikativ abgeschlossene Teilmenge (mit $1 \in S$), so kann man die Lokalisierung R_S bilden. Elemente werden als Brüche $\frac{r}{s}$ mit $r \in R$, $s \in S$ geschrieben. Der kanonische Ringmorphismus $\mathrm{can} : R \to R_S$, $r \mapsto \frac{r}{1}$, hat die folgende universelle Eigenschaft: Ist $\varphi : R \to A$ ein Morphismus von Ringen mit $\varphi(S) \subset A^\times$, so gibt es genau einen Morphismus von Ringen $\varphi' : R_S \to A$ so dass

$$\begin{array}{ccc} R & \xrightarrow{\mathrm{can}} & R_S \\ & \searrow^{\varphi} & \downarrow{\scriptstyle \varphi'} \\ & & A \end{array}$$

kommutiert. Es gilt $\varphi'(\frac{r}{s}) = \varphi(r)\varphi(s)^{-1}$.

Ist speziell R ein Integritätsring (= Integritätsbereich) und $S = R - \{0\}$, so ist

$$\mathrm{Quot}(R) := R_S$$

ein Körper und wird der **Quotientenkörper** von R genannt.

Beispielsweise erhält man so die Körper

$$\mathbb{Q} = \operatorname{Quot}(\mathbb{Z})$$

und (für K einen Körper)

$$K(X) := \operatorname{Quot}(K[X])$$
$$K(X_1, X_2, \dots, X_n) := \operatorname{Quot}(K[X_1, X_2, \dots, X_n]).$$

Letztere heißen **Körper der rationalen Funktionen in** X bzw. **in** X_1**,** $X_2, \dots, X_n$.

1. Algebraische Körpererweiterungen

1.1. **Primkörper und Charakteristik eines Körpers.** Sei K ein Körper. Ist $E \subset K$ ein Unterring, der selbst ein Körper ist, so nennen wir E einen **Teilkörper** von K. Wir sagen auch, dass E ein **Unterkörper** von K ist, oder dass K ein **Oberkörper** von E ist.

Beobachtung: Sind $(E_i)_{i\in I}$ Teilkörper von K, so ist auch $\bigcap_{i\in I} E_i$ Teilkörper von K.

Ist $M \subset K$ eine Teilmenge, so gibt es also einen kleinsten Teilkörper von K, der M enthält, nämlich den Durchschnitt aller solchen Teilkörper; dieser heißt **der von** M **erzeugte Teilkörper von** K.

Insbesondere enthält K einen eindeutig bestimmten kleinsten Unterkörper P (der von $\emptyset$ erzeugte Teilkörper). Dieser wird als **Primkörper** von K bezeichnet.

Sei

$$\varphi : \mathbb{Z} \to K$$

der eindeutige Morphismus von Ringen. Es gilt

$$\varphi(n) = n \cdot 1 := \begin{cases} \overbrace{1 + 1 + \cdots + 1}^{n\text{-mal}} & \text{falls } n \geq 0, \\ -(\underbrace{1 + 1 + \cdots + 1}_{(-n)\text{-mal}}) & \text{falls } n < 0. \end{cases}$$

Da $\mathbb{Z}$ ein Hauptidealring ist, gilt $\ker \varphi = (p) = p\mathbb{Z}$ für ein eindeutig bestimmtes $p \in \mathbb{N}$. Wir nennen p die **Charakteristik** $\operatorname{char} K$ von K. Es gilt $(\operatorname{char} K) \cdot k = 0$ für alle $k \in K$.

Lemma 1.1. *Die Charakteristik $p = \operatorname{char} K$ ist entweder Null oder eine Primzahl. Für den Primkörper P von K gilt:*

$$P \cong \begin{cases} \mathbb{Q} & \textit{falls } \operatorname{char} K = 0, \\ \mathbb{F}_p & \textit{falls } \operatorname{char} K > 0, \end{cases}$$

und dieser Isomorphismus ist eindeutig.

Proof. Sei $\varphi : \mathbb{Z} \to K$ wie oben, also $\ker \varphi = (p)$. Dann faktorisiert φ zu einem injektiven Morphismus

$$\overline{\varphi} : \mathbb{Z}/(p) \hookrightarrow K$$

von Ringen. Da K ein Integritätsring ist, ist $\mathbb{Z}/(p)$ ein Integritätsring und somit (p) ein Primideal. Also gilt $p = 0$ oder p ist eine Primzahl.

Ist p eine Primzahl, so ist $\mathbb{F}_p = \mathbb{Z}/(p)$ ein Körper und das Bild von $\overline{\varphi} : \mathbb{F}_p \hookrightarrow K$ ist in jedem Unterkörper von K enthalten. Also ist dieses Bild der kleinste Unterkörper von K.

Sei $p = 0$. Dann ist $\varphi : \mathbb{Z} \to K$ injektiv und bildet alle Elemente von $\mathbb{Z} - \{0\}$ auf Einheiten an. Also faktorisiert $\overline{\varphi}$ über $\mathbb{Z} \to \mathrm{Quot}(\mathbb{Z}) = \mathbb{Q}$ zu einem injektiven Morphismus

$$\mathbb{Q} \hookrightarrow K.$$

Wie oben ist sein Bild der kleinste Unterkörper von K.

Der Isomorphismus ist eindeutig, da es genau einen Morphisms $\mathbb{Q} \to \mathbb{Q}$ (bzw. $\mathbb{F}_p \to \mathbb{F}_p$) von Ringen/Körpern gibt. □

1.2. **Endliche und algebraische Körpererweiterungen.** Eine **Körpererweiterung** ist ein Körper L mitsamt einem Unterkörper $K \subset L$. Wir notieren eine solche Körpererweiterung als L/K[1] oder als $K \subset L$. Wir sagen auch (etwas unpräzise), dass L eine Körpererweiterung oder ein Erweiterungskörper von K ist.

Ein **Zwischenkörper** einer Körpererweiterung L/K ist ein Körper E mit $K \subset E \subset L$.

Ist L/K eine Körpererweiterung, so restringiert die Multiplikation $L \times L \to L$ zu $K \times L \to L$, und so wird die abelsche Gruppe $(L, +)$ ein K-Vektorraum.

Definition 1.2. Sei L/K ein Körpererweiterung. Der **Grad** $[L : K]$ von L/K ist die Dimension von L als K-Vektorraum,

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

Eine Körpererweiterung heißt **endlich** genau dann, wenn $[L : K] < \infty$, und sonst **unendlich**.

Offensichtlich ist $[L : K]$ zu $L = K$ äquivalent.

Examples 1.3. Die Körpererweiterung $\mathbb{R} \subset \mathbb{C}$ ist endlich,

$$[\mathbb{C} : \mathbb{R}] = 2.$$

Die Körpererweiterung $K \subset K(X)$ ist unendlich (da bereits $K[X] \subset K(X)$ unendlichdimensional). Ebenso $\mathbb{Q} \subset \mathbb{R}$.

Theorem 1.4 (Gradsatz, Multiplikativität des Grad)**.** *Seien $K \subset L \subset M$ Körpererweiterungen. Dann gilt die* ***Gradformel***

$$[M : K] = [M : L][L : K],$$

wobei $n \cdot \infty = \infty \cdot n = \infty$ für $n \in \mathbb{N} \cup \{\infty\}$.

Ende 1. Vorlesung Montag 2. April 2012.

[1] Wir meinen damit nie den Quotientenvektorraum.

Proof. Sei $(l_i)_{i\in I}$ eine K-Basis von L und $(m_j)_{j\in J}$ eine L-Basis von M. Es genügt zu zeigen, dass dann $(l_i m_j)_{(i,j)\in I\times J}$ eine K-Basis von M ist.

K-Erzeugendensystem: Ist $x \in M$, so habe $x = \sum_{j\in j} \lambda_j m_j$ mit eindeutigen $\lambda_j \in L$, fast alle Null. Jedes λ_j hat Darstellung $\lambda_j = \sum_{i\in I} \kappa_i^{(j)} l_i$ mit eindeutigen $\kappa_i^{(j)} \in K$, fast alle Null. Also

$$x = \sum_{j\in j} \lambda_j m_j = \sum_{j\in j} \sum_{i\in I} \kappa_i^{(j)} l_i m_j.$$

K-lineare Unabhängigkeit: Gelte

$$0 = \sum_{(i,j)\in I\times J} a_{ij} l_i m_j$$

für $a_{ij} \in K$, fast alle a_{ij} Null. Dann

$$0 = \sum_{j\in J} \Big(\sum_{i\in I} a_{ij} l_i \Big) m_j,$$

und da $(m_j)_{j\in J}$ L-Basis von M ist folgt $0 = \sum_{i\in I} a_{ij} l_i$ für jedes $j \in J$. Da $(l_i)_{i\in I}$ K-Basis von L ist folgt $a_{ij} = 0$ für alle $(i,j) \in I \times J$. □

Corollary 1.5. *Ist $[M : K]$ eine Primzahl, so $K = L$ oder $L = M$.*

Corollary 1.6. *Sind $K \subset L \subset M$ Körpererweiterungen, so ist M/K endlich genau dann wenn M/L und L/K endlich sind.*

Sei $K \subset L$ eine Körpererweiterung und $M \subset L$ eine Teilmenge. Sei

$$K(M)$$

der von $K \cup M$ erzeugte Teilkörper, also der kleinste Zwischenkörper von $K \subset L$, der M enthält. Man sagt, dass $K(M)$ aus K **durch Adjunktion von** M entsteht. [2]

Sei

$$K[M]$$

der kleinste Unterring von L, der $K \cup M$ enthält (Existenz: Schnitt über alle solchen Unterringe).

Besteht M aus den endlich vielen Elementen $a_1, a_2, \dots, a_n$, so schreibt man[3]

$$K(M) = K(a_1, a_2, \dots, a_n) \text{ und}$$
$$K[M] = K[a_1, a_2, \dots, a_n].$$

Offensichtlich gelten

$$K[a_1, a_2, \dots, a_n] = \{f(a_1, \dots, a_n) \mid f \in K[X_1, \dots, X_n]\}$$

[2] oder: Der Körper K wird über k von M erzeugt.

[3] Die Reihenfolge spielt keine Rolle

und

$$K(a_1, a_2, \ldots, a_n) = \{\frac{f(a_1, \ldots, a_n)}{g(a_1, \ldots, a_n)} \mid f, g \in K[X_1, \ldots, X_n], g(a_1, \ldots, a_n) \neq 0\}.$$

Nun ist klar, dass

$$K(a_1, a_2, \ldots, a_n) = \mathrm{Quot}(K[a_1, a_2, \ldots, a_n]).$$

Genauer: Die universelle Eigenschaft des Quotientenkörpers liefert einen kanonischen Isomorphimsus

$$\mathrm{Quot}(K[a_1, a_2, \ldots, a_n]) \xrightarrow{\sim} K(a_1, a_2, \ldots, a_n).$$

Analoge Resultate gelten, falls M nicht endlich ist.[4]

Beachte: Im Fall $K \subset L = \mathrm{Quot}(K[X])$ gilt $K(X) = \mathrm{Quot}(K[X])$ in Übereinstimmung mit der obigen Definition.

Variation: Ist $\mathcal{A} = (a_i)_{i \in I}$ eine Familie von Elementen von L gegeben, so setze $M := \{a_i \mid i \in I\}$ und definiere $K[\mathcal{A}] := K[M]$ und $K(M) = K(\mathcal{A})$.

Definition 1.7. Sei $K \subset L$ eine Körpererweiterung und $a \in L$. Es heißt a **algebraisch über** K, wenn a Nullstelle einer Gleichung (irrelevant, dass normiert)

$$X^n + c_1 X^{n-1} + c_2 X^{n-2} + \cdots + c_n = 0$$

mit Koeffizienten $c_1, c_2, \ldots, c_n \in K$ ist (vgl. (0.1) in der Einleitung).

Andernfalls heißt a **transzendent über** K.

Die Körpererweiterung $K \subset L$ heißt **algebraisch**, falls alle Elemente von L algebraisch über K sind.

Example 1.8. (a) Betrachte $\mathbb{Q} \subset \mathbb{C}$.
$\sqrt{2}$ und i sind algebraisch über $\mathbb{Q}$.
Ist $1 + i$ algebraisch über $\mathbb{Q}$?
π und e sind transzendent über $\mathbb{Q}$ (Lindemann 1882, Hermite 1873).

(b) $K \subset K(X)$. Dann ist X transzendent über K.

Sei $K \subset L$ eine Körpererweiterung und $a \in L$. Betrachte den Einsetzungsmorphismus

$$\begin{aligned} \varphi : K[X] &\to L, \\ g(X) &\mapsto g(a). \end{aligned} \tag{1.1}$$

Eventuell Diagramm

$$\begin{array}{ccc} K & \hookrightarrow & \\ \downarrow & \searrow & \\ K[X] & \xrightarrow[\exists! X \mapsto a]{} & L \end{array}$$

Dann ist a algebraisch über K genau dann, wenn φ nicht injektiv ist.

[4] Dann nimm $K[X_m \mid m \in M]$ statt $K[X_1, \ldots, X_n]$. Werte aus per $X_m \mapsto m$.

Sei a tranzendent. Dann induziert φ per universeller Eigenschaft der Lokalisierung (des Quotientenkörpers) einen Isomorphismus

$$K(X) = \operatorname{Quot}(K[X]) \xrightarrow{\sim} K(a).$$

Wir nehmen nun an, dass a algebraisch über K ist. Weil $K[X]$ ein Hauptidealring ist, gilt $\ker \varphi = (f)$ für ein Element $f \in K[X]$. Da $f \neq 0$ können wir annehmen, dass f normiert ist. Dies legt f eindeutig fest. Wir nennen f das **Minimalpolynom von a (über K)** und notieren es oft als $\min_{a/K}$.

Theorem 1.9 (über das Minimalpolynom)**.** *Sei $K \subset L$ eine Körpererweiterung und sei $a \in L$ algebraisch über K, mit Minimalpolynom $f = \min_{a/K}$.*

(a) Das Minimalpolynom f ist das eindeutige normierte Polynom $g \in K[X]$ minimalen Grades, das $g(a) = 0$ erfüllt.[5] [6]

(b) Das Minimalpolynom f ist das eindeutige irreduzible normierte Polynom $g \in K[X]$ mit $g(a) = 0$.

(c) $K[a]$ ist ein Körper, $K[a] = K(a)$, und der Einsetzungsmorphismus φ (siehe (1.1)*) induziert einen Isomorphismus*

$$K[X]/(f) \xrightarrow{\sim} K[a]$$

von Körpern.

(d) Die Elemente 1, a, $a^2, \dots a^{\deg(f)-1}$ bilden eine K-Basis von $K[a]$. Somit ist $K \subset K[a]$ eine endliche Körpererweiterung vom Grad[7]

$$[K[a] : K] = \deg(f).$$

Proof. (a), Offensichtlich ist $f = \min_{a/K}$ normiert und hat a als Nullstelle. Sei $g \in K[X]$ ein normiertes Polynom mit $g(a) = 0$. Es folgt $g \in \ker \varphi = (f)$, also $g = hf$ für ein $h \in K[X]$, und somit $\deg(f) = \deg(h) + \deg(g) \leq \deg(g)$ mit Gleichheit genau dann, wenn $h = 1$ (da f und g beide normiert sind).

(c): Das Bild von φ ist offensichtlich gerade $K[a]$. Somit induziert φ einen Isomorphismus

$$\overline{\varphi} : K[X]/(f) \xrightarrow{\sim} K[a].$$

Da $K[a]$ als Unterring von L ein Integritätsring ist, ist (f) ein Primideal. Primideale $\neq \{0\}$ in Hauptidealringen sind bereits maximale Ideale. Also ist (f) ein maximales Ideal, und somit ist $K[X]/(f) \xrightarrow{\sim} K[a]$ ein Körper, also $K[a] = K(a)$.

(b): Da (f) ein Primideal ist und $K[X]$ ein Hauptidealring (und somit faktoriell), ist f irreduzibel (hier äquivalent zu prim). Ist umgekehrt $g \in$

[5] Das erklärt die Bezeichnung Minimalpolynom.

[6] Für $b \in L$ sei $M_b : L \to L$, $l \mapsto bl$, die Multiplikationsabbildung. Ist $g \in K[X]$ so gilt $M_{g(a)} = g(M_a)$ in $\operatorname{End}_K(L)$. Außerdem $M_b = 0$ genau dann wenn $b = 0$. Also gilt für $g \in K[X]$, dass $g(a) = 0$ gdw. $M_{g(a)} = 0$ gdw. $g(M_a) = 0$.

Das Minimalpolynom der K-linearen Abbildung M_a stimmt also mit dem Minimalpolynom von a über K überein.

Vgl. Jantzen-Schwermer S. 178.

[7] Der Grad des Minimalpolynoms f von a ist also der Grad der Körpererweiterung $K \subset K[a]$. Daher rührt wohl die Bezeichnung „Grad einer Körpererweiterung“.

$K[X]$ irreduzibel mit $g(a) = 0$, so $g \in (f)$, also $g = hf$ wie oben. Da f und g normiert und irreduzibel sind, folgt $g = f$.

(d): Sei $d := \deg(f)$ und $K[X]_{<d} \subset K[X]$ der K-Untervektorraum der Polynome vom Grad $< d$. Division mit Rest durch f besagt, dass es für jedes $h \in K[X]$ eindeutig bestimmte Elemente q, $r \in K[X]$ gibt mit

$$h = qf + r \quad \text{und } r \in K[X]_{<d}.$$

Dies bedeutet, dass

$$K[X] = (f) \oplus K[X]_{<d}$$

als K-Vektorraum. Jede K-Basis von $K[X]_{<d}$, etwa 1, X, $X^2, \dots, X^{d-1}$, liefert also eine K-Basis von $K[X]/(f)$. Die Behauptungen folgen nun aus (c). □

Example 1.10. Betrachte $\mathbb{Q} \subset \mathbb{R}$. Sei p eine Primzahl und $n \in \mathbb{N} - \{0\}$. Dann ist $\sqrt[n]{p} \in \mathbb{R}$ algebraisch über $\mathbb{Q}$ mit Minimalpolynom $X^n - p \in \mathbb{Q}[X]$, denn dieses Polynom ist irreduzibel nach dem Eisenstein-Kriterium [Bos, Satz 2.8/1] (basierend auf dem Satz von Gauß [Bos, Satz 2.7/7], welcher unter anderem besagt, dass ein irreduzibles Polynom vom Grad > 0 in $\mathbb{Z}[X]$ auch in $\mathbb{Q}[X]$ irreduzibel ist). Also

$$[\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}] = \deg(X^n - p) = n.$$

Proposition 1.11. *Sei $K \subset L$ eine Körpererweiterung. Für $a \in L$ sind äquivalent:*

(a) a ist algebraisch über K;
(b) $[K(a) : K] < \infty$;
(c) Es gibt einen Zwischenkörper $K \subset E \subset L$ mit $[E : K] < \infty$ und $a \in E$.

Proof. (a) ⇒ (b) folgt unmittelbar aus dem Satz 1.9 über das Minimalpolynom, und (b) ⇒ (c) ist trivial.

Gelte (c). Dann lander der Auswertungsmorphismus $K[X] \to L$ in E, induziert also einen Morphisms $K[X] \to E$. Wegen $\dim_K K[X] = \infty$ kann dieser nicht injektiv sein. Also ist a algebraisch über K. Andere Formulierung: $\{1, a, a^2, \dots\} \subset E$ ist linear abhängig. □

Corollary 1.12. *Jede endliche Körpererweiterung $K \subset L$ ist algebraisch.*

Proof. Das folgt direkt aus (c) ⇒ (a) in Proposition 1.11. □

Ende 2. Vorlesung Donnerstag 5. April 2012.

Sei $K \subset L$ eine Körpererweiterung. Man sagt, dass L **endlich erzeugt**[8] **über** K ist, falls $K(a_1, a_2, \dots, a_n) = L$ für geeignete $a_1, a_2, \dots, a_n \in L$.

Die Erweiterung heißt **einfach** (oder **primitiv**), falls es ein $a \in L$ gibt mit $K(a) = L$. Ein solches a heißt **primitives Element von** L/K.
[9]

[8] besser: erzeugbar

[9] mündlich: Erinnerung: Ist a transzendent über K, so $K(X) \xrightarrow{\sim} L$, $X \mapsto a$. Ist a algebraisch über K (vgl. Einleitung), so $K[X]/(\min_{a/K} \xrightarrow{\sim} L$, $X \mapsto a$.

Für $a \in L$ wird $[K(a) : K]$ auch als der **Grad von a über K** bezeichnet, notiert $\deg(a)$ oder genauer $\deg_K(a)$. Ist a algebraisch über K, so gilt nach dem Satz 1.9 über das Minimalpolynom

$$\deg(a) = \deg(\min\nolimits_{a/K}).$$

Ist a transzendent, so $\deg(a) = \infty$.

Example 1.13. Sei K ein Körper. Dann ist $K(X)$ endlich erzeugt über K und einfach, aber nicht endlich.

Theorem 1.14. *Sei $L = K(a_1, \dots, a_n)$ eine endlich erzeugte Körpererweiterung von K. Sind $a_1, a_2, \dots, a_n$ algebraisch über K, so gelten*

(a) $L = K(a_1, \dots, a_n) = K[a_1, \dots, a_n]$
(b) L ist endliche und damit insbesondere algebraische Körpererweiterung von K.

Example 1.15. (a) (Könnte auch direkt nach Korollar 1.12 stehen.)
Ist $L = K(a)$ und a algebraisch über K, so ist jedes Element von L algebraisch über K.
Beispiel: Für $n \in \mathbb{N} - \{0\}$ ist $\cos \frac{\pi}{n}$ algebraisch über $\mathbb{Q}$: Als Nullstelle von $X^{2n} - 1$ ist $e^{\pi i/n}$ algebraisch über $\mathbb{Q}$. Aus $e^{i\alpha} = \cos\alpha + i \sin\alpha$ folgt

$$\cos\frac{\pi}{n} = \frac{1}{2}(e^{i\pi/n} + e^{-i\pi/n}).$$

(b) Alle Elemente von $\mathbb{Q}(\sqrt[5]{17}, \sqrt[3]{5})$ (als Teilkörper von $\mathbb{C}$) sind algebraisch über $\mathbb{Q}$.

Proof. Induktion über n. Der Fall $n = 1$ folgt aus dem Satz 1.9 über das Minimalpolynom. (kann/sollte(?) Induktion auch beim Trivialfall $n = 0$ starten.) Gelte $n > 1$. Per Induktion wissen wir, dass $K \subset K[a_1, \dots, a_{n-1}]$ eine endliche Körpererweiterung ist. Nach dem Satz 1.9 über das Minimalpolynom ist $K[a_1, \dots, a_{n-1}][a_n] = K[a_1, \dots, a_{n-1}, a_n]$ eine endliche Körpererweiterung von $K[a_1, \dots, a_{n-1}]$. Nach Korollar 1.6 ist somit $K \subset K[a_1, \dots, a_{n-1}, a_n]$ endliche Körpererweiterung. Da $K[a_1, \dots, a_{n-1}, a_n]$ ein Körper ist folgt $K[a_1, \dots, a_n] = K(a_1, \dots, a_n) = L$. □

(Zusammenfassung von Korollar 1.12 und Satz 1.14:)

Corollary 1.16. *Sei $K \subset L$ eine Körpererweiterung. Dann sind äquivalent:*

(a) L/K ist endlich.
(b) L wird über K von endlich vielen algebraischen Elementen erzeugt.
(c) L ist endlich erzeugte algebraische Körpererweiterung von K.

Proof. Da jede endliche Körpererweiterung offensichtlich endlich erzeugt ist folgt dies aus Korollar 1.12 und Satz 1.14. □

Corollary 1.17. *Für eine Körpererweiterung $K \subset L$ sind äquivalent:*

(a) L/K ist algebraisch.

(b) *Es gibt eine Teilmenge $M \subset L$ von über K algebraischen Elementen mit $L = K[M]$.*
(c) *Es gibt eine Teilmenge $M \subset L$ von über K algebraischen Elementen mit $L = K(M)$.*

Ist M wie in (c), so gilt bereits $L = K[M]$ (vgl. Blatt 1, Aufgabe 2).

Proof. Für (a) $\Rightarrow$ (b) nimm $M = L$, und (b) $\Rightarrow$ (c) ist trivial.

Gelte (c). Beachte

$$K(M) = \bigcup_{E \subset M \text{ endlich}} K(E).$$

Nach Satz 1.14 ist jedes $K \subset K(E)$ eine algebraische Körpererweiterung von K, was (a) zeigt, und es gilt $K(E) = K[E]$. Aus

$$K[M] = \bigcup_{E \subset M \text{ endlich}} K[E]$$

folgt dann $K[M] = K(M) = L$. □

Theorem 1.18. *Seien $K \subset L \subset M$ Körpererweiterungen, mit $K \subset L$ algebraisch. Ist $a \in M$ algebraisch über L, so ist a algebraisch über K.*

Proof. Sei

$$X^n + c_{n-1}X^{n-1} + \cdots + c_0 \in L[X]$$

das Minimalpolynom von a über L. Dann ist a bereits algebraisch über $K(c_0, c_1, \ldots, c_{n-1})$. Nach dem Satz 1.9 über das Minimalpolynom ist

$$K(c_0, c_1, \ldots, c_{n-1}) \subset K(c_0, c_1, \ldots, c_{n-1})(a) = K(c_0, c_1, \ldots, c_{n-1}, a)$$

endlich, und nach Korollar 1.16 ist $K \subset K(c_0, c_1, \ldots, c_{n-1})$ endlich. Also ist $K \subset K(c_0, c_1, \ldots, c_{n-1}, a)$ endlich (Korollar 1.6) und somit algebraisch (Korollar 1.12). Insbesondere ist a algebraisch über K. □

Corollary 1.19. *Sind $K \subset L \subset M$ Körpererweiterungen, so ist M/K algebraisch genau dann wenn M/L und L/K algebraisch sind.*

Proof. Ist M/K algebraisch, so sind offensichtlich M/L und L/K algebraisch.

Seien M/L und L/K algebraisch. Jedes $a \in M$ ist algebraisch über K nach Satz 1.18, also ist M/K algebraisch. □

Corollary 1.20. *Sei $K \subset L$ eine Körpererweiterung. Dann ist*

$$L_{\text{alg}} := L_{\text{alg}/K} := \{a \in L \mid a \text{ algebraisch über } K\}$$

ein Zwischenkörper von $K \subset L$ und $K \subset L_{\text{alg}}$ ist eine algebraische Körpererweiterung. Kein $b \in L - L_{\text{alg}}$ ist algebraisch über L_{alg}.

*L_{alg} heißt der **algebraische Abschluss von K in L**.*

Proof. Sind $a_1, a_2 \in L_{\text{alg}}$, so ist $K \subset K(a_1, a_2)$ algebraisch (Satz 1.14). Also ist L_{alg} ein Körper. Somit ist $K \subset L_{\text{alg}}$ eine algebraische Körpererweiterung.

Ist $b \in L$ algebraisch über L_{alg}, so ist es auch algebraisch über K nach Satz 1.18, also bereits in L_{alg}. □

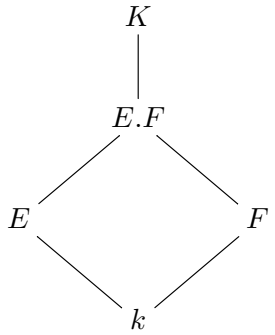
Example 1.21. Beispiel für Körpererweiterung, die weder endlich erzeugt noch endlich ist: Betrachte $\mathbb{Q} \subset \mathbb{C}$. Sei $\overline{\mathbb{Q}} := \mathbb{C}_{\text{alg}}$. Die Körpererweiterung $\mathbb{Q} \subset \overline{\mathbb{Q}}$ ist nicht endlich, da $[\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}] = n$. Da $\mathbb{Q} \subset \overline{\mathbb{Q}}$ algebraisch ist, kann diese Erweiterung nicht endlich erzeugt sein.

Sind E und F zwei Teilkörper eines Körpers K, so bezeichnet man den von $E \cup F$ erzeugten Teilkörper von K,

$$E.F := E(F) = F(E),$$

als das **Kompositum von E und F.**

Theorem 1.22. *Sei $k \subset K$ eine Körpererweiterung mit Zwischenkörpern E und F.*



Dann gelten (die mir merkenswerter erscheinenden Aussagen sind hervorgehoben):

(a) $\boxed{E/k \text{ endlich} \Rightarrow E.F/F \text{ endlich.}}$

(b) E/k *und* F/k *endlich* $\Leftrightarrow$ $E.F/k$ *endlich.*

und

(a') $\boxed{E/k \text{ algebraisch} \Rightarrow E.F/F \text{ algebraisch.}}$

(b') E/k *und* F/k *algebraisch* $\Leftrightarrow$ $E.F/k$ *algebraisch.*

Proof. Beobachtung: Ist $M \subset E$ mit $E = k(M)$, so $E.F = F(E) = F(M)$ (da $E = k(M) \subset F(M)$).

(a): Ist E/k endlich, so finden wir $M \subset E$ endlich, bestehend aus über k algebraischen Elementen. Diese sind erst recht algebraisch über F, und somit ist $F \subset F(M) = E.F$ endlich (Korollar 1.16).

(b) folgt nun aus Korollar 1.6.

(a') Ist E/k algebraisch, so ist $F \subset F(E) = E.F$ algebraisch nach Korollar 1.17.

(b') folgt nun aus Korollar 1.19. □

Exercise 1.23. (Anwesenheitsaufgabe) Bestimme das Minimalpolynom von $1 + i$ über $\mathbb{R}$.

Exercise 1.24. (Übungsaufgabe) Quadratische Körpererweiterungen. Sei $K \subset L$ eine Körpererweiterung mit $\operatorname{char} K \neq 2$. Dann sind äquivalent:

(a) L/K ist eine **quadratische Körpererweiterung**, d. h. $[L : K] = 2$.

(b) L entsteht durch Adjunktion (= Hinzufügen) einer Quadratwurzel, d. h. $L = K(a)$ für ein $a \in L - K$ mit $a^2 \in K$.

1.3. **Konstruktion mit Zirkel und Lineal.** [10]

Ziel diese Abschnitts ist die Lösung der drei klassischen Problemen der antiken Mathematik (Quadratur des Kreises, Verdopplung des Würfels, Winkeldreiteilung).

Die Lösbarkeit dieser Probleme hängt davon ab, welchen Begriff der Konstruierbarkeit man verwendet. Wir präzisieren deswegen zunächst diesen Begriff.

Wir identifizieren die Zeichenebene $\mathbb{R}^2$ mit der komplexen Zahlenebene $\mathbb{C}$.

Definition 1.25. Sei $M \subset \mathbb{C}$ eine Teilmenge mit mindestens zwei Elementen.

(i) Betrachte

$$\mathcal{G}_M := \{g \subset \mathbb{C} \mid g \text{ Gerade durch zwei verschiedene Punkte von } M\},$$

$$\mathcal{S}_M := \left\{S \subset \mathbb{C} \mid \begin{array}{l} S \text{ ist Kreis mit Mittelpunkt in } M \text{ und Radius} \\ |a-b|, \text{ für geeignete } a, b \in M \end{array}\right\}.$$

Ein Punkt $p \in \mathbb{C}$ heißt **elementar konstruierbar aus** M, falls es $A, B \in \mathcal{G}_M \cup \mathcal{S}_M$, $A \neq B$ gibt mit $p \in A \cap B$.

(ii) Sei $M = M^{(0)}$ und induktiv

$$M^{(n+1)} := \{p \in \mathbb{C} \mid p \text{ ist elementar konstruierbar aus } M^{(n)}\}$$

die Menge aller aus $M^{(n)}$ elementar konstruierbarer Punkte.

Wir nennen

$$\mathrm{Kon}(M) := \bigcup_{n \in \mathbb{N}} M^{(n)}$$

die Menge der **aus** M **(mit Zirkel und Lineal) konstruierbaren Punkte**. Wir nennen eine Gerade oder einen Kreis **(mit Zirkel und Lineal) konstruierbar aus** M, wenn er in $\mathcal{G}_{\mathrm{Kon}(M)}$ oder in $\mathcal{S}_{\mathrm{Kon}(M)}$ liegt.

Observations 1.26.

(a) Es gilt $M^{(n)} \subset M^{(n+1)}$ für alle $n \in \mathbb{N}$, da M zweielementig.

(b) $\mathrm{Kon}(M)$ ist die kleinste Teilmenge $S \subset \mathbb{C}$, die M enthält und abgeschlossen ist unter „elementaren Konstruktionen“, d. h. $S = S^{(1)}$ erfüllt.

Remark 1.27. höchstens mündlich

Stelle Automat vor, der induktiv $\mathrm{Kon}(M)$ bestimmt.

---

[10] Abschnitt hier eingeschoben, da für die Lösung der klassischen Probleme relativ wenig Theorie benötigt wird.

Wer mag, kann sofort zu Abschnitt 1.4 springen und mit der allgemeinen Theorie fortfahren.

Liefert keine explizite Konstruktionsanweisung für einen gegebenen Punkt in $\mathrm{Kon}(M)$.

Im Folgenden nehmen wir stets $0, 1 \in M$ an. Bis auf Verschiebung, Streckung und Drehung stellt dies (in Bezug auf Konstruierbarkeit) keine Einschränkung der Allgemeinheit dar (sofern M aus mindestens zwei Elementen besteht). (Alternativ: wähle zwei verschiedene Punkte von M, nenne sie 0 und 1, und identifiziere nun erst die Zeichenebene mit $\mathbb{C}$.)

Das Ziel dieses Abschnitts ist:

Theorem 1.28. *Sei $M \subset \mathbb{C}$ mit $0, 1 \in M$.*

(a) $\mathrm{Kon}(M)$ *ist der kleinste Unterkörper von $\mathbb{C}$, der $M \cup \overline{M}$ enthält und stabil ist unter dem Bilden von Quadratwurzeln.*

(b) Ist $a \in \mathbb{C}$ konstruierbar aus M, so ist a algebraisch über $\mathbb{Q}(M \cup \overline{M})$ von Zweierpotenzgrad. [11]

Ende 3. Vorlesung Donnerstag 12. April 2012

Nachzuholen: Aus M konstruierbare Geraden/Kreise.

Seien $p, q \in \mathbb{C}$, $p \neq q$, und sei $r \in \mathbb{R}_{\geq 0}$. Wir schreiben $K(p; r)$ für den Kreis um p mit Radius r und $L(p; q)$ für die Gerade durch p und q.

Example 1.29. $\mathbb{Z} \subset \mathrm{Kon}(M)$: Der Kreis $K(1; 1) = K(1; |1 - 0|)$ schneidet die Gerade $L(0; 1)$ in den Punkten 0 und 2. Analog erhalte $\mathbb{Z} \subset \mathrm{Kon}(M)$.

Example 1.30. Sind zwei verschiedene Punkte a und b aus M konstruierbar, so ist auch ihre Mittelsenkrechte, d. h. die Menge aller Punkte, die zu a und b denselben Abstand haben, konstruierbar: Die beiden Kreise $K(a; |a - b|)$ und $K(b; |a - b|)$ schneiden sich in zwei Punkten; die Gerade durch diese beiden Punkte ist die gesuchte Mittelsenkrechte.

Example 1.31. Sind eine Gerade g und ein Punkt p aus M konstruierbar (p darf auf g liegen), so ist die Senkrechte zu g durch p konstruierbar (aus M): Wähle $n \in \mathbb{N}$ so groß, dass $K(p; n)$ die Gerade g in zwei Punkten a und b schneidet. Dieser Kreis ist konstruierbar, da $\mathbb{Z} \subset \mathrm{Kon}(M)$. Die Mittelsenkrechte von a und b ist die gesuchte Gerade.

Example 1.32. Sind eine Gerade g und ein Punkt p aus M konstruierbar (p darf auf g liegen), so ist die Parallele zu g durch p konstruierbar: Sei s die Senkrechte zu g durch p. Die Senkrechte zu s durch p ist die gesuchte Parallele.

Lemma 1.33. *Es sei $M \subset \mathbb{C}$ eine Teilmenge mit $0, 1 \in M$. Sei $z \in \mathbb{C}$. Dann sind äquivalent:*

(i) $z \in \mathrm{Kon}(M)$*;*

(ii) $\mathrm{Re}\, z \in \mathrm{Kon}(M)$ *und* $\mathrm{Im}\, z \in \mathrm{Kon}(M)$*;*

[11] Die umgekehrte Implikation ist im allgemeinen falsch, siehe etwa [Bos, Aufgabe 6.4.1 samt Lösung hinten].

(iii) $|z| \in \mathrm{Kon}(M)$ *und* $\frac{z}{|z|} \in \mathrm{Kon}(M)$. *(Beachte: Gilt* $z = re^{it}$ *mit* $r \in \mathbb{R}_{\geq 0}$ *und* $t \in \mathbb{R}$, *so* $|z| = r$ *und* $e^{it} = \frac{z}{|z|}$.*)*

Insbesondere enthält $\mathrm{Kon}(M)$ *die Zahl* i *und ist abgeschlossen unter komplexer Konjugation* $z \mapsto \overline{z}$.

Proof. Die imaginäre Achse ist als Senkrechte zur reellen Achse durch 0 konstruierbar.

Sei a eine reelle Zahl. Der Kreis $K(0;a)$ zeigt, dass a konstruierbar ist genau dann, wenn ia (oder $-a$) konstruierbar ist.

Sei z konstruierbar. Dann schneidet die Parallele zur reellen Achse durch z die imaginäre Achse in $i\mathrm{Im}\, z$; analog schneidet die Parallele zur imaginären Achse durch z die reelle Achse in $\mathrm{Re}\, z$. Die Gerade $L(0;z)$ schneidet den Kreis $K(0;1)$ in $\frac{z}{|z|}$, und der Kreis $K(0;|z|)$ schneidet die reelle Achse in $|z|$.

Sind $\mathrm{Re}\, z$ und $\mathrm{Im}\, z$ konstruierbar, so schneiden sich die Parallele zur imaginären Achse durch $\mathrm{Re}\, z$ und die Parallele zur reellen Achse durch $i\mathrm{Im}\, z$ in z.

Sind $|z|$ und $\frac{z}{|z|}$ konstruierbar, so ist z einer der Schnittpunkte des Kreises $K(0;|z|)$ mit der Geraden $L(0;\frac{z}{|z|})$. □

Theorem 1.34. *Sei* $M \subset \mathbb{C}$ *mit* $0,1 \in M$. *Dann ist* $\mathrm{Kon}(M)$ *ein Zwischenkörper von* $\mathbb{Q}(M \cup \overline{M}) \subset \mathbb{C}$, *der stabil ist unter komplexer Konjugation und unter dem Bilden von Quadratwurzeln: Aus* $z^2 \in \mathrm{Kon}(M)$ *folgt* $z \in \mathrm{Kon}(M)$.

Proof. Seien z, w in $\mathrm{Kon}(M)$.

(a) Behauptung: $\mathrm{Kon}(M)$ ist abgeschlossen unter Addition und additiver Inversenbildung.

Es ist $z + w$ enthalten in $K(z;|w|) \cap K(w;|z|)$. Falls $z = w$ so $2z \in K(z;|z|) \cap L(0;z)$. Der Fall $z = 0$ ist trivial.

Als Schnittpunkt von $K(0;|w|)$ mit $L(0;w)$ liegt $-w$ in $\mathrm{Kon}(M)$. Der Fall $w = 0$ ist trivial.

(b) Behauptung: Ist $w \neq 0$, so $zw^{-1} \in \mathrm{Kon}(M)$.

Schreibe $w = a + bi$. Dann gilt $w^{-1} = \frac{a-bi}{a^2+b^2}$. Um die Behauptung zu zeigen, genügt es also nach dem bereits bewiesenen und Lemma 1.33, die folgenden Aussagen zu zeigen:

- Ist $r \neq 0$ reell und konstruierbar, so ist auch $\frac{1}{r}$ konstruierbar: Die Parallele zu $L(i;r)$ durch 1 schneidet die imaginäre Achse nach dem Strahlensatz im Punkte $i\frac{1}{r}$.
- Sind r und s reell und konstruierbar, so ist rs konstruierbar: Offensichtlich ist is konstruierbar. Die Parallele zu $L(i,r)$ durch is schneidet die reelle Achse im Punkte rs (Strahlensatz).

Wegen $0,1 \subset \mathrm{Kon}(M)$ ist somit $\mathrm{Kon}(M)$ ein Unterkörper der komplexen Zahlen. Wir wissen bereits, dass $\mathrm{Kon}(M)$ stabil ist unter komplexer Konjugation; es folgt $\mathbb{Q}(M \cup \overline{M}) \subset \mathrm{Kon}(M)$.

Sei nun $z = re^{it} \in \mathrm{Kon}(M)$, mit $r \in \mathbb{R}_{\geq 0}$ und $t \in \mathbb{R}$. Es folgt $r, e^{it} \in \mathrm{Kon}(M)$. Um zu zeigen, dass $\pm\sqrt{z}$ in $\mathrm{Kon}(M)$ liegt, genügt es zu zeigen, dass $\sqrt{r}$ und $e^{it/2}$ in $\mathrm{Kon}(M)$ liegen.

- Sei m der Schnittpunkt der reellen Geraden mit der Mittelsenkrechten von -1 und r. Der Kreis $K(m; r-m)$ schneidet die imaginäre Achse nach dem Satz von Thales und dem Höhensatz in den Punkten $\pm i\sqrt{r}$.
- $e^{it/2}$ ist konstruierbar: Der Fall $e^{it} = 1$ ist trivial. Sonst schneidet die Mittelsenkrechte zu 1 und e^{it} den Einheitskreis $K(0;1)$ in den beiden Punkten $\pm e^{it/2}$.

□

Lemma 1.35. *Sei $L \subset \mathbb{C}$ ein Körper, der stabil ist unter komplexer Konjugation. Ist $a \in \mathbb{C}$ elementar konstruierbar aus L, so ist $L[a] = L(a)$ ein Körper, der stabil unter komplexer Konjugation ist, und es gilt $[L(a) : L] \leq 2$.*

Proof. Der Fall $a \in L$ ist trivial. Gelte also $a \notin L$. (Eigentlich verwende nur $a \neq 0$ im folgenden.) Dann ist a Schnittpunkt zweier verschiedener Elemente von $\mathcal{G}_L \cup \mathcal{S}_L$.

1. Fall: Beide Elemente Kreise:

Da sich $L[a]$ nicht ändert, wenn wir a durch $\lambda a + \mu$ mit $\lambda, \mu \in L$, $\lambda \neq 0$, ersetzen, und a elementar konstruierbar aus L genau dann, wenn $\lambda a + \mu$ elementar konstruierbar aus L, können wir ohne Einschränkung annehmen, dass einer der beteiligten Kreise den Mittelpunkt 0, der andere den Mittelpunkt 1 hat.

Sei also a im Schnitt der beiden Kreise $K(0;|r|)$ und $K(1;|R|)$, für $r, R \in L$. Beachte $|r|^2 = r\overline{r} \in L \cap \mathbb{R}_{\geq 0}$ und analog $|R|^2 \in L \cap \mathbb{R}_{\geq 0}$. Es gelten also

$$|a|^2 = a\overline{a} = |r|^2,$$
$$|a-1|^2 = (a-1)(\overline{a}-1) = |R|^2.$$

Aus der ersten Gleichung folgt $\overline{a} = \frac{|r|^2}{a}$, was in die zweite Gleichung eingesetzt

$$(a-1)\Big(\frac{|r|^2}{a} - 1\Big) = |R|^2 \quad \text{bzw.} \quad (a-1)(|r|^2 - a) = a|R|^2$$

ergibt. Also ist a Nullstelle des quadratischen Polynoms

$$X^2 + (|R|^2 - |r|^2 - 1)X + |r|^2$$

mit Koeffizienten in $L \cap \mathbb{R}$. Somit ist klar, dass a algebraisch über L ist, also $L[a] = L(a)$, und dass $[L(a) : L] \leq 2$. Zu zeigen bleibt, dass $L(a)$ stabil unter $z \mapsto \overline{z}$ ist. Es genügt zu zeigen, dass $\overline{a} \in L(a)$. Im Fall $a \in \mathbb{R}$ ist das trivial (dieser Fall tritt aber nur in trivialen Spezialfällen ein, aufgrund der Lage der beiden Kreise).

Im Fall $a \in \mathbb{C} \setminus \mathbb{R}$ hat unser quadratisches reelles Polynom genau die beiden verschiedenen Nullstellen a und $\overline{a}$ und zerfällt in $L(a)$ in Linearfaktoren. Es folgt $\overline{a} \in L(a)$.

2. Fall: Ein Element ein Kreis, das andere eine Gerade:

Per Translation und Drehstreckung können wir ähnlich wie oben annehmen, dass der Kreis die Form $K(0;|r|)$ mit $r \in L$ und die Gerade die Form $L(1;q)$ mit $q \in L \setminus \{1\}$ hat. Wie oben gilt $|r|^2 = r\overline{r} \in L$. Sei $v = q - 1 \in L \setminus \{0\}$. Da a auf Kreis und Gerade liegt, existiert ein $t \in \mathbb{R}$ mit

$$\begin{aligned} a\overline{a} &= |r|^2, \\ a &= 1 + tv. \end{aligned}$$

Die zweite Gleichung zeigt $L[a] = L[t]$, und setzen wir die zweite in die erste ein, so ergibt sich

$$(1 + tv)(1 + t\overline{v}) = |r|^2 \quad \text{bzw.} \quad v\overline{v}t^2 + (v + \overline{v})t + 1 - |r|^2 = 0.$$

Also ist t reelle Nullstelle des quadratischen Polynoms $|v|^2X^2 + (v + \overline{v})X + (1 - |r|^2)$ (mit Koeffizienten in $L \cap \mathbb{R}$). Wegen $L[a] = L[t]$ und $t \in \mathbb{R}$ folgen die Behauptungen.

3. Fall: Beide Elemente Geraden:

Ist eine Gerade als $L(p';q')$ gegeben, mit $p', q' \in L$, so können wir per Translation $p' = 0$ erreichen, und dann per Drehstreckung $q' = 1$.

Ohne Einschränkung ist also eine Gerade die reelle Achse, die andere ist gegeben als $p + \mathbb{R}v$ für geeignete $p, v \in L$, $v \neq 0$. Da a auf beiden Geraden liegt, existieren t, $s \in \mathbb{R}$ mit

$$\begin{aligned} a &= t, \\ a &= p + sv. \end{aligned}$$

Insbesondere ist a reell, und komplexe Konjugation der zweiten Gleichung liefert

$$a = \overline{p} + s\overline{v}.$$

Die Differenz der beiden letzten Gleichungen liefert

$$0 = p - \overline{p} + s(v - \overline{v}) \quad \text{bzw.} \quad s = \frac{\overline{p} - p}{v - \overline{v}},$$

wobei wir beachten, dass $v \neq \overline{v}$, da sonst die beiden Geraden gleich wären (da sie a enthalten). Insbesondere liegt s und damit a in L, also $L = L[a]$.

□

Ende 4. Vorlesung Montag 16. April 2012

Corollary 1.36. *Sei $M \subset \mathbb{C}$ eine Teilmenge mit $0, 1 \in M$, und sei $a \in \mathbb{C}$. Dann sind äquivalent:*

(a) a ist konstruierbar aus M (also $a \in \mathrm{Kon}(M)$).

(b) Es gibt einen Körperturm

$$\mathbb{Q}(M \cup \overline{M}) = L_0 \subset L_1 \subset \cdots \subset L_n \subset \mathbb{C} \tag{1.2}$$

mit $a \in L_n$ *und* $[L_i : L_{i-1}] = 2$ *für alle* $1 \le i \le n$.

12

Proof. Setze $k := \mathbb{Q}(M \cup \overline{M})$.

(a) $\Rightarrow$ (b): Wir finden eine endliche Folge $a_1, a_2, \dots, a_n = a$ so dass jedes a_i elementar konstruierbar aus $M \cup \{a_1, \dots, a_{i-1}\}$ ist. Wir dürfen Lemma 1.35 wiederholt anwenden und erhalten einen Körperturm

$$k \subset k(a_1) \subset k(a_1, a_2) \subset \cdots \subset k(a_1, a_2, \dots, a_n),$$

in dem alle Erweiterungen Grad 1 oder 2 haben. Durch Weglassen erhalten wir den gesuchten Körperturm.

(b) $\Rightarrow$ (a): Offensichtlich gilt $k = L_0 \subset \operatorname{Kon}(M)$. In Charakteristik $\neq 2$ ist jede Erweiterung vom Grad 2 gegeben durch Adjunktion einer geeigneten Quadratwurzel (das folgt aus (0.2) bzw. war Übungsaufgabe) Da $\operatorname{Kon}(M)$ abgeschlossen unter dem Bilden von Quadratwurzeln ist (Satz 1.34), folgt induktiv $L_i \subset \operatorname{Kon}(M)$, also $a \in \operatorname{Kon}(M)$. □

Beweis von Satz 1.28. Sei $k = \mathbb{Q}(M \cup \overline{M})$.

(a): Wir wissen bereits, dass $\operatorname{Kon}(M)$ die geforderten Bedingungen erfüllt (Satz 1.34).

Sei $F \subset \mathbb{C}$ ein Unterkörper, der $M \cup \overline{M}$ enthält und stabil ist unter dem Bilden von Quadratwurzeln. Offensichtlich gilt $k \subset F$. Wir zeigen $\operatorname{Kon}(M) \subset F$. Ist $z \in \operatorname{Kon}(M)$, so gibt es einen Körperturm (2.23) aus Erweiterungen vom Grad 2 mit $z \in L$ (nach Korollar 1.36). Da $L_0 = k \subset F$ und L_{i+1} aus L_i durch Adjunktion einer Quadratwurzel entsteht, sind alle L_i in F enthalten. Es folgt $z \in F$ wie behauptet.

(b): Sei $a \in \mathbb{C}$ konstruierbar aus M. Dann gibt es nach Korollar 1.36 eine Körpererweiterung $k \subset L$ von Zweierpotenzgrad (wegen der Gradformel, Satz 1.4) mit $a \in L$. Diese hat den Zwischenkörper $k(a)$. Die Behauptung folgt nun aus dem Gradsatz 1.4 und aus Korollar 1.12 (endliche Erweiterungen sind algebraisch). □

1.3.1. *Lösung der drei klassischen Probleme.* Die drei klassischen Probleme sind allesamt nicht per Konstruktion mit Zirkel und Lineal lösbar.

Die Quadratur des Kreises. Gegeben ein Kreis mit Radius $r \in \mathbb{R}_{>0}$, kann man $a \in \mathbb{R}$ konstruieren mit $a^2 = \pi r^2$?

Umformuliert: Ist $\sqrt{\pi} r$ konstruierbar aus $M = \{0, r\} \subset \mathbb{C}$?

Per Streckung äquivalent: Ist $\sqrt{\pi}$ konstruierbar aus $M = \{0, 1\}$?

Dies ist nicht der Fall: Sonst wäre nach Satz 1.28 $\sqrt{\pi}$ algebraisch über $\mathbb{Q}$. Äquivalent: π algebraisch über $\mathbb{Q}$. Dies ist aber nicht der Fall (Ferdinand von Lindemann, 1882; siehe z. B. Bundschuh, „Einführung in die Zahlentheorie“, [Bun92]).

[12] Für eine weitere äquivalente Bedingung siehe Satz 2.64.

Verdopplung der Würfels – Delisches Problem. Gegeben ein Würfel mit Kantenlänge a, ist es möglich, die Kantenlänge eines Würfels mit doppeltem Volumen zu konstruieren?

Wie oben formuliert man das um zu: Ist $\sqrt[3]{2}$ aus $\{0,1\}$ konstruierbar?

Dies ist nicht der Fall: Sonst wäre nach Satz 1.28 der Grad der Körpererweiterung $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ eine Zweierpotenz. Aber es gilt $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ (siehe Beispiel 1.10).

Winkeldreiteilung. Sei ein Winkel $0 < \varphi < 2\pi$ gegeben. Die Frage ist, ob $e^{i\varphi/3} \in \mathrm{Kon}(\{0, 1, e^{i\varphi}\})$ gilt.

Lemma 1.37. *Es gilt $e^{i\pi/9} \notin \mathrm{Kon}(\{0, 1, e^{i\pi/3}\})$, der Winkel von $60°$ kann also nicht mit Zirkel und Lineal gedrittelt werden.*

Proof. Die Zahl $e^{i\pi/3}$ ist konstruierbar aus $\{0,1\}$. Es gilt also

$$\mathrm{Kon}(\{0, 1, e^{i\pi/3}\}) = \mathrm{Kon}(\{0,1\}).$$

Angenommen es gilt $e^{i\pi/9} \in \mathrm{Kon}(\{0,1\})$. Dann ist auch der Realteil $\cos\frac{\pi}{9}$ konstruierbar aus $\{0,1\}$. Wir führen dies zum Widerspruch.

Die Additionstheoreme[13] zeigen

$$4(\cos\theta)^3 - 3\cos\theta - \cos(3\theta) = 0.$$

Für $\theta = \frac{\pi}{9}$ folgt wegen $\cos\frac{\pi}{3} = \frac{1}{2}$

$$4\big(\cos\frac{\pi}{9}\big)^3 - 3\cos\big(\frac{\pi}{9}\big) - \frac{1}{2} = 0.$$

Für $a := 2\cos\frac{\pi}{9}$ gilt also

$$a^3 - 3a - 1 = 0.$$

[14] Das Polynom $X^3 - 3X - 1$ ist irreduzibel $\mathbb{Q}[X]$ nach dem Reduktionskriterium [Bos, Satz 2.8.2] (reduziere modulo 2) [15], und somit das Minimalpolynom von a über $\mathbb{Q}$. Es folgt $[\mathbb{Q}(a) : \mathbb{Q}] = 3$, und somit (Satz 1.28) ist a und also auch $a/2 = \cos\frac{\pi}{9}$ nicht konstruierbar aus $\{0,1\}$. □

[13] einfacher: Aus $e^{i\theta} = \cos\theta + i\sin\theta$ und $e^{i(3\theta)} = (e^{i\theta})^3$ und $\sin^2 + \cos^2 = 1$ folgt

$$\begin{aligned}\cos(3\theta) &= (\cos\theta)^3 - 3(\cos\theta)(\sin\theta)^2 \\ &= (\cos\theta)^3 - 3(\cos\theta)(1 - (\cos\theta)^2) \\ &= 4(\cos\theta)^3 - 3(\cos\theta).\end{aligned}$$

[14] Wir wissen bereits, dass a algebraisch über $\mathbb{Q}$ ist, siehe Beispiel 1.15 (a).

[15] Das folgt auch direkt aus dem Korollar 2.56, denn ein linearer Faktor kann ohne Einschränkung als normiert angenommen werden, und dann folgt, dass die entsprechende Nullstelle in $\mathbb{Z}$ liegen muss und ein Teiler von -1 in $\mathbb{Z}$ ist. Jedoch sind ± 1 keine Nullstellen.

1.4. **Der algebraische Abschluss.**

Theorem 1.38 (Satz von Kronecker)**.** *Sei k ein Körper und f ein nichtkonstantes Polynom aus $k[X]$. Dann gibt es eine endliche (und damit algebraische) Körpererweiterung L von k und ein $a \in L$ mit $f(a) = 0$.*

Proof. Sei g ein irreduzibler Teiler von f in $k[X]$. Dann ist (g) ein maximales Ideal in $k[X]$, also $L := k[X]/(g)$ ein Körper. Die offensichtliche Verknüpfung

$$k \hookrightarrow k[X] \twoheadrightarrow k[X]/(g) = L$$

ist injektiv als Morphismus von Körpern, und das Element $\overline{X} := X+(g) \in L$ ist eine Nullstelle von g und damit von f.

Explizit:[16] Schreibe $k[X] \twoheadrightarrow k[X]/(g) = L$ als $p \mapsto \overline{p}$. Ist $g = \sum_{i=0}^{n} c_i X^i$, so gilt

$$g(\overline{X}) = \sum_{i=0}^{n} \overline{c_i}\,\overline{X}^i = \overline{\sum_{i=0}^{n} c_i X^i} = \overline{g} = 0.$$

□

Example 1.39. $f = X^2 + 1 \in \mathbb{R}[X]$ hat Nullstelle $\overline{X}$ in in $\mathbb{R}[X]/(X^2+1)$ $(\xrightarrow{\sim} \mathbb{C},\ X \mapsto i$.

Lemma-Definition 1.40. *Für einen Körper k sind die folgenden drei Bedingungen äquivalent:*

- *(a) Ist $k \subset K$ eine algebraische Erweiterung, so $k = K$.*
- *(b) Jedes nicht konstante Polynom $f \in k[X]$ besitzt eine Nullstelle in k.*
- *(c) Jedes Polynom in $k[X]$* ***zerfällt (vollständig) in Linearfaktoren*** *d. h. ist Produkt einer Konstante aus k und Linearfaktoren $X - a$, für $a \in K$. (D. h. die (normierten) irreduziblen Elemente von $k[X]$ sind genau die (normierten) Linearfaktoren.)*

Sind sie erfüllt, heißt k ***algebraisch abgeschlossen****.*

Proof. (a) ⇒ (b): Folgt aus dem Satz 1.38 von Kronecker.

(b) ⇒ (c): Ist $f \in k[X]$ konstant, so Aussage trivial. Sonst kann Linearfaktoren abspalten: Sei $a \in k$ Nullstelle von f. Polynomdivison liefert

$$f = (X - a)g + r$$

mit $\deg(r) < \deg(X - a_1) = 1$, also $r \in k$. Aus $f(a) = 0$ folgt $r = 0$. Induktion über $\deg(f)$ zeigt die Behauptung.

(c) ⇒ (a): Minimalpolynome von Elementen von K haben Grad eins. □

Example 1.41. Hauptsatz der Algebra: Die komplexen Zahlen sind algebraisch abgeschlossen. (Es ist jedoch kein rein algebraischer Beweis bekannt.)

Beweis: später.

[16] Das folgende Argument gilt für beliebiges (sogar konstantes) $g \in k[X]$. In diesem Fall ist eben $k[X]/(g)$ nur ein Ring (und sogar der Nullring, falls g konstant), aber $\overline{X}$ ist Nullstelle von g.

Remark 1.42. Sei k ein Körper und $f \in k[X]$ nichtkonstant. Das Verfahren von Kronecker stellt eine „externe“ Methode dar, um in einer endlichen Erweiterung von k eine Wurzel (= Nullstelle) von f zu finden.

Weiss man bereits, dass k Unterkörper eines algebraisch abgeschlossenen Körpers K ist, so gibt es die folgende „interne“ Methode: f hat eine Nullstelle $a \in K$. Dann ist a algebraisch über k und eine Nullstelle in der endlichen Körpererweiterung $k(a) = k[a]$ von k.

Definition 1.43. Sei $k \subset K$ eine Körpererweiterung. Man nennt K einen **algebraischen Abschluss von** k, wenn K algebraisch abgeschlossen und K/k algebraisch ist.

Example 1.44.
(a) $\mathbb{C}$ ist ein algebraische Abschluss von $\mathbb{R}$ (wegen Hauptsatz).
(b) Sei $\overline{\mathbb{Q}} = \mathbb{C}_{\mathrm{alg}/\mathbb{Q}}$ in $\mathbb{Q} \subset \mathbb{C}$ der Körper der algebraischen Zahlen. Dann ist $\overline{\mathbb{Q}}$ ein algebraischer Abschluss von $\mathbb{Q}$. Dies folgt aus dem Hauptsatz und dem folgenden Lemma 1.45.

Lemma 1.45. *Sei $k \subset L$ eine Körpererweiterung mit L algebraisch abgeschlossen. Dann ist L_{alg} ein algebraischer Abschluss von k.*

Proof. Setze $K := L_{\mathrm{alg}}$. Korollar 1.20 besagt, dass $k \subset K$ algebraisch ist.

Sei $f \in K[X]$ nichtkonstant. Da L algebraisch abgeschlossen ist, existiert ein $b \in L$ mit $f(b) = 0$. Also ist b algebraisch über K, und somit bereits in K (nach dem bereits verwendeten Korollar oder direkt mit Satz 1.18). Also hat f eine Nullstelle in K, und K ist algebraisch abgeschlossen. □

Theorem 1.46. *Jeder Körper k besitzt einen algebraischen Abschluss.*

Ende 5. Vorlesung Donnerstag 19. April 2012.

Erinnerung: Zornsches Lemma und Existenz maximaler Ideale in Ring $\neq 0$.

Proof. Wir betrachten den Polynomring in unendlich vielen Variablen X_f, die indiziert werden durch die nichtkonstanten Polynome $f \in k[X]$:

$$R := k[X_f \mid f \in k[X] \setminus k\}.$$

In R betrachten wir das Ideal

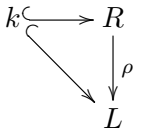
$$\mathfrak{a} := \langle f(X_f) \mid f \in k[X] \setminus k \rangle.$$

Beachte, dass jedes nichtkonstante Polynom $f \in k[X]$ in dem Ring $R/\mathfrak{a}$ die Nullstelle $X_f + \mathfrak{a}$ hat. (Argument wie im Beweis des Satzes 1.38 von Kronecker: f hat bereits in $R/(f(X_f))$ die Nullstelle $X_f + (f(X_f))$, die unter $R/(f(X_f)) \to R/\mathfrak{a}$ eine Nullstelle bleibt.)

Wir behaupten, dass $\mathfrak{a} \subsetneq R$. Sonst gibt es eine Gleichung

$$1 = \sum_{i=1}^{n} p_i f_i(X_{f_i}) \text{ in } R \tag{1.3}$$

mit $f_i \in k[X] \setminus k$ und $p_i \in R$; wir können und werden annehmen, dass die $f_1, f_2, \ldots, f_n$ paarweise verschieden sind. Iteriertes Anwenden des Satzes 1.38 von Kronecker liefert einen Oberkörper L von k, in dem jedes f_i eine Nullstelle a_i hat. Sei $\rho : R \to L$ der eindeutige Ringhomomorphismus, der



kommutativ macht und X_{f_i} auf a_i (für $1 \leq i \leq n$) und alle anderen X_f auf Null abbildet[17]. Wenden wir ρ auf (1.3) an, so beweist der Widerspruch

$$\begin{aligned} 1 = \rho(1) &= \sum_{i=1}^{n} \rho(p_i) f_i(\rho(X_{f_i})) \\ &= \sum_{i=1}^{n} \rho(p_i) f_i(a_i) \\ &= 0 \end{aligned}$$

unsere Behauptung.

Sei $\mathfrak{m} \subset R$ ein maximales Ideal, dass $\mathfrak{a}$ enthält (Zornsches Lemma). Dann ist die Verknüpfung

$$k \hookrightarrow R \twoheadrightarrow R/\mathfrak{m} =: k_1$$

injektiv als Homomorphismus von Körpern, und jedes nichtkonstante Polynom $f \in k[X]$ hat in k_1 eine Nullstelle (nämlich $X_f + \mathfrak{m}$). Wir fassen k_1 als Oberkörper von k auf. Wegen

$$k_1 = k(\{X_f + \mathfrak{m} \mid f \in k[X] \setminus k\}),$$

ist die Körpererweiterung $k \subset k_1$ algebraisch (Korollar 1.17).

Wendet man dasselbe Verfahren auf k_1 an, so erhält man eine algebraische Körpererweiterung $k_1 \subset k_2$, und jedes nichtkonstante Polynom aus $k_1[X]$ hat eine Nullstelle in k_2.

Weitere Iteration liefert eine aufsteigende Folge von Körpern

$$k \subset k_1 \subset k_2 \subset k_3 \subset \ldots.$$

Ihre Vereinigung $K = \bigcup_{i \in \mathbb{N}} k_i$ ist ein Oberkörper von k, die Körpererweiterung $k \subset K$ ist algebraisch, und jedes nichtkonstante Polynom $f \in K[X]$ hat eine Nullstelle in K: die endlich vielen Koeffizienten von f liegen in einem geeigneten k_i, also $f \in k_i[X]$, und somit hat f ein Nullstelle in k_{i+1}; also ist K ein algebraischer Abschluss von k. □

Remark 1.47. Es gilt $k_1 = K$, wie aus Aufgabe 1.96 folgt.

Wir werden im folgenden zeigen, dass ein algebraischer Abschluss eindeutig ist bis auf (uneindeutige) Isomorphie.

[17] Man könnte jedes „andere“ X_f auch auf ein beliebiges Element in L abbilden.

Dazu studiere das Problem der Fortsetzbarkeit von Körpermorphismen $k \to L$ auf algebraische Erweiterungen $k \subset K$. Dies ist auch für später relevant (für Charakterisierung separabler Erweiterungen als auch für Galoistheorie).

Notation: Sei $\sigma : K \to L$ ein Körpermorphismus. Induziert Morphismus von Ringen

$$K[X] \to L[X], \quad f \mapsto f^\sigma.$$

Klar: Ist $a \in K$ Nullstelle von f, so ist $\sigma(a)$ Nullstelle von f^σ. (Explizit: $f = \sum c_i X^i$. Aus $0 = f(a) = \sum c_i a^i$ folgt $0 = \sum \sigma(c_i)\sigma(a)^i = f^\sigma(\sigma(a))$.)

Theorem 1.48 (Fortsetzungssatz für einfache algebraische Körpererweiterungen)**.** *Sei $k \subset K = k(a)$ eine einfache algebraische Erweiterung. Sei $f = \min_{a/k}$. Sei $\sigma : k \to L$ ein Körpermorphismus.*

(a) Für jeden Morphismus $\widetilde{\sigma} : K \to L$ von Körpern, der σ fortsetzt, ist $\widetilde{\sigma}(a)$ eine Nullstelle von f^σ.

(b) Ist umgekehrt $b \in L$ eine Nullstelle von $f^\sigma \in L[X]$, so existiert genau eine Fortsetzung $\widetilde{\sigma}$ von σ mit $\widetilde{\sigma}(a) = b$.

Also ist

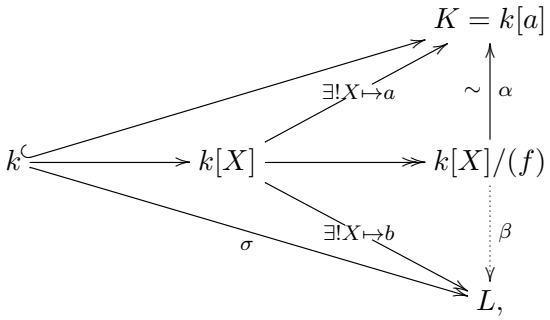
$$\{\text{Fortsetzungen } K \to L \text{ von } \sigma\} \xrightarrow{\sim} \{b \in L \mid (\min_{a/k})^\sigma(b) = 0\}, \quad \widetilde{\sigma} \mapsto \widetilde{\sigma}(a), \tag{1.4}$$

bijektiv. (Später (vielleicht bereits in Rot?): Linke Seite ist $\mathrm{Hom}_k(K, L)$, wobei man $\sigma : k \to L$ als Körpererweiterung auffasse.) (rechts will eigentlich σ als Index weglassen).

Insbesondere ist die Anzahl der verschiedenen Fortsetzungen von σ gleich der Anzahl der verschiedenen Nullstellen von f^σ (also $\leq \deg(f)$).

Proof. (a): Bereits klar (da $f^\sigma = f^{\widetilde{\sigma}}$).

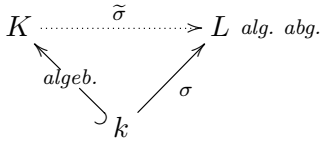
(b). Eindeutigkeit klar, weil a die Erweiterung erzeugt ($K = k(a)$, sogar $= k[a]$). Existenz: Betrachte das kommutative Diagramm



in dem β existiert, da $k[X] \to L$ gegeben ist durch $g \mapsto g^\sigma(b)$. Setze $\widetilde{\sigma} = \beta \circ \alpha^{-1}$ und teste, dass Fortsetzung. □

Theorem 1.49 (Allgemeiner Fortsetzungssatz für algebraische Erweiterungen)**.** *Sei $k \subset K$ algebraisch und sei $\sigma : k \to L$ ein Morphismus von Körpern,*

mit L algebraisch abgeschlossen. Dann läßt sich σ zu $\widetilde{\sigma} : K \to L$ fortsetzen:



Falls zusätzlich K algebraisch abgeschlossen ist und $L/\sigma(k)$ algebraisch ist, so ist jede Fortsetzung $\widetilde{\sigma}$ ein Isomorphismus.

Proof. Der Beweis beruht auf dem Zornschen Lemma. Wir betrachten die Menge

$$\mathcal{M} := \{(K', \sigma') \mid K' \text{ Zwischenkörper von } k \subset K \text{ und } \sigma' : K' \to L \text{ mit } \sigma'|_k = \sigma\}.$$

Diese Menge ist partiell geordnet bezüglich der Relation

$$(K', \sigma') \leq (K'', \sigma'') \quad :\Leftrightarrow \quad K' \subset K'' \text{ und } \sigma''|_{K'} = \sigma'.$$

und nichtleer. Jede total geordnete Teilmenge (oder aufsteigende Kette von Elementen) von $\mathcal{M}$ hat eine obere Schranke. Also enthält $\mathcal{M}$ ein maximales Element (K_0, σ_0). Falls $K_0 \subsetneq K$, existiert ein $a \in K \setminus K_0$. Da a algebraisch über K_0 ist und L algebraisch abgeschlossen, können wir σ_0 ausdehnen zu $\widetilde{\sigma}_0 : K_0[a] = K_0(a) \to L$ (nach Satz 1.48, weil $(\min_{a/K_0})^{\sigma_0}$ eine Nullstelle in L hat). Dies ist ein Widerspruch zur Maximalität. Es folgt $K = K_0$.

Sei nun $\widetilde{\sigma} : K \to L$ ein solche Fortsetzung. Seien K algebraisch abgeschlossen und $L/\sigma(k)$ algebraisch. Dann ist $\widetilde{\sigma}(K)$ algebraisch abgeschlossen und $\widetilde{\sigma}(K) \subset L$ eine algebraische Erweiterung. Dies impliziert $\widetilde{\sigma}(K) = L$. Also ist $\widetilde{\sigma}$ surjektiv und damit bijektiv. □

Definition 1.50. Seien $k \subset L$ und $k \subset M$ Körpererweiterungen (oder etwas allgemeiner (injektive) Morphismen von Körpern). Ein **k-Morphismus** $L \to M$ ist ein Morphismus von Körpern $\tau : L \to M$ der $\mathrm{id}_k : k \to k$ fortsetzt (d. h. $\tau|_k = \mathrm{id}_k$), d. h. das „Diagramm“

$$\begin{array}{ccc} L & \xrightarrow{\tau} & M \\ \cup & & \cup \\ k & = & k \end{array}$$

kommutiert. (Vgl. Morphismus von k-Algebren.) Ein solches τ heißt **k-Isomorphismus**, falls τ bijektiv ist.

$\mathrm{Hom}_k(L, M) :=$ Menge der k-Morphismen $L \to M$.

$\mathrm{End}_k(L) := \mathrm{Hom}_k(L, L) =$ Menge der k-Endomorphismen von L.

Ein k-Endomorphismus, der bijektiv ist, heißt k-Automorphismus.

$\mathrm{Aut}_k(L) :=$ Menge der k-Automorphismen von L.

Kann k-Morphismen verknüpfen. Es ist τ ein k-Isomorphismus, falls ein k-Morphismus $\sigma : M \to L$ mit $\sigma\tau = \mathrm{id}_L$ und $\tau\sigma = \mathrm{id}_M$ existiert.

Remark 1.51. Nun kann linke Seite in (1.4) umschreiben zu $\mathrm{Hom}_k(K, L)$, wobei man den (injektiven) Morphismus $\sigma : k \to L$ als Körpererweiterung auffasse.

Corollary 1.52. *Der algebraische Abschluss eines Körpers ist eindeutig bis auf (im Allgemeinen nicht eindeutigen) k-Isomorphismus: Sind $k \subset K$ und $k \subset K'$ algebraische Abschlüsse eines Körpers k, so existiert ein k-Isomorphismus $\tau : K \xrightarrow{\sim} K'$.*

Proof. Folgt direkt aus dem obigen Satz für σ die Inklusion $k \subset K'$.

Beispiel für die Nichteindeutigkeit: Betrachte $k = \mathbb{R}$ und $K = K' = \mathbb{C}$. Dann kann für τ die Identität oder die komplexe Konjugation nehmen. □

Ende 6. Vorlesung Montag 23. April 2012.

1.5. **Zerfällungskörper und normale Erweiterungen.** Sei k ein Körper.

Corollary 1.53 (zum Satz von Kronecker)**.** *Sei $f \in k[X]$. Dann existiert eine endliche Erweiterung K/k, so dass f in $K[X]$ in Linearfaktoren zerfällt.*

Proof. 1. Beweis. Induktion über $\deg(f)$. Der Fall $\deg(f) \leq 1$ ist trivial. Gelte $\deg(f) > 1$. Nach dem Satz 1.38 von Kronecker gibt es eine endliche Körpererweiterung $k \subset K'$ so dass f eine Nullstelle $a \in K'$ hat. Dann gilt $f = (X - a)g$ in $K'[X]$. Da $\deg(g) < \deg(f)$ gibt es per Induktion eine endliche Erweiterung $K' \subset K$ so dass g in $K[X]$ in Linearfaktoren zerfällt. Dann zerfällt auch f in $K[X]$ in Linearfaktoren, und $k \subset K$ ist endlich.

2. Beweis: Sei $k \subset \overline{k}$ ein algebraischer Abschluss von k. Seien $a_1, \ldots, a_n \in \overline{k}$ die Nullstellen von f. Dann ist $k \subset K := k(a_1, \ldots, a_n)$ endliche Erweiterung, und f zerfällt in $K[X]$ in Linearfaktoren. □

Definition 1.54. Sei $f \in k[X]$. Ein **Zerfällungskörper von** f [18] ist eine Erweiterung K/k mit folgenden Eigenschaften:

(a) f zerfällt in $K[X]$ in Linearfaktoren, d. h.

$$f = c(X - a_1) \ldots (X - a_n)$$

mit $c \in K$ und $a_1, \ldots, a_n \in K$.

(b) die Körpererweiterung $k \subset K$ wird von den Nullstellen von f (in K) erzeugt[19], d. h. $K = k(a_1, \ldots, a_n)$.

Remark 1.55. Ein Zerfällungskörper K von $f \in k[X]$ ist minimal mit der Eigenschaft, dass f in $K[X]$ in Linearfaktoren zerfällt: Gilt (a), so ist (b) äquivalent zu der folgenden Bedingung (b').

(b') Kein Zwischenkörper $k \subset E \subsetneq K$ hat die Eigenschaft, dass f in $E[X]$ in Linearfaktoren zerfällt.

[18] besser wäre wohl **minimaler Zerfällungskörper von** f.

[19] besser? der Körper K wird über k von den Nullstellen von f (in K) erzeugt

Proof. Seien wie oben $a_1, \dots, a_n$ die Nullstellen von f in K. Gelte $K = k(a_1, \dots, a_n)$. Ist $k \subset E \subset K$ Zwischenkörper, so dass f in $E[X]$ zerfällt, so folgt $a_i \in E$ für alle i, also $K = k(a_1, a_2, \dots, a_n) \subset E$, also $E = K$. Umgekehrt gebe es kein solches $k \subset E \subsetneq K$. Da $k(a_1, \dots, a_n)$ diese Eigenschaft hat und Zwischenkörper ist, muss $k(a_1, \dots, a_n) = K$ gelten. □

Definition 1.56. Allgemeiner: Ist $\mathcal{F} = (f_i)_{i \in I}$ eine Familie von Elementen von $k[X]$. Ein **Zerfällungskörper von** $\mathcal{F}$ ist eine Erweiterung K/k mit folgenden Eigenschaften:

(a) Alle f_i zerfallen in $K[X]$ in Linearfaktoren,

$$f_i = c_i \prod_{j \in J_i} (X - a_j^{(i)}).$$

(b) Die Körpererweiterung $k \subset K$ wird von den Nullstellen der f_i (in K) erzeugt, d. h. $K = k(a_j^{(i)} \mid i \in I, j \in J_i)$.

Falls (a) gilt, so ist analog zu oben (b) äquivalent zur Bedingung, dass es keinen Zwischenkörper $k \subset E \subsetneq K$ gibt so dass alle f_i in $E[X]$ in Linearfaktoren zerfallen.

Ist K ein Zerfällungskörper von f (oder $\mathcal{F}$), so ist $k \subset K$ eine algebraische Erweiterung (nach Korollar 1.17).

Falls $\mathcal{F}$ endlich ist, so ist ein Zerfällungskörper von $\mathcal{F}$ dasselbe wie ein Zerfällungskörper von $\prod_{i \in I} f_i$.

Lemma 1.57. *Sind K_1 und K_2 zwei Zerfällungskörper von $\mathcal{F}$, die in einem gemeinsamen Oberkörper L von k enthalten sind, so gilt $K_1 = K_2$.*

Proof. Sei

$$N = \{a \in L \mid \exists i \in I : f_i(a) = 0\}$$

die Menge[20] der Nullstellen der f_i in L. Sie stimmt überein mit der Menge der Nullstellen der f_i in K_1, da jedes f_i in K_1 in Linearfaktoren zerfällt. Analog für K_2. Also $K_1 = k(N) = K_2$. □

Theorem 1.58. *Sei $\mathcal{F} = (f_i)_{i \in I}$ eine Familie in $k[X]$. Dann existiert ein Zerfällungskörper von $\mathcal{F}$, und er ist eindeutig bis auf (im Allgemeinen uneindeutigen) k-Isomorphismus.*

Genauer:

(a) Existenz: Sei $k \subset L$ eine Körpererweiterung, so dass jedes f_i in $L[X]$ in Linearfaktoren zerfällt (z. B. könnte L der algebraische Abschluss von k sein). Ist N die Menge der Nullstellen der f_i in L, so ist $k(N)$ ein Zerfällungskörper von $\mathcal{F}$.

[20] Genauer meinen wir hier und im Folgenden stets die Vereinigung der Menge der Nullstellen der f_i; wenn wir den Schnitt meinen, ist es wohl sinnvoll, von der Menge der gemeinsamen Nullstellen zu sprechen.

(b) *Eindeutigkeit: Sind K_1 und K_2 Zerfällungskörper von $\mathcal{F}$, so induziert jeder k-Isomorphismus*

$$\sigma : \overline{K_1} \xrightarrow{\sim} \overline{K_2}$$

zwischen algebraischen Abschlüssen von K_1 und K_2 einen k-Isomorphismus

$$\sigma : K_1 \xrightarrow{\sim} K_2$$

Proof. Existenz: Klar.

Eindeutigkeit: Sei $\sigma : \overline{K_1} \xrightarrow{\sim} \overline{K_2}$ ein k-Isomorphismus wie oben (existiert wegen Satz 1.46 und Korollar 1.52 (jedes $\overline{K_i}$ ist auch algebraischer Abschluss von k)).

Sei zunächst $\mathcal{F}$ endlich. Sei $f = \prod_{i\in I} f_i \in k[X]$. Da sich der Zerfällungskörper nicht ändert, wenn wir f mit einem Element von $k - \{0\}$ multiplizieren, können wir annehmen, dass f normiert ist. Sei $\deg(f) = n$ und seien $a_1, a_2, \ldots, a_n \in K_1$ bzw. $b_1, b_2, \ldots, b_n \in K_2$ die Nullstellen von f mit Vielfachheiten. Aus $f \in k[X] \subset \overline{K_1}[X]$ folgt $f = f^\sigma \in \overline{K_2}[X]$. Also

$$\prod_{i=1}^{n}(X - b_i) = f = f^\sigma = \Big(\prod_{i=1}^{n}(X - a_i)\Big)^\sigma = \prod_{i=1}^{n}(X - \sigma(a_i)) \in K_2[X].$$

Also induziert σ eine Bijektion

$$\sigma : \{a_1, \ldots, a_n\} \xrightarrow{\sim} \{b_1, \ldots, b_n\}.$$

Es folgt

$$\sigma(k(a_1, \ldots, a_n)) = k(\sigma(a_1), \ldots, \sigma(a_n)) = k(b_1, \ldots, b_n),$$

und somit induziert $\sigma : \overline{K_1} \xrightarrow{\sim} \overline{K_2}$ einen Isomorphismus

$$\sigma : K_1 = k(a_1, \ldots, a_n) \xrightarrow{\sim} k(b_1, \ldots, b_n) = K_2.$$

Im allgemeinen Fall verwende man, dass K_1 und K_2 die Vereinigung der Zerfällungskörper aller endlichen Teilfamilien von $\mathcal{F}$ sind (das zeigt Surjektivität; Injektivität entweder da Körpermorphismus oder da endliche Teilfamilien gerichtetes System).

□

Examples 1.59. (a) Der Zerfällungskörper von $f(X) = X^n - 1 \in \mathbb{Q}[X]$, für $n \in \mathbb{N}$.

Sei $\zeta = \zeta_n = e^{2\pi i/n} \in \mathbb{C}$. Dann sind

$$1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$$

n verschiedene Nullstellen von f. Also

$$f = (X - 1)(X - \zeta)\ldots(X - \zeta^{n-1}) \in \mathbb{C}[X].$$

Also ist $\mathbb{Q}(\zeta_n)$ ein Zerfällungskörper von $X^n - 1$.

(Kreisteilungskörper, Grad wird später bestimmt, regelmäßiges n-Eck.)

(b) Der Zerfällungskörper von $X^3 - 2 \in \mathbb{Q}[X]$. Sei $\alpha = \sqrt[3]{2} \in \mathbb{R}$. Dann gilt

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

Quadratische Ergänzung: $X^2 + \alpha X + \alpha^2 = (X + \frac{\alpha}{2})^2 + \frac{3}{4}\alpha^2$. Also hat $X^2 + \alpha X + \alpha^2 = 0$ die beiden Lösungen

$$-\frac{\alpha}{2} \pm \frac{i\sqrt{3}}{2}\alpha.$$

Es folgt

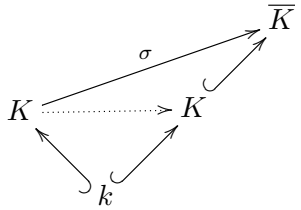
$$X^3 - 2 = (X - \alpha)(X + \frac{\alpha}{2} - \frac{i\sqrt{3}}{2}\alpha)(X + \frac{\alpha}{2} + \frac{i\sqrt{3}}{2}\alpha).$$

Somit ist $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ ein Zerfällungskörper von $X^3 - 2$. Da $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ (siehe oben, Eisenstein) und $[\mathbb{Q}(i\sqrt{3}) : \mathbb{Q}] = 2$ folgt sofort

$$[\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q}] = 6.$$

Theorem-Definition 1.60. *Sei $k \subset K$ eine algebraische Körpererweiterung. Dann sind äquivalent:*

(a) Jeder k-Morphismus $\sigma : K \to \overline{K}$ in einen algebraischen Abschluss $\overline{K}$ von K erfüllt $\sigma(K) = K$, induziert also einen k-Automorphismus von K. Im Bild (am Rand, illustriert diese und die nächste Bedingung):



(b) Jeder k-Morphismus $\sigma : K \to \overline{K}$ in einen algebraischen Abschluss von K erfüllt $\sigma(K) \subset K$.

(c) Jedes irreduzible Polynom aus $k[X]$, das in K eine Nullstelle hat, zerfällt in $K[X]$ in Linearfaktoren.[21]

(d) K ist Zerfällungskörper einer Familie(/Menge?) von Polynomen in $k[X]$.[22]

Eine Körpererweiterung K/k heißt ***normal***[23]*, wenn sie algebraisch ist und diese Bedingungen erfüllt.*

---

[21] Äquivalent (per Normieren): Alle Minimalpolynome über k von Elementen $a \in K$ zerfallen in $K[X]$ in Linearfaktoren.

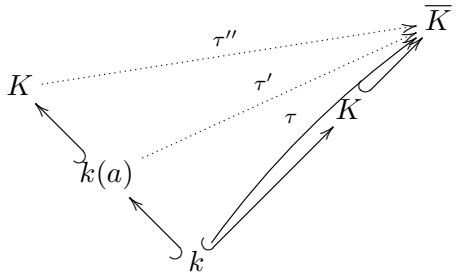
[22] Man kann z.B. die Minimalpolynome über k aller Elemente von K nehmen.

Das hat den Vorteil, dass dann jedes Element von K Nullstelle eine Polynoms in der Familie/Menge ist.

[23] Normal zu sein ist aber für eine Körpererweiterung etwas Besonderes.

Proof. (a) ⇒ (b) ist trivial.

(b) ⇒ (c): Sei $f \in k[X]$ irreduzibel und $a \in K$ eine Nullstelle von f. Wir können annehmen, dass f normiert ist; somit ist f das Minimalpolynom von a über k. Sei $\overline{K}$ ein algebraischer Abschluss von K. Dann zerfällt f in $\overline{K}[X]$ in Linearfaktoren. Also genügt es zu zeigen, dass jede Nullstelle $b \in \overline{K}$ von f bereits in K liegt.



Nach Satz 1.48 (Fortsetzungssatz für einfache algebraische Körpererweiterungen) lässt sich $\tau : k \subset \overline{K}$ eindeutig zu $\tau' : k(a) \to \overline{K}$ mit $\tau'(a) = b$ fortsetzen, und dieses τ' läßt sich nach Satz 1.49 (Allgemeiner Fortsetzungssatz) fortsetzen zu $\tau'' : K \to \overline{K}$. Die Annahme besagt nun, dass $b = \tau''(a) \in \tau''(K) \subset K$.

(c) ⇒ (d): Sei $K = k(a_i; i \in I)$ für geeignete $a_i \in K$ (es kann etwa a_i alle Elemente von K durchlaufen). Sei $f_i = \min_{a_i/k}$. Laut Annahme zerfällt f_i in $K[X]$ in Linearfaktoren. Also ist K ein Zerfällungskörper von $(f_i)_{i\in I}$.

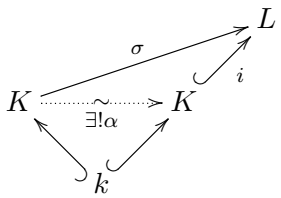
(d) ⇒ (a): Sei $\sigma : K \to \overline{K}$ ein k-Morphismus in einen algebraischen Abschluss von K. Sei K Zerfällungskörper einer Familie $\mathcal{F} = (f_i)_{i\in I}$ von Polynomen in $k[X]$. Dann ist $\sigma(K)$ Zerfällungskörper der Familie $\mathcal{F}^\sigma := (f_i^\sigma)_{i\in I} = \mathcal{F}$. Die beiden Zerfällungskörper K und $\sigma(K)$ von $\mathcal{F}$ liegen in dem gemeinsamen Oberkörper $\overline{K}$ und sind somit bereits gleich nach Lemma 1.57. □

Ende 7. Vorlesung Donnerstag 26. April 2012

Corollary 1.61. *Seien $k \subset K \subset L$ Erweiterungen, mit $k \subset K$ normal. Sei $i : K \hookrightarrow L$ die Inklusion. Jeder k-Morphismus $\sigma : K \to L$ ist von der Form*

$$\sigma = i \circ \alpha$$

für ein eindeutiges $\alpha \in \mathrm{Aut}_k(K)$.



Proof. Da σ notwendig K nach $L_{\mathrm{alg}/K} = L_{\mathrm{alg}/k}$ abbildet, können wir ohne Einschränkung annehmen (ersetze L durch $L_{\mathrm{alg}/k}$), dass L/K algebraisch

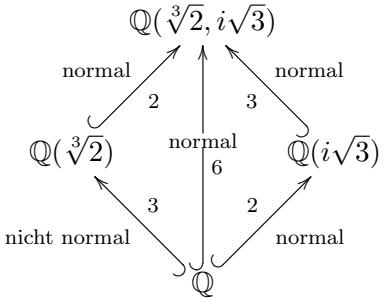
ist. Sei $\overline{L}$ ein algebraischer Abschluss von L, und damit auch von K. Die Behauptung folgt nun aus der Definition: Wende (a) in Satz-Definition 1.60 an auf die Komposition $K \xrightarrow{\sigma} L \subset \overline{L}$. □

Example 1.62.

(a) Ist $\overline{k}$ ein algebraischer Abschluss von k, so ist $k \subset \overline{k}$ normal.

(b) Jede quadratische (:= Grad 2 laut englischer Wikipedia) Erweiterung $k \subset K$ ist normal: Ist $f \in k[X]$ irreduzibel mit Nullstelle $a \in K$, so ist f (bis auf Einheit) das Minimalpolynom von a, insbesondere $\deg(f) \leq 2$. Ein lineares oder quadratisches Polynom mit einer Nullstelle zerfällt aber bereits in Linearfaktoren.

(c) Wir betrachten erneut Beispiel 1.59 (b).



(d) Also (aus (c)): Kubische (:= Grad 3) Erweiterungen sind nicht notwendig normal (können aber normal sein).

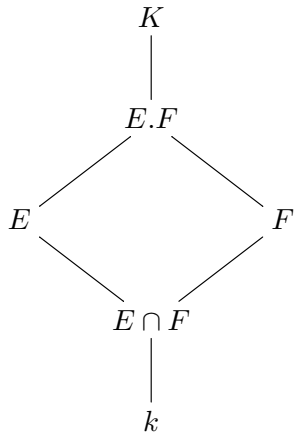
(e) Seien $k \subset F \subset K$ Körpererweiterungen. Ist $k \subset K$ normal, so auch $F \subset K$ (einfach: kann jedes der Kriterien aus Satz-Definition 1.60 anwenden; folgt auch aus Satz 1.63 (b) unten), aber nicht $k \subset E$ im Allgemeinen (siehe (c)).

(f) Normalität ist nicht transitiv:

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[2]{2}) \subset \mathbb{Q}(\sqrt[4]{2})$$

Beide Teilerweiterungen quadratisch, aber das Minimalpolynom $X^4 - 2$ von $\sqrt[4]{2}$ über $\mathbb{Q}$ (Eisenstein) hat Nullstelle $i\sqrt[4]{2} \notin \mathbb{R}$, kann also nicht über $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$ zerfallen.

Theorem 1.63. *Sei $k \subset K$ eine Körpererweiterung mit Zwischenkörpern E und F.*



Dann gelten:

(a) E/k normal $\Rightarrow$ $E.F/F$ normal.
(b) K/k normal $\Rightarrow$ K/F normal. (Braucht nur $k \subset F \subset K$.)
(c) E/k und F/k normal $\Rightarrow$ (i) $E \cap F/k$ normal und (ii) $E.F/k$ normal.

Proof. Für die Algebraizität der angegebene Erweiterungen siehe Satz 1.22.

(a): Per Zerfällungskörper-Kriterium (Satz 1.60 (d)). Sei E Zerfällungskörper einer Familie $\mathcal{F}$ in $k[X]$. Dann ist $E.F$ Zerfällungskörper von $\mathcal{F}$, nun aufgefaßt als Familie in $F[X]$: Alle Polynome zerfallen bereits in E in Linearfaktoren. Bezeichnet N die Menge der Nullstellen der Elemente (Mitglieder?) von $\mathcal{F}$ (kann $\mathcal{F}$ so wählen, dass $N = E$), so gilt $E = k(N)$. Es folgt $E.F = F(E) = F(N)$.

(b): Ist Spezialfall von (a) für $E = K$.

(c): (i) Per Nullstellen irreduzibler Polynome (Satz 1.60 (c)). Sei $p \in k[X]$ irreduzibel, mit Nullstelle $a \in E \cap F$. Da E/k und F/k normal, liegen alle Nullstellen in E und in F, also in $E \cap F$. Also zerfällt p über $E \cap F$ in Linearfaktoren. Somit ist $E \cap F/k$ normal.

(ii) Per Zerfällungskörper. Sei E Zerfällungskörper einer Familie $\mathcal{E}$ in $k[X]$, und sei M die Menge der Nullstellen der Elemente von $\mathcal{E}$. Also $E = k(M)$.

Analog sei F Zerfällungskörper von $\mathcal{F}$ in $k[X]$ mit Nullstellen N. Also $F = k(N)$.

Dann ist $E.F$ Zerfällungskörper von $\mathcal{E} \cup \mathcal{F}$: Alle Elemente von $\mathcal{E} \cup \mathcal{F}$ zerfallen in $E.F$, und es gilt $E.F = E(N) = k(M \cup N)$. □

Definition 1.64. Sei K/k algebraisch Eine **normale Hülle von** K/k (oder ein **Normalkörper von** K/k, english: **normal closure**) ist ein Erweiterungskörper N von K, so dass N/k normal ist, aber kein Zwischenkörper von $K \subset E \subsetneq N$ normal über k ist.

Theorem 1.65.

(a) Existenz: Jede algebraische Erweiterung K/k besitzt eine normale Hülle N . Ist K/k endlich, so auch N/k.

Genauer: Ist L/K eine (notwendig algebraische) Körpererweiterung, so dass L/k normal ist, so existiert genau eine normale Hülle N von K/k mit $N \subset L$. Falls $K = k(A)$ für $A \subset K$ eine Teilmenge (etwa $A = K$), so gilt

$$N = k(\textit{Nullstellen der } \min_{a/k} \textit{ in } L, \textit{ für } a \in A). \tag{1.5}$$

*Man bezeichnet dann N auch als die **normale Hülle von** K/k **in** L.*

(b) Eindeutigkeit: Falls N_1 und N_2 zwei normalen Hüllen von K/k sind, so existiert ein K-Isomorphismus $\sigma : N_1 \xrightarrow{\sim} N_2$.

Example 1.66. In Beispiel 1.62 (c) ist $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ eine normale Hülle von $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$.

Proof. (a): Sei $K \subset L$ mit $k \subset L$ normal (etwa L ein algebraischer Abschluss von K (und damit von k)).

Eindeutigkeit der normalen Hülle in L: Seien N, N' normale Hüllen von K/k, die beide in L enthalten sind. Dann ist $N \cap N'$ normal über k (Satz 1.63, (c)), und Zwischenkörper von $K \subset N$ und $K \subset N'$. Also $N = N \cap N' = N'$.

Existenz der normalen Hülle in L: Sei $A \subset K$ mit $K = k(A)$ und sei $\mathcal{F} = (f_a := \min_{a/k})_{a \in A}$. Dann zerfallen alle f_a in L in Linearfaktoren (da irreduzibel in $k[X]$ und L/k normal). Sei S die Menge der Nullstellen der f_a in L. Somit ist $k(S)$ der Zerfällungskörper von $\mathcal{F}$ über k (Satz 1.58 über den Zerfällungskörper), also normal über k.

Behauptung: $k(S)$ ist eine normale Hülle von K/k.

Aus $A \subset S$ folgt $K = k(A) \subset k(S)$. Sei $K \subset E \subset k(S)$ ein Zwischenkörper mit $k \subset E$ normal. Da jedes (irreduzible) $f_a \in k[X]$ die Nullstelle $a \in K \subset E$ hat, zerfällt es in Linearfaktoren in $E[X]$. Also $S \subset E$ und damit $k(S) \subset E$. Also $E = k(S)$.

Ist K/k endlich, so kann A endlich wählen. Dann besteht S aus endlich vielen über k algebraischen Elementen, und somit ist $k \subset k(S)$ endlich.

(b): Seien N_1 und N_2 zwei normale Hüllen von K/k. Sei $\overline{N}_i$ ein algebraischer Abschluss von N_i (und damit von K). Nach obigem ist N_i (der) Zerfällungskörper von $\mathcal{F}$ (in $\overline{N}_i$) über k und auch über K. Sei $\sigma : \overline{N}_1 \to \overline{N}_2$ ein K-Isomorphismus. Nach Satz 1.58 über den Zerfällungskörper restringiert σ zu dem gesuchten K-Isomorphismus. □

Remark 1.67. [24] In der Situation (a) von Satz 1.65 kann man N auch beschreiben als

$$N = k(\sigma(K); \sigma \in \operatorname{Hom}_k(K, L)). \tag{1.6}$$

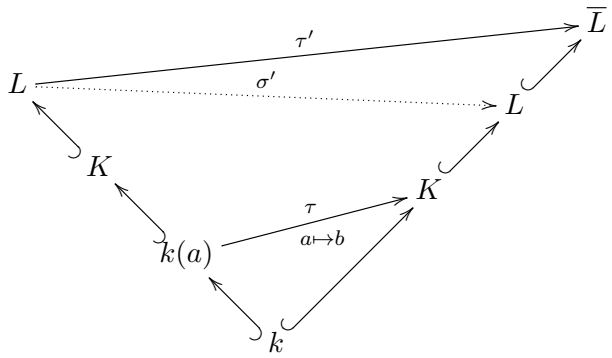
[24] Nicht in Vorlesung gemacht. Sollte es aber machen! Musste zwei workarounds machen später!

Proof. Wir zeigen (1.6). In der Notation des obigen Beweises sei $A = K$, und S damit die Menge der Nullstellen der Minimalpolynome der Elemente von K. Es genügt zu zeigen, dass

$$S = \{\sigma(K) \mid \sigma \in \mathrm{Hom}_k(K, L)\}.$$

Inklusion $\supset$: Ist $a \in K$, so ist a Nullstelle von f_a, und $\sigma(a)$ ist Nullstelle von $(f_a)^\sigma = f_a$, also $\sigma(a) \in S$.

Inklusion $\subset$: Sei $b \in S$. Dann ist b Nullstelle eines f_a, für ein $a \in K$. Im Diagramm



finde τ mit $\tau(a) = b$ (Fortsetzungssatz 1.48 für einfache algebraische Körpererweiterungen) und dann τ' (Allgemeiner Forsetzungsatz 1.49), so dass dieses Diagramm kommutiert. Da $k \subset L$ normal ist, faktorisiert τ' zu dem gestrichelten σ', so dass das Diagramm kommutativ bleibt. Sei $\sigma := \sigma'|_K \in \mathrm{Hom}_k(K, L)$. Dann $b = \tau(a) = \sigma(a) \in \sigma(K)$. □

Ende 8. Vorlesung Montag 30. April 2012

1.6. **Separable Erweiterungen.** Sei k ein Körper und $\overline{k}$ ein algebraischer Abschluss.

Motivation: Satz 1.48 besagt: Ist $a \in \overline{k}$ (algebraisch über k) mit Minimalpolynom f, so gilt

$$\mathrm{Hom}_k(k(a), \overline{k}) \xrightarrow{\sim} \{b \in \overline{k} \mid f(b) = 0\}. \tag{1.7}$$

Deswegen studiere: Wieviele **verschiedene** Nullstellen kann ein irreduzibles Polynom vom Grad n in $\overline{k}$ haben?

Definition 1.68. Sei $f \in k[X]$ und $a \in \overline{k}$. Falls $f \neq 0$, so habe

$$f = (X - a)^n g(X) \quad \text{in } \overline{k}[X]$$

für eindeutige $n \in \mathbb{N}$ und $g \in \overline{k}[X]$ mit $g(a) \neq 0$. Falls $f = 0$ setze $n := \infty$. Dann heißt n die **Vielfachheit von f in a**, und a ist Nullstelle (bzw. **einfache Nullstelle** bzw. **mehrfache Nullstelle**) **von** f genau dann, wenn $n \geq 1$ (bzw. $n = 1$ bzw. $n \geq 2$).

Definition 1.69. (a) Ein Polynom $f \in k[X]$ heißt **separabel**, falls es in $\overline{k}$ nur einfache Nullstellen hat. Sonst **inseparabel**. [25] Unabhängig von $\overline{k}$ wegen Eindeutigkeit des algebraischen Abschlusses. [26]

(b) Sei $k \subset K$ eine algebraische Körpererweiterung und $a \in K$.[27] Dann heißt a **separabel** bzw. **inseparabel**, falls $\min_{a/k}$ es ist. (Für separabel äquivalent: a ist Nullstelle eines separablen Polynoms in $k[X]$.)

(c) Eine Körpererweiterung $k \subset K$ heißt **separabel**, falls sie algebraisch ist und alle Elemente von K separabel über k sind.

Theorem 1.70. *Sei $f \in k[X]$ irreduzibel.*

(a) Falls $\operatorname{char} k = 0$, so ist f separabel.

(b) Fall $\operatorname{char} k = p > 0$: Sei $r \in \mathbb{N}$ maximal so, dass f ein Polynom in X^{p^r} ist, d. h. dass es ein $g \in k[X]$ gibt mit $f(X) = g(X^{p^r})$. Dann ist g irreduzibel in $k[X]$ und separabel. Jede Nullstelle von f (in $\overline{k}$) hat die Vielfachheit p^r, und die Nullstellen von f sind die (eindeutigen) p^r-ten Wurzeln der Nullstellen von g.

Vergleiche Aufgabe 1.72, war in etwa Übungsaufgabe.

Brauchen Hilfsmittel: Erinnerung(?), (verallgemeinert Ableitung aus Analysis auf reellen oder komplexen Polynomen, aufgefaßt als Funktionen, zu Polynomringen über beliebigen Körpern): Formale Ableitung: Definiere

$$k[X] \to k[X],$$
$$f = \sum_{i=0}^{n} c_i X^i \mapsto f' := \sum_{i=1}^{n} i c_i X^i.$$

Ist k-linear und erfüllt $(fg)' = f'g + fg'$ (nachrechnen).

Lemma 1.71. *Sei $f \in k[X] \setminus k$. Nullstellen = Nullstellen in $\overline{k}$.*

(a) (Wie aus Analysis (Taylorentwicklung) zu erwarten:) Die mehrfachen Nullstellen von f stimmen überein mit den gemeinsamen Nullstellen von f und seiner Ableitung f', oder, äquivalent, mit den Nullstellen von $\operatorname{ggT}(f, f')$ (gebildet in $k[X]$).

(b) Ist f irreduzibel, so hat f genau dann eine mehrfache Nullstelle (= ist inseparabel), wenn $f' = 0$. (Und in diesem Fall sind alle Nullstellen mehrfach.)

---

[25] Nicht definiert: Es heißt **rein inseparabel**, falls es in $\overline{k}$ genau eine Nullstelle hat.

[26] Beobachtung: Hier und in obiger Definition kann statt $\overline{k}$ einen beliebigen Oberkörper von k nehmen, über dem f in Linearfaktoren zerfällt, etwa einen Zerfällungskörper. (In der ersten Definition hätte es sogar gereicht, dass a in einem Oberkörper von k liegt; oder gar $a \in k$.)

[27] reicht a algebraisch über k. Genau: Deswegen nächstes Mal besser eine beliebige Körpererweiterung $k \subset K$ nehmen und in Definition von a separabel Algebraizität verlangen!

Dies ist geschickter für das Schlüssellemma 2.1.

Proof. (a): Sei $a \in \overline{k}$. Dann

$$f = (X-a)^n g(X) \quad \text{in } \overline{k}[X]$$

für eindeutige $n \geq 0$ und $g \in \overline{k}[X]$ mit $g(a) \neq 0$. Dann

$$f' = n(X-a)^{n-1} g(X) + (X-a)^n g'(X).$$

Ist a mehrfache Nullstelle von f, so ist a Nullstelle von f und von f'.

Umgekehrt folgt aus $f(a) = 0$, dass $n \geq 1$. Für $n = 1$ gilt $f'(a) = g(a) \neq 0$. Also $n \geq 2$.

Sei d der ggT(f, f') gebildet in $k[X]$ (eindeutig bis auf Einheit in k). Da $k[X]$ ein Hauptidealring ist, ist d charakterisiert durch

$$d \cdot k[X] = f \cdot k[X] + f' \cdot k[X].$$

Dies impliziert

$$d \cdot \overline{k}[X] = f \cdot \overline{k}[X] + f' \cdot \overline{k}[X].$$

Somit ist d auch der ggT(f, f') gebildet in $\overline{k}[X]$.

Ist a Nullstelle von d, so ist a gemeinsame Nullstelle von f und f'. Ist a gemeinsame Nullstelle von f und f', so teilt $X - a$ sowohl f als auch f' (in $\overline{k}[X]$), also den ggT d. Also ist a Nullstelle von d.

(b) Ist $f' = 0$, so ist nach (a) jede Nullstelle von f eine mehrfache Nullstelle, und in $\overline{k}$ hat f ein Nullstelle. Sei umgekehrt $a \in \overline{k}$ eine mehrfache Nullstelle von f. Dann $f'(a) = 0$ nach (a). Da f (bis auf Normierung) das Minimalpolynom von a ist und $\deg(f') < \deg(f)$ folgt $f' = 0$ (sonst kann f' normieren und habe so normiertes Polynom mit Grad $< \deg(f)$, das a als Nullstelle hat; Widerspruch zu f Minimalpolynom). □

Beobachtung: Sei $f = \sum c_i X^i \in k[X]$. Aus $f' = 0$ folgt ic_i für alle $i \geq 1$.

- In Charakteristik 0 ist also $f' = 0$ äquivalent zu $f \in k$ (wie in Analysis).
- In Charakteristik p ist $f' = 0$ äquivalent zu $f = g(X^p)$ für ein $g \in k[X]$. (Nämlich $g = \sum c_{ip} X^i$.)

Beweis von Satz 1.70. (a): Ist f inseparabel, so $f' = 0$, und somit $f \in k$. Widerpruch.

(b): Sei $f = g(X^{p^r})$ wie im Satz.

Offensichtlich ist g irreduzibel ($g = ab$, so $f = a(X^{p^r})b(X^{p^r})$, damit a oder $b \in k$).

Falls g nicht separabel, so $g' = 0$, also $g = h(X^p)$ und somit $f = h((X^{p^r})^p) = h(X^{p^{r+1}})$ im Widerspruch zur Maximalität von r.

Erinnerung: Sei p eine Primzahl. Ist R ein Ring, in dem $p \cdot 1 = 0$ gilt (etwa k oder $k[X]$ für einen Körper k der Charakteristik p), so ist

$$\begin{aligned} R &\to R, \\ a &\mapsto a^p, \end{aligned}$$

ein Ringmorphismus, es gilt also $(a \pm b)^p = a^p \pm b^p$ (da $\binom{p|p}{i}$ für alle $1 \leq i \leq p-1$) Also ist auch $a \mapsto a^{p^r}$ ein Ringmorphismus (r-faches Anwenden). Für k einen Körper der Charakteristik p heißt

$$\begin{aligned} \mathrm{Fr} : k &\to k, \\ a &\mapsto a^p, \end{aligned}$$

der **Frobenius-(Homo)Morphismus** von k. Er ist stets injektiv. Insbesondere sind p^r-te Wurzeln in k, falls sie existieren, eindeutig.

Larsen hat den Frobenius-Morphismus mit φ abgekürzt.

In $\overline{k}[X]$ gilt

$$g(X) = (X - a_1) \dots (X - a_n)$$

für paarweise verschiedene a_i. Sei $c_i \in \overline{k}$ die p^r-te Wurzel aus a_i. Dann gilt

$$\begin{aligned} f(X) = g(X^{p^r}) &= (X^{p^r} - a_1) \dots (X^{p^r} - a_n) \\ &= (X^{p^r} - c_1^{p^r}) \dots (X^{p^r} - c_n^{p^r}) \\ &= (X - c_1)^{p^r} \dots (X - c_n)^{p^r}. \end{aligned}$$

□

Exercise 1.72. Sei k ein Körper der Charakteristik $p > 0$. Sei $g \in k[X]$ ein normiertes irreduzibles Polynom, so dass nicht alle Koeffizienten von g p-te Potenzen (in k) sind. Dann ist $g(X^p)$ irreduzibel (und normiert und inseparabel). (Per Induktion gilt dasselbe für alle $g(X^{p^r})$.

Umgekehrt ist jedes inseparable normierte irreduzible Polynom in $k[X]$ von dieser Form (für ein eindeutiges g). Lösung siehe 1.73.

Solution 1.73. Sei g wie in der Aufgabenstellung. Setze $f = g(X^p)$. Dies ist offensichtlich inseparabel, denn jede Nullstelle von g ist mindestens p-fache Nullstelle von f; alternativ berechne man $f' = g'(X^p)pX^{p-1} = 0$ und sieht so, dass jede Nullstelle von f bereits eine mehrfache Nullstelle ist.

Wir nehmen an, dass f nicht irreduzibel ist. **1. Fall:** In der Zerlegung in Primfaktoren von f kommen zwei verschiedene irreduzible Faktoren vor. Dann gilt $f = h_1 h_2$ für geeignete $h_1, h_2 \in k[X]$ mit h_1, h_2 teilerfremd nichtkonstant. Aus $0 = f' = h_1' h_2 + h_1 h_2'$ folgt $h_1 | h_1' h_2$, also $h_1 | h_1'$ und dann aus Gradgründen $h_1' = 0$. Dies bedeutet, dass $h_1 = \overline{h}_1(X^p)$ für ein $\overline{h}_1 \in k[X]$. Analog $h_2 = \overline{h}_2(X^p)$ für ein $\overline{h}_2 \in k[X]$. Aus $h(X^p) = h_1 h_2 = \overline{h}_1(X^p)\overline{h}_2(X^p)$ folgt $h = \overline{h}_1 \overline{h}_2$. Da h irreduzibel ist, ist ein $\overline{h}_i$ konstant, und damit auch h_i, im Widerspruch zur Annahme. Dieser Fall tritt also nicht ein. **1. Fall:** In der Zerlegung in Primfaktoren von f kommt genau ein irreduzible Faktor h vor. Ohne Einschränkung können wir annehmen, dass h normiert ist, und dann erhalten wir $f = h^m$ für ein $m \geq 1$ (da f normiert). Dann $0 = f' = mh^{m-1}h'$. Da $h^{m-1} \neq 0$ folgt $m = 0$ in k oder $h' = 0$. Falls $h' = 0$, so $h = \overline{h}(X^p)$ für ein $\overline{h} \in k[X]$, und dann $g(X^p) = f = h^m(X) = \overline{h}^m(X^p)$, also $g = \overline{h}^m$ und wegen der Irreduzibilität von g folgt $m = 1$. Also ist $f = h^1 = h$ irreduzibel und wir freuen uns. Sonst gilt $m = px$ in $\mathbb{Z}$ für ein $x \in \mathbb{N}$. Dann folgt $f = (h^x)^p$, und somit sind alle Koeffizienten von f p-te Potenzen. Diese stimmen aber mit den Koeffizienten von g überein, was einen Widerspruch liefert.

Sei umgekehrt $f \in k[X]$ inseparabel normiert und irreduzibel. Irreduzibel und inseparabel impliziert $f' = 0$, also $f = g(X^p)$ für ein eindeutiges $g \in k[X]$. Offenbar ist g normiert und irreduzibel, denn aus $g = ab$ folgt $g = a(X^p)b(X^p)$, als oE $a(X^p) \in k$ und damit $a \in k$. Sei $g = \sum_{i=0}^n c_i X^i$. Falls alle Koeffizienten von g p-Potenzen sind, so sei $a_i = \sqrt[p]{c_i}$ (eindeutig, da Frobenius als Körpermorphismus injektiv). Sei $H = \sum_{i=0}^n a_i X^i$. Dann gilt $H^p = \sum_{i=1}^n a_i^p (X^p)^i = g(X^p) = f$ im Widerspruch zur Irreduzibilität von f.

Definition 1.74. Ein Körper k heißt **perfekt** oder **vollkommen**, falls jede algebraische Erweiterung $k \subset K$ separabel ist.

Corollary 1.75. *Körper der Charakteristik* 0 *sind vollkommen.*

Proof. In Charakteristik Null ist jedes irreduzible Polynom separabel. □

Später: Endliche Körper sind vollkommen.

Exercise 1.76. Ein Körper k der Charakteristik $p > 0$ ist vollkommen genau dann, wenn $k^p = k$ (d. h. jedes Element von k hat eine p-te Wurzel in k), wenn also der Frobenius bijektiv ist.

Folgern Sie, dass endliche Körper vollkommen sind.

Beweis: Sei k vollkommen. Sei $b \in k$. Sei $a \in \overline{k}$ mit $a^p = b$. Da k vollkommen ist, ist $k \subset k(a)$ separabel. Also ist $f = \min_{a/k}$ separabel. Da a Nullstelle von $X^p - b$, ist f ein Teiler von von $X^p - b$. Da $X^p - b = (X - a)^p \in \overline{k}[X]$ und f separabel, folgt $f = X - a$. Also $a \in k$.

Gelte umgekehrt $k = k^p$. Sei $k \subset K$ eine algebraische Erweiterung. Sei $a \in K$. Sei $f = \min_{a/k}$. Sei $f = g(X^{p^r})$ wie oben mit maximalem r. Dann ist g separabel und irreduzibel. Sei $\overline{g}$ das Polynom, das aus g hervorgeht, indem man jeden Koeffizienten durch seine p^r-te Wurzel ersetzt. Dann $\overline{g}^{p^r} = g(X^{p^r}) = f$. Da f irreduzibel ist, folgt $p^r = 1$, also $r = 0$, und somit ist $f = g$ und somit separabel.

Example 1.77. Beispiel für eine nicht separable (ich vermeide „inseparabel“, um es nicht mit „rein inseparabel“ zu verwecheln) Erweiterung. (Muss in Charakteristik $p > 0$ sein und mit unendlichem Körper starten.)

Sei $k = \mathbb{F}_p(t)$ der Körper der rationalen Funktionen in t über $\mathbb{F}_p$. Dann ist $X^p - t \in k[X]$ irreduzibel (Übung 1.72, oder Eisenstein bezüglich $t \in \mathbb{F}_p[t]$ zeigt, dass $X^p - t$ irreduzibel in $\mathbb{F}_p[t][X]$ und damit auch in $k[X]$), und nicht separabel, den seine Ableitung verschwindet. Also ist

$$k \subset k[X]/(X^p - t)$$

eine nicht separable Erweiterung. Sie ist isomorph zu

$$\mathbb{F}_p(s^p) \subset \mathbb{F}_p(s)$$

per $t \mapsto s^p$, $X \mapsto s$ mit Inversem $s \mapsto X$. Obiges Polynom ist dann schlicht $X^p - s^p \in \mathbb{F}_p(s^p)[X]$, und zerfällt in $\mathbb{F}_p(s)[X]$ als $(X - s)^p$ in Linearfaktoren. Wir werden die Erweiterung $\mathbb{F}_p(s^p) \subset \mathbb{F}_p(s)$ später als rein inseparabel erkennen, siehe Beispiel 1.91.

Definition 1.78. (vgl. Motivation) Sei $k \subset K$ eine algebraische Körpererweiterung.

$$[K : k]_s := \# \operatorname{Hom}_k(K, \overline{k})$$

heißt der **Separabilitätsgrad von** K/k. (unabhängig von Wahl von $\overline{k}$.)

Lemma 1.79. *Sei $k \subset K = k(a)$ eine einfache algebraische Körpererweiterung. Sei $f = \min_{a/k}$.*

(a) $[K : k]_s$ *= Anzahl der verschiedenen Nullstellen von f in $\overline{k}$.*
(b) a separabel über $k \Leftrightarrow [K : k] = [K : k]_s$.
(c) Gilt $\operatorname{char} k = 0$*, so $[K : k] = [K : k]_s$.*
(d) Gilt $\operatorname{char} k = p > 0$*, und ist p^r die Vielfachheit der Nullstelle a von f (siehe Satz 1.70, (b)), so gilt*

$$[K : k] = p^r [K : k]_s.$$

Proof. (a): Bereits bekannt (Fortsetzungssatz 1.48 für einfache algebraische Körpererweiterungen).

(b): Sei $n = \deg(f)$. Dann $[K : k] = n$ nach dem Satz 1.9 über das Minimalpolynom, und nach (a) gilt $[K : k]_s = n$ genau dann, wenn f n verschiedene Nullstellen hat, also genau dann, wenn f separabel ist.

(c) In Charakteristik Null ist a separabel über k.

(d) Nach Satz 1.70, (b)) ist n/p^r die Anzahl der verschiedenen Nullstellen von f. Verwende bereits benutzte Gleichungen. □

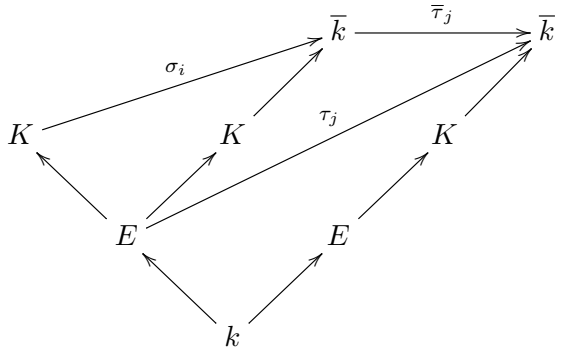
Theorem 1.80 (Multiplikativität des Separabilitätsgrades)**.** *Seien $k \subset E \subset K$ algebraische Körpererweiterungen. Dann gilt*

$$[K : k]_s = [K : E]_s [E : k]_s.$$

Proof. Sei $\overline{k}$ ein algebraischer Abschluß von K (und E und k). Sei

$$\operatorname{Hom}_E(K, \overline{k}) = \{\sigma_i \mid i \in I\} \qquad \text{und} \qquad \operatorname{Hom}_k(E, \overline{k}) = \{\tau_j \mid j \in J\}$$

mit paarweise verschiedenen σ_i bzw. τ_j. Setze τ_j fort zu einem E-Isomorphismus $\overline{\tau}_j : \overline{k} \to \overline{k}$ (Allgemeiner Fortsetzungssatz 1.49) wie im folgenden Bild.



Genügt zu zeigen, dass

$$\operatorname{Hom}_k(K, \overline{k}) = \{\overline{\tau}_j \circ \sigma_i \mid i \in I, j \in J\}$$

und dass die $\overline{\tau}_j \circ \sigma_i$ paarweise verschieden sind.

Inklusion $\supset$ klar.

Inklusion $\subset$: Sei $\varphi \in \mathrm{Hom}_k(K, \overline{k})$. Dann $\varphi|_E \in \mathrm{Hom}_k(E, \overline{k})$, also $\varphi|_E = \tau_j$ für genau ein $j \in J$. Beachte $\overline{\tau}_j^{-1} \circ \varphi \in \mathrm{Hom}_{\boxed{E}}(K, \overline{k})$, also $\overline{\tau}_j^{-1} \circ \varphi = \sigma_i$ für genau ein $i \in I$. Es folgt

$$\varphi = \overline{\tau}_j \circ \sigma_i$$

für eindeutige $i \in I$, $j \in J$. Liefert auch paarweise Verschiedenheit. □

Ende 9. Vorlesung Donnerstag 3. Mai 2012

Theorem 1.81. *Sei $k \subset K$ eine endliche Körpererweiterung.*

(a) Falls $\mathrm{char}\, k = 0$*, so* $[K : k] = [K : k]_s$*.*

(b) Falls $\mathrm{char}\, k = p > 0$*, so* $[K : k] = p^r [K : k]_s$ *für ein* $r \in \mathbb{N}$*.*

Insbesondere $1 \leq [K : k]_s \leq [K : k]$*, und* $[K : k]_s$ *teilt* $[K : k]$*.*

Proof. Folgt per Induktion aus Lemma 1.79 und Multiplikativität von Grad und Separabilitätsgrad (Sätze 1.80 und 1.4). □

Theorem 1.82. *Sei $k \subset K$ endliche Erweiterung. Dann sind äquivalent:*

(a) $k \subset K$ ist separabel.

(b) Es gibt über k separable Elemente $a_1, \ldots, a_n$ mit $K = k(a_1, \ldots, a_n)$.

(c) $[K : k]_s = [K : k]$*.*

Proof. (a) $\Rightarrow$ (b): Klar.

(b) $\Rightarrow$ (c): Jedes a_i ist separabel über $k(a_1, \ldots, a_{i-1})$. Verwende Lemma 1.79 und Multiplikativität von Grad und Separabilitätsgrad (Sätze 1.80 und 1.4).

(c) $\Rightarrow$ (a): Trivial in Charakteristik Null. Sei $p = \mathrm{char}\, k > 0$. Sei $a \in K$ und p^r die Vielfachheit jeder Nullstelle von $\min_{a/k}$ von a (Satz 1.70 (b)). Stets habe (Lemma 1.79 und Multiplikativität von Grad und Separabilitätsgrad, Sätze 1.80 und 1.4)

$$[K : k] = [K : k(a)][k(a) : k] \geq [K : k(a)]_s p^r [k(a) : k]_s = p^r [K : k]_s.$$

Aus (c) folgt $p^r = 1$, also ist jede Nullstelle von $\min_{a/k}$ einfach, und somit ist a separabel über k. □

Corollary 1.83. *Sei $k \subset K$ algebraisch. Sei $A \subset K$ mit $K = k(A)$. Dann $k \subset K$ ist separabel $\Leftrightarrow$ jedes $a \in A$ ist separabel über k.*

Gelten diese Bedingungen, so $[K : k] = [K : k]_s$*. „falls separabel, so kann Index s streichen“ (und umgekehrt, falls endlich).*

Proof. Äquivalenz klar, da $K = \bigcup k(E)$, für $E \subset A$ endliche Teilmenge.

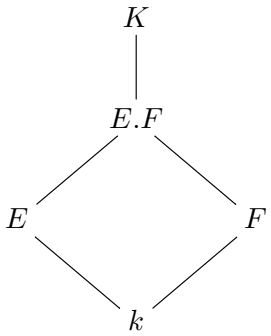
Gelten die Bedingungen. Behauptete Gleichheit gilt, falls $[K : k]$ endlich ist. Sei $k \subset F \subset K$ mit $k \subset F$ endlich. Dann $[K : k]_s \geq [F : k]_s = [F : k]$. Gilt $[K : k] = \infty$, so finde F mit $[F : k]$ größer als jedes gegebene $n \in \mathbb{N}$. Also $[K : k]_s = \infty$. □

Terminologie aus Lang: Algebra, „Ausgezeichnete Klasse von Erweiterungen“ (distinguished class) einführen. Einnere an Beispiele: endlich + algebraisch.

(a) a+b implizieren c (und in c gilt auch Umkehrung)
(b) separable Erweiterungen bilden ausgezeichnete Klasse.
(c) rein inseparable Erweiterungen bilden ausgezeichnete Klasse.

Theorem 1.84. *Separable Erweiterungen bilden eine ausgezeichnete Klasse von Körpererweiterungen.*

Sei $k \subset K$ eine Körpererweiterung mit Zwischenkörpern E und F.



Dann gelten:

(a) $k \subset K$ separabel $\Leftrightarrow$ $k \subset E$ separabel und $E \subset K$ separabel.
(b) E/k separabel $\Rightarrow$ $E.F/F$ separabel.
(c) E/k und F/k separabel $\Leftrightarrow$ $E.F/k$ separabel.

Proof. Algebraizität schon bekannt.

(a): $\Rightarrow$ klar.

$\Leftarrow$: Ist K/k endlich, so zeigt

$$[K : k] = [K : E][E : k] \geq [K : E]_s[E : k]_s = [K : k]_s$$

die Behauptung (zeigt auch $\Rightarrow$, da der Separabilitätsgrad stets $\leq$ dem Grad).

Allgemeiner Fall: Sei $a \in K$. Seine $c_0, \dots, c_n \in E$ die Koeffizienten von $\min_{a/E}$. Dann ist a separabel über $L := k(c_0, \dots, c_n)$ (da Nullstelle des separablen Polynoms $\min_{a/E} \in L[X]$; ist auch $= \min_{a/L}$). Somit sind $L \subset L(a)$ und $k \subset L$ separabel und endlich. Damit ist $k \subset L(a)$ endlich. In diesem Fall haben wir bereits gesehen, dass $k \subset L(a)$ separabel ist, also a separabel über k ist.

(b): Alle Elemente von E sind auch separabel über F. Nach Korollar 1.83 ist dann $E.F = F(E)$ separabel über F.

(c): folgt aus (a) und (b). □

1.6.1. *Satz vom primitiven Element.*

Theorem 1.85 (Satz vom primitiven Element)**.** *Jede endliche separable Erweiterung ist primitiv: Sei $k \subset K$ eine endliche separable Erweiterung. Dann existiert ein $a \in K$ mit $K = k(a)$.*

Proof. **Fall k unendlich:** Sei $K = k(a_1, \ldots, a_n)$. Per Induktion genügt es, den Fall $K = k(b, c)$ zu betrachten. Sei $\overline{k}$ ein algebraischer Abschluss von K.

(Wir brauchen nur, dass c separabel über k ist. Im allgemeinen müssen also alle a_i bis auf eines separabel sein; das nicht separable Element betrachtet man dann am Ende.)

Seien $b = b_1, \ldots, b_r$ die (**verschiedenen**) Nullstellen von $f := \min_{b/k}$ in $\overline{k}$.

Seien $c = c_1, \ldots, c_s$ die **verschiedenen** (einfachen) Nullstellen von $g := \min_{c/k}$ in $\overline{k}$.

Gesucht: a mit $k(b, c) = k(a)$.

Ansatz: $a = b + uc$, mit $u \in k$ (das später bestimmt wird).

Reicht zu zeigen: $c \in k(a)$, denn dann $b = a - uc \in k(a)$.

Setze

$$G(X) := f(a - uX) \in k(a)[X].$$

Dann $G(c) = f(a - uc) = f(b) = 0$. Somit ist c gemeinsame Nullstelle von G und g.

Behauptung: Man kann $u \in k$ so wählen, dass G und g keine weitere gemeinsame Nullstelle in $\overline{k}$ haben.

Für $2 \leq j \leq s$ gilt

$$\begin{aligned} G(c_j) = 0 &\Leftrightarrow \exists 1 \leq i \leq r : a - uc_j = b_i \\ &\Leftrightarrow \exists 1 \leq i \leq r : b + uc - uc_j = b_i \\ &\Leftrightarrow \exists 1 \leq i \leq r : u = \frac{b_i - b}{c - c_j} \end{aligned}$$

Also wähle u so, dass es die endlich vielen Werte

$$\frac{b_i - b}{c - c_j} \quad \text{für } 1 \leq i \leq r, 2 \leq j \leq s$$

vermeidet.

Sei $\mathrm{ggT}(G, g)$ der normierte ggT in $k(a)[X]$. Dieser ist dann auch der normierte ggT in $\overline{k}[X]$ (siehe Beweis von Lemma 1.71), welcher $X - c$ ist, da g separabel ist und c die einzige gemeinsame Nullstelle von g und G in $\overline{k}$. Es folgt $c \in k(a)$.

Beachte: Wir haben nur verwendet, dass c separabel über k ist.

Fall k endlich: Dann ist auch K endlich, und nach Lemma 1.86 ist $K^\times = \langle a \rangle$ für ein $a \in K$. Es folgt $K = k[a] = k(a)$.

Beachte: Hier haben wir nur verwendet, dass $k \subset K$ eine endliche Erweiterung ist. Eine solche Erweiterung ist aber stets separabel, siehe Korollar 1.100 unten oder Übungsaufgabe 1.76. □

Lemma 1.86. *Sei K ein Körper und $A \subset K^\times$ eine endliche Untergruppe. Dann ist A zyklisch.*

Proof. Hauptsatz über endlich erzeugte abelsche Gruppen: Schreibe

$$A = A(p_1) \times \cdots \times A(p_n)$$

mit paarweise verschiedenen Primzahlen p_i, so dass $A(p_i)$ die p_i-Sylowgruppe in A ist. (Da A endlich ist, taucht kein Faktor $\cong \mathbb{Z}^l$ auf.)

Beispiel: Hauptsatz liefert etwa (links multiplikativ, rechts additiv geschrieben)

$$A \cong \underbrace{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/2^2\mathbb{Z}}_{A(2)} \times \underbrace{\mathbb{Z}/3}_{A(3)} \times \underbrace{\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5^2\mathbb{Z}}_{A(5)}.$$

Fixiere i und setze $p = p_i$. Behauptung: $A(p)$ ist zyklisch.

Definiere $m = m_i \in \mathbb{N}$ durch

$$p^m = \max\{\operatorname{ord}(a) \mid a \in A(p)\}.$$

Beachte: Die Ordnung jedes Elements von $A(p)$ ist p-Potenz. Somit teilt die Ordnung jedes Elements p^m.

Es folgt $a^{p^m} = 1$ für jedes $a \in A(p)$. Also ist jedes $a \in A(p)$ Nullstelle von $X^{p^m} - 1 \in K[X]$, und es folgt

$$|A(p)| \leq p^m.$$

Sei $a \in A(p)$ ein Element der (maximalen) Ordnung p^m. Dann hat $\langle a \rangle$ die Ordnung p^m. Somit ist

$$A(p) = \langle a \rangle \cong \mathbb{Z}/p^m\mathbb{Z}$$

zyklisch.

(Im Beispiel bestehen also $A(2)$, $A(3)$, $A(5)$ nur aus je einem Faktor.)

Insgesamt ergibt sich mit dem Chinesischen Restsatz

$$A = A(p_1) \times \cdots \times A(p_n) \cong \mathbb{Z}/p_1^{m_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_n^{m_n}\mathbb{Z} \xleftarrow{\sim} \mathbb{Z}/p_1^{m_1} \dots p_n^{m_n}\mathbb{Z},$$

und somit ist A zyklisch. □

Exercise 1.87. Sei q eine Primzahlpotenz. Wieviele Elemente $\mathbb{F}_q$ sind Quadrate?

1.6.2. *Rein inseparable Erweiterungen.* Sei k ein Körper der Charakteristik $p > 0$. (Alle Resultate dieses Kapitels haben triviale Formulierung in Charakteristk Null.)

Lemma-Definition 1.88. *Sei $k \subset K$ eine algebraische Körpererweiterung, und sei $a \in K$. Dann sind äquivalent:*

(a) $\min_{a/k}$ *hat genau eine (eventuell mehrfache) Nullstelle in* $\overline{k}$. [28] [29]

(b) $a^{p^m} \in k$ *für ein* $m \geq 0$.

[28] Unabhängig von p formuliert, auch sinnvoll für Charakteristik Null. Dort äquivalent zu $a \in k$.

[29] Könnte oben algebraisch weglassen und es hier zusätzlich verlangen.

*Falls diese Bedingungen erfüllt sind, heißt a **rein inseparabel über** k.*

Ist a rein inseparabel über k und ist $m \in \mathbb{N}$ minimal, so dass $a^{p^m} \in k$, so ist $X^{p^m} - a^{p^m}$ das Minimalpolynom von a über k.

Bemerkung ($k \subset K$ algebraisch): Ist $a \in K$ separabel und rein inseparabel über k, so hat $\min_{a/k}$ genau eine einfache Nullstelle in $\overline{k}$, ist also gleich $X-a$. Also $a \in k$.

Proof. Sei $f = \min_{a/k}$. Sei $f = g(X^{p^r})$ wie oben mit r maximal. Dann ist g separabel.

(a) $\Rightarrow$ (b): In diesem Fall gilt $g = X - b$, also $f = X^{p^r} - b$ und somit $a^{p^r} = b \in k$.

(b) $\Rightarrow$ (a): Das Polynom $X^{p^m} - a^{p^m} \in k[X]$ hat a als Nullstelle, also ist f ein Teiler von $X^{p^m} - a^{p^m}$. In $\overline{k}[X]$ gilt $X^{p^m} - a^{p^m} = (X - a)^{p^m}$. Also hat f genau eine Nullstelle.

Sei a rein inseparabel über k, und m minimal mit $a^{p^m} \in k$. Nach obigem ist $f = X^{p^r} - a^{p^r}$ das Minimalpolynom von a über k. Wegen $a^{p^r} \in k$ folgt $m \leq r$. Andererseits teilt f das Polynom $X^{p^m} - a^{p^m}$, und somit $p^r \leq p^m$, also $r \leq m$. □

Definition 1.89. Ein Körpererweiterung $k \subset K$ heisst **rein inseparabel**, falls sie algebraisch ist und alle $a \in K$ rein inseparabel über k sind.

30

Bemerkung: Jede separable und rein inseparable Körpererweiterung $k \subset K$ ist trivial: $k = K$.

Ende 10. Vorlesung Montag 7. Mai 2012

Theorem 1.90. *Sei $k \subset K$ algebraisch. Dann sind äquivalent:*

(a) $k \subset K$ ist rein inseparabel.
(b) (Trivial nach Definition:) Zu jedem $a \in K$ gibt es ein $n \in \mathbb{N}$ mit $a^{p^n} \in K$.)
(c) Es gibt $A \subset K$ bestehend aus über k rein inseparablen Elementen, so dass $K = k(A)$.
(d) $[K : k]_s = 1$.

Proof. (a) $\Leftrightarrow$ (b) $\Rightarrow$ (c): Trivial.

(c) $\Rightarrow$ (d): Stimmen zwei k-Morphismen $K \to \overline{k}$ auf allen Elementen von A überein, so sind sie gleich.

Es genügt also zu zeigen: Sei $a \in A$. Dann $[k(a) : k]_s = 1$.

Sei $n \in \mathbb{N}$ mit $a^{p^n} \in k$. Sei $\sigma \in \mathrm{Hom}_k(k(a), \overline{k})$. Dann gilt $\sigma(a)^{p^n} = \sigma(a^{p^n}) = a^{p^n}$. Also ist $\sigma(a)$ die eindeutige p^n-te Wurzel aus a^{p^n} in $\overline{k}$. (Falls $K \subset \overline{k}$, so $\sigma(a) = a$.)

(d) $\Rightarrow$ (a): Sei $a \in K$. Dann zeigt $1 = [K : k]_s = [K : k(a)]_s[k(a) : k]_s$, dass $[k(a) : k]_s = 1$. Also hat $\min_{a/k}$ genau eine Nullstelle in $\overline{k}$. □

30 In Charakteristik Null sind nur triviale Erweiterungen $k = K$ rein inseparabel.

Example 1.91. Die Körpererweiterung $\mathbb{F}_p(s^p) \subset \mathbb{F}_p(s)$ aus Beispiel 1.77 ist rein inseparabel: Das Element s ist rein inseparabel über $\mathbb{F}_p(s^p)$ (mit Minimalpolynom $X^p - s^p$) nach Definition 1.88, und somit ist die Erweiterung rein inseparabel nach Satz 1.90.

Theorem 1.92. *Rein inseparable Erweiterungen bilden eine ausgezeichnete Klasse von Körpererweiterungen.*

Proof. Klar per Multiplikativität Separabilitätsgrad, und offensichtlich für Schluss von E/k auf $E.F/F$ nach Definition. □

Theorem 1.93. *Sei $k \subset K$ algebraisch. Dann existiert genau ein Zwischenkörper $k \subset K_{\text{sep}} \subset K$ so dass*

$$k \underset{\text{separabel}}{\subset} K_{sep} \underset{\text{rein inseparabel}}{\subset} K,$$

genannt der ***separable Abschluss von*** *k* ***in*** *K. Es gilt*

$$K_{\text{sep}} = K_{\text{sep}/k} := \{a \in K \mid a \text{ separabel über } k\}. \tag{1.8}$$

Es gilt

$$[K : k]_s = [K_{\text{sep}} : k].$$

Ist $k \subset K$ normal, so auch $k \subset K_{\text{sep}}$.

Proof. Existenz: Sei K_{sep} definiert durch (1.8). Wir zeigen zunächst, dass K_{sep} die gewünschten Eigenschaften hat.

Seien $a, b \in K_{\text{sep}}$. Dann ist $k \subset k(a, b)$ separabel, also $k(a, b) \subset K_{\text{sep}}$. Dies zeigt, dass K_{sep} ein Zwischenkörper ist.

Offensichtlich ist $k \subset K_{\text{sep}}$ separabel.

Sei $a \in K$. Sei $f = \min_{a/k}$. Wie oben $f = g(X^{p^r})$ mit g separabel. Wegen $0 = f(a) = g(a^{p^r})$ ist a^{p^r} Nullstelle des separablen Polynoms g, also $a^{p^r} \in K_{\text{sep}}$. Also ist $K_{\text{sep}} \subset K$ rein inseparabel.

Eindeutigkeit: Sei $k \subset L \subset K$ ein Zwischenkörper, so dass

$$k \underset{\text{separabel}}{\subset} L \underset{\text{rein inseparabel}}{\subset} K.$$

Jedes $x \in L$ ist separabel über k, also $L \subset K_{\text{sep}}$. Die Erweiterung $L \subset K_{\text{sep}}$ ist separabel (da $k \subset K_{\text{sep}}$ separabel) und rein inseparabel (da $L \subset K$ rein inseparabel). Also $L = K_{\text{sep}}$.

Die Aussage über die Grade folgt aus

$$[K : k]_s = \underbrace{[K : K_{\text{sep}}]_s}_{=1 \text{ (da rein inseparabel)}} \quad [K_{\text{sep}} : k]_s = [K_{\text{sep}} : k]_s \underset{\text{da separabel}}{=} [K_{\text{sep}} : k].$$

Sei $k \subset K$ normal. Sei $f \in k[X]$ irreduzibel und ohne Einschränkung normiert, mit einer Nullstelle $a \in K_{\text{sep}}$. Also ist $f = \min_{a/k}$ separabel. Es zerfällt f in $K[X]$ in Linearfaktoren. Jede Nullstelle von f in K ist separabel über k und liegt also in K_{sep}. Also zerfällt f bereits über K_{sep} in Linearfaktoren. Also ist $k \subset K_{\text{sep}}$ normal. [31] □

[31] Alternativ:

Exercise 1.94. Sei $k \subset K$ normal. Dann

$$\mathrm{Aut}_k(K) \xrightarrow{\sim} \mathrm{Aut}_k(K_{\mathrm{sep}})$$

in natürlicher Weise.

Exercise 1.95. Sei $k \subset K$ normal. Dann

$$\mathrm{Aut}_k(K) \xrightarrow{\sim} \mathrm{Aut}_{K_i}(K)$$

in natürlicher Weise.

Sei $p = \mathrm{char}\, k > 0$. Zeige

$$K_i := \{a \in K \mid \text{es gibt } m \in \mathbb{N} \text{ mit } a^{p^m} \in k\}.$$

Für Inklusion $\supset$ wende Satz an auf $k(a) \subset K$.

Exercise 1.96. [Bos, Aufgabe 3.8.10] Sei $k \subset K$ eine algebraische Körpererweiterung mit der Eigenschaft, dass jedes irreduzible Polynom aus $k[X]$ eine Nullstelle in K habe. Dann ist K ein algebraischer Abschluss von k.

Zeigen Sie, dass es also im Beweis von Satz 1.46 (Existenz des algebraischen Abschlusses) genügt, das dortige Verfahren einmal anzuwenden.

1.7. **Endliche Körper.** Erinnerung: Die Charakteristik eines endlichen Körpers K ist eine Primzahl p, und sein Primkörper ist eindeutig isomorph zu $\mathbb{F}_p$. Wir fassen deshalb $\mathbb{F}_p$ als Unterkörper von K auf.

Theorem 1.97 (Klassifikation endlicher Körper)**.** *Die Kardinalität eines endlichen Körpers ist stets eine Primzahlpotenz, und zu gegebener Primzahlpotenz gibt bis auf Isomorphismus genau einen endlichen Körper mit dieser Kardinalität.*

Prägnanter:

$$\{\textit{endliche Körper}\}/\cong \xrightarrow{\sim} \{\textit{Primzahlpotenzen}\},$$
$$K \mapsto |K|,$$
$$(\textit{Zerfällungskörper von } X^q - X \in \mathbb{F}_p[X]) \hookleftarrow q = p^n.$$

Genauer: Sei p eine Primzahl.

(a) Sei K ein endlicher Körper der Charakteristik p. Dann gilt

$$\#K = p^n \quad \textit{für } n = [K : \mathbb{F}_p].$$

Sei $q = p^n$. Es ist K ein Zerfällungskörper von $X^q - X \in \mathbb{F}_p[X]$, und somit ist ein endlicher Körper mit q Elementen eindeutig bis auf Isomorphismus (= $\mathbb{F}_p$-Isomorphismus).

(b) Sei $q = p^n$ eine p-Potenz. Dann existiert ein endlicher Körper mit q Elementen.

Jeder k-Morphismus $\sigma : K_{\mathrm{sep}} \to \overline{K}$ erweitert zu einem k-Morphismus $K \to \overline{K}$, der wegen der Normalität von $k \subset K$ zu einem k-Automorphismus von K restringiert. Insbesondere folgt $\sigma(K_{\mathrm{sep}}) \subset K$, und natürlich bildet σ Elemente, die separabel über k sind, auf ebensolche ab.

Proof. (a): Sei $n = [K : \mathbb{F}_p]$. Dann $K \cong \mathbb{F}_p^n$ als $\mathbb{F}_p$-Vektorraum, also $\#K = p^n = q$.

Die multiplikative Gruppe $K^\times$ hat Ordnung $q-1$, also ist jedes Element von $K^\times$ Nullstelle von $X^{q-1}-1$, und jedes Element von K ist Nullstelle von $X^q - X$. Also $X^q - X = \prod_{a\in K}(X-a) \in K[X]$, und K ist Zerfällungskörper von $X^q - X \in \mathbb{F}_p[X]$.

(b): Sei Z ein Zerfällungskörper von $f = X^q - X$ (etwa in $\overline{\mathbb{F}}_p$). Wegen $f' = -1$ ist f separabel. Also hat f genau q einfache Nullstellen in Z. Diese Nullstellen bilden einen Teilkörper von Z (etwa: Sind a, b Nullstellen, so $(a \pm b)^q = a^q \pm b^q = a \pm b$), der mit Z übereinstimmen muss. □

Example 1.98. In $\mathbb{F}_5$ sind 0 und ± 1 die einzigen Quadrate. Also ist $\mathbb{F}_5(\sqrt{2})$ ein endlicher Körper mit 25 Elementen. Jedes Element läßt sich eindeutig als $a + b\sqrt{2}$ schreiben, mit $a, b \in \mathbb{F}_5$.

Fixiere p eine Primzahl und einen algebraischen Abschluss $\overline{\mathbb{F}}_p$ von $\mathbb{F}_p$. Sei $q = p^n$. Dann ist also

$$\mathbb{F}_q = \mathbb{F}_{p^n} := \{a \in \overline{\mathbb{F}}_p \mid a^q = a\}$$

der endliche Körper in $\overline{\mathbb{F}}_p$ mit q Elementen, und jeder endliche Unterkörper von $\overline{\mathbb{F}}_p$ ist von dieser Gestalt.

Corollary 1.99. *Sei $q = p^n$ und $q' = p^{n'}$. Dann gilt*

$$\mathbb{F}_q \subset \mathbb{F}_{q'} \quad \Leftrightarrow \quad n \text{ teilt } n'.$$

Proof. Gelte $\mathbb{F}_q \subset \mathbb{F}_{q'}$. Dann ist $\mathbb{F}_{q'}$ ein $\mathbb{F}_q$-Vektorraum, also $q' = q^m$ für ein $m \in \mathbb{N}_{>0}$ (genauer $m = [\mathbb{F}_{q'} : \mathbb{F}_q]$). Also $(p^n)^m = p^{n'}$, also $nm = n'$.

Umgekehrt sei $nm = n'$. Also $q' = p^{n'} = (p^n)^m = q^m$. Aus $a^q = a$ folgt $a^{q'} = a^{q^m} = ((a^q)^q \dots)^q = a$. Also $\mathbb{F}_q \subset \mathbb{F}_{q'}$. □

Corollary 1.100. *Jede algebraische Erweiterung eines endlichen Körper ist normal und separabel. Insbesondere sind endliche Körper vollkommen.*

Proof. Sei k ein endlicher Körper, und $p = \operatorname{char} k > 0$.

Sei $k \subset E$ eine endliche Erweiterung. Sei $q = \#E$. Dann ist E Zerfällungskörper des separablen Polynoms $X^q - X$ (über dem Primkörper $\mathbb{F}_p$ und) über k. Also ist $k \subset E$ normal und separabel.

Ist allgemein $k \subset K$ algebraisch, so gilt $K = \bigcup E$, wobei E die Zwischenkörper von $k \subset K$ mit $[E : k] < \infty$ durchläuft. Die Behauptung folgt dann aus dem obigen (normal: etwa per irreduzibles Polynom in $k[X]$. separabel: klar). □

Remark 1.101. Sei k ein endlicher Körper der Charakteristik p und $k \subset K$ eine algebraische Erweiterung. Dann kann $k \subset K$ in $\overline{\mathbb{F}}_p$ „realisieren“:

Beachte $\mathbb{F}_p \subset k$. Setze $\mathbb{F}_p \subset \overline{\mathbb{F}}_p$ erst fort zu $k \to \overline{\mathbb{F}}_p$ und dann zu $K \to \overline{\mathbb{F}}_p$.

(Ist K ebenfalls endlich, so einfacher (zumindest nach aller Vorarbeit): K ist isomorph zu einem $\mathbb{F}_q$.)

Exercise 1.102. Male ein Diagramm, dass die Inklusionen aller endlichen Körper der Charakteristik 2 und 3 veranschaulicht. Dasselbe für eine beliebige Primzahl p.

Exercise 1.103. Sei p eine Primzahl und $\overline{\mathbb{F}}_p$ fixiert. Sei $\mathcal{F}$ die Kategorie aller endlichen Körper der Charakteristik p. Sei $\mathcal{N}$ die (volle Unter-)Kategorie der endlichen Unterkörper von $\overline{\mathbb{F}}_p$. Zeigen Sie, dass die Inklusion $\mathcal{N} \subset \mathcal{F}$ eine Äquivalenz von Kategorien ist.

Corollary 1.104 (zu Lemma 1.86)**.** *Die multiplikative Gruppe von $\mathbb{F}_q$ ist zyklisch von der Ordnung $q-1$.*

Proof. Jede endliche Untergruppe der multiplikativen Gruppe eines Körpers ist zyklisch, siehe Lemma 1.86. □

Theorem 1.105. *Sei $F \subset E$ eine Erweiterung endlicher Körper der Charakteristik p, vom Grad $d = [E : F]$. Sei $q = \#F$. Dann ist $\mathrm{Aut}_F(E)$ zyklisch von der Ordnung d und wird vom **relativen Frobenius (über F)***

$$\begin{aligned} \mathrm{Fr}_q : E &\to E, \\ x &\mapsto x^q, \end{aligned}$$

erzeugt. Mit anderen Worten,

$$\begin{aligned} \mathbb{Z}/d\mathbb{Z} &\xrightarrow{\sim} \mathrm{Aut}_F(E), \\ n &\mapsto (\mathrm{Fr}_q)^n, \end{aligned}$$

ist ein Isomorphismus von Gruppen.

(Insbesondere gelten diese Aussagen für $\mathbb{F}_q \subset \mathbb{F}_{q^d}$.)

Ende 11. Vorlesung Donnerstag 10. Mai 2012

Proof. Es gilt

$$F = E^{\mathrm{Fr}_q} := \{a \in E \mid \mathrm{Fr}_q(a) = a\} = \{a \in E \mid a^q = a\},$$

denn $|F| = q$, $F \subset E^{\mathrm{Fr}_q}$ und $|E^{\mathrm{Fr}_q}| \leq q$ (da $X^q - X$ separabel).

Weil E endlich ist, folgt $\mathrm{Fr}_q \in \mathrm{Aut}_F(E)$. Also habe wohldefinierte Abbildung

$$\begin{aligned} \varphi : \mathbb{Z} &\to \mathrm{Aut}_F(E), \\ n &\mapsto (\mathrm{Fr}_q)^n. \end{aligned}$$

Behauptung: $\ker \varphi = d\mathbb{Z}$.

Beachte $\#E = q^d$. Für $e \in E$ gilt $e = e^{q^d} = (\mathrm{Fr}_q)^d(e)$. Also $d \in \ker \varphi$. Angenommen es gibt $1 \leq a < d$ mit $a \in \ker \varphi$. Dann gilt $e = (\mathrm{Fr}_q)^a = e^{q^a}$ für alle $e \in E$, und somit sind alle Elemente von E Nullstellen des Polynoms $X^{q^a} - X$ vom Grad q^a. Dies implizert $q^d = \#E \leq q^a$, also $d \leq a$ im Widerspruch zur Annahme. Dies zeigt die Behauptung.

Also faktorisiert φ zu einem injektiven Gruppenmorphismus

$$\overline{\varphi} : \mathbb{Z}/d\mathbb{Z} \hookrightarrow \mathrm{Aut}_F(E).$$

Weil $E \subset F$ normal ist gilt $\operatorname{Aut}_F(E) = \operatorname{Hom}_F(E, \overline{E})$, und weil $E \subset F$ separabel ist, erhalten wir damit

$$d = [E : F] = [E : F]_s = \# \operatorname{Hom}_F(E, \overline{E}) = \# \operatorname{Aut}_F(E).$$

Also ist $\overline{\varphi}$ bijektiv. □

Exercise 1.106. Bestimmen Sie alle Morphismen $\mathbb{F}_q \to \mathbb{F}_{q'}$ von Körpern, für q und q' Primzahlpotenzen.

2. Galois-Theorie

John Baez LECTURES ON n-CATEGORIES AND COHOMOLOGY:

1. The Basic Principle of Galois Theory 1.1. Galois theory. Around 1832, Galois discovered a basic principle: We can study the ways a little thing k can sit in a bigger thing K:

$$k \hookrightarrow K$$

by keeping track of the symmetries of K that fix k. These form a subgroup of the symmetries of K: $\operatorname{Gal}(K/k) \subset \operatorname{Aut}(K)$.

Sei K ein Körper und $G \subset \operatorname{Aut}(K)$ eine Untergruppe der Gruppe der Körper-Automorphismen von K. Dann operiert G auf K durch Körperautomorphismen: Die Abbildung

$$\begin{aligned} G \times K &\to K, \\ (g, x) &\mapsto g.x := g(x), \end{aligned}$$

ist eine Operation der Gruppe G auf der Menge K, und für jedes $g \in G$ ist die Abbildung

$$\begin{aligned} g : K &\to K, \\ x &\mapsto g.x, \end{aligned}$$

ein Morphismus von Körpern (mit Inversem g^{-1}).

Die Fixpunkte

$$K^G := \{x \in K \mid g(x) = x \text{ für alle } g \in G\}$$

dieser Operation bilden einen Unterkörper von K, den **Fixkörper** oder **Invariantenkörper von** G.

Notation/Erinnerung: Gegeben $a \in K$ heißt

$$G.a := \{g.a \mid g \in G\}$$

die **Bahn von** a.

Lemma 2.1 (Schlüssellemma)**.** *Sei K ein Körper, $G \subset \operatorname{Aut}(K)$ eine Untergruppe, und $a \in K$. Wir nehmen an, dass die Bahn $G.a$ endlich ist (dies ist etwa der Fall, falls G endlich ist).*

Dann ist a algebraisch und separabel über K^G mit Minimalpolynom

$$\min_{a/K^G} = \prod_{b \in G.a} (X - b).$$

Insbesondere gilt $\deg_{K^G}(a) = |G.a|$.

Bemerkung: G operiert auf $K[X]$ durch Ringautomorphismen

$$G \times K[X] \to K[X],$$
$$(g, f = \sum c_i) \mapsto g.f := g(f) := f^g = \sum g(c_i) X^i.$$

Proof. Sei $k := K^G$. Sei $f = \prod_{b \in G.a}(X - b)$. Dann

$$\begin{aligned} g.f &= \prod_{b \in G.a} g(X - b) \\ &= \prod_{b \in G.a} (X - g(b)) \\ &= f, \end{aligned}$$

also $f \in K^G[X] = k[X]$. Weil $f(a) = 0$ folgt $\min_{a/k} | f$ in $k[X]$. Wegen $G \subset \mathrm{Aut}_{\boxed{k}}(K)$ ist mit a auch $g(a)$ eine Nullstelle von $\min_{a/k}$, für beliebiges $g \in G$. Also ist jedes $X - b$ für $b \in G.a$ ein Teiler von $\min_{a/k}$ in $K[X]$. Es folgt $f | \min_{a/k}$ in $K[X]$. Also $f = \min_{a/k}$. □

Corollary 2.2. *Sei $k \subset K$ eine $\boxed{\text{algebraische}}$ Erweiterung, und $G \subset \mathrm{Aut}_k(K)$ eine Untergruppe. Dann ist die Erweiterung $K^G \subset K$ separabel und normal.*

Proof. Gegeben $a \in K$ ist $G.a$ endlich: Sei $f = \min_{a/k}$. Ist $g \in G$, so gilt $f(g.a) = (g.f)(g.a) = g.(f(a)) = g.0 = 0$. Also ist $G.a$ in den endlich vielen Nullstellen von f enthalten. Wir können also das Schlüssellemma 2.1 anwenden. Dies zeigt auch, dass das Minimalpolynom jedes Elements $a \in K$ bereits in $K[X]$ in Linearfaktoren zerfällt. Also ist K der Zerfällungskörper all dieser Minimalpolynome (= irreduzible normierte Polynome unten, die Nullstelle oben haben). □

Corollary 2.3. *Sei $k \subset K$ eine $\boxed{\text{normale}}$ algebraische Erweiterung und $G := \mathrm{Aut}_k(K)$. Dann gilt*

$$k \underset{\text{rein inseparabel}}{\subset} K^G \underset{\text{separabel}}{\subset} K.$$

Es ist K^G der eindeutige Zwischenkörper von $k \subset K$ mit diesen Eigenschaften. Manchmal wird die Notation $K_i = K^G$ verwendet (in Analogie zu $k \subset K_{\mathrm{sep}} \subset K$, vgl. Satz 1.93).

Example 2.4. Normalität nötig: Siehe Morandi: Field and Galois Theory, p. 48 Example 4.24.

Proof. Wir haben gerade gesehen, dass $K^G \subset K$ separabel ist.

Wegen der Normalität von $k \subset K$ gilt $G = \mathrm{Aut}_k(K) = \mathrm{Hom}_k(K, \overline{K})$.

Behauptung: $k \subset K^G$ ist rein inseparabel: Sei $\sigma : K^G \to \overline{K}$ ein k-Morphismus. Dann kann σ zu $\widetilde{\sigma} : K \to \overline{K}$ fortsetzen, also $\widetilde{\sigma} \in G$. Es folgt $\sigma = \widetilde{\sigma}|_{K^G} = \mathrm{id}_{K^G}$. Also $[K^G : k]_s = 1$, was die Behauptung zeigt.

Eindeutigkeit: Ist $k \subset E \subset K$ mit $k \subset E$ rein inseparabel, so folgt $g|_E = \mathrm{id}_E$ für alle $g \in G$. Also $E \subset K^G$. Ist zusätzlich $E \subset K$ separabel, so ist $E \subset K^G$ separabel und rein inseparabel. Also $E = K^G$. □

Theorem 2.5. *Sei K ein Körper und sei $G \subset \mathrm{Aut}(K)$ eine Untergruppe. Dann*

$$G \text{ endlich} \quad \Leftrightarrow \quad K^G \subset K \text{ endlich.}$$

Sind diese Bedingungen erfüllt, so ist $K^G \subset K$ separabel und normal vom Grad

$$|G| = [K : K^G],$$

und es gilt

$$G = \mathrm{Aut}_{K^G}(K).$$

Proof. Offensichtlich gilt $G \subset \mathrm{Aut}_{K^G}(K)$.

Ist $K^G \subset K$ endlich (und damit algebraisch), so habe $\mathrm{Aut}_{K^G}(K) \subset \mathrm{Hom}_{K^G}(K, \overline{K})$ und somit

$$|G| \leq |\mathrm{Aut}_{K^G}(K)| \leq [K : K^G]_s \leq [K : K^G] < \infty. \tag{2.1}$$

Sei umgekehrt G endlich. Wir zeigen genauer

$$[K : K^G] \leq |G|. \tag{2.2}$$

32

---

32 Alternativbeweis (ohne Schlüssellemma, im wesentlichen aus E. Artin: Algebra): (Übungsaufgabe) Das geht per Charaktere!!!

Sei $n = |G|$. Seien $a_1, a_2, \ldots, a_{n+1} \in K$. Zu zeigen ist, dass diese Elemente linear abhängig sind über K^G. Sei $G = \{g_1 = \mathrm{id}, g_2, \ldots, g_n\}$. Betrachte die lineare Abbildung

$$\varphi := \begin{bmatrix} a_1 & a_2 & \ldots & a_{n+1} \\ g_2(a_1) & g_2(a_2) & \ldots & g_2(a_{n+1}) \\ \vdots & \vdots & \ddots & \vdots \\ g_n(a_1) & g_n(a_2) & \ldots & g_n(a_{n+1}) \end{bmatrix} : K^{n+1} \to K^n.$$

Ihr Kern ist mindestens eindimensional. Sei $m \leq n+1$ minimal so dass es einen Vektor $\xi \in \ker(\varphi)$ der Form

$$\xi = (\xi_1, \xi_2, \ldots, \xi_m \neq 0, 0, \ldots, 0)$$

gibt. Sei ξ ein solcher Vektor. Ohne Einschränkung können wir $\xi_m = 1$ annehmen.

Die Aussage $\xi \in \ker(\varphi)$ ist äquivalent zu

$$g(a_1)\xi_1 + g(a_2)\xi_2 + \cdots + g(a_{m-1})\xi_{m-1} + g(a_m) = 0 \quad \text{für alle } g \in G.$$

Wendet man darauf $h \in G$ an, so erhält man

$$hg(a_1)h(\xi_1) + hg(a_2)h(\xi_2) + \cdots + hg(a_{m-1})h(\xi_{m-1}) + hg(a_m) = 0 \quad \text{für alle } g \in G.$$

Da mit g auch hg alle Elemente von G durchläuft, folgt

$$h(\xi) := (h(\xi_1), h(\xi_2), \ldots, h(\xi_m) = 1, 0, \ldots, 0) \in \ker(\varphi).$$

Es folgt

$$\xi - h(\xi) = (\xi_1 - h(\xi_1), \xi_2 - h(\xi_2), \ldots, \xi_{m-1} - h(\xi_{m-1}), 0, 0, \ldots, 0) \in \ker(\varphi).$$

Wegen der Wahl von m folgt $\xi = h(\xi)$, also

$$h(\xi_i) = \xi_i \quad \text{für alle } 1 \leq i \leq n+1$$

(beachte wobei $\xi_m = 1$ und $\xi_i = 0$ für alle $i > m$).

Sei $K^G \subset E \subset K$ ein Zwischenkörper mit $K^G \subset E$ endlich. Nach dem Schlüssellemma 2.1 (da G endlich) ist $K^G \subset E$ separabel, und nach dem Satz 1.85 vom primitiven Element von der Form $E = K^G(a)$; das Schlüssellemma 2.1 wiederum liefert $[E : K^G] = |G.a| \leq |G|$.

Das Schlüssellemma 2.1 schon wieder zeigt, dass $K^G \subset K$ algebraisch ist. Ist $[K : K^G] > |G|$, so sei $A \subset K$ eine endliche K^G-linear unabhängige Teilmenge mit $|A| > |G|$. Setze $E = K^G(A)$. Dann ist $[E : K^G] \geq |A| > |G|$ im Widerspruch zu obigem. Dies zeigt die Behauptung.

Wir nehmen nun an, dass G und $K^G \subset K$ endlich sind. [33] Wir dürfen dann (2.1) und (2.2) anwenden und erhalten

$$|G| = |\operatorname{Aut}_{K^G}(K)| = [K : K^G]_s = [K : K^G].$$

Dies zeigt einerseits die Separabilität (Satz 1.82, da Erweiterung endlich), und andererseits, dass die Inklusionen $G \subset \operatorname{Aut}_{K^G}(K) \subset \operatorname{Hom}_{K^G}(K, \overline{K})$ Gleichheiten sind. Dies liefert $G = \operatorname{Aut}_{K^G}(K)$ und Normalität. □

Ende 12. Vorlesung Montag 14. Mai 2012

Definition 2.6. Eine Erweiterung $k \subset K$ heißt **galoissch** oder **Galois-Erweiterung**, falls sie normal und separabel ist. Man bezeichnet dann $\operatorname{Gal}(K/k) := \operatorname{Aut}_k(K)$ als die **Galois-Gruppe von** K/k.

Eine Galois-Erweiterung heißt **zyklisch** bzw. **abelsch**, falls ihre Galoisgruppe diese Eigenschaft hat.

Remark 2.7. (a) Galoiserweiterungen = Zerfällungskörper von Familien separabler Polynome: Das folgt aus Satz 1.60 und Korollar 1.83. (Begründung: Gegeben eine Galoiserweiterung, nimm die Minimalpolynome von erzeugenden Elementen.) (besser: von Familie von Polynomen, deren jeder irreduzible Faktor separabel ist?)

(b) endliche Galoiserweiterung = Zerfällungskörper eines separablen Polynoms. (Gegeben $k \subset K$ endlich galoissch, finde $b \in K$ mit $K = k(b)$ (Satz 1.85 vom primitiven Element). Dann zerfällt $\min_{b/k}$ in Linearfaktoren in $K[X]$ und ist separabel, und K ist sein Zerfällungskörper.)

Examples 2.8. (a) Charakteristik Null: stets separabel.

(a) Sei $k \subset K$ ein Zerfällungskörper von $f \in k[X]$. Dann ist $k \subset K$ galoissch.

Da $h \in G$ beliebig war, folgt $\xi \in (K^G)^{n+1}$. Wegen $\xi \neq 0$ liefert das die gesuchte K^G-lineare Abhängigkeit der $a_1, a_2, \ldots, a_{n+1}$.

Dies zeigt $[K : K^G] \leq |G|$.

[33] besserer(?) Beweis:

Korollar 2.2 (hatte normal vergessen in Vorlesung), angewandt auf die endliche und damit algebraische Erweiterung $K^G \subset K$ (beachte $G \subset \operatorname{Aut}_{K^G}(K)$) liefert Separabilität und Normalität. Wir dürfen (2.1) und (2.2) anwenden und erhalten so

$$|G| = |\operatorname{Aut}_{K^G}(K)| = [K : K^G]_s = [K : K^G].$$

Dies zeigt, dass die Inklusion $G \subset \operatorname{Aut}_{K^G}(K)$ eine Gleichheit ist.

besser: endliche Galoiserweiterung = Zerfällungskörper eines Polynoms.
   (b) nicht extra erwähnt: $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ ist nicht galoissch, da nicht normal.
(b) Charakteristik $p > 0$:
   (a) $\mathbb{F}_q \subset \mathbb{F}_{q^d}$ ist Galois-Erweiterung mit zyklischer Galoisgruppe $\mathbb{Z}/d\mathbb{Z} \xrightarrow{\sim} \operatorname{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$, $1 \mapsto \operatorname{Fr}_q$.
   (b) nicht extra erwähnt: $\mathbb{F}_p(s^p) \subset \mathbb{F}_p(s)$ ist nicht galoissch (da nicht separabel).

Remark 2.9. Ist K ein Körper und $G \subset \operatorname{Aut}(K)$ eine Untergruppe, so ist die Erweiterung $K^G \subset K$ galoissch genau dann, wenn sie algebraisch ist.

Denn: Eine Richtung ist trivial, die andere folgt aus Korollar 2.2, angewandt auf $k = K^G$.

Proposition 2.10. *Sei $k \subset K$ galoissch (möglicherweise unendlich). Dann gelten*

$$|\operatorname{Gal}(K/k)| = [K : k],$$

und

$$k = K^{\operatorname{Gal}(K/k)}.$$

Proof. Da $k \subset K$ normal ist, gilt $\operatorname{Aut}_k(K) = \operatorname{Hom}_k(K, \overline{K})$. Da $k \subset K$ separabel ist, gilt $[K : k]_s = [K : k]$. Dies zeigt die erste Behauptung.

Setze $G = \operatorname{Gal}(K/k)$. Dann offensichtlich $k \subset K^G$. Angenommen, es gibt $a \in K^G - k$. Das (nichtlineare) separable Polynom $\min_{a/k}$ hat also eine Nullstelle $b \in \overline{K}$ mit $a \neq b$ (wegen der Normalität gilt $b \in K$). Der Fortsetzungssatz 1.48 (für einfache algebraische Erweiterungen liefert $\sigma : k(a) \xrightarrow{\sim} k(b)$ mit $\sigma(a) = b$. Der allgemeine Fortsetzungssatz 1.49 liefert eine Fortsetzung $\widetilde{\sigma} : K \to \overline{K}$ von σ, die wegen der Normalität zu einem $g \in \operatorname{Aut}_k(K) = G$ restringiert. Wegen $g(a) = b \neq a$ folgt $a \notin K^G$ im Widerspruch zur Annahme. □

Theorem 2.11. *Eine Körpererweiterung $k \subset K$ ist genau dann endlich galoissch, wenn es eine endliche Untergruppe $G \subset \operatorname{Aut}(K)$ gibt mit $k = K^G$. Gibt es eine solche Gruppe G, so gilt $G = \operatorname{Gal}(K/k)$.*

Proof. $\Leftarrow$: Satz 2.5 besagt, dass dann $k = K^G \subset K$ endlich und galoissch ist, und dass $G = \operatorname{Gal}(K/k)$ gilt.

$\Rightarrow$: Sei $k \subset K$ galoissch und $G = \operatorname{Gal}(K/k)$. Nach Proposition 2.10 gilt $k = K^G$. Ist $k = K^G \subset K$ zusätzlich endlich, so ist G endlich nach Satz 2.5. □

Ab jetzt behandeln wir nur endliche Galoiserweiterungen (ich will es aber immer dazuschreiben).

Bemerkung: Endliche Galoiserweiterungen sind immer primitiv (Satz 1.85 vom primitiven Element).

Remark 2.12. Ist $G \subset \mathrm{Aut}(K)$ eine endliche Untergruppe, so ergibt das Schlüssellemma 2.1 eine praktische Methode, Minimalpolynome für die endliche Galois-Erweiterung $K^G \subset K$ zu berechnen.

Example 2.13. Die Erweiterung $k = \mathbb{Q} \subset K = \mathbb{Q}(i, \sqrt{2})$ ist endlich und galoissch (Satz 1.63 für Normalität).

Der Fortsetzungssatz 1.48 (für einfache algebraische Erweiterungen) zeigt, dass $G := \mathrm{Gal}(K/k) = \langle\sigma\rangle \times \langle\tau\rangle = \mathbb{Z}/2 \times \mathbb{Z}/2$, wobei $\sigma(i) = -i$, $\sigma(\sqrt{2}) = \sqrt{2}$, und $\tau(i) = i$, $\tau(\sqrt{2}) = -\sqrt{2}$.

Es gilt $k = K^G$. Sei $a = i + 3\sqrt{2}$. Die Bahn von a ist

$$G.a = \{\pm i \pm 3\sqrt{2}\}.$$

Also

$$\begin{aligned}\min_{a/\mathbb{Q}} &= (X - i - 3\sqrt{2})(X + i + 3\sqrt{2})(X - i + 3\sqrt{2})(X + i - 3\sqrt{2}) \\ &= (X^2 - 17 - 6\sqrt{2}i)(X^2 - 17 + 6\sqrt{2}i) \\ &= X^4 - 34X^2 + (289 - 72) \\ &= X^4 - 34X^2 + 361.\end{aligned}$$

Example 2.14. Privat: $K = \mathbb{C}(t)$, $G \subset \mathrm{PGL}(2, \mathbb{C}) \xrightarrow{\sim} \mathrm{Aut}_{\mathbb{C}}(\mathbb{C}(t))$ endlich. Dann ist $K^G \cong \mathbb{C}(w)$ nach Satz von Lüroth. Wir geben Beispiele.

Example 2.15. Beispiel für Berechnung des Invariantenkörpers. Sei $K = \mathbb{C}(t)$ und $G = \mathbb{Z}/2 = \langle\tau\rangle$, wobei $\tau(t) = -t$ und $\tau|_{\mathbb{C}} = \mathrm{id}_{\mathbb{C}}$.

Bahn von t:

$$t \xrightarrow{\tau} -t \xrightarrow{\tau} t$$

Also

$$\begin{aligned}\min_{t/K^G} &= (X - t)(X + t) \\ &= X^2 - t^2.\end{aligned}$$

Also $u := t^2 \in K^G$, und somit

$$\mathbb{C}(u) \subset K^G \subset K.$$

Weil $\min_{t/K^G} \in \mathbb{C}(u)[X]$ und $\mathbb{C}(u)(t) = K$ folgt $[K : \mathbb{C}(u)] \leq 2$. Weil G endlich ist (und damit $K^G \subset K$ endliche Galois-Erweiterung), gilt $[K : K^G] = |G| = 2$. Also $\mathbb{C}(u) = K^G$.

Example 2.16. Interessanteres Beispiel (Aus E. Artin, Algebra): $G = S_3$ auf $\mathbb{C}(t)$ per $\sigma = (12) = \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right] : t \mapsto t^{-1}$, $\tau = (23) = \left[\begin{smallmatrix} -1 & 1 \\ 0 & 1 \end{smallmatrix}\right] : t \mapsto 1 - t$, und $\tau|_{\mathbb{C}} = \sigma|_{\mathbb{C}} = \mathrm{id}_{\mathbb{C}}$.

Dann gilt

$$\mathbb{C}(t)^G = \mathbb{C}(w) \quad \text{für } w = \frac{(t^2 - t + 1)^3}{t^2(t-1)^2}.$$

Denn: Man rechnet leicht nach, dass $\sigma(w) = w$ und $\tau(w) = w$, so dass also $w \in \mathbb{C}(t)^G$. Also haben wir einen Körperturm $\mathbb{C}(w) \subset \mathbb{C}(t)^G \subset \mathbb{C}(t)$. Die

Erweiterung $\mathbb{C}(t)^G \subset \mathbb{C}(t)$ hat Grad $|S_3| = 6$ (nach Satz 2.5). Andererseits erfüllt das Element t offensichtlich die Gleichung

(2.3)
$$(X^2 - X + 1)^3 - wX^2(X-1)^2 \in \mathbb{C}(w)[X]$$
$$\big[\text{ausmultipliziert} = X^6 - 3X^5 + (6-w)X^4 + (2w-7)X^3 + (6-w)X^2 - 3X + 1\big]$$

vom Grad 6 in X, und so hat $\mathbb{C}(w) \subset \mathbb{C}(t)$ Grad ≤ 6. Es folgt $\mathbb{C}(w) = \mathbb{C}(t)^G$, und somit ist (2.3) das Minimalpolynom von t über $\mathbb{C}(w) = \mathbb{C}(t)^G$.

Remark 2.17. Satz von Lüroth (1874): Ist k ein Körper, so hat jeder Zwischenkörper von $k \subset k(t)$ die Form $k(w)$ für ein $w \in k(t)$. (Beweis eventuell später.) Wir haben dies in zwei Beispielen gesehen.

Sei $k \subset K$ eine beliebige Erweiterung, und sei $G := \mathrm{Aut}_k(K)$.

Mündlich: Ist $k \subset E \subset K$ ein Zwischenkörper, so ist $\mathrm{Aut}_E(K) \subset G$ eine Untergruppe. Ist $H \subset G$ eine Untergruppe, so ist K^H ein Zwischenkörper von $k \subset K$.

Also habe Abbildungen

$$\begin{aligned}\{\text{Zwischenkörper von } K/k\} &\rightleftarrows \{\text{Untergruppen von } G = \mathrm{Aut}_k(K)\},\\ E &\mapsto \mathrm{Aut}_E(K),\\ K^H &\hookleftarrow H.\end{aligned}$$

Offensichtlich gelten

$$E \subset K^{\mathrm{Aut}_E(K)}, \quad H \subset \mathrm{Aut}_{K^H}(K). \tag{2.4}$$

und

$$\begin{aligned} E \subset E' \quad &\Rightarrow \quad \mathrm{Aut}_E(K) \supset \mathrm{Aut}_{E'}(K),\\ H \subset H' \quad &\Rightarrow \quad K^H \supset K^{H'}.\end{aligned}$$

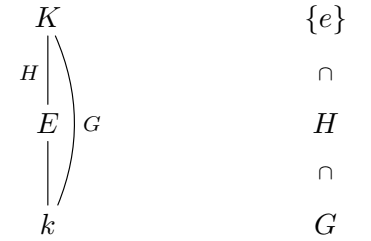
Theorem 2.18 (Hauptsatz der Galoistheorie)**.** *Sei $k \subset K$ eine endliche Galois-Erweiterung mit (endlicher) Galoisgruppe $G = \mathrm{Gal}(K/k)$.*

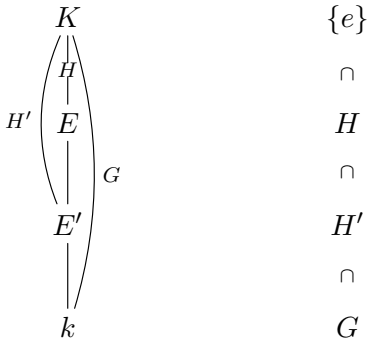
(a) Ist E ein Zwischenkörper, so ist K/E endlich galoissch.
(b) Die Abbildungen

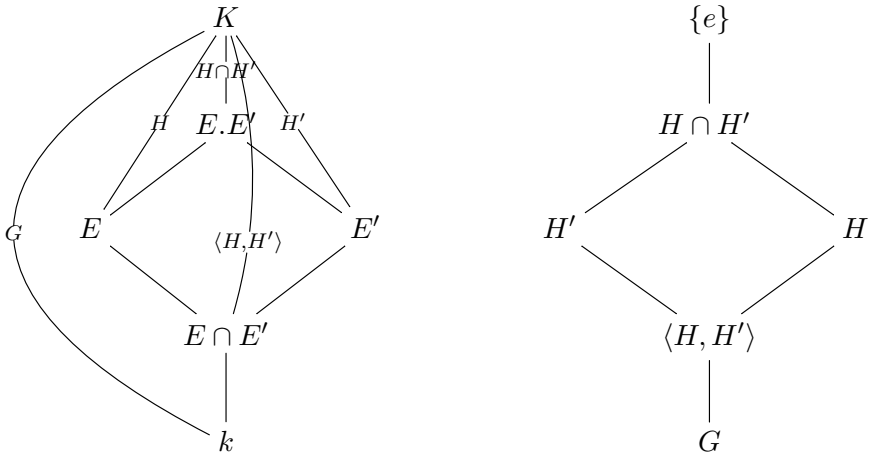
$$\begin{aligned}\{\textit{Zwischenkörper von } K/k\} &\rightleftarrows \{\textit{Untergruppen von } G\},\\ E &\mapsto \mathrm{Gal}(K/E) = \mathrm{Aut}_E(K),\\ K^H &\hookleftarrow H,\end{aligned}$$

sind zueinander inverse Bijektionen, die die Inklusionsrelationen umkehren. Gilt $E \mapsto H$ und $E' \mapsto H'$ so $E.E' \mapsto H \cap H$ und $E \cap E' \mapsto \langle H, H' \rangle$.

Bilder dazu:





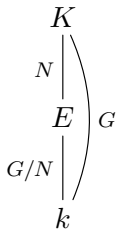


(c) *Ein Zwischenkörper E ist galoissch über k genau dann, wenn* $\mathrm{Gal}(K/E) \subset G$ *ein Normalteiler ist. In diesem Fall ist*

$$G/\operatorname{Gal}(K/E) \xrightarrow{\sim} \operatorname{Gal}(E/k),$$
$$\overline{g} \mapsto g|_E,$$

ein Isomorphismus (von Gruppen).

Bild dazu: Sei $E \mapsto N$ Normalteiler.



Proof. (a): Das ist bekannt.

(b): (Darf $\mathrm{Gal}(K/E)$ schreiben nach (a).)

Sei $k \subset E \subset K$ ein Zwischenkörper. Dann ist $E \subset K$ eine (endliche) Galois-Erweiterung, so dass nach Proposition 2.10 $E = K^{\mathrm{Gal}(K/E)}$ gilt.

Sei $H \subset G$ eine Untergruppe. Es ist H endlich. Nach Satz 2.11, angewandt auf $K^H \subset K$, gilt notwendig $H = \mathrm{Gal}(K/K^H)$. Also sind die beiden Abbildungen zueinander inverse Bijektionen.

Gelten $E \mapsto H$ und $E' \mapsto H'$. Dann $\mathrm{Gal}(K/E.E') = \mathrm{Gal}(K/E) \cap \mathrm{Gal}(K/E') = H \cap H'$, und $K^{\langle H,H'\rangle} = K^H \cap K^{H'}$.

(c): Sei $k \subset E \subset K$ ein Zwischenkörper. Für $g \in G$ beliebig gilt

$$g\,\mathrm{Gal}(K/E)g^{-1} = \mathrm{Gal}(K/g(E)).$$

(Die Inklusion $\subset$ ist trivial, für die Inklusion $\supset$ sei $x \in \mathrm{Gal}(K/g(E))$. Dann $g^{-1}xg \in \mathrm{Gal}(K/E)$ und $x = g(g^{-1}xg)g^{-1}$.)

Ist E/k galoissch, so ist es insbesondere normal, und es gilt für beliebiges $g \in G$, dass $g(E) = E$, also $g\,\mathrm{Gal}(K/E)g^{-1} = \mathrm{Gal}(K/E)$, und somit ist $\mathrm{Gal}(K/E)$ Normalteiler in G.

Sei umgekehrt $\mathrm{Gal}(K/E)$ Normalteiler in G. Sei $x \in \mathrm{Hom}_k(E, \overline{K})$ gegeben. Wir können x fortsetzen zu $g \in \mathrm{Hom}_k(K, \overline{K}) = \mathrm{Aut}_k(K) = G$ (hier verwende Normalität von $k \subset K$). Die Annahme und obiges liefern

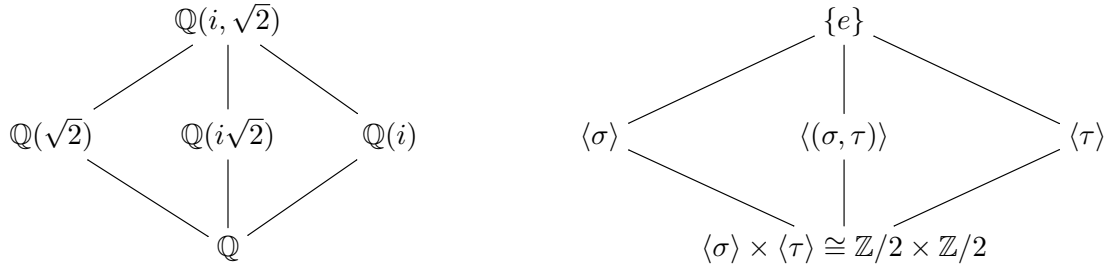
$$\mathrm{Gal}(K/E) = g\,\mathrm{Gal}(K/E)g^{-1} = \mathrm{Gal}(K/g(E)).$$

Nimmt man den Fixkörper beider Seiten, so erhält man $E = g(E) = x(E)$. Also ist $k \subset E$ normal. Separabilität ist trivial.

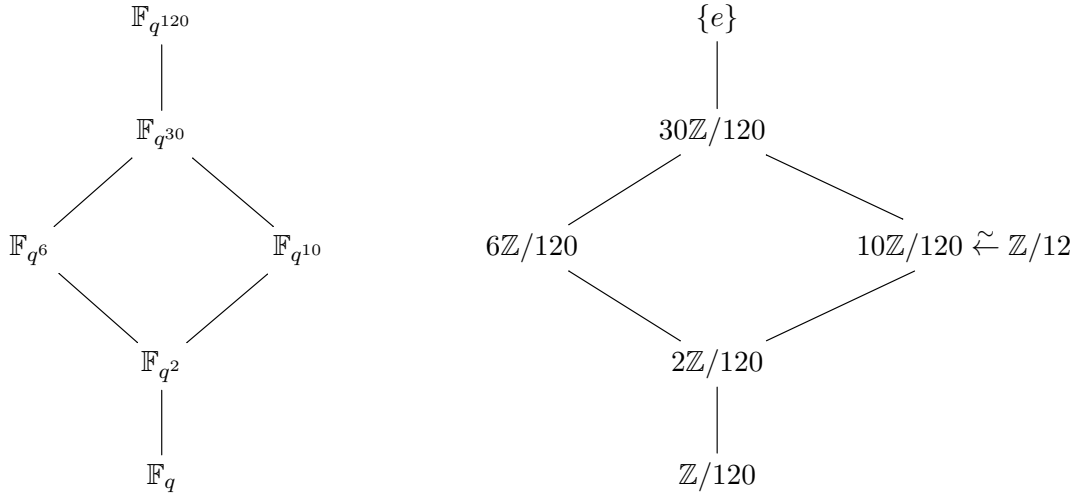
Gelten diese Bedingungen, so ist die Einschränkungsabbildung $G \to \mathrm{Gal}(E/k)$ wohldefiniert und hat als Kern offensichtlich $\mathrm{Gal}(K/E)$. Sie ist surjektiv, denn jeder k-Morphismus $x : E \to E$ läßt sich fortsetzen zu $\widetilde{x} : K \to \overline{K}$, was wegen der Normalität von $k \subset K$ von einem eindeutigen $g \in G$ herkommt. □

Ende 13. Vorlesung Montag 21. Mai 2012

Example 2.19. Fortsetzung von Beispiel 2.13.



Example 2.20.



Es ist $30 = \mathrm{kgV}(6,10)$ und $2 = \mathrm{ggT}(6,10)$.

Remark 2.21. Ist $k \subset K$ eine endlich abelsche (bzw. zyklische) Galois-Erweiterung, so auch $k \subset E$ und $E \subset K$.

Denn: Untergruppen abelscher Gruppen sind stets Normalteiler. Quotienten und Untergruppen abelscher (bzw. zyklischer) Gruppen sind wieder abelsch (bzw. zyklisch).

Corollary 2.22. *Eine endliche separable Körpererweiterung $k \subset K$ hat nur endlich viele Zwischenkörper.*

Vgl. *-Aufgabe, Blatt 5: Endliche Erweiterung genau dann einfach, wenn nur endlich viele Zwischenkörper. Korollar folgt daraus und aus dem Satz 1.85 vom primitiven Element.

Proof. Sei $K = k(A)$, mit $A \subset K$ endlich. Dann ist

$$N = k(\text{Nullstellen der } \min_{a/k} \text{ in } \overline{K}, \text{ für } a \in A)$$

die normale Hülle von $k \subset K$ in $\overline{K}$, siehe Satz 1.65. Es ist N/k endlich und separabel, da alle $\min_{a/k}$ separabel sind. Also ist $k \subset N$ endlich und galoissch, und (sogar) diese Erweiterung hat nur endlich viele Zwischenkörper, da $\mathrm{Gal}(N/k)$ endlich ist. □

Proposition 2.23. *Sei $k \subset K$ ein Körpererweiterung mit Zwischenkörpern E und F.*

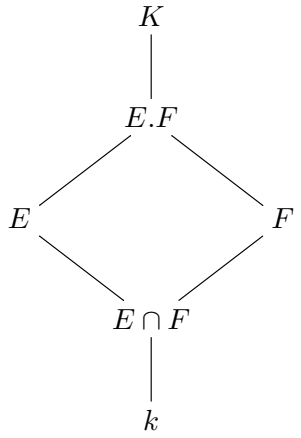
(a) Translationssatz: Sei $k \subset E$ endlich galoissch. Dann sind $F \subset E.F$ und $E \cap F \subset E$ endlich galoissch, und

$$\begin{aligned} \mathrm{Gal}(E.F/F) &\xrightarrow{\sim} \mathrm{Gal}(E/E \cap F), \\ g &\mapsto g|_E, \end{aligned}$$

ist ein Isomorphismus (von Gruppen). Insbesondere gilt

$$[E.F : F] = [E : E \cap F] \text{ teilt } [E : k].$$

Das Diagramm dazu:



(b) Übungsaufgabe:
Seine $k \subset E$ und $k \subset F$ endlich und galoissch. Dann ist $E.F/k$ endlich und galoissch, und

$$\begin{aligned} \mathrm{Gal}(E.F/k) &\hookrightarrow \mathrm{Gal}(E/k) \times \mathrm{Gal}(F/k), \\ g &\mapsto (g|_E, g|_{E'}), \end{aligned}$$

ist injektiv (etwa die diagonale Einbettung im Trivialbeispiel $E = F$) und das Bild sind genau die Paare (σ, τ) mit $\sigma|_{E\cap F} = \tau|_{E\cap F}$.[34] *Insbesondere ist die Abbildung genau dann bijektiv, wenn $k = E \cap F$.*

Proof. (a): Die beiden Erweiterungen sind endlich und galoissch, da sich endlich, separabel und normal (siehe Satz 1.63) entsprechend vererben. Die Abbildung ist ein wohldefinierter Morphismus von Gruppen und offenbar injektiv. Sei H sein Bild. Dann zeigt der Hauptsatz

$$E^H = E \cap (E.F)^{\mathrm{Gal}(E.F/F)} = E \cap F = E^{\mathrm{Gal}(E/E\cap F)},$$

und somit $H = \mathrm{Gal}(E/E \cap F)$. Der Rest ist klar.

(b): Es ist bereits bekannt, dass dann $E.F/k$ endlich und galoissch ist. Die Abbildung ist ein wohldefinierter Morphismus von Gruppen, offensichtlich injektiv, und das Bild erfüllt die genannte Bedingung. Sei (σ, τ) gegeben mit $\sigma|_{E\cap F} = \tau|_{E\cap F} \in \mathrm{Gal}(E \cap F/k)$ (indem diese Gruppe hinschreibe, verwende dass $k \subset E \cap F$ normal und somit galoissch ist). Es ist $\mathrm{Gal}(E.F/k) \to \mathrm{Gal}(E \cap F/k)$ surjektiv (Hauptsatz, oder direkter Fortsetzungssatz plus Normalität).

Sei $g \in \mathrm{Gal}(E.F/k)$ mit $g|_{E\cap F} = \sigma|_{E\cap F} = \tau|_{E\cap F}$.

Dann gelten

$$g^{-1}|_E \circ \sigma \in \mathrm{Gal}(E/E \cap F) \quad \text{und} \quad g^{-1}|_F \circ \tau \in \mathrm{Gal}(F/E \cap F).$$

Nach (a) kommen diese beiden Elemente her von $\widetilde{\sigma} \in \mathrm{Gal}(E.F/F)$ bzw. $\widetilde{\tau} \in \mathrm{Gal}(E.F/E)$. Das Element

$$g \circ \widetilde{\sigma} \circ \widetilde{\tau} \in \mathrm{Gal}(E.F/E)$$

ist nun das gesuchte Urbild, denn es gelten

$$(g \circ \widetilde{\sigma} \circ \widetilde{\tau})|_E = (g \circ \widetilde{\sigma})|_E = g|_E \circ g^{-1}|_E \circ \sigma = \sigma$$

und

$$(g \circ \widetilde{\sigma} \circ \widetilde{\tau})|_F = g_F \circ \widetilde{\sigma}|_F \circ g^{-1}|_F \circ \tau = g_F \circ g^{-1}|_F \circ \tau = \tau.$$

Gilt $k = E \cap F$, so ist die Abbildung offensichtlich bijektiv. Im Fall $k \subsetneq E \cap F$ (was galoissch) kann man $\sigma', \tau' \in \mathrm{Gal}(E \cap F/k)$ verschieden finden (da Kardinalität dieser Galoisgruppe gleich dem Körpergrad). Diese kann man zu $\sigma \in \mathrm{Gal}(E/k)$ bzw. $\tau \in \mathrm{Gal}(F/k)$ fortsetzen. Dann hat das Paar (σ, τ) offensichtlich kein Urbild. □

[34] In besserer Sprache ist also

$$\begin{array}{ccc} \mathrm{Gal}(E.F/k) & \longrightarrow & \mathrm{Gal}(F/k) \\ \downarrow & & \downarrow \\ \mathrm{Gal}(E/k) & \longrightarrow & \mathrm{Gal}(E \cap F/k) \end{array}$$

ein kartesisches (oder Pullback-)Diagramm. Man liest daraus auch sofort

$$[E.F : k][E \cap F : k] = [E : k][F : k]$$

ab, was aber auch nach (a) klar ist.

2.1. **Galois-Gruppe eines Polynoms und Diskriminante.**

Definition 2.24. Sei k ein Körper und $f \in k[X]$ ein separables Polynom. Sei $k \subset K$ ein Zerfällungskörper von f. (Dann ist $k \subset K$ galoissch.) Dann heißt $\mathrm{Gal}(K/k)$ die **Galois-Gruppe von f (über k)**. (Ist bis auf Isomorphismus unabhängig von der Wahl des Zerfällungskörpers.)

Seien k, f und K wie in der Definition, jedoch $f \neq 0$ (uninteressant). Wir können oE annehmen, dass f normiert ist. In $K[X]$ zerfällt f in Linearfaktoren, $f = (X - a_1)(X - a_2)\dots(X - a_n)$. Es ist $\{a_1, a_2, \dots, a_n\}$ die Menge der Nullstellen von f in K. Da f separabel ist, hat diese Menge genau n Elemente.

Observations 2.25. (a) Die Abbildung

$$i : \mathrm{Gal}(K/k) \hookrightarrow \mathrm{Sym}(\{a_1, a_2, \dots, a_n\}) \cong S_n,$$
$$g \mapsto g|_{\{a_1,\dots,a_n\}},$$

ist ein injektiver Morphismus von Gruppen. Somit operiert $\mathrm{Gal}(K/k)$ (treu) auf der Menge der Nullstellen von f.

Beweis: Mit a_i ist auch $g(a_i)$ eine Nullstelle von $f \in k[X]$. Jedes $g \in \mathrm{Gal}(K/k)$ ist injektiv und permutiert deswegen die endlich vielen Nullstellen. Also ist i wohldefiniert.

Die Injektivität von i folgt aus $K = k(a_1, \dots, a_n)$.

(b) Im Allgemeinen ist die obige Abbildung i nicht bijektiv: Da $k \subset K$ separabel und endlich ist, gibt es ein $b \in K$ mit $K = k(b)$ (Satz 1.85 vom primitiven Element). Da $k \subset K$ normal ist, zerfällt $\min_{b/k}$ in $K[X]$ vollständig in Linearfaktoren (Satz-Definition 1.60). Also ist $\mathrm{Gal}(K/k)$ auch die Galoisgruppe des (separablen) Polynoms $\min_{b/k}$, und der entsprechende Morphismus

$$\mathrm{Gal}(K/k) \hookrightarrow \mathrm{Sym}(\text{Nullstellen von } \min_{b/k})$$

ist nicht bijektiv: Sei $m = \deg(\min_{b/k})$. Dann hat die linke Seite m Elemente, die rechte jedoch $m!$.

(c) Sei $\deg(f) \geq 1$ (für $f = 1$ dummerweise falsch). Die Operation von $G = \mathrm{Gal}(K/k)$ auf der Menge der Nullstellen von f ist transitiv genau dann, wenn f irreduzibel ist.

Beweis: Sei $a \in K$ eine Nullstelle von f (verwendet die Annahme $\deg(f) \geq 1$). Nach dem Schlüssellemma 2.1 gilt $\min_{a/k} = \prod_{b \in G.a}(X - b)$, und dies ist ein Teiler von f in $k[X]$. Die Operation ist transitiv genau dann, wenn $\min_{a/k} = f$, was genau dann der Fall ist, wenn f irreduzibel in $k[X]$ ist.

Sei

$$\delta := \prod_{i<j}(a_i - a_j) \in K.$$

(Vorzeichen hängt von der Anordnung $(a_1, a_2, \dots, a_n)$ der Nullstellen von f ab.) Wir identifizieren $\mathrm{Sym}(\{a_1, \dots, a_n) = S_n$ in offensichtlicher Weise.

Observations 2.26. (a) $\delta \neq 0$, da die a_i paarweise verschieden. (auch okay für $f = 1$).

(b) Sei sign : $\mathrm{Sym}(\{a_1, \ldots, a_n) = S_n \twoheadrightarrow \{\pm 1\}$ die Signatur (= der eindeutige Morphismus von Gruppen, der surjektiv ist, falls $n \geq 2$). Dann gilt

$$g(\delta) = \mathrm{sign}(i(g))\delta \quad \text{für } g \in \mathrm{Gal}(K/k).$$

Sei A_n der Kern von sign. Dann sind äquivalent (falls $\mathrm{char}\, k \neq 2$):
(a) $i(\mathrm{Gal}(K/k)) \subset A_n$,
(b) $g(\delta) = \delta$ für alle $g \in \mathrm{Gal}(K/k)$,
(c) $\delta \in k$.
(Aus (a) folgt offensichtlich (b), und aus (b) folgt wegen $\delta \neq 0$, dass $1 - \mathrm{sign}(g) = 0$ in k für alle $g \in \mathrm{Gal}(K/k)$, woraus wegen unserer Annahme an die Charakteristik $1 = \mathrm{sign}(g)$ folgt. Die Äquivalenz von (b) und (c) gilt wegen $k = K^{\mathrm{Gal}(K/k)}$.)

(c) Stets gilt $\Delta := \delta^2 \in k$ (und das ist unabhängig von der Anordnung der a_i).

Definition 2.27. Ist $f \in k[X]$ ein normiertes Polynom vom Grad n, und seien $a_1, \ldots, a_n$ seine Nullstellen (mit Vielfachheit) in einem Zerfällungskörper. So heißt

$$\Delta := \Delta_f := \prod_{i<j} (a_i - a_j)^2$$

die Diskriminante von f. [35]

Remark 2.28.
- Unabhängig von der Anordnung der Nullstellen.
- f ist separabel $\Leftrightarrow \Delta \neq 0$.
- Es gibt eine allgemeine Formel, um Δ aus den Koeffizienten von f zu berechnen (eventuell später). Insbesondere zeigt diese Formel, dass $\Delta \in k$.

2.1.1. *Quadratische Gleichung.* Sei $f = X^2 + bX + c \in k[X]$ (und am Ende $\mathrm{char}\, k \neq 2$).

Seien a_1, a_2 die beiden Wurzeln (eventuell gleich) in einem Zerfällungskörper. Dann $\delta = a_1 - a_2$, $\Delta = (a_1 - a_2)^2 = a_1^2 - 2a_1a_2 + a_2^2$.

$$f = (X - a_1)(X - a_2) = X^2 - (a_1 + a_2)X + a_1a_2.$$

Es folgt

$$\Delta = b^2 - 4c.$$

[35] Manchmal wird auch

$$(-1)^{n(n-1)/2}\Delta = \prod_{i \neq j} (a_i - a_j)$$

als Diskriminante bezeichnet.

Ab jetzt $\operatorname{char} k \neq 2$. Aus $a_1 + a_2 = -b$ und $a_1 - a_2 = \delta$ erhalten wir die Lösungsformeln (wobei δ als $\sqrt{\Delta}$ gewählt)

$$a_{1/2} = \frac{-b \pm \sqrt{\Delta}}{2} = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

[36]

Als Motivation für den kubischen Fall: Sei K ein Zerfällungskörper von f. Dann ist $k \subset K$ galoissch (im Falle, dass f nicht separabel, also $\Delta = 0$, gilt $k = K$) vom Grad ≤ 2. Es folgt

$$\operatorname{Gal}(K/k) \cong \begin{cases} \{\mathrm{id}\}, & \text{falls } \Delta \text{ eine Quadratwurzel in } k \text{ hat,} \\ \mathbb{Z}/2\mathbb{Z} & \text{sonst.} \end{cases}$$

Ende 14. Vorlesung Donnerstag 24. Mai 2012

2.1.2. *Kubische Gleichung.*

Proposition 2.29. *Sei k ein Körper mit $\operatorname{char} k \neq 2$, und sei $f = X^3 + b_2X^2 + b_1X + b_0 \in k[X]$ (normiert und) irreduzibel und separabel*[37]*. Sei $k \subset K$ ein Zerfällungskörper von f. Für die Galoisgruppe von f über k gilt*

$$\operatorname{Gal}(K/k) \cong \begin{cases} A_3 \cong \mathbb{Z}/3\mathbb{Z}, & \textit{falls } \Delta \textit{ eine Quadratwurzel in } k \textit{ hat,} \\ S_3 & \textit{sonst.} \end{cases}$$

Proof. Via i fassen wir $\operatorname{Gal}(K/k) \subset S_3$ als Untergruppe auf. Also ist $|\operatorname{Gal}(K/k)|$ Teiler von $3! = 6$. Da f irreduzibel vom Grad 3 ist, gilt $|\operatorname{Gal}(K/k)| \geq 3$. Es folgt $|\operatorname{Gal}(K/k) = [K : k] \in \{3, 6\}$. Da A_3 die einzige Untergruppe von S_3 der Ordnung 3 ist (die 3-Sylow) (jedes Element von $S_3 \setminus A_3$ hat Ordnung 2), erhalten wir die Behauptung aus (b) in Beobachtung 2.26 (dort ist $\operatorname{char} k \neq 2$ vorausgesetzt). □

Remark 2.30.
- Fall $\operatorname{Gal}(K/k) \cong A_3$: Dann hat $k \subset K$ keine nichttrivialen Zwischenkörper.
- Fall $\operatorname{Gal}(K/k) \cong S_3$: Dann hat $k \subset K$ als nichttriviale Zwischenkörper
  (a) genau drei Zwischenkörper E vom Grad 3 über k entsprechend den Untergruppen (2-Sylows) $\langle(12)\rangle$, $\langle(13)\rangle$, $\langle(23)\rangle$ von S_3.
  (b) genau einen Zwischenkörper vom Grad 2 über k, nämlich $k(\sqrt{\Delta})$, entsprechend der eindeutigen 3-Sylow A_3.

[36] Falls k ein Unterkörpe von $\mathbb{R}$ ist: Je nachdem, ob Δ grösser/gleich/kleiner als Null, sind die Nullstellen reell und verschieden/gibt es genau eine doppelte reelle Nullstelle/gibt es zwei komplex konjugierte nicht reelle Nullstellen.

[37] Ist $\operatorname{char} \neq 3$, so ist das normitert und irreduzible Polynom f wegen $f' = 3X^2 + \cdots \neq 0$ automatisch separabel (siehe Lemma 1.71).

Lösungsformel und Diskriminante. Es gelte $\operatorname{char} k \neq 2, 3$. Betrachte

$$X^3 + b_2X^2 + b_1X + b_0.$$

Die Substitution $X = Z - \frac{1}{3}b_2$ (wegen Charakteristik $\neq 3$ erlaubt) eliminiert das quadratisches Glied, und verändert die Diskriminante nicht.

Es genügt also zu betrachten

$$f = X^3 + bX + c.$$

[38]

Übungsaufgabe: Es gilt: Nach langer(?) Rechnung (geht auch kurz, steht im [FS78, S. 232] verwende wohl $a_1 + a_2 + a_3 = 0$; wir leiten dies etwas einfacher (als die lange Rechnung) in (2.10) aus der Cardano'schen Formel her) erhalte

$$\Delta = -4b^3 - 27c^2. \tag{2.5}$$

Lösungsformel (von Cardano, Tartaglia) für Nullstellen von

$$f = X^3 + bX + c \in k[X], \tag{2.6}$$

wobei k ein Körper mit $\operatorname{char} k \neq 2, 3$ (diese Zahlen tauchen in der folgenden Rechnung im Nenner auf; außerdem ist für die Umformung einer beliebigen kubischen Gleichung in obige Gestalt die Annahme char $\neq 3$ sinnvoll (nötig?)).

Ansatz: Schreibe $x = u + v$. Wir wollen u und v so bestimmen, dass $f(x) = 0$ gilt. Das ist äquivalent zu

$$u^3 + v^3 + (3uv + b)(u + v) + c = 0.$$

Letzteres gilt sicherlich, wenn die beiden Gleichungen

$$3uv = -b, \tag{2.7}$$

$$u^3 + v^3 = -c \tag{2.8}$$

gelten. [39] Wir nehmen nun zunächst an, dass diese beiden Gleichungen lösbar sind, und fixieren eine Lösung (u, v). Sie implizieren

$$\begin{aligned}(u^3 - v^3)^2 &= (u^3 + v^3)^2 - 4u^3v^3 \\ &= c^2 + \frac{4}{27}b^3.\end{aligned}$$

Dann gilt

$$u^3 - v^3 = 2\sqrt{\frac{c^2}{4} + \frac{b^3}{27}} \tag{2.9}$$

[38] Seien a_1, a_2, a_3 die Nullstellen in einem Zerfällungskörper. Also $a_1 + a_2 + a_3 = 0$.

$$\delta = (a_1 - a_2)(a_1 - a_3)(a_2 - a_3).$$

$$f = (X - a_1)(X - a_2)(X - a_3) = X^3 + (a_1a_2 + a_1a_3 + a_2a_3)X - a_1a_2a_3.$$

[39] Dies und der obiges Ansatz $x = u + v$ sind zwei Ansätze, die wie in der Lösung 2.32 plausibel machen.

für die richtige Wahl der Wurzel auf der rechten Seite. Per Addition/Subtraktion von (2.8) folgen

$$u^3 = -\frac{c}{2} + \sqrt{\frac{c^2}{4} + \frac{b^3}{27}},$$
$$v^3 = -\frac{c}{2} - \sqrt{\frac{c^2}{4} + \frac{b^3}{27}},$$

und dann

$$u = \sqrt[3]{-\frac{c}{2} + \sqrt{\frac{c^2}{4} + \frac{b^3}{27}}},$$
$$v = \sqrt[3]{-\frac{c}{2} - \sqrt{\frac{c^2}{4} + \frac{b^3}{27}}},$$

wobei wir hier wieder die dritten Wurzeln richtig wählen müssen.

Dadurch motiviert können wir umgekehrt Lösungen von (2.7) und (2.8) finden. A priori gibt es sowohl für u als auch für v jeweils 6 Wahlen. Trifft man für u eine Wahl eines Radikals, so existiert eine Wahl eines Radikals für v (eindeutig, falls $b \neq 0$), so dass diese beiden Gleichungen gelten. So kann man alle Lösungen von (2.6) finden, und dann auch die obige Formel (2.5) für die Diskriminante überprüfen. Dies war eine Übungsaufgabe.

Ausführliche Lösung der Übungsaufgabe:

Wir wählen eine Quadratwurzel (möglicherweise in einem geeigneten Erweiterungskörper) aus $\frac{c^2}{4} + \frac{b^3}{27}$ und bezeichnen sie mit $\sqrt{\frac{c^2}{4} + \frac{b^3}{27}}$. Dann wählen wir ein Kubikwurzel aus $-\frac{c}{2} + \sqrt{\frac{c^2}{4} + \frac{b^3}{27}}$ und bezeichnen sie mit u_0. Ebenso wählen wir eine Kubikwurzel aus $-\frac{c}{2} - \sqrt{\frac{c^2}{4} + \frac{b^3}{27}}$ und nennen sie v_0'. Dann gilt offensichtlich

$$u_0^3 + v_0'^3 = -c,$$

also löst (u_0, v_0) bereits die Gleichung (2.7). Wegen

$$u_0^3 v_0'^3 = \frac{c^2}{4} - \Big(\frac{c^2}{4} + \frac{b^3}{27}\Big) = \Big(-\frac{b}{3}\Big)^3$$

gibt es genau ein $i \in \{0, 1, 2\}$ so dass

$$u_0 v_0' \zeta^i = -\frac{b}{3}$$

gilt, wobei ζ eine fixierte primitive dritte Einheitswurzel ist. Es folgt, dass

$$(u_0, v_0) := (u_0, v_0' \zeta^i)$$

eine Lösung von (2.8) und offensichtlich auch von (2.7) ist. Wir erhalten insgesamt die folgenden drei Lösungen

$$(u_0, v_0), \quad (u_0\zeta, v_0\zeta^2), \quad (u_0\zeta^2, v_0\zeta)$$

von (2.7) und (2.8). Beachte, dass hier als linker Eintrag genau die möglichen Wahlen der Kubikwurzel auftauchen, und dann die andere Kubikwurzel als der rechte Eintrag gewählt werden muss, um (2.7) zu erfüllen. Die Wahl der Quadratwurzel ist insofern irrelevant, dass sie nur die beiden Einträge der obigen Paare vertauscht (was offensichtlich wieder Lösungen von (2.7) und (2.8) liefert).

Insgesamt zeigt dies, dass die Lösungen von (2.7) und (2.8) genau durch

$$\{(u_0, v_0), (u_0\zeta, v_0\zeta^2), (u_0\zeta^2, v_0\zeta), (v_0, u_0), (v_0\zeta^2, u_0\zeta), (v_0\zeta, u_0\zeta^2)\}$$

gegeben sind. (Es könnnen jedoch Paare übereinstimmen, etwa ist $(0, 0)$ die einzige Lösung, falls $b = c = 0$.)

Damit sind

$$\begin{aligned}\alpha &:= u_0 + v_0,\\ \beta &:= u_0\zeta + v_0\zeta^2,\\ \gamma &:= u_0\zeta^2 + v_0\zeta,\end{aligned}$$

Lösungen von $f(X) = X^3 + bX + c = 0$. Polynomdivision von f durch $X - \alpha$ liefert

$$f = (X - \alpha)(X^2 + \alpha X + (\alpha^2 + b))$$

Dann rechnet man explizit unter Verwendung von $\zeta^2 + \zeta + 1 = 0$ und $3u_0v_0 = -b$ (2.7) nach, dass $X^2 + \alpha X + (\alpha^2 + b) = (X - \beta)(X - \gamma)$ gilt. Insgesamt also

$$f = (X - \alpha)(X - \beta)(X - \gamma),$$

so dass die α, β, γ also genau die Nullstellen von f (in einem geeigneten fixierten Erweiterungskörper) sind.

Eine weitere Rechnung, die neben $\zeta^2 + \zeta + 1 = 0$ auch $\zeta - \zeta^2 = \sqrt{-3}$ verwendet (letzteres gilt, denn ζ ist Nullstelle von $X^2 + X + 1$, also zeigt die Lösungsformel für quadratische Gleichungen $\zeta = \frac{-1+\sqrt{-3}}{2}$ für die richtige Wahl von $\sqrt{-3}$ (bzw. eine Wahl von $\sqrt{3}$ liefert ein ζ)), zeigt

$$(\alpha - \beta)(\alpha - \gamma)(\beta - \gamma) = 3\sqrt{-3}(u_0^3 - v_0^3).$$

Durch Quadrieren erhalten wir mit (2.9) die (obige Formel für die) Diskriminante

$$\Delta = -27(u_0^3 - v_0^3)^2 = -27c^2 - 4b^3. \tag{2.10}$$

Remark 2.31. Entsprechendes läßt sich noch für Gleichungen 4. Grades machen. Aber von Grad 5 an aufwärts ändert sich die Situation grundlegend.

Solution 2.32. Lösung der Sternaufgabe:

Warum Ansatz plausibel:

Identifiziere $A_3 = \mathbb{Z}/3\mathbb{Z} = \{e, g, g^2\}$, wobei $g = (123)$. Sei $k' = k(\zeta)$, wobei ζ eine primitive dritte Einheitswurzel ist. (Da Charakteristik $\neq 3$ gilt $1 \neq \zeta$.)

Wir diagonalisieren im Folgenden schlicht den Endomorphismus g von $k'T_1 \oplus k'T_2 \oplus k'T_3$, auch wenn wir etwas höhere Sprache verwenden. Die Eigenvektoren werden sein s_1, U und V.

Für die Gruppenalgebra $k'A_3$ gilt

$$k'A_3 = k' \times k' \times k' = k'e_0 \times k'e_1 \times k'e_2$$

mit paarweise orthogonalen Idempotenten

$$\begin{aligned} e_0 &= \frac{1}{3}(1 + g + g^2), \\ e_1 &= \frac{1}{3}(1 + \zeta^2 g + \zeta g^2), \\ e_2 &= \frac{1}{3}(1 + \zeta g + \zeta^2 g^2). \end{aligned}$$

(Nachrechnen oder etwa Serre: Linear representations of finite groups, Fourier inversion formula in Chapter 6.2, Proposition 11.)

Es gilt $T_i = e_0T_i + e_1T_i + e_2T_i$. Setzt man[40]

$$\begin{aligned} U &:= \frac{1}{3}(T_1 + \zeta^2 T_2 + \zeta T_3), \\ V &:= \frac{1}{3}(T_1 + \zeta T_2 + \zeta^2 T_3), \end{aligned}$$

so erhält man damit

$$\begin{aligned} T_1 &= \frac{1}{3}s_1 + U + V, \\ T_2 &= \frac{1}{3}s_1 + \zeta U + \zeta^2 V, \\ T_3 &= \frac{1}{3}s_1 + \zeta^2 U + \zeta V. \end{aligned}$$

Beachte, dass $g.s_1 = s_1$ und $g.U = \frac{1}{3}(T_2 + \zeta^2 T_3 + \zeta T_1) = \zeta U$ und $g.V = \zeta^2 V$ gelten. Wir haben also schlicht die Operation von g alias A_3 auf $k'T_1 \oplus k'T_2 \oplus k'T_3$ diagonalisiert.

Die allgemeine Gleichung dritten Grade

$$f(X) = X^3 - s_1X^2 + s_2X - s_3 \in k(T_1, T_2, T_3)^{S_3}[X] \subset k(T_1, T_2, T_3)[X]$$

hat die Lösungen T_1, T_2, T_3. Also hat

$$g(X) := f(X + \frac{1}{3}s_1) = X^3 + bX + c \in k(T_1, T_2, T_3)^{S_3}[X] \subset k(T_1, T_2, T_3)[X]$$

[40] Schreibt man da noch $s_1 = \frac{1}{3}(T_1 + T_2 + T_3)$ dazu, so ist man im wesentlichen bei den drei obersten Formeln auf Seite 273 in [Bos].

die Lösungen

$$\begin{aligned} T_1 - \frac{1}{3}s_1 &= U + V, \\ T_2 - \frac{1}{3}s_1 &= \zeta U + \zeta^2 V, \\ T_3 - \frac{1}{3}s_1 &= \zeta^2 U + \zeta V. \end{aligned}$$

Für $i \in \{0,1,2\}$ ist also $\zeta^i U + \zeta^{2i} V$ eine Lösung von $g(X) = X^3 + bX + c \in k(T_1,T_2,T_3)^{S_3}[X]$. Ausmultipliziert bedeutet dies, dass

$$\underbrace{U^3 + V^3 + c}_{g:1} + \underbrace{U\zeta^i(3UV+b)}_{g:\zeta} + \underbrace{V\zeta^{2i}(3UV+b)}_{g:\zeta^2} = 0$$

in $k(T_1,T_2,T_3)$ gilt. Die durch Klammern zusammengefaßten Terme sind in den Eigenräumen von g mit den angegebenen Eigenwerten (auf $3UV+b$ operiert g durch den Eigenwert 1). Da Eigenräume zu verschiedenen Eigenwerten linear unabhängig sind, folgern wir

$$\begin{aligned} U^3 + V^3 + c &= 0, \\ 3UV + b &= 0. \end{aligned}$$

(Das kann man (vermutlich mühevoll) auch direkt nachrechnen, wenn man b und c in den s_1, s_2, s_3 ausdrückt.) Dies sind genau die Gleichungen (2.7) (2.8).

2.2. **Allgemeine Gleichung n-ten Grades.** Sei k_0 ein Körper und

$$K = k_0(T_1, T_2, \ldots, T_n) = \mathrm{Quot}(k_0[T_1, \ldots, T_n])$$

der rationale Funktionenkörper in n Veränderlichen. Es operiert S_n durch Vertauschen der $T_1, \ldots, T_n$ durch Körperautomorphismen auf K. Also $S_n \subset \mathrm{Aut}(K)$ (klar, dass Operation treu, also wirklich Inklusion). Sei

$$k := K^{S_n}$$

der **Körper der symmetrischen rationalen Funktionen (mit Koeffizienten in** k_0. Es ist uns bereits bekannt, dass $k \subset K$ endlich und galoissch ist, mit $\mathrm{Gal}(K/k) = S_n$ (siehe Satz 2.11).

Aufgabe: Bestimme k.

Nach dem Schlüssellemma 2.1 ist das Minimalpolynom f von T_1 (oder T_2 oder ... oder T_n) über k gegeben durch

$$\begin{aligned} f = f(X) &:= \prod_{i=1}^{n}(X - T_i) \\ &=: \sum_{j=0}^{n}(-1)^j s_j(T_1, \ldots, T_n) X^{n-j} \in K^{S_n}[X] = k[X]. \end{aligned} \tag{2.11}$$

Beachte, dass sogar $f \in k_0[T_1, \ldots, T_n][X]$, also $s_j \in k_0[T_1, \ldots, T_n]^{S_n} \subset K^{S_n} = k$. Dies wird auch aus den folgenden expliziten Formeln klar.

Es heißt s_j das **j-te elementarsymmetrische Polynom in** $T_1, \dots, T_n$. Es ist homogen vom Grad j. Es gelten

$$
\begin{aligned}
s_0 &= 1,\\
s_1 &= T_1 + T_2 + \dots + T_n,\\
s_2 &= \sum_{i_1<i_2} T_{i_1} T_{i_2},\\
&\dots\\
s_j &= \sum_{i_1<i_2<\dots<i_j} T_{i_1} T_{i_2} \dots T_{i_j},\\
&\dots\\
s_n &= T_1 T_2 \dots T_n.
\end{aligned}
\tag{2.12}
$$

Betrachte die Körpererweiterungen

$$k_0(s_1, \dots, s_n) \subset k = \underbrace{K^{S_n} \subset K}_{\text{Grad } |S_n| = n!} .$$

Da andererseits K der Zerfällungskörper von f über $k_0(s_1, \dots, s_n)$ ist und $\deg(f) = n$, gilt $[K : k_0(s_1, \dots, s_n)] \leq n!$. Dies zeigt den ersten Teil des folgenden Satzes 2.35, für dessen Formulierung wir eine weitere Definition benötigen.

Definition 2.33. Sei $E \subset F$ eine Erweiterung von Körpern (oder Ringen). Ein System $(x_1, \dots, x_n)$ von Elementen von F heißt **algebraisch unabhängig** (oder **transzendent**) **über** E, falls der Ringmorphismus

$$
\begin{aligned}
E[X_1, \dots, X_n] &\to F,\\
p(X_1, \dots, X_n) &\mapsto p(x_1, \dots, x_n),
\end{aligned}
$$

injektiv ist, und sonst **algebraisch abhängig**.

Remark 2.34. Ist $(x_1, \dots, x_n)$ algebraisch unabhängig über E, so induziert die obige Abbildung einen Isomorphismus $E[X_1, \dots, X_n] \xrightarrow{\sim} E[x_1, \dots, x_n]$. Sind E und F Körper, so induziert diese Abbildung einen Isomorphismus $E(X_1, \dots, X_n) \xrightarrow{\sim} E(x_1, \dots, x_n)$.

Theorem 2.35. *Es gelten:*

(a) $k_0(s_1, \dots, s_n) = k_0(T_1, \dots, T_n)^{S_n}$.

(b) $s_1, s_2, \dots, s_n$ *sind algebraisch unabhängig über* k_0.

In Worten: Jede symmetrische rationale Funktion in $k_0(T_1, \dots, T_n)$ *läßt sich eindeutig als rationale Funktion in den elementarsymmetrischen Polynomen* $s_1, \dots, s_n$ *darstellen.*

Proof. Aussage (a) ist klar nach dem Obigen. Aussage (b) folgt aus dem folgenden allgemeineren Satz 2.36 (er sagt, dass die offensichtliche Abbildung $k_0[S_1, \dots, S_n] \to k_0[T_1, \dots, T_n]$ injektiv ist; dann ist aber auch die Verknüpfung mit der Inklusion $k_0[T_1, \dots, T_n] \subset k_0(T_1, \dots, T_n)$ injektiv. □

Sei R ein beliebiger Ring (etwa $\mathbb{Z}$ oder ein Körper k_0). Dann operiert S_n auf $R[T_1, \dots, T_n]$ durch Ringautomorphismen (oder genauer Automorphismen von R-Algebren), wir können den Ring $R[T_1, \dots, T_n]^{S_n}$ der Invarianten betrachen; seine Elemente heißen **symmetrische Polynome**. Die oben definierten elementarsymmetrischen Polynome kann man in diesem Setting analog definieren, oder auch direkt per (2.12); sie liegen offenbar in $R[T_1, \dots, T_n]^{S_n}$, was den Namen rechtfertigt.

Theorem 2.36 (Hauptsatz über elementarsymmetrische Polynome)**.** *Sei R ein Ring Es gelten:*

(a) $R[s_1, \dots, s_n] = R[T_1, \dots, T_n]^{S_n}$.
(b) $s_1, s_2, \dots, s_n$ *sind algebraisch unabhängig über* R.

Example 2.37. Das symmetrische Polynom $T_1^2 + T_2^2 + \cdots + T_n^2$ hat (wie in (a) behauptet) die Darstellung

$$T_1^2 + T_2^2 + \cdots + T_n^2 = s_1^2 - 2s_2.$$

Sie ist eindeutig nach (b).

Ende 15. Vorlesung Montag 4. Juni 2012

Proof. Eventuell: Erkläre

$$\begin{aligned} R[T_1, \dots, T_n] &= \bigoplus_{\alpha \in \mathbb{N}^n} RT^\alpha \\ &= \bigoplus_{d \in \mathbb{N}} \underbrace{\bigoplus_{\substack{\alpha \in \mathbb{N}^n \\ \sum \alpha_i = d}} RT^\alpha}_{=: R[T_1, \dots, T_n]_d}, \end{aligned}$$

wobei $T^\alpha = T_1^{\alpha_1} T_2^{\alpha_2} \dots T_n^{\alpha_n}$ in Multiindexschreibweise. Die Elemente von $R[T_1, \dots, T_n]_d$, also die R-Linearkombinationen von Monomen $T_1^{\alpha_1} \dots T_n^{\alpha_n}$ mit $\sum \alpha_i = d$, heißen **homogene Polynome vom Grad** d. Die Operation von S_n erhält die homogenen Komponenten $R[T_1, \dots, T_n]_d$.

Allgemein: Für $n \geq 2$ seien $\sigma'_1, \dots, \sigma'_{n-1}$ die elementarsymmetrischen Polynome in $T_1, \dots, T_{n-1}$. Offenbar gilt (man multiplizere (2.11) für $n-1$ mit $X - T_n$)

$$\begin{aligned} s_1 &= s'_1 + T_n, \\ s_2 &= s'_2 + s'_1 T_n, \\ &\dots \\ s_i &= s'_i + s'_{i-1} T_n, \\ &\dots \\ s_{n-1} &= s'_{n-1} + s'_{n-2} T_n, \\ s_n &= s'_{n-1} T_n. \end{aligned} \tag{2.13}$$

Für beliebiges $1 \le i \le n-1$ gilt danach offensichtlich (unter der Anwesenheit von T_n und s'_{i-1} kann man s_i durch s'_i „ersetzen“ und umgekehrt (dabei $s'_0 = 1$))

$$R[s'_1, \dots, s'_{i-1}, s_i, s_{i+1}, \dots, s_{n-1}, T_n] = R[s'_1, \dots, s'_{i-1}, s'_i, s_{i+1}, \dots, s_{n-1}, T_n],$$

und das impliziert

$$R[s_1, \dots, s_{n-1}, T_n] = R[s'_1, \dots, s'_{n-1}, T_n]. \tag{2.14}$$

(a): Es ist klar, dass $R[s_1, \dots, s_n] \subset R[T_1, \dots, T_n]^{S_n}$ gilt.

Die umgekehrte Inklusion zeigen wir per (äußerer) Induktion über n. Sei $n \ge 2$ (sonst ist die Behauptung offensichtlich). Sei $f \in R[T_1, \dots, T_n]^{S_n}$.

(Alt: Mit homogenen Komponenten bzw. Grad beziehen wir uns stets auf den Totalgrad, das Monom $T_1 T_3^4 T_5^2$ etwa ist homogen vom Grad 7.)

Da jede homogene Komponente von f symmetrisch ist, können wir annehmen, dass f homogen ist vom Grad N. Für $f = 0$ oder $N = 0$ gilt offensichtlich $f \in R[s_1, \dots, s_n]$, so dass wir per (innerer) Induktion $N > 0$ annehmen können.

Wir entwickeln f bezüglich T_n als

$$f = \sum_i f_i(T_1, \dots, T_{n-1}) T_n^i.$$

Dann sind alle f_i symmetrisch in den $T_1, \dots, T_{n-1}$. Per Induktion und (2.14) erhalten wir

$$f_i \in R[T_1, \dots, T_{n-1}]^{S_{n-1}} = R[s'_1, \dots, s'_{n-1}] \subset R[s'_1, \dots, s'_{n-1}, T_n] = R[s_1, \dots, s_{n-1}, T_n].$$

Jedes f_i ist also eine R-Linearkombination von Monomen in den $s_1, \dots, s_{n-1}, T_n$. Insgesamt folgt daraus, dass wir $f = \sum_i f_i T_n^i$ schreiben können als

$$f = p(s_1, \dots, s_{n-1}) + q(s_1, \dots, s_{n-1}, T_n) T_n,$$

mit $p \in R[S_1, \dots, S_{n-1}]$ und $q \in R[S_1, \dots, S_{n-1}, T_n]$. Wir schreiben dies kurz als $f = p(s) + q(s, T_n) T_n$. Da f homogen vom Grad N ist, können wir (durch Weglassen von Monomen in den s_i vom falschen Grad) annehmen, dass $p(s)$ homogen vom Grad N (oder $p(s) = 0$) und $q(s, T_n)$ homogen vom Grad $N - 1$ (oder $q(s, T_n) = 0$) ist.

Es gilt $q(s, T_n) T_n = f - p(s) \in R[T_1, \dots, T_n]^{S_n} + R[s_1, \dots, s_{n-1}] = R[T_1, \dots, T_n]^{S_n}$; dieses Polynom ist durch T_n teilbar und auf Grund der Symmetrie dann auch durch jedes T_i, also auch durch $s_n = T_1 T_2 \dots T_n$. Wir können also schreiben $q(s, T_n) T_n = s_n g$ für ein $g \in R[T_1, \dots, T_n]$ vom Grad $N - n$ (oder $g = 0$). Es gilt $g \in R[T_1, \dots, T_n]^{S_n}$ (denn $s_n g = q(s, T_n) T_n$ ist symmetrisch, so dass für $\sigma \in S_n$ gilt $s_n g = \sigma(s_n g) = s_n \sigma(g)$; da $s_n = T_1 T_2 \dots T_n$ kein Nullteiler in $R[T_1, \dots, T_n]$ ist, folgt $g = \sigma(g)$). Per (innerer) Induktion erhalten wir $g \in R[s_1, \dots, s_n]$. Dies impliziert

$$f = p(s) + q(s, T_n) T_n = p(s) + s_n g \in R[s_1, \dots, s_{n-1}] + s_n R[s_1, \dots, s_n] = R[s_1, \dots, s_n].$$

(b): Sonst sei n minimal, so dass es ein $F \in R[S_1, \dots, S_n]$ gibt mit $F \neq 0$ aber $F(s_1, \dots, s_n) = 0$ in $R[T_1, \dots, T_n]$. Wir können zusätzlich annehmen,

dass F von minimalem Grad (Totalgrad in den S_i, oder Grad in S_n) ist (wobei n fixiert ist). Es gilt sicherlich $n \geq 2$.

Wegen $s_j(T_1, \ldots, T_{n-1}, 0) = s'_j$ (für $1 \leq n-1$) und $s_n(T_1, \ldots, T_{n-1}, 0) = 0$ (vgl. 2.13) folgt aus $F(s_1, \ldots, s_n) = 0$ in $R[T_1, \ldots, T_n]$, dass

$$0 = F(s_1, \ldots, s_n)(T_1, \ldots, T_{n-1}, 0) = F(s'_1, \ldots, s'_{n-1}, 0)$$

in $R[T_1, \ldots, T_{n-1}]$ gilt. Also muss (wegen der Minimalität von n) $F(S_1, \ldots, S_{n-1}, 0) \in R[S_1, \ldots, S_{n-1}]$ das Nullpolynom sein. Es folgt $F = S_n g$ für ein $g \in R[S_1, \ldots, S_n]$. Es gilt $0 = F(s_1, \ldots, s_n) = s_n g(s_1, \ldots, s_n)$. Da s_n kein Nullteiler ist, folgt $g(s_1, \ldots, s_n) = 0$. Der Grad von g ist echt kleiner als der von F, so dass laut Annahme $g = 0$ gelten muss. Dann $F = S_n g = 0$ im Widerspruch zur Annahme. □

Definition 2.38. Sei k_0 ein Körper. Seien $S_1, S_2, \ldots, S_n$ Variablen. Es heißt

$$X^n + S_1 X^{n-1} + \cdots + S_{n-1} X + S_n \in k_0[S_1, S_2, \ldots, S_n][X]$$

das **allgemeine Polynom n-ten Grades über k_0**.

Ein spezielles (normiertes) Polynom $X^n + a_1 X^{n-1} + \cdots + a_n \in k_0[X]$ n-ten Grades ergibt sich durch die Substitution $S_i \mapsto a_i$.

Theorem 2.39. *Das allgemeine Polynom n-ten Grades ist irreduzibel (in $k_0[S_1, S_2, \ldots, S_n][X]$ und) in $k_0(S_1, S_2, \ldots, S_n)[X]$ und separabel. Seine Galois-Gruppe ist die S_n.*

Proof. Wir erinnern daran, dass

$$k := k_0(T_1, \ldots, T_n)^{S_n} \subset K := k_0(T_1, \ldots, T_n)$$

eine Galois-Erweiterung mit Galoisgruppe S_n ist, und dass K der Zerfällungskörper des irreduziblen separablen Polynoms

$$\prod_{i=1}^{n} (X - T_i) = \sum_{j=0}^{n} (-1)^j s_j(T_1, \ldots, T_n) X^{n-j} \in k[X]$$

ist (siehe die Erläuterungen bei (2.11)).

Nach Satz 2.35 gilt

$$k_0(S_1, \ldots, S_n) \xrightarrow{\sim} k_0(s_1, \ldots, s_n) = k$$

via $S_i \mapsto (-1)^i s_i$ (wir dürfen natürlich hier mit den Vorzeichen spielen), und auf Niveau der Polynomringe ist das Bild des allgemeinen Polynoms n-ten Grades gerade das obige Polynom. □

Remark 2.40. Jede endliche Gruppe G tritt als Galois-Gruppe auf:

Per

$$G \to \mathrm{Sym}(G),$$
$$g \mapsto \Big((g\cdot) : h \mapsto gh \Big)$$

können wir G als Untergruppe von $\mathrm{Sym}(G) \cong S_n$, mit $n = |G|$ auffassen (Satz von Cayley). Sei K ein Körper auf dem S_n durch Körperautomorphismen operiert, etwa $K = k_0(T_1, \dots, T_n)$ wie oben. Dann ist $K^G \subset K$ eine Galois-Erweiterung mit Galois-Gruppe G (siehe Satz 2.11).

Theorem 2.41. *Es gibt genau ein Polynom $\Delta_n \in \mathbb{Z}[S_1, \dots, S_n]$, genannt die n-**te Diskriminante**, so dass gilt: Sind $s_1, \dots, s_n \in \mathbb{Z}[T_1, \dots, T_n]$ die elementarsymmetrischen Funktionen in den Variablen $T_1, \dots, T_n$, so gilt*

$$\Delta_n(s_1, \dots, s_n) = \prod_{i<j} (T_i - T_j)^2. \tag{2.15}$$

(Soergel schreibt rechts $\prod_{i \neq j}(T_i - T_j)$, was mir eigentlich besser gefällt... müßte Definition der Diskriminante ändern.)

Proof. Der Morphismus $\mathbb{Z}[S_1, \dots, S_n] \xrightarrow{\sim} \mathbb{Z}[T_1, \dots, T_n]$, $S_i \mapsto s_i$, ist nach Satz 2.36 injektiv mit Bild $\mathbb{Z}[T_1, \dots, T_n]^{S_n}$. Es gilt $\prod_{i<j}(T_i - T_j)^2 \in \mathbb{Z}[T_1, \dots, T_n]^{S_n}$, denn bis auf Vorzeichen ist dieses Produkt gerade $\prod_{i \neq j}(T_i - T_j)$. Die Behauptung folgt. □

Remark 2.42. Vorbemerkung: Ersetzt man in (2.15) jedes T_i durch $-T_i$, so bleibt die rechte Seite unverändert, so dass also

$$\Delta_n(S_1, S_2, S_3, \dots, S_n) = \Delta_n(-S_1, S_2, -S_3, \dots, (-1)^n S_n) \tag{2.16}$$

gilt.

Remark 2.43. Diskriminante als Polynom in den Koeffizienten:

Sei $f = X^n + b_1 X^{n-1} + \dots b_{n-1} X + b_n \in k[X]$ ein normiertes Polynom n-ten Grades mit Koeffizienten in einem Körper (oder einem Ring) k. Seien $a_1, \dots, a_n$ die Nullstellen von f in einem Erweiterungskörper K. In der Notation des Beweises betrachte die Abbildung

$$\begin{aligned} \mathbb{Z}[T_1, \dots, T_n] &\to K, \\ T_i &\mapsto a_i. \end{aligned}$$

Dann gilt $s_i \mapsto (-1)^i b_i$, und somit folgt aus (2.15) und (2.16), dass

$$\Delta_f = \prod_{i<j} (a_i - a_j)^2 = \Delta_n(-b_1, \dots, (-1)^n b_n) = \Delta_n(b_1, \dots, b_n)$$

gilt. Wir erkennen so, dass die Diskriminante Δ_f von f ein „Polynom in den Koeffizienten von f“ ist.

Explizite Formel: Siehe Übungsaufgabe.

2.3. **Einheitswurzeln und Kreisteilungskörper.** Wir fixieren einen Körper k mitsamt einem algebraischen Abschluss $\overline{k}$.

Sei $n \in \mathbb{N}_+ := \mathbb{N} \setminus \{0\}$. Die Nullstellen von $X^n - 1$ in $\overline{k}$ heißen die **n-ten Einheitswurzeln** (sind stets algebraisch über Primkörper). Sei[41]

$$U_n := \{x \in \overline{k} \mid x^n = 1\}$$

[41] In der Literatur ist μ_n gebräuchlich!

die Menge der n-ten Einheitswurzeln (Buchstabe U wohl wegen „n-th roots of **u**nity“). Sie bilden eine Untergruppe der multiplikativen Gruppe $\overline{k}^\times$ von $\overline{k}$.

- Gilt $\operatorname{char} k = 0$, so ist $X^n - 1$ separabel, denn es hat keine gemeinsame Nullstelle mit seiner Ableitung nX^{n-1} (Lemma 1.71). Es folgt $|U_n| = n$.
- Gelte $\operatorname{char} k = p > 0$. Schreibe $n = p^r n'$ mit $p \nmid n'$. Dann ist $X^{n'} - 1$ separabel (denn die einzig mögliche Nullstelle seiner Ableitung $n'X^{n'-1} \neq 0$ ist 0). Wegen $(X^{n'} - 1)^{p^r} = X^n - 1$ gilt $U_n = U_{n'}$, und diese Menge hat n' Elemente.

Beim Studium von U_n können wir uns deswegen stets auf den Fall $\operatorname{char} k \nmid n$ beschränken (auch okay, falls Charakteristik $= 0$).

Theorem 2.44. *Sei $n \in \mathbb{N}_+$ mit $\operatorname{char} k \nmid n$. Dann ist die Gruppe U_n zyklisch von der Ordnung n.*

Proof. Dies folgt aus Obigem und Lemma 1.86. □

Definition 2.45. ($n \in \mathbb{N}_+$ mit $\operatorname{char} k \nmid n$.) Eine Einheitswurzel $\zeta \in U_n$ heißt **primitive n-te Einheitswurzel**, falls sie die Gruppe U_n erzeugt: $U_n = \langle \zeta \rangle$.

Es ist klar, dass eine primitive n-te Einheitswurzel Ordnung n hat.

($n \in \mathbb{N}_+$ mit $\operatorname{char} k \nmid n$.) Sei ζ_n eine primitive n-te Einheitswurzel. Dann ist die Abbildung

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &\xrightarrow{\sim} U_n, \\ i &\mapsto \zeta_n^i, \end{aligned} \tag{2.17}$$

ein Isomorphismus von Gruppen (Abbildung offensichtlich wohldefinierter surjektiver Morphismus von Gruppen, bijektiv wegen Kardinalität).

Example 2.46. Beispiel: In den komplexe Zahlen ist $e^{2\pi i/n}$ eine primitive n-te Einheitswurzel, und es gilt

$$U_n = \{e^{2\pi a i/n} \mid a \in \mathbb{Z}\}.$$

Bild für $n = 6$, teilen den Einheitskreis.

Deswegen heißt $\mathbb{Q}(U_n) = \mathbb{Q}(\zeta)$, wobei ζ eine primitive n-te Einheitswurzel ist, der **n-te Kreisteilungskörper** (englisch: **cyclotomic field**).

Definition 2.47. Die Abbildung

$$\begin{aligned} \varphi : \mathbb{N}_+ &\to \mathbb{N}, \\ n &\mapsto \varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^\times| \end{aligned}$$

heißt **Eulersche φ-Funktion**.

Lemma 2.48. *($n \in \mathbb{N}_+$ mit $\operatorname{char} k \nmid n$.) Die Anzahl der primitiven n-ten Einheitswurzeln ist gerade $\varphi(n)$.*

Proof. Wegen des Isomorphismus (2.17) ist zu zeigen, dass die Erzeuger der additiven Gruppe $\mathbb{Z}/n\mathbb{Z}$ gerade die Elemente von $(\mathbb{Z}/n\mathbb{Z})^\times$ sind. Dies ist offensichtlich. □

Ende 16. Vorlesung Montag 11. Juni 2012

Proposition 2.49.

(a) *Für $n \in \mathbb{N}_+$ gilt*

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \mid a \in \mathbb{Z} \text{ mit } \operatorname{ggT}(a,n) = 1\}. \tag{2.18}$$

Insbesondere

$$\varphi(n) = \#\{a \in \mathbb{N} \mid 0 \le a < n \text{ und } \operatorname{ggT}(a,n) = 1\}$$

(b) *Multiplikativität der φ-Funktion: Sind $m, n \in \mathbb{N}_+$ teilerfremd, so gilt $\varphi(nm) = \varphi(n)\varphi(m)$.*

(c) *Ist p eine Primzahl und $\nu \in \mathbb{N}_+$, so gilt $\varphi(p^\nu) = p^\nu - p^{\nu-1} = p^{\nu-1}(p-1)$.*

(d) *Ist $n = p_1^{\nu_1} p_2^{\nu_2} \dots p_r^{\nu_r}$ die Primfaktorzerlegung von n mit paarweise verschiedenen Primzahlen p_i und Exponenten $\nu_i > 0$, so gilt*

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

Example 2.50. $\varphi(1) = 1$ (da im Nullring $0 = 1$ Einheit).
$\varphi(p) = p - 1$ für p Primzahl.
$\varphi(2000) = \varphi(16 \cdot 125) = \varphi(16)\varphi(125) = (16-8)(125-25) = 800$.

42

Proof. (a): Es ist $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ eine Einheit genau dann, wenn es $x, y \in \mathbb{Z}$ gibt mit $ax + ny = 1$, was genau dann der Fall ist, wenn $\operatorname{ggT}(a,n) = 1$.

(b): Der Chinesische Restsatz liefert $\mathbb{Z}/nm\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Es folgt $(\mathbb{Z}/nm\mathbb{Z})^\times \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$.

(c) Eine Zahl $0 \le a < p^\nu$ erfüllt $\operatorname{ggT}(a, p^\nu) = 1$ genau dann, wenn sie nicht durch p teilbar ist, also nicht eine der $p^{\nu-1}$ Zahlen $0, p, 2p, 3p, \dots, p^\nu - p = (p^{\nu-1} - 1)p$ ist.

(d): Folgt direkt aus (b) und (c). □

Remark 2.51. privat: Die Einheitengruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ ist genau dann zyklisch, wenn $n \in \{1, 2, 4, p^s, 2p^s \mid p \text{ ungerade Primzahl und } s \ge 1\}$. Das ist Satz 6.2 im Zahlentheorie-Skript von Holger Brenner.

[42] Bemerkung: Sei $n = 2^\mu p_1^{\nu_1} p_2^{\nu_2} \dots p_r^{\nu_r}$ die Primfaktorzerlegung von n mit paarweise verschiedenen Primzahlen $p_i \neq 2$ und $\nu_i > 0$, und $\mu \ge 0$. Stets ist $\varphi(2^\mu)$ eine Zweierpotenz. Also ist $\varphi(n)$ eine Zweierpotenz genau dann, wenn für alle $1 \le i \le r$ gilt, dass $\nu_i = 1$ und dass $p_i - 1$ eine Primzahl ist.

Lemma 2.52. *(Ist H eine beliebige Gruppe, so bezeichnet man mit* $\mathrm{Aut}(H)$ *die Menge aller Gruppenautomorphismen $H \xrightarrow{\sim} H$; sie wird mit der Komposition solcher Automorphismen als Multiplikation eine Gruppe.) Sei U eine zyklische Gruppe der Ordnung n (etwa die Gruppe U_n für $n \in \mathbb{N}_+$ mit* $\mathrm{char}\, k \nmid n$*). Dann ist*

$$(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Aut}(U), \quad \overline{r} \mapsto (\zeta \mapsto \zeta^r), \tag{2.19}$$

ein (kanonischer) Isomorphismus von Gruppen. Wir schreiben deshalb Gleichheit,

$$(\mathbb{Z}/n\mathbb{Z})^\times = \mathrm{Aut}(U).$$

Proof. Es genügt zu zeigen, dass

$$(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}), \quad \overline{r} \mapsto (m \mapsto rm),$$

ein Isomorphismus ist. Für eine beliebigen kommutativen Ring R (etwa $R = \mathbb{Z}/n\mathbb{Z}$) ist

$$R \xrightarrow{\sim} \mathrm{End}_R(R), \quad r \mapsto (m \mapsto rm),$$

ein Isomorphismus[43] von Ringen (wobei $\mathrm{End}_R(R)$ die Endomorphismen des R-Moduls R) mit Inversem $\alpha \mapsto \alpha(1)$. Auf den Einheitengruppen induziert er einen Isomorphismus $R^\times \xrightarrow{\sim} \mathrm{Aut}_R(R)$. Für $R = \mathbb{Z}/n\mathbb{Z}$ gilt $\mathrm{Aut}_R(R) = \mathrm{Aut}(R)$. □

Theorem 2.53. *Sei k ein Körper und $\zeta_n \in \overline{k}$ eine primitive n-te Einheitswurzel, wobei $n \in \mathbb{N}_+$ mit* $\mathrm{char}\, k \nmid n$*. Dann ist $k \subset k(\zeta_n)$ eine endliche abelsche Galois-Erweiterung, deren Grad $\varphi(n)$ teilt (es ist ja etwa $\zeta_n \in k$ zugelassen). Die Abbildung*

$$\psi : \mathrm{Gal}(k(\zeta_n)/k) \hookrightarrow \mathrm{Aut}(U_n) = (\mathbb{Z}/n\mathbb{Z})^\times, \quad g \mapsto g|_{U_n}, \tag{2.20}$$

ist ein injektiver Morphismus von Gruppen (die Gleichheit ist (2.19)*).*

Proof. Da $k(\zeta_n) = k(U_n)$ Zerfällungskörper des separablen Polynoms $X^n - 1$ ist, ist $k \subset k(\zeta_n)$ eine endliche Galois-Erweiterung. Es ist klar, dass ψ wohldefiniert ist und die angegebenen Eigenschaften hat. Also können wir $\mathrm{Gal}(k(\zeta_n)/k)$ als Untergruppe der abelschen Gruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ auffassen. Dies zeigt, dass die Galois-Erweiterung $k \subset k(\zeta_n)$ abelsch ist und dass ihr Grad ein Teiler von $\varphi(n)$ ist. □

[43] Das stimmt auch, falls R nicht kommutativ: Dann muss rechts R als Rechts-R-Modul auffassen.

Theorem 2.54 (Kreisteilungskörper)**.** *Sei $\zeta_n \in \overline{\mathbb{Q}}$ eine primitive n-te Einheitswurzel. Dann ist der n-te Kreisteilungskörper $\mathbb{Q}(\zeta_n)$ eine endliche abelsche Galois-Erweiterung von $\mathbb{Q}$ vom Grad $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ mit Galois-Gruppe*

$$\operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \xrightarrow{\sim} \operatorname{Aut}(U_n) = (\mathbb{Z}/n\mathbb{Z})^\times,$$

wobei der Isomorphismus die Restriktion auf U_n ist, und die Gleichheit der kanonische Isomorphismus (2.19)*.*

Wir bestimmen in Satz 2.58 das Minimalpolynom über $\mathbb{Q}$ einer primitiven Einheitswurzel. Damit kann man dann auch praktisch rechnen (etwa per Computer).

Wir erinnern an den Satz von Gauss und insbesondere an ein Korollar: Sei R ein faktorieller Ring. Wir fixieren ein Repräsentantensystem P der Primelemente von R. Ist $x \neq 0$ ein Element des Quotientenkörper $Q(R)$ von R, so hat es eine eindeutige Zerlegung $x = \varepsilon \prod_{p\in P} p^{\nu_p(x)}$, wobei $\varepsilon \in R^\times$ eine Einheit ist und $\nu_p(x) \in \mathbb{Z}$ für alle $p \in P$, und fast alle $\nu_p(x) = 0$ sind. Dies definiert die ganzen Zahlen $\nu_p(x)$. Wir setzen $\nu_p(0) = \infty$. Für $x \in Q(R)$ ist dann $x \in R$ äquivalent zu $\nu_p(x) \geq 0$ für alle $p \in P$. Offenbar gilt

$$\nu_p(xy) = \nu_p(x) + \nu_p(y)$$

für alle $x, y \in Q(R)$ und $p \in P$.

Wir setzen $\nu_p : Q(R) \to \mathbb{Z} \cup \{\infty\}$ wie folgt fort zu $\nu_p : Q(R)[X] \to \mathbb{Z} \cup \{\infty\}$. Für ein Polynom $f = \sum_i a_i X^i \in Q(R)[X]$ und $p \in P$ setzt man

$$\nu_p(f) := \min_i \nu_p(a_i).$$

Es ist $f = 0$ genau dann, wenn ein/alle $\nu_p(f) = \infty$. Es gilt $f \in R[X]$ genau dann, wenn $\nu_p(f) \geq 0$ für alle $p \in P$.

Lemma 2.55 (siehe [Bos, 2.7 Lemma 5])**.** *Es sei R ein faktorieller Ring. Für $f, g \in Q(R)[X]$ gilt dann*

$$\nu_p(fg) = \nu_p(f) + \nu_p(g)$$

für alle Primelemente $p \in P$.

Proof. Ist f oder g konstant, also in $Q(R)$, so gilt die Gleichung offenbar. Ebenso ist die Gleichung trivial, falls f oder g Null ist.

Wir nehmen zunächst an, dass $\nu_p(f) = 0$ und $\nu_p(g) = 0$ gelten für alle $p \in P$. Es ist zu zeigen, dass $\nu_p(fg) = 0$ gilt. Wir fixieren dafür ein $p \in P$. Betrachte den Reduktionsmorphismus

$$\Phi : R[X] \to (R/pR)[X].$$

Es gilt

$$\ker \Phi = \{h \in R[X] \mid \nu_p(h) > 0\}.$$

Laut Annahme folgt $\Phi(f) \neq 0$ und $\Phi(g) \neq 0$. Da R/pR und damit $(R/pR)[X]$ Integritätsringe sind, folgt $\Phi(fg) = \Phi(f)\Phi(g) \neq 0$, also $\nu_p(fg) = 0$.

Seien nun f und g allgemein. Sei $a = \prod_{p\in P} p^{-\nu_p(f)} \in Q(R)$. Dann gilt

$$\nu_p(af) = \nu_p(a) + \nu_p(f) = 0$$

für alle $p \in P$. Analog definieren wir $b \in Q(R)$, so dass $\nu_p(bg) = 0$ für alle $p \in P$ gilt. Mit dem bereits Bewiesenen erhalten wir nun

$$\begin{aligned}\nu_p(fg) + \nu_p(a) + \nu_p(b) &= \nu_p(afbg)\\ &= \nu_p(af) + \nu_p(bg)\\ &= \nu_p(f) + \nu_p(a) + \nu_p(g) + \nu_p(b)\end{aligned}$$

und somit die Behauptung. □

Corollary 2.56 (siehe [Bos, 2.7 Korollar 6])**.** *Sei R ein faktorieller Ring und $h \in R[X]$ ein normiertes Polynom. Sind $f, g \in Q(R)[X]$ normierte Polynome mit $h = fg$ (in $Q(R)[X]$), so gilt bereits $f, g \in R[X]$.*

Proof. Sei $p \in P$ fixiert. Da h normiert ist und in $R[X]$ liegt, gilt $\nu_p(h) = 0$. Das Lemma 2.55 von Gauss zeigt

$$0 = \nu_p(h) = \nu_p(f) + \nu_p(g).$$

Da f und g normiert sind, gelten $\nu_p(f) \leq 0$ und $\nu_p(g) \leq 0$. Es folgt $\nu_p(f) = \nu_p(g) = 0$. Da p beliebig war, folgt die Behauptung. □

Proof. Sei $f := \min_{\zeta_n/\mathbb{Q}}$. Nach Satz 2.53 wissen wir, dass $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg(f) \mid \varphi(n)$ gilt. Somit müssen wir $\deg(f) \geq \varphi(n)$ zeigen.

Wir zeigen dafür, dass jede der $\varphi(n)$ primitiven n-ten Einheitswurzeln eine Nullstelle von f ist.

Offenbar ist f ein Teiler von $X^n - 1$ (denn dies hat ζ_n als Nullstelle), wir finden also ein $h \in \mathbb{Q}[X]$ mit

$$X^n - 1 = fh.$$

Da $X^n - 1$ und f beide normiert sind, ist auch h normiert, so dass Korollar 2.56 $f, h \in \mathbb{Z}[X]$ zeigt.

Sei $\zeta \in U_n$ eine primitive n-te Einheitswurzel. Dann $\zeta = \zeta_n^a$ für ein $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, n) = 1$ (denn unter dem Isomorphismus (2.17) entsprechen die primitiven n-ten Einheitswurzeln genau $(\mathbb{Z}/n\mathbb{Z})^\times$, wie im Beweis von Lemma 2.48 erklärt, und weiter verwende man (2.18)). Also ist a ein Produkt von Primzahlen, die n nicht teilen.

Es genügt also zu zeigen, dass für eine Primzahl p mit $p \nmid n$ auch (die primitive n-te Einheitswurzel) ζ_n^p eine Nullstelle von f ist.[44]

Angenommen, dies ist nicht der Fall. Wegen $0 = (X^n - 1)(\zeta_n^p) = f(\zeta_n^p)h(\zeta_n^p)$ folgt dann $h(\zeta_n^p) = 0$. Also ist ζ_n Nullstelle von $h(X^p)$, so dass also $h(X^p) = fg$ für ein (normiertes) $g \in \mathbb{Q}[X]$. Wie oben zeigt Korollar 2.56, dass $g \in \mathbb{Z}[X]$. Reduktion modulo p

$$\begin{aligned} \mathbb{Z}[X] &\to \mathbb{Z}/p\mathbb{Z}[X] = \mathbb{F}_p[X], \\ s &\mapsto \overline{s}, \end{aligned}$$

liefert $\overline{h}^p = \overline{h}(X^p) = \overline{h(X^p)} = \overline{f}\overline{g}$. Dies zeigt, dass $\overline{f}$ (was Grad ≥ 1 hat) und $\overline{h}$ nicht teilerfremd in $\mathbb{F}_p[X]$ sind, also insbesondere eine gemeinsame Nullstelle in $\overline{\mathbb{F}}_p$ haben. Folglich hat das Polynom $X^n - 1 = \overline{fh} \in \mathbb{F}_p[X]$ in $\overline{\mathbb{F}}_p$ eine mehrfache Nullstelle. Es ist aber separabel, denn seine Ableitung $nX^{n-1} \neq 0$ hat höchstens die Nullstelle 0. Dieser Widerspruch zeigt, dass $f(\zeta_n^p) = 0$ gelten muss. □

[44] Besser: Ist ζ_n' eine beliebige primitive n-te Einheitswurzel, die Nullstelle von f ist, so ist auch $\zeta_n'^p$ Nullstelle von f.

Definition 2.57. Sei k ein Körper und $n \in \mathbb{N}_+$ mit $\operatorname{char} k \nmid n$. Seien $\zeta_1, \dots, \zeta_{\varphi(n)}$ die primitiven n-ten Einheitswurzeln in $\overline{k}$. Dann heißt

$$\Phi_n = \prod_{i=1}^{\varphi(n)} (X - \zeta_i)$$

das **n-te Kreisteilungspolynom über k**.

Theorem 2.58.

(a) *Φ_n ist ein normiertes separables Polynom* $\boxed{\text{in } k[X]}$ *vom Grad $\varphi(n)$.*
(b)

$$X^n - 1 = \prod_{d|n, d>0} \Phi_d. \tag{2.21}$$

(c) *Für $k = \mathbb{Q}$ ist Φ_n das Minimalpolynom jeder primitiven n-ten Einheitswurzel über $\mathbb{Q}$ (und damit insbesondere irreduzibel in $\mathbb{Q}[X]$). Es gilt sogar $\Phi_n \in \boxed{\mathbb{Z}[X]}$, und Φ_n ist irreduzibel in $\mathbb{Z}[X]$.*
(d) *Ist k ein Körper mit $\operatorname{char} k \nmid n$, so ist das Bild des n-ten Kreisteilungspolynoms $\Phi_n \in \mathbb{Z}[X]$ über $\mathbb{Q}$ unter $\mathbb{Z}[X] \to k[X]$ das n-te Kreisteilungspolynom über k.*

Remark 2.59. Teil (b) liefert eine induktive Methode zur Berechnung der Kreisteilungspolynome.

Beispiele (über $\mathbb{Q}$):

$$\Phi_1 = X - 1.$$

Sei p eine Primzahl.

$$\begin{aligned} \Phi_p &= \frac{X^p - 1}{\Phi_1} \\ &= \frac{X^p - 1}{X - 1} \\ &= X^{p-1} + X^{p-2} + \dots X + 1. \end{aligned}$$

Mehr Beispiele:

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

Undsoweiter.

Ende 17. Vorlesung Donnerstag 14. Juni 2012.

Proof. (a): Jedes Element von $\mathrm{Gal}(k(U_n)/k)$ induziert einen Automorphismus von U_n, der die primitiven n-ten Einheitswurzeln (= die Erzeuger der Gruppe) permutiert. Also $\Phi_n \in (k(U_n)[X])^{\mathrm{Gal}(k(U_n)/k)} = k[X]$.

(b): Beachte, dass aus $d|n$ folgt, dass $\mathrm{char}\, k \nmid d$, so dass also Φ_d definiert ist. Es gilt $X^n-1 = \prod_{\zeta\in U_n}(X-\zeta)$, und jedes $\zeta \in U_n$ ist primitive $\mathrm{ord}(\zeta)$-te Einheitswurzel, und die Ordnung von ζ ist ein Teiler von $|U_n| = n$. Man fasse die Linearfaktoren also entsprechend zusammen.

(c): Ist $\zeta \in \overline{\mathbb{Q}}$ eine primitive n-te Einheitswurzel, so ist ζ Nullstelle des Polynoms $\Phi_n \in \mathbb{Q}[X]$ vom Grad $\varphi(n)$. Also $\min_{\zeta/\mathbb{Q}} \mid \Phi_n$. Nach Satz 2.54 gilt

$$\deg(\min_{\zeta/\mathbb{Q}}) = [\mathbb{Q}(\zeta):\mathbb{Q}] = \varphi(n) = \deg(\Phi_n).$$

Es folgt $\min_{\zeta/\mathbb{Q}} = \Phi_n$.

(Alternative: Aus Satz 2.54 folgt, dass die Bahn einer primitiven n-ten Einheitswurzel unter $\mathrm{Gal}(k(\zeta_n)/k)$ die Menge der primitiven n-ten Einheitswurzeln ist. Das Schlüssellemma 2.1 liefert somit, dass $\min_{\zeta/\mathbb{Q}} = \Phi_n$.)

Da das normierte Polynom Φ_n ein Teiler des ganzzahligen normierten Polynoms X^n-1 ist (in $\mathbb{Q}[X]$), zeigt Korollar 2.56, dass $\Phi_n \in \mathbb{Z}[X]$. Dieses Polynom ist irreduzibel in $\mathbb{Z}[X]$ (es ist als normiertes Polynom primitiv in $\mathbb{Z}[X]$ und nach obigem irreduzibel in $\mathbb{Q}[X]$; also können wir [Bos, Satz 2.7/7] verwenden).

(d): Sei k fixiert. Wir zeigen die Aussage per Induktion für alle n mit $\mathrm{char}\, k \nmid n$. Für solche n sei $\Phi_n \in \mathbb{Z}[X]$ das n-te Kreisteilungspolynom über $\mathbb{Q}$ und $\widetilde{\Phi}_n$ dasjenige über k. Sei $\tau : \mathbb{Z}[X] \to k[X]$ der kanonische Morphismus. Zu zeigen ist $\tau(\Phi_n) = \widetilde{\Phi}_n$ für alle n wie oben.

Es gilt $\Phi_1 = X-1$ und $\widetilde{\Phi}_1 = X-1$, so dass die Aussage sicherlich für $n=1$ stimmt. Sei nun $n>1$. Wir wissen (2.21) sowohl für $\mathbb{Q}$ als auch für

k. Damit erhalten wir

$$X^n - 1 = \tau(\Phi_n) \prod_{d|n, 0<d<n} \tau(\Phi_d)$$

und

$$X^n - 1 = \widetilde{\Phi}_n \prod_{d|n, 0<d<n} \widetilde{\Phi}_d$$

in $k[X]$. Per Induktion gilt für alle Teiler $0 < d < n$ von n, dass $\tau(\Phi_d) = \widetilde{\Phi}_d$. Da $k[X]$ nullteilerfrei ist, folgt somit $\tau(\Phi_n) = \widetilde{\Phi}_n$. □

Remark 2.60. Wir geben den Satz von Kronecker-Weber ohne Beweis:

Theorem 2.61 (Satz von Kronecker-Weber). *Jede endliche abelsche Galois-Erweiterung der rationalen Zahlen ist in einem Kreisteilungskörper enthalten: Ist $\mathbb{Q} \subset K$ eine endliche abelsche Galois-Erweiterung, so $K \subset \mathbb{Q}(U_n)$ für ein geeignetes $n \in \mathbb{N}_+$ (hier $U_n \subset \overline{K}$).*

Beispiel: Ist $z \in \mathbb{C}$ algebraisch über $\mathbb{Q}$ mit abelscher Galoisgruppe (= Galoisgruppe der normalen Hülle von $\mathbb{Q} \subset \mathbb{Q}(Z)$), so ist z eine $\mathbb{Q}$-Linearkombination von Einheitswurzeln. (Ist $z \in \mathbb{C}$ eine ganzalgebraische Zahl mit abelscher Galoisgruppe, so ist z eine $\mathbb{Z}$-Linearkombination von Einheitswurzeln.)

Beispiel $\sqrt{5}$ ist ganzalgebraisch, da Nullstelle des normierten Polynoms $X^2 - 5 \in \mathbb{Z}[X]$. (das ist aus Wikipedia; falls Aufgabe, so bitte leicht variieren) Wir behaupten

$$\sqrt{5} = 1 + 2\zeta^2 + 2\zeta^3$$

wobei ζ eine primitive fünfte Einheitswurzel ist.

Beweis: Das Quadrat der rechten Seite ist

$$\begin{aligned} &1 + 2\zeta^2 + 2\zeta^3 \\ &+2\zeta^2 + 4\zeta^4 + 4 \\ &+2\zeta^3 + 4 + 4\zeta = 1 + 4 + 4\underbrace{(1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4)}_{=\Phi_4(\zeta)=0} = 5. \end{aligned}$$

Theorem 2.62. *Sei q eine Prim(zahl)potenz und $\mathbb{F}_q$ der Körper mit q Elementen. Gelte $\operatorname{ggT}(n, q) = 1$ (also $\operatorname{char} \mathbb{F}_q \nmid n$), und sei $\zeta \in \overline{\mathbb{F}}_q$ eine primitive n-te Einheitswurzel.*

(a) Die Injektion

$$\psi : \operatorname{Gal}(\mathbb{F}_q(\zeta)/\mathbb{F}_q) \hookrightarrow \operatorname{Aut}(U_n) = (\mathbb{Z}/n\mathbb{Z})^\times$$

aus (2.20) *bildet den relativen Frobenius Fr_q auf $\overline{q} \in (\mathbb{Z}/n\mathbb{Z})^\times$ ab (wegen $\operatorname{ggT}(n, q) = 1$ ist $\overline{q}$ wirklich eine Einheit in $\mathbb{Z}/n\mathbb{Z}$). Insbesondere induziert ψ einen Isomorphismus*

$$\psi : \operatorname{Gal}(\mathbb{F}_q(\zeta)/\mathbb{F}_q) \xrightarrow{\sim} \langle \overline{q} \rangle \subset (\mathbb{Z}/n\mathbb{Z})^\times.$$

(b) *Es gilt*

$$[\mathbb{F}_q(\zeta) : \mathbb{F}_q] = |\operatorname{Gal}(\mathbb{F}_q(\zeta)/\mathbb{F}_q)| = \operatorname{ord}(\overline{q}; (\mathbb{Z}/n\mathbb{Z})^\times).$$

Ist also $d = \operatorname{ord}(\overline{q}; (\mathbb{Z}/n\mathbb{Z})^\times)$ *diese Ordnung, so gilt* $\mathbb{F}_q(\zeta) = \mathbb{F}_{q^d}$.

(c) *Das* n*-te Kreisteilungspolynom* Φ_n *über* $\mathbb{F}_q$ *ist genau dann irreduzibel in* $\mathbb{F}_q[X]$*, wenn* $\overline{q}$ *die Gruppe* $(\mathbb{Z}/n\mathbb{Z})^\times$ *erzeugt.*

Insbesondere: Ist $(\mathbb{Z}/n\mathbb{Z})^\times$ *nicht zyklisch, so ist* Φ_n *über* $\mathbb{F}_q$ *nicht irreduzibel (für alle Primzahlpotenzen* q *mit* $\operatorname{ggT}(n, q) = 1$ *wie oben angegeben).*

Proof. Diese Aussagen folgen allesamt direkt aus den bereits vorhandenen Resultaten (abgesehen von den Resultaten dieses Kapitels benötigt man Satz 1.105).

(a): Der relative Frobenius Fr_q erhebt jedes Element in die q-te Potenz, und somit auch jede Einheitswurzel. Dies ist aber genau der Automorphismus von U_n, der dem Element $\overline{q} \in (\mathbb{Z}/n\mathbb{Z})^\times$ unter dem Isomorphismus (2.19) entspricht.

(b): klar.

(c): Die Gruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ wird von $\overline{q}$ erzeugt genau dann, wenn in

$$\deg(\min\nolimits_{\zeta/\mathbb{F}_q}) = [\mathbb{F}_q(\zeta) : \mathbb{F}_q] = \operatorname{ord}(\overline{q}; (\mathbb{Z}/n\mathbb{Z})^\times) \boxed{=} |(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n) = \deg(\Phi_n)$$

die hervorgehobene Gleichheit gilt; die anderen Gleichheiten sind bereits bekannt. Da $\Phi_n(\zeta) = 0$ gilt, ist dies äquivalent zu $\Phi_n = \min_{\zeta/\mathbb{F}_q}$. □

Remark 2.63. nicht in Vorlesung gemacht, da bereits im Satz oben integriert.

Es kann also Φ_n nur dann irreduzibel sein über einem endlichen Körper (dessen Charakteristik kein Teiler von n ist), falls $(\mathbb{Z}/n\mathbb{Z})^\times$ zyklisch ist, vergleiche Bemerkung 2.51.

Beispiel dazu, nicht in Vorlesung gemacht.

- $(\mathbb{Z}/4\mathbb{Z})^\times$ zyklisch, erzeugt von $\overline{3}$. Also ist $\Phi_4 = X^2 + 1$
  - irreduzibel über $\mathbb{F}_3$ oder $\mathbb{F}_7$ (denn $\overline{3} = \overline{7} = \overline{1} \in (\mathbb{Z}/4\mathbb{Z})^\times$ ist Erzeuger), aber
  - nicht irreduzibel über $\mathbb{F}_9$ oder $\mathbb{F}_5$ (denn $\overline{9} = \overline{5} = \overline{1} \in (\mathbb{Z}/4\mathbb{Z})^\times$ hat Ordnung 1).
- $(\mathbb{Z}/8\mathbb{Z})^\times$ ist nicht zyklisch, denn die drei nichttrivialen Elemente $\overline{3}, \overline{5}, \overline{7}$ haben alle Ordnung 2.

  Das 8-te Kreisteilungspolynom ist

$$\begin{aligned} \Phi_8 &= \frac{X^8 - 1}{\Phi_1 \Phi_2 \Phi_4} \\ &= \frac{X^8 - 1}{(X-1)(X+1)(X^2+1)} \\ &= \frac{X^8 - 1}{X^4 - 1} \\ &= X^4 + 1 \end{aligned} \tag{2.22}$$

Es ist nicht irreduzibel in jedem $\mathbb{F}_q[X]$ (auch für $q = 2$, denn $(X+1)^4 = X^4 + 1$, falls man es dort als Bild des Kreisteilungspolynoms über $\mathbb{Q}$ definiert). Beispielsweise haben wir

$$X^4+1 = X^4+4X^2+4-X^2 = ((X^2+2)+X)((X^2+2)-X) = (X^2+X+2)(X^2-X+2)$$

in $\mathbb{F}_3[X]$ oder

$$X^4 + 1 = (X^2 + 2)(X^2 - 2) = (X^2 + 2)(X^2 + 3)$$

in $\mathbb{F}_5[X]$.

2.4. **Konstruktion des regelmäßigen n-Ecks.** Ziel: Satz 2.65. Eine Implikation bereits klar. Für die andere benötige Vorarbeit, nämlich die Implikation (c) ⇒ (a) des folgenden Satzes 2.64. (Könnte als die andere Implikation weglassen.)

Wir erweitern Korollar 1.36 um eine äquivalente Bedingung.

Theorem 2.64. *Sei $M \subset \mathbb{C}$ eine Teilmenge mit $0, 1 \in M$, und sei $a \in \mathbb{C}$. Dann sind äquivalent:*

(a) a ist konstruierbar aus M (also $a \in \operatorname{Kon}(M)$).
(b) Es gibt einen Körperturm

$$\mathbb{Q}(M \cup \overline{M}) = L_0 \subset L_1 \subset \cdots \subset L_n \subset \mathbb{C} \tag{2.23}$$

mit $a \in L_n$ und $[L_i : L_{i-1}] = 2$ für alle $1 \le i \le n$.
(c) a ist enthalten in einer Galois-Erweiterung L von $\mathbb{Q}(M \cup \overline{M})$ von Zweierpotenzgrad (mit $L \subset \mathbb{C}$).

Proof. Die Äquivalenz von (a) und (b) ist bereits gezeigt, siehe Korollar 1.36.

(b) ⇒ (c):

Sei $k := L_0$ und $K := L_n$. Sei $K = k(b)$ nach dem Satz 1.85 vom primitiven Element (wir sind in Charakteristik Null) für ein $b \in K$. Sei $N = 2^n$ und seien $b = b_1, b_2, \dots, b_N$ die Nullstellen[45] von $\min_{b/k}$ in $\mathbb{C}$. Dann ist

$$E = k(b_1, \dots, b_N) = k(b_1).k(b_2).\cdots.k(b_N) \tag{2.24}$$

die normale Hülle von $k \subset K$ in $\mathbb{C}_{\mathrm{alg}/k}$, siehe Satz 1.65. Es ist $k \subset E$ eine endliche Galoiserweiterung, mit $a \in E$. Da alle $k(b_i)$ isomorph sind, entstehen sie alle durch sukzessives Ziehen von Quadratwurzeln aus k (reicht auch: Adjungieren von Elementen von Grad 2). Insgesamt entsteht also E aus k durch sukzessives Ziehen von Quadratwurzeln (reicht: Adjungieren von Elementen von Grad 1 oder 2), und somit hat $k \subset E$ Zweierpotenzgrad.

Besser (ohne Satz vom primitiven Element): Nach Bemerkung 1.67 gilt $E = K.\sigma_2(K).\cdots.\sigma_n(K)$, falls $e = \sigma_1, \dots, \sigma_n$ die Elemente von $\operatorname{Hom}_k(K, \mathbb{C}_{\mathrm{alg}/k})$ sind. Die $\sigma_i(K)$ sind natürlich genau die $k(a_i)$.

[45] Hier wird verwendet, dass $\mathbb{C}$ algebraisch abgeschlossen ist! Dies beweisen wir später, siehe Satz 4.1.

(c) $\Rightarrow$ (b): Wir können annehmen, dass $L \subset \mathbb{C}$ gilt (sonst kann die Inklusion $\mathbb{Q}(M \cup \overline{M} \cup \{a\}) \subset \mathbb{C}$ fortsetzen zu $\sigma : L \to \mathbb{C}$ (Allgemeiner Fortsetzungssatz 1.49; wir verwenden, dass $\mathbb{C}$ algebraisch abgeschlossen ist); dann kann L durch $\sigma(L)$ ersetzen).

Setze $G := \mathrm{Gal}(L/\mathbb{Q}(M \cup \overline{M}))$. Dann ist G eine 2-Gruppe (= Gruppe, deren Ordnung eine Potenz von 2 ist). Sei $|G| = 2^n$. Nach [Bos, Korollar 4 in Abschnitt 5.2] gibt es eine (absteigende) Kette von Untergruppen

$$G = G_n \supset G_{n-1} \supset \cdots \supset G_1 \supset G_0 = \{1\}.$$

so dass $|G_i| = 2^n$ gilt und (wir brauchen das folgende nicht) jedes G_{i-1} ein Normalteiler in G_l ist (und sogar in G; dies folgt sofort aus dem Beweis in [Bos]), für $1 \leq l \leq n$ (= eine Normalreihe mit Faktoren $\cong \mathbb{Z}/p\mathbb{Z}$).

Setze $L_i := L^{G_i}$. Dann ist $L_i \subset L$ eine Galois-Erweiterung vom Grad $|G_i| = 2^i$. In der (aufsteigenden) Kette

$$\mathbb{Q}(M \cup \overline{M}) = L_n \subset L_{n-1} \subset \cdots \subset L_1 \subset L_0 = L$$

ist somit jede Erweiterung $L_{i-1} \subset L_i$ vom Grad 2. □

Theorem 2.65. *Sei $n \in \mathbb{N}_+$ eine positive natürliche Zahl. Das regelmäßige n-Eck ist genau dann konstruierbar (also $e^{2\pi i/n} \in \mathrm{Kon}(\{0,1\})$), wenn $\varphi(n)$ eine Zweierpotenz ist.*

Proof. Es ist $\mathbb{Q} \subset \mathbb{Q}(U_n)$ eine abelsche Galois-Erweiterung vom Grad $\varphi(n)$, siehe Satz 2.54.

Aus $e^{2\pi i/n} \in \mathrm{Kon}(\{0,1\})$ folgt, dass $\varphi(n)$ eine Zweierpotenz ist (siehe Satz 1.28, Teil (b)); folgt auch direkt aus (b) in Satz 2.64.

Sei umgekehrt $\varphi(n)$ eine Zweierpotenz. Die Implikation (c) $\Rightarrow$ (a) in Satz 2.64 zeigt dann, dass $e^{2\pi i/n} \in \mathrm{Kon}(\{0,1\})$ gilt. □

Sei $n = 2^\mu p_1^{\nu_1} p_2^{\nu_2} \dots p_r^{\nu_r}$ die Primfaktorzerlegung von n mit paarweise verschiedenen Primzahlen p_i ungleich 2 und Exponenten $\nu_i > 0$ und $\mu \geq 0$. Dann gilt nach Proposition 2.49, Teil (c), dass

$$\varphi(n) = \varphi(2^\mu) \prod_{i=1}^{r} p_i^{\nu_i - 1}(p_i - 1)$$

gilt. Stets ist $\varphi(2^\mu)$ eine Zweierpotenz, denn $\varphi(1) = 1$ und $\varphi(2^\mu) = 2^{\mu-1}$ für $\mu \geq 1$.

Also ist das $\varphi(n)$ eine Zweierpotenz genau dann, wenn für alle $1 \leq i \leq r$ gilt, dass $\nu_i = 1$ und dass $p_i - 1$ eine Zweierpotenz ist.

Definition 2.66. Eine Primzahl p heißt **Fermatsch**, falls $p - 1$ eine Zweierpotenz ist und p ungerade ist.

Wir erhalten

Corollary 2.67. *Sei $n \in \mathbb{N}_+$. Das regelmäßige n-Eck ist konstruierbar genau dann, wenn $n = 2^\mu p_1 \dots p_r$ für $\mu \in \mathbb{N}$ und $p_1, \dots, p_r$ paarweise verschiedene Fermatsche Primzahlen.*

Ende 18. Vorlesung Montag 18. Juni 2012.
Ab hier bis Ende dieses Abschnitts Übungsaufgabe:

Lemma 2.68. *Sei $m \in \mathbb{N}_+$. Ist $1 + 2^m$ eine Primzahl, so muss m eine Zweierpotenz sein.*

Proof. Für beliebiges $q \in \mathbb{Q}$ und $l \in \mathbb{N}$ gilt

$$(1+q)(1-q+q^2-+\cdots+(-1)^l q^l) = 1+(-1)^l q^{l+1}.$$

Angenommen, m ist keine Zweierpotenz. Sei $m = uv$ mit $u, v \in \mathbb{N}_+$ und $u \geq 3$ ungerade. Mit $q = 2^v$ und $l = u - 1$ (gerade) wird obiges zu

$$(1+2^v)(1-2^v+2^{2v}-+\cdots+2^{v(u-1)}) = 1+2^m.$$

Beide Faktoren links sind > 1: Für $1 + 2^v$ ist das offensichtlich; für den zweiten Faktor hebt jeweils der nachfolgende positive Summand den vorhergehenden negativen Summanden mehr als weg (alternativ: Das Produkt ist $1 + 2^m > 1$, also ist der zweite Faktor positiv; wäre er $= 1$, so folgt $2^v = 2^m$, also $v = m = uv$ im Widerspruch zur Annahme $u \geq 3$).

Also ist $1 + 2^m$ keine Primzahl. □

Es heißt

$$F_k = 1 + 2^{2^k}$$

die **k-te Fermatsche Zahl**.

Aus Lemma 2.68 folgt, dass die Fermatschen Primzahlen genau die Fermatschen Zahlen sind, die Primzahlen sind.

Es sind $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ Primzahlen, jedoch ist $F_5 = 641 \cdot 6700417$ keine Primzahl: Beweis ohne lange Rechnung: Wegen $641 = 625 + 16 = 5^4 + 2^4$ und $641 = 5 \cdot 128 + 1 = 5 \cdot 2^7 + 1$ hat man in $\mathbb{Z}/641\mathbb{Z}$

$$F_5 = 1 + 2^{32} = 1 + 2^4(2^7)^4 = 1 - 5^4(2^7)^4 = 1 - (5 \cdot 2^7)^4 = 1 - (-1)^4 = 0.$$

Die ersten ungeraden Zahlen, für die das regelmäßige n-Eck konstruierbar ist, sind also

$$1, F_0 = 3, F_1 = 5, 15 = 3{\cdot}5, F_2 = 17, 51 = 3{\cdot}17, 85 = 5{\cdot}17, 255 = 3{\cdot}5{\cdot}17, F_3 = 257, \ldots$$

Die Zahlen $n \leq 20$, für die das regelmäßige n-Eck konstruierbar ist, sind also

$$1, 2, 3, 4, 5, 6, \not7, 8, \not9, 10, \not11, 12, \not13, \not14, 15, 16, 17, \not18, \not19, 20.$$

Dies zeigt noch einmal, dass nicht alle Winkel per Zirkel und Lineal gedrittelt werden können: Etwa ist das Dreieck und somit der Winkel $120°$ konstruierbar, das Neuneck und der Winkel $40°$ aber nicht.

2.5. **Lineare Unabhängigkeit von Charakteren.**

Definition 2.69. Sei G eine Gruppe und K ein Körper, so heißt ein Morphismus

$$\chi : G \to K^\times$$

von Gruppen ein **K-wertiger Charakter von G** oder ein **Charakter von G in K**.

Beispiel:

- Der **triviale** Charakter $\chi_{\text{triv}} : G \to K$, $g \mapsto 1$.
- Jeder Morphismus $\varphi : K \to K$ von Körpern liefert einen K-wertigen Charakter $\varphi : K^\times \to K^\times$ von $K^\times$.
- (nicht in Vorlesung:) Ist G endlich, etwa $n = |G|$, so ist jeder Charakter $\chi : G \to K^\times$ automatisch ein Charakter $\chi : G \to U_n$, denn für jedes $g \in G$ gilt $\chi(g)^n = \chi(g^n) = \chi(e) = 1$.

Die K-wertigen Charaktere bilden eine Gruppe mit neutralem Element χ_{triv}. Sind χ_1, χ_2 Charaktere, so ist ihr Produkt $\chi_1 \cdot \chi_2$ definiert durch

$$\begin{aligned} \chi_1 \cdot \chi_2 : G &\to K, \\ g &\mapsto \chi_1(g)\chi_2(g). \end{aligned}$$

Dies ist wieder ein Charakter, denn $K^\times$ ist abelsch.

Die K-wertigen Charaktere bilden eine eine Teilmenge des K-Vektorraums $\text{Abb}(G, K)$ aller Abbildungen von G nach K.

Theorem 2.70 (Lineare Unabhängigkeit von Charakteren [Dedekind, E. Artin])**.** [46]

Verschiedene Charaktere einer Gruppe G mit Werten in einem Körper K sind K-linear unabhängig (in $\text{Abb}(G, K)$*).* [47]

Proof. Sei sonst $n \in \mathbb{N}$ minimal, so dass verschiedene Charaktere $\chi_1, \ldots, \chi_n$ existieren, die K-linear abhängig sind. Es muss $n \geq 2$ gelten, denn (die leere Menge ist linear unabhängig und) ein Charakter nimmt Werte in $K^\times$ an. Seien $a_1, \ldots a_n \in K$, nicht alle Null, mit

$$a_1\chi_1 + a_2\chi_2 + \cdots + a_n\chi_n = 0 \tag{2.25}$$

in $\text{Abb}(G, K)$. Wegen der Minimalität sind alle $a_i \neq 0$. Seien $g, h \in G$. Dann folgt

$$a_1\chi_1(gh) + a_2\chi_2(gh) + \cdots + a_n\chi_n(gh) = 0$$

in K. Wegen $\chi_i(gh) = \chi_i(g)\chi_i(h)$ zeigt dies, dass

$$a_1\chi_1(g)\chi_1 + a_2\chi_2(g)\chi_2 + \cdots + a_n\chi_n(g)\chi_n = 0$$

---

[46] Kann statt einer Gruppe auch ein Monoid betrachten.

[47] Alternative Formulierung: Die Menge $X(G, K)$ der Charatere von G in K ist K-linear unabhängig.

in $\mathrm{Abb}(G,K)$ gilt. Wegen $\chi_1 \neq \chi_2$ finden wir $g \in G$ mit $\chi_1(g) \neq \chi_2(g)$. Ziehen wir von der letzten Gleichung das $\chi_1(g)$-fache von (2.25) ab, so erhalten wir

$$a_2\big[\chi_2(g) - \chi_1(g)\big]\chi_2 + \cdots + a_n\big[\chi_n(g) - \chi_1(g)\big]\chi_n = 0$$

in $\mathrm{Abb}(G,K)$. Der Koeffizient bei χ_2 verschwindet nicht, und deswegen sind $\chi_2, \dots, \chi_n$ K-linear abhängig, im Widerspruch zur angenommenen Minimalität. □

2.6. **Norm und Spur.** Sei $k \subset K$ eine endliche Körpererweiterung. Für $a \in K$ ist

$$\begin{aligned} \lambda_a : K &\to K, \\ x &\mapsto ax, \end{aligned}$$

ein Endomorphismus von K-Vektorräumen, und insbesondere von k-Vektorräumen.

Die beiden Verknüpfungen (dabei End Endomorphismen als Vektorraum)

(2.26)
$$\begin{array}{ccccc} K & \xrightarrow[\sim]{\lambda} & \mathrm{End}_K(K) & \subset & \mathrm{End}_k(K) \\ a & \longmapsto & \lambda_a & & \end{array} \qquad \begin{array}{c} \xrightarrow{\mathrm{tr}} k \\ \\ \xrightarrow{\det} k \end{array}$$

definieren die Spur und die Norm (hier benötigen wir, dass K ein endlichdimensionaler k-Vektorraum ist). Explizit:

Definition 2.71. Die **Spur bezüglich** K/k ist definiert als

$$\begin{aligned} \mathrm{Sp}_{K/k} : K &\to k, \\ a &\mapsto \mathrm{tr}(\lambda_a), \end{aligned}$$

und die **Norm bezüglich** K/k durch

$$\begin{aligned} \mathrm{N}_{K/k} : K &\to k, \\ a &\mapsto \det(\lambda_a). \end{aligned}$$

Aus (2.26) ist offensichtlich, wenn man beachtet, dass λ ein Isomorphismus von Ringen (genauer: K-Algebren):

- Die Spur $\mathrm{Sp}_{K/k}$ ist eine k-lineare Abbildung (= ein Morphismus von k-Vektorräumen).
- Die Norm $\mathrm{N}_{K/k}$ ist multiplikativ, $\mathrm{N}_{K/k}(ab) = \mathrm{N}_{K/k}(a)\,\mathrm{N}_{K/k}(b)$, und für $s \in k$ und $a \in K$ gilt $\mathrm{N}_{K/k}(sa) = s^{[K:k]}\,\mathrm{N}_{K/k}(a)$.

  Insbesondere kann man die Norm als k-wertigen Charakter $\mathrm{N}_{K/k} : K^\times :\to k^\times$ von $K^\times$ auffassen.
- Beispiel: Für $\mathbb{R} \subset \mathbb{C}$ wird die Multiplikation λ_a mit $a = x + iy$ bezüglich der $\mathbb{R}$-Basis $1, i$ von $\mathbb{C}$ durch die Matrix

$$\begin{bmatrix} x & -y \\ y & x \end{bmatrix}$$

dargestellt. Es folgt

$$\mathrm{Sp}_{\mathbb{C}/\mathbb{R}}(a) = 2x = 2\mathrm{Re}\,(a),$$
$$\mathrm{N}_{\mathbb{C}/\mathbb{R}}(a) = x^2 + y^2 = |a|^2.$$

Lemma 2.72. *Sei $k \subset K$ eine endliche Erweiterung. Ist $a \in K$ und $g \in \mathrm{Aut}_k(K)$ (Automorphismen des Körpers), so gelten*

$$\mathrm{Sp}_{k(a)/k}(g.a) = \mathrm{Sp}_{k(a)/k}(a), \qquad \mathrm{N}_{k(a)/k}(g.a) = \mathrm{N}_{k(a)/k}(a).$$

„Spur und Norm sind $\mathrm{Aut}_k(K)$-äquivariant“(dabei operiert $\mathrm{Aut}_k(K)$ trivial auf k).

Beispiel: Prüfe dies am obigen Beispiel $\mathbb{R} \subset \mathbb{C}$.

Proof. Das Diagramm von k-Vektorraümen und k-linearen Abbildungen

$$\begin{array}{ccc} K & \xrightarrow{\lambda_a} & K \\ {\scriptstyle\sim}\downarrow{\scriptstyle g} & & {\scriptstyle\sim}\downarrow{\scriptstyle g} \\ K & \xrightarrow{\lambda_{g.a}} & K \end{array}$$

ist kommutativ. Also $\lambda_{g.a} = g\lambda_a g^{-1}$, und somit haben $\lambda_{g.a}$ und λ_a dieselbe Spur und Determinante. □

Lemma 2.73. *Sei $k \subset K$ eine endliche Erweiterung.*

(a) [48] *Ist $n = [K : k]$, so gilt für $a \in k$:*

$$\mathrm{Sp}_{K/k}(a) = na, \qquad \mathrm{N}_{K/k}(a) = a^n.$$

(b) Ist $a \in K$ mit $\min_{a/k} = X^d + c_{d-1}X^{d-1} + \cdots + c_0$, so gelten für Spur und Norm von a bezüglich der einfachen algebraischen Erweiterung $k(a)/k$ die Formeln

$$\mathrm{Sp}_{k(a)/k}(a) = -c_{d-1}, \qquad \mathrm{N}_{k(a)/k}(a) = (-1)^d c_0.$$

(c) Sei $a \in K$ und $s = [K : k(a)]$. Dann gelten

$$\mathrm{Sp}_{K/k}(a) = s\,\mathrm{Sp}_{k(a)/k}(a) = \mathrm{Sp}_{k(a)/k}(\mathrm{Sp}_{K/k(a)}(a)),$$
$$\mathrm{N}_{K/k}(a) = (\mathrm{N}_{k(a)/k}(a))^s = \mathrm{N}_{k(a)/k}(\mathrm{N}_{K/k(a)}(a)).$$

(Spezialfall der Transitivität von Norm und Spur, siehe Proposition 2.75.)

Beispiel: Prüfe dies am obigen Beispiel $\mathbb{R} \subset \mathbb{C}$.

[48] Je nach Definition von det und tr ist diese Aussage wohl trivial. Per Matrizen nicht, per induziertem Skalar auf maximalem äußerem Wedge-Produkt bzw. per Verjüngung $V \otimes_k V^* \to k$ nicht, aber wohl per Koeffizienten des charakteristischen Polynoms (falls weiter oben gezeigt wurde, dass dieses mit dem Minimalpolynom übereinstimmt).

Proof. (a): Die Matrix von λ_a bezüglich jeder k-Basis von K ist das a-fache der Einheitsmatrix.

(b): Die Matrix von λ_a bezüglich der k-Basis $1, a, a^2, \dots, a^{d-1}$ von $k(a)$ ist

$$A := \begin{bmatrix} 0 & 0 & 0 & \dots & 0 & -c_0 \\ 1 & 0 & 0 & \dots & 0 & -c_1 \\ 0 & 1 & 0 & \dots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & -c_{d-2} \\ 0 & 0 & 0 & \dots & 1 & -c_{d-1} \end{bmatrix}$$

Daraus folgen die Behauptungen.

(c): Sei nun $x_1, \dots, x_s$ eine $k(a)$-Basis von K. Dann bilden

$$\begin{aligned} x_1 1, x_1 a, x_1 a^2, \dots, x_1 a^{d-1}, \\ x_2 1, x_2 a, x_2 a^2, \dots, x_2 a^{d-1}, \\ \dots, \\ x_s 1, x_s a, x_2 a^2, \dots, x_s a^{d-1} \end{aligned}$$

eine k-Basis von K (siehe Beweis des Gradsatzes 1.4), und bezüglich dieser Basis ist λ_a dargestellt durch die Blockdiagonalmatrix

$$\begin{bmatrix} A & & 0 \\ & \ddots & \\ 0 & & A \end{bmatrix}$$

mit s Matrizen A auf der Diagonalen. Dies zeigt die jeweils ersten Gleichheiten, und die jeweils zweiten Gleichheiten folgen aus der Additivität der Spur, der Multiplikativität der Norm und (a). □

Sei $k \subset K$ eine endliche Erweiterung. In Satz 1.81 haben wir gesehen, dass $[K : k] = q[K : k]_s$ gilt, wobei $q = 1$ ist, falls $\operatorname{char} k = 0$, und eine p-Potenz, falls $\operatorname{char} k = p > 0$. Sei $\overline{K}$ ein algebraischer Abschluss von K. Dann definieren wir Abbildungen

$$\begin{aligned} \mathrm{Sp}'_{K/k} : K &\to \overline{K}, \\ a &\mapsto q \sum_{\sigma \in \mathrm{Hom}_k(K, \overline{K})} \sigma(a), \end{aligned}$$

und

$$\begin{aligned} \mathrm{N}'_{K/k} : K &\to \overline{K}, \\ a &\mapsto \prod_{\sigma \in \mathrm{Hom}_k(K, \overline{K})} \sigma(a^q) = \Big(\prod_{\sigma \in \mathrm{Hom}_k(K, \overline{K})} \sigma(a) \Big)^q. \end{aligned}$$

Beachte, dass $\mathrm{Sp}'_{K/k} = 0$ gilt, falls K/k nicht separabel ist, denn dann ist das Bild von q in k Null.

Beobachtungen:

(a) Es ist $\mathrm{Sp}'_{K/k}$ k-linear und $\mathrm{N}'_{K/k}$ multiplikativ (und es gilt $\mathrm{N}'_{K/k}(sa) = s^{[K:k]}\,\mathrm{N}'_{K/k}(a)$ für $s \in k$ und $a \in K$).

(b) Die Abbildung $\mathrm{Sp}'_{K/k}$ hat Bild in k. Es genügt, denn Fall K/k separabel zu betrachten. Dann ist $q = 1$. Angenommen $b := \mathrm{Sp}'_{K/k}(a) \notin k$ für ein $a \in K$. Da a separabel über k ist, gilt dasselbe für alle $\sigma(a)$ und damit für b. Also hat $\min_{b/k}$ eine Nullstelle $\neq b$ in $\overline{K}$, und wir finden mit den Fortsetzungssätzen ein $\tau \in \mathrm{Aut}_k(\overline{K})$ mit $\tau(b) \neq b$. Aber es gilt

$$\tau(b) = \sum_{\sigma \in \mathrm{Hom}_k(K,\overline{K})} \tau(\sigma(a)) = b,$$

denn $(\tau\circ?) : \mathrm{Hom}_k(K,\overline{K}) \xrightarrow{\sim} \mathrm{Hom}_k(K,\overline{K})$ ist bijektiv.

(c) Die Abbildung $\mathrm{N}'_{K/k}$ hat Bild in k. Beachte, dass für jedes $a \in K$ das Element a^q separabel über k ist: Mit Satz 1.93 zerlegen wir $k \subset K$ als $k \subset K_{\mathrm{sep}} \subset K$. Es gilt $[K : k]_s = [K_{\mathrm{sep}} : k]$, also $q = [K : K_{\mathrm{sep}}]$. Da $K_{\mathrm{sep}} \subset K$ rein inseparabel ist, gibt es ein $m \in \mathbb{N}$ mit $a^{p^m} \in K_{\mathrm{sep}}$; wir wählen m minimal mit dieser Eigenschaft. Dann gilt nach Lemma 1.88 $[K_{\mathrm{sep}}(a) : K_{\mathrm{sep}}] = p^m$. Insbesondere ist p^m ein Teiler von q. Somit gilt erst recht $a^q \in K_{\mathrm{sep}}$.

Wie oben erhalten wir so, dass $\mathrm{N}'_{K/k}(a)$ separabel über k ist, und wir schließen wie oben auf $\mathrm{N}'_{K/k}(a) \in k$.

Unser Ziel ist Satz 2.76, der insbesondere besagt, dass $\mathrm{Sp}'_{K/k} = \mathrm{Sp}_{K/k}$ und $\mathrm{N}'_{K/k} = \mathrm{N}_{K/k}$. Wir benötigen dazu einige vorbereitende Aussagen.

Lemma 2.74. *Die Aussagen (a), (b) aus Lemma 2.73 stimmen auch für* Sp' *und* N'.

Proof. (a): Dies ist klar, denn $\mathrm{Hom}_k(K,\overline{K})$ hat genau $[K : k]_s$ Elemente, die alle Elemente von k fixieren.

(b): Ist die Charakteristik von k Null, so setze $p = 1$. Andernfalls sei $p = \mathrm{char}\, k > 0$. Sei $f = \min_{a/k}$. Wir verwenden Satz 1.70. Sei p^r die Vielfachheit der Nullstelle a von f (falls $\mathrm{char}\, k = 0$, so kann r beliebig wählen, etwa $r = 0$). Dann gilt (verwende (1.7))

$$f = \prod_{b \in \overline{k(a)}, f(b)=0} (X-b)^{p^r} = \prod_{\sigma \in \mathrm{Hom}_k(k(a),\overline{k(a)})} (X - \sigma(a))^{p^r}.$$

Nach Lemma 1.79 gilt $d = [k(a) : k] = p^r[k(a) : k]_s$. Also gelten ($c_i$ sind die Koeffizienten von f)

$$c_0 = (-1)^{[k(a):k]_s p^r} \prod_{\sigma \in \mathrm{Hom}_k(k(a),\overline{k(a)})} \sigma(a)^{p^r} = (-1)^d\,\mathrm{N}'_{k(a)/k}(a)$$

und

$$c_{d-1} = -\sum_{\sigma \in \mathrm{Hom}_k(k(a),\overline{k(a)})} p^r\sigma(a) = -\,\mathrm{Sp}'_{k(a)/k}(a).$$

□

Ende 19. Vorlesung Donnerstag 21. Juni 2012.

Proposition 2.75. *Transitivität von* N' *und* Sp'*: Sind* $k \subset E \subset K$ *endliche Körpererweiterungen, so gelten*

$$\mathrm{Sp}'_{K/k} = \mathrm{Sp}'_{E/k} \circ \mathrm{Sp}'_{K/E},$$
$$\mathrm{N}'_{K/k} = \mathrm{N}'_{E/k} \circ \mathrm{N}'_{K/E}.$$

Proof. Sei $[K : E] = q_1[K : E]_s$ und $[E : k] = q_2[E : k]_s$. Dann gilt $[K : k] = q_1q_2[K : k]_s$ (Multiplikativität von Körpergrad, Satz 1.4, und Separabilitätsgrad, Satz 1.80).

Wie im Beweis des Satzes 1.80 über die Multiplikativität des Separabilitätsgrades sei

$$\mathrm{Hom}_E(K, \overline{K}) = \{\sigma_1, \dots, \sigma_s\} \qquad \text{und} \qquad \mathrm{Hom}_k(E, \overline{K}) = \{\tau_1, \dots, \tau_t\}$$

mit paarweise verschiedenen σ_i bzw. τ_j, und sei $\overline{\tau}_j \in \mathrm{Aut}_k(\overline{K})$ eine Fortsetzung von τ_j. Wir haben dort gesehen, dass

$$\mathrm{Hom}_k(K, \overline{K}) = \{\overline{\tau}_j \circ \sigma_i \mid 1 \le i \le s, 1 \le j \le t\}.$$

Somit berechnen wir für $a \in K$

$$\begin{aligned}
\mathrm{Sp}'_{K/k}(a) &= q_1q_2 \sum_{1\le i\le s, 1\le j\le t} \overline{\tau}_j(\sigma_i(a)) \\
&= q_2 \sum_{1\le j\le t} \overline{\tau}_j\Big(q_1 \sum_{1\le i\le s} \sigma_i(a)\Big) \\
&= q_2 \sum_{1\le j\le t} \tau_j\Big(\underbrace{\mathrm{Sp}'_{K/E}(a)}_{\in E}\Big) \\
&= \mathrm{Sp}'_{E/k}(\mathrm{Sp}'_{K/E}(a))
\end{aligned}$$

und analog für N'. □

Theorem 2.76.

(a) Ist $k \subset K$ *eine endliche Körpererweiterung, so gelten*

$$\mathrm{Sp}'_{K/k} = \mathrm{Sp}_{K/k}, \qquad \mathrm{N}'_{K/k} = \mathrm{N}_{K/k}.$$

Insbesondere gilt $\mathrm{Sp}_{K/k} = 0$*, falls* K/k *nicht separabel ist.*

(b) Transitivität von Norm und Spur:

Kurzversion: N *und* Sp *sind transitiv.*

Langversion: Sind $k \subset E \subset K$ *endliche Körpererweiterungen, so gelten*

$$\mathrm{Sp}_{K/k} = \mathrm{Sp}_{E/k} \circ \mathrm{Sp}_{K/E},$$
$$\mathrm{N}_{K/k} = \mathrm{N}_{E/k} \circ \mathrm{N}_{K/E}.$$

Proof. (a): Dies folgt direkt aus den Lemmata 2.73 und 2.74 unter Verwendung von Proposition 2.75.

Ausführlich gelten für $a \in K$ und $s = [K : k(a)]$

$$\begin{aligned}\mathrm{Sp}_{K/k}(a) &= s\,\mathrm{Sp}_{k(a)/k}(a)\\ &= s\,\mathrm{Sp}'_{k(a)/k}(a)\\ &= \mathrm{Sp}'_{k(a)/k}(sa)\\ &= \mathrm{Sp}'_{k(a)/k}(\mathrm{Sp}'_{K/k(a)}(a)),\\ &= \mathrm{Sp}'_{K/k}(a)\end{aligned}$$

und analog für die Norm

$$\begin{aligned}\mathrm{N}_{K/k}(a) &= (\mathrm{N}_{k(a)/k}(a))^s\\ &= (\mathrm{N}'_{k(a)/k}(a))^s\\ &= \mathrm{N}'_{k(a)/k}(a^s)\\ &= \mathrm{N}'_{k(a)/k}(\mathrm{N}'_{K/k(a)}(a))\\ &= \mathrm{N}'_{K/k}(a)\end{aligned}$$

(b): Dies folgt nun aus Proposition 2.75. □

Theorem 2.77. *Ist Übungsaufgabe für* Sp'.

Eine endliche Erweiterung $k \subset K$ ist genau dann separabel, wenn die k-lineare Abbildung $\mathrm{Sp}_{K/k} : K \to k$ nicht die Nullabbildung (und damit surjektiv) ist. Ist $k \subset K$ separabel, so ist die symmetrische k-Bilinearform

$$\begin{aligned}\mathrm{Sp} : K \times K &\to k,\\ (x, y) &\mapsto \mathrm{Sp}_{K/k}(xy),\end{aligned}$$

nicht ausgeartet.

Proof. Ist $k \subset K$ nicht separabel, so wissen wir bereits, dass $\mathrm{Sp}_{K/k} : K \to k$ die Nullabbildung ist.

Sei $k \subset K$ separabel, und sei

$$\mathrm{Hom}_k(K, \overline{K}) = \{\sigma_1, \ldots, \sigma_r\},$$

mit paarweise verschiedenen σ_i. Nach Satz 2.76 gilt

$$\mathrm{Sp}_{K/k} = \sigma_1 + \cdots + \sigma_r.$$

Aufgefaßt als Abbildung $K^\times \to \overline{K}$ ist dies eine nichttriviale $\overline{K}$-Linearkombination der paarweise verschiedenen Charaktere $\sigma_i : K^\times \to \overline{K}^\times$ und somit nicht die Nullabbildung (Satz 2.70), es gibt also ein $a \in K$ mit $\mathrm{Sp}_{K/k}(a) \neq 0$. Als k-lineare Abbildung ist $\mathrm{Sp}_{K/k} : K \to k$ damit surjektiv.

Gegeben $x \in K \setminus \{0\}$ gilt dann $\mathrm{Sp}(x, x^{-1}a) = \mathrm{Sp}_{K/k}(xx^{-1}a) \neq 0$. Somit ist Sp nicht ausgeartet. □

Corollary 2.78. *Sei $k \subset K$ eine endliche separable Erweiterung, und sei $x_1, \dots, x_n$ eine k-Basis von K. Dann existiert eine eindeutig bestimmte k-Basis $y_1, \dots, y_n$ von K mit $\mathrm{Sp}_{K/k}(x_i y_j) = \delta_{ij}$ für alle $i, j = 1, \dots, n$.*

Proof. Offensichtlich. □

2.7. **Zyklische Erweiterungen.** Ein wenig Gruppenkohomologie. Sei G eine Gruppe. Es operiere G durch Gruppenautomorphismen auf einer abelschen Gruppe A, d. h. es ist ein Morphismus $G \to \mathrm{Aut}(A)$ gegeben. Man definiert die folgenden Untergruppen der abelschen Gruppe $\mathrm{Abb}(G, A)$ aller Abbildungen $G \to A$, wobei wir A additiv schreiben.

$$Z^1(G, A) = \{f \in \mathrm{Abb}(G, A) \mid f(gh) = f(g) + g.f(h) \text{ für alle } g, h \in G\},$$

$$B^1(G, A) = \{f \in \mathrm{Abb}(G, A) \mid \text{es existiert } a \in A \text{ mit } f(g) = a - g.a \text{ für alle } g \in G\}.$$

(Leicht: Sind Untergruppen von $\mathrm{Abb}(G, A)$.) Es ist $Z^1(G, A)$ die **Gruppe der 1-Kozykel (cocycles) von G mit Werten in A** und $B^1(G, A)$ die **Gruppe der 1-Koränder (coboundaries) von G mit Werten in A**. Es gilt $B^1(G, A) \subset Z^1(G, A)$, denn ist $f \in B^1(G, A)$ gegeben mit $f(g) = a - g.a$ für ein $a \in A$, so gilt

$$f(gh) = a - (gh).a = a - g.a + g.a - g.h.a = f(g) + g.f(h).$$

Man nennt den Quotienten

$$H^1(G, A) = Z^1(G, A)/B^1(G, A)$$

die **erste Kohomologie-Gruppe von G mit Werten in A**.

Der Name des folgenden Theorems rührt her von der Nummer des entsprechenden Satzes in David Hilberts Zahlbericht [Hil97]. Der Originalversion ist von Ernst Eduard Kummer (1855), die hier gegebene Version von Emmy Noether (1933).

Theorem 2.79 (Hilbert 90, multiplikative Form)**.** *Sei K ein Körper und $G \subset \mathrm{Aut}(K)$ eine endliche Untergruppe. (Es operiert somit G auf $K^\times$ durch Gruppenautomorphismen.) Dann gilt*

$$H^1(G, K^\times) = \{1\}.$$

Remark 2.80. Eine äquivalente Formulierung ist (vgl. Satz 2.11):

Sei $k \subset K$ eine endliche Galois-Erweiterung. Dann gilt

$$H^1(\mathrm{Gal}(K/k), K^\times) = \{1\}.$$

Proof. Sei $f : G \to K^\times$ ein 1-Kozykel (also $f(gh) = f(g)g(f(h))$ für alle $g, h \in G$, denn die Verknüpfung in $K^\times$ wird multiplikativ geschrieben). Wir fassen die Elemente von G als Charaktere $K^\times \to K^\times$ auf. Sie sind K-linear unabhängig nach Satz 2.70, so dass also

$$\varphi := \sum_{h \in G} f(h)h : K^\times \to K$$

nicht die Nullabbildung ist. Es existiert also ein $c \in K^\times$, so dass $\varphi(c) \neq 0$. Dann gilt für $g \in G$

$$\begin{aligned} g(\varphi(c)) &= \sum_{h\in G} g(f(h)h(c)) \\ &= \sum_{h\in G} g(f(h))g(h(c)) \\ &= \sum_{h\in G} f(g)^{-1}f(gh)(gh)(c) \\ &= f(g)^{-1}\varphi(c), \end{aligned}$$

d. h. für $a := \varphi(c) \in K^\times$ gilt

$$f(g) = ag(a)^{-1} = \frac{a}{g(a)}.$$

Also ist f ein 1-Korand. □

Corollary 2.81. *Sei $k \subset K$ eine endliche Galoiserweiterung mit Galoisgruppe G. Ist $\chi : G \to k^\times$ ein Charakter, so gibt es ein $a \in K^\times$ (welches eindeutig ist bis auf Multiplikation mit Elementen aus $k^\times$), so dass $\chi(g) = \frac{a}{g(a)}$ für alle $g \in G$ gilt.*

Umgekehrt, gegeben $a \in K^\times$ mit $\frac{a}{g(a)} \in k^\times$ für alle $g \in G$, so ist

$$\begin{aligned} \chi_a : G &\to k^\times, \\ g &\mapsto \frac{a}{g(a)} \end{aligned}$$

ein Charakter von G in $k^\times$ (genauer: in U^n, falls $n = |G|$). [49]

Example 2.82. Betrachte $\mathbb{R} \subset \mathbb{C}$. Offensichtlich gibt es genau zwei Charaktere $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \to \mathbb{R}^\times$ (oder auch $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \to \mathbb{C}^\times$).

Für $a = re^{i\varphi} \in \mathbb{C}^\times$ mit $r \in \mathbb{R}^\times$, $0 \leq \varphi < \pi$ (Achtung: negativer Radius erlaubt!) ist die Bedingung $\frac{a}{g(a)} \in \mathbb{R}^\times$ äquivalent dazu, dass

$$\frac{a}{\overline{a}} = \frac{re^{i\varphi}}{re^{-i\varphi}} = e^{2i\varphi}$$

rell ist, also zu $\varphi \in \{0, \pi/2\}$. Es liefert $\varphi = 0$ den trivialen Charakter und $\varphi = \pi/2$ den Charakter $\mathrm{id}_\mathbb{C} \mapsto 1$, $\overline{?} \mapsto -1$.

Proof. Ein Charakter von G in k ist dasselbe wie ein Element von $Z^1(G, K^\times)$, das nur Werte in $k^\times$ annimmt. Nach Hilbert 90 2.79 ist solche Charakter bereits ein 1-Kozykel, also von der angegebenen Form.

[49] Genauer: Sei $a \in K^\times$ gegeben. Setze $\chi_a : G \to K^\times$, $g \mapsto \frac{a}{g(a)}$. Dann ist χ_a ein Charakter von G in $K^\times$ genau dann, wenn für alle $g, h \in G$ die hervorgehobene Gleichheit in

$$\chi_a(gh) = \frac{a}{gh(a)} = \frac{a}{g(a)}g\Big(\frac{a}{h(a)}\Big) \boxed{=} \frac{a}{g(a)}\frac{a}{h(a)} = \chi_a(g)\chi_a(h)$$

gilt, was genau dann der Fall ist, wenn $\frac{a}{h(a)} \in k^\times$ gilt für alle $h \in G$.

Eindeutigkeit: Seien $a, b \in K^\times$. Gilt $\frac{a}{g(a)} = \frac{b}{g(b)}$ für alle $g \in G$, so folgt $\frac{a}{b} = g(\frac{a}{b})$ für alle $g \in G$, also $\frac{a}{b} \in k^\times$.

Die letzte Aussage folgt aus

$$\chi_a(gh) = \frac{a}{gh(a)} = \frac{a}{g(a)} g\Big(\frac{a}{h(a)}\Big) = \frac{a}{g(a)} \frac{a}{h(a)} = \chi_a(g)\chi_a(h)$$

für $g, h \in G$ beliebig.

Ist allgemein $\chi : G \to K^\times$ ein Charakter und $n = |G|$, so gilt $g^n = e$ für jedes $g \in G$ und damit $\chi(g)^n = \chi(g^n) = \chi(e) = 1$. □

Theorem 2.83 (Hilbert 90 für zyklische Galois-Erweiterungen)**.** *Sei $k \subset K$ eine endliche* zyklische *Galois-Erweiterung, und sei $g \in \mathrm{Gal}(K/k)$ ein erzeugendes Element. Sei $b \in K$. Dann sind äquivalent:*

(a) $\mathrm{N}_{K/k}(b) = 1$.

(b) Es existiert ein $a \in K^\times$ mit $b = \frac{a}{g(a)}$.

Alternativ formuliert: Die einzigen Lösungen der Gleichung $\mathrm{N}_{K/k}(b) = 1$ in K sind die Elemente $\frac{a}{g(a)}$ für $a \in K^\times$ (eindeutig bis auf Faktor aus $k^\times$).

Example 2.84. Betrachte $\mathbb{Q} \subset \mathbb{Q}(i)$. Die Norm von $z = a + bi$ ist $|z|^2 = a^2 + b^2$. Satz 2.83 besagt also, dass aus $|z| = 1$ eine Darstellung $z = \frac{x}{\overline{x}}$ folgt. Schreibt man $x = c + di$, so bedeutet dies

$$z = \frac{x}{\overline{x}} = \frac{c + di}{c - di} = \frac{c^2 - d^2}{c^2 + d^2} + \frac{2cd}{c^2 + d^2} i.$$

Dies hat mit Pythagoräischen Tripeln zu tun, siehe englische Wikipedia zu Hilbert 90, oder besser: Elkies: Pythagorean triples and Hilbert's Theorem 90. Ist auch Übungsaufgabe in [Bos].

Proof. Gelte $b = a/g(a)$ für ein $a \in K^\times$. Da die Norm multiplikativ ist und mit der Operation der Galoisgruppe verträglich (nach Lemma 2.72), erhalten wir

$$\mathrm{N}_{K/k}(b) = \mathrm{N}_{K/k}(a)\,\mathrm{N}_{K/k}(g(a))^{-1} = \mathrm{N}_{K/k}(a)\,\mathrm{N}_{K/k}(a)^{-1} = 1.$$

Gelte umgekehrt $\mathrm{N}_{K/k}(b) = 1$. Sei $n = |G|$, also $bg(b) \dots g^{n-1}(b) = 1$. Definiere

$$\begin{aligned} f : G &\to K^\times, \\ g^i &\mapsto \prod_{\nu=0}^{i-1} g^\nu(b) \quad (\text{für } i \in \mathbb{N}) \end{aligned}$$

Das ist wohldefiniert, denn

$$f(g^{i+n}) = \Big(\prod_{\nu=0}^{i-1} g^\nu(b)\Big) g^i \Big(\underbrace{\prod_{\mu=0}^{n-1} g^\mu(b)}_{\mathrm{N}_{K/k}(b)=1}\Big) = f(g^i).$$

Weiter ist f ein 1-Kozykel, denn

$$\begin{aligned} f(g^i)g^i(f(g^j)) &= \Big(\prod_{\nu=0}^{i-1} g^\nu(b)\Big) g^i\Big(\prod_{\mu=0}^{j-1} g^\mu(b)\Big) \\ &= \prod_{\nu=0}^{i+j-1} g^\nu(b) \\ &= f(g^{i+j}). \end{aligned}$$

Satz 2.79 (Hilbert 90, multiplikativ) besagt nun, dass f ein 1-Korand ist, dass es also ein $a \in K^\times$ gibt mit $f(h) = a/h(a)$ für alle $h \in G$. Speziell erhalten wir $b = f(g) = a/g(a)$. □

Theorem 2.85. *Sei $k \subset K$ eine Körpererweiterung und $n \in \mathbb{N}_+$ mit $\operatorname{char} k \nmid n$. Es enthalte k eine/alle primitive(n) n-te(n) Einheitswurzel(n).*

(a) Ist $k \subset K$ eine zyklische Galois-Erweiterung vom Grad n, so gilt $K = k(a)$ für ein $a \in K$ mit $\min_{a/k} = X^n - c$.

(b) Gilt $K = k(a)$ für ein $a \in K$, das Nullstelle eines Polynoms $X^n - c \in k[X]$ ist, so ist $k \subset K$ eine zyklische Galois-Erweiterung. Weiter ist $d := [K : k]$ ein Teiler von n, und $X^d - a^d$ ist das Minimalpolynom von a über k.

Falls $c \neq 0$ gilt, so stimmt d überein mit der Ordnung von c in $k^\times/k^{\times n}$, wobei $k^{\times n} = \{b^n \mid b \in k^\times\}$; in Formeln $d = \operatorname{ord}(c; k^\times/k^{\times n})$.

(Was ist sinnvolle Aussage, falls $\operatorname{char} k \mid n$ (und dann halt alle n-Einheitswurzeln in k)? Das beste, was wir zeigen, ist wohl der Satz 2.93 von Artin-Schreier.)

Remark 2.86. Die Bedingung, dass die primitiven n-ten Einheitswurzeln in k liegen, ist notwendig für (b): Etwa ist $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ nicht einmal Galoissch. Nimmt man stattdessen den Zerfällungskörper $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ von $X^3 - 2 \in \mathbb{Q}[X]$, vergleiche Beispiel 1.59 (b), so hat diese Galois-Erweiterung Grad 6 und Galoisgruppe S_3, ist also nicht zyklisch.

Proof. Sei $\zeta \in k$ eine primitive n-te Einheitswurzel.

(a): Wegen $\zeta \in k$ gilt $\mathrm{N}_{K/k}(\zeta^{-1}) = \zeta^{-n} = 1$ (nach Lemma 2.73, Teil (a)). Satz 2.83 (Hilbert 90 für zyklische Erweiterungen) liefert ein $a \in K^\times$ mit $\zeta^{-1} = \frac{a}{g(a)}$, also $g(a) = \zeta a$, wobei $g \in \mathrm{Gal}(K/k)$ ein fixiertes erzeugendes Element von $\mathrm{Gal}(K/k)$ ist. Induktiv folgt $g^i(a) = \zeta^i a$ für $i \in \mathbb{Z}$. Insbesondere sind die Elemente

$$a, g(a), g^2(a), \ldots, g^{n-1}(a)$$

paarweise verschieden. Sie sind Nullstellen von $\min_{a/k}$, so dass $[k(a) : k] \geq n$ folgt. Aus $[K : k] = n$ folgt $K = k(a)$. Wegen $g(a) = \zeta a$ folgt $g(a^n) = a^n$, so dass also $X^n - a^n \in k[X]$. Dies muss aus Gradgründen bereits das Minimalpolynom von a über k sein.

(b): Der Fall $a = 0$ ist trivial. Sei also $a \neq 0$ (und damit $c \neq 0$). Weil $a, a\zeta, a\zeta^2, \ldots, a\zeta^{n-1}$ insgesamt n paarweise verschieden Nullstellen von $X^n -$

c sind, ist $k(a)$ der Zerfällungskörper von $X^n - c$. Die Ableitung von $X^n - c$ ist $nX^{n-1} \neq 0$; somit haben $X^n - c$ und seine Ableitung keine gemeinsame Nullstelle, so dass $X^n - c$ separabel ist. Also ist $k \subset k(a)$ galoissch.

Für jedes $g \in \mathrm{Gal}(k(a)/k)$ ist $g(a)$ eine Nullstelle von $X^n - c$, und somit $\omega_g := \frac{a}{g(a)} \in U_n \subset k$.

Wie in Korollar 2.81 erklärt, ist damit

$$\chi := \chi_a : \mathrm{Gal}(k(a)/k) \to U_n, \qquad g \mapsto \chi(g) = \frac{a}{g(a)},$$

ein Charakter; er ist injektiv wegen $g(a) = \chi(g)^{-1}a$. Als Untergruppe der zyklischen Gruppe U_n (siehe Satz 2.44) ist damit $\mathrm{Gal}(k(a)/k)$ zyklisch, und es gilt

$$d = [k(a) : k] = |\mathrm{Gal}(k(a)/k)| \text{ teilt } |U_n| = n.$$

Sei $g \in \mathrm{Gal}(k(a)/k)$ ein Erzeuger von $\mathrm{Gal}(k(a)/k)$. Dann

$$g(a^d) = g(a)^d = \big((\frac{a}{\chi(g)}\big)^d = \frac{a^d}{\chi(g^d)} = a^d$$

und somit $a^d \in k$. Aus Gradgründen ist dann $X^d - a^d \in k[X]$ das Minimalpolynom von a über k.

Wegen $c = a^n$ gilt $c^d = a^{nd} = (a^d)^n \in k^{\times n}$, so dass also $\mathrm{ord}(c; k^\times/k^{\times n}) \leq d$ gilt. Sei $0 < d'$ mit $c^{d'} = b^n$ für ein $b \in k^\times$. Aus $c = a^n$ folgt $(a^{d'})^n = c^{d'} = b^n$, also $a^{d'} \in U_n b \subset k$. Also ist a Nullstelle von $X^{d'} - a^{d'} \in k[X]$. Es folgt $d \leq d'$. □

Ende 20. Vorlesung Montag 25. Juni 2012.

Theorem 2.87 (Hilbert 90, additive Form)**.** *Sei K ein Körper und $G \subset \mathrm{Aut}(K)$ eine endliche Untergruppe. Dann operiert G auf der (additiv geschriebenen) abelschen Gruppe $A = K$ durch Gruppenautomorphismen, und die zugehörige erste Kohomologie-Gruppe ist trivial:*

$$H^1(G, K) = \{0\}.$$

Alternativ: Jeder 1-Kozykel von G mit Werten in K ist von der Form $g \mapsto a - g(a)$ für ein $a \in K$ (eindeutig bis auf Addition von Elementen von k).

Alternativ: Sei $k \subset K$ eine endliche Galois-Erweiterung. Dann gilt

$$H^1(\mathrm{Gal}(K/k), K) = \{0\}.$$

Proof. Sei $f : G \to K$ ein 1-Kozykel (also $f(gh) = f(g) + g(f(h))$). Wir fassen die Elemente von G als Charaktere $K^\times \to K^\times$ auf. Betrachte

$$\varphi := \sum_{h \in G} f(h)h : K \to K.$$

Sei $k := K^G$; somit ist $k \subset K$ eine Galois-Erweiterung mit Galois-Gruppe $G = \mathrm{Gal}(K/k)$.

Sei $c \in K$. Dann gilt für $g \in G$

$$\begin{aligned} g(\varphi(c)) &= \sum_{h\in G} g(f(h)h(c)) \\ &= \sum_{h\in G} g(f(h))g(h(c)) \\ &= \sum_{h\in G} [f(gh) - f(g)]g(h(c)) \\ &= \sum_{h\in G} f(gh)(gh)(c) - f(g)\sum_{h\in G}(gh)(c) \\ &= \varphi(c) - f(g)\,\mathrm{Sp}_{K/k}(c). \end{aligned}$$

Weil $k \subset K$ separabel ist, können wir nach Satz 2.77 (war Übungsaufgabe). $c \in K$ so wählen, dass $\mathrm{Sp}_{K/k}(c) \neq 0$.

Explizit: Beachte $\mathrm{Sp}_{K/k} = \sum_{g\in G} g$. Da die Elemente von G, aufgefaßt als Charaktere $g : K^\times \to K^\times$, linear unabhängig sind über K (nach Satz 2.70, gilt $\mathrm{Sp}_{K/k} \neq 0$ in $\mathrm{Abb}(G, K)$. Sei $c \in K$ mit $\mathrm{Sp}_{K/k}(c) \neq 0$.

Für beliebiges $g \in G$ gilt dann

$$\begin{aligned} f(g) &= \frac{\varphi(c)}{\mathrm{Sp}_{K/k}(c)} - \frac{g(\varphi(c))}{\mathrm{Sp}_{K/k}(c)} \\ &= \frac{\varphi(c)}{\mathrm{Sp}_{K/k}(c)} - \frac{g(\varphi(c))}{g(\mathrm{Sp}_{K/k}(c))} \\ &= \frac{\varphi(c)}{\mathrm{Sp}_{K/k}(c)} - g\Big(\frac{\varphi(c)}{\mathrm{Sp}_{K/k}(c)}\Big). \end{aligned}$$

Dies zeigt, dass f ein 1-Korand ist. □

Theorem 2.88 (Hilbert 90, additive Form, für zyklische Galois-Erweiterungen)**.** *Sei $k \subset K$ eine endliche zyklische Galois-Erweiterung, und sei $g \in \mathrm{Gal}(K/k)$ ein erzeugendes Element. Sei $b \in K$. Dann sind äquivalent:*

(a) $\mathrm{Sp}_{K/k}(b) = 0$.
(b) Es existiert ein $a \in K$ mit $b = a - g(a)$.

Alternativ: Die einzigen Lösungen $b \in K$ von $\mathrm{Sp}_{K/k}(b) = 0$ sind die Elemente $a - g(a)$ für $a \in K$.

Proof. Gelte $b = a - g(a)$. Da die Spur additiv ist und mit der Operation der Galoisgruppe verträglich (nach Lemma 2.72), erhalten wir

$$\mathrm{Sp}_{K/k}(b) = \mathrm{Sp}_{K/k}(a) - \mathrm{Sp}_{K/k}(g(a)) = \mathrm{Sp}_{K/k}(a) - \mathrm{Sp}_{K/k}(a) = 0.$$

Gelte umgekehrt $\mathrm{Sp}_{K/k}(b) = 0$. Sei $n = |G|$, also $b+g(b)+\cdots+g^{n-1}(b) = 0$. Wie im Beweis von Satz 2.83 (Hilbert 90 für zyklische Erweiterungen) sieht

man, dass

$$f : G \to K,$$
$$g^i \mapsto \sum_{\nu=0}^{i-1} g^\nu(b) \quad (\text{für } i \in \mathbb{N})$$

ein wohldefinierter 1-Kozykel ist.

Satz 2.87 (Hilbert 90, additiv) besagt nun, dass f ein 1-Korand ist, dass es also ein $a \in K$ gibt mit $f(h) = a - h(a)$ für alle $h \in G$. Speziell erhalten wir $b = f(g) = a - g(a)$. □

Definition 2.89. Sei k ein Körper positiver Charakteristik $p > 0$. Ein Polynom der Form

$$X^p - X - c \in k[X]$$

heißt **Artin-Schreier-Polynom**.

Observation 2.90. $\operatorname{char} k = p > 0$. Ist a eine Nullstelle (in $\overline{k}$) eines Artin-Schreier-Polynoms $f = X^p - X - c \in k[X]$, so ist wegen

$$f(a+1) = (a+1)^p - (a+1) - c = a^p + 1 - a - 1 - c = f(a)$$

auch $a + 1$ eine Nullstelle von f.

Also sind $a, a+1, a+2, \dots, a+(p-1)$ genau die Nullstellen von f, f ist separabel, und es gilt

$$f = \prod_{i \in \mathbb{F}_p} (X - (a+i)) \quad \text{in } k(a)[X].$$

Remark 2.91. $\operatorname{char} k = p > 0$.

In Analogie zur Definition von $\sqrt[n]{c}$ als eine Nullstelle von $X^n - c$ definieren wir $R(c)$ als eine Nullstelle des Artin-Schreier-Polynoms $X^p - X - c$. (Eindeutig bis auf Addition von Elementen des Primkörpers $\mathbb{F}_p$.)

Remark 2.92. Lösungsformel für Gleichungen zweiten Grades in Charakteristik 2, $\operatorname{char} k = 2$.

Sei

$$f(X) = X^2 + bX + c \in k[X]$$

gegeben. Im Fall $b = 0$ hat dies die eindeutige Lösung $\sqrt{-c} = \sqrt{c}$ (in geeignetem Erweiterungskörper).

Gelte $b \neq 0$. (Quadratische Ergänzung geht nicht.) Die Substitution $X = bZ$ liefert

$$f(bZ) = b^2 Z^2 + b^2 Z + c$$

bzw.

$$b^{-2} f(bZ) = Z^2 + Z + b^{-2} c = Z^2 - Z - b^{-2} c.$$

Dies hat die beiden Lösungen

$$R\Big(\frac{c}{b^2}\Big), R\Big(\frac{c}{b^2}\Big) + 1.$$

Also hat f die beiden Lösungen

$$bR\Big(\frac{c}{b^2}\Big), bR\Big(\frac{c}{b^2}\Big) + b.$$

Theorem 2.93 (Artin-Schreier)**.** *Sei $k \subset K$ eine Körpererweiterung in Charakteristik $p > 0$.*

(a) Ist $k \subset K$ eine zyklische Galois-Erweiterung vom Grad p, so gilt $K = k(a)$ für ein Element $a \in K$ mit $\min_{a/k} = X^p - X - c$.

(b) Gilt $K = k(a)$ für ein $a \in K$, das Nullstelle eines Polynoms $X^p - X - c \in k[X]$ ist, so ist $k \subset K$ eine zyklische Galois-Erweiterung. In $k[X]$ ist $X^p - X - c$ entweder irreduzibel oder zerfällt (vollständig) in Linearfaktoren. Im ersten Fall hat $k \subset K$ Grad p, im zweiten Fall Grad 1.

Proof. (a): Für jedes $b \in k$ gilt $\mathrm{Sp}_{K/k}(b) = pb = 0$ nach Lemma 2.73, Teil (a). Insbesondere gilt das für $b = -1$, so dass wir nach Satz 2.88 ein $a \in K$ finden mit $-1 = a - g(a)$, wobei wir einen Erzeuger g von $\mathrm{Gal}(K/k)$ fixiert haben. Es folgt $g^i(a) = a + i$ für alle $i \in \mathbb{Z}$. Für $i = 0, \ldots, p-1$ sind die Elemente $g^i(a)$ paarweise verschiedene Nullstellen von $\min_{a/k}$ in K, so dass $[k(a) : k] \geq p$ folgt, und damit $K = k(a)$. Es gilt

$$g(a^p - a) = g(a)^p - g(a) = (a+1)^p - (a+1) = a^p + 1 - a - 1 = a^p - a$$

und somit $c := a^p - a \in k$. Es ist also a Nullstelle von $X^p - X - c$, und dieses Polynom ist aus Gradgründen bereits das Minimalpolynom von a über k.

(b): Wie oben erklärt hat dann $f := X^p - X - c$ genau die p verschiedenen Nullstellen

$$a, a+1, a+2, \ldots, a+p-1 \in K,$$

ist separabel und zerfällt über $k(a)$ in Linearfaktoren. Somit ist $k \subset k(a)$ Zerfällungskörper des separablen Polynoms f und somit galoissch.

- 1. Fall: f hat eine Nullstelle in k:
  Dann gilt $k = k(a)$.
- 2. Fall: f hat keine Nullstelle in k:
  Wir behaupten zunächst, dass dann f irreduzibel über k ist. Sonst hat f in $k[X]$ eine Faktor h vom Grad $1 \leq d < p$, den wir ohne Einschränkung als normiert annehmen können. In $K[X]$ haben wir die Zerlegung

  $$f = \prod_{i=0}^{p-1} (X - a - i).$$

  Es besteht h aus gewissen dieser Faktoren. Der Koeffizient von X^{d-1} in g liegt in k und hat die Gestalt $-da + j$ für ein Element j im Primkörper $\mathbb{F}_p \subset k$. Es folgt $-da \in k$ und $a \in k$, denn d ist invertierbar in $\mathbb{F}_p$. Dann hat aber f die Nullstelle a in k. Dieser Widerspruch zeigt, dass f irreduzibel in $k[X]$ ist.

Also ist f das Minimalpolynom von a über k, und $k \subset k(a)$ hat Grad p. Die Galoisgruppe $\mathrm{Gal}(K/k)$ hat somit Mächtigkeit p und muss somit zyklisch sein.[50]

□

3. Auflösbarkeit algebraischer Gleichungen

Ziel: Gleichungen zum Auflösen algebraischer Gleichungen vom Grad ≥ 5 gibt es aus prinzipiellen Gründen nicht.

Erinnerung:

Definition 3.1. Sei G eine Gruppe. Eine **Normalreihe** ist eine (endliche) Kette von Untergruppen

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_n = \{e\}, \tag{3.1}$$

so dass jedes G_{i+1} Normalteiler in G_i ist, für alle $0 \leq i \leq n-1$.[51] Die Quotienten G_i/G_{i+1} werden als **Faktorgruppen** der Normalreihe bezeichnet.

Es heißt G **auflösbar**, falls G eine Normalreihe mit abelschen Faktoren besitzt.

Observation 3.2.

- Untergruppen und Quotienten(gruppen) auflösbarere Gruppen sind auflösbar. (Schneide bzw. projiziere Normalreihe; Faktoren werden Untergruppen bzw. Quotienten der gegebenen Faktoren.)
- Ist G eine Gruppe und $N \subset G$ ein Normalteiler, so ist G auflösbar genau dann, wenn N und G/N auflösbar sind. (Sind N und G/N auflösbar, so kombiniere man gegebene Normalreihen geeignet; die umgekehrte Implikation folgt bereits aus dem vorigen Punkt.)

  „Kurze exakte Sequenz

  $$N \hookrightarrow G \twoheadrightarrow G/N$$

  von Gruppen.“
- Produkte auflösbarer Gruppen sind auflösbar (kombiniere Normalreihen in offensichtlicher Weise, oder betrachte die Reihe der abgeleiteten Gruppen). (Für endliche Produkte folgt das aus dem vorhergehenden Punkt.)
- Ist G endlich und auflösbar, so besitzt G eine Normalreihe mit zyklischen Faktoren von Primzahlgrad.

  Beweis: Sei eine Normalreihe (3.1) der Länge n gegeben.

[50] Explizit kann man auch einen Erzeuger wie folgt finden: Der Fortsetzungssatz 1.48 für einfache algebraische Erweiterungen liefert einen Körpermorphismus $g : k(a) \to k(a+1) = k(a)$ mit $g(a) = a+1$ und $g|_k = \mathrm{id}_k$, der offensichtlich bijektiv ist; somit $g \in \mathrm{Gal}(k(a)/k)$. Wegen $g^i(a) = a + i$ hat g die Ordnung p, und ist somit ein Erzeuger von $\mathrm{Gal}(k(a)/k)$.

[51] Ich folge hier Bosch in der Terminologie. Besser gefällt mir der Begriff Subnormalreihe dafür. Bei Normalreihe verlangt man dann zusätzlich, dass alle G_i normal in G sind.

Der Fall $n = 0$ ist trivial. Gelte $n = 1$. Dann ist G abelsch und endlich, und die Behauptung ist offensichtlich: Falls $G \neq \{e\}$, so finde ein Element $g \in G$ von Primzahlordnung. Dann ist $N := \langle g \rangle \subset G$ ein Normalteiler und wir können induktiv mit G/N weitermachen.

Gelte $n > 1$. Dann haben wir eine kurze exakte Sequenz

$$G_1 \hookrightarrow G \twoheadrightarrow G/G_1,$$

denn $G_1 \subset G$ ist normal. Per Induktion haben sowohl G_1 als auch G/G_1 Normalreihen mit zyklischen Faktoren von Primzahlgrad (denn G_1 hat offensichtlich eine Normalreihe der Länge $n-1$ und G/G_1 (als abelsche Gruppe) eine der Länge 1). Kombination dieser Normalreihen liefert die gesuchte Normalreihe.

Definition 3.3. Sei $k \subset K$ eine endliche Körpererweiterung. Wir sagen, dass $k \subset K$ durch **Radikale auflösbar** ist, falls es einen Erweiterungskörper E von K gibt sowie eine Körperkette

$$k = E_0 \subset E_1 \subset \cdots \subset E_m = E, \tag{3.2}$$

so dass jeweils $E_i = E_{i-1}(a_i)$ gilt für $a_i \in E_i$ ein Element des folgenden Typs:

(EW) ($\sqrt[?]{1}$) eine Einheitswurzel, oder

(Wurzel) ($\sqrt[n]{c}$) eine Nullstelle eines Polynoms $X^n - c \in E_{i-1}[X]$ mit $\operatorname{char} k \nmid n$, oder

(Artin-Schreier) (AS) eine Nullstelle eines Polynoms $X^p - X - c \in E_{i-1}[X]$, falls $\operatorname{char} k = p > 0$.

(Dabei sind natürlich n und c abhängig von a_i.)

Remark 3.4.

- Der Fall (EW) ist Spezialfall von (Wurzel): Sei $\zeta \in \overline{K}$ eine Einheitswurzel. Sei n die Ordnung von ζ. Dann ist Nullstelle von $X^n - 1$ und $\operatorname{char} k \nmid n$, denn:

  Es hat $\langle \zeta \rangle$ genau n Elemente und ist enthalten in U_n, was höchstens n Elemente hat. Also $\langle \zeta \rangle = U_n$. Somit hat U_n genau n Elemente, so dass also $X^n - 1$ separabel ist. Es folgt $nX^{n-1} \neq 0$ (Lemma 1.71.(a)), also $n \neq 0$ in k und damit die Behauptung.

  Diese Argument zeigt also, dass man (EW) umschreiben kann zu

  (EW') ($\sqrt[n]{1}$) eine n-te primitive Einheitswurzel mit $\operatorname{char} k \nmid n$.

  Es ist jedoch geschickt für die folgenden Beweise, den Einheitswurzelfall separat zu behandeln.
- Im Fall $\operatorname{char} k = 0$ entsteht also jedes E_i aus E_{i-1} durch Adjunktion einer Nullstelle eines Polynoms $X^n - c \in E_{i-1}[X]$.
- Die Erweiterung $k \subset E$ ist separabel, denn alle $E_{i-1} \subset E_i$ sind separabel.
- Insbesondere: Ist $k \subset K$ durch Radikale auflösbar, so ist $k \subset K$ separabel.

Definition 3.5. Eine endliche Erweiterung $k \subset K$ heißt **galois-theoretisch auflösbar** (übliche Terminologie: **auflösbar**), falls es eine Erweiterung $K \subset E$ gibt, so dass $k \subset E$ eine endliche Galois-Erweiterung ist mit auflösbarer Galois-Gruppe.

Ende 21. Vorlesung Donnerstag 28. Juni 2012.

Observation 3.6.

- Ist $k \subset K$ galois-theoretisch auflösbar, so ist $k \subset K$ separabel.
- ($k \subset K$ endlich.)
  Ist N die normale Hülle von K/k in $\overline{K}$, so ist $k \subset K$ galois-theoretisch auflösbar genau dann, wenn $k \subset K$ separabel ist und $\mathrm{Gal}(N/k)$ auflösbar.

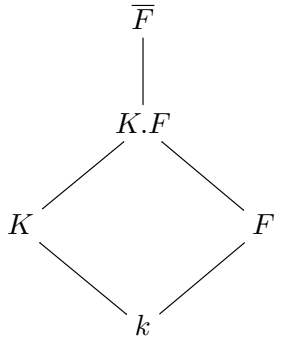
  Proof. $\Rightarrow$: Ist E wie in der Definition, so ist sicherlich $k \subset K$ separabel. Damit ist $k \subset N$ separabel und damit galoissch. Wir können (mit Hilfe der Fortsetzungssätze bzw. der Eindeutigkeit des algebraischen Abschlusses) ohne Einschränkung annehmen, dass $E \subset \overline{K}$. Es folgt $N \subset E$, und die Restriktionsabbildung $\mathrm{Gal}(E/k) \to \mathrm{Gal}(N/k)$ ist surjektiv. Quotienten auflösbarer Gruppen sind auflösbar.
  $\Leftarrow$: Ist $k \subset K$ separabel, so ist $k \subset N$ endlich und galoissch, und hat laut Annahme auflösbare Galois-Gruppe. □

- Insbesondere ist eine endliche Galois-Erweiterung $k \subset K$ galois-theoretisch auflösbar genau dann, wenn $\mathrm{Gal}(K/k)$ eine auflösbare Gruppe ist.

Remark 3.7. Sei $f \in k[X]$ ein nicht konstantes Polynom, und sei $k \subset K$ ein Zerfällungskörper von f. Dann sagt man, das die Gleichung $f(x) = 0$ **über** k **galois-theoretisch auflösbar** (bzw. **über** k **durch Radiakale auflösbar**) ist, genau dann, wenn $k \subset K$ diese Eigenschaft hat.
(unabhängig von Wahl des Zerfällungskörpers.)

Lemma 3.8. *Sei $k \subset F$ eine beliebige Erweiterung, und sei $k \subset K$ eine endliche Erweiterung mit $K \subset \overline{F}$. Dann vererben sich die folgenden Eigenschaften von K/k auf $K.F/F$:*

(I) galois-theoretisch auflösbar;
(II) galoissch und galois-theoretisch auflösbar;
(III) durch Radikale auflösbar;
(IV) (wohl nicht verwendet:) ausschöpfbar durch eine Körperkette der Form (3.2)*.*



Proof. (I): Sei $K \subset E$ mit $k \subset E$ endlich galoissch und $\mathrm{Gal}(E/k)$ auflösbar. Ohne Einschränkung können wir $E \subset \overline{F}$ annehmen (denn $\overline{F}$ enthält den algebraischen Abschluss $\overline{F}_{\mathrm{alg}/K}$ von K, siehe Lemma 1.45).

Es ist bekannt, dass $F \subset E.F$ endlich galoissch ist, und offenbar ist Restriktion $\mathrm{Gal}(E.F/F) \xrightarrow{(?)|_E} \mathrm{Gal}(E/k)$ ein wohldefinierter injektiver Morphismus von Gruppen. Also ist $\mathrm{Gal}(E.F/F)$ auflösbar als Untergruppe einer auflösbaren Gruppe.
[52]

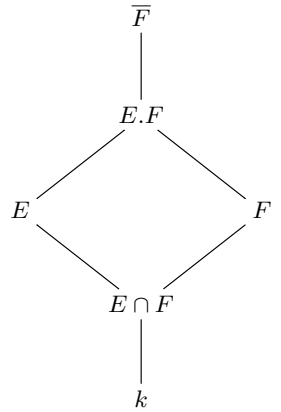
(II): Folgt aus dem Beweis von (I), wenn man $E = K$ wählt.

(III) und (IV): Das ist trivial. Man wende schlicht auf die gegebene Körperkette (3.2) die Abbildung $?.F$ an. □

Lemma 3.9. *Sei $k \subset F \subset K$ ein Turm endlicher Erweiterungen. Dann sind äquivalent:*

(a) $k \subset K$ ist galois-theoretisch auflösbar.

[52] Genauer: Betrachte



Nach Proposition 2.23, Teil (a) (Translationssatz) ist dann $F \subset E.F$ endlich galoissch mit Galoisgruppe

$$\mathrm{Gal}(E.F/F) \xrightarrow[\sim]{(?)|_E} \mathrm{Gal}(E/E \cap F) \subset \mathrm{Gal}(E/k).$$

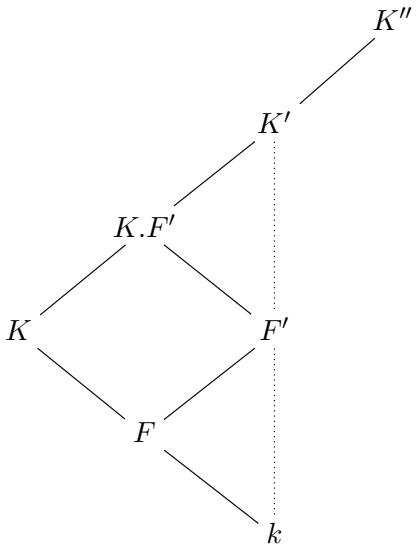
Also ist $\mathrm{Gal}(E.F/F)$ isomorph zu einer Untergruppe einer auflösbaren Gruppe und damit auflösbar.

(b) $k \subset F$ und $F \subset K$ sind galois-theoretisch auflösbar.

Ersetzen wir „galois-theoretisch auflösbar“ durch „durch Radikale auflösbar“, so bleiben die beiden Bedingungen äquivalent.

Proof. (a) $\Rightarrow$ (b): Sei $K \subset K'$ mit $k \subset K$ endlich galoissch mit $\mathrm{Gal}(K'/k)$ auflösbar. Dann ist offensichtlich $k \subset F$ galois-theoretisch auflösbar. Außerdem ist $F \subset K'$ endlich galoissch, und $\mathrm{Gal}(K'/F) \subset \mathrm{Gal}(K'/k)$ ist auflösbar als Untergruppe einer auflösbaren Gruppe. Damit ist $F \subset K$ galois-theoretisch auflösbar.

(b) $\Rightarrow$ (a): Wir erklären das folgende (kommutative) Diagramm, in dem gestrichelte Linien für endliche Galois-Erweiterungen mit auflösbarer Galoisgruppe stehen.



Wir können ohne Einschränkung annehmen, dass alle folgenden Erweiterungen in einem fixierten algebraischen Abschluss $\overline{K}$ von K stattfinden.

Zunächst wähle $F \subset F'$, so dass $k \subset F'$ eine endliche Galois-Erweiterung ist mit auflösbarer Galoisgruppe. Nach Lemma 3.8 (I) ist $F' \subset K.F'$ galois-theoretisch aufösbar. Wir können also $K.F' \subset K'$ finden, so dass $F' \subset K'$ eine endliche Galois-Erweiterung mit auflösbarer Galoisgruppe ist.

Es ist $k \subset K'$ nicht notwendig normal. Sei K'' das folgende Kompositum

$$K'' := \prod_{\sigma \in \mathrm{Hom}_k(K', \overline{K})} \sigma(K').$$

Es ist K'' die normale Hülle von $k \subset K'$ (in $\overline{K}$).

(Beweis: Da $k \subset K'$ separabel und endlich, habe $K' = k(a)$ für ein $a \in K'$ nach dem Satz 1.85 vom primitiven Element. Dann gilt $\sigma(K') = k(\sigma(a))$ für jedes $\sigma \in \mathrm{Hom}_k(K', \overline{K})$, also ist $K'' = k(\text{Nullstellen von } \min_{a/k} \text{ in } \overline{K})$. Nun verwende Satz 1.65.)

Sowohl $k \subset F'$, $F' \subset K''$ und $k \subset K''$ sind endlich galoissch. Wir haben also eine „kurze exakte Sequenz“ von Gruppen

$$\mathrm{Gal}(K''/F') \hookrightarrow \mathrm{Gal}(K''/k) \twoheadrightarrow \mathrm{Gal}(F'/k)$$

nach dem Hauptsatz 2.18 (c) der Galois-Theorie.

Zu zeigen bleibt, dass $\mathrm{Gal}(K''/k)$ auflösbar ist. Da $\mathrm{Gal}(F'/k)$ auflösbar ist, reicht es zu zeigen, dass $\mathrm{Gal}(K''/F')$ auflösbar ist.

Sei $\sigma \in \mathrm{Hom}_k(K', \overline{K})$. Weil $k \subset F'$ normal ist, gilt $\sigma(F') = F'$. Mit $F' \subset K'$ ist auch $F' = \sigma(F') \subset \sigma(K')$ endlich galoissch mit auflösbarer Galoisgruppe. Insbesondere ist die Restriktionsabbildung

$$\begin{aligned} \mathrm{Gal}(K''/F') &\to \mathrm{Gal}(\sigma(K')/F'), \\ g &\mapsto g|_{\sigma(K')}, \end{aligned}$$

ein wohldefinierter Morphismus von Gruppen.

Indem wir nun σ variieren, erhalten wir einen Gruppenmorphismus

$$\mathrm{Gal}(K''/F') \to \prod_{\sigma \in \mathrm{Hom}_k(K', \overline{K})} \mathrm{Gal}(\sigma(K')/F').$$

Dieser ist offenbar injektiv. Die Gruppe auf der rechten Seite ist auflösbar; somit ist $\mathrm{Gal}(K''/F')$ auflösbar.

Wir zeigen nun die Äquivalenz für „durch Radikale auflösbar“.

(a) $\Rightarrow$ (b): Sei $k \subset K$ durch Radikale auflösbar. Dann ist sicherlich auch $k \subset F$ durch Radiakale auflösbar. Aber auch $F \subset K$ ist dann durch Radikale auflösbar. Gegeben eine Kette (3.2) wie in der Definition, ersetze man schlicht E_i durch $F.E_i$.

(b) $\Rightarrow$ (a): Sei $F \subset F'$ eine Erweiterung, so dass $k \subset F'$ durch eine Kette des Typs (3.2) ausgeschöpft werden kann.

Nach Lemma 3.8 (III) ist mit $F \subset K$ auch $F' \subset K.F'$ durch Radikale auflösbar. Mithilfe der obigen Kette folgt sofort, dass $k \subset K.F'$ durch Radikale auflösbar ist. Also ist erst recht $k \subset K$ durch Radikale auflösbar. □

Ende 22. Vorlesung Montag 2. Juli 2012.

Theorem 3.10. *Sei $k \subset K$ eine endliche Körpererweiterung. Dann ist $k \subset K$ durch Radikale auflösbar genau dann, wenn $k \subset K$ galois-theoretisch auflösbar ist.*

Proof. $\boxed{\Leftarrow:}$ Sei $k \subset K$ galois-theoretisch auflösbar. Indem wir K vergrößern, dürfen wir annehmen, dass $k \subset K$ eine Galois-Erweiterung ist. Dies verwendet neben der Definition die „durch Radikale auflösbar“-Version von Lemma 3.9.

Wir arbeiten in einem fixierten algebraischen Abschluss von K.

Sei m das Produkt aller Primzahlen $\neq \mathrm{char}\, k$, die $[K : k]$ teilen. Sei $F := k(\zeta_m)$ für ζ_m eine primitive m-te Einheitswurzel. Dann ist $k \subset F$ vom Typ (EW') und somit durch Radikale auflösbar.

Es genügt also zu zeigen (nach der „durch Radikale auflösbar“-Version von Lemma 3.9), dass $F \subset F.K$ durch Radikale auflösbar ist.

Nach Lemma 3.8 (II) ist $F \subset F.K$ galoissch mit auflösbarer Galoisgruppe $G := \mathrm{Gal}(F.K/F)$.

Sei

$$G = G_0 \supset G_1 \supset \cdots \supset G_i \supset G_{i+1} \supset \cdots \supset G_n = \{e\},$$

eine Normalreihe mit Faktoren, die zyklisch sind von Primzahlgrad, also etwa $G_i/G_{i-1} \cong \mathbb{Z}/p_i\mathbb{Z}$ für p_i eine Primzahl.

Nach dem Hauptsatz 2.18 der Galois-Theorie korrespondiert zu dieser Normalreihe eine Körperkette

$$F = F_0 \subset F_1 \subset \cdots \subset F_i \subset F_{i+1} \subset \cdots \subset F_n = F.K$$

Fixiere $0 \leq i < n$.

Es ist $F_i \subset F.K$ eine Galois-Erweiterung mit Galois-Gruppe G_i; da $G_{i+1} \subset G_i$ Normalteiler ist, ist $F_i \subset F_{i+1}$ (normal und) galoissch mit Galoisgruppe $G_i/G_{i+1} \cong \mathbb{Z}/p_i\mathbb{Z}$, also vom Grad p_i.

1. Fall: $p_i \neq \mathrm{char}\, k$**.** Beachte, dass

$$p_i \mid |G| = [F.K : F] = [K : K \cap F] \mid [K : k]$$

(Proposition 2.23 (a) (Translationssatz)). Also ist p_i ein Teiler von m, und somit enhalten F und F_i alle p_i-ten Einheitswurzeln. Nach Satz 2.85 (a) ensteht also F_{i+1} aus F_i durch Adjunktion eines Elements a mit Minimalpolynom $X^{p_i} - c$ über F_i. Die Erweiterung $F_i \subset F_{i+1}$ ist also vom Typ (Wurzel).

2. Fall: $p_i = \mathrm{char}\, k$**.** Nach dem Satz 2.93 von Artin-Schreier, Teil (a) entsteht dann F_{i+1} aus F_i durch Adjunktion eines Elements a mit Minimalpolynom $X^p - X - c$ über F_i. Die Erweiterung $F_i \subset F_{i+1}$ ist also vom Typ (Artin-Schreier).

Also ist $F \subset F.K$ durch eine Körperkette des Typs (3.2) ausschöpfbar und insbesondere durch Radikale auflösbar.

$\boxed{\Rightarrow:}$ Sei umgekehrt $k \subset K$ durch Radikale auflösbar. Wegen der Definition und Lemma 3.9 (Version „galois-theoretisch auflösbar“) genügt es anzunehmen dass $k \subset K$ vom Typ (EW), (Wurzel) oder (Artin-Schreier) wie in Definition 3.3 ist.

Der Fall (EW) bzw. genauer (und äquivalent) (EW') ergibt eine endliche abelsche Galois-Erweiterung nach Satz 2.53.

Der Fall (Artin-Schreier) ergibt eine endliche zyklische Galois-Erweiterung nach dem Satz 2.93 von Artin-Schreier, Teil (b); insbesondere ist diese galois-theoretisch auflösbar.

Es bleibt der Fall (Wurzel) zu betrachten. Es gelte also $K = k(a)$, wobei a Nullstelle von $X^n - c \in k[X]$ ist mit $\mathrm{char}\, k \nmid n$. Sei ζ_n eine primitive n-te Einheitswurzel in $\overline{K}$. Dann ist $k \subset k(\zeta_n)$ galois-theoretisch auflösbar, wie gerade im Fall (EW) bemerkt, und $k(\zeta_n) \subset k(\zeta_n, a)$ ist endliche zyklische Galois-Erweiterung nach Satz 2.85 (b). Nach Lemma 3.9 (Version „galois-theoretisch auflösbar“) sind dann auch $k \subset k(\zeta_n, a)$ und $k \subset k(a) = K$ galois-theoretisch-auflösbar. □

Corollary 3.11. *Jede separable Erweiterung $k \subset K$ vom Grad ≤ 4 ist galois-theoretisch auflösbar und durch Radikale auflösbar.*

Proof. Der Satz 1.85 vom primitiven Element liefert $K = k(a)$. Sei K' ein Zerfällungskörper von $\min_{a/k}$ (also die normale Hülle von $k \subset K$). Es hat $\min_{a/k}$ genau vier Nullstellen in K', und wir haben eine Einbettung $\mathrm{Gal}(K'/k) \subset \mathrm{Sym}(\text{Nst. von } \min_{a/k}) \cong S_4$. Mit S_4 ist damit auch $\mathrm{Gal}(K'/k)$ auflösbar. □

Corollary 3.12 (Satz von Abel-Ruffini)**.** *Wikipedia: Die allgemeine Gleichung fünften und höheren Grades ist nicht durch Radikale auflösbar.*

Es existieren endliche separable Erweiterungen, die nicht durch Radikale auflösbar sind. Beispielsweise ist die allgemeine Gleichung n-ten Grades für $n \geq 5$ nicht durch Radikale auflösbar.

Proof. Die allgemeine Gleichung n-ten Grades hat Galoisgruppe S_n. Für $n \geq 5$ ist S_n nicht auflösbar. □

Remark 3.13. Bosch: Für jede Primzahl p gibt es eine Galoiserweiterung $\mathbb{Q} \subset K$ mit Galoisgruppe S_p.

Man kann zeigen, dass es für jedes $n \in \mathbb{N}_+$ unendlich viele Galoiserweiterungen $\mathbb{Q} \subset K$ gibt mit $\mathrm{Gal}(K/\mathbb{Q}) = S_n$ (oder auch A_n).

Siehe Wikipedia "Inverse Galois Theory".

Steht so in Einleitung von Malle-Matzat: Inverse Galois Theory.

4. Vermischtes am Ende

4.1. **Der Fundamentalsatz der Algebra.**

Theorem 4.1. *Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen.*

Wir verwenden die folgenden Fakten (Konstruktion von $\mathbb{R}$ aus $\mathbb{Q}$ ist „ analytisch" (Vervollständigung). Deswegen(?) benötige analytischen Input. Der Fundamentalsatz der Algebra hat also (anscheinend) keinen rein algebraischen Beweis.)

(a) Jedes relle Polynom ungeraden Grades hat eine Nullstelle in $\mathbb{R}$.
Zwischenwertsatz plus „ Asymptotik" für $x \to \pm\infty$.

(b) Jedes komplexe Polynom zweiten Grades hat eine Nullstelle in $\mathbb{C}$.
(Nach der Lösungsformel ist nur zu zeigen, dass jede komplexe Zahl eine Quadratwurzel in $\mathbb{C}$ hat. Dies ist geometrisch klar. Man kann dies leicht aus der Tatsache folgern, dass jede reelle Zahl ≥ 0 eine Quadratwurzel in $\mathbb{R}$ hat.

Bosch hat einen Alternativbeweis als Übungsaufgabe, der wohl auf Laplace zurueck. Ich habe die Lösung im Internet gefunden und auf meinem Rechner unter beweise-fundamentalsatz-der-algebra.pdf.

Proof. Sei $\mathbb{C} \subset L$ eine endliche Körpererweiterung. Wir können durch eventuellen Übergang zur normalen Hülle von $\mathbb{R} \subset L$ annehmen, dass $\mathbb{R} \subset L$ eine Galois-Erweiterung ist. Zu zeigen ist $L = \mathbb{C}$.

Sei $G = \mathrm{Gal}(L/\mathbb{R})$. Schreibe

$$[L : \mathbb{R}] = |G| = 2^t m \quad \text{mit } m \text{ ungerade und } t \in \mathbb{N}.$$

Offensichtlich gilt $t \geq 1$. Sei $S \subset G$ eine 2-Sylow, also $|S| = 2^t$. Den Inklusionen $G \supset S \supset \{1\}$ entsprechen auf Körperseite Inklusionen

$$\mathbb{R} \subset L^S \subset L.$$

Es hat $\mathbb{R} \subset L^S$ den ungeraden Grad m. Der Satz 1.85 vom primitiven Element liefert $L = \mathbb{R}(a)$ für ein $a \in L$. Wegen $\deg(\min_{a/\mathbb{R}}) = m$ (ungerade) hat $\min_{a/\mathbb{R}}$ eine reelle Nullstelle. Es folgt $m = 1$, also $\mathbb{R} = L^S$.

Also ist $\mathbb{R} \subset L$ eine Galoiserweiterung vom Grad 2^t, und $\mathbb{C} \subset L$ ist eine Galoiserweiterung vom Grad 2^{t-1}. Es ist $\mathrm{Gal}(L/\mathbb{C})$ auflösbar, hat also eine Normalreihe deren sämtliche Faktoren isomorph zu $\mathbb{Z}/2\mathbb{Z}$ sind. Insbesondere entsteht L aus $\mathbb{C}$ durch sukzessives Adjungieren von Elementen vom Grad 2. Da aber kein Element Grad 2 über $\mathbb{C}$ hat, muss $\mathbb{C} = L$ gelten. □

4.2. **Netter Satz von Artin.**

Theorem 4.2 (Satz von E. Artin(-Schreier?), siehe [Lan52, Cor. VI.9.3]; wir folgem dem Beweis in [Bos, Abschnitt 6.3, Satz 2])**.** *Ist k ein Körper, so dass (s)ein algebraischer Abschluss $\overline{k}$ endlichen Grad über k hat, so gilt*

- *entweder: $k = \overline{k}$,*
- *oder: k hat Charakteristik Null, die Körpererweiterung $k \subset \overline{k}$ hat Grad zwei und es gibt $i \in \overline{k}$ mit $i^2 = -1$ und $k(i) = \overline{k}$.*

Proof. Es ist $k \subset \overline{k}$ normal.

Wir behaupten, dass $k \subset \overline{k}$ separabel ist. Im Fall $\operatorname{char} k = 0$ ist dies trivial. Gelte $\operatorname{char} k = p > 0$. Nach Satz 1.93 haben wir

$$k \underset{\text{separabel}}{\subset} E := \overline{k}_{sep/k} \underset{\text{rein inseparabel}}{\subset} \overline{k}.$$

Sei $\mathrm{Fr} := \mathrm{Fr}_p : \overline{k} \to \overline{k}$, $x \mapsto x^p$ der Frobenius-Morphismus. Er ist ein Automorphismus, da $\overline{k}$ algebraisch abgeschlossen ist. Es gilt $\mathrm{Fr}(E) \subset E$ und

$$[\overline{k} : E] = [\mathrm{Fr}(\overline{k}) : \mathrm{Fr}(E)] = [\overline{k} : \mathrm{Fr}(E)]$$

ist endlich. Es folgt $\mathrm{Fr}(E) = E$. Insbesondere induziert Fr einen Automorphismus von E. Jedes $a \in \overline{k}$ ist rein inseparabel über E, wird also von einer Potenz von Fr nach E abgebildet, und muss damit bereits in E liegen. Es folgt $E = \overline{k}$. Dies zeigt, dass $k \subset \overline{k}$ separabel ist.

Ab jetzt ist $\operatorname{char} k$ wieder beliebig. Wir wissen also, dass $k \subset \overline{k}$ eine endliche Galois-Erweiterung ist.

Sei $i \in \overline{k}$ mit $i^2 = -1$. Dann ist auch $k(i) \subset \overline{k}$ eine Galois-Erweiterung.

Wir nehmen an, dass $k(i) \subsetneq \overline{k}$ gilt. Dann gibt es eine Untergruppe $U \subset \mathrm{Gal}(\overline{k}/k(i))$, deren Ordnung eine Primzahl ℓ ist. Ihr entspricht ein Zwischenkörper $k(i) \subset L := \overline{k}^U \subset \overline{k}$ mit $[\overline{k} : L] = \ell$. Die Erweiterung $L \subset \overline{k}$ ist endlich zyklisch galoissch.

1. Fall: Gelte $\operatorname{char} k = \ell$**:** Nach dem Satz 2.93 von Artin-Schreier, Teil (a) gilt dann $\overline{k} = L(a)$ für ein $a \in \overline{k}$ mit Minimalpolynom $X^\ell - X - c \in L[X]$. Betrachte die Abbildung

$$\begin{aligned} \tau : \overline{k} &\to \overline{k}, \\ x &\mapsto x^\ell - x. \end{aligned}$$

Sie ist surjektiv, da $\overline{k}$ algebraisch abgeschlossen ist. Die Abbildung $\mathrm{Sp} := \mathrm{Sp}_{\overline{k}/L} : \overline{k} \to L$ ist ebenfalls surjektiv nach Satz 2.77. Sicherlich restringiert τ eine Abbildung $\tau|_L : L \to L$. Wir behaupten, dass das Diagramm

$$\begin{array}{ccc} \overline{k} & \xrightarrow{\tau} & \overline{k} \\ \big\downarrow{\scriptstyle \mathrm{Sp}} & & \big\downarrow{\scriptstyle \mathrm{Sp}} \\ L & \xrightarrow{\tau} & L \end{array}$$

kommutiert. Dies folgt aus

$$\mathrm{Sp}(x^\ell) = \sum_{g \in \mathrm{Gal}(\overline{k}/L)} g(x^\ell) = \Big(\sum_{g \in \mathrm{Gal}(\overline{k}/L)} g(x) \Big)^\ell = \big(\mathrm{Sp}(x) \big)^\ell$$

für $x \in \overline{k}$. Somit ist auch $\tau|_L : L \to L$ surjektiv, und somit hat dass über L irreduzible Polynom $X^\ell - X - c$ eine Nullstelle in L.

Dieser Widerspruch zeigt, dass der Fall 1 nicht eintreten kann.

2. Fall: Gelte $\operatorname{char} k \neq \ell$**:** (Dies deckt auch den Fall $\operatorname{char} k = 0$ ab.) Sei $\zeta \in \overline{k}$ eine primitive ℓ-te Einheitswurzel. Die Erweiterung $L \subset L(\zeta)$ hat nach Satz 2.53 einen Grad $\leq \varphi(\ell) = \ell - 1 < \ell = [\overline{k} : L]$. Da $[\overline{k} : L]$ eine Primzahl ist, muss $L = L(\zeta)$ gelten. Nach Satz 2.85 (a) folgt $\overline{k} = L(a)$ für ein $a \in \overline{k}$ mit Minimalpolynom $X^\ell - c$ über L.

Sei $\alpha \in \overline{k}$ mit $\alpha^\ell = a$, und setze $\beta := \mathrm{N}_{\overline{k}/L}(\alpha) \in L$. Die Multiplikativität der Norm und Lemma 2.73 (b) zeigen

$$\beta^\ell = \mathrm{N}_{\overline{k}/L}(\alpha)^\ell = \mathrm{N}_{\overline{k}/L}(\alpha^\ell) = \mathrm{N}_{\overline{k}/L}(a) = (-1)^\ell(-c) = (-1)^{\ell+1}c.$$

Ist ℓ ungerade, so ist also $\beta \in L$ eine ℓ-te Wurzel aus c, was der Irreduzibilität von $X^\ell - c \in L[X]$ widerspricht. Also muss $\ell = 2$ gelten. Dann ist $\beta \in L$ eine Quadratwurzel aus $-c$. Wegen $i \in k(i) \subset L$ gilt $i\beta \in L$, und das ist eine Quadratwurzel von c, ebenfalls im Widerspruch zur Irreduzibilität von $X^2 - c$.

Dieser Widerspruch zeigt, dass der Fall 2 nicht eintreten kann.

Insgesamt zeigt dies, dass $k(i) = \overline{k}$ gilt. Die Erweiterung $k \subset k(i) = \overline{k}$ hat also Grad eins oder zwei.

Wir müssen nur noch zeigen, dass im Fall $[\overline{k} : k] = 2$ die Charakteristik von k Null ist.

Gelte also $k \subsetneq k(i) = \overline{k}$. Insbesondere gilt $\overline{k} = k \oplus ki$.

Wir behaupten, dass die Summe zweier Quadrate in k wieder ein Quadrat ist. Seien $a, b \in k$. Sei $x + iy \in \overline{k} = k \oplus ki$ eine Quadratwurzel aus $a + bi$. Es

gilt also $x^2 - y^2 + 2ixy = a + bi$. Es folgt

$$a^2 + b^2 = (x^2 - y^2)^2 + (2xy)^2 = (x^2 + y^2)^2.$$

Per Induktion ist jede endliche Summe von Quadraten in k wieder ein Quadrat in k.

Gilt $\operatorname{char} k = p > 0$, so ist -1 die $(p-1)$-fache Summe des Quadrats $1 = 1^2$,

$$-1 = p - 1 = \underbrace{1^2 + \cdots + 1^2}_{p-1 \text{ mal}},$$

und somit ein Quadrat in k. Dies impliziert $\pm i \in k$ im Widerspruch zur Annahme.

Die Charakteristik von k muss also Null sein. □

Ende 23. Vorlesung Donnerstag 5. Juli 2012. (Satz 4.1 nachzutragen.)

Corollary 4.3. *Sei $K \subset \mathbb{R}$ ein Unterkörper von endlichem Grad. Dann gilt $K = \mathbb{R}$.*

Proof. Nach dem Satz 4.2 von Artin(-Schreier?), angewendet auf $K \subset \mathbb{C}$, hat diese Erweiterung Grad 2. Aus $K \subset \mathbb{R} \subset \mathbb{C}$ folgt dann $K = \mathbb{R}$. □

4.3. **Das Quadratische Reziprozitätsgesetz.** Frage: Seien $a, b \in \mathbb{Z}$ gegeben. Gibt es ganze Zahlen $x, y \in \mathbb{Z}$ mit

$$a = x^2 + by.$$

Äquivalent: Ist $\overline{a}$ ein Quadrat in $\mathbb{Z}/b\mathbb{Z}$?

Ist dies der Fall, so heißt a ein **quadratischer Rest modulo** b oder ein **Quadrat modulo** b.

Man kann dieses Problem auf den Fall reduzieren, dass b eine Primzahl ist. Ich habe es am Ende der Vorlesung sogar kurz erklärt.

Exercise 4.4. Konkrete Frage (für Studierende): Ist 94 ein quadratischer Rest modulo 109?

Antwort siehe Lösung 4.15

Wir reduzieren das Problem zunächst auf den Fall, dass b eine Primzahl ist, und erklären dann die Lösung durch das quadratische Reziprozitätsgesetz, eine jedenfalls auf den ersten Blick verblüffende Aussage.

- Seine $b_1, b_2 \in \mathbb{Z}$ teilerfremd. Dann ist a ein Quadrat modulo $b_1 b_2$ genau dann, wenn es ein Quadrat modulo b_1 und ein Quadrat modulo b_2 ist: Der Chinesische Restsatz liefert den Ringisomorphismus

  $$\mathbb{Z}/b_1 b_2 \mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/b_1\mathbb{Z} \times \mathbb{Z}/b_2\mathbb{Z},$$

  der die obige Aussage unmittelbar zeigt.

  Ohne Einschränkung können wir also b als Primzahlpotenz auffassen.

  (Wir nehmen hier an, dass wir die Primfaktorzerlegung von b kennen. Zumindest, falls wir explizit rechnen möchten.)

- Sei b eine Primzahlpotenz, etwa $b = p^s$. Sei $a = p^r\alpha$ mit α teilerfremd zu p. Wir wollen
$$p^r\alpha = x^2 + p^s y$$
lösen.

  Falls $r \geq s$, so ist dies trivial: Nimm $x = 0$ und $y = p^{r-s}\alpha$.

  Gelte $r < s$, also $r + t = s$ für $t > 0$. Zu lösen ist also
$$p^r(\alpha - yp^t) = x^2.$$
Der Faktor $\alpha - yp^t$ ist teilerfremd zu p, so dass unsere Gleichung höchstens lösbar ist, wenn r gerade ist.

  Gelte also $r = 2r'$. Dann ist unsere Gleichung lösbar genau dann, wenn
$$\alpha = x'^2 + p^t y$$
lösbar ist.

  In der ursprünglichen Frage können wir also oE annehmen, dass b eine Primahlpotenz ist und dass dass a teilerfremd zu b ist.
- 1. Fall: Sei p eine ungerade Primzahl und a teilerfremd zu p.

  Behauptung: Sei $n \geq 1$. Dann ist a ein Quadrat modulo p^n genau dann, wenn a ein Quadrat modulo p ist.

  Beweis: Die Implikation $\Rightarrow$ ist klar, und für die Implikation $\Leftarrow$ reicht es, das folgende zu zeigen: Ist a Quadrat modulo p^n, so auch modulo p^{n+1}.

  Gelte $a = \widetilde{x}^2 + \widetilde{y}p^n$ für $\widetilde{x}, \widetilde{y} \in \mathbb{Z}$. Zur Lösung von $a = x^2 + yp^{n+1}$ machen wir den Ansatz $x = \widetilde{x} + \lambda p^n$ und finden für λ (und y) die Gleichung
$$a = \widetilde{x}^2 + 2\lambda p^n\widetilde{x} + \lambda^2 p^{2n} + yp^{n+1}.$$
Wegen $a - \widetilde{x}^2 = \widetilde{y}p^n$ können wir dies umschreiben zu
$$\widetilde{y}p^n = 2\lambda p^n\widetilde{x} + \lambda^2 p^{2n} + yp^{n+1}$$
oder gekürzt
$$\widetilde{y} = 2\lambda\widetilde{x} + \lambda^2 p^n + yp.$$
Dies ist aber lösbar: Reduziert nach $\mathbb{Z}/p\mathbb{Z}$ ist $\widetilde{y} \equiv 2\lambda\widetilde{x}$ lösbar, denn 2 und $a \equiv \widetilde{x}^2$ und somit $\widetilde{x}$ sind invertierbar in $\mathbb{F}_p$. Also finden wir $\lambda \in \mathbb{Z}$ mit $\widetilde{y} - 2\lambda\widetilde{x} \in p\mathbb{Z}$; erst recht ist $\widetilde{y} - 2\lambda\widetilde{x} - \lambda^2 p^n$ in $p\mathbb{Z}$ enthalten und somit von der Form yp für ein $y \in \mathbb{Z}$.
- 2. Fall, Teil (a): Sei nun $p = 2$ und a ungerade (= teilerfremd zu 2).

  Behauptung: Sei $n \geq 3$. Dann ist a ein Quadrat modulo 2^n genau dann, wenn a ein Quadrat modulo 8 (alias kongruent zu 1 modulo 8) ist.

  Beweis: Die Quadrate in $\mathbb{Z}/8\mathbb{Z}$ sind $0, 1, 4$, das einzige ungerade Quadrat ist also 1. Die Implikation $\Rightarrow$ ist trivial. Wir zeigen die Implikation $\Leftarrow$ wieder per Induktion. Sei a ein Quadrat module 2^n, also $a = x^2 + y2^n$ für geeignete $x, y \in \mathbb{Z}$. Beachte, dass x ungerade sein muss.

Ist y gerade, etwa $y = 2y'$, so gilt $a = x^2 + y'2^{n+1}$, und a ist Quadrat modulo 2^{n+1}.

Ist y ungerade, so sei $x' := x - 2^{n-1}$, was ungerade ist. Dann gilt

$$\begin{aligned} a &= x^2 + y2^n \\ &= (x' + 2^{n-1})^2 + y2^n \\ &= x'^2 + x'2^n + 2^{2n-2} + y2^n \\ &= x'^2 + 2^n(x' + 2^{n-2} + y). \end{aligned}$$

Man beachte, dass der eingeklammerte Term gerade ist (denn $n \geq 3$), so dass wir unmittelbar fertig sind.

- 2. Fall, Teil (b):
  Die Quadrate in $\mathbb{Z}/2\mathbb{Z}$ sind $0, 1$, das einzige ungerade Quadrat ist also 1.
  Die Quadrate in $\mathbb{Z}/4\mathbb{Z}$ sind $0, 1$, das einzige ungerade Quadrat ist also 1.

Theorem 4.5 (Quadratisches Reziprozitätsgesetz (Theorema Aureum), erster vollständiger Beweis wohl von Gauß 1796, erschienen 1801; davor Euler, Legendre; suche Lemmermeyer)**.** *Seien p und q zwei verschiedene ungerade Primzahlen.*

(a) Ist p oder q kongruent zu 1 modulo 4, so ist p ein Quadrat modulo q genau dann, wenn q ein Quadrat modulo p ist.

(b) Sind p und q kongruent zu 3 modulo 4, so ist p ein Quadrat modulo q genau dann, wenn q kein Quadrat modulo p ist.

Example 4.6.

- Fall (a):
  (a) $p = 5$, $q = 31$: Es ist 31 ein Quadrat modulo 5:

$$31 = 1 = 1^2 \quad \text{in } \mathbb{F}_5$$

  Also ist 5 ein Quadrat modulo 31. In der Tat

$$5 = 31 + 5 = 36 = 6^2 \quad \text{in } \mathbb{F}_{31}.$$

  (b) $p = 5$, $q = 7$: Es ist 5 kein Quadrat modulo 7, denn die Quadrate modulo 7 sind $0, 1, 4, 2$.
  Es ist 7 kein Quadrat modulo 5, denn die Quadrate modulo 5 sind $0, 1, 4$.
- Fall (b): $p = 7$, $q = 11$. Wegen

$$q = 11 = 4 = 2^2 \quad \text{in } \mathbb{F}_7$$

  ist 11 ein Quadrat modulo 7. Also ist 7 kein Quadrat modulo 11; in der Tat sind die Quadrate in $\mathbb{F}_{11}$ gegeben durch $0, 1, 4, 9, 5, 3$.
- Sei $p = 5$. Wir sind also im ersten Fall. Die Quadrate modulo 5 sind $0, 1, 4$. Alle Primzahlen q der Form $1 + 5n$ oder $4 + 5n$ sind also Quadrate modulo 5. Beispiele sind $11, 31$ oder $19, 29$.

In der Tat ist 5 ein quadratischer Rest modulo dieser Primzahlen:

$$\begin{aligned} 4^2 = 16 = 11 + 5 = 5 & \quad \text{in } \mathbb{F}_{11} \\ 6^2 = 36 = 31 + 5 = 5 & \quad \text{in } \mathbb{F}_{31} \\ 9^2 = 81 = 4 \cdot 19 + 5 = 5 & \quad \text{in } \mathbb{F}_{19} \\ 11^2 = 121 = 4 \cdot 29 + 5 = 5 & \quad \text{in } \mathbb{F}_{29} \end{aligned}$$

- $p = 7$ und $q = 11$. Wir sind im zweiten Fall. Die Quadrate in $\mathbb{F}_7$ sind $0, 1, 4, 2$. Insbesondere ist 11 ein Quadrat modulo 7. Also ist 7 kein Quadrat modulo 11. In der Tat sind die Quadrate in $\mathbb{F}_{11}$ gegeben durch $0, 1, 4, 9, 5, 3$.

Definition 4.7. Sei p eine Primzahl und $a \in \mathbb{Z}$. Das **Legendre-Symbol** ist definiert durch die Vorschrift

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & \text{falls } a \in p\mathbb{Z}, \\ 1 & \text{falls } a \notin p\mathbb{Z}, \text{ aber } a \text{ Quadrat modulo } p, \\ -1 & \text{sonst.} \end{cases}$$

Example 4.8. Es gilt (falls definiert für 2 unten)

$$\left(\frac{a}{2}\right) = \begin{cases} 0 & \text{falls } a \text{ gerade}, \\ 1 & \text{falls } a \text{ ungerade}. \end{cases}$$

$$\left(\frac{a}{3}\right) = \begin{cases} 0 & \text{falls } a \equiv 0 \mod 3, \\ 1 & \text{falls } a \equiv 1 \mod 3, \\ -1 & \text{falls } a \equiv 2 \mod 3. \end{cases}$$

$$\left(\frac{1}{p}\right) = 1$$

Remark 4.9. Satz 4.5 ist äquivalent zu

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = \begin{cases} -1 & \text{falls } p = q = 3 \text{ in } \mathbb{Z}/4\mathbb{Z}, \\ 1 & \text{sonst.} \end{cases} \tag{4.1}$$

für p und q verschiedene ungerade Primzahlen, wobei die rechte Gleichheit trivial ist. (Denn $\frac{p-1}{2} \in 1 + 2\mathbb{Z}$ gdw $p - 1 \in 2 + 4\mathbb{Z}$ gdw $p \in 3 + 4\mathbb{Z}$.)

Exercise 4.10. Bestimmen Sie

$$\left(\frac{p}{q}\right)$$

für p und q große Primzahlen!

Lemma 4.11. *Sei p eine ungerade Primzahl.*

(a) $\left(\frac{a}{p}\right)$ *hängt nur von der Klasse von a in $\mathbb{F}_p$ ab.*

(b) Es gilt

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \quad \text{in } \mathbb{F}_p. \tag{4.2}$$

(Dies war wohl Legendres Definition zusammen mit der Bedingung $\left(\frac{a}{p}\right) \in \{-1, 0, 1\} \subset \mathbb{Z}$*.)*

(c) Vollständige Multiplikativität: Für $a, b \in \mathbb{Z}$ *gilt*

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

(Es gelten (a) und (c) trivialerweise auch für $p = 2$*.)*

Proof. (a) ist trivial.

Sei $n \in \mathbb{N}_+$. Wir betrachten die zyklische Gruppe $\mathbb{Z}/2n\mathbb{Z}$ der Ordnung $2n$.

Es ist $(n\cdot) : \mathbb{Z}/2n\mathbb{Z} \to \mathbb{Z}/2n\mathbb{Z}$ ein Morphismus abelscher Gruppen mit Bild $\{\overline{0}, \overline{n}\} \subset \mathbb{Z}/2n\mathbb{Z}$. Der Kern hat demnach n Elemente und ist somit $2\mathbb{Z}/2n\mathbb{Z}$, denn dies liegt im Kern (ist auch einzige Untergruppe/Normalteiler dieser Mächtigkeit). Wir haben also eine kurze exakte Sequenz

$$2\mathbb{Z}/2n\mathbb{Z} \hookrightarrow \mathbb{Z}/2n\mathbb{Z} \xrightarrow{n\cdot} \{\overline{0}, \overline{n}\}$$

abelscher Gruppen (Surjektion rechts).

Sei nun speziell $n = \frac{p-1}{2}$. Da $\mathbb{F}_p^\times$ zyklisch der Ordnung $2n$ ist, ist die obere Zeile des folgenden Diagramms nach obigem eine kurze exakte Sequenz.

$$\begin{array}{ccccc}
\mathbb{F}_p^{\times 2} & \longrightarrow & \mathbb{F}_p^\times & \xrightarrow{(?)^n} & \{\pm 1\} \quad \subset \quad \mathbb{F}_p^\times \\
 & & \cap & & \cap \\
 & & \mathbb{F}_p & \xrightarrow{(?)^n} & \{0, 1, -1\} \quad \subset \quad \mathbb{F}_p \\
 & & \uparrow & \left(\frac{?}{p}\right) & = \uparrow \\
 & & \mathbb{Z} & \longrightarrow & \{0, 1, -1\} \quad \subset \quad \mathbb{Z}
\end{array}$$

Beide Quadrate sind kommutativ: Für das obere Quadrat ist das offensichtlich, für das untere Quadrat ist es klar für Elemente aus $p\mathbb{Z}$, und für andere Elemente folgt es aus der kurzen exakten Sequenz in der ersten Zeile.

Dies zeigt alle Behauptungen. □

Corollary 4.12 (1. Ergänzungssatz)**.** *Ist* p *eine ungerade Primzahl, so gilt*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{falls } p \equiv 1 \mod 4, \\ -1 & \text{falls } p \equiv 3 \mod 4, \end{cases} \quad \text{in } \mathbb{Z}. \tag{4.3}$$

Proof. Die Restriktion von $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ auf $\{\pm 1\}$ ist bijektiv. Es reicht also, unsere Gleichung in $\mathbb{F}_p$ zu zeigen, wo sie aber nach (4.2) richig ist. □

Lemma 4.13. *Sei $k \subset K$ eine endliche Galoiserweiterung mit zyklischer Galoisgruppe G gerader Ordnung. Dann gibt es genau einen surjektiven Morphismus $\chi : G \to \{\pm 1\}$ von Gruppen, und es gelten:*

(a) Es gibt genau einen Zwischenkörper $k \subset Z \subset K$ mit $k \subset Z$ quadratisch (= vom Grad 2).

Gelte $\operatorname{char} k = 0$. *(Es reicht* $\operatorname{char} k \nmid \{2, \# \ker \chi\}$.*)*

(b) Es gilt $Z = k(\alpha)$ für ein und jedes von Null verschiedenen Element der Gestalt

$$\alpha = \alpha(x) = \sum_{g \in G} \chi(g) g(x) \quad \text{mit } x \in K.$$

(c) Für alle $g \in G$ und $\alpha = \alpha(x)$ wie oben gilt $g(\alpha) = \chi(g)\alpha$.

Proof. Die zyklische Gruppe gerader Ordnung G hat genau einen Normalteiler (/eine Untergruppe) H vom Index 2 (nämlich $n\mathbb{Z}/2n\mathbb{Z}$, falls $G \cong \mathbb{Z}/2n\mathbb{Z}$). Dies zeigt Existenz und Eindeutigkeit von χ.

Der Fixkörper K^H ist die gesuchte eindeutige quadratische Erweiterung von k.

Gelte $\operatorname{char} k = 0$.

Als quadratische Erweiterung ist $k \subset K^H$ normal, hat also die zweielementige Galoisgruppe G/H (und es gilt $G/H \xrightarrow[\sim]{\chi} \{\pm 1\}$).

Sei $x \in K$. Für $g' \in G$ gilt

$$\begin{aligned} g'(\alpha(x)) &= g'\big(\sum_{g \in G} \chi(g) g(x)\big) \\ &= \sum_{g \in G} \chi(g')\chi(g'g)(g'g)(x) \\ &= \chi(g')\alpha(x) \end{aligned}$$

Es folgt einerseits $\alpha(x) \in K^H$ und andererseits, dass das nichttriviale Element von G/H das Element $\alpha(x)$ auf $-\alpha(x)$ abbildet; insbesondere folgt $\alpha(x)^2 \in K^G = k$. Falls $\alpha(x) \neq 0$ gilt $\alpha(x) \notin k = K^G$ (denn $\operatorname{char} k \neq 2$) und somit $K^H = k(\alpha(x))$.

Es bleibt zu zeigen, dass es ein $x \in K$ gibt mit $\alpha(x) \neq 0$.[53] Sei $y \in K^H$ und $g \in G \setminus H$. Dann gilt

$$\begin{aligned} \alpha(y) &= \sum_{h \in H} \chi(h) h(y) + \sum_{h \in H} \chi(gh)(gh)(y) \\ &= \sum_{h \in H} h(y) - \sum_{h \in H} (gh)(y) \\ &= |H|(y - g(y)). \end{aligned}$$

[53] Alternativbeweis: $\sum_{g \in G} \chi(g) g : K^\times \to K$ ist nicht die Nullabbildung wegen der linearen Unabhängigkeit von Charakteren, Satz 2.70.

Für $y \in K^H \setminus k$ gilt $y \neq g(y)$. Wegen $\operatorname{char} k \nmid \#H$ ist in diesem Fall $\alpha(y) \neq 0$. □

Ende 24. Vorlesung Montag 9. Juli 2012.

Beweis von Satz 4.5. Sei p eine ungerade Primzahl. Wir betrachten den p-ten Kreisteilungskörper $\mathbb{Q}(\zeta_p)$, wobei $\zeta_p \in \overline{\mathbb{Q}}$ eine primitive p-te Einheitswurzel ist. Nach Satz 2.54 ist $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$ eine endliche Galois-Erweiterung mit Galoisgruppe $G \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{F}_p^\times$ (kanonischer Isomorphismus); letztere Gruppe ist zyklisch der geraden Ordnung $p-1$ nach Lemma 1.86.

Wir wenden Lemma 4.13 an (es ist χ die Verknüpfung $G \xrightarrow{\sim} \mathbb{F}_p^\times \xrightarrow{\left(\frac{?}{p}\right)} \{\pm 1\}$): Der eindeutige Zwischenkörper $\mathbb{Q} \subset Z \subset \mathbb{Q}(\zeta_p)$ mit $[Z : \mathbb{Q}] = 2$ wird erzeugt von dem Element

$$\alpha := \alpha(\zeta_p) = \sum_{g \in G} \chi(g) g(\zeta_p) = \sum_{a \in \mathbb{F}_p^\times} \Big(\frac{a}{p}\Big) \zeta_p^a \in \mathbb{Z}[\zeta_p],$$

denn dieses Element ist nicht Null: Die Elemente $1, \zeta_p, \dots, \zeta^{p-2}$ bilden eine $\mathbb{Q}$-Basis von $\mathbb{Q}(\zeta_p)$, und somit auch die Elemente $\zeta_p, \zeta_p^2, \dots, \zeta^{p-1}$ (als Bild unter dem $\mathbb{Q}$-linearen Endomorphismus $(\zeta_p \cdot)$ von $\mathbb{Q}(\zeta_p)$).

Wir behaupten

$$\alpha^2 = (-1)^{\frac{p-1}{2}} p \in \mathbb{Z}. \tag{4.4}$$

In der Tat berechnen wir (unter Verwendung von $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ und $\left(\frac{a'b^2}{p}\right) = \left(\frac{a'}{p}\right)\left(\frac{b^2}{p}\right) = \left(\frac{a'}{p}\right)$ für $b \notin p\mathbb{Z}$)

$$\begin{aligned}
\alpha^2 &= \sum_{b \in \mathbb{F}_p^\times} \sum_{a \in \mathbb{F}_p^\times} \Big(\frac{ab}{p}\Big) \zeta_p^{a+b} \\
\text{(Substitution } a = a'b) &= \sum_{b \in \mathbb{F}_p^\times} \sum_{a' \in \mathbb{F}_p^\times} \Big(\frac{a'b^2}{p}\Big) \zeta_p^{a'b+b} \\
&= \sum_{b \in \mathbb{F}_p^\times} \sum_{a' \in \mathbb{F}_p^\times} \Big(\frac{a'}{p}\Big) \zeta_p^{(a'+1)b} \\
&= \sum_{a' \in \mathbb{F}_p^\times} \Big[\Big(\frac{a'}{p}\Big) \sum_{b \in \mathbb{F}_p^\times} (\zeta_p^{a'+1})^b\Big]
\end{aligned}$$

Für $a' = -1$ ergibt sich als Summand $\left(\frac{-1}{p}\right)(p-1)$.

Für $a' \neq -1$ ist $\eta := \zeta_p^{a'+1}$ eine p-te Einheitswurzel $\neq 1$ und erfüllt somit die Gleichung

$$1 + \eta + \eta^2 + \cdots + \eta^{p-1} = 0.$$

(Da $a'+1$ teilerfremd zu p ist, ist η sogar eine primitive p-te Einheitswurzel. Es ist $\Phi_p = 1+X+X^2+\cdots+X^{p-1}$ das p-te Kreisteilungspolynom.) Damit ist der entsprechende Summand gerade $-\left(\frac{a'}{p}\right)$.

Also erhalten wir (die letzte Gleichheit folgt aus Korollar 4.12)

$$\begin{aligned}\alpha^2 &= \left(\frac{-1}{p}\right)(p-1) - \sum_{a'\in\mathbb{F}_p^\times; a'\neq -1}\left(\frac{a'}{p}\right)\\ &= \left(\frac{-1}{p}\right)(p-1) + \left(\frac{-1}{p}\right) - \underbrace{\sum_{a'\in\mathbb{F}_p^\times}\left(\frac{a'}{p}\right)}_{=0}\\ &= \left(\frac{-1}{p}\right)p\\ &= (-1)^{\frac{p-1}{2}}p,\end{aligned}$$

was genau die Behauptung (4.4) ist. Es besitzt also $(-1)^{\frac{p-1}{2}}p$ die Quadratwurzel α in $\mathbb{Z}[\zeta_p]$.

Sei q eine eine von p verschiedene ungerade Primzahl.

Aus (4.4) und Gleichung (4.2) in Lemma 4.11 erhalten wir folgt

$$a^{q-1} = (\alpha^2)^{\frac{q-1}{2}} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}p^{\frac{q-1}{2}} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right) \quad \text{in } \mathbb{F}_q. \tag{4.5}$$

Sei $R := \mathbb{Z}[\zeta_p]$. Beachte $\alpha \in R$. Wir arbeiten mit dem Diagramm

$$\begin{array}{ccccc}\mathbb{Q}(\zeta_p) & \supset & R & \twoheadrightarrow & R/qR\\ \cup & & \cup & & \cup\\ \mathbb{Q} & \supset & \mathbb{Z} & \twoheadrightarrow & \mathbb{F}_q\end{array}$$

und müssen die rechte Inklusion erklären: Es ist R ein freier $\mathbb{Z}$-Modul mit Basis $1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-2}$, denn diese Elemente erzeugen sicherlich R als $\mathbb{Z}$-Modul und sind $\mathbb{Z}$-linear unabhängig, denn sie sind $\mathbb{Q}$-linear unabhängig. Es folgt $qR \cap \mathbb{Z} = q\mathbb{Z}$, und dies erklärt die Inklusion auf der rechten Seite.

Sei $\sigma_q \in G$ dasjenige Element, das jede p-te Einheitswurzel auf ihre q-te Potenz abbildet, als $\sigma_q \mapsto \overline{q}$ unter $G \xrightarrow{\sim} \mathbb{F}_p^\times$. Lemma 4.13.(c) liefert

$$\sigma_q(\alpha) = \chi(\overline{q})\alpha = \left(\frac{q}{p}\right)\alpha \quad \text{in } R.$$

Der Automorphismus $\sigma_q : \mathbb{Q}(\zeta_p) \xrightarrow{\sim} \mathbb{Q}(\zeta_p)$ induziert einen Automorphismus $\sigma_q : R \xrightarrow{\sim} R$, $\sum c_i\zeta_p^i \mapsto \sum c_i\zeta_p^{qi}$. Dieser bildet das Ideal qR bijektiv in sich ab und induziert so einen Isomorphismus $\overline{\sigma}_q : R/qR \xrightarrow{\sim} R/qR$. Für jedes $c \in \mathbb{Z}$ gilt $c^q = c$ in $\mathbb{F}_q$, also $c^q - c \in q\mathbb{Z} \subset qR$. Also ist $\overline{\sigma}_q$ die Abbildung $x \mapsto x^q$. Es folgt

$$\left(\frac{q}{p}\right)\overline{\alpha} = \overline{\sigma_q(\alpha)} = \overline{\sigma}_q(\overline{\alpha}) = \overline{\alpha}^q \quad \text{in } R/qR. \tag{4.6}$$

Mit $\overline{p}$ is nach (4.4) auch $\overline{\alpha}$ eine Einheit in R/qR. Mit (4.5) liefert (4.6) also

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right)$$

in R/qR, ja sogar in $\mathbb{F}_q$ und sogar in $\mathbb{Z}$, denn beide Terme sind in $\{\pm 1\} \subset \mathbb{Z}$ und q ist ungerade. Multiplikation mit $\left(\frac{p}{q}\right)$ liefert unsere alternative Formulierung des quadratischen Reziprozitätsgesetzes in Bemerkung 4.9. □

Proposition 4.14 (2. Ergänzungssatz)**.** *Ist q eine ungerade Primzahl, so gilt (in $\mathbb{Z}$)*

$$\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}} = \begin{cases} 1 & \text{falls } q \equiv \pm 1 \mod 8, \\ -1 & \text{sonst (also falls } q \equiv \pm 3 \mod 8\text{).} \end{cases} \tag{4.7}$$

Proof. Für die zweite Gleichheit überlegt man sich dass $q \in \pm 1 + 8\mathbb{Z}$ zuerst $q^2 \in 1+16\mathbb{Z}$ und dann $\frac{q^2-1}{8}$ gerade impliziert, und dass $q \in \pm 3+8\mathbb{Z}$ zunächst $q^2 \in 9 + 16\mathbb{Z}$ und somit $\frac{q^2-1}{8}$ ungerade impliziert.

Es gilt $\Phi_8 = X^4 + 1$, siehe (2.22). Sei $\zeta = \zeta_8$ eine primitive 8-te Einheitswurzel. Insbesondere erhalten wir $\zeta^4 = -1$ und $\zeta^3 = -\zeta^{-1}$, $\zeta^2 = -\zeta^{-2}$ etc..

Wie im vorhergenden Beweis haben wir $\sigma_q \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/8\mathbb{Z})^\times$ (nur ist diese Gruppe nicht zyklisch).

Betrachte $\alpha := \zeta + \zeta^{-1}$. Dann gilt $\alpha^2 = \zeta^2 + 2 + \zeta^{-2} = 2$. Also ist α eine Wurzel aus 2 und somit nicht in $\mathbb{Q}$, und σ_q muss α auf $\pm\alpha$ schicken. Sei $\varepsilon_q \in \{\pm 1\}$ definiert durch $\sigma_q(\alpha) = \varepsilon_q \alpha$.

Analog wie im obigen Beweis sei $R = \mathbb{Z}(\zeta)$; beachte $\mathbb{Z} \cap qR = q\mathbb{Z}$. In R/qR erhalten wir

$$\varepsilon_q \alpha = \sigma_q(\alpha) = \zeta^q + \zeta^{-q} \equiv (\zeta + \zeta^{-1})^q = \alpha^q.$$

Wegen $\alpha^2 = 2$ ist α invertierbar in R/qR, so dass wir $\varepsilon_q = \alpha^{q-1} = (\alpha^2)^{\frac{q-1}{2}} = 2^{\frac{q-1}{2}}$ in R/qR erhalten, ja sogar in $\mathbb{Z}/q\mathbb{Z} = \mathbb{F}_q$. Mit Gleichung (4.2) in Lemma 4.11 erhalten wir

$$\varepsilon_q = \left(\frac{2}{q}\right) \quad \text{in } \mathbb{F}_q, \text{ ja sogar in } \mathbb{Z}.$$

Wir berechnen ε_q in beiden Fällen:

(a) Ist $q \equiv \pm 1 \mod 8$, so gilt $\sigma_q(\alpha) = \alpha$, also $\varepsilon_q = 1$.
(b) Ist $q \equiv \pm 3 \mod 8$, so gilt $\sigma_q(\alpha) = \zeta^3 + \zeta^{-3} = -\zeta^{-1} - \zeta^1 = -\alpha$, also $\varepsilon_q = -1$.

□

Solution 4.15. Lösung der Aufgabe 4.4.

Man prüft leicht, dass 109 eine Primzahl ist. Wir berechnen

$$\begin{aligned}
&\Big(\frac{94}{109}\Big)\\
\text{(Multiplikativität)} &= \Big(\frac{2}{109}\Big)\Big(\frac{47}{109}\Big)\\
\text{(2. Ergänzungssatz (4.7))} &= -\Big(\frac{47}{109}\Big)\\
\text{(Reziprozität (4.1))} &= -\Big(\frac{109}{47}\Big)\\
\text{(modulo 47)} &= -\Big(\frac{15}{47}\Big)\\
\text{(Multiplikativität)} &= -\Big(\frac{3}{47}\Big)\Big(\frac{5}{47}\Big)\\
\text{(Reziprozität (4.1))} &= +\Big(\frac{47}{3}\Big)\Big(\frac{47}{5}\Big)\\
\text{(modulo 3 bzw. 5)} &= \Big(\frac{-1}{3}\Big)\Big(\frac{2}{5}\Big)\\
\text{(1. Ergänzungssatz (4.3) oder direkt)} &= -\Big(\frac{2}{5}\Big)\\
\text{(2. Ergänzungssatz (4.7))} &= 1.
\end{aligned}$$

Also ist 94 ein quadratischer Rest modulo 109. Explizit gilt

$$51^2 = 2601 = 23 \cdot 109 + 94 = 94 \quad \text{in } \mathbb{F}_{109}.$$

Ende 25. und letzte Vorlesung Donnerstag 12. Juli 2012.

Literatur

[Bos] Siegfried Bosch, *Algebra*, Springer-Verlag.

[Bun92] Peter Bundschuh, *Einführung in die Zahlentheorie*, second ed., Springer-Lehrbuch. [Springer Textbook], Springer-Verlag, Berlin, 1992.

[FS78] Gerd Fischer and Reinhard Sacher, *Einführung in die Algebra*, B. G. Teubner, Stuttgart, 1978, Zweite überarbeitete Auflage, Teubner Studienbücher: Mathematik.

[Hil97] D. Hilbert, *Theory of algebraic number fields. (Die Theorie der algebraischen Zahlkörper.)*, Deutsche Math. Ver. **4** (1897), I–XVIII, 175–546 (German).

[Jan] Joachim Jantzen, Jens-Carsten und Schwermer, *Algebra*, Springer-Verlag.

[Lan52] Serge Lang, *On quasi algebraic closure*, Ann. of Math. (2) **55** (1952), 373–390.

[Lor92] Falko Lorenz, *Einführung in die Algebra. Teil I*, second ed., Bibliographisches Institut, Mannheim, 1992.

[Neu99] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

Mathematisches Institut, Universität Bonn, Endenicher Allee 60, 53115 Bonn, Germany

E-mail address: olaf.schnuerer@math.uni-bonn.de