Algebra – Zusammenfassung

Dr. Urs Hartl
WS 02/03

Einleitung: Auflösen von Polynomgleichungen

Der Name „Algebra“ ist arabischen Ursprungs und bedeutete „Rechnen mit Gleichungen und Lösen derselben“. In der Algebra interessiert man sich meist für polynomiale Gleichugen

$$(*) \qquad f(X) = a_nX^n + \ldots + a_1X + a_0 \;=\; 0\,, \qquad a_i \in K\,,\; a_n \neq 0\,.$$

Problem: Wieviele Lösungen besitzt $(*)$, in welchem Zahlenbereich liegen diese und wie lassen sie sich explizit aus den Koeffizienten berechnen?

Mit Vielfachheiten gezählt besitzt $(*)$ genau n Lösungen (Folgerung 3.5.2).

Fundamentalsatz der Algebra: Jedes Polynom mit komplexen Koeffizienten besitzt eine Nullstelle in den komplexen Zahlen.

Berechnung der Lösungen:

$n = 2$: Quadratische Ergänzung (Ende des 3. Jahrtausends v. Ch.),
$n = 3$: Cardano'sche Formeln (1515),
$n = 4$: Lösungsformel von Ferrari (1545).

Fazit: Die allgemeine Gleichung vom Grad $n \leq 4$ ist durch Radikale auflösbar.

Auflösbarkeit für $n \geq 5$:

Galois (1832): Kriterium für die Auflösbarkeit einer Gleichung mit Hilfe ihrer „Galois-Gruppe“

Galois-Theorie

Sei L/K ein Zerfällungskörper von f über K (Satz 3.4.6), dann enthält L „sämtliche“ Lösungen von $(*)$.

Untersuchung der Struktur von L/K mit Hilfe der Galois-Gruppe $\mathrm{Gal}(L/K) := \mathrm{Aut}_K(L)$

Die Zwischenkörper von L/K entsprechen eins zu eins den Untergruppen von $\mathrm{Gal}(L/K)$ (Satz 4.3.1).

Die Gleichung $(*)$ ist genau dann durch Radikale auflösbar, wenn die Gruppe $\mathrm{Gal}(L/K)$ auflösbar ist (Satz 4.7.4).

Abel, Ruffini (1826): Die allgemeine Gleichung n-ten Grades ist für $n \geq 5$ nicht durch Radikale auflösbar. (Satz 4.7.6)

Beweis: Die Galois-Gruppe des allgemeinen Polynoms n-ten Grades ist die symmetrische Gruppe S_n (Korollar 4.4.11). Die Gruppe S_n ist genau dann auflösbar, wenn $n \leq 4$ ist (Satz 1.9.6).

1 Elementare Gruppentheorie

1.1 Gruppen

1.2 Gruppenmorphismen

1.3 Untergruppen

Untergruppenkriterium, Links- und Rechtsnebenklassen,

Satz 1.3.10 (Satz von Lagrange)
Sei G eine Gruppe und $H < G$ eine Untergruppe. Dann gilt $\#G = [G : H] \, \#H$.

1.4 Normalteiler

Definition, Rechnen mit Nebenklassen, Faktorgruppe

1.5 Isomorphiesätze

Satz 1.5.1 (Homomorphiesatz)
Sei $\varphi : G \to G'$ ein Homomorphismus von Gruppen. Dann induziert φ einen Isomorphismus

$$\overline{\varphi} : G/\ker(\varphi) \longrightarrow \mathrm{im}(\varphi)$$

und φ faktorisiert als $\varphi = i \circ \overline{\varphi} \circ \rho$

$$G \xrightarrow{\rho} G/\ker\varphi \xrightarrow{\overline{\varphi}} \mathrm{im}(\varphi) \xrightarrow{i} G'$$

wobei ρ der kanonische Epimorphismus und i die Inklusionsabbildung der Untergruppe $\mathrm{im}(\varphi)$ von G' ist.

Erster und zweiter Isomorphiesatz

1.6 Zyklische Gruppen C_n, C_∞

Satz 1.6.4 (Klassifikation der zyklischen Gruppen)
Sei $G = \langle g \rangle$ eine zyklische Gruppe. Dann ist G kommutativ. Genauer gilt mit $n = \#G$

1. Ist $n = \infty$, so ist $\varphi : \mathbb{Z} \to G, m \mapsto g^m$ ein Isomorphismus.

2. Ist $n < \infty$, so ist $\overline{\varphi} : \mathbb{Z}/n\mathbb{Z} \to G, \overline{m} \mapsto g^m$ wohldefiniert und ein Isomorphismus.

Untergruppen von zyklischen Gruppen, Kriterium für zyklische Gruppen

1.7 Permutationsgruppen S_n, A_n

Zyklen, Transpositionen, Signum

1.8 Endlich erzeugte, abelsche Gruppen

Satz 1.8.7 (Elementarteilersatz)
Sei G eine endlich erzeugte, freie, abelsche Gruppe und $G' < G$ eine Untergruppe. Dann existiert eine Basis $\{x_1, \ldots, x_r\}$ von G und Zahlen $m_1, \ldots, m_r \in \mathbb{N}_0$ mit $m_1|m_2, \ldots, m_{r-1}|m_r$, so dass G' die von $\{m_1x_1, \ldots, m_rx_r\}$ erzeugte freie, abelsche Gruppe ist.

Satz 1.8.9 (Hauptsatz über endlich erzeugte, abelsche Gruppen)
Sei G eine endlich erzeugte, abelsche Gruppe und $T(G)$ ihre Torsionsuntergruppe. Dann gilt

1. $G \cong T(G) \times G/T(G)$,
2. $G/T(G) \cong {C_\infty}^r$,
3. $T(G) \cong C_{m_1} \times \ldots \times C_{m_s}$ mit $m_i \in \mathbb{Z}, m_i \geq 2$ und $m_1|m_2, \ldots, m_{s-1}|m_s$.

Der Rang r und die Zahlen $m_1, \ldots, m_s$ sind eindeutig bestimmt.

1.9 Auflösbare Gruppen

Kommutatoruntergruppe, Normalreihe

Satz 1.9.6
Die symmetrische Gruppe S_n und die alternierende Gruppe A_n sind genau dann auflösbar, wenn $n \leq 4$ ist.

Übertragung von Auflösbarkeit auf (und von) Untergruppen und Faktorgruppen

1.10 Operationen von Gruppen auf Mengen

Definition, Bahn, Stabilisatoruntergruppe, Fixpunkt

Satz 1.10.4 (Bahnengleichung)
Sei $G \times X \to X$ eine Operation der Gruppe G auf der endlichen Menge X und seien $G.x_1, \ldots, G.x_r$ die Bahnen. Dann gilt

$$\#X = \sum_{i=1}^{r} [G : G_{x_i}]$$

1.11 Sylowsätze

p-Gruppe, p-Sylowuntergruppe

Satz 1.11.2 (Erster Sylow'scher Satz)
Jede endliche Gruppe besitzt eine p-Sylowuntergruppe.

Satz 1.11.4 (Zweiter Sylow'scher Satz)
Je zwei p-Sylowuntergruppen einer endlichen Gruppe sind konjugiert.

Satz 1.11.5 (Dritter Sylow'scher Satz)
Die Anzahl der p-Sylowuntergruppen einer endlichen Gruppe G teilt $\#G$ und ist kongruent zu 1 modulo p.

2 Ringe und Polynome

2.1 Grundbegriffe

2.2 Ringmorphismen und Ideale

Ideale, Faktorring, Homomorphisatz,

Satz 2.2.12 (Chinesischer Restsatz)
Seien R ein kommutativer Ring und $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subset$ Ideale mit $\mathfrak{a}_i + \mathfrak{a}_j = R$ für alle $i \neq j$. Dann gilt $\mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n$ und

$$R/(\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n) \cong R/\mathfrak{a}_1 \times \ldots \times R/\mathfrak{a}_n \,.$$

2.3 Integritätsbereich und Quotientenkörper

Satz 2.3.4 (Existenz des Quotientenkörpers)
Sei R ein Integritätsbereich. Dann existiert ein Körper Q und ein injektiver Ringhomomorphismus $i : R \to Q$, so dass sich jedes $x \in Q$ in der Form $x = i(a)/i(b)$ mit $a, b \in R, b \neq 0$ schreiben lässt.

2.4 Der Polynomring

Satz 2.4.3 (Existenz und universelle Eigenschaft des Polynomrings)
Sei R ein kommutativer Ring. Dann existiert ein Polynomring über R in einer Unbestimmten X. Dieser besteht aus einem Oberring $R[X] \supset R$ und einem ausgezeichneten Element $X \in R[X]$ und erfüllt die folgende universelle Eigenschaft:

$\forall\, \varphi : R \to S$ Ringhomomorphismus mit S kommutativ, $\forall\, x \in S$
$\exists!\, \Phi : R[X] \to S$ eindeutig bestimmter Ringhomomorphismus mit $\Phi|_R = \varphi$ und $\Phi(X) = x$.

$$\begin{tikzcd}
R \arrow[r, hook] \arrow[dr, "\varphi"'] & R[X] \arrow[d, dashed, "\exists!\,\Phi"] & \ni X \arrow[d, mapsto] \\
& S & \ni x
\end{tikzcd}$$

Division mit Rest, euklidische Ringe

Satz 2.4.13 (Anzahl der Nullstellen)
Sei R ein Integritätsbereich und $f \in R[X]$. Dann hat f höchstens $\deg(f)$ verschiedene Nullstellen in R.

2.5 Hauptideale, Primideale, maximale Ideale

Satz 2.5.2
Jeder euklidische Ring ist ein Hauptidealring.

Satz 2.5.8
Sei R ein kommutativer Ring. Genau dann ist $R[X]$ ein Hauptidealring, wenn R ein Körper ist.

2.6 Teilbarkeit in Integritätsringen

Größter gemeinsamer Teiler, faktorielle Ringe, Primelemente, irreduzible Elemente

Satz 2.6.7 (Euklidischer Algorithmus)
Sei R ein euklidischer Ring mit Größenfunktion $\delta : R \setminus \{0\} \to \mathbb{N}_0$. Seien $a_1, a_2 \in R$ mit $\delta(a_1) \geq \delta(a_2)$. Für $i \geq 3$ sei $a_i \in R$ rekursiv definiert durch

$$a_{i-2} = q_i\, a_{i-1} + a_i \qquad \text{mit} \quad a_i = 0 \text{ oder } \delta(a_i) < \delta(a_{i-1})\,.$$

Dann existiert ein $m \in \mathbb{N}$ mit $a_{m+1} = 0, a_m \neq 0$. Es ist a_m ein ggT von a_1 und a_2 in R. Setzt man $b_1 = 1 = c_2, b_2 = 0 = c_1, b_i = b_{i-2} - q_i\, b_{i-1}$ und $c_i = c_{i-2} - q_i\, c_{i-1}$, so gilt $a_m = b_m\, a_1 + c_m\, a_2$.

Satz 2.6.13
Jeder Hauptidealring ist faktoriell.

2.7 Polynomringe über faktoriellen Ringen

Satz 2.7.8 (Gauß)
Der Polynomring über einem faktoriellen Ring ist wieder faktoriell.

2.8 Irreduzibilität von Polynomen

Eisenstein'sches Irreduzibilitätskriterium, Reduktionskriterium

3 Algebraische Körpererweiterungen

3.1 Grundbegriffe

Grad einer Körpererweiterung, Charakteristik eines Körpers

Satz 3.1.4 (Gradsatz)
Ist $M/L/K$ ein Körperturm, so gilt $[M:K] = [M:L] \cdot [L:K]$.

3.2 Endliche und algebraische Körpererweiterungen

algebraische und transzendente Elemente einer Körpererweiterung, Minimalpolynom

Satz 3.2.10
Endlichkeit ist eine ausgezeichnete Eigenschaft von Körperweiterungen, d.h. ist L/K eine Körpererweiterung und sind E und F Zwischenkörper von L/K, so gilt:

1. Ist $F \subset E$, so ist E/K endlich genau dann, wenn E/F und F/K endlich sind.

2. Ist E/K endlich, so ist auch EF/F endlich.

3. Sind E/K und F/K endlich, so ist auch EF/K endlich.

Satz 3.2.13
Algebraizität ist eine ausgezeichnete Eigenschaft von Körperweiterungen.

3.3 Der algebraische Abschluss

Satz 3.3.1 (Verfahren von Kronecker)
Sei K ein Körper, $f \in K[X]$, $\deg(f) \geq 1$. Dann gibt es eine algebraische Körpererweiterung L/K und eine Nullstelle $\alpha \in L$ von f.

Satz 3.3.8
Jeder Körper besitzt einen algebraischen Abschluss.

3.4 Zerfällungskörper, normale Erweiterungen

Satz 3.4.6 (Existenz von Zerfällungskörpern)
Sei K ein Körper und $\mathcal{F}$ eine Familie von nicht-konstanten Polynomen aus $K[X]$. Dann existiert ein Zerfällungskörper von $\mathcal{F}$ über K.

Satz 3.4.8 (Charakterisierung normaler Erweiterungen)
Sei L/K eine algebraische Körpererweiterung. Dann sind die folgenden Aussagen äquivalent:

1. L/K ist normal,

2. L/K ist Zerfällungskörper einer Familie von nicht-konstanten Polynomen aus $K[X]$,

3. Jeder K-Homomorphismus $\varphi : L \to \overline{L}$ in einen algebraischen Abschluss $\overline{L}$ von L ist ein K-Automorphismus von L.

Konstruktionsverfahren für $\mathrm{Aut}_K(L)$ für eine endliche, normale Körpererweiterung L/K

3.5 Separable Körpererweiterungen

Separabilitätsgrad einer Körperweiterung, Gradsatz für den Separabilitätsgrad

Satz 3.5.11
Separabilität ist eine ausgezeichnete Eigenschaft von Körperweiterungen.

Satz 3.5.12 (Satz vom primitiven Element)
Jede endliche separable Körpererweiterung L/K ist einfach, d.h. es existiert ein primitives Element $\delta \in L$ mit $L = K(\delta)$.

Formale Differentiation von Polynomen zur Charakterisierung mehrfacher Nullstellen

Satz 3.5.20
Jeder Körper der Charakteristik 0 ist perfekt, d.h. jede seiner algebraischen Körpererweiterungen ist separabel.

Satz 3.5.22
Jeder endliche Körper ist perfekt.

3.6 Endliche Körper

Satz 3.6.1
Ist K ein endlicher Körper, so ist $q := \#K$ eine Potenz der Charakteristik von K und die Elemente von K sind genau die Nullstellen des separablen Polynoms $X^q - X$.

Satz 3.6.2
Zu jeder Primzahlpotenz q existiert ein endlicher Körper mit q Elementen. Je zwei solche sind isomorph. (Bezeichnung $\mathbb{F}_q$)

Satz 3.6.5
Sei q eine Primzahlpotenz und $d \in \mathbb{N}$. Dann ist

$$\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{F}_{q^d}) = \{\, (\mathrm{Frob}_q)^\nu : \nu = 0, \dots, d-1\}$$

zyklisch von der Ordnung d mit kanonischem Erzeuger $\mathrm{Frob}_q : \alpha \mapsto \alpha^q$.

4 Galois-Theorie

4.1 Motivation

4.2 Galois-Erweiterungen

Def 4.2.3 Eine algebraische Körpererweiterung heißt galoissch, falls sie normal und separabel ist.

Satz 4.2.4 (Charakterisierung von galoisschen Erweiterungen)
Sei L/K eine Körpererweiterung. Dann sind folgende Aussagen äquivalent:

1. L/K ist galoissch,
2. L ist Zerfällungskörper einer Familie separabler Polynome über K,
3. $L^{\mathrm{Gal}(L/K)} = K$.

Ist L/K endlich, so sind 1. – 3. zusätzlich äquivalent zu

4. $\#\,\mathrm{Gal}(L/K) = [L : K]$.

4.3 Der Hauptsatz der Galois-Theorie

Satz 4.3.1 (Hauptsatz der Galois-Theorie)
Sei L/K eine endliche, galoissche Körpererweiterung mit $G = \mathrm{Gal}(L/K)$. Dann sind die Zuordnungen

$$\begin{array}{rcl} \{\, E : \text{ Zwischenkörper von } L/K \,\} & \longleftrightarrow & \{\, H : \text{ Untergruppen von } G \,\} \\ E & \longmapsto & \mathrm{Gal}(L/E) \\ L^H & \longleftarrow\!\shortmid & H \end{array}$$

bijektiv und invers zueinander. L ist galoissch über L^H mit Galois-Gruppe H. Es ist L^H normal und damit galoissch über K genau dann, wenn H Normalteiler in G ist. In diesem Fall gilt $\mathrm{Gal}(L^H/K) = G/H$.

Translationssatz, Galois-Gruppe des Kompositums

4.4 Die Galois-Gruppe einer Gleichung – Beispiele

Operation der Galois-Gruppe auf den Nullstellen der Gleichung
Berechnung des Fixkörpers
Die allgemeine Gleichung n-ten Grades, elementar-symmetrische Polynome

Korollar 4.4.11 Seien $T_1, \ldots, T_n$ Unbestimmte über einem Körper K. Dann ist das allgemeine Polynom n-ten Grades

$$p(X) := X^n + T_1 X^{n-1} + \ldots + T_{n-1} X + T_n \quad \in \quad K[T_1, \ldots, T_n][X]$$

separabel und irreduzibel in $K(T_1, \ldots, T_n)[X]$. Ist L Zerfällungskörper von p über $K(T_1, \ldots, T_n)$, so ist $\mathrm{Gal}\big(L/K(T_1, \ldots, T_n)\big) = S_n$.

4.5 Einheitswurzeln und Kreisteilungskörper

Satz 4.5.8 Sei K ein Körper und $n \in \mathbb{N}$ mit $\mathrm{char}(K) \nmid n$. Sei $\zeta \in \mu_n(\overline{K})$ eine primitive n-te Einheitswurzel. Dann ist $K(\zeta)$ Zerfällungskörper des separablen Polynoms $X^n - 1$ über K. Es ist $K(\zeta)/K$ galoissch und es gibt einen injektiven Gruppenhomomorphismus

$$\mathrm{Gal}\big(K(\zeta)/K\big) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times, \quad \sigma \mapsto m(\sigma)$$

mit $\sigma(\zeta) = \zeta^{m(\sigma)}$. Insbesondere ist $K(\zeta)/K$ endlich, abelsch und $[K(\zeta)/K]$ teilt $\varphi(n)$.

Kreisteilungspolynom, Irreduzibilität über $\mathbb{Q}$

4.6 Zyklische Körpererweiterungen

Norm- und Spurabbildung von Körpererweiterungen
Unabhängigkeit von Charakteren
Hilbert 90

Satz 4.6.11 (Kummer-Erweiterungen)
Sei K ein Körper, $n \in \mathbb{N}$ mit $\mathrm{char}(K) \nmid n$. Es existiere eine primitive n-te Einheitswurzel $\zeta \in K$. Dann gilt:

1. Ist L/K eine zyklische Körperweiterung vom Grad n, so existiert ein $\alpha \in L$ mit $L = K(\alpha)$ und $a := \alpha^n \in K$, sowie $m_{\alpha/K} = X^n - a$.

2. Ist $a \in K$ und $\alpha \in \overline{K}$ eine Nullstelle von $X^n - a$, so ist $K(\alpha)/K$ zyklisch vom Grad d mit $d|n$. Es ist $c := \alpha^d \in K$ und $m_{\alpha/K} = X^d - c$.

Satz 4.6.13 (Artin-Schreier-Erweiterungen)
Sei K ein Körper mit $\mathrm{char}(K) = p > 0$. Dann gilt:

1. Ist L/K zyklisch vom Grad p, so existiert ein $\alpha \in L$ mit $L = K(\alpha)$ und $a := \alpha^p - \alpha \in K$, sowie $m_{\alpha/K} = X^p - X - a$.

2. Ist $a \in K$ und $f = X^p - X - a$, so gilt: Entweder f zerfällt in $K[X]$ vollständig in Linearfaktoren, oder f ist irreduzibel in $K[X]$ und für jede Nullstelle $\alpha \in \overline{K}$ von f ist $K(\alpha)/K$ Zerfällungskörper von f und zyklische Galois-Erweiterung vom Grad p mit $\mathrm{Gal}\big(K(\alpha)/K\big) = \langle\sigma\rangle$, wobei $\sigma : \alpha \mapsto \alpha + 1$ ist.

4.7 Auflösbarkeit durch Radikale

Satz 4.7.4 (Galois)
Für eine Körperweiterung L/K sind äquivalent:

1. L/K ist durch Radikale auflösbar,

2. L/K ist endlich, separabel und die normale Hülle N von L/K ist auflösbar über K, d.h. $\mathrm{Gal}(N/K)$ ist eine auflösbare Gruppe.

Satz 4.7.6 (Abel, Rufini)
Die allgemeine Gleichung n-ten Grades ist für $n \geq 5$ nicht durch Radikale auflösbar.

4.8 Konstruktionen mit Zirkel und Lineal

Satz 4.8.5 (Unlösbarkeit der Konstruktionsprobleme der Antike)
Die drei Konstruktionsprobleme der Antike

Quadratur des Kreises: Konstruiere zu einem gegebenen Kreis ein flächengleiches Quadrat

Dreiteilung des Winkels: Zerlege einen Winkel in drei gleiche Teile

Verdoppelung des Würfels: Konstruiere zu einem gegebenen Würfel einen Würfel des doppelten Volumens

sind mit Zirkel und Lineal unlösbar.

Satz 4.8.6 (Konstruktion des regulären n-Ecks, Gauß)
Sei $n \in \mathbb{N}$ mit $n \geq 3$. Das reguläre n-Eck lässt sich genau dann mit Zirkel und Lineal konstruieren, wenn $\varphi(n)$ (Euler'sche φ-Funktion) eine Potenz von 2 ist.