§6. Gleichungen 2. und 3. Grades

(siehe weiter)

Quadratische Gleichungen

(1) K Körper, char $K \neq 2$. Betrachte

(Q) $\qquad x^2 + ax + b = 0 \quad , \quad a, b \in K$

(2) Quadratische Ergänzung

$$
\begin{aligned}
(Q) \qquad x^2 + ax + \frac{a^2}{4} - \frac{a^2}{4} + b &= 0 \\
\left(x + \frac{a}{2}\right)^2 - \frac{a^2}{4} + b &= 0 \\
\left(x + \frac{a}{2}\right)^2 &= \frac{1}{4} D
\end{aligned}
$$

Def 1 $\qquad D = a^2 - 4b \qquad$ Diskriminante von (Q)

Lösungsformel: $\quad x_{1,2} = -\frac{a}{2} \pm \frac{1}{2}\sqrt{D}$

(3) „Tschirnhaus-Transformation"

Setze in (Q): $\qquad y = x + \frac{a}{2}$.

$$
\begin{aligned}
(Q') \qquad \left(y - \frac{a}{2}\right)^2 + a\left(y - \frac{a}{2}\right) + b &= 0 \\
y^2 + \frac{a^2}{4} - \frac{a^2}{2} + b &= 0 \\
y^2 - \frac{1}{4} D &= 0 \\
y_{1,2} &= \pm\frac{1}{2}\sqrt{D}
\end{aligned}
$$

(4) Führe die Nullstellen x_1, x_2 von (Q) ein. Dann:

(Q) $\qquad x^2 + ax + b = (x - x_1)(x - x_2)$

Koeffizientenvergleich

(V) $$x_1 + x_2 = -a$$
$$x_1 x_2 = b$$

Satz 1. $(x_1 - x_2)^2 = D$ $\left(\rightsquigarrow D = 0 \Leftrightarrow x_1 = x_2 \right)$

Beweis. Unter der Vertauschung $x_1 \leftrightarrow x_2$ bleibt die linke Seite invariant, also $\in K$. Ferner

$$(x_1 - x_2)^2 = x_1^2 - 2x_1 x_2 + x_2^2$$
$$= (x_1 + x_2)^2 - 4 x_1 x_2$$
$$= a^2 - 4b$$

Aus (V) und Satz 1 $\rightsquigarrow$ Lösungsformel.

Bezeichnungen: $(1, x) = x_1 + x_2$
$(-1, x) = x_1 - x_2$
„Lagrangesche Resolvente"
$$\delta = \sqrt{D} \quad (= x_1 - x_2)$$

⑤ E Zerfällungskörper von $f(x)$. Also
$E = K \Leftrightarrow \delta \in K \Leftrightarrow x_1$ und $x_2 \in K$
oder
$E = K(x_1) = K(x_2) = K(\delta)$, $[E:K] = 2$,
$\mathrm{Gal}(E, K) = S_2 = \{ id, \sigma \}$.
$\sigma x_1 = x_2 \quad \sigma x_2 = x_1, \quad \sigma\delta = -\delta$

Kubische Gleichungen

① (K) $x^3 + ax^2 + bx + c = 0$, $a, b, c \in K$
$\mathrm{char}\, K \neq 2, 3$

② Tschirnhaus - Transformation

$x' = x + \frac{a}{3}$

$(x' - \frac{a}{3})^3 + a(x' - \frac{a}{3})^2 + b(x' - \frac{a}{3}) + c = 0$
$x'^3 - ax'^2 + \dots + ax'^2 + \dots = 0$

Mit neuen Koeffizienten a', b' wird aus (K)

(K') $x'^3 + a'x' + b' = 0$

Ist x' eine Lösung von (K'), so löst $x = x' - \frac{a}{3}$ die Gleichung (K). Es reicht also, (K') zu untersuchen: ~~~~ der Zerfällungskörper von f ist der von f', wenn (K): $f(x) = 0$; (K') $= f'(x') = 0$.

③ Wir schreiben wieder K für K', alle Striche fallen weg:

(K): $f(x) = x^3 + ax + b = 0$; $a, b \in K$.

(4) Wir nehmen (K) als irreduzibel über K an, x_1, x_2, x_3 seien die 3 Nullstellen in einem Zerfällungskörper E von f.

Für jedes x_j gilt

$$[K(x_j):K]=3, \qquad K(x_j) \subset E.$$

Also $\quad K \subset K(x_j) \subset E = K(x_1, x_2, x_3)$

(O.E. $j=1$.) Man hat – Koeffizientenvergleich –

$$(V) \qquad \begin{aligned} x_1 + x_2 + x_3 &= 0 \\ x_1 x_2 + x_2 x_3 + x_3 x_1 &= a \\ x_1 x_2 x_3 &= -b \end{aligned}$$

Also ist $\quad E = K(x_1, x_2) \quad$ (oder x_1, x_3; x_2, x_3)

Fall 1 $\quad E = K(x_1)$.

Dann ist $\quad [E:K]=3$, $\mathrm{Gal}(E|K) = C_3$, notwendig x_2 ein Polynom in x_1. ~~Fall tritt insbesondere ein, wenn Nullstellen zusammenfallen.~~

Fall 2 $\quad K(x_1) \neq E$. Dann

$$f(x) = (x-x_1)(x-x_2)(x-x_3) = (x-x_1)\,g(x)$$

also $x_2, x_3 \notin K(x_1)$, aber $g(x)$ Polynom vom Grad 2 über $K(x_1)$, damit

$$[E : K(x_1)] = 2,$$
$$\mathrm{Gal}(E|K(x_1)) = C_2$$
$$[E:K] = 6$$

Nun operiert $\mathrm{Gal}(E|K)$ treu auf $\{x_1, x_2, x_3\}$, also ist (wegen $\operatorname{ord} G.. = 6$):

$$\mathrm{Gal}(E|K) = S_3$$

Zurück zu Fall 1. $\mathrm{Gal}(E|K) \subset S_3$, also wegen $\operatorname{ord} = 3$:

$$\mathrm{Gal}(E|K) = A_3 .$$

(5) Bestimmung der Zwischenkörper

Fall 1 Es gibt keine, da A_3 keine echten Untergruppen hat.

Fall 2 S_3 hat 4 echte Untergruppen: A_3, ferner 3 zyklische C_2, konjugiert, mit $\mathrm{Fix}(x_j)$, $j = 1, 2, 3$. Die Fixkörper der C_2 sind genau $K(x_j)$, untereinander isomorph. Was ist $\mathrm{Fix}\, A_3$? $Z \overset{\mathrm{Def}}{=} \mathrm{Fix}\, A_3 \Rightarrow [Z:K] = 2$.

$$\mathrm{Gal}(E/Z) = A_3$$

(6) Die Diskriminante

Betrachte
$$\delta = (x_1-x_2)(x_2-x_3)(x_3-x_1) \quad \in E.$$
Unter A_3 bleibt δ fest, d.h. $\delta \in Z$.

Fall 1. $\delta \in K$. Dann kann $Gal(E|K)$ keine ungeraden Permutationen enthalten ($\delta \mapsto -\delta$), also $Gal(E|K) = A_3$, wir sind im vorigen Fall 1. Also

Fall 2 $\delta \notin K$. Damit aber

$D = \delta^2 \in K$, da D unter allen Permutationen fest bleibt. Es folgt

$$[Z:K] = [K(\delta):K] = 2, \text{ also}$$

$$Z = K(\delta)$$
$$Gal(Z|K) = C_2 = S_3/A_3.$$

Def 2 D Diskriminante von f.

Also: $D = (x_1-x_2)^2(x_2-x_3)^2(x_3-x_1)^2 \quad \in K$

Genau dann, wenn D ein Quadrat in K ist, ist $[E:K] = 3$. (Insbesondere, wenn $D=0$ gilt).

Zur Berechnung benutze (V) und

Satz 2 (Redei) $D = -f'(x_1)f'(x_2)f'(x_3)$

Also: $$D = -(3x_1^2+a)(3x_2^2+a)(3x_3^2+a)$$
$$= -\left(27x_1^2x_2^2x_3^2 + 9a(x_1^2x_2^2+x_1^2x_3^2+x_2^2x_3^2) + 3a^2(x_1^2+x_2^2+x_3^2)+a^3\right)$$

Nun ist wegen $x_1+x_2+x_3 = 0$:
$$x_1^2+x_2^2+x_3^2 = -2(x_1x_2+x_1x_3+x_2x_3) = -2a$$
$$x_1^2x_2^2+x_1^2x_3^2+x_2^2x_3^2 = (x_1x_2+x_1x_3+x_2x_3)^2 = a^2$$

Schließlich $x_1^2x_2^2x_3^2 = b^2$. Damit

$$D = -(27b^2+9a^3-6a^3+a^3)$$
$$= -27b^2-4a^3$$

Satz 3 $-D = 4a^3+27b^2$

⑦ Cardanosche Formeln

Wir nehmen an, daß K die 3-ten Einheitswurzeln enthält: $1, \zeta, \zeta^2$. Notiere

(EW) $1+\zeta+\zeta^2 = 0$.

Man hat $[E : K(\delta)] = 3$, also sei σ ein Erzeugendes von $\mathrm{Gal}(E|K(\delta))$.
Wir numerieren: $\sigma x_1 = x_2$, $\sigma x_2 = x_3$.
Betrachte

$$
\begin{aligned}
&(1, x) = x_1 + x_2 + x_3 = 0\\
(L)\quad &(\zeta, x) = x_1 + \zeta x_2 + \zeta^2 x_3\\
&(\zeta^2, x) = x_1 + \zeta^2 x_2 + \zeta x_3,
\end{aligned}
$$

die Lagrangeschen Resolventen. Es ist

$$(\zeta, x)^3 = (x_1 + \zeta x_2 + \zeta^2 x_3)(\zeta x_1 + \zeta^2 x_2 + x_3)(\zeta^2 x_1 + \zeta x_2 + x_3)$$

invariant unter $\mathrm{Gal}(E|K(\delta))$, also $\in K(\delta)$.
Ebenso $(\zeta^2, x)^3$.

Wir lösen (L) nach x_1, x_2, x_3 auf.
Addiere und beachte (EW), wobei (L) mit ζ bzw. ζ^2 multipliziert wird.

$$
\begin{aligned}
&3x_1 = (\zeta, x) + (\zeta^2, x)\\
(C_1)\quad &3x_2 = \zeta^2(\zeta, x) + \zeta(\zeta^2, x)\\
&3x_3 = \zeta(\zeta, x) + \zeta^2(\zeta^2, x)
\end{aligned}
$$

Es bleibt die Berechnung der 3-ten Potenzen der Resolventen mittels a und b

$$
\begin{aligned}
(\zeta_1 x)^3 &= (x_1 + \zeta x_2 + \zeta^2 x_3)^3 \\
&= x_1^3 + x_2^3 + x_3^3 && A \\
&\quad + 3\zeta(x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1) && + 3\zeta B \\
&\quad + 3\zeta^2 (x_1 x_2^2 + x_2 x_3^2 + x_3 x_1^2) && + 3\zeta^2 C \\
&\quad + 6 x_1 x_2 x_3 && + 6F
\end{aligned}
$$

Nun

$$
\begin{aligned}
\delta &= (x_1 - x_2)(x_2 - x_3)(x_3 - x_1) \\
&= (x_1 x_2 - x_1 x_3 - x_2^2 + x_2 x_3)(x_3 - x_1) \\
&= x_1 x_2 x_3 - x_1^2 x_2 - x_1 x_3^2 + x_1^2 x_3 - x_2^2 x_3 + x_2^2 x_1 + x_2 x_3^2 \\
&\qquad - x_2 x_3 x_1 \\
&= -B + C
\end{aligned}
$$

Benutze (V):

$$
\begin{aligned}
0 &= (x_1 + x_2 + x_3)^3 && R \\
&= x_1^3 + x_2^3 + x_3^3 && A \\
&\quad + 3(x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1) && + 3B \\
&\quad + 3(x_1 x_2^2 + x_2 x_3^2 + x_3 x_1^2) && + 3C \\
&\quad + 6 x_1 x_2 x_3 && + 6F
\end{aligned}
$$

$$
\begin{aligned}
0 &= (x_1 + x_2 + x_3)(x_1 x_2 + x_2 x_3 + x_3 x_1) \\
&= x_1^2 x_2 + x_1 x_2 x_3 + x_1^2 x_3 \\
&\quad + x_1 x_2^2 + x_3 x_2^2 + x_1 x_2 x_3 \\
&\quad + x_1 x_2 x_3 + x_3^2 x_2 + x_3^2 x_1 \\
&= B + C + 3F
\end{aligned}
$$

$$
\begin{array}{lrcl}
(\mathrm{I}) & (\zeta,x)^3 & = & A + 3\zeta B + 3\zeta^2 C + 6F \\
(\mathrm{II}) & \delta & = & -B + C \\
(\mathrm{III}) & 0 & = & A + 3B + 3C + 6F \\
(\mathrm{IV}) & 0 & = & B + C + 3F
\end{array}
$$

Ferner:
$$\zeta = -\tfrac{1}{2} + \tfrac{1}{2}\sqrt{-3}$$
$$\zeta^2 = -\tfrac{1}{2} - \tfrac{1}{2}\sqrt{-3}$$

(I) − (III) liefert

$$
\begin{aligned}
(\zeta,x)^3 &= 3(\zeta-1)B + 3(\zeta^2-1)C \\
&= \left(-\tfrac{3}{2} + \tfrac{3}{2}\sqrt{-3} - 3\right)B + \left(-\tfrac{3}{2} - \tfrac{3}{2}\sqrt{-3} - 3\right)C \\
&= -\tfrac{9}{2}(B+C) + \tfrac{3}{2}\sqrt{-3}\,(B-C)
\end{aligned}
$$

(nach II, IV, V):

$$
\begin{aligned}
&= \tfrac{27}{2}F - \tfrac{3}{2}\sqrt{-3}\,\delta \\
&= -\tfrac{27}{2}b - \tfrac{3}{2}\sqrt{-3}\,\delta
\end{aligned}
$$

Entsprechend (nach Vertauschen von ζ und ζ^2):

$$(\zeta^2,x)^3 = -\tfrac{27}{2}b + \tfrac{3}{2}\sqrt{-3}\,\delta$$

Notiere noch:

$$
\begin{aligned}
(\zeta,x)(\zeta^2,x) \\
&= (x_1+\zeta x_2+\zeta^2 x_3)(x_1+\zeta^2 x_2+\zeta x_3) \\
&= x_1^2+x_2^2+x_3^2 + \underbrace{(\zeta+\zeta^2)}_{-1}(x_1x_2+x_2x_3+x_3x_1)
\end{aligned}
$$

= (siehe Beweis zu Satz 3)

$$-2a - a$$

$$= -3a$$

⑧ Zusammenfassung

$$
\begin{aligned}
3x_1 &= (\zeta,x) + (\zeta^2,x) \\
3x_2 &= \zeta^2(\zeta,x) + \zeta(\zeta^2,x) \\
3x_3 &= \zeta(\zeta,x) + \zeta^2(\zeta^2,x)
\end{aligned}
$$

$$
\begin{aligned}
(\zeta,x)^3 &= -27/2\, b - \tfrac{3}{2}\sqrt{-3}\,\delta \\
(\zeta^2,x)^3 &= -27/2\, b + \tfrac{3}{2}\sqrt{-3}\,\delta
\end{aligned}
$$

$$\delta^2 = -4a^3 - 27b^2$$

$$(\zeta,x)(\zeta^2,x) = -3a$$

Etwas mehrdeutig klassische Cardanische Formeln

$$
\begin{aligned}
3x_{1,2,3} = &\sqrt[3]{-\frac{27}{2}b+\frac{3}{2}\sqrt{-3}\sqrt{-4a^3-27b^2}} \\
&+ \sqrt[3]{-\frac{27}{2}b-\frac{3}{2}\sqrt{-3}\sqrt{-4a^3-27b^2}}
\end{aligned}
$$

(9) Eine allgemeine Bemerkung für beliebiges n

K Körper, char $K \neq 2$, $\mathcal{G} = \mathrm{Gal}(E|K)$,
E Zerfällungskörper des (separablen) Polynoms
f vom Grad n ist. Dann kann
$\mathcal{G}$ als Untergruppe von S_n (Permutationen der $x_1, \ldots, x_n$, Wurzeln von f) aufgefaßt werden. Es sei

$$D = \mathrm{diskr}\, f = \prod_{i<j} (x_i - x_j)^2,$$

also $D \neq 0$. D invariant unter $\mathcal{G}$, sogar unter S_n, also $D \in K$.

2 Fälle: 1) $D = \delta^2$ mit $\delta \in K$.
D.h.

$$\delta = \prod_{i<j} x_i - x_j \quad \in K.$$

Da δ genau unter den geraden Permutationen invariant bleibt, ist damit $\mathrm{Gal}(E|K) \subset A_n$.

2) $\delta \notin K$. Dann ~~hat~~ $[K(\delta):K] = 2$,
$\mathrm{Gal}(E|K(\delta)) = A_n \cap \mathcal{G}$.

(10) Casus irreducibilis

$K = \mathbb{R}$, (K) habe 3 reelle Wurzeln.
Dann ist D (Diskriminante) > 0, also

$\sqrt{-3D}$ rein imaginär. D.h. die Wurzeln werden aus ~~nichtreellen Zahl~~ den kubischen Wurzeln nichtreeller komplexer Zahlen gewonnen. Man kann zeigen: es gibt keine Konstruktion der Wurzeln aus reellen Radikalen.

(11) Die Galoisgruppe von f ist S_3 oder A_3: welcher Fall tritt nun auf? Genau, wenn D ein Quadrat $\in K$ ist, liegt der Fall A_3 vor. Also: bei beliebiger Wahl von a und b in

im Fall $K = \mathbb{Q}$

$$x^3 + ax + b = 0$$

ist mit Wahrscheinlichkeit 1 D kein Quadrat, und die Gal.gruppe ist S_3. D.h. jede Permutation der 3 Wurzeln setzt sich zu einem Automorphismus des Zerfällungskörpers fort.

Exkurs: Das 17-eck

Satz 1. Es sei $p \geq 3$ eine Primzahl. Es sei $f(x) = x^p - 1$, E der Zerfällungskörper. Dann ist $\mathrm{Gal}(E|\mathbb{Q}) = \mathrm{Gal}\, f(x) \cong \mathbb{F}_p^*$

Beweis $f(x) = (x-1)(x^{p-1} + x^{p-2} + \dots + x + 1)$

$$= (x-1)\, g(x).$$

$g(x)$ irreduzibel (über $\mathbb{Q}$), die Wurzeln sind die p-ten EW (ohne 1), alle primitiv, d.h. sie erzeugen die zyklische Gruppe dieser Elem ($\cong \mathbb{Z}_{17}$). Es sei ζ eine (beliebige) Nullstelle von ~~f~~ g und $\sigma \in \mathrm{Gal}\, f(x)$. Definiere

$$v(\sigma) = i \quad \Leftrightarrow \quad \sigma(\zeta) = \zeta^i \; (\neq 1)$$

Es ist i eindeutig mod p, also $i \in \mathbb{F}_p^*$.

Ist $\tau \in \mathrm{Gal}\, f(x)$, $\tau(\zeta) = \zeta^j$, so folgt

$$\tau\sigma(\zeta) = \tau(\zeta^i) = \zeta^{ij}$$

$$\rightsquigarrow \quad v(\tau\sigma) = v(\tau) \cdot v(\sigma).$$

Offenbar ist $v(id) = 1 \in \mathbb{F}_p^*$. Ferner ist v injektiv, da σ durch $\sigma(\zeta)$ festgelegt ist. Beide Gruppen sind gleichgroß – Ordnung $= p-1$ –,

$$\rightsquigarrow \quad \mathrm{Gal}\, f(x) \underset{v}{\cong} \mathbb{F}_p^*$$

Folgerung. 1) $\mathrm{Gal}\, f(x)$ ist zyklisch

2) Es sei $\mathcal{G} = \mathrm{Gal}\, f(x)$. Da $\mathcal{G}$ zyklisch ist, enthält $\mathcal{G}$ zu jedem Teiler von $p-1$ genau eine Untergruppe dieser Ordnung.

Galoistheorie: es sei $p = 17$. Dann gibt es eine Körperkette

$$E = K_0 \supset K_1 \supset K_2 \supset K_3 \supset K_4 = \mathbb{Q}$$

$$\{1\} \subset C_2 \subset C_4 \subset C_8 \subset C_{16} = \mathcal{G}$$

mit $\quad K_1 = \mathrm{Fix}\, C_2, \ldots, K_4 = \mathrm{Fix}\, \mathcal{G} = \mathbb{Q}$

Der Körpergrad ist jeweils der Index von $C_j \subset C_{2j}$, also 2: $\quad [K_1|K_0] = [K_2|K_1] = [K_3|K_2] = [K_4|K_3] = 2$.

E entsteht also durch sukzessive quadratische Erweiterungen. Damit ist insbesondere jedes ζ konstruierbar.

<u>Satz</u> (Gauß) Das regelmäßige 17-eck ist konstruierbar, ebenso jedes regelmäßige p-eck mit

$$p = 2^{2^n} + 1.$$

Genauere Analyse zeigt: für andere Primzahlen p sind die regulären p-ecke nicht konstruierbar.