KAPITEL 10

Die Galoisgruppe eines Polynoms

1. Allgemeines

Erinnerung:

(1) Ist M eine Menge, so bildet die Menge der bijektiven Abbildungen $f : M \to M$ mit der Komposition von Abbildungen eine Gruppe, die man auch mit $S(M)$ bezeichnet und **symmetrische Gruppe** (auf der Menge M) nennt, also

$$S(M) = \{f : M \to M \text{ bijektiv}\}.$$

(2) Für $n \in \mathbb{N}$ schreibt man statt $S(\{1, 2, \ldots, n\})$ auch einfach S_n und nennt S_n einfach die **symmetrische Gruppe** S_n.

(3) Ist M endlich, nummeriert man die Elemente von M, also

$$M = \{\alpha_1, \ldots, \alpha_n\},$$

ist $\sigma \in S(\{\alpha_1, \ldots, \alpha_n\}$, so gibt es eine Permutation $\widetilde{\sigma} \in S_n$ mit

$$\sigma(\alpha_i) = \alpha_{\widetilde{\sigma}(i)} \text{ für } i = 1, \ldots, n.$$

Die Abbildung

$$S(\{\alpha_1, \ldots, \alpha_n\}) \to S_n, \quad \sigma \mapsto \widetilde{\sigma}$$

ist ein Gruppenisomorphismus.

(4) Ist $M = \{\alpha_1, \ldots, \alpha_n\}$, so beschreibt man die Elemente $\sigma \in S(\{\alpha_1, \ldots, \alpha_n\})$ auch manchmal in Tabellenform:

$$\sigma = \begin{pmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \sigma(\alpha_1) & \sigma(\alpha_2) & \ldots & \sigma(\alpha_n) \end{pmatrix}.$$

(5) Für S_n verwendet wir oft auch die **Zykeldarstellung** von Permutationen.

(6) Eine Untergruppe G von $S(\{\alpha_1, \ldots, \alpha_n\})$ nennt man eine **transitive Untergruppe**, wenn es zu je zwei Indizes $i, j \in \{1, \ldots, n\}$ ein $\sigma \in G$ gibt mit $\sigma(\alpha_i) = \alpha_j$.

DEFINITION. *Ist K ein Körper und $f \in K[x]$ ein separables, nicht nichtwendig irreduzibles, normiertes Polynom, ist Z ein Zerfällungskörper von f über K, so ist $Z|K$ galoissch und die Galoisgruppe* $\mathrm{Gal}(Z|K)$ *wird die* **Galoisgruppe des Polynoms** *f genannt, in Zeichen:*

$$\mathrm{Gal}(f|K) = \mathrm{Gal}(Z|K).$$

Anders formuliert: Sind $\alpha_1, \ldots, \alpha_n$ die Nullstellen von f im algebraischen Abschluss von K, so ist $K(\alpha_1, \ldots, \alpha_n)$ der Zerfällungskörper von f über K und

$$\mathrm{Gal}(f|K) = \mathrm{Gal}(K(\alpha_1, \ldots, \alpha_n)|K).$$

Beispiele:

(1) Für $f = x^2 - 2 \in \mathbb{Q}[x]$ gilt

$$f(x) = (x - \sqrt{2})(x + \sqrt{2}) \in \overline{\mathbb{Q}}[x],$$

der Zerfällungskörper von f ist $\mathbb{Q}(\sqrt{2})$, also ist

$$\mathrm{Gal}(x^2 - 2|\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\sqrt{2})|\mathbb{Q}) \simeq \mathbb{Z}_2.$$

Datei: kt_pol.tex. Version vom 15.7.2024

(2) Für $f = x^2 - 1 \in \mathbb{Q}[x]$ gilt

$$f(x) = (x-1)(x+1) \in \mathbb{Q}[x].$$

Der Zerfällungskörper ist $\mathbb{Q}$, also gilt

$$\mathrm{Gal}(x^2-1|\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}|\mathbb{Q}) = \{\mathrm{id}\} \simeq \mathbb{Z}_1.$$

Erinnerung: Sei K ein Körper und $f \in K[x]$ ein Polynom vom Grad ≥ 1 mit der Zerlegung

$$f(x) = (x-\alpha_1)\dots(x-\alpha_n) \in \overline{K}[x].$$

Dann gilt:

$$\sigma(\{\alpha_1,\dots,\alpha_n\}) = \{\alpha_1,\dots,\alpha_n\} \text{ für alle } \sigma \in \mathrm{Aut}(\overline{K}|K).$$

Die Automorphismen permutieren die Nullstellen des Polynoms. (Ist nämlich $f(x) = \sum_i c_i x^i$ und $f(\alpha) = 0$, so folgt für $\sigma \in \mathrm{Aut}(\overline{K}|K)$

$$0 \quad = \quad \sigma(0) = \sigma(f(\alpha)) = \sigma(\sum_i c_i\alpha^i) = \sum_i \sigma(c_i)\sigma(\alpha)^i = \sum_i c_i\sigma(\alpha)^i = f(\sigma(\alpha)),$$

also ist auch $\sigma(\alpha)$ eine Nullstelle von f.)

Satz. *Sei K ein Körper und $f \in K[x]$ ein separables, nicht notwendig irreduzibles, normiertes Polynom vom Grad $n \geq 1$. Sei Z ein Zerfällungskörper von f. Dann gibt es (paarweise verschiedene) $\alpha_1,\dots,\alpha_n \in Z$ mit*

$$Z = K(\alpha_1,\dots,\alpha_n) \quad \textit{und} \quad f = (x-\alpha_1)\dots(x-\alpha_n).$$

Dann ist $Z|K$ galoissch. Es gilt:

(1) *Durch*

$$\pi : \mathrm{Gal}(Z|K) \to S(\{\alpha_1,\dots,\alpha_n\}), \quad \sigma \mapsto \sigma|_{\{\alpha_1,\dots,\alpha_n\}},$$

also

$$\pi(\sigma) = \begin{pmatrix} \alpha_1 & \dots & \alpha_n \\ \sigma(\alpha_1) & \dots & \sigma(\alpha_n) \end{pmatrix}$$

wird ein injektiver Gruppenhomomorphismus definiert.

(2) *Daher kann man* $\mathrm{Gal}(f|K) = \mathrm{Gal}(Z|K)$ *als Untergruppe von* $S(\{\alpha_1,\dots,\alpha\})$ *auffassen.*

(3) *Es gilt*

$$|\mathrm{Gal}(f|K)| \mid n!.$$

(4) *f ist genau dann irreduzibel, wenn* $\mathrm{Bild}(\pi)$ *eine transitive Untergruppe von* $S(\{\alpha_1,\dots,\alpha_n\})$ *ist.*

Beweis:

(1) Wir haben zuvor daran erinnert, dass Automorphismen $\sigma \in \mathrm{Gal}(Z|K)$ die Nullstellen von f permutieren. Daher ist $\sigma|_{\{\alpha_1,\dots,\alpha_n\}}$ eine Permutation. Da Elemente σ von $\mathrm{Gal}(Z|K)$ wegen $Z = K(\alpha_1,\dots,\alpha_n)$ durch $\sigma|_{\{\alpha_1,\dots,\alpha_n\}}$ bestimmt sind, ist π injektiv.
Warum ist π ein Gruppenhomomorphismus? Für $\sigma,\tau \in \mathrm{Gal}(Z|K)$ gilt:

$$\begin{aligned}(\pi(\sigma)\circ\pi(\tau))(\alpha_i) &= \pi(\sigma)\left(\pi(\tau)(\alpha_i)\right) = \pi(\sigma)(\tau(\alpha_i)) = \sigma(\tau(\alpha_i)) = (\sigma\circ\tau)(\alpha_i) = \\ &= \pi(\sigma\circ\tau)(\alpha_i),\end{aligned}$$

also $\pi(\sigma)\circ\pi(\tau) = \pi(\sigma\circ\tau)$, wie behauptet.

(2) Da π injektiv ist, ist $\mathrm{Gal}(Z|K)$ zu seinem Bild $\pi(\mathrm{Gal}(Z|K))$, was die Aussage beweist.

(3) Dies folgt aus der Tatsache, dass $\mathrm{Bild}(\pi)$ eine Untergruppe von $S(\{\alpha_1,\dots,\alpha_n\})$ ist, dass damit auch $|\mathrm{Bild}(\pi)| \mid |S(\{\alpha_1,\dots,\alpha_n\})|$ gilt.

(4)
- Sei f irreduzibel. Seien α_i, α_j Nullstellen von f. Da f irreduzibel ist, ist f das Minimalpolynom von α_i. Zu α_i gibt es dann einen K-Körperhomomorphismus $\sigma_0 : K(\alpha_i) \to \overline{K}$ mit $\sigma_0(\alpha_i) = \alpha_j$. Da $Z|K$ normal ist, lässt sich σ_0 zu einem Element $\sigma \in \mathrm{Gal}(Z|K)$ mit $\sigma(\alpha_i) = \alpha_j$ fortsetzen. Dies zeigt, dass $\mathrm{Bild}(\pi)$ eine transitive Untergruppe der symmetrischen Gruppe ist.

- Sei f reduzibel. Wir können also zerlegen $f = gh$ mit $g, h \in K[x]$ normiert vom Grad ≥ 1. Wir können schreiben

$$g = (x - \beta_1) \dots (x - \beta_m) \quad \text{und} \quad h = (x - \gamma_1) \dots (h - \gamma_{n-m}).$$

Für $\sigma \in \mathrm{Gal}(L|K)$ folgt

$$\sigma(\{\beta_1, \dots, \beta_m\}) = \{\beta_1, \dots, \beta_m\} \quad \text{und} \quad \sigma(\{\gamma_1, \dots, \gamma_{n-m}\}) = \{\gamma_1, \dots, \gamma_{n-m}\}.$$

Daher ist $\mathrm{Bild}(\pi)$ keine transitive Untergruppe von $S(\{\alpha_1, \dots, \alpha_n\})$. ■

Bemerkung: Wenn wir uns die Nullstellen von f nummeriert denken, also $\alpha_1, \dots, \alpha_n$, so können wir statt $S(\{\alpha_1, \dots, \alpha_n\}$ auch mit S_n arbeiten:

$$\widetilde{\pi} : \mathrm{Gal}(L|K) \to S_n, \quad \sigma \mapsto \widetilde{\pi}(\sigma) \text{ mit } \sigma(\alpha_i) = \alpha_{\widetilde{\pi}(\sigma)(i)}.$$

Beispiel: Wir betrachten das Polynom $f = x^3 - x^2 + x - 1 \in \mathbb{Q}[x]$. Es ist

$$f = x^3 - x^2 + x - 1 = (x-1)x^2 + (x-1) = (x-1)(x^2+1) = (x-1)(x-i)(x+i).$$

Die Nullstellen von f sind also $1, i, -i$, der Zerfällungskörper von f ist $\mathbb{Q}(i)$. Der einzige nichttriviale Automorphismus von $\mathbb{Q}(i)|\mathbb{Q}$ ist die komplexe Konjugation, die wir hier mit σ bezeichnen. Damit erhalten wir

$$\pi : \mathrm{Gal}(\mathbb{Q}(i)|\mathbb{Q}) \to S(\{1, i, -i\}) \text{ mit } \pi(\mathrm{id}) = \begin{pmatrix} 1 & i & -i \\ 1 & i & -i \end{pmatrix} \text{ und } \pi(\sigma) = \begin{pmatrix} 1 & i & -i \\ 1 & -i & i \end{pmatrix}.$$

Schreiben wir $\alpha_1 = 1$, $\alpha_2 = i$, $\alpha_3 = -i$, so können wir $S(\{1, i, -i\})$ mit S_3 identifizieren. Dann ist $\pi(\mathrm{id}) = (1)$ und $\pi(\sigma) = (23)$.

Bemerkung: Der vorangegangene Satz legt es nahe, die Galoisgruppe eines Polynoms f als Permutationsgruppe seiner Wurzeln $\alpha_1, \dots, \alpha_n$ zu betrachten. In gängigen Algebra-Lehrbüchern[1] wird $\mathrm{Gal}(f|K)$ aber nur als $\mathrm{Gal}(K(\alpha_1, \dots, \alpha_n)|K)$ definiert.

Beispiel: Wir betrachten das Polynom $f = x^4 + 5x^2 + 5 \in \mathbb{Q}[x]$, das nach Eisenstein für $p = 5$ irreduzibel ist. Ist $\alpha \in \mathbb{C}$ eine Nullstelle von f, so ist $K = \mathbb{Q}(\alpha)$ vom Grad 4 über $\mathbb{Q}$. Man kann f über K in Linearfaktoren zerlegen:

$$f = (x - \alpha)(x + \alpha)(x - (3\alpha + \alpha^3))(x + (3\alpha + \alpha^3)).$$

Definieren wir

$$\beta = 3\alpha + \alpha^3,$$

so ist

$$f = (x - \alpha)(x - \beta)(x + \alpha)(x + \beta).$$

K ist also Zerfällungskörper von f und damit galoissch über $\mathbb{Q}$. Die Galoisgruppe hat also 4 Elemente. Für jedes $\xi \in \{\alpha, \beta, -\alpha, -\beta\}$ gibt es einen Automorphismus σ mit $\sigma(\alpha) = \xi$. Wir gehen die vier Möglichkeiten durch:

- **Fall $\sigma_1(\alpha) = \alpha$:** Dann ist $\sigma_1 = \mathrm{id}$. Natürlich gilt

$$\pi(\sigma_1) = \begin{pmatrix} \alpha & \beta & -\alpha & -\beta \\ \alpha & \beta & -\alpha & -\beta \end{pmatrix} \simeq (1).$$

- **Fall $\sigma_2(\alpha) = \beta$:** Dann gilt

$$\sigma_2(\beta) = \sigma_2(3\alpha + \alpha^3) = 3\sigma_2(\alpha) + \sigma_2(\alpha)^3 = 3\beta + \beta^3 = 3(3\alpha + \alpha^3) + (3\alpha + \alpha^3)^3 = \dots = -\alpha,$$

sodass wir

$$\pi(\sigma_2) = \begin{pmatrix} \alpha & \beta & -\alpha & -\beta \\ \beta & -\alpha & -\beta & \alpha \end{pmatrix} \simeq (1234)$$

erhalten.

[1] Bosch: Algebra (2023). Fischer: Lehrbuch der Algebra (2017). Plaumann: Algebra (2023). Wüstholz: Algebra (2020)

- **Fall** $\sigma_3(\alpha) = -\alpha$**:** Dann ist

$$\sigma_3(\beta) = \sigma_3(3\alpha + \alpha^3) = 3(-\alpha) + (-\alpha)^3 = -(3\alpha + \alpha^3) = -\beta$$

und

$$\pi(\sigma_3) = \begin{pmatrix} \alpha & \beta & -\alpha & -\beta \\ -\alpha & -\beta & \alpha & \beta \end{pmatrix} \simeq (13)(24).$$

- **Fall** $\sigma_4(\alpha) = -\beta$**:** Dann ist

$$\sigma_4(\beta) = \sigma_4(3\alpha + \alpha^3) = 3(-\beta) + (-\beta)^3 = -(3\beta + \beta^3) = \alpha$$

und

$$\pi(\sigma_4) = \begin{pmatrix} \alpha & \beta & -\alpha & -\beta \\ -\beta & \alpha & \beta & -\alpha \end{pmatrix} \simeq (1432).$$

Die Galoisgruppe $\mathrm{Gal}(\mathbb{Q}(\alpha)|\mathbb{Q})$ ist also isomorph zur zyklischen Untergruppe

$$\{(1), (12)(34), (1234), (1423)\}$$

von S_4.

2. Zwischenbetrachtungen

Quadratische Polynome: Sei K ein Körper und $f = x^2 + ax + b \in K[x]$. Sei L ein Zerfällungskörper von f und $\alpha_1, \alpha_2 \in L$ mit

$$f = (x - \alpha_1)(x - \alpha_2) \quad \text{und} \quad L = K(\alpha_1, \alpha_2).$$

Aus $f = x^2 - (\alpha_1 + \alpha_2)x + \alpha_1\alpha_2$ folgt durch Koeffizientenvergleich

$$\alpha_1 + \alpha_2 = -a \quad \text{und} \quad \alpha_1\alpha_2 = b.$$

Wir betrachten

$$\delta = \alpha_1 - \alpha_2.$$

Es ist

$$\delta^2 = \alpha_1^2 - 2\alpha_1\alpha_2 + \alpha_2^2 = (\alpha_1^2 + 2\alpha_1\alpha_2 + \alpha_2^2) - 4\alpha_1\alpha_2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = a^2 - 4b.$$

Es ist also $\delta = \pm\sqrt{a^2 - 4b}$. Aus

$$\alpha_1 + \alpha_2 = -a \quad \text{und} \quad \alpha_1 - \alpha_2 = \delta$$

erhalten wir durch Addition und Subtraktion

$$2\alpha_1 = -a + \delta \quad \text{und} \quad 2\alpha_2 = -a - \delta.$$

Um weiterzumachen, müssen wir $\mathrm{char}(K) \neq 2$ voraussetzen. Dann gilt

$$\alpha_1 = \frac{-a + \delta}{2}, \quad \alpha_2 = \frac{-a - \delta}{2},$$

also

$$\{\alpha_1, \alpha_2\} = \{\frac{-a + \sqrt{a^2 - 4b}}{2}, \frac{-a - \sqrt{a^2 - 4b}}{2}\}.$$

Wir erhalten also die üblichen Auflösungsformeln für quadratische Gleichungen. Leider funktioniert dies bei höherem Grad nicht so einfach.

Quadratische Ergänzung: Sei $f = x^2 + ax + b \in K[x]$ und $\mathrm{char}(K) \neq 2$. Dann können wir **quadratische Ergänzung** machen:

$$f = x^2 + ax + b = x^2 + 2 \cdot \frac{1}{2}a \cdot x + b = (x^2 + 2 \cdot \frac{1}{2}a \cdot x + \frac{1}{4}a^2) + b - \frac{1}{4}a^2 = (x + \frac{1}{2}a)^2 - \frac{a^2 - 4b}{4}.$$

Kubische Ergänzung: Sei $f = x^3 + ax^2 + bx + c \in K[x]$. Wir wollen den Term ax^2 durch **kubische Ergänzung** (und eine Koordinatentransformation) zu Null machen. Wir müssen $\mathrm{char}(K) \neq 3$ voraussetzen. Wir setzen $x = y - \frac{1}{3}x$:

$$\begin{aligned} f &= x^3 + ax^2 + bx + c = (y - \frac{1}{3}a)^3 + a(y - \frac{1}{3}a)^2 + b(y - \frac{1}{3}a) + c = \\ &= \Big(y^3 - ay^2 + \frac{1}{3}a^2y - \frac{1}{27}a^3\Big) + \Big(ay^2 - \frac{2}{3}a^2y + \frac{1}{9}a^3\Big) + \Big(by - \frac{1}{3}ab\Big) + c = \\ &= y^3 + \Big(b - \frac{1}{3}a^2\Big)y + \Big(\frac{2}{27}a^3 - \frac{1}{3}ab + c\Big). \end{aligned}$$

Als Polynom in $y = x + \frac{1}{3}a$ hat nun f keinen quadratischen Term mehr. Dies funktioniert auch allgemein:

Vereinfachung eines Polynoms vom Grad n: Sei $f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n \in K[x]$ ein normiertes Polynom vom Grad n. Wir setzen voraus, dass $n \neq 0$ in K gilt. Setzen wir $x = y - \frac{1}{n}a_1$, so folgt

$$\begin{aligned} f &= x^n + a_1x^{n-1} + \cdots = \\ &= \Big(y - \frac{1}{n}a_1\Big)^n + a_1\Big(y - \frac{1}{n}a_1\Big)^{n-1} + \cdots = \\ &= \Big(y^n - a_1y^{n-1} + \ldots\Big) + a_1\Big(y^{n-1} + \ldots\Big) + \cdots = \\ &= y^n + 0 \cdot y^{n-1} + \ldots \end{aligned}$$

Der Koeffizient bei y^{n-1} ist also 0. Sind $\beta_1, \ldots, \beta_n$ die Nullstellen in y, so sind die Nullstellen in x einfach $\beta_1 - \frac{1}{n}a_1, \ldots, \beta_n - \frac{1}{n}a_1$. Um gewisse Situationen zu vereinfachen kann man diese Transformation durchführen. Man beachte aber, dass n im Grundkörper K nicht 0 sein darf, d.h. $\mathrm{char}(K) \nmid n$.

3. Kubische Polynome

Bemerkung: Die symmetrische Gruppe S_3 hat nur zwei transitive Untergruppen, nämlich

$$A_3 = \{(1), (123), (132)\} \simeq \mathbb{Z}_3 \quad \text{und} \quad S_3 = \{(1), (12), (13), (23), (123), (132)\}.$$

(Daneben gibt es noch die nichttransitiven Untergruppen mit jeweils 2 Elementen: $\{(1), (12)\}$, $\{(1), (13)\}$, $\{(1), (23)\}$.)

Satz. *Sei K ein Körper und $f = x^3 + ax + b \in K[x]$, sei L ein Zerfällungskörper von f über K, d.h. es gibt $\alpha_1, \alpha_2, \alpha_3 \in L$ mit*

$$L = K(\alpha_1, \alpha_2, \alpha_3) \quad \textit{und} \quad f = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3).$$

Sei weiter

$$\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) \in L.$$

Dann gilt:

1. *Es ist $\delta^2 = -4a^3 - 27b^2$. (Man nennt $\mathrm{disc}\,(f) = -4a^3 - 27b^2$) die* **Diskriminante** *von f.)*
2. *f ist genau dann separabel, wenn $-4a^3 - 27b^2 \neq 0$ ist.*
3. *Sei nun $\mathrm{char}(K) \neq 2$, f irreduzibel über K und $-4a^3 - 27b^2 \neq 0$. Dann gilt:*
   (a) *Ist $-4a^3 - 27b^2 \in K^{*2}$, so ist*

$$[L : K] = 3 \quad \textit{und} \quad \mathrm{Gal}(L|K) \simeq \mathbb{Z}_3.$$

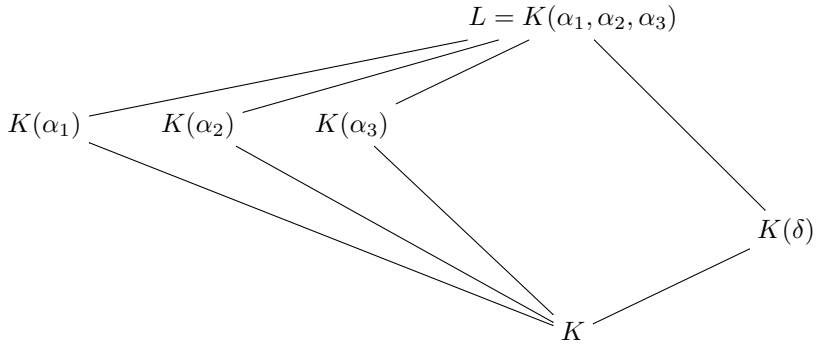
Das Unterkörperdiagramm ist

$$\begin{array}{c} L = K(\alpha_1) = K(\alpha_2) = K(\alpha_3) \\ \Big| \\ K = K(\delta) \end{array}$$

(b) *Ist* $-4a^3 - 27b^2 \in K^* \setminus K^{*2}$*, so gilt*

$$[L : K] = 6 \quad \textit{und} \quad \mathrm{Gal}(L|K) \simeq S_3.$$

Das Unterkörperdiagramm ist



Beweis:

(1) Aus

$$\begin{aligned} f &= (x-\alpha_1)(x-\alpha_2)(x-\alpha_3) = \\ &= x^3 - (\alpha_1+\alpha_2+\alpha_3)x^2 + (\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3)x - \alpha_1\alpha_2\alpha_3 \end{aligned}$$

folgt durch Koeffizientenvergleich

$$\alpha_1+\alpha_2+\alpha_3 = 0, \quad \alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3 = a, \quad \alpha_1\alpha_2\alpha_3 = -b.$$

Mit $\alpha_3 = -\alpha_1 - \alpha_2$ folgt

$$a = -\alpha_1^2 - \alpha_1\alpha_2 - \alpha_2^2, \quad b = \alpha_1^2\alpha_2 + \alpha_1\alpha_2^2, \quad \delta = 2\alpha_1^3 + 3\alpha_1^2\alpha_2 - 3\alpha_1\alpha_2^2 - 2\alpha_2^3.$$

Nun rechnet man nach

$$\delta^2 + 4a^3 + 27b^2 = 0,$$

was gezeigt werden sollte.

(2) Dies folgt sofort aus der Definition von δ und (1).

(3) Da f irreduzibel ist, kann man $\mathrm{Gal}(L|K)$ als transitive Untergruppe von $S_3 \simeq S(\{\alpha_1, \alpha_2, \alpha_3\})$ auffassen. Es gibt aber nur zwei transitive Untergruppen von S_3, nämlich A_3 und S_3. Wir unterscheiden also zwei Fälle:

- **Fall** $\mathrm{Gal}(L|K) \simeq A_3 \simeq Z_3$**:** Dann ist $[L : K] = 3$, woraus dann

$$L = K(\alpha_1) = K(\alpha_2) = K(\alpha_3)$$

folgt. Da δ höchstens quadratisch über K ist, folgt aus $[L : K] = 3$ sofort $\delta \in K$, und damit $-4a^3 - 27b^2 \in K^{*2}$.

- **Fall** $\mathrm{Gal}(L|K) \simeq S_3$**:** Dann ist $[L : K] = 6$ und $[K(\alpha_1) : K] = [K(\alpha_2) : K] = [K(\alpha_3) : K] = 3$. Gehört σ zu einer ungeraden Permutation, so ist $\sigma(\delta) = -\delta$. Im Fall $\mathrm{char}(K) \neq 2$ folgt $\delta \notin K$, und damit $-4a^3 - 27b^2 \notin K^{*2}$. ■

Beispiele:

(1) $f = x^3 + 7x - 7 \in \mathbb{Q}[x]$. Das Polynom ist nach Eisenstein für $p = 7$ irreduzibel, die Diskriminante ist

$$\mathrm{disc}\,(f) = -4 \cdot 7^3 - 27 \cdot (-7)^2 = -2695 = -5 \cdot 7^2 \cdot 11.$$

Da die Diskriminante kein Quadrat in $\mathbb{Q}$ ist, gilt

$$\mathrm{Gal}(f|\mathbb{Q}) \simeq S_3.$$

(2) $f = x^3 - 21x - 7 \in \mathbb{Q}[x]$. Das Polynom ist nach Eisenstein für $p = 7$ irreduzibel. Es ist

$$\operatorname{disc}(f) = -4(-21)^3 - 27(-7)^2 = 35721 = 3^6 \cdot 7^2.$$

Die Diskriminante ist ein Quadrat in $\mathbb{Q}$, weswegen

$$\mathrm{Gal}(f|\mathbb{Q}) \simeq \mathbb{Z}_3$$

gilt.

Anmerkung zur Wahl von f: Wir betrachten den 7-ten Kreisteilungskörper $\mathbb{Q}(\zeta_7)$. Das Element $\zeta_7 + \zeta_7^{-1}$ hat das Minimalpolynom $g(x) = x^3 + x^2 - 2x - 1$. Nun ist $f(x) = g(\frac{x-1}{3})$.

(3) $f = x^3 - 8x - 7 \in \mathbb{Q}[x]$. Man findet

$$f = (x+1)(x^2 - x - 7) = (x-1)(-\frac{1+\sqrt{29}}{2})(x - \frac{1-\sqrt{29}}{2}).$$

Also ist der Zerfällungskörper von f der quadratische Körper $\mathbb{Q}(\sqrt{29})$, und damit

$$\mathrm{Gal}(f|\mathbb{Q}) \simeq \mathbb{Z}_2.$$

Als Anwendung bestimmen wir im S_3-Fall primitive Elemente.

SATZ. *Sei K ein Körper der Charakteristik $\neq 2, 3$, $f = x^3 + ax + b \in K[x]$ ein irreduzibles Polynom, sodass die Diskriminante* $\operatorname{disc}(f) = -4a^3 - 27b^2$ *kein Quadrat in K ist. Sei L der Zerfällungskörper von f über K und $\alpha_1, \alpha_2, \alpha_3 \in L$ mit*

$$L = K(\alpha_1, \alpha_2, \alpha_3) \quad \textit{und} \quad f = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3).$$

Dann ist $L|K$ galoissch vom Grad 6 mit Galoisgruppe S_3. Für $\lambda \in K$ gilt

$$L = K(\alpha_1 + \lambda\alpha_2) \quad \Longleftrightarrow \quad \lambda \neq 0, 1.$$

(Im Fall $\lambda = 0$ ist $K(\alpha_1) \neq L$, im Fall $\lambda = 1$ ist $K(\alpha_1 + \alpha_2) = K(\alpha_3) \neq L$.)

Beweis: Nur die letzte Aussage müssen wir noch zeigen. Wegen $K(\alpha_1) \neq K(\alpha_2)$ sind α_1 und α_2 linear unabhängig über K. Da der Koeffizient von f bei x^2 Null ist, gilt $\alpha_1 + \alpha_2 + \alpha_3 = 0$, also

$$\alpha_3 = -\alpha_1 - \alpha_2.$$

Sei nun $\lambda \in K \setminus \{0\}$. Wir schauen, was die Galoisgruppe mit $\alpha_1 + \lambda\alpha_2$ macht. Der einfacheren Notation halber identifizieren wir die Elemente der S_3 mit den Elementen der Galoisgruppe.

$$\begin{aligned}
(12)(\alpha_1 + \lambda\alpha_2) &= \alpha_2 + \lambda\alpha_1 = \lambda\alpha_1 + \alpha_2, \\
(13)(\alpha_1 + \lambda\alpha_2) &= \alpha_3 + \lambda\alpha_2 = (-\alpha_1 - \alpha_2) + \lambda\alpha_2 = -\alpha_1 + (\lambda - 1)\alpha_2, \\
(123)(\alpha_1 + \lambda\alpha_2) &= \alpha_2 + \lambda\alpha_3 = \alpha_2 + \lambda(-\alpha_1 - \alpha_2) = -\lambda\alpha_1 + (1 - \lambda)\alpha_2, \\
(132)(\alpha_1 + \lambda\alpha_2) &= \alpha_3 + \lambda\alpha_1 = (-\alpha_1 - \alpha_2) + \lambda\alpha_1 = (\lambda - 1)\alpha_1 - \alpha_2.
\end{aligned}$$

Im Fall $\lambda \neq 1$ bleibt $\alpha_1 + \lambda\alpha_2$ nur unter der Identität fest, die Fixgruppe ist also $\{\mathrm{id}\}$, woraus dann

$$K(\alpha_1 + \lambda\alpha_2) = L$$

folgt. ■

Das folgende Beispiel soll zeigen, dass das Diskriminantenkriterium in Charakteristik 2 nicht funktioniert.

Beispiel: Sei $K = \mathbb{F}_2(t)$ (mit einer Unbestimmten t) und $f = x^3 - t$. ζ mit $\zeta^2 + \zeta + 1$ ist dann eine primitive 3-te Einheitswurzel und vom Grad 2 über $\mathbb{F}_2$. Sei $\xi^3 = t$. Dann gilt

$$f = x^3 - t = x^3 - \xi^3 = (x - \xi)(x - \zeta\xi)(x - \zeta^2\xi).$$

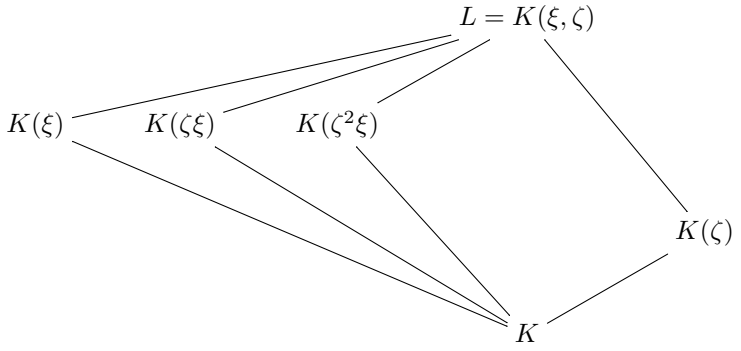
Der Zerfällungskörper ist

$$L = K(\xi, \zeta) \quad \text{mit} \quad [L : K] = 6.$$

Wir betrachten

$$\begin{aligned}\delta &= (\xi-\zeta\xi)(\xi-\zeta^2\xi)(\zeta\xi-\zeta^2\xi) = \xi^3\cdot(1-\zeta)(1-\zeta^2)(\zeta-\zeta^2) = \\ &= \xi^3\cdot(1-\zeta)(1-\zeta^2)\zeta(1-\zeta) = t\cdot\zeta\cdot(1-\zeta)^4 = t\cdot\zeta\cdot(1-\zeta) = \\ &= t\cdot\zeta\cdot(1+\zeta) = t\cdot(\zeta+\zeta^2) = t.\end{aligned}$$

Der quadratische Zwischenkörper wird in diesem Fall von ζ erzeugt.



Wir haben also auch hier eine S_3-Erweiterung, wenn auch das Kriterium mit $-4a^3-27b^2=t^2$ hier nicht funktioniert.

4. Diskriminanten

Erinnerung: Ist $\pi\in S_n$, so lässt sich das Signum/Vorzeichen der Permutation durch

$$\prod_{1\le i<j\le n}(x_{\pi(i)}-x_{\pi(j)}) = \operatorname{sgn}(\pi)\cdot\prod_{1\le i<j\le n}(x_i-x_j)$$

charakterisieren, wobei $x_1,\dots,x_n$ Unbestimmte über $\mathbb{Z}$ sind. Natürlich bleibt die Gleichung richtig, wenn man für $x_1,\dots,x_n$ Elemente eines Körpers einsetzt.

Wir setzen hier $\operatorname{char}(K)\neq 2$ voraus. Sei $f\in K[x]$ ein normiertes Polynom, L ein Zerfällungskörper von f und $\alpha_1,\dots,\alpha_n\in L$ mit

$$f=(x-\alpha_1)\dots(x-\alpha_n) \quad \text{und} \quad L=K(\alpha_1,\dots,\alpha_n).$$

Wir bilden

$$\delta=\prod_{1\le i<j\le n}(\alpha_i-\alpha_j).$$

f ist genau dann separabel, wenn $\delta\neq 0$ gilt. Ist dies der Fall, so ist $L|K$ galoissch. Ist $\sigma\in\operatorname{Gal}(L|K)$, so gilt

$$\sigma(\delta)=\operatorname{sgn}(\pi(\sigma))\cdot\delta.$$

Dann folgt

$$\Delta=\delta^2\in K.$$

Δ wird auch die **Diskriminante** $\operatorname{disc}(f)$ des (normierten) Polynoms f genannt.

Beispiele:

$$\operatorname{disc}(x^2+ax+b)=a^2-4b, \quad \operatorname{disc}(x^3+ax+b)=-4a^3-27b^2.$$

5. Die Galoisgruppe der Polynome $x^4 + ax^2 + b$

Überlegungen: Wir betrachten ein Polynom $f = x^4 + ax^2 + b \in K[x]$, die Koeffizienten bei x^3 und x sind also 0. Für die Diskriminante findet man

$$\operatorname{disc}(x^4 + ax^2 + b) = 16b(a^2 - 4b)^2.$$

Wir setzen voraus, dass die Diskriminante von 0 verschieden ist. Dann ist f separabel und $\operatorname{char}(K) \neq 2$. Sei L ein Zerfällungskörper von f. Da mit α auch $-\alpha$ eine Nullstelle von f ist, gibt es $\alpha, \beta \in L$ mit

$$L = K(\alpha, \beta) \quad \text{und} \quad f = (x - \alpha)(x - \beta)(x + \alpha)(x + \beta).$$

Wir erhalten dann einen Gruppenhomomorphismus

$$\pi : \operatorname{Gal}(L|K) \to S(\{\alpha, \beta, -\alpha, -\beta\}), \quad \sigma \mapsto \begin{pmatrix} \alpha & \beta & -\alpha & -\beta \\ \sigma(\alpha) & \sigma(\beta) & -\sigma(\alpha) & -\sigma(\beta) \end{pmatrix}.$$

Wir wollen untersuchen, welche Bilder in Frage kommen. Wir verwenden dazu folgende Bedingung: Ist $\sigma(\alpha)$ gegeben, so kennt man $\sigma(-\alpha) = -\sigma(\alpha)$, also folgt für β die Einschränkung

$$\sigma(\beta) \in \{\alpha, \beta, -\alpha, -\beta\} \setminus \{\sigma(\alpha), -\sigma(\alpha)\}.$$

Für jedes α gibt es also höchstens zwei Möglichkeiten für $\sigma(\beta)$. Wir erhalten also 8 Möglichkeiten. Welche davon zu Automorphismen gehören, muss noch bestimmt werden. (Mit $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = (\alpha, \beta, -\alpha, -\beta)$ schreiben wir rechts die Zykelzerlegung der Indizes an.)

(1) **Falls $\sigma(\alpha) = \alpha$, $\sigma(\beta) = \beta$:**

$$\pi(\sigma) = \begin{pmatrix} \alpha & \beta & -\alpha & -\beta \\ \alpha & \beta & -\alpha & -\beta \end{pmatrix} \simeq (1).$$

(2) **Falls $\sigma(\alpha) = \alpha$, $\sigma(\beta) = -\beta$:**

$$\pi(\sigma) = \begin{pmatrix} \alpha & \beta & -\alpha & -\beta \\ \alpha & -\beta & -\alpha & \beta \end{pmatrix} \simeq (24).$$

(3) **Falls $\sigma(\alpha) = -\alpha$, $\sigma(\beta) = \beta$:**

$$\pi(\sigma) = \begin{pmatrix} \alpha & \beta & -\alpha & -\beta \\ -\alpha & \beta & \alpha & -\beta \end{pmatrix} \simeq (13).$$

(4) **Falls $\sigma(\alpha) = -\alpha$, $\sigma(\beta) = -\beta$:**

$$\pi(\sigma) = \begin{pmatrix} \alpha & \beta & -\alpha & -\beta \\ -\alpha & -\beta & \alpha & \beta \end{pmatrix} \simeq (13)(24).$$

(5) **Falls $\sigma(\alpha) = \beta$, $\sigma(\beta) = \alpha$:**

$$\pi(\sigma) = \begin{pmatrix} \alpha & \beta & -\alpha & -\beta \\ \beta & \alpha & -\beta & -\alpha \end{pmatrix} \simeq (12)(34).$$

(6) **Falls $\sigma(\alpha) = \beta$, $\sigma(\beta) = -\alpha$:**

$$\pi(\sigma) = \begin{pmatrix} \alpha & \beta & -\alpha & -\beta \\ \beta & -\alpha & -\beta & \alpha \end{pmatrix} \simeq (1234).$$

(7) **Falls $\sigma(\alpha) = -\beta$, $\sigma(\beta) = \alpha$:**

$$\pi(\sigma) = \begin{pmatrix} \alpha & \beta & -\alpha & -\beta \\ -\beta & \alpha & \beta & -\alpha \end{pmatrix} \simeq (1432).$$

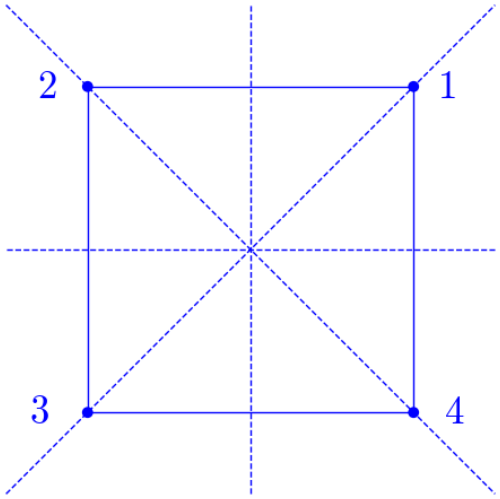
(8) **Falls $\sigma(\alpha) = -\beta$, $\sigma(\beta) = -\alpha$:**

$$\pi(\sigma) = \begin{pmatrix} \alpha & \beta & -\alpha & -\beta \\ -\beta & -\alpha & \beta & \alpha \end{pmatrix} \simeq (14)(23).$$

Die 8 Permutationen bilden eine Untergruppe von S_4 mit 8 Elementen, eine Diedergruppe D_8:

$$D_8 = \{(1), (24), (13), (13)(24), (12)(34), (1234), (1432), (14)(23)\}.$$

D_8 kann als Symmetriegruppe eines Quadrats interpretiert werden:



- Drehungen
  - Drehung um 0^0: (1)
  - Drehung um 90^0: (1234)
  - Drehung um 180^0: (13)(24)
  - Drehung um 90^0: (1432)
- Spiegelung an den Diagonalen
  - (13)
  - (24)
- Spiegelung an den Geraden durch die Mitten gegenüberliegender Seiten
  - (12)(34)
  - (14)(23)

Wir bestimmen nun die transitiven Untergruppen. Dazu genügt es die Untergruppen der Ordnung 4 zu bestimmen. (Beachte: Das Produkt zweier Spiegelungen, deren Achsen den Winkel φ einschließen, ist eine Drehung um den Winkel 2φ.)

- $\langle(1234)\rangle$: Dies sind die 4 Drehungen. Die Gruppe ist zyklisch.
- $\{(1), (13), (24), (13)(24)\}$. Dies Gruppe hat zwar 4 Elemente, ist aber keine transitive Untergruppe.
- $\{(1), (12)(34), (13)(24), (14)(23)\}$. Dies ist eine transitive Untergruppe, die isomorph zu $Z_2 \times Z_2$ ist.

Wir stellen nochmals die drei transitiven Untergruppen zusammen, wobei wir auch vorausschauend das Verhalten von $\alpha\beta$ und $\frac{\alpha}{\beta} - \frac{\beta}{\alpha}$ einbeziehen:

Die Diedergruppe D_8:

σ	$\sigma(\alpha)$	$\sigma(\beta)$	$\sigma(-\alpha)$	$\sigma(-\beta)$	$\pi(\sigma)$	$\frac{\sigma(\alpha\beta)}{\alpha\beta}$	$\frac{\sigma(\frac{\alpha}{\beta}-\frac{\beta}{\alpha})}{\frac{\alpha}{\beta}-\frac{\beta}{\alpha}}$
σ_1	α	β	$-\alpha$	$-\beta$	(1)	1	1
σ_2	α	$-\beta$	$-\alpha$	β	(24)	-1	-1
σ_3	$-\alpha$	β	α	$-\beta$	(13)	-1	-1
σ_4	$-\alpha$	$-\beta$	α	β	(13)(24)	1	1
σ_5	β	α	$-\beta$	$-\alpha$	(12)(34)	1	-1
σ_6	β	$-\alpha$	$-\beta$	α	(1234)	-1	1
σ_7	$-\beta$	α	β	$-\alpha$	(1432)	-1	1
σ_8	$-\beta$	$-\alpha$	β	α	(14)(23)	1	-1

Die zyklische Gruppe $\langle(1234)\rangle \simeq Z_4$:

σ	$\sigma(\alpha)$	$\sigma(\beta)$	$\sigma(-\alpha)$	$\sigma(-\beta)$	$\pi(\sigma)$	$\frac{\sigma(\alpha\beta)}{\alpha\beta}$	$\frac{\sigma(\frac{\alpha}{\beta}-\frac{\beta}{\alpha})}{\frac{\alpha}{\beta}-\frac{\beta}{\alpha}}$
σ_1	α	β	$-\alpha$	$-\beta$	(1)	1	1
σ_4	$-\alpha$	$-\beta$	α	β	(13)(24)	1	1
σ_6	β	$-\alpha$	$-\beta$	α	(1234)	-1	1
σ_7	$-\beta$	α	β	$-\alpha$	(1432)	-1	1

Die Untergruppe $\{(1), (12)(34), (13)(24), (14)(23)\} \simeq Z_2 \times Z_2$:

σ	$\sigma(\alpha)$	$\sigma(\beta)$	$\sigma(-\alpha)$	$\sigma(-\beta)$	$\pi(\sigma)$	$\frac{\sigma(\alpha\beta)}{\alpha\beta}$	$\frac{\sigma(\frac{\alpha}{\beta}-\frac{\beta}{\alpha})}{\frac{\alpha}{\beta}-\frac{\beta}{\alpha}}$
σ_1	α	β	$-\alpha$	$-\beta$	(1)	1	1
σ_4	$-\alpha$	$-\beta$	α	β	(13)(24)	1	1
σ_5	β	α	$-\beta$	$-\alpha$	(12)(34)	1	-1
σ_8	$-\beta$	$-\alpha$	β	α	(14)(23)	1	-1

Wir kommen $\alpha\beta$ und $\frac{\alpha}{\beta} - \frac{\beta}{\alpha}$ ins Spiel? Aus

$$x^4 + ax^2 + b = (x-\alpha)(x+\alpha)(x-\beta)(x+\beta) = (x^2-\alpha^2)(x^2-\beta^2) = x^4 - (\alpha^2+\beta^2)x^2 + \alpha^2\beta^2$$

folgt

$$\alpha^2 + \beta^2 = -a, \quad \alpha^2\beta^2 = b.$$

Damit erhält man

$$(\alpha\beta)^2 = b$$

und weiter:

$$\begin{aligned}(\frac{\alpha}{\beta} - \frac{\beta}{\alpha})^2 &= (\frac{\alpha^2-\beta^2}{\alpha\beta})^2 = \frac{\alpha^4 - 2\alpha^2\beta^2 + \beta^4}{\alpha^2\beta^2} = \frac{\alpha^4 + 2\alpha^2\beta^2 + \beta^4 - 4\alpha^2\beta^2}{\alpha^2\beta^2} = \\ &= \frac{(\alpha^2+\beta^2)^2 - 4\alpha^2\beta^2}{\alpha^2\beta^2} = \frac{a^2-4b}{b}\end{aligned}$$

Wir erhalten folgenden Satz:

SATZ. *Sei K ein Körper und $f = x^4 + ax^2 + b \in K[x]$ ein irreduzibles Polynom, sodass* $\operatorname{disc}(f) = 16b(a^2-4b)^2 \neq 0$ *ist.*

(1) *Es ist $a^2 - 4b \in K^* \setminus K^{*2}$.*
(2) *Es gibt drei Fälle:*
   - **Fall $b \in K^{*2}$:** *Dann ist*

$$\operatorname{Gal}(f|K) \simeq Z_2 \times Z_2.$$

Die quadratischen Teilkörper von $K(\alpha)$ sind

$$K(\sqrt{a^2-4b}), \quad K(\sqrt{-a+2\sqrt{b}}), \quad K(\sqrt{-a-2\sqrt{b}}).$$

- **Fall** $\frac{a^2-4b}{b} \in K^{*2}$**:** *Dann ist*

$$\mathrm{Gal}(f|K) \simeq Z_4.$$

- **Fall** $b \in K^* \setminus K^{*2}$ **und** $\frac{a^2-b}{b} \in K^* \setminus K^{*2}$**:** *Dann ist*

$$\mathrm{Gal}(f|\mathbb{Q}) \simeq D_8.$$

Beispiele:

(1) Die reellen Zahlen $\alpha = \sqrt{5+2\sqrt{6}}$ und $\beta = \sqrt{5-2\sqrt{6}}$ haben beide das Minimalpolynom $f = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$. Mit $a = -10$, $b = 1$ gilt

$$b = 1 \in \mathbb{Q}^{*2}, \quad \frac{a^2-4b}{b} = 96 \notin \mathbb{Q}^{*2}.$$

Daher gilt

$$\mathrm{Gal}(\mathbb{Q}(\alpha,\beta)|\mathbb{Q}) \simeq Z_2 \times Z_2.$$

Es gilt

$$\sqrt{5+2\sqrt{6}} = \sqrt{2}+\sqrt{3} \quad \text{und} \quad \sqrt{5-2\sqrt{6}} = \sqrt{3}-\sqrt{2}.$$

Die quadratischen Zwischenkörper sind also $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{6})$.

(2) Wir betrachten die reellen Zahlen $\alpha = \sqrt{10+\sqrt{10}}$ und $\beta = \sqrt{10-\sqrt{10}}$. Sie haben beide das Minimalpolynom $f = x^4 - 20x^2 + 90 \in \mathbb{Q}[x]$. Mit $a = -20$, $b = 90$ gilt

$$b \notin \mathbb{Q}^{*2}, \quad \frac{a^2-4b}{b} = \frac{4}{9} \in \mathbb{Q}^{*2}.$$

Also gilt

$$\mathrm{Gal}(\mathbb{Q}(\alpha,\beta)|\mathbb{Q}) \simeq Z_4.$$

(3) Wir haben zuvor die reellen Zahlen $\alpha = \sqrt{3+\sqrt{3}}$ und $\beta = \sqrt{3-\sqrt{3}}$ betrachtet, die beide das Minimalpolynom $f = x^4 - 6x^2 + 6$ haben. f ist irreduzibel und mit $a = -6$, $b = 6$ gilt

$$b = 6 \notin \mathbb{Q}^{*2}, \quad \frac{a^2-4b}{b} = 2 \notin \mathbb{Q}^{*2}.$$

Also gilt

$$\mathrm{Gal}(\mathbb{Q}(\alpha,\beta)|\mathbb{Q}) \simeq D_8.$$

6. „Incredible Identities“

Auf Shanks geht folgendes Beispiel zurück: Betrachtet man die reellen Zahlen

$$A = \sqrt{5}+\sqrt{22+2\sqrt{5}} \quad \text{und} \quad B = \sqrt{11+2\sqrt{29}}+\sqrt{16-2\sqrt{29}+2\sqrt{55-10\sqrt{29}}},$$

so stellt man fest, dass sie numerisch (mindestens) sehr nahe beieinander liegen. Shanks skizziert dann, dass die Zahlen gleich sind, und nennt dies eine „incredible identity“. Man kann dies zeigen und weitere solcher Identitäten herleiten, wenn man sich mit Gleichungen 4. Grades intensiver beschäftigt.

7. Polynome vom Grad p

Satz. *Sei p eine Primzahl und $f \in \mathbb{Q}[x]$ ein irreduzibles normiertes Polynom vom Grad p mit $p-2$ reellen und 2 nichtreellen komplexen Nullstellen. Dann gilt*

$$\mathrm{Gal}(f|\mathbb{Q}) \simeq S_p.$$

8. Das Umkehrproblem der Galoistheorie

Welche Gruppen treten als Galoisgruppen von endlichen Galoiserweiterungen von $\mathbb{Q}$ auf?

Beispiele:

- Wir haben an Beispielen gesehen, dass die Gruppen $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$, S_3 als Galoisgruppen über $\mathbb{Q}$ vorkommen.
- Ist ζ_n eine primitive n-te Einheitswurzel, so gilt
$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \simeq \mathbb{Z}_n^*.$$
Die Erweiterung $\mathbb{Q}(\zeta_n)|\mathbb{Q}$ ist also sogar abelsch.
- Mit (2) kann man zeigen, dass jede endliche abelsche Gruppe als Galoisgruppe über $\mathbb{Q}$ auftritt.

Der folgende Satz unterstreicht die Wichtigkeit der Kreisteilungskörper:

Satz (Kronecker-Weber). *Ist $K|\mathbb{Q}$ eine endliche Galoiserweiterung mit abelschen Galoisgruppe, so gibt es eine Einheitswurzel ζ_n mit*
$$K \subseteq \mathbb{Q}(\zeta_n).$$

Bisher ungelöst ist folgende Vermutung:

Vermutung (Umkehrproblem der Galoistheorie): Ist G eine endliche Gruppe, so gibt es eine Galoiserweiterung $K|\mathbb{Q}$ mit
$$\mathrm{Gal}(K|\mathbb{Q}) \simeq G.$$