WS 08/09 Algebra 1 Musterlösung Blatt 9:

3. Aufgabe:

(b) Beachte zuerst folgendes **Lemma**: Seien f,g (in unserem Fall normierte, gilt aber allgemein) Polynome:

$$f = \prod_{i=1}^{n}(X-\alpha_i) \qquad g = \prod_{i=1}^{m}(X-\beta_i)$$

$$\Longrightarrow g(\alpha_j) = \prod_{i=1}^{m}(\alpha_j - \beta_i)$$

$$\Longrightarrow \prod_{j=1}^{n} g(\alpha_j) = \prod_{\substack{1\le i\le n\\ 1\le j\le m}}(\alpha_j-\beta_i) \overset{Blatt8Aufgabe2}{=} Res(f,g)$$

Setze nun $g(x) = f'(x)$

$$f'(X) = \Big(\prod_{i=1}^{n}(X-\alpha_i)\Big)' = \sum_{i=1}^{n}\prod_{j\neq i}(X-\alpha_j)$$

$$\Longrightarrow \prod_{k=1}^{n} f'(\alpha_k) = \prod_{k=1}^{n}\sum_{i=1}^{n}\underbrace{\prod_{j\neq i}(\alpha_k-\alpha_j)}_{=0 \text{ für } i\neq k} = \prod_{k=1}^{n}\prod_{j\neq k}(\alpha_k-\alpha_j) = \prod_{1\le j<k\le n}(\alpha_j-\alpha_k) * \prod_{1\le j<k\le n}(-1)(\alpha_j-\alpha_k)$$

$$= (-1)^{n(n-1)/2}\prod_{1\le j<k\le n}(\alpha_j-\alpha_k)^2 = D(f)$$

(a) Da $\mathrm{Res}(f,g') \in K$ nach Def. gilt auch $D(f) \in K$.

(c) Sei $\tau_{i,j} \in S_n$ die Transposition, die α_i mit α_j vertauscht (oBdA $i<j$). Für $\sigma \in S_n$ definiere:

$$\sigma\Big(\prod_{1\le k<l\le n}(\alpha_k-\alpha_l)\Big) := \prod_{1\le k<l\le n}(\sigma(\alpha_k)-\sigma(\alpha_l))$$

Dies ist nur formal so definiert, stimmt aber für $\sigma \in Gal(f,K)$ mit dem entsprechenden Körperautomorphismus überein. Betrachte nun:

$$\tau_{i,j}\Big(\prod_{1\le k<l\le n}(\alpha_k-\alpha_l)\Big) = -\prod_{1\le k<l\le n}(\alpha_k-\alpha_l)$$

denn für $i=k, j=l$ ist $(\tau_{i,j}(\alpha_k)-\tau_{i,j}(\alpha_l) = -(\alpha_k-\alpha_l)$, alle anderen Elemente werden nur umsortiert. Die Operation ist aber Veträglich mit der Gruppenstruktur der S_n und damit gilt für $\sigma \in Gal(f,K)$:

$$\sigma\Big(\prod_{1\le k<l\le n}(\alpha_k-\alpha_l)\Big) = \mathrm{sign}(\sigma)\Big(\prod_{1\le k<l\le n}(\alpha_k-\alpha_l)\Big)$$

Nun gilt (für char(K) $\neq 2$):

$$\begin{aligned}
D(f)\in K^2 &\Longleftrightarrow \prod_{1\le k<l\le n}(\alpha_k-\alpha_l)\in K\\
&\Longleftrightarrow \forall\sigma\in Gal(f,K): \sigma\Big(\prod_{1\le k<l\le n}(\alpha_k-\alpha_l)\Big) = \prod_{1\le k<l\le n}(\alpha_k-\alpha_l) = \mathrm{sign}(\sigma)\Big(\prod_{1\le k<l\le n}(\alpha_k-\alpha_l)\Big)\\
&\Longleftrightarrow \forall\sigma\in Gal(f,K): sign(\sigma)=1\\
&\Longleftrightarrow Gal(f,k)\subseteq A_n
\end{aligned}$$

(d) Die Diskriminante von $f = X^6 - 1536X - 5120$ berechnet sich über die Resultantenformel zu $20519525802206822400000 0 = 2^{54}\cdot 3^6\cdot 5^6 \in \mathbb{Q}^2$.

$$\Longrightarrow Gal(f,K)\subseteq A_6$$

4. Aufgabe:

(a) $Q(X) = (X - z_1)(X - z_2)(X - z_3) = X^3 - (z_1 + z_2 + z_3)X^2 + (z_1z_2 + z_1z_3 + z_2z_3)X - z_1z_2z_3$. Da die Galoisgruppe die Nullstellen permutiert permutiert sie offenbar die z_i. Da die Koeffizienten von $Q(X)$ symmetrisch in den z_i sind, sieht man hier schon dass $Q(X) \in K[X]$. Setze $b_1 = z_1 + z_2 + z_3, b_2 = z_1z_2 + z_1z_3 + z_2z_3, b_3 = z_1z_2z_3$. Die Koeffizienten des Polynoms f sind die Elementarsymmetrischen Funktionen in den x_i:

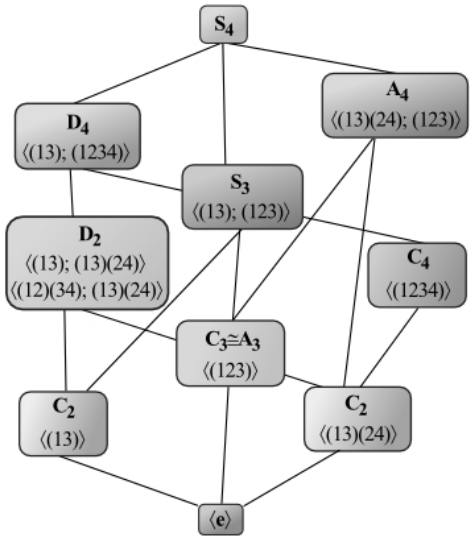
$$\begin{aligned}
\sigma_1 &= \sum_{i=1}^{4} x_i && = 0 \\
\sigma_2 &= \sum_{i<j} x_ix_j && = p \\
\sigma_3 &= \sum_{i<j<k} x_ix_jx_k && = q \\
\sigma_4 &= x_1x_2x_3x_4 && = r
\end{aligned}$$

Ausmultiplizieren zeigt:

$$\begin{aligned}
b_1 &= 2\sigma_2 = 2p \\
b_2 &= \sigma_2^2 + \sigma_1\sigma_3 - 4\sigma_4 = p^2 - 4r \\
b_3 &= \sigma_1\sigma_2\sigma_3 - \sigma_1^2\sigma_4 - \sigma_3^2 = -q^2
\end{aligned}$$

(b) Jeder der 3 Diedergruppen in der S_4 lässt eines der z_i fest, so ist z.B. $z_2 = (x_1 + x_3)(x_2 + x_4)$ invariant unter $\{(13), (24), (13)(24), (1234), (1423), (12)(34), (14)(23)\}$. Dies zeigt "$\Rightarrow$"
Zu "$\Leftarrow$"
Sei $Q(X)$ irreduzibel also oBdA $Q(z_2) = 0$. $S_4 = D_4 \cup (123)D_4 \cup (132)D_4$. Wir wissen z_2 ist invariant unter D_4 (der obigen). aber $(123)z_2 = z_1, (132)z_2 = z_3$. Sei $\sigma \notin D_4$ also oBdA $\sigma \in (123)D_4$. Dann gilt $\sigma(z_2) = z_1 = z_2$ da ja $z_2 \in K$. Somit gilt:
$0 = z_1 - z_2 = (x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 - x_1x_2 - x_1x_4 - x_2x_3 - x_3x_4) =$
$(x_1x_3 + x_2x_4 - x_1x_2 - x_3x_4) = (x_1 - x_4)(x_3 - x_2)$
Dies ist aber ein Widerspruch zu f seperabel.

(c) Wir wissen das die S_4 als Galoisgruppe eines Zerfällungskörpers eines Polynoms 4. Grades vorkommt. Ein Algemeines normiertes Polynom 4. Grades hat die Form: $g(X) = X^4 + aX^3 + bX^2 + cX + d$. Betrachte nun $f(X) = g(X - \frac{a}{4}) = X^4 + pX^2 + qX + r$. Seien $\alpha_1, ..., \alpha_4$ die Nullstellen von g, dann sind $\alpha_1 + \frac{a}{4} = \beta_1, ..., \alpha_4 + \frac{a}{4} = \beta_4$ die Nullstellen von f. Also gilt $K[\alpha_1, ..., \alpha_4] = K[\beta_1, ..., \beta_4] \implies \#Gal(f, K) = \#Gal(g, K)$. Somit kommt jede Gruppe als Galoisgruppe infrage, zu der es ein irreduzibles Polynom gibt. Dies sind genau alle Transitiv operierenden Gruppen. Betrachte alle Untergruppen der S_4:



Die A_4 operiert offenbar transitiv (Doppeltranspositionen), die D_4 auch (siehe D_4 oben). Letztendlich ist die zyklische Gruppe der Ordnung 4 auch transitiv. (3 mal enthalten erzeugt von $(1234), (1324), (1342)$). Man sieht schnell ein, dass S_3, A_3, D_2, die zyklischen Gruppen der Ordnung 2,3 nicht transitiv operieren. Die V_4 operiert transitiv in der Gestalt
$V_4 = \{id, (12)(34), (13)(24), (14)(23)\}$ als Normalteiler der A_4, in den anderen Einbettungen nicht ($V_4 = \{id, (12), (34), (12)(34)\}$). Die S_4 selbst ist natürlich transitiv, die Identität öffenbar nicht. Die 8 transitiven Gruppen sind also: $S_4, A_4, V_4, 3 \cdot D_4, 3 \cdot \mathbb{Z}/4\mathbb{Z}$. Die größte Gruppe, in der alle anderen enthalten sind ist offenbar die S_4, weiterhin ist je eine der zyklischen Gruppen in einer Diedergruppe enthalten, die V_4 in der A_4.