1 Final remarks II

Definition 1 (Resolvent invariant)**.** Let $G \leqslant S_n$ and $P \in K[x_1, \ldots, x_n]$. Then P is *resolvent invariant* for G if $P^g = P \iff g \in G$.

Lemma 1.1. Let P be resolvent invariant for G. Then

1. $P^a = P^b \iff ab^{-1} \in G$ (obvious: $P^a = P^b \iff P^{ab^{-1}} = P$)
2. P^a is resolvent invariant for $a^{-1}Ga$

Corollary 1. Let $S_n = \sqcup_j a_j G$. Then P is resolvent invariant for $G \iff P^{a_j}$ are distinct.

Definition 2 (Resolvent)**.** Let P be a resolvent polynomial for $G \leqslant S_n$ and $S_n = \sqcup_{j=1}^{s} a_j G$. Then

$$R_G(z) = R_G(z, x_1, \ldots, x_n) = (z - P^{a_1}) \cdots (z - P^{a_s})$$

is a *resolvent* for G (depends on P).

Lemma 1.2. Let $G \leqslant S_n$, $f \in K[t]$ be a separable polynomial. If $\mathrm{Gal}_K(f) \leqslant G$ (and its conjugation), then $\exists \jmath \in K$ such that $R_{G,f}(\jmath) = 0$

Lemma 1.3. Let $|K| = \infty$ and $f \in K[t]$ be a separable polynomial. Then $\exists c_1, \ldots, c_n \in K$ such that for all k,

$$h_k(x_1, \ldots, x_k) = c_1 x_1 + \cdots + c_k x_k$$

has the property

$$h_k^a(\alpha_1, \ldots, \alpha_k) = h_k^b(\alpha_1, \ldots, \alpha_k) \iff x_i^a = x_i^b \mathrm{for} i = 1, \ldots, k,$$

where $a, b \in S_n$ are any permutations.

Theorem 1.4. Let $|K| = \infty$, $f \in K[t]$ be a separable polynomial, and $G \leqslant S_n$. Then there exists a resultant $R_{G,f}(z)$ with no multiple roots.

Theorem 1.5. Let $|K| = \infty$ and $f \in K[t]$ be irreducible and separable with $\deg f = 4$. Then

1. $\sqrt{D} \notin K$ and $R_{V_4}^{(f)}$ has no roots in $K \implies G \cong S_4$ or $G \cong Z_4$
2. $\sqrt{D} \in K$ and $R_{V_4}^{(f)}$ has no roots in $K \implies G \cong A_4$
3. $\sqrt{D} \in K$ and $R_{V_4}^{(f)}$ has a roots in $K \implies G \cong V_4$
4. $\sqrt{D} \notin K$ and $R_{V_4}^{(f)}$ has no roots in $K \implies G \cong S_4$ or $G \cong D_4$

Exercise, the point is to show that computing each $R_{V_4,D_4,Z_4,A_4}^{(f)}$ is not necessary