HOMEWORK 7
SOLUTIONS

Problem 1 [14.6.35] Prove that the discriminant D of the polynomial $x^n + px + q$ is given by

$$(-1)^{n(n-1)/2} n^n q^{n-1} + (-1)^{(n-1)(n-2)/2} (n-1)^{n-1} p^n.$$

Proof. Let $\alpha_1, \ldots, \alpha_n$ be the roots of $f(x) = x^n + px + q$. Recall the following identity (obtained by taking the derivative of $\log f(x) = \sum_{i=1}^n \log(x - \alpha_i)$)

$$\frac{f'(x)}{f(x)} = \sum_{i=1} \frac{1}{x - \alpha_i} \Longrightarrow f'(\alpha_j) = \prod_{\substack{i=1 \\ i \neq j}}^{n} (\alpha_j - \alpha_i).$$

This implies that

$$D = \prod_{i<j} (\alpha_i - \alpha_j)^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j} (\alpha_i - \alpha_j) = (-1)^{\frac{n(n-1)}{2}} \prod_{k=1}^{n} f'(\alpha_k).$$

Note that

$$f'(\alpha_i) = n{\alpha_i}^{n-1} + p = n(\frac{-p\alpha_i - q}{\alpha_i}) + p = -(n-1)p - \frac{nq}{\alpha_i}.$$

Hence

$$\begin{aligned}
D &= (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} (-(n-1)p - \frac{nq}{\alpha_i}) \\
&= (-1)^{\frac{n(n-1)}{2}} \frac{(n-1)^n p^n}{\prod \alpha_i} \prod_{i=1}^{n} (-\frac{nq}{(n-1)p} - \alpha_i) \\
&= (-1)^{\frac{n(n-1)}{2}} \frac{(n-1)^n p^n}{(-1)^n q} f(-\frac{nq}{(n-1)p}) \\
&= (-1)^{\frac{n(n-1)}{2}} \frac{(n-1)^n p^n}{(-1)^n q} ((-\frac{nq}{(n-1)p})^n + p(-\frac{nq}{(n-1)p}) + q) \\
&= (-1)^{\frac{n(n-1)}{2}} n^n q^{n-1} + (-1)^{\frac{(n-1)(n-2)}{2}} (n-1)^{n-1} p^n.
\end{aligned}$$

□

Problem 2 [14.6.43] Express each of the following in terms of the elementary symmetric functions:

(a) $A := \sum_{i \neq j} x_i^2 x_j$.

(b) $B := \sum_{i,j,k \text{ distinct}} x_i^2 x_j x_k$.

(c) $C := \sum_{i,j,k \text{ distinct}} x_i^2 x_j^2 x_k^2$.

Solution. (a) Note that

$$\begin{aligned} s_1 s_2 &= (\sum_{i=1}^{n} x_i)(\sum_{j<k} x_j x_k) = \sum_{j<k} \sum_{i=1}^{n} x_i x_j x_k \\ &= \sum_{j<k} (x_j^2 x_k + x_j x_k^2 + \sum_{i \neq j,k} x_i x_j x_k) \\ &= \sum_{j \neq k} x_j^2 x_k + 3 \sum_{i<j<k} x_i x_j x_k = A + 3 s_3. \end{aligned}$$

Hence $A = s_1 s_2 - 3 s_3$.

(b) Similarly,

$$\begin{aligned} s_1 s_3 &= (\sum_{t=1}^{n} x_t)(\sum_{i<j<k} x_i x_j x_k) = \sum_{i<j<k} \sum_{t=1}^{n} x_t x_i x_j x_k \\ &= \sum_{i<j<k} \Big((x_i^2 x_j x_k + x_i x_j^2 x_k + x_i x_j x_k^2) + \sum_{t \neq i,j,k} x_t x_i x_j x_k \Big) \\ &= \frac{B}{2} + 4 s_4. \end{aligned}$$

Thus $B = 2 s_1 s_3 - 8 s_4$.

(c) We have,

$$\begin{aligned} s_3^2 &= (\sum_{i<j<k} x_i x_j x_k)^2 \\ &= \sum_{i<j<k} x_i^2 x_j^2 x_k^2 + \frac{1}{2} \sum_{\substack{i,j,k,l \\ \text{distinct}}} x_i^2 x_j^2 x_k x_l + \frac{1}{4} \sum_{\substack{i,j,k,l,m \\ \text{distinct}}} x_i^2 x_j x_k x_l x_m + \frac{1}{36} \sum_{\substack{i,j,k,l,m,n \\ \text{distinct}}} x_i x_j x_k x_l x_m x_n \\ &= \frac{C}{6} + \frac{1}{2} \sum_{\substack{i,j,k,l \\ \text{distinct}}} x_i^2 x_j^2 x_k x_l + \frac{1}{4} \sum_{\substack{i,j,k,l,m \\ \text{distinct}}} x_i^2 x_j x_k x_l x_m + 20 s_6. \end{aligned}$$

In addition,

$$\begin{aligned} s_1 s_5 &= (\sum_{i=1}^{n} x_i)(\sum_{j<k<l<m<n} x_j x_k x_l x_m x_n) = \sum_{j<k<l<m<n} \sum_{i=1}^{n} x_i x_j x_k x_l x_m x_n \\ &= \frac{1}{4!} \sum_{\substack{i,j,k,l,m \\ \text{distinct}}} x_i^2 x_j x_k x_l x_m + 6 \sum_{i<j<k<l<m<n} x_i x_j x_k x_l x_m x_n \\ &= \frac{1}{24} \sum_{\substack{i,j,k,l,m \\ \text{distinct}}} x_i^2 x_j x_k x_l x_m + 6 s_6 \end{aligned}$$

and thus

$$\begin{aligned} s_2 s_4 &= (\sum_{i<j} x_i x_j)(\sum_{k<l<m<n} x_k x_l x_m x_n) \\ &= \frac{1}{4} \sum_{\substack{i,j,k,l \\ \text{distinct}}} x_i^2 x_j^2 x_k x_l + \frac{1}{6} \sum_{\substack{i,j,k,l,m \\ \text{distinct}}} x_i^2 x_j x_k x_l x_m + 15 \sum_{i<j<k<l<m<n} x_i x_j x_k x_l x_m x_n \\ &= \frac{1}{4} \sum_{\substack{i,j,k,l \\ \text{distinct}}} x_i^2 x_j^2 x_k x_l + 4(s_1 s_5 - 6 s_6) + 15 s_6 \\ &= \frac{1}{4} \sum_{\substack{i,j,k,l \\ \text{distinct}}} x_i^2 x_j^2 x_k x_l + 4 s_1 s_5 - 9 s_6. \end{aligned}$$

Consequently,

$$\begin{aligned} s_3^2 &= \frac{C}{6} + (2 s_2 s_4 - 8 s_1 s_5 + 18 s_6) + (6 s_1 s_5 - 36 s_6) + 20 s_6 \\ &= \frac{C}{6} + 2 s_2 s_4 - 2 s_1 s_5 + 2 s_6 \end{aligned}$$

showing that $C = 6(s_3^2 - 2 s_2 s_4 + 2 s_1 s_5 - 2 s_6)$.

□

Problem 3 [14.6.50] Suppose K is a field and $f(x) = x^3 + ax^2 + bx + c \in K[x]$ is irreducible, so the Galois group of $f(x)$ over K is either S_3 or A_3.

(a) Show that the Galois group of $f(x)$ is A_3 if and only if the resultant quadratic polynomial $g(x) = x^2 + (ab - 3c)x + (b^3 + a^3 c - 6abc + 9c^2)$ has a root in K.

(b) If $ch(k) \neq 2$ show that the Galois group is A_3 iff the discriminant of $f(x)$ is a square in K.

(c) If $ch(k) = 2$ show that the discriminant of $f(x)$ is always a square. Show that $f(x)$ can be taken to be of the form $x^3 + px + q$ and that the Galois group of $f(x)$ is A_3 iff the quadratic $x^2 + qx + (p^3 + q^2)$ has a root in K.

Proof. (a) Let G be the Galois group of f over K.

($\Longrightarrow$) Assume that $G = A_3$. Then G is composed of the following elements

$$\sigma_1 : \begin{cases} \alpha \mapsto \alpha \\ \beta \mapsto \beta \\ \gamma \mapsto \gamma \end{cases} \quad \sigma_2 : \begin{cases} \alpha \mapsto \beta \\ \beta \mapsto \gamma \\ \gamma \mapsto \alpha \end{cases} \quad \sigma_3 : \begin{cases} \alpha \mapsto \gamma \\ \beta \mapsto \alpha \\ \gamma \mapsto \beta \end{cases} .$$

Let $\theta_1 = \alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2$ and $\theta_2 = \alpha^2\beta + \beta^2\gamma + \gamma^2\alpha$. Since $\alpha + \beta + \gamma = -a$, $\alpha\beta + \beta\gamma + \gamma\alpha = b$ and $\alpha\beta\gamma = -c$, some straightforward computations show that $\theta_1 + \theta_2 = 3c - ab$ and $\theta_1\theta_2 = b^3 + a^3c - 6abc + 9c^2$, so θ_1 and θ_2 are the roots of g.

Now it is easy to check that σ_i $(1 \le i \le 3)$ fixes θ_j $(1 \le j \le 2)$. In particular, this implies that g has a root in K.

($\Longleftarrow$) Conversely, assume that g has a root in K, say $\theta_1 \in K$. If $G = S_3$ then G contains the element

$$\sigma : \begin{cases} \alpha \mapsto \beta \\ \beta \mapsto \alpha \\ \gamma \mapsto \gamma. \end{cases}$$

This means that $\sigma(\theta_1) = \theta_2$, and since σ fixes K we must have $\theta_1 = \theta_2$. However, $\theta_2 - \theta_1 = (\alpha - \beta)(\beta - \gamma)(\gamma - \alpha) \neq 0$, since α, β, γ are all distinct (f is irreducible). This is a contraction, so $G = A_3$.

Finally, in view of the usual discriminant formula for a quadratic and (14.18') we see that

$$D(g) = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc = D(f).$$

(b) Let Δ be the discriminant of g. By (a) we infer that $G = A_3$ iff $\frac{1}{2}[(3c - ab) \pm \sqrt{\Delta}] \in K$, which is equivalent to saying that Δ is a square in K. Since Δ is also the discriminant of f, the conclusion follows.

(c) If $char(K) = 2$ then $D = (ab - c)^2$ is always a square in K. As shown on page 611, f can be written in the form $x^3 + px + q$, where $p = b - \frac{a^2}{3}$ and $q = \frac{1}{27}(2a^3 - 9ab + 27c)$. In characteristic 2, it is not hard to see that the resultant polynomial becomes $g(x) = x^2 + qx + (p^3 + q^2)$ and by (a) we are done.

□

Problem 4. Determine the Galois groups of the following polynomials in $\mathbb{Q}[x]$: $x^4 - 25$, $x^4 + 4$, $x^4 + 2x^2 + x + 3$, $x^5 + x - 1$, $x^5 + 20x + 16$.

Solution.

- Let $f(x) = x^4 - 25$. Then $F = \mathbb{Q}(\sqrt{5}, i)$ is a splitting field of the separable polynomial f and $[F : \mathbb{Q}] = 4$. Thus, $Gal(F/\mathbb{Q}) = \mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Note that $Gal(F/\mathbb{Q})$ contains the following distinct elements of order two:

$$\phi : \begin{cases} \sqrt{5} \mapsto \sqrt{5} \\ i \mapsto -i \end{cases} \quad \text{and } \psi : \begin{cases} \sqrt{5} \mapsto -\sqrt{5} \\ i \mapsto i. \end{cases}$$

  Therefore, $Gal(F/\mathbb{Q})$ is the Klein four-group.

- Let $f(x) = x^4 + 4 = (x^2 - 2x + 2)(x^2 + 2x + 2)$. The roots of f are $\pm 1 \pm i$, so the splitting field is $\mathbb{Q}(i)$, which has degree 2 over $\mathbb{Q}$. Therefore, the Galois group of f is cyclic of order 2.

- Let $f(x) = x^4 + 2x^2 + x + 3$. Note that f is irreducible over $\mathbb{Q}$ and the discriminant $D = 3877$ is not a square. From the discussion on page 615 we infer that the Galois group of f is S_4.

- Let $f(x) = x^5 + x - 1 = (x^2 - x + 1)(x^3 + x^2 - 1) = f_1 f_2$. Clearly, the splitting field of f_1 is $K_1 = \mathbb{Q}(\sqrt{-3})$ and $Gal(K_1/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$. Now, since the discriminant of f_2 is -23 the remarks on page 613 imply that the splitting field of f_2 is $K_2 = \mathbb{Q}(\theta, \sqrt{-23})$ and $Gal(K_2/\mathbb{Q}) = S_3$ (for any one of the roots θ of f_2). By [13.4.6] we know that $K_1 K_2$ is the splitting field of f. It is easy to see that $K_1 \cap K_2 = \mathbb{Q}$ so by Proposition 21 we conclude that $Gal(K_1 K_2/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times S_3$.

- Let $f(x) = x^5 + 20x + 16$. Note that f has discriminant $2^{16}5^6$ (by Problem 1), which implies that its Galois group is a subgroup of A_5 (by Prop 34, Sec. 14.6). It is straightforward to check that f is irreducible modulo 3, so it is also irreducible over $\mathbb{Q}$ and thus the Galois group contains a 5-cycle. Modulo 7, $f(x)$ factors as

$$x^5 + 20x + 16 \equiv (x - 4)(x - 5)(x^3 + 2x^2 + 5x + 5) \pmod 7,$$

  showing that the Galois group also contains a 3-cycle. Since a 3-cycle and a 5-cycle generate all of A_5, it follows that the Galois group of $f(x)$ is A_5.

□

Problem 5. Let p be a prime. A finite extension of fields K/F is said to be a p-extension if $[K : F]$ is a power of p.

(a) Suppose K/F is a Galois p-extension and L/K is another Galois p-extension. Let E/L be any extension such that E/F is Galois. Show that there exists a Galois p-subextension E_p/K of E/K which is maximal among the Galois p-subextensions of E/K.

(b) Show that E_p/F is Galois and deduce that the Galois closure of L/F is a p-extension of F.

(c) Give an example of a p-extension K/F and a Galois p-extension L/K such that the Galois closure of L/F is not a p-extension of F.

Proof. (a) Since E/F is a Galois extension it follows that E/K is Galois (so finite) and thus there are only finitely many subfields of E that contain K. Let $\mathcal{S}$ be the set of all Galois p-subextensions E/K (clearly $\mathcal{S} \neq \emptyset$ because $L \in \mathcal{S}$). By the above $\mathcal{S}$ is finite, so we can write $\mathcal{S} = \{E_1, \ldots, E_n\}$. Take E_p to be the the composite $E_p := E_1 E_2 \ldots E_n$.

By Prop.21 (Sec.14.4) E_p is Galois over K. Moreover, since $[E_i : K] = p^{a_i}$ for some $a_i \in \mathbb{N}$, we obtain that $[E_p : K] \mid p^{\sum_{i=1}^n a_i}$ (by Cor. 20, Sec. 14.4) and therefore E_p/K is a Galois p-subextension of E/K. By construction, any Galois p-subextension of E/K is a subextension of E_p/K, thus E_p/K is maximal among the Galois p-subexntesions of E/K.

(b) Let $\sigma \in Gal(E/F)$, it is enough to show that σ fixes E_p. Indeed, since K/F is Galois we have that $\sigma(K) = K$ and hence $\sigma(E_p)$ contains K. Moreover E_p and $\sigma(E_p)$ are naturally isomorphic, implying that $\sigma(E_p)/K$ is a Galois p-extension. Consider the composite $M = \sigma(E_p)E_p$, then (as

above) $[M : K] \mid [E_p : K][\sigma(E_p) : K]$ so M/K is a Galois p-extension. By maximality, we infer that $M = E_p$ and thus $\sigma(E_p) = E_p$.

Finally, note that $L \in \mathcal{S}$ so the Galois closure of L/F is a subextension of E_p/F, and hence a p-extension of F (by degree considerations).

(c) Take $F = \mathbb{Q}$, $K = L = \mathbb{Q}(\sqrt[3]{2})$. Then K/F is a 3-extension and L/K is trivially a Galois 3-extension. However, the Galois closure $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ of L is of degree 6 over F, which is not a power of 3.

□