1. Newton's recursion for the power sums. Fix $n \geqslant 1$ and variables $x_1, \ldots, x_n$. For any $m \geqslant 1$ the m-th power sum is $P_m = x_1^m + x_2^m + \cdots + x_n^m$. Since P_m is a symmetric polynomial Newton's theorem tells us we may express P_m in terms of the elementary symmetric polynomials $e_1, \ldots, e_n$. A recursive formula, also due to Newton, gives a quick way to do this.

For purposes of the recursion we will use the symbol e_r for all $r \geqslant 1$, with the convention that $e_r = 0$ if $r > n$. We also set $P_0 = 1$, contrary to the formula for $m \geqslant 1$. Newton's recursion is

$$P_m = e_1 P_{m-1} - e_2 P_{m-2} + e_3 P_{m-3} - \cdots - (-1)^{m-1} e_{m-1} P_1 - (-1)^m m e_m P_0.$$

(Don't miss the factor of m in the final term.) Starting with $P_1 = e_1$, this tells us how to express the power sums in terms of the elementary symmetric polynomials. E.g., when $n = 2$ we have

$$P_1 = e_1; \quad P_2 = e_1 P_1 - 2e_2 P_0 = e_1^2 - 2e_2; \quad P_3 = e_1 P_2 - e_2 P_1 + 3e_3 P_0 = e_1^3 - 3e_1 e_2.$$

Note that in computing P_3 we have used our convention that $e_3 = 0$ (since $n = 2$).

(a) Suppose that $n = 3$. Use Newton's recursion to compute the formulae for P_2, P_3, and P_4.

(b) Let α_1, α_2, and α_3 be the roots of $f = x^3 + 5x^2 + 6x - 4$. Compute $\alpha_1^4 + \alpha_2^4 + \alpha_3^4$.

Solution.

(a) When $n = 3$ we have

$$\begin{aligned}
P_1 & & &= e_1; \\
P_2 &= e_1 P_1 - 2e_2 P_0 & &= e_1^2 - 2e_2; \\
P_3 &= e_1 P_2 - e_2 P_1 + 3e_3 P_0 & &= e_1^3 - 3e_1 e_2 + 3e_3; \text{ and} \\
P_4 &= e_1 P_3 - e_2 P_2 + e_3 P_1 - 4e_4 P_0 & &= e_1^4 - 4e_1^2 e_2 + 4e_1 e_3 + 2e_2^2.
\end{aligned}$$

In the formula for P_4 we have used our convention that $e_4 = 0$ since $n = 3$.

(b) The values of the elementary symmetric polynomials evaluated at the roots of f are $e_1(\alpha_1, \alpha_2, \alpha_3) = -5$, $e_2(\alpha_1, \alpha_2, \alpha_3) = 6$, and $e_3(\alpha_1, \alpha_2, \alpha_3) = 4$. Substituting this into our formula from part (a) we get

$$\alpha_1^4 + \alpha_2^4 + \alpha_3^4 = P_4(\alpha_1, \alpha_2, \alpha_3) = (-5)^4 - 4(-5)^2 \cdot 6 + 4(-5)(4) + 2(6)^2 = 17.$$

2. For each of the following cubic polynomials f compute $\mathrm{Gal}(L/\mathbb{Q})$ where L is the splitting field of f. If you are claiming that the polynomial f is irreducible over $\mathbb{Q}$, be sure to include a justification. (CAUTION: at least one of the cubics is reducible.) Also recall that if $f = x^3 + bx^2 + cx + d$, then

$$\Delta(f) = b^2c^2 + 18bcd - 4b^3d - 4c^3 - 27d^2.$$

(a) $f_1 = x^3 + 4x^2 + x + 1$.

(b) $f_2 = x^3 + 4x^2 + 2x - 2$.

(c) $f_3 = x^3 + 4x^2 + 3x - 1$.

(d) $f_4 = x^3 + 4x^2 + 4x + 1$.

Solution. If a cubic f is irreducible over $\mathbb{Q}$, then we know that its Galois group is C_3 or S_3, and that $\delta(f) = \sqrt{\Delta(f)}$ distinguishes between these cases. Specifically, $\delta(f) \in \mathbb{Q}$ if and only if the Galois group is C_3. (In general $\delta(f)$ detects whether or not the Galois group is contained in the alternating group A_d.)

(a) $f_1 = x^3+4x^2+x+1$ is irreducible. One way to see this is that $f_1 \equiv x^3+x+1 \bmod 2$, and over $\mathbb{F}_2[x]$ the cubic x^3+x+1 has no roots. Its discriminant is $\Delta(f_1) = -199$, and $\delta(f) = \sqrt{-199} \notin \mathbb{Q}$. Therefore the Galois group is S_3.

(b) $f_2 = x^3 + 4x^2 + 2x - 2$ is irreducible. One way to see this is to apply Eisenstein's criterion with the prime $p = 2$. Its discriminant is $\Delta(f_2) = 148 = 2^2 \cdot 37$, and $\delta(f_2) = \sqrt{148} = 2\sqrt{37} \notin \mathbb{Q}$. Therefore the Galois group is S_3 again.

(c) $f_3 = x^3+4x^2+3x-1$ is irreducible. One way to see this is that $f_3 \equiv x^3+x+1 \bmod 2$, which we've already seen is irreducible in $\mathbb{F}_2$. The discriminant is $\Delta(f_3) = 49$, and $\delta(f_3) = 7 \in \mathbb{Q}$. Therefore the Galois group is C_3.

(d) $f_4 = x^3+4x^2+4x+1 = (x+1)(x^2+3x+1)$. The factor x^2+3x+1 is irreducible over $\mathbb{Q}$, for instance because its discriminant $3^2 - 4 \cdot 1 \cdot 1 = 5$ has no square root in $\mathbb{Q}$. The splitting field of f_4 is therefore a quadratic extension over $\mathbb{Q}$, obtained by adjoining the roots of $x^2 + 3x + 1$ and the root $x = -1$ of $x + 1$. Specifically the splitting field is $\mathbb{Q}(\sqrt{5})$. Like all degree 2 extensions its Galois group is S_2, the cyclic group of order 2.

3. In this problem we will see what the sign of the discriminant of a real cubic polynomial tells us about its real or complex roots. Let $f = x^3 + bx^2 + cx + d \in \mathbb{R}[x]$. We assume that f has distinct roots, that is, that $\Delta(f) \neq 0$. We do not need to assume that f is irreducible.

(a) Explain why f has to have at least one real root. (Hint: This is really a problem in calculus, in particular, the intermediate value theorem may be useful.)

Let α_1 be any real root, and α_2 and α_3 the other two roots.

(b) Assume that α_2 and α_3 are real. Show that $\Delta(f) > 0$. (Suggestion: first show that $\delta(f) \in \mathbb{R}$.)

(c) Now assume that α_2 is not real. Show that $\alpha_3 = \overline{\alpha}_2$, i.e., that α_2 and α_3 are conjugate complex numbers.

(d) By (c) we may write $\alpha_2 = a - bi$ and $\alpha_3 = a + bi$ for some $a, b \in \mathbb{R}$, with $b \neq 0$. Show that $\Delta(f) < 0$. (Suggestion: first show that $\delta(f)$ is purely imaginary, i.e., of the form $i \cdot t$ for some real number $t \neq 0$.)

Solution.

(a) The leading term of f is x^3, so $\lim_{x\to\infty} f(x) = \infty$, $\lim_{x\to\infty} f(x) = -\infty$. Since f is a continuous function, by the intermediate value theorem f takes on every value in between. In particular, there is some $\alpha \in \mathbb{R}$ such that $f(\alpha) = 0$.

(b) We have $\delta(f) = (\alpha_3 - \alpha_2)(\alpha_3 - \alpha_1)(\alpha_2 - \alpha_1)$. Since $\alpha_1,\ \alpha_2,\ \alpha_3 \in \mathbb{R}$, $\delta(f) \in \mathbb{R}$, and therefore $\Delta(f) = \delta(f)^2 \geqslant 0$. We already know that $\Delta(f) \neq 0$, and therefore $\Delta(f) > 0$.

(c) Since f has real coefficients, $\overline{f(x)} = f(x)$. Therefore

$$0 = \overline{0} = \overline{f(\alpha_2)} = \overline{f}(\overline{\alpha}_2) = f(\overline{\alpha}_2).$$

I.e., $\overline{\alpha}_2$ is also a root of f. Since α_2 is not real, $\overline{\alpha}_2 \neq \alpha_2$, and therefore $\overline{\alpha}_2$ is a root of f different from α_2. We also cannot have $\overline{\alpha}_2 = \alpha_1$, because α_1 is real. Therefore $\overline{\alpha}_2$ must be equal to the only remaining root, namely α_3.

Remark. The computation above is one we've done many times : if σ is an automorphism of a field L, with fixed field K, then for any polynomial $f(x) \in K[x]$, σ takes roots of f to roots of f. In (c) we are applying this with $L = \mathbb{C}$, σ =complex conjugation, and $K = \mathbb{R}$.

(d) We have $(\alpha_3-\alpha_2) = 2bi$, and $(\alpha_3-\alpha_1)(\alpha_2-\alpha_1) = (\overline{\alpha}_2-\alpha_1)(\alpha_2-\alpha_1) = \|\alpha_2-\alpha_1\|^2$. Therefore

$$\delta(f) = (\alpha_3 - \alpha_2)(\alpha_3 - \alpha_1)(\alpha_2 - \alpha_1) = 2b \cdot \|\alpha_2 - \alpha_1\|^2 \cdot i.$$

Thus

$$\Delta(f) = \delta(f)^2 = 2b^2\|\alpha_2 - \alpha_1\|^4 \cdot (i)^2 = -4b^2\|\alpha_2 - \alpha_1\| \leqslant 0.$$

Since we already know that $\Delta(f) \neq 0$, this means that $\Delta(f) < 0$.

4. In this problem we will work out a few other identities involving the discriminant. Let $f \in K[x]$ be a monic polynomial of degree n, with roots $\alpha_1, \ldots, \alpha_n$.

(a) For any $c \in K$, show that $\Delta(f(x + c)) = \Delta(f(x))$. That is, show that translating the polynomial does not change the discriminant. (E.g. for $f = x^3 + 5x^2 + 3x + 1$, $f(x - 2) = (x - 2)^3 + 5(x - 2)^2 + 3(x - 2) + 1 = x^3 - x^2 - 5x + 7$ has the same discriminant as f.) Suggestion: What are the roots of $f(x + c)$?

(b) For any number β, explain why $(\beta - \alpha_1)(\beta - \alpha_2)\cdots(\beta - \alpha_n) = f(\beta)$.

(c) Let $g \in K[x]$ be a monic polynomial of degree m with roots $\beta_1, \ldots, \beta_m$. Show that $\left(\prod_{i=1}^m f(\beta_i)\right)^2 = \left(\prod_{j=1}^n g(\alpha_j)\right)^2$

(d) Show that $\Delta(f \cdot g) = \Delta(f) \cdot \Delta(g) \cdot (\prod_{i=1}^m f(\beta_i))^2$.

Solution.

(a) The roots of $f(x + c)$ are $\alpha_1 - c$, $\alpha_2 - c, \ldots, \alpha_n - c$, and so

$$\Delta(f(x + c)) = \prod_{1\leqslant i<j\leqslant n} \Big((\alpha_j - c) - (\alpha_i - c)\Big) = \prod_{1\leqslant i<j\leqslant n} (\alpha_j - \alpha_i) = \Delta(f(x)).$$

(b) We have $f(x) = \prod_{j=1}^n \Big(x - \alpha_j\Big)$, since $\alpha_1, \ldots, \alpha_n$ are the roots of the monic polynomial f, and so substituting $x = \beta$ gives $\prod_{j=1}^n(\beta - \alpha_j) = f(\beta)$.

(c) Using (b) twice (once for f and once for g), as well as $(\beta_i - \alpha_j)^2 = (\alpha_j - \beta_i)^2$ and switching the order of the product, we have

$$\left(\prod_{i=1}^m f(\beta_i)\right)^2 = \prod_{j=1}^n \left(\prod_{i=1}^m (\beta_i - \alpha_j)^2\right) = \prod_{j=1}^n \left(\prod_{i=1}^m (\alpha_j - \beta_i)^2\right) = \left(\prod_{j=1}^n g(\alpha_j)\right)^2.$$

(d) If $\alpha_1, \ldots, \alpha_n$ are the roots of f, and $\beta_1, \ldots, \beta_m$ the roots of g, then the roots of $f \cdot g$ are $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m$. The number $\Delta(f \cdot g)$ is the product of the difference of all pairs of roots, squared. As we have seen from class, it does not matter which order we take the product in (Δ is a symmetric function in the roots).

We can organize the product in $\Delta(f \cdot g)$ as :

- The product of the squares of all the differences of roots in $\alpha_1, \ldots, \alpha_n$;
- The product of the squares of all the differences of roots in $\beta_1, \ldots, \beta_m$; and
- the product of the square of the difference between a root in $\alpha_1, \ldots, \alpha_n$ and a root in $\beta_1, \ldots, \beta_m$.

The product in the first group is $\Delta(f)$, that in the second group is $\Delta(g)$, and that in the third group is

$$\prod_{j=1}^{n} \left(\prod_{i=1}^{m} (\beta_i - \alpha_j)^2 \right) = \left(\prod_{i=1}^{m} f(\beta_i) \right)^2$$

by (c).

Therefore the product of all three is $\Delta(f \cdot g) = \Delta(f)\Delta(g) \prod_{i=1}^{m} f(\beta_i)^2$. (Which we could equally well write as $\Delta(f \cdot g) = \Delta(f)\Delta(g) \prod_{j=1}^{n} g(\alpha_j)^2$.)