

Solutions to David A.Cox "Galois Theory"

Richard Ganaye

October 9, 2021

2 Chapter 2

2.1 POLYNOMIALS OF SEVERAL VARIABLES

Ex. 2.1.1 Show that $\langle x, y \rangle = \{xg + yh \mid g, h \in F[x, y]\} \subset F[x, y]$ is not a principal ideal in $F[x, y]$.

Proof. We show first that $\langle x, y \rangle \neq F[x, y]$. If not, $1 \in \langle x, y \rangle$, so

$$1 = xu + yv, \quad u, v \in F[x, y].$$

If we evaluate this identity at $x = 0, y = 0$, we obtain $1 = 0$, which is a contradiction, thus

$$\langle x, y \rangle \neq F[x, y].$$

If $\langle x, y \rangle$ was a principal ideal, generated by $p \in F[x, y]$, then $\langle x, y \rangle = \langle p \rangle$, and

$$x = pq, y = pr, \quad q, r \in F[x, y].$$

$\deg(p) + \deg(q) = \deg(x) = 1$, so $\deg(p) \leq 1$, and $p \neq 0$.

If $\deg(p) = 0$, then $p = \lambda \in F^*$, and $\langle x, y \rangle = \langle \lambda \rangle = F[x, y]$, but we have proved that this is impossible.

Thus $\deg(p) = 1$, so $p = \alpha x + \beta y + \gamma$, $\alpha, \beta, \gamma \in F$, and $\deg(q) = \deg(r) = 0$, so $q = \lambda \in F^*, r = \mu \in F^*$:

$$\begin{aligned} x &= \lambda(\alpha x + \beta y + \gamma), \\ y &= \mu(\alpha x + \beta y + \gamma). \end{aligned}$$

This implies $\lambda\beta = 0$ and $\mu\alpha = 0$.

As $\lambda \neq 0, \mu \neq 0, \alpha = \beta = 0$, which is in contradiction with $\deg(p) = 1$.

We have proved that $\langle x, y \rangle$ is not a principal ideal, et thus $F[x, y]$ is not a principal ideal domain. \square

Ex. 2.1.2 Express each the following polynomials as a polynomial in y with coefficients that are polynomials in the remaining variables.

(a) $x^2y + 3y^2 - xy^2 + 3x + xy^2 + 7x^2y^2$.

(b) $(y - (x_1 + x_2))(y - (x_1 + x_3))(y - (x_2 + x_1))$.

Proof. (a)

$$\begin{aligned} p &= x^2y + 3y^2 - xy^2 + 3x + xy^2 + 7x^3y^3 \\ &= (7x^3)y^3 + 3y^2 + x^2y + 3x. \end{aligned}$$

(b) let

$$q = (y - (x_1 + x_2))(y - (x_1 + x_3))(y - (x_2 + x_3)).$$

Consider $p = (x + x_1)(x + x_2)(x + x_3) = x^3 + \sigma_1x^2 + \sigma_2x + \sigma_3$.

Then

$$\begin{aligned} q &= (y - \sigma_1 + x_3)(y - \sigma_1 + x_2)(y - \sigma_1 + x_1) \\ &= p(y - \sigma_1) \\ &= (y - \sigma_1)^3 + \sigma_1(y - \sigma_1)^2 + \sigma_2(y - \sigma_1) + \sigma_3 \\ &= (y^3 - 3\sigma_1y^2 + 3\sigma_1^2y - \sigma_1^3) + (\sigma_1y^2 - 2\sigma_1^2y + \sigma_1^3) + (\sigma_2y - \sigma_1\sigma_2) + \sigma_3 \\ &= y^3 - 2\sigma_1y^2 + (\sigma_1^2 + \sigma_2)y + (\sigma_3 - \sigma_1\sigma_2). \end{aligned}$$

□

Ex. 2.1.3 Given positive integers n and r with $1 \leq r \leq n$, let $\binom{n}{r}$ be the number of ways of choosing r elements from a set with n elements. Recall that $\binom{n}{r} = \frac{n!}{r!(n-r)!}$.

(a) Show that the polynomial σ_r is a sum of $\binom{n}{r}$ terms.

(b) Show that $\sigma_r(-\alpha, \dots, -\alpha) = (-1)^r \binom{n}{r} \alpha^r$.

(c) Let $f = (x + \alpha)^n$. Use part (b) and Corollary 2.1.5 to prove that

$$(x + \alpha)^n = \sum_{r=0}^n \binom{n}{r} \alpha^r x^{n-r},$$

where $\binom{n}{0} = 1$. This shows that the binomial theorem follows from Corollary 2.1.5.

Proof. (a) The number of terms in

$$\sigma_r = \sum_{1 \leq i_1 < \dots < i_r \leq n} x_{i_1} x_{i_2} \dots x_{i_r} \quad (1)$$

is the number of strictly increasing sequences (i_1, i_2, \dots, i_r) in the integer interval $\llbracket 1, n \rrbracket$. It is equal to the number of subsets with r elements in the set $\llbracket 1, n \rrbracket$ with n elements. Thus it is equal to $\binom{n}{r}$.

(b) Evaluating (1) with $x_1 = x_2 = \dots = x_n = -\alpha$, we obtain

$$\begin{aligned} \sigma_r(-\alpha, \dots, -\alpha) &= \sum_{1 \leq i_1 < \dots < i_r \leq n} (-\alpha)^r \\ &= (-1)^r \binom{n}{r} \alpha^r. \end{aligned}$$

(c) By Corollary 2.1.5, with the substitution $x_1 = -\alpha, x_2 = -\alpha, \dots, x_n = -\alpha$,

$$f = (x + \alpha)^n = x^n + a_1 x^{n-1} + \dots + a_n,$$

where

$$\begin{aligned} a_r &= (-1)^r \sigma_r(-\alpha, \dots, -\alpha) \\ &= \binom{n}{r} \alpha^r. \end{aligned}$$

Consequently,

$$(x + \alpha)^n = \sum_{i=1}^n \binom{n}{i} \alpha^i x^{n-i}.$$

With the substitution $x = \beta$, $\beta \in F$, we obtain the binomial formula

$$(\alpha + \beta)^n = \sum_{i=1}^n \binom{n}{i} \alpha^i \beta^{n-i}.$$

□

2.2 SYMMETRIC POLYNOMIALS

Ex. 2.2.1 Show that the leading term of σ_r is $x_1 x_2 \dots x_r$.

Proof. We show that the leading term of σ_r for the graded lexicographic order is $x_1 x_2 \dots x_r$.

Let $x_{i_1} x_{i_2} \dots x_{i_r}$ ($i_1 < i_2 < \dots < i_r$) any term of σ_r , distinct of $x_1 x_2 \dots x_r$. We must show that $x_1 x_2 \dots x_r > x_{i_1} x_{i_2} \dots x_{i_r}$.

If $i_1 > 1$, then x_1 has no occurrence in $x_{i_1} x_{i_2} \dots x_{i_r}$. Its exponent is 0 in the right monomial, and 1 in the left monomial, so

$$x_1 x_2 \dots x_r > x_{i_1} x_{i_2} \dots x_{i_r},$$

and the proof is done in this case.

If $i_1 = 1$, let j ($1 < j < n$) the first subscript such that $i_j \neq j$. Then

$$i_1 = 1, i_2 = 2, \dots, i_{j-1} = j-1, i_j \neq j.$$

Such a subscript exists, otherwise $x_1 x_2 \dots x_r = x_{i_1} x_{i_2} \dots x_{i_r}$. As $i_j > i_{j-1} = j-1$, $i_j \geq j$, and as $i_j \neq j$, $i_j > j$, so the exponent of x_j is 0 in the right monomial.

Therefore

$$x_1 x_2 \dots x_{j-1} x_j \dots x_r > x_1 x_2 \dots x_{j-1} x_{i_j} \dots x_{i_r} = x_{i_1} x_{i_2} \dots x_{i_r}.$$

So the leading term of σ_r is $x_1 x_2 \dots x_r$.

□

Ex. 2.2.2 This exercise will study the order relation defined in (2.5). Given an exponent vector $\alpha = (a_1, \dots, a_n)$, where each $a_i \geq 0$ is an integer, let x^α denote the monomial

$$x^\alpha = x_1^{a_1} \cdots x_n^{a_n}.$$

If α and β are exponent vectors, note that $x^\alpha x^\gamma = x^{\alpha+\beta}$. Also, the leading term of a nonzero polynomial $f \in F[x_1, \dots, x_n]$ will be denoted $\text{LT}(f)$.

(a) Suppose that $x^\alpha > x^\beta$, and let x^γ be any monomial. Prove that $x^{\alpha+\beta} > x^{\beta+\gamma}$.

(b) Suppose that $x^\alpha > x^\beta$ and $x^\gamma > x^\delta$. Prove that $x^{\alpha+\gamma} > x^{\beta+\delta}$.

(c) Let $f, g \in F(x_1, \dots, x_n]$ be nonzero. Prove that $\text{LT}(fg) = \text{LT}(f)\text{LT}(g)$.

Proof. (a) Let $\alpha = (a_1, a_2, \dots, a_n), \beta = (b_1, b_2, \dots, b_n), \gamma = (c_1, c_2, \dots, c_n)$ and suppose that $x^\alpha > x^\beta$.

Then $a_1 + a_2 + \dots + a_n \geq b_1 + b_2 + \dots + b_n$, otherwise $x^\alpha < x^\beta$.

If $a_1 + a_2 + \dots + a_n > b_1 + b_2 + \dots + b_n$, then $(a_1 + c_1) + \dots + (a_n + c_n) > (b_1 + c_1) + \dots + (b_n + c_n)$, thus $x^{\alpha+\gamma} > x^{\beta+\gamma}$.

We suppose now that $a_1 + a_2 + \dots + a_n = b_1 + b_2 + \dots + b_n$.

By definition of the graded lexicographical order, $a_1 \geq b_1$, otherwise $x^\alpha < x^\beta$.

If $a_1 > b_1$, then $a_1 + c_1 > b_1 + c_1$, which implies $x^{\alpha+\gamma} > x^{\beta+\gamma}$.

It remains the case where $a_1 = b_1$.

Let j ($j < n$) the first subscript such that $a_i \neq b_i$:

$$a_1 = b_1, a_2 = b_2, \dots, a_{j-1} = b_{j-1}, a_j \neq b_j.$$

As $x^\alpha > x^\beta$, such a subscript exists, otherwise $x^\alpha = x^\beta$.

If $a_j < b_j$, we would have $x^\alpha < x^\beta$, which is false by hypothesis, so $a_j > b_j$.

Then $a_1 + c_1 = b_1 + c_1, \dots, a_{j-1} + c_{j-1} = b_{j-1} + c_{j-1}$ et $a_j + c_j > b_j + c_j$, so

$$x^{\alpha+\gamma} > x^{\beta+\gamma}.$$

Conclusion :

$$x^\alpha > x^\beta \Rightarrow x^{\alpha+\gamma} > x^{\beta+\gamma}.$$

(b) If $x^\alpha > x^\beta$ et $x^\gamma > x^\delta$, then by (a),

$$x^{\alpha+\gamma} > x^{\beta+\gamma},$$

$$x^{\beta+\gamma} > x^{\beta+\delta}.$$

So, by transitivity

$$x^{\alpha+\gamma} > x^{\beta+\delta}.$$

(c) Let $cx^\alpha = \text{LT}(f), dx^\beta = \text{LT}(g)$. By definition of the leading term, for every term ux^γ in f , distinct of $\text{LT}(f)$,

$$x^\alpha > x^\gamma,$$

and for every term vx^δ in g , distinct of $\text{LT}(g)$,

$$x^\beta > x^\delta.$$

Every monomial in fg distinct of $cdx^{\alpha+\beta}$ is a sum of terms of the form $gx^{\gamma+\delta}$, where β, γ verify $\alpha \geq \gamma, \beta > \delta$, or $\alpha > \gamma, \beta \geq \delta$. In both cases, by (a) and (b),

$$x^{\alpha+\beta} > x^{\gamma+\delta}.$$

Therefore $cdx^{\alpha+\beta}$ is the leading term of fg , so

$$\text{LT}(fg) = \text{LT}(f) \text{LT}(g).$$

□

Ex. 2.2.3 Prove (2.13)-(2.16). For (2.13), a computer will be helpful; the others can be proved by hand using the identity

$$(y_1 + \cdots + y_m)^2 = y_1^2 + \cdots + y_m^2 + 2 \sum_{i < j} y_i y_j.$$

Proof. Let

$$f = \Sigma_4 x_1^3 x_2^2 x_3.$$

We must write f as a polynomial in $\sigma_1, \sigma_2, \sigma_3, \sigma_4$.

The leading term of f for the graded lexicographical order being $x_1^3 x_2^2 x_3^1 x_4^0$, the algorithm of section 2.2 asks to subtract to f the monomial $\sigma_1^{3-2} \sigma_2^{2-1} \sigma_3^{1-0} \sigma_4^0 = \sigma_1 \sigma_2 \sigma_3$.

(a)

$$\begin{aligned} \sigma_1 \sigma_2 \sigma_3 &= (x_1 + x_2 + x_3 + x_4) \times (x_1 x_2 + x_1 x_3 + x_1 x_4 + x_2 x_3 + x_2 x_4 + x_3 x_4) \\ &\quad \times (x_1 x_2 x_3 + x_1 x_2 x_4 + x_1 x_3 x_4 + x_2 x_3 x_4) \\ &= 3x_1 x_2^3 x_3 x_4 + 8x_1^2 x_2^2 x_3 x_4 + 8x_2^2 x_4^2 x_1 x_3 + 8x_2^2 x_3^2 x_1 x_4 + 8x_1^2 x_2 x_4^2 x_3 \\ &\quad + 8x_1^2 x_2 x_3^2 x_4 + 8x_2 x_3^2 x_4^2 x_1 + 3x_1^3 x_2 x_3 x_4 + 3x_2 x_4^3 x_1 x_3 + 3x_2 x_3^3 x_1 x_4 \\ &\quad + x_1^3 x_4^2 x_3 + 3x_2^2 x_3^2 x_4^2 + x_1^2 x_2^3 x_3 + x_3^2 x_4^3 x_2 + x_2^2 x_3^3 x_1 + 3x_1^2 x_2^2 x_3^2 \\ &\quad + x_1^2 x_3^3 x_4 + x_3^3 x_4^2 x_2 + x_2^3 x_3^2 x_4 + x_2^2 x_3^3 x_4 + x_3^2 x_4^3 x_1 + x_2^3 x_3^2 x_1 \\ &\quad + x_2^3 x_4^2 x_1 + x_2^2 x_4^3 x_1 + x_2^3 x_4^2 x_3 + x_3^3 x_4^2 x_1 + x_1^3 x_2^2 x_3 + x_1^3 x_3^2 x_2 \\ &\quad + x_1^2 x_4^3 x_2 + 3x_1^2 x_2^2 x_4^2 + x_1^3 x_3^2 x_4 + x_1^3 x_2^2 x_4 + 3x_1^2 x_3^2 x_4^2 + x_2^2 x_4^3 x_3 \\ &\quad + x_1^3 x_4^2 x_2 + x_1^2 x_2^3 x_4 + x_1^2 x_4^3 x_3 + x_1^2 x_3^3 x_2 \\ &= 8\Sigma_4 x_1^2 x_2^2 x_3 x_4 + 3\Sigma_4 x_1^3 x_2 x_3 x_4 + 3\Sigma_4 x_1^2 x_2^2 x_3^2 + \Sigma_4 x_1^3 x_2^2 x_3. \end{aligned}$$

We find the 96 terms of the product $\sigma_1 \sigma_2 \sigma_3$ (see Ex. 2.2.12):

$\Sigma_4 x_1^2 x_2^2 x_3 x_4$ has $\frac{4!}{2!2!} = 6$ terms, with the coefficient 8 : 48 terms.

$\Sigma_4 x_1^3 x_2 x_3 x_4$ has $\frac{4!}{1!3!} = 4$ terms, with the coefficient 3 : 12 terms.

$\Sigma_4 x_1^2 x_2^2 x_3^2$ has $\frac{4!}{3!1!} = 4$ terms, with the coefficient 3 : 12 terms.

$\Sigma_4 x_1^3 x_2^2 x_3$ has $\frac{4!}{1!1!1!1!} = 24$ terms, with the coefficient 1 : 24 terms..

We obtain this product with the following Maple instructions :

```
> P = (x + x1).(x + x2).(x + x3)(x + x4);
> p := expand(P);
> q := collect(p, x);
> sigma1 := coeff(q, x, 3); sigma2 := coeff(q, x, 2); sigma3 := coeff(q, x, 1); sigma4 := coeff(q, x, 1);
> expand(sigma1.sigma2.sigma3);
```

With sage :

```
e = SymmetricFunctions(QQ).e()
g = (e([1])* e([2])*e([3])).expand(4);g
```

(b) So

$$\begin{aligned} f_1 &= f - \sigma_1\sigma_2\sigma_3 \\ &= -8\Sigma_4x_1^2x_2^2x_3x_4 - 3\Sigma_4x_1^3x_2x_3x_4 - 3\Sigma_4x_1^2x_2^2x_3^2. \end{aligned}$$

The leading of f_1 is $-3x_1^3x_2x_3x_4$, so we must subtract $-3\sigma_1^2\sigma_4$ to f_1 .

$$\begin{aligned} \sigma_1^2\sigma_4 &= (\Sigma_4x_1)^2(x_1x_2x_3x_4) \\ &= (\Sigma_4x_1^2 + 2\Sigma_4x_1x_2)x_1x_2x_3x_4 \\ &= \Sigma_4x_1^3x_2x_3x_4 + 2\Sigma_4x_1^2x_2^2x_3x_4, \end{aligned}$$

therefore

$$f_2 = f - \sigma_1\sigma_2\sigma_3 + 3\sigma_1^2\sigma_4 = -3\Sigma_4x_1^2x_2^2x_3^2 - 2\Sigma_4x_1^2x_2^2x_3x_4.$$

(c) The leading term of f_2 is $-3x_1^2x_2^2x_3^2$, so must subtract $-3\sigma_3^2$ to f_2 .

$$\begin{aligned} \sigma_3^2 &= (\Sigma_4x_1x_2x_3)^2 \\ &= \Sigma_4x_1^2x_2^2x_3^2 + 2\Sigma_4x_1^2x_2^2x_3x_4, \end{aligned}$$

$$f_3 = f - \sigma_1\sigma_2\sigma_3 + 3\sigma_1^2\sigma_4 + 3\sigma_3^2 = 4\Sigma_4x_1^2x_2^2x_3x_4.$$

(d) The leading term of f_3 is $4x_1^2x_2^2x_3x_4$, so we must subtract $4\sigma_2\sigma_4$ to f_3 .

$$\begin{aligned} \sigma_2\sigma_4 &= (\Sigma_4x_1x_2)(x_1x_2x_3x_4) \\ &= \Sigma_4x_1^2x_2^2x_3x_4, \end{aligned}$$

$$\text{so } f_4 = f - \sigma_1\sigma_2\sigma_3 + 3\sigma_1^2\sigma_4 + 3\sigma_3^2 - 4\sigma_2\sigma_4 = 0.$$

$$f = \Sigma_4x_1^3x_2^2x_3 = \sigma_1\sigma_2\sigma_3 - 3\sigma_1^2\sigma_4 - 3\sigma_3^2 + 4\sigma_2\sigma_4.$$

□

Ex. 2.2.4 Let $f = x^3 + bx^2 + cx + d \in F[x]$ have roots $\alpha_1, \alpha_2, \alpha_3$ in the field L containing F , and let g be the polynomial defined in (2.17). Show carefully that

$$g(x) = x^3 + 2bx^2 + (b^2 + c)x + bc - d.$$

Proof. Let

$$\begin{aligned} f &= x^3 + bx^2 + cx + d \\ &= (x - \alpha)(x - \beta)(x - \gamma) \\ &= x^3 - \sigma_1(\alpha, \beta, \gamma)x^2 + \sigma_2(\alpha, \beta, \gamma)x - \sigma_3(\alpha, \beta, \gamma), \end{aligned}$$

which gives

$$\begin{aligned} \sigma_1(\alpha, \beta, \gamma) &= -b, \\ \sigma_2(\alpha, \beta, \gamma) &= +c, \\ \sigma_3(\alpha, \beta, \gamma) &= -d. \end{aligned}$$

Let

$$G(x) = (x - (x_1 + x_2))(x - (x_1 + x_3))(x - (x_2 + x_3)).$$

Then

$$g(x) = (x - (\alpha_1 + \alpha_2))(x - (\alpha_1 + \alpha_3))(x - (\alpha_2 + \alpha_3))$$

is obtained from G by the evaluation morphism which sends x_1, x_2, x_3 on $\alpha_1, \alpha_2, \alpha_3$.

$$\text{Let } p = (x + x_1)(x + x_2)(x + x_3) = x + \sigma_1 x^2 + \sigma_2 x + \sigma_3.$$

Then

$$\begin{aligned} G &= (x - \sigma_1 + x_3)(x - \sigma_1 + x_2)(x - \sigma_1 + x_1) \\ &= p(x - \sigma_1) \\ &= (x - \sigma_1)^3 + \sigma_1(x - \sigma_1)^2 + \sigma_2(x - \sigma_1) + \sigma_3 \\ &= (x^3 - 3\sigma_1 x^2 + 3\sigma_1^2 x - \sigma_1^3) + (\sigma_1 x^2 - 2\sigma_1^2 x + \sigma_1^3) + (\sigma_2 x - \sigma_1 \sigma_2) + \sigma_3 \\ &= x^3 - 2\sigma_1 x^2 + (\sigma_1^2 + \sigma_2)x + (\sigma_3 - \sigma_1 \sigma_2). \end{aligned}$$

The previous evaluation morphism sends σ_1 on $\sigma_1(\alpha_1, \alpha_2, \alpha_3) = -b$, σ_2 on $\sigma_2(\alpha_1, \alpha_2, \alpha_3) = c$, σ_3 on $\sigma_3(\alpha_1, \alpha_2, \alpha_3) = -d$.

$$g(x) = x^3 + 2bx^2 + (b^2 + c)x + bc - d.$$

In the example 2.2.6,

$$f(x) = x^3 + 2x^2 + x + 7,$$

where

$$b = 2, c = 1, d = 7,$$

$\alpha_1, \alpha_2, \alpha_3$ being the roots of g in \mathbb{C} , we obtain

$$\begin{aligned} g(x) &= (x - (\alpha_1 + \alpha_2))(x - (\alpha_1 + \alpha_3))(x - (\alpha_2 + \alpha_3)) \\ &= x^3 + 2bx^2 + (b^2 + c)x + bc - d \\ &= x^3 + 4x^2 + 5x - 5. \end{aligned}$$

□

Ex. 2.2.5 This exercise will complete the proof of Theorem 2.2.7. Let $h \in F[u_1, \dots, u_n]$ be a nonzero polynomial. The goal is to prove that $h(\sigma_1, \dots, \sigma_n)$ is not the zero polynomial in x_1, \dots, x_n .

- (a) If $cu_1^{b_1} \dots u_n^{b_n}$ is a term of h , then use Exercise 2 to show that the leading term of $c\sigma_1^{b_1} \dots \sigma_n^{b_n}$ is $cx_1^{b_1+\dots+b_n} x_2^{b_2+\dots+b_n} \dots x_n^{b_n}$.
- (b) Show that $(b_1, \dots, b_n) \mapsto (b_1 + \dots + b_n, b_2 + \dots + b_n, \dots, b_n)$ is one-to-one.
- (c) To see why $h(\sigma_1, \dots, \sigma_n)$ is nonzero, consider the term of $h(u_1, \dots, u_n)$ for which the leading term of $c\sigma_1^{b_1} \dots \sigma_n^{b_n}$ is maximal. Prove that this leading term is in fact the leading term of $h(\sigma_1, \dots, \sigma_n)$, and explain how this proves what we want.

Proof. (a) Let $h \in F[u_1, u_2, \dots, u_n]$, $h \neq 0$, and $cu_1^{b_1} u_2^{b_2} \dots u_n^{b_n}$ a term of h .

The leading term of a product is the product of the leading term of the factors (Ex 2.2.2), and the leading term of σ_r is $x_1 x_2 \dots x_r$ (Ex 2.2.1), so the leading term of $c\sigma_1^{b_1} \sigma_2^{b_2} \dots \sigma_n^{b_n}$ is

$$\begin{aligned} \text{LT}(c\sigma_1^{b_1} \sigma_2^{b_2} \dots \sigma_n^{b_n}) &= c(x_1)^{b_1} (x_1 x_2)^{b_2} \dots (x_1 x_2 \dots x_n)^{b_n} \\ &= cx_1^{b_1+b_2+\dots+b_n} x_2^{b_2+\dots+b_n} \dots x_n^{b_n}. \end{aligned}$$

- (b) Si $a_i, b_i \in \mathbb{Z}$, the system of equations

$$\begin{aligned} b_1 + b_2 + \dots + b_n &= a_1, \\ b_2 + \dots + b_n &= a_2, \\ &\dots \\ b_n &= a_n, \end{aligned}$$

is equivalent to

$$\begin{aligned} b_1 &= a_1 - a_2, \\ b_2 &= a_2 - a_3, \\ &\dots \\ b_{n-1} &= a_n - a_{n-1}, \\ b_n &= a_n. \end{aligned}$$

So the application $f : \mathbb{Z}^n \rightarrow \mathbb{Z}^n$ defined by

$$(b_1, b_2, \dots, b_n) \mapsto (b_1 + b_2 + \dots + b_n, b_2 + \dots + b_n, \dots, b_n)$$

is bijective (one-to-one and onto).

- (c) As $h \neq 0$, there exists a term $cu_1^{b_1} u_2^{b_2} \dots u_n^{b_n}$ of h such that the leading term $cx_1^{a_1} \dots x_n^{a_n}$ of $c\sigma_1^{b_1} \sigma_2^{b_2} \dots \sigma_n^{b_n}$ is maximal. Then every other term $c'u_1^{d_1} u_2^{d_2} \dots u_n^{d_n}$ of h verifies $(b'_1, b'_2, \dots, b'_n) \neq (b_1, b_2, \dots, b_n)$ and the leading term $c'x_1^{a'_1} \dots x_n^{a'_n}$ of $c'\sigma_1^{d_1} \sigma_2^{d_2} \dots \sigma_n^{d_n}$ is less than $cx_1^{a_1} \dots x_n^{a_n}$: it can not be greater because this term is maximal, and $(a_1, a_2, \dots, a_n) \neq (a'_1, a'_2, \dots, a'_n)$, since the application f in (b) is bijective. The graded lexicographic order defined on the monomials $x_1^{a_1} \dots x_n^{a_n}$ being a total order, $x_1^{a_1} \dots x_n^{a_n} > x_1^{a'_1} \dots x_n^{a'_n}$.

So $cx_1^{a_1} \cdots x_n^{a_n}$ is greater than the leading terms of every other term $c' \sigma_1^{d_1} \sigma_2^{d_2} \cdots \sigma_n^{d_n}$ of $h(\sigma_1, \dots, \sigma_n) \neq 0$, so is a fortiori greater than every other term of $h(\sigma_1, \dots, \sigma_n)$.

It can't be cancelled in the sum of these terms, and consequently $h(\sigma_1, \dots, \sigma_n) \neq 0$. \square

Ex. 2.2.6 Here is an example of polynomials which are not algebraically independent. Consider $x_1^2, x_1x_2, x_2^2 \in F[x_1, x_2]$, and let $\phi : F[u_1, u_2, u_3] \rightarrow F[x_1, x_2]$ be defined by

$$\phi(u_1) = x_1^2, \phi(u_2) = x_1x_2, \phi(u_3) = x_2^2.$$

Show that ϕ is not one-to-one by finding a nonzero polynomial $h \in F[u_1, u_2, u_3]$ such that $\phi(h) = 0$.

Proof. Let $h = u_1u_3 - u_2^2$.

Then the unique algebra morphism ϕ such that

$$\phi(u_1) = x_1^2, \phi(u_2) = x_1x_2, \phi(u_3) = x_2^2$$

verifies

$$\phi(h) = \phi(u_1)\phi(u_3) - (\phi(u_2))^2 = x_1^2x_2^2 - (x_1x_2)^2 = 0.$$

So $h \neq 0$ is in the kernel of ϕ , and ϕ is not one-to-one. Thus x_1^2, x_1x_2, x_2^2 are not algebraically independent. \square

Ex. 2.2.7 Given a polynomial $f \in F[x_1, \dots, x_n]$ and a permutation $\sigma \in S_n$, let $\sigma \cdot f$ denote the polynomial obtained from f by permuting the variables according to σ . Show that $\prod_{\sigma \in S_n} \sigma \cdot f$ and $\sum_{\sigma \in S_n} \sigma \cdot f$ are symmetric polynomials.

Proof. We use the relations (2.31) p. 48, (or (6.7) p. 138) proved in Exercices 6.4.3 et 6.4.4 : for all $\sigma, \tau \in S_n$, and all $f, g \in F[x_1, x_2, \dots, x_n]$:

$$\sigma \cdot (f + g) = \sigma \cdot f + \sigma \cdot g, \quad (2)$$

$$\sigma \cdot (fg) = (\sigma \cdot f)(\sigma \cdot g), \quad (3)$$

$$\tau \cdot (\sigma \cdot f) = (\tau \circ \sigma) \cdot f. \quad (4)$$

(We will use the notation $\tau \circ \sigma = \tau\sigma$.)

Let $g = \prod_{\sigma \in S_n} \sigma \cdot f$.

Then, if $\tau \in S_n$, using (3) et (4)

$$\begin{aligned} \tau \cdot g &= \tau \cdot \prod_{\sigma \in S_n} \sigma \cdot f \\ &= \prod_{\sigma \in S_n} \tau \cdot (\sigma \cdot f) \\ &= \prod_{\sigma \in S_n} (\tau\sigma) \cdot f. \end{aligned}$$

As the application $S_n \rightarrow S_n, \sigma \mapsto \tau\sigma$ is bijective, the index change $\sigma' = \tau\sigma$ gives

$$\prod_{\sigma \in S_n} (\tau\sigma) \cdot f = \prod_{\sigma' \in S_n} \sigma' \cdot f = \prod_{\sigma \in S_n} \sigma \cdot f = g$$

So, for all $\tau \in S_n, \tau \cdot g = g$: thus g is a symmetric polynomial.

Same proof for $\tau \cdot \sum_{\sigma \in S_n} \sigma \cdot f = \sum_{\sigma \in S_n} \sigma \cdot f$: use (2) in place of (3).

Conclusion : $\prod_{\sigma \in S_n} \sigma \cdot f$ and $\sum_{\sigma \in S_n} \sigma \cdot f$ are symmetric polynomials. \square

Ex. 2.2.8 In this exercise, you will prove that if $\varphi \in F(x_1, \dots, x_n)$ is symmetric, then φ is a rational function in $\sigma_1, \dots, \sigma_n$ with coefficients in F . To begin the proof, we know that $\varphi = A/B$, where A and B are in $F[x_1, \dots, x_n]$. Note that A and B need not be symmetric, only their quotient $\varphi = A/B$ is. Let

$$C = \prod_{\sigma \in S_n \setminus \{e\}} \sigma \cdot B,$$

where we are using the notation of Exercise 7.

- (a) Use Exercise 7 to show that BC is a symmetric polynomial.
- (b) Then use the symmetry of $\varphi = A/B$ to show that AC is a symmetric polynomial.
- (c) Use $\varphi = (AC)/(BC)$ and theorem 2.2.2 to conclude that φ is a rational function in the elementary symmetric polynomials with coefficients in F .

Proof. Let $\varphi = A/B \in F(x_1, \dots, x_n)$ a symmetric rational function:

$$\forall \sigma \in S_n, \sigma \cdot \varphi = \sigma \cdot A / \sigma \cdot B = \varphi = A/B.$$

- (a) Let

$$C = \prod_{\sigma \in S_n \setminus \{e\}} \sigma \cdot B.$$

Then

$$BC = \prod_{\sigma \in S_n} \sigma \cdot B.$$

By Exercise 2.2.7, BC is then a symmetric polynomial.

- (b) Note that the rules (2.31) for polynomials extend to rational functions. In particular, if $\varphi = A/B, \psi = A_1/B_1 \in F(x_1, \dots, x_n)$, and $\sigma \in S_n$,

$$\sigma \cdot (\varphi\psi) = (\sigma \cdot \varphi) (\sigma \cdot \psi).$$

Indeed,

$$(\sigma \cdot \varphi) (\sigma \cdot \psi) = \frac{\sigma \cdot A}{\sigma \cdot B} \frac{\sigma \cdot A_1}{\sigma \cdot B_1} = \frac{\sigma \cdot (AA_1)}{\sigma \cdot (BB_1)} = \sigma \cdot (\varphi\psi).$$

Using this property, for all $\sigma \in S_n$, from $AC = \varphi BC$, we obtain

$$\sigma \cdot (AC) = (\sigma \cdot \varphi)(\sigma \cdot (BC)) = \varphi BC = AC.$$

So AC is a symmetric polynomial.

- (c) So $\varphi = \frac{AC}{BC}$ is the quotient of two symmetric polynomials, thus there exists $h, k \in F[x_1, \dots, x_n]$ such that

$$\varphi = \frac{AC}{BC} = \frac{h(\sigma_1, \dots, \sigma_n)}{k(\sigma_1, \dots, \sigma_n)} = \left(\frac{h}{k} \right) (\sigma_1, \dots, \sigma_n).$$

$\varphi \in F(\sigma_1, \dots, \sigma_n)$ is a rational function in the elementary symmetric polynomials with coefficients in F .

□

Ex. 2.2.9 In the Historical Notes, we gave Gauss's definition of lexicographic order.

- (a) Give a definition (in English) of lexicographic order.
- (b) In the proof of Theorem 2.2.2, we showed that grade lexicographic order has the property that there are only finitely many monomials less than a given monomial. In contrast this property fails for lexicographic order. Give an explicit example to illustrate this.
- (c) In spite of part (b), lexicographic order does have an interesting finiteness property. Namely, prove that there is no infinite sequence of polynomials f_1, f_2, f_3, \dots that have strictly decreasing terms according to lexicographic order.
- (d) Explain how part (c) allows one to prove Theorem 2.2.2 using lexicographic order.

Proof. (a) For the lexicographic order, $x_1^{a_1} \cdots x_n^{a_n} < x_1^{b_1} \cdots x_n^{b_n}$ is equivalent by definition to

$$\exists j \in [1, n], (\forall i \in \mathbb{N}, 1 \leq i < j \Rightarrow a_i = b_i) \text{ and } a_j < b_j.$$

(The property $(\forall i \in \mathbb{N}, 1 \leq i < j \Rightarrow a_i = b_i)$ is automatically verified for $j = 1$, since $1 \leq i < j$ is false, so the implication is true.)

In informal terms :

$a_1 < b_1$ or $(a_1 = b_1 \text{ and } a_2 < b_2)$ or $(a_1 = b_1, a_2 = b_2 \text{ and } a_3 < b_3)$ or \dots

In other words, $x_1^{a_1} \cdots x_n^{a_n} < x_1^{b_1} \cdots x_n^{b_n}$ iff the first subscript i such that $a_i \neq b_i$ exists and verifies $a_i < b_i$.

This relation \leq is a total order.

- (b) The monomials less than $x_1 = x_1^1 x_2^0 \cdots x_n^0$ for the lexicographic order contain the monomials $x_1^0 x_2^{a_2} \cdots x_n^{a_n}$, where a_2, \dots, a_n are arbitrary integers in $\mathbb{N} = \mathbb{Z}_{\geq 0}$. There are infinitely many such monomials.
- (c) We show this property by induction on the numbers of variables x_i .

If there is a unique variable, say x_1 , then a strictly decreasing sequence of monomial $x_1^{n_0} > x_1^{n_1} > \cdots$, with $n_i \in \mathbb{N}$, is such that $n_0 > n_1 > \cdots$: such a sequence is necessary finite. This is a property of the natural order in \mathbb{N} : Every non empty subset of \mathbb{N} has a smallest element, so a strictly decreasing infinite sequence in \mathbb{N} doesn't exist.

Suppose that this property is true for $n - 1$ variables, say x_2, \dots, x_n . Consider the sequence

$$x_1^{i_{1,1}} \cdots x_n^{i_{1,n}} > x_1^{i_{2,1}} \cdots x_n^{i_{2,n}} > \cdots > x_1^{i_{k,1}} \cdots x_n^{i_{k,n}} > \cdots$$

By the induction hypothesis, for each fixed exponent $i_{k,1}$ of x_1 , there exists only finitely monomial in this sequence with this exponent for x_1 . As these exponents are at most $i_{1,1}$, the sequence is finite and the induction is done.

- (d) The beginning of the demonstration of Theorem 2.2.2 remains unchanged with the lexicographic order. Then we builds a sequence

$$f, f_1 = f - cg, f_2 = f - cg - c_1 g_1, \dots$$

of polynomials whose leading terms constitute a strictly decreasing sequence for this order, until $f_i = 0$. By (c), this sequence is finite, so one polynomial f_i is zero, which completes the algorithm. \square

Ex. 2.2.10 Apply the proof of theorem 2.2.2 to express $\sum_3 x_1^2 x_2$ in terms of $\sigma_1, \sigma_2, \sigma_3$.

Proof. Explicitly,

$$f = \sum_3 x_1^2 x_2 = x_1^2 x_2 + x_1^2 x_3 + x_1 x_2^2 + x_1 x_3^2 + x_2^2 x_3 + x_2 x_3^2.$$

Note that $x_1^2 x_2 = x_1^2 x_2^1 x_3^0$ is the leading term for the graded lexicographic order, so the following term in the sequence is $g = f - \sigma_1^{2-1} \sigma_2^{1-0} \sigma_3^0 = f - \sigma_1 \sigma_2$.

$$\begin{aligned} \sigma_1 \sigma_2 &= (x_1 + x_2 + x_3)(x_1 x_2 + x_1 x_3 + x_2 x_3) \\ &= x_1^2 x_2 + x_1^2 x_3 + x_1 x_2 x_3 + x_1 x_2^2 + x_2^2 x_3 + x_1 x_2 x_3 + x_1 x_3^2 + x_2 x_3^2 + x_1 x_2 x_3 \\ &= f + 3x_1 x_2 x_3, \end{aligned}$$

thus

$$f = \sum_3 x_1^2 x_2 = \sigma_1 \sigma_2 - 3\sigma_3.$$

\square

Ex. 2.2.11 Let the roots of $y^3 + 2y^2 - 3y + 5$ be $\alpha, \beta, \gamma \in \mathbb{C}$. Find polynomials with integers coefficients that have the following roots:

(a) $\alpha\beta, \alpha\gamma$ and $\beta\gamma$.

(b) $\alpha + 1, \beta + 1$, and $\gamma + 1$.

(c) α^2, β^2 , and γ^2 .

(a) $f = y^3 + 2y^2 - 3y + 5 = (y - \alpha)(y - \beta)(y - \gamma) = y^3 - \sigma_1 y^2 + \sigma_2 y - \sigma_3$,
so $\sigma_1 = -2, \sigma_2 = -3, \sigma_3 = -5$.

$$\begin{aligned} g &= (y - \alpha\beta)(y - \alpha\gamma)(y - \beta\gamma) \\ &= y^3 - (\alpha\beta + \alpha\gamma + \beta\gamma)y^2 + (\alpha^2\beta\gamma + \alpha\beta^2\gamma + \alpha\beta\gamma^2)y + \alpha^2\beta^2\gamma^2 \\ &= y^3 - \sigma_2 y^2 + \sigma_3 \sigma_1 y + \sigma_3^2 \\ &= y^3 + 3y^2 + 10y + 25. \end{aligned}$$

$y^3 + 3y^2 + 10y + 25$ is the polynomial whose roots are $\alpha\beta, \alpha\gamma, \beta\gamma$.

(b)

$$\begin{aligned} g &= (y - \alpha - 1)(y - \beta - 1)(y - \gamma - 1) \\ &= f(y - 1) \\ &= (y - 1)^3 + 2(y - 1)^2 - 3(y - 1) + 5 \\ &= y^3 - 3y^2 + 3y - 1 + 2y^2 - 4y + 2 - 3y + 3 + 5 \\ &= y^3 - y^2 - 4y + 9. \end{aligned}$$

(c) Let $h(y) = (y - \alpha^2)(y - \beta^2)(y - \gamma^2)$. Then

$$\begin{aligned}
h(y^2) &= (y^2 - \alpha^2)(y^2 - \beta^2)(y^2 - \gamma^2) \\
&= (y - \alpha)(y - \beta)(y - \gamma)(y + \alpha)(y + \beta)(y + \gamma) \\
&= (y^3 + 2y^2 - 3y + 5)(y^3 - 2y^2 - 3y - 5) \\
&= (y^3 - 3y)^2 - (2y^2 + 5)^2 \\
&= y^6 - 6y^4 + 9y^2 - 4y^4 - 20y^2 - 25 \\
&= y^6 - 10y^4 - 11y^2 - 25.
\end{aligned}$$

Thus

$$h(y) = (y - \alpha^2)(y - \beta^2)(y - \gamma^2) = y^3 - 10y^2 - 11y - 25.$$

(In particular, $\sigma_2(\alpha^2, \beta^2, \gamma^2) = -11$, which we can verify directly :

$$\alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2 = \sigma_2^2 - 2\sigma_1\sigma_3 = 9 - 20 = -11.)$$

Ex. 2.2.12 Consider the symmetric polynomial $f = \sum_n x_1^{a_1} \cdots x_n^{a_n}$.

(a) Prove that f has $n!$ terms when a_1, \dots, a_n are distinct.

(b) (More challenging) Suppose that the exponents a_1, \dots, a_n break up into r disjoint groups so that exponent within the same group are equal, but exponents from different groups are unequal. Let l_i denote the number of elements in the i th group, so that $l_1 + l_2 + \cdots + l_r = n$. Prove that the number of terms in f is

$$\frac{n!}{l_1! \cdots l_r!}.$$

Proof. (a) Here we suppose that the exponents a_i are distinct

If $\sigma, \tau \in S_n$ and $\sigma \neq \tau$, then $x_{\sigma(1)}^{a_1} \cdots x_{\sigma(n)}^{a_n} \neq x_{\tau(1)}^{a_1} \cdots x_{\tau(n)}^{a_n}$.

Then $\sum_n x_1^{a_1} \cdots x_n^{a_n} = \sum_{\sigma \in S_n} x_{\sigma(1)}^{a_1} \cdots x_{\sigma(n)}^{a_n}$ has $n! = |S_n|$ terms.

(b) Now we suppose that the exponents have same value on $I_1 = \llbracket 1, l_1 \rrbracket$ and on each interval $I_k = \llbracket l_1 + \cdots + l_{k-1} + 1, l_1 + \cdots + l_k \rrbracket$, ($k = 2, \dots, r$), with distinct constants on each interval.

The terms of $\sum_n x_1^{a_1} \cdots x_n^{a_n}$ are the terms of the image of the application

$$\begin{aligned}
\varphi: S_n &\rightarrow F[x_1, \dots, x_n] \\
\sigma &\mapsto x_{\sigma(1)}^{a_1} \cdots x_{\sigma(n)}^{a_n} = \sigma \cdot (x_1^{a_1} \cdots x_n^{a_n}).
\end{aligned}$$

This image is the orbit \mathcal{O}_t de $t = x_1^{a_1} \cdots x_n^{a_n}$ for the group operation defined by $(\sigma, f) \mapsto \sigma \cdot f$.

As $|\mathcal{O}_t| = |S_n|/|\text{Stab}_{S_n}(t)|$, it is sufficient to compute the cardinality of this stabilizer $S = \text{Stab}_{S_n}(t)$, stabilizer in S_n of $x_1^{a_1} \cdots x_n^{a_n}$:

$$S = \{\sigma \in S_n \mid x_{\sigma(1)}^{a_1} \cdots x_{\sigma(n)}^{a_n} = x_1^{a_1} \cdots x_n^{a_n}\}.$$

Note that $\sigma \in S$ iff σ applies I_k on itself :

$$\sigma(I_k) = I_k, k = 1, \dots, r.$$

Let ψ the application

$$\psi : \begin{array}{ccc} S & \rightarrow & S(I_1) \times S(I_2) \times \cdots S(I_r) \\ \sigma & \mapsto & (\sigma_1, \sigma_2, \dots, \sigma_r) \end{array}$$

where $\sigma_k = \sigma|_{I_k}$ is the restriction of σ to I_k .

ψ is bijective, so

$$|S| = l_1!l_2! \cdots l_r!.$$

So the number of terms in $\Sigma_n x_1^{a_1} \cdots x_n^{a_n}$, equal to the cardinality of the orbit of the monomial t , is equal to

$$|\mathcal{O}_t| = |S_n|/|\text{Stab}_{S_n}(x_1^{a_1} \cdots x_n^{a_n})| = \frac{n!}{l_1!l_2! \cdots l_r!}$$

□

Ex. 2.2.13 Let $g_1, g_2 \in F[x_1, \dots, x_n]$ be homogeneous of total degree d_1, d_2 .

(a) Show that $g_1 g_2$ is homogeneous of total degree $d_1 + d_2$.

(b) When is $g_1 + g_2$ homogeneous ?

Proof. (a) Every term m of $g_1 g_2$ is a product of a term m_1 of g_1 with a term m_2 of g_2 .
 $\deg(m) = \deg(m_1 m_2) = \deg(m_1) + \deg(m_2) = d_1 + d_2$. So $g_1 g_2$ is homogeneous of degree $d_1 + d_2$.

(b) $g_1 + g_2$ is homogeneous iff $d_1 = d_2$.

□

Ex. 2.2.14 We define the weight of $\sigma_1^{a_1} \cdots \sigma_n^{a_n}$ to be $a_1 + 2a_2 + \cdots + na_n$.

(a) Prove that $\sigma_1^{a_1} \cdots \sigma_n^{a_n}$ is homogeneous and that its weight is the same as its total degree when considered as a polynomial in x_1, \dots, x_n .

(b) Let $f = F(x_1, \dots, x_n]$ be symmetric and homogeneous of total degree d . Show that f is a linear combination of products $\sigma_1^{a_1} \cdots \sigma_n^{a_n}$ of weight d .

Proof. (a) By Ex. 2.2.13, each σ_k being homogeneous of degree k , the product $\sigma_1^{a_1} \cdots \sigma_n^{a_n}$ is homogeneous. As $\deg(\sigma_k) = k$, $\deg(\sigma_1^{a_1} \cdots \sigma_n^{a_n}) = a_1 + 2a_2 + \cdots + na_n$ is equal to the weight of $\sigma_1^{a_1} \cdots \sigma_n^{a_n}$.

(b) Since f is symmetric, f is a linear combination of products $\sigma_1^{a_1} \cdots \sigma_n^{a_n}$. These products being homogeneous of degree $a_1 + 2a_2 + \cdots + na_n$, and f being homogeneous, by Ex 2.2.13(b), each term of this sum has degree d .

Conclusion : f is a linear combination of products $\sigma_1^{a_1} \cdots \sigma_n^{a_n}$ of weight d .

□

Ex. 2.2.15 Given a polynomial $f \in F[x_1, \dots, x_n]$, let $\deg_i(f)$ be the maximal exponent of x_i which appears in f . Thus $f = x_1^3 x_2 + x_1 x_2^4$ has degree $\deg_1(f) = 3$ and $\deg_2(f) = 4$.

(a) If f is symmetric, explain why the $\deg_i(f)$ are the same for $i = 1, \dots, n$.

(b) Show that $\deg_i(\sigma_1^{a_1} \cdots \sigma_n^{a_n}) = a_1 + a_2 + \cdots + a_n$ for $i = 1, \dots, n$.

Proof. (a) If x_1 appears in a term $c x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ of f , then the transposition $\tau = (1, 2)$ applied to f show that $c x_1^{a_2} x_1^{a_1} \cdots x_n^{a_n}$ is a term of f , so x_2 appears in a term of f with the same exponent. Thus the maximal exponent is the same for the two variables :

$$\deg_1(f) = \deg_2(f),$$

and the same is true for any pair of variables.

(b) As $\sigma_k = \sum_{1 \leq i_1 < \cdots < i_k \leq n} x_{i_1} x_{i_2} \cdots x_{i_k}$, $\deg_i(\sigma_k) = 1$. For polynomial of one variable x , $\deg(pq) = \deg(p) + \deg(q)$, and $\deg_1(f)$ is the degree in x_1 of f as an element of $k[x_2, \dots, x_n][x_1]$, so

$$\deg_i(fg) = \deg_i(f) + \deg_i(g).$$

Therefore $\deg_i(\sigma_1^{a_1} \cdots \sigma_n^{a_n}) = a_1 \deg_i(\sigma_1) + \cdots + a_n \deg_i(\sigma_n) = a_1 + \cdots + a_n$. □

Ex. 2.2.16 This exercise is based on [7, pp. 110-112] and will express the discriminant $\Delta = (x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2$ in terms of the elementary symmetric functions without using a computer. We will use the terminology of Exercises 14 and 15. Note that Δ is homogeneous of total degree 6 and $\deg_i(\Delta) = 4$ for $i = 1, 2, 3$.

(a) Find all products $\sigma_1^{a_1} \sigma_2^{a_2} \sigma_3^{a_3}$ of weight 6 and $\deg_i(\sigma_1^{a_1} \sigma_2^{a_2} \sigma_3^{a_3}) \leq 4$.

(b) Explain how part (a) implies that there are constants l_1, \dots, l_5 such that

$$\Delta = l_1 \sigma_3^2 + l_2 \sigma_1 \sigma_2 \sigma_3 + l_3 \sigma_1^3 \sigma_3 + l_4 \sigma_2^3 + l_5 \sigma_1^2 \sigma_2^2.$$

(c) We will compute the l_i by using the universal property of the elementary symmetric polynomial. For example, to determine l_1 , use the cube roots of unity $1, \omega, \omega^2$ to show that $x^3 - 1$ has coefficient -27 . By applying the ring homomorphism defined by $x_1 \mapsto 1, x_2 \mapsto \omega, x_3 \mapsto \omega^2$ to part (b), conclude that $l_1 = -27$.

(d) Show that $x^3 - x$ has roots $0, \pm 1$ and discriminant 4. By adapting the argument of part (c), conclude that $l_4 = -4$.

(e) Similarly, use $x^3 - 2x^2 + x$ to show that $l_4 = 1$.

(f) Next, note that $x^3 - 2x^2 - x + 2$ has roots $\pm 1, 2$ and use this (together with the known values of l_1, l_4, l_5) to conclude that $l_5 = 1$.

(g) Finally use $x^3 - 3x^2 + 3x - 1$ to show $l_2 + 3l_3 = 6$. Using part (f), this implies $l_2 = 18, l_3 = -4$ and gives the usual formula for Δ .

Proof. (a) By Ex. 14, 15, to find all products $\sigma_1^{a_1} \sigma_2^{a_2} \sigma_3^{a_3}$ of weight 6 verifying $\deg_i(\sigma_1^{a_1} \sigma_2^{a_2} \sigma_3^{a_3}) \leq 4$, it suffices to solve the system of equations

$$\begin{cases} a_1 + 2a_2 + 3a_3 &= 6 \\ a_1 + a_2 + a_3 &\leq 4 \end{cases}$$

The solutions of the first equation are

$$(0, 0, 2), (1, 1, 1), (3, 0, 1), (0, 3, 0), (2, 2, 0), (4, 1, 0), (6, 0, 0).$$

Only the two last solutions don't verify the second condition. So the solutions of the system are

$$(0, 0, 2), (1, 1, 1), (3, 0, 1), (0, 3, 0), (2, 2, 0),$$

which correspond to the symmetric polynomials

$$\sigma_3^2, \sigma_1\sigma_2\sigma_3, \sigma_1^3\sigma_3, \sigma_2^3, \sigma_1^2\sigma_2^2.$$

- (b) As Δ is homogeneous of total degree $\deg(\Delta) = 6$ and as $\deg_i(\Delta) = 4$, $i = 1, 2, 3$, by Ex. 14,15, Δ is a linear combination of products $\sigma_1^{a_1}\sigma_2^{a_2}\sigma_3^{a_3}$ of weight 6.

Moreover, the relative degree to the i -th variable of each of these products is at most 4 : if f has the form

$$\begin{aligned} f &= f_1 + c\sigma_1^4\sigma_2 + d\sigma_1^6 \\ &= f_1 + c(x_1 + x_2 + x_3)^4(x_1x_2 + x_1x_3 + x_2x_3) + d(x_1 + x_2 + x_3)^6, \end{aligned}$$

where $\deg_i(f_1) \leq 4$, then the comparison of degree of x_1^6 gives $d = 0$, and the term in x_1^5 gives $c = 0$.

So there exists coefficients $l_i \in \mathbb{Z}$ such that

$$\Delta = l_1\sigma_3^2 + l_2\sigma_1\sigma_2\sigma_3 + l_3\sigma_1^3\sigma_3 + l_4\sigma_2^3 + l_5\sigma_1^2\sigma_2^2.$$

- (c) The discriminant of $x^3 - 1$ is equal to

$$\Delta(1, \omega, \omega^2) = (1 - \omega)^2(1 - \omega^2)^2(\omega - \omega^2)^2$$

$$\begin{aligned} \sqrt{\Delta} &= (1 - \omega)(1 - \omega^2)(\omega - \omega^2) \\ &= - \begin{vmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{vmatrix} \\ &= -(3\omega^2 - 3\omega) = 3(\omega - \omega^2) \\ &= 3i\sqrt{3}. \end{aligned}$$

Therefore

$$\Delta(1, \omega, \omega^2) = -27.$$

The ring homomorphism defined by $x_1 \mapsto 1, x_2 \mapsto \omega, x_3 \mapsto \omega^2$ sends Δ on $\Delta(1, \omega, \omega^2)$ and σ_k on $\sigma_k(1, \omega, \omega^2)$. As

$$\sigma_1(1, \omega, \omega^2) = \sigma_2(1, \omega, \omega^2) = 0, \sigma_3(1, \omega, \omega^2) = 1,$$

$$l_1 = \Delta(1, \omega, \omega^2) = -27.$$

(d) $x^3 - x = x(x-1)(x+1)$ has roots $0, 1, -1$.

$$\Delta(0, 1, -1) = (0-1)^2(0+1)^2(1+1)^2 = 4 \text{ and } \sigma_1 = 0, \sigma_2 = -1, \sigma_3 = 0, \text{ so } l_4\sigma_2^3 = -l_4 = 4.$$

$$l_4 = -4.$$

(e) $x^3 - 2x^2 + x = x(x-1)^2$ has a discriminant equal to 0, and $\sigma_1 = 2, \sigma_2 = 1, \sigma_3 = 0$, so $l_4 + 4l_5 = 0$, with $l_4 = -4$.

$$l_5 = 1.$$

(f) $x^3 - 2x^2 - x + 2 = x^2(x-2) - (x-2) = (x^2-1)(x-2)$ has roots $1, -1, 2$. Its discriminant is $\Delta = 2^2 1^2 3^2 = 36$, with $\sigma_1 = 2, \sigma_2 = -1, \sigma_3 = -2$.

Thus

$$\begin{aligned} 36 &= l_1\sigma_3^2 + l_2\sigma_1\sigma_2\sigma_3 + l_3\sigma_1^3\sigma_3 + l_4\sigma_2^3 + l_5\sigma_1^2\sigma_2^2 \\ &= 4l_1 + 4l_2 - 16l_3 - l_4 + 4l_5 \\ &= -4 \times 27 + 4l_2 - 16l_3 + 4 + 4. \end{aligned}$$

With a division by 4, $l_2 - 4l_3 = \frac{36+4 \times 27-8}{4} = 9 + 27 - 2 = 34$.

$$l_2 - 4l_3 = 34.$$

(g) $x^3 - 3x^2 + 3x - 1 = (x-1)^3$ has a discriminant equal to 0, with $\sigma_1 = 3, \sigma_2 = 3, \sigma_3 = 1$.

$$\begin{aligned} 0 &= l_1 + 9l_2 + 27l_3 + 27l_4 + 81l_5 \\ &= -27 + 9l_2 + 27l_3 - 27 \times 4 + 81. \end{aligned}$$

With a division by 9, $l_2 + 3l_3 = 3 + 12 - 9 = 6$. So l_2, l_3 are solutions of the system of equations

$$\begin{cases} l_2 - 4l_3 &= 34, \\ l_2 + 3l_3 &= 6. \end{cases}$$

Thus $l_2 = 18, l_3 = -4$, and

$$\Delta = -27\sigma_3^2 + 18\sigma_1\sigma_2\sigma_3 - 4\sigma_1^3\sigma_3 - 4\sigma_2^3 + \sigma_1^2\sigma_2^2.$$

□

Ex. 2.2.17 Use the Newton identities (2.22) to express the power sum s_2, s_3, s_4 in terms of the elementary symmetric polynomials $\sigma_1, \sigma_2, \sigma_3, \sigma_4$.

Proof. $s_r = x_1^r + x_2^r + \cdots + x_n^r$.

We suppose here that the number n of variables is at least 4. Then

$$s_r = \sigma_1 s_{r-1} - \sigma_2 s_{r-2} + \cdots + (-1)^r \sigma_{r-1} s_1 + (-1)^{r-1} r \sigma_r.$$

$$s_1 = \sigma_1,$$

$$\begin{aligned} s_2 &= \sigma_1 s_1 - 2\sigma_2 \\ &= \sigma_1^2 - 2\sigma_2, \end{aligned}$$

$$\begin{aligned} s_3 &= \sigma_1 s_2 - \sigma_2 s_1 + 3\sigma_3 \\ &= \sigma_1(\sigma_1^2 - 2\sigma_2) - \sigma_2 \sigma_1 + 3\sigma_3 \\ &= \sigma_1^3 - 3\sigma_1 \sigma_2 + 3\sigma_3, \end{aligned}$$

$$\begin{aligned} s_4 &= \sigma_1 s_3 - \sigma_2 s_2 + \sigma_3 s_1 - 4\sigma_4 \\ &= \sigma_1(\sigma_1^3 - 3\sigma_1 \sigma_2 + 3\sigma_3) - \sigma_2(\sigma_1^2 - 2\sigma_2) + \sigma_3 \sigma_1 - 4\sigma_4 \\ &= \sigma_1^4 - 4\sigma_1^2 \sigma_2 + 4\sigma_1 \sigma_3 + 2\sigma_2^2 - 4\sigma_4. \end{aligned}$$

Verification with Sage:

```
e = SymmetricFunctions(QQ).e()
e1, e2, e3, e4 = e([1]).expand(4), e([2]).expand(4), e([3]).expand(4), e([4]).expand(4)
R.<x0,x1,x2,x3,y1,y2,y3,y4> = PolynomialRing(QQ, order = 'lex')
J = R.ideal(e1-y1, e2-y2, e3-y3, e4-y4)
G = J.groebner_basis()
s2 = x0^2 + x1^2 + x2^2 + x3^2
s3 = x0^3 + x1^3 + x2^3 + x3^3
s4 = x0^4 + x1^4 + x2^4 + x3^4
g2, g3, g4 = s2.reduce(G), s3.reduce(G), s4.reduce(G)
var('sigma_1,sigma_2,sigma_3,sigma_4')
h2 = g2.subs(y1=sigma_1, y2=sigma_2, y3=sigma_3, y4=sigma_4)
h3 = g3.subs(y1=sigma_1, y2=sigma_2, y3=sigma_3, y4=sigma_4)
h4 = g4.subs(y1=sigma_1, y2=sigma_2, y3=sigma_3, y4=sigma_4)
h2, h3, h4
```

$$(\sigma_1^2 - 2\sigma_2, \sigma_1^3 - 3\sigma_1 \sigma_2 + 3\sigma_3, \sigma_1^4 - 4\sigma_1^2 \sigma_2 + 2\sigma_2^2 + 4\sigma_1 \sigma_3 - 4\sigma_4).$$

□

Ex. 2.2.18 Suppose that complex numbers α, β, γ satisfy the equations

$$\begin{aligned} \alpha + \beta + \gamma &= 3, \\ \alpha^2 + \beta^2 + \gamma^2 &= 5, \\ \alpha^3 + \beta^3 + \gamma^3 &= 12. \end{aligned}$$

Show that $\alpha^n + \beta^n + \gamma^n \in \mathbb{Z}$ for all $n \geq 4$. Also compute $\alpha^4 + \beta^4 + \gamma^4$.

Proof. α, β, γ are the root of

$$p = (x - \alpha)(x - \beta)(x - \gamma) = x^3 - \sigma_1 x^2 + \sigma_2 x - \sigma_3.$$

(We write σ_i in place of $\sigma_i(\alpha, \beta, \gamma)$.)

By Exercice 17, with $n = 3$:

$$\begin{cases} 3 &= s_1 &= \sigma_1 \\ 5 &= s_2 &= \sigma_1^2 - 2\sigma_2 \\ 12 &= s_3 &= \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3. \end{cases}$$

Thus $\sigma_1 = 3, \sigma_2 = \frac{1}{2}(\sigma_1^2 - 5) = \frac{1}{2}(9 - 5) = 2$.

$$\sigma_3 = \frac{1}{3}(12 - \sigma_1^3 + 3\sigma_1\sigma_2) = 4 + \sigma_1\sigma_2 - \frac{\sigma_1^3}{3} = 4 + 6 - 9 = 1.$$

α, β, γ are the roots of $p = x^3 - 3x^2 + 2x - 1$.

If $n \geq 4$, $\alpha^n = 3\alpha^{n-1} - 2\alpha^{n-2} + \alpha^{n-3}$, and similar equations for β, γ . Summing these equations, we obtain

$$s_n = 3s_{n-1} - 2s_{n-2} + s_{n-3}. \quad (5)$$

(This is a particular case of Newton identities (2.22).)

$s_0 = 3, s_1, s_2, s_3$ are in \mathbb{Z} . If we suppose that $s_k \in \mathbb{Z}$ for all $k, 1 \leq k < n$, then (5) show that $s_n \in \mathbb{Z}$, and the induction is done.

$$\forall k \in \mathbb{N}, s_n \in \mathbb{Z}.$$

In particular, $s_4 = 3s_3 - 2s_2 + s_1 = 3 \times 12 - 2 \times 5 + 3 \times 3 = 35$. □

Ex. 2.2.19 Suppose that F is a field of characteristic 0.

(a) Use the Newton identities (2.22) and Theorem 2.2.2 to prove that every symmetric polynomial in $F[x_1, \dots, x_n]$ can be expressed as a polynomial in s_1, \dots, s_n .

(b) Show how to express $\sigma_4 \in F[x_1, x_2, x_3, x_4]$ as a polynomial in s_1, s_2, s_3, s_4 .

Proof. For all $r, 1 \leq r \leq n$,

$$s_r = \sigma_1 s_{r-1} - \sigma_2 s_{r-2} + \dots + (-1)^r \sigma_{r-1} s_1 + (-1)^{r-1} r \sigma_r,$$

and $\sigma_1 = s_1$.

If we suppose that $\sigma_1, \sigma_2, \dots, \sigma_{r-1}$ are polynomials in s_1, s_2, \dots, s_n , the characteristic of the field F being 0 (this allows the division by r), then

$$\sigma_r = \frac{(-1)^{r-1}}{r} (s_r - \sigma_1 s_{r-1} + \sigma_2 s_{r-2} + \dots + (-1)^{r-1} \sigma_{r-1} s_1)$$
 is a polynomial in s_1, \dots, s_n .

Conclusion : for all $r, 1 \leq r \leq n$, σ_r can be expressed as a polynomial in s_1, \dots, s_n .

By Ex. 2.2.17, we obtain

$$\sigma_1 = s_1,$$

$$\begin{aligned}\sigma_2 &= -\frac{1}{2}(s_2 - \sigma_1 s_1) \\ &= \frac{1}{2}(s_1^2 - s_2),\end{aligned}$$

$$\begin{aligned}\sigma_3 &= \frac{1}{3}(s_3 - \sigma_1 s_2 + \sigma_2 s_1) \\ &= \frac{1}{3}\left[s_3 - s_1 s_2 + \frac{1}{2}s_1(s_1^2 - s_2)\right] \\ &= \frac{1}{6}(2s_3 + s_1^3 - 3s_1 s_2),\end{aligned}$$

$$\begin{aligned}\sigma_4 &= -\frac{1}{4}(s_4 - \sigma_1 s_3 + \sigma_2 s_2 - \sigma_3 s_1) \\ &= -\frac{1}{4}\left[s_4 - s_1 s_3 + \frac{1}{2}s_2(s_1^2 - s_2) - \frac{s_1}{6}(2s_3 - 3s_1 s_2 + s_1^3)\right] \\ &= -\frac{1}{24}[6s_4 - 6s_1 s_3 + 3s_2(s_1^2 - s_2) - s_1(2s_3 - 3s_1 s_2 + s_1^3)] \\ &= \frac{1}{24}(-6s_4 + 8s_1 s_3 - 6s_1^2 s_2 + 3s_2^2 + s_1^4).\end{aligned}$$

□

Ex. 2.2.20 Let \mathbb{F}_2 be the field with two elements. Show that in $\mathbb{F}_2[x_1, \dots, x_n]$, it is impossible to express σ_2 as a polynomial in s_1, \dots, s_n when $n \geq 2$.

Proof. Suppose that $\sigma_2 = f(s_1, s_2, \dots, s_n)$, where f is a polynomial with coefficients in \mathbb{F}_2 . If we use the evaluation defined by $x_1 = x_2 = \dots = x_n = 0$, we obtain $0 = f(0, \dots, 0)$.

With the evaluation defined by $x_1 = x_2 = 1$ et $x_i = 0, i > 2$, as $\sigma_2 = \sum_{i < j} x_i x_j$, then $\sigma_2(1, 1, 0, \dots, 0) = 1 \times 1 = 1$ and $s_k(1, 1, 0, \dots, 0) = 1^k + 1^k = 1 + 1 = 0$, so $1 = f(0, \dots, 0)$. As $1 \neq 0$ in \mathbb{F}_2 , this is a contradiction. So it is impossible to express σ_2 as a polynomial in s_1, \dots, s_n when $n \geq 2$. □

2.3 COMPUTING WITH SYMMETRIC POLYNOMIALS

Ex. 2.3.1 Examples 2.3.1 and 2.3.2 showed that the roots of $y^3 + 41y^2 + 138y + 125$ are the cubes of the roots of $y^3 + 2y^2 - 3y + 5$. Verify this numerically.

Proof. We repeat Examples 2.3.1 and 2.3.2 with Sage :

- We build the Groebner basis of the ideal $\langle e_1 - y_1, e_2 - y_2, e_3 - y_3 \rangle$, where e_1, e_2, e_3 are the elementary symmetric polynomials in x_0, x_1, x_2 :

```
e = SymmetricFunctions(QQ).e()
e1, e2, e3 = e([1]).expand(3), e([2]).expand(3), e([3]).expand(3)
R.<x0,x1,x2,y1,y2,y3> = PolynomialRing(QQ, order = 'degrevlex')
```

```
J = R.ideal(e1-y1, e2-y2, e3-y3)
G = J.groebner_basis()
```

• We compute the coefficients of $f = (x - x_0^3)(x - x_1^3)(x - x_2^3)$ as polynomials in x_1, x_2, x_3 :

```
f = (x-x0^3) * (x-x1^3) * (x-x2^3)
coeffs = f.coefficients(x, sparse = False)
coeffs = map(lambda c : R(c), coeffs)
coeffs
```

$$[-x_0^3 x_1^3 x_2^3, x_0^3 x_1^3 + x_0^3 x_2^3 + x_1^3 x_2^3, -x_0^3 - x_1^3 - x_2^3, 1]$$

• The same coefficients as polynomials in $\sigma_1, \sigma_2, \sigma_3$:

```
var('sigma_1,sigma_2,sigma_3')
ncoeffs = [c.reduce(G) for c in coeffs]
nncoeffs = [c.subs(y1 = sigma_1, y2 = sigma_2, y3 = sigma_3) for c in ncoeffs]
nncoeffs
```

$$[-\sigma_3^3, \sigma_2^3 - 3\sigma_1\sigma_2\sigma_3 + 3\sigma_3^2, -\sigma_1^3 + 3\sigma_1\sigma_2 - 3\sigma_3, 1]$$

• We apply the substitution $\sigma_1 \mapsto -2, \sigma_2 \mapsto -3, \sigma_3 \mapsto -5$ and compute the polynomial p whose roots are $\alpha_1^3, \alpha_2^3, \alpha_3^3$, where $\alpha_1, \alpha_2, \alpha_3$ are the roots of $y^3 + 2y^2 - 3y + 5$.

```
nncoeffs = [c.subs(sigma_1 = -2, sigma_2 = -3, sigma_3 = -5) for c in nncoeffs]
p = sum(nncoeffs[i]*y^i for i in range(1+f.degree(x)))
p
```

$$y^3 + 41y^2 + 138y + 125$$

• Numerical verification:

```
S.<y> = PolynomialRing(ComplexField(prec = 40))
[c[0] for c in S(p).roots()]

[-37.399476110, -1.8002619448 - 0.31835473525 i, -1.8002619448 + 0.31835473525 i]

q = y^3+2*y^2-3*y+5
l = [c[0]^3 for c in q.roots()]
l

[-37.399476110, -1.8002619448 - 0.31835473525 i, -1.8002619448 + 0.31835473525 i]
```

□

Ex. 2.3.2 Use the method of Example 2.3.1 or 2.3.2 to find the cubic polynomial whose roots are the fourth powers of the roots of the polynomial $y^3 + 2y^2 - 3y + 5$.

Proof. Same method in Sage as in Ex.2.3.1

```

e = SymmetricFunctions(QQ).e()
e1, e2, e3 = e([1]).expand(3), e([2]).expand(3), e([3]).expand(3)
R.<x0,x1,x2,y1,y2,y3> = PolynomialRing(QQ, order = 'degrevlex')
J = R.ideal(e1-y1, e2-y2, e3-y3)
G = J.groebner_basis()
f = (x-x0^4) * (x-x1^4) * (x-x2^4)
coeffs = f.coefficients(x, sparse = False)
coeffs = map(lambda c : R(c), coeffs)
coeffs

[-x0^4x1^4x2^4, x0^4x1^4 + x0^4x2^4 + x1^4x2^4, -x0^4 - x1^4 - x2^4, 1]
var('sigma_1,sigma_2,sigma_3,y')
ncoeffs = [c.reduce(G) for c in coeffs]
nncoeffs = [c.subs(y1 = sigma_1, y2 = sigma_2, y3 = sigma_3) for c in ncoeffs]
nncoeffs

[-x0^4x1^4x2^4, x0^4x1^4 + x0^4x2^4 + x1^4x2^4, -x0^4 - x1^4 - x2^4, 1]
nnncoeffs = [c.subs(sigma_1 = -2, sigma_2 = -3, sigma_3 = -5) for c in nncoeffs]
p = sum(nnncoeffs[i]*y^i for i in range(1+f.degree(x)))
p

```

$$y^3 - 122y^2 - 379y - 625.$$

So the cubic polynomial whose roots are the fourth powers of the roots of the polynomial $y^3 + 2y^2 - 3y + 5$ is

$$y^3 - 122y^2 - 379y - 625.$$

□

Ex. 2.3.4 Given a cubic $x^3 + bx^2 + cx + d$, what condition must b, c, d satisfy in order that one root be the average of the other two ?

Proof. • Suppose that the polynomial $f = x^3 + bx^2 + cx + d = (x - x_1)(x - x_2)(x - x_3)$ has one root which is the average of the other two. We choose a numbering of the roots such that

$$x_3 = \frac{x_1 + x_2}{2}.$$

Then

$$\begin{aligned}
-b = \sigma_1 &= x_1 + x_2 + \left(\frac{x_1 + x_2}{2}\right) \\
&= \frac{3}{2}(x_1 + x_2), \\
c = \sigma_2 &= x_1x_2 + x_2x_3 + x_1x_3 \\
&= x_1x_2 + \left(\frac{x_1 + x_2}{2}\right)(x_1 + x_2) \\
&= x_1x_2 + \frac{1}{2}(x_1 + x_2)^2, \\
-d = \sigma_3 &= x_1x_2 \left(\frac{x_1 + x_2}{2}\right) \\
&= \frac{1}{2}(x_1 + x_2)x_1x_2.
\end{aligned}$$

Let $s = x_1 + x_2, p = x_1x_2$. The preceding equations give

$$b = -\frac{3}{2}s, \quad (6)$$

$$c = p + \frac{1}{2}s^2, \quad (7)$$

$$d = -\frac{1}{2}sp. \quad (8)$$

We eliminate s, p from these equations :

$$\begin{aligned} s &= -\frac{2}{3}b, \\ p &= c - \frac{1}{2}\left(-\frac{2}{3}b\right)^2 \\ &= c - \frac{2}{9}b^2, \\ d &= -\frac{1}{2}\left(-\frac{2}{3}b + \frac{4}{27}b^3\right) \\ &= \frac{1}{3}bc - \frac{2}{27}b^3. \end{aligned}$$

So the coefficients b, c, d verify

$$2b^3 - 9bc + 27d = 0.$$

• Conversely, suppose that b, c, d verify

$$2b^3 - 9bc + 27d = 0. \quad (9)$$

Let $s = -\frac{2}{3}b, p = c - \frac{2}{9}b^2$. Then $b = -\frac{3}{2}s, c = p + \frac{2}{9}b^2 = p + \frac{1}{2}\left(\frac{2}{3}b\right)^2 = p + \frac{1}{2}s^2$: (6) et (7) sont vérifiés.

By the equation (9),

$$\begin{aligned} d &= \frac{1}{3}bc - \frac{2}{27}b^3 \\ &= -\frac{1}{2}\left(-\frac{2}{3}b\right)\left(c - \frac{2}{9}b^2\right) \\ &= -\frac{1}{2}sp. \end{aligned}$$

So s, p verify the system (6),(7),(8) :

$$\begin{aligned} b &= -\frac{3}{2}s, \\ c &= p + \frac{1}{2}s^2, \\ d &= -\frac{1}{2}sp. \end{aligned}$$

Let x_1, x_2 the complex roots of $x^2 - sx + p$. Then $x_1 + x_2 = s, x_1x_2 = p$. Let $x_3 = \frac{x_1+x_2}{2} = \frac{1}{2}s$. Then

$$\begin{aligned}\sigma_1 &= x_1 + x_2 + x_3 \\ &= \frac{3}{2}s \\ &= -b \\ \sigma_2 &= x_1x_2 + x_2x_3 + x_1x_3 \\ &= x_1x_2 + \left(\frac{x_1+x_2}{2}\right)(x_1+x_2) \\ &= x_1x_2 + \frac{1}{2}(x_1+x_2)^2 \\ &= p + \frac{1}{2}s^2 \\ &= c \\ \sigma_3 &= x_1x_2x_3 \\ &= \frac{1}{2}sp \\ &= -d\end{aligned}$$

Thus x_1, x_2, x_3 are the roots of $(x - x_1)(x - x_2)(x - x_3) = x^3 - \sigma_1x^2 + \sigma_2x - \sigma_3 = x^3 + bx^2 + cx + d$, and $x_3 = \frac{x_1+x_2}{2}$.

Conclusion : one of the roots of $x^3 + bx^2 + cx + d$ the average of the other two iff $2b^3 - 9bc + 27d = 0$. \square

Ex. 2.3.5 Given a quartic $x^4 + bx^3 + cx^2 + dx + e$, what condition must b, c, d, e satisfy in order that one root be the negative of another ?

Proof. The polynomial

$$f = x^4 + bx^3 + cx^2 + dx + e = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \alpha_4)$$

has two opposite roots iff

$$(\alpha_1 + \alpha_2)(\alpha_1 + \alpha_3)(\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3)(\alpha_2 + \alpha_4)(\alpha_3 + \alpha_4) = 0$$

Let

$$u = (x_1 + x_2)(x_1 + x_3)(x_1 + x_4)(x_2 + x_3)(x_2 + x_4)(x_3 + x_4).$$

u is symmetric, so is a polynomial in $\sigma_1, \sigma_2, \sigma_3, \sigma_4$.

We obtain this polynomial with the following Sage instructions

```
e = SymmetricFunctions(QQ).e()
e1,e2,e3,e4 = e([1]).expand(4),e([2]).expand(4),e([3]).expand(4),e([4]).expand(4)
R.<x0,x1,x2,x3,y1,y2,y3,y4> = PolynomialRing(QQ, order = 'lex')
J = R.ideal(e1-y1,e2-y2,e3-y3,e4-y4)
G = J.groebner_basis()
u = (x0+x1)*(x0+x2)*(x0+x3)*(x1+x2)*(x1+x3)*(x2+x3)
var('sigma_1,sigma_2,sigma_3,sigma_4')
u.reduce(G).subs(y1=sigma_1, y2 = sigma_2,y3=sigma_3,y4=sigma_4)
```


$$\sigma_1\sigma_2\sigma_3 - \sigma_1^2\sigma_4 - \sigma_3^2.$$

So

$$u = \sigma_1\sigma_2\sigma_3 - \sigma_1^2\sigma_4 - \sigma_3^2.$$

The evaluation ring homomorphism defined by $x_i \mapsto \alpha_i, i = 1, 2, 3, 4$ verifies

$$\sigma_1 \mapsto -b, \sigma_2 \mapsto c, \sigma_3 \mapsto -d, \sigma_4 \mapsto e.$$

So $(\alpha_1 + \alpha_2)(\alpha_1 + \alpha_3)(\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3)(\alpha_2 + \alpha_4)(\alpha_3 + \alpha_4) = bcd - b^2e - d^2$.

Conclusion : $f = x^4 + bx^3 + cx^2 + dx + e$ is such that one root is the negative of another iff $bcd - b^2e - d^2 = 0$. \square

Ex. 2.3.6 Find the quartic polynomial whose roots are obtained by adding 1 to each of the roots of $x^4 + 3x^2 + 4x + 7$.

Proof. Let $f = x^4 + 3x^2 + 4x + 7 = (x - x_1)(x - x_2)(x - x_3)(x - x_4)$.

The polynomial whose roots are $1 + x_1, 1 + x_2, 1 + x_3, 1 + x_4$ is

$$\begin{aligned} g &= (x - 1 - x_1)(x - 1 - x_2)(x - 1 - x_3)(x - 1 - x_4) \\ &= f(x - 1) \\ &= (x - 1)^4 + 3(x - 1)^2 + 4(x - 1) + 7 \\ &= x^4 - 4x^3 + 6x^2 - 4x + 1 + 3x^2 - 6x + 3 + 4x - 4 + 7 \\ &= x^4 - 4x^3 + 9x^2 - 6x + 7. \end{aligned}$$

If x_1, x_2, x_3, x_4 are the roots of f , then $x_1 + 1, x_2 + 1, x_3 + 1, x_4 + 1$ are the roots of

$$g = x^4 - 4x^3 + 9x^2 - 6x + 7.$$

\square

2.4 THE DISCRIMINANT

Ex. 2.4.1 Let M be the $n \times n$ matrix appearing on the right-hand side of the Vandermonde formula given in Proposition 2.4.5. Prove that (2.32) follows from the fact that M and its transpose both have determinant $\sqrt{\Delta}$.

Proof. Let a_1, a_2, \dots, a_n be elements of a field F , and

$$A_n = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ a_1^2 & a_2^2 & \cdots & a_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{n-1} & a_2^{n-1} & \cdots & a_n^{n-1} \end{pmatrix}$$

We show by induction on $n, n \geq 2$ that

$$\det(A_n) = \prod_{1 \leq i < j \leq n} (a_j - a_i).$$

$$\det(A_2) = \begin{vmatrix} 1 & 1 \\ a_1 & a_2 \end{vmatrix} = a_2 - a_1 = \prod_{1 \leq i < j \leq 2} (a_j - a_i).$$

Suppose that this formula is true for the integer $n - 1, n \geq 3$. We will show that it is true for the integer n .

If there exists a pair $(i, j), i \neq j$ such that $a_i = a_j$, then two columns of A_n are identical, so $\det(A_n) = 0 = \prod_{1 \leq i < j \leq n} (a_j - a_i)$.

We can so suppose that the $a_i, 1 \leq i \leq n$ are distinct.

Let the polynomial $P \in F[X]$ given by

$$P = \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ a_1 & a_2 & \cdots & a_{n-1} & X \\ a_1^2 & a_2^2 & \cdots & a_{n-1}^2 & X^2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_1^{n-1} & a_2^{n-1} & \cdots & a_{n-1}^{n-1} & X^{n-1} \end{pmatrix}$$

Then $\det(A_n) = P(a_n)$, and $P(a_1) = P(a_2) = \cdots = P(a_{n-1}) = 0$. As a_1, a_2, \dots, a_{n-1} are distinct roots of P , with $\deg(P) = n - 1$, P is factored as

$$P = k(X - a_1) \cdots (X - a_{n-1}), k \in F,$$

where k is the coefficient of X^{n-1} in P , so k is the cofactor of X^{n-1} in $\det(P)$: so

$$k = \det(A_{n-1}) = \prod_{1 \leq i < j \leq n-1} (a_j - a_i)$$

by the induction hypothesis.

Therefore

$$\det(A_n) = P(a_n) = \prod_{1 \leq i < j \leq n-1} (a_j - a_i) \prod_{i=1}^n (a_n - a_i) = \prod_{1 \leq i < j \leq n} (a_j - a_i),$$

which completes the induction.

The matrix

$$B_n = \begin{pmatrix} a_1^{n-1} & a_2^{n-1} & \cdots & a_n^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \cdots & a_n \\ 1 & 1 & \cdots & 1 \end{pmatrix}$$

is obtained from A_n by $\frac{n(n-1)}{2}$ transpositions of rows: $n - 1$ to put the last row in first position, then $n - 2$ to put which is now the last row in second position, and so on.

Thus $\det(B_n) = (-1)^{(n(n-1))/2} \det(A_n)$.

As the number of factors in $\prod_{1 \leq i < j \leq n} (a_j - a_i)$ is $\frac{n(n-1)}{2}$,

$$\prod_{1 \leq i < j \leq n} (a_j - a_i) = (-1)^{(n(n-1))/2} \prod_{1 \leq i < j \leq n} (a_i - a_j).$$

Consequently,

$$\det(B_n) = \prod_{1 \leq i < j \leq n} (a_i - a_j).$$

Applying this result in the field $F(x_1, \dots, x_n)$, we obtain that

$$\sqrt{\Delta} = \prod_{1 \leq i < j \leq n} (x_i - x_j) = \begin{vmatrix} x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \\ x_1^{n-2} & x_2^{n-2} & \cdots & x_n^{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ x_1 & x_2 & \cdots & x_n \\ 1 & 1 & \cdots & 1 \end{vmatrix}$$

If $A = \begin{pmatrix} x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} \\ x_1^{n-2} & x_2^{n-2} & \cdots & x_n^{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ x_1 & x_2 & \cdots & x_n \\ 1 & 1 & \cdots & 1 \end{pmatrix}$, then ${}^t A = \begin{pmatrix} x_1^{n-1} & x_1^{n-2} & \cdots & x_1 & 1 \\ x_2^{n-1} & x_2^{n-2} & \cdots & x_2 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_n^{n-1} & x_n^{n-2} & \cdots & x_n & 1 \end{pmatrix}$

thus

$$\Delta = \det(A)^2 = \det(A {}^t A) = \begin{vmatrix} s_{2n-2} & s_{2n-3} & \cdots & s_n & s_{n-1} \\ s_{2n-3} & s_{2n-4} & \cdots & s_{n-1} & s_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ s_n & s_{n-1} & \cdots & s_2 & s_1 \\ s_{n-1} & s_{n-2} & \cdots & s_1 & s_0 \end{vmatrix}$$

□

Ex. 2.4.2 Let F have characteristic $\neq 2$, and let $f \in F[x_1, \dots, x_n]$ satisfy $\tau \cdot f = -f$ for all transpositions $\tau \in S_n$. Prove that $f = B\sqrt{\Delta}$ for some $B \in F[\sigma_1, \dots, \sigma_n]$.

Proof. Here, the field F have characteristic $\neq 2$.

Let $f \in F[x_1, \dots, x_n]$ such that $\tau \cdots f = -f$ for all transpositions $\tau \in S_n$.

If $\sigma \in A_n$ is an even permutation, then σ is product of an even number of permutations :

$$\sigma = \tau_1 \tau_2 \cdots \tau_{2k}.$$

As the group S_n acts on $F[x_1, \dots, x_n]$, $\sigma \cdot f = \tau_1 \cdot (\tau_2 \cdot (\cdots (\tau_{2k} \cdot f) \cdots)) = (-1)^{2k} f = f$. Therefore f is invariant under A_n and so the theorem 2.4.4 applies:

There exist $A, B \in F[\sigma_1, \dots, \sigma_n]$ such that

$$f = A + B\sqrt{\Delta}.$$

Therefore $-f = \tau \cdot f = \tau \cdot A + (\tau \cdot B)(\tau \cdot \sqrt{\Delta}) = A - B\sqrt{\Delta}$ (by 2.31).

So $f = A + B\sqrt{\Delta}$ and $f = -A + B\sqrt{\Delta}$, thus $2A = 0$. Since the characteristic is not 2, $A = 0$, therefore

$$f = B\sqrt{\Delta}, B \in F[\sigma_1, \dots, \sigma_n].$$

□

Ex. 2.4.3 Let $f = x^2 + bx + c \in F[x]$. Use the definition of discriminant given in the text to show that $\Delta(f) = b^2 - 4c$.

Proof. Let $f = x^2 + bx + c$, $b, c \in F$.

$$\Delta = (x_1 - x_2)^2 = x_1^2 + x_2^2 - 2x_1x_2 = (x_1 + x_2)^2 - 4x_1x_2 = \sigma_1^2 - 4\sigma_2.$$

The ring homomorphism which sends σ_1 on $-b$ and σ_2 on c send Δ on

$$\Delta(-b, c) = b^2 - 4c,$$

which is by definition the discriminant of $x^2 + bx + c$.

□

Ex. 2.4.4 Let $f \in F[x]$ be monic, and suppose that $f = (x - \alpha_1) \cdots (x - \alpha_n)$ in some field F containing F . Prove that $\Delta(f) \neq 0$ if and only if $\alpha_1, \dots, \alpha_n$ are distinct. This shows that f has distinct roots if and only if its discriminant is nonvanishing.

Proof. Let $f \in F[x]$ such that $f = (x - \alpha_1) \cdots (x - \alpha_n)$ in an extension L of K .

By Proposition 2.4.3,

$$\Delta(f) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2. \quad (10)$$

- If $\Delta(f) \neq 0$, by (10), for all pairs (i, j) , $1 \leq i < j \leq n$, $\alpha_i - \alpha_j \neq 0$. The roots α_i are so distinct.

- If the roots α_i , $1 \leq i \leq n$, are distinct roots, then $\alpha_i - \alpha_j \neq 0$ for all (i, j) such that $1 \leq i < j \leq n$, thus $\Delta(f) \neq 0$. □

Ex. 2.4.5 Show that $\sqrt{\Delta} \in F[x_1, \dots, x_n]$ is symmetric if and only if F is a field of characteristic 2.

Proof. By Proposition 2.4.1, if τ is a transposition in S_n ,

$$\tau \cdot \sqrt{\Delta} = -\sqrt{\Delta}.$$

- If the field F is of characteristic 2, $-\sqrt{\Delta} = +\sqrt{\Delta}$, so for all transpositions τ ,

$$\tau \cdot \sqrt{\Delta} = \sqrt{\Delta}.$$

Therefore $\sqrt{\Delta}$ is a symmetric polynomial.

- If the field F is not of characteristic 2, as $\sqrt{\Delta} \neq 0$,

$$\tau \cdot \sqrt{\Delta} = -\sqrt{\Delta} \neq \sqrt{\Delta},$$

so $\sqrt{\Delta}$ is not symmetric. □

Ex. 2.4.6 This exercise will describe how to solve quadratic equations over a field F of characteristic 2.

- Given $b \in F$, we will assume there is a larger field $F \subset L$ such that $b = \beta^2$ for some $\beta \in L$. Show that β is unique and that β is the unique root of $x^2 + b$. Because of this, we denote β by \sqrt{b} .
- Now suppose that $f = x^2 + ax + b$ is a quadratic polynomial in $F[x]$ with $a \neq 0$. Suppose also that f is irreducible over F , so that it has no roots in F . We will see in Chapter 3 that f has a root α in a field L containing F . Prove that α cannot be written in the form $\alpha = u + v\sqrt{w}$, where $u, v, w \in F$.
- Part (b) shows that solving a quadratic equation with nonzero x -coefficient requires more than square roots. We do this as follows. If $b \in F$, let $R(b)$ denote a root of $x^2 + x + b$ (possibly lying in some larger field). We call $R(b)$ and $R(b) + 1$ the 2-roots of b . Prove that the roots of $x^2 + x + b$ are $R(b)$ and $R(b) + 1$, and explain why adding 1 to the second 2-root gives the first.
- Show that the roots of $f = x^2 + ax + b$, $a \neq 0$, are $aR(b/a^2)$ and $a(R(b/a^2) + 1)$.

Proof. (a) Let L and extension of F and $\beta \in L$ such that $\beta^2 = b$.

As $x^2 - b = x^2 - \beta^2 = (x - \beta)^2$, β is the unique root of $x^2 - b = x^2 + b$. We write $\beta = \sqrt{b} \in L$.

- (b) Suppose that $f = x^2 + ax + b$, $a \neq 0$ is irreducible on F . As $\deg(f) = 2$, this is equivalent to the fact that f has no root in F . f has a root α in an extension $L \supset F$.

If $\alpha = u + v\sqrt{w}$, $u, v, w \in F$, then $v \neq 0$, otherwise $\alpha \in F$, in contradiction with the irreducibility of f .

Then

$$\begin{aligned} 0 &= \alpha^2 + a\alpha + b \\ &= u^2 + wv^2 + a(u + v\sqrt{w}) + b \\ &= u^2 + wv^2 + au + b + av\sqrt{w} \\ &= s + t\sqrt{w}, \end{aligned}$$

where $s = u^2 + wv^2 + au + b \in F, t = av \in F, t \neq 0$.

Thus $\sqrt{w} = -s/t \in F$, so $\alpha \in F$, in contradiction with the irreducibility of f .

Conclusion : $\alpha = u + v\sqrt{w}$, $u, v, w \in F$ is impossible.

- (c) Write $R(b)$ a root of $x^2 + x + b$ in an extension of F .

As $R(b)^2 + R(b) + b = 0$, $(R(b) + 1)^2 + (R(b) + 1) + b = R(b)^2 + 1 + R(b) + 1 + b = R(b)^2 + R(b) + b = 0$.

As $R(b) + 1 + 1 = R(b)$, the two (distinct) roots of $x^2 + x + b$ are $R(b), R(b + 1)$, and $\sigma : x \mapsto x + 1$ exchanges the two roots.

- (d) For all $y \in F$,

$$\begin{aligned} f(y) = 0 &\iff y^2 + ay + b = 0 \\ &\iff \left(\frac{y}{a}\right)^2 + \left(\frac{y}{a}\right) + \frac{b}{a^2} = 0 \\ &\iff \frac{y}{a} \in \left\{ R\left(\frac{b}{a^2}\right), R\left(\frac{b}{a^2}\right) + 1 \right\} \\ &\iff y \in \left\{ aR\left(\frac{b}{a^2}\right), a\left[R\left(\frac{b}{a^2}\right) + 1\right] \right\}. \end{aligned}$$

The roots of $x^2 + ax + b, a \neq 0$ are so $aR\left(\frac{b}{a^2}\right), a\left[R\left(\frac{b}{a^2}\right) + 1\right]$.

□

Ex. 2.4.7 Explain how the third property of (2.31) was used (implicitly) in (2.28) in the proof of Proposition 2.4.1.

Proof. Knowing that $\tau \cdot \sqrt{\Delta} = -\sqrt{\Delta}$ for a transposition $\tau \in S_n$, we show by induction on l that

$$(\tau_l \cdots \tau_1) \cdot \sqrt{\Delta} = (-1)^l \sqrt{\Delta}.$$

By the induction hypothesis $(\tau_l \cdots \tau_1) \cdot \sqrt{\Delta} = -\sqrt{\Delta}$, we deduce, using 2.31

$$\begin{aligned} (\tau_{l+1} \tau_l \cdots \tau_1) \cdot \sqrt{\Delta} &= \tau_{l+1} \cdot [(\tau_l \cdots \tau_1) \cdot \sqrt{\Delta}] \\ &= \tau_{l+1} \cdot ((-1)^l \sqrt{\Delta}) \\ &= (-1)^l \tau_{l+1} \cdot \sqrt{\Delta} \\ &= (-1)^{l+1} \sqrt{\Delta}. \end{aligned}$$

□

Ex. 2.4.8 In this exercise, you will prove that although Δ factors in $F[x_1, \dots, x_n]$, it is irreducible in $F[\sigma_1, \dots, \sigma_n]$ when F has characteristic different from 2. To begin the proof, assume that $\Delta = AB$, where $A, B \in F[\sigma_1, \dots, \sigma_n]$ are nonconstant.

- (a) Using the definition of Δ and unique factorization in $F[x_1, \dots, x_n]$, show that A is divisible in $F[x_1, \dots, x_n]$ by $x_i - x_j$ for some $1 \leq i < j \leq n$.
- (b) Given $1 \leq i < j \leq n$ and $1 \leq l < m \leq n$, show that there is a permutation $\sigma \in S_n$ such that $\sigma(i) = l$ and $\sigma(j) = m$.
- (c) Use part (a) and (b) to show that A is divisible by $x_l - x_m$ for all $1 \leq l < m \leq n$.
- (d) Conclude that A is a multiple of $\sqrt{\Delta}$ and that the same is true for B .
- (e) Show that part (d) implies that A and B are constant multiples of $\sqrt{\Delta}$ and explain why this contradicts $A, B \in F[\sigma_1, \dots, \sigma_n]$.
- (f) Finally, suppose that F has characteristic 2. Prove that Δ is not irreducible.

Proof. (a) Suppose that $\Delta = AB$, where $A, B \in F[\sigma_1, \dots, \sigma_n]$ are nonconstant.

As A is not a constant, it is divisible by an irreducible factor $h \in F[x_1, \dots, x_n]$. This irreducible factor h divides Δ , whose only irreducible factors are associate to $x_i - x_j, 1 \leq i < j \leq n$. $F[x_1, \dots, x_n]$ being a factorial domain, there exists a pair of subscripts (i, j) and $\lambda \in F^*$ such that $h = \lambda(x_i - x_j), 1 \leq i < j \leq n$.

Conclusion :

A is divisible in $k[x_1, \dots, x_n]$ by a factor $x_i - x_j$, for some $(i, j), 1 \leq i < j \leq n$.

- (b) The set $U = \llbracket 1, n \rrbracket \setminus \{i, j\}$ et $V = \llbracket 1, n \rrbracket \setminus \{l, m\}$ have same cardinality $n - 2$, so there exists a bijection $f : U \rightarrow V$.

Let $\sigma : \llbracket 1, n \rrbracket \rightarrow \llbracket 1, n \rrbracket$ defined by $\sigma(k) = f(k)$ if $k \in U, \sigma(i) = l, \sigma(j) = m$. Then σ is bijective (the application τ defined by $\tau(m) = f^{-1}(m)$ if $m \in V, \tau(l) = i, \tau(m) = j$ satisfies $\tau \circ \sigma = \sigma \circ \tau = e$).

There exists $\sigma \in S_n$ such that $\sigma(i) = l, \sigma(j) = m$.

- (c) By (a), $A = (x_i - x_j)C, C \in k[x_1, \dots, x_n]$.

As A is symmetric, using the permutation σ of (b),

$$\begin{aligned} A &= \sigma \cdot A \\ &= \sigma \cdot [(x_i - x_j)C] \\ &= \sigma \cdot (x_i - x_j) \sigma \cdot C \\ &= (x_l - x_m)(\sigma \cdot C). \end{aligned}$$

So A is divisible by $x_l - x_m, 1 \leq l < m \leq n$.

(d) As these factors are irreducible and not associate, their product divides A , thus

$$\sqrt{\Delta} = \prod_{1 \leq l < m \leq n} (x_l - x_m) \mid A.$$

The same reasoning applies to B , which is also divisible by $\sqrt{\Delta}$.

(e) $A = A_1\sqrt{\Delta}, B = B_1\sqrt{\Delta}$, where $A_1, B_1 \in F[x_1, \dots, x_n]$.

Thus $\Delta = AB = A_1B_1\Delta$, with $\Delta \neq 0$, therefore $A_1B_1 = 1$, which implies that $A_1 = a \in F^*, B_1 = b \in F^*$:

$$A = a\sqrt{\Delta}, B = b\sqrt{\Delta}, a, b \in F^*.$$

But $A \in F[\sigma_1, \dots, \sigma_n]$, thus for all transposition τ in S_n ,

$$A = \tau \cdot A = \tau \cdot (a\sqrt{\Delta}) = a\tau \cdot \sqrt{\Delta} = -a\sqrt{\Delta} = -A.$$

So $2A = 0$, and as the characteristic of F is not 2, $A = 0$, so $\Delta = 0$, which is a contradiction.

Conclusion : Δ is irreducible in $F[\sigma_1, \dots, \sigma_n]$.

(f) If the characteristic of F is 2, then $\sqrt{\Delta}$ is symmetric, since for all transposition τ , $\tau \cdot \sqrt{\Delta} = -\sqrt{\Delta} = \sqrt{\Delta}$.

Thus $\Delta = (\sqrt{\Delta})^2 = D^2$, where $D = \sqrt{\Delta} \in F[\sigma_1, \dots, \sigma_n]$: therefore Δ is not irreducible in $F[\sigma_1, \dots, \sigma_n]$ if the characteristic of F is 2. □

Ex. 2.4.9 For $n = 4$, the variables x_1, x_2, x_3, x_4 have discriminant

$$\Delta = (x_1 - x_2)^2(x_1 - x_3)^2(x_1 - x_4)^2(x_2 - x_3)^2(x_2 - x_4)^2(x_3 - x_4)^2.$$

Let $y_1 = x_1x_2 + x_3x_4, y_2 = x_1x_3 + x_2x_4, y_3 = x_1x_4 + x_2x_3$, and consider

$$\theta(y) = (y - y_1)(y - y_2)(y - y_3).$$

This is a cubic polynomial in y . As in the text, the discriminant of θ will be denoted $\Delta(\theta)$. Show that $\Delta(\theta) = \Delta$.

Proof.

$$\begin{aligned} y_1 - y_2 &= x_1x_2 + x_3x_4 - x_1x_3 - x_2x_4 = x_1(x_2 - x_3) - x_4(x_2 - x_3) = (x_1 - x_4)(x_2 - x_3) \\ y_1 - y_3 &= x_1x_2 + x_3x_4 - x_1x_4 - x_2x_3 = x_1(x_2 - x_4) - x_3(x_2 - x_4) = (x_1 - x_3)(x_2 - x_4) \\ y_2 - y_3 &= x_1x_3 + x_2x_4 - x_1x_4 - x_2x_3 = x_1(x_3 - x_4) - x_2(x_3 - x_4) = (x_1 - x_2)(x_3 - x_4), \end{aligned}$$

Therefore

$$\begin{aligned} \Delta(\theta) &= (y_1 - y_2)^2(y_1 - y_3)^2(y_2 - y_3)^2 \\ &= [(x_1 - x_4)(x_2 - x_3)(x_1 - x_3)(x_2 - x_4)(x_1 - x_2)(x_3 - x_4)]^2 \\ &= \Delta. \end{aligned}$$
□

Ex. 2.4.10 Let $C, D \in F[\sigma_1, \dots, \sigma_n]$ be nonzero and relatively prime. This exercise will show that C and D remain relatively prime when regarded as elements of $F[x_1, \dots, x_n]$.

- (a) Show that C^m, D^m are relatively prime in $F[\sigma_1, \dots, \sigma_n]$ for any positive integer m .
- (b) Suppose that $p \in F[x_1, \dots, x_n]$ is a nonconstant polynomial dividing C and D . Prove that $\sigma \cdot p$ divides C and D for all $\sigma \in S_n$.
- (c) As in Exercise 7 of Section 2.2, let $P = \prod_{\sigma \in S_n} \sigma \cdot p$. Show that P divides $C^{n!}$ and $D^{n!}$, and then use part (a) and Exercise 7 of Section 2.2 to obtain a contradiction.

Proof. (a) If p is an irreducible factor in $F[\sigma_1, \dots, \sigma_n]$ which divides C^m and D^m ($m \in \mathbb{N}^*$), as $F[\sigma_1, \dots, \sigma_n] \simeq F[u_1, \dots, u_n]$ is a factorial domain, p divides C and p divides D , which is in contradiction with the fact that C, D are relatively prime in $F[\sigma_1, \dots, \sigma_n]$. Consequently C^m, D^m are relatively prime in $F[\sigma_1, \dots, \sigma_n]$.

- (b) If p is an irreducible factor in $F[x_1, \dots, x_n]$ which divides C et D , then $C = pE, E \in F[x_1, \dots, x_n]$. As C is symmetric, we obtain, using 2.31:

$$C = \sigma \cdot C = (\sigma \cdot p)(\sigma \cdot E). \quad (11)$$

Therefore $\sigma \cdot p$ divides C for all $\sigma \in S_n$, and it is the same for D .

- (c) The product, for all $\sigma \in S_n$ of the relations (11) gives :

$$C^{n!} = \prod_{\sigma \in S_n} \sigma \cdot p \prod_{\sigma \in S_n} \sigma \cdot E.$$

Therefore $P = \prod_{\sigma \in S_n} \sigma \cdot p$ divides $C^{n!}$ in $F[x_1, \dots, x_n]$, and similarly for D .

- (d) By Exercise 2.2.7, P is symmetric, and $C^{n!} = PQ, D^{n!} = PS, Q, S \in F[x_1, \dots, x_n]$.

As $C^{n!}, D^{n!}, P$ are symmetric, Q, S are also symmetric. Indeed, for all $\sigma \in S_n$, $PQ = C^{n!} = \sigma \cdot C^{n!} = (\sigma \cdot P)(\sigma \cdot Q) = P(\sigma \cdot Q)$, thus $Q = \sigma \cdot Q$.

Therefore $P = P_1(\sigma_1, \dots, \sigma_n)$, and $P_1 \in F[\sigma_1, \dots, \sigma_n]$ divides $C^{n!}, D^{n!}$ in $F[\sigma_1, \dots, \sigma_n]$. As the irreducible polynomial p divides P , P_1 is not a constant. Therefore the two polynomials $C^{n!}, D^{n!}$ are not relatively prime in $F[\sigma_1, \dots, \sigma_n]$, and by (a), C, D are not relatively prime in $F[\sigma_1, \dots, \sigma_n]$, in contradiction with the hypothesis.

Conclusion : two relatively prime polynomials in $F[\sigma_1, \dots, \sigma_n]$ are also relatively prime in $F[x_1, \dots, x_n]$. □

Ex. 2.4.11 Exercise 8 of section 2.2 showed that if $\varphi \in F(x_1, \dots, x_n)$ is symmetric, then $\varphi \in F(\sigma_1, \dots, \sigma_n)$. In this exercise, you will refine this result as follows. Suppose that $\varphi \in F(x_1, \dots, x_n)$ is symmetric, and write $\varphi = A/B$, where $A, B \in F[x_1, \dots, x_n]$ are relatively prime. The claim is that A, B are themselves symmetric and hence lie in $F[\sigma_1, \dots, \sigma_n]$. We can assume that A and B are nonzero.

- (a) Use the previous exercise and Exercise 8 of section 2.2 to show that $\varphi = C/D$ where $C, D \in F[\sigma_1, \dots, \sigma_n]$ are relatively prime in $F[x_1, \dots, x_n]$.
- (b) Show that $AD = BC$ and then use unique factorization in $F[x_1, \dots, x_n]$ to show that A and B are constant multiples of C and D respectively.

(c) Conclude that $A, B \in F[\sigma_1, \dots, \sigma_n]$ as claimed.

Proof. (a) As $\varphi \in F(\sigma_1, \dots, \sigma_n)$, by Exercise 2.2.8,

$$\varphi = C/D, \quad C, D \in F[\sigma_1, \dots, \sigma_n].$$

Reducing this fraction, we can suppose that C, D are relatively prime in $F[\sigma_1, \dots, \sigma_n]$, thus relatively prime in $F[x_1, \dots, x_n]$ by Exercise 2.4.10.

(b) $\varphi = A/B = C/D$, so $AD = BC$, where C, D are symmetric and relatively prime in $F[x_1, \dots, x_n]$, and also A, B relatively prime in $F[x_1, \dots, x_n]$.

As $F[x_1, \dots, x_n]$ is a unique factorisation domain, as $A \mid BC$ and A, B are relatively prime, $A \mid C$. Similarly, $C \mid AD$, and C, D are relatively prime, so $C \mid A$: A and C are associate, therefore

$$A = kC, B = kD, k \in F^*.$$

(c) Since C, D are symmetric, A, B are also symmetric.

Conclusion : if $\varphi = A/B$ is symmetric, where $A, B \in F[x_1, \dots, x_n]$ are relatively prime, then A, B are symmetric.

□