Solutions to David A.Cox "Galois Theory"

Richard Ganaye

May 18, 2020

12 Chapter 12 : LAGRANGE, GALOIS, AND KRONECKER

12.1 LAGRANGE

Ex. 12.1.1 *Let $\theta(x)$ be the resolvent polynomial defined in (12.3). Use the second bullet following (12.1) to show that $\theta(x) \in K[x]$.*

Proof. Let σ be any permutation of S_n. Since

$$\theta(x) = \prod_{i=1}^{r}(x - \varphi_i),$$

then

$$
\begin{aligned}
\sigma \cdot \theta(x) &= \sigma \cdot \prod_{i=1}^{r}(x - \varphi_i) \\
&= \prod_{i=1}^{r} \sigma \cdot (x - \varphi_i) \\
&= \prod_{i=1}^{r}(x - \varphi_{\sigma(i)}) \\
&= \prod_{j=1}^{r}(x - \varphi_j) \qquad (j = \sigma(i)) \\
&= \theta(x)
\end{aligned}
$$

By Exercise 2.2.8, $\sigma \cdot \theta(x) = \theta(x)$ implies that $\theta(x) \in K(x)$. $\qquad\square$

Ex. 12.1.2 *Work out the details of Example 12.1.2.*

Proof. Let $K = \mathbb{Q}[\omega]$, $z_1 = \frac{1}{3}(x_1 + \omega^2 x_2 + \omega x_3) \in \mathbb{Q}[\omega][x_1, x_2, x_3]$, and $\theta(z) \in \mathbb{Q}[\omega][z]$ be

the resolvent polynomial of z_1. The orbit of z_1 under the action of S_n is composed of

$$z_1 = \frac{1}{3}(x_1 + \omega^2 x_2 + \omega x_3),$$

$$(2,3) \cdot z_1 = \frac{1}{3}(x_1 + \omega^2 x_3 + \omega x_2) = \frac{1}{3}(x_1 + \omega x_2 + \omega^2 x_3) = z_2$$

$$(1,3) \cdot z_1 = \frac{1}{3}(x_3 + \omega^2 x_2 + \omega x_1) = \frac{1}{3}(\omega x_1 + \omega^2 x_2 + x_3) = \omega z_2$$

$$(1,2) \cdot z_1 = \frac{1}{3}(x_2 + \omega^2 x_1 + \omega x_3) = \frac{1}{3}(\omega^2 x_1 + x_2 + \omega x_3) = \omega^2 z_2$$

$$(1,2,3) \cdot z_1 = \frac{1}{3}(x_2 + \omega^2 x_3 + \omega x_1) = \frac{1}{3}(\omega x_1 + x_2 + \omega^2 x_3) = \omega z_1$$

$$(1,3,2) \cdot z_1 = \frac{1}{3}(x_3 + \omega^2 x_1 + \omega x_2) = \frac{1}{3}(\omega^2 x_1 + \omega x_2 + x_3) = \omega^2 z_1.$$

So the orbit of z_1 is

$$\mathcal{O}_{z_1} = \{z_1, z_2, \omega z_1, \omega z_2, \omega^2 z_1, \omega^2 z_2\},$$

and these six elements are distinct in $K[x_1, x_2, x_3]$.

Moreover,

$$\theta(z) = (z - z_1)(z - z_2)(z - \omega z_1)(z - \omega z_2)(z - \omega^2 z_1)(z - \omega^2 z_2)$$
$$= (z^3 - z_1^3)(z^3 - z_2^3)$$
$$= z^6 - (z_1^3 + z_2^3)z^3 + (z_1 z_2)^3$$

and

$$z_1 z_2 = \frac{1}{9}(x_1 + \omega^2 x_2 + \omega x_3)(x_1 + \omega x_2 + \omega^2 x_3)$$

$$= \frac{1}{9}(x_1^2 + x_2^2 + x_3^2 - x_1 x_2 - x_2 x_3 - x_1 x_3)$$

$$= \frac{1}{9}[(x_1 + x_2 + x_3)^2 - 3(x_1 x_2 + x_2 x_3 + x_1 x_3)]$$

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

so

$$z_1^3 z_2^3 = \frac{1}{36}(\sigma_1^2 - 3\sigma_1)^3 = -\frac{1}{27}\left(-\frac{\sigma_1^2}{3} + \sigma_2\right)^3 = -\frac{p^3}{27}, \text{ where } p = -\frac{\sigma_1^2}{3} + \sigma_2.$$

$$z_1^3 + z_2^3 = \frac{1}{27}\left[2(x_1^3 + x_2^3 + x_3^3) - 3(x_1^2 x_2 + x_1 x_2^2 + x_1^2 x_3 + x_2^2 x_3 + x_1 x_3^2 + x_2 x_3^2) + 12 x_1 x_2 x_3\right]$$

$$s = x_1^2 x_2 + x_1 x_2^2 + x_1^2 x_3 + x_2^2 x_3 + x_1 x_3^2 + x_2 x_3^2$$
$$= (x_1 x_2 + x_2 x_3 + x_1 x_3)(x_1 + x_2 + x_3) - 3 x_1 x_2 x_3$$
$$= \sigma_2 \sigma_1 - 3\sigma_3$$

$$x_1^3 + x_2^3 + x_3^3 = (x_1^2 + x_2^2 + x_3^2)^2(x_1 + x_2 + x_3) - (x_1^2 x_2 + x_1 x_2^2 + x_1^2 x_3 + x_2^2 x_3 + x_1 x_3^2 + x_2 x_3^2)$$
$$= (\sigma_1^2 - 2\sigma_2)\sigma_1 - (\sigma_2 \sigma_1 - 3\sigma_3)$$
$$= \sigma_1^3 - 3\sigma_1 \sigma_2 + 3\sigma_3.$$

Thus

$$z_1^3 + z_2^3 = \frac{1}{27}\left[2(\sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3) - 3(\sigma_1\sigma_2 - 3\sigma_3) + 12\sigma_3\right]$$

$$= \frac{1}{27}(2\sigma_1^3 - 9\sigma_1\sigma_2 + 27\sigma_3)$$

$$= \frac{2\sigma_1^3}{27} - \frac{\sigma_1\sigma_2}{3} + \sigma_3$$

Finally,

$$\theta(z) = z^6 + qz^3 - \frac{p^3}{27},$$

where

$$p = -\frac{\sigma_1^2}{3} + \sigma_2, \quad q = -\frac{2\sigma_1^3}{27} + \frac{\sigma_1\sigma_2}{3} - \sigma_3.$$

$\square$

Ex. 12.1.3 *This exercise concerns Examples 12.1.3 and 12.1.5.*

(a) *Compute the resolvent $\theta(y)$ of Example 12.1.3. This can be done using the methods of Section 2.3.*

(b) *Let $y_1 = x_1x_2 + x_3x_4$. Show that $H(y_1) = \langle(1\,2),(1\,3\,2\,4)\rangle \subset S_4$.*

(c) *Show that $H(y_1)$ is not normal in S_4.*

(d) *Show that $H(y_1)$ is isomorphic to D_8, the dihedral group of order 8.*

Proof. (a) $y_1 = x_1x_2 + x_3x_4, y_2 = (2\,3)\cdot y_1 = x_1x_3 + x_2x_4, y_3 = (2\,4)\cdot y_1 = x_1x_4 + x_2x_3$ are distinct elements of the orbit of y_1.

Since $|H(y_1)| = |\text{Stab}_{S_n}(y_1)| = 8$ (see Part (d)), $|\mathcal{O}_{y_1}| = 3$, so y_1, y_2, y_3 are all the elements of $\mathcal{O}_{y_1}$.

$$\mathcal{O}_{y_1} = \{y_1, y_2, y_3\} = \{x_1x_3 + x_2x_4, x_1x_3 + x_2x_4, x_1x_4 + x_2x_3\}.$$

Therefore

$$\theta(y) = \left((y - (x_1x_2 + x_3x_4)\right)\left(y - (x_1x_3 + x_2x_4)\right)\left(y - (x_1x_4 + x_2x_3)\right)$$

Using the methods of section 2.3, we obtain 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.<y,x0,x1,x2,x3,y1,y2,y3,y4> = PolynomialRing(QQ, order = 'degrevlex')
J = R.ideal(e1-y1, e2-y2, e3-y3,e4-y4)
G = J.groebner_basis()

z1 = x0*x1 + x2*x3
z2 = x0*x2 + x1*x3
z3 = x0*x3 + x1*x2
f = (y-(x0*x1 + x2*x3))*(y-(x0*x2 + x1*x3))*(y-(x0*x3 + x1*x2))

var('sigma_1,sigma_2,sigma_3,sigma_4')
g=f.reduce(G).subs(y1=sigma_1,y2=sigma_2,y3=sigma_3,y4=sigma_4)
g.collect(y)
```

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

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

(b)
$$(1\,2)\cdot y_1 = x_2 x_1 + x_3 x_4 = y_1, \qquad (1\,3\,2\,4)(y_1) = x_3 x_4 + x_2 x_1 = y_1,$$

therefore
$$\langle(1\,2),(1\,3\,2\,4)\rangle \subset H(y_1).$$

Moreover
$$\langle(1\,2),(1\,3\,2\,4)\rangle = \{(),(1\,2),(1\,3\,2\,4),(1\,3)(2\,4),(1\,2)(3\,4),(1\,4)(2\,3),(3\,4),(1\,4\,2\,3)\}.$$

We obtain this by hand, or with the Dimino algorithm, or with the Sage instructions:

```
G = PermutationGroup([(1,2),(1,3,2,4)])
G.list()
```

The orbit of y_1 contains three distinct elements y_1, y_2, y_3, so $|\mathcal{O}_{y_1}| \geq 3$. Since $|\mathcal{O}_{y_1}| = (S_n : H(y_1))$, $|H(y_1)| \leq 8$. But $H(y_1)$ contains the 8 elements of $\langle(1\,2),(1\,3\,2\,4)\rangle$, thus
$$H(y_1) = \langle(1\,2),(1\,3\,2\,4)\rangle.$$

(c) $(2\,3)(1\,3\,2\,4)(2\,3)^{-1} = (1\,2\,3\,4) \notin H(y_1)$, so $H(y_1)$ is not normal in S_4.

(d) If we use the number the 4 consecutive summits of the square $(1,3,2,4)$, then $H(y_1)$ is isomorphic to the group generated by the rotation of angle $\pi/2$ corresponding to $(1\,3\,2\,4)$ and the reflection relative to the diagonal $(3,4)$ corresponding to $(1\,2)$, and this the dihedral group D_8.

$$H(y_1) \simeq D_8.$$

$\square$

Ex. 12.1.4   *Verify (12.9) and (12.10).*

Proof. Starting from
$$x^4 - \sigma_1 x^3 = -\sigma_2 x^2 + \sigma_3 x - \sigma_4,$$

wee add the quantity
$$yx^2 + \frac{1}{4}(-\sigma_1 x + y)^2 = \left(y + \frac{\sigma_1^2}{4}\right)x^2 - \frac{\sigma_1}{2}yx + \frac{y^2}{4},$$

so
$$x^4 - \sigma_1 x^3 + yx^2 + \frac{1}{4}(-\sigma_1 x + y)^2 = -\sigma_2 x^2 + \sigma_3 x - \sigma_4 + \left(y + \frac{\sigma_1^2}{4}\right)x^2 - \frac{\sigma_1}{2}yx + \frac{y^2}{4},$$

Since

$$x^4 - \sigma_1 x^3 + yx^2 + \frac{1}{4}(-\sigma_1 x + y)^2 = x^4 + (-\sigma_1 x + y)x^2 + \frac{1}{4}(-\sigma_1 x + y)^2$$

$$= \left(x^2 + \frac{1}{2}(-\sigma_1 x + y) \right)^2$$

$$= \left(x^2 - \frac{\sigma_1}{2}x + \frac{y}{2} \right)^2$$

we obtain

$$\left(x^2 - \frac{\sigma_1}{2}x + \frac{y}{2} \right)^2 = \left(y + \frac{\sigma_1^2}{4} - \sigma_2 \right) x^2 + \left(-\frac{\sigma_1}{2}y + \sigma_3 \right) x + \frac{y^2}{4} - \sigma_4.$$

The discriminant of the right member $Ax^2 + Bx + C$ is

$$\Delta = B^2 - 4AC = \left(-\frac{\sigma_1}{2}y + \sigma_3 \right)^2 - 4 \left(y + \frac{\sigma_1^2}{4} - \sigma_2 \right) \left(\frac{y^2}{4} - \sigma_4 \right).$$

$$4\Delta = (-\sigma_1 y + 2\sigma_3)^2 - (4y + \sigma_1^2 - 4\sigma_2)(y^2 - 4\sigma_4)$$
$$= (\sigma_1^2 y^2 - 4\sigma_1\sigma_3 y + 4\sigma_3^2) - (4y^3 - 16\sigma_4 y + (\sigma_1^2 - 4\sigma_2)y^2 - 4\sigma_1^2\sigma_4 + 16\sigma_2\sigma_4)$$
$$= -4y^3 + 4\sigma_2 y^2 + (-4\sigma_1\sigma_3 + 16\sigma_4)y + (4\sigma_3^2 + 4\sigma_4\sigma_1^2 - 16\sigma_2\sigma_4)$$
$$= -4(y^3 - \sigma_2 y^2 + (\sigma_1\sigma_3 - 4\sigma_4)y - \sigma_3^2 - \sigma_1^2\sigma_4 + 4\sigma_2\sigma_4)$$

So the second member is a perfect square if and only if the Ferrari resolvent

$$R(y) = y^3 - \sigma_2 y^2 + (\sigma_1\sigma_3 - 4\sigma_4)y - \sigma_3^2 - \sigma_1^2\sigma_4 + 4\sigma_2\sigma_4$$

is zero for the chosen y. $\qquad\square$

Ex. 12.1.5 *This exercise will study the quadratic equations (12.11). Each quadratic has two roots, which together make up the four roots x_1, x_2, x_2, x_4 of our quadric.*

(a) *For the moment, forget all the theory developed so far, and let y be some root of the Ferrari resolvent (12.10. Given only this, can we determine how y relates to the x_i? This is surprisingly easy to do. Suppose x_i, x_j. are the roots of (12.11) for one choice of sign, and x_k, x_l are the roots for the other. Thus i, j, k, l are the number 1,2,3,4 in some order. Prove that y is given by $y = x_i x_j + x_k x_l$.*

(b) *Now let $y = x_1 x_2 + x_3 x_4$, and define the square root in (12.11) using (12.12). Show that the roots of (12.11) are x_1, x_2 for the plus sign and $x_3 x_4$ for the minus sign.*

Proof. If y is some root of the Ferrari resolvent, then x_i, x_j are the roots of

$$x^2 - \frac{\sigma_1}{2}x + \frac{y}{2} = +\sqrt{y + \frac{\sigma_1^2}{4} - \sigma_2} \left(x + \frac{-\frac{\sigma_1}{2}y + \sigma_3}{2(y + \frac{\sigma_1^2}{4} - \sigma_2)} \right).$$

The product $x_i x_j$ is given by

$$x_i x_j = \frac{y}{2} - \sqrt{y + \frac{\sigma_1^2}{4} - \sigma_2} \left(\frac{-\frac{\sigma_1}{2}y + \sigma_3}{2(y + \frac{\sigma_1^2}{4} - \sigma_2)} \right).$$

Similarly x_k, x_l are the roots of

$$x^2 - \frac{\sigma_1}{2}x + \frac{y}{2} = -\sqrt{y + \frac{\sigma_1^2}{4} - \sigma_2}\left(x + \frac{\frac{-\sigma_1}{2}y + \sigma_3}{2(y + \frac{\sigma_1^2}{4} - \sigma_2)}\right).$$

and the product $x_k x_l$ is given by

$$x_k x_l = \frac{y}{2} + \sqrt{y + \frac{\sigma_1^2}{4} - \sigma_2}\left(\frac{\frac{-\sigma_1}{2}y + \sigma_3}{2(y + \frac{\sigma_1^2}{4} - \sigma_2)}\right).$$

Adding these two formulas, we obtain

$$x_i x_j + x_k x_l = y.$$

Using $y_1 = x_1 x_2 + x_3 x_4$, and setting

$$t_1 = x_1 + x_2 - x_3 - x_4,$$

then

$$y_1 + \frac{\sigma_1^2}{4} - \sigma_2$$

$$= x_1 x_2 + x_3 x_4 + \frac{1}{4}(x_1 + x_2 + x_3 + x_4)^2 - (x_1 x_2 + x_1 x_3 + x_1 x_4 + x_2 x_3 + x_2 x_4 + x_3 x_4)$$

$$= \frac{1}{4}\left[x_1^2 + x_2^2 + x_3^2 + x_4^2 - 2(x_1 x_2 + x_1 x_3 + x_1 x_4 + x_2 x_3 + x_2 x_4 + x_3 x_4) + 4(x_1 x_2 + x_3 x_4)\right]$$

$$= \frac{1}{4}\left[x_1^2 + x_2^2 + x_3^2 + x_4^2 + 2x_1 x_2 + 2x_3 x_4 - 2(x_1 x_3 + x_1 x_4 + x_2 x_3 + x_2 x_4)\right]$$

$$= \frac{1}{4}\left[(x_1 + x_2)^2 + (x_3 + x_4)^2 - 2(x_1 + x_2)(x_3 + x_4)^2 - 2(x_1 + x_2)(x_3 + x_4)\right]$$

$$= \frac{1}{4}(x_1 + x_2 - x_3 - x_4)^2$$

$$= \frac{t_1^2}{4}$$

We choose the square root such that

$$\sqrt{y_1 + \frac{\sigma_1^2}{4} - \sigma_2} = \frac{t_1}{2}.$$

Then the quadratic equation with $y = y_1$ and the plus sign is

$$x^2 - \frac{\sigma_1}{2}x + \frac{y_1}{2} = +\sqrt{y_1 + \frac{\sigma_1^2}{4} - \sigma_2}\left(x + \frac{\frac{-\sigma_1}{2}y_1 + \sigma_3}{2(y_1 + \frac{\sigma_1^2}{4} - \sigma_2)}\right),$$

or otherwise

$$x^2 - \left(\frac{\sigma_1}{2} + \frac{t_1}{2}\right)x + \frac{y_1}{2} + \frac{1}{2t_1}(\sigma_1 y_1 - 2\sigma_3).$$

Let u, v be the roots of this equation, and $S = u + v, P = uv$ the sum and product of these roots. Then

$$S = \frac{\sigma_1}{2} + \frac{t_1}{2}$$

$$= \frac{1}{2}(x_1 + x_2 + x_3 + x_4 + x_1 + x_2 - x_3 - x_4)$$

$$= x_1 + x_2$$

6

$$P = \frac{y_1}{2} + \frac{1}{2t_1}(\sigma_1 y_1 - 2\sigma_3)$$

$$= \frac{y_1}{2} + \frac{1}{2t_1}\left[(x_1 + x_2 + x_3 + x_4)(x_1 x_2 + x_3 x_4) - 2(x_1 x_2 x_3 + x_1 x_2 x_4 + x_1 x_3 x_4 + x_2 x_3 x_4)\right]$$

$$= \frac{y_1}{2} + \frac{1}{2t_1}\left[x_1^2 x_2 + x_1 x_2^2 + x_3^2 x_4 + x_3 x_4^2 - x_1 x_3 x_4 - x_2 x_3 x_4 - x_1 x_2 x_3 - x_1 x_2 x_4\right]$$

$$= \frac{y_1}{2} + \frac{1}{2t_1}(x_1 + x_2 - x_3 - x_4)(x_1 x_2 - x_3 x_4)$$

$$= \frac{1}{2}(x_1 x_2 + x_3 x_4 + x_1 x_2 - x_3 x_4)$$

$$= x_1 x_2$$

Thus u, v are the roots of $x^2 - Sx + P = (x - x_1)(x - x_2)$, so $\{u, v\} = \{x_1, x_2\}$.

x_1, x_2 are the roots of (12.11) with the plus sign, so x_3, x_4 are the roots of (12.11) with the minus sign.

$\square$

Ex. 12.1.6 *Explain why the polynomial $\theta(t)$ (12.13) has coefficients in $K = F(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$.*

(b) *Proof.*

$$\theta(t) = (t^2 - 4y_1 - \sigma_1^2 + 4\sigma_2)(t^2 - 4y_2 - \sigma_1^2 + 4\sigma_2)(t^2 - 4y_3 - \sigma_1^2 + 4\sigma_2).$$

Recall that

$$y_1 = x_1 x_2 + x_3 x_4$$
$$y_2 = x_1 x_3 + x_2 x_4$$
$$y_3 = x_1 x_4 + x_2 x_3$$

Let $\tau = (1\,2), \sigma = (1\,2\,3\,4)$. Then

$$\tau \cdot y_1 = x_2 x_1 + x_3 x_4 = y_1, \quad \tau \cdot y_2 = x_2 x_3 + x_1 x_4 = y_3, \quad \tau \cdot y_3 = x_2 x_4 + x_1 x_3 = y_2,$$

and of course $\tau \cdot \sigma_1 = \sigma_1, \tau \cdot \sigma_2 = \sigma_2$.
    Therefore $\tau \cdot \theta(t) = \theta(t)$.
    Similarly,

$$\sigma \cdot y_1 = x_2 x_3 + x_4 x_1 = y_3, \quad \sigma \cdot y_2 = x_2 x_4 + x_3 x_1 = y_2, \quad \sigma \cdot y_3 = x_2 x_1 + x_3 x_4 = y_1.$$

Therefore $\sigma \cdot \theta(t) = \theta(t)$.
    Since $S_n = \langle \sigma, \tau \rangle$, every permutation in S_n lets the coefficients of $\theta(t)$ unchanged, therefore $\theta(t)$ has coefficients in $K = F(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ and $\theta(t) \in K[t]$. $\square$

Ex. 12.1.7

Proof. We know that

$$\sigma_1 = x_1 + x_2 + x_3 + x_4,$$
$$t_1 = x_1 + x_2 - x_3 - x_4,$$
$$t_2 = x_1 - x_2 + x_3 - x_4,$$
$$t_3 = x_1 - x_2 - x_3 + x_4.$$

The sum of these equations gives

$$\sigma_1 + t_1 + t_2 + t_3 = 4x_1,$$

so

$$x_1 = \frac{1}{4}\left(\sigma_1 + t_1 + t_2 + t_3\right).$$

We can compute similarly $\sigma_1 + t_1 - t_2 - t_3$, ...

More conceptually, let $\sigma = (1\,2)(3\,4)$. Then

$$\sigma \cdot x_1 = x_2, \quad \sigma \cdot t_1 = t_1, \quad \sigma \cdot t_2 = -t_2, \quad \sigma \cdot t_3 = -t_3.$$

Therefore

$$x_2 = \frac{1}{4}\left(\sigma_1 + t_1 - t_2 - t_3\right).$$

Similarly, if $\tau = (1\,3)(2\,4)$,

$$\sigma \cdot x_1 = x_3, \quad \tau \cdot t_1 = -t_1, \quad \tau \cdot t_2 = t_2, \quad \tau \cdot t_3 = -t_3.$$

Therefore

$$x_3 = \frac{1}{4}\left(\sigma_1 - t_1 + t_2 - t_3\right).$$

Finally, if $\zeta = (1\,4)(2\,3)$,

$$\zeta \cdot x_1 = x_4, \quad \zeta \cdot t_1 = -t_1, \quad \zeta \cdot t_2 = -t_2, \quad \zeta \cdot t_3 = t_3.$$

Therefore

$$x_4 = \frac{1}{4}\left(\sigma_1 - t_1 - t_2 + t_3\right).$$

In conclusion

$$x_1 = \frac{1}{4}\left(\sigma_1 + t_1 + t_2 + t_3\right),$$
$$x_2 = \frac{1}{4}\left(\sigma_1 + t_1 - t_2 - t_3\right),$$
$$x_3 = \frac{1}{4}\left(\sigma_1 - t_1 + t_2 - t_3\right),$$
$$x_4 = \frac{1}{4}\left(\sigma_1 - t_1 - t_2 + t_3\right).$$

$\square$

Ex. 12.1.8 *Let t_1, t_2, t_3 defined as in (12.15).*

(a) *Lagrange noted that any transposition fixes exactly one of t_1, t_2, t_3 and interchanges the other two, possibly changing the sign of both. Prove this and use it to show that $t_1 t_2 t_3$ is fixed by all elements of S_4.*

(b) *Use the methods of Chapter 2 to express $t_1 t_2 t_3$ in terms of the σ_i. The result should be the identity (12.16).*

Proof. (a)

$$t_1 = x_1 + x_2 - x_3 - x_4,$$
$$t_2 = x_1 - x_2 + x_3 - x_4,$$
$$t_3 = x_1 - x_2 - x_3 + x_4.$$

Since $H(t_1) = \langle (1\,2), (3\,4) \rangle$ has order 4, the orbit $\mathcal{O}_{t_1}$ of t_1 under S_n has $4!/4 = 6$ elements, so

$$\mathcal{O}_{t_1} = \{t_1, t_2, t_3, -t_1, -t_2, -t_3\}.$$

$$(1\,2) \cdot t_1 = t_1, \quad (1\,2) \cdot t_2 = -t_3, \quad (1\,2) \cdot t_3 = -t_2,$$

therefore

$$(1\,2) \cdot (t_1 t_2 t_3) = t_1 (-t_3)(-t_2) = t_1 t_2 t_3.$$

$$\begin{aligned}
(1\,2\,3\,4) \cdot t_1 &= x_2 + x_3 - x_4 - x_1 \\
&= -x_1 + x_2 + x_3 - x_4 \\
&= -(x_1 - x_2 - x_3 + x_4) \\
&= -t_3
\end{aligned}$$

With similar computations, we obtain

$$(1\,2\,3\,4) \cdot t_1 = -t_3, \quad (1\,2\,3\,4) \cdot t_2 = -t_2, \quad (1\,2\,3\,4) \cdot t_3 = t_1,$$

thus

$$(1\,2\,3\,4) \cdot (t_1 t_2 t_3) = (-t_3)(-t_2) t_1 = t_1 t_2 t_3.$$

Since $(1\,2) \cdot (t_1 t_2 t_3) = t_1 t_2 t_3, (1\,2\,3\,4) \cdot (t_1 t_2 t_3) = t_1 t_2 t_3$, and $S_4 = \langle (1\,2), (1\,2\,3\,4) \rangle$, then $t_1 t_2 t_3$ is fixed by all elements of S_4, and so is in $F(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$.

(b) With the methods of Chapter 2, 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()
t1= x0+x1-x2-x3; t2 = x0-x1+x2-x3; t3 = x0-x1-x2+x3
u = t1*t2*t3
var('sigma_1,sigma_2,sigma_3,sigma_4')
v = u.reduce(G).subs(y1=sigma_1, y2 = sigma_2,y3=sigma_3,y4=sigma_4)
```

give

$$\sigma_1^3 - 4\,\sigma_1 \sigma_2 + 8\,\sigma_3.$$

So

$$\begin{aligned}
t_1 t_2 t_3 &= (x_1 + x_2 - x_3 - x_4)(x_1 - x_2 + x_3 - x_4)(x_1 - x_2 - x_3 + x_4) \\
&= \sigma_1^3 - 4\,\sigma_1 \sigma_2 + 8\,\sigma_3.
\end{aligned}$$

$\square$

Ex. 12.1.9 *Let H be a subgroup of S_n. In this exercise you will give two proofs that there is $\varphi \in L$ such that $H = H(\varphi)$.*

(a) *(First Proof.) The fixed field L_H gives an extension $K \subset L_H$. Explain why the Theorem of the Primitive Element applies to give $\varphi \in L_H$ such that $L_H = K(\varphi)$. Show that this φ has the desired property.*

(b) *(Second Proof.) Let $m = x_1^{a_1} \cdots x_n^{a_n}$ be a monomial in $x_1, \ldots, x_n$ with distinct exponents $a_1, \ldots, a_n$. Then define*

$$\varphi = \sum_{\sigma \in H} \sigma \cdot m = \sum_{\sigma \in H} x_{\sigma(1)}^{a_1} \cdots x_{\sigma(n)}^{a_n}.$$

Prove that $H(\varphi) = H$.

Proof.   (a) Here $K = F(\sigma_1, \ldots, \sigma_n), L = F(x_1, \ldots, x_n)$, where F has characteristic 0.

We know (Theorem 6.4.1) that $K \subset L$ is a Galois extension, and that

$$\psi : \left\{ \begin{array}{ccc} S_n & \to & \mathrm{Gal}(L/K) \\ \tau & \mapsto & \tilde{\tau} \left\{ \begin{array}{ccc} L & \to & L \\ f & \mapsto & \tau \cdot f \end{array} \right. \end{array} \right.$$

(where $\tau \cdot f(x_1, \ldots, x_n) = f(x_{\tau(1)}, x_{\tau(2)}, \ldots, x_{\tau(n)})$)

is an isomorphism from S_n to $\mathrm{Gal}(L/K)$.

Write $\tilde{H} = \psi(H)$ the subgroup of $\mathrm{Gal}(L/K)$ corresponding to $H \subset S_n$, and $L_{\tilde{H}}$ its fixed field (we can write $L_H = L_{\tilde{H}}$).

$K \subset L$ is a finite extension, and $K \subset L_H \subset L$, so $K \subset L_H$ is a finite extension. Since the characteristic of F is 0, the Theorem of the Primitive Element (Corollary 5.4.2 (b)) applies to give $\varphi \in L_H$ such that $L_H = K(\varphi)$.

Since $K \subset L$ is a Galois extension, the Galois correspondence (Theorem 7.3.1) gives

$$\tilde{H} = \mathrm{Gal}(L/L_{\tilde{H}}) = \mathrm{Gal}(L/K(\varphi)).$$

We show that $H = H(\varphi)$:

- If $\tau \in H$, then $\tilde{\tau} = \psi(\tau) \in \tilde{H} = \mathrm{Gal}(L/K(\varphi))$. Since $\varphi \in K(\varphi)$, $\tau \cdot \varphi = \tilde{\tau}(\varphi) = \varphi$, so $\tau \in H(\varphi)$.
- If $\tau \in H(\varphi)$, then $\tau \cdot \varphi = \varphi$. If $u(x_1, \ldots, x_n) \in K(\varphi)$, then $u(x_1, \ldots, x_n) = f(\varphi(x_1, \ldots, x_n))$, where $f \in K(x)$. Therefore

  $$\tau \cdot u(x_1, \ldots, x_n) = f(\varphi(x_{\tau(1)}, \ldots, x_{\tau(n)})) = f(\varphi(x_1, \ldots, x_n)) = u(x_1, \ldots, x_n),$$

  so $\tilde{\tau}(u) = \tau \cdot u = u$ for all $u \in K(\varphi)$, thus $\tilde{\tau} \in \mathrm{Gal}(L/K(\varphi)) = \tilde{H}$, and so $\tau \in H$.

Conclusion: if H is a subgroup of S_n, there is $\varphi \in L$ such that $H = H(\varphi)$.

(b) Let $\varphi = \sum_{\sigma \in H} \sigma \cdot m$, where $m = x_1^{a_1} \cdots x_n^{a_n}$ with distinct exponents $a_1, \ldots, a_n$.

- If $\tau \in H$, by (6.7),

  $$\tau \cdot \varphi = \sum_{\sigma \in H} (\tau\sigma) \cdot m = \sum_{\sigma' \in H} \sigma' \cdot m = \varphi \qquad (\sigma' = \tau\sigma).$$

  Therefore $\tau \in H(\varphi)$.

10

- If $\tau \in H(\varphi)$, $\tau \cdot \varphi = \varphi$, so

$$\sum_{\sigma \in H} (\tau\sigma) \cdot m = \sum_{\chi \in H} \chi \cdot m,$$

$$\sum_{\sigma \in H} x_{(\tau\sigma)(1)}^{a_1} \cdots x_{(\tau\sigma)(n)}^{a_n} = \sum_{\chi \in H} x_{\chi(1)}^{a_1} \cdots x_{\chi(n)}^{a_n}.$$

Moreover,

$$\prod_{i=1}^{n} x_{\chi(i)}^{a_i} = \prod_{j=1}^{n} x_j^{a_{\chi^{-1}(j)}}, \qquad (j = \chi(i)),$$

so

$$\sum_{\sigma \in H} x_1^{a_{(\tau\sigma)^{-1}(1)}} \cdots x_n^{a_{(\tau\sigma)^{-1}(n)}} = \sum_{\chi \in H} x_1^{a_{\chi^{-1}(1)}} \cdots x_n^{a_{\chi^{-1}(n)}}$$

Since the exponents $a_1, \ldots, a_n$ are distinct, the k terms of $\sum_{\chi \in H} \chi \cdot m$, where $k = |H|$, are distinct, so there exist exactly one term in the right member which is the same as the term $x_1^{a_{\tau^{-1}(1)}} \cdots x_n^{a_{\tau^{-1}(n)}}$ of the left member corresponding to $\sigma = e$, so there exists $\chi \in H$ such that

$$x_1^{a_{\tau^{-1}(1)}} \cdots x_n^{a_{\tau^{-1}(n)}} = x_1^{a_{\chi^{-1}(1)}} \cdots x_n^{a_{\chi^{-1}(n)}}.$$

This implies $a_{\tau^{-1}(i)} = a_{\chi^{-1}(i)}$, $1 \le i \le n$. Since the exponents are distinct, $a_k = a_l$ implies $k = l$, so we obtain $\tau^{-1}(i) = \chi^{-1}(i)$ for all i, therefore $\tau^{-1} = \chi^{-1}$ and $\tau = \chi \in H$.

We have proved $H = H(\varphi)$.

$\square$

Ex. 12.1.10 *Prove that the subset $N \subset S_n$ defined in the proof of Theorem 12.1.10 is a subgroup of S_n.*

Proof. Let

$$N = \{\sigma \in S_n \mid \sigma \cdot \varphi_i = \varphi_i \text{ for all } i = 1, \ldots, r\}.$$

Then

$$N = \bigcap_{1 \le i \le r} \text{Stab}_{S_n}(\varphi_i) = \bigcap_{1 \le i \le r} H(\varphi_i)$$

is the intersection of r subgroups of S_n, so is a subgroup of S_n. $\square$

Ex. 12.1.11 *Let H be a proper subgroup of A_n with $n \ge 5$. Prove that $[A_n : H] \ge n$.*

Proof. As H is a subgroup of A_n, by Exercise 9, there exists $\varphi \in A_n$ such that $H = H(\varphi)$. Let $\mathcal{O}_\varphi$ the orbit of φ under the action of A_n:

$$\mathcal{O}_\varphi = \{\sigma \cdot \varphi \mid \sigma \in H\} = \{\varphi_1 = \varphi, \varphi_2, \ldots, \varphi_s\},$$

and let G the subgroup of A_n defined by

$$G = \{\sigma \in A_n \mid \forall i \in [\![1, s]\!], \sigma\varphi_i = \varphi_i\} = \bigcap_{1 \le i \le s} \text{Stab}_{A_n}(\varphi_i).$$

Then $G \subset H(\varphi_1) = H$. We show that G is normal in A_n.

Let $\tau \in A_n$ and $\sigma \in G$. Fix i between 1 and s. Then $\tau \cdot \varphi_i \in \mathcal{O}_\varphi$, so $\tau \cdot \varphi_i = \varphi_j$ for some $j \in [\![1, s]\!]$. Then

$$(\tau^{-1}\sigma\tau) \cdot \varphi_i = (\tau^{-1}\sigma) \cdot \varphi_j = \tau^{-1} \cdot (\sigma \cdot \varphi_j) = \tau^{-1} \cdot \varphi_j = \varphi_i,$$

so $\tau^{-1}\sigma\tau \in G$. Since A_n is a simple group for $n \geq 5$, $G = \{e\}$ or $G = A_n$. Since $G \subset H$ and $H \subset A_n, H \neq A_n$, then $G \neq A_n$, therefore $G = \{e\}$.

$H = H(\varphi) = \mathrm{Stab}_{A_n}(\varphi)$, therefore $s = |\mathcal{O}_\varphi| = (A_n : H)$.

If we suppose that $(A_n : H) < n$, then $s < n$. Then $s \leq n - 1$, therefore $s! \leq (n-1)! < n!/2$. Since there are $n!/2$ permutations in A_n, and only s permutations of $\{\varphi_1, \varphi_2, \ldots, \varphi_s\}$ there exist two distinct permutations $\tau_1, \tau_2 \in A_n$ such that

$$\tau_1 \cdot \varphi_i = \tau_2 \cdot \varphi_i \qquad \text{for all } i = 1, \ldots, r.$$

So $e \neq \tau_2^{-1}\tau_1 \in N$, $N \neq \{e\}$: this is a contradiction. This proves $(A_n : H) \geq n$. $\qquad \square$

Ex. 12.1.12 *The discussion following Theorem 12.1.10 shows that if we are going to use Lagrange's strategy when $n \geq 5$, then we need to begin with $\varphi = \sqrt{\Delta}$, which has isotropy subgroup A_n. Suppose that $\psi \in L$ is our next choice, and let $\theta(x)$ be the resolvent of ψ. Since we regard $K(\sqrt{\Delta})$ as known, we may assume that $\psi \notin K(\sqrt{\Delta})$. The idea is to factor $\theta(x)$ over $K(\sqrt{\Delta})$, say $\theta = R_1 \cdots R_s$, where $R_i \in K(\sqrt{\Delta})[x]$ is irreducible. This is similar to how (12.13) factors the resolvent of t_1 over $K(y_1)$. Suppose that ψ enables us to continue Lagrange's inductive strategy. This means that some factor of θ, say R_j, has degree $< n$. Your goal is to prove that this implies the existence of a proper subgroup of A_n of index $< n$.*

(a) *Prove that $\deg(R_j) \geq 2$.*

(b) *Since θ splits completely over L, the same is true for R_j. Let $\psi_j \in L$ be a root of R_j and consider the fields*

$$K \subset K(\sqrt{\Delta}) \subset M = K(\sqrt{\Delta}, \psi_j) \subset L.$$

Let $H_j \subset S_n$ be the subgroup corresponding to $\mathrm{Gal}(L/M) \subset \mathrm{Gal}(L/K)$ under (12.1). Prove that $H_j \subset A_n$ and that $[A_n : H_j]$ is the degree of R_j.

(c) *Conclude that $\deg(R_j) < n$ implies that H_j is a proper subgroup of A_n of index $< n$. With more work, one can show that $\deg(R_i) = [A_n : A_n \cap H(\psi)]$ for all i and that*

$$s = \frac{2}{[H(\psi) : A_n \cap H(\psi)]}.$$

It follows that $s = 1$ or 2.

Proof. (a) Here $K = F(\sigma_1, \ldots, \sigma_n)$ and $L = F(x_1, \ldots, x_n)$.

The roots of the resolvent θ are all the distinct $\sigma \cdot \psi$, where $\sigma \in S_n$. If $\deg(R_j) = 1$, then $R_j(x) = x - \sigma \cdot \psi$ for some $\sigma \in S_n$. Since $R_j \in K(\sqrt{\Delta})[x]$, then $\sigma \cdot \psi \in K(\sqrt{\Delta})$. If $\sigma \in A_n$ then $\sigma^{-1} \in A_n$ fixes $\sqrt{\Delta}$, and so $\psi = \sigma^{-1} \cdot (\sigma \cdot \psi) \in K(\sqrt{\Delta})$, which contradicts our assumption, therefore $\sigma \in S_n \setminus A_n$ and $\sigma \cdot \sqrt{\Delta} = -\sqrt{\Delta}$.

As $\sigma \cdot \psi \in K(\sqrt{\Delta})$, $\sigma \cdot \psi = A + B\sqrt{\Delta}$, $A, B \in K = F(\sigma_1, \ldots, \sigma_n)$. Therefore $\psi = \sigma^{-1} \cdot (A + B\sqrt{\Delta}) = A - B\sqrt{\Delta} \in K(\sqrt{\Delta})$: this is a contradiction.

Thus $\deg(R_j) \geq 2$.

12

(b) Since $L \subset K(\sqrt{\Delta}) \subset M$, the Galois correspondence being order reversing,

$$\mathrm{Gal}(L/M) \subset \mathrm{Gal}(L/K(\sqrt{\Delta})) \subset \mathrm{Gal}(L/K).$$

The same inclusions are true for the corresponding subgroups of S_n:

$$H_j \subset A_n \subset S_n.$$

By the fundamental Theorem (Theorem 7.3.1), since $K \subset L$, a fortiori $K(\sqrt{\Delta})) \subset L$ are Galois extensions, the index $(A_n : H_j) = (\mathrm{Gal}(L/K(\sqrt{\Delta}) : \mathrm{Gal}(L/M))$ is equal to $[M : K(\sqrt{\Delta})] = [K(\sqrt{\Delta}, \psi_j) : K(\sqrt{\Delta})]$. The minimal polynomial of ψ_j over $K(\sqrt{\Delta})$ being R_j, $[K(\sqrt{\Delta}, \psi_j) : K(\sqrt{\Delta})] = \deg(R_j)$, so

$$(A_n : H_j) = \deg(R_j).$$

(c) If $H_j = A_n$, then by the Galois correspondence $K(\sqrt{\Delta}, \psi_j) = K(\sqrt{\Delta})$, and then $\psi_j \in K(\sqrt{\Delta})$. But this implies that $R_j = x - \psi_j$ has degree 1, which is impossible by part (a). So H_j is a proper subgroup of A_n. if $\deg(R_j) < n$, then A_j is a proper subgroup of A_n such that $(A_n : H_j) < n$. This is impossible for all $n \geq 5$.

$\square$

Ex. 12.1.13 *Let ζ be a primitive nth root of unity, and let $\alpha = x_1 + \zeta x_2 + \cdots + \zeta^{n-1} x_n$. Prove that $H(\alpha^n) = \langle (1\,2\ldots n) \rangle \subset S_n$.*

Proof. $(1\,2\ldots n) \cdot \alpha = x_2 + \zeta x_3 + \cdots + \zeta^{n-1} x_1 = \zeta^{-1} \alpha$, therefore $(1\,2\ldots n) \cdot \alpha^n = (\zeta^{-1} \alpha)^n = \alpha^n$, so

$$\langle (1\,2\ldots n) \rangle \subset H(\alpha^n).$$

Conversely, suppose that $\sigma \in H(\alpha^n)$. Then $\sigma \cdot \alpha^n = \alpha^n$, so

$$(x_{\sigma(1)} + \zeta x_{\sigma(2)} + \cdots + \zeta^{n-1} x_{\sigma(n)})^n = (x_1 + \zeta x_2 + \cdots + \zeta^{n-1} x_n)^n.$$

Therefore, there exists a nth root of unity ξ such that

$$x_{\sigma(1)} + \zeta x_{\sigma(2)} + \cdots + \zeta^{n-1} x_{\sigma(n)} = \xi(x_1 + \zeta x_2 + \cdots + \zeta^{n-1} x_n).$$

Then

$$\xi \sum_{i=1}^{n} \zeta^{i-1} x_i = \sum_{j=1}^{n} \zeta^{j-1} x_{\sigma(j)}$$

$$= \sum_{i=1}^{n} \zeta^{\sigma^{-1}(i)-1} x_i, \qquad (i = \sigma(j))$$

Therefore, for all $i = 1, \ldots, n$,

$$\xi \zeta^{i-1} = \zeta^{\sigma^{-1}(i)-1}$$

For $i = 1$, we obtain $\xi = \zeta^{\sigma^{-1}(1)-1}$, so $\zeta^{\sigma^{-1}(1)-1+i-1} = \zeta^{\sigma^{-1}(i)-1}$.

Since ζ is a primitive nth root of unity,

$$\sigma^{-1}(1) + i - 1 \equiv \sigma^{-1}(i) \pmod{n} \qquad (1 \leq i \leq n).$$

If $k = \sigma^{-1}(1) - 1$, then

$$\sigma^{-1}(i) \equiv i + k \pmod{n},$$

therefore $\sigma^{-1} = (1\,2\ldots n)^k, \sigma = (1\,2\ldots n)^{n-k}$ are in the subgroup $\langle (1\,2\ldots n) \rangle$.

$$H(\alpha^n) = \langle (1\,2\ldots n) \rangle.$$

$\square$

Ex. 12.1.14 *Let α_i be as in (12.18), with $\sigma = (1\,2\ldots n) \in S_n \simeq \mathrm{Gal}(L/K)$:*

$$\alpha_i = x_1 + \zeta^{-i}\sigma \cdot x_1 + \zeta^{-2i}\sigma_2 \cdot x_1 + \cdots + \zeta^{-i(n-1)}\sigma^{n-1} \cdot x_1$$
$$= x_1 + \zeta^{-i}x_2 + \zeta^{-2i}x_3 + \cdots + \zeta^{-i(n-1)} \cdot x_n$$

The quotation given in the discussion following (12.18) can be paraphrased as saying that the roots of the resolvent of $\theta_i = \alpha_i^n$ come from the permutations of the $n-1$ roots $x_2, \ldots, x_n$ that ignore the root x_1. What does this mean?

(a) Show that each left coset of $\langle (1\,2\ldots n) \rangle$ in S_n can be written uniquely as $\sigma \langle (1\,2\ldots n) \rangle$, where σ fixes 1.

(b) Explain how Lagrange's statement follows from part (a).

Proof.   (a) Write $\rho = (1\,2\ldots n) \in S_n$ and $H = \langle \rho \rangle$. Let τH any coset relative to H, with $\tau \in S_n$. We must prove that there exists a unique $\sigma \in \tau H$ such that $\sigma(1) = 1$

- Existence. Let $k = \tau^{-1}(1)$ and $\sigma = \tau\rho^{k-1}$. Then $\sigma \in \tau H$, and

$$\sigma(1) = (\tau\rho^{k-1})(1) = \tau(k) = 1.$$

- Unicity. If $\sigma H = \sigma' H$, with $\sigma(1) = \sigma'(1) = 1$, then $\sigma' \in \sigma H$, so

$$\sigma' = \sigma\rho^l, \quad l \in \mathbb{Z}.$$

   Since $\sigma'(1) = 1$, we have $\sigma(\rho^l(1)) = 1 = \sigma(1)$. σ is one-to-one, so $\rho^l(1) = 1$, therefore $l \equiv 0 \pmod n$, so $\rho^l = e$ and $\sigma = \sigma'$.

(b) As $H = \langle \rho \rangle$ is the stabilizer of $\theta_i = \alpha_i^n$, the value of $\tau \cdot \theta_i$ are the all the same when τ is in σH, where σ is the unique representative of the coset τH such that $\sigma(1) = 1$. We obtain the elements of the orbit $\mathcal{O}_{\theta_i}$ under the action of S_n, by taking the value of $\sigma \cdot \theta_i$ with $\sigma(1) = 1$.

$$\mathcal{O}_{\theta_i} = \{\sigma \cdot \theta_i \mid \sigma \in S_n,\ \sigma(1) = 1\}.$$

Moreover these values are distinct. Indeed, if $\sigma \cdot \theta_i = \sigma' \cdot \theta_i$, where $\sigma(1) = \sigma'(1) = 1$, then $\sigma'^{-1}\sigma \in H$, so $\sigma H = \sigma' H$. By part (a) (unicity), we obtain $\sigma = \sigma'$. (Thus $|\mathcal{O}_{\theta_i}| = (n-1)!$ is the degree of the Lagrange resolvent.)

So the resolvent is the product

$$R(x) = \prod_{\sigma \in S_n,\ \sigma(1)=1} (x - \sigma \cdot \alpha_i^n).$$

As Lagrange says, the roots of the resolvent of $\theta_i = \alpha_i^n$ come from the permutations of the $n-1$ roots $x_2, \ldots, x_n$ that ignore the root x_1.

$\square$

Ex. 12.1.15 *Given the Lagrange resolvent $\alpha_1, \ldots, \alpha_{p-1}$ defined in (12.19),*

$$\alpha_i = x_1 + \zeta_p^i x_2 + \zeta_p^{2i} x_3 + \cdots + \zeta_p^{(p-1)i} x_p,$$

the goal of this exercise is to prove that

$$x_i = \frac{1}{p}\left(\sigma_1 + \sum_{j=1}^{p-1} \zeta_p^{-j(i-1)} \alpha_j\right).$$

(a) *Write $\alpha_j = \sum_{l=1}^{p} \zeta_p^{j(l-1)} x_l$ for $1 \leq j \leq p$, so that $\alpha_p = \sigma_1$. Then show that*

$$\sum_{j=1}^{p} \zeta_p^{-j(i-1)} \alpha_j = \sum_{j,l=1}^{p} (\zeta_p^{l-i})^j x_l.$$

(b) *Given an integer m, use Exercise 9 of section A.2 to prove that*

$$\sum_{j=1}^{p} (\zeta_p^m)^j = \begin{cases} p, & \text{if } m \equiv 0 \mod p, \\ 0, & \text{otherwise.} \end{cases}$$

Proof. (a) By definition,

$$\alpha_j = \sum_{l=1}^{p} \zeta_p^{j(l-1)} x_l, \qquad 1 \leq j \leq p.$$

Therefore

$$\sum_{j=1}^{p} \zeta_p^{-j(i-1)} \alpha_j = \sum_{j=1}^{p} \zeta_p^{-j(i-1)} \sum_{l=1}^{p} \zeta_p^{j(l-1)} x_l$$

$$= \sum_{l=1}^{p} \left[\sum_{j=1}^{p} (\zeta_p^{l-i})^j\right] x_l$$

(b) • If $m \equiv 0 \mod p$, then $\zeta_p^m = 1$, so $\sum_{j=1}^{p} (\zeta_p^m)^j = p$.

• If $m \not\equiv 0 \mod p$, then $\zeta_p^m \neq 1$, so

$$\sum_{j=1}^{p} (\zeta_p^m)^j = \zeta_p^m (1 + \zeta_p^m + \zeta_p^{2m} + \cdots + \zeta_p^{(p-1)m}) = \zeta_p^m \frac{1 - (\zeta_p^m)^p}{1 - \zeta_p^m} = 0.$$

Thus,

$$\sum_{j=1}^{p} (\zeta_p^m)^j = \begin{cases} p, & \text{if } m \equiv 0 \mod p, \\ 0, & \text{otherwise.} \end{cases}$$

(c) With $m = l - i$, part (b) gives

$$\sum_{j=1}^{p} (\zeta_p^{l-i})^j = \begin{cases} p, & \text{if } l \equiv i \mod p, \\ 0, & \text{otherwise.} \end{cases}$$

Therefore, by part (a),

$$\sum_{j=1}^{p} \zeta_p^{-j(i-1)} \alpha_j = \sum_{l=1}^{p} \left[\sum_{j=1}^{p} (\zeta_p^{l-i})^j \right] x_l$$

$$= p x_i.$$

For all $i = 1, 2, \ldots, p$,

$$x_i = \frac{1}{p} \sum_{j=1}^{p} \zeta_p^{-j(i-1)} \alpha_j$$

$$= \frac{1}{p} \left(\alpha_p + \sum_{j=1}^{p} \zeta_p^{-j(i-1)} \alpha_j \right)$$

Since $\alpha_p = \sum_{l=1}^{p} \zeta_p^{p(l-1)} x_l = x_1 + \cdots + x_p = \sigma_1$, we obtain

$$x_i = \frac{1}{p} \left(\sigma_1 + \sum_{j=1}^{p-1} \zeta_p^{-j(i-1)} \alpha_j \right).$$

$\square$

Ex. 12.1.16 *Prove that Theorem 7.4.4 follows from Theorem 12.1.6 and Proposition 2.4.1.*

Proof. • Suppose that $\psi \in F(x_1, \ldots, x_n)$ is invariant under S_n.

Let $\varphi = 1$ (or any element in K). Then φ is invariant under S_n, so ψ is fixed by every permutation fixing φ. By Theorem 12.1.6. ψ is a rational function of φ with coefficients in $K = F(\sigma_1, \ldots, \sigma_n)$, i.e., $\psi \in K(\varphi) = K(1) = K$. So $\psi \in F(\sigma_1, \ldots, \sigma_n)$.

• Suppose that $\psi \in F(x_1, \ldots, x_n)$ is invariant under A_n. Let $\varphi = \sqrt{\Delta}$. As the characteristic is not 2, by Proposition 2.4.1, $\sigma \cdot \sqrt{\Delta} = \sqrt{\Delta}$ if and only if $\sigma \in A_n$, so $H(\varphi) = H(\sqrt{\Delta}) = A_n$. Thus ψ is fixed by every permutation fixing φ.

By Theorem 12.1.6. ψ is a rational function of $\varphi = \sqrt{\Delta}$ with coefficients in $K = F(\sigma_1, \ldots, \sigma_n)$, so $\psi \in K(\sqrt{\Delta})$.

$\sqrt{\Delta} \notin K$, because $\tau \cdot \sqrt{\Delta} = -\sqrt{\Delta} \neq \sqrt{\Delta}$ for every transposition τ. Therefore $K \subset K(\sqrt{\Delta})$ is a quadratic extension, and $(1, \sqrt{\Delta})$ is a basis of $K(\sqrt{\Delta})$ over K. Therefore

$$\psi = A + B\sqrt{\Delta}, \qquad A, B \in K = F(\sigma_1, \ldots, \sigma_n).$$

So Theorem 7.4.4 follows from Theorem 12.1.6.

$\square$

Ex. 12.1.17 *In Theorem 12.1.9, we used Galois correspondence to show that rational functions φ and ψ are similar if and only if $K(\varphi) = K(\psi)$. Give another proof of this result that uses only Theorem 12.1.6.*

Proof. If $\varphi, \psi \in F(x_1, \ldots, x_n)$ are similar, then $H(\varphi) = H(\psi)$. So $\sigma \cdot \psi = \psi$ for every $\sigma \in H(\varphi)$. By Theorem 12.1.6, $\psi \in K(\varphi)$. Exchanging φ and ψ, we obtain similarly $\varphi \in K(\psi)$. Therefore

$$K(\varphi) = K(\varphi, \psi) = K(\psi, \varphi) = K(\psi).$$

Conversely, if $K(\varphi) = K(\psi)$, then $\psi \in K(\varphi)$, so $\psi(x_1, \ldots, x_n) = f(\varphi(x_1, \ldots, x_n))$, where $f \in K(x)$. Therefore, for all $\sigma \in H(\varphi)$,

$$\sigma \cdot \psi = f(\varphi(x_{\sigma(1)}, \ldots, x_{\sigma(n)})) = f(\varphi(x_1, \ldots, x_n)) = \psi.$$

So $H(\varphi) \subset H(\psi)$, and similarly $H(\psi) \subset H(\varphi)$, thus $H(\varphi) = H(\psi)$. $\qquad\square$

Ex. 12.1.18 *Consider the quartic polynomial $f = x^4 + 2x^2 - 4x + 2 \in \mathbb{Q}[x]$.*

(a) Show that the Ferrari resolvent of (12.10) is $y^3 - 2y^2 - 8y$.

(b) Using the root $y_1 = 0$ of the cubic of part (a), show that (12.11) becomes

$$x^2 = \pm\sqrt{-2}(x - 1)$$

and conclude that the four roots of f are

$$\frac{\sqrt{2}}{2}i \pm \frac{1}{2}\sqrt{-2 - 4i\sqrt{2}} \text{ and } \frac{\sqrt{2}}{2}i \pm \frac{1}{2}\sqrt{-2 + 4i\sqrt{2}}.$$

(c) Use Euler's solution (12.17) to find the roots of f. The formulas are surprisingly different. We will see in Chapter 13 that this quartic is especially simple. For most quartics, the formulas for the roots are much more complicated.

Proof.   (a) The Ferrari resolvent $\theta(y)$ is given by Exercise 4:

$$\theta(y) = y^3 - \sigma_2 y^2 + (\sigma_1\sigma_3 - 4\sigma_4)y - \sigma_1^2\sigma_4 - \sigma_3^2 + 4\sigma_2\sigma_4.$$

As $f = x^4 + 2x^2 - 4x + 2 \in \mathbb{Q}[x]$, $\sigma_1 = 0, \sigma_2 = 2, \sigma_3 = 4, \sigma_4 = 2$, so

$$\theta(y) = y^3 - 2y^2 - 8y.$$

(b) We use the root $y_1 = 0$ of the Ferrari resolvent in (12.11)

$$x^2 - \frac{\sigma_1}{2}x + \frac{y_1}{2} = \pm\sqrt{y_1 + \frac{\sigma_1^2}{4} - \sigma_2}\left(x + \frac{\frac{-\sigma_1}{2}y_1 + \sigma_3}{2(y_1 + \frac{\sigma_1^2}{4} - \sigma_2)}\right),$$

Here $\sigma_1 = 0, \sigma_2 = 2, \sigma_3 = 4, \sigma_4 = 2$, therefore $y_1 + \frac{\sigma_1^2}{4} - \sigma_2 = -2$, so the roots of f are the solutions of

$$x^2 = \pm\sqrt{-2}(x - 1),$$

(More directly, the equation is

$$x^4 = -2x^2 + 4x - 2 = -2(x^2 - 2x + 1) = -2(x - 1)^2 = [\sqrt{-2}(x - 1)]^2,$$

so
$$x^2 = \pm\sqrt{-2}(x-1).)$$

The roots of f are the roots of
$$x^2 - i\sqrt{2}\,x + i\sqrt{2} \qquad \text{or} \qquad x^2 + i\sqrt{2}\,x - i\sqrt{2}.$$

$$
\begin{aligned}
x^2 - i\sqrt{2}\,x + i\sqrt{2} &= \left(x - i\frac{\sqrt{2}}{2}\right)^2 + \frac{1}{2} + i\sqrt{2} \\
&= \left(x - i\frac{\sqrt{2}}{2}\right)^2 - \frac{1}{4}\left(-2 - 4i\sqrt{2}\right) \\
&= \left(x - i\frac{\sqrt{2}}{2}\right)^2 - \left(\frac{1}{2}\sqrt{-2 - 4i\sqrt{2}}\right)^2 \\
&= \left(x - i\frac{\sqrt{2}}{2} - \frac{1}{2}\sqrt{-2 - 4i\sqrt{2}}\right)\left(x - i\frac{\sqrt{2}}{2} + \frac{1}{2}\sqrt{-2 - 4i\sqrt{2}}\right),
\end{aligned}
$$

and similarly
$$x^2 + i\sqrt{2}\,x - i\sqrt{2} = \left(x + i\frac{\sqrt{2}}{2} - \frac{1}{2}\sqrt{-2 + 4i\sqrt{2}}\right)\left(x + i\frac{\sqrt{2}}{2} + \frac{1}{2}\sqrt{-2 + 4i\sqrt{2}}\right).$$

so the roots of f are
$$i\frac{\sqrt{2}}{2} + \frac{1}{2}\sqrt{-2 - 4i\sqrt{2}}, \; i\frac{\sqrt{2}}{2} - \frac{1}{2}\sqrt{-2 - 4i\sqrt{2}}, \; -i\frac{\sqrt{2}}{2} + \frac{1}{2}\sqrt{-2 + 4i\sqrt{2}}, \; -i\frac{\sqrt{2}}{2} - \frac{1}{2}\sqrt{-2 + 4i\sqrt{2}}$$

Moreover
$$
\begin{aligned}
(a + ib)^2 = -2 - 4i\sqrt{2} &\iff a^2 + b^2 = |-2 - 4i\sqrt{2}| = 6, \; a^2 - b^2 = -2, \; ab < 0 \\
&\iff a + ib = \pm(\sqrt{2} - 2i)
\end{aligned}
$$

so
$$\sqrt{-2 - 4i\sqrt{2}} = \pm(\sqrt{2} - 2i), \qquad \sqrt{-2 + 4i\sqrt{2}} = \pm(\sqrt{2} + 2i).$$

The roots of f are $x_1, x_2, x_3 = \overline{x_1}, x_4 = \overline{x_2}$, where
$$x_1 = \frac{\sqrt{2}}{2} + i\left(\frac{\sqrt{2}}{2} - 1\right),$$
$$x_2 = -\frac{\sqrt{2}}{2} + i\left(-\frac{\sqrt{2}}{2} - 1\right).$$

Note: $x_1, x_2, x_3, x_4 \in \mathbb{Q}(i, \sqrt{2})$, so $\mathbb{Q}(x_1, x_2, x_3, x_4) \subset \mathbb{Q}(i, \sqrt{2})$.
$\sqrt{2} = x_1 + \overline{x_1} = x_1 + x_3 \in \mathbb{Q}(x_1, x_2, x_3, x_4)$ and $i = -\frac{1}{2}(x_1 + x_2) \in \mathbb{Q}(x_1, x_2, x_3, x_4)$. Therefore the splitting field of f over $\mathbb{Q}$ is $L = \mathbb{Q}(i, \sqrt{2})$.

The Galois group is $\mathrm{Gal}(L/\mathbb{Q}) = \langle \sigma, \tau \rangle$, where $\sigma(\sqrt{2}) = -\sqrt{2}, \sigma(i) = i$, and τ is the complex conjugation. As permutation group, $\mathrm{Gal}_\mathbb{Q}(f) = \langle (1\,2)(3\,4), (1\,3)(2\,4) \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ has order 4.

(c) The Euler's solution gives the roots

$$\alpha = \frac{1}{4}\left(\sigma_1 + \varepsilon_1\sqrt{4y_1 + \sigma_1^2 - 4\sigma_2} + \varepsilon_2\sqrt{4y_2 + \sigma_1^2 - 4\sigma_2} + \varepsilon_3\sqrt{4y_3 + \sigma_1^2 - 4\sigma_2}\right),$$

where $\sigma_1 = 0, \sigma_2 = 2$ and $y_1 = 0, y_2, y_3$ are the roots of

$$y^3 - 2y^2 - 8y = y(y^2 - 2y - 8) = y(y - 4)(y + 2),$$

so $y_1 = 0, y_2 = 4, y_3 = -2$.

So

$$\alpha = \frac{1}{4}(\varepsilon_1\sqrt{-8} + \varepsilon_2\sqrt{8} + \varepsilon_3\sqrt{-16})$$
$$= \varepsilon_1 i\frac{\sqrt{2}}{2} + \varepsilon_2\frac{\sqrt{2}}{2} + \varepsilon_3 i$$

Morever $\varepsilon_i = \pm 1$ satisfy

$$t_1 t_2 t_3 = \varepsilon_1\varepsilon_2\varepsilon_3(i\sqrt{8})(\sqrt{8})4i = \sigma_1^3 - 4\sigma_1\sigma_2 + 8\sigma_3 = 8\sigma_3 = 32,$$

so $\varepsilon_3 = -\varepsilon_1\varepsilon_2$. We obtain the four roots

$$x_1 = \frac{\sqrt{2}}{2} + i\left(\frac{\sqrt{2}}{2} - 1\right), \qquad x_3 = \overline{x_1} = \frac{\sqrt{2}}{2} - i\left(\frac{\sqrt{2}}{2} - 1\right),$$
$$x_2 = -\frac{\sqrt{2}}{2} + i\left(-\frac{\sqrt{2}}{2} - 1\right), \quad x_4 = \overline{x_2} = -\frac{\sqrt{2}}{2} - i\left(-\frac{\sqrt{2}}{2} - 1\right)$$

Le formulas are NOT surprisingly different.

$\square$

Ex. 12.1.19 *This exercise will prove a version of Theorem 12.1.10 for a subgroup H of an arbitrary finite group G. When $G = S_n$, Theorem 12.1.10 used the action of S_n on L and wrote $H = H(\varphi)$ for some $\varphi \in L$. In general , we us the action of G on the left cosets of H defined by $g \cdot hH = ghH$ for $g, h \in G$.*

(a) *Prove that $g \cdot hH = ghH$ is well defined, i.e., $hH = h'H$ implies that $ghH = gh'H$.*

(b) *Prove that H is the isotropy subgroup of the identity coset eH.*

(c) *Let $m = [G : H]$, so that left cosets of H can be labeled $g_1 H, \ldots, g_m H$. Then, for $g \in G$, let $\sigma \in S_m$ be the permutation such that $g \cdot g_i H = g_{\sigma(i)}H$. Prove that the map $g \mapsto \sigma$ defines a group homomorphism $G \to S_m$.*

(d) *Let N the kernel of the map of part (c). Thus N is a normal subgroup of G. Prove that $N \subset H$.*

(e) *Prove that $[G : N]$ divides $m!$.*

(f) *Explain why you have proved the following result: If H is a subgroup of a finite group G, then H contains a normal subgroup of G whose index divides $[G : H]!$.*

(g) *Use part (f) and Proosition 8.4.6 to give a quick proof of Theorem 12.1.10.*

Proof. (a) If $hH = h'H$, then $ghH = gh'H$. Indeed, if $u \in ghH$, then $u = ghx$, where $x \in H$. Since $hH = h'H$, then $hx \in hH$ implies $hx \in h'H$, so $hx = h'x'$ for some $x' \in H$. So $u = ghx = gh'x', x' \in H$, therefore $u \in gh'x'$, so $ghH \subset gh'H$, and similarly $gh'H \subset ghH$, so $ghH = gh'H$, and $g \cdot hH = ghH$ is well defined.

Moreover $e \cdot hH = ehH = hH$ and $g \cdot (g' \cdot H) = g \cdot g'H = gg'H = (gg') \cdot H$, so $g \cdot hH = ghH$ defines a left action of G on the set of left cosets.

(b) Let u any element of G.

$$u \in \mathrm{Stab}_G(eH) \iff u \cdot eH = eH \iff ueH = eH \iff uH = H \iff u \in H.$$

The last equivalence is true, because $uH = H$ implies $u = ue \in H$, and conversely, if $u \in H$, $uH \subset H$ and every element $x \in H$ satisfies $x = u(u^{-1}x)$, where $u^{-1}x \in H$, so $x \in uH$.

$$\mathrm{Stab}_G(eH) = H.$$

(c) Let
$$\psi \begin{cases} G & \to & S_m \\ g & \mapsto & \sigma : \quad \forall i \in [\![1, m]\!], \; g \cdot g_i H = g_{\sigma(i)} H \end{cases}$$

Let $g, g' \in G$, $\sigma = \psi(g), \sigma' = \psi(g')$. For all $i, 1 \le i \le n$,

$$(gg') \cdot g_i H = g \cdot (g' \cdot g_i H) = g \cdot g_{\sigma'(i)} H = g_{\sigma(\sigma'(i))} H = g_{(\sigma \circ \sigma')(i)} H.$$

Therefore $\psi(gg') = \sigma \circ \sigma'$, so $\psi : G \to S_m$ is a group homomorphism.

(d) Let N be the kernel of ψ. For every $g \in G$,

$$\begin{aligned} g \in N &\iff \forall i \in [\![1, m]\!], \; g \cdot g_i H = g_i H \\ &\iff \forall h \in G, \; ghH = hH \\ &\iff \forall h \in G, \; h^{-1}ghH = H \\ &\iff \forall h \in G, \; h^{-1}gh \in H \\ &\iff \forall h \in G, \; g \in hHh^{-1} \\ &\iff g \in \bigcap_{h \in G} hHh^{-1} \end{aligned}$$

so

$$N = \bigcap_{h \in G} hHh^{-1}.$$

(N is the *core* of H in G. We write $N = \mathrm{Core}_G(H)$.)
Since $H = eHe^{-1} \subset \bigcap_{h \in G} hHh^{-1}$, $H \subset N$.

(e) The first isomorphism theorem for groups gives the isomorphism

$$G/N = G/\ker(\psi) \simeq \mathrm{Im}(\psi),$$

so $[G : N] = |\mathrm{Im}(\psi)|$ divides $|S_m| = m!$ by Lagrange's theorem.

$$[G : N] \mid m!.$$

(f) We can conclude that for any subgroup H of a finite group G, then H contains the core N of H in G, which is a normal subgroup of G whose index divides $[G : H]!$.

(g) • Let $H \subset S_n$ be a subgroup of index $[S_n : H] > 1$, where $n \geq 5$.

Let $N = \text{Core}_{S_n}(H)$. Then $N \subset H \subset S_n$, and N is normal in S_n, and $N \neq S_n$ (since $[S_n : H] > 1$). By Proposition 8.4.6, $N = A_n$ or $N = \{e\}$.

If $N = A_n$, then $N = A_n \subset H \subset S_n$, thus $1 < [S_n : H] \leq [S_n : A_n] = 2$, therefore$[S_n : H] = 2 = [S_n : A_n]$, where $A_n \subset H$, so $H = A_n$.

In the other case, $N = \{e\}$. By part (e), $[S_n : N] \mid [S_n : H]!$, thus $n! \mid m!$, where $m = [S_n : H]$. So $n \leq m = [S_n : H]$. This proves part (a) of Theorem 12.1.10.

• Let $H \subset A_n$ be a subgroup of index $[A_n : H] > 1$.

Let $N = \text{Core}_{A_n}(H)$. Then $N \subset H \subset A_n$ and N is normal in A_n. Since A_n is simple for $n \geq 5$, and $N \subset H \neq A_n$, $N = \{e\}$.

By part (e), $[A_n : N] \mid [A_n : H]!$, so $n!/2 \mid m!$, where $m = [A_n : H]$.

If $m < n$ then $m \leq n - 1, m! \leq (n-1) < n!/2$ (since $n > 2$), in contradiction with $n!/2 \mid m!$. Therefore

$$n \leq m = [A_n : H].$$

This proves part (b) of Theorem 12.1.10.

□

Ex. 12.1.20 *Let G be a finite group and let p be the smallest prime dividing $|G|$. Prove that every subgroup of index p in G is normal.*

Proof. Let $N = \text{Core}_G(H)$. Then $N \subset H \subset G$, and N is normal in G.
By Exercise 19 part (f),
$$[G : N] \mid [G : H]! = p!.$$

Moreover,
$$[G : N] = [G : H][H : N] = p[H : N],$$

so
$$[H : N] \mid (p-1)!.$$

If $[H : N] \neq 1$, there exists a prime q such that $q \mid [H : N]$. Since $[H : N] \mid (p-1)!$, $q < p$. But q divides [H:N] , so q divides $|H|$, which divides $|G|$. But p is the smallest prime divisor of $|G|$: this is a contradiction.
So $[H : N] = 1$, $N = H$. Therefore $H = N$ is normal in G.   □

Ex. 12.1.21 *Part (a) of Theorem 12.1.10 implies that when $n \geq 5$, the index of a proper subgroup of S_n is either 2 or $\geq n$.*

(a) *Prove that S_n always has a subgroup H of index n. This means that equality can occur in the bound $[S_n : H] \geq n$.*

(b) *Give an example to prove that Theorem 12.1.10 is false when $n = 4$.*

Proof. (a) The subgroup H of S_n of the permutations σ that fix n is a subgroup isomorphic to S_{n-1}, and $[S_n : H] = n!/(n-1)! = n$.

(b) In the Exercise 3, we saw that $H = H(y_1)$, where $y_1 = x_1x_2 + x_3x_4$ is a group isomorphic to D_8:

$$\langle (1\,2), (1\,3\,2\,4) \rangle = \{(), (1\,2), (1\,3\,2\,4), (1\,3)(2\,4), (1\,2)(3\,4), (1\,4)(2\,3), (3\,4), (1\,4\,2\,3)\},$$

so $[S_4 : H] = 3 < n = 4$. This proves that the Theorem 12.1.10 is false if we forget the hypothesis $n \geq 5$.

$\square$