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, and

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

where $\varphi_1 = \varphi, \varphi_2, \ldots \varphi_r$ are the *distinct* conjugates of φ:

$$A := \{\tau \cdot \varphi \mid \tau \in S_n\} = \{\varphi_1, \ldots, \varphi_r\}.$$

As in the proof of Theorem 7.1.1, we first show that σ permute the φ_i.

If $\varphi_i \in A$, then $\varphi_i = \tau \cdot \varphi$ for some $\tau \in S_n$. Therefore

$$\sigma \cdot \varphi_i = \sigma \cdot (\tau\varphi) = (\sigma\tau) \cdot \varphi.$$

Since $\sigma' = \sigma\tau \in S_n$, $\sigma' \cdot \varphi = (\sigma\tau) \cdot \varphi \in A$, therefore

$$\{\sigma \cdot \varphi_1, \ldots, \sigma \cdot \varphi_r\} \subset \{\varphi_1, \ldots, \varphi_r\}.$$

Since the map $\psi \mapsto \sigma \cdot \psi$ is injective, the elements $\sigma \cdot \varphi_i$ are distinct, and A is finite, thus we can conclude that

$$\{\sigma \cdot \varphi_1, \ldots, \sigma \cdot \varphi_r\} = \{\varphi_1, \ldots, \varphi_r\}.$$

Hence the exists some $\tau \in S_r$ such that,

$$\sigma \cdot \varphi_i = \varphi_{\tau(i)}, \quad 1 \le i \le r.$$

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

Since $\sigma \cdot \theta(x) = \theta(x)$ for all $\sigma \in S_n$, the coefficients of θ are in K by theorem 2.2.7, so $\theta(x) \in K[x]$. $\qquad \square$

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

Proof. Let $F = \mathbb{Q}(\omega)$, $z_1 = \frac{1}{3}(x_1 + \omega^2 x_2 + \omega x_3) \in K = \mathbb{Q}(\omega)(x_1, x_2, x_3)$, 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 $F(x_1, x_2, x_3)$.

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

$$z_1^3 z_2^3 = \frac{1}{3^6}(\sigma_1^2 - 3\sigma_1)^3 = -\frac{1}{27}\left(-\frac{\sigma_1^2}{3} + \sigma_2\right)^3 = -\frac{p^3}{27}, \text{ where } p = -\frac{\sigma_1^2}{3} + \sigma_2.$$

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

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

2

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

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 $y_1 = x_1 x_2 + x_3 x_4$. 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) $y_1 = x_1 x_2 + x_3 x_4, y_2 = (2\,3) \cdot y_1 = x_1 x_3 + x_2 x_4, y_3 = (2\,4) \cdot y_1 = x_1 x_4 + x_2 x_3$ are distinct elements of the orbit of y_1.

Since $|H(y_1)| = |\text{Stab}_{S_4}(y_1)| = 8$ (see Part (b)), $|\mathcal{O}_{y_1}| = 3$, so y_1, y_2, y_3 are all the elements of $\mathcal{O}_{y_1}$.

$$\mathcal{O}_{y_1} = \{y_1, y_2, y_3\} = \{x_1 x_3 + x_2 x_4, x_1 x_3 + x_2 x_4, x_1 x_4 + x_2 x_3\}.$$

Therefore

$$\theta(y) = \left((y - (x_1 x_2 + x_3 x_4))\right)\left((y - (x_1 x_3 + x_2 x_4))\right)\left((y - (x_1 x_4 + x_2 x_3))\right)$$

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()
```

3

```
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's 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 number the 4 consecutive summits of the square in the order $(1, 3, 2, 4)$, 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 is 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
$$x^4 - \sigma_1 x^3 = -\sigma_2 x^2 + \sigma_3 x - \sigma_4,$$

we 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 quadratic.*

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

5

(b) *Now let $y_1 = x_1x_2 + x_3x_4$, 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. (a) 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

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

(b) Using $y_1 = x_1x_2 + x_3x_4$, and setting

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

then

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

$$= x_1x_2 + x_3x_4 + \frac{1}{4}(x_1 + x_2 + x_3 + x_4)^2 - (x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4)$$

$$= \frac{1}{4}\left[x_1^2 + x_2^2 + x_3^2 + x_4^2 - 2(x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4) + 4(x_1x_2 + x_3x_4)\right]$$

$$= \frac{1}{4}\left[x_1^2 + x_2^2 + x_3^2 + x_4^2 + 2x_1x_2 + 2x_3x_4 - 2(x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4)\right]$$

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

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

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

We choose the square root such that

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

6

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

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

which gives

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

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

$$S = \frac{\sigma_1}{2} + \frac{t_1}{2}$$
$$= \frac{1}{2}(x_1 + x_2 + x_3 + x_4 + x_1 + x_2 - x_3 - x_4)$$
$$= x_1 + x_2$$

$$P = \frac{y_1}{2} + \frac{1}{2t_1}(\sigma_1 y_1 - 2\sigma_3)$$
$$= \frac{y_1}{2} + \frac{1}{2t_1}[(x_1 + x_2 + x_3 + x_4)(x_1 x_2 + x_3 x_4) - 2(x_1 x_2 x_3 + x_1 x_2 x_4 + x_1 x_3 x_4 + x_2 x_3 x_4)]$$
$$= \frac{y_1}{2} + \frac{1}{2t_1}\left[x_1^2 x_2 + x_1 x_2^2 + x_3^2 x_4 + x_3 x_4^2 - x_1 x_3 x_4 - x_2 x_3 x_4 - x_1 x_2 x_3 - x_1 x_2 x_4 \right]$$
$$= \frac{y_1}{2} + \frac{1}{2t_1}(x_1 + x_2 - x_3 - x_4)(x_1 x_2 - x_3 x_4)$$
$$= \frac{1}{2}(x_1 x_2 + x_3 x_4 + x_1 x_2 - x_3 x_4)$$
$$= x_1 x_2$$

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 $K = F(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$.*

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

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

7

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 $S_4 = \langle \sigma, \tau \rangle$, every permutation in S_4 lets the coefficients of $\theta(t)$ unchanged, therefore $\theta(t)$ has coefficients in $K = F(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ and $\theta(t) \in K[t]$. $\qquad \square$

Ex. 12.1.7 *Show that (12.15) implies the equations for x_1, x_2, x_3, x_4 given in the text.*

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

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

To conclude

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

$\qquad \square$

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) By (12.15),

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

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);v
```

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

So
$$t_1 t_2 t_3 = (x_1 + x_2 - x_3 - x_4)(x_1 - x_2 + x_3 - x_4)(x_1 - x_2 - x_3 + x_4)$$
$$= \sigma_1^3 - 4\,\sigma_1\sigma_2 + 8\,\sigma_3.$$

$\square$

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
$$\psi : \begin{cases} S_n & \to & \mathrm{Gal}(L/K) \\ \tau & \mapsto & \tilde{\tau} \begin{cases} L & \to & L \\ f & \mapsto & \tau \cdot f \end{cases} \end{cases}$$

(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 $\tau \in H$.

10

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

- If $\tau \in H(\varphi)$, $\tau \cdot \varphi = \varphi$, where $\varphi = \sum_{\sigma \in H} \sigma \cdot m$, 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 exists 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 $n \geq 5$. Prove that $[A_n : H] \geq n$.*

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

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

and let G the subgroup of A_n defined by

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

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 $\{\varphi_1, \varphi_2, \dots, \varphi_s\}$ there exist two distinct permutations $\tau_1, \tau_2 \in A_n$ such that

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

So $e \neq \tau_2^{-1}\tau_1 \in G$, $G \neq \{e\}$: 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 $\deg(R_j) \geq 2$.

(b) Since $K \subset K(\sqrt{\Delta}) \subset M$, 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 H_j is a proper subgroup of A_n such that $(A_n : H_j) < n$. By Theorem 12.1.10(b), 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 $\xi = \zeta^{\sigma^{-1}(1)-1}$, thus $\zeta^{\sigma^{-1}(1)-1+i-1} = \zeta^{\sigma^{-1}(i)-1}$.

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 be 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 $\sigma(\rho^l(1)) = 1 = \sigma(1)$ and 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 $\sum_{j=1}^{p} (\zeta_p^m)^j = p$.

15

- 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 $i = 1, 2, \ldots, p$,

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

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

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 $\varphi = 1$. 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 $H(\varphi) = H(\psi)$. $\square$

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

$$x^2 - i\sqrt{2}\,x + i\sqrt{2} \qquad \text{or} \qquad x^2 + i\sqrt{2}\,x - i\sqrt{2}.$$

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

$$= \left(x - i\frac{\sqrt{2}}{2}\right)^2 - \frac{1}{4}\left(-2 - 4i\sqrt{2}\right)$$

$$= \left(x - i\frac{\sqrt{2}}{2}\right)^2 - \left(\frac{1}{2}\sqrt{-2 - 4i\sqrt{2}}\right)^2$$

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

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

$$(a + ib)^2 = -2 - 4i\sqrt{2} \iff a^2 + b^2 = |-2 - 4i\sqrt{2}| = 6, \ a^2 - b^2 = -2, \ ab < 0$$

$$\iff a + ib = \pm(\sqrt{2} - 2i)$$

so

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

18

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

Therefore

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

$$= \varepsilon_1 i\frac{\sqrt{2}}{2} + \varepsilon_2\frac{\sqrt{2}}{2} + \varepsilon_3 i$$

Moreover $\varepsilon_i = \pm 1$ 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

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

The 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 Proposition 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 $u \in gh'H$, 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.

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

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 $x \in uH$.

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

(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 $i, 1 \leq i \leq m$,

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

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 $N = \text{Core}_G(H)$.)

Since $H = eHe^{-1} \supset \bigcap_{h \in G} hHh^{-1}$, $H \supset N$.

20

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

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

so $[G : N] = |\operatorname{Im}(\psi)|$ 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 $N = \operatorname{Core}_{S_n}(H)$. 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 $m = [S_n : H]$. Therefore $n \leq m = [S_n : H]$. This proves part (a) of Theorem 12.1.10.

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

Let $N = \operatorname{Core}_{A_n}(H)$. 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), $[A_n : N] \mid [A_n : H]!$, thus $n!/2 \mid m!$, 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.

$\square$

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

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

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

If $[H : N] \neq 1$, there exists a prime q such that $q \mid [H : N]$. Since $[H : N] \mid (p-1)!$, we see that $q < p$. 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.
   Thus $[H : N] = 1$, $N = H$. Therefore $H = N$ is normal in G. $\square$

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 $y_1 = x_1 x_2 + x_3 x_4$ 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 $n \geq 5$.

$\square$

12.2 GALOIS

Ex. 12.2.1 *Let F an infinite field and let V be a finite-dimensional vector space over F. The goal of this exercise is to prove that V cannot be the union of a finite number of proper subspaces. This will be used in Exercise 2 to prove the existence of Galois resolvents.*

Let $W_1, \ldots, W_m$ be proper subspaces of V such that $V = W_1 \cup \cdots \cup W_m$, where $m > 1$ is the smallest positive integer for which this is true. We derive a contradiction as follows.

(a) *Explain why there is $v \in W_1 \setminus (W_2 \cup \cdots \cup W_m)$.*

(b) *There is $w \in V \setminus W_1$, since W_1 is a proper subspace. Using v from part (a), we have $\lambda v + w \in V = W_1 \cup \cdots \cup W_m$ for all $\lambda \in F$. Explain why this implies that there are $\lambda_1 \neq \lambda_2$ in F such that $\lambda_1 v + w, \lambda_2 v + w \in W_i$ for some i.*

(c) *Now derive the desired contradiction.*

Proof. (a) If there is no $v \in W_1 \setminus (W_2 \cup \cdots \cup W_m)$, then $W_1 \subset W_2 \cup \cdots W_m$. Therefore $V = W_2 \cup \cdots W_m$, so V is the union of $m - 1$ proper subspaces, in contradiction with the definition of m. Thus there is $v \in W_1 \setminus (W_2 \cup \cdots \cup W_m)$.

(b) There is $w \in V \setminus W_1$, since W_1 is a proper subspace. Since $v \in W_1 \subset V$, and $w \in V$, $\lambda v + w \in V = W_1 \cup \cdots \cup W_m$, for every $\lambda \in F$.

Let $\mu_1, \ldots, \mu_{m+1}$ be $m + 1$ distinct elements of F. Since F is infinite, it is possible to find such elements. For $i = 1, \ldots, m + 1$, $\mu_i v + w \in W_1 \cup \cdots \cup W_m$.

Since there are more μ_i than subspaces W_j, there exist two distinct values $\mu_j \neq \mu_k$ such that $\mu_j v + w, \mu_k v + w$ are in the same subspace W_i. If we write $\lambda_1 = \mu_i, \lambda_2 = \mu_j$, then

$$\lambda_1 \neq \lambda_2, \qquad \lambda_1 v + w = r \in W_i, \quad \lambda_2 v + w = s \in W_i \text{ for some } i, \ 1 \leq i \leq m.$$

(c) Note that $W_i \neq W_1$, otherwise $w = r - \lambda_1 v \in W_1$, and this is a contradiction with the definition of w. Therefore

$$r - s = (\lambda_1 - \lambda_2)v \in W_i \text{ for some } i = 2, \ldots, m.$$

Since $\lambda_1 - \lambda_2 \neq 0$, $v \in W_2 \cup \cdots \cup W_m$, which is contradictory with the choice of v.

Conclusion: a finite dimensional vector space over an infinite field cannot be the union of a finite number of proper subspaces.

$\square$

Ex. 12.2.2 *Suppose that we have an extension $F \subset L$, where F is infinite. The goal of this exercise is to show that if $\alpha_1, \ldots, \alpha_n \in L$ are distinct, then $t_1, \ldots, t_n \in F$ can be chosen so that the polynomial $s(y)$ defined in (12.21) has distinct roots. Given $\sigma \neq \tau$ in S_n, let*

$$W_{\sigma,\tau} = \{(t_1, \ldots, t_n) \in F^n \mid \sum_{i=1}^{n}(\alpha_{\sigma(i)} - \alpha_{\tau(i)})t_i = 0\}.$$

(a) *Prove that $W_{\sigma,\tau}$ is a subspace of F^n and that $W_{\sigma,\tau} \neq F^n$.*

(b) *Show that part (a) and Exercise 1 imply that there are $t_1, \ldots, t_n \in F$ such that the polynomial $s(y)$ from (12.21) has distinct roots.*

Proof. (a) $(0, \ldots, 0) \in W_{\sigma,\tau}$. If $\lambda, \mu \in F$ and $v = (t_1, \ldots, t_n) \in W_{\sigma,\tau}$, $w = (s_1, \ldots, s_n) \in W_{\sigma,\tau}$, then $\sum_{i=1}^{n}(\alpha_{\sigma(i)} - \alpha_{\tau(i)})t_i = 0$ and $\sum_{i=1}^{n}(\alpha_{\sigma(i)} - \alpha_{\tau(i)})s_i = 0$, therefore

$$0 = \lambda \sum_{i=1}^{n}(\alpha_{\sigma(i)} - \alpha_{\tau(i)})t_i + \mu \sum_{i=1}^{n}(\alpha_{\sigma(i)} - \alpha_{\tau(i)})s_i = \sum_{i=1}^{n}(\alpha_{\sigma(i)} - \alpha_{\tau(i)})(\lambda t_i + \mu s_i),$$

so $\lambda v + \mu w \in W_{\sigma,\tau}$. Thus $W_{\sigma,\tau}$ is a subspace of F^n.

More shortly, $W_{\sigma,\tau}$ is the kernel of the linear map

$$(t_1, \ldots, t_n) \mapsto \sum_{i=1}^{n}(\alpha_{\sigma(i)} - \alpha_{\tau(i)})t_i.$$

Since $\sigma \neq \tau$, there exists $k \in [\![1, n]\!]$ such that $\sigma(k) \neq \tau(k)$. Moreover the α_i are distinct, so $\alpha_{\sigma(k)} \neq \alpha_{\tau(k)}$. Let $v = (t_1, \ldots, t_k, \ldots, t_n) = (0, \ldots, 1, \ldots, 0)$, where $t_k = 1$ and $t_i = 0$ if $i \neq k$. Then $v \in F^n$ satisfies $\sum_{i=1}^{n}(\alpha_{\sigma(i)} - \alpha_{\tau(i)})t_i = \alpha_{\sigma(k)} - \alpha_{\tau(k)} \neq 0$, so $W_{\sigma,\tau} \neq F^n$.

Therefore $W_{\sigma,\tau}$ is a proper subspace of F^n, for all $\sigma, \tau \in S_n$.

(b) By Exercise 1,

$$\bigcup_{(\sigma,\tau) \in S_n \times S_n, \sigma \neq \tau} W_{\sigma,\tau} \neq F^n.$$

Therefore there exists $(t_1, \ldots, t_n) \in F^n$ such that $(t_1, \ldots, t_n) \notin W_{\sigma,\tau}$ for all $\sigma, \tau \in S_n, \sigma \neq \tau$. This means that

$$\sum_{i=1}^{n} \alpha_{\sigma(i)} t_i \neq \sum_{i=1}^{n} \alpha_{\tau(i)} t_i, \qquad \text{for all } \sigma, \tau \in S_n, \sigma \neq \tau,$$

so the $n!$ roots of

$$s(y) = \prod_{\sigma \in S_n} \left(y - (t_1 \alpha_{\sigma(1)} + \cdots + t_n \alpha_{\sigma(n)}) \right)$$

are distinct.

$\square$

Ex. 12.2.3 *This exercise will prove Galois's Lemma III using the methods of Lagrange. Let $V = t_1\alpha_1 + \cdots + t_n\alpha_n$, where $t_1, \ldots, t_n$ are chosen so that the Galois resolvent $s(y)$ from (12.21) is separable. Also let $V_\sigma = t_1\alpha_{\sigma(1)} + \cdots + t_n\alpha_{\sigma(n)}$ for $\sigma \in S_n$. Prove that each α_j can be written as a rational function in V with coefficients in F by adapting the second proof of Theorem 12.1.6.*

Proof. We know from Section 12.2.B the definition of the Galois resolvent

$$s(y) = \prod_{\sigma \in S_n} (y - V_\sigma) \in F[y].$$

Let $j \in [\![1,n]\!]$ be a fixed integer. We show that $\alpha_j \in F(V)$, where $V = V_e = t_1\alpha_1 + \cdots + t_n\alpha_n$.

Let

$$\psi_j(y) = \sum_{\sigma \in S_n} \alpha_{\sigma(j)} \frac{s(y)}{y - V_\sigma}$$

$$= \sum_{\sigma \in S_n} \alpha_{\sigma(j)} \prod_{\tau \neq \sigma} (y - V_\tau).$$

If $p_\sigma = \prod_{\tau \neq \sigma}(y - V_\tau)$, then for $\varphi \in S_n$, $p_\sigma(V_\varphi) = 0$ if $\varphi \neq \sigma$, and $\prod_{\tau \neq \sigma}(V_\sigma - V_\tau)$ if $\varphi = \sigma$. Therefore, for $\varphi = e$,

$$\psi_j(V) = \alpha_j \prod_{\tau \neq e} (V - V_\tau).$$

Moreover $s'(y) = \sum_{\sigma \in S_n} \prod_{\tau \neq \sigma}(y - V_\tau)$, so

$$s'(V) = \prod_{\tau \neq e} (V - V_\tau).$$

Since the Galois resolvent $s(y)$ is separable, $s'(V) = \prod_{\tau \neq e}(V - V_\tau) \neq 0$, so

$$\alpha_j = \frac{\psi_j(V)}{s'(V)}.$$

We know that $s(y), s'(y)$ are in $F[y]$. It remains to prove that $\psi_j(y) \in F[y]$. We use $V(x_1, \ldots, x_n) = t_1 x_1 + \cdots + t_n x_n \in F[x_1, \ldots, x_n]$, so that

$$V_\sigma = V(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}),$$

and

$$\Psi_j(y, x_1, \ldots, x_n) = \sum_{\sigma \in S_n} x_{\sigma(j)} \prod_{\tau \neq \sigma} (y - V(x_{\tau(1)}, \ldots, x_{\tau(n)})),$$

so that $\psi_j(y) = \Psi_j(y, \alpha_1, \ldots, \alpha_n)$. Then, for all $\varphi \in S_n$,

$$\varphi \cdot \Psi_j = \sum_{\sigma \in S_n} x_{(\varphi\sigma)(j)} \prod_{\tau \neq \sigma} (y - V(x_{(\varphi\tau)(1)}, \ldots, x_{(\varphi\tau)(n)}))$$

$$= \sum_{\sigma \in S_n} x_{(\varphi\sigma)(j)} \prod_{\tau' \neq \varphi\sigma} (y - V(x_{\tau'(1)}, \ldots, x_{\tau'(n)})) \qquad (\tau' = \varphi\tau)$$

$$= \sum_{\sigma' \in S_n} x_{\sigma'(j)} \prod_{\tau' \neq \sigma'} (y - V(x_{\tau'(1)}, \ldots, x_{\tau'(n)})) \qquad (\sigma' = \varphi\sigma)$$

$$= \Psi_j$$

Therefore the coefficients of Ψ_j lie in the field $F(\sigma_1, \ldots, \sigma_n)$, and the evaluation $x_i \mapsto \alpha_i$ gives

$$\psi_j(y) \in F[y].$$

Therefore $\alpha_j = \frac{\psi_j(V)}{s'(V)} \in F(V)$, $j = 1, \ldots, n$, and $V \in F(\alpha_1, \ldots, \alpha_n)$, so

$$F(\alpha_1, \ldots, \alpha_n) = F(V).$$

$\square$

Ex. 12.2.4 *In the discussion preceding (12.25), we have extensions $F \subset L$, which is a splitting field of $f \in F[x]$, and $F \subset K = F(\beta)$, where β is a root of an irreducible polynomial in $F[x]$. Given the many ways in which extension fields can be constructed, these extensions might not have to do with each other. Prove that there is an extension $F \subset M$ that contains subfields $F \subset L_1 \subset M$ and $F \subset K_1 \subset M$ such that L_1, K_1 are isomorphic to L, K, respectively, where the isomorphisms are the identity on F. Thus, by replacing L, K with the isomorphic fields L_1, K_1, we can assume that L, K lie in a larger field, as claimed in the text.*

Proof. Let g be the minimal polynomial of β over F, and M a splitting field of fg over F. Write $\alpha_1, \ldots, \alpha_n$ the roots of f in M, and $\beta_1, \ldots, \beta_m$ the roots of g in M.

Then $L_1 = F(\alpha_1, \ldots, \alpha_n)$ is a splitting field of f over F. Since L, L_1 are splitting fields of f over F, there exists by Corollary 5.1.7 an isomorphism $\varphi : L \simeq L_1$ which is the identity on F.

Write $K_1 = F(\beta_1)$. Since g is irreducible over F, $K_1 \simeq F[x]/\langle g \rangle \simeq K$, where the isomorphisms are the identity on F. Here K_1, L_1 are subfields of M.

Thus, by replacing L, K with the isomorphic fields L_1, K_1, we can assume that L, K lie in a larger field M. $\square$

Ex. 12.2.5 *Suppose that $F \subset L$ is the splitting field of a separable polynomial $f \in F[x]$. Also suppose that we have another finite extension $F \subset K$ such that the compositum KL is defined. Prove that $K \subset KL$ is the splitting field of f over K.*

Proof. By hypothesis, K, L are subfields of a field M.

Write $\alpha_1, \ldots, \alpha_n$ the roots of f in L, so $L = F(\alpha_1, \ldots, \alpha_n)$. Since $F \subset K$ is a finite extension, there are $\beta_1, \ldots, \beta_m$ in K such that $K = F(\beta_1, \ldots, \beta_m)$. Then $F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m)$ is the smallest subfield of M containing K and L, so is the compositum KL:

$$KL = F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m).$$

Therefore

$$KL = F(\beta_1, \ldots, \beta_m)(\alpha_1, \ldots, \alpha_n) = K(\alpha_1, \ldots, \alpha_n).$$

Since $\alpha_1, \ldots, \alpha_n$ are the roots of f in K, a fortiori in KL, KL is the splitting field of the separable polynomial f over K, so $K \subset KL$ is a Galois extension. $\square$

Ex. 12.2.6 *This exercise will complete the proof of Theorem 12.2.5. Given $\sigma \in \mathrm{Gal}(KL/K)$, we showed in the text that $\sigma|_L$ maps L to L.*

(a) Show that $(\sigma\tau)|_L = \sigma|_L \, \tau|_L$.

(b) Use part (a) to show that $\sigma^{-1}|_L$ is the inverse function of $\sigma|L$.

(c) *Use part (a) to show that (12.26) is a group homomorphism.*

(d) *Let σ be an automorphism of KL that is the identity on both K and L. Prove that σ is the identity on KL.*

Proof. In the proof of Theorem 12.2.5, we cannot use Theorem 7.2.5, since we don't know if $F \subset KL$ is a Galois extension, so we prefer a direct argument.

(Consider the following counterexample: $F = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2})$ is a Galois extension of F, and $K = \mathbb{Q}(\sqrt[3]{2})$. Then $F \subset KL = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ is not a Galois extension.)

If $\sigma \in \mathrm{Gal}(KL/K)$, then σ fixes $F \subset K$. Let $\alpha \in L$, and let $f \in F[x]$ be the minimal polynomial of α over F. Then $0 = \sigma(f(\alpha)) = f(\sigma(\alpha))$, so $\sigma(\alpha)$ is a root of f. Since $F \subset L$ is a normal extension, $\sigma(\alpha) \in L$, thus $\sigma(L) \subset L$. Moreover, σ is F-linear, injective, and $[L : F] < \infty$, therefore

$$\sigma(L) = L.$$

Write $\sigma|_L$ the map $\sigma|_L : L \to L$ defined by $\alpha \mapsto \sigma(\alpha)$.

(a) $\sigma\tau \in \mathrm{Gal}(KL/K)$, so $(\sigma\tau)|_L : L \to L$, and also $\sigma|_L\tau|_L : L \to L$.

   If $\alpha \in L$, then

$$(\sigma|_L \circ \tau|_L)(\alpha) = \sigma|_L(\tau|_L(\alpha)) = \sigma(\tau(\alpha)) = (\sigma \circ \tau)(\alpha) = (\sigma \circ \tau)|_L(\alpha),$$

   so

$$(\sigma\tau)|_L = \sigma|_L\,\tau|_L.$$

(b) By part (a),
$$\sigma|_L\sigma^{-1}|_L = (\sigma\sigma^{-1})|_L = (\mathrm{id}_{KL})|L = \mathrm{id}_L,$$

   and similarly $\sigma^{-1}|_L\,\sigma|_L = \mathrm{id}_L$. Therefore

$$\sigma^{-1}|_L = (\sigma|_L)^{-1}.$$

(c) Let

$$\varphi \begin{cases} \mathrm{Gal}(KL/K) & \to & \mathrm{Gal}(L/F) \\ \sigma & \mapsto & \sigma|_L, \end{cases}$$

   where $\sigma|_L$ lies in $\mathrm{Gal}(L/F)$, since $\sigma|_L : L \to L$ is a field automorphism, and for every $\alpha \in F \subset K \subset KL$, $\sigma|_L(\alpha) = \sigma(\alpha) = \alpha$. By part (a), if $\sigma, \tau \in \mathrm{Gal}(KL/K)$,

$$\varphi(\sigma\tau) = (\sigma\tau)|_L = \sigma|_L\,\tau|_L = \varphi(\sigma)\varphi(\tau),$$

   so φ is a group homomorphism.

(d) Let σ be an automorphism of KL that is the identity on both K and L. Let $M = \{\alpha \in KL \mid \sigma(\alpha) = \alpha\}$. Then M is a field, the fixed field of σ in KL. By hypothesis, $K \subset M$ and $L \subset M$. By definition of the compositum KL, $KL \subset M$. Since $M \subset KL$ by definition, $KL = M$, so σ is the identity on KL.

   This prove that φ is injective.

$\square$

Ex. 12.2.7 *This exercise is concerned with the details of Example 12.2.6. As in the example, let L be the splitting field of $f = x^3 + 9x - 2$ over $\mathbb{Q}$ and set $K = \mathbb{Q}(\beta)$, where $\beta = \sqrt[3]{1 + 2\sqrt{7}}$.*

(a) Show that $\sqrt[3]{1 - 2\sqrt{7}} \in K$.

(b) Show that $K' = K(\omega), \omega = e^{2\pi i/3}$, contains all roots of f.

Proof. (a) Here the cubic roots are reals, so

$$\sqrt[3]{1 + 2\sqrt{7}}\sqrt[3]{1 - 2\sqrt{7}} = \sqrt[3]{(1 + 2\sqrt{7})(1 - 2\sqrt{7})} = \sqrt[3]{1 - 28} = \sqrt[3]{-27} = -3.$$

Therefore $\sqrt[3]{1 - 2\sqrt{7}} = -3/\beta \in K$.

(b) Consider the following formula in $\mathbb{Q}(x, u, v)$

$$(x - u - v)(x - \omega u - \omega^2 v)(x - \omega^2 u - \omega v) = x^3 - 3uvx - (u^3 + v^3).$$

If we use the evaluation $u \mapsto \beta = \sqrt[3]{1 + 2\sqrt{7}}, v \mapsto \gamma = \sqrt[3]{1 - 2\sqrt{7}}$, since

$$uv \mapsto -3, u^3 + v^3 \mapsto 2,$$

we obtain

$$x^3 + 9x - 2 = (x - (\beta + \gamma))(x - (\omega\beta + \omega^2\gamma))(x - (\omega^2\beta + \omega\gamma)),$$

so the root of f are

$$\alpha_1 = \beta + \gamma, \qquad \alpha_2 = \omega\beta + \omega^2\gamma, \qquad \alpha_3 = \omega^2\beta + \omega\gamma.$$

Since $\beta, \gamma \in K$, $\alpha_1, \alpha_2, \alpha_3$ lie in $K' = K(\omega)$:

$$K(\omega) \text{ contains all roots of } f.$$

$\square$

Ex. 12.2.8 *In Theorem 12.2.5, we have the map (12.26) defined by $\sigma \mapsto \sigma|_L$. However, if $F \subset L$ is the splitting field of a separable polynomial $f \in F[x]$ of degree n, then we also have maps (12.28) and (12.29). Prove that these maps are compatible, i.e., that $\sigma \in \mathrm{Gal}(KL/K)$ and $\sigma|_L \in \mathrm{Gal}(L/F)$ map to the same element of S_n under (12.28) and (12.29).*

Proof. Write $\chi : \mathrm{Gal}(KL/K) \to \mathrm{Gal}(L/F)$ the injective homomorphism (12.26) defined by $\sigma \mapsto \sigma|_L$.

Let $\alpha_1, \ldots, \alpha_n$ be a numbering of the roots of f, and $\varphi : \mathrm{Gal}(L/F) \to S_n$, the isomorphism defined for every $\tau \in \mathrm{Gal}(L/F)$ by

$$\tilde{\tau} = \varphi(\tau) \iff \tau(\alpha_i) = \alpha_{\tilde{\tau}(i)}, \quad i = 1, \ldots, n.$$

Similarly, since KL is the splitting field over K of the same polynomial f, the isomorphism $\psi : \mathrm{Gal}(KL/K) \to S_n$ is defined for every $\sigma \in \mathrm{Gal}(KL/K)$ by

$$\tilde{\sigma} = \psi(\sigma) \iff \sigma(\alpha_i) = \alpha_{\tilde{\sigma}(i)}, \quad i = 1, \ldots, n.$$

If $\tau = \sigma|_L$, and $\tilde{\tau} = \varphi(\tau), \tilde{\sigma} = \psi(\sigma)$, then for all i, $\tau(\alpha_i) = (\sigma|_L)(\alpha_i) = \sigma(\alpha_i)$, therefore

$$\alpha_{\tilde{\tau}(i)} = \tau(\alpha_i) = \sigma(\alpha_i) = \alpha_{\tilde{\sigma}(i)}, \qquad i = 1, \ldots, n$$
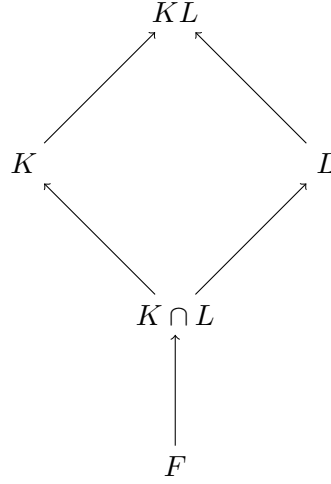
Since the roots $\alpha_1, \ldots, \alpha_n$ are distinct and $\alpha_{\tilde{\tau}(i)} = \alpha_{\tilde{\sigma}(i)}$ for every i, then $\tilde{\tau} = \tilde{\sigma}$, so

$$\psi(\tau) = \varphi(\tau|_L),$$

for every $\sigma \in \mathrm{Gal}(KL/K)$. Hence $\psi = \varphi \circ \chi$.

As a conclusion, $\tau \in \mathrm{Gal}(KL/K)$ and $\tau|_L \in \mathrm{Gal}(L/F)$ map to the same element of S_n under (12.28) and (12.29). $\qquad \square$

Ex. 12.2.9 *In the situation of Theorem 12.2.5, suppose that $F \subset K$ is an extension of prime degree p. Prove that $\mathrm{Gal}(KL/K)$ is isomorphic to either $\mathrm{Gal}(L/F)$ or a subgroup of index p in $\mathrm{Gal}(L/F)$.*

$$
\begin{array}{ccc}
 & KL & \\
\nearrow & & \nwarrow \\
K & & L \\
\nwarrow & & \nearrow \\
 & K \cap L & \\
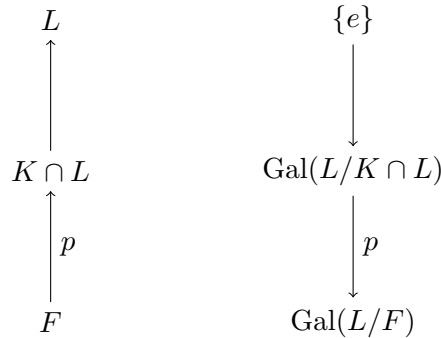 & \uparrow & \\
 & F &
\end{array}
$$

Proof. Since $p = [K : F] = [K : K \cap L] \cdot [K \cap L : F]$ is prime, the factor $[K \cap L : F]$ of p is 1 or p.

If $[K \cap L : F] = 1$, then $F = K \cap L$ and so $\mathrm{Gal}(KL/K) \simeq \mathrm{Gal}(L/F)$.

If $[K \cap L : F] = p$, then by the Galois correspondence (Theorem 7.3.1), $\mathrm{Gal}(L/K \cap L)$ corresponds to $K \cap L$, and

$$[K \cap L : F] = p = (\mathrm{Gal}(L/F) : \mathrm{Gal}(L/K \cap L)).$$

Therefore $\mathrm{Gal}(KL/K) \simeq \mathrm{Gal}(L/K \cap L)$ is isomorphic to a subgroup of index p in $\mathrm{Gal}(L/F)$.

$$
\begin{array}{ccc}
L & & \{e\} \\
\uparrow & & \downarrow \\
K \cap L & & \mathrm{Gal}(L/K \cap L) \\
\uparrow \, p & & \downarrow \, p \\
F & & \mathrm{Gal}(L/F)
\end{array}
$$

$\qquad \square$

Ex. 12.2.10 *Suppose that we have a diagram (12.25) as in Theorem 12.2.5. Also assume that $K = F(\beta)$, and let $K' = F(\beta')$, where β' and β have the same minimal polynomial over F. You will show that $\mathrm{Gal}(KL/K)$ and $\mathrm{Gal}(K'L/K')$ give conjugate subgroups of $\mathrm{Gal}(L/F)$. This is the modern version of what Galois says in 1° of Proposition II.*

(a) *Let $F \subset M'$ be the Galois closure of the extension $F \subset M$ constructed in Exercise 4. Explain why we can regard L, K, and K' as subfields of M'.*

(b) *Explain why we can find $\tau \in \mathrm{Gal}(M'/F)$ such that $\tau(K) = K'$.*

(c) *Show that $\tau|_L \in \mathrm{Gal}(L/F)$ maps $K \cap L$ to $K' \cap L$. Thus $K \cap L$ and $K' \cap L$ are conjugate subfields of L.*

(d) *Use Lemma 7.2.4 to show that in Theorem 12.2.5, $\mathrm{Gal}(KL/K)$ and $\mathrm{Gal}(K'L/K')$ map to conjugate subgroups of $\mathrm{Gal}(L/F)$.*

Proof. (a) Since $F \subset L$ is a Galois extension, there is a polynomial $f \in F[x]$ such that $L = F(\alpha_1, \ldots, \alpha_n)$, where $\alpha_1, \ldots, \alpha_n$ are the roots of f in L.

By Exercise 4, we can take $M = F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m)$ the splitting field of fg, where $\beta_1, \ldots, \beta_m$ the roots in M of the common minimal polynomial g of β, β'. If we replace the initial fields by the new fields, written K, L, and β, β' by β_1, β_2, then

$$F \subset K = F(\beta) \subset M, \qquad F \subset K' = F(\beta') \subset M \qquad F \subset L \subset M.$$

We must suppose g separable. Then $F \subset M$ is separable (Theorem 5.3.15 (a)), so there exists a Galois closure $F \subset M'$ of the extension $F \subset M$.

Since $M \subset M'$, L, K, and K' are subfields of M'.

(b) $F \subset M'$ is a Galois extension (therefore M' is a splitting field over F of some polynomial), and β, β' have the same minimal polynomial. By Proposition 5.1.8 there exists an F-automorphism τ of M' which sends β on β'. Since $\tau(\beta) = \beta'$, $\tau(K) = \tau(F(\beta)) = F(\tau(\beta)) = F(\beta') = K'$.

(c) Since $F \subset L$ is normal, $\tau(L) = L$, so $\tau|_L \in \mathrm{Gal}(L/F)$, and by part (b), $\tau(K) = K'$. Therefore $\tau(K \cap L) = K' \cap L$, so $\tau|_L$ sends $K \cap L$ on $K' \cap L$. Thus $K \cap L$ and $K' \cap L$ are conjugate subfields of L.

(d) Since $K' \cap L = \sigma(K \cap L)$, where $\sigma = \tau|_L \in \mathrm{Gal}(L/F)$, by Lemma 7.2.4,

$$\mathrm{Gal}(L/K' \cap L) = \mathrm{Gal}(L/\sigma(K \cap L)) = \sigma \mathrm{Gal}(L/K \cap L)\sigma^{-1}.$$

Since the isomorphisms of Theorem 7.2.4 send $\mathrm{Gal}(KL/K)$ on $\mathrm{Gal}(L/K \cap L)$ and $\mathrm{Gal}(K'L/K')$ on $\mathrm{Gal}(L/K' \cap L)$, $\mathrm{Gal}(KL/K)$ and $\mathrm{Gal}(K'L/K')$ map to conjugate subgroups of $\mathrm{Gal}(L/F)$.

$\square$

Ex. 12.2.11   *Let A denote the set of arrangements described by Galois. This is Galois's "group". For simplicity, we write the first arrangement on Galois's list as $\alpha_1 \ldots \alpha_n$. Then let G be the set of permutations that take the first element of A to the others . Theorem 12.2.3 implies that G is a subgroup of S_n isomorphic to $\mathrm{Gal}(L/F)$.*

We also have the action of S_n on the set of all n! arrangements of roots by

$$\sigma \cdot \alpha_{i_1} \cdots \alpha_{i_n} = \alpha_{\sigma(i_1)} \cdots \alpha_{\sigma(i_n)}.$$

This induces an action of G on the set of arrangements.

(a) Explain why A is the orbit of $\alpha_1 \cdots \alpha_n$ under the G action.

(b) Show that the map $G \to A$ defined by $\sigma \mapsto \sigma \cdot \alpha_1 \cdots \alpha_n$ is one-to-one and onto.

Proof.   (a) We use the notations of Theorem 12.2.3: $V = V^{(0)}, V' = V^{(1)}, \ldots, V^{(m-1)}$ are the roots of the polynomial h, irreducible over F. Moreover $\alpha_1, \ldots, \alpha_n$ are the roots of f, and $L = F(\alpha_1, \ldots, \alpha_n) = F(V)$.

Write
$$\mathrm{Gal}(L/F) = \{\sigma_0 = e, \sigma_1, \ldots, \sigma_{m-1}\},$$
where σ_i is the unique F-automorphism of L such that
$$\sigma_i(V) = V^{(i)}, \qquad 0 \leq i \leq n-1.$$

Let $\tau_i \in S_n$ the permutation associate to σ_i, defined by
$$\sigma_i(\alpha_j) = \alpha_{\tau_i(j)}, \qquad 0 \leq i \leq m-1, \qquad 1 \leq j \leq n.$$

Since $F(\alpha_1, \ldots, \alpha_n) = F(V)$, there are $\varphi_j \in F(x)$ such that
$$\alpha_j = \varphi_{j-1}(V), \qquad 1 \leq j \leq n.$$

Then
$$\begin{aligned}
\alpha_{\tau_i(j)} &= \sigma_i(\alpha_j) \\
&= \sigma_i(\varphi_{j-1}(V)) \\
&= \varphi_{j-1}(\sigma_i(V)) \\
&= \varphi_{j-1}(V^{(i)})
\end{aligned}$$

Thus
$$\alpha_{\tau_i(j)} = \varphi_{j-1}(V^{(i)}), \qquad 0 \leq i \leq m-1, \qquad 1 \leq j \leq n.$$

Therefore the orbit of the arrangement $a = (\alpha_1, \ldots, \alpha_n)$ under the action of $G = \{\tau_0, \ldots, \tau_{m-1}\}$, $G \subset S_n$, $G \simeq \mathrm{Gal}(L/F)$ is given by

$$\begin{aligned}
a = &\ (\alpha_1 = \varphi(V), & \alpha_2 = \varphi_1(V), & \quad \ldots, & \alpha_n = \varphi_{n-1}(V)) \\
\tau_1 \cdot a = &\ (\alpha_{\tau_1(1)} = \varphi(V'), & \alpha_{\tau_1(2)} = \varphi_1(V'), & \quad \ldots, & \alpha_{\tau_1(n)} = \varphi_{n-1}(V')) \\
&\ \cdots \\
\tau_{m-1} \cdot a = &\ (\alpha_{\tau_{m-1}(1)} = \varphi(V^{(m-1)}), & \alpha_{\tau_{m-1}(2)} = \varphi_1(V^{(m-1)}), & \quad \ldots, & \alpha_{\tau_{m-1}(n)} = \varphi_{n-1}(V^{(m-1)}))
\end{aligned}$$

The set of arrangements A described by Galois is the orbit of the arrangement $(\alpha_1, \ldots, \alpha_n)$ under the G-action, where G is the subgroup G of S_n isomorphic to $\mathrm{Gal}(L/F)$.

(b) Let $\psi : G \to A = \mathcal{O}_a$ defined by $\sigma \mapsto \sigma \cdot a$.

- If $\tau_k \cdot a = \tau_l \cdot a$, where $a = (\alpha_1, \ldots, \alpha_n)$ and $\tau_k, \tau_l \in G$, then

$$\alpha_{\tau_k(j)} = \alpha_{\tau_l(j)}, \qquad 1 \le j \le n.$$

If $\sigma_k, \sigma_l \in \mathrm{Gal}(L/F)$ are the automorphisms associate to $\tau_k, \tau_l \in S_n$, then

$$\sigma_k(\alpha_j) = \sigma_l(\alpha_j), \qquad 1 \le j \le n.$$

Since $L = F(\alpha_1, \ldots, \alpha_n)$, this implies that $\sigma_k = \sigma_l$, thus $\tau_k = \tau_l$, and ψ is injective.

- Moreover $|G| = |A| = m$, therefore the injective map ψ is also surjective.

$\psi : G \to A$ is a bijection.

$\square$

Ex. 12.2.12 *In the situation of Theorem 12.2.5, let $G \subset S_n$ correspond to $\mathrm{Gal}(L/F)$, and $H \subset S_n$ correspond to $\mathrm{Gal}(KL/K)$. By Exercise 8, we know that $H \subset G$. Also let A be the set of arrangements studied in Exercise 11. Then a left coset $\sigma H \subset G$ gives a subset $\sigma H \cdot \alpha_1 \cdots \alpha_n \subset A$, and since the map $\sigma \cdot \alpha_1 \cdots \alpha_n$ is one-to-one and onto, the sets $\sigma H \cdot \alpha_1 \cdots \alpha_n$ partition A into disjoint subsets. We claim that these are the "groups" that appear in $1°$ and $2°$ of Galois Proposition II.*

(a) *Given any two such "groups" $\sigma H \cdot \alpha_1 \cdots \alpha_n$ and $\tau H \cdot \alpha_1 \cdots \alpha_n$, prove that there is $\gamma \in G$ such that (as Galois says in $2°$) one passes from one to the other by applying γ to all arrangements in the first.*

(b) *So far, it seems like Galois describing cosets. However, as pointed out in [12], Galois thought of these "groups" differently. This is seen by explaining how they relate to $1°$ of Galois' proposition. Let M' be the field used in Exercise 10, and let $\tau \in \mathrm{Gal}(M'/F)$. Then $K' = \tau(K)$ is a conjugate of K. Let $\sigma \in G$ be the permutation corresponding to $\tau|_L \in \mathrm{Gal}(L/F)$. Show that $\sigma H \sigma^{-1}$ is a subgroup of S_n corresponding to $\mathrm{Gal}(K'L/K')$.*

(c) *Using the setup of part (b), consider the "group" $\sigma H \cdot \alpha_1 \cdots \alpha_n \subset A$. Prove that $\sigma H \sigma^{-1} \subset S_n$ is the set of all permutations of S_n that map the first element of this "group", namely $\sigma \cdot \alpha_1 \cdots \alpha_n$, to another element of the "group". (Remember that this is the process for turning a "group" of arrangements into a subgroup of S_n.)*

Combining parts (b) and (c), we see that what Galois says in $1°$ of Proposition II is fully consistent with what we did in Exercise 10.

Proof. (a) Let $\gamma = \tau \sigma^{-1}$. Since G is a subgroup of S_n, $\gamma \in G$, and, for all $h \in H$,

$$\gamma \cdot (\sigma h \cdot \alpha_1 \cdots \alpha_n) = \gamma \sigma h \cdot \alpha_1 \cdots \alpha_n$$
$$= \tau h \cdot \alpha_1 \cdots \alpha_n,$$

so

$$\gamma \cdot (\sigma H \cdot \alpha_1 \cdots \alpha_n) = \tau H \cdot \alpha_1 \cdots \alpha_n.$$

There exists $\gamma \in G$ such that one passes from one to the other by applying γ to all arrangements in the first.

(b) By Exercise 10(d), we know that

$$\mathrm{Gal}(L/K' \cap L) = (\tau|_L)\mathrm{Gal}(L/K \cap L)(\tau|_L)^{-1}.$$

The map $\mathrm{Gal}(L/F) \to S_n$ given by the action of the Galois group on the roots is a morphism. As σ is the image of $\tau|_L$ by this morphism, we obtain

$$H' = \sigma H \sigma^{-1},$$

where H is the subgroup of S_n corresponding to $\mathrm{Gal}(L/K \cap L)$, and H' to $\mathrm{Gal}(L/K' \cap L)$.

These two subgroups of S_n are the images of $\mathrm{Gal}(KL/K)$ and $\mathrm{Gal}(K'L/K')$ under the injective homomorphism (12.29), which is compatible with (12.28) and (12.29) by Exercise 8, i.e. τ and $\tau|_L$ map to the same element of S_n.

Conclusion: if $H \subset S_n$ is corresponding to $\mathrm{Gal}(KL/K)$, then $\sigma H \sigma^{-1}$ is a subgroup of S_n corresponding to $\mathrm{Gal}(K'L/K')$ (where $K' = \tau K$, and $\sigma \in G$ is the permutation corresponding to $\tau|L \in \mathrm{Gal}(L/F)$).

(c) Let $\gamma \in S_n$. Then γ maps $\sigma \cdot \alpha_1 \cdots \alpha_n$ on $\sigma H \cdot \alpha_1 \cdots \alpha_n$ if and only if, there exists $h \in H$ such that

$$\gamma \cdot (\sigma \cdot \alpha_1 \cdots \alpha_n) = (\sigma h) \cdot \alpha_1 \cdots \alpha_n.$$

This is equivalent to $(\gamma\sigma) \cdot \alpha_1 \cdots \alpha_n = (\sigma h) \cdot \alpha_1 \cdots \alpha_n,\ h \in H$.

Since $\sigma \mapsto \sigma \cdot \alpha_1 \cdots \alpha_n$ is bijective (Exercise 11(b)), this is equivalent to

$$\gamma\sigma = \sigma h,\ h \in H,$$

or equivalent to $\gamma \in \sigma H \sigma^{-1}$.

$$\gamma \cdot (\sigma \cdot \alpha_1 \cdots \alpha_n) \in \sigma H \cdot \alpha_1 \cdots \alpha_n \iff \gamma \in \sigma H \sigma^{-1}.$$

$\square$

Ex. 12.2.13 *This exercise will show that not all choices of the t_i in (12.21) give Galois resolvents. As in Example 12.2.1, $f = (x^2-2)(x^2-3)$ has roots $\sqrt{2}, -\sqrt{2}, \sqrt{3},$ and $-\sqrt{3}$. This time we will use $(t_1, t_2, t_3, t_4) = (0, 1, 2, 3)$. Show that (12.21) gives the polynomial*

$$s(y) = 16$$

This does not have distinct roots, so that $s(y)$ is not a Galois resolvent.

Note. The results in Example 12.2.1 are false for $(t_1, t_2, t_3, t_4) = (0, 1, 2, 4)$. The first given factor of $s(y)$ is $900 - 132y^2 + y^4$, which has root $\sqrt{66 + 24\sqrt{6}} = 3\sqrt{2} + 4\sqrt{3}$ and this root can't be written $t_{\sigma(1)}\sqrt{2} + t_{\sigma(2)}(-\sqrt{2}) + t_{\sigma(3)}\sqrt{3} + t_{\sigma(4)}(-\sqrt{3})$ for any permutation $\sigma \in S_4$. Idem for the second factor $25 - 118y^2 + y^4$.

The following Sage instructions gives the right answer :

```
t1,t2,t3,t4 = 0,1,2,4
var('x1,x2,x3,x4')
V = t1*x1 + t2*x2 + t3*x3 + t4*x4
from itertools import permutations
R.<y> = ZZ[]
t = 1
for perm in permutations([x1,x2,x3,x4]):
```

```
    t = t * (y - V.subs(x1 = perm[0], x2 = perm[1], x3 = perm[2], x4 = perm[3]))
s0= t.subs(x1 = sqrt(2),x2 = -sqrt(2), x3 = sqrt(3),x4 = -sqrt(3))
s = R(s0.expand())
s
```

$$s(y) = y^{24} - 350y^{22} + 52395y^{20} - 4390200y^{18} + 226512195y^{16} - 7470312150y^{14}$$
$$+ 158533048725y^{12} - 2128033120500y^{10} + 17319964832940y^{8} - 79514980673600y^{6}$$
$$+ 185487963684016y^{4} - 182187606350400y^{2} + 57817774440000$$

and

```
s.factor()
```

gives the Galois resolvent $s(y)$:

$$(y^4 - 100y^2 + 2116) \cdot (y^4 - 70y^2 + 361) \cdot (y^4 - 70y^2 + 841) \cdot (y^4 - 60y^2 + 36) \cdot (y^4 - 28y^2 + 100) \cdot (y^4 - 22y^2 + 25)$$

The minimal polynomial of $V = -\sqrt{2} - 2\sqrt{3}$ is the factor $h = y^4 - 28y^2 + 100$.

Proof. The same instructions with $t_1, t_2, t_3, t_4 = 0, 1, 2, 3$ give

$$s(y) = y^{24} - 200y^{22} + 16620y^{20} - 743400y^{18} + 19430070y^{16} - 302989800y^{14}$$
$$+ 2777491500y^{12} - 14100111000y^{10} + 34064189265y^{8} - 25798725200y^{6}$$
$$+ 7753861216y^{4} - 910060800y^{2} + 36000000$$
$$= (y^4 - 58y^2 + 625) \cdot (y^4 - 42y^2 + 225) \cdot (y^4 - 40y^2 + 16)^2 \cdot (y^4 - 10y^2 + 1)^2$$

This does not have distinct roots, so that $s(y)$ is not a Galois resolvent.
  (But the result is not the same as in the statement.) $\square$

Ex. 12.2.14 *Use Theorem 12.2.5 and standard results about Galois extensions to prove that $|\mathrm{Gal}(KL/K)| = [L : K \cap L]$. Then explain that $|\mathrm{Gal}(KL/K)| < |\mathrm{Gal}(L/F)|$ if and only if F is a proper subfield of $K \cap L$.*

Proof. By Theorem 12.2.5,

$$\mathrm{Gal}(KL/K) \simeq \mathrm{Gal}(L/K \cap L).$$

Moreover, $F \subset L$ is a Galois extension, where $F \subset K \cap L$, thus $K \cap L \subset L$ is also a Galois extension. Therefore $|\mathrm{Gal}(L/K \cap L)| = [L : K \cap L]$. We obtain the conclusion

$$|\mathrm{Gal}(KL/K)| = [L : K \cap L].$$

Since $F \subset K \cap L \subset L$,

$$|\mathrm{Gal}(KL/K)| < |\mathrm{Gal}(L/F)| \iff [L : K \cap L] < [L : F]$$
$$\iff K \cap L \neq F$$

So $|\mathrm{Gal}(KL/K)| < |\mathrm{Gal}(L/F)|$ if and only if F is a proper subfield of $K \cap L$. $\square$

Ex. 12.2.15 *Let $F \subset L$ and $F \subset K$ be Galois extensions such that KL is defined. We will also assume that $K \cap L = F$. The goal of this exercise is to prove that $F \subset KL$ is a Galois extension with Galois group*

$$\mathrm{Gal}(KL/F) \simeq \mathrm{Gal}(L/F) \times \mathrm{Gal}(K/F).$$

(a) *Prove that $F \subset KL$ is Galois and that $\sigma \in \mathrm{Gal}(KL/F)$ implies that $\sigma|_L \in \mathrm{Gal}(L/F)$ and $\sigma|_K \in \mathrm{Gal}(L/K)$.*

(b) *Use part (d) of Exercise 6 to show that there is a one-to-one group homomorphism*

$$\mathrm{Gal}(KL/F) \to \mathrm{Gal}(L/F) \times \mathrm{Gal}(K/F).$$

(c) *Use Exercise 14 and the Tower Theorem to show that $[KL : F] = [K : F][L : F]$.*

(d) *Conclude that the map of part (b) is an isomorphism.*

Proof. (a) The Exercise 8.2.7 proves that $F \subset KL$ is Galois. Let $\sigma \in \mathrm{Gal}(KL/F)$. By Theorem 7.2.5, since $F \subset L$ is normal, $\sigma L = L$, and σ fixes the elements of F, so $\sigma|_L \in \mathrm{Gal}(L/F)$. Similarly $\sigma|_K \in \mathrm{Gal}(K/F)$ (there is a misprint in the statement).

(b) Let

$$\varphi : \begin{cases} \mathrm{Gal}(KL/F) & \to & \mathrm{Gal}(L/F) \times \mathrm{Gal}(K/F) \\ \sigma & \mapsto & (\sigma|_L, \sigma|_K) \end{cases}$$

Then φ is a group homomorphism. Moreover, if $(\sigma|_L, \sigma|_K) = (\mathrm{id}_L, \mathrm{id}_K)$, then σ is the identity on both K and L. By Exercise 6(d), σ is the identity on KL, so φ is injective.

(c) By the Tower Theorem

$$[KL : F] = [KL : K][K : F].$$

Moreover, Theorem 12.2.5 shows that $\mathrm{Gal}(KL : K) \simeq \mathrm{Gal}(L/K \cap L) = \mathrm{Gal}(L/F)$, thus $[KL : K] = [L : F]$. The conclusion is

$$[KL : F] = [K : F][L : F].$$

(d) So the finite sets $\mathrm{Gal}(KL/F), \mathrm{Gal}(L/F) \times \mathrm{Gal}(K/F)$ have same cardinality, and φ is injective, therefore φ is bijective , so φ is a group isomorphism.

$\square$

12.3 KRONECKER

Ex. 12.3.1 *Prove that $y^2 - 4x^3 - x$ is irreducible when considered as an element of $\mathbb{Q}(x)[y]$.*

Proof. Since the degree in y of $f(y) = y^2 - 4x^3 - x$ is 2, it is sufficient to prove that f has no root in $\mathbb{Q}[x]$, or in other words that $\sqrt{4x^3 + x}$ is not a polynomial.

This is equivalent to the impossibility of the equality $4x^3 + x = p(x)^2$, where $p(x) \in \mathbb{Q}[x]$.

If we assume that $4x^3 + x = p^2$, $p \in \mathbb{Q}[x]$, then the irreducible polynomial x divides p^2, therefore it divides p, thus x^2 divides p^2, so $x^2 \mid 4x^3 + x$, $x \mid 4x^2 + 1$, $x \mid 1$, which is false.

Conclusion: the polynomial $y^2 - 4x^3 - x$ is irreducible when considered as an element of $\mathbb{Q}(x)[y]$.

$\square$

Ex. 12.3.2 *Show that (12.31) follows from the Theorem of the Primitive Element and the theorem of Steinitz mentioned in the Mathematical Notes to Section 4.1.*

Proof. The extensions $\mathbb{Q} \subset L$ considered by Kronecker are extensions generated by finitely many elements $\alpha_1, \cdots, \alpha_n$, so $L = \mathbb{Q}(\alpha_1, \cdots \alpha_n)$.

The result of Steinitz mentioned in the Mathematical Notes to Sections 4.1 says that L can be written in the form

$$\mathbb{Q} \subset K = \mathbb{Q}(\beta_1, \ldots, \beta_m) \subset K(\gamma_1, \ldots, \gamma_l) = L,$$

where $m \leq n$, $\beta_1, \ldots, \beta_m$ are algebraically independent over $\mathbb{Q}$, and $\gamma_1, \ldots, \gamma_l$ are algebraic over $\mathbb{Q}$.

The Theorem of the Primitive Element, applied to the field K with characteristic 0, gives a primitive element $\gamma \in L$ such that $L = K(\gamma)$. Therefore, $L = \mathbb{Q}(\beta_1, \ldots, \beta_m, \gamma)$, where $\beta_1, \ldots, \beta_m$ are variables, and γ is algebraic over $\mathbb{Q}(\beta_1, \ldots, \beta_m)$.

With the notations used by Kronecker, we obtain (12.31). $\qquad\square$

Ex. 12.3.3 *Let R be a commutative ring and let $M_1, \ldots, M_s$ be elements of R. Prove that the set $\langle M_1, \ldots, M_s \rangle = \{\sum_{i=1}^{s} A_i M_i \mid A_i \in R\}$ is an ideal of R.*

Proof. Write $I = \langle M_1, \ldots, M_s \rangle$. I is a subgroup of R, since $0 \in I$, and if $M, N \in I$, then $M = \sum_{i=1}^{s} A_i M_i, A_i \in R, N = \sum_{i=1}^{s} B_i M_i, B_i \in R$, so $M - N = \sum_{i=1}^{s} C_i M_i$, where $C_i = A_i - B_i \in R$, so $M - N \in I$.

Moreover, if $M \in I$ and $A \in R$, then $M = \sum_{i=1}^{s} A_i M_i, A_i \in R$, therefore $AM = \sum_{i=1}^{s} D_i M_i$, where $D_i = AA_i \in R$.

$I = \langle M_1, \ldots, M_s \rangle$ is an ideal of R. $\qquad\square$

Ex. 12.3.4 *In the discussion leading up to Theorem 12.3.3, we have the polynomial $S(y) \in F[\sigma_1, \ldots, \sigma_n, y]$ defined in (12.36). Then $s(y) \in F[y]$ is obtained by $\sigma_i \mapsto c_i$, where c_i is as in (12.34). Both of these polynomials depend on $t_1, \ldots, t_n$. The goal of this exercise is to show that if f is separable, then $\Delta(s)$ is a nonzero polynomial when $t_1, \ldots, t_n$ are regarded as variables. Since F has characteristic 0, part (a) of Exercise 5 implies that $\Delta(s) \neq 0$ for some $t_1, \ldots, t_n \in \mathbb{Z}$.*

To prove that $\Delta(s)$ is a nonzero polynomial in $t_1, \ldots, t_n$, let $F \subset L$ be the splitting field of f constructed in Theorem 3.1.4. Thus $f = (x - \alpha_1) \cdots (x - \alpha_n)$ in $L[x]$.

(a) *If we regard the t_i as variables, explain why $S(y)$ becomes a polynomial in y with coefficients in $F[\sigma_1, \ldots, \sigma_n, t_1, \ldots, t_n]$. Conclude that $s(y) \in F[t_1, \ldots, t_n, y]$ and hence that $\Delta(s) \in F[t_1, \ldots, t_n]$.*

(b) *Explain why $s(y) = \prod_{\sigma \in S_n} \left(y - (t_1 \alpha_{\sigma(1)} + \cdots + t_n \alpha_{\sigma(n)}) \right)$ in $L[t_1, \ldots, t_n, y]$.*

(c) *Use part (b) and the separability of f to show that $s(y)$ has distinct roots, all of which lie in $L[t_1, \ldots, t_n]$. Conclude that $\Delta(s)$ is a nonzero element of $F[t_1, \ldots, t_n]$.*

Proof. (a) Write $\beta = t_1 x_1 + \cdots + t_n x_n \in F[t_1, \ldots, t_n, x_1, \ldots, x_n]$, where $t_1, \ldots, t_n, x_1, \ldots, x_n$ are variables, and

$$S(y) = \prod_{\sigma \in S_n} \left(y - (t_1 x_{\sigma(1)} + \cdots + t_n x_{\sigma(n)}) \right) = \prod_{\sigma \in S_n} (y - \sigma \cdot \beta).$$

Then, for all $\tau \in S_n$,

$$\tau \cdot S(y) = \tau \cdot \prod_{\sigma \in S_n} (y - \sigma \cdot \beta)$$

$$= \prod_{\sigma \in S_n} (y - \tau \cdot (\sigma \cdot \beta))$$

$$= \prod_{\sigma \in S_n} (y - (\tau \circ \sigma) \cdot \beta))$$

$$= \prod_{\sigma' \in S_n} (y - \sigma' \cdot \beta) \qquad (\sigma' = \tau \circ \sigma)$$

$$= S(y).$$

By Theorem 2.2.7, $S(y)$ is a polynomial in y with coefficients in $F[\sigma_1, \ldots, \sigma_n, t_1, \ldots, t_n]$, so

$$S(y) \in F[\sigma_1, \ldots, \sigma_n, t_1, \ldots, t_n, y].$$

The evaluation $\sigma_i \mapsto c_i$, $c_i \in F$ gives

$$s(y) \in F[t_1, \ldots, t_n, y].$$

Since the coefficients a_i of $s(y) = \sum_{i=0}^{n!} a_i y^i$ are in the ring $F[t_1, \ldots, t_n]$, by (2.30),

$$\Delta(s) = \Delta(-a_1, \ldots, (-1)^i a_i, \ldots, a_{n!}) \in F[t_1, \ldots, t_n].$$

(b) By part (a), $s(y) \in F[t_1, \ldots, t_n, y]$, and $F \subset L$, so $s(y) \in L[t_1, \ldots, t_n, y]$. Moreover, since $\alpha_i \in L$, each factor of s satisfies

$$y - (t_1 \alpha_{\sigma(1)} + \cdots + t_n \alpha_{\sigma(n)}) \in L[t_1, \ldots, t_n, y].$$

(c) Since f is separable, the n roots $\alpha_1, \ldots, \alpha_n$ of f are distinct. Therefore, for all $\sigma, \tau \in S_n$ such that $\sigma \neq \tau$, there exists some $i, 1 \leq i \leq n$ such that $\sigma(i) \neq \tau(i)$, so $\alpha_{\sigma(i)} \neq \alpha_{\tau(i)}$. Hence

$$\sigma \neq \tau \Rightarrow t_1 \alpha_{\sigma(1)} + \cdots + t_n \alpha_{\sigma(n)} \neq t_1 \alpha_{\tau(1)} + \cdots + t_n \alpha_{\tau(n)}.$$

So $s(y)$ has $n!$ distinct roots. By Proposition 2.4.3, $\Delta(s)$ is a nonzero element of $F[t_1, \ldots, t_n]$.

$\square$

Ex. 12.3.5 *Let F be a field, and let $g \in F[t_1, \ldots, t_n]$ be nonzero.*

(a) *Suppose that F has characteristic 0, so that $\mathbb{Q} \subset F$. For each i, pick a nonnegative integer N_i such that the highest power of t_i appearing in g is at most N_i, and let*

$$A = \{(a_1, \ldots, a_n) \mid a_i \in \mathbb{Z}, 0 \leq a_i \leq N_i\}.$$

Prove that there is $(a_1, \ldots, a_n) \in A$ such that $g(a_1, \ldots, a_n) \neq 0$.

(b) *Now suppose that F has characteristic p and is infinite. Modify the argument of part (a) to show that there are $a_1, \ldots, a_n \in F$ such that $g(a_1, \ldots, a_n) \neq 0$.*

(c) *Give an example to illustrate why the hypothesis "F is infinite" is needed in part (b).*

Proof. Suppose that $n = 1$, and $g \in F[t_1], g \neq 0$. Then g has at most $\deg(g) \leq N_1$ roots. The cardinality of $\{0, 1, \ldots, N_1\}$ is $N_1 + 1$, therefore some integer $a_1 \in \{0, 1, \ldots, N_1\}$ is not a root of g. The property is so established if $n = 1$.

Reasoning by induction, suppose that the property is true for $n-1$ variables $t_1, \cdots, t_{n-1}$, and let $g \in F[t_1, \ldots, t_n]$ a nonzero polynomial. Write

$$g = c_d(t_1, \ldots, t_{n-1})t_n^d + \cdots + c_0(t_1, \cdots, t_{n-1}),$$

where d is the partial degree of g relative to the variable t_n.

If $d = 0$, then $g = c_0 \neq 0$, and the induction hypothesis gives $(a_1, \ldots, a_{n-1})$, with $0 \leq a_i \leq N_i$ for each i, $0 \leq i \leq n-1$, such that $c_0(a_1, \ldots, a_{n-1}) \neq 0$. If we take $a_n = 0$, then $(a_1, \ldots, a_n) \in A$ is such that $g(a_1, \ldots, a_n) \neq 0$.

If $d > 0$, the induction hypothesis gives $(a_1, \ldots, a_{n-1})$, with $0 \leq a_i \leq N_i$ for each i, $0 \leq i \leq n-1$, such that $c_d(a_1, \ldots, a_{n-1}) \neq 0$. Then $h(t_n) = g(a_1, \ldots, a_{n-1}, t_n)$ is a polynomial in t_n with degree $d \leq N_n$, so with the same argumentation as in the case $n = 1$, there exists some a_n, $0 \leq a_n \leq N_n$ such that $h(a_n) \neq 0$. Therefore $(a_1, \ldots a_n) \in A$ and $g(a_1, \ldots, a_n) \neq 0$. The induction is done.

(b) Now suppose that F has characteristic p and is infinite. A nonzero polynomial p in $F[x]$ has at most $\deg(p)$ roots. The same induction gives an element a_n in the infinite field which is not a root of the polynomial, so the property is true in any infinite field.

(c) If $F = \mathbb{F}_p$, and $g = t_1^p - t_1$, then $g \neq 0$ but all elements a_1 in $\mathbb{F}_p$ satisfy $g(a_1) = 0$ (Fermat's little Theorem).

Another such counterexample with $n = 2$ is the nonzero polynomial $g = t_1^p t_2 - t_1 t_2^p$ in $\mathbb{F}_p[t_1, t_2]$, such that $g(a_1, a_2) = 0$ for all $a_1, a_2 \in \mathbb{F}_p$. $\qquad \square$

Ex. 12.3.6 *In $F[x_1, \ldots, x_n]$, consider the polynomial*

$$\tilde{f} = (x - x_1) \cdots (x - x_n) = x^n - \sigma_1 x^{n-1} + \cdots + (-1)^n \sigma_n.$$

As noted in Section 2.2, we can regard $\tilde{f} \in F[\sigma_1, \ldots, \sigma_n]$ as the universal polynomial of degree n. The goal of this exercise is to show that if $\tilde{f}'$ denotes the derivative of $\tilde{f}$, then there are polynomials $\tilde{A}, \tilde{B} \in F[\sigma_1, \ldots, \sigma_n, x]$ such that $\deg(\tilde{A}) \leq n - 2, \deg(\tilde{B}) \leq n - 1$, and

$$\tilde{A}\tilde{f} + \tilde{B}\tilde{f}' = \Delta.$$

Here Δ is the discriminant defined in Section 2.4. The proof given here is taken from Gauss's 1815 proof of the Fundamental Theorem of Algebra (see [14, pp. 293-295]).

(a) Show that

$$\tilde{B} = \frac{\Delta(x - x_2) \cdots (x - x_n)}{(x_1 - x_2)^2 \cdots (x_1 - x_n)^2} + \frac{\Delta(x - x_1)(x - x_3) \cdots (x - x_n)}{(x_2 - x_1)^2 (x_2 - x_3)^2 \cdots (x_2 - x_n)^2}$$
$$+ \frac{\Delta(x - x_1) \cdots (x - x_{n-1})}{(x_n - x_1)^2 \cdots (x_n - x_{n-1})^2}$$

is a polynomial in x of degree at most $n - 1$ whose coefficients are symmetric polynomials in $x_1, \ldots, x_n$. Conclude that $\tilde{B} \in F[\sigma_1, \ldots, \sigma_n, x]$.

(b) Prove that $\Delta - \tilde{B}\tilde{f}'$ vanishes when $x = x_i$.

(c) Conclude that $\Delta - \tilde{B}\tilde{f}'$ is divisible by $\tilde{f}$, and set

$$\tilde{A} = \frac{\Delta - \tilde{B}\tilde{f}'}{\tilde{f}}.$$

Show that $\tilde{A}$ and $\tilde{B}$ have the desired properties.

Proof. (a) Each term of $\tilde{B}$ has degree $n-1$ in x, so $\deg(\tilde{B}) \leq n-1$.

Let $\tau = (1\,2)$. Then τ exchanges the two first terms of $\tilde{B}$,

$$\tau \cdot \left(\frac{\Delta(x-x_2)(x-x_3)\cdots(x-x_n)}{(x_1-x_2)^2(x_1-x_3)^2\cdots(x_1-x_n)^2} \right) = \frac{\Delta(x-x_1)(x-x_3)\cdots(x-x_n)}{(x_2-x_1)^2(x_2-x_3)^2\cdots(x_2-x_n)^2},$$

and fixes the other terms. Therefore $\tau \cdot \tilde{B} = \tilde{B}$.

Let $\sigma = (1\,2\,\cdots\,n)$. Then

$$\sigma \cdot \left(\frac{\Delta(x-x_2)(x-x_3)\cdots(x-x_n)}{(x_1-x_2)^2(x_1-x_3)^2\cdots(x_1-x_n)^2} \right) = \frac{\Delta(x-x_3)(x-x_4)\cdots(x-x_1)}{(x_2-x_3)^2(x_2-x_4)^2\cdots(x_2-x_1)^2}$$

$$= \frac{\Delta(x-x_1)(x-x_3)\cdots(x-x_n)}{(x_2-x_1)^2(x_2-x_3)^2\cdots(x_2-x_n)^2},$$

so σ maps the first term on the second, and similarly the second on the third,..., and the last on the first. Therefore $\sigma \cdot \tilde{B} = \tilde{B}$. Since σ, τ are generators of the group S_n, every permutation of S_n fixes $\tilde{B}$. So the coefficients of $\tilde{B}$ are symmetric polynomials in $x_1, \cdots, x_n$. By Theorem 2.2.2,

$$\tilde{B} \in F[\sigma_1, \ldots, \sigma_n, x].$$

(b) For each index i, $1 \leq i \leq n$

$$\tilde{B}(x_i) = \frac{\Delta(x_i-x_1)\cdots(x_i-x_{i-1})(x_i-x_{i+1})\cdots(x_i-x_n)}{(x_i-x_1)^2\cdots(x_i-x_{i-1})^2(x_i-x_{i+1})^2\cdots(x_i-x_n)^2}$$

$$= \frac{\Delta}{(x_i-x_1)\cdots(x_i-x_{i-1})(x_i-x_{i+1})\cdots(x_i-x_n)}$$

$$= \frac{\Delta}{\tilde{f}'(x_i)}$$

So $\Delta - \tilde{B}(x_i)\tilde{f}'(x_i) = 0$: $\Delta - \tilde{B}\tilde{f}'$ vanishes when $x = x_i$.

(c) By part (b), $x - x_i$ divides $\Delta - \tilde{B}\tilde{f}'$ for each i, $1 \leq i \leq n$. Since the polynomials $x - x_i$, $1 \leq i \leq n$, are relatively prime, their product $\tilde{f}$ divides $\Delta - \tilde{B}\tilde{f}'$ in $F[x_1, \ldots, x_n, x]$:

$$\tilde{f} \mid \Delta - \tilde{B}\tilde{f}'.$$

Set

$$\tilde{A} = \frac{\Delta - \tilde{B}\tilde{f}'}{\tilde{f}} \in F[x_1, \ldots, x_n, x].$$

Then $\tilde{A}\tilde{f} + \tilde{B}\tilde{f}' = \Delta$.

Moreover, $\tilde{f} \in F[\sigma_1, \ldots, \sigma_n, x]$, therefore $\tilde{f}' \in F[\sigma_1, \ldots, \sigma_n, x]$. Since every $\sigma \in S_n$ fixes $\Delta, \tilde{f}, \tilde{f}'$, σ fixes $\tilde{A}$, so

$$\tilde{A} \in F[\sigma_1, \ldots, \sigma_n, x].$$

By part (a), $\deg(\tilde{B}) \le n - 1$.

Since $\deg(\Delta) = 0$, $\deg(\tilde{A}\tilde{f}) = \deg(\Delta - \tilde{B}\tilde{f}') \le \deg(\tilde{B}\tilde{f}') = \deg(\tilde{B}) + \deg(\tilde{f}') \le (n-1) + (n-1)$. Therefore $\deg(\tilde{A}) + n \le 2n - 2$, so $\deg(\tilde{A}) \le n - 2$.

$\tilde{A}, \tilde{B}$ have the desired properties:

There exist $\tilde{A}, \tilde{B} \in F[\sigma_1, \ldots, \sigma_n, x]$ such that

$$\tilde{A}\tilde{f} + \tilde{B}\tilde{f}' = \Delta, \ \deg(\tilde{A}) \le n - 2, \deg(\tilde{B}) \le n - 1.$$

$\square$

Ex. 12.3.7 *Let $f \in F[x]$ be monic of degree $n > 0$ with discriminant $\Delta(f) \in F$. Use Exercise 6 to show that thre are $A, B \in F[x]$ with $\deg(A) \le n - 2, \deg(B) \le n - 1$, such that the coefficients of A and B are polynomials in the coefficients of f and $Af + Bf' = \Delta(f)$.*

Proof. Set $f = x^n - c_1 x^{n-1} + \cdots + (-1)^n c_0$ any monic polynomial of degree n.

By Exercise 6, there exist $\tilde{A}, \tilde{B} \in F[\sigma_1, \ldots, \sigma_n, x]$ such that

$$\tilde{A}\tilde{f} + \tilde{B}\tilde{f}' = \Delta, \ \deg(\tilde{A}) \le n - 2, \deg(\tilde{B}) \le n - 1.$$

The evaluation $\sigma_i \to c_i$ maps Δ to $\Delta(f)$, $\tilde{f}$ to f, $\tilde{f}'$ on f'. Write $A(x) = \tilde{A}(c_1, \cdots, c_n, x), B(x) = \tilde{B}(c_1, \ldots, c_n, x)$, so the evaluation maps $\tilde{A}, \tilde{B}$ to A, B, and $\deg(A) \le \deg(\tilde{A}), \deg(B) \le \tilde{B}$. Since $\Delta(f) = \Delta(c_1, \ldots, c_n)$ by 2.30, the evaluation of the two members of $\tilde{A}\tilde{f} + \tilde{B}\tilde{f}' = \Delta$ gives

$$Af + Bf' = \Delta(f), \ \deg(A) \le n - 2, \deg(B) \le n - 1.$$

$\square$

Ex. 12.3.8 *This exercise is concerned with $\Psi_i(y)$ from (12.37). Let $S(y)$ be as in (12.36).*

(a) *Show that applying (12.5) and (12.8) from the proof of Theorem 12.1.6 with $f = \beta = t_1 x_1 + \cdots + t_n x_n$ and $g = x_i$ gives*

$$x_i = \frac{\Phi_i(\beta)}{S'(\beta)},$$

where

$$\Phi_i(y) = \sum_{\sigma \in S_n} \frac{S(y) x_{\sigma(i)}}{y - \sigma \cdot \beta}.$$

Also prove that $\Phi_i(y) \in F[\sigma_1, \ldots, \sigma_n, y]$.

(b) *Use Exercice 7 to show that there are polynomials $A, B \in F[\sigma_1, \ldots, \sigma_n, y]$ such that $A(y)S(y) + B(y)S'(y) = \Delta(S)$. Also show that $B(\beta)S'(\beta) = \Delta(S)$.*

(c) *Use part (b) to show that (12.37) holds with $\Psi_i(y) = B(y)\Phi_i(y)$.*

Proof. (a) Let

$$S(y) = \prod_{\sigma \in S_n} \left(y - (t_1 x_{\sigma(1)} + \cdots + t_n x_{\sigma(n)}) \right) = \prod_{\sigma \in S_n} (y - \sigma \cdot \beta),$$

where $\beta = t_1 x_1 + \cdots + t_n x_n$.

As in (12.5), where here $\sigma \in S_n$ is the index of the sum, and $\psi = x_i, \varphi = \beta, \varphi_\sigma = \sigma \cdot \beta, \psi_\sigma = \sigma \cdot \psi = x_{\sigma(i)}, \theta = S$, define

$$\Phi_i(y) = \sum_{\sigma \in S_n} \frac{S(y)x_{\sigma(i)}}{y - \sigma \cdot \beta}.$$

Since $\frac{S(y)}{y-\sigma\cdot\beta} = \prod_{\tau \in S_n \setminus \{\sigma\}} (y - \tau \cdot \beta)$, Φ_i is a polynomial in y, with coefficients in $F[x_1, \ldots, x_n]$. Moreover, for all $\tau \in S_n$, since $\tau \cdot S(y) = S(y)$,

$$\begin{aligned}
\tau \cdot \Phi_i(y) &= \sum_{\sigma \in S_n} \frac{S(y)x_{(\tau \circ \sigma)(i)}}{y - (\tau \circ \sigma) \cdot \beta} \\
&= \sum_{\sigma' \in S_n} \frac{S(y)x_{\sigma'(i)}}{y - \sigma' \cdot \beta} \qquad (\sigma' = \tau \circ \sigma) \\
&= \Phi_i(y)
\end{aligned}$$

Therefore,

$$\Phi_i(y) \in F[\sigma_1, \ldots, \sigma_n, y].$$

If we evaluate the polynomial

$$\frac{S(y)}{y - \sigma \cdot \beta} = \prod_{\tau \in S_n \setminus \{\sigma\}} (y - \tau \cdot \beta)$$

at β, then we get $\prod_{\tau \neq e}(\beta - \tau \cdot \beta)$ if $\sigma = e$ and 0 otherwise. Therefore

$$\Phi_i(\beta) = x_i \prod_{\tau \neq e}(\beta - \tau \cdot \beta).$$

Moreover $S(y) = \prod_{\sigma \in S_n}(y - \sigma \cdot \beta)$, thus $S'(\beta) = \prod_{\tau \neq e}(\beta - \tau \cdot \beta)$. We conclude, as in (12.8), that

$$x_i = \frac{\Phi_i(\beta)}{S'(\beta)}.$$

(b) The conclusion of Exercise 7 applied to $S = f$ shows that there are polynomials A, B such that

$$A(y)S(y) + B(y)S'(y) = \Delta(S).$$

Since the coefficients of A and B are polynomials in the coefficients of S, $A, B \in F[\sigma_1, \ldots, \sigma_n, y]$.

The definition of S gives $S(\beta) = 0$. Therefore

$$B(\beta)S'(\beta) = \Delta(S).$$

(c) If we define $\Psi_i(y) = B(y)\Phi_i(y)$, then

$$x_i = \frac{\Phi_i(\beta)}{S'(\beta)} = \frac{B(\beta)\Phi_i(\beta)}{B(\beta)S'(\beta)} = \frac{\Psi_i(\beta)}{\Delta(S)}.$$

$\square$