13 Chapter 13 : LAGRANGE, COMPUTING GALOIS GROUPS

13.1 QUARTIC POLYNOMIALS

Ex. 13.1.1 *Let $f \in F[x]$ be separable of degree n, and let $\alpha_1, \dots, \alpha_n$ be the roots of f in a splitting field $F \subset L$ of f. In Section 6.3 we used the action of the Galois group on the roots to construct a one-to-one group homomorphism $\phi_1 : \mathrm{Gal}(L/F) \to S_n$. Now let $\beta_1, \dots, \beta_n$ be the same roots, possibly written in a different order. This gives $\phi_2 : Gal(L/F) \to S_n$. To relate ϕ_1 and ϕ_2, note that there is $\gamma \in S_n$ such that $\beta_i = \alpha_{\gamma(i)}$ for $1 \le i \le n$. Now define the conjugation map $\hat{\gamma} : S_n \to S_n$ by $\hat{\gamma}(\tau) = \gamma^{-1}\tau\gamma$.*

(a) Prove that $\phi_2 = \hat{\gamma} \circ \phi_1$.

(b) Let $G \subset S_n$ be the image of ϕ_1. Explain why part (a) justifies the assertion made in the text that "if we change the labels, then G gets replaced with a conjugate subgroup".

Proof. (a) By definition of the isomorphism $\phi_1 : \mathrm{Gal}(L/F) \to S_n$ in Section 6.3, if $\tau_1 = \phi_1(\sigma)$, then

$$\sigma(\alpha_i) = \alpha_{\tau_1(i)}, \qquad i = 1, \dots, n. \tag{1}$$

As $\beta_1, \dots, \beta_n$ are the same roots in a different order, there exists a permutation $\gamma \in S_n$ such that

$$\beta_i = \alpha_{\gamma(i)}, \qquad i = 1, \dots, n. \tag{2}$$

This numbering of the roots is associate to the isomorphism ϕ_2. If $\tau_2 = \phi_2(\sigma)$, then

$$\sigma(\beta_i) = \beta_{\tau_2(i)}, \qquad i = 1, \dots, n. \tag{3}$$

Therefore, for all $i = 1, \dots, n$, using (2), (3), and (2) again,

$$\sigma(\alpha_{\gamma(i)}) = \sigma(\beta_i) = \beta_{\tau_2(i)} = \alpha_{\gamma(\tau_2(i))}. \tag{4}$$

Now, with the substitution $i \to \gamma(i)$ in (1), we get

$$\sigma(\alpha_{\gamma(i)}) = \alpha_{\tau_1(\gamma(i))}. \tag{5}$$

Thus , by (4),(5), $\alpha_{\gamma(\tau_2(i))} = \alpha_{\tau_1(\gamma(i))}$ for all i. Since $i \mapsto \alpha_i$ is one-to-one,

$$\gamma(\tau_2(i)) = \tau_1(\gamma(i)), \qquad i = 1, \dots, n,$$

so

$$\gamma\tau_2 = \tau_1\gamma.$$

Therefore $\tau_2 = \gamma^{-1}\tau_1\gamma$, so $\phi_2(\sigma) = \hat{\gamma}(\phi_1(\sigma))$, for all $\sigma \in \mathrm{Gal}(L/F)$:

$$\phi_2 = \hat{\gamma} \circ \phi_1.$$

(b) Let G the image of ϕ_1 in S_n: $G = \{\phi_1(\sigma) \mid \sigma \in \mathrm{Gal}(L/F)\} \subset S_n$.

Similarly the image of ϕ_2 is $G' = \{\phi_2(\sigma) \mid \sigma \in \mathrm{Gal}(L/F)\} \subset S_n$.

Since $\phi_2(\sigma) = \gamma^{-1}\phi_1(\sigma)\gamma$ for all $\sigma \in \mathrm{Gal}(L/F)$ by part (a),

$$G' = \gamma^{-1}G\gamma.$$

So, if we change the labels, then G gets replaced with a conjugate subgroup. □

Ex. 13.1.2 *Prove that A_4 is the only subgroup of S_4 with 12 elements.*

Proof. Let H a subgroup of S_n such that $[S_n : H] = 2$. Then H is normal in S_n (by Exercise 12.1.20). Thus $S_n/H \simeq \{1, -1\}$. So there exists a group homomorphism

$$\varphi : S_n \to \{1, -1\}, \qquad \text{with } \ker(\varphi) = H.$$

Any two transpositions $\tau_1 = (a\,b), \tau_2 = (c\,d)$ of S_n are conjugate: if $\gamma = (a\,c)(b\,d)$, then $\tau_2 = \gamma\tau_1\gamma^{-1}$ (even if $b = c$).

Since $\{1, -1\} \simeq \mathbb{Z}/2\mathbb{Z}$ is abelian,

$$\begin{aligned}\varphi(\tau_2) &= \varphi(\gamma)\varphi(\tau_1)\varphi(\gamma)^{-1}\\ &= \varphi(\gamma)\varphi(\gamma)^{-1}\varphi(\tau_1)\\ &= \varphi(\tau_1)\end{aligned}$$

So $\tau_1, \tau_2 \in H$, or $\tau_1, \tau_2 \in S_n \setminus H$.

If τ_1, τ_2 are in $S_n \setminus H$, then $\varphi(\tau_1\tau_2) = \varphi(\tau_1)\varphi(\tau_2) = (-1) \times (-1) = 1$, so $\tau_1\tau_2 \in H$. In both cases $\tau_1\tau_2 \in H$.

Since every permutation σ of A_n is the product of an even number of transpositions, $\sigma \in H$, so $A_n \subset H$. As $|A_n| = |H| = n!/2$, $H = A_n$.

A_n is the only subgroup of S_n with $n!/2$ elements. □

Ex. 13.1.3 *Explain carefully why (13.6) follows from Exercise 9 of section 2.4.*

Proof. By definition,

$$y_1 = x_1x_2 + x_3x_4, \qquad y_2 = x_1x_3 + x_2x_4, \qquad y_3 = x_1x_4 + x_2x_3.$$

By Exercise 2.4.9, we know that

$$\Delta(\theta) = (y_1-y_2)^2(y_1-y_3)^2(y_2-y_3)^2 = [(x_1-x_4)(x_2-x_3)(x_1-x_3)(x_2-x_4)(x_1-x_2)(x_3-x_4)]^2 = \Delta$$

As the evaluation is a ring homomorphism, if we applied the evaluation defined by $x_1 \mapsto \alpha_1, \ldots, x_4 \mapsto \alpha_4$ to this equality in $F[x_1, x_2, x_3, x_4]$, we obtain that the roots

$$\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4, \qquad \beta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4, \qquad \beta_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3,$$

are the images of y_1, y_2, y_3 and satisfy

$$\begin{aligned}\Delta(\theta_f) &= (\beta_1 - \beta_2)^2(\beta_1 - \beta_3)^2(\beta_2 - \beta_3)^2\\ &= [(\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_4)(\alpha_1 - \alpha_2)(\alpha_3 - \alpha_4)]^2\\ &= \Delta(f)\end{aligned}$$

□

Ex. 13.1.4 *Use Example 7.3.4 from Chapter 7 to show that (13.8) gives all subgroups of $\langle(1\,3\,2\,4), (1\,2)\rangle$ of order 4 or 8.*

Proof. We obtain all subgroups of $D_8 \simeq \langle\sigma, \tau\rangle$, where $\sigma = (1\,3\,2\,4), \tau = (1\,2)$, in Exercise 7.3.3

$$
\begin{tikzcd}
 & & & & \{e\} \arrow[dllll] \arrow[dll] \arrow[d] \arrow[drr] \arrow[drrrr] & & & & \\
\langle \tau \rangle \arrow[drr] & & \langle \sigma^2\tau \rangle \arrow[d] & & \langle \sigma^2 \rangle \arrow[dll] \arrow[d] \arrow[drr] & & \langle \sigma\tau \rangle \arrow[d] & & \langle \sigma^3\tau \rangle \arrow[dll] \\
 & & \langle \sigma^2, \tau \rangle \arrow[drr] & & \langle \sigma \rangle \arrow[d] & & \langle \sigma^2, \sigma\tau \rangle \arrow[dll] & & \\
 & & & & G = \langle \sigma, \tau \rangle & & & &
\end{tikzcd}
$$

If G is a subgroup of order 4 or 8, then G is one of the four groups

$$\langle \sigma^2, \tau \rangle, \quad \langle \sigma \rangle, \quad \langle \sigma^2, \sigma\tau \rangle, \quad \langle \sigma, \tau \rangle,$$

Moreover $\sigma^2 = (1\,2)(3\,4)$ and $\sigma\tau = (1\,4)(2\,3)$, so

$$\langle \sigma^2, \tau \rangle = \langle (1\,2)(3\,4), (1\,2) \rangle = \langle (3\,4), (1\,2) \rangle,$$

and

$$\langle \sigma^2, \sigma\tau \rangle = \langle (1\,2)(3\,4), (1\,4)(2\,3) \rangle = \langle (1\,2)(3\,4), (1\,3)(2\,4) \rangle$$

is the group of double transpositions $\{(), (1\,2)(3\,4), (1\,4)(2\,3), (1\,3)(2\,4)\}$.

Therefore G is one of the four groups given in the text

$$\langle (1\,2), (3\,4) \rangle, \qquad \langle (1\,2)(3\,4), (1\,3)(2\,4) \rangle, \qquad \langle (1\,3\,2\,4) \rangle, \qquad \langle (1\,3\,2\,4), (1\,2) \rangle.$$

$\square$

Ex. 13.1.5 *Let F be a field of characteristic $\neq 2$, and let $g \in F[x]$ be a monic cubic polynomial that has a root in F. Prove that g splits completely over F if and only if $\Delta(g) \in F^2$.*

Proof. Let $g = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$, where $\alpha_1, \alpha_2, \alpha_3$ lie in some splitting field of F, and $\alpha_1 \in F$.

- If g splits completely over F, then $\alpha_1, \alpha_2, \alpha_3$ lie in F, therefore $\delta = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) \in F$, so $\Delta(g) = \delta^2 \in F^2$.
- Conversely, suppose that $\Delta(g) \in F^2$. Then $\Delta(g) = a^2,\ a \in F$, so $\delta = \pm a \in F$. Since $\alpha_1 \in F$, the Euclidean division of $g(x)$ by $x - \alpha_1 \in F[x]$ gives

  $$g(x) = (x - \alpha_1)(x^2 + px + q), \qquad p, q \in F.$$

  Then $x^2 + px + q = (x - \alpha_2)(x - \alpha_3)$, hence $\alpha_2 + \alpha_3 = -p \in F, \alpha_2\alpha_3 = q \in F$, and

  $$(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3) = \alpha_1^2 + p\alpha_1 + q \in F.$$

  If $\alpha_1 = \alpha_2$, then $\alpha_3 = -p - \alpha_2 = -p - \alpha_1 \in F$, so g splits completely over F, and similarly the same conclusion is true if $\alpha_1 = \alpha_3$.

In the remaining case, $(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)\neq 0$, so

$$\alpha_2-\alpha_3=\delta[(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)]^{-1}\in F.$$

Since $\alpha_2+\alpha_3\in F$, and $\alpha_2-\alpha_3\in F$, and since the characteristic of F is not 2,

$$\alpha_2=\frac{1}{2}[(\alpha_2+\alpha_3)+(\alpha_2-\alpha_3)]\in F, \alpha_3=\frac{1}{2}[(\alpha_2+\alpha_3)-(\alpha_2-\alpha_3)]\in F.$$

Therefore $g=(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$ splits completely over F.

□

Ex. 13.1.6 *This exercise is concerned with the proof of part (c) of Theorem 13.1.1. Let $f(x)=x^4-c_1x^3+c_2x^2-c_3x+c_4$ as in the theorem.*

(a) Suppose that f has roots $\alpha_1,\alpha_2,\alpha_3,\alpha_4$ such that $\alpha_1+\alpha_2-\alpha_3-\alpha_4=\alpha_1\alpha_2-\alpha_3\alpha_4=0$. Prove that f is not separable.

(b) Let β be a root of the resolvent $\theta_f(y)$. Use part (a) to prove that $4\beta+c_1^2-4c_2$ and β^2-4c_4 can't both vanish when f is separable.

(c) Suppose that $4\beta+c_1^2-4c_2=0$ in part (c) of Theorem 13.1.1. Prove carefully that G is conjugate to $\langle(1\,3\,2\,4),(1\,2)\rangle$ if and only if $\Delta(f)(\beta^2-4c_4)\notin(F^*)^2$.

Proof. (a) If $\alpha_1+\alpha_2-\alpha_3-\alpha_4=\alpha_1\alpha_2-\alpha_3\alpha_4=0$, then

$$\begin{aligned} s &:= \alpha_1+\alpha_2=\alpha_3+\alpha_4\\ p &:= \alpha_1\alpha_2=\alpha_3\alpha_4 \end{aligned}$$

Thus $x^2-sx+p=(x-\alpha_1)(x-\alpha_2)=(x-\alpha_3)(x-\alpha_4)$, therefore

$$\{\alpha_1,\alpha_2\}=\{\alpha_3,\alpha_4\}.$$

Since $\alpha_3=\alpha_1$ or $\alpha_3=\alpha_2$, f is not separable.

(b) If β is a root of the resolvent θ_f, we can relabel the roots of f so that $\beta=\alpha_1\alpha_2+\alpha_3\alpha_4$ and

$$4\beta+c_1^2-4c_2=(\alpha_1+\alpha_2-\alpha_3-\alpha_4)^2.$$

Since $\beta^2-4c_4=(\alpha_1\alpha_2-\alpha_3\alpha_4)^2$, if $4\beta+c_1^2-4c_2$ and β^2-4c_4 both vanish, then $\alpha_1+\alpha_2-\alpha_2-\alpha_4=0$ and $\alpha_1\alpha_2-\alpha_3\alpha_4=0$. Then, by part (a), f is not separable.

Therefore $4\beta+c_1^2-4c_2$ and β^2-4c_4 can't both vanish when f is separable.

(c) Suppose that $4\beta+c_1^2-4c_2=0$ in part (c) of Theorem 13.1.1, where $\theta_f(y)$ has a unique root β in F. We know that f is separable by Lemme 5.3.5.

Therefore $\Delta(f)\neq 0$, and, by part (b), $\beta^2-4c_4\neq 0$, so

$$\Delta(f)(\beta^2-4c_4)\neq 0.$$

We know that $G=\langle(1\,3\,2\,4)\rangle$ or $G=\langle(1\,3\,2\,4),(1,2)\rangle$.

- Suppose that $G = \langle (1\,3\,2\,4) \rangle$. Then $\mathrm{Gal}(L/F) = \langle \sigma \rangle$, where σ corresponds to $(1\,3\,2\,4)$. We choose

$$\sqrt{\Delta(f)(\beta^2 - 4c_4)} = \sqrt{\Delta(f)}(\alpha_1\alpha_2 - \alpha_3\alpha_4).$$

  Since $(1\,3\,2\,4) = (1\,3)(3\,2)(2\,4) \not\in A_4$, $\sigma(\sqrt{\Delta(f)}) = -\sqrt{\Delta(f)}$, and

$$\sigma(\alpha_1\alpha_2 - \alpha_3\alpha_4) = \alpha_3\alpha_4 - \alpha_2\alpha_1 = -(\alpha_1\alpha_2 - \alpha_3\alpha_4).$$

  Therefore σ fixes $\sqrt{\Delta(f)(\beta^2 - 4c_4)}$, so $\sqrt{\Delta(f)(\beta^2 - 4c_4)} \in F^*$, and

$$\Delta(f)(\beta^2 - 4c_4) \in (F^*)^2.$$

- Suppose that $G = \langle (1\,3\,2\,4), (1,2) \rangle$. Then $\mathrm{Gal}(L/F) = \langle \sigma, \tau \rangle$, where τ corresponds to $(1\,2)$. $\tau(\sqrt{\Delta(f)}) = -\sqrt{\Delta(f)}$ and $\tau(\alpha_1\alpha_2 - \alpha_3\alpha_4) = \alpha_2\alpha_1 - \alpha_3\alpha_4 = \alpha_1\alpha_2 - \alpha_3\alpha_4$, so $\tau(\sqrt{\Delta(f)(\beta^2 - 4c_4)}) = -\sqrt{\Delta(f)(\beta^2 - 4c_4)}$. Since the characteristic is not 2, and $\Delta(f)(\beta^2 - 4c_4) \neq 0, \sqrt{\Delta(f)(\beta^2 - 4c_4)} \not\in F$, so

$$\Delta(f)(\beta^2 - 4c_4) \not\in (F^*)^2.$$

  Therefore G is conjugate to $\langle (1\,3\,2\,4), (1\,2) \rangle$ if and only if $\Delta(f)(\beta^2 - 4c_4) \not\in (F^*)^2$.

$\square$

Ex. 13.1.7 *In Exercise 18 of section 12.1 you found the roots of $f = x^4 + 2x^2 - 4x + 2 \in \mathbb{Q}[x]$ using the formula developed in that section. At the end of the exercise, we said that "this quartic is especially simple". Justify this assertion using Theorem 13.1.1*

Proof. By Exercise 12.1.18,

$$\theta_f(y) = y^3 - 2y^2 - 8y = y(y-4)(y+2).$$

Moreover f is irreducible over $\mathbb{Q}$ (from the instruction **f.is_irreducible()** in Sage).

Since $\theta_f(y)$ splits completely over F, by Theorem 13.1.1,

$$G = \langle (1\,2)(3\,4), (1\,3)(2\,4) \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

(This result was already proved in Exercise 12.1.18, since the splitting field of f is $\mathbb{Q}(i, \sqrt{2})$.) $\square$

Ex. 13.1.8 *In Example 10.3.10, we showed that the roots of $f = 7m^4 - 16m^3 - 21m^2 + 8m + 4 \in \mathbb{Q}[m]$ can be constructed using origami. Show that the splitting field of f is an extension of $\mathbb{Q}$ of degree 24. By the results of Section 10.1, it follows that the roots of f are not constructible with straightedge and compass, since 24 is not a power of 2.*

Proof. The discriminant of $g = \frac{1}{7}f$ is

$$\Delta(g) = \frac{174446784}{117649} = 2^6 \cdot 3^6 \cdot 3739 \cdot 7^{-6},$$

so $\Delta(g)$ is not a square in $\mathbb{Q}$.

The Ferrari resolvent is

$$\theta_f(y) = y^3 + 3y^2 - \frac{240}{49}y - \frac{3824}{343}.$$

and

$$7^3\theta_f(y) = 343y^3 + 1029y^2 - 1680y - 3824$$

has no root in $\mathbb{Q}$, so is irreducible over $\mathbb{Q}$.

By theorem 13.1.1, $G = S_4$. Therefore the splitting field L of f has degree

$$[L : \mathbb{Q}] = |G| = 24.$$

Sage instructions :

```
var('m')
R.<m> = QQ[m]
f= 7*m^4-16*m^3-21*m^2+8*m+4
g=f/7
d=g.discriminant()
d.factor()
```

$$2^6 \cdot 3^6 \cdot 7^{-6} \cdot 3739$$

```
R.<y> = QQ[]
l = f.coefficients(sparse=False);
c1 = -l[3]/l[4]; c2 = l[2]/l[4];c3 = -l[1]/l[4]; c4 = l[0]/l[4];
theta_f = y^3 -c2*y^2 +(c1*c3-4*c4)*y - c3^2-c1^2*c4 + 4*c2*c4;
```

$$y^3 + 3y^2 - \frac{240}{49}y - \frac{3824}{343}$$

```
theta_f.is_irreducible()
```

True

□

Ex. 13.1.9 *As in Example 13.1.3, let $f = x^4 + ax^3 + bx^2 + ax + 1 \in F[x]$, and let α be a root of f in some splitting field of f over F. Show that α^{-1} is also a root of f, and then use (13.5) to conclude that 2 is a root of the resolvent $\theta_f(y)$.*

Proof. If α is a root of f in some splitting field L of F, then $\alpha^4 + a\alpha^3 + b\alpha^2 + a\alpha + 1 = 0$. If we divide by α^4, we obtain $1 + a\alpha^{-1} + b\alpha^{-2} + a\alpha^{-3} + \alpha^{-4}$, so $f(\alpha^{-1}) = 0$. Note that

$$\begin{aligned} x^4 + ax^3 + bx^2 + ax + 1 &= x^2\left[\left(x^2 + \frac{1}{x^2}\right) + a\left(x + \frac{1}{x}\right) + b\right] \\ &= x^2\left[\left(x + \frac{1}{x}\right)^2 + a\left(x + \frac{1}{x}\right) + b - 2\right] \end{aligned}$$

As 0 is not a root of f, the roots of f are the roots of $z = x + \frac{1}{x}$, where z is a root of $z^2 + az + b - 2$, so the roots of f are the roots of the two polynomials

$$x^2 - z_1x + 1, \qquad x^2 - z_2x + 1,$$

where z_1, z_2 are the roots in L of

$$z^2 + az + b - 2.$$

If we relabel the roots so that α_1, α_2 are the roots of $x^2 - z_1x + 1$, and α_3, α_4 the roots of $x^2 - z_2x + 1$, then $\alpha_1\alpha_2 = 1, \alpha_3\alpha_4 = 1$, therefore $\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4 = 2$ is a root of the Ferrari resolvent $\theta_f(y)$. □

Ex. 13.1.10 *As in Example 13.1.4, let $f = x^4 + bx^2 + d \in F[x]$, where $d \not\in F^2$. Compute $\Delta(f)$ and $\theta_f(y)$.*

Proof. The discriminant of f is

$$\Delta(f) = 16b^4d - 128b^2d^2 + 256d^3 = 16\ d\,(b^2 - 4d)^2.$$

The Ferrari resolvent is

$$\theta_f(y) = y^3 - by^2 - 4dy + 4bd = (y - b)(y^2 - 4d).$$

Sage instructions:

```
R.<x,b,d> = QQ[]
f=x^4+b*x^2+d
c1 = 0; c2 = b; c3 = 0; c4 = d;
theta_f = x^3 - c2*x^2 + (c1*c3-4*c4)*x - c3^2-c1^2*c4 + 4*c2*c4;
factor(theta_f)
```

$$(-x + b) \cdot (-x^2 + 4d)$$

```
Delta = theta_f.discriminant(x)
factor(Delta)
```

$$(16) \cdot d \cdot (-b^2 + 4d)^2$$

Thus $\theta_f(y) = (y - b)(y - 2\sqrt{d})(y + 2\sqrt{d})$ has a unique root in F if $d \not\in F^2$, and the discriminant is not a square in F^2. $\square$

Ex. 13.1.11 *In Example 13.1.7 we showed that if $f = x^4 + ax^3 + bx^2 + ax + 1 \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Q}$, then its Galois group is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ if and only if there is $c \in \mathbb{Q}$ such that $4a^2 + c^2 = (b + 2)^2$.*

(a) Show that $c \in \mathbb{Z}$, and use the irreducibility of f to prove that $c \neq 0$. Hence we may assume that $c > 0$, so that $(2a, c, b + 2)$ is a Pythagorean triple.

(b) Show that $3^2 + 4^2 = 5^2, 5^2 + 12^2 = 13^2, 7^2 + 24^2 = 25^2$, and $8^2 + 15^2 = 17^2$ give two examples of polynomials with $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ as Galois group (two of the triples give reducible polynomials).

Proof. (a) $c \in \mathbb{Q}$ is such that $c^2 = n \in \mathbb{Z}$. Write $c = a/b, b > 0, a \wedge b = 1$. Then $a^2 = nb^2$. If $b \neq 1$, there is a prime p such that $p \mid b$. But then $p \mid a^2$, thus $p \mid a$, in contradiction with $a \wedge b = 1$. So $c \in \mathbb{Z}$.

If $c = 0$, then $(b + 2)^2 = 4a^2$, so $b + 2 = 2\varepsilon a$, $b = -2 + 2\varepsilon a$, where $\varepsilon = \pm 1$.

In Exercise 9, we saw that

$$f = x^4 + ax^3 + bx^2 + ax + 1 = (x^2 - z_1x + 1)(x^2 - z_2x + 1),$$

where z_1, z_2 are the roots of $z^2 + az + b - 2$. Here $b = -2 + 2\varepsilon a$, so z_1, z_2 are the roots of

$$z^2 + az - 4 + 2\varepsilon a = (z + a - 2\varepsilon)(z + 2\varepsilon),$$

so

$$z_1 = -a + 2\varepsilon \in \mathbb{Z}, \qquad z_2 = -2\varepsilon \in \mathbb{Z},$$

so f is not irreducible over $\mathbb{Q}$, in contradiction with the hypothesis. We have proved that $c \neq 0$ if f is irreducible, and so $(2a, c, b + 2)$ is a Pythagorean triple.

(b) $3^2+4^2=5^2$ gives $a=2, b=3$, and $f=x^4+2x^3+3x^2+2x+1=(x^2+x+1)^2$ is not irreducible.

$5^2+12^2=13^2$ gives $a=6, b=11$, and $f=x^4+6x^3+11x^2+6x+1=(x^2+3x+1)^2$ is not irreducible.

$7^2+24^2=25^2$ gives $a=12, b=23$, and $f=x^4+12x^3+23x^2+12x+1$ which is irreducible. So the Galois group of

$$f=x^4+12x^3+23x^2+12x+1$$

is isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

Verification with Sage:

```
R.<x> = QQ[]
f= x^4 + 12*x^3 + 23*x^2 + 12*x + 1
f.is_irreducible()
```

True

```
G = f.galois_group()
G.gens()
```

$$[(1,2)(3,4),(1,4)(2,3)]$$

```
G.structure_description()
```

$$C2\times C2$$

□

$8^2+15^2=17^2$ gives $a=4, b=15$, and $f=x^4+4x^3+15x^2+4x+1$, which is irreducible. The Galois group of

$$f=x^4+4x^3+15x^2+4x+1$$

is isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

Note: the polynomial associate to $7^2+24^2=25^2$ is

$$\begin{aligned} f &= x^4+12x^3+23x^2+12x+1\\ &= (x^2+6x+1)^2-15x^2\\ &= (x^2+(6+\sqrt{15})x+1)(x^2+(6-\sqrt{15})x+1) \end{aligned}$$

The discriminant of the first factor is $\Delta_1=47+12\sqrt{15}$ and the discriminant of the second is $\Delta_2=47-12\sqrt{15}$. Since

$$\left(\sqrt{47+12\sqrt{15}}\right)\left(\sqrt{47-12\sqrt{15}}\right)=\sqrt{47^2-144\times 15}=\sqrt{49}=7\in\mathbb{Q}^*),$$

the splitting field of f over $\mathbb{Q}$ is $\mathbb{Q}\left(\sqrt{47+12\sqrt{15}}\right)$, which is a quadratic extension of a quadratic extension. The minimal polynomial of $a=\sqrt{47+12\sqrt{15}}$ is x^4-94x^2+49, whose Galois group is also $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ (here $d=49$ is a square).

Ex. 13.1.12 *This exercise is concerned with the proof of Proposition 13.1.5.*

(a) Prove (13.12).

(b) Prove that the two polynomials h_1 and h_2 defined in the proof of the proposition factor as $h_1 = (y - (\alpha_1 + \alpha_2))(y - (\alpha_3 + \alpha_4))$ and $h_2 = (y - \alpha_1\alpha_2)(y - \alpha_3\alpha_4)$.

Proof. (a) Let $g = y^2 + Ay + B \in F[y]$ and let $F \subset F(\sqrt{a})$, $a \in F$, be a quadratic extension.

If $\Delta(g) = 0$ then $a\Delta(g) = 0 \in F^2$. Suppose now that g is irreducible over F.

- Suppose that g splits completely over $F(\sqrt{a})$, so
$$g = (y - y_1)(y - y_2), \qquad y_1, y_2 \in F(\sqrt{a}).$$
Then $\Delta(g) = (y_1 - y_2)^2 = A^2 - 4B \in F$. We choose $\sqrt{\Delta(g)} = y_2 - y_1 \in F(\sqrt{a})$. Here $\deg(g) = 2$, and g is irreducible over F, therefore the roots of g
$$\begin{aligned} y_1 &= \frac{1}{2}((y_1 + y_2) + (y_1 - y_2)) = \frac{1}{2}\left(-A - \sqrt{\Delta(g)}\right), \\ y_2 &= \frac{1}{2}((y_1 + y_2) - (y_1 - y_2)) = \frac{1}{2}\left(-A + \sqrt{\Delta(g)}\right), \end{aligned}$$
are not in F, and this is equivalent to
$$\sqrt{\Delta(g)} \notin F.$$
Since $\sqrt{\Delta(g)} \in F(\sqrt{a})$, and $\sqrt{\Delta(g)} \notin F$,
$$\sqrt{\Delta(g)} = u + v\sqrt{a}, \qquad u, v \in F, \qquad v \neq 0.$$
Therefore
$$\begin{aligned} u^2 &= \left(\sqrt{\Delta(g)} - v\sqrt{a}\right)^2 \\ &= \Delta(g) + av^2 - 2v\sqrt{a}\sqrt{\Delta(g)} \end{aligned}$$
Since $v \neq 0$, and $\mathrm{char}(F) \neq 2$,
$$\sqrt{a}\sqrt{\Delta(g)} = \frac{\Delta(g) + av^2 - u^2}{2v} \in F,$$
so
$$a\Delta(g) \in F^2.$$

- Conversely, suppose that $a\Delta(g) \in F^2$. Here $a \neq 0$ since $F(\sqrt{a})$ is a quadratic extension of F. There exists $w \in F$ such that $a\Delta(g) = w^2$.
We choose $\sqrt{\Delta(g)}$ such that
$$\sqrt{\Delta(g)} = \frac{w}{\sqrt{a}} = \frac{w}{a}\sqrt{a} \in F(\sqrt{a}).$$
Then
$$\begin{aligned} y_1 &= \frac{1}{2}((y_1 + y_2) + (y_1 - y_2)) = \frac{1}{2}\left(-A - \sqrt{\Delta(g)}\right), \\ y_2 &= \frac{1}{2}((y_1 + y_2) - (y_1 - y_2)) = \frac{1}{2}\left(-A + \sqrt{\Delta(g)}\right), \end{aligned}$$
are in $F(\sqrt{a})$, so $g = (y - y_1)(y - y_2)$ splits completely over $F(\sqrt{a})$.
Finally, if $\Delta(g) = 0$, $g = (y - y_0)^2$, where $y_0 = -A/2 \in F$, splits completely over F, a fortiori over $F(\sqrt{a})$.

Conclusion:

Let $g = y^2 + Ay + B$ and $F(\sqrt{a})$ a quadratic extension of F, with $\mathrm{char}(F) \neq 2$. If $\Delta(g) = 0$, or if g is irreducible over F, then

$$g \text{ splits completely over } F(\sqrt{a}) \iff a\Delta(g) \in F^2.$$

(b)

$$\begin{aligned}
&(y - (\alpha_1 + \alpha_2))(y - (\alpha_3 + \alpha_4))\\
&= y^2 - (\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)y + (\alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4)\\
&= y^2 - c_1 y + (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4) - (\alpha_1\alpha_2 + \alpha_3\alpha_4)\\
&= y^2 - c_1 y + c_2 - \beta,
\end{aligned}$$

so

$$h_1 = y^2 - c_1 y + c_2 - \beta = (y - (\alpha_1 + \alpha_2))(y - (\alpha_3 + \alpha_4)).$$

Similarly

$$\begin{aligned}
&(y - \alpha_1\alpha_2)(y - \alpha_3\alpha_4)\\
&= y^2 - (\alpha_1\alpha_2 + \alpha_3\alpha_4)y + \alpha_1\alpha_2\alpha_3\alpha_4\\
&= y^2 - \beta y + c_4
\end{aligned}$$

so

$$h_2 = y^2 - \beta y + c_4 = (y - \alpha_1\alpha_2)(y - \alpha_3\alpha_4).$$

We have proved that h_1, h_2 split completely over L. Since $\deg(h_1) = 2$, h_1 splits over a quadratic extension $F \subset M$, with $M \subset L$. But the unique such quadratic extension is $F(\sqrt{\Delta(f)})$ (since $\mathrm{Gal}(L/F) \simeq \mathbb{Z}/4\mathbb{Z}$ has a unique subgroup of index 2). Therefore $M = F(\sqrt{\Delta(f)})$, and h_1 splits completely over $F(\sqrt{\Delta(f)})$, and also h_2. $\square$

Ex. 13.1.13 *Suppose that $f \in F[x]$ satisfies the hypothesis of part (c) of Theorem 13.1.1, and let α be a root of f. Prove that $G \simeq \mathbb{Z}/4\mathbb{Z}$ if f splits completely over $F(\alpha)$, and $G \simeq D_8$ otherwise. This gives a version of part (c) that doesn't use resolvents. Since we can factor over extension fields by Section 4.2, this method is useful in practice.*

Proof. With the hypothesis of part (c), $\Delta(f) \notin F^2$, so $\Delta(f) \neq 0$ and f is separable.

- If $G \simeq \mathbb{Z}/4\mathbb{Z}$, then $G = \langle \sigma \rangle \subset S_4$, where σ corresponds to $\tilde{\sigma} \in \mathrm{Gal}(L/F)$. Write $G_\alpha = \mathrm{Stab}_G(\alpha)$. Since f is irreducible, $\mathcal{O}_\alpha = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ is the set of the four roots of f, therefore $4 = |\mathcal{O}_\alpha| = (G : G_\alpha)$, so $G_\alpha = \{e\}$. Hence $\tilde{\sigma}^i(\alpha) \neq \tilde{\sigma}^j(\alpha)$ if $1 \leq i < j \leq 4$. We choose the numbering of the roots such that $\alpha_1 = \alpha$, and $\tilde{\sigma}(\alpha_1) = \alpha_3, \tilde{\sigma}(\alpha_3) = \alpha_2, \tilde{\sigma}(\alpha_2) = \alpha_4$ are the four distinct roots of f, so $\sigma = (1\,3\,2\,4)$.

  $$f = (x - \alpha_1)(x - \alpha_3)(x - \alpha_2)(x - \alpha_4) = (x - \alpha)(x - \tilde{\sigma}(\alpha))(x - \tilde{\sigma}^2(\alpha))(x - \tilde{\sigma}^3(\alpha)).$$

  As $\Delta(f) \notin F^2$, $F(\sqrt{\Delta(f)})$ is a quadratic extension of F.

  Since the only subgroup of G are $\{e\} \subset H = \langle \sigma^2 \rangle \subset G = \langle \sigma \rangle$, by the Galois correspondence, the only intermediate fields of $F \subset L$ are $F \subset F(\sqrt{\Delta(f)}) \subset L$, and the fixed field of $H = \langle \sigma^2 \rangle$ is $L_H = F(\sqrt{\Delta(f)})$.

If $F(\alpha) \subset F(\sqrt{\Delta(f)})$, then $\alpha \in F(\sqrt{\Delta(f)}) = L_H$, therefore $\sigma^2(\alpha) = \alpha$, and so $\alpha_2 = \alpha_1$, in contradiction with the separability of f. Hence $F(\alpha) \not\subset F(\sqrt{\Delta(f)})$, so

$$F(\alpha) = L = F(\alpha_1, \alpha_2, \alpha_3, \alpha_4).$$

Then f splits completely over $F(\alpha)$.

- If $G \not\simeq \mathbb{Z}/4\mathbb{Z}$, then by Theorem 13.1.1, $G \simeq D_8$. Therefore $[L : F] = |G| = 8$, and $[F(\alpha) : F] = \deg(f) = 4$, which implies $F(\alpha) \neq L = F(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$. Therefore one of the roots α_i is not in $F(\alpha)$, and so $f = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \alpha_4)$ doesn't splits completely over $F(\alpha)$.

Conclusion. Let f be a quadratic polynomial, and let α be a root of f.
If $\Delta(f) \notin F^2$ and $\theta_f(y)$ is reducible over F, then

$$\begin{aligned} f \text{ splits completely over } F(\alpha) &\iff \mathrm{Gal}_F(f) \simeq \mathbb{Z}/4\mathbb{Z}, \\ f \text{ doesn't split completely over } F(\alpha) &\iff \mathrm{Gal}_F(f) \simeq D_8. \end{aligned}$$

□

Example 1: $f = x^4 - 12x^2 + 18$ over $\mathbb{Q}$.

```
R.<x> = QQ[]
f = x^4-12*x^2 + 18
print(f.is_irreducible())
factor(f.discriminant()), f.discriminant().is_square()
```

True

$$(2^{11} \cdot 3^6, \text{False}).$$

```
l = f.coefficients(sparse=False);
c1 = -l[3]/l[4]; c2 = l[2]/l[4];c3 = -l[1]/l[4]; c4 = l[0]/l[4];
S.<y> = QQ[]
theta_f = y^3 -c2*y^2 +(c1*c3-4*c4)*y - c3^2-c1^2*c4 + 4*c2*c4;
factor(theta_f)
```

$$(y + 12) \cdot (y^2 - 72)$$

```
K.<a>= NumberField(f)
S.<x> = K[]
f = x^4-12*x^2 + 18
factor(f)
```

$$(x - a) \cdot (x + a) \cdot (x - \frac{1}{3}a^3 + 3a) \cdot (x + \frac{1}{3}a^3 - 3a)$$

These results prove that the Galois group of $f = x^4 - 12x^2 + 18$ over $\mathbb{Q}$ is isomorphic to $\mathbb{Z}/4\mathbb{Z}$. Verification with Sage:

```
R.<x> = QQ[]
f = x^4-12*x^2 + 18
f.galois_group().gens()
```

$$[(1, 2, 3, 4)]$$

```
f.galois_group().structure_description()
```

$$C4$$

Example 2: $f = x^4 - 2$ over $\mathbb{Q}$.

```
R.<x> = QQ[]
f = x^4-2
print(f.is_irreducible())
factor(f.discriminant()), f.discriminant().is_square()
```

$$\text{True}$$

$$(-1 \cdot 2^{11}, \text{False})$$

```
l = f.coefficients(sparse=False);
c1 = -l[3]/l[4]; c2 = l[2]/l[4];c3 = -l[1]/l[4]; c4 = l[0]/l[4];
S.<y> = QQ[]
theta_f = y^3 -c2*y^2 +(c1*c3-4*c4)*y - c3^2-c1^2*c4 + 4*c2*c4;
factor(theta_f)
```

$$y \cdot (y^2 + 8)$$

```
K.<a>= NumberField(f)
S.<x> = K[]
f = x^4-2
factor(f)
```

$$(x - a) \cdot (x + a) \cdot (x^2 + a^2)$$

Thus the Galois group of $x^4 - 2$ over $\mathbb{Q}$ is D_8. Verification with Sage:

```
R.<x> = QQ[]
f = x^4-2
f.galois_group().gens()
```

$$[(1, 2, 3, 4), (1, 3)]$$

```
f.galois_group().structure_description()
```

$$D4$$

Example 3: $f = x^4 - 18x^2 + 9$ over $\mathbb{Q}$.

```
R.<x> = QQ[]
f = x^4-18*x^2 + 9
print(f.is_irreducible())
factor(f.discriminant()), f.discriminant().is_square()
```

$$\text{True}$$

$$(2^{14} \cdot 3^6, \text{True})$$

```
l = f.coefficients(sparse=False);
c1 = -l[3]/l[4]; c2 = l[2]/l[4];c3 = -l[1]/l[4]; c4 = l[0]/l[4];
S.<y> = QQ[]
theta_f = y^3 -c2*y^2 +(c1*c3-4*c4)*y - c3^2-c1^2*c4 + 4*c2*c4;
factor(theta_f)
```

$$(y-6)\cdot(y+6)\cdot(y+18)$$

The Galois group of $f = x^4 - 18x^2 + 9$ over $\mathbb{Q}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. Verification with Sage:

```
R.<x> = QQ[]
f = x^4-18*x^2 + 9
f.galois_group().gens()
```

$$[(1,2)(3,4),(1,4)(2,3)]$$

```
f.galois_group().structure_description()
```

$$C2\times C2$$

Ex. 13.1.14 *Use Theorem 13.1.1 to compute the Galois groups of the following polynomials in $\mathbb{Q}[x]$:*

(a) x^4+4x+2.

(b) $x^4+8x+12$.

(c) x^4+1.

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

(e) x^4-2.

Proof. (a) $f = x^4+4x+2$.

$\Delta(f) = -2^8\cdot 19$ is not a square in $\mathbb{Q}$, and $\theta_f(y) = y^3-8y-16$ is irreducible over $\mathbb{Q}$, so $\mathrm{Gal}_{\mathbb{Q}}(f)\simeq S_4$ (part (a) of Theorem 13.1.11).

(b) $f = x^4+8x+12$.

$\Delta(f) = 2^{12}\cdot 3^4$ is a square in $\mathbb{Q}$, and $\theta_f(y) = y^3-48y-64$ is irreducible over $\mathbb{Q}$, so $\mathrm{Gal}_{\mathbb{Q}}(f)\simeq A_4$ (part (a) of Theorem 13.1.11).

(c) $f = x^4+1$.

$\Delta(f) = 2^8$ is a square in $\mathbb{Q}$ and $\theta_f(y) = y(y-2)(y+2)$ splits completely over $\mathbb{Q}$, so $\mathrm{Gal}_{\mathbb{Q}}(f)\simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ (part (b) of Theorem 13.1.11).

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

$\Delta(f) = 5^3$ is not a square, and $\theta_f(y) = (y-2)(y^2+y+1)$ has a unique root in $\mathbb{Q}$, so part (c) of Theorem 13.1.1 applies. Let ζ a root of f. Then

$$f = (x-\zeta)(x-\zeta^2)(x-\zeta^3)(x-\zeta^4)$$

splits completely over $\mathbb{Q}(\zeta)$. By Exercise 13,

$$G\simeq \mathbb{Z}/4\mathbb{Z}.$$

(we know already this result, since $f = \Phi_5$.)

(e) $f = x^4 - 2$.

By Exercise 13, Example 2, $\Delta(f) = -2^{11}$ is not a square, and $\theta_f(y) = y(y^2+8)$ has a unique root in $\mathbb{Q}$. Moreover if $a = \sqrt[4]{2}$,

$$f = (x-a)(x+a)(x^2+a^2)$$

doesn't splits completely over $\mathbb{Q}$, so

$$G \simeq D_8.$$

$\square$

Ex. 13.1.15 *In the situation of Theorem 13.1.1, assume that $\theta_f(y)$ has a root in F. In the proof of the theorem, we used (13.5) and (13.7) to show that G is conjugate to a subgroup of D_8. Show that the weaker assertion that $|G| = 4$ or 8 can be proved directly from (12.17).*

Proof. By (12.17), the roots of the quartic $f = x^4 - c_1x^3 + c_2x^2 - c_3x + c_4$ are

$$\alpha = \frac{1}{4}\left(c_1 + \varepsilon_1\sqrt{4y_1 + c_1^2 - 4c_2} + \varepsilon_2\sqrt{4y_2 + c_1^2 - 4c_2} + \varepsilon_3\sqrt{4y_3 + c_1^2 - 4c_2}\right),$$

where y_1, y_2, y_3 are the roots of the Ferrari resolvent

$$\theta_f(y) = y^3 - c_2y^2 + (c_1c_3 - 4c_4)y - c_3^2 - c_1^2c_4 + 4c_2c_4,$$

and the $\varepsilon_i = \pm 1$ are chosen so that the product of the radicals $t_i = +\varepsilon_i\sqrt{4y_i + c_1^2 - 4c_2}$ is

$$t_1t_2t_3 = c_1^3 - 4c_1c_2 + 8c_3.$$

Let $L = F(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ be the splitting field of F.

Here $\theta_f(y)$ has a root in F, say y_1. Thus

$$\theta_f(y) = (y - y_1)g(y),$$

where $g(y) = y^2 + ay + b \in F[y]$. Therefore the roots y_2, y_3 of g are in $F(\sqrt{\delta})$, where $\delta = a^2 - 4b \in F$ is the discriminant of g. Moreover $t_1 = \alpha_1 + \alpha_2 - \alpha_3 - \alpha_4 = \sqrt{4y_1 + c_1^2 - 4c_2} \in L$, and similarly $t_2, t_3 \in L$, so $F(t_1, t_2, t_3) \subset L$, and by (12.17), $L \subset F(t_1, t_2, t_3)$, therefore

$$L = F(t_1, t_2, t_3) = F\left(\sqrt{4y_1 + c_1^2 - 4c_2}, \sqrt{4y_2 + c_1^2 - 4c_2}, \sqrt{4y_3 + c_1^2 - 4c_2}\right).$$

Since $\Delta(\theta_f) = \Delta(f) \neq 0$, there is at most one t_i equal to 0. So we can choose the numbering such that $t_1t_2 \neq 0$ (perhaps $t_3 = 0$). Since $t_1t_2t_3 = c_1^3 - 4c_1c_2 + 8c_3 \in F$, $t_3 \in F(t_1, t_2)$, so

$$L = F(t_1, t_2, t_3) = F(t_1, t_2) = F\left(\sqrt{4y_1 + c_1^2 - 4c_2}, \sqrt{4y_2 + c_1^2 - 4c_2}\right).$$

Note that $t_i^2 = 4y_i + c_1^2 - 4c_2 \in L$, so $y_i \in L$, $i = 1, 2, 3$, so $\sqrt{\delta} = y_2 - y_3 \in L$, therefore $L(\sqrt{\delta}) = L$. Consider the chain of inclusions

$$\begin{aligned} F \subset F\left(\sqrt{4y_1 + c_1^2 - 4c_2}\right) &\subset F\left(\sqrt{4y_1 + c_1^2 - 4c_2}, \sqrt{\delta}\right) \\ &\subset F\left(\sqrt{4y_1 + c_1^2 - 4c_2}, \sqrt{\delta}, \sqrt{4y_2 + c_1^2 - 4c_2}\right) = L. \end{aligned}$$

Since $4y_1 + c_1^2 - 4c_2 \in F, \delta \in F$ and $4y_2 + c_1^2 - 4c_2 \in F(\sqrt{\delta})$, the degree of each extension is 1 or 2, so

$$[L : F] \mid 8.$$

Moreover $L \supset F(\alpha_1)$, and the minimal polynomial of α_1 is f, so

$$[L : F] \geq [F(\alpha_1) : F] = \deg(f) = 4.$$

Since $|G| = [L : F]$,

$$|G| = 4 \text{ or } |G| = 8.$$

$\square$

Ex. 13.1.16 *Consider the subgroups $\langle(1\,2),(3\,4)\rangle$ and $\langle(1\,2)(3\,4),(1\,3)(2\,4)\rangle$ of S_4.*

(a) Prove that these subgroups are isomorphic but not conjugate. This shows that when classifying subgroups of a given group, it can happen that nonconjugate subgroups can be isomorphic as abstract groups.

(b) Explain why the subgroup $\langle(1\,2),(3\,4)\rangle$ isn't mentioned in Theorems 13.1.1 and 13.1.6.

Proof. (a)

$$\begin{aligned} H_1 &= \langle(1\,2),(3\,4)\rangle = \{(),(1\,2),(3\,4),(1\,2)(3\,4)\},\\ H_2 &= \langle(1\,2)(3\,4),(1\,3)(2\,4)\rangle = \{(),(1\,2)(3\,4),(1\,3)(2\,4),(1\,4)(2\,3)\} \end{aligned}$$

are both isomorphic to the Klein's group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Every conjugate of $(1\,2) \in H_1$ by $\sigma \in S_4$ is $(\sigma(1)\,\sigma(2))$, which is not in H_2. The subgroups H_1, H_2 are not conjugate.

(b) $H_1 = \langle(1\,2),(3\,4)\rangle$ is not a transitive subgroup of S_4 (the orbit of 1 is $\{1,2\}$), so isn't mentioned in Theorems 13.1.1 and 13.1.6.

$\square$

13.2 QUINTIC POLYNOMIALS

Ex. 13.2.1 *As explained in the text, we can regard $\mathrm{AGL}(1,\mathbb{F}_5)$ as a subgroup of S_5.*

(a) Prove that $\mathrm{AGL}(1,\mathbb{F}_5)$ is generated by $(1\,2\,3\,4\,5)$ and $(1\,2\,4\,3)$.

(b) Prove that $\mathrm{AGL}(1,\mathbb{F}_5) \cap A_5$ is generated by $(1\,2\,3\,4\,5)$ and $(1\,4)(2\,3)$.

(c) Prove that the group of part (b) is isomorphic to the dihedral group D_{10} of order 10.

(d) Prove that $\langle(1\,2\,3\,4\,5)\rangle, \mathrm{AGL}(1,\mathbb{F}_5) \cap A_5$, and $\mathrm{AGL}(1,\mathbb{F}_5)$ are the only subgroups of $\mathrm{AGL}(1,\mathbb{F}_5)$ containing $\langle(1\,2\,3\,4\,5)\rangle$.

Proof. (a) Let $r = \gamma_{1,1} : \mathbb{F}_5 \to \mathbb{F}_5, x \mapsto x+1$ and $s = \gamma_{2,0} : \mathbb{F}_5 \to \mathbb{F}_5, x \mapsto 2x$, corresponding to the permutations $\rho = (1\,2\,3\,4\,5)$ and $\sigma = (1\,2\,4\,3)$.

Since 2 is a generator of $\mathbb{F}_5^*$ ($2^2 \equiv -1 \mod 5$), every $a \in \mathbb{F}_p^*$ is of the form $a = 2^k,\ k \in \mathbb{N}$, so every $f \in \mathrm{AGL}(1,\mathbb{F}_5)$, defined by $x \mapsto ax+b,\ a = 2^k \in \mathbb{F}_p^*, b \in \mathbb{F}_p$ is equal to $f = r^b \circ s^k$. Therefore $\mathrm{AGL}(1,\mathbb{F}_5) = \langle r,s\rangle$, and the corresponding subgroup G of S_5, isomorphic to $\mathrm{AGL}(1,\mathbb{F}_5)$, is generated by $\rho = (1\,2\,3\,4\,5)$ and $\sigma = (1\,2\,4\,3)$.

(b) By part (a), every permutation χ of $\mathrm{AGL}(1,\mathbb{F}_5)$ is of the form $\chi = \rho^b\sigma^k,\ 0 \le b \le 4, 0 \le k \le 3$. Since $\rho \in A_5$ and $\sigma \in S_5 \setminus A_5$, $\chi \in A_5$ if and only if k is even. Moreover, since $\sigma^4 = e$, for each integer l, $\sigma^{2l} = e$ or $\sigma^{2l} = \sigma^2$, so

$$\begin{aligned}\mathrm{AGL}(1,\mathbb{F}_5) \cap A_5 &= \{\rho^k \mid 0 \le k \le 4\} \cup \{\rho^k\sigma^2 \mid 0 \le k \le 4\}\\ &= \{e, \rho, \rho^2, \rho^3, \rho^4, \sigma^2, \rho\sigma^2, \rho^2\sigma^2, \rho^3\sigma^2, \rho^4\sigma^2\}.\end{aligned}$$

Thus

$$\mathrm{AGL}(1,\mathbb{F}_5) \cap A_5 = \langle \rho, \sigma^2\rangle = \langle (1\,2\,3\,4\,5), (1\,4)(2\,3)\rangle.$$

(c) For every $x \in \mathbb{F}_p$, $(s^2 \circ r)(x) = 4(x+1)$, and $(r^{-1} \circ s^2)(x) = 4x-1 = 4x+4 = 4(x+1)$, so $s^2 \circ r = r^{-1} \circ s^2$ and $\sigma^2\rho = \rho^{-1}\sigma^2$.

Write $\sigma' = \sigma^2$. Since $\mathrm{AGL}(1,\mathbb{F}_5) \cap A_5 = \langle \rho, \sigma'\rangle$, the relations

$$\rho^5 = e, \qquad \sigma'^2 = e, \qquad \sigma'\rho = \rho^{-1}\sigma'$$

characterize the dihedral group D_{10}.

(d) Let $H \supsetneq \langle (1\,2\,3\,4\,5)\rangle$ be a subgroup of $\mathrm{AGL}(1,\mathbb{F}_5)$. By part (a), H contains an element $\rho^b\sigma^k$, with $k \in \{1,2,3\}$.

Since $\rho \in H$, $\sigma^k = \rho^{-b}(\rho^b\sigma^k) \in H$.

If $k = 1$, then $\sigma \in H$, and if $k = 3$, then $\sigma^3 = \sigma^{-1} \in H$. In both cases, $\sigma \in H$. Since $\mathrm{AGL}(1,\mathbb{F}_5)$ is generated by $\rho = (1\,2\,3\,4\,5)$ and $\sigma = (1\,2\,4\,3)$, then $H = \mathrm{AGL}(1,\mathbb{F}_5)$.

It remains the case where H contains σ^2 and doesn't contain σ. Then $H \supset \langle \rho, \sigma^2\rangle$. No element of the form $\rho^b\sigma^{2k+1}$ is in H, otherwise $\sigma \in H$, so

$$H = \langle \rho, \sigma^2\rangle = \mathrm{AGL}(1,\mathbb{F}_5) \cap A_5.$$

Thus the only subgroups of $\mathrm{AGL}(1,\mathbb{F}_5)$ containing $\langle (1\,2\,3\,4\,5)\rangle$ are

$$\langle (1\,2\,3\,4\,5)\rangle, \qquad \mathrm{AGL}(1,\mathbb{F}_5) \cap A_5, \qquad \mathrm{AGL}(1,\mathbb{F}_5).$$

□

Ex. 13.2.2 *This exercise will consider some simple properties of S_5.*

(a) Prove that $\langle (1\,2\,3\,4\,5)\rangle$ is a 5-Sylow subgroup of S_5 and more generally is a 5-Sylow subgroup of any subgroup $G \subset S_5$ containing $\langle (1\,2\,3\,4\,5)\rangle$.

(b) Prove that S_5 has twenty-four 5-cycles.

Proof. (a) As $|S_5| = 5! = 5 \cdot 24$, where $\gcd(5,24) = 1$, any subgroup of S_5 with order 5 is a 5-Sylow of S_5, so $\langle (1\,2\,3\,4\,5)\rangle$ is a 5-Sylow of S_5.

Let G be a subgroup of S_5 containing $\langle (1\,2\,3\,4\,5)\rangle$. Then 5 divides $|G|$ and $|G|$ divides $5! = 5 \cdot 24$, so $|G| = 5d$, where $d \mid 24$, thus $\gcd(5,d) = 1$. Therefore $\langle (1\,2\,3\,4\,5)\rangle$ is a 5-Sylow of G.

(b) There are $5!$ arrangements $(a_1, a_2, a_3, a_4, a_5)$, with distinct a_i in $\{1,2,3,4,5\}$. The 5 arrangements $(a_1, a_2, a_3, a_4, a_5), (a_2, a_3, a_4, a_5, a_1), \ldots$ correspond to the same permutation $(a_1\,a_2\,a_3\,a_4\,a_5)$, so there are $5!/5 = 24$ 5-cycles in S_5.

□

Ex. 13.2.3 *Let $G \subset S_5$ be transitive, and let N be the number of subgroups of G of order 5. In this exercise, you will use an argument from [Postnikov] to prove that $N = 1$ or 6 without using the Sylow Theorems. Let $C = \{\tau \in S_5 \setminus G \mid \tau \text{ is a 5-cycle}\}$.*

(a) Prove that $\sigma \cdot \tau = \sigma\tau\sigma^{-1}$ defines an action of G on C.

(b) Let $\tau \in S_5$ be a 5-cycle. Prove that $\sigma \in S_5$ satisfies $\sigma\tau\sigma^{-1} = \tau$ if and only if $\sigma \in \langle \tau \rangle$.

(c) Use parts (a) and (b) to prove that $|G|$ divides $|C|$.

(d) Prove that $4N + |C| = 24$.

(e) Use parts (c) and (d) to prove that $N = 1$ or 6.

Proof. (a) Let $\sigma \in G$ and $\tau \in S_5 \setminus G$. If $\sigma\tau\sigma^{-1} \in G$, then $\tau \in G$, in contradiction with the hypothesis. So, if $\sigma \in G$,

$$\tau \in C \Rightarrow \sigma \cdot \tau \in C.$$

Moreover, if $\sigma, \sigma' \in G$, and $\tau \in C$, then $e \cdot \tau = e\tau e^{-1} = \tau$, and

$$\sigma \cdot (\sigma' \cdot \tau) = \sigma \cdot (\sigma'\tau\sigma'^{-1}) = \sigma\sigma'\tau\sigma'^{-1}\sigma^{-1} = (\sigma\sigma') \cdot \tau.$$

Therefore $\sigma \cdot \tau = \sigma\tau\sigma^{-1}$ defines an action of G on C.

(b) Let $\tau = (a_1\, a_2\, a_3\, a_4\, a_5) \in S_5$ be a 5-cycle.

- Suppose that $\sigma \in S_5$ satisfies $\sigma\tau\sigma^{-1} = \tau$. Then $(\sigma(a_1)\, \sigma(a_2)\, \sigma(a_3)\, \sigma(a_4)\, \sigma(a_5)) = (a_1\, a_2\, a_3\, a_4\, a_5)$.
  Therefore $\sigma(a_1) \in \{a_1, a_2, a_3, a_4, a_5\}$, so $\sigma(a_1) = a_i$ for some $i \in [\![1, 5]\!]$.
  Then, for all $j \in [\![1, 5]\!]$, since $\sigma\tau = \tau\sigma$,

$$\begin{aligned}
\sigma(a_j) &= (\sigma\tau^{j-1})(a_1)\\
&= (\tau^{j-1}\sigma)(a_1)\\
&= \tau^{j-1}(a_i)\\
&= \tau^{j-1}(\tau^{i-1}(a_1))\\
&= \tau^{i-1+j-1}(a_1)\\
&= \tau^{i-1}(a_j),
\end{aligned}$$

  Since $\{a_1, a_2, a_3, a_4, a_5\} = \{1, 2, 3, 4, 5\}$, $\sigma = \tau^{i-1} \in \langle \tau \rangle$.
- Conversely, suppose that $\sigma \in \langle \tau \rangle$. Since $\langle \tau \rangle$ is cyclic, it is an Abelian subgroup, therefore $\sigma\tau = \tau\sigma$, so $\sigma\tau\sigma^{-1} = \tau$.

Conclusion: If $\tau \in S_5$ is a 5-cycle,

$$\forall \sigma \in S_5, \quad \sigma\tau\sigma^{-1} = \tau \iff \sigma \in \langle \tau \rangle.$$

(c) By part (b), the stabilizer of $\tau \in C$ in G is

$$\mathrm{Stab}_G(\tau) = \langle \tau \rangle \cap G.$$

Since $\tau \in C$, $\tau \notin G$. If $\tau^k \in G$ for some $k \in \{2,3,4\}$, since $k \wedge 5 = 1$, $uk + 5v = 1$ for some integers u, v, so $\tau = \tau^{uk}\tau^{5v} = (\tau^k)^u \in G$, which is a contradiction, so $\tau, \tau^2, \tau^3, \tau^4$ are not in G, so $\langle \tau \rangle \cap G = \{e\}$. Therefore

$$G_\tau = \mathrm{Stab}_G(\tau) = \{e\}.$$

If $\mathcal{O}_\tau$ is the orbit of τ for the action defined in part (a),

$$|\mathcal{O}_\tau| = (G : G_\tau) = |G|.$$

As $C = \coprod_{\tau \in S} \mathcal{O}_\tau$, where S is a complete system of the representatives of the orbits, if $m = |S|$ is the number of orbits, $|C| = m|G|$, so

$$|G| \text{ divides } |C|.$$

(d) By Exercise 2, S_5 has 24 5-cycles.

$$\begin{aligned}\{\tau \in S_5 \mid \tau \text{ is a 5-cycle}\} &= \{\tau \in G \mid \tau \text{ is a 5-cycle}\} \cup \{\tau \in S_5 \setminus G \mid \tau \text{ is a 5-cycle}\} \\ &= \{\tau \in G \mid \tau \text{ is a 5-cycle}\} \cup C,\end{aligned}$$

where the union is a disjoint union.

Moreover, G has N subgroups of order 5, and the intersection of two such subgroups is $\{e\}$, so G has $N \times 4$ 5-cycles. Therefore

$$24 = 4N + |C|.$$

(e) Since $G \subset S_5$ is a transitive subgroup, by Lemma 13.2.1, $5 \mid |G|$, and by part (c), $|G| \mid |C|$, so part (d) implies

$$5 \mid 24 - 4N.$$

Therefore $4N \equiv 24 \equiv 4 \pmod 5$, so $N \equiv 1 \pmod 5$, and since $4N \leq 24$, $N \leq 6$, so

$$N = 1 \text{ or } N = 6.$$

□

Ex. 13.2.4 *Prove that (13.19) gives coset representatives of* $\mathrm{AGL}(1, \mathbb{F}_5)$ *in* S_5*.*

Proof. As the index $(S_5 : \mathrm{AGL}(1, \mathbb{F}_5)) = 120/20 = 6$, it is sufficient to verify that the 6 permutations

$$S = \{e, (1\,2\,3), (2\,3\,4), (3\,4\,5), (1\,4\,5), (1\,2\,5)\}$$

are in distinct coset, by verifying that the 15 permutations $uv^{-1} \notin \mathrm{AGL}(1, \mathbb{F}_5)$, where

$$u, v \in S, \qquad u \neq v.$$

$$\begin{aligned}\mathrm{AGL}(1, \mathbb{F}_5) = \{&e, (1,2,4,3), (1,2,3,4,5), (1,3,5,2,4), (1,4,5,2), (1,3,2,5), \\ &(1,4)(2,3), (1,4,2,5,3), (2,5)(3,4), (1,5,3,4), (2,3,5,4), (1,3)(4,5), \\ &(1,3,4,2), (1,5)(2,4), (1,2)(3,5), (1,5,4,3,2), (2,4,5,3), (1,4,3,5), \\ &(1,2,5,4), (1,5,2,3)\}\end{aligned}$$

$$\{uv^{-1} \mid u \in S, v \in S, u \neq v\} =$$
$$\{(1,3,2),(2,4,3),(3,5,4),(1,5,4),(1,5,2),(1,2,3,5,4),(2,3,5),$$
$$(1,3,4),(1,5,4,2,3),(1,5,2,3,4),(1,3,4,5,2),(2,4,5),(1,5,3),$$
$$(1,5,3,4,2),(1,2,4)\}$$

Sage instructions

```
S5 = SymmetricGroup(5)
a = S5([(1,2,3,4,5)])
b = S5([(1,2,4,3)])
G = PermutationGroup([a,b])
l =  [S5([]),S5([(1,2,3)]),S5([(2,3,4)]),S5([(3,4,5)]),S5([(1,4,5)]),S5([(1,2,5)])]
[u*v^(-1) in G for u in l for v in l if u< v]
```

[False, False, ..., False]

So S is a set of coset representatives of $\mathrm{AGL}(1,\mathbb{F}_5)$ in S_5. $\square$

Ex. 13.2.5 *Complete the proof of part (b) of Theorem 13.2.6. Then prove part (c).*

Proof. • In the context of the proof of part (b) of Theorem 13.2.6, $A_5 \subset G$. Let

$$\tau_1 = e, \quad \tau_2 = (1\,2\,3), \quad \tau_3 = (2\,3\,4), \quad \tau_4 = (3\,4\,5), \quad \tau_5 = (1\,4\,5), \quad \tau_6 = (1\,2\,5),$$

and $h_i = \tau_i \cdot h,\ i = 1, \ldots, 6$, where $h = u^2$ and

$$\begin{aligned} u = {} & x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1 \\ & - x_1x_3 - x_3x_5 - x_5x_2 - x_2x_4 - x_4x_1. \end{aligned}$$

By definition,

$$\beta_i = h_i(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5).$$

Since $A_5 \subset G$ and $\tau_i \in A_5$, there exists $\sigma_i \in \mathrm{Gal}(L/F)$ such that σ_i maps to τ_i for every $i \in [\![1, 6]\!]$, so

$$\sigma_i(\alpha_j) = \alpha_{\tau_i(j)}, \qquad i \in [\![1,6]\!], \qquad j \in [\![1,5]\!].$$

Then, for all $i \in [\![1, 6]\!]$,

$$\begin{aligned} \sigma_i(\beta_1) &= \sigma_i(h(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)) \\ &= h(\sigma_i(\alpha_1), \sigma_i(\alpha_2), \sigma_i(\alpha_3), \sigma_i(\alpha_4), \sigma_i(\alpha_5)) \\ &= h(\alpha_{\tau_i(1)}, \alpha_{\tau_i(2)}, \alpha_{\tau_i(3)}, \alpha_{\tau_i(4)}, \alpha_{\tau_i(5)}) \\ &= (\tau_i \cdot h)(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5) \\ &= h_i(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5) \\ &= \beta_i \end{aligned}$$

So

$$\sigma_i(\beta_1) = \beta_i, \qquad i = 1, \ldots, 6.$$

By assumption, some β_j is in F, therefore $\beta_1 = \sigma_j^{-1}(\beta_j) = \beta_j \in F$, and $\beta_i = \sigma_i(\beta_1) = \beta_1$ for all $i \in [\![1, 6]\!]$. We obtain the identity

$$(y - \beta_1)^6 = (y^3 + b_2 y^2 + b_4 y + b_6)^2 - 2^{10}\Delta(f)y.$$

Multiplying this out, we obtain

$$y^6 - 6\beta_1 y^5 + 15\beta_1^2 y^4 - 20\beta_1^3 y^3 + 15\beta_1^4 y^2 - 6\beta_1^5 y + \beta_1^6 =$$
$$y^6 + 2b_2 y^5 + (b_2^2 + 2b_4)y^4 + (2b_6 + 2b_2 b_4)y^3 + (b_4^2 + 2b_2 b_6)y^2 + (2b_4 b_6 - 2^{10}\Delta(f))y + b_6^2,$$

so

$$\begin{aligned} -6\beta_1 &= 2b_2, \\ 15\beta_1^2 &= b_2^2 + 2b_4, \\ -20\beta_1^3 &= 2b_2 b_4 + 2b_6. \end{aligned}$$

Therefore, since F has characteristic $\neq 2$,

$$\begin{aligned} b_2 &= -3\beta_1, \\ b_4 &= \frac{1}{2}(15\beta_1^2 - 9\beta_1^2) \\ &= 3\beta_1^2, \\ b_6 &= \frac{1}{2}(-20\beta_1^3 + 18\beta_1^3) \\ &= -\beta_1^3, \end{aligned}$$

so

$$b_2 = -3\beta_1, \qquad b_4 = 3\beta_1^2, \qquad b_6 = -\beta_1^3.$$

The precedent identity becomes

$$\begin{aligned} (y - \beta_1)^6 &= (y^3 + b_2 y^2 + b_4 y + b_6)^2 - 2^{10}\Delta(f)y \\ &= (y^3 - 3\beta_1 y^2 + 3\beta_1^2 y - \beta_1^3)^2 - 2^{10}\Delta(f)y \\ &= (y - \beta_1)^6 - 2^{10}\Delta(f)y. \end{aligned}$$

Hence $2^{10}\Delta(f) = 0$. Yet F has characteristic $\neq 2$, and $\Delta(f) \neq 0$, since f is separable. This contradiction completes the proof of the theorem.

- We prove part (c) of Theorem 13.2.6.

  Suppose that G is conjugate to $\langle(1\,2\,3\,4\,5)\rangle$. Let $L = F(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)$ be the splitting field of f. We choose the numbering of the roots such that $\mathrm{Gal}(L/F) = \langle\sigma\rangle$, where σ corresponds to $(1\,2\,3\,4\,5)$.

  $[L : F] = |\mathrm{Gal}(L/F)| = 5$, so the Tower Theorem implies that $[F(\alpha) : F]$ divides 5.

  Since f is irreducible, $\alpha \notin F$, so $[F(\alpha) : F] \neq 1$, $[F(\alpha) : F] = 5$ and $L = F(\alpha)$. Therefore $\alpha_i \in F(\alpha)$, $i = 1, \ldots, 5$, and so $f = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4)(x-\alpha_5)$ splits completely over $F(\alpha)$.

  Conversely suppose that f splits completely over $F(\alpha)$. Then $\alpha_i \in F(\alpha)$, $i = 1, \ldots, 5$, so the splitting field of f is $L = F(\alpha)$. Therefore $|\mathrm{Gal}(L/F)| = [L : F] = 5$ is prime, so $\mathrm{Gal}(L/F)$ is cyclic. $G \simeq \mathrm{Gal}(L/F)$ is cyclic of order 5, so $G = \langle\tau\rangle$, where $\tau \in S_5$ is a permutation of order 5. τ is a product of disjoint cycles whose order is the least common multiple of the length of the cycles, so τ is a 5-cycle.

$G = \langle (a_1\, a_2 a_3 a_4 a_5) \rangle = \sigma \langle (1\,2\,3\,4\,5) \rangle \sigma^{-1}$, where σ is defined by $\sigma(i) = a_i$, $i = 1, \ldots, 5$. G is conjugate to $\langle (1\,2\,3\,4\,5) \rangle$.

$\square$

Ex. 13.2.6 *In this exercise, you will use Maple or Mathematica (or Sage!), to prove (13.23) and (13.24).*

(a) The first step is to enter (13.17) and call it, for example $u1$. Then use substitution commands and (13.19) to create $u2, \ldots u6$. For example, $u2$ is obtained by applying $(1\,2\,3)$ to $u1$. In Maple, this is done via the command

```
u2 := subs({x1=x2,x2=x3,x3=x1},u1);
```

whereas in Mathematica one uses

```
u2 := u1 /. {x1->x2,x2->x3,x3->x1}
```

(b) Now multiply out $\Theta(y) = (y - u1) \cdots (y - u6)$ and use the methods of section 2.3 to express the coefficients of $\Theta(y)$ in terms of the elementary symmetric polynomials.

(c) Show that your results imply (13.23) and (13.24).

Proof. Sage instructions :

```
R.<y,x,x1,x2,x3,x4,x5,y1,y2,y3,y4,y5> = PolynomialRing(QQ, order = 'degrevlex')
elt = SymmetricFunctions(QQ).e()
e = [elt([i]).expand(5).subs(x0=x1, x1=x2, x2=x3, x3 = x4, x4 = x5)
               for i in range(6)]
J = R.ideal(e[1]-y1, e[2]-y2, e[3]-y3,e[4]-y4,e[5]-y5)
G = J.groebner_basis()
u1 =x1*x2 + x2*x3 + x3*x4 + x4*x5 + x5*x1 - x1*x3 - x3*x5 -x5*x2 - x2*x4 -x4*x1
u2 = u1.subs(x1 = x2, x2 = x3, x3 = x1)
u3 = u1.subs(x2 = x3, x3 = x4, x4 = x2)
u4 = u1.subs(x3 = x4, x4 = x5, x5 = x3)
u5 = u1.subs(x1 = x4, x4 = x5, x5 = x1)
u6 = u1.subs(x1 = x2, x2 = x5, x5 = x1)
f1 = (y-u1) * (y-u2) * (y-u3) * (y-u4) * (y-u5) * (y-u6)
var('sigma_1,sigma_2,sigma_3,sigma_4,sigma_5')
g = f1.reduce(G).subs(y1=sigma_1, y2=sigma_2, y3=sigma_3, y4=sigma_4, y5= sigma_5)
h = g.collect(y);
```

Now we can verify (13.23) and (13.24):

```
h.coefficient(y^5),h.coefficient(y^3)
```

$$(0, 0)$$

```
B2 = h.coefficient(y^4); B2
```

$$-3\,\sigma_2^2 + 8\,\sigma_1\sigma_3 - 20\,\sigma_4$$

```
B4 = h.coefficient(y^2); B4
```

$$3\,\sigma_2^4 - 16\,\sigma_1\sigma_2^2\sigma_3 + 16\,\sigma_1^2\sigma_3^2 + 16\,\sigma_1^2\sigma_2\sigma_4 - 64\,\sigma_1^3\sigma_5 + 16\,\sigma_2\sigma_3^2 - 8\,\sigma_2^2\sigma_4 \\ - 112\,\sigma_1\sigma_3\sigma_4 + 240\,\sigma_1\sigma_2\sigma_5 + 240\,\sigma_4^2 - 400\,\sigma_3\sigma_5$$

```
B6 = h.subs(y = 0);B6
```

$$- \sigma_2^6 + 8\,\sigma_1\sigma_2^4\sigma_3 - 16\,\sigma_1^2\sigma_2^2\sigma_3^2 - 16\,\sigma_1^2\sigma_2^3\sigma_4 + 64\,\sigma_1^3\sigma_2\sigma_3\sigma_4 \\ - 64\,\sigma_1^4\sigma_4^2 - 16\,\sigma_2^3\sigma_3^2 + 64\,\sigma_1\sigma_2\sigma_3^3 + 28\,\sigma_2^4\sigma_4 - 112\,\sigma_1\sigma_2^2\sigma_3\sigma_4 - 128\,\sigma_1^2\sigma_3^2\sigma_4 + 224\,\sigma_1^2\sigma_2\sigma_4^2 \\ + 48\,\sigma_1\sigma_2^3\sigma_5 - 192\,\sigma_1^2\sigma_2\sigma_3\sigma_5 + 384\,\sigma_1^3\sigma_4\sigma_5 - 64\,\sigma_3^4 + 224\,\sigma_2\sigma_3^2\sigma_4 - 176\,\sigma_2^2\sigma_4^2 - 64\,\sigma_1\sigma_3\sigma_4^2 \\ - 80\,\sigma_2^2\sigma_3\sigma_5 + 640\,\sigma_1\sigma_3^2\sigma_5 - 640\,\sigma_1\sigma_2\sigma_4\sigma_5 - 1600\,\sigma_1^2\sigma_5^2 + 320\,\sigma_4^3 - 1600\,\sigma_3\sigma_4\sigma_5 + 4000\,\sigma_2\sigma_5^2$$

The coefficient c_1 of y in $h = \Theta(y)$ is not symmetric in $x_1, \ldots, x_5$, but we verify that $c_1 = 2^5\sqrt{\Delta}\, y$, computing first $\sqrt{\Delta}$:

```
c1  = f1.coefficient(y)
x = [1,x1,x2,x3,x4,x5]
sqrtDelta = 1
for i in range(1,6):
    for j in range(i+1,6):
        sqrtDelta *= (x[i] -x[j])
sqrtDelta
c1 + 2^5 * sqrtDelta
```

$$0$$

So (13.23) and (13.24) are verified. $\square$

Ex. 13.2.7 *Consider* $\mathrm{AGL}(1, \mathbb{F}_5) \cap A_5 \subset S_5$*, and let* u *be defined as in (13.17).*

(a) Prove that the symmetry group of u *is* $\mathrm{AGL}(1, \mathbb{F}_5) \cap A_5$.

(b) Prove that (13.19) gives coset representatives of $\mathrm{AGL}(1, \mathbb{F}_5) \cap A_5$ *in* A_5.

Proof. (a) Let G be the symmetry group of u.

- If $\sigma \in G$, then $\sigma \cdot u = u$, therefore $\sigma \cdot h = \sigma \cdot u^2 = u^2 = h$. By Lemma 13.2.4, $\sigma \in \mathrm{AGL}(1, \mathbb{F}_5)$, so $G \subset \mathrm{AGL}(1, \mathbb{F}_5)$. $G \neq \mathrm{AGL}(1, \mathbb{F}_5)$, otherwise $(1\,2\,4\,3) \in G$, but $(1\,2\,4\,3) \cdot u = -u \neq u$ (see (13.2.B)). Therefore $G \subsetneq \mathrm{AGL}(1, \mathbb{F}_5)$.
  Moreover $(1\,2\,3\,4\,5)\cdot u = u$, so $\langle (1\,2\,3\,4\,5)\rangle \subset G$ and G is transitive. By Theorem 13.2.2,
  $$G \subset \mathrm{AGL}(1, \mathbb{F}_5) \cap A_5.$$
- If $\chi \in \mathrm{AGL}(1, \mathbb{F}_5) \cap A_5$, by Exercise 1 part (b),
  $$\chi = (1\,2\,3\,4\,5)^k[(1\,4)(2\,3)]^l, \qquad k, l \in \mathbb{N}.$$
  $(1\,2\,3\,4\,5)\cdot u = u$ and $(1\,2\,4\,3)\cdot u = -u$, therefore $(1\,4)(2\,3)\cdot u = (1\,2\,4\,3)^2\cdot u = u$. Thus $\chi \in G$.
  $$G = \mathrm{AGL}(1, \mathbb{F}_5) \cap A_5.$$

(b) In Exercise 4, we verified that for $u, v \in S, u \neq v$, with

$$S = \{e, (1\,2\,3), (2\,3\,4), (3\,4\,5), (1\,4\,5), (1\,2\,5)\} \subset A_5,$$

then $uv^{-1} \notin \mathrm{AGL}(1, \mathbb{F}_5)$, a fortiori $uv^{-1} \notin \mathrm{AGL}(1, \mathbb{F}_5) \cap A_5$.

Moreover the index $(A_5 : \mathrm{AGL}(1, \mathbb{F}_5) \cap A_5) = 60/10 = 6$, so S is a complete system of coset representatives of $\mathrm{AGL}(1, \mathbb{F}_5) \cap A_5$ in A_5.

□

Ex. 13.2.8 *Let $u_1, \ldots, u_6$ be as in the proof of Proposition 13.2.5, and let $\tau \in S_5$ be a transposition.*

(a) For each i, prove that $\tau \cdot u_i = -u_j$ for some j.

(b) Let $\Theta(y) = \prod_{i=1}^{6}(y - u_i)$ and write this polynomial as

$$\Theta(y) = y^6 + B_1 y^5 + B_2 y^4 + B_3 y^3 + B_4 y^2 + B_5 y + B_6.$$

Use part (a) to show that $\tau \cdot B_i = (-1)^i B_i$ for $i = 1, \ldots, 6$.

(c) Explain how part (b) and the results of Chapter 2 imply that the coefficients B_2, B_4, B_6 are polynomials in $\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5$. This explains why the formulas (13.24) exist.

(d) Use Exercise 3 of Section 7.4 to show that the coefficients B_1, B_3, B_5 must be of the form $B\sqrt{\Delta}$, where B is a polynomial in $\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5$.

(e) Note that $\sqrt{\Delta}$ has degree 10 as a polynomial in x_1, x_2, x_3, x_4, x_5. By considering the degrees of B_1, B_3, B_5 as polynomials in x_1, x_2, x_4, x_4, x_5, show that part (d) implies that $B_1 = B_3 = 0$ and that B_5 is a constant multiple of $\sqrt{\Delta}$. This explains (13.23).

Proof. (a) Let $\tau \in S_5 \setminus A_5$ be a transposition, and write $\sigma = (1\,2\,4\,3) \in S_5 \setminus A_5$. We know that $\sigma \cdot u = -u$.

Since $\sigma \in S_5 \setminus A_5$, S_5 is the disjoint union $S_5 = A_5 \cup A_5\sigma$, so $S_5 \setminus A_5 = A_5\sigma$. Since $\tau\tau_i \in S_5 \setminus A_5$, then $\tau\tau_i \in A_5\sigma$, so

$$\tau\tau_i = \psi\sigma, \qquad \psi \in A_5.$$

By Exercise 7, $\{\tau_1, \tau_2, \cdots, \tau_6\} = \{e, (1\,2\,3), (2\,3\,4), (3\,4\,5), (1\,4\,5), (1\,2\,5)\}$ is a complete system of coset representatives of $\mathrm{AGL}(1, \mathbb{F}_5) \cap A_5$ in A_5. Therefore

$$\psi = \tau_j\varphi, \qquad j \in [\![1, 6]\!], \qquad \varphi \in \mathrm{AGL}(1, \mathbb{F}_5) \cap A_5.$$

Since $\varphi \in \mathrm{AGL}(1, \mathbb{F}_5) \cap A_5$, by Exercise 7 part (a), $\varphi \cdot u = u$. Therefore

$$\begin{aligned}
\tau \cdot u_i &= (\tau\tau_i) \cdot u \\
&= (\tau_j\varphi\sigma) \cdot u \\
&= -(\tau_j\varphi) \cdot u = -\tau_j u = -u_j
\end{aligned}$$

For each $i \in [\![1, 6]\!]$, there exists $j \in [\![1, 6]\!]$ such that $\tau \cdot u_i = -u_j$.

(b) Let

$$\Theta(y) = \prod_{i=1}^{6}(y-u_i) = y^6 + B_1y^5 + B_2y^4 + B_3y^3 + B_4y^2 + B_5y + B_6.$$

Note that if $\tau \cdot u_i = \tau \cdot u_j$, $i,j \in [\![1,6]\!]$, then $\tau^2 \cdot u_i = \tau^2 \cdot u_j$, so $u_i = u_j$ and $i = j$. Therefore τ maps the set $\{u_1,\ldots,u_6\}$ on $\{-u_1,\ldots,-u_6\}$. Consequently

$$\begin{aligned}\tau \cdot \Theta(y) &= \prod_{i=1}^{6}(y - \tau \cdot u_i)\\ &= \prod_{j=1}^{6}(y+u_j)\\ &= y^6 - B_1y^5 + B_2y^4 - B_3y^3 + B_4y^2 - B_5y + B_6\end{aligned}$$

Since

$$\tau \cdot \Theta(y) = y^6 + \tau \cdot B_1y^5 + \tau \cdot B_2y^4 + \tau \cdot B_3y^3 + \tau \cdot B_4y^2 + \tau \cdot B_5y + \tau \cdot B_6,$$

we conclude

$$\tau \cdot B_i = (-1)^i B_i, \qquad i = 1,\ldots,6.$$

(c) For $i = 2,4,6$, $\tau \cdot B_i = B_i$ for every transposition τ. Since every $\sigma \in S_5$ is a product of transpositions, for all $\sigma \in S_5$, $\sigma \cdot B_i = B_i$, where $B_i \in F[x_1,\ldots,x_5]$, therefore $B_i \in F[\sigma_1,\ldots,\sigma_5]$.

B_2, B_4, B_6 are polynomials in $\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5$.

(d) For $i = 1,3,5$, $\tau \cdot B_i = -B_i$, thus B_i is invariant under A_5. Since the characteristic of F is not 2, by Exercise 7.4.3, $B_i = C_i + D_i\sqrt{\Delta}$, where C_i, D_i are polynomials in the σ_i. Then $-C_i - D_i\sqrt{\Delta} = -B_i = \tau \cdot B_i = C_i - D_i\sqrt{\Delta}$, so $C_i = 0$.

$$B_i = D_i\sqrt{\Delta}, \qquad D_i \in F[\sigma_1,\ldots,\sigma_5] \qquad \text{for } i = 1,3,5.$$

(e) Since $\sqrt{\Delta} = \prod_{1\le i<j\le 5}(x_i - x_j)$, $\sqrt{\Delta}$ has degree $1+2+3+4 = 10$ as a polynomial in x_1,x_2,x_3,x_4,x_5. $B_1 = u_1+u_2+u_3+u_4+u_5$, with $\deg(u_i) = 2$, thus $\deg(D_1\sqrt{\Delta}) \le 2$. Therefore $D_1 = 0$.

$B_3 = u_1u_2u_3 + \cdots$, so $\deg(B_3) = \deg(D_3\sqrt{\Delta}) \le 6$. Therefore $D_3 = 0$, and $B_3 = 0$.

$B_5 = u_1u_2u_3u_4u_5 + \cdots$, so $\deg(B_5) \le 10$. Therefore $\deg(D_5) \le 0$, so $D_5 = c \in F$ is a constant.

$$\Theta(y) = y^6 + B_2y^4 + B_4y^2 + B_6 + c\sqrt{\Delta}y, \qquad B_2,B_4,B_6 \in F[\sigma_1,\ldots,\sigma_5], \qquad c \in F.$$

By Exercise 7, $c = -2^5$.

□

Ex. 13.2.9 *This exercise will prove the first equivalence of Proposition 13.2.7.*

(a) *First suppose that $\theta_f(y)$ is irreducible. Prove that $|G|$ is divisible by 6, and explain why this implies that $A_5 \subset G$.*

(b) *Now suppose that $A_5 \subset G$. Prove that* $\mathrm{Gal}(L/F)$ *acts transitively on $\beta_1, \ldots, \beta_6$. However, we don't know that $\beta_1, \ldots, \beta_6$ are distinct.*

(c) *Let $p(y)$ be the minimal polynomial of β_1 over F. By part (b), it is also the minimal polynomial of $\beta_2, \ldots, \beta_6$. Prove that $\theta_f(y) = p(y)^m$, where $m = 1, 2, 3,$ or 6. The proof of Theorem 13.2.6 shows that $m = 6$ cannot occur, and $m = 1$ implies that $\theta_f(y)$ is irreducible over F. It remains to consider what happens when $m = 2$ or 3.*

(d) *Show that $(y^3 + ay^2 + by + c)^2 = \theta_f(y)$ implies that $\Delta(f) = 0$. Hence this case can't occur.*

(e) *Show that $(y^2 + ay + b)^3 = \theta_f(y)$ implies that $4b = a^2$, and then use this to show that $\Delta(f) = 0$.*

Proof. (a) Suppose that $\theta_f(y) = \prod_{i=1}^6 (y - \beta_i)$ is irreducible over F. Then $\theta_f(y)$ is the minimal polynomial of $\beta_1 = h(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)$ over F. Therefore

$$[F(\beta_1) : F] = \deg \theta_f(y) = 6.$$

Since $\beta_1 = h(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5) \in F(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5) = L$,

$$F \subset F(\beta_1) \subset F(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5) = L.$$

By the Tower Theorem,

$$[F(\beta_1) : F] \mid [L : F],$$

therefore

$$6 \mid [L : F] = |\mathrm{Gal}(L/F)| = |G|.$$

Since $6 \nmid |\mathrm{AGL}(1, \mathbb{F}_5)| = 20$, G is not a subgroup of $\mathrm{AGL}(1, \mathbb{F}_5)$. By Theorem 13.2.2, since G is a transitive subgroup of S_5, $G = A_5$ or $G = S_5$:

$$A_5 \subset G.$$

(b) Now suppose that $A_5 \subset G$. Then

$$G \supset \{\tau_1, \ldots, \tau_6\} = \{e, (1\,2\,3), (2\,3\,4), (3\,4\,5), (1\,4\,5), (1\,2\,5)\},$$

so $\tau_i \in G$ and the corresponding σ_i are in $\mathrm{Gal}(L/F)$. By Exercise 13.2.5, $\sigma_i(\beta_1) = \beta_i$, thus the orbit of β_1 under the action of $\mathrm{Gal}(L/F)$ is $\mathcal{O}_{\beta_1} = \{\beta_1, \ldots, \beta_6\}$. This is sufficient to prove that $\mathrm{Gal}(L/F)$ acts transitively on $\beta_1, \ldots, \beta_6$.

(c) Let $p(y)$ be the minimal polynomial of β_1 over F. There exists $\sigma_i \in \mathrm{Gal}(L/F)$ such that $\sigma_i(\beta_1) = \beta_i$, and since $p(y) \in F[y]$, $0 = \sigma_i(p(\beta_1)) = p(\sigma_i(\beta_1)) = p(\beta_i)$, so β_i is a root of p, where p is irreducible. Therefore p is the minimal polynomial over F of $\beta_1, \ldots, \beta_6$.

Under the hypothesis of Theorem 13.2.7 (and 13.2.6), $F \subset L$ is a separable extension, so β_1 is separable, therefore

$$p(x) = (x - \gamma_1) \cdots (x - \gamma_r),$$

where $\gamma_1, \ldots, \gamma_r$ are distinct. Since p is the minimal polynomial over F of $\beta_1, \ldots, \beta_6$, each β_j is a γ_i for some $i, 1 \leq i \leq r$, and since $p(y)$ divides $\theta_f(y)$, each γ_i is a β_j, so $\{\gamma_1, \ldots, \gamma_r\} = \{\beta_1, \ldots, \beta_6\}$, and $\gamma_1, \ldots, \gamma_r$ are the distinct roots of $\theta_f(y)$.

Let k_i the order of multiplicity of β_i in $\theta_f(y)$, so $\theta_f(y) = (y - \beta_i)^{k_i} q_i(y)$, $q_i(y) \in L[y]$. Let $\sigma \in \mathrm{Gal}(L/F)$ such that $\sigma(\beta_i) = \beta_j$. Applying σ to $\theta_f(y)$, we obtain $\theta_f(y) = (y - \beta_j)^{k_i} (\sigma \cdot q_i)(y)$, so $k_j \geq k_i$, and similarly $k_i \geq k_j$, so the distinct γ_i have the same order of multiplicity m in $\theta_f(y)$. Therefore

$$\theta_f(y) = (x - \gamma_1)^m \cdots (x - \gamma_r)^m = p(y)^m.$$

Since $6 = \deg(\theta_f(y)) = m \deg(p(y))$, $m \mid 6$, so $m = 1, 2, 3$ or 6.

$m = 6$ gives $\theta_f(y) = (x - \beta_1)^6$. Since the characteristic of f is not 2, this is impossible by the proof of Theorem 13.2.6. It remains to prove the impossibility of $m = 2$ or $m = 3$.

(d) If $m = 2$,

$$\theta_f(y) = (y^3 + ay^2 + by + c)^2, \qquad a, b, c \in F.$$

By Proposition 13.2.5, this gives

$$(y^3 + b_2 y^2 + b_4 y + b_6)^2 - 2^{10} \Delta(f) y = (y^3 + ay^2 + by + c)^2,$$

so

$$\begin{aligned} 2^{10}\Delta(f) y &= (y^3 + b_2 y^2 + b_4 y + b_6)^2 - (y^3 + ay^2 + by + c)^2 \\ &= [(b_2 - a)y^2 + (b_4 - b)y + (b_6 - c)][2y^3 + (b_2 + a)y^2 + (b_4 + b)y + (b_6 + c)] \end{aligned}$$

Therefore the coefficient in y^5 is $2(b_2 - a) = 0$. Since the characteristic is not 2,

$$b_2 = a.$$

Using $b_2 = a$, the coefficient in y^4 is $2(b_4 - b) = 0$, so

$$b_4 = b,$$

and then the coefficient in y^3 is $2(b_6 - c)$, so

$$b_6 = c.$$

Therefore $2^{10}\Delta(f) y = 0$. Since the characteristic is not 2, $\Delta(f) = 0$, in contradiction with the assumed separability of f.

(e) If $m = 3$, there exist coefficients $a, b \in F$ such that

$$\theta_f(y) = (y^2 + ay + b)^3 = (y^3 + b_2 y^2 + b_4 y + b_6)^2 - 2^{10}\Delta(f) y.$$

$$\begin{aligned} 0 = \theta_f(y) - (y^2 + ax + b)^3 = {} & -(3\,a - 2\,b_2) y^5 - \big(3\,a^2 - b_2^2 + 3\,b - 2\,b_4\big) y^4 \\ & - \big(a^3 + 6\,ab - 2\,b_2 b_4 - 2\,b_6\big) y^3 - \big(3\,a^2 b + 3\,b^2 - b_4^2 - 2\,b_2 b_6\big) y^2 \\ & - \big(3\,ab^2 - 2\,b_4 b_6 + 1024\,\Delta(f)\big) y - b^3 + b_6^2. \end{aligned}$$

We obtain b_2, b_4, b_6 with the equations corresponding to the coefficients of y^5, y^4, y^3:

$$\begin{cases} 0 & = -3\,a + 2\,b_2, \\ 0 & = -3\,a^2 + b_2^2 - 3\,b + 2\,b_4, \\ 0 & = -a^3 - 6\,ab + 2\,b_2 b_4 + 2\,b_6, \end{cases}$$

which gives

$$b_2 = \frac{3}{2}\,a, \qquad b_4 = \frac{3}{8}\,a^2 + \frac{3}{2}\,b, \qquad b_6 = -\frac{1}{16}\,a^3 + \frac{3}{4}\,ab.$$

If we substitute these values in the coefficient of y^3, we obtain

$$\begin{aligned} a^3 + 6\,ab - 2\,b_2 b_4 - 2\,b_6 &= a^3 + 6\,ab - 2\left(\frac{3}{2}\,a\right)\left(\frac{3}{8}\,a^2 + \frac{3}{2}\,b\right) + 2\left(\frac{1}{16}\,a^3 + \frac{3}{4}\,ab\right) \\ &= 0. \end{aligned}$$

The coefficient of y^2 gives $-\frac{3}{64}\left(a^4 - 8\,a^2 b + 16\,b^2\right) = -\frac{3}{64}(a^2 - 4b)^2 = 0$.
If we suppose that the characteristic is not 3, then

$$a^2 = 4b.$$

The coefficient of y gives

$$\begin{aligned} 0 &= -\frac{3}{64}\,a^5 + \frac{3}{8}\,a^3 b - \frac{3}{4}\,ab^2 - 2^{10}\,\Delta(f) \\ &= -\frac{3}{64}\,a\left(a^2 - 4b\right)^2 - 2^{10}\,\Delta(f) \\ &= -2^{10}\,\Delta(f) \end{aligned}$$

Therefore

$$\Delta(f) = 0.$$

Since f is separable, this is a contradiction, so $\theta_f(y)$ is irreducible.
It remains the case where the characteristic is 3. Then the equation

$$\theta_f(y) = (y^2 + ay + b)^3 = (y^3 + b_2 y^2 + b_4 y + b_6)^2 - 2^{10}\Delta(f)y$$

gives the system

$$\begin{cases} 0 & = 2\,b_2, \\ 0 & = b_2^2 + 2\,b_4, \\ 0 & = -a^3 + 2\,b_2 b_4 + 2\,b_6, \end{cases}$$

Therefore $b_2 = b_4 = 0$, so the initial equation gives

$$y^6 + a^3 y^3 + b^3 = y^6 + 2b_6 y^3 - 2^{10}\Delta(f)y + b_6^2,$$

and we have the same contradiction $\Delta(f) = 0$, and the same conclusion:

$$\theta_f(y) \text{ is irreducible over } F.$$

We give here the corresponding Sage instructions:

```
y,b2,b4,b6,Delta,a,b,c = var('y,b2,b4,b6,Delta,a,b,c')
u = (y^3+b2*y^2+b4*y+b6)^2 - 2^10*Delta*y - (y^2+a*y+b)^3
u = u.expand().collect(y); u
```

$$-(3\,a - 2\,b_2)y^5 - \left(3\,a^2 - b_2^2 + 3\,b - 2\,b_4\right)y^4 - \left(a^3 + 6\,ab - 2\,b_2b_4 - 2\,b_6\right)y^3 - b^3 \\ -\left(3\,a^2b + 3\,b^2 - b_4^2 - 2\,b_2b_6\right)y^2 + b_6^2 - \left(3\,ab^2 - 2\,b_4b_6 + 1024\,\Delta\right)y$$

```
eq = [u.coefficient(y^i) for i in range(3,6)]
solve(eq,b2,b4,b6)
```

$$\left[\left[b_2 = \frac{3}{2}\,a, b_4 = \frac{3}{8}\,a^2 + \frac{3}{2}\,b, b_6 = -\frac{1}{16}\,a^3 + \frac{3}{4}\,ab\right]\right]$$

```
v = u.coefficient(y^3)
w = v.subs(b2 == 3/2*a, b4 == 3/8*a^2 + 3/2*b, b6 == -1/16*a^3 + 3/4*a*b)
w.expand()
```

$$0$$

```
s = u.coefficient(y^2)
t = s.subs(b2 == 3/2*a, b4 == 3/8*a^2 + 3/2*b, b6 == -1/16*a^3 + 3/4*a*b)
t.expand().factor()
```

$$-\frac{3}{64}\left(a^2 - 4\,b\right)^2$$

```
p = u.coefficient(y)
q = p.subs(b2 == 3/2*a, b4 == 3/8*a^2 + 3/2*b, b6 == -1/16*a^3 + 3/4*a*b)
q.expand()
```

$$-\frac{3}{64}\,a^5 + \frac{3}{8}\,a^3b - \frac{3}{4}\,ab^2 - 1024\,\Delta$$

```
q.expand().subs(b = a^2/4)
```

$$-1024\Delta$$

We obtained $\Delta(f) = 0$.

□

Ex. 13.2.10 *This exercise will prove the second equivalence of Proposition 13.2.7. Note that one direction follows trivially from Theorem 13.2.6. So we can assume that $G \subset \mathrm{AGL}(1, \mathbb{F}_5)$ and that $\theta_f(y) = (y - \beta_1)g(y)$ where $\beta_1 \in F$.*

(a) *Use $(1\,2\,3\,4\,5) \in G$ to prove that $\mathrm{Gal}(L/F)$ acts transitively on $\beta_2, \dots, \beta_6$. As in the previous exercise, we don't know if $\beta_2, \dots, \beta_6$ are distinct.*

(b) *Let $p(y)$ be the minimal polynomial of β_2 over F. By part (a), it is also the minimal polynomial of $\beta_2, \dots, \beta_6$. Prove that $\theta_f(y) = (y - \beta_1)p(y)^m$, where $m = 1$ or 5. If $m = 1$, then we are done. So we need to rule out $m = 5$.*

(c) *Show that $(y - \beta_1)(y - \beta_2)^5 = \theta_f(y)$ implies that $\beta_1 = \beta_2$, and then use this to show that $\Delta(f) = 0$.*

Proof. If $\theta_f(y)$ has a root $\beta \in F$, then by Theorem 13.2.6(b), G is conjugate to a subgroup of $\mathrm{AGL}(1, \mathbb{F}_5)$.

Conversely, assume that G is conjugate to a subgroup of $\mathrm{AGL}(1, \mathbb{F}_5)$. Relabeling the roots, we may assume that $\langle (1\,2\,3\,4\,5) \rangle \subset G \subset \mathrm{AGL}(1, \mathbb{F}_5)$, and by Theorem 13.2.6(b), $\theta_f(y)$ has a root $\beta_1 \in F$, so $\theta_f(y) = (y - \beta_1)g(y)$.

(a) Write $\rho = (1\,2\,3\,4\,5)$ and $\tilde{\rho} \in \mathrm{Gal}(L/F)$ the corresponding automorphism. Then

$$\tilde{\rho}(\alpha_1) = \alpha_2, \ \dots, \quad \tilde{\rho}(\alpha_4) = \alpha_5, \quad \tilde{\rho}(\alpha_5) = \alpha_1,$$

and $\sigma_i \in \mathrm{Gal}(L/F)$ corresponds to τ_i.

We name the left coset representatives of $\mathrm{AGL}(1, \mathbb{F}_5)$ given in S_5:

$$\tau_1 = e, \ \tau_2 = (1\,2\,3), \ \tau_3 = (2\,3\,4), \ \tau_4 = (3\,4\,5), \ \tau_5 = (1\,4\,5), \ \tau_6 = (1\,2\,5).$$

Note that these cosets representatives verify $\rho\tau_1\rho^{-1} = \tau_1 = e$, and

$$\rho\tau_2\rho^{-1} = \tau_3, \quad \cdots, \quad \rho\tau_5\rho^{-1} = \tau_6, \quad \rho\tau_6\rho^{-1} = \tau_2.$$

By definition, $h_i = \tau_i \cdot h, \ i = 1, \dots, 6$, where $h = u^2$ and u is given in (13.17), and

$$\sigma_i(\beta_1) = (\tau_i \cdot h)(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5) = \beta_i$$

(see Exercise 13.2.5). Since $\rho \in \mathrm{AGL}(1, 5)$, $\rho \cdot h = h$, therefore, for $2 \le i \le 5$

$$(\rho\tau_i) \cdot h = (\rho\tau_i\rho^{-1}) \cdot (\rho \cdot h) = \tau_{i+1} \cdot h,$$

and $(\rho\tau_6) \cdot h = \tau_2 \cdot h$.

If $\tilde{\varphi} \in \mathrm{Gal}(L/F)$ corresponds to some $\varphi \in S_5$, then $\tilde{\varphi}(\alpha_i) = \alpha_{\varphi(i)}, \ i = 1, \dots, 5$, so

$$\tilde{\varphi}(h(\alpha_1, \dots, \alpha_5)) = h(\alpha_{\varphi(1)}, \dots, \alpha_{\varphi(5)}) = (\varphi \cdot h)(\alpha_1, \dots, \alpha_5).$$

Since $\tilde{\rho} \circ \sigma_i \in \mathrm{Gal}(L/F)$ corresponds to $\rho\tau_i$,

$$\begin{aligned}
\tilde{\rho}(\beta_i) &= \tilde{\rho}(\sigma_i(\beta_1)) \\
&= (\tilde{\rho} \circ \sigma_i)(h(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)) \\
&= [(\rho\,\tau_i) \cdot h](\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5) \\
&= [(\rho\tau_i\rho^{-1}) \cdot (\rho \cdot h)](\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5) \\
&= (\tau_{i+1} h)(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5) \\
&= \beta_{i+1}, \qquad i = 2, 3, 4, 5,
\end{aligned}$$

and similarly $\tilde{\rho}(\beta_6) = \beta_2$. So the images of β_i by the automorphism $\tilde{\rho}$ corresponding to $\rho = (1\,2\,3\,4\,5)$ are given by

$$\beta_2 \mapsto \beta_3 \mapsto \beta_4 \mapsto \beta_5 \mapsto \beta_6 \mapsto \beta_2, \qquad \beta_1 \mapsto \beta_1,$$

therefore $\mathrm{Gal}(L/F)$ acts transitively on $\beta_2, \ldots, \beta_6$.

(b) Let $p(y) \in F[y]$ be the minimal polynomial of β_2 over F. Since $\tilde{\rho} \in \mathrm{Gal}(L, F)$, $p(\beta_3) = p(\tilde{\rho}(\beta_2)) = \tilde{\rho}(p(\beta_2)) = 0$, so β_3, and similarly $\beta_4, \beta_5, \beta_6$ are roots of p, so p is the minimal polynomial of $\beta_2, \ldots, \beta_6$.

$\theta_f(y) = (y - \beta_1)g(y)$, therefore $g(y) \in F[y]$.

$F \subset L$ is a separable extension, so β_2 is separable, therefore

$$p(y) = (y - \gamma_1) \cdots (y - \gamma_r),$$

where $\gamma_1, \ldots, \gamma_r$ are distinct. As p is the minimal polynomial of β_2 over F, and $g(\beta_2) = 0$, with $g \in F[y]$, $p(y)$ divides $\theta_f(y)$, so each γ_i is a β_j, and each β_j, $2 \leq j \leq j$, is a root of p so is a γ_i. Therefore $\{\gamma_1, \ldots, \gamma_r\} = \{\beta_2, \ldots, \beta_6\}$, and $\gamma_1, \ldots, \gamma_r$ are the distinct roots of g.

Since $\mathrm{Gal}(L/F)$ acts transitively on $\beta_2, \ldots, \beta_6$, then the distinct roots $\gamma_1, \cdots, \gamma_r$ have the same order of multiplicity m (as in Exercise 9). Therefore $g(y) = p(y)^m$, so

$$\theta_f(y) = (y - \beta_1)p(y)^m.$$

Since $5 = \deg(g) = m \deg(p)$, $5 \mid m$, so $m = 1$ or $m = 5$. We need to rule out $m = 5$.

(c) If $m = 5$,

$$\theta_f(y) = (y - \beta_1)(y - \beta_2)^5.$$

Then, with some formal computations,

$$\begin{aligned}
0 &= (y^3 + b_2 y^2 + b_4 y + b_6)^2 - 2^{10}\Delta(f)y - (y - \beta_1)(y - \beta_2)^5 \\
&= (2\,b_2 + \beta_1 + 5\,\beta_2)y^5 + \big(b_2^2 - 5\,\beta_1\beta_2 - 10\,\beta_2^2 + 2\,b_4\big)y^4 + 2\,\big(5\,\beta_1\beta_2^2 + 5\,\beta_2^3 + b_2 b_4 + b_6\big)y^3 \\
&\quad - \big(10\,\beta_1\beta_2^3 + 5\,\beta_2^4 - b_4^2 - 2\,b_2 b_6\big)y^2 + \big(5\,\beta_1\beta_2^4 + \beta_2^5 + 2\,b_4 b_6 - 1024\,\Delta(f)\big)y - \beta_1\beta_2^5 + b_6^2.
\end{aligned}$$

The coefficients of y^5, y^4, y^3 give

$$\begin{aligned}
0 &= 2\,b_2 + \beta_1 + 5\,\beta_2, \\
0 &= b_2^2 - 5\,\beta_1\beta_2 - 10\,\beta_2^2 + 2\,b_4, \\
0 &= 10\,\beta_1\beta_2^2 + 10\,\beta_2^3 + 2\,b_2 b_4 + 2\,b_6,
\end{aligned}$$

so

$$\begin{aligned}
b_2 &= -\frac{1}{2}\,\beta_1 - \frac{5}{2}\,\beta_2, \\
b_4 &= -\frac{1}{8}\,\beta_1^2 + \frac{5}{4}\,\beta_1\beta_2 + \frac{15}{8}\,\beta_2^2, \\
b_6 &= -\frac{1}{16}\,\beta_1^3 + \frac{5}{16}\,\beta_1^2\beta_2 - \frac{15}{16}\,\beta_1\beta_2^2 - \frac{5}{16}\,\beta_2^3.
\end{aligned}$$

Substituting these values in the equation, we obtain

$$0 = ay^2 + by + c,$$

where

$$\begin{aligned}
a &= \frac{5}{64}(\beta_1^4 - 4\,\beta_1^3\beta_2 + 6\,\beta_1^2\beta_2^2 - 4\,\beta_1\beta_2^3 + \beta_2^4) = \frac{5}{64}(\beta_1 - \beta_2)^4,\\
b &= \frac{1}{64}\,\beta_1^5 - \frac{15}{64}\,\beta_1^4\beta_2 + \frac{25}{32}\,\beta_1^3\beta_2^2 - \frac{35}{32}\,\beta_1^2\beta_2^3 + \frac{45}{64}\,\beta_1\beta_2^4 - \frac{11}{64}\,\beta_2^5 - 1024\,\Delta(f),\\
c &= \frac{1}{256}\,\beta_1^6 - \frac{5}{128}\,\beta_1^5\beta_2 + \frac{55}{256}\,\beta_1^4\beta_2^2 - \frac{35}{64}\,\beta_1^3\beta_2^3 + \frac{175}{256}\,\beta_1^2\beta_2^4 - \frac{53}{128}\,\beta_1\beta_2^5 + \frac{25}{256}\,\beta_2^6.
\end{aligned}$$

Since $a = 0$, if the characteristic is not 5, then $\beta_1 = \beta_2$, so $\theta_f(y) = (y - \beta_1)^6$. But the proof of Theorem 13.2.6 shows that this implies that $\Delta(f) = 0$, and this is a contradiction. Thus $m = 1$ and g is irreducible over F. This proves Proposition 13.2.7. in characteristic $\neq 5$.

Sage instructions for part (e):

```
x,y,beta1,beta2,Delta,b2,b4,b6 = var('x,y,beta1,beta2,Delta,b2,b4,b6')
p = (y^3 + b2*y^2 + b4*y + b6)^2 - 2^10*Delta*y - (y-beta1)*(y-beta2)^5
p = p.expand().collect(y)
R.<y>=QQ[]
l = [p.coefficient(y,i) for i in range(5,-1,-1)]
eq = l[:3]
solve(eq,b2,b4,b6)
q=p.subs(b2 == -1/2*beta1 - 5/2*beta2,
      b4 == -1/8*beta1^2 + 5/4*beta1*beta2 + 15/8*beta2^2,
      b6 == -1/16*beta1^3 + 5/16*beta1^2*beta2 -15/16*beta1*beta2^2 - 5/16*beta2
q=q.expand().collect(y)
q.coefficient(y,2).factor()
```

$$\frac{5}{64}\,(\beta_1 - \beta_2)^4$$

It remains the case where the characteristic is 5. Then the equations $b = 0, c = 0$ become,

$$\begin{aligned}
0 &= \frac{1}{64}(\beta_1^5 - \beta_2^5) - 2^{10}\Delta(f),\\
0 &= \frac{1}{256}\beta_1(\beta_1^5 - \beta_2^5).
\end{aligned}$$

If $\beta_1 \neq 0$, then $\beta_1^5 - \beta_2^5 = 0$, hence $2^{10}\Delta(f) = 0$. Since the characteristic is not 2, we obtain $\Delta(f) = 0$, which is impossible since f is separable by hypothesis.

If $\beta_1 = 0$, it remains a unique equation

$$0 = \beta_2^5 + 2^{16}\Delta(f),$$

that is

$$0 = \beta_2^5 + \Delta(f).$$

In this case

$$\theta_f(y) = y(y-\beta_2)^5 = y(y^5 - \beta_2^5) = y^6 + \Delta(f) y.$$

Since

$$\theta_f(y) = (y^3 + b_2 y^2 + b_4 y + b_6)^2 - 2^{10}\Delta(f) y = (y^3 + b_2 y^2 + b_4 y + b_6)^2 + \Delta(f) y,$$

this condition is equivalent to $b_2 = b_4 = b_6 = 0$.

I don't see an immediate contradiction ...

In fact, with this analysis, we can show a counterexample of Proposition 13.2.7:

Let $f = x^5 - x + 1 \in \mathbb{F}_5[x]$, where $c_1 = c_2 = c_3 = 0, c_4 = -1, c_5 = -1$. Then f is irreducible, separable, and the Sage instructions given in Exercise 6, where we replace the field $\mathbb{Q}$ by $\mathbb{F}_5$ show that $b_2 = b_4 = b_6 = 0$, and

$$\begin{aligned} \Delta(f) &= -1, \\ \theta_f(y) &= y^6 - y. \end{aligned}$$

(We verify this directly on the formulas (13.24) : almost all the terms of B_2, B_4, B_6 contain σ_1, σ_2 or σ_3, if not, the coefficient is a multiple of 5, so $b_2 = b_4 = b_6 = 0$.)

Therefore $\beta = 0$ is a root of θ_f, and $\theta_f(y) = (y-\beta)g(y)$, where $g(y) = y^5 - 1 = (y-1)^5$ is **not** irreducible over $\mathbb{F}_5$.

The second equivalence of Proposition 13.2.7 is false if the characteristic of F is 5.

Note : Here we know explicitly the roots of f in $\mathbb{F}_{5^5}[x]$. If α is a root of f in this field, the roots of f are $\alpha, \alpha+1, \alpha+2, \alpha+3, \alpha+4$ (see Ex. 6.2.5). If we substitute (with the help of Sage) these roots in $h_1, \ldots, h_6$, we obtain $0, 1, 1, 1, 1, 1$, therefore

$$\theta_f(y) = \prod_{i=1}^{6} (y - h_i(\alpha_1, \ldots, \alpha_5)) = y(y-1)^5 = y^6 - y.$$

This is a confirmation of the previous results.

□

Ex. 13.2.11 *Show that the table preceding Example 13.2.8 follows from the diagram (13.16) and Theorem 13.2.6.*

Proof.

- Suppose that $\theta_f(y)$ has no root in F (lines 1 and 2 of the table). By Theorem 13.2.6 (b), G is not conjugate to a subgroup of $\mathrm{AGL}(1, \mathbb{F}_5)$. Therefore by diagram (13.6) and Theorem 13.2.2, $G = A_5$ or $G = S_5$ (no conjugacy here). By Theorem 13.2.6 (a), $G = A_5$ if $\Delta(f) \in F^2$, and $G = S_5$ otherwise.
- Suppose now that $\theta_f(y)$ has a root in F (lines 3,4,5 of the table). Then, by Theorem 13.2.6 (b) (and Theorem 13.2.2), G is conjugate to a subgroup of $\mathrm{AGL}(1, \mathbb{F}_5)$ containing $\langle (1\,2\,3\,4\,5) \rangle$.

  So, by diagram (13.16), G is conjugate to $\mathrm{AGL}(1, \mathbb{F}_5)$, $\mathrm{AGL}(1, \mathbb{F}_5) \cap A_5$, or $\langle (1\,2\,3\,4\,5) \rangle$.

  If $\Delta(f) \notin F^2$, $G \not\subset A_5$, therefore $G = \mathrm{AGL}(1, \mathbb{F}_5)$. This is the third line of the table.

  If $\Delta(f) \in F^2$, $G \subset A_5$, therefore G is conjugate to $\mathrm{AGL}(1, \mathbb{F}_5) \cap A_5$, or $\langle (1\,2\,3\,4\,5) \rangle$.

  By theorem 13.2.6 (c), G is conjugate to $\langle (1\,2\,3\,4\,5) \rangle$ if and only if f splits completely over $F(\alpha)$, and this gives the two last lines of the table.

□

Ex. 13.2.12 *Let $f = x^5 - 6x + 3 \in \mathbb{Q}[x]$. Compute $\Delta(f)$ and $\theta_f(y)$ and show that $\theta_f(y)$ is irreducible over $\mathbb{Q}$.*

Proof. By the Schönemann-Eisenstein Criterion for $p = 3$, we know that f is irreducible over $\mathbb{Q}$.

The discriminant $f = x^5 + ax + b, a, b \in \mathbb{Q}$ is given (see Ex. 15) by

$$\Delta(f) = 256a^5 + 3125b^4,$$

so

$$\Delta(f) = -256 \cdot 6^5 + 3125 \cdot 3^4 = -1737531.$$

If we apply on the resolvent $\theta_f(y)$ the evaluation $\sigma_1 \mapsto 0, \sigma_2 \mapsto 0, \sigma_3 \mapsto 0, \sigma_4 \mapsto a, \sigma_5 \mapsto -b$, we obtain

$$\theta_f(y) = \left(y^3 - 20\,ay^2 + 240\,a^2y + 320\,a^3\right)^2 - 2^{10}(256\,a^5 + 3125\,b^4)y$$

With $a = -6, b = 3$, we obtain

$$\begin{aligned}\theta_f(y) &= \left(y^3 + 120\,y^2 + 8640\,y - 69120\right)^2 + 2^{10}\,1737531\,y\\ &= y^6 + 240\,y^5 + 31680\,y^4 + 1935360\,y^3 + 58060800\,y^2 + 584838144\,y + 4777574400\end{aligned}$$

The Schönemann-Eisenstein Criterion doesn't apply.

With Sage, we obtain

```
R.<y> = QQ[]
p=y^6 + 240*y^5 + 31680*y^4 + 1935360*y^3 + 58060800*y^2 + 584838144*y + 4777574400
p.is_irreducible()
```

True

$\theta_f(y)$ is irreducible over $\mathbb{Q}$. A fortiori, $\theta_f(y)$ has no root in $\mathbb{Q}$.

Since $\Delta(f) < 0$ is not a square in $\mathbb{Q}$, the Galois group of f is S_5. $\square$

Ex. 13.2.13 *Let $f = x^5 - 2 \in \mathbb{Q}(\sqrt{5})[x]$ be as in Example 13.2.9.*

(a) Compute $\Delta(f)$ and $\theta_f(y)$.

(b) In Section 6.4 we showed that the Galois group of f over $\mathbb{Q}$ is isomorphic to $\mathrm{AGL}(1, \mathbb{F}_5)$. *Use this and the Galois correspondence to show that the Galois group over $\mathbb{Q}(\sqrt{5})$ is isomorphic to* $\mathrm{AGL}(1, \mathbb{F}_5) \cap A_5$.

Proof. (a) We use the formulas of Exercise 15 for $f = x^5 + ax + b$:

$$\begin{aligned}\Delta(f) &= 256a^5 + 3125b^4,\\ \theta_f(y) &= \left(y^3 - 20\,ay^2 + 240\,a^2y + 320\,a^3\right)^2 - 2^{10}\Delta(f)y.\end{aligned}$$

With $a = 0, b = -2$, we obtain

$$\begin{aligned}\Delta(f) &= 50000 = 2^4\,5^5,\\ \theta_f(y) &= y^6 - 2^{14}\,5^5\,y.\end{aligned}$$

Let L be the splitting field of $x^5 - 2$ over $\mathbb{Q}$. $\Delta(f)$ is not a square in $\mathbb{Q}$, and $\theta_f(y)$ has a root 0 in $\mathbb{Q}$. So, by Theorem 13.2.6 and Exercise 11, $\mathrm{Gal}(L/\mathbb{Q})$ is isomorphic to $\mathrm{AGL}(1, \mathbb{F}_5)$. This result is already proved in Section 6.4.

(b) We know that $\zeta_5 = (\zeta_5 \sqrt[5]{2})/\sqrt[5]{2} \in L$, and also $\sqrt{5} = \zeta_5 + \zeta_5^{-1} - \zeta_5^2 - \zeta_5^{-2} \in L$ (see the quadratic Gauss sum page 249).

Since $\mathbb{Q} \subset \mathbb{Q}(\sqrt{5})$ is a quadratic extension, by the Galois correspondence, $\mathrm{Gal}(L/\mathbb{Q}(\sqrt{5}))$ is a subgroup of index 2 in $\mathrm{Gal}(L/\mathbb{Q})$ and the subgroup $H \subset S_5$ corresponding to $\mathrm{Gal}(L/\mathbb{Q}(\sqrt{5}))$ has index 2 in $G \simeq \mathrm{AGL}(1, \mathbb{F}_5)$. Thus $|H| = 10$, and since $5 \mid |H|$, H contains a 5-cycle and is a transitive subgroup of S_5. By Theorem 13.2.2, H is conjugate to $\langle (1\,2\,3\,4\,5) \rangle$ or to $\mathrm{AGL}(1, \mathbb{F}_5) \cap A_5$. Since $(G : H) = 2$, H is conjugate to $\mathrm{AGL}(1, \mathbb{F}_5) \cap A_5$, so

$$\mathrm{Gal}(L/\mathbb{Q}(\sqrt{5})) \simeq H \simeq \mathrm{AGL}(1, \mathbb{F}_5) \cap A_5.$$

□

Ex. 13.2.14 *Let $f = x^5 + px^3 + \frac{1}{5}p^2 x + q \in \mathbb{Q}[x]$ be as in Example 13.2.10, and assume that f is irreducible over $\mathbb{Q}$.*

(a) Compute $\Delta(f)$ and $\theta_f(y)$.

(b) Factor $\theta_f(y) \in \mathbb{Q}[x]$, and conclude that $5p^2 \in \mathbb{Q}$ is a root of $\theta_f(y)$.

(c) Show that the substitution $x = z - \frac{p}{5z}$ transforms f into $z^5 - \frac{p^5}{5^5 z^5} + q$.

(d) Use part (c) to give an elementary proof that f is solvable by radicals over $\mathbb{Q}$.

Proof. (a) We obtain the discriminant with Sage:

```
S.<p,q,x> = QQ[]
f = x^5 + p*x^3 +(1/5)*p^2*x + q
Delta = f.discriminant(x);Delta.factor()
```

$$\left(\frac{1}{3125}\right) \cdot (4p^5 + 3125q^2)^2$$

So

$$\Delta(f) = \frac{1}{5^5} \cdot (4p^5 + 3125q^2)^2.$$

We use the following procedure to compute a sextic resolvent with the same method as in Exercise 6:

```
def resolvent(f):
    l = f.coefficients(sparse = False)
    R.<Delta,x1,x2,x3,x4,x5,y1,y2,y3,y4,y5,y,P,Q,e> = PolynomialRing(QQ, order =
    elt = SymmetricFunctions(QQ).e()
    e = [elt([i]).expand(5).subs(x0=x1, x1=x2, x2=x3, x3 = x4, x4 = x5)
                for i in range(6)]
    J = R.ideal(e[1]-y1, e[2]-y2, e[3]-y3,e[4]-y4,e[5]-y5)
    G = J.groebner_basis()
    u1 =x1*x2 + x2*x3 + x3*x4 + x4*x5 + x5*x1 - x1*x3 - x3*x5 -x5*x2 - x2*x4 -x4
    u2 = u1.subs(x1 = x2, x2 = x3, x3 = x1)
    u3 = u1.subs(x2 = x3, x3 = x4, x4 = x2)
    u4 = u1.subs(x3 = x4, x4 = x5, x5 = x3)
```

```
    u5 = u1.subs(x1 = x4, x4 = x5, x5 = x1)
    u6 = u1.subs(x1 = x2, x2 = x5, x5 = x1)
    f1 = (y-u1) * (y-u2) * (y-u3) * (y-u4) * (y-u5) * (y-u6)
    var('sigma_1,sigma_2,sigma_3,sigma_4,sigma_5')
    g = f1.reduce(G).subs(y1=sigma_1, y2=sigma_2, y3=sigma_3, y4=sigma_4, y5= si
    h = g.collect(y);
    B2 = h.coefficient(y,4)
    B4 = h.coefficient(y,2)
    B6 = h.coefficient(y,0)
    b2 = B2.subs(sigma_1 = -l[4], sigma_2= l[3],sigma_3 = -l[2], sigma_4 = l[1],
    b4 = B4.subs(sigma_1 = -l[4], sigma_2= l[3],sigma_3 = -l[2], sigma_4 = l[1],
    b6 = B6.subs(sigma_1 = -l[4], sigma_2= l[3],sigma_3 = -l[2],
                 sigma_4 = l[1], sigma_5 = -l[0])
    theta_f = [(y^3+b2*y^2+b4*y+b6)^2 - 2^10*Delta*y,b2,b4,b6]
    return theta_f
```

Then we obtain b_2, b_4, b_6 and $\theta_f(y)$:

```
K.<p,q> = QQ[]
S.<x> =PolynomialRing(K, order = 'degrevlex')
f = x^5 + p*x^3 +(1/5)*p^2*x + q
resolvent(f)[1:4]
```

$$\left(-7\,p^2, 11\,p^4, \frac{3}{25}\,p^6 + 4000\,pq^2\right)$$

```
theta_f=resolvent(f)[0];theta_f
```

$$\begin{aligned}\theta_f(y) &= \frac{1}{625}\left(3p^6 + 275p^4y - 175p^2y^2 + 100000pq^2 + 25y^3\right)^2 - 1024\Delta(f)y \\ &= \left(y^3 - 7\,p^2y^2 + 11p^4y + \frac{3}{25}\,p^6 + 4000\,pq^2\right)^2 - 2^{10}\Delta(f)y\end{aligned}$$

We obtained the results given in the text.

(b) To find the rational root of f we write

```
theta_f.subs(Delta = (1/5)^5*(4*p^5+3125*q^2)^2)).factor()
```

$$\frac{1}{3125}\,(5\,p^2 - y)\,(9\,p^{10} - 1625\,p^8y + 74250\,p^6y^2 + 600000\,p^5q^2 - 81250\,p^4y^3 + 50000000\,p^3q^2y + 28125\,p^2y^4 - 25000000\,pq^2y^2 - 3125\,y^5 + 10000000000\,q^4)$$

Thus

$$\theta_f(5p^2) = 0.$$

By Corollary 13.2.11, f is solvable by radicals over $\mathbb{Q}$.

(c) The substitution $x = z - \frac{p}{5z}$ is obtained by

```
z = var('z')
g = f.subs(x = z - p/(5*z))
g.expand()
```

$$z^5 + q - \frac{p^5}{3125\, z^5}$$

Thus

$$g(z) = f\left(z - \frac{p}{5z}\right) = z^5 - \frac{p^5}{5^5\, z^5} + q.$$

(d) Let $\beta \in \mathbb{C}$.

$$\begin{aligned} g(\beta) = 0 &\iff \beta^{10} + q\,\beta^5 - \left(\frac{p}{5}\right)^5 = 0 \\ &\iff \left(\beta^5 + \frac{q}{2}\right)^2 - \left[\left(\frac{q}{2}\right)^2 + \left(\frac{p}{5}\right)^5\right] = 0 \\ &\iff \left[\beta^5 + \frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{5}\right)^5}\right]\left[\beta^5 + \frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{5}\right)^5}\right] = 0. \end{aligned}$$

So the 10 roots of g are

$$\beta_{k,\varepsilon} = \zeta^k \sqrt[5]{-\frac{q}{2} + \varepsilon\sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{5}\right)^5}}, \qquad \varepsilon = \pm 1,\ k = 0, 1, 2, 3, 4.$$

where $\zeta = \zeta_5 = e^{2i\pi/5}$.

Let α be a root of f in $\mathbb{C}$. There exists $\beta \in \mathbb{C}$ such that $\alpha = \beta - \frac{p}{5\beta}$, so

$$0 = f(\alpha) = f\left(\beta - \frac{p}{5\beta}\right) = g(\beta).$$

Since $g(\beta) = 0$, $\beta = \beta_{k,\varepsilon}$ for some $k \in \{0, \ldots, 4\}, \varepsilon \in \{-1, 1\}$. If L is the splitting field of f in $\mathbb{C}$, then

$$L \subset \mathbb{Q}(\beta_{0,1}, \ldots, \beta_{4,1}, \beta_{0,-1}, \ldots, \beta_{4,-1}).$$

Write $\delta = \left(\frac{q}{2}\right)^2 + \left(\frac{p}{5}\right)^5 \in \mathbb{Q}$. Since $\beta_{k,\varepsilon} \in \mathbb{Q}\left(\sqrt{\delta}, \zeta, \sqrt[5]{-\frac{q}{2} + \varepsilon\sqrt{\delta}}\right)$,

$$L \subset \mathbb{Q}\left(\zeta_5, \sqrt{\delta}, \sqrt[5]{-\frac{q}{2} + \sqrt{\delta}}, \sqrt[5]{-\frac{q}{2} - \sqrt{\delta}}\right),$$

where $\delta, q \in \mathbb{Q}$, so L is included in some radical extension of $\mathbb{Q}$.

Therefore f is solvable by radicals over $\mathbb{Q}$.

Note: We can choose $\sqrt[5]{-\frac{q}{2} - \sqrt{\delta}}$ so that $\sqrt[5]{-\frac{q}{2} + \sqrt{\delta}}\,\sqrt[5]{-\frac{q}{2} - \sqrt{\delta}} = -\frac{p}{5} \in \mathbb{Q}$. Therefore

$$L \subset \mathbb{Q}\left(\zeta_5, \sqrt{\delta}, \sqrt[5]{-\frac{q}{2} + \sqrt{\delta}}\right),$$

where the chain of inclusions

$$\mathbb{Q} \subset \mathbb{Q}(\zeta_5) \subset \mathbb{Q}\left(\zeta_5, \sqrt{\delta}\right) \subset \mathbb{Q}\left(\zeta_5, \sqrt{\delta}, \sqrt[5]{-\frac{q}{2} + \sqrt{\delta}}\right)$$

proves that this last field is a radical extension.

$\square$

Ex. 13.2.15 *As in Theorem 13.2.12, let $f = x^5 + ax + b$. Compute $\Delta(f)$ and $\theta_f(y)$.*

Proof. With the same Sage procedure as in Exercise 14, we obtain:

```
S.<a,b,x> = QQ[]
f = x^5 + a*x + b
Delta = f.discriminant(x);Delta.factor()
```

$$\Delta(f) = 256a^5 + 3125b^4,$$

```
K.<a,b> = QQ[]
S.<x> =PolynomialRing(K, order = 'degrevlex')
f = x^5 + a*x + b
theta_f=resolvent(f)[0];theta_f.subs(Delta = f.discriminant())
```

$$\theta_f(y) = \left(y^3 - 20\,ay^2 + 240\,a^2y + 320\,a^3\right)^2 - 2^{10}(256\,a^5 + 3125\,b^4)y.$$

□

Ex. 13.2.16 *Let $f = x^5 + ax + b \in F[x]$, where f is separable and irreducible and F has characteristic 5. The goal of this exercise is to prove the observation of [28] that the Galois group of f over F is solvable.*

(a) Prove that $a \neq 0$.

(b) Use Exercise 5 from Section 6.2 to show that the Galois group of f over F is cyclic when $a = -1$.

(c) Show that there is a Galois extension $F \subset L$ with solvable Galois group such that f is equivalent (as defined in the Mathematical Notes) to a polynomial of the form $x^5 - x + b'$ for some $b' \in L$.

(d) Conclude that the Galois group of f over F is solvable.

(e) Show that there is a field F of characteristic 5 and a monic, separable, irreducible quintic $g \in F[x]$ that cannot be transformed to one in Bring-Jerrard form defined over any Galois extension $F \subset L$ with solvable Galois group.

In [28] Ruppert explores the geometric reasons why things go wrong in characteristic 5.

Proof. (a) If $a = 0$, then $f = x^5 + b$, so $f = x^5 - \alpha^5$, where α is a root of f in some extension of F. Since the characteristic of F is 5, $f = x^5 - \alpha^5 = (x - \alpha)^5$ is not separable, in contradiction with the hypothesis, so $a \neq 0$.

(b) If $a = -1$, by Exercise 5.3.16 and 6.2.5, we know that

$$x^5 - x + b = (x - \alpha)(x - \alpha - 1)(x - \alpha - 2)(x - \alpha - 3)(x - \alpha - 4),$$

where α is a root of f in some extension. Then $K = F(\alpha)$ is the splitting field of f over F. By part (c) of exercise 6.2.5, we know also that

$$\varphi \left\{ \begin{array}{ccc} \mathrm{Gal}(L/F) & \to & \mathbb{Z}/5\mathbb{Z} \\ \sigma & \mapsto & \sigma(\alpha) - \alpha \end{array} \right.$$

is a group isomorphism, so $\mathrm{Gal}(L/F)$ is cyclic of order 5.

(c) We search λ such that

$$x^5 - x + b' = \lambda^{-5}((\lambda x)^5 + a(\lambda x) + b)$$

for some b'.

This is equivalent to

$$\lambda^5 x^5 - \lambda^5 x + \lambda^5 b' = \lambda^5 x^5 + a\lambda x + b,$$

so $a\lambda = -\lambda^5, \lambda^4 = -a$. Let L a splitting field of $x^4 + a$, and choose

$$\lambda = \sqrt[4]{-a}$$

a fixed root of $x^4 + a$ in L.

The characteristic is 5, so $2^2 = -1$, and

$$x^4 + a = x^4 - \lambda^4 = (x^2 + \lambda^2)(x^2 - \lambda^2) = (x + 2\lambda)(x - 2\lambda)(x - \lambda)(x + \lambda)$$

splits completely over F. Since $\lambda \neq 0$, and since the characteristic is 5, the roots of $x^4 + a$ are distinct. Therefore $L = F(\lambda)$ is the splitting field of the separable polynomial $x^4 + a$ over F. Hence $F \subset L = F(\lambda)$ is a Galois extension.

So there exists λ in some solvable Galois extension L of F such that $x^5 - x + b' = \lambda^{-5}((\lambda x)^5 + a(\lambda x) + b)$ with $b' = (\sqrt[4]{-a})^{-5} b$, where $\lambda, b' \in L$.

(d) If β is in some extension of F, β is a root of f if and only if $\lambda^{-1}\beta$ is a root of $x^5 - x + b'$. If α is a fixed root of $x^5 - x + b'$, then by part (b) the roots of $x^5 - x + b'$ are $\alpha, \alpha+1, \alpha+2, \alpha+3, \alpha+4$, so the roots of f are

$$\beta_0 = \lambda\alpha, \beta_1 = \lambda(\alpha+1), \beta_2 = \lambda(\alpha+2), \beta_3 = \lambda(\alpha+3), \beta_4 = \lambda(\alpha+4).$$

A splitting field of f over F is

$$K = F(\beta_0, \ldots, \beta_4) = F(\lambda\alpha, \lambda(\alpha+1), \ldots, \lambda(\alpha+4)).$$

Since $\lambda = \lambda(\alpha+1) - \lambda\alpha = \beta_1 - \beta_0 \in K$, and $\alpha = (\lambda\alpha)/\lambda = \beta_0/(\beta_1 - \beta_0) \in K$, $F(\lambda, \alpha) \subset K$, and $\lambda\alpha, \ldots, \lambda(\alpha+4) \in F(\lambda, \alpha)$, so $K \subset F(\lambda, \alpha)$:

$$K = F(\lambda, \alpha)$$

is the splitting field of $f = x^5 + ax + b$ over F.

Since $F(\lambda) = L \subset K$, $K = L(\alpha)$.

Since f is irreducible over F, $5 = \deg(f) = [F(\beta_0) : F] \mid [K : F]$.

$\mathrm{Gal}(L/F)$ is isomorphic to a subgroup of S_4, so $5 \nmid [L : F] = |\mathrm{Gal}(L/F)|$.

Since $[K : F] = [K : L][L : F]$, $5 \mid [K : L] = [L[\alpha] : L]$, where $\alpha^5 - \alpha + b' = 0$. Therefore $x^5 - x + b'$ is irreducible over L and by part (b),

$$\mathrm{Gal}(K/L) \simeq \mathbb{Z}/5\mathbb{Z} \text{ is cyclic.}$$

Since $F \subset L$ is a Galois extension,

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

$\mathrm{Gal}(L/F)$ is isomorphic to a subgroup of S_4, so is solvable, and $\mathrm{Gal}(K/L)$ is cyclic, a fortiori solvable. Therefore $\mathrm{Gal}(K/F)$ is solvable:

The Galois group of f over F is solvable.

(e) Let $F = \mathbb{F}_5(\sigma_1, \ldots, \sigma_5) \subset \mathbb{F}_5(x_1, \ldots, x_5)$. The Galois group of $f = x^5 - \sigma_1 x^4 + \sigma_2 x^3 - \sigma_3 x^2 + \sigma_4 x - \sigma_5$ is S_5, and S_5 is not solvable. Therefore f cannot be equivalent to a polynomial $x^5 + ax + b$ whose Galois group over F is solvable.

□

Ex. 13.2.17 *Following Example 13.2.14, consider the equations $x^3 + 3x + 1 = 0$, and $y = a + bx + x^2$.*

(a) Use Maple or Mathematica and Section 2.3 to eliminate x and obtain (13.26).

(b) Show that coefficients of y^2 and y in (13.26) both vanish if and only if $a = 2$ and $b^2 + b - 1 = 0$.

(c) The equation for y becomes trivial to solve when $a = 2$ and $b = (\sqrt{5} - 1)/2$. We could then solve for x using $y = a + bx + x^2$, but there is a better way to proceed. Note that

$$x^3 = -bx^2 - ax + yx$$

follows from $y = a + bx + x^2$. Furthermore, we can use $y = a + bx + x^2$ to eliminate the x^2 in the above equation. Then use $x^3 + 3x + 1 = 0$ to obtain an equation in which x appears only to the first power. Solving this gives a formula for x in terms of y. The general version of this argument can be found in [Lagrange, p.223].

Proof. (a) We eliminate x between the two polynomials

$$f = x^3 + 3x + 1,$$
$$g = x^2 + bx + (a - y),$$

with the resultant $\mathrm{Res}_x(f, g) = \det(S)$, where

$$S = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & b & 1 & 0 \\ 3 & 0 & a-y & b & 1 \\ 1 & 3 & 0 & a-y & b \\ 0 & 1 & 0 & 0 & a-y \end{pmatrix}$$

We can obtain this determinant with Sage:

```
R.<a,b,x,y> = QQ[]
f = x^3 + 3*x + 1
g = x^2 + b*x + (a-y)
S = matrix(R,[[1, 0, 1,   0,   0  ],
              [0, 1, b,   1,   0  ],
              [3, 0, a-y, b,   1  ],
              [1, 3, 0,   a-y, b  ],
              [0, 1, 0,   0,   a-y]])
R = S.det(); R
```

$$a^3 + 3ab^2 - b^3 - 3a^2y - 3b^2y + 3ay^2 - y^3 - 6a^2 + 3ab + 12ay - 3by - 6y^2 + 9a - 3b - 9y + 1$$

But it is more easy to call the method "resultant" to obtain the same result:

```
res = f.resultant(g,x);res
```

The list of coefficients of $-\mathrm{Res}_x(f,g)$ is given by

```
l =[-res.subs(y=0)] +  [-res.coefficient(y^k) for k in range(1,4)]
l
```

$\left[-a^3 - 3ab^2 + b^3 + 6a^2 - 3ab - 9a + 3b - 1, \quad 3a^2 + 3b^2 - 12a + 3b + 9, \quad -3a + 6, \quad 1\right]$

We find the equation(13.26):

$$y^3 + (6 - 3a)y^2 + (9 + 3b + 3b^2 - 12a + 3a^2)y + P(a,b) = 0,$$

where $P(a,b) = -a^3 - 3ab^2 + b^3 + 6a^2 - 3ab - 9a + 3b - 1$.

(b) The coefficient of y^2 vanishes if $a = 2$, and then the coefficient of y vanishes if $0 = 9 + 3b + 3b^2 - 12a + 3a^2 = 3b + 3b^2 - 3$:

$$b^2 + b - 1 = 0$$

so $b = \frac{\sqrt{5}-1}{2}$ is a solution.

If we pick $b = (\sqrt{5} - 1)/2$, then the above cubic equation becomes

$$y^3 + \frac{5}{2}\sqrt{5} - \frac{25}{2} = 0,$$

so

$$\begin{aligned} y^3 &= \frac{25 - 5\sqrt{5}}{2} \\ &= \sqrt{5}^3\, \frac{\sqrt{5} - 1}{2}. \end{aligned}$$

By the property of the resultant, if y is evaluated to $y_0 = \omega^k\, \sqrt{5}\, \sqrt[3]{\frac{\sqrt{5}-1}{2}}$, $k = 0, 1, 2$, $\omega = e^{2i\pi/3}$, then there exists a common root of f and g in $\mathbb{C}$, where

$$\begin{aligned} f &= x^3 + 3x + 1 \\ g &= x^2 + \frac{\sqrt{5} - 1}{2} x + 2 - y_0. \end{aligned}$$

(c) The Euclidean division of f by g gives

$$x^3 + 3x + 1 = (x^2 + bx + a - y)(x - b) + (y + b^2 + 3 - a)x + 1 + ab - by.$$

If x_0 is a common root of f, g, then the remainder is 0, so

$$x_0 = \frac{by_0 - ab - 1}{y_0 + b^2 + 3 - a},$$

and this gives a formula for the roots x_0 of f in terms of the roots y_0 of the resultant.

Since y_0 is an algebraic number of degree 3 over $\mathbb{Q}$, and $x_0 \in \mathbb{Q}(\sqrt{5}, y_0)$, there exists some polynomial p of degree 2 such that $x_0 = p(y_0)$.

To find this more simple formula for x_0, we search the gcd of f, g in the field $\mathbb{Q}\left(\sqrt{5}, \sqrt[3]{\frac{\sqrt{5}-1}{2}}\right)$ by the extended Euclid's algorithm.

This is obtained with the following Sage instructions:

```
K.<u>= QQ[sqrt(5)]
R.<z> = K[]
res = z^3 - (u-1)/2
L.<w> = K.extension(res)
A.<x> = L[]
f = x^3 + 3*x + 1
g = x^2 + (u - 1)/2 * x + (2 - u*w)
gcd(f,g)
```

$$x + \left(\frac{1}{2}\sqrt{5} + \frac{1}{2}\right) w^2 - w$$

We have obtained that

$$\gcd(f, g) = x + \frac{\sqrt{5}+1}{2} w^2 - w, \text{ where } w^3 = \frac{\sqrt{5}-1}{2}.$$

Since $w^3 = \frac{\sqrt{5}-1}{2}$, so $w^2 = \frac{\sqrt{5}-1}{2} w^{-1}$, $\frac{\sqrt{5}+1}{2} w^2 = w^{-1}$.

Therefore the roots of f are

$$\begin{aligned} x_0 &= w - \frac{\sqrt{5}+1}{2} w^2 \\ &= w - w^{-1} \end{aligned}$$

We can write $w = \omega^k \sqrt[3]{\frac{\sqrt{5}-1}{2}}$, $k = 0, 1, 2$, then $w^{-1} = \omega^{2k} \sqrt[3]{\frac{\sqrt{5}+1}{2}}$, where the cubic roots are chosen so that their product is real, equal to 1. Then

$$\omega^k \sqrt[3]{\frac{\sqrt{5}-1}{2}} - \omega^{2k} \sqrt[3]{\frac{\sqrt{5}+1}{2}}, \qquad k = 0, 1, 2$$

are the roots of f. This is identical to the formulas obtained with Cardano's formulas, with more sweat.

□

Ex. 13.2.18 *This exercise is concerned with the polynomials (13.28). As in the Historical Notes, we will assume that they lie in $\mathbb{Q}[x]$ and are irreducible.*

(a) Show that $\sqrt[5]{Q^2/P} + (P/Q)\sqrt[5]{Q^2/P}^2$ is a root of $x^5 - 5Px^2 - 5Qx - Q^2/P - P^3/Q$.

(b) Prove that the Galois group of $x^5 - 5Px^2 - 5Qx - Q^2/P - P^3/Q$ over $\mathbb{Q}$ is isomorphic to $AGL(1, \mathbb{F}_5)$.

(c) Prove that over $\mathbb{Q}(\sqrt{5})$, the first two polynomials of (13.28) have cyclic Galois group while the third has Galois group isomorphic to $\mathrm{AGL}(1, \mathbb{F}_5) \cap A_5$.

Proof. (a) As in Cardan's method, we substitute $u + v$ to x in

$$f(x) = x^5 - 5Px^2 - 5Qx - \frac{Q^2}{P} - \frac{P^3}{Q}.$$

We obtain

$$\begin{aligned} f(u+v) &= u^5 + 5\,u^4 v + 10\,u^3 v^2 + 10\,u^2 v^3 + 5\,uv^4 + v^5 \\ &\qquad - 5\,Pu^2 - 10\,Puv - 5\,Pv^2 - 5\,Qu - 5\,Qv - \frac{Q^2}{P} - \frac{P^3}{Q} \\ &= \left(u^5 + v^5 - \frac{Q^2}{P} - \frac{P^3}{Q}\right) + 5\,\big(u^3 v + u^2 v^2 + uv^3 - Pu - Pv - Q\big)(u+v). \end{aligned}$$

Then we verify that $u = \sqrt[5]{Q^2/P} = P^{-\frac{1}{5}} Q^{\frac{2}{5}}, v = (P/Q)\sqrt[5]{Q^2/P}^2 = P^{\frac{3}{5}} Q^{-\frac{1}{5}}$ is a solution of the system

$$\begin{aligned} 0 &= u^5 + v^5 - \frac{Q^2}{P} - \frac{P^3}{Q}, \\ 0 &= u^3 v + u^2 v^2 + uv^3 - Pu - Pv - Q. \end{aligned}$$

Indeed

$$u^5 + v^5 - \frac{Q^2}{P} - \frac{P^3}{Q} = \frac{Q^2}{P} + \frac{P^3}{Q} - \frac{Q^2}{P} - \frac{P^3}{Q} = 0,$$

and, since $P = uv^2, Q = u^3 v$,

$$u^3 v + u^2 v^2 + uv^3 - Pu - Pv - Q = u^3 v + u^2 v^2 + uv^3 - u^2 v^2 - uv^3 - u^3 v = 0.$$

Therefore

$$u + v = \sqrt[5]{Q^2/P} + (P/Q)\sqrt[5]{Q^2/P}^2$$

is a root of $x^5 - 5Px^2 - 5Qx - Q^2/P - P^3/Q$. If we replace $\sqrt[5]{Q}$ by another fifth root $\zeta^k \sqrt[5]{Q},\ k = 1,2,3,4$, (where $\zeta = e^{2i\pi/5}$), in the equation

$$0 = u^3 v + u^2 v^2 + uv^3 - Pu - Pv - Q, \qquad \text{where } u = \sqrt[5]{P}^{-1}\sqrt[5]{Q}^2, v = \sqrt[5]{P}^3\sqrt[5]{Q}^{-1},$$

then u is replaced by $\zeta^{2k} u$, and v is replace by $\zeta^{4k} v$, therefore $\zeta^{2k} u, \zeta^{4k} v$ is a solution of the preceding system, so $\zeta^{2k} u + \zeta^{4k} v$ is also a root of f. So

$$u+v, \quad \zeta^2 u + \zeta^4 v, \quad \zeta^4 u + \zeta^3 v, \quad \zeta u + \zeta^2 v, \quad \zeta^3 u + \zeta v,$$

are roots of f, where

$$u = \sqrt[5]{Q^2/P}, \qquad v = (P/Q)\sqrt[5]{Q^2/P}^2.$$

These roots are the five roots of f, as proved in the following expansion:

$$\begin{aligned} &(x-(u+v))(x-(\zeta^2 u + \zeta^4 v))(x-(\zeta^4 u + \zeta^3 v))(x-(\zeta u + \zeta^2 v))(x-(\zeta^3 u + \zeta v)) \\ &= x^5 - 5uv^2 x^2 - 5u^3 v x - u^5 - v^5. \end{aligned}$$

Since

$$P = uv^2, \qquad Q = u^3 v,$$

we obtain

$$u^5 = \frac{Q^2}{P}, \qquad v^5 = \frac{P^3}{Q},$$

so

$$
\begin{aligned}
f &= x^5 - 5Px^2 - 5Qx - \frac{Q^2}{P} - \frac{P^3}{Q} \\
&= (x-(u+v))(x-(\zeta^2 u+\zeta^4 v))(x-(\zeta^4 u+\zeta^3 v))(x-(\zeta u+\zeta^2 v))(x-(\zeta^3 u+\zeta v))
\end{aligned}
$$

Therefore the roots of f are $\zeta^{2k}u + \zeta^{4k}v,\ k = 0,1,2,3,4.$

This was perhaps the Euler's starting point.

(b) We obtain the discriminant of f with

```
R.<P,Q,u,v,e,x> = QQ[]
f = x^5 - 5*P*x^2 - 5*Q*x -e;
Delta = f.discriminant(x).subs(e = Q^2/P + P^3/Q).factor()
Delta
```

$$(3125) \cdot Q^{-4} \cdot P^{-4} \cdot (-P^8 - 11P^4Q^3 + Q^6)^2$$

so

$$\Delta = 5^5 \frac{(P^8 + 11P^4Q^3 - Q^6)^2}{P^4Q^4}.$$

Thus Δ is not a square in $\mathbb{Q}$.

Using the resolvent() function of Exercise 14, we obtain the sextic resolvent:

```
K.<P,Q,e> = QQ[]
S.<x> =PolynomialRing(K, order = 'degrevlex')
f = x^5 - 5*P*x^2 - 5*Q*x -e
theta = resolvent(f)[0]; theta.subs(e = Q^2/P + P^3/Q)
```

$$
\begin{aligned}
\theta_f(y) &= \left(100\,Qy^2 + y^3 + 2000\left(3\,Q^2 - \left(P^4 + Q^3\right)/Q\right)y\right)^2 - 1024\,\Delta(f)y \\
&= \left(y^3 + 100\,Qy^2 - 2000\left(\frac{P^4}{Q} - 2\,Q^2\right)y\right)^2 - 1024\,\Delta(f)y,
\end{aligned}
$$

which has root $0 \in \mathbb{Q}$ ($b_6 = 0$). By Section 13.2, the Galois group of f is $\mathrm{AGL}(1,\mathbb{F}_5)$ up to conjugacy.

(c) By Exercise 13, we know that the Galois group of x^5-2 over $\mathbb{Q}(\sqrt{5})$ is $\mathrm{AGL}(1,\mathbb{F}_5)\cap A_5$ which is not cyclic, so there is a misprint in the sentence.

- The polynomial $f = x^5 - D \in \mathbb{Q}(\sqrt{5})[x], D \in \mathbb{Q}$, is irreducible over $\mathbb{Q}$ by hypothesis. Let α be a root of f. Since $[\mathbb{Q}(\alpha):\mathbb{Q}] = 5$ and $[\mathbb{Q}(\sqrt{5}):\mathbb{Q}] = 2$, we obtain that $10 = 2\times 5$ divides $[\mathbb{Q}(\sqrt{5},\alpha):\mathbb{Q}]$, where $[\mathbb{Q}(\sqrt{5},\alpha):\mathbb{Q}] \le 10$. Therefore

  $$10 = [\mathbb{Q}(\sqrt{5},\alpha):\mathbb{Q}] = [\mathbb{Q}(\sqrt{5},\alpha):\mathbb{Q}(\sqrt{5})][\mathbb{Q}(\sqrt{5}):\mathbb{Q}],$$

  so $[\mathbb{Q}(\sqrt{5},\alpha):\mathbb{Q}(\sqrt{5})] = 5$. If p is the minimal polynomial of α over $\mathbb{Q}(\sqrt{5})$, then $\deg(p) = [\mathbb{Q}(\sqrt{5},\alpha):\mathbb{Q}(\sqrt{5})] = 5$, and p divides f, therefore $p = f$, and we have proved that f is irreducible over $\mathbb{Q}(\sqrt{5})$.

Moreover

$$\Delta(f) = 5^5 D^4 = (5^2 D^2 \sqrt{5})^2$$

is a square in $\mathbb{Q}(\sqrt{5})$, and $0 \in \mathbb{Q}(\sqrt{5})$ is a root of the resolvent

$$\Theta_f(y) = y^6 - \Delta(f) y.$$

If $\alpha = \sqrt[5]{D} \in \mathbb{R}$, and $\zeta = \zeta_5$, then

$$x^5 - D = (x-\alpha)(x-\zeta\alpha)(x-\zeta^2\alpha)(x-\zeta^3\alpha)(x-\zeta^4\alpha).$$

But $\zeta\alpha \not\in \mathbb{R}$, so $\zeta\alpha \not\in \mathbb{Q}(\sqrt{5})(\alpha) \subset \mathbb{R}$. f doesn't split completely over $F(\alpha)$, where α is a root of f. By Theorem 13.2.6 and the table 13.2.C,

$$\mathrm{Gal}(L/\mathbb{Q}(\sqrt{5})) \simeq \mathrm{AGL}(1, \mathbb{F}_5) \cap A_5,$$

where L is the splitting field of $x^5 - D$.

- Now $f = x^5 - 5Px^2 - 5Qx - \frac{Q^2}{P} - \frac{P^3}{Q}$, and f is assumed irreducible over $\mathbb{Q}$. With the same proof as in the first bullet, f remains irreducible over $\mathbb{Q}(\sqrt{5})$. By part (b),

$$\Delta = 5^5 \frac{(P^8 + 11P^4Q^3 - Q^6)^2}{P^4Q^4}$$

is a square in $\mathbb{Q}(\sqrt{5})$, and

$$\theta_f(y) = \left(y^3 + 100\,Qy^2 - 2000\left(\frac{P^4}{Q} - 2\,Q^2\right)y\right)^2 - 1024\,\Delta(f)y,$$

has root $0 \in \mathbb{Q}(\sqrt{5})$. By part (a),

$$\begin{aligned} f &= x^5 - 5Px^2 - 5Qx - \frac{Q^2}{P} - \frac{P^3}{Q} \\ &= (x-(u+v))(x-(\zeta^2u+\zeta^4v))(x-(\zeta^4u+\zeta^3v))(x-(\zeta u+\zeta^2v))(x-(\zeta^3u+\zeta v)) \end{aligned}$$

We prove that $\alpha_2 = \zeta^2 u + \zeta^4 v$ is not real. If $\alpha_2 \in \mathbb{R}$, then $\alpha_2 = \overline{\alpha_2}$, so $(\zeta^2 - \zeta^3)u + (\zeta^4 - \zeta)v = 0$.

Then, using $\sqrt{5} = \zeta - \zeta^2 - \zeta^3 + \zeta^4$ and $\zeta^2 + \zeta^3 = \frac{-1+\sqrt{5}}{2}$,

$$\begin{aligned} \frac{v}{u} &= \frac{\zeta^2 - \zeta^3}{\zeta - \zeta^4} = \frac{\zeta - \zeta^2}{1 - \zeta^3} \\ &= \frac{(\zeta - \zeta^2)(1 - \zeta^2)}{(1-\zeta^3)(1-\zeta^2)} \\ &= \frac{\zeta - \zeta^2 - \zeta^3 + \zeta^4}{1 - (\zeta^2 + \zeta^3) + \zeta^5} \\ &= \frac{\sqrt{5}}{2 + \frac{1+\sqrt{5}}{2}} \\ &= \frac{\sqrt{5} - 1}{2} \end{aligned}$$

Since $\frac{v}{u} = \frac{P}{Q}\sqrt[5]{\frac{Q^2}{P}}$, we would have $\sqrt[5]{\frac{Q^2}{P}} \in \mathbb{Q}(\sqrt{5})$, and then the root $\alpha_1 = u + v \in \mathbb{Q}(\sqrt{5})$, in contradiction with the irreducibility of f over $\mathbb{Q}(\sqrt{5})$.

So $\alpha_2 \not\in \mathbb{R}$ is not in the field $\mathbb{Q}(\sqrt{5})(\alpha_1)$, and f doesn't split completely over $\mathbb{Q}(\sqrt{5})(\alpha_1)$.

By the table 13.2.C, $\mathrm{Gal}(L/\mathbb{Q}(\sqrt{5}) \simeq \mathrm{AGL}(1, \mathbb{F}_5) \cap A_5$.

- The third Euler's polynomial is $f = x^5 - 5Px^3 + 5P^2x - D$.
  If $p = -5P, q = -D$, we obtain $f = x^5 + px^3 + \frac{1}{5}p^2x + q$, which is Example 13.2.10. We know from this example and from Exercise 14 that the Galois group of f over $\mathbb{Q}$ is $\mathrm{AGL}(1, \mathbb{F}_5)$.
  With the same proof as in the first bullet, f remains irreducible over $\mathbb{Q}(\sqrt{5})$.
  By Exercise 14,
  $$\Delta(f) = \frac{1}{5^5} \cdot (4p^5 + 3125q^2)^2$$
  is a square in the field $\mathbb{Q}(\sqrt{5})$, and
  $$\theta_f(y) = \left(y^3 - 7\,p^2y^2 + 11p^4y + \frac{3}{25}\,p^6 + 4000\,pq^2\right)^2 - 2^{10}\Delta(f)y$$
  has the root $5p^2 \in \mathbb{Q}$.
  It remains to know if f splits completely over $\mathbb{Q}(\sqrt{5})$.
  Note that
  $$f(u+v) = u^5 + v^5 + q + (u^2 + uv + v^2 + \frac{p}{5})(5uv + p)(u+v).$$
  Therefore if $uv = -\frac{p}{5}$, $f(u+v) = u^5 + v^5 + q$, so we find (see Exercise 14) that
  $$f\left(z - \frac{p}{5z}\right) = z^5 - \frac{p^5}{5^5 z^5} + q.$$
  So $u + v$ is a root of f if
  $$\left\{\begin{array}{rcl} u^5 + v^5 & = & -q = D \\ uv & = & -\frac{p}{5} = P \end{array}\right.$$
  Therefore u^5, v^5 are the roots of $x^2 + qx - (\frac{p}{5})^5$ and satisfy $uv = -p/5 \in \mathbb{Q}$.
  If $u + v$ is a root, so is $\zeta^k u + \zeta^{-k} v,\ k \in \mathbb{Z}$ (where $\zeta = \zeta_5 = e^{2i\pi/5}$).
  Conversely
  $$\begin{aligned}&(x - u - v)(x - \zeta u - \zeta^{-1}v)(x - \zeta^2 u - \zeta^{-2}v)(x - \zeta^3 u - \zeta^{-3}v)(x - \zeta^4 u - \zeta^{-4}v)\\ &= x^5 - 5uvx^3 + 5u^2v^2x - u^5 - v^5\\ &= x^5 - 5Px^3 + 5P^2x - D\end{aligned}$$
  So the roots of $f = x^5 - 5Px^3 + 5P^2x - D = x^5 + px^3 + \frac{1}{5}p^2x + q$ are
  $$u + v, \quad \zeta u + \zeta^{-1}v, \quad \zeta^2 u + \zeta^{-2}v, \quad \zeta^3 u + \zeta^{-3}v, \quad \zeta^4 u + \zeta^{-4}v,$$
  where (u, v) is a solution of the system
  $$uv = P = -\frac{p}{5}, \qquad u^5 + v^5 = D = -q,$$
  so
  $$\begin{aligned} u &= \sqrt[5]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{5}\right)^5}},\\ v &= \sqrt[5]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{5}\right)^5}},\end{aligned}$$

(where we choose the real roots, so $u, v \in \mathbb{R}$).
We obtained the factorization of f:

$$\begin{aligned} f &= x^5 - 5Px^3 + 5P^2x - D \\ &= (x-u-v)(x-\zeta u - \zeta^{-1}v)(x-\zeta^2 u - \zeta^{-2} v)(x - \zeta^3 u - \zeta^{-3} v)(x - \zeta^4 u - \zeta^{-4} v) \end{aligned}$$

If the root $\alpha_2 = \zeta u + \zeta^{-1} v$ is real, then $u = v$, so $\left(\frac{q}{2}\right)^2 + \left(\frac{p}{5}\right)^5 = 0$, and this imply $\Delta(f) = 0$, in contradiction with the assumed separability of f.
Therefore $\alpha_2 \notin \mathbb{Q}(\sqrt{5})(\alpha_1) \subset \mathbb{R}$, where $\alpha_1 = u + v \in \mathbb{R}$ is a root of f, so f doesn't split completely over $\mathbb{Q}(\sqrt{5})(\alpha_1)$.
$\mathrm{Gal}(L/\mathbb{Q}(\sqrt{5}))$ is isomorphic to $\mathrm{AGL}(1, \mathbb{F}_5) \cap A_5$.

We obtained the same Galois group for the 3 Euler's polynomials of (13.28).

□

Ex. 13.2.19 *Use the methods of this section to compute the Galois group over $\mathbb{Q}$ of each of the following polynomials. Be sure to check that they are irreducible. Remember that in Section 4.2 we learned how to factor polynomials over a finite extension of $\mathbb{Q}$.*

(a) $x^5 + x + 1$.

(b) $x^5 + 20x + 16$.

(c) $x^5 + 2$.

(d) $x^5 - 5x + 12$.

(e) $x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$.

Proof. We use the Exercise 14 resolvent() procedure to compute a sextic resolvent, and the additional procedure to verify that this resolvent has a rational root (the polynomials are supposed, as in this exercise, monic with integer coefficients, i.e., $f \in \mathbb{Z}[x]$, hence resolvent rational root is an integer):

```
def rational_root(theta):
    n = Integer(theta.subs(y=0))
    if n == 0:
        return True, 0
    for d in n.divisors():
        if theta.subs(y = d) == 0:
            return True, d
        if theta.subs(y = -d)== 0:
            return True, -d
    return False, None
```

(a)
```
R.<x> = QQ[]
f = x^5 + x + 1;f
```

$$x^5 + x + 1$$

```
f.is_irreducible()
```

False

```
f.factor()
```

$$f = (x^2 + x + 1) \cdot (x^3 - x^2 + 1)$$

The roots of $x^2 + x + 1$ are ω, ω^2. Write x_1, x_2, x_3 the roots of $x^3 - x^2 + 1$. Then $L = \mathbb{Q}(\omega, x_1, x_2, x_3)$ is the splitting field of f over $\mathbb{Q}$. As $L = \mathbb{Q}(\omega)(x_1, x_2, x_3)$, L is also the splitting field of $g = x^3 - x^2 + 1$ over $\mathbb{Q}(\omega)$. The discriminant of g is $\Delta(g) = -23$. We show that $-23 \not\in \mathbb{Q}(\omega)^2$.

If $-23 = (a + b\omega)^2,\ a, b \in \mathbb{Q}$, then $-23 = a^2 - b^2 - \omega b(b - 2a)$. Therefore

$$\left\{ \begin{array}{rcl} -23 & = & a^2 - b^2, \\ 0 & = & b(b - 2a). \end{array} \right.$$

Thus $b = 0$ or $b = 2a$. If $b = 0$, then $-23 = a^2$, which is impossible since $a \in \mathbb{Q}$, and $b = 2a$ gives $a^2 = 23/3$, which is also impossible. Therefore $\Delta(g)$ is not a square in $\mathbb{Q}(\omega)$, so the Galois group G_1 of g over $\mathbb{Q}(\omega)$ is S_3. This implies that $[L : \mathbb{Q}(\omega)] = |G_1| = 6$. Since $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$, $[L : \mathbb{Q}] = 12$, so the Galois group G of $f = x^5 + x + 1$ has order 12:

$$|G| = 12.$$

Since -23 is not a square of $\mathbb{Q}$, $\mathrm{Gal}(\mathbb{Q}(x_1, x_2, x_3)/\mathbb{Q}) \simeq S_3$.

Let

$$\varphi \left\{ \begin{array}{ccc} \mathrm{Gal}(L/\mathbb{Q}) & \to & \mathrm{Gal}(\mathbb{Q}(x_1, x_2, x_3)/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \\ \sigma & \mapsto & \left(\sigma|_{\mathbb{Q}(x_1,x_2,x_3)},\ \sigma|_{\mathbb{Q}(\omega)} \right). \end{array} \right.$$

Then φ is a group homomorphism, and the kernel of φ is $\{\mathrm{id}\}$, since every $\mathbb{Q}$-automorphism of L which fixes ω, x_1, x_2, x_3 is the identity of L. So φ is injective, and $|\mathrm{Gal}(L/\mathbb{Q})| = |\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(x_1, x_2, x_3)/\mathbb{Q})| = 12$, thefore φ is a group isomorphism.

$$\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathrm{C}_2 \times S_3.$$

If we choose the numbering $x_1, x_2, x_3, x_4 = \omega, x_5 = \omega^2$ of the roots of f, then the Galois group G of f is

$$G = \mathrm{Gal}_{\mathbb{Q}}(f) = \langle (1\,2), (1\,2\,3), (4\,5) \rangle \simeq S_3 \times C_2.$$

(b)

```
R.<x> = QQ[]
f = x^5 + 20 *x + 16;f
```

$$x^5 + 20x + 16$$

```
f.is_irreducible()
```

True

```
theta = resolvent(f)[0]; theta.subs(Delta = f.discriminant()).expand()
```

$$y^6 - 800\, y^5 + 352000\, y^4 - 71680000\, y^3 + 7168000000\, y^2 - 557056000000\, y + 6553600000000$$

```
res = rational_root(theta); res
```

$$(\text{False, None})$$

```
f.discriminant().factor(),f.discriminant().is_square()
```

$$(2^{16} \cdot 5^6, \text{True})$$

Thus the Galois group of $f = x^5 + 20x + 16$ over $\mathbb{Q}$ is A_5.
Verification:

```
f.galois_group().gens()
```

$$\langle (3,4,5), (1,2,3,4,5) \rangle$$

(c)
```
R.<x> = QQ[]
f = x^5 + 2;f
```

$$x^5 + 2$$

```
f.is_irreducible()
```

$$\text{True}$$

```
theta = resolvent(f)[0]; theta.subs(Delta = f.discriminant()).expand()
```

$$y^6 - 51200000\, y$$

```
res = rational_root(theta); res
```

$$(\text{True, } 0)$$

```
f.discriminant().factor(),f.discriminant().is_square()
```

$$(2^4 \cdot 5^5, \text{False})$$

Thus the Galois group of $f = x^5 + 2$ over $\mathbb{Q}$ is $\mathrm{AGL}(1, \mathbb{F}_5)$, up to conjugacy.
Verification:

```
f.galois_group().gens()
```

$$\langle (1,2,3,4,5), (1,2,4,3) \rangle$$

(d)
```
R.<x> = QQ[]
f = x^5 -5*x + 12;f
```

$$x^5 - 5x + 12$$

```
f.is_irreducible()
```

$$\text{True}$$

```
theta = resolvent(f)[0]; theta.subs(Delta = f.discriminant()).expand()
```

$$y^6 + 200\,y^5 + 22000\,y^4 + 1120000\,y^3 + 28000000\,y^2 - 66016000000\,y + 1600000000$$

```
res = rational_root(theta); res
```

$$(\text{True}, 100)$$

```
f.discriminant().factor(),f.discriminant().is_square()
```

$$(2^{12} \cdot 5^6, \text{True})$$

```
K.<alpha> = NumberField(f)
S.<X> = K[]
g = f.change_ring(S)
g.factor()
```

$$(x-\alpha)\cdot\left(x^2+\left(\frac{1}{4}\alpha^4+\frac{1}{4}\alpha^3+\frac{1}{4}\alpha^2+\frac{1}{4}\alpha-1\right)x-\frac{1}{2}\alpha^3-\frac{1}{2}\alpha-1\right)$$
$$\cdot\left(x^2+\left(-\frac{1}{4}\alpha^4-\frac{1}{4}\alpha^3-\frac{1}{4}\alpha^2+\frac{3}{4}\alpha+1\right)x-\frac{1}{4}\alpha^4-\frac{1}{4}\alpha^3-\frac{1}{4}\alpha^2-\frac{5}{4}\alpha+2\right)$$

Thus the Galois group of $f = x^5 + 20x + 16$ over $\mathbb{Q}$ is $\mathrm{AGL}(1, \mathbb{F}_5) \cap A_5$, up to conjugacy.

Verification:

```
f.galois_group().gens()
```

$$\langle (1,2,3,4,5), (1,4)(2,3) \rangle$$

(e)
```
R.<x> = QQ[]
f = x^5 + x^4 - 4*x^3 - 3*x^2 + 3*x + 1
f
```

$$x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$$

```
f.is_irreducible()
```

$$\text{True}$$

```
theta = resolvent(f)[0]; theta.subs(Delta = f.discriminant()).expand()
```

$$y^6 - 264\,y^5 + 25168\,y^4 - 1022208\,y^3 + 14992384\,y^2 - 14992384\,y$$

```
res = rational_root(theta); res
```

$$(\text{True}, 0)$$

```
f.discriminant().factor(),f.discriminant().is_square()
```

$$(11^4, \text{True})$$

```
K.<alpha> = NumberField(f)
S.<X> = K[]
g = f.change_ring(S)
g.factor()
```

$$(x-\alpha)\cdot(x-\alpha^2+2)\cdot(x+\alpha^4+\alpha^3-3\alpha^2-2\alpha+1)\cdot(x-\alpha^3+3\alpha)\cdot(x-\alpha^4+4\alpha^2-2)$$

Thus the Galois group of $f = x^5+20x+16$ over $\mathbb{Q}$ is $\langle(1\,2\,3\,4\,5)\rangle$, up to conjugacy.
Verification:

```
f.galois_group().gens()
```

$$\langle(1,2,3,4,5)\rangle$$

□

Ex. 13.2.20 *In the Mathematical Notes to Section 10.3, we noted that the roots of the polynomial $x^5-4x^4+2x^3+4x^2+2x-6 \in \mathbb{Q}[x]$ can be constructed using a marked ruler and compass. Show that this polynomial is not solvable by radicals over $\mathbb{Q}$.*

Proof. With the same procedures as in Exercise 19, we obtain

```
R.<x> = QQ[]
f = x^5 - 4*x^4 + 2*x^3 + 4 *x^2 + 2*x -6;f
```

$$x^5-4x^4+2x^3+4x^2+2x-6$$

```
f.is_irreducible()
```

$$\text{True}$$

```
theta = resolvent(f)[0]; theta.subs(Delta = f.discriminant()).expand()
```

$$y^6-360\,y^5+47856\,y^4-3025152\,y^3+103474944\,y^2-1812875264\,y+14770999296$$

```
res = rational_root(theta); res
```

$$(\text{False}, \text{None})$$

```
f.discriminant().factor(),f.discriminant().is_square()
```

$$(-1\cdot 2^4\cdot 4003, \text{False})$$

So the Galois group of f is S_5, and f is not solvable by radicals over $\mathbb{Q}$.
Verification:

```
f.galois_group().gens()
```

$$\langle(1,2),(1,2,3,4,5)\rangle$$

□

13.3 Resolvents

Ex. 13.3.1 *Let $f(x) \in \mathbb{Q}[x]$.*

(a) Prove that there are $\lambda, \mu \in \mathbb{Q}^*$ such that $g(x) = \lambda f(\mu x) \in \mathbb{Z}[x]$ is monic.

(b) Prove that f and g have isomorphic Galois groups over $\mathbb{Q}$.

Proof.

(a) Let $f(x) = \frac{a_0}{b_0}x^n + \frac{a_1}{b_1}x^{n-1} + ... + \frac{a_n}{b_n} = \sum_{i=0}^n \frac{a_i}{b_i}x^{n-i}$, where $a_i, b_i \in \mathbb{Z}$, and $\nu = \operatorname{lcm}(b_0, b_1, ..., b_n)$, then $\nu f(x) = \sum_{i=0}^n \frac{a_i}{b_i}\nu x^{n-i} = \sum_{i=0}^n c_i x^{n-i}$, where $c_i = \frac{a_i}{b_i}\nu \in \mathbb{Z}$.

After multiplication by c_0^{n-1} we have

$$c_0^{n-1}f(x) = \sum_{i=0}^n c_i c_0^{n-1} x^{n-i} = (c_0 x)^n + \sum_{i=1}^n c_i c_0^{i-1}(c_0 x)^{n-i} = g(c_0 x),\ c_i c_0^{i-1} \in \mathbb{Z}.$$

Hence $g(x)$ is monic and $g(x) = \lambda f(\mu x) \in \mathbb{Z}[x]$, where $\lambda = c_0^{n-1}\nu, \mu = 1/c_0, c_0 = \frac{a_0}{b_0}\nu$, i.e. $\lambda, \mu \in \mathbb{Q}^*$.

(b) If $\alpha_1, \ldots, \alpha_n$ are the roots of f in a splitting field $L = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ of f over $\mathbb{Q}$, then $\beta_1 = \alpha_1/\mu, \ldots, \beta_n = \alpha_n/\mu$ are the roots of g in L, which splits completely over L, so L is also a splitting field of g. Then

$$G_f \simeq \operatorname{Gal}(L/F) \simeq G_g.$$

Thus the Galois groups G_f, G_g of f, g over $\mathbb{Q}$ are isomorphic.

Note: If $\tau \in G_f \subset S_n$ corresponds to σ for a given numbering of the roots $\alpha_1, \ldots, \alpha_n$ of f, for the corresponding numbering $\beta_1, \ldots, \beta_n$, $\tau \in G_g$, so $G_f = G_g$ for these chosen numbering.

□

Ex. 13.3.2 *Let $f(x) = x^n - c_1 x^{n-1} + ... + (-1)^n c_n \in \mathbb{Z}[x]$, and let $\Theta_f(y)$ be the resolvent built from $\varphi \in \mathbb{Z}[x_1, ..., x_n]$. Prove that $\Theta_f(y) \in \mathbb{Z}[y]$.*

Proof. Let G be the symmetry group of φ and $\tau_1, ..., \tau_l$ be representatives for the left cosets of G in S_n. The universal resolvent is $\Theta(y) = \prod_{i=1}^l (y - (\tau_i \cdot \varphi)(x_1, ..., x_n))$. Since $\varphi \in \mathbb{Z}[x_1, ..., x_n]$, for each $i, 1 \leq i \leq l$, $(\tau_i \cdot \varphi)(x_1, ..., x_n) \in \mathbb{Z}[x_1, ..., x_n]$, hence the coefficients of $\Theta(y)$ are in $\mathbb{Z}[x_1, ..., x_n]$, i.e., $\Theta(y) \in \mathbb{Z}[x_1, ..., x_n][y]$.

Suppose that $\sigma \in S_n$, then $(\sigma \cdot \Theta)(y) = \prod_{i=1}^l (y - (\sigma\tau_i) \cdot \varphi(x_1, ..., x_n))$. But the set $\sigma\tau_1, ..., \sigma\tau_l$ is also a set of left coset representatives of G in S_n. Thus the application of σ has merely permuted the roots of $\Theta(y)$ leaving the coefficients fixed. It means that coefficients of $\Theta(y)$ are symmetric and are polynomials in $\sigma_1, ..., \sigma_n$ with integers coefficients (cf. Ex.9.1.6), i.e., $\Theta(y) \in \mathbb{Z}[\sigma_1, ..., \sigma_n][y]$. The application of evaluation map $x_i \mapsto \alpha_i$ to $\Theta(y)$, so that $\sigma_i \mapsto c_i$, gives $\Theta_f(y) \in \mathbb{Z}[c_1, ..., c_n][y] = \mathbb{Z}[y]$. □

Ex. 13.3.3 *In the proof of proposition 13.3.2, we asserted that*

$$\varphi(\alpha_1, ..., \alpha_n) = \varphi(\alpha_{\tau(1)}, ..., \alpha_{\tau(n)})$$

follows from $\beta = \varphi(\alpha_1, ..., \alpha_n) \in F$ and $\tau \in G_f$. Prove this.

Proof. Let $\sigma \in \mathrm{Gal}(L/F)$ corresponding to $\tau \in G_f$, so that $\sigma(\alpha_i) = \alpha_{\tau(i)},\ i = 1, \dots, n$.
Since F is fixed for σ, and $\beta = \varphi(\alpha_1, ..., \alpha_n) \in F$, $\beta = \sigma(\beta)$, so that

$$\varphi(\alpha_1, ..., \alpha_n) = \sigma(\varphi(\alpha_1, ..., \alpha_n)).$$

Moreover

$$\begin{aligned}\sigma(\varphi(\alpha_1, ..., \alpha_n)) &= \varphi(\sigma(\alpha_1), \dots, \sigma(\alpha_n) \\ &= \varphi(\alpha_{\tau(1)}, ..., \alpha_{\tau(n)}).\end{aligned}$$

Therefore, $\varphi(\alpha_1, ..., \alpha_n) = \varphi(\alpha_{\tau(1)}, ..., \alpha_{\tau(n)})$ for $\varphi(\alpha_1, ..., \alpha_n) \in F$ and $\tau \in G_f$. □

Ex. 13.3.4 *As in Examples 13.3.3 and 13.3.4, let* $\varphi = \sqrt{\Delta}(x_1 + x_2 - x_3 - x_4)$.

(a) *Show that the symmetry group of* φ *is* $G = \langle(1324)\rangle \subset S_4$ *in characteristic* $\neq 2$.

(b) *Show that in the universal case,* φ *leads to the resolvent*

$$\Theta(y) = \prod_{i=1}^{3}(y^2 - \Delta(4y_i + \sigma_1^2 - 4\sigma_2)),$$

where $y_1 = x_1x_2 + x_3x_4, y_2 = x_1x_3 + x_2x_4, y_3 = x_1x_4 + x_2x_3$ *are the roots of the universal Ferrari resolvent* $\theta(y)$.

(c) *Let* $\Theta_f(y)$ *be obtained by specializing the resolvent* $\Theta(y)$ *of part (b) to* $f = x^4 + bx^2 + d$. *Show that*

$$\Theta_f(y) = y^2((y^2 + 4b\Delta(f))^2 - 2^6 d\Delta(f)^2).$$

Proof.

(a) Write $H(\varphi)$ the symmetry group of $\varphi = \sqrt{\Delta}\,(x_1 + x_2 - x_3 - x_4)$.
Since $(1\,3\,2\,4)$ is an odd permutation, $(1\,3\,2\,4) \cdot \sqrt{\Delta} = -\sqrt{\Delta}$, so

$$(1\,3\,2\,4) \cdot \varphi = -\sqrt{\Delta}\,(x_3 + x_4 - x_2 - x_1) = \varphi.$$

Therefore

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

To prove the converse, we show that the orbit $\mathcal{O}_\varphi$ of φ under the action of S_n contains at least 6 elements.

σ	$\sigma \cdot (x_1 + x_2 - x_3 - x_4)$	$\sigma \cdot \varphi$
$()$	$x_1 + x_2 - x_3 - x_4$	$\sqrt{\Delta}(x_1 + x_2 - x_3 - x_4)$
$(3\,4)$	$x_1 + x_2 - x_3 - x_4$	$\sqrt{\Delta}(-x_1 - x_2 + x_3 + x_4)$
$(2\,3)$	$x_1 - x_2 + x_3 - x_4$	$\sqrt{\Delta}(-x_1 + x_2 - x_3 + x_4)$
$(1\,4)$	$-x_1 + x_2 - x_3 + x_4$	$\sqrt{\Delta}(x_1 - x_2 + x_3 - x_4)$
$(1\,3)$	$-x_1 + x_2 + x_3 - x_4$	$\sqrt{\Delta}(x_1 - x_2 - x_3 + x_4)$
$(2\,4)$	$x_1 - x_2 - x_3 + x_4$	$\sqrt{\Delta}(-x_1 + x_2 + x_3 - x_4)$

Since the six elements in the right column are distinct (if the characteristic is not 2), we see that $|\mathcal{O}_\varphi| \geq 6$.

The stabilizer G_φ of φ in S_n is $H(\varphi)$, which contains $\langle (1\,3\,2\,4)\rangle$, therefore $|G_\varphi| \ge 4$, and $|\mathcal{O}_\varphi| = \frac{|S_n|}{|G_\varphi|} \le \frac{24}{4} = 6$, so $|\mathcal{O}_\varphi| = 6$ and $|H(\varphi)| = |G_\varphi| = 4$, thus

$$\langle (1\,3\,2\,4)\rangle \subset H(\varphi),$$

and the orbit of φ under S_4 is given by $\mathcal{O}_\varphi = \{\varphi_0 = \varphi, \varphi_1, \dots, \varphi_5\}$, where

$$\begin{aligned}
\varphi_0 &= \quad () \cdot \varphi = \sqrt{\Delta}\,(x_1 + x_2 - x_3 - x_4),\\
\varphi_1 &= (3\,4) \cdot \varphi = \sqrt{\Delta}\,(-x_1 - x_2 + x_3 + x_4),\\
\varphi_2 &= (2\,3) \cdot \varphi = \sqrt{\Delta}\,(-x_1 + x_2 - x_3 + x_4),\\
\varphi_3 &= (1\,4) \cdot \varphi = \sqrt{\Delta}\,(x_1 - x_2 + x_3 - x_4),\\
\varphi_4 &= (1\,3) \cdot \varphi = \sqrt{\Delta}\,(x_1 - x_2 - x_3 + x_4),\\
\varphi_5 &= (2\,4) \cdot \varphi = \sqrt{\Delta}\,(-x_1 + x_2 + x_3 - x_4).
\end{aligned}$$

(b) Since $\varphi_1 = -\varphi_0, \varphi_3 = -\varphi_2, \varphi_5 = -\varphi_4$,

$$\begin{aligned}
\Theta(y) &= \prod_{\psi \in \mathcal{O}_\varphi} (y - \psi) = \prod_{i=0}^{5} (y - \varphi_i)\\
&= (y^2 - \varphi_0^2)(y^2 - \varphi_2^2)(y^2 - \varphi_4^2).
\end{aligned}$$

Moreover,

$$\varphi_0^2 = \Delta(x_1 + x_2 - x_3 - x_4)^2,$$

where

$$\begin{aligned}
(x_1 + x_2 - x_3 - x_4)^2 &= (x_1 + x_2)^2 + (x_3 + x_4)^2 - 2(x_1 + x_2)(x_3 + x_4)\\
&= (x_1 + x_2 + x_3 + x_4)^2 - 4(x_1 + x_2)(x_3 + x_4)\\
&= (x_1 + x_2 + x_3 + x_4)^2 - 4(x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4)\\
&= 4(x_1x_2 + x_3x_4) + (x_1 + x_2 + x_3 + x_4)^2\\
&\qquad - 4(x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4)\\
&= 4y_1 + \sigma_1^2 - 4\sigma_2.
\end{aligned}$$

Thus

$$(y - \varphi_0)^2 = y^2 - \Delta(4y_1 + \sigma_1^2 - 4\sigma_2),$$

where $y_1 = x_1x_2 + x_3x_4$.

If we apply the permutation $(2\,3)$ on this equality, we obtain

$$(y - \varphi_2)^2 = y^2 - \Delta(4y_2 + \sigma_1^2 - 4\sigma_2),$$

where $y_2 = x_2x_4 + x_1x_3$.

If we apply the permutation $(1\,3)$ on the same equality, we obtain

$$(y - \varphi_4)^2 = y^2 - \Delta(4y_3 + \sigma_1^2 - 4\sigma_2),$$

where $y_3 = x_4x_1 + x_3x_2$.

Finally,

$$\Theta(y) = \prod_{i=1}^{3} \left(y^2 - \Delta(4y_i + \sigma_1^2 - 4\sigma_2)\right),$$

where $y_1 = x_1x_2 + x_3x_4, y_2 = x_1x_3 + x_2x_4, y_3 = x_1x_4 + x_2x_3$ are the roots of the universal Ferrari resolvent $\theta(y)$.

(c) Let $\Theta_f(y)$ is obtained by specializing the resolvent $\Theta(y)$ of part (b) to $f = x^4 + bx^2 + d$. Then x_i maps to the root α_i, $i = 1, \ldots, 4$, σ_1 maps to 0, σ_2 to b, Δ to $\Delta(f)$, and y_i to β_i,where

$$\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4, \qquad \beta_2 = \alpha_2\alpha_4 + \alpha_1\alpha_3, \qquad \beta_3 = \alpha_4\alpha_1 + \alpha_3\alpha_2$$

are the roots of the Ferrari resolvent of $x^4 + bx^2 + d$.

We obtain

$$\begin{aligned}
\Theta_f(y) &= \prod_{i=1}^{3} \left(y^2 - \Delta(f)(4\beta_i - 4b)\right) \\
&= \prod_{i=1}^{3} (y^2 + 4b\Delta(f) - 4\Delta(f)\beta_i)
\end{aligned}$$

If we write for simplicity

$$u = y^2 + 4b\Delta(f), \qquad v = 4\Delta(f) \neq 0,$$

then

$$\begin{aligned}
\Theta_f(y) &= \prod_{i=1}^{3} (u - v\beta_i) \\
&= v^3 \prod_{i=1}^{3} \left(\frac{u}{v} - \beta_i\right).
\end{aligned}$$

We know from Exercise 13.1.10 that the Ferrari resolvent of $x^4 + bx^2 + d$ is

$$\Theta_f(y) = (y - \beta_1)(y - \beta_2)(y - \beta_3) = (y - b)(y^2 - 4d).$$

The substitution $y \mapsto \frac{u}{v}$ gives

$$\begin{aligned}
\Theta_f(y) &= v^3 \left(\frac{u}{v} - \beta_1\right)\left(\frac{u}{v} - \beta_2\right)\left(\frac{u}{v} - \beta_3\right) \\
&= v^3 \left(\frac{u}{v} - b\right)\left(\frac{u^2}{v^2} - 4d\right) \\
&= (u - bv)(u^2 - 4dv^2) \\
&= y^2 \left((y^2 + 4b\Delta(f))^2 - 4d(4\Delta(f))^2\right) \\
&= y^2 \left((y^2 + 4b\Delta(f))^2 - 2^6 d\Delta(f)^2\right).
\end{aligned}$$

$\square$

Ex. 13.3.5 *This problem will state and prove a relative version of Proposition 13.3.2. Fix a subgroup $H \subset S_n$ and suppose that $f \in F[x]$ is separable of degree n and that $G_f \subset H$. Now let $G \subset H$ be a subgroup. We want to know whether or not G_f lies in the smaller subgroup G. Let $\varphi \in F[x_1, ..., x_n]$ have G as its symmetry group and let $\varphi_1 = \varphi, \varphi_2, ..., \varphi_l$ be the orbit of H acting on φ. Then set*

$$\Theta^H(y) = \prod_{i=1}^{l}(y - \varphi_i) \in F[x_1, ..., x_n][y].$$

Finally, if $\alpha_1, ..., \alpha_n$ are the roots of f in the splitting field L, let

$$\Theta^H_f(y) = \prod_{i=1}^{l}(y - \varphi_i(\alpha_1, ..., \alpha_n)) \in L[y]$$

be the polynomial obtained by $x_i \mapsto \alpha_i$.

(a) Explain why the degree of $\Theta^H_f(y)$ is the index of G in H.

(b) Prove that $\Theta^H_f(y) \in F[y]$.

(c) Assume that G_f is conjugate within H to a subgroup of G (this means that $\tau G_f \tau^{-1} \subset G$ for some $\tau \in H$). Prove that $\Theta^H_f(y)$ has a root in F.

(d) Assume that $\Theta^H_f(y)$ has a simple root in F. Prove that G_f is conjugate within H to a subgroup of G.

Proof.

(a) G is the symmetry group of φ, therefore $G \subset H$ is the isotropy subgroup of φ under the action of H ($\mathrm{Stab}_H(\varphi) = H \cap \mathrm{Stab}_{S_n}(\varphi) = H \cap G = G$), and $[H : G] = |H \cdot \varphi| = l$ (cf. Theorem A.4.9). The degree of $\Theta^H_f(y)$ is equal to l, hence $\deg(\Theta^H_f(y)) = [H : G]$.

(b) Let $\tau_1, ..., \tau_l$ be representatives for the left cosets of G in H. Then

$$\Theta^H_f(y) = \prod_{i=1}^{l}(y - (\tau_i \cdot \varphi)(\alpha_1, ..., \alpha_n)).$$

Since $\varphi \in F[x_1, ..., x_n]$, for each $i, 1 \le i \le l$, $(\tau_i \cdot \varphi)(\alpha_1, ..., \alpha_n) = \varphi(\alpha_{\tau_i(1)}, \dots, \alpha_{\tau_i(n)}) \in F[\alpha_1, ..., \alpha_n]$, hence the coefficients of $\Theta^H_f(y)$ are in $F[\alpha_1, ..., \alpha_n]$.

Suppose $\sigma \in G_f$, then $\sigma \in H$ and $\sigma \cdot \Theta^H_f(y) = \prod_{i=1}^{l}(y - (\sigma\tau_i) \cdot \varphi(\alpha_1, ..., \alpha_n))$. But the set $\sigma\tau_1, ..., \sigma\tau_l$ is also a set of left coset representatives of G in H. Thus the action of σ has merely permuted the roots of $\Theta^H_f(y)$ leaving the coefficients fixed. It means that the coefficients of $\Theta^H_f(y)$ are in F, i.e., $\Theta^H_f(y) \in F[y]$.

(c) Assume that G_f is congugate within H to a subgroup K of G, so that $G_f = \tau K \tau^{-1}, \tau \in H$. Then $\tau^{-1} G_f \tau \subset G$.

Let $\tilde{\sigma} \in \mathrm{Gal}(L/F)$ (where $L = F(\alpha_1, \dots, \alpha_n)$), and $\sigma \in G_f$ the associated permutation, so that $\tilde{\sigma}(\alpha_i) = \alpha_{\sigma(i)},\ i = 1, \dots, n$. Since $\tau^{-1}\sigma\tau \in G$ fixes φ, $(\tau^{-1}\sigma\tau) \cdot \varphi = \varphi$, so that

$$\begin{aligned}
\tilde{\sigma}((\tau\cdot\varphi)(\alpha_1,\dots,\alpha_n)) &= \tilde{\sigma}(\varphi(\alpha_{\tau(1)},\dots,\alpha_{\tau(n)})\\
&= \varphi(\tilde{\sigma}(\alpha_{\tau(1)}),\dots,\tilde{\sigma}(\alpha_{\tau(n)}))\\
&= \varphi(\alpha_{(\sigma\tau)(1)},\dots,\alpha_{(\sigma\tau)(n)})\\
&= ((\sigma\tau)\cdot\varphi)(\alpha_1,\dots,\alpha_n)\\
&= (\tau\cdot((\tau^{-1}\sigma\tau)\cdot\varphi))(\alpha_1,\dots,\alpha_n)\\
&= (\tau\cdot\varphi)(\alpha_1,\dots,\alpha_n).
\end{aligned}$$

Since this is true for any $\tilde{\sigma}\in \mathrm{Gal}(L/F)$, this proves that $(\tau\cdot\varphi)(\alpha_1,\dots,\alpha_n)\in F$.

Moreover $\tau\in H$, thus $\tau\cdot\varphi$ is in the orbit $H\cdot\varphi$, so $\beta=(\tau\cdot\varphi)(\alpha_1,\dots,\alpha_n)$ is a root of $\Theta_\varphi^H(y)=\prod\limits_{\psi\in H\cdot\varphi}(y-\psi)$, and β is in F.

(d) We mimic the proof of Proposition 13.3.2, with an explicitation of the relabeling of the roots, as in part (c).

Let β be a simple root of $\Theta_f^H(y)$ in F. By definition of $\Theta_f^H(y)$, there is $\tau\in H$ such that

$$\beta=(\tau\cdot\varphi)(\alpha_1,\dots,\alpha_n)=\varphi(\alpha_{\tau(1)},\dots,\alpha_{\tau(n)}).$$

We will prove that $\tau^{-1}G_f\tau\subset G$. If not, there is some $\sigma\in\tau^{-1}G_f\tau$ such that $\sigma\notin G$.

Then $\sigma'=\tau\sigma\tau^{-1}\in G_f$ corresponds to some $\rho\in\mathrm{Gal}(L/F)$, so that $\rho(\alpha_i)=\alpha_{\sigma'(i)}$, $i=1,\dots,n$.

Since $\beta\in F$, $\beta=\rho(\beta)$, so that

$$\begin{aligned}
\beta &= \rho(\varphi(\alpha_{\tau(1)},\dots,\alpha_{\tau(n)})\\
&= \varphi(\rho(\alpha_{\tau(1)}),\dots,\rho(\alpha_{\tau(n)}))\\
&= \varphi(\alpha_{(\sigma'\tau)(1)},\dots,\alpha_{(\sigma'\tau)(n)})\\
&= \varphi(\alpha_{(\tau\sigma)(1)},\dots,\alpha_{(\tau\sigma)(n)})\\
&= ((\tau\sigma)\cdot\varphi)(\alpha_1,\cdots,\alpha_n)
\end{aligned}$$

We conclude that

$$(\tau\cdot\varphi)(\alpha_1,\dots,\alpha_n)=((\tau\sigma)\cdot\varphi)(\alpha_1,\cdots,\alpha_n)\qquad(=\beta).$$

Since β is a root of Θ_f^H, $y-\beta=y-(\tau\cdot\varphi)(\alpha_1,\dots,\alpha_n)$ is a factor of $\Theta_f^H(y)$.

But $\sigma\notin G$, thus $\varphi\neq\sigma\cdot\varphi$, therefore $\tau\cdot\varphi\neq(\tau\sigma)\cdot\varphi$.

From $\tau\in H, G_f\subset H$, and $\sigma\in\tau^{-1}G_f\tau$, we know that $\tau\sigma\in H$, thus

$$(y-((\tau\sigma)\cdot\varphi)(\alpha_1,\cdots,\alpha_n)$$

is another factor of $\Theta_f^H(y)$, therefore the relative resolvent may be written

$$\begin{aligned}
\Theta_f^H(y) &= (y-(\tau\cdot\varphi)(\alpha_1,\dots,\alpha_n))(y-((\tau\sigma)\cdot\varphi(\alpha_1,\dots,\alpha_n))\cdots\\
&= (y-\beta)^2\cdots
\end{aligned}$$

This is a contradiction, since by assumption β is a simple root of $\Theta_f^H(y)$. This proves that $\tau^{-1}G_f\tau\subset G$. If $K=\tau^{-1}G_f\tau$, K is a subgroup of G, and $G_f=\tau K\tau^{-1},\tau\in H$, is conjugate within H to a subgroup of G. $\square$

Ex. 13.3.6 *Let* $D = \sum_{\sigma \in A_4} \sigma \cdot x_1^3 x_2^2 x_3 \in F[x_1, x_2, x_3, x_4]$.

(a) Prove that $D = \frac{1}{2}(\sigma_1\sigma_2\sigma_3 - 3\sigma_1^2\sigma_4 - 3\sigma_3^2 + 4\sigma_2\sigma_4) + \frac{1}{2}\sqrt{\Delta}$ *in characteristic* $\neq 2$.

(b) Prove that $\sqrt{\Delta} = D - (12) \cdot D$ *in all characteristics.*

Proof.

(a) Since

$$\sum_{\sigma \in S_4} \sigma = \sum_{\sigma \in A_4} \sigma + \sum_{\sigma \in S_4 \setminus A_4} \sigma = \sum_{\sigma \in A_4} \sigma + (12) \cdot \sum_{\sigma \in A_4} \sigma$$

and based on results of Ex.2.2.3, we have:

$$\sum_{\sigma \in S_4} \sigma \cdot x_1^3 x_2^2 x_3 = D + (12) \cdot D = \sigma_1\sigma_2\sigma_3 - 3\sigma_1^2\sigma_4 - 3\sigma_3^2 + 4\sigma_2\sigma_4$$

Sage verification:

```
R.<x1,x2,x3,x4,y1,y2,y3,y4> = PolynomialRing(QQ, order = 'degrevlex')
elt = SymmetricFunctions(QQ).e()
e = [elt([i]).expand(4).subs(x0=x1, x1=x2, x2=x3, x3 = x4) for i in range(5)]
J = R.ideal(e[1]-y1, e[2]-y2, e[3]-y3,e[4]-y4)
G = J.groebner_basis()
D = x1^3*x2^2*x3;
D=D+D.subs(x1=x3,x2=x4,x3=x1)+D.subs(x1=x2,x2=x1,x3=x4)+D.subs(x1=x4,x2=x3,x3=x2)
D=D+D.subs(x1=x2,x2=x3,x3=x1)+D.subs(x1=x2,x2=x3,x3=x1).subs(x1=x2,x2=x3,x3=x1)
u=D+D.subs(x1=x2,x2=x1)
var('sigma_1,sigma_2,sigma_3,sigma_4')
u.reduce(G).subs(y1=sigma_1, y2 = sigma_2,y3=sigma_3,y4=sigma_4)
```

$$\sigma_1\sigma_2\sigma_3 - 3\sigma_1^2\sigma_4 - 3\sigma_3^2 + 4\sigma_2\sigma_4$$

Assuming that $D - (12) \cdot D = \sqrt{\Delta}$ is valid, then $2D \neq 0$ in characteristic $\neq 2$ and

$$2D = 2(\frac{1}{2}(\sigma_1\sigma_2\sigma_3 - 3\sigma_1^2\sigma_4 - 3\sigma_3^2 + 4\sigma_2\sigma_4) + \frac{1}{2}\sqrt{\Delta}).$$

(b) We use Sage to prove that $D - (12) \cdot D - \sqrt{\Delta} = 0$:

```
Delta = (x1-x2)*(x1-x3)*(x1-x4)*(x2-x3)*(x2-x4)*(x3-x4)
D-D.subs(x1=x2,x2=x1)-Delta==0
```

True

Hence in all characteristics

$$\sqrt{\Delta} = D - (12) \cdot D.$$

∎

Ex. 13.3.7 *As in Example 13.3.7, let $f = x^4 + (u+1)x^2 + ux + 1 \in F[x]$, where $F = \mathbb{F}_2(u)$.*

(a) Use Gauss's Lemma and the Schönemann-Eisenstein criterion to show that f is irreducible over F. (These results apply since $\mathbb{F}_2[u]$ is a PID.)

(b) Verify the formulas for $D_f(y)$ and $\theta_f(y)$ given in Example 13.3.7.

(c) Show that $y^2 + uy + 1$ is irreducible over the splitting field of $D_f(y)$.

Proof.

(a) u is a prime of the PID $\mathbb{F}_2[u]$, but the reduction modulo u is $\overline{f} = x^4 + x^2 + 1$, which is not irreducible, since $x^4 + x^2 + 1 = (x^2 + x + 1)^2$. Nor the Schönemann-Eisenstein not the reduction modulo u applies here.

We give a direct proof of the irreducibility of f, by proving that f has no factor with degree 1 ou 2. By Gauss's Lemma, if f has no factorisation in $\mathbb{F}_2[[u][x]$, then f is irreducible in $\mathbb{F}_2[u](x)$.

• If f has a factor with degree 1, then f has a root $\frac{a(u)}{b(u)} \in \mathbb{F}_2(u)$, where $a(u), b(u)$ are relatively prime. Then

$$a(u)^4 + (u+1)a(u)^2 b(u)^2 + ua(u)b(u)^3 + b(u)^4 = 0,$$

therefore $a \mid b^4$, and $a \wedge b = 1$, hence $a \mid 1$, and similarly $b \mid 1$. Thus $a, b \in \mathbb{F}_2$, where $a \neq 0, b \neq 0$, so that $a(u) = b(u) = 1$. But $f(1) = 1 \neq 0$, therefore f has no factor with degree 1 in $F[x]$.

• If f has a factor with degree 2, then

$$f = (a(u)x^2 + b(u)x + c(u))(d(u)x^2 + e(u)x + f(u),$$

where a, b, c, d, e, f are in $\mathbb{F}_2[u]$. Since $a(u)d(u) = 1$, $a(u)$ and $d(u)$ are units of $\mathbb{F}_2[u]$, so are in F_2, therefore $a(u) = d(u) = 1$, and similarly $c(u) = f(u) = 1$, so that

$$f = (x^2 + b(u)x + 1)(x^2 + e(u)x + 1).$$

The comparison of the terms in x^3 gives $b(u) + e(u) = 0$, so that

$$\begin{aligned} f &= (x^2 + b(u)x + 1)(x^2 - b(u)x + 1) \\ &= (x^2 + 1)^2 - b(u)^2 x^2 \\ &= x^4 - b(u)^2 x^2 + 1. \end{aligned}$$

This is a contradiction, since f has a nonzero term $ux, u \neq 0$. Therefore f is irreducible over F.

Sage verification:

```
F = Frac(GF(2)['u']); u = F.gen()
f = x^4 + (u+1)*x^2 + u*x +1
f.is_irreducible()
```

True

```
gcd(f,f.derivative(x))
```

This is a verification that f is irreducible, separable.

(b) For the given polynomial $c_1 = \sigma_1 = 0, c_2 = \sigma_2 = u+1, c_3 = \sigma_3 = -u, c_4 = \sigma_4 = 1$. For $D_f(y)$ we have (cf. Ex.13.3.6,13.3.4 and (13.3),(13.32)):

$$A = D(f) + D'(f) = \sigma_1\sigma_2\sigma_3 - 3\sigma_1^2\sigma_4 - 3\sigma_3^2 + 4\sigma_2\sigma_4 = \sigma_3^2 = c_3^2 = u^2 \pmod 2$$
$$B = D(f)D'(f) = c_2^3c_3^2 + c_3^4 = (u+1)^3u^2 + u^4 = u^5 + u^3 + u^2 \pmod 2$$
$$D_f(y) = y^2 - Ay + B = y^2 + u^2y + u^5 + u^3 + u^2$$

$$a = \sigma_2 = c_2 = u+1,\ b = \sigma_1\sigma_3 - 4\sigma_4 = c_1c_3 - 4c_4 = 0,$$
$$c = \sigma_1^2\sigma_4 + \sigma_3^2 - 4\sigma_2\sigma_4 = c_1^2c_4 + c_3^2 - 4c_2c_4 = u^2$$
$$\theta_f(y) = y^3 - ay^2 + by - c = y^3 + (u+1)y^2 + u^2 = (y+u)(y^2+y+u)$$

Sage verification:

```
R.<x1,x2,x3,x4,y1,y2,y3,y4> = PolynomialRing(QQ, order = 'degrevlex')
elt = SymmetricFunctions(QQ).e()
e = [elt([i]).expand(4).subs(x0=x1, x1=x2, x2=x3, x3 = x4) for i in range(5)]
J = R.ideal(e[1]-y1, e[2]-y2, e[3]-y3,e[4]-y4)
G = J.groebner_basis()
D = x1^3*x2^2*x3;
D=D+D.subs(x1=x3,x2=x4,x3=x1)+D.subs(x1=x2,x2=x1,x3=x4)
  +D.subs(x1=x4,x2=x3,x3=x2)
D=D+D.subs(x1=x2,x2=x3,x3=x1)
  +D.subs(x1=x2,x2=x3,x3=x1).subs(x1=x2,x2=x3,x3=x1)
d1=x1*x2+x3*x4;d2=d1.subs(x2=x3,x3=x2);d3=d1.subs(x1=x3,x3=x1);
S1=d1+d2+d3; S2=d1*d2+d1*d3+d2*d3; S3=d1*d2*d3

S.<c1,c2,c3,c4,u> = PolynomialRing(ZZ, order = 'degrevlex')
A=(D+D.subs(x1=x2,x2=x1)).reduce(G).subs(y1=c1,y2=c2,y3=c3,y4=c4)
A=A.subs(c1=0,c2=u+1,c3=-u,c4=1).change_ring(GF(2));
B=(D*D.subs(x1=x2,x2=x1)).reduce(G).subs(y1=c1,y2=c2,y3=c3,y4=c4)
B=B.subs(c1=0,c2=u+1,c3=-u,c4=1).change_ring(GF(2));
a=S1.reduce(G).subs(y1=c1, y2 = c2,y3=c3,y4=c4)
a=a.subs(c1=0,c2=u+1,c3=-u,c4=1).change_ring(GF(2));
b=S2.reduce(G).subs(y1=c1, y2 = c2,y3=c3,y4=c4)
b=b.subs(c1=0,c2=u+1,c3=-u,c4=1).change_ring(GF(2));
c=S3.reduce(G).subs(y1=c1, y2 = c2,y3=c3,y4=c4)
c=c.subs(c1=0,c2=u+1,c3=-u,c4=1).change_ring(GF(2));
show("A= ",A,",  B= ",B)
show("a=",a,", b=",b,", c=",c)
show((y^3+a*y^2+b*y+c).factor())
```

$$A = u^2,\ B = u^5 + u^3 + u^2$$
$$a = u+1,\ b = 0,\ c = u^2$$
$$(u+y)\cdot(y^2+u+y)$$

(c) As per (b), $D_f(y) = y^2+u^2y+u^5+u^3+u^2 = (y+u)^2+u^2(y+u)+u^5 = u^4(Y^2+Y+u)$, where $Y = (y+u)/u^2$.

Then the splitting field of $D_f(y)$ is $F(D(f)) = \mathbb{F}_2(u, \alpha)$, where $\alpha^2 + \alpha + u = 0$. Since $u = \alpha^2 + \alpha$, $\mathbb{F}_2(u, \alpha) = \mathbb{F}_2(\alpha)$ and $g(y) = y^2 + uy + 1 = y^2 + (\alpha^2 + \alpha)y + 1$. Then $g(y + 1) = (y + 1)^2 + (\alpha^2 + \alpha)(y + 1) + 1 = y^2 + (\alpha^2 + \alpha)y + (\alpha^2 + \alpha)$ is irreducible in $\mathbb{F}_2[\alpha][y]$ (and in $\mathbb{F}_2(\alpha)[y]$) by the Schönemann-Eisenstein criterion. Therefore $g(y)$ is irreducible over the splitting field $\mathbb{F}_2(\alpha)$ of $D(f)$

This criterion applies here because $[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = [\mathbb{F}_2(u, \alpha) : \mathbb{F}_2] = [\mathbb{F}_2(u, \alpha) : \mathbb{F}_2(u)][\mathbb{F}_2(u) : \mathbb{F}_2] = \infty$ (u is a variable), therefore α is transcendental over $\mathbb{F}_2$, so that we may consider α as a variable x: $\mathbb{F}_2[\alpha] \simeq \mathbb{F}_2[x]$. Hence $\mathbb{F}_2[\alpha]$ is a PID, and α is a prime in $\mathbb{F}_2[\alpha]$. Gauss's Lemma and the Schönemann-Eisenstein Criterion apply here.

As an alternative proof of the irreducibility of $g(y) = y^2 + uy + 1$ over $F(D(f))$, without this criterion, it is sufficient to prove that $g(y)$ has no root in $F(D(f)) = \mathbb{F}_2(\alpha)$, where $\alpha^2 + \alpha + u = 0$ as above. Such a root is under the form $a(\alpha)/b(\alpha)$, where $a(\alpha)$ and $b(\alpha)$ are relatively prime in the PID $\mathbb{F}_2[\alpha]$. Then

$$a(\alpha)^2 + (\alpha^2 + \alpha)a(\alpha)b(\alpha) + b^2(\alpha) = 0,$$

hence $a(\alpha) \mid b^2(\alpha)$, with $a(\alpha), b(\alpha)$ relatively prime, thus $a(\alpha) \mid 1$, $a(\alpha) = 1$, and similarly $b(\alpha) = 1$. But $g(1) = u \neq 0$, so g has no root in $F(D(f))$.

Thus $y^2 + uy + 1$ is irreducible over the splitting field of $D_f(y)$, therefore $G_f \simeq D_8$ by Proposition 13.3.6. $\square$

Ex. 13.3.8 *Let $f \in F[x]$ be an irreducible quartic, where F has characteristic $\neq 2$. Also let $\Theta_f(y)$ be the sextic resolvent defined in Example 13.3.4. The goal of this exercise is to show that $G_f \subset S_4$ determines the irreducible factorization of $\Theta_f(y)$ over F. We will assume that $\Theta_f(y)$ is separable.*

(a) First suppose $G_f = A_4$ or S_4. Prove that $\Theta_f(y)$ is irreducible over F.

(b) Now suppose that $G_f = \langle(1324), (12)\rangle$. Prove that $\Theta_f(y) = g(y)h(y)$, where $g(y), h(y) \in F[x]$ are irreducible of degree 2 and 4 respectively.

(c) Suppose that $G_f = \langle(12)(34), (13)(24)\rangle$. Prove that $\Theta_f(y) = g_1(y)g_2(y)g_3(y)$, where $g_1(y), g_2(y), g_3(y) \in F[x]$ are irreducible of degree 2.

(d) Finally, suppose that $G_f = \langle(1324)\rangle$. Prove that $\Theta_f(y) = g_1(y)g_2(y)g_3(y)$, where $g_1(y), g_2(y), g_3(y) \in F[x]$ are irreducible of degree 1,1 and 4 respectively.

(e) Explain why parts (a) through (d) enable one to determine G_f up to conjugacy using only $\Theta_f(y)$ and $\Delta(f)$.

Proof. (a) Let $\varphi = \sqrt{\Delta}(x_1 + x_2 - x_3 - x_4)$. We know by Ex. 13.3.4(a) that the orbit $\mathcal{O}_\varphi = S_n \cdot \varphi$ is

$$\mathcal{O}_\varphi = \{\varphi_0, \varphi_1, \ldots, \varphi_5\},$$

where

$$\begin{aligned}
\varphi_0 = \quad () \cdot \varphi &= \sqrt{\Delta}\,(x_1 + x_2 - x_3 - x_4),\\
\varphi_1 = (3\,4) \cdot \varphi &= \sqrt{\Delta}\,(-x_1 - x_2 + x_3 + x_4),\\
\varphi_2 = (2\,3) \cdot \varphi &= \sqrt{\Delta}\,(-x_1 + x_2 - x_3 + x_4),\\
\varphi_3 = (1\,4) \cdot \varphi &= \sqrt{\Delta}\,(x_1 - x_2 + x_3 - x_4),\\
\varphi_4 = (1\,3) \cdot \varphi &= \sqrt{\Delta}\,(x_1 - x_2 - x_3 + x_4),\\
\varphi_5 = (2\,4) \cdot \varphi &= \sqrt{\Delta}\,(-x_1 + x_2 + x_3 - x_4).
\end{aligned}$$

We verify that the orbit $A_n \cdot \varphi$ is $\mathcal{O}_\varphi$. Since A_n fixes $\sqrt{\Delta}$, we obtain

σ	$\sigma \cdot \varphi$
$()$	$\sqrt{\Delta}(x_1 + x_2 - x_3 - x_4)$
$(1\,3)(2\,4)$	$\sqrt{\Delta}(-x_1 - x_2 + x_3 + x_4)$
$(1\,2\,4)$	$\sqrt{\Delta}(-x_1 + x_2 - x_3 + x_4)$
$(2\,3\,4)$	$\sqrt{\Delta}(x_1 - x_2 + x_3 - x_4)$
$(2\,4\,3)$	$\sqrt{\Delta}(x_1 - x_2 - x_3 + x_4)$
$(1\,3\,4)$	$\sqrt{\Delta}(-x_1 + x_2 + x_3 - x_4)$

This proves $A_n \cdot \varphi \supset S_n \cdot \varphi$, and since $A_n \subset S_n$, $A_n \cdot \varphi \subset S_n \cdot \varphi$, so that

$$A_n \cdot \varphi = S_n \cdot \varphi.$$

Here $G_f = A_n$ or $G_f = S_n$. Therefore G_f acts transitively over the roots φ_i of the universal resolvent $\Theta(y) = \prod_{i=0}^{5} (y - \varphi_i)$.

Write $L = F(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ be the splitting field of f, and $\beta = \varphi_i(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \in L, \beta_i = \varphi(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \in L$.

Since $\Theta_f(y) = \prod_{i=0}^{5} (y - \varphi_i(\alpha_1, \alpha_2, \alpha_3, \alpha_4)) \in F[y]$, $\mathrm{Gal}(L/F)$ acts on the roots of $\Theta_f(y)$. We show that this action is transitive.

We know that $A_n \cdot \varphi = \{\varphi_0, \ldots, \varphi_5\}$, so that for each subscript $i \in \{0, \ldots, 5\}$, there exists $\tau \in A_n$ such that $\tau \cdot \varphi = \varphi_i$.

Since $G_f \supset A_n$, $\tau \in G_f$, thus there is a corresponding $\sigma \in \mathrm{Gal}(L/F)$ such that $\sigma(\alpha_j) = \alpha_{\tau(j)},\ j = 1, 2, 3, 4$. Then

$$\begin{aligned}
\sigma(\beta) &= \sigma(\varphi(\alpha_1, \ldots, \alpha_4))\\
&= \varphi(\tau(\alpha_1), \ldots, \tau(\alpha_5))\\
&= (\tau \cdot \varphi)(\alpha_1, \ldots, \alpha_4)\\
&= \varphi_i(\alpha_1, \ldots, \alpha_4)\\
&= \beta_i.
\end{aligned}$$

Therefore the orbit of β under the action of $\mathrm{Gal}(L/F)$ is $\{\beta = \beta_0, \ldots, \beta_5\}$.

Then we prove that $\Theta_f(y)$ is irreducible with the same argument as in the proof of Theorem 7.1.1 or Proposition 6.3.7.

If h is the minimal polynomial of β over F, then h divides $\Theta_f(y)$. $h \in F[y]$, and β is a root of h, therefore $\beta_i = \sigma(\beta), \sigma \in \mathrm{Gal}(L/F)$ is a root of h. The six β_i are distinct, as $\Theta_f(y)$ is separable, so that $\deg(h) \geq 6$, where $h \mid \Theta_f$, thus $\Theta_f = h$ is irreducible.

(b) Write, as in part (a),

$$\begin{aligned}
\varphi &= \sqrt{\Delta}(x_1 + x_2 - x_3 - x_4),\\
\varphi_2 &= (1\,2\,4) \cdot \varphi = \sqrt{\Delta}(-x_1 + x_2 - x_3 + x_4),\\
\varphi_4 &= (2\,4\,3) \cdot \varphi = \sqrt{\Delta}(x_1 - x_2 - x_3 + x_4).
\end{aligned}$$

Then the orbit of φ is $S_n \cdot \varphi = \{\varphi, -\varphi, \varphi_2, -\varphi_2, \varphi_4, -\varphi_4\}$, and the universal resolvent is

$$\Theta(y) = (y^2 - \varphi^2)(y^2 - \varphi_2^2)(y^2 - \varphi_4^2).$$

Here $G_f = \langle (1\,3\,2\,4), (1\,2) \rangle$ is the dihedral group D_8. We compute the orbits of φ and of φ_2 under the action of G_f.

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

so that $G_f \cdot \varphi = \{\varphi, -\varphi\}$.

Write $\beta = \varphi(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = \sqrt{\Delta(f)}(\alpha_1 + \alpha_2 - \alpha_3 - \alpha_4)$, and similarly $\beta_2 = \varphi_2(\alpha_1, \alpha_2, \alpha_3, \alpha_4), \beta_4 = \varphi_4(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$.Then

$$\Theta_f(y) = (y^2 - \beta^2)(y^2 - \beta_2^2)(y^2 - \beta_4^2).$$

If $\sigma \in \mathrm{Gal}(L/F)$, and if $\tau \in G_f$ is the corresponding permutation, then, as in part (a),

$$\sigma(\beta) = (\tau \cdot \varphi)(\alpha_1, \ldots, \alpha_4) = \pm\varphi(\alpha_1, \ldots, \alpha_4) = \pm\beta.$$

We know that $\beta \neq 0$, as Θ_f is separable. Thus $\sigma(\beta) \neq \beta$, so that $\beta \notin F$, but $\sigma(\beta^2) = (\pm\beta)^2 = \beta^2$, thus $\beta^2 \in F$. This proves that the factor $g(y) = y^2 - \beta^2 \in F[y]$, and $y^2 - \beta^2$ is irreducible over F.

Moreover,

$$\begin{aligned}
(1\,3\,2\,4) \cdot \varphi_2 &= (-\sqrt{\Delta})(-x_3 + x_4 - x_2 + x_1)\\
&= \sqrt{\Delta}(-x_1 + x_2 + x_3 - x_4)\\
&= -\varphi_4\\
(1\,3\,2\,4)^2 \cdot \varphi_2 &= -(1\,3\,2\,4) \cdot \varphi_4\\
&= -(-\sqrt{\Delta})(x_3 - x_4 - x_2 + x_1)\\
&= \sqrt{\Delta}(x_1 - x_2 + x_3 - x_4)\\
&= -\varphi_2\\
(1\,3\,2\,4)^3 \cdot \varphi_2 &= -(1\,3\,2\,4) \cdot \varphi_2 = \varphi_4\\
(1\,2) \cdot \varphi_2 &= (-\sqrt{\Delta})(-x_2 + x_1 - x_3 + x_4)\\
&= \sqrt{\Delta}(-x_1 + x_2 + x_3 - x_4),
\end{aligned}$$

so that $G_f \cdot \varphi_2 = \{\varphi_2, -\varphi_2, \varphi_4, -\varphi_4\}$. Therefore the orbit of β_2 under the action of $\mathrm{Gal}(L/F)$ is $\{\pm\beta_2, \pm\beta_4\}$.

Write $h(y) = (y^2 - \beta_2^2)(y^2 - \beta_4^2)$. Since $h(y) = \Theta_f(y)/g(y)$, $h(y) \in F[y]$. The action of $\mathrm{Gal}(L/F)$ on the roots of the separable polynomial h is transitive, thus, as in part (a), h is irreducible over F.

$\Theta_f(y) = g(y)h(y)$, where $g(y), h(y) \in F[y]$ are irreducible of degree 2 and 4 respectively.

(c) By computing the orbits of $\varphi, \varphi_2, \varphi_4$, we obtain

$$\begin{aligned}(1\,2)(3\,4) \cdot \varphi &= \varphi,\\ (1\,3)(2\,4) \cdot \varphi &= -\varphi,\\ (1\,2)(3\,4) \cdot \varphi_2 &= -\varphi_2,\\ (1\,3)(2\,4) \cdot \varphi_2 &= -\varphi_2,\\ (1\,2)(3\,4) \cdot \varphi_4 &= -\varphi_4,\\ (1\,3)(2\,4) \cdot \varphi_4 &= -\varphi_4.\end{aligned}$$

Therefore

$$G_f \cdot \varphi = \{\varphi, -\varphi\}, \qquad G_f \cdot \varphi_2 = \{\varphi_2, -\varphi_2\}, \qquad G_f \cdot \varphi_4 = \{\varphi_4, -\varphi_4\},$$

and the orbits of β, β_2, β_4 under the action of $G = \mathrm{Gal}(L/F)$ are

$$G \cdot \beta = \{\beta, -\beta\}, \qquad G \cdot \beta_2 = \{\beta_2, -\beta_2\}, \qquad G \cdot \beta_4 = \{\beta_4, -\beta_4\}.$$

If $\sigma \in \mathrm{Gal}(L/F)$ corresponds to $(1\,2)(3\,4)$, then $\sigma(\beta) = -\beta \neq \beta$, and $\sigma(\beta^2) = \beta^2$, so that $\beta \notin F, \beta^2 \in F$, and the factor $y^2 - \beta^2 \in F[y]$ is irreducible over F. Similarly, the two other factors are irreducible in $F[y]$.

$\Theta_f(y) = (y^2 - \beta^2)(y^2 - \beta_2^2)(y^2 - \beta_4^2)$ is a decomposition in three irreducible factors of $F[y]$.

(d) Suppose now that $G_f = \langle (1\,3\,2\,4) \rangle$. We know that

$$(1\,3\,2\,4) \cdot \varphi = \varphi,$$

thus the corresponding $\sigma \in \mathrm{Gal}(L/F)$ fixes $\beta = \varphi(\alpha_1, \ldots, \alpha_4)$, so that $\beta \in F$.

$g_1(y) = y - \beta, g_2(y) = y + \beta$ are two factors of degree 1 of $\Theta_f(y)$.

Moreover, we know from part (b) that

$$(1\,3\,2\,4) \cdot \varphi_2 = -\varphi_4, (1\,3\,2\,4)^2 \cdot \varphi_2 = -\varphi_2, (1\,3\,2\,4)^3 \cdot \varphi_2 = \varphi_4$$

As in part *b*, $\mathrm{Gal}(L/F)$ acts transitively on the distinct roots of $(y^2 - \beta_2^2)(y^2 - \beta_4^2) \in F[y]$, thus this polynomial is irreducible over F:

$\Theta_f(y) = g_1(y)g_2(y)g_3(y)$, where $g_1(y), g_2(y), g_3(y) \in F[y]$ are irreducible of degree 1,1 and 4 respectively.

(e) By Theorem 13.1.1, G_f is conjugate to a permutation group examined in parts (a),(b), (c) or (d), and the four conclusions are mutually exclusive, so the factorisation of $\Theta_f(y)$ over F enables to determine this case. In part (a), $\Delta(f)$ enables in characteristic $\neq 2$ to distinguish the cases $G_f = A_4$ and $G_f = A_4$. Therefore the factorisation of $\Theta_f(y)$ and $\Delta(f)$ give an algorithm to determine G_f up to conjugacy. □

Ex. 13.3.9 *The action of* $\mathrm{GL}(3, \mathbb{F}_2)$ *on the nonzero vectors of* $\mathbb{F}_2^3$ *gives a group homomorphism* $\mathrm{GL}(3, \mathbb{F}_2) \to S_7$. *Prove that this map is one-to-one.*

Proof. Let

$$\psi \left\{ \begin{array}{ccl} \mathrm{GL}(3, \mathbb{F}_2) & \to & S_7 \\ g & \mapsto & \sigma : \quad \forall i \in \{1, ..., 7\},\ g \cdot \nu_i = \nu_{\sigma(i)} \end{array} \right.$$

If $\psi(g) = \psi(g')$, then $g \cdot \nu_i = g' \cdot \nu_i$ for all $i \in \{1, ..., 7\}$, then particularly $g \cdot e_1 = g' \cdot e_1, g \cdot e_2 = g' \cdot e_2, g \cdot e_3 = g' \cdot e_3$, where $e_1 = (1, 0, 0), e_2 = (0, 1, 0), e_3 = (0, 0, 1)$ is the standard basis of $\mathbb{F}_2^3$. Since a linear map (or its matrix) is determined by the images of the vectors of a base, $g = g'$

$\psi : G \to S_m$ is a one-to-one group homomorphism. □

Ex. 13.3.10 *Consider the vector space* $\mathbb{F}_2^3$.

(a) Prove that $\mathbb{F}_2^3$ *has exactly seven two-dimensional subspaces.*

(b) For a field F, let $B = \{\{\nu_1, \nu_2, \nu_3\} \subset F^3 \mid \nu_1, \nu_2, \nu_3$ *are linearly independent over* $F\}$. *Prove that* $\mathrm{GL}(3, F)$ *acts transitively on B.*

(c) Let F be as in part (b). Prove that $\mathrm{GL}(3, F)$ *acts transitively on the set of two-dimensional subspaces of* F^3.

Proof. (a) An orderer pair $(u, v) \in \mathbb{F}_2^2$ is a base of a vectorial plane if $u \neq 0$, and $v \notin \langle u \rangle = \{0, u\}$, so there are 7×6 (ordered) bases of planes in $\mathbb{F}_3^2$.

A vectorial plane P of $\mathbb{F}_3^2$, which contains 4 vectors, has 3×2 bases, with the same reasoning: 3 choices for the first non null vector, and 2 choices for the second vector.

Therefore the number of two-dimensional subspaces of $\mathbb{F}_2^3$ is $\frac{7 \times 6}{3 \times 2} = 7$.

(b) Let $\{e_1, e_2, e_3\}$ be the standard basis of F^3, where $e_1 = (1, 0, 0), e_2 = (0, 1, 0), e_3 = (0, 0, 1)$. Any element of $\mathrm{GL}(3, F)$ applies a base on a base, thus the orbit of $\{e_1, e_2, e_3\}$ is included in B.

Conversely, let $\{\nu_1, \nu_2, \nu_3\}$ be any element of B. Define $g = [\nu_1, \nu_2, \nu_2]$ the matrix whose columns are ν_1, ν_2, ν_3. Since ν_1, ν_2, ν_3 are linearly independent, $g \in \mathrm{GL}(3, \mathbb{F}_2)$, and $g \cdot e_1 = \nu_1, g \cdot e_2 = \nu_2, g \cdot e_3 = \nu_3$, so that $\{\nu_1, \nu_2, \nu_3\} = g \cdot \{e_1, e_2, e_3\}$ is in the orbit of $\{e_1, e_2, e_3\}$. Therefore the orbit of $\{e_1, e_2, e_3\}$ is B, thus $\mathrm{GL}(3, F)$ acts transitively over B.

(c) Let P, Q be two-dimensional subspaces of F^3. Take $\{\nu_1, \nu_2\}$ a basis of P, and $\{\nu_1', \nu_2'\}$ a basis of Q. We can complete them into bases of F^3, say $b = \{\nu_1, \nu_2, \nu_3\}$ and $b' = \{\nu_1', \nu_2', \nu_3'\}$. By part b, there exists $g \in \mathrm{GL}(3, F)$ such that $g \cdot b = b'$. Since g maps a basis of P on a basis of Q, $g \cdot P = Q$. Therefore $\mathrm{GL}(3, F)$ acts transitively on the set of two-dimensional subspaces of F^3

Note: Since there are exactly 3 nonzero vectors in a two-dimensional subspace of $\mathbb{F}_2^3$, each triple of distinct nonzero linearly dependant vectors in $\mathbb{F}_2^3$ determines a unique two-dimensional space. Therefore part (c) explains the statement in the proof of 13.3.9, that $\mathrm{GL}(3, \mathbb{F}_2^3)$ acts transitively on this set of triples. □

Ex. 13.3.11 *Prove that* $\mathrm{GL}(3,\mathbb{F}_2) = \mathrm{SL}(3,\mathbb{F}_2) \simeq \mathrm{PGL}(3,\mathbb{F}_2) = \mathrm{PSL}(3,\mathbb{F}_2)$.

Proof. A matrix $M \in \mathrm{GL}(3,\mathbb{F}_2)$ is such that $\det(M)$ is invertible in $\mathbb{F}_2$, but only 1 is invertible in $\mathbb{F}_2$, so that $\det(M) = 1$ and $M \in \mathrm{SL}(3,\mathbb{F}_2)$. Therefore $\mathrm{GL}(3,\mathbb{F}_2) \subset \mathrm{SL}(3,\mathbb{F}_2)$, and $\mathrm{SL}(3,F) \subset \mathrm{GL}(3,F)$ is true in every field F, thus

$$\mathrm{GL}(3,\mathbb{F}_2) = \mathrm{SL}(3,\mathbb{F}_2).$$

By definition, in any field F, $\mathrm{PGL}(n,F) = \mathrm{GL}(n,F)/F^*I$ and $\mathrm{PSL}(n,F) = \mathrm{SL}(n,F)/(F^*I \cap \mathrm{SL}(n,F))$. When $F = \mathbb{F}_2$, then $\mathbb{F}_2^* = \{1\}$, i.e., $\mathbb{F}_2^* I = (\mathbb{F}_2^* I \cap \mathrm{SL}(n,\mathbb{F}_2)) = \{I\}$. Therefore, for n=3,

$$\mathrm{GL}(3,\mathbb{F}_2) = \mathrm{SL}(3,\mathbb{F}_2) \simeq \mathrm{PGL}(3,\mathbb{F}_2) = \mathrm{PSL}(3,\mathbb{F}_2).$$

□

Ex. 13.3.12 *Prove that (13.31) from Example 13.3.4 is an example of a relative resolvent in the sense of Exercise 5.*

Proof. Suppose $f = x^4 - c_1x^3 + c_2x^2 - c_3x + c_4 \in F[x]$ is separable and irreducible. Let $H = \langle (1324), (12) \rangle$, $G = \langle (1324)) \rangle \subset H$ and $\varphi = \sqrt{\Delta}(x_1 + x_2 - x_3 - x_4)$. By Exercise 4, G is the symmetry group of φ. Since $(12) \cdot \varphi = -\varphi$, $H \cdot \varphi = \{\varphi, -\varphi\}$ is the orbit of φ under the action of H. Then

$$\Theta_f^H(y) = (y - \varphi(\alpha_1, ..., \alpha_4))(y + \varphi(\alpha_1, ..., \alpha_4)) = (y^2 - \varphi^2(\alpha_1, ..., \alpha_4)),$$

where $\varphi^2(\alpha_1, ..., \alpha_4) = \Delta(f)(4\beta_1 + c_1^2 - 4c_2)$, $\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4$. By the assumption of Example 13.3.4, $\beta_1 \in F$, therefore $\Theta_f^H(y) \in F[y]$ and it is the relative resolvent in the sense of Exercise 5.

Since $G_f \subset H$, depending on whether $\Theta_f^H(y)$ is reducible or not in F, the conclusion about whether $G_f = \langle (1324)) \rangle$ or $G_f = \langle (1324), (12) \rangle$ can be done.

□

Ex. 13.3.13 *In the proof of Proposition 13.3.9, we showed that when* $\mathrm{GL}(3,\mathbb{F}_2) \subset S_7$ *acts on three-element subsets of* $\{1,\ldots,7\}$*, the orbits have lengths* 7 *and* 28*. We also asserted that up to conjugacy,* $\mathrm{GL}(3,\mathbb{F}_2)$ *is the only subgroup of* S_7 *with this property. In this exercise, you will study the action of some other subgroups of* S_7*.*

- *(a) Prove that* A_7 *and* S_7 *act transitively on three-element subsets of* $\{1,\ldots,7\}$*. Thus there is one orbit of length* 35 *for these groups.*
- *(b) In Section 13.2, the group* $\mathrm{AGL}(1,\mathbb{F}_5) \subset S_5$ *played an important role in understanding the Galois group of a quintic. In a similar way, we have* $\mathrm{AGL}(1,\mathbb{F}_7) \subset S_7$ *provided we think of the indices as congruences classes modulo* 7*. Prove that the orbits of* $\mathrm{AGL}(1,\mathbb{F}_7)$ *acting on the triples* $\{0,1,2\}$ *and* $\{0,1,3\}$ *have* 21 *and* 14 *elements, respectively.*

Proof. The action of a group G on the set of three-elements subsets of $\{1,\ldots,7\}$ is transitive when, for all triples of distinct elements i,j,k and distinct elements i',j',k', there is a $g \in G$ such that $\{g \cdot i, g \cdot j, g \cdot k\} = \{i',j',k'\}$ (which is less constraining that $\sigma(i) = i', \sigma(j) = j', \sigma(k) = k'$).

The distinctness of elements means $i \neq j$ and $j \neq k$ and $i \neq k$. The possibilities $i = i'$ (or j' or k') or $j = j'$ (or i' or k') or $k = k'$ (or i' or j') is allowed.

(a) Let A be the set of three-elements subsets of $\{1,\dots,7\}$. If $\{i,j,k\} \in A$, we show the existence of $\sigma \in A_7$ such that $\sigma(1),\sigma(2),\sigma(3) = \{i,j,k\}$.

Since $\mathrm{Card}(\{1,2,3\}) = \mathrm{Card}(\{i,j,k\}) = 3$, there exists some bijection $\sigma_1 : \{1,2,3\} \to \{i,j,k\}$, for instance $\sigma_1 : 1 \mapsto k, 2 \mapsto i, 3 \mapsto j$.

Since $\mathrm{Card}(\{4,5,6,7\}) = \mathrm{Card}(\{1,\dots,7\} \setminus \{i,j,k\}) = 4$, there exists a bijection $\sigma_2 : \{4,5,6,7\} \to \{1,\dots,7\} \setminus \{i,j,k\}$.

Then the map s defined by $s(i) = \sigma_1(i)$ if $i \in \{1,2,3\}$ and $s(i) = \sigma_2(i)$ if $i \in \{4,5,6,7\}$ is a bijection, so that $s \in S_7$.

If s is even, take $\sigma = s$, and if s is odd, take $\sigma = s \circ (1\,2)$. In both cases $\sigma \in A_n$ and $\sigma(\{1,2,3\}) = \{i,j,k\}$.

Therefore the orbit of $\{1,2,3\}$ is $A_n \cdot \{1,2,3\} = A$, which has 35 elements, so that A_7 acts transitively on three-element subsets of $\{1,\dots,7\}$. A fortiori $S_n \supset A_n$ acts transitively on the same set.

(b) The following Sage instructions give the length of the orbits of $\{0,1,2\}$ and $\{0,1,3\}$

```
F = GF(7)

def t(a,b,i):
    return F(a*i + b)

def orbit(u,v,w):
    """ returns the orbit of {u,v,w} """
    orb = set()
        for a in range(1,7):
            for b in range(7):
                l = [t(a,b,u), t(a,b,v), t(a,b,w)]
                l.sort()
                orb.add(tuple(l))
    return orb

print(len(orbit(0,1,2)), len(orbit(0,1,3)))
```

(21,14)

For instance, the orbit of $\{0,1,3\}$ is

$$\begin{aligned}\mathrm{AGL}(1,\mathbb{F}_7)\cdot\{0,1,3\} = \{&\{3,4,6\},\{2,3,5\},\{0,4,5\},\{2,4,5\},\{0,2,3\},\{0,2,6\},\{1,5,6\},\\ &\{3,5,6\},\{1,2,4\},\{1,3,4\},\{0,1,5\},\{1,2,6\},\{0,1,3\},\{0,4,6\}\}.\end{aligned}$$

Alternatively, one can find the isotropy group of these unordered triples :

The one-dimensional affine linear group $\mathrm{AGL}(1,\mathbb{F}_7)$ is the group of order $7\times 6 = 42$ consisting of maps $i \mapsto ai+b$ where $i,a,b \in \mathbb{F}_7$ and $a \neq 0$. The isotropy group of an unordered triple $x^3 = \{x_1,x_2,x_3\}$ is the subgroup $G_{x^3} = \{g \in \mathbb{F}_7 \,|\, g\cdot x^3 = x^3\}$. Solutions to the equations $ax_i + b = x_{\sigma(i)}$, $i \in (1,2,3), \sigma \in S_3$ are giving the elements of isotropy group.

In matrix form the equations are:

$$\begin{pmatrix} x_1 & 1 \\ x_2 & 1 \\ x_3 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} x_{\sigma(1)} \\ x_{\sigma(2)} \\ x_{\sigma(3)} \end{pmatrix}$$

The extended matrix for all $\sigma \in S_3$ excluding identity permutation is:

$$\left(\begin{array}{cc|ccccc} x_1 & 1 & x_1 & x_2 & x_2 & x_3 & x_3 \\ x_2 & 1 & x_3 & x_1 & x_3 & x_1 & x_2 \\ x_3 & 1 & x_2 & x_3 & x_1 & x_2 & x_1 \end{array}\right)$$

- Case $x^3 = (0, 1, 2)$: Gauss transformation of extended matrix to bring the first two columns to

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$$

gives:

$$\begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 2 & 2 \\ 1 & 1 & 2 & 0 & 2 & 0 & 1 \\ 2 & 1 & 1 & 2 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 2 & 2 \\ 1 & 0 & 2 & 6 & 1 & 5 & 6 \\ 2 & 1 & 1 & 2 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 2 & 2 \\ 1 & 0 & 2 & 6 & 1 & 5 & 6 \\ 0 & 1 & 4 & 4 & 5 & 5 & 2 \end{pmatrix}$$

There is only one solution corresponding to $a = 6, b = 2$, i.e., the order of isotropy group is 2 and (cf. Theorem A.4.9) the appropriate orbit has $42/2 = 21$ elements.

- Case $x^3 = (0, 1, 3)$:

$$\begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 3 & 3 \\ 1 & 1 & 3 & 0 & 3 & 0 & 1 \\ 3 & 1 & 1 & 3 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 3 & 3 \\ 1 & 0 & 3 & 6 & 2 & 4 & 5 \\ 3 & 1 & 1 & 3 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 3 & 3 \\ 1 & 0 & 3 & 6 & 2 & 4 & 5 \\ 0 & 1 & 6 & 6 & 1 & 3 & 6 \end{pmatrix}$$

There are two solutions corresponding to $a = 2, b = 1$ and $a = 4, b = 3$, i.e., the order of isotropy group is 3, hence the appropriate orbit has $42/3 = 14$ elements.

$\square$

Ex. 13.3.14 *The quadratic resolvent $D_f(y)$ used in Theorem 13.3.5 to compute the Galois group of a quartic in all characteristics was defined for a polynomial f of degree 4. Here you will study what happens when f is monic of degree n. We begin with the polynomial*

$$D = \sum_{\sigma \in A_n} \sigma \cdot x_1^{n-1} x_2^{n-2} \dots x_{n-2}^2 x_{n-1} \in F[x_1, ..., x_n],$$

where F is a field of any characteristic.

(a) Prove that A_n is the symmetry group of D.

(b) Prove that $\sqrt{\Delta} = \prod_{1 \le i < j \le n}(x_i - x_j)$ satisfies $\sqrt{\Delta} = D - D'$, where $D' = (12) \cdot D$.

(c) Let $f \in F[x]$ be monic of degree n and let $\alpha_1, ..., \alpha_n$ be the roots of f in some splitting field L. Then define $D(f) = D(\alpha_1, ..., \alpha_n)$ and $D'(f) = D'(\alpha_1, ..., \alpha_n)$ and set

$$D_f(y) = (y - D(f))(y - D'(f)).$$

Prove that $D_f(y) \in F[y]$ and that the discriminant of $D_f(y)$ is $\Delta(f) = \prod_{1\le i<j\le n}(\alpha_i - \alpha_j)^2$. Note that D(f) and $D'(f)$ depend on how we order the roots while the polynomial $D_f(y)$ depends only on f.

(d) *Assume that f is separable and let $Gal(L/F) \simeq G_f \subset S_n$. Prove that $G_f \subset A_n$ if and only if $D_f(y)$ splits over F.*

Proof. (a) We proved in Exercise 12.1.9(b) that the symmetry group of

$$\sum_{\sigma\in H} \sigma \cdot x_1^{n-1}x_2^{n-2}\dots x_{n-2}^2 x_{n-1}$$

is H.

Thus, A_n is the symmetry group of

$$D = \sum_{\sigma\in A_n} \sigma \cdot x_1^{n-1}x_2^{n-2}\dots x_{n-2}^2 x_{n-1}.$$

(b) We proved in Ex. 2.4.1 the formula

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

By definition of the determinant, if $A = (a_{i,j})_{1\le i,j\le n}$

$$\det(A) = \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma)\prod_{i=1}^n a_{\sigma(i),i},$$

and

$$\det(A) = \det({}^tA) = \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma)\prod_{i=1}^n a_{i,\sigma(i)}.$$

Applying this formula to $a_{i,j} = x_j^{n-i}$, with $\varphi = x_1^{n-1}x_2^{n-2}\cdots x_{n-1}$ and $\tau = (1\,2)$, we obtain

$$\begin{aligned}
\sqrt{\Delta} &= \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) x_{\sigma(1)}^{n-1}x_{\sigma(2)}^{n-2}\cdots x_{\sigma(n-1)}\\
&= \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma)\ \sigma\cdot x_1^{n-1}x_2^{n-2}\cdots x_{n-1}\\
&= \sum_{\sigma\in A_n}\sigma\cdot\varphi - \sum_{\sigma\in S_n\setminus A_n}\sigma\cdot\varphi\\
&= \sum_{\sigma\in A_n}\sigma\cdot\varphi - \sum_{\sigma\in A_n}(\tau\sigma)\cdot\varphi\\
&= D - \tau\cdot D = D - D'.
\end{aligned}$$

(c) Since $S_n = A_n \coprod \tau A_n$,

$$D + D' = \sum_{\sigma \in S_n} \sigma \cdot \varphi.$$

For each $\chi \in S_n$,

$$\chi \cdot (D + D') = \sum_{\sigma \in S_n} (\chi\sigma) \cdot \varphi = \sum_{\sigma' \in S_n} \sigma' \cdot \varphi = D + D' \qquad (\sigma' = \chi\sigma).$$

Therefore the symmetry group of $D + D'$ is S_n.

Since $(D(f) + D'(f) = (D + D')(\alpha_1, \dots, \alpha_n)$, where $D + D'$ is a symmetric polynomial, $D(f) + D'(f) \in F$.

Moreover

$$DD' = \sum_{\sigma \in A_n} \sigma \cdot \varphi \sum_{\sigma' \in A_n} (\tau\sigma') \cdot \varphi.$$

Similarly, if $\chi \in A_n$, then $\chi \cdot D = D$. Since

$$D' = \sum_{\sigma' \in A_n} (\tau\sigma') \cdot \varphi = \sum_{\sigma'' \in A_n} (\sigma''\tau) \cdot \varphi,$$

$\chi \cdot D' = D'$.

Therefore $\chi \cdot (DD') = DD'$ for all $\chi \in A_n$, and

$$\tau \cdot (DD') = \sum_{\sigma \in A_n} (\tau\sigma) \cdot \varphi \sum_{\sigma' \in A_n} \sigma' \cdot \varphi = D'D = DD',$$

so that $\chi \cdot (DD') = DD'$ for all $\chi \in S_n$, and DD' is a symmetric polynomial. Thus $D(f)D'(f) = (DD')(\alpha_1, \dots, \alpha_n) \in F$.

This proves

$$D_f(y) = (y - D(f))(y - D'(f)) = y^2 - (D(f) + D'(f))y + D(f)D'(f) \in F[y].$$

Finally, the evaluation mapping $(x_1, \dots, x_n) \mapsto (\alpha_1, \dots, \alpha_n)$ gives

$$\sqrt{\Delta(f)} = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j),$$

thus

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

(d) The discriminant of $D_f(y)$ is $(D(f) - D'(f))^2 = \sqrt{\Delta(f)} \neq 0$, since we assumed that f is separable. Therefore $D_f(y)$ is separable, so that the roots $D(f), D'(f)$ are simple roots.

Since $D_f(y)$ is the resolvent associated to φ with symmetry group A_n, Proposition 13.3.2 shows that $G_f \subset A_n$ if and only if $D_f(y)$ has a root in F, if and only if $D_f(y)$ splits over F.

□

Ex. 13.3.15 *Let $f = x^3 - c_1x^2 + c_2x - c_3 \in F[x]$ and let $D_f(y) \in F[y]$ be as in the previous exercise.*

(a) Show that $D_f(y) = y^2 - (c_1c_2 - 3c_3)y + c_2^3 + c_1^3c_3 - 6c_1c_2c_3 + 9c_3^2$.

(b) Assume in addition that f is separable and irreducible. Explain how $D_f(y)$ determines Galois group of f up to isomorphism.

Proof. (a) By (2.26), we obtain

$$\Delta(f) = -4c_2^3 - 27c_3^2 + c_1^2c_2^2 - 4c_1^3c_3 + 18c_1c_2c_3,$$

and by Ex.2.2.10,

$$D + D' = \sum_{\sigma\in A_3} \sigma \cdot x_1^2x_2 + (12) \sum_{\sigma\in A_3} \sigma \cdot x_1^2x_2 = \sum_{\sigma\in S_3} \sigma \cdot x_1^2x_2 = \sigma_1\sigma_2 - 3\sigma_3,$$

so that

$$D(f) + D'(f) = c_1c_2 - 3c_3.$$

(Note: If the characteristic is not 2, we could write

$$D(f) = \frac{1}{2}(D(f) + D'(f) + (D(f) - D'(f)) = \frac{1}{2}(c_1c_2 - 3c_3 \pm \sqrt{\Delta(f)}),$$

and compute $D(f)D'(f)$, but here we compute in all characteristic.)

But DD' is symmetric, where

$$\begin{aligned} DD' &= \left(\sum_{\sigma\in A_3} \sigma \cdot x_1^2x_2\right)\left(\sum_{\sigma\in A_3} (\tau\sigma) \cdot x_1^2x_2\right) \\ &= (x_1^2x_2 + x_2^2x_3 + x_3^2x_1)(x_2^2x_1 + x_1^2x_3 + x_3^2x_2) \\ &= x_1^3x_2^3 + x_1^4x_2x_3 + x_1x_2^4x_3 + 3x_1^2x_2^2x_3^2 + x_1^3x_3^3 + x_2^3x_3^3 + x_1x_2x_3^4 \end{aligned}$$

With the usual Sage instructions, we obtain $D(f)D'(f)$

```
R.<x1,x2,x3,y1,y2,y3> = PolynomialRing(QQ, order = 'degrevlex')
elt = SymmetricFunctions(QQ).e()
e = [elt([i]).expand(3).subs(x0=x1, x1=x2, x2=x3) for i in range(4)]
J = R.ideal(e[1]-y1, e[2]-y2, e[3]-y3)
G = J.groebner_basis()
f = (x1^2*x2+x2^2*x3+x3^2*x1)*(x2^2*x1+x1^2*x3+x3^2*x2)
var('sigma_1,sigma_2,sigma_3')
var('c1,c2,c3')
g=f.reduce(G).subs(y1=c1,y2=c2,y3=c3)
g
```

$$c_1^3c_3 + c_2^3 - 6\,c_1c_2c_3 + 9\,c_3^2$$

Then

$$D(f)D'(f) = c_2^3 + c_1^3c_3 - 6c_1c_2c_3 + 9c_3^2$$

and

$$\begin{aligned} D_f(y) &= y^2 - (D(f) + D'(f))y + D(f)D'(f) \\ &= y^2 - (c_1c_2 - 3c_3)y + c_2^3 + c_1^3c_3 - 6c_1c_2c_3 + 9c_3^2 \end{aligned}$$

(b) By Ex.6.2.6, f being irreducible and separable, we know that $3 \mid |G_f|$. Therefore $G_f = A_3$ or $G_f = S_3$. Then Ex.14(d) proves that

$$\begin{aligned} G_f = A_3 &\iff D_f(y) \text{ splits over } F, \\ G_f = S_3 &\iff D_f(y) \text{ is irreducible over } F. \end{aligned}$$

□

13.4 Other Methods

Ex. 13.4.1 *Verify the computations given in Example 13.4.1.*

Proof. The following Sage instructions:

```
R.<y,x1,x2,x3,sigma1,sigma2,sigma3,u1,u2,u3> = PolynomialRing(QQ, order = 'lex')
elt = SymmetricFunctions(QQ).e()
e = [elt([i]).expand(3).subs(x0=x1, x1=x2, x2=x3) for i in range(4)]
J = R.ideal(e[1]-sigma1, e[2]-sigma2, e[3]-sigma3)
G = J.groebner_basis()
S = y-(u1*x1 + u2*x2 + u3*x3)
S1 = S  * S.subs(x1=x1,x2=x3,x3=x2) * S.subs(x1=x2,x2=x1,x3=x3)
S1 = S1 * S.subs(x1=x2,x2=x3,x3=x1) * S.subs(x1=x3,x2=x1,x3=x2)
S = S1 * S.subs(x1=x3,x2=x2,x3=x1)
S = S.subs(u1=-1,u2=1,u3=2)
f = S.reduce(G).polynomial(y)
f
```

give output $S(y)$:

$$\begin{aligned} &y^6 - 4\sigma_1 y^5 + (2\sigma_1^2 + 14\sigma_2)y^4 + (8\sigma_1^3 - 44\sigma_1\sigma_2 + 20\sigma_3)y^3 \\ &+ (-7\sigma_1^4 + 18\sigma_1^2\sigma_2 + 49\sigma_2^2 - 40\sigma_1\sigma_3)y^2 + (-4\sigma_1^5 + 44\sigma_1^3\sigma_2 \\ &- 112\sigma_1\sigma_2^2 - 20\sigma_1^2\sigma_3 + 140\sigma_2\sigma_3)y + 4\sigma_1^6 - 32\sigma_1^4\sigma_2 + 55\sigma_1^2\sigma_2^2 \\ &+ 36\sigma_2^3 + 76\sigma_1^3\sigma_3 - 322\sigma_1\sigma_2\sigma_3 + 343\sigma_3^2. \end{aligned}$$

Using $\sigma_1 \mapsto -1, \sigma_2 \mapsto -2, \sigma_3 \mapsto 1$, we obtain:

```
f1 = f.subs(sigma_1=-1, sigma_2=-2, sigma_3=1); f1
```

$$y^6 + 4y^5 - 26y^4 - 76y^3 + 193y^2 + 240y - 377$$

The Sage output coincides with Example 13.4.1:

```
factor(f1)
```

$$(y^3 + 2y^2 - 15y - 29) \cdot (y^3 + 2y^2 - 15y + 13)$$

□

Ex. 13.4.2 *Prove that the polynomial $s_u(y)$ defined in (13.41) lies in $K[u_1, ..., u_n, y]$.*

Proof. Let $f(x) = x^n - c_1x^{n-1} + ... + (-1)^n c_n \in K[x]$. The universal version of $s_u(y)$ is given by :

$$S(y) = \prod_{\sigma \in S_n} (y - (u_1 x_{\sigma(1)} + ... + u_n x_{\sigma(n)})) \in K[x_1, ..., x_n, u_1, ..., u_n, y]$$

For any $\tau \in S_n$,

$$\begin{aligned} \tau \cdot S(y) &= \prod_{\sigma \in S_n} (y - (u_1 x_{(\tau\sigma)(1)} + ... + u_n x_{(\tau\sigma)(n)})) \\ &= \prod_{\sigma' \in S_n} (y - (u_1 x_{\sigma'(1)} + ... + u_n x_{\sigma'(n)})) = S(y). \end{aligned}$$

Thus the application of τ has merely permuted the roots of $S(y)$ leaving the coefficients fixed. It means that the coefficients of $S(y)$ are symmetric and are polynomials in $\sigma_1, ..., \sigma_n$ (cf. Ex.9.1.6), i.e., $S(y) \in K[\sigma_1, ..., \sigma_n, u_1, ..., u_n, y]$.

The application of evaluation map $\sigma_i \mapsto c_i$ to $S(y)$ gives $s_u(y) \in K[c_1, ..., c_n, u_1, ..., u_n, y] = K[u_1, ..., u_n, y]$.

□

Ex. 13.4.3 *This exercise is concerned with the proof of Theorem 13.4.2.*

(a) *Let $\beta_1, ..., \beta_n \in L$. Prove that $y + \sum_{i=1}^r \beta_i u_i$ is irreducible in $L[u_1, ..., u_n, y]$. (This implies that (13.41) is the irreducible factorization of $s_u(y)$ in $L[u_1, ..., u_n, y]$.)*

(b) *Let $g, h \in F[u_1, ..., u_n, y]$, and assume that in the larger ring $L[u_1, ..., u_n, y]$ we have $h = gq$ for some $q \in L[u_1, ..., u_n, y]$. Prove that $q \in F[u_1, ..., u_n, y]$.*

(c) *In the final part of the proof of Theorem 13.4.2, we showed that $G \subset \sigma^{-1} G_f \sigma$. Prove the opposite inclusion.*

Proof. (a) Assume that $h = y + \sum_{i=1}^r \beta_i u_i$ is reducible, i.e., $h = ge$ with $g, e \in L[u_1, ..., u_n, y]$. In the ring $L[u_1, ..., u_n][y]$ the polynomial h is clearly irreducible as every polynomial of degree 1. Then g or e is in $L[u_1, ..., u_n]$. In case $g \in L[u_1, ..., u_n]$, the comparison of coefficients in y gives $g \mid 1$, and then g is a unit in $L[u_1, \ldots, u_n, y]$.

Hence the assumption is wrong and h is irreducible in $L[u_1, ..., u_n, y]$.

(b) The equality $h = gq$, where $h, g, q \in L[u_1, \ldots, u_n, y]$, is also true in the ring $L(u_1, \ldots, u_n)[y] = K[y]$, where $K = L(u_1, \ldots, u_n)$ is a field, so that $K[y]$ is an Euclidean ring. Write $k = F(u_1, \ldots, u_n)$.

The division in the Euclidean ring $k[y]$ gives $q_1, r_1 \in k[y]$ such that $h = gq_1 + r_1$. The two equalities $f = gq = q_1 g + r_1$ in $K[y]$, and the unicity of the division in this ring proves $q = q_1 \in F(u_1, \ldots, u_n)[y]$. Moreover $q \in L[u_1, \ldots, u_n, y]$ is a polynomial, therefore $q \in F[u_1, \ldots, u_n, y]$.

(c) By the proof of Theorem 13.4.2,

$$h = \prod_{\mu \in G_f} \left(y - \prod_{i=1}^n u_i \alpha_{\mu\sigma(i)} \right) \qquad (= \tilde{h}).$$

Let $\tau \in \sigma^{-1} G_f \sigma$. There exists $\nu \in G_f$ such that $\tau = \sigma^{-1}\nu^{-1}\sigma$. Then

$$\begin{aligned}
\tau \cdot h &= \prod_{\mu \in G_f} \left(y - \prod_{i=1}^{n} u_{(\sigma^{-1}\nu^{-1}\sigma)(i)} \alpha_{(\mu\sigma)(i)} \right) \\
&= \prod_{\mu \in G_f} \left(y - \prod_{j=1}^{n} u_{(\sigma^{-1}\nu^{-1})(j)} \alpha_{\mu(j)} \right) \qquad (j = \sigma(i)) \\
&= \prod_{\mu \in G_f} \left(y - \prod_{k=1}^{n} u_k \alpha_{(\mu\nu\sigma)(k)} \right) \qquad (k = (\sigma^{-1}\nu^{-1})(j)) \\
&= \prod_{\lambda \in G_f} \left(y - \prod_{k=1}^{n} u_k \alpha_{(\lambda\sigma)(k)} \right) \qquad (\lambda = \mu\nu) \\
&= \prod_{\mu \in G_f} \left(y - \prod_{i=1}^{n} u_i \alpha_{(\mu\sigma)(i)} \right) \\
&= h.
\end{aligned}$$

Therefore $\tau \in G$. We have proved $\sigma^{-1} G_f \sigma \subset G$.

$\square$

Ex. 13.4.4 *Consider the polynomial $s_u(y)$ when $f = x^3 + x^2 - 2x - 1$ from Example 13.4.3.*

(a) Compute $s_u(y) \in \mathbb{Q}[u_1, u_2, u_3, y]$, and derive factorization given in Example 13.4.3.

(b) Let h be the first factor of $s_u(y)$ given in Example 13.4.3, multiplied by -1 so that it is monic in y. Using Sage, write h as a polynomial in y so that its coefficients are of the form

a symmetric polynomial in u_1, u_2, u_3 + a remainder in u_1, u_2, u_3.

This should give the formula for h given in Example 13.4.3.

Proof. (a) The following Sage instructions:

```
R.<y,x1,x2,x3,sigma1,sigma2,sigma3,u1,u2,u3> = PolynomialRing(QQ, order = 'lex')
elt = SymmetricFunctions(QQ).e()
e = [elt([i]).expand(3).subs(x0=x1, x1=x2,x2=x3) for i in range(4)]
J = R.ideal(e[1]-sigma1, e[2]-sigma2, e[3]-sigma3)
G = J.groebner_basis()
S = y - (u1*x1 + u2*x2 + u3*x3)
S1 = S * S.subs(x1=x1,x2=x3,x3=x2) *S .subs(x1=x2,x2=x1,x3=x3)
S1 = S1 * S.subs(x1=x2,x2=x3,x3=x1) * S.subs(x1=x3,x2=x1,x3=x2)
S = S1 * S.subs(x1=x3,x2=x2,x3=x1)
s = S.reduce(G).polynomial(y)
sf = s.subs(sigma1=-1,sigma2=-2,sigma3=1)
dec = sf.factor(); dec
```

give the same output as in Example 13.4.3:

$$
\begin{aligned}
s_u(y) = &\left(-y^3 + (-u_1 - u_2 - u_3)\,y^2 + \left(2u_1^2 - 3u_1u_2 + 2u_2^2 - 3u_1u_3 - 3u_2u_3 + 2u_3^2\right)y\right.\\
&\left.+ u_1^3 - 4u_1^2u_2 + 3u_1u_2^2 + u_2^3 + 3u_1^2u_3 - u_1u_2u_3 - 4u_2^2u_3 - 4u_1u_3^2 + 3u_2u_3^2 + u_3^3\right)\\
&\cdot\left(-y^3 + (-u_1 - u_2 - u_3)\,y^2 + \left(2u_1^2 - 3u_1u_2 + 2u_2^2 - 3u_1u_3 - 3u_2u_3 + 2u_3^2\right)y\right.\\
&\left.+ u_1^3 + 3u_1^2u_2 - 4u_1u_2^2 + u_2^3 - 4u_1^2u_3 - u_1u_2u_3 + 3u_2^2u_3 + 3u_1u_3^2 - 4u_2u_3^2 + u_3^3\right)
\end{aligned}
$$

(b) The following Sage instruction:

```
h =  (-1)* dec[1][0]; h
```

gives the second (it's the good one) irreducible factor h of $s_u(y)$, given in Example 13.4.3, multiplied by -1:

$$
\begin{aligned}
h =& y^3 + (u_1 + u_2 + u_3)\,y^2 + \left(-2u_1^2 + 3u_1u_2 - 2u_2^2 + 3u_1u_3 + 3u_2u_3 - 2u_3^2\right)y\\
&- u_1^3 - 3u_1^2u_2 + 4u_1u_2^2 - u_2^3 + 4u_1^2u_3 + u_1u_2u_3 - 3u_2^2u_3 - 3u_1u_3^2 + 4u_2u_3^2 - u_3^3
\end{aligned}
$$

A second reduction doesn't give quite the expected result

```
R.<y,u1,u2,u3,sigma1,sigma2,sigma3> = PolynomialRing(QQ, order = 'lex')
elt = SymmetricFunctions(QQ).e()
e = [elt([i]).expand(3).subs(x0=u1, x1=u2,x2=u3) for i in range(4)]
J = R.ideal(e[1]-sigma1, e[2]-sigma2, e[3]-sigma3)
G = J.groebner_basis()
g = R(h).reduce(G).polynomial(y); g
```

$$y^3+\sigma_1y^2+\left(-2\sigma_1^2+7\sigma_2\right)y+21u_2u_3^2-14u_2u_3\sigma_1-7u_3^2\sigma_1+7u_3\sigma_1^2-\sigma_1^3+7u_2\sigma_2-7u_3\sigma_2+7\sigma_3$$

But this last instructions verify the formula of the text:

```
S.<u1,u2,u3>=ZZ[]
A=S(h(0))
B = 7*sigma3 -sigma1^3 + 7*(u1*u2^2  + u1^2*u3 + u2*u3^2)
B = B.subs(sigma1 = e[1],sigma2=e[2], sigma3=e[3])
B = S(B)
A-B
```

$$0$$

This is a verification of

$$
\begin{aligned}
h = &y^3 + (u_1 + u_2 + u_3)y^2 + (7(u_1u_2 + u_1u_3 + u_2u_3) - 2(u_1 + u_2 + u_3)^2)y\\
&+ 7u_1u_2u_3 - (u_1 + u_2 + u_3)^3 + 7(u_1u_2^2 + u_1^2u_3 + u_2u_3^2).
\end{aligned}
$$

□

Ex. 13.4.5 *Use the method of part (a) of Exercise 4 to derive the factorization of $s_u(y)$ given in Example 13.4.4.*

Proof. The following Sage instructions :

```
R.<y,x1,x2,x3,sigma1,sigma2,sigma3,u1,u2,u3> = PolynomialRing(QQ, order = 'lex')
elt = SymmetricFunctions(QQ).e()
e = [elt([i]).expand(3).subs(x0=x1, x1=x2,x2=x3) for i in range(4)]
J = R.ideal(e[1]-sigma1, e[2]-sigma2, e[3]-sigma3)
G = J.groebner_basis()
S = y - (u1*x1 + u2*x2 + u3*x3)
S1 = S * S.subs(x1=x1,x2=x3,x3=x2) * S.subs(x1=x2,x2=x1,x3=x3)
S1 = S1 * S.subs(x1=x2,x2=x3,x3=x1) * S.subs(x1=x3,x2=x1,x3=x2)
S = S1 * S.subs(x1=x3,x2=x2,x3=x1)
s = S.reduce(G).polynomial(y)
sf = s.subs(sigma1=0,sigma2=0,sigma3=1)
dec = sf.factor(); dec
```

give the same output as in Example 13.4.4:

$$\begin{aligned} s_u(y) =&(y^2 + (-2u_1 + u_2 + u_3)\, y + u_1^2 - u_1u_2 + u_2^2 - u_1u_3 - u_2u_3 + u_3^2)\cdot \\ &(y^2 + (u_1 - 2u_2 + u_3)\, y + u_1^2 - u_1u_2 + u_2^2 - u_1u_3 - u_2u_3 + u_3^2)\cdot \\ &(y^2 + (u_1 + u_2 - 2u_3)\, y + u_1^2 - u_1u_2 + u_2^2 - u_1u_3 - u_2u_3 + u_3^2) \end{aligned}$$

□

Ex. 13.4.6 *As in the proof of Theorem 13.4.5, suppose that we have $s_u(y) \in \mathbb{Z}[u_1, ..., u_n, y]$ and $h \in \mathbb{Q}[u_1, ..., u_n, y]$ is an irreducible factor of $s_u(y)$ when $s_u(y)$ is regarded as an element of $\mathbb{Q}[u_1, ..., u_n, y]$. In this exercise we will study how close h is to being an irreducible factor of $s_u(y)$ in $\mathbb{Z}[x_1, ..., x_n, y]$.*

- *(a) We know that the rings $\mathbb{Z}[x_1, ..., x_n, y]$ and $\mathbb{Q}[x_1, ..., x_n, y]$ are both UFDs. Prove that if $f \in \mathbb{Z}[x_1, ..., x_n, y]$ is irreducible and nonconstant, then it is also irreducible when regarded as an element of $\mathbb{Q}[x_1, ..., x_n, y]$.*
- *(b) Prove that $s_u(y)$ and h are as above, then h is a $\mathbb{Q}$-multiple of an irreducible factor of $s_u(y)$ in $\mathbb{Z}[x_1, ..., x_n, y]$.*

Proof. (a) Assume that $f \in \mathbb{Z}[x_1, ..., x_n, y]$ is irreducible and nonconstant.

Suppose that $f = gh$, where g, h are in $\mathbb{Q}[x_1, \dots, x_n, y]$. There are positive integers r, s such that $rg, sh \in \mathbb{Z}[x_1, \dots, x_n, y]$ (it is not needed to take r, s as small as possible). Then $rsf = (rg)(sh) = g_1h_1$, where $g_1 = rg, h_1 = sh$ are in $\mathbb{Z}[x_1, \dots, x_n, y]$.

Write $rs = p_1^{a_1} \cdots p_r^{a_r}$ the decomposition of rs in prime integers. Note that every prime in $\mathbb{Z}$ is irreducible in $\mathbb{Z}[x_1, \dots, x_n]$, so that

$$rsf = p_1^{a_1} \cdots p_r^{a_r} f$$

is a decomposition in irreducible factors in $\mathbb{Z}[x_1, \dots, x_n]$. The only units of this UFD are ± 1, so that the unicity of the decomposition in irreducible factors in $\mathbb{Z}[x_1, \dots, x_n]$ shows that the decompositions of $g_1 = rg, h_1 = sh$ are in the form

$$g_1 = \pm p_1^{b_1} \cdots p_r^{b_r} f, \qquad h_1 = \pm p_1^{c_1} \cdots p_r^{c_r},$$

or

$$g_1 = \pm p_1^{b_1} \cdots p_r^{b_r}, \qquad h_1 = \pm p_1^{c_1} \cdots p_r^{c_r} f.$$

Therefore h_1 or g_1 is in $\mathbb{Z}$, thus g or h is in $\mathbb{Q}$, so is a unit in $\mathbb{Q}[x_1, \ldots, x_n, y]$. This proves that f is irreducible in $\mathbb{Q}[x_1, \ldots, x_n, y]$.

(b) Since $\mathbb{Z}[x_1, ..., x_n, y]$ is UFD, $s_u(y)$ can be uniquely factorized $s_u(y) = h_1 \cdots h_n$, where $h_1, ..., h_n \in \mathbb{Z}[x_1, ..., x_n, y]$ and are irreducible. By the part (a), $h_1, ..., h_n$ are irreducible when regarded as elements of $\mathbb{Q}[x_1, ..., x_n, y]$. Hence for any irreducible factor $h \in \mathbb{Q}[x_1, ..., x_n, y]$ of $s_u(y)$, there exists i such that $h \mid h_i$. It follows that h is associate to h_i, $h = \lambda h_i, \lambda \in \mathbb{Q}$, is the product of h_i by a suitable constant from $\mathbb{Q}$, where h_i is a factor of $s_u(y)$ irreducible in $\mathbb{Z}[x_1, ..., x_n, y]$.

□

Ex. 13.4.7 *Let $f = x^5 + 20x + 16 \in \mathbb{Q}[x]$ be the polynomial of Example 13.4.6. Show that f is irreducible over $\mathbb{Q}$, and compute its discriminant and irreducible factorization modulo 7.*

Proof. The given polynomial f is irreducible, since $f(x-1) = (x-1)^5 + 20(x-1) + 16 = x^5 - 5x^4 + 10x^3 - 10x^2 + 25x - 5$ is irreducible by Schönemann-Eisenstein criterion with $p = 5$.

The discriminant may be calculated by the formula (cf. Ex.13.2.15):

$$\Delta(f) = 256a^5 + 3125b^4,$$

where $a = 20, b = 16$. Then

$$\Delta(f) = 2^8 20^5 + 5^5 16^4 = 2^{18} 5^5 + 5^5 2^{16} = 2^{16} 5^5 (4+1) = 2^{16} 5^6.$$

Reducing the polynomial modulo 7 gives: $\bar{f}(x) = x^5 + 6x + 2$.

We have $\bar{f}(4) = \bar{f}(5) = 0$ and $\bar{f}(i) \neq 0$ for $i \in \{0, 1, 2, 3, 6\}$. Division of $\bar{f}$ by $(x-4) = (x+3)$ and $(x-5) = (x+2)$ gives:

$$\bar{f} = (x+2)(x+3)(x^3 + 2x^2 + 5x + 5) \ \ in\ \mathbb{F}_7.$$

□

Ex. 13.4.8 *Compute the Galois group of $f = x^5 - 6x + 3$ over $\mathbb{Q}$ using reduction modulo 11 and the method of Example 13.4.6.*

Proof. The discriminant calculation (cf. Ex.13.2.15):

$$\Delta(f) = 256a^5 + 3125b^4,$$

where $a = -6, b = 3$. Then

$$\Delta(f) = 2^8(-6)^5 + 5^5 3^4 = 3^4(5^5 - 3 \cdot 2^{13}) = 3^4(3125 - 256 \cdot 96) = -3^4 \cdot 19 \cdot 1129.$$

Reducing the polynomial modulo 11 gives: $\bar{f}(x) = x^5 + 5x + 3$.

The Sage instructions :

```
R.<x> = PolynomialRing(GF(11))
f = x^5 - 6*x + 3
f.factor()
```

gives the irreducible factorization:

$$\bar{f} = (x^2 + 3x + 8)(x^3 + 8x^2 + x + 10).$$

Since $\Delta(f) < 0$, the Galois group $G_f \subset S_5$ of f over $\mathbb{Q}$ is not a subgroup of A_5. The classification of transitive subgroups of S_5 given in (13.16) shows that $G_f = S_5$ or $G_f \simeq \mathrm{AGL}(1, \mathbb{F}_5)$.

Since $11 \nmid \Delta(f)$, by Theorem 13.4.5, G_f contains the disjoint product of a 3-cycle and a 2-cycle, which has order 6, thus the order of the Galois group is divisible by 3 and 2.

The order of $\mathrm{AGL}(1, \mathbb{F}_5)$ is 20. Hence the Galois group G_f of f over $\mathbb{Q}$ is $G_f = S_5$.

□

Ex. 13.4.9 *Prove that two permutations in S_n are conjugate if and only if they have the same cycle type.*

Proof. Let $\sigma \in S_n$ have cycle type $(k_1, k_2, ..., k_l)$. Then σ can be expressed uniquely as the product of disjoint cycles $\sigma = \alpha_1\alpha_2 \cdots \alpha_l$, where α_i is a k_i-cycle.

Let $\tau \in S_n$ such that $\rho = \tau\sigma\tau^{-1}$. Then:

$$\tau\sigma\tau^{-1} = \tau\alpha_1\alpha_2 \cdots \alpha_l\tau^{-1} = \tau\alpha_1\tau^{-1}\tau\alpha_2\tau^{-1} \cdots \tau\alpha_l\tau^{-1} = \alpha_{\tau(1)}\alpha_{\tau(2)} \cdots \alpha_{\tau(l)}$$

Since α_i and α_j are disjoint for $i, j \in \{1, 2, ..., l\}$, then $\tau\alpha_i\tau^{-1}$ and $\tau\alpha_j\tau^{-1}$ are also disjoint.

Indeed, being disjoint means no number is moved by both α_i and α_j, i.e., there is no k such that $\alpha_i(k) \neq k$ and $\alpha_j(k) \neq k$. If $\tau\alpha_i\tau^{-1}$ and $\tau\alpha_j\tau^{-1}$ are not disjoint, then they both move some number l. Then $\tau\alpha_i\tau^{-1}(l) \neq l$ and $\tau\alpha_j\tau^{-1}(l) \neq l$, hence $\alpha_i\tau^{-1}(l) \neq \tau^{-1}(l)$ and $\alpha_j\tau^{-1}(l) \neq \tau^{-1}(l)$, which means that $\tau^{-1}(l)$ is moved by both α_i and α_j. This is a contradiction.

Therefore $\tau\sigma\tau^{-1}$ is the product of τ-conjugates of disjoint cycles for σ, and these τ-conjugates are disjoint cycles with the same respective lengths, i.e., $\tau\sigma\tau^{-1}$ has the same cycle type as σ.

For the converse direction, suppose σ_1 and σ_2 have the same cycle type $(k_1, k_2, ..., k_l)$. Then

$$\sigma_1 = (a_1a_2...a_{k_1})(a_{k_1+1}a_{k_1+2}...a_{k_1+k_2}) \cdots$$

and

$$\sigma_2 = (b_1b_2...b_{k_1})(b_{k_1+1}b_{k_1+2}...b_{k_1+k_2}) \cdots$$

where the cycles are disjoint. Let define the permutation $\tau \in S_n$ by $\tau(a_i) = b_i$ for all i. Then $\tau\sigma_1\tau^{-1} = \sigma_2$, i.e., σ_1 and σ_2 are τ-conjugate.

□

Ex. 13.4.10 *Let G be a subgroup of S_n. For a fixed cycle type $d_1, ..., d_r$, consider the set (13.44) of all elements of G with this cycle type.*

(a) Prove that this set is either empty or a union of conjugacy classes of G.

(b) Give an example where the set is empty, and give another example where it is a union of two conjugacy classes of G.

Proof. (a) For an element g of a subgroup G, its conjugacy class is the set of elements conjugate to it:

$$\{xgx^{-1} : x \in G\}.$$

Suppose the conjugacy classes of g and h overlap, i.e., $xgx^{-1} = yhy^{-1}$ for some x and y in the subgroup. Therefore

$$g = x^{-1}yhy^{-1}x = (x^{-1}y)h(x^{-1}y)^{-1},$$

which shows each element of G that is conjugate to g is also conjugate to h. In the other way, from $xgx^{-1} = yhy^{-1}$ write $h = (y^{-1}x)h(y^{-1}x)^{-1}$, and similar calculation shows that each element of G that is conjugate to h is also conjugate to g.

Hence the conjugacy classes are equal, which means that subgroup G is the set of distinct conjugacy classes $\{S_1, S_2, ..., S_l\}$ and any element $x \in G$ belongs to one of the conjugacy class.

Let $S = \{\sigma \in G \mid \sigma \text{ has cycle type } d_1, ..., d_r\}$. If G does not have element with cycle type $d_1, ..., d_r$, then S is empty.

If S is not empty, then any $\sigma \in S$ belongs to some conjugacy class. Let the subset $\{S_{k_1}, S_{k_2}, ..., S_{k_m}\} \subset \{S_1, S_2, ..., S_l\}$ is such that any element of S belongs to one of subset in $\{S_{k_1}, S_{k_2}, ..., S_{k_m}\}$.

In Ex. 13.4.9 has been showed that all elements of conjugate class have the same cycle type. It means that if $\tau \in S_{k_i}$, then τ has cycle type $d_1, ..., d_r$, i.e., $\tau \in S$, and this is valid for all $S_{k_i}, k_i \in (k_1, ..., k_m)$.

Therefore, $S = \cup_{i=1}^{m} S_{k_i}$, i.e., the set of elements of G with the same cycle type is either empty or a union of conjugacy classes of G.

(b) Consider subgroup $A_3 \subset S_3$. Since A_3 doesn't have transpositions, the cycle type $(d_1, d_2) = (1, 2)$ is not possible and set of A_3 elements with cycle type (1,2) is empty.

Consider subgroup $A_4 \subset S_4$.

The 3-cycle (123) and its inverse (132) are not conjugate in A4. To see this, let's determine all possible $\sigma \in S_4$ that conjugate (123) to (132). For $\sigma \in S_4$, the condition $\sigma(123)\sigma^{-1} = (132)$ is the same as $(\sigma(1)\sigma(2)\sigma(3)) = (132)$. There are three possibilities:

- $\sigma(1) = 1$, so $\sigma(2) = 3$ and $\sigma(3) = 2$, and necessarily $\sigma(4) = 4$. Thus $\sigma = (23)$.
- $\sigma(1) = 3$, so $\sigma(2) = 2$ and $\sigma(3) = 1$, and necessarily $\sigma(4) = 4$. Thus $\sigma = (13)$.
- $\sigma(1) = 2$, so $\sigma(2) = 1$ and $\sigma(3) = 3$, and necessarily $\sigma(4) = 4$. Thus $\sigma = (12)$.

Therefore the only possible σ's are transpositions, which are not in A_4. It is obvious that all other 3-cycles are conjugate to (123) or (132).

Hence, all elements of A_4 with cycle type $(d_1, d_2) = (1, 3)$ are in the union of two conjugacy classes with the representatives $\{(123), (132)\}$.

□

Ex. 13.4.11 *This exercise will explore the ideas introduced in Example 13.4.8.*

(a) For each transitive subgroup of S_4, make a table similar to (13.46) that lists the number of elements of each possible cycle type for that subgroup.

(b) For each polynomial in Exercise 14 of Section 13.1, compute its factorization modulo 200 primes, and record your results in a table similar to (13.45). Use this to guess the Galois group of each polynomial.

Proof. (a) There are five transitive subgroups of S_4 - $\{S_4, A_4, C_2 \times C_2, C_4, D_8\}$. The following Sage instructions produce the similar to (13.46) table with the percentage of elements of each possible cycle for each subgroup:

```
S4 = SymmetricGroup(4)
A4 = AlternatingGroup(4)
C2C2 = PermutationGroup(["(1,3)(2,4)","(1,2)(3,4)"])
C4 = CyclicPermutationGroup(4)
D8 = DihedralGroup(4)
G =[S4,A4,C2C2,C4,D8]

for j in range(5):
    V =[g.cycle_type() for g in G[j]]
    K=[0,0,0,0,0]
    for i in range(len(V)):
        if V[i]==[1,1,1,1] : K[0]=K[i]+1
        elif V[i]==[2,1,1] : K[1]=K[1]+1
        elif V[i]==[3,1] : K[2]=K[2]+1
        elif V[i]==[2,2] : K[3]=K[3]+1
        elif V[i]==[4] : K[4]=K[4]+1
        else : print("Error")
        Sm=sum(K)
    if j==0 :
        row = matrix([round(K[0]/Sm*100.0,1), round(K[1]/Sm*100.0,1)
            ,round(K[2]/Sm*100.0,1)*1,round(K[3]/Sm*100.0,1)
            ,round(K[4]/Sm*100.0,1)])
    else :
        U = [round(K[0]/Sm*100.0,1), round(K[1]/Sm*100.0,1)
            ,round(K[2]/Sm*100.0,1)*1,round(K[3]/Sm*100.0,1)
            ,round(K[4]/Sm*100.0,1)]]
        row = matrix(row.rows()+[U])
C=[["1,1,1,1","1,1,2","1,3","2,2","4"]]+[list(row) for row in row]
A = ["cycle type","S_4","A_4","C_2xC_2","C_4","D_8"]
C = [[a] + u for a, u in zip(A, C)]
(table(C, header_row=True, frame=True))
```

cycle type	1,1,1,1	1,1,2	1,3	2,2	4
S_4	4.2	25.0	33.3	12.5	25.0
A_4	8.3	0.0	66.7	25.0	0.0
$C_2 \times C_2$	25.0	0.0	0.0	75.0	0.0
C_4	25.0	0.0	0.0	25.0	50.0
D_8	12.5	25.0	0.0	37.5	25.0

(b) The following Sage instructions produce the similar to (13.45) table. The percentage of primes corresponding to each possible cycle for 200 primes $7 \leq p \leq 1237$ is calculated for each polynomial in Exercise 13.1.14 and the polynomial from Example 13.4.8:

```
R.<X> = PolynomialRing(ZZ)
P = Primes()
f=[X^4 - 7*X^3 + 19*X^2 - 23*X + 11,X^4 + 4*X + 2,X^4 + 8*X + 12
    ,X^4 + 1,X^4 + X^3 + X^2 + X + 1,X^4 - 2]
for r in range(6):
    K=[0,0,0,0,0]
    for i in range(2,203):
        R11.<x> = PolynomialRing(GF(P.unrank(i)))
        S=[0,0,0,0]
        for j in range(len(R11(f[r]).factor())):
            d=R11(f[r]).factor()[j][0].degree()
            m=R11(f[r]).factor()[j][1]
            S[d-1]=S[d-1]+m
        if S[0]==4: K[0]=K[0]+1
        elif S[0]==2 and S[1]==1: K[1]=K[1]+1
        elif S[0]==1 and S[2]==1: K[2]=K[2]+1
        elif S[1]==2 : K[3]=K[3]+1
        elif S[3]==1 : K[4]=K[4]+1
        else : print("Error")
        Sm=sum(K)
    if r==0 :
        row = matrix([round(K[0]/Sm*100.0,1), round(K[1]/Sm*100.0,1)
            ,round(K[2]/Sm*100.0,1)*1,round(K[3]/Sm*100.0,1)
            ,round(K[4]/Sm*100.0,1)])
    else :
        U = [round(K[0]/Sm*100.0,1), round(K[1]/Sm*100.0,1)
            ,round(K[2]/Sm*100.0,1)*1,round(K[3]/Sm*100.0,1)
            ,round(K[4]/Sm*100.0,1)]
        row = matrix(row.rows()+[U])
C=[["1,1,1,1","1,1,2","1,3","2,2","4"]]+[list(row) for row in row]
A = ["cycle type"]+f
C = [[a] + u for a, u in zip(A, C)]
B = ["Galois group","C_4","S_4","A_4","C_2xC_2","C_4","D_8"]
C = [a + [u] for a, u in zip(C, B)]
(table(C, header_row=True, frame=True))
```

cycle type	1,1,1,1	1,1,2	1,3	2,2	4	Galois group
$X^4 - 7X^3 + 19X^2 - 23X + 11$	25.4	0.0	0.0	22.9	51.7	C_4
$X^4 + 4X + 2$	3.0	26.9	33.8	13.4	22.9	S_4
$X^4 + 8X + 12$	6.5	0.0	67.2	26.4	0.0	A_4
$X^4 + 1$	22.9	0.0	0.0	77.1	0.0	$C_2 \times C_2$
$X^4 + X^3 + X^2 + X + 1$	25.4	0.0	0.0	22.9	51.7	C_4
$X^4 - 2$	10.4	25.4	0.0	37.3	26.9	D_8

The last column provides the guess about the Galois group of each polynomial. The comparison with Exercise 14 of Section 13.1 and Example 13.4.8 results supports the Chebotarev Density Theorem.

$\square$