Solutions to David A.Cox "Galois Theory"

Richard Ganaye

May 22, 2020

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 $\alpha_1, \ldots, \alpha_n$ 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 $\beta_1, \ldots, \beta_n$ 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 $1 \leq i \leq n$. 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

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

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

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

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

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

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

$$\begin{aligned}\sigma(\alpha_{\gamma(i)}) &= \alpha_{\gamma(\tau_2(i))}\\ \sigma(\alpha_{\gamma(i)}) &= \alpha_{\tau_1(\gamma(i))}.\end{aligned}$$

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

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

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 $\sigma \in \mathrm{Gal}(L/F)$,

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

So, if we change the labels, then G gets replaces 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 $G/H \simeq \{1, -1\}$. So there exists a group homomorphism

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

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 $\tau_1\tau_2 \in H$.

Sine 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 to this equality in $F[x_1, x_2, x_3, x_4]$ the evaluation defined by $x_1 \mapsto \alpha_1, \ldots, x_4 \mapsto \alpha_4$, 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

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

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

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

□

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 $\Delta = \delta^2 \in F^2$.
- Conversely, if $\Delta \in F^2$,then $\Delta = a^2,\ a \in F$, 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

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

$\alpha_2+\alpha_3 = -p \in F, \alpha_2\alpha_3 = q \in F$, so

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

If $\alpha_1 = \alpha_2$ or $\alpha_1 = \alpha_3$, then $\Delta(f) = 0 \in F^2$.

In the other 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 $4\beta+c_1^2-4c_2^2 = 0$ 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

$$s := \alpha_1+\alpha_2 = \alpha_3+\alpha_4$$
$$p := \alpha_1\alpha_2 = \alpha_3\alpha_4$$

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 $4\beta+c_1^2-4c_2^2 = 0$ in part (c) of Theorem 13.1.1, where $\theta_f(y)$ has a unique root β in F. Therefore $\theta_f(y) = (y-\beta)(y-\beta')(y-\beta'')$, where $\beta' \notin F, \beta'' \notin F$.

If θ_f was not separable, then $\beta' = \beta''$, and $\theta_f(t) = (y-\beta)(y-\beta')^2 \in F[y], \beta \in F$, thus $(y-\beta'^2) = y^2 - 2\beta' y + \beta'^2 \in F[y]$, which implies that $2\beta' \in F$.

Since the characteristic of F is not 2, $\beta' \in F$. This is a contradiction, so θ_f is separable. Since the discriminant of θ_f and f are equal, f is separable.

Then by part (b), $\beta^2 - 4c_4 \neq 0$, and since f is separable, $\Delta(f) \neq 0$, 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 $(1\,3\,2\,4) = (1\,3)(3\,2)(2\,4) \notin A_4$, $\sigma(\sqrt{\Delta(f)}) = -\sqrt{\Delta(f)}$, 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, $\sqrt{\Delta(f)(\beta^2 - 4c_4)} \notin F$, so

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

  Therefore G is conjugate to $\langle (1\,3\,2\,4), (1\,2) \rangle$ if and only if $\Delta(f)(\beta^2 - 4c_4) \notin (F^*)^2$.

$\square$

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,

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

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()
```

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

```
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

$$x^2 - z_1 x + 1, \qquad x^2 - z_2 x + 1,$$

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 $x^2 - z_1 x + 1$, and α_3, α_4 the roots of $x^2 - z_2 x + 1$, 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 $\theta_f(y)$. $\square$

Ex. 13.1.10 *As in Example 13.1.4, let $f = x^4 + bx^2 + d \in F[x]$, where $d \notin F^2$. Compute $\Delta(f)$ and $\theta_f(y)$.*

Proof. The discriminant of f is

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

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 if F if $d \notin F^2$, and the discriminant is not a square in F^2. $\square$

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

$$f = x^4 + ax^3 + bx^2 + ax + 1 = (x^2 - z_1 x + 1)(x^2 - z_2 x + 1),$$

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()
```

$$C2 \times C2$$

$\square$

$8^2 + 15^2 = 17^2$ 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 $\sqrt{\Delta(g)} = y_1 - y_2 \in F(\sqrt{a})$. As $\deg(g) = 2$, 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, which 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

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

□

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, $4 = |\mathcal{O}_\alpha| = (G : G_\alpha)$, so $G_\alpha = \{e\}$. Therefore $\tilde{\sigma}^i \neq \tilde{\sigma}^j$ if $1 \leq i < j \leq 4$. So $\tilde{\sigma}(\alpha_1) = \alpha_3, \tilde{\sigma}(\alpha_3) = \alpha_2, \tilde{\sigma}(\alpha_2) = \alpha_4$ are the four distinct roots of f, and $\sigma = (1\,3\,2\,4)$.

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

  As $\Delta(f) \notin F^2$, $F(\sqrt{\Delta})$ 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 $F \subset F(\sqrt{\Delta}) \subset L$, and the fixed field of $H = \langle\sigma^2\rangle$ is $L_H = F(\sqrt{\Delta})$.

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

$$\text{True}$$

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

```
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 $\mathbb{Z}/4\mathbb{Z}$.

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.

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 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

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 $\mathrm{Gal}_{\mathbb{Q}}(f) \simeq S_4$ (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 $f = \Phi_4$.)

(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

$$G \simeq D_8.$$

□

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

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

There is at most one t_i equal to 0. Indeed, if $t_1 = t_2 = 0$ (for instance), then $y_1 = y_2$ and θ_f and f would not be separable, in contradiction with $\Delta(f) \neq 0$ in part (c) of Theorem 13.1.1. 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 $t_i^2 = 4y_i + C_1^2 - 4c_2 \in L$, 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

$$F \subset F(\sqrt{4y_1 + c_1^2 - 4c_2}) \subset F(\sqrt{4y_1 + c_1^2 - 4c_2}, \sqrt{\delta}) \subset F(\sqrt{4y_1 + c_1^2 - 4c_2}, \sqrt{\delta}, \sqrt{4y_2 + c_1^2 - 4c_2}) = L.$$

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 4, 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 $(1\,2)(3\,4)$ by $\sigma \in S_4$ is $(\sigma(1)\,\sigma(2))(\sigma(3)\,\sigma(4))$, so is not in H_1. The groups 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.

$\square$