Homework 4
Algebra

Joshua Ruiter

February 21, 2018

Chapter V

Proposition 0.1 (Exercise 20a)**.** *Let $F \subset L$ be a field extension and let $x \in L$ be transcendental over F. Let $K \neq F$ be an intermediate field satisfying*

$$F \subset K \subset F(x)$$

Then x is algebraic over K.

Proof. Since $K \neq F$, there exists $\alpha \in K \setminus F$. We know that

$$F(x) = \left\{ \frac{f(x)}{g(x)} : f, g \in F[y], g(x) \neq 0 \right\}$$

The requirement $g(x) = 0$ can be dropped, since x is transcendental over F. Since $\alpha \in K \subset F(x)$, we can write α as

$$\alpha = \frac{f(x)}{g(x)} \implies \alpha g(x) - f(x) = 0$$

for some $f, g \in F[y]$. Then define $h(y) \in K[y]$ by $h(y) = \alpha g(y) - f(y)$. By the above, h has x as a root. Also note that h cannot be the zero polynomial, since if it were, then $\alpha g = f$, but f has coefficients in F and the coefficients of αg lie outside F, since $\alpha \notin F$. Thus x is a root of $h \in K[y]$, so x is algebraic over K. □

Proposition 0.2 (Gauss's Lemma)**.** *Let R be a unique factorization domain with field of fractions F. A non-constant polynomial in $R[x]$ is irreducible in $R[x]$ if and only if it is both irreducible in $F[x]$ and primitive (coefficients have gcd 1) in $R[x]$.*

Proposition 0.3 (Exercise 20b)**.** *Let F be a field and let x be transcendental over F. Let $y = \frac{f(x)}{g(x)}$ be a rational function with $f, g \in F[x]$. Let $n = \max(\deg f, \deg g)$ and assume $n \geq 1$. Then*

$$[F(x) : F(y)] = n$$

Proof. We think of f, g as polynomials in $F[x]$. Then we can define

$$h(t) = f(t) - yg(t) \in F[y,t]$$

Note that $F[y][t] = F[t][y] = F[y,t] \subset F(y)[t]$. We claim that h is not the zero polynomial. Since $n \geq 1$, y is not in F. If h were zero, then $f(t) = yg(t)$ and the leading coefficient of $f(t)$ is in F and the leading coefficient of $yg(t)$ is not, which is a contradiction. Thus h is not the zero polynomial.

By construction, x is a root of h, so the irreducible polynomial of x over $F(y)$ divides h. Note that $F(y)$ is the quotient field of $F[y]$. As a polynomial in the variable y with coefficients in $F[t]$, h is linear, so it is irreducible. That is, h is irreducible in $(F[t])[y]$, so it is irreducible in $F[y][t]$. Then by Gauss's Lemma (see above for statement), h is irreducible in $F(y)[t]$. Thus h is the irreducible polynomial of x over $F(y)$.

Finally, note that the degree of h as a polynomial in t with coefficients in $F(y)$ is $\max(\deg f, \deg g) = n$. Then by Proposition 1.6 (Lang pg 227),

$$[F(y) : F(x)] = \deg h = n$$

□

Proposition 0.4 (Exercise 24a)**.** *Let k be a field of characteristic p, and let t, u be algebraically indepenent over k. Then $k(t,u)$ has degree p^2 over $k(t^p, u^p)$. Symbolically, $[k(t,u) : k(t^p, u^p)] = p^2$.*

Proof. We have the tower of fields

$$k(t^p, u^p) \subset k(t, u^p) \subset k(t,u)$$

Since t, u are algebraically independent over k, t^p does not have a pth root in $k(t^p, u^p)$, so the polynomial $f(x) = x^p - t^p \in k(t^p, u^p)[x]$ is irreducible by Exercise 15 from previous homework (Lang pg 254). Also, f splits linearly as

$$f(x) = x^p - t^p = (x-t)^p$$

so f is the irreducible polynomial of t over $k(t^p, u^p)$, and the splitting field of f is $k(t, u^p)$. Thus by Proposition 1.4 (Lang pg 225),

$$[k(t, u^p) : k(t^p, u^p)] = \deg f = p$$

Similarly, u^p does not have a pth root in $k(t, u^p)$, so the polynomial $g(x) = x^p - u^p \in k(t, u^p)[x]$ is irreducible by Exercise 15. It splits linearly as

$$g(x) = x^p - u^p = (x-u)^p$$

so g is the irreducible polynomial of u over $k(t, u^p)$, and the splitting field of g is $k(t,u)$. Thus by Proposition 1.4,

$$[k(t,u) : k(t, u^p)] = \deg g = p$$

Then by multiplicativity of degrees for towers,

$$[k(t,u) : k(t^p, u^p)] = [k(t,u) : k(t, u^p)][k(t, u^p) : k(t^p, u^p)] = p^2$$

□

Proposition 0.5 (Exercise 24b)**.** *Let k be a field of characteristic p, and let t, u be algebraically independent over k. Then there are infinitely many extensions E such that*

$$k(t^p, u^p) \subset E \subset k(t, u)$$

Proof. By part (a), $k(t, u)$ is a finite extension of $k(t^p, u^p)$, so we can apply the Primitive Element Theorem. By the PET, there exists an element $\alpha \in k(t, u)$ such that $k(t^p, u^p, \alpha) = k(t, u)$ if and only if there are only a finite number of intermediate extensions E satisfying

$$k(t^p, u^p) \subset E \subset k(t, u)$$

So in order to show that there are infinitely many extensions, we just need to show that such an α does not exist. Suppose such an α exists. Since $\alpha \in k(t, u)$, we can write α as

$$\alpha = \frac{f(t, u)}{g(t, u)}$$

where f, g are polynomials in t, u with coefficients in k. Then raising to the pth power, since $\operatorname{char} k = p$,

$$\alpha^p = \left(\frac{f(t, u)}{g(t, u)} \right)^p = \frac{f^p(t^p, u^p)}{g^p(t^p, u^p)} \in k(t^p, u^p)$$

where f^p, g^p indicate raising the coefficients from k to the pth power. Thus $\alpha^p \in k(t^p, u^p)$. Thus the polynomial

$$x^p - \alpha^p = (x - \alpha)^p$$

is in $k(t^p, u^p)[x]$, with α as a root, so $\operatorname{Irr}(\alpha, k(t^p, u^p))$ divides $x^p - \alpha^p$. In particular, it has degree $\leq p$. The degree of $k(t^p, u^p)(\alpha)$ over $k(t^p, u^p)$ is bounded above by the degree of the irreducible polynomial of α, so

$$[k(t^p, u^p)(\alpha) : k(t^p, u^p)] \leq p$$

By assumption, $k(t^p, u^p, \alpha) = k(t, u)$, so

$$[k(t, u) : k(t^p, u^p)] \leq p$$

But we showed in part (a) that the degree above is precisely p^2, which is decidedly not less than p. Thus no such α exists, so by the reasoning at the beginning involving the PET, there are infinitely manyintermediate extensions $k(t^p, u^p) \subset E \subset k(t, u)$. □

Lemma 0.6 (for Exercise 25)**.** *Any finite field extension of a finite field is generated by a single element.*

Proof. Let k be finite and E/k a finite extension. Then E is finite, so $E^\times = E \setminus \{0\}$ is a cyclic multiplicative group. Let α be a generator. Then $E = k(\alpha)$. □

The next lemma is the same claim as for Exercise 25, with the extra hypothesis that E/k is purely inseparable. This is used for the proof of the more general statement.

Lemma 0.7 (for Exercise 25)**.** *Let k be a field of characteristic $p > 0$, and let E be a finite, purely inseparable extension of k. Let $p^r = [E : k]_i$. Suppose that there is no $s < r$ so that $E^{p^s} k$ is separable over k. (Equivalently, α^{p^s} is separable over k for each $\alpha \in E$.) Then E can be generated by one element over k.*

Proof. By hypothesis, there is no $s < r$ such that β^{p^r} is separable over k for every $\beta \in E$. Thus there exists $\alpha \in E$ such that $\alpha^{p^{r-1}}$ is not separable over k. Note that $[k(\alpha) : k]_1 = 1$ since E/k is purely inseparable. By Proposition 6.1 (Lang pg 251),

$$[k(\alpha) : k] = p^\mu [k(\alpha) : k]_2 = p^\mu$$

for some $\mu \geq 0$, and α^{p^μ} is separable over k. If $r < \mu$, then $\alpha^{p^{r-1}}$ is separable (using the hypotheses) but $\alpha^{p^{r-1}}$ is not separable, so $\mu \geq r$. On the other hand, $p^\mu = [k(\alpha) : k]$ must divide $[E : k] = [E : k]_i = p^r$, so $\mu \leq r$. Thus $\mu = r$. Thus

$$p^r = [E : k] = [E : k(\alpha)][k(\alpha) : k] = [E : k(\alpha)]p^\mu = [E : k(\alpha)]p^r \implies [E : k(\alpha)] = 1$$

which implies $E = k(\alpha)$. □

Proposition 0.8 (Exercise 25)**.** *Let k be a field of characteristic $p > 0$, and let E be a finite extension of k. Let $p^r = [E : k]_i$. Suppose that there is no $s < r$ so that $E^{p^s} k$ is separable over k. (Equivalently, α^{p^s} is separable over k for each $\alpha \in E$.) Then E can be generated by one element over k.*

Proof. We may assume that k is infinite, since if k is finite we apply Lemma 0.6.

By Proposition 6.6 (Lang pg 250), we can choose an intermediate field $k \subset E_0 \subset E$ so that E/E_0 is purely inseparable and E_0/k is separable. By the Primitive Element Theorem (Theorem 4.6 on pg 243 of Lang), $E_0 = k(\alpha)$ for some $\alpha \in E_0$. By Lemma 0.7 above, $E = E_0(\beta)$ for some $\beta \in E$. Thus $E = k(\alpha, \beta)$. We will use α, β to construct a primitive element.

$$\begin{array}{c} E = E_0(\beta) \\ \Big| \text{ purely inseparable} \\ E_0 = k(\alpha) \\ \Big| \text{ separable} \\ k \end{array}$$

By hypothesis, there exists $\mu \geq 0$ so that β^{p^μ} is separable over k. Thus $\beta^{p^\mu} \in E_0$, since E_0 is the maximal separable extension. Since $E_0 = k(\alpha)$, using the PET there are only finitely many subextensions $k \subset F \subset E_0$. For $\delta \in k^\times$, we have a subextension

$$k \subset k\left(\alpha^{p^\mu} + \delta^{p^\mu} \beta^{p^\mu}\right) \subset E_0$$

since $\alpha, \delta, \beta^{p^\mu} \in E_0$. By Exercise 15 of Chapter V (Lang pg 254) from previous homework,

$$E_0 = k(\alpha) = k\left(\alpha^{p^n}\right) \qquad \forall n \geq 0$$

Combining this with the fact that $\beta^{p^\mu} \in E_0$,

$$E_0 = k(\alpha) = k\left(\alpha^{p^\mu}\right) = k\left(\alpha^{p^\mu}, \beta^{p^\mu}\right)$$

Because k is infinite, $k^\times$ is infinite, so there are infinitely many distinct $\alpha^{p^\mu} + \delta^{p^\mu}\beta^{p^\mu}$. Then by the pigeonhole principle, there exist δ_1, δ_2 with $\delta_1 \neq \delta_2$ so that

$$\widetilde{k} := k\left(\alpha^{p^\mu} + \delta_1^{p^\mu}\beta^{p^\mu}\right) = k\left(\alpha^{p^\mu} + \delta_2^{p^\mu}\beta^{p^\mu}\right)$$

(This defines $\widetilde{k}$.) Then

$$\left(\alpha^{p^\mu} - \delta_1^{p^\mu}\beta^{p^\mu}\right) - \left(\alpha^{p^\mu} - \delta_2^{p^\mu}\beta^{p^\mu}\right) = \left(\delta_1^{p^\mu} - \delta_2^{p^\mu}\right)\beta^{p^\mu} = (\delta_1 - \delta_2)^{p^\mu}\beta^{p^\mu} \in \widetilde{k}$$

Since $\delta_1 \neq \delta_2$, we have $\delta_1 - \delta_2 \neq 0$, so $(\delta_1 - \delta_2)^{p^\mu} \in k^\times$, so $\beta^{p^\mu} \in \widetilde{k}$. This implies that $\alpha^{p^\mu} \in \widetilde{k}$ as well. Thus

$$E_0 = k\left(\alpha^{p^\mu}, \beta^{p^\mu}\right) \subset \widetilde{k}$$

Since $\widetilde{k} \subset E_0$, this implies that $E_0 = \widetilde{k}$. Finally, we claim that $E = k(\alpha + \delta\beta)$. For convenience, define $\delta = \delta_1$. We already know that $k(\alpha + \delta\beta) \subset E$. Recall that $E = k(\alpha, \beta)$, so to show the other inclusion we just need to show that $\alpha, \beta \in k(\alpha + \delta\beta)$. Note that

$$(\alpha + \delta\beta)^{p^\mu} = \alpha^{p^\mu} + \delta^{p^\mu}\beta^{p^\mu} \implies E_0 = k\left(\alpha^{p^\mu} + \delta^{p^\mu}\beta^{p^\mu}\right) \subset k(\alpha + \delta\beta)$$

Since $\alpha \in E_0$, this implies $\alpha \in k(\alpha + \delta\beta)$. Since $\alpha + \delta\beta$ is also in there, this gives us $\delta\beta \in k(\alpha + \delta\beta)$, and since $\delta \in k^\times$ we get $\beta \in k(\alpha + \delta\beta$. Thus

$$E = k(\alpha, \beta) = k(\alpha + \delta\beta)$$

so E is generated by a single element over k.

□

Chapter VI

Note: We use the notation D_8 for the dihedral group with eight elements, which has the presentation

$$\langle\, \sigma, \tau \mid \tau^2 = 1, \tau\sigma\tau^{-1} = \sigma^3 \,\rangle$$

We often use the fact that any group with 8 elements satisfying the above relations is isomorphic to D_8.

Lemma 0.9 (for Exercise 1)**.** *Let α be algebraic over $\mathbb{Q}$. Then the quotient field of $\mathbb{Z}[\alpha]$ is $\mathbb{Q}(\alpha)$.*

Proof. By definition, $\mathbb{Q}(\alpha)$ is the smallest subfield of $\mathbb{C}$ that contains $\mathbb{Q}$ and α, so it is also the smallest subfield of $\mathbb{C}$ that contains $\mathbb{Z}$ and α, which is by definition the quotient field of $\mathbb{Z}[\alpha]$. □

Lemma 0.10 (for Exercise 1)**.** *Let k be a field, and let $f(x) \in k[x]$ be irreducible and separable. Let K be the splitting field of f, and let G be the Galois group of K over k. Then G acts transitively on the roots of f.*

Proof. From class. □

Lemma 0.11 (for Exercise 1)**.** *Let k be a field and let $f, g \in k[x]$ be irreducible. Let F, G be the splitting fields of f, g respectively. Then the compositum FG is the splitting field of fg.*

Proof. From class. □

Proposition 0.12 (Exercise 1ab)**.** .

a*) The Galois group of $x^3 - x - 1$ over $\mathbb{Q}$ is S_3.*

b*) The Galois group of $x^3 - 10$ over $\mathbb{Q}$ is S_3.*

Proof. As shown on page 270 of Lang, an irreducible cubic polynomial over a field with characteristic $\neq 2, 3$ is S_3 if and only if the discriminant is not a square in k. If it is, then the Galois group is A_3.

(a) By the integral root test, any root of $x^3 - x - 1$ in $\mathbb{Q}$ must be ± 1, but neither is a solution, so f is irreducible. The discriminant is $-4(-1)^3 - 27(-1)^2 = 4 - 27 = -23$ which is not a square in $\mathbb{Q}$, so the Galois group is S_3.

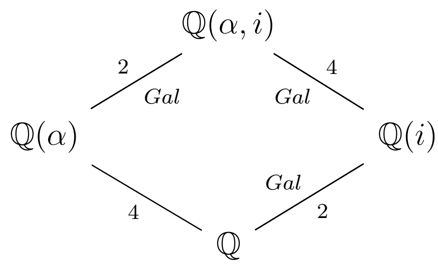
(b) By Eisenstein's Criterion for the prime 2 (or 5), $x^3 - 10$ is irreducible over $\mathbb{Q}$. The discriminant is $-4(0)^3 - 27(10)^2 = -2700$ which is not a square in $\mathbb{Q}$, so the Galois group is S_3. □

Proposition 0.13 (Exercise 1f)**.** *Let $f(x) = x^4 - 5$. The Galois group of f is*

1. *D_8 (the dihedral group with 8 elements) over $\mathbb{Q}$.*
2. *$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ over $\mathbb{Q}(\sqrt{5})$.*
3. *$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ over $\mathbb{Q}(\sqrt{-5})$.*
4. *$\mathbb{Z}/4\mathbb{Z}$ over $\mathbb{Q}(i)$.*

Proof. First we compute the Galois group over $\mathbb{Q}$. Note that f is irreducible over $\mathbb{Q}$ by Eisenstein's criterion (at the prime 5). Let α be a real root of f. Then the set of roots is $\{\pm\alpha, \pm i\alpha\}$, and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg f = 4$, so the splitting field of f is $\mathbb{Q}(\alpha, i)$. We know that $\mathbb{Q}(\alpha) \cap \mathbb{Q}(i)$ has degree 1 or 2 over $\mathbb{Q}$, but the degree is not 2 since α is real. Thus $[\mathbb{Q}(\alpha) \cap \mathbb{Q}(i) : \mathbb{Q}] = 1$ so $\mathbb{Q}(\alpha) \cap \mathbb{Q}(i) = \mathbb{Q}$.

Note that $\mathbb{Q}(i)$ is Galois over $\mathbb{Q}$, so by Theorem 1.12 (Lang pg 266), $\mathbb{Q}(\alpha, i)$ is Galois over $\mathbb{Q}(\alpha)$. We also know that $\mathbb{Q}(\alpha, i)$ is Galois over $\mathbb{Q}(i)$, since it is the splitting field of f over $\mathbb{Q}(i)$. Thus we can write the degrees in the following diagram, along with "Gal" for Galois extensions:



Since the Galois group of $\mathbb{Q}(\alpha, i)$ over $\mathbb{Q}(\alpha)$ has order 2, so there exists an automorphism $\tau : \mathbb{Q}(\alpha, i) \to \mathbb{Q}(\alpha, i)$ over $\mathbb{Q}(\alpha)$ mapping i to $-i$. This implies that $\tau^2 = \mathrm{Id}$. Since $\mathrm{Gal}(\mathbb{Q}(\alpha, i)/\mathbb{Q}(i))$ acts transitivly on the roots of f, there exists an automorphism σ over $\mathbb{Q}(i)$ such that $\sigma(\alpha) = i\alpha$. Then

$$\sigma^2(\alpha) = -\alpha \qquad \sigma^3(\alpha) = -i\alpha$$

so $\sigma, \sigma^2, \sigma^3$ are all distinct. Thus $G = \mathrm{Gal}(\mathbb{Q}(\alpha, i)/\mathbb{Q})$ has an element τ of order 2 and an element σ of order 4, so these elements generate G. Further,

$$\begin{aligned} \tau\sigma(\alpha) &= \tau(i\alpha) = -i\alpha & \sigma^3\tau(\alpha) &= \sigma^3(\alpha) = -i\alpha \\ \tau\sigma(i) &= \tau(i) = -i & \sigma^3\tau(i) &= \sigma^3(-i) = -i \end{aligned}$$

so $\tau\sigma = \sigma^3\tau$. Thus

$$G = \langle\ \sigma, \tau \mid \tau\sigma\tau^{-1} = \sigma^3\ \rangle$$

which is precisely the standard presentation of the dihedral group with 8 elements, D_8.

Now consider f over $\mathbb{Q}(\sqrt{5}) = \mathbb{Q}(\alpha^2)$. Let $G = \mathrm{Gal}(\mathbb{Q}(\alpha, i)/\mathbb{Q}(\alpha^2))$. We know that G has order 4 using the tower rule, since $\mathbb{Q}(\alpha^2)$ has degree 2 over $\mathbb{Q}$. An automorphism of $\mathbb{Q}(\alpha, i)$ over $\mathbb{Q}(\alpha^2)$ must permute the set of roots and fix α^2. So if $\sigma \in G$, then

$$\sigma(\alpha^2) = \sigma(\alpha)^2 = \alpha^2 \implies \sigma(\alpha) = \pm\alpha$$

Two such automorphisms are $\sigma = (\alpha\ \ {-\alpha})$ and $\tau = (\alpha\ \ {-\alpha})(i\alpha\ \ {-i\alpha})$. We can see easily that τ, σ both square to the identity. Thus G is a group of order four with two elements of order 2, so $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Now consider f over $\mathbb{Q}(\sqrt{-5}) = \mathbb{Q}(i\alpha^2)$, and let G be the Galois group. $|G| = 4$ using the tower law. Elements of G must permute $\{\pm\alpha, \pm i\alpha\}$, and fix $i\alpha^2$. Two such permutations are $(\alpha\ {-\alpha})(i\alpha\ {-i\alpha})$ and $(\alpha\ i\alpha)(-\alpha\ {-i\alpha})$ which both square to zero, so G has two elements of order 2, so it must be $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Now consider f over $\mathbb{Q}(i)$. Once again, the Galois group has order 4, and the automorphism τ of $\mathbb{Q}(\alpha, i)$ over $\mathbb{Q}(i)$ defined by the cycle $(\alpha\ i\alpha\ \ {-\alpha}\ \ {-i\alpha})$ is of order 4. Thus G is cyclic, so $G \cong \mathbb{Z}/4\mathbb{Z}$. □

Proposition 0.14 (Exercise 1g)**.** *Let $f(x) = x^4 - a$ where $a \in \mathbb{Z}$ and $a \neq 0$, $a \neq \pm 1$, and a is square free. Then the Galois group of f over $\mathbb{Q}$ is D_8.*

Proof. Let α be a root of f in some splitting field. Then we can factor f as

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

Thus the splitting field of f is $\mathbb{Q}(i,\alpha)$. let $G = \text{Gal}(\mathbb{Q}(i,\alpha)/\mathbb{Q})$. $\mathbb{Q}(\alpha,i)/\mathbb{Q}(\alpha)$ is Galois because it is degree 2, so there exists $\tau : \mathbb{Q}(\alpha,i) \to \mathbb{Q}(\alpha,i)$ fixing α and taking i to $-i$. Since $\mathbb{Q}(\alpha,i)$ is the splitting field of f over $\mathbb{Q}(i)$, this extension is also Galois, so there exists $\sigma : \mathbb{Q}(\alpha,i) \to \mathbb{Q}(\alpha,i)$ fixing i and mapping α to $i\alpha$. Then $\sigma, \sigma^2, \sigma^3, \sigma^4$ are all distinct, and live in a group of order 4, so σ has order 4. Since $\tau \notin \langle\sigma\rangle$, G is generated by τ,σ. As always (see 1n), $\tau\sigma\tau^{-1} = \sigma^3$, so $G \cong D_8$. □

Proposition 0.15 (Exercise 1h)**.** *Let $a \in \mathbb{Z}$ be square free and ≥ 2. Then the Galois group of $x^3 - a$ over $\mathbb{Q}$ is S_3.*

Proof. Since a is square free, it is not a cube, so $x^3 - a$ has no roots in $\mathbb{Q}$, so it is irreducible. The discriminant is $-27a^2$, which is not a square in $\mathbb{Q}$, so the Galois group is S_3. □

Proposition 0.16 (Exercise 1i)**.** *Let $f(x) = x^4 + 2$. The Galois group of f over $\mathbb{Q}$ is D_8. The Galois group of f over $\mathbb{Q}(i)$ is $\mathbb{Z}/4\mathbb{Z}$.*

Proof. We can factor f linearly as

$$x^4 + 2 = (x^2 - i\sqrt{2})(x^2 + i\sqrt{2}) = (x-\alpha)(x+\alpha)(x-i\alpha)(x+i\alpha)$$

where

$$\alpha = \frac{\sqrt{2}}{2}(1+i)\sqrt[4]{2} = \frac{(\sqrt[4]{2})^3(1+i)}{2}$$

Thus the splitting field of f over $\mathbb{Q}$ is $\mathbb{Q}(\alpha,i)$. $\mathbb{Q}(\alpha,i)$ is Galois over $\mathbb{Q}(\alpha)$ because it is degree 2, so there exists an automorphism τ of $\mathbb{Q}(\alpha,i)$ over $\mathbb{Q}(\alpha)$ mapping i to $-i$. Since $\mathbb{Q}(\alpha,i)$ is Galois over $\mathbb{Q}(i)$ (because it is the splitting field of f over $\mathbb{Q}(i)$), there exists an automorphism σ of $\mathbb{Q}(\alpha,i)$ over $\mathbb{Q}(i)$ such that $\sigma(\alpha) = i\alpha$. Then $\sigma, \sigma^2, \sigma^3, \sigma^4$ are all distinct, and σ lives inside a group of order 4, so σ has order 4. Note that $\tau \neq \sigma^k$ for any k, so the Galois group G of $\mathbb{Q}(\alpha,i)$ over $\mathbb{Q}$ is generated by σ,τ. We have the relation $\tau\sigma\tau^{-1} = \sigma^3$ (see 1n for same reasoning), so $G \cong D_8$.

Over $\mathbb{Q}(i)$, the Galois group of $\mathbb{Q}(\alpha,i)$ still is generated by σ, so the Galois group is cyclic of order 4. □

Lemma 0.17 (for Exericse 1jk)**.** *Let $p_1,\ldots,p_n$ be primes. For each i, let $K_i = \mathbb{Q}(\sqrt{p_i})$ be the splitting field of $x^2 - p_i$ over $\mathbb{Q}$. Then*

$$K_n \cap (K_1 \ldots K_{n-1}) = \mathbb{Q}$$

Proof. Suppose the intersection is not empty. Then $\sqrt{p_n}$ lies in $K_1 \ldots K_{n-1}$, so it can be written as a multivariate polynomial in the $\sqrt{p_j}$,

$$\sqrt{p_n} = \sum_i \left(a_i \prod_j \sqrt{p_j} \right)$$

where $a_i \in \mathbb{Q}$. Taking the square of both sides, we see that p_n can be written as

$$p_n = \left(\sum_i \left(a_i \prod_j \sqrt{p_j} \right) \right)^2$$

Thus the RHS must be an integer. This implies that all of the $\sqrt{p_j}$ terms are zero, so

$$\sqrt{p_n} = \sum_i a_i$$

But now the RHS is rational, but this is a contradiction, since the square root of a prime is never rational. $\square$

Proposition 0.18 (Exercise 1jk)**.** *Let $p_1, \dots p_n$ be distinct primes in $\mathbb{N}$. Then the Galois group of*

$$f(x) = (x^2 - p_1) \dots (x^2 - p_n)$$

over $\mathbb{Q}$ is

$$\prod_{i=1}^{n} \mathbb{Z}/2\mathbb{Z}$$

(this is 1k). As a consequence, the Galois group of $(x^2-2)(x^2-3)(x^2-5)(x^2-7)$ over $\mathbb{Q}$ is $\prod_{i=1}^{4} \mathbb{Z}/2\mathbb{Z}$ (this is 1j).

Proof. Let K_i be the splitting field of $x^2 - p_i$. Then the splitting field of f is the compositum $K_1 \dots K_n$ in $\overline{\mathbb{Q}}$. The Galois group of $K_i/\mathbb{Q}$ is $\mathbb{Z}/2\mathbb{Z}$ since it is a quadratic. By the previous lemma

$$K_{i+1} \cap (K_1 \dots K_i) = \mathbb{Q}$$

for each $i = 1, \dots, n-1$. Then applying Corollary 1.1t (Lang pg 267), the Galois group of the compositum $K_1 \dots K_n$ is the product of the Galois groups $K_1, \dots, K_n$.

$$\text{Gal}(f) \cong \prod_{i=1}^{n} \mathbb{Z}/2\mathbb{Z}$$

To get the Galois group of $(x^2-2)(x^2-3)(x^2-5)(x^2-7)$, just take $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7$. $\square$

Proposition 0.19 (Exercise 1ℓ)**.** *The Galois group of $f(x) = (x^3-2)(x^3-3)(x^2-2)$ over $\mathbb{Q}(\sqrt{-3})$ is $A_3 \times A_3 \times \mathbb{Z}/2\mathbb{Z}$. (Another way to write this group is $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2$.)*

Proof. Note that each of x^3-2, x^3-3, and x^2-2 are irreducible over $\mathbb{Q}(\sqrt{-3})$, since they have no roots. The Galois group of x^2-2 is $\mathbb{Z}/2\mathbb{Z}$, as for all quadratics. The Galois group of x^3-2 is A_3 since the discriminant is $-108 = (6\sqrt{-3})^2$. The Galois group of x^3-3 is A_3, since the discriminant is $-3^5 = (9\sqrt{-3})^2$, which is a square in $\mathbb{Q}(\sqrt{-3})$.

The Galois group of f embeds into the product of these groups, by Corollary 1.15. By the same kind of logic as in Lemma 0.17, the intersection of the splitting fields of these polynomials over $\mathbb{Q}(\sqrt{-3})$ is just $\mathbb{Q}(\sqrt{-3})$, so this embedding is an isomorphism. $\square$

Proposition 0.20 (Exercise 1m)**.** *Let t be transcendental over $\mathbb{C}$ and $n \in \mathbb{N}$, and let $f(x) = x^n - t$. Then the Galois group of f over $\mathbb{C}(t)$ is $\mathbb{Z}/n\mathbb{Z}$.*

Proof. Let ω be a root of f in some splitting field, and let β be a primitive nth root of unity. Then

$$\{\omega, \beta\omega, \ldots, \beta^{n-1}\omega\}$$

are all roots of f, since $(\beta^k\omega)^n = \beta^{nk}\omega^n = \omega^n = t$. Thus these are all the roots of f, since f can't have more than n roots. Thus the splitting field of f is $\mathbb{C}(\omega)$. Elements of $G = \mathrm{Gal}(\mathbb{C}(\omega)/\mathbb{C}(t))$ permute the roots and fix $\mathbb{C}$. In particular, they fix β, so an element of G is determined by how it acts on ω, so

$$G = \{\sigma_i : 0 \le i \le n-1\}$$

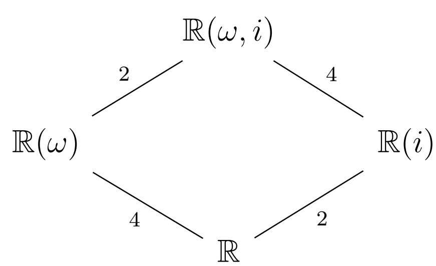
where $\sigma_i(\omega) = \beta^i\omega$. We can see that σ_1 generates G, so $G \cong \mathbb{Z}/n\mathbb{Z}$. □

Proposition 0.21 (Exercise 1n)**.** *Let t be transcendental over $\mathbb{C}$. Let $f(x) = x^4 - t$. The Galois group of f over $\mathbb{R}$ is D_8.*

Proof. Let ω be a root of f is some splitting field. Then we can factor f as

$$x^4 - t = (x^2 - \omega^2)(x^2 + \omega^2) = (x-\omega)(x+\omega)(x-i\omega)(x+i\omega)$$

Thus $\mathbb{R}(\omega, i)$ is the splitting field for f. Note that $[\mathbb{R}(i) : \mathbb{R}] = 2$ since $\deg \mathrm{Irr}(i, \mathbb{R}) = \deg(x^2 + 1) = 2$. Also note that $\mathbb{R}(\omega, i)$ is the splitting field of f over $\mathbb{R}(i)$, and $[\mathbb{R}(\omega, i) : \mathbb{R}(i)] = 4$ since $\deg(\mathrm{Irr}(\omega, \mathbb{R}(i)) = \deg f = 4$, so $\mathbb{R}(\omega, i)/\mathbb{R}(i)$ is Galois. So we have the following diagram of field extensions, with degrees.



Since $\mathbb{R}(\omega, i)/\mathbb{R}(\omega)$ is degree 2, it is Galois, so there exists an automorphism τ over $\mathbb{R}(\omega)$ such that $\tau(i) = -i$, and $\tau^2 = \mathrm{Id}$. Since $\mathbb{R}(\omega, i)/\mathbb{R}(i)$ is Galois, there exists an automorphism σ of $\mathbb{R}(\omega, i)$ over $\mathbb{R}(i)$ sending ω to $i\omega$. Then $\sigma, \sigma^2, \sigma^3, \sigma^4$ are all distinct, so $|\sigma| = 4$. Let $G = \mathrm{Gal}(\mathbb{R}(\omega, i)/\mathbb{R})$. Note that $\tau \notin \langle \sigma \rangle$, and that $|G| = 8$. Thus we have τ, σ in G of order 2 and 4 generating disjoint subgroups, so $G = \langle \tau, \sigma \rangle$. We can check that $\tau\sigma\tau^{-1} = \sigma^3$, so $G \cong D_8$. We just have to check that they agree on ω and i.

$$\begin{aligned} \tau\sigma\tau^{-1}(i) &= \tau\sigma(-i) = \tau(-i) = i & \sigma^3(i) &= i \\ \tau\sigma\tau^{-1}(\omega) &= \tau\sigma(\omega) = \tau(i\omega) = -i\omega & \sigma^3(\omega) &= i^3\omega = -i\omega \end{aligned}$$

□

Proposition 0.22 (Exercise 2)**.** *For each of the following polynomials, we compute the Galois group over $\mathbb{Q}$.*

a) $x^3 + x + 1$, $G = S_3$

b) $x^3 - x + 1$, $G = S_3$

c) $x^3 + 2x + 1$, $G = S_3$

d) $x^3 - 2x + 1$, $G = \mathbb{Z}/2\mathbb{Z}$

e) $x^3 - x - 1$, $G = S_3$

f) $x^3 - 12x + 8$, $G = A_3$

g) $x^3 + x^2 - 2x - 1$, $G = A_3$

Proof. (a) By the integral root test, the only possible rational roots are ± 1, and we check that these are not roots, so $x^3 + x + 1$ is irreducible. The discriminant is -31, which is not a square, so the Galois group is S_3.

(b) By the integral root test, the only possible rational roots are ± 1, which we can check are not roots, so $x^3 - x + 1$ is irreducible. The discriminant is -23, which is not a square, so the Galois group is S_3.

(c) By the integral root test, the only possible rational roots are ± 1, which are not roots, so $x^3 + 2x + 1$ is irreducible over $\mathbb{Q}$. The discriminant is -59, which is not a square, so the Galois group is S_3.

(d) We can factor $x^3 - 2x + 1$ as $(x-1)(x^2 + x - 1)$, so the splitting field of $x^3 - 2x + 1$ over $\mathbb{Q}$ is the splitting field of $x^2 + x - 1$. This is a quadratic extension, so the Galois group is $\mathbb{Z}/2\mathbb{Z}$.

(e) By the integral root test, the only possible rational roots are ± 1, which are not roots, so $x^3 - x - 1$ is irreducible. The discriminant is -23, which is not a square, so the Galois group is S_3.

(f) By the integral root test, the only possible rational roots are $\pm 1, \pm 2, \pm 4, \pm 8$, which we check tediously are not roots of $x^3 - 12x + 8$, so it is irreducible over $\mathbb{Q}$. The discriminant is 5184, which is a square ($5184 = 72^2$), so the Galois group is A_3.

(g) By substituting $x = y + \frac{1}{3}$, we get

$$x^3 + x^2 - 2x - 1 = y^3 - \frac{7}{3}y - \frac{7}{27}$$

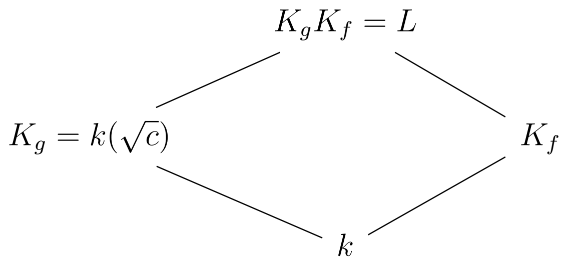
So the Galois group of the polynomial in x is the same as the Galois group of the polynomial in y. By the integral root test, it is irreducible over $\mathbb{Q}$. The discriminant is 49, which is a square, so the Galois group is A_3. $\square$

Proposition 0.23 (Exercise 5a)**.** *Let k be a field of characteristic $\neq 2, 3$. Let $f \in k[x]$ be an irreducible cubic with discriminant $D \in k$ and let $g = x^2 - c \in k[x]$ be irreducible. Suppose that*

$$[k(\sqrt{D}) : k] = 2 \qquad k(\sqrt{D}) \neq k(\sqrt{c})$$

Let L be the splitting field of fg. Then $[L : k] = 12$.

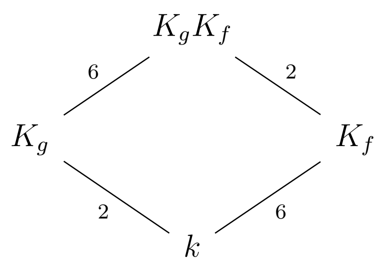
Proof. Let K_f be the splitting field of f and let $K_g = k(\sqrt{c})$ be the splitting field of g. Then $L = K_g K_f$ (in some algebraic closure), and we can draw the following diagram of field extensions:



Since $\operatorname{char} k \neq 2, 3$, f and g can't have repeated roots, so all the above extensions are separable. The extensions $K_g/k, K_f/k$, and K_gK_f/k are all normal, as they are splitting fields. Then by Theorem 3.4 (Lang pg 238), K_gK_f/K_g and K_gK_f/K_f are normal. Thus all the extensions in the diagram are Galois.

Because g is irreducible, $\sqrt{c} \notin k$, so $[k(\sqrt{c}) : k] = 2$. Note that $k(\sqrt{D})$ is the splitting field of $x^2 - D \in k[x]$, since $[k(\sqrt{D}) : k] = 2$, this implies that D is not a square in k. Thus by the theorem on page 270 of Lang, the Galois group of K_f/k is S_3. Since K_f is a splitting field of a cubic, by Exercise 8 (last homework), $[K_f : k]$ divides 6. But the size of the Galois group cannot exceed the degree of the extension, so $[K_f : k] = 6$.

We claim that $K_g \cap K_f = k$. Since $k(\sqrt{c}) \neq k(\sqrt{D})$, $\sqrt{c}$ cannot be a root of f, so $\sqrt{c} \notin K_f$. Thus $K_f \cap K_g = k$. Then applying Theorem 1.12 (Lang pg 266), we get that $[K_gK_f : K_f] = 2$ and $[K_gK_f : K_g] = 6$.



Then by the multiplicative tower law, $[K_gK_f : k] = 12$. □

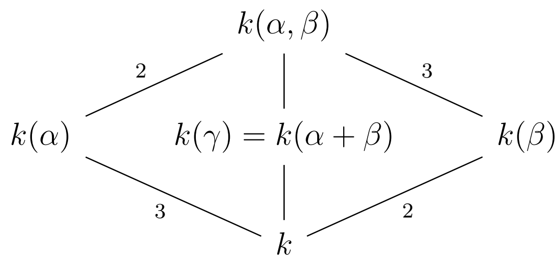
Proposition 0.24 (Exercise 5b)**.** *Let k be a field of characteristic $\neq 2, 3$. Let $f \in k[x]$ be an irreducible cubic with discriminant D and a root α (in an algebraic closure). Let $g = x^2 - c \in k[x]$ be irreducible with a root β. Suppose that*

$$[k(\sqrt{D}) : k] = 2 \qquad k(\sqrt{D}) \neq k(\sqrt{c})$$

Let $\gamma = \alpha + \beta$. Then

$$[k(\gamma) : k] = 6$$

Proof. We have $k(\gamma) \subset k(\alpha, \beta)$, and $[k(\alpha) : k] = \deg f = 3$ and $[k(\beta) : k] = \deg g = 2$. Then using Corollary 1.13 and the tower law and the fact that 2 and 3 are coprime, we can conclude that $[k(\alpha, \beta) : k(\alpha)] = 2$ and $[k(\alpha, \beta) : k(\beta)] = 3$, so $[k(\alpha, \beta) : k] = 3$.



Thus $[k(\gamma) : k] \leq 6$. Since $k(\alpha, \beta)/k$ is a separable extension with degree 6, there are 6 distinct embeddings of $k(\alpha, \beta)$ over k into $\overline{k}$ (algebraic closure of k). Let $\alpha_1, \alpha_2, \alpha_3 \in \overline{k}$ be the roots of f. Then the 6 embeddings of $k(\alpha, \beta)$ over k into $\overline{k}$ are determined by sending α to some α_i and sending β to $\pm\beta$. So we have $\sigma_i^{\pm}$ where $\sigma_i^{\pm}(\alpha) = \alpha_i$ and $\sigma_i^{\pm}(\beta) = \pm\beta$.

$$
\begin{aligned}
\sigma_1^+(\alpha) &= \alpha_1 & \sigma_1^+(\beta) &= \beta \\
\sigma_2^+(\alpha) &= \alpha_2 & \sigma_2^+(\beta) &= \beta \\
\sigma_3^+(\alpha) &= \alpha_3 & \sigma_3^+(\beta) &= \beta \\
\sigma_1^-(\alpha) &= \alpha_1 & \sigma_1^-(\beta) &= -\beta \\
\sigma_2^-(\alpha) &= \alpha_2 & \sigma_2^-(\beta) &= -\beta \\
\sigma_3^-(\alpha) &= \alpha_3 & \sigma_3^-(\beta) &= -\beta
\end{aligned}
$$

Then we restrict each $\sigma_i^{\pm}$ to an embedding of $k(\gamma)$ over k into $\overline{k}$. Restricted to $k(\gamma)$, they are determined by $\sigma_i^{\pm}(\gamma) = \sigma_i^{\pm}(\alpha) + \sigma_i^{\pm}(\beta) = \alpha_i \pm \beta$.

We claim that the six elements $\alpha_i \pm \beta$ for $i = 1, 2, 3$ are all distinct. Since each α_i is distinct, $\alpha_1 + \beta, \alpha_2 + \beta, \alpha_3 + \beta$ are distinct, and likewise for $\alpha_i - \beta$. Suppose $\alpha_i + \beta = \alpha_j - \beta$ for some $i \neq j$. This implies $\alpha_j - \alpha_i = 2\beta$, which would imply that the splitting field of f contains $k(\beta)$. But by hypothesis, D is not a square in k so the Galois group of f over k is S_3, which has a unique index two subgroup. Using the Galois correspondence, there is a unique degree 2 subextension between f and its splitting field, which is $k(\sqrt{D})$, which is not $k(\beta)$ by hypothesis. Thus the splitting field of f cannot contain $k(\beta)$, so we can conclude that all the $\alpha_i \pm \beta$ are distinct.

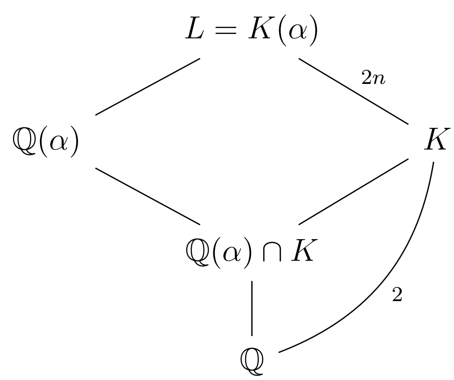
Thus there are six distinct embeddings of $k(\gamma)$ over k into $\overline{k}$, so $[k(\gamma) : k] \geq [k(\gamma) : k]_s = 6$. Combining this with the opposite inequality, we get $[k(\gamma) : k] = 6$. □

Proposition 0.25 (Exercise 7a)**.** *Let $K = \mathbb{Q}(\sqrt{a})$ where $a \in \mathbb{Z}, a < 0$. Then K cannot be embedded in a cyclic extension whose degree over $\mathbb{Q}$ is divisible by 4.*

Proof. Suppose that there exists a field L such that $\mathbb{Q} \subset K \subset L$ such that $L/\mathbb{Q}$ is cyclic of degree divisible by 4. We may assume all these fields lie in an algebraic closure of $\mathbb{Q}$ which is contained in $\mathbb{C}$. Let $G = \mathrm{Gal}(L/\mathbb{Q})$, so G is cyclic of order $4n$. Let σ be a generator.

Since $L/\mathbb{Q}$ is Galois, it is separable, so L/K is separable. Then by the Primitive Element Theorem there exists $\alpha \in L$ such that $L = K(\alpha) = \mathbb{Q}(\sqrt{a}, \alpha)$.

Note that $K = \mathbb{Q}(\sqrt{a})$ is the splitting field of $x^2 - a$ over $\mathbb{Q}$, which is irreducible as it has no roots in $\mathbb{Q}$, so $[K : \mathbb{Q}] = 2$. Then by the Galois correspondence, $\mathrm{Gal}(L/K)$ is an index-2 subgroup of $\mathrm{Gal}(L/\mathbb{Q}) = \langle\sigma\rangle$. The only index-2 subgroup is $\langle\sigma^2\rangle$, so $\mathrm{Gal}(L/K) = \langle\sigma^2\rangle$. (A finite cyclic group of order m has a unique subgroup of order d for each divisor d of m.) Hence $\sigma^2, \sigma^4, \ldots, \sigma^{4n}$ are all automorphisms of L over K. In particular, σ^{2n} fixes K.

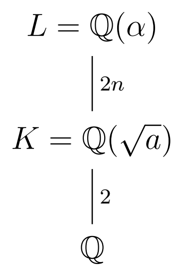


By the tower law,

$$[K : \mathbb{Q}(\alpha) \cap K][\mathbb{Q}(\alpha) \cap K : \mathbb{Q}] = 2$$

so one of them must be 1 and the other must be 2. We consider these in two separate cases. We reach a contradiction in both cases.

Case 1: First suppose $[\mathbb{Q}(\alpha) \cap K : \mathbb{Q}] = 2$. Then $\mathbb{Q}(\alpha) \cap K = K$, which implies $K \subset \mathbb{Q}(\alpha)$, which implies $L = \mathbb{Q}(\alpha)$.

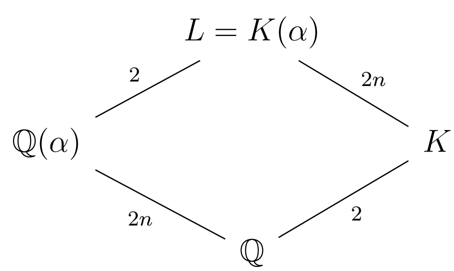


Let $\tau : \mathbb{C} \to \mathbb{C}$ be complex conjugation ($x + iy \mapsto x - iy$). It restricts to an automorphism of L over $\mathbb{Q}$, so $\tau \in G = \mathrm{Gal}(L/\mathbb{Q})$. Since $a < 0$, we can think of $\sqrt{a}$ as $i\sqrt{-a}$, and then

$$\tau(\sqrt{a}) = \tau(i\sqrt{-a}) = -i\sqrt{-a} = -\sqrt{a}$$

Thus τ does not fix K, so τ is not the identity. Since $\tau^2 = \mathrm{Id}$, it has order 2. But there is a unique element of order 2 in $G = \langle \sigma \rangle$, namely σ^{2n}. As previously shown, σ^{2n} is an automorphism over K, so we reach a contradiction. This rules out Case 1 as a possibility.

Case 2: Now suppose $[\mathbb{Q}(\alpha) \cap K : \mathbb{Q}] = 1$, which immediately implies $\mathbb{Q}(\alpha) \cap K = \mathbb{Q}$. Applying Theorem 1.12 (Lang pg 266), we can fill in the degrees on the following diagram.



Then by the Galois correspondence, $\mathrm{Gal}(L(\mathbb{Q}(\alpha))$ is a subgroup of $G = \mathrm{Gal}(L/\mathbb{Q})$ of index 2, so it must be $\langle \sigma^2 \rangle$. In particular, $\sigma^{2n} \in \mathrm{Gal}(L/\mathbb{Q}(\alpha))$, so σ^{2n} fixes $\mathbb{Q}(\alpha)$. Since σ^{2n} also fixes K, this implies that σ^{2n} fixes all of L. Thus $\sigma^{2n} = \mathrm{Id}_L$, but this is a contradiction since σ has order $4n$.

We reached a contradiction in both Case 1 and Case 2, so we conclude that no such field extension L exists. $\square$

Lemma 0.26 (for Exercise 7c)**.** *Let k be a field of characteristic $\neq 2$, and let $f(x) = x^4 + ax^2 + b \in k[x]$ be irreducible with roots $\pm\alpha, \pm\beta$ in an algebraic closure. Let G be the Galois group of f. Then*

1. *If b is a square in k, then $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*
2. *If b is not a square in k and $b(a^2 - 4b)$ is a square in k, then $G \cong \mathbb{Z}/4\mathbb{Z}$.*

Proof. We know that G is a transitive subgroup on the symmetric group on the set $\{\pm\alpha, \pm\beta\}$. Any $\sigma \in G$ must also satisfy $\sigma(-\alpha) = -\sigma(\alpha)$ and $\sigma(-\beta) = -\sigma(\beta)$ since it must fix k. The subgroup of S_4 on these letters that satisfies these two relations is (using cycle notation)

$$\begin{aligned} H = \{\mathrm{id},&(\alpha\ -\alpha), (\beta\ -\beta), (\alpha\ \beta)(-\alpha\ -\beta), (\alpha\ -\beta)(-\alpha\ \beta), \\ &(\alpha\ \beta\ -\alpha\ -\beta), (\alpha\ -\beta\ -\alpha\ \beta), (\alpha\ -\alpha)(\beta\ -\beta)\} \end{aligned}$$

This H has three transitive subgroups: all of H, and

$$\begin{aligned} H_1 &= \{\mathrm{id}(\alpha\ -\alpha)(\beta\ -\beta), (\alpha\ \beta)(-\alpha\ -\beta), (\alpha\ -\beta)(-\alpha\ \beta)\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\ H_2 &= \{\mathrm{id}, (\alpha\ -\alpha)(\beta\ -\beta), (\alpha\ \beta\ -\alpha\ -\beta), (\alpha\ -\beta\ -\alpha\ \beta)\} \cong \mathbb{Z}/4\mathbb{Z} \end{aligned}$$

Note that f factors as

$$f(x) = x^4 + ax^2 + b = (x^2 - \alpha^2)(x^2 - \beta^2) \implies b = (\alpha\beta)^2 \text{ and } a = -\alpha^2 - \beta^2$$

Now we can prove (1). If b is a square in k, since $b = (\alpha\beta)^2$, we get $\alpha\beta \in k$. Then applying $\tau_1 = (\alpha\ -\beta\ -\alpha\ \beta) \in H_2$ to $\alpha\beta$,

$$\tau_1(\alpha\beta) = \tau_1(\alpha)\tau_1(\beta) = -\beta\alpha$$

thus τ_1 does not fix $\alpha\beta$, which is an element of k, so $\tau_1 \notin G$. Thus in this case, $G = H_1 \cong \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$.

Now we prove (2). Suppose $b(a^2 - 4b)$ is a square in k. We can rewrite it as

$$\begin{aligned} b(a^2 - 4b) &= \alpha^2\beta^2((-\alpha^2 - \beta)^2 - 4\alpha^2\beta^2) = \alpha^2\beta^2(\alpha^4 + 2\alpha^2\beta^2 + \beta^4 - 4\alpha^2\beta^2) \\ &= \alpha^2\beta^2(\alpha^4 - 2\alpha^2\beta^2 + \beta^4) = \alpha^2\beta^2(\alpha^2 - \beta^2)^2 = \Big(\alpha\beta(\alpha^2 - \beta^2)\Big)^2 \end{aligned}$$

so if $b(a^2 - 4b)$ is a square in k, then $\alpha\beta(\alpha^2 - \beta^2) \in k$. Then applying $\tau_2 = (\alpha\ \beta)(-\alpha - \beta) \in H_1$ to $\alpha\beta(\alpha^2 - \beta^2)$, we get

$$\tau_2\Big(\alpha\beta(\alpha^2 - \beta^2)\Big) = \tau_2(\alpha)\tau_2(\beta)\Big(\tau_2(\alpha)^2 - \tau_2(\beta)^2\Big) = \beta\alpha\Big(\beta^2 - \alpha^2\Big) = -\alpha\beta(\alpha^2 - \beta^2)$$

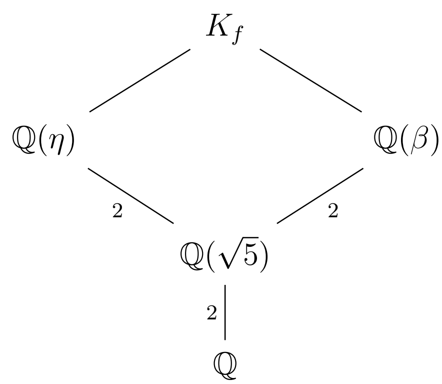
Thus τ_2 does not fix $\alpha\beta(\alpha^2 - \beta^2)$, which lies in k, so $\tau_2 \notin G$. Since $\tau_2 \in H_1$, this implies that $G = H_2 \cong \mathbb{Z}/4\mathbb{Z}$. $\square$

Proposition 0.27 (Exercise 7b)**.** *Let $f(x) = x^4 + 30x^2 + 45$. Let α be a root of f in an algebraic closure of $\mathbb{Q}$. Then $\mathbb{Q}(\alpha)$ is cyclic of degree 4 over $\mathbb{Q}$.*

Proof. Note that f is irreducible by Eisenstien's Criterion with $p = 5$. Let K_f be the splitting field of f in an algebraic closure of $\mathbb{Q}$. The roots of f are $\pm\eta, \pm\beta \in K_f$ where

$$\eta = i\sqrt{15 + 6\sqrt{5}} \qquad \beta = i\sqrt{15 - 6\sqrt{5}}$$

We notice that $\eta^2 = -15 - 6\sqrt{5}$ and $\beta^2 = -15 + 6\sqrt{5}$, so $\mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\eta), \mathbb{Q}(\beta)$. So we have the following diagram,



We know that $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$ since it is the splitting field of $x^2 - 5$. We also know $[\mathbb{Q}(\eta) : \mathbb{Q}(\sqrt{5})] = [\mathbb{Q}(\beta) : \mathbb{Q}(\sqrt{5})] = 2$ since they are the respective splitting fields of

$$x^2 - (-15 - 6\sqrt{5}) \qquad x^2 - (-15 + 5\sqrt{5})$$

over $\mathbb{Q}(\sqrt{5})$. Using the previous lemma, we check that

$$b(a^2 - 4b) = 45(30^2 - 4(45)) = 32400 = 180^2$$

Since this is a square, the Galois group of $K_f/\mathbb{Q}$ is $\mathbb{Z}/4\mathbb{Z}$, so $[K_f : \mathbb{Q}] = 4$. But by the tower law,

$$[K_f : \mathbb{Q}] = [K_f : \mathbb{Q}(\eta)][\mathbb{Q}(\eta) : \mathbb{Q}(\sqrt{5})][\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 4[K_f : \mathbb{Q}(\eta)] \leq 4$$
$$[K_f : \mathbb{Q}] = [K_f : \mathbb{Q}(\beta)][\mathbb{Q}(\beta) : \mathbb{Q}(\sqrt{5})][\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 4[K_f : \mathbb{Q}(\beta)] \leq 4$$

which implies $[K_f : \mathbb{Q}(\beta)] = [K_f : \mathbb{Q}(\eta)] = 1$ which implies $\mathbb{Q}(\eta) = \mathbb{Q}(\beta) = \mathbb{Q}(-\eta) = \mathbb{Q}(-\beta) = K_f$. Since the Galois group of $K_f/\mathbb{Q}$ is $\mathbb{Z}/4\mathbb{Z}$, this says that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is cyclic of degree 4 for any root $(\pm\eta, \pm\beta)$ of f. □

Proposition 0.28 (Exercise 7c)**.** *Let $f(x) = x^4 + 4x^2 + 2$. Then f is irreducible over $\mathbb{Q}$ and the Galois group of f is cyclic.*

Proof. By Eisenstein's Criterion at the prime 2, f is irreducible. The constant coefficient is not one, and

$$b(a^2 - 4b) = 2(4^2 - 4(2)) = 2(16 - 8) = 16 = 4^2$$

so by the previous lemma, the Galois group is $\mathbb{Z}/4\mathbb{Z}$. □

For convenience, for Exercise 13, we list some low degree monic irreducible polynomials mod 2 and 3.

$\mathbb{F}_2[x]$

Degree	Irreducibles	Reducibles
0	1	none
1	$x, x+1$	none
2	x^2+x+1	x^2+1
3	x^3+x+1, x^3+x^2+1	x^3+1, x^3+x^2+x+1
4	$x^4+x+1, x^4+x^3+1, x^4+x^3+x^2+x+1$	(everything else of degree 4)

$\mathbb{F}_3[x]$

Degree	Irreducibles	Reducibles
0	$1, 2$	none
1	$x, x+1, x+2$	none
2	$x^2+1, \dots$	$x^2+2, \dots$
3	$x^3+2x+1, \dots$	$\dots$

I give a statement of the following theorem because Lang doesn't label it and doesn't state it in the way I want to frequently apply it, so that I can easily refer to it.

Theorem 0.29 (Dedekind)**.** *Let $f \in \mathbb{Z}[x]$ be monic, irreducible, and separable. Let $p \in \mathbb{Z}$ be prime and let $f_p \in \mathbb{F}_p[x]$ be the reduction of the coefficients of f mod p. Let K be the splitting field of f. If f_p factors as a product*

$$f_p(x) = \prod_{i=1}^{r} q_i(x)$$

where each q_i is irredubile (in $\mathbb{F}_p[x]$) with $d_i = \deg q_i$, then $\mathrm{Gal}(K/\mathbb{Q})$ contains an element of cycle type $(d_1, \dots, d_r)$.

In particular, if $f_p(x)$ is irreducible in $\mathbb{F}_p[x]$, then the Galois group of f contains a cycle of length $\deg f_p = \deg f$.

Lemma 0.30 (for Exercise 13)**.** *A subgroup of S_4 containing a 4-cycle and a 3-cycle is S_4.*

Proof. The 3-cycle and 4-cycle together generate a subgroup of size at least 12, so the subgroup must be either S_4 or A_4. But A_4 has no elements of order 4, so it must be S_4. □

Proposition 0.31 (Exercise 13a)**.** *Let $f(x) = x^4 + 2x^2 + x + 3$. The Galois group of f over $\mathbb{Q}$ is S_4.*

Proof. First note that f is separable (using a computer to check that it has 4 distinct roots in $\mathbb{C}$). Let G be the Galois group of f. Reducing f mod 2 we get $x^4 + x + 1$, which is irreducible (see table). Then by Theorem 0.29 above, G contains a 4-cycle. Reducing f mod 3, we get

$$x^4 + 2x^2 + x = x(x^3 + 2x + 1)$$

This cubic is irreducible over $\mathbb{F}_3$ because it has no roots (just check $0, 1, 2$). Then by Theorem 0.29, G contains a 3-cycle. We know that G is (isomorphic to) a subgroup of S_4, so by Lemma 0.30, $G \cong S_4$. □

Proposition 0.32 (Exercise 13b)**.** *The Galois group of* $f(x) = x^4 + 3x^3 - 3x - 2$ *over* $\mathbb{Q}$ *is* S_4*.*

Proof. First note that f is separable (use a computer to check that f has 4 distinct roots in $\mathbb{C}$). Let G be the Galois group of f. We know that G embeds in S_4, since f has degree 4. Reducing f mod 2 we get $x^4 + x^3 + x = x(x^3 + x^2 + 1)$, which has an irreducible cubic (see table). Thus G contains a 3-cycle. Reducing f mod 5 we get $x^4 + 3x^3 + 2x + 3$, which is irreducible (checked via computer). Thus G contains a 4-cycle. Since G has a 4-cycle and a 3-cycle, it is S_4. □