By *Vincent Dumoncel*
Autumn 2021

Galois theory: exercises solutions

1 Roots and irreducible polynomials

Exercise 1. Consider $f(X) = X^4 + 3X^2 + 3X + 9 \in \mathbb{Q}[X]$.
(i) From Proposition 1.2, the only possible roots of f in $\mathbb{Q}$ are ± 1, $\pm\frac{1}{3}$ and $\pm\frac{1}{9}$. One directly checks that $f(\pm 1) \neq 0$, $f(\pm\frac{1}{3}) \neq 0$ and $f(\pm\frac{1}{9}) \neq 0$, so f has no roots in $\mathbb{Q}$.
(ii) We have $\overline{f}(X) = X^4 + X^2 + X + 1 = (X-1)(X^3 + X^2 + 1)$ in $\mathbb{F}_2[X]$.
(iii) If f is not irreducible in $\mathbb{Q}[X]$, it factors as the product of two degree 2 irreducible polynomials, since it has no roots in $\mathbb{Q}$. But then this implies that $\overline{f}$ also factors as the product of two degree 2 irreducible polynomials in $\mathbb{F}_2[X]$, which is excluded by point (ii). Thus f is irreducible in $\mathbb{Q}[X]$.

Exercise 3. (i) Apply Eisenstein's criterion with $p = 2$.
(ii) Likewise, apply Eisenstein with p any prime divisor of a.

Exercise 7. In $\mathbb{F}_2[X]$, there is only one irreducible degree 2 polynomial, namely $X^2 + X + 1$. Irreducibles of degree 3 and 4 are

$$\begin{aligned}&\text{degree } 3 : X^3 + X + 1,\ X^3 + X^2 + 1\\ &\text{degree } 4 : X^4 + X + 1,\ X^4 + X^3 + 1,\ X^4 + X^3 + X^2 + X + 1.\end{aligned}$$

In $\mathbb{F}_3[X]$, we get

$$\begin{aligned}&\text{degree } 2 : X^2 + 1,\ X^2 + X + 2,\ X^2 + 2X + 2\\ &\text{degree } 3 : X^3 + 2X + 1,\ X^3 + 2X + 2,\ X^3 + X^2 + 2,\ X^3 + X^2 + X + 2,\\ &\qquad X^3 + X^2 + 2X + 1,\ X^3 + 2X^2 + X + 1,\ X^3 + 2X^2 + 2X + 2,\ X^3 + 2X^2 + 1.\end{aligned}$$

Finally, in $\mathbb{F}_5[X]$ we get ten irreducible polynomials of degree 2, which are

$$\begin{aligned}&X^2 + 2,\ X^2 + 3,\ X^2 + X + 1,\ X^2 + X + 2,\ X^2 + 2X + 3,\\ &X^2 + 2X + 4,\ X^2 + 3X + 3,\ X^2 + 3X + 4,\ X^2 + 4X + 1,\ X^2 + 4X + 2.\end{aligned}$$

Exercise 12. First, suppose that f and g are relatively prime in $K[X]$. Then Bezout's theorem implies there exist $u, v \in K[X]$ so that

$$f(X)u(X) + g(X)v(X) = 1$$

in $K[X]$. A fortiori, if L is a field containing K, this relation also holds in $L[X]$, and if f and g have a common root α in L, replacing X by α in the above equality provides a contradiction.
Conversely, if f and g are not relatively prime, they have a non-trivial common divisor $d(X)$ in $K[X]$. Considering an irreducible factor $h(X)$ of $d(X)$, the quotient $K[X]/(h(X))$ is a field containing K in which f and g have a common root, as wanted.

Exercise 13. Let $f(X) = X^3 + X + 1 \in \mathbb{F}_2[X]$.
(i) As $f(0) = f(1) = 1 \neq 0$, f has no roots in $\mathbb{F}_2$, and since it has degree 3, it is therefore irreducible in $\mathbb{F}_2$. The quotient $F = \mathbb{F}_2[X]/(f(X))$ is then a field.

(*ii*) Clearly, $|F| = 8$ and if $\alpha := \overline{X}$, then $\alpha^3 + \alpha + 1 = 0$, *i.e.* $\alpha^3 = -\alpha - 1 = \alpha + 1$. Thus

$$F = \{0, 1, \alpha, \alpha^2, \alpha + 1, \alpha^2 + 1, \alpha^2 + \alpha + 1, \alpha^2 + \alpha\}.$$

(*iii*) We have $\alpha^3 + \alpha = -1 = 1$, so $\alpha(\alpha^2 + 1) = 1$, and $1 + \alpha^2$ is the inverse of α in F.

Exercise 14. Clearly, if $\pi(X)$ divides $h(X)$, then $h(\alpha) = 0$. Conversely, we use exercise 12: if $h(\alpha) = 0$, then h and π have a common root in a field containing K, so they cannot be relatively prime in $K[X]$, which means they have a non-trivial common divisor $d(X)$ in $K[X]$. As $\pi(X)$ is irreducible, we must have $d(X) = \pi(X)$, and $\pi(X)$ divides $h(X)$.

Exercise 15. (*i*) First of all, $f(0) = f(1) = 1 \neq 0$ so f has no roots in $\mathbb{F}_2$. Thus, if it is not irreducible, it factors as the product of two degree 2 irreducible polynomials. The only degree 2 irreducible polynomial in $\mathbb{F}_2[X]$ is $X^2 + X + 1$, and $f(X) \neq (X^2 + X + 1)^2$, so f is irreducible.
(*ii*) As f is irreducible, $F = \mathbb{F}_2[X]/(f(X))$ is a field in which f has a root, namely $\alpha = \overline{X}$. Using Theorem 1.19, with $p = 2$ and $d = 4$, we have that α, α^2, α^4 and α^8 are all roots of f. Also

$$\alpha^4 + \alpha + 1 = 0 \Longrightarrow \alpha^4 = -\alpha - 1 = \alpha + 1$$

and $\alpha^8 = (\alpha^4)^2 = (\alpha + 1)^2 = \alpha^2 + 1$.
(*iii*) Clearly, raising α, α^2 or α^4 to the power 2 produces another root of f. For the last one, we compute

$$(\alpha^8)^2 = (\alpha^2 + 1)^2 = \alpha^4 + 1 = \alpha + 1 + 1 = \alpha$$

so Corollary 1.15 holds in this case.
(*iv*) One has $|F| = 2^4 = 16$ and

$$F = \{0, 1, \alpha, \alpha^2, \alpha^3, 1+\alpha, 1+\alpha^2, 1+\alpha^3, \alpha+\alpha^2, \alpha+\alpha^3, \alpha^2+\alpha^3, 1+\alpha+\alpha^2, 1+\alpha+\alpha^3, 1+\alpha^2+\alpha^3, \alpha+\alpha^2+\alpha^3, 1+\alpha+\alpha^2+\alpha^3\}.$$

Exercise 17. (*i*) Since any polynomial of the form $X - c$, where $c \in \mathbb{F}_p$, is irreducible, we have $N_p(1) = p$.
(*ii*) By Theorem 1.20, we have the factorization

$$X^{p^n} - X = \prod_{d|n} \prod_{\deg(\pi)=d} \pi(X)$$

where $\pi(X)$ is irreducible and monic. Taking degrees of both sides yields

$$p^n = \sum_{d|n} dN_p(d).$$

(*iii*) By Möbius inversion formula, it follows from the previous point that

$$nN_p(n) = \sum_{d|n} \mu(d) p^{n/d}$$

and then $N_p(n) = \dfrac{1}{n} \displaystyle\sum_{d|n} \mu(d) p^{n/d}$.
(*iv*) We directly compute with $n = 12$ and $p = 19$ that $N_{19}(12) = \frac{1}{12}(19^{12} - 19^6 - 19^4 + 19^2) = 184442905990860$.
(*v*) $N_3(3) = \frac{1}{3}(3^3 - 3) = 8$, and we got 8 irreducible monic polynomials in exercise 7.

Exercise 18. It is a direct corollary to the previous exercise.

2 Fields extensions

Exercise 2. (*i*) If L/K has degree $[L : K] = n$, we can choose $a_1, \ldots, a_n$ a $K-$basis of L, and we have $L = K(a_1, \ldots, a_n)$. The converse is not true: for instance $\mathbb{Q}(\alpha)/\mathbb{Q}$, with α transcendantal over $\mathbb{Q}$, is of finite type, but has infinite degree.
(*ii*) Suppose $[L : K] = p$ with p a prime number. Let $\alpha \in L \setminus K$. Consider the tower of extensions $K \subset K(\alpha) \subset L$. Then $[K(\alpha) : K]$ divides p, so $[K(\alpha) : K] = 1$ or $[K(\alpha) : K] = p$. The first possibility is excluded since $\alpha \notin K$. Then $[K(\alpha) : K] = p$, so $K(\alpha)$ is a $K-$vector space of dimension $[L : K]$. Since $K(\alpha) \subset L$, we must have $L = K(\alpha)$.

Exercice 3. We show $\mathbb{Q}(i,\sqrt{3}) = \mathbb{Q}(i+\sqrt{3})$, proving both inclusions.
Since i, $\sqrt{3} \in \mathbb{Q}(i,\sqrt{3})$, $i+\sqrt{3} \in \mathbb{Q}(i,\sqrt{3})$, so $\mathbb{Q}(i,\sqrt{3}) \supset \mathbb{Q}(i+\sqrt{3})$. For the reverse inclusion, we compute

$$(i+\sqrt{3})^2 = 2 + 2i\sqrt{3}$$
$$(i+\sqrt{3})^3 = (i+\sqrt{3})(2+2i\sqrt{3}) = 8i$$

and it follows that $i = \frac{1}{8}(i+\sqrt{3})^3 \in \mathbb{Q}(i+\sqrt{3})$. Likewise, $\sqrt{3} = (i+\sqrt{3}) - i \in \mathbb{Q}(i+\sqrt{3})$. This implies $\mathbb{Q}(i,\sqrt{3}) \subset \mathbb{Q}(i+\sqrt{3})$, and concludes the proof.

Exercise 6. (i) By multiplicativity, one has

$$[\mathbb{Q}(\sqrt{2},i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2},i) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$$

Now, X^2-2 is the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$, whence $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, and X^2+1 is the minimal polynomial of i over $\mathbb{Q}(\sqrt{2})$. Hence $[\mathbb{Q}(\sqrt{2},i) : \mathbb{Q}] = 2 \cdot 2 = 4$.

(ii) We compute the minimal polynomial of $\gamma := \sqrt{1+\sqrt{3}}$ over $\mathbb{Q}$. We have $\gamma^2 = 1+\sqrt{3}$, whence $(\gamma^2-1)^2 = 3$. It follows that

$$\gamma^4 - 2\gamma^2 + 1 = 3 \Longrightarrow \gamma^4 - 2\gamma^2 - 2 = 0.$$

The poynomial $X^4 - 4X^2 - 2$ is unitary, irreducible by Eisenstein, and has γ as a root. It is therefore its minimal polynomial, and $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 4$.

(iii) We begin by noticing that $\sqrt{6} = \sqrt{2}\sqrt{3} \in \mathbb{Q}(\sqrt{2},\sqrt{3})$, so we just need to compute $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}]$. As in (i), we directly show this degree is 4.

Exercice 7. First of all, X^2+X+1 is the minimal polynomial of ω over $\mathbb{Q}$, since it is unitary, admits ω as a root (indeed $0 = \omega^3 - 1 = (\omega-1)(\omega^2+\omega+1) \Longrightarrow \omega^2+\omega+1 = 0$) and is irreducible over $\mathbb{Q}$. Thus $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$.
We now claim that $\sqrt{3} \notin \mathbb{Q}(\omega)$. Indeed, if $\sqrt{3} \in \mathbb{Q}(\omega)$, $\mathbb{Q}(\omega)$ contains $\mathbb{Q}(\sqrt{3})$ as a subfield, and comparing degrees implies $\mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\omega)$. Such an equality is excluded, as the first field is contained in $\mathbb{R}$, and the second one contains some complex numbers. Suppose now $i \in \mathbb{Q}(\omega)$. Then there exists a, $b \in \mathbb{Q}$ such that $i = a + b\omega = a + b(\frac{-1}{2} + i\frac{\sqrt{3}}{2})$, which implies $2i = (2a-b) + ib\sqrt{3}$. It follows that $2a - b = 0$ and $b\sqrt{3} = 1$, and thus $\sqrt{3} = \frac{1}{b} \in \mathbb{Q}$. This is absurd, thus $i \notin \mathbb{Q}(\omega)$. This also implies $\omega \notin \mathbb{Q}(i)$ since otherwise we get as above that $\mathbb{Q}(\omega) = \mathbb{Q}(i)$, and in particular $i \in \mathbb{Q}(\omega)$, which is impossible as we just showed.

Exercise 8. This is the same reasoning as above: if $\alpha \in \mathbb{Q}(\beta)$, then $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\beta)$. Since these two $\mathbb{Q}-$vector spaces have the same dimension, and one is contained in the other, they must coincide, and $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$.

Exercise 9. Both fields are isomorphic to the quotient $\mathbb{Q}[X]/(X^4-2)$.

Exercise 10. (i) First, $\sqrt{3}$ is a root of X^2-3 over $\mathbb{Q}(\sqrt{2})$. To check it is the minimal polynomial, it is enough to see $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. By contradiction, suppose there exists a, $b \in \mathbb{Q}$ such that $\sqrt{3} = a + b\sqrt{2}$. This implies $\sqrt{3} - a = b\sqrt{2}$, and taking squares of both sides yields

$$(\sqrt{3}-a)^2 = (b\sqrt{2})^2 \Longrightarrow 3 + a^2 - 2a\sqrt{3} = 2b^2 \Longrightarrow \sqrt{3} = \frac{3+a^2-2b^2}{2a}$$

It follows that $\sqrt{3}$ is rational. This is impossible, and we conclude that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, so X^2-3 is the minimal polynomial of $\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$. On the other hand, $(\sqrt[4]{2})^2 = \sqrt{2}$ so $X^2 - \sqrt{2}$ is the minimal polynomial of $\sqrt[4]{2}$ over $\mathbb{Q}(\sqrt{2})$.

(ii) We denote $\gamma := \sqrt{2} + \sqrt[3]{2}$. Then $(\gamma - \sqrt{2})^3 = 2$, and one has

$$2 = (\gamma-\sqrt{2})^3 = \gamma^3 - 3\gamma^2\sqrt{2} + 6\gamma - 2\sqrt{2}$$

so $(3\gamma^2+2)\sqrt{2} = \gamma^3 + 6\gamma - 2$. Taking squares provides

$$2(9\gamma^4 + 12\gamma^2 + 4) = \gamma^6 + 36\gamma^2 + 4 + 12\gamma^4 - 4\gamma^3 - 24\gamma$$

which implies $\gamma^6 - 6\gamma^4 - 4\gamma^3 + 12\gamma^2 - 24\gamma - 4 = 0$. Then γ is a root of $X^6 - 6X^4 - 4X^3 + 12X^2 - 24X - 4$. Furthermore, this polynomial is unitary, and we check easily it is irreducible over $\mathbb{Q}$. It is then the minimal polynomial of γ over $\mathbb{Q}$.

Exercise 11. (i) Since $\beta \in \mathbb{Q}(\alpha)$, we have $\mathbb{Q}(\beta) \subset \mathbb{Q}(\alpha)$, so $[\mathbb{Q}(\beta) : \mathbb{Q}]$ divides $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, and since $\beta \notin \mathbb{Q}$, we get $[\mathbb{Q}(\beta) : \mathbb{Q}] = 3$. Since β has degree 3 over $\mathbb{Q}$, and that $\mathbb{Q}(\beta) \subset \mathbb{Q}(\alpha)$, these two fields must coincide, so $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha)$.

(*ii*) Let $\gamma := 2 - \alpha$. Then $\gamma \in \mathbb{Q}(\alpha) \setminus \mathbb{Q}$, so $\mathbb{Q}(\gamma) = \mathbb{Q}(\alpha)$ by (*i*). Thus the minimal polynomial of γ over $\mathbb{Q}(\alpha)$ is $X - \gamma$. Over $\mathbb{Q}$, we compute

$$\gamma = 2 - \alpha \iff \alpha = 2 - \gamma \iff 2 = \alpha^3 = (2-\gamma)^3 = 8 - 12\gamma + 6\gamma^2 - \gamma^3 \iff \gamma^3 - 6\gamma^2 + 12\gamma - 6 = 0$$

so γ is a root of $X^3 - 6X^2 + 12X - 6$. This polynomial is furthermore monic, and irreducible by Eisenstein. It is thus the minimal polynomial of γ over $\mathbb{Q}$.

Exercise 12. We compute the minimal polynomial of $\gamma := \sqrt{2} + \sqrt[3]{2+\sqrt{2}}$. We begin by noticing that $(\gamma - \sqrt{2})^3 = 2 + \sqrt{2}$, which yields to

$$\gamma^3 - \gamma^2\sqrt{2} + 2\gamma - 3\sqrt{2} = 2 \iff \gamma^3 + 2\gamma - 2 = (\gamma^2 + 2)\sqrt{2}.$$

Therefore we get

$$\gamma^6 + 4\gamma^2 + 4 + 4\gamma^4 - 4\gamma^3 - 8\gamma = 2\gamma^4 + 8\gamma^2 + 8$$

and so $\gamma^6 + 2\gamma^4 - 4\gamma^3 - 4\gamma^2 - 8\gamma - 4 = 0$. As above, we check $X^6 + 2X^4 - 4X^3 - 4X^2 - 8X - 4$ is irreducible over $\mathbb{Q}$. It is thus the minimal polynomial of γ, and we conclude that $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 6$.

Exercise 13. To start, we note that $a \in K(a)$, so $a^2 \in K(a)$, and we look at the tower of extensions

$$K \subset K(a^2) \subset K(a).$$

The polynomial $X^2 - a^2 \in K(a^2)[X]$ has a as a root, so $[K(a) : K(a^2)] \leq \deg(X^2 - a^2) = 2$. Moreover, by multiplicativity, $[K(a) : K(a^2)]$ divides $[K(a) : K]$, which is odd. Necessarily $[K(a) : K(a^2)] \neq 2$, which implies $[K(a) : K(a^2)] = 1$. Hence $K(a^2) = K(a)$. In particular, a^2 is algebraic over K. This is not true anymore if $[K(a) : K]$ is not odd: consider for instance $K = \mathbb{Q}$ et $a = \sqrt[4]{2}$.

Exercise 14. (*i*) One easily checks that $z := \omega\alpha$ is a root of $X^3 - 2$, and this polynomial is irreducible over $\mathbb{Q}$ by Eisenstein. Hence $[\mathbb{Q}(z) : \mathbb{Q}] = 3$, and we alreary saw above that $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$.

(*ii*) Suppose that $\overline{z} \in \mathbb{Q}(z)$. Then $\overline{z} = \overline{\omega}\alpha = \omega^2\alpha$ is in $\mathbb{Q}(z)$, and $z = \omega\alpha$ is in $\mathbb{Q}(z)$, so also $\omega = \frac{\overline{z}}{z} \in \mathbb{Q}(z)$.

(*iii*) The previous point implies then that $\mathbb{Q}(\omega) \subset \mathbb{Q}(z)$, and it follows that $[\mathbb{Q}(\omega) : \mathbb{Q}]$ divides $[\mathbb{Q}(z) : \mathbb{Q}]$ by degree multiplicativity. Using (*i*), this means that 2 divides 3, which is absurd. We conclude that $\overline{z} \notin \mathbb{Q}(z)$.

Exercise 15. We will prove that every prime number divides the degree $[\tilde{\mathbb{Q}} : \mathbb{Q}]$. In particular, it will imply this number cannot be finite, otherwise it would be divisible by only finitely many primes. Let then p be a prime number, and consider the polynomial $f = X^p - p \in \mathbb{Q}[X]$, which is irreducible by Eisenstein. Then the quotient $\mathbb{Q}[X]/(f(X))$ is a field, which contains a root a of f, and there exists an isomorphism $\mathbb{Q}[X]/(f(X)) \simeq \mathbb{Q}(a)$. Also a is then algebraic over $\mathbb{Q}$, and $\tilde{\mathbb{Q}}$ contains the subfield $\mathbb{Q}(a)$, which is an extension of $\mathbb{Q}$ of degree p. Hence p divides $[\tilde{\mathbb{Q}} : \mathbb{Q}]$, finishing the exercise.

Exercise 16. Let $a > 0$. We show rather that a is algebraic over $\mathbb{Q}$ if and only if $\sqrt{a}$ is algebraic over $\mathbb{Q}$.
$\Longrightarrow$: If a is algebraic over $\mathbb{Q}$, there exists $f(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Q}[X]$ such that $f(a) = 0$. We consider then $h(X) \in \mathbb{Q}[X]$ defined as

$$h(X) := a_n X^{2n} + a_{n-1}X^{2(n-1)} + \cdots + a_0$$

and we get $h(\sqrt{a}) = f(a) = 0$. This proves that $\sqrt{a}$ is algebraic over $\mathbb{Q}$.
$\Longleftarrow$: If $\sqrt{a}$ is algebraic over $\mathbb{Q}$, then $a = \sqrt{a}\sqrt{a}$ is the product of two algebraic numbers over $\mathbb{Q}$, and so is also algebraic over $\mathbb{Q}$.

Exercise 17. We show the contrapositive. Suppose $f(\alpha)$ is algebraic over K. By definition, there exists $h(X) \in K[X]$ such that $h(f(\alpha)) = 0$. This implies $h \circ f \in K[X]$ has α as a root, which is then algebraic over K.

3 Normal and separable extensions

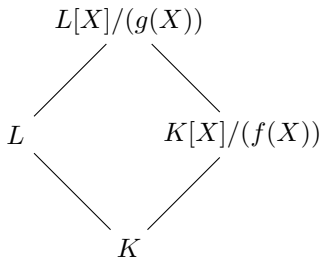
Exercise 1. Clearly, f has a root in $\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$, and in fact splits over this field, so $\mathbb{Q}(a) = \mathbb{Q}(\sqrt{2})$ is the splitting field of f. Also, the roots of g are

$$\frac{4 \pm \sqrt{8}}{2} = 2 \pm \sqrt{2}$$

and lie in $\mathbb{Q}(\sqrt{2})$. Hence $\mathbb{Q}(a) = \mathbb{Q}(b)$.

Exercise 2. (i) $\Longrightarrow$: If $f \in K[X]$ is irreducible, then $K[X]/(f(X))$ is a field, isomorphic to $K(a)$, where a is a root of f. It is the smallest field containing a root of f, and $[K(a) : K] = n$. Therefore, a field extension L/K with $[L : K] \leq \frac{n}{2}$ cannot contain any root of f.
$\Longleftarrow$: One can check separately the cases $n \in \{1, 2, 3\}$, and we take $n \geq 4$. To reach a contradiction, suppose $f \in K[X]$ is not irreducible. Then we factor f as $f = gh$ with g, $h \in K[X]$, and at least one of these factors has degree $\leq \frac{n}{2}$. Indeed if $\deg(g)$, $\deg(h) > \frac{n}{2}$, then $n = \deg(f) = \deg(g) + \deg(h) > \frac{n}{2} + \frac{n}{2} = n$, which is impossible. Without restriction, say $\deg(g) \leq \frac{n}{2}$. Take then $g_1 \in K[X]$ an irreducible factor of g. The quotient $L := K[X]/(g_1(X))$ is a field, containing a root a of g_1, which is also a root of f, and isomorphic to $K(a)$. Therefore $[L : K] = [K(a) : K] = \deg(g_1) \leq \frac{n}{2}$. Then we built an extension L/K containing a root of f and of degree bounded from above by $\frac{n}{2}$. This contradicts our hypothesis, and hence f must be irreducible in $K[X]$.

(ii) By contradiction, suppose f is not irreducible in $L[X]$. Take $g \in L[X]$ an irreducible factor of f, of degree $1 \leq d < n$. The quotient $L[X]/(g(X))$ is an extension of L of degree d, containing a root of g, which a root of f as well. Since L is an extension of K, $L[X]/(g(X))$ is an extension of K, containing a root of f. But $K[X]/(f(X))$ is the smallest extension of K containing a root of f. Hence we must have the containment $K[X]/(f(X)) \subset L[X]/(g(X))$. Denote now by x the degree of this extension. To sum up, we have



By multiplicativity of the degrees, one has $md = nx$. This implies that n divides md, and as n and m are coprime, n divides d. In particular, $n \leq d$. Recalling where d comes from, we also have $d < n$. This is the desired contradiction. We conclude that f is irreducible in $L[X]$.

(iii) This is a straightforward application of the previous point. The polynomial $f = X^5 - 9X^3 + 15X + 6$ is irreducible in $\mathbb{Q}[X]$ by Eisenstein, and $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ is coprime with $\deg(X^5 - 9X^3 + 15X + 6) = 5$. Hence $X^5 - 9X^3 + 15X + 6$ is irreducible in $\mathbb{Q}(\sqrt{2}, \sqrt{3})[X]$.

Exercise 3. (i) In $\mathbb{C}$, the roots of $X^4 - 1$ are 1, -1, i and $-i$. Hence $L = \mathbb{Q}(i)$ is the splitting field of $X^4 - 1$ over $\mathbb{Q}$. Here $[L : \mathbb{Q}] = 2$.

(ii) On the other hand, the roots of $X^4 + 1$ are $e^{i\frac{\pi}{4}}$, $e^{i\frac{3\pi}{4}}$, $e^{i\frac{5\pi}{4}}$ and $e^{i\frac{7\pi}{4}}$. Hence we must adjoign $e^{i\frac{\pi}{4}}$ to $\mathbb{Q}$, and since $e^{i\frac{\pi}{4}} = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$, it is enough to adjoign $\sqrt{2}$ and i. Thus $L = \mathbb{Q}(\sqrt{2}, i)$ is a splitting field for $X^4 + 1$ over $\mathbb{Q}$ and $[L : \mathbb{Q}] = 4$.

(iii) One can solve the quartic equation $X^4 - 4X^2 + 2 = 0$ by setting $Y := X^2$. Then we are left to solve $Y^2 - 4Y + 2 = 0$. Solutions of this equation are

$$Y_1 = \frac{4 - \sqrt{8}}{2} = 2 - \sqrt{2},\ Y_2 = 2 + \sqrt{2}$$

and so the solutions to $X^4 - 4X^2 + 2 = 0$ are $\sqrt{2 - \sqrt{2}}$, $-\sqrt{2 - \sqrt{2}}$, $\sqrt{2 + \sqrt{2}}$ and $-\sqrt{2 + \sqrt{2}}$. Set $\alpha := \sqrt{2 + \sqrt{2}}$, $\beta := \sqrt{2 - \sqrt{2}}$ and $L := \mathbb{Q}(\alpha)$. Then L contains α, $-\alpha$, and

$$\alpha\beta = \sqrt{2} = \alpha^2 - 2 \Longrightarrow \beta = \frac{\alpha^2 - 2}{\alpha} \in L$$

so β, $-\beta \in L$ as well. This proves L is the splitting field of $X^4 - 4X^2 + 2$ over $\mathbb{Q}$, and $[L : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(X^4 - 4X^2 + 2) = 4$, as $X^4 - 4X^2 + 2$ is the minimal polynomial of α over $\mathbb{Q}$.

(iv) Clearly $\mathbb{Q}(\sqrt{2}, i\sqrt{3})$ is the splitting field we are looking for. Additionally, $[\mathbb{Q}(\sqrt{2}, i\sqrt{3}) : \mathbb{Q}] = 4$.

(v) We start by noticing that 1 is a root of $X^3 - 5X^2 + 9X - 5$, and this polynomial factors in $\mathbb{Q}[X]$ as

$$X^3 - 5X^2 + 9X - 5 = (X - 1)(X^2 - 4X + 5).$$

The roots of $X^2 - 4X + 5$ are complex with integer imaginary part, so we just need to add i to $\mathbb{Q}$, and $\mathbb{Q}(i)$ is the splitting field of $X^3 - 5X^2 + 9X - 5$ over $\mathbb{Q}$. Furthermore, it has degree 2 over $\mathbb{Q}$.

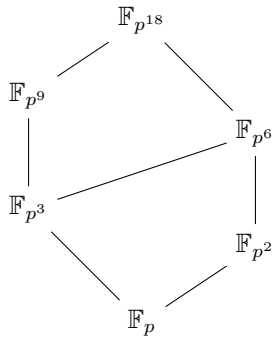
Exercise 6. Clearly, $\mathbb{Q}(\sqrt{3}, i)$ is a splitting field of $(X^2 - 3)(X^2 + i)$ over $\mathbb{Q}$, and exactly as in chapter 2, one easily establishes that $\mathbb{Q}(\sqrt{3}, i) = \mathbb{Q}(i + \sqrt{3})$.

Exercise 8. $\Longrightarrow$: Suppose first $\mathbb{F}_{p^m}$ is an extension of $\mathbb{F}_{p^n}$. In particular, we can see $\mathbb{F}_{p^m}$ as an $\mathbb{F}_{p^n}-$vectorspace and by denoting $s := \dim_{\mathbb{F}_{p^n}} \mathbb{F}_{p^m}$, one has $m = ns$.
$\Longleftarrow$: Conversely, suppose $m = ns$, and take $x \in \mathbb{F}_{p^n}$. Then $x^{p^n} = x$ and it follows that

$$x^{p^m} = x^{p^{ns}} = (x^{p^n})^{p^{n(s-1)}} = x^{p^{n(s-1)}} = \cdots = x^{p^n} = x$$

and this proves that $x \in \mathbb{F}_{p^m}$.

Exercise 9. By the previous exercise, the diagram looks like the diagram of the divisors of 18. One has



Exercise 10. First of all, $X^3 + X + 1$ has no roots in $\mathbb{F}_2$, and has degree 3, so it is irreducible over $\mathbb{F}_2$. To prove irreducibility over $\mathbb{F}_{16}$ and $\mathbb{F}_{32}$, we use point (ii) of exercise 2 above: $\mathbb{F}_{16}$ and $\mathbb{F}_{32}$ are both extensions of $\mathbb{F}_2$, of degrees 4 and 5 respectively. As 4 and 5 are coprime with $3 = \deg(X^3 + X + 1)$, we conclude that $X^3 + X + 1$ is irreducible over $\mathbb{F}_{16}$ and $\mathbb{F}_{32}$. On the other hand, $\mathbb{F}_8 = \mathbb{F}_{2^3} \simeq \mathbb{F}_2[X]/(X^3 + X + 1)$ is the splitting field of $X^3 + X + 1$ and is contained in $\mathbb{F}_{64} = \mathbb{F}_{2^6}$. Hence $X^3 + X + 1$ is not irreducible over $\mathbb{F}_{64}$.

Exercise 11. We prove the contrapositive. Let us fix K a finite field. Then the polynomial

$$f = 1_K + \prod_{k \in K} (X - k) \in K[X]$$

has no roots in K, since $f(k) = 1_K$ for all $k \in K$. Thus K is not algebraically closed.

Exercise 12. (i) By definition, $\tilde{K}/K$ is algebraic.
By contradiction, suppose $\tilde{K}$ is not algebraically closed. Then, by Proposition 3.8, it has an non-trivial algebraic extension $\tilde{K} \subsetneq M$. Since $M/\tilde{K}$ is algebraic and $\tilde{K}/K$ is algebraic, M/K is algebraic by Theorem 2.19. Now let $\alpha \in M \setminus \tilde{K}$. Then α is algebraic over K by what we just showed, which implies α in $\tilde{K}$. This is the desired contradiction and thus $\tilde{K}$ cannot have a non-trivial algebraic extension, which means it is algebraically closed.

(ii) A finite extension L of $\mathbb{Q}$ takes the form $L = \mathbb{Q}(a_1, \ldots, a_n)$ where $a_1, \ldots, a_n \in L$ are algebraic over $\mathbb{Q}$. This is then clearly a subfield of $\tilde{\mathbb{Q}}$.

Exercise 14. The extension $\mathbb{Q}(\sqrt{2}, i\sqrt{3}, \sqrt[3]{5})/\mathbb{Q}$ is normal because it is a splitting field of $f = (X^2 - 2)(X^2 + 3)(X^3 - 5)$. To compute the degree we consider the tower

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{5}) \subset \mathbb{Q}(\sqrt[3]{5}, \sqrt{2}) \subset \mathbb{Q}(\sqrt[3]{5}, \sqrt{2}, i\sqrt{3}).$$

The first extension has degree 3, and the second has degree 2 because $\sqrt{2}$ has $X^2 - 2$ for minimal polynomial over $\mathbb{Q}(\sqrt[3]{5})$. The last one has also degree 2 because the minimal polynomial of $i\sqrt{3}$ is $X^2 + 3$. Thus $[\mathbb{Q}(\sqrt{2}, i\sqrt{3}, \sqrt[3]{5}) : \mathbb{Q}] = 3 \cdot 2 \cdot 2 = 12$.
To justify the irreducibility of $X^2 - 2$ over $\mathbb{Q}(\sqrt[3]{5})$, one can use exercise $2(ii)$ in the same section.

Exercise 15. The extension $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$ has degree 2, and hence is normal by one example of the course. Indeed the minimal polynomial of ω over $\mathbb{Q}(\sqrt[3]{2})$ is $X^2 + X + 1$, and this polynomial is irreducible over $\mathbb{Q}(\sqrt[3]{2})$ precisely because its roots ω and $\overline{\omega}$ are complex, and therefore cannot lie in $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$.
Again, to justify irreducibility of $X^2 + X + 1$ over $\mathbb{Q}(\sqrt[3]{2})$, think about exercise $2(ii)$ of the same section.

Exercise 16. (i) $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ is normal over $\mathbb{Q}$ since it is a splitting field of $(X^2 - 2)(X^2 - 3)$.

(ii) $\mathbb{Q}(\sqrt[3]{7})/\mathbb{Q}$ is not normal: $X^3 - 7$ is irreducible in $\mathbb{Q}[X]$ and has one root in $\mathbb{Q}(\sqrt[3]{7})$, but doesn't split in this field since its other roots are complex and do not lie in $\mathbb{Q}(\sqrt[3]{7}) \subset \mathbb{R}$.

(*iii*) Let $\alpha := \sqrt{2+\sqrt{2}}$. Then $(\alpha^2-2)^2 = 2$, so $\alpha^4 - 4\alpha^2 + 2 = 0$, and α is a root of $X^4 - 4X^2 + 2 \in \mathbb{Q}[X]$. Its other roots are $-\alpha$, β and $-\beta$, where $\beta = \sqrt{2-\sqrt{2}}$. Next we compute

$$\alpha\beta = \sqrt{2} = \alpha^2 - 2 \Longrightarrow \beta = \frac{\alpha^2-2}{\alpha}$$

so $\beta \in \mathbb{Q}(\alpha)$. Hence $\mathbb{Q}(\alpha)$ contains all roots of $X^4 - 4X^2 + 2$, and $\mathbb{Q}(\alpha)/\mathbb{Q}$ is normal.

(*iv*) Here $\alpha := \sqrt{1+\sqrt{3}}$ is a root of $X^4 - 2X^2 - 2$, which is irreducible in $\mathbb{Q}[X]$ by Eisenstein's criterion, and the others root of this polynomial are $-\alpha$, $\beta := \sqrt{1-\sqrt{3}}$ and $-\beta$. Nevertheless β and $-\beta$ are complex numbers, so they don't lie in $\mathbb{Q}(\alpha) \subset \mathbb{R}$. This implies $\mathbb{Q}(\sqrt{1+\sqrt{3}})/\mathbb{Q}$ is not normal.

(*v*) This is a normal extension of $\mathbb{F}_2$, by theorem 1.19.

(*vi*) The considered extension is a splitting field for $X^n - 1 \in \mathbb{Q}[X]$.

Exercise 17. $\Longrightarrow$: Suppose $f(X) \in K[X] \setminus \{0\}$ is separable. Then, if α is a root of f, it is simple, which implies $f'(\alpha) \neq 0$ by Lemma 3.19. Thus f and f' have no common root in any extension of K, which means they are relatively prime by exercise 12 of chapter 1.
$\Longleftarrow$: Suppose f and f' are relatively prime, and by contradiction suppose α is a multiple root of f.
By Bezout's theorem, there exists $u(X)$, $v(X) \in K[X]$ such that

$$u(X)f(X) + v(X)f'(X) = 1.$$

Since α is repeated, we have $f(\alpha) = f'(\alpha) = 0$, and substitute α for X provides a contradiction. Thus f is separable.

Exercise 18. (*i*) The polynomial $X^4 - 2X - 14 \in \mathbb{Q}[X]$ is irreducible by Eisenstein, and $\mathbb{Q}$ has caracteristic 0, so $X^4 - 2X - 14$ is separable by Proposition 3.21.

(*ii*) We showed in exercise 10 in chapter 1 that $X^3 + Y^2X^2 - YX - Y^3 + Y^2$ is irreducible in $\mathbb{C}[X,Y]$. Since we are in caracteristic 0, separability is given by Proposition 3.21.

(*iii*) Same argument as above.

(*iv*) $X^4 + 1 = (X+1)^4 \in \mathbb{F}_2[X]$ admits -1 as repeated root. Therefore it is not separable.

Exercise 19. We directly see that if $\mathrm{char}(K)$ divides n, then $f' = nX^{n-1} = 0$, so f is not separable, and on the other hand, if $\mathrm{char}(K)$ does not divide n, then $f' \neq 0$, and f is separable. Thus f is separable $\Longleftrightarrow n \neq 0$ in K.

Exercise 20. The formal derivative of $f = X^p - X - a$ is $f' = -1$, which is always non-zero. So f is separable by Lemma 3.19(*i*). Immediately, the same applies for polynomials of the form $f = g(X^p) + cX$, with $c \in K^*$, since in this case the derivative is $f' = pX^{p-1}g'(X^p) + c = c$ as $\mathrm{char}(K) = p$. The two particular cases are immediate.

Exercise 21. $\Longrightarrow$: Suppose first that $f \in K[X]$ is separable. This implies, by exercise 16 above, that f and f' are relatively prime in $K[X]$. From Bezout's theorem, there exists $u(X)$, $v(X) \in K[X]$ such that

$$u(X)f(X) + v(X)f'(X) = 1_K$$

in $K[X]$. Applying $\tilde{\sigma}$ to this equation and using the fact it is a ring morphism (so it preserves addition and product of polynomials, and sends 1_K to 1_L), one gets

$$\tilde{\sigma}(u)\tilde{\sigma}(f) + \tilde{\sigma}(v)\tilde{\sigma}(f') = 1_L$$

and noticing $\tilde{\sigma}(f') = \tilde{\sigma}(f)'$ (which also follows from $\tilde{\sigma}$ being a ring morphism), we see that $\tilde{\sigma}(f)$ and $\tilde{\sigma}(f)'$ are relatively prime in $L[X]$. Then $\tilde{\sigma}(f)$ is separable, by exercise 16 above.
$\Longleftarrow$: Conversely, if $f \in K[X]$ is not separable, then f and f' have a non-trivial common divisor, say $d(X)$. Since $\tilde{\sigma}$ is a ring morphism, $\tilde{\sigma}(d) \in L[X]$ is a non-trivial common divisor to $\tilde{\sigma}(f)$ and $\tilde{\sigma}(f)'$. Thus these two last polynomials are not relatively prime in $L[X]$, which proves $\tilde{\sigma}(f) \in L[X]$ is not separable.

Exercise 22. By contradiction, suppose L/K is not separable. Then there exists $\alpha \in L$ which is not separable, which means its minimal polynomial $f \in K[X]$ is not separable. By Proposition 3.21(*ii*), which we may use since f is irreducible, we deduce $f \in K[X^p]$. In particular, $n = \deg(f)$ is a multiple of p, which contradicts the fact that n and p are relatively prime. Thus L/K is separable.

Exercise 23. Note first that a finite field is of the form $\mathbb{F}_{p^n}$ for a prime number p and $n \geq 1$, *i.e.* it is an algebraic extension of $\mathbb{F}_p$. Note also that $\mathbb{F}_p$ is perfect, combining Theorem 1.19 and Proposition 3.24. Hence we will be done if

we show that any algebraic extension of a perfect field is perfect.
Let then K be perfect, and L/K be algebraic. Let M/L be algebraic. By Theorem 2.19, M/K is algebraic. Since K is perfect, it follows that M/K is separable. By Corollary 3.31(i), M/L is also separable. Thus we proved every algebraic extension M of L is separable, which exactly says that L is perfect.

Exercise 24. Write $K = \mathbb{F}_q$ where $q = p^n$ is a power of a prime number p. Note that $|K^*| = q - 1$, so it is sufficient to show that K^* has an element of order $q - 1$. Let d be the maximal order of the elements of K^* and let $a \in K^*$ having order d. Then in particular, d divides $|K^*|$, so $d \leq q - 1$. Also, every element of K^* has order a divisor of d (by maximality of d), and hence is a root of $X^d - 1$. It follows that $q - 1 \leq d$, and thus $d = q - 1$. This concludes the proof.

Exercise 25. Let L/K be finite, normal and separable. Since L/K is finite and separable, the primitive element theorem ensures the existence of $a \in L$ such that $L = K(a)$. Consider $f \in K[X]$ the minimal polynomial of a over K, which exists since L/K is algebraic (since it is finite). Then f has a root in L, namely a, and therefore splits in L since L/K is normal. This proves $L = K(a)$ is the splitting field of f, an irreducible separable polynomial of $K[X]$.

Exercise 26. (i) Let $\gamma := i + \sqrt{2}$. Then $\gamma \in \mathbb{Q}(\sqrt{2}, i)$, so $\mathbb{Q}(\gamma) \subset \mathbb{Q}(\sqrt{2}, i)$. To see these fields actually coincide, we compare degrees. Clearly, $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4$. To find $[\mathbb{Q}(\gamma) : \mathbb{Q}]$, we compute its minimal polynomial, noticing that $(\gamma - \sqrt{2})^2 = -1$. This implies

$$\gamma^2 - 2\sqrt{2}\gamma + 2 = -1 \iff \gamma^2 + 3 = 2\sqrt{2}\gamma \iff (\gamma^2 + 3)^2 = (2\sqrt{2}\gamma)^2 \iff \gamma^4 - 2\gamma^2 + 9 = 0.$$

Hence $X^4 - 2X^2 + 9$ is the minimal polynomial of γ over $\mathbb{Q}$, and $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 4$. Therefore, both $\mathbb{Q}(\gamma)$ and $\mathbb{Q}(\sqrt{2}, i)$ have degree 4 over $\mathbb{Q}$, and one is contained in the other, so they must be equal. We conclude that $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(i + \sqrt{2})$, and $i + \sqrt{2}$ is a primitive element for $\mathbb{Q}(\sqrt{2}, i)$.

(ii) First, remark that $\sqrt{15} = \sqrt{3}\sqrt{5}$ is already in $\mathbb{Q}(\sqrt{3}, \sqrt{5})$. So we are left to find a primitive element of $\mathbb{Q}(\sqrt{3}, \sqrt{5})$. Exactly as in (i), we prove that $\sqrt{3} + \sqrt{5}$ is such a primitive element.

(iii) Let $\gamma := \sqrt{2} + \sqrt[3]{2}$. Clearly, $\gamma \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$, so $\mathbb{Q}(\gamma) \subset \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$. To prove the other inclusion, we compare degrees. On the one hand, we have

$$[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}), \mathbb{Q}] = 3 \cdot 2 = 6$$

since $X^2 - 2$ is the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ and $X^3 - 2$ is the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}(\sqrt{2})$. On the other hand, as $(\gamma - \sqrt{2})^3 = 2$, we have

$$\gamma^3 - 3\gamma^2\sqrt{2} + 6\gamma - 2\sqrt{2} = 2 \Longrightarrow \gamma^3 + 6\gamma - 2 = \sqrt{2}(3\gamma^2 + 2).$$

Taking squares of both sides and expanding now provides $\gamma^6 + 36\gamma^2 + 4 + 12\gamma^4 - 24\gamma - 4\gamma^3 = 2(3\gamma^2 + 2)^2$, whence

$$\gamma^6 + 36\gamma^2 + 4 + 12\gamma^4 - 24\gamma - 4\gamma^3 = 2(9\gamma^4 + 12\gamma^2 + 4) = 18\gamma^4 + 24\gamma^2 + 8$$

and finally $\gamma^6 - 6\gamma^4 - 4\gamma^3 + 12\gamma^2 - 24\gamma - 8 = 0$. One directly checks that $X^6 - 6X^4 - 4X^3 + 12X^2 - 24X - 8$ is irreducible over $\mathbb{Q}$, and thus it is the minimal polynomial of γ over $\mathbb{Q}$. We conclude that $\mathbb{Q}(\gamma)/\mathbb{Q}$ also has degree 6, and because of the containment $\mathbb{Q}(\gamma) \subset \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$, it follows that $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) = \mathbb{Q}(\gamma)$, and γ is a primitive element for $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})/\mathbb{Q}$.

(iv) Exactly in the same way, one shows that $\gamma := \sqrt[3]{2} + \omega$ is a primitive element for the considered extension.

Exercise 27. As shown in the previous exercise, $\sqrt{2} + \sqrt[3]{2}$ is a primitive element for $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$. We claim that $\sqrt[6]{2}$ is another such primitive element. Indeed, it also has degree 6 over $\mathbb{Q}$, since its minimal polynomial is $X^6 - 2$, and as

$$(\sqrt[6]{2})^2 = \sqrt[3]{2},\ (\sqrt[6]{2})^3 = \sqrt{2}$$

we deduce that $\mathbb{Q}(\sqrt[6]{2}) \supset \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$. Now both fields are degree 6 extensions of $\mathbb{Q}$, so they must coincide, and $\mathbb{Q}(\sqrt[6]{2}) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$.

Exercise 29. Let L/K be finite and simple, and $K \subset M \subset L$ a subextension.
Since L/K is simple, the previous exercise tells us there is finitely many intermediate subfields between K and L, so in particular there is finitely many subfields between K and M, and again using the previous exercise, it implies that M/K is simple.

Exercise 30. Consider the extension $\mathbb{F}_{p^n}/\mathbb{F}_p$. It is finite of degree n, in particular algebraic, and since $\mathbb{F}_p$ is perfect (corollary 3.26), $\mathbb{F}_{p^n}/\mathbb{F}_p$ is separable. By the primitive element theorem, there exists $\gamma \in \mathbb{F}_{p^n}$ such that $\mathbb{F}_{p^n} = \mathbb{F}_p(\gamma)$. The minimal polynomial of γ is then an irreducible polynomial of degree n with coefficients in $\mathbb{F}_p$.

4 Galois theory

Exercise 1. Let K be such that $\mathrm{char}(K) \neq 2$, and suppose L/K is such that $[L:K] = 2$. Then there exists $d \in K$ such that $L = K(\sqrt{d})$, by exercise 4 of chapter 2, and the minimal polynomial of $\sqrt{d}$ over K is $f = X^2 - d$. Then L/K is normal, as it is the splitting field of f over K. Moreover, f is separable since $f' = 2X \neq 0$ in K, as $\mathrm{char}(K) \neq 2$. It follows that $\sqrt{d}$ is separable over K, and then L/K is separable by Corollary 3.31(ii). This proves L/K is Galois.

Exercise 2. (i) Suppose L/K is finite and separable. Then there exists $a_1, \dots, a_n \in L$ algebraic over K such that $L = K(a_1, \dots, a_n)$, by Theorem 2.17. Consider $f_1, \dots, f_n \in K[X]$ the minimal polynomials of $a_1, \dots, a_n$ over K, and N the normal closure of L/K, which is built by adding the others roots of $f_1, \dots, f_n$ to L. Then N/K is normal by definition. Moreover, since L/K is separable by hypothesis, a_i is separable over K for all $i = 1, \dots, n$, so f_i is separable over K for all $i = 1, \dots, n$, so its other roots, those we add to L to get N, are also separable over K. Hence N/K is separable by Corollary 3.31(ii), and thus Galois. Furthermore, it clearly contains L as a subfield.

(ii) Suppose L/K is finite and inseparable, and suppose to reach a contradiction that it can be embedded in a finite Galois extension N of K. Then N/K is separable, and since subextensions of separable extensions are separable (Corollary 3.31(i)), L/K is separable as well. This is absurd, and we get the result.

Exercise 3. Note that, by the construction of $\overline{K}$, $\overline{K}/K$ is normal. By Proposition 3.24 and Theorem 4.4, one has

$$K \text{ is perfect } \iff \overline{K}/K \text{ is separable } \iff \overline{K}/K \text{ is Galois } \iff \overline{K}^G = K.$$

Exercise 4. In the field L, f has a root α, and factors as $f = X^p - Y = (X - \alpha)^p$. Moreover, $L = K(\alpha)$ and an element $\sigma \in \mathrm{Gal}(L/K)$ must send α to another root of f, which forces $\sigma(\alpha) = \alpha$. Then $\sigma = \mathrm{id}_L$, and $\mathrm{Gal}(L/K) = \{1\}$. On the other hand, $f \in K[X]$ is monic, irreducible by Eisenstein and has α as a root. It is then its minimal polynomial, and hence $[L:K] = [K(\alpha):K] = \deg(f) = p > 1 = |\mathrm{Gal}(L/K)|$. By Corollary 4.6, L/K is not Galois. Note this is also clear from the writing $f = (X - \alpha)^p$, which shows that α is not separable over K, since its minimal polynomial f has a multiple root.

Exercise 5. Fix $n \geq 2$. Then the polynomial f defined as

$$f(X) := (X - i)(X + i)(X - 2i)(X + 2i) \dots (X - ni)(X + ni) = (X^2 + 1)(X^2 + 4) \dots (X^2 + n^2)$$

has degree $2n$, is in $\mathbb{Q}[X]$ (even in $\mathbb{Z}[X]$), and is separable by construction. Nonetheless, all roots of f lie in $\mathbb{Q}(i)$, so $\mathrm{Gal}(f) = \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$.

Exercise 6. (i) The claim is false. A counter example is given by the tower of extensions

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2}).$$

Both subextensions are quadratic, hence normal, and separability is automatic in characteristic 0, so they are both Galois. However we already saw $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not Galois, since $X^4 - 2$ is an irreducible polynomial of $\mathbb{Q}[X]$ with all but two roots in $\mathbb{Q}(\sqrt[4]{2})$.

(ii) If M/K is Galois, then M/L is normal (corollary 3.15(i)) and separable (corollary 3.31(i)), hence M/L is Galois. However, L/K is not Galois in general. Consider for instance the tower of extensions

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[3]{2}, \omega)$$

with ω a primitive cubic root of 1. There $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois, as it is not normal ($X^3 - 2$ has a root in this field but does not split).

(iii) If we assume additionally that $\mathrm{Gal}(M/K)$ is abelian, then L/K is normal since $\mathrm{Gal}(M/L)$ is a normal subgroup of $\mathrm{Gal}(M/K)$ (theorem 4.7(v)). Further, L/K is separable because every subextension of a separable extension is separable. Thus L/K is Galois.

Exercise 7. Let $L := \mathbb{Q}(\sqrt{2}, i)$, and $K := \mathbb{Q}$. The extension L/K is normal, since L is the splitting field of $f = (X^2 - 2)(X^2 + 1)$ over K. As separability is automatic in characteristic 0, L/K is Galois. An element $\sigma \in \mathrm{Gal}(L/K)$ is determined by its values on $\sqrt{2}$ and i, and these values must be roots of $X^2 - 2$ and $X^2 + 1$ respectively. Then $\sigma(\sqrt{2}) \in \{-\sqrt{2}, \sqrt{2}\}$ and $\sigma(i) \in \{-i, i\}$, and hence $\mathrm{Gal}(L/K)$ contains 4 elements, namely

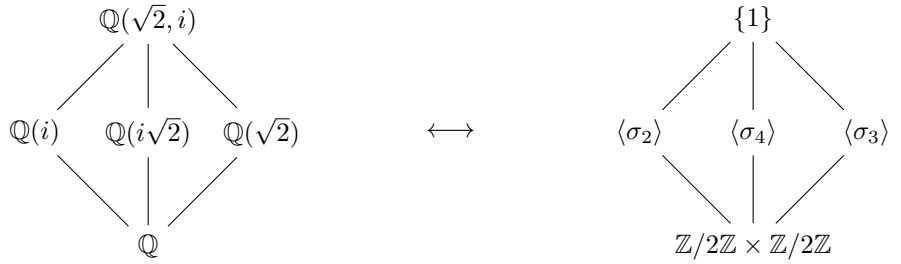
$$\sigma_1 \colon \sqrt{2} \longmapsto \sqrt{2},\ i \longmapsto i$$

$$\sigma_2 \colon \sqrt{2} \longmapsto -\sqrt{2},\ i \longmapsto i$$
$$\sigma_3 \colon \sqrt{2} \longmapsto \sqrt{2},\ i \longmapsto -i$$
$$\sigma_4 \colon \sqrt{2} \longmapsto -\sqrt{2},\ i \longmapsto -i$$

Then $\sigma_1 = \mathrm{id}_L$ has order 1, and σ_2, σ_3, σ_4 have order 2, so $\mathrm{Gal}(L/K) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Each of these three automorphisms generates a subgroup of order 2 in the Galois group, and we have

$$L^{\langle\sigma_2\rangle} = \mathbb{Q}(i),\ L^{\langle\sigma_3\rangle} = \mathbb{Q}(\sqrt{2}),\ L^{\langle\sigma_4\rangle} = \mathbb{Q}(i\sqrt{2}).$$

Indeed, for instance, σ_2 fixes $\mathbb{Q}$ and i, so $\mathbb{Q}(i) \subset L^{\langle\sigma_2\rangle}$. Since these two fields are both quadratic extensions of $\mathbb{Q}$, they must agree, so $L^{\langle\sigma_2\rangle} = \mathbb{Q}(i)$. Likewise we find the other two fixed fields. Therefore the Galois correspondence takes the form



Lastly, $\mathrm{Gal}(L/K) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is abelian, so all its subgroups are normal, and every extension appearing on the left is normal.

Exercise 8. Let $a := \sqrt{2+\sqrt{2}}$, and $f \in \mathbb{Q}[X]$ be the minimal polynomial of a over $\mathbb{Q}$.
We begin by noticing that

$$(a^2-2)^2 = 2$$

and it follows that $a^4 - 4a^2 + 2 = 0$. Thus $X^4 - 4X^2 + 2$ has a for root. It is furthermore unitary, and irreducible by Eisenstein's criterion. Hence $f(X) = X^4 - 4X^2 + 2$. We also have $f(-a) = f(b) = f(-b) = 0$, where $b := \sqrt{2-\sqrt{2}}$, and so these are all the roots of f. We also get

$$ab = \sqrt{2+\sqrt{2}}\sqrt{2-\sqrt{2}} = \sqrt{4-2} = \sqrt{2} = a^2 - 2 \Longrightarrow b = \frac{a^2-2}{a} \in \mathbb{Q}(a).$$

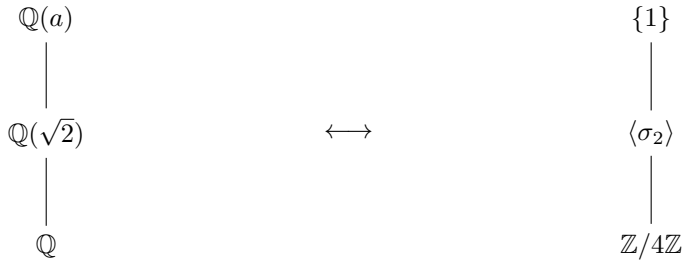
Obviously $-a$, $-b \in \mathbb{Q}(a)$, and $\mathbb{Q}(a)$ is the splitting field of f over $\mathbb{Q}$. Also $[\mathbb{Q}(a) : \mathbb{Q}] = \deg(f) = 4$, and since $\mathbb{Q}(a)/\mathbb{Q}$ is Galois, $|\mathrm{Gal}(f)| = [\mathbb{Q}(a) : \mathbb{Q}] = 4$. It implies $\mathrm{Gal}(f) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\mathrm{Gal}(f) \simeq \mathbb{Z}/4\mathbb{Z}$. An element of $\mathrm{Gal}(f) = \mathrm{Gal}(\mathbb{Q}(a)/\mathbb{Q})$ is determined by its image on a, and we can write down explicitly all four $\mathbb{Q}-$automorphisms. We get

$$\sigma_1 \colon a \longmapsto a,\ b \longmapsto b$$
$$\sigma_2 \colon a \longmapsto -a,\ b \longmapsto -b$$
$$\sigma_3 \colon a \longmapsto b,\ b \longmapsto -a$$
$$\sigma_4 \colon a \longmapsto -b,\ b \longmapsto a$$

by using the two relations $b = \frac{a^2-2}{a}$ and $b^2 - 2 = -(a^2-2)$. A direct computation shows $\sigma_2^2 = \mathrm{id}_{\mathbb{Q}(a)}$, $\sigma_3^2(b) = -b = \sigma_4^2(b)$. Hence σ_3 and σ_4 have both order 4, and $\mathrm{Gal}(f) \simeq \mathbb{Z}/4\mathbb{Z}$. Thus $\langle\sigma_2\rangle$ is the unique subgroup of order 2 in $\mathrm{Gal}(f)$, and the corresponding fixed field is $\mathbb{Q}(\sqrt{2})$. Indeed, we compute

$$\sigma_2(\sqrt{2}) = \sigma_2(a^2-2) = (-a)^2 - 2 = \sqrt{2}$$

which implies $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(a)^{\langle\sigma_2\rangle}$, and since both fields have degree 2 over $\mathbb{Q}$, they must coincide. The Galois correspondence then takes the form



Exercise 9. (i) Reducing modulo 5, one checks directly that f is irreducible over $\mathbb{Q}$. Exactly as in the previous exercise, we solve the equation $f = 0$ directly to get that the roots of f are $\alpha := \sqrt{6+3\sqrt{2}}, -\sqrt{6+3\sqrt{2}}, \beta := \sqrt{6-3\sqrt{2}}$ and $-\sqrt{6-3\sqrt{2}}$. Also we compute

$$\alpha\beta = \sqrt{18} = 3\sqrt{2} = \alpha^2 - 6 \Longrightarrow \beta = \frac{\alpha^2-6}{\alpha} \in \mathbb{Q}(\alpha)$$

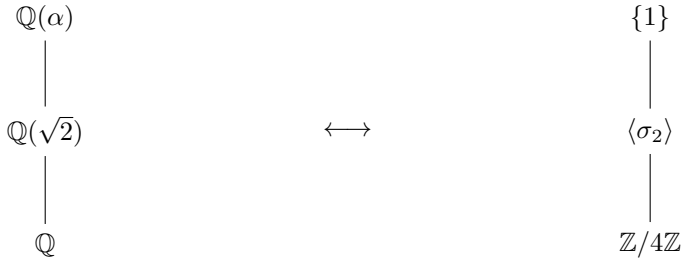
and thus all roots of f are in $\mathbb{Q}(\alpha)$. So $L = \mathbb{Q}(\alpha)$ is the splitting field of f over $\mathbb{Q}$, and $[L:\mathbb{Q}] = [\mathbb{Q}(\alpha):\mathbb{Q}] = 4$.

(ii) An element $\sigma \in \mathrm{Gal}(f)$ is determined by $\sigma(\alpha)$, which must be an other root of f. Explicitly, the four $\mathbb{Q}-$automorphisms are

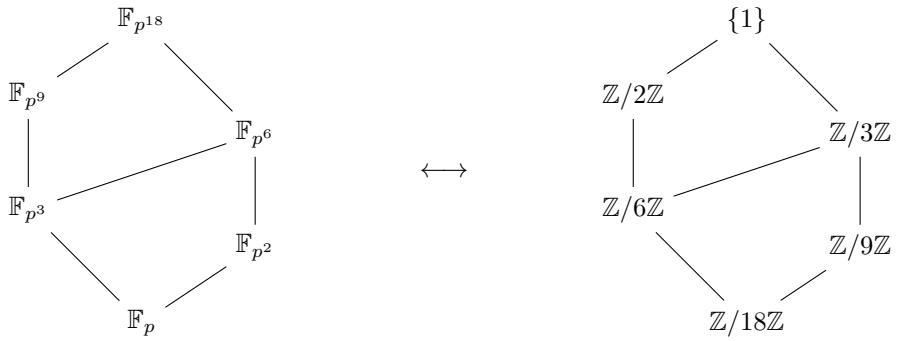
$$\sigma_1 \colon \alpha \longmapsto \alpha,\ \sigma_2 \colon \alpha \longmapsto -\alpha,\ \sigma_3 \colon \alpha \longmapsto \beta,\ \sigma_4 \colon \alpha \longmapsto -\beta.$$

Computations at α show that $\sigma_3^2(\alpha) = -\alpha$, so $\sigma_3^2 \neq \mathrm{id}_L$, but $\sigma_3^3(\alpha) = -\beta$ and hence $\sigma_3^4(\alpha) = \alpha$. So α has order 4 and is then a generator of $\mathrm{Gal}(f) = \mathrm{Gal}(L/\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$.

(iii) Since $\mathrm{Gal}(f)$ has a unique subgroup of order two, generated by σ_2, L has a unique subfield K of order 2 over $\mathbb{Q}$. Since $\alpha^2 = 6+3\sqrt{2}$, we see that $\mathbb{Q}(\alpha^2) = \mathbb{Q}(\sqrt{2})$, and $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$, so $K = \mathbb{Q}(\sqrt{2})$. The Galois correspondence is then



Exercise 10. We proceed exactly as in the example (iv) of section 4.3. One gets



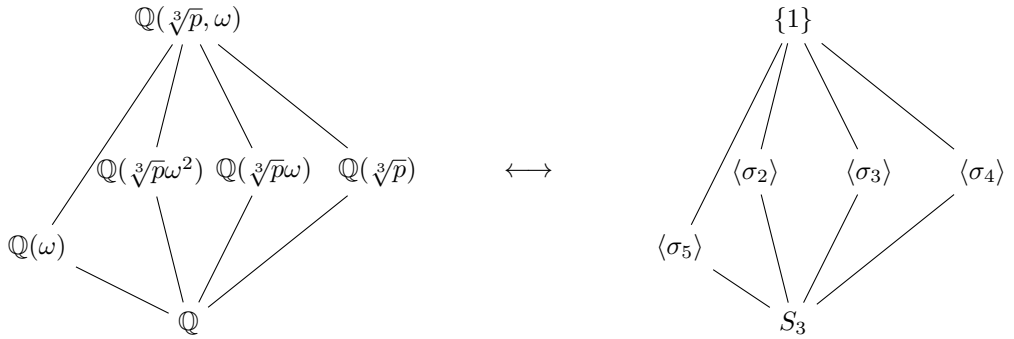
Exercise 11. Let p be a prime number, and let L be a splitting field of $f = X^3 - p$ over $\mathbb{Q}$.
The extension $L/\mathbb{Q}$ is indeed Galois, and the roots of f are $\sqrt[3]{p}$, $\sqrt[3]{p}\omega$, $\sqrt[3]{p}\omega^2$, where ω is a primitive cubic root of 1. Therefore $L = \mathbb{Q}(\sqrt[3]{p}, \omega)$, and thus $[L:\mathbb{Q}] = 6$. It follows that $|\mathrm{Gal}(f)| = 6$, so $\mathrm{Gal}(f) \simeq \mathbb{Z}/6\mathbb{Z}$ or $\mathrm{Gal}(f) \simeq S_3$. But L contains three cubic subfields, $\mathbb{Q}(\sqrt[3]{p})$, $\mathbb{Q}(\sqrt[3]{p}\omega)$, $\mathbb{Q}(\sqrt[3]{p}\omega^2)$, and one quadratic subfield $\mathbb{Q}(\omega)$, so by Galois correspondence $\mathrm{Gal}(f) = \mathrm{Gal}(L/\mathbb{Q})$ contains three subgroups of index 3 and one subgroup of index 2. Thus $\mathrm{Gal}(f) \simeq S_3$. We can also write down explicitly all $\mathbb{Q}-$automorphisms, by their effect on the roots of f. We get

$$\begin{aligned}
\sigma_1 &\colon \sqrt[3]{p} \longmapsto \sqrt[3]{p},\ \sqrt[3]{p}\omega \longmapsto \sqrt[3]{p}\omega,\ \sqrt[3]{p}\omega^2 \longmapsto \sqrt[3]{p}\omega^2\\
\sigma_2 &\colon \sqrt[3]{p} \longmapsto \sqrt[3]{p}\omega,\ \sqrt[3]{p}\omega \longmapsto \sqrt[3]{p},\ \sqrt[3]{p}\omega^2 \longmapsto \sqrt[3]{p}\omega^2\\
\sigma_3 &\colon \sqrt[3]{p} \longmapsto \sqrt[3]{p}\omega^2,\ \sqrt[3]{p}\omega \longmapsto \sqrt[3]{p}\omega,\ \sqrt[3]{p}\omega^2 \longmapsto \sqrt[3]{p}\\
\sigma_4 &\colon \sqrt[3]{p} \longmapsto \sqrt[3]{p},\ \sqrt[3]{p}\omega \longmapsto \sqrt[3]{p}\omega^2,\ \sqrt[3]{p}\omega^2 \longmapsto \sqrt[3]{p}\omega\\
\sigma_5 &\colon \sqrt[3]{p} \longmapsto \sqrt[3]{p}\omega,\ \sqrt[3]{p}\omega \longmapsto \sqrt[3]{p}\omega^2,\ \sqrt[3]{p}\omega^2 \longmapsto \sqrt[3]{p}\\
\sigma_6 &\colon \sqrt[3]{p} \longmapsto \sqrt[3]{p}\omega^2,\ \sqrt[3]{p}\omega \longmapsto \sqrt[3]{p},\ \sqrt[3]{p}\omega^2 \longmapsto \sqrt[3]{p}\omega
\end{aligned}$$

and the corresponding fixed fields are

$$L^{\langle\sigma_2\rangle} = \mathbb{Q}(\sqrt[3]{p}\omega^2),\ L^{\langle\sigma_3\rangle} = \mathbb{Q}(\sqrt[3]{p}\omega),\ L^{\langle\sigma_4\rangle} = \mathbb{Q}(\sqrt[3]{p}),\ L^{\langle\sigma_5\rangle} = \mathbb{Q}(\omega) = L^{\langle\sigma_6\rangle}.$$

Therefore the Galois correspondence takes the form



Exercise 12. Let $\eta = e^{i\frac{2\pi}{5}}$ be a root of $X^5 - 1 = (X-1)(X^4 + X^3 + X^2 + X + 1)$. By a result in the first chapter (and also in the last chapter below), $f = X^4 + X^3 + X^2 + X + 1$ is irreducible over $\mathbb{Q}$ and is therefore the minimal polynomial of η over $\mathbb{Q}$. Also $L = \mathbb{Q}(\eta)$ is a splitting field for f, as any 5-th root of unity is a power of η. In particular, $[L:\mathbb{Q}] = \deg(f) = 4$, $L/\mathbb{Q}$ is a Galois extension, and $|\mathrm{Gal}(L/\mathbb{Q})| = 4$. Let us now define

$$\begin{aligned}\sigma\colon L &\longrightarrow L\\ \eta &\longmapsto \eta^2.\end{aligned}$$

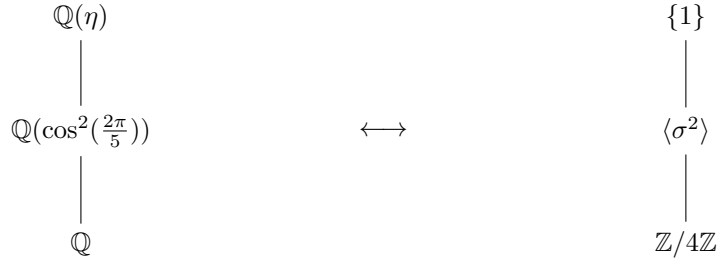
Then we compute $\sigma^2(\eta) = \eta^4 = -\eta^3 - \eta^2 - \eta - 1$, $\sigma^3(\eta) = \eta^8 = \eta^3$ and $\sigma^4(\eta) = \eta$, showing that $\mathrm{Gal}(L/\mathbb{Q}) = \langle\eta\rangle \simeq \mathbb{Z}/4\mathbb{Z}$. Hence, there is a unique intermediate subfield between $\mathbb{Q}$ and L, corresponding to the subgroup $\langle\sigma^2\rangle$ of $\mathrm{Gal}(L/\mathbb{Q})$. To find it, we proceed as in Example (v) of section 4.3. If $x = a + b\eta + c\eta^2 + d\eta^3 \in L$ is fixed by σ^2, then

$$a + b\eta + c\eta^2 + d\eta^3 = x = \sigma^2(x) = a + b\eta^4 + c\eta^3 + d\eta^2 = (a-b) - b\eta + (d-b)\eta^2 + (c-b)\eta^3$$

by using the relation $\eta^4 = -\eta^3 - \eta^2 - \eta - 1$. This equality then implies $b = 0$ and $c = d$, so x must take the form $x = a + c\eta^2 + c\eta^3 = a + c(\eta^2 + \eta^{-2}) \in \mathbb{Q}(\eta^2 + \eta^{-2})$. This proves that $L^{\langle\sigma^2\rangle} \subset \mathbb{Q}(\eta^2 + \eta^{-2})$, and since these fields both have degree 2 over $\mathbb{Q}$, they actually coincide. Finally, we can also compute

$$\eta^2 + \eta^{-2} = \eta^2 + \eta^{-2} + 2 - 2 = (\eta + \eta^{-1})^2 - 2 = \left(2\cos\left(\frac{2\pi}{5}\right)\right)^2 - 2 = 4\cos^2\left(\frac{2\pi}{5}\right) - 2$$

and so $\mathbb{Q}(\eta^2 + \eta^{-2}) = \mathbb{Q}(\cos^2(\frac{2\pi}{5}))$. The Galois correspondence takes then the form



Exercise 13. Consider $f = X^6 - 2 \in \mathbb{Q}[X]$.
First, f is irreducible in $\mathbb{Q}[X]$ by Eisenstein's criterion, and its roots in $\mathbb{C}$ are products of $\sqrt[6]{2}$ and $\omega := e^{i\frac{\pi}{3}}$. It follows that $L = \mathbb{Q}(\sqrt[6]{2},\omega)$ is a splitting field of f over $\mathbb{Q}$. Moreover, we compute

$$[L:\mathbb{Q}] = [\mathbb{Q}(\sqrt[6]{2})(\omega) : \mathbb{Q}(\sqrt[6]{2})][\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 2 \cdot 6 = 12$$

and since $L/\mathbb{Q}$ is Galois, we get $|\mathrm{Gal}(f)| = |\mathrm{Gal}(L/\mathbb{Q})| = [L:\mathbb{Q}] = 12$. We define two $\mathbb{Q}-$automorphisms σ and τ by

$$\begin{aligned}\sigma(\sqrt[6]{2}) &= \sqrt[6]{2}\omega,\ \sigma(\omega) = \omega\\ \tau(\sqrt[6]{2}) &= \sqrt[6]{2},\ \tau(\omega) = \omega^{-1} = \omega^5.\end{aligned}$$

Computations at $\sqrt[6]{2}$ and ω show that $\sigma^6 = \tau^2 = \mathrm{id}_L$ and $\tau\sigma\tau = \sigma^{-1}$. We can therefore conclude that $\mathrm{Gal}(f) \simeq D_6$, the diedral group of order 12.

Exercise 14. (i) Since K is perfect (Corollary 3.26), L/K is separable by Proposition 3.24. It is furthermore normal by definition of L. If $[L:K] := n < \infty$, then L would be an $\mathbb{F}_p-$vectorspace of dimension n, *i.e.* L would be $\mathbb{F}_{p^n}$, in particular L would be finite. It is impossible since L is algebraically closed and thus infinite. So $[L:K] = \infty$.

(ii) We pretend that $L^H = K$.
$\subseteq$: If $x \in L^H$, then in particular x is fixed by σ, meaning that $x^p = x$, and then $x \in \mathbb{F}_p = K$.
$\supseteq$: Conversely, if $x \in K$, then x is fixed by σ, and so by every element in H since they are all powers of σ. Hence $x \in L^H$.

(iii) Let $L' = \bigcup_{n\geq 0} \mathbb{F}_{p^{2^n}}$. Since 2^n divides $(2^n)!$, we have $\mathbb{F}_{p^{2^n}} \subset \mathbb{F}_{p^{(2^n)!}}$ and it follows that $L' \subset L$. If the reverse inclusion holds, it implies that $\mathbb{F}_{p^{3!}} \subset \mathbb{F}_{p^{2^n}}$ for a certain $n \geq 0$. As $\mathbb{F}_{p^{3!}}$ contains $\mathbb{F}_{p^3}$, we also have that $\mathbb{F}_{p^3} \subset \mathbb{F}_{p^{2^n}}$. This implies that 3 divides 2^n, which is of course excluded. Thus $L' \neq L$.

(iv) First, L/L' is indeed Galois. If $\mathrm{Gal}(L/L')$ is trivial, then $L' = L^{\mathrm{Gal}(L/L')} = L$, which contradicts the previous point.

(v) Let $\pi \in \mathrm{Gal}(L/L') \setminus \{\mathrm{id}_L\}$. Then $\pi \notin H$. If it is the case, then $\pi = \sigma^k$ for some $k \geq 1$, and $\pi(a) = a^{p^k}$ for all $a \in L$. The fixed field of π consists then of all $a \in L$ such that $a = a^{p^k}$, and this fixed field is contained in $\mathbb{F}_{p^k}$, in particular it is finite. This implies that L' is finite, which is absurd. Hence $\pi \notin H$.
For the second claim, if $H = \mathrm{Gal}(L/K)$, then $\mathrm{Gal}(L/L') \leqslant \mathrm{Gal}(L/K) = H$, which contradicts what we just showed.
(vi) Suppose that there exists $K \subset M \subset L$ with $\mathrm{Gal}(L/M) = H$. It follows that

$$M = L^{\mathrm{Gal}(L/M)} = L^H = K$$

and thus $H = \mathrm{Gal}(L/M) = \mathrm{Gal}(L/K)$, which contradicts (v).

Exercise 15. Recall that if $\sigma \in S_n$ and $\tau = (i_1 \dots i_k)$, then $\sigma\tau\sigma^{-1} = (\sigma(i_1) \dots \sigma(i_k))$. Now denote $H \subset S_n$ the subgroup generated by (12) and $(12\dots n)$. Conjugating (12) by $(12\dots n)$, we see that H contains (23). Likewise, conjugating (23) by $(12\dots n)$, H contains (34). The same reasoning shows that in fact H contains all transpositions of the form $(i\ i+1)$. Now H contains also $(12)(23) = (13)$, and then $(13)(34) = (14), \dots, (1\ n-1)(n-1\ n) = (1n)$, *i.e.* all transpositions of the form $(1i)$, $1 \leq i \leq n$. For any $i \neq j$, one has

$$(ij) = (1i)(1j)(1i)$$

and this implies that H contains all transpositions of S_n. As they generate S_n, we conclude that $H = S_n$.

Exercise 16. The symmetric group S_3 has 6 elements, and we enumerate all its subgroups: $\{(1), (12)\}$, $\{(1), (13)\}$, $\{(1), (23)\}$, $\{(1), (123), (132)\} = A_3$, and S_3. The only transitive subgroups in this list are A_3 and S_3.

Exercise 17. Let H be a transitive subgroup of S_n containing a transposition and a $(n-1)-$cycle. Up to relabeling, we may assume the cycle is $(12\dots n-1)$, and the transposition is (ij) for some $i, j \in \{1, \dots, n\}$. As H is transitive, there is σ so that $\sigma(i) = n$, and conjugating (ij) by σ, we see that H contains a transposition of the form (kn), $1 \leq k < n$. Conjugating the latter with powers of $(12\dots n-1)$ proves that H contains in fact all transpositions of the form (rn), $1 \leq r < n$, and therefore $H = S_n$.

Exercise 18. First consider $f = X^3 - X - 1$. Its reduction modulo 2 is $X^3 + X + 1$, which is irreducible in $\mathbb{F}_2[X]$, because it has no roots in $\mathbb{F}_2$ and has degree 3. Hence $X^3 - X - 1$ is irreducible in $\mathbb{Q}[X]$. Its discriminant $\Delta_f = -4(-1)^3 - 27 \cdot (-1)^2 = -23$ is not a square in $\mathbb{Q}$, so $\mathrm{Gal}(f) \simeq S_3$. Next we see that $f = X^3 - 2X - 1$ is not irreducible in $\mathbb{Q}[X]$, because -1 is a root of f. We have

$$f = (X+1)(X^2 - X - 1)$$

and the roots of the second polynomial are $\frac{1+\sqrt{5}}{2}$ and $\frac{1-\sqrt{5}}{2}$. Hence $\mathrm{Gal}(f) = \mathrm{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$. Let's turn now to $f = X^3 - 3X - 1$. As before, f is easily be seen to be irreducible in $\mathbb{Q}[X]$, and $\Delta_f = -4(-3)^3 - 27 \cdot (-1)^2 = 81 = 9^2$ is a square in $\mathbb{Q}$, so $\mathrm{Gal}(f) \simeq A_3$. The reasoning for the other polynomials is very similar.

Exercise 19. Let $k \in \mathbb{Z}$, and $a := k^2 + k + 7$.
First we observe that k and k^2 have the same parity, so adding 7 makes a always odd. Therefore, reducing $f := X^3 - aX + a$ modulo 2 one has $X^3 + X + 1$, which is irreducible in $\mathbb{F}_2[X]$, so f is irreducible in $\mathbb{Q}[X]$. Next we compute that $\Delta_f = -4(-a)^3 - 27a^2 = 4a^3 - 27a^2 = a^2(4a - 27)$, so it is enough to show $4a - 27$ is a perfect square in $\mathbb{Q}$. But

$$4a - 27 = 4(k^2 + k + 7) - 27 = 4k^2 + 4k + 1 = (2k+1)^2$$

and then $\Delta_f = (a(2k+1))^2$ is a square in $\mathbb{Q}$, so $\mathrm{Gal}(f) \simeq A_3$ by corollary 4.17.

Exercise 20. (i) First of all, $f = X^3 - 7X - 1$ is irreducible in $\mathbb{Q}[X]$ since it has degree 3 and no roots in $\mathbb{Q}$. Its discriminant is $\Delta_f = -4(-7)^3 - 27(-1)^2 = 1345$, which is not a square in $\mathbb{Q}$, so $\mathrm{Gal}(f) \simeq S_3$ by corollary 4.17.

(*ii*) The polynomial $X^3 - 7X^2 + 14X - 7$ is irreducible by Eisenstein, and we compute

$$\Delta_f = (-7)^2 \cdot 14^2 + 18(-7)^2 \cdot 14 - 4 \cdot 14^3 - 4 \cdot (-7)^4 - 27 \cdot (-7)^2 = 11025 - 10976 = 49 = 7^2$$

and thus $\mathrm{Gal}(X^3 - 7X^2 + 14X - 7) \simeq A_3$.

(*iii*) We remark that 1 is a root of $X^3 - 7X^2 + 14X - 8$, and this polynomial factors as $(X-1)(X^2 - 6X + 8)$. In fact, also the second polynomial has integer roots, namely 2 and 4. It then follows that $\mathrm{Gal}(X^3 - 7X^2 + 14X - 8) \simeq \{1\}$.

(*iv*) Here as well, one gets $\mathrm{disc}(X^3 - X^2 - 2X + 1) = 49 = 7^2$, and so $\mathrm{Gal}(X^3 - X^2 - 2X + 1) \simeq A_3$ by corollary 4.17.

Additionally, over $\mathbb{F}_5$, the discriminant of $X^3 + X + 1$ is $-4 - 27 = -31 = 4 = 2^2$, so its Galois group is isomorphic to A_3.

Exercise 23. Let K be a field of characteristic different than 2, and $f = X^4 + bX^2 + d \in K[X]$ be irreducible.
We start by computing the cubic resolvant of f. We get

$$R_f = X^3 - bX^2 - 4dX + 4bd$$

and we see that $b \in K$ is a root of it. Furthermore we can factor $R_f = (X-b)(X^2 - 4d)$. Using the hypothesis, we write $d = \delta^2$ for some $\delta \in K$, and hence

$$R_f = (X-b)(X^2 - 4d) = (X-b)(X^2 - 4\delta^2) = (X-b)(X - 2\delta)(X + 2\delta)$$

splits completely over K, as $2\delta \neq -2\delta$. Then we may apply Theorem 4.21 to get $\mathrm{Gal}(f) \simeq V$.

Exercise 24. Let $p \in \mathbb{Z}$ be prime, and $f = X^n - p \in \mathbb{Q}[X]$.
First, f is irreducible by Eisenstein. Let K be a splitting field of f over $\mathbb{Q}$. If $\mathrm{Gal}(f) = \mathrm{Gal}(K/\mathbb{Q})$ is abelian, then all its subgroups are normal, and hence all intermediate fields between $\mathbb{Q}$ and K are normal extensions of $\mathbb{Q}$. Then $\mathbb{Q}(\sqrt[n]{p}/\mathbb{Q})$ is normal, which is excluded: indeed f has a root in $\mathbb{Q}(\sqrt[n]{p})$, but does not split there. More generally, if $f \in \mathbb{Q}[X]$ is irreducible with at least one real root a, then its splitting field L contains the subfield $\mathbb{Q}(a) \subset \mathbb{R}$. This subfield cannot be a normal extension of $\mathbb{Q}$ since it contains one root of f but others are missing, namely the complex ones. Hence the corresponding subgroup in $\mathrm{Gal}(L/\mathbb{Q})$ cannot be normal, and $\mathrm{Gal}(L/\mathbb{Q}) = \mathrm{Gal}(f)$ is not abelian.

5 Applications of Galois theory

Exercise 1. (*i*) From example (*v*) in section 4.3, we know explicitely each element of $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$ and its effect on $\sqrt[4]{2}$ and i. We can therefore compute the orbit of $\sqrt[4]{2} + i$ under the action of $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q})$, to get

$$\begin{aligned}
r(\sqrt[4]{2} + i) &= i\sqrt[4]{2} + i \\
r^2(\sqrt[4]{2} + i) &= -\sqrt[4]{2} + i \\
r^3(\sqrt[4]{2} + i) &= -i\sqrt[4]{2} + i \\
s(\sqrt[4]{2} + i) &= \sqrt[4]{2} - i \\
rs(\sqrt[4]{2} + i) &= i\sqrt[4]{2} - i \\
r^2s(\sqrt[4]{2} + i) &= -\sqrt[4]{2} - i \\
r^3s(\sqrt[4]{2} + i) &= -i\sqrt[4]{2} - i
\end{aligned}$$

in addition of the identity which sends $\sqrt[4]{2}+i$ to itself. This list is composed of 8 different elements, and $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = 8$, so $\sqrt[4]{2} + i$ is a primitive element of $\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}$ by Theorem 5.1.

(*ii*) Likewise, we have

$$\begin{aligned}
r(i\sqrt[4]{2} + \sqrt[4]{2}) &= -\sqrt[4]{2} + i\sqrt[4]{2} \\
r^2(i\sqrt[4]{2} + \sqrt[4]{2}) &= -i\sqrt[4]{2} - \sqrt[4]{2} \\
r^3(i\sqrt[4]{2} + \sqrt[4]{2}) &= -i\sqrt[4]{2} + \sqrt[4]{2} \\
s(i\sqrt[4]{2} + \sqrt[4]{2}) &= -i\sqrt[4]{2} + \sqrt[4]{2} \\
rs(i\sqrt[4]{2} + \sqrt[4]{2}) &= i\sqrt[4]{2} + \sqrt[4]{2} \\
r^2s(i\sqrt[4]{2} + \sqrt[4]{2}) &= -\sqrt[4]{2} + i\sqrt[4]{2}
\end{aligned}$$

$$r^3 s(i\sqrt[4]{2} + \sqrt[4]{2}) = -i\sqrt[4]{2} - \sqrt[4]{2}$$

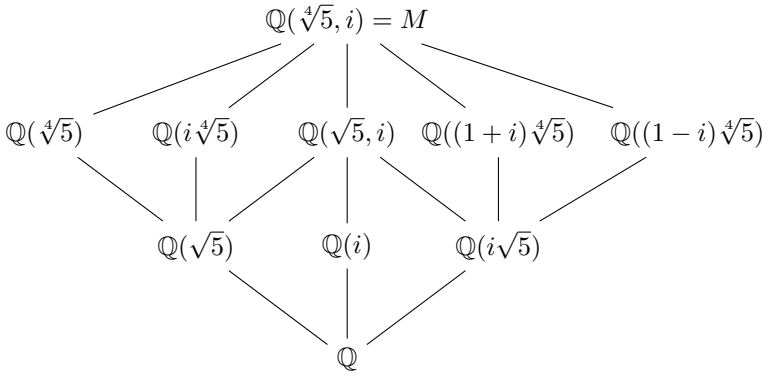
so the orbit of $i\sqrt[4]{2} + \sqrt[4]{2}$ counts 4 elements, and Theorem 5.1 indicates $i\sqrt[4]{2} + \sqrt[4]{2}$ is not a primitive element for $\mathbb{Q}(\sqrt[4]{2}, i)$. Moreover, it has degree 4 over $\mathbb{Q}$, and we see that

$$(i\sqrt[4]{2} + \sqrt[4]{2})^4 = ((1+i)\sqrt[4]{2})^4 = -8$$

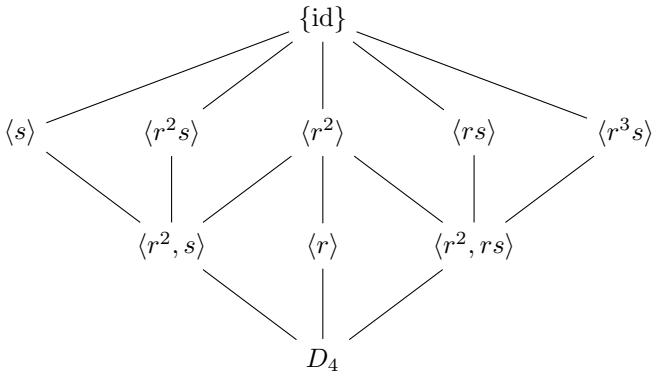
so $X^4 + 8$ has $i\sqrt[4]{2} + \sqrt[4]{2}$ for root. It is unitary and has degree 4, so it is its minimal polynomial.

Exercise 6. Recall the following corollary of Lagrange's theorem in group theory: if G is a finite group, and $g \in G$, then $g^{|G|} = e_G$. We apply it with $G = (\mathbb{Z}/n\mathbb{Z})^*$ and $g = [a] \in G$ since a is prime with n. Since $|G| = \varphi(n)$, we indeed get $a^{\varphi(n)} \equiv 1 \mod n$.

Exercise 7. (i) Let $a := \sqrt[4]{5} \in \mathbb{C}$, $b := a + ia$, and M the normal closure of $\mathbb{Q}(b)/\mathbb{Q}$.
We are highly inspire by the example (v) in section 4.3. Here we get $M = \mathbb{Q}(a, i)$ to be the splitting field of $f = X^4 - 5 \in \mathbb{Q}[X]$, which is irreducible by Eisenstein. One can work out readily the same arguing, to see that the Galois group of f is diedral of order 8, get a subfield lattice of the form



and the corresponding subgroups of D_4



In particular, $M/\mathbb{Q}$ is neither cyclic nor abelian. However, D_4 is solvable (actually even nilpotent), so $M/\mathbb{Q}$ is sovable.

(ii) We note that $L = \mathbb{Q}(i)$ contains a primitive root of unity, so $\mathrm{Gal}(M/L)$ is cyclic by Theorem 5.16. Its order is the degree of the extension M/L, which is indeed 4. Alternatively, we can directly look at the subgroups of D_4 of order 4: $\langle r \rangle$, $\langle r^2, s \rangle$ and $\langle r^2, rs \rangle$. Among these, just the first one is cyclic, and corresponds indeed to $\mathbb{Q}(i)$ by the diagram.

Exercise 9. (i) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is obviously an abelian extension of $\mathbb{Q}$.

(ii) D_4 is nilpotent by not abelian, so any Galois extension of $\mathbb{Q}$ with D_4 as Galois group does the job. For instance, one can consider L the splitting field of $X^4 - 2$ over $\mathbb{Q}$, as in example (v) of section 4.3.

(iii) Consider L the splitting field of $X^3 - 2$ over $\mathbb{Q}$. Then $\mathrm{Gal}(L/\mathbb{Q}) \simeq S_3$ is solvable, but not nilpotent.

(iv) By Theorem 4.10, any finite Galois extension of $\mathbb{F}_p$ is cyclic, in particular abelian, nilpotent and solvable. Therefore, similar examples to (ii) and (iii) cannot exist.

Exercise 10. We can consider for instance $K = \mathbb{Q}$ and L a splitting field for $X^3 - 2$ over K. We already saw that $\mathrm{Gal}(L/K) \simeq S_3$ which is obviously not cyclic.

Exercise 11. Let $f = X^6 - 2 \in \mathbb{Q}[X]$.
(i) We already determined at exercise 12 of chapter 4 that $L = \mathbb{Q}(\sqrt[6]{2}, \omega)$ is a splitting field for f over $\mathbb{Q}$, where $\omega = \exp(\frac{\pi i}{3})$.

(ii) Moreover, in the same exercise we computed $|\mathrm{Gal}(f)| = |\mathrm{Gal}(L/\mathbb{Q})| = 12$. It remains to find $\mathrm{Gal}(L/\mathbb{Q}(\omega))$. By theorem 4.7, since $\mathbb{Q}(\omega)/\mathbb{Q}$ is normal, $\mathrm{Gal}(L/\mathbb{Q}(\omega))$ is a normal subgroup of $\mathrm{Gal}(L/\mathbb{Q})$, and we have an isomorphism

$$\mathbb{Z}/2\mathbb{Z} \simeq \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \simeq \mathrm{Gal}(L/\mathbb{Q})/\mathrm{Gal}(L/\mathbb{Q}(\omega)) \simeq D_6/\mathrm{Gal}(L/\mathbb{Q}(\omega)).$$

From there it follows $\mathrm{Gal}(L/\mathbb{Q}(\omega))$ has order 6 and index 2. There are three such subgroups in D_6, namely

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

However, only the first one in this list has fixed field $\mathbb{Q}(\omega)$. We conclude then $\mathrm{Gal}(L/\mathbb{Q}(\omega)) = \langle\sigma\rangle \simeq \mathbb{Z}/6\mathbb{Z}$.

Exercise 13. Let L_1/K, L_2/K be finite and Galois.
(i) By definition, $L_1L_2 = K(L_1 \cup L_2)$ is obtained from K by adjoining separable elements, since L_1 and L_2 are separable over K. By Corollary 3.31(ii), L_1L_2 is separable over K. Now, since L_1/K and L_2/K are normal, by Theorem 3.14, there exists $f_1, f_2 \in K[X] \setminus K$ such that L_1 is the splitting field of f_1 over K and L_2 is the splitting field of L_2 over K. In particular, $L_1 = K(a_1, \ldots, a_n)$ and $L_2 = K(b_1, \ldots, b_m)$, where $a_1, \ldots, a_n$ (resp. $b_1, \ldots, b_m$) are the roots of f_1 (resp. f_2) in L_1 (resp. L_2). It follows that $L_1L_2 = K(a_1, \ldots, a_n, b_1, \ldots, b_m)$ is the splitting field of f_1f_2 over K. Again by Theorem 3.14, L_1L_2 is normal over K. Hence L_1L_2/K is Galois.

(ii) We define

$$\begin{aligned} \varphi\colon \mathrm{Gal}(L_1L_2/K) &\longrightarrow \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K) \\ \sigma &\longmapsto (\sigma_{|L_1}, \sigma_{|L_2}) \end{aligned}$$

Clearly, φ is a well-defined group homomorphism. It is also injective, because if $\varphi(\sigma) = (\mathrm{id}_{L_1}, \mathrm{id}_{L_2})$, then σ is the identity on L_1 and L_2, and since these fields generate L_1L_2, σ is the identity on L_1L_2. In particular, $\mathrm{Gal}(L_1L_2/K)$ is (isomorphic to) a subgroup of $\mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$.

(iii) If both $\mathrm{Gal}(L_1/K)$ and $\mathrm{Gal}(L_2/K)$ are abelian, then so is their direct product, and then so is $\mathrm{Gal}(L_1L_2/K)$ since every subgroup of an abelian group is abelian.

(iv) The same is not true for cyclic extensions. For instance $L_1 = \mathbb{Q}(\sqrt{2})$ and $L_2 = \mathbb{Q}(\sqrt{3})$ are both cyclic over $\mathbb{Q}$, but $L_1L_2 = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ is not cyclic over $\mathbb{Q}$, since it has Galois group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. However, the same is true for solvable extensions, with the same reasoning as in (iii): direct products and subgroups of solvable groups are solvable.

Exercise 14. (i) θ is well defined because if $\sigma \in \mathrm{Gal}(L_1L_2/L_2)$ fixes L_2, it fixes in particular $L_1 \cap L_2$. It is furthermore a group homomorphism since $(\sigma\tau)_{|L_1} = \sigma_{|L_1}\tau_{|L_1}$. Finally, if $\theta(\sigma) = \mathrm{id}_{L_1}$, then $\sigma \in \mathrm{Gal}(L_1L_2/L_2)$ fixes both L_1 and L_2, so σ fixes L_1L_2, *i.e.* $\sigma = \mathrm{id}_{L_1L_2}$.
(ii) The equality $L_1^{\mathrm{Im}(\theta)} = L_1 \cap L_2$ is straightforward. From (i) and the first isomorphism theorem it then follows that

$$\mathrm{Gal}(L_1L_2/L_2) \simeq \mathrm{Im}(\theta) = \mathrm{Gal}(L_1/L_1^{\mathrm{Im}(\theta)}) = \mathrm{Gal}(L_1/L_1 \cap L_2).$$

(iii) We have

$$\begin{aligned} [L_1L_2 : K] &= [L_1L_2 : L_1 \cap L_2][L_1 \cap L_2 : K] \\ &= [L_1L_2 : L_2][L_2 : L_1 \cap L_2][L_1 \cap L_2 : K] \\ &= [L_1 : L_1 \cap L_2][L_2 : L_1 \cap L_2][L_1 \cap L_2 : K] \\ &= [L_1 : K][L_2 : L_1 \cap L_2] \\ &= [L_1 : K][L_2 : L_1 \cap L_2]\frac{[L_1 \cap L_2 : K]}{[L_1 \cap L_2 : K]} \\ &= \frac{[L_1 : K][L_2 : K]}{[L_1 \cap L_2 : K]} \end{aligned}$$

by using multiplicativity of the degrees several times, and the isomorphism in (ii) to get the third equality.

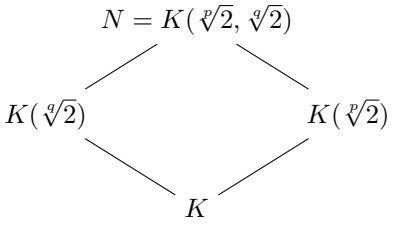
Exercise 16. Let p, q be two distinct primes, $n := pq$ and ξ be a primitive $n-$th root of unity. Set $K := \mathbb{Q}(\xi)$, $f = (X^p - 2)(X^q - 2)$ and N the splitting field of f over K. In $\mathbb{C}$, the roots of f are $\sqrt[p]{2}$, $\sqrt[p]{2}\exp(\frac{2\pi i}{p}), \ldots, \sqrt[p]{2}\exp(\frac{2(p-1)\pi i}{p})$ and $\sqrt[q]{2}$, $\sqrt[q]{2}\exp(\frac{2\pi i}{q}), \ldots, \sqrt[q]{2}\exp(\frac{2(q-1)\pi i}{q})$. Since $\xi = \exp(\frac{2\pi i}{pq})$, we see that

$$\exp\left(\frac{2\pi i}{p}\right) = \xi^q \in K,\ \exp\left(\frac{2\pi i}{q}\right) = \xi^p \in K$$

and hence we only need to add $\sqrt[p]{2}$ and $\sqrt[q]{2}$ to K to get N. Thus $N = K(\sqrt[p]{2}, \sqrt[q]{2})$. Finally we show $K(\sqrt[p]{2}, \sqrt[q]{2}) = K(\sqrt[pq]{2})$. The inclusion from the left to the right is clear, as $\sqrt[p]{2} = (\sqrt[pq]{2})^q$ and $\sqrt[q]{2} = (\sqrt[pq]{2})^p$. On the other hand, p and q are relatively prime, so their exists x, $y \in \mathbb{Z}$ such that $1 = px + qy$, and it follows that

$$\sqrt[pq]{2} = 2^{\frac{1}{pq}} = 2^{\frac{px+qy}{pq}} = 2^{\frac{x}{q}} 2^{\frac{y}{p}} = (\sqrt[p]{2})^y (\sqrt[q]{2})^x \in K(\sqrt[p]{2}, \sqrt[q]{2}).$$

We conclude that $K(\sqrt[pq]{2}) \subset K(\sqrt[p]{2}, \sqrt[q]{2})$, proving the desired equality. Then $N = K(\sqrt[pq]{2})$ and the theorem 5.16(i), which we may use since K contains a primitive root of unity, assures us N/K is cyclic. An alternative way, without appealing Bezout is the following. We showed $N = K(\sqrt[p]{2}, \sqrt[q]{2})$. So we have the diagram of fields

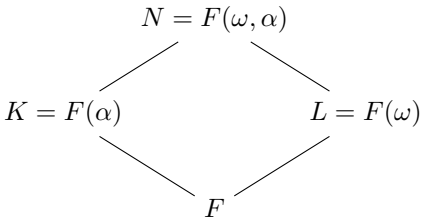


Again by Theorem 5.16, $K(\sqrt[p]{2})/K$ and $K(\sqrt[q]{2})/K$ are cyclic, respectively of degree p and q. Then $\mathrm{Gal}(K(\sqrt[p]{2})/K) \simeq \mathbb{Z}/p\mathbb{Z}$ and $\mathrm{Gal}(K(\sqrt[q]{2})/K) \simeq \mathbb{Z}/q\mathbb{Z}$. It follows that $\mathrm{Gal}(N/K) \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \simeq \mathbb{Z}/pq\mathbb{Z}$ is cyclic, where the last isomorphism is, again, due to the fact that p and q are relatively prime.

Exercise 17. (i) If ω is an $n-$th primitive root of unity, and $a = \alpha^n$, then the roots of $X^n - a$ are $\alpha, \omega\alpha, \omega^2\alpha, \ldots, \omega^{n-1}\alpha$, so $F(\omega, \alpha)$ is a splitting field for $X^n - a$.

(ii) Denote $N := F(\omega, \alpha)$, $K := F(\alpha)$ and $L := F(\omega)$. L is a splitting field of $X^n - 1$ over F, and since $\mathrm{char}(F) \nmid n$, the latter is also separable over F. This way, L/F is Galois. N/L is cyclic by Theorem 5.16(i), which we may use since L contains a primitive $n-$th root of unity and $\alpha^n = a$.

(iii) The hypothesis implies that $[L : F] = 2$, and $[N : L] = n$. The situation can be represented as



Now we argue that $[K : F] = n$ and $[N : K] = 2$. Since $\alpha^n = a$, we have $[K : F] \leq n$ and since ω is cancelled by a degree two polynomial over F, it is *a fortiori* cancelled by a degree two polynomial over K, and so $[N : K] \leq 2$. If $[K : F] < n$, then

$$2n = [L : F][N : L] = [N : F] = [N : K][K : F] < [N : K]n \leq 2n$$

which is absurd. Hence $[K : F] = n$ and also $[N : K] = 2$. Finally, we define first

$$\begin{aligned} \sigma \colon N &\longrightarrow N \\ \alpha &\longmapsto \omega\alpha \\ \omega &\longmapsto \omega \end{aligned}$$

and this allows us to see $\sigma \in \mathrm{Gal}(N/L) \leqslant \mathrm{Gal}(N/F)$. Similarly, we set

$$\begin{aligned} \tau \colon N &\longrightarrow N \\ \alpha &\longmapsto \alpha \\ \omega &\longmapsto \omega^{-1} \end{aligned}$$

and we get $\tau \in \mathrm{Gal}(N/K) \leqslant \mathrm{Gal}(N/F)$. It is clear that $\sigma^n = \tau^2 = \mathrm{id}_L$, and a computation at ω and α proves the relation $\tau\sigma\tau^{-1} = \sigma^{-1}$.

(iv) From (iii), we then have $\mathrm{Gal}(N/F) = \langle \sigma, \tau \mid \sigma^n = \tau^2 = 1, \tau\sigma\tau = \sigma^{-1} \rangle \simeq D_n$, the diedral group of order $2n$.

Exercise 18. (i) Let $f = X^5 - X^3 - 5X^2 + 5$. We see that $f(1) = 1 - 1 - 5 + 5 = 0$, so $f = (X - 1)g(X)$, where $g(X) \in \mathbb{Q}[X]$ is a polynomial of degree 4. Hence non-rationnal roots of f are non-rationnal roots of g, and since g is

of degree 4, its Galois group is (isomorphic to) a subgroup of S_4, and therefore is solvable. Then $g = 0$ is solvable by radicals thanks to Theorem 5.20, and then so is $f = 0$.

(*ii*) Let $f = X^5+2X^3+X^2+X+1$. Here f does not have an obvious root, but is reducible, since $f = (X^3+X+1)(X^2+1)$. Let us denote $L_1 = \mathbb{Q}(a_1, a_2, a_3)$ a splitting field of $X^3 + X + 1$ over $\mathbb{Q}$ and $L_2 = \mathbb{Q}(i)$ a splitting field of $X^2 + 1$ over $\mathbb{Q}$. By exercise 11, $L_1L_2 = \mathbb{Q}(a_1, a_2, a_3, i)$ is a splitting field for f over $\mathbb{Q}$, and $\mathrm{Gal}(f) = \mathrm{Gal}(L_1L_2/\mathbb{Q})$ is a subgroup of the direct product $\mathrm{Gal}(L_1/\mathbb{Q}) \times \mathrm{Gal}(L_2/\mathbb{Q})$. We see easily that $\mathrm{Gal}(L_1/\mathbb{Q}) \simeq S_3$ (for instance by computing the discriminant, or by using theorem 4.14) and $\mathrm{Gal}(L_2/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$. Hence $\mathrm{Gal}(f)$ is a subgroup of $S_3 \times \mathbb{Z}/2\mathbb{Z}$ which is solvable, so $\mathrm{Gal}(f)$ is solvable, and $f = 0$ is solvable by radicals. (In fact, we can directly conclude from $f = (X^3 + X + 1)(X^2 + 1)$, since these polynomials are both solvable by radicals.)

(*iii*) Here we denote $f = X^5 - 10X + 5$. We compute $f' = 5X^4 - 10 = 5(X^4 - 2)$, and we see this derivative has exactly 2 roots in $\mathbb{R}$, $\sqrt[4]{2}$ and $-\sqrt[4]{2}$, and exactly 2 roots in $\mathbb{C} \setminus \mathbb{R}$, $i\sqrt[4]{2}$ and $-i\sqrt[4]{2}$. Furthermore, one can does standard function analysis to get variations of f, and with the two real roots of the derivative, it implies f has at least three roots in $\mathbb{R}$. It can not have a fourth root in $\mathbb{R}$, since it would force f' to have an additional root in $\mathbb{R}$, which is excluded. Hence f has three real roots, two complex roots, and is irreducible by Eisenstein. Theorem 4.14 tells us then that $\mathrm{Gal}(f) \simeq S_5$, which is not solvable, so $f = 0$ is not solvable by radicals.

(*iv*) We already computed that $\mathrm{Gal}(X^6 - 2) \simeq D_6$, and since a diedral group is solvable, we get that $X^6 - 2 = 0$ is solvable by radicals.

(*v*) Denote $f = X^7 - X^5 - 4X^3 - X^2 + 4X + 1$. We remark that 1 and -1 are roots of f, and f factors as $f = (X - 1)(X + 1)(X^5 - 4X - 1)$. Exactly as in (*iii*) we show $\mathrm{Gal}(X^5 - 4X - 1) \simeq S_5$ is not solvable, and thus $f = 0$ is not solvable by radicals.

Exercise 19. (*i*) If $[N : \mathbb{Q}]$ is a power of 2, then $|\mathrm{Gal}(N/\mathbb{Q})|$ is a power of 2. By a standard result in group theory, we can find a chain of subgroups

$$\{e\} = G_0 \leqslant G_1 \leqslant \cdots \leqslant G_r = \mathrm{Gal}(N/\mathbb{Q})$$

such that $[G_{i+1} : G_i] = 2$ for all $i = 0, \ldots, r - 1$. By Galois correspondence, we then find a tower of extensions

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_r = N$$

with $[K_{i+1} : K_i] = 2$ for all $i = 0, \ldots, r - 1$. By Wantzel's theorem (theorem 5.29), we conclude that c is constructible.

(*ii*) Conversely, suppose that $c \in \mathbb{R}$ is constructible and algebraic over $\mathbb{Q}$. Then we can find a chain of subfields $\mathbb{Q} \subset K_1 \subset \cdots \subset K_m$ of succesive degree 2 extensions, with $c \in K_m$. Denote N the normal closure of $\mathbb{Q}(c)/\mathbb{Q}$. Consider $f \in \mathbb{Q}[X]$ the minimal polynomial of c over $\mathbb{Q}$. Then $N = \mathbb{Q}(\gamma_1 = c, \ldots, \gamma_s)$ where $\gamma_1 = c, \ldots, \gamma_s$ are the roots of f. Since c is constructible, and that $\mathbb{Q}(c)$ and $\mathbb{Q}(\gamma_i)$ are isomorphic as fields for all $i = 2, \ldots, s$, we deduce that in fact *all* roots of f are constructible. Then, suppose we find γ_2 in the last field appearing in a tower of the form $\mathbb{Q} \subset L_1 \subset \cdots \subset L_j$ with each extension of degree 2. That means $L_j = L_{j-1}(\sqrt{d_{j-1}})$ for some $d_{j-1} \in L_{j-1}$, and thus $L_r = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_r})$. We can then attach these elements to our original tower, and form

$$\mathbb{Q} \subset K_1 \subset \cdots \subset K_m \subset K_m(\sqrt{d_1}) \subset K_m(\sqrt{d_1}, \sqrt{d_2}) \subset \cdots \subset K_m(\sqrt{d_1}, \ldots, \sqrt{d_r}).$$

Each extension there is of degree 1 or 2, and is contained in N. Continuing analogously for each γ_i, we at the end finish with N, and we showed $[N : \mathbb{Q}]$ must be a power of 2.

Exercise 20. (*i*) If $\mathrm{Gal}(N/\mathbb{Q})$ is D_4 or of order 4 we can use point (*i*) of the previous exercise to directly conclude that c is contructible.

(*ii*) On the other hand, if $\mathrm{Gal}(N/\mathbb{Q})$ is either A_4 or S_4, we can use point (*ii*) of the same exercise to see that c is not constructible.

Exercise 21. Let $f = X^4 - 4X + 2 \in \mathbb{Q}[X]$.
(*i*) A rational root of f can only be ± 2, and we quickly check that $f(2), f(-2) \neq 0$.
Next we compute the derivative $f' = 4X^3 - 4 = 4(X - 1)(X^2 + X + 1)$, and we see it has only one root in $\mathbb{R}$. Moreover $f(0) = 2$, $f(1) = -1$ and $f(2) = 10$, so the intermediate values theorem assure us that f has at least two real distinct roots, one in $(0, 1)$ and an other in $(1, 2)$. Having a third root in $\mathbb{R}$ would force f' to have one more zero in $\mathbb{R}$, which is excluded. Thus f has exactly two real roots. Let us call them a_1 and a_2.

(*ii*) This follows directly from (*i*), as f is divisible by $(X - a_1)(X - a_2)$.

(*iii*) We have $X^4 - 4X + 2 = f = (X^2 + \alpha X + \beta)(X^2 + \gamma X + \delta)$, so by expanding the latter we get that $\gamma = -\alpha$, $b := \beta + \delta = \alpha^2$, $\alpha\delta + \beta\gamma = -4$ and $\beta\delta = 2$. Thus $\alpha\delta - \beta\alpha = -4$, so $(\delta - \beta)^2\alpha^2 = 16$ and then $b(\delta - \beta)^2 = 16$. We also

note that $(\delta-\beta)^2=(\delta+\beta)^2-4\beta\delta=b^2-8$. We get finally $b(b^2-8)=16$, so b is a root of a polynomial over $\mathbb{Q}$, which shows b is algebraic over $\mathbb{Q}$. Reducing modulo 5, we see that $X^3-8X-16$ is irreducible over $\mathbb{Q}$, so it is the minimal polynomial of b over $\mathbb{Q}$, and $[\mathbb{Q}(b):\mathbb{Q}]=3$.

(*iv*) Again, f is irreducible by Eisenstein, so it is the minimal polynomial of a_1 and a_2 over $\mathbb{Q}$. It then follows that $[\mathbb{Q}(a_1):\mathbb{Q}]=[\mathbb{Q}(a_2):\mathbb{Q}]=4$.
(*v*) If both a_1 and a_2 are constructible, then so is their product $a_1a_2=\beta$ by Proposition 5.26. It implies that also $\delta=\frac{2}{\beta}$ is constructible, and so $b=\beta+\delta$ is constructible. Then $[\mathbb{Q}(b):\mathbb{Q}]=3$ is a power of 2, which is absurd. Hence at least one of them is not constructible.

(*vi*) The two fields $\mathbb{Q}(a_1)$ and $\mathbb{Q}(a_2)$ are isomorphic, so if one of them is not constructible, then so is the other.

Exercise 23. The minimal polynomial of $\eta:=\exp(\frac{2\pi}{5})$ is the 5-th cyclotomic polynomial $X^4+X^3+X^2+X+1=0$. So

$$\eta^4+\eta^3+\eta^2+\eta+1=0.$$

Multiplying this equation by η^{-2} yields to

$$\eta^2+\eta+1+\eta^{-1}+\eta^{-2}=0$$

and by letting $\alpha:=\eta+\eta^{-1}=2\cos(\frac{2\pi}{5})$, the above exactly says $\alpha^2+\alpha-1=0$. Then $\cos(\frac{2\pi}{5})$ is a root of $4X^2+2X-1$, so its minimal polynomial is $X^2+\frac{1}{2}X-\frac{1}{4}$. For the second claim, we can explicitely compute the roots of $4X^2+2X-\frac{1}{4}$. These are $\frac{-1\pm\sqrt{5}}{4}$, and since $\cos(\frac{2\pi}{5})$ is positive, we indeed get $\cos(\frac{2\pi}{5})=\frac{-1+\sqrt{5}}{4}$.

(*ii*) The angle $\frac{2\pi}{5}$ can be trisected if and only if $\cos(\frac{2\pi}{15})$ is constructible, and this is also equivalent to construct a $15-$gon. We compute then

$$\varphi(15)=\varphi(3)\varphi(5)=2\cdot 2^2=2^3$$

which is a power of 2, so Theorem 5.32 tells us $\cos(\frac{2\pi}{15})$ is constructible. Thus $\frac{2\pi}{5}$ can be trisected.