Solutions to David A.Cox "Galois Theory"

Richard Ganaye

October 25, 2021

8 Chapter 8 : SOLVABILITY BY RADICALS

8.1 SOLVABLE GROUPS

Ex. 8.1.1 *Consider the groups A_4 and S_4.*

(a) Show that $\{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ is a normal subgroup of S_4.

(b) Show that A_4 and S_4 are solvable.

Proof. (a) Write $a = (1\,2)(3\,4), b = (1\,3)(2\,4), c = (1\,4)(2\,3)$. Note that e, a, b, c are even permutations, so $K = \{e, a, b, c\} \subset A_4$. They satisfy the relations

$$a^2 = b^2 = c^2 = e, ab = ba = c, ac = ca = b, bc = cb = a.$$

This gives the same Cayley table of the Klein's four-group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, where we write

$$e' = (0,0), a' = (1,0), b' = (0,1), c' = (1,1).$$

The mapping $(e \mapsto e', a \mapsto a', b \mapsto b', c \mapsto c')$ is an isomorphism.

If $\sigma \in S_4$, $\sigma a \sigma^{-1} = \sigma[(1\,2)(3\,4))]\sigma^{-1} = (\sigma(1)\,\sigma(2))(\sigma(3)\,\sigma(4)) \in K$, and the same is true for b and c, so K is normal in S_4 (a fortiori in A_4).

Conclusion: $K = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ is a normal subgroup of S_4 included in A_4, and K is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(b) So we obtain a chain

$$S_4 \supset A_4 \supset K \supset \langle a \rangle \supset \{e\},$$

- A_4 has index 2 in S_4, so A_4 is a normal subgroup of S_4, and $S_4/A_4 \simeq \mathbb{Z}/2\mathbb{Z}$.
- By part (a), we know that K is normal in A_4.

As $|A_4/K| = 3$, $A_4/K \simeq \mathbb{Z}/3\mathbb{Z}$.

- K being Abelian, $\langle a \rangle$ is normal in K, and $K/\langle a \rangle \simeq \mathbb{Z}/2\mathbb{Z}$.
- $\langle a \rangle / \{e\} \simeq \mathbb{Z}/2\mathbb{Z}$.

Conclusion: S_4 is solvable (and also A_4).

□

Ex. 8.1.2 *This exercise is concerned with the first part of the proof of Theorem 8.1.4.*

(a) Prove assertions (a)–(d) made in the proof of the theorem.

(b) Suppose that $\phi : M_1 \to M_2$ is an onto group homomorphism. If $|M_1| = p$, where p is prime, then prove that $|M_2| = 1$ or p.

(c) Explain how part (b) proves the assertion made in the text that $\tilde{G}_{i-1}/\tilde{G}_i$ either is trivial or has prime order.

Proof. Let G solvable, and H a normal subgroup of G. We must prove that G/H is solvable.

There exist subgroups G_i of G such that

$$\{e\} = G_n \subset \cdots \subset G_i \subset G_{i-1} \subset \cdots \subset G_0 = G,$$

where $G_i \lhd G_{i-1}$, and G_i/G_{i-1} is of prime order.

(a) Let $\pi : G \to G/H, g \mapsto gH$ the canonical projection, and $\tilde{G}_i = \pi(G_i)$.

- As $G_0 = G$, $\tilde{G}_0 = \pi(G) = G/H$ since π is surjective.
- As $G_n = \{e\}, \tilde{G}_n = \pi(\{e\}) = \{eH\} = \{\overline{e}\}$, where we write $\overline{e}$ the identity of G/H.
- We know that $G_i \lhd G_{i-1}$. Then we show that $\tilde{G}_i \lhd \tilde{G}_{i-1}$.

Let any $\overline{x} \in \tilde{G}_{i-1}$, and $\overline{y} \in \tilde{G}_i$, with $\overline{x} = xH, \overline{y} = yH, x \in G_{i-1}, y \in G_i$.

$\overline{x}\,\overline{y}\,\overline{x}^{-1} = xHyHx^{-1}H = xyx^{-1}H = zH$, where $z = xyx^{-1} \in G_i$, since $G_i \lhd G_{i-1}$.

Therefore $\overline{x}\,\overline{y}\,\overline{x}^{-1} = \pi(z) \in \pi(G_i) = \tilde{G}_i$. So $\tilde{G}_i \lhd \tilde{G}_{i-1}$.

- Let φ be the mapping

$$\varphi : \left\{ \begin{array}{ccc} G_{i-1} & \to & \tilde{G}_{i-1}/\tilde{G}_i \\ g & \mapsto & \pi(g)\tilde{G}_i \end{array} \right.$$

(if $g \in G_{i-1}, \pi(g) \in \tilde{G}_{i-1}$, thus $\pi(g)\tilde{G}_i \in \tilde{G}_{i-1}/\tilde{G}_i$).

If $g \in G_i, \pi(g) = gH \in \tilde{G}_i$, thus $\varphi(g) = \pi(g)\tilde{G}_i = \tilde{G}_i$, which is the identity of $\tilde{G}_{i-1}/\tilde{G}_i$, so $g \in \ker(\varphi)$. This proves

$$G_i \subset \ker(\varphi).$$

As $G_i \subset \ker(\varphi)$, if two elements g, g' of G_{i-1} are congruent modulo G_i, i.e. $gG_i = g'G_i$, then $g^{-1}g' \in G_i \subset \ker(\varphi)$, so g, g' have the same image by φ. Consequently $\varphi(g)$ depends only of the class gG_i of g in G_{i-1}/G_i.

The mapping $\overline{\varphi} : G_{i-1}/G_i \to \tilde{G}_{i-1}/\tilde{G}_i$ defined by $gG_i \mapsto \pi(g)\tilde{G}_i$ is so well defined, and is a group homomorphism.

Let $y = v\tilde{G}_i$ be any element of $\tilde{G}_{i-1}/\tilde{G}_i$, where $v \in \tilde{G}_{i-1}$, so $v = \pi(g)$ for some $g \in G_{i-1}$. Therefore $y = \pi(g)\tilde{G}_i = \varphi(g) = \overline{\varphi}(gG_i)$, so $\overline{\varphi}$ is surjective.

(b) Let $\phi : M_1 \to M_2$ be a surjective group homomorphism, and suppose that $|M_1| = p$ is prime.

Then $M_2 \simeq M_1/\ker(\phi)$. The order of the subgroup $\ker(\phi)$ of M_1 divides $|M_1| = p$, so $|\ker(\phi)| = 1$ or p, thus $|M_2| = |M_1|/|\ker(\phi)| = p$ or 1.

(c) By hypothesis $|G_{i-1}/G_i = p$ is prime. By part (b) applied to the surjective group homomorphism $\phi = \varphi : G_{i-1}/G_i \to \tilde{G}_{i-1}/\tilde{G}_i$, we know that $|\tilde{G}_{i-1}/\tilde{G}_i| = 1$ or p.

Therefore $\tilde{G}_{i-1}/\tilde{G}_i$ is trivial, or of prime order.

To conclude:

$$\{\overline{e}\} = \tilde{G}_n \subset \cdots \subset \tilde{G}_i \subset \tilde{G}_{i-1} \subset \cdots \subset \tilde{G}_0 = G/H,$$

with $\tilde{G}_i \lhd \tilde{G}_{i-1}, \tilde{G}_i/\tilde{G}_{i-1}$ trivial or of prime order. By discarding duplicates, we obtain a composition series which proves that G/H is solvable.

□

Ex. 8.1.3 *Consider the map $\pi : G \to G/H$ used in the proof of Theorem 8.1.4. Given a subgroup $K \subset G/H$, define $\pi^{-1}(K)$ as in (8.1).*

(a) Show that $\pi^{-1}(K)$ is a subgroup of G containing H.

(b) Show that H is the kernel of π and that $H = \pi^{-1}(\{eH\})$.

(c) Show that $G = \pi^{-1}(G/H)$.

Proof. Let $\pi : G \to G/H$ the canonical projection, and K a subgroup of G/H.

(a) $\pi^{-1}(K) \subset G$ is the pre-image of a subgroup by the group homomorphism π, so is a subgroup of G. Moreover $\{\overline{e}\} = \{eH\} \subset K$, thus $H = \pi^{-1}(\{\overline{e}\}) \subset \pi^{-1}(K)$. So $\pi^{-1}(K)$ is a subgroup of G which contains H.

(b) For all $x \in G$, $x \in \ker(\pi) \iff xH = H \iff x \in H$.

Thus $\ker(\pi) = H$.

$eH = H$ being the identity of G/H, by definition of the kernel, $H = \ker(\pi) = \pi^{-1}(\{eH\})$.

(c) As π is a mapping of G in G/H, $\pi^{-1}(G/H)$ is the whole group G.

□

Ex. 8.1.4 *In the situation of (8.2), prove that G_i is normal in G_{i-1} and that $gG_i \mapsto \pi(g)\tilde{G}_i$ gives the isomorphism (8.2).*

Proof. As $\tilde{G}_i \lhd \tilde{G}_{i-1}$, and as π is a group homomorphism, then $\pi^{-1}(\tilde{G}_i) \lhd \pi^{-1}(\tilde{G}_{i-1})$, so $G_i \lhd G_{i-1}$.

Indeed, if $x \in G_{i-1}, y \in G_i$, then $x' = \pi(x) \in \tilde{G}_i, y' = \pi(y) \in \tilde{G}_{i-1}$, where $\tilde{G}_i \lhd \tilde{G}_{i-1}$, so $x'y'x'^{-1} \in \tilde{G}_i$, then $\pi(xyx^{-1}) = \pi(x)\pi(y)\pi(x)^{-1} \in \tilde{G}_i$, and $xyx^{-1} \in \pi^{-1}(\tilde{G}_i) = G_i$.

As π est surjective, $\pi(G_i) = \tilde{G}_i$, and the situation is the same as in Exercise 2, where we have proved that $\overline{\varphi} : G_{i-1}/G_i \to \tilde{G}_{i-1}/\tilde{G}_i$ given by $gG_i \mapsto \pi(g)\tilde{G}_i$ is well defined, and is a surjective group homomorphism. It remains to verify that $\overline{\varphi}$ is injective.

If $gG_i \in \ker(\overline{\varphi})$, then $\overline{\varphi}(gG_i) = \tilde{G}_i$, that is $\pi(g)\tilde{G}_i = \tilde{G}_i$, thus $\pi(g) \in \tilde{G}_i$, so $g \in G_i$, and $gG_i = G_i$ is the identity of G/G_i. Therefore $\overline{\varphi}$ is injective. $\overline{\varphi}$ is a group isomorphism:

$$G_{i-1}/G_i \simeq \tilde{G}_{i-1}/\tilde{G}_i$$

□

Ex. 8.1.5 *In this exercise, you will prove Theorem 8.1.7.*

(a) In any group, show that $\langle g \rangle$ is normal for all $g \in Z(G)$.

(b) Prove Theorem 8.1.7 using induction on n, where $|G| = p^n$ and p is prime.

Proof. (a) Consider the right action of G on itself defined by conjugation with $x^g = g^{-1}xg$, then G in the disjoint union of the associate orbits:

$$G = \bigcup_{x \in S} O_x,$$

where S is a complete set of representative for the conjugacy classes: for all $y \in G$, $|O_y \cap S| = 1$.

The stabilizer of x is the set of $g \in G$ such that $g^{-1}xg = x$, so $xg = gx$: this is the normalizer C_x of x.

Consequently $|O_x| = (G : C_x)$, and so

$$|G| = \sum_{x \in S} (G : C_x).$$

Note that

$$(G : C_x) = 1 \iff C_x = G \iff \forall g \in G,\, gx = xg \iff x \in Z = Z(G).$$

If we take apart these elements in the preceding sum, we obtain (noting that $Z \subset S$ since $O_x = \{x\}$ for all $x \in Z$)

$$|G| = \sum_{x \in S} (G : C_x) = \sum_{x \in Z} (G : C_x) + \sum_{x \in S - Z} (G : C_x) = |Z| + \sum_{x \in S - Z} (G : C_x).$$

Writing $T = S - Z$, we obtain so the class formula

$$|G| = |Z| + \sum_{x \in T} (G : C_x).$$

If G is a p-groupe of order p^n, then for all $x \in S - Z$, $(G : C_x) > 1$ is a power of p, so $(G : C_x) = p^k, k \geq 1$, thus p divides $(G : C_x)$ for all $x \in T$.

As p divides also $|G|$, the class formula implies that p divides $|Z| \geq 1$, and so $|Z| \geq p$. Therefore the center of a p-group is not trivial.

(b) If $g \in Z(G)$, then for all $x \in G$, and for all $k \in \mathbb{Z}$, $g^k \in Z$, so $xg^k = g^k x$, $xg^k x^{-1} = g^k \in Z$, therefore $\langle g \rangle$ is normal in G.

(c) If $n = 1$, every group of order $p^n = p$ is cyclic, a fortiori solvable.

Using induction, suppose that all groups of order $p^k, k < n$ are solvable. Let G a group of order p^n.

Fix $g \in Z, g \neq e$. This is possible since Z is not trivial. By part (b), $H = \langle g \rangle$ is a normal cyclic subgroup G, so H is solvable, and G/H as for cardinality a factor

of p^n, so $|G/H| = p^k$, with $k < n$ since $|H| > 1$. The induction hypothesis implies that $G/H = G/\langle g \rangle$ is solvable.

As H and G/H are solvable, by Theorem 8.1.4 G is also solvable, and the induction is done.

Every finite p-group is solvable.

□

Ex. 8.1.6 *In this exercise you will prove that groups of order 30 are solvable.*

(a) Use the method of Example 8.1.10 to prove that groups of order 10 or 15 are solvable.

(b) Show that a group of order 30 is solvable if and only if it has a proper normal subgroup different from $\{e\}$.

(c) Let G a group of order 30. Use the third Sylow theorem to show that G has one or ten 3-Sylow subgroups and one or six 5-Sylow subgroups.

(d) Show that the group G can't simultaneously have ten 3-Sylow subgroups and six 5-Sylow subgroups. Conclude that G must be solvable.

Proof. (a) Let G be a group of order 10, and N the number of 5-Sylow subgroups of G. Then $N \equiv 1 \pmod 5$ and $N \mid 10$. Therefore $N = 1$. A group of order 10 has a unique 5-Sylow H, and as all 5-Sylow subgroup are conjugate, H is normal in G, since the conjugate of a 5-Silow is a 5-Sylow. Then $|H| = 5$ and $|G/H| = 2$ are prime, so H and G/H are cyclic of prime order. This implies that G is solvable.

Same reasoning if $|G| = 15$: then $N \equiv 1 \pmod 5$, and $N \mid 15$, therefore $N = 1$.

(b) Let G be a group of order 30.

- If G is Abelian, a fortiori solvable, it contains a 5-Sylow subgroup, necessarily normal in G.
- If G is a non Abelian solvable group, there exists a composition series

$$\{e\} = G_n \subsetneq G_{n-1} \subsetneq \cdots \subsetneq G_0 = G.$$

Then $n \geq 2$, otherwise a short series $\{e\} = G_1 \subsetneq G_0 = G$, with $G_0/G_1 = G$ Abelian, is in contradiction with the hypothesis "G non Abelian". Then the subgroup G_1 is normal in G, and $G_1 \neq \{e\}, G_1 \neq G$.
Consequently the hypothesis G solvable implies the existence of a proper non trivial subgroup of G.

- Conversely, suppose that G has a normal subgroup H, with $H \neq \{e\}, H \neq G$. then $q = |H|$ divides 30, and $q \neq 1, q \neq 30$, so $q \in \{2, 3, 5, 6, 10, 15\}$.
If $q = 10$ or $q = 15$, then H is solvable by part (a), and the quotient group G/H is then of order 3 or 2 both prime, so G/H is cyclic. This proves that G is solvable.
If $q = 2$ or $q = 3$, then H is cyclic, and G/H of order 15 or 10 is solvable by part (a), so G is solvable.
A group of order 5 is cyclic, a fortiori solvable, and a group of order 6 est isomorphic to the cyclic group C_6, or to S_3, and in both cases is solvable.
If $q = 5$ ou $q = 6$, H et G/H are both solvable, so G is solvable.

Conclusion: a group G of order 30 is solvable if and only if it contains a proper non trivial normal subgroup.

(c) The number N of 3-sylow subgroups of G satisfies $N \equiv 1 \pmod 3$, and N divides 30, so $N = 1$ or $N = 10$.

The number N' of 5-sylow subgroups of G satisfies $N \equiv 1 \pmod 5$, and N' divisdes 30, so $N' = 1$ or $N' = 6$.

(d) Suppose that G contains ten 3-Sylow subgroups of G and six 5-Sylow subgroups.

Two distinct cyclic subgroups of order p, with p prime, have a trivial intersection, otherwise any non trivial element in the intersection would be a generator of these two subgroups, which would then be identical.

Consequently, two 3-Sylow subgroups have an intersection reduced to the identity of G, and this is the same for the 5-Sylow.

The union of 3-Sylow has then $1 + 10 \times 2 = 21$ elements, and the union of the 5-Sylow $1 + 6 \times 4 = 25$ elements. As a 5-Sylow and a 3-Sylow have a trivial intersection, G would contains at least $21 + 25 - 1 = 45$ elements, in contradiction with $|G| = 30$.

Therefore $N = 1$ or $N' = 1$. In the first case, a 3-Sylow is normal in G, and in the second case, this is a 5-Sylow. By part (b), G is solvable.

□

Ex. 8.1.7 *Use Burnside's $p^n q^m$ Theorem (Theorem 8.1.8) to show that groups of order < 60 are solvable, with the possible exception of groups of order 30 or 42. When combined with the previous exercise and Example 8.1.11, this implies that groups of order < 60 are solvable.*

Proof. The positive integers $n < 60$ have at most two prime factors, except $30 = 2 \times 3 \times 5$ and $42 = 2 \times 3 \times 7$. The Burnside's $p^n q^m$ Theorem shows then that groups of order < 60 are solvable, with the possible exception of groups of order 30 or 42. Exercise 6 proves that the groups of order 30 are solvable, and Example 8.1.11 shows that the groups of order 42 are also solvable. So all groups of order less that 60 are solvable. □

Ex. 8.1.8 *Let G be a finite group, and suppose that we have subgroups*

$$\{e\} = G_n \subset \cdots \subset G_0 = G,$$

such that G_i is normal in G_{i-1} for $i = 1, \ldots, n$.

(a) Prove that G is solvable if G_{i-1}/G_i is Abelian for $i = 1, \ldots, n$.

(b) Prove that G is solvable if G_{i-1}/G_i is solvable for $i = 1, \ldots, n$.

Proof. Suppose that

$$\{e\} = G_n \subset \cdots \subset G_0 = G,$$

with $G_i \lhd G_{i-1},\ i = 1, \cdots, n$.

(a) Suppose that G_{i-1}/G_i is Abelian for $i = 1, \cdots, n$. Then G_{i-1}/G_i is solvable (Proposition 8.1.5), so we can find a composition series $(\tilde{G}_{i,k})_{0\leq k\leq n_i}$ of G_{i-1}/G_i, with cyclic quotients of prime order. The proof of Theorem 8.1.4 (see Exercises 2,3,4) shows that the pre-images $G_{i,k} = \pi^{-1}(\tilde{G}_{i,k})$ of $\tilde{G}_{i,k}$ by the canonical projection $\pi : G_{i-1} \to G_{i-1}/G_i$ form a composition series

$$G_i = G_{i,n_i} \subset G_{i,n_i-1} \subset \cdots \subset G_{i,k} \subset G_{i,k-1} \subset \cdots \subset G_{i,0} = G_{i-1},$$

such that $G_{i,k} \lhd G_{i,k-1},\ i = 1, \cdots n_i$ and such that $(G_{i,k-1} : G_{i,k})$ is prime.

If we glue together all these composition series for $i = 1, \cdots, n$, we obtain a composition series of G where all quotients are of prime order, so G is solvable according to Definition 8.1.1.

(b) The proof of part (a) shows that it is sufficient that the quotients G_{i-1}/G_i are solvable to prove that G is solvable.

□

8.2 RADICAL AND SOLVABLE EXTENSIONS

Ex. 8.2.1 *As in Example 8.2.3, let L be the splitting field of $x^3 + x^2 - 2x - 1$ over $\mathbb{Q}$. Also let $\zeta_7 = e^{2\pi i/7}$.*

(a) Show that the roots of $x^3 + x^2 - 2x - 1$ are $2\cos(2j\pi/7) = \zeta_7^j + \zeta_7^{-j}$ for $j = 1, 2, 3$.

(b) Show that $\mathbb{Q} \subset L \subset \mathbb{Q}(\zeta_7)$, and explain why $\mathbb{Q} \subset \mathbb{Q}(\zeta_7)$ is radical.

Proof. (a) Let $f = x^3 + x^2 - 2x - 1 \in \mathbb{Q}[x]$.

The polynomial $\Phi_7 = \frac{x^7-1}{x-1} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ has the roots $e^{\frac{2ik\pi}{7}}, 1 \leq k \leq 6$.

As $\Phi_7(0) \neq 0$, for all $z \in \mathbb{C}$,

$$\Phi_7(z) = 0 \iff \left(z^3 + \frac{1}{z^3}\right) + \left(z^2 + \frac{1}{z^2}\right) + \left(z + \frac{1}{z}\right) + 1 = 0.$$

Writing $u = z + \frac{1}{z}$, we obtain $u^2 = z^2 + \frac{1}{z^2} + 2$, that is $z^2 + \frac{1}{z^2} = u^2 - 2$.
$u^3 = z^3 + \frac{1}{z^3} + 3(z + \frac{1}{z})$, so $z^3 + \frac{1}{z^3} = u^3 - 3u$.

Therefore

$$\begin{aligned}\Phi_7(z) = 0 &\iff \exists u \in \mathbb{C}, u = z + \frac{1}{z} \text{ and } (u^3 - 3u) + (u^2 - 2) + u + 1 = 0\\ &\iff \exists u \in \mathbb{C}, u = z + \frac{1}{z} \text{ and } f(u) = u^3 + u^2 - 2u - 1 = 0\end{aligned}$$

Applying this equivalence to $z = e^{\frac{2ik\pi}{7}}, 1 \leq k \leq 3$, we obtain

$$f(2\cos(2k\pi/7)) = f(\zeta_7^k + \zeta_7^{-k}) = 0, \quad k = 1, 2, 3.$$

These 3 roots of f are distinct, since the function cos is strictly decreasing on $[0, \pi]$.

Therefore

$$\begin{aligned}f = x^3 + x^2 - 2x - 1 &= (x - 2\cos(2\pi/7))(x - 2\cos(4\pi/7))(x - 2\cos(6\pi/7))\\ &= (x - \zeta_7 - \zeta_7^{-1})(x - \zeta_7^2 - \zeta_7^{-2})(x - \zeta_7^3 - \zeta_7^{-3})\end{aligned}$$

(b) L is the splitting field of f over $\mathbb{Q}$, so by definition

$$L = \mathbb{Q}(\zeta_7 + \zeta_7^{-1}, \zeta_7^2 + \zeta_7^{-2}, \zeta_7^3 + \zeta_7^{-3}).$$

Therefore $L \supset \mathbb{Q}$, and as the three roots of f lie in $\mathbb{Q}[\zeta]$,

$$\mathbb{Q} \subset L \subset \mathbb{Q}(\zeta_7).$$

As $\zeta_7^7 = 1 \in \mathbb{Q}, \mathbb{Q}(\zeta_7)$ is by defintion a radical extension of $\mathbb{Q}$, so $\mathbb{Q} \subset L$ is a solvable extension.

□

Ex. 8.2.2 *In the situation of Example 8.2.3, assume that $\mathbb{Q} \subset L$ is radical. Prove that $L = \mathbb{Q}(\gamma)$, where $\gamma^m \in \mathbb{Q}$ for some $m \geq 3$.*

Proof. $f(x) = x^3 + x^2 - 2x - 1 \in \mathbb{Q}[x]$: $\sigma_1 = -1, \sigma_2 = -2, \sigma_3 = 1$.

Note that f of degree 3 is irreducible over $\mathbb{Q}$, otherwise it would have a rational root $\alpha = p/q \in \mathbb{Q}, p \wedge q = 1, q > 0$.

Then $p^3 + p^2q - 2pq^2 - q^3 = 0$, so $p \mid q^3, p \wedge q = 1$, therefore $p \mid 1$, and similarly $q \mid 1$, thus $\alpha = \pm 1$, but neither 1 nor -1 is a root of f, so f is irreducible.

By Exercise 8.2.1, the splitting field of f over $\mathbb{Q}$ is

$$L = \mathbb{Q}(\zeta_7 + \zeta_7^{-1}, \zeta_7^2 + \zeta_7^{-2}, \zeta_7^3 + \zeta_7^{-3}) \subset \mathbb{R}.$$

$\operatorname{discr}(f) = -4\sigma_2^3 - 27\sigma_3^2 + \sigma_1^2\sigma_2^2 - 4\sigma_1^3\sigma_3 + 18\sigma_1\sigma_2\sigma_3 = 32 - 27 + 4 + 4 + 36 = 49$.

$\operatorname{discr}(f) = 49$ is a square in $\mathbb{Q}$, so $\operatorname{Gal}(L/\mathbb{Q})$ is the cyclic group $C_3 \simeq \mathbb{Z}/3\mathbb{Z}$ (Prop. 7.4.2), and so $[L : \mathbb{Q}] = 3$.

Assume that the extension $\mathbb{Q} \subset L$ is radical.

As $[L : \mathbb{Q}] = 3$, it doesn't exists any strict sub-extension of $\mathbb{Q} \subset L$, so the definition of a radical extension imply the existence of $\gamma \in L$ and of an integer $m > 1$ such that $L = \mathbb{Q}(\gamma)$ and $\gamma^m \in \mathbb{Q}$. As the extension is of degree 3, it it not a quadratic extension, so $m \geq 3$.

We conclude the reasoning (Example 8.2.3):

Let p be the minimal polynomial of γ over $\mathbb{Q}$. Then $\deg(p) = [L : \mathbb{Q}] = 3$. As γ is a root of $x^m - \gamma^m \in \mathbb{Q}[x]$, p divides $x^m - \gamma^m$.

As the extension $\mathbb{Q} \subset L$ is a Galois extension, all the roots of p are in L so are real since $L \subset \mathbb{R}$. Thus the three real distinct roots of p are among the roots of $x^m - \gamma^m$, that is

$$\gamma, \zeta_m\gamma, \zeta_m^2\gamma, \cdots, \zeta_m^{m-1}\gamma, \qquad \gamma \in \mathbb{R}.$$

But this is impossible since at most two of these roots are real.

Conclusion: $\mathbb{Q} \subset L$ is not a radical extension (but $\mathbb{Q} \subset L \subset \mathbb{Q}(\zeta_7)$, so $\mathbb{Q} \subset L$ is solvable). □

Ex. 8.2.3 *Here you will prove two properties of compositums.*

(a) Prove that the compositum K_1K_2 exits.

(b) Prove (8.3)

Proof. (a) Let A be the set of the subfields of L containing K_1 and K_2. Then $A \neq \emptyset$, since $L \in A$.

The intersection of the subfields of L containing K_1 and K_2 is a subfield of L containing K_1 and K_2, so

$\bigcap_{X \in A} X$ is an element of A, and this is the smallest element of A for inclusion.

So there exists a smallest subfield of L containing K_1 and K_2, that is K_1K_2.

(b) Suppose that $K_1 = F(\alpha_1, \alpha_2, \cdots, \alpha_n), K_2 = F(\beta_1, \beta_2, \cdots, \beta_m)$.

$K = K_1K_2$ contains K_1 and K_2, so contains F , and also $\alpha_1, \alpha_2, \cdots, \alpha_n, \beta_1, \beta_2, \cdots, \beta_m$, therefore $K \supset F(\alpha_1, \alpha_2, \cdots, \alpha_n, \beta_1, \beta_2, \cdots, \beta_m)$.

Conversaly, as $K = F(\alpha_1, \alpha_2, \cdots, \alpha_n, \beta_1, \beta_2, \cdots, \beta_m)$ is a subfield of L containing $K_1 = F(\alpha_1, \alpha_2, \cdots, \alpha_n)$ and $K_2 = F(\beta_1, \beta_2, \cdots, \beta_m)$, $K \in A$, so K contains the smallest element of A, which is K_1K_2.

Conclusion: $K_1K_2 = F(\alpha_1, \alpha_2, \cdots, \alpha_n, \beta_1, \beta_2, \cdots, \beta_m)$.

□

Ex. 8.2.4 *This exercise is concerned with the proof of Proposition 8.2.6.*

(a) Show that $K = F(\alpha_1, \ldots, \alpha_r)$ is the Galois closure of $F \subset L$.

(b) Prove that the conjugates of L in M are the fields $F(\alpha_i)$ for $i = 1, \ldots, r$.

Proof. (a) $F \subset L \subset M$, and $F \subset M$ is a Galois extension.

The Theorem of the Primitive Element implies that $L = F(\alpha)$ for some $\alpha \in L$.

Since $F \subset M$ is a Galois extension, the minimal polynomial h of α over F is separable and splits completely over M, say $h(x) = (x - \alpha_1) \cdots (x - \alpha_r)$, where $\alpha_1 = \alpha$.

$K = F(\alpha_1, \alpha_2, \cdots, \alpha_r)$ is a Galois extension of F containing L, since K is the splitting field of a separable polynomial $h \in F[x]$.

We show that $F \subset K$ is the Galois closure of $F \subset L$.

• $F \subset K$ is a Galois extension (as previously proved) and $K \supset L$.

• Suppose that $L \subset K'$ is another extension such that K' is Galois over F.

As $F \subset K'$ is normal, and $\alpha \in L \subset K'$, the polynomial $h \in F[x]$ with a root in K' splits completely over K':

$h(x) = (x - \beta_1) \cdots (x - \beta_r)$, where $\beta_1 = \alpha$, and $\beta_i \in K', 1 \leq i \leq r$.

Let $K'' = F(\beta_1, \cdots, \beta_r)$.

K and K'' are both splitting fields of h over F. By the Theorem of Unicity of the splitting field, there exist an isomorphism $\varphi : K \to K''$ which is the identity on F. As $K'' \subset K'$, φ gives a field homomorphism of K in K' which is the identity on F.

By definition of a Galois closure, $F \subset K$ is a Galois closure of $F \subset L$.

Note: in Exercise 7.3.13, we have seen that there exists a *unique* sub-extension of $F \subset M$ which is a Galois closure of $F \subset L$, so K is the unique Galois closure of $F \subset L$ included in M, the smallest subfield K of M such that $F \subset L \subset K \subset M$ which is Galois over F. If $\alpha \in K'$, $L \subset K'$, and $F \subset K'$ is a Galois extension, then $\alpha = \alpha_1 \in K'$ implies that $\alpha_1, \ldots, \alpha_r \in K'$, so $K = F(\alpha_1, \ldots, \alpha_r) \subset K'$.

(b) If L' is a conjugate field of L in M, there exists a F-automorphism σ of the field M such that $L' = \sigma(L)$, $\sigma \in \mathrm{Gal}(M/F)$.

As σ sends α on a conjugate of α, $\sigma(\alpha) = \alpha_i,\ 1 \leq i \leq r$, and

$$L' = \sigma(L) = \sigma(F(\alpha)) = F(\alpha_i).$$

Indeed, an element $u \in L$ is of the form $u = g(\alpha), g \in F[x]$, so $\sigma(u) = g(\alpha_i) \in F(\alpha_i)$, therefore $\sigma(L) \subset F(\alpha_i)$.

Conversely, an element $v \in F(\alpha_i)$ is of the form $v = g(\alpha_i)$. So v is the image of $u = g(\alpha) \in L$ by σ, so $L' = \sigma(L) = F(\alpha_i)$, therefore the conjugates of L are among the $F(\alpha_i), 1 \leq i \leq r$.

Moreover, if $L'' = F(\alpha_i)$, for any $i = 1, \ldots, r$, we know that there exists $\sigma \in \mathrm{Gal}(M/F)$ such that $\sigma(\alpha) = \alpha_i$ (Prop.5.1.8). As previously proved, $L'' = F(\alpha_i) = \sigma(F(\alpha)) = \sigma(L)$.

The conjugate fields of L in M are the r subfields $F(\alpha_i), 1 \leq i \leq r$.

□

Ex. 8.2.5 *This exercise will complete the proof of part (b) of Lemma 8.2.7.*

(a) Prove (8.5).

(b) Prove that the field F'_n defined in (8.4) is the compositum K_1K_2.

Proof. (a) By hypothesis, $F \subset K_2$, so $F_0 = F \subset K_2 = F'_0$.

Using induction, if we suppose that $F_{i-1} \subset F'_{i-1}, 1 \leq i < n$, then $F_{i-1}(\gamma_i) \subset F'_{i-1}(\gamma_i)$, therefore $F_i \subset F'_i$.

Conclusion: $\forall i, 0 \leq i \leq n,\ F_i \subset F'_i$.

Consequently, $\gamma_i^{m_i} \in F_{i-1} \subset F'_{i-1},\ i = 1, \cdots, n$, so $K_2 \subset F'_n$ is a radical extension.

(b) We show that $K'_n = K_1K_2$.

$K_1 = F(\gamma_1, \cdots, \gamma_n)$, and $F \subset K_2$, therefore $K_1K_2 = K_2(\gamma_1, \cdots, \gamma_n) = F'_n$.

Indeed, $F'_n = K_2(\gamma_1, \cdots, \gamma_n)$ by construction, and

- $$K_2(\gamma_1, \cdots, \gamma_n) \supset K_2,$$
  $$K_2(\gamma_1, \cdots, \gamma_n) \supset F(\gamma_1, \cdots, \gamma_n) = K_1,$$
  therefore $F'_n \supset K_1, F'_n \supset K_2$.
- If K is any subfield of L which contains K_1, K_2, $K \supset K_1 = F(\gamma_1, \cdots, \gamma_n)$, so
  $$K \supset \{\gamma_1, \cdots, \gamma_n\} \text{ and } K \supset K_2,$$
  therefore $K \supset K_2(\gamma_1, \cdots, \gamma_n) = F'_n$.

So F'_n is the smallest subfield of L which contains K_1 and K_2,

$$K_1K_2 = F'_n.$$

We conclude that K_1K_2 is a radical extension of K_2.

□

Ex. 8.2.6 *Suppose we have finite extensions $F \subset L \subset M$ and $\sigma \in \mathrm{Gal}(M/F)$, and assume that $F \subset L$ is radical. Prove that $F \subset \sigma L$ is also radical.*

Proof. Let $\sigma \in \mathrm{Gal}(M/F)$.

There exists an ascending series $(F_i)_{0 \leq i \leq n}$ of subfields of L such that

$$F = F_0 \subset F_1 = F_0(\gamma_1) \subset \cdots \subset F_i = F_{i-1}(\gamma_i) \subset \cdots \subset F_n = F_{n-1}(\gamma_n) = L,$$

where $\gamma_i^{m_i} \in F_{i-1}$.

Write $F_i' = \sigma F_i,\ i = 0, \cdots, n$, and $\gamma' i = \sigma(\gamma_i)$. Then $F_0' = \sigma F_0 = \sigma F = F$ and $F_n' = \sigma L$.

As $F_i = F_{i-1}(\gamma_i),\ i = 1, \cdots, n$, then

$$F_i' = \sigma F_i = \sigma(F_{i-1}(\gamma_i)) = (\sigma F_{i-1})(\sigma(\gamma_i)) = F_{i-1}'(\gamma_{i-1}').$$

So

$$F = F_0' \subset F_1' = F_0'(\gamma_1') \subset \cdots \subset F_i' = F_{i-1}'(\gamma_i') \subset \cdots \subset F_n' = F_{n-1}'(\gamma_n) = \sigma L,$$

Moreover, $(\gamma_i')^{m_i} = \sigma(\gamma_i)^{m_i} = \sigma(\gamma_i^{m_i}) \in \sigma(F_{i-1}) = F_{i-1}'$.

Consequently $F \subset \sigma L$ is a radical extension. □

Ex. 8.2.7 *Suppose that we have extensions $F \subset K_1 \subset L$ and $F \subset K_2 \subset L$ such that $F \subset K_1$ and $F \subset K_2$ are galois. Prove that $F \subset K_1 K_2$ is Galois. This will show that the compositum of two Galois extensions is again Galois.*

Proof. $F \subset K_1$ and $F \subset K_2$ are Galois extensions, so are separable extensions. By the Theorem of the Primitive Element, $K_1 = F(\alpha), K_2 = F(\beta),\ \alpha \in K_1, \beta \in K_2$, with α, β separable over F, therefore $K_1 K_2 = F(\alpha, \beta)$ is separable (Proposition 7.1.6).

By Proposition 7.1.7, the Galois closure exists: let M a Galois closure of $F \subset K_1 K_2$, and σ any element of $\mathrm{Gal}(M/F)$.

Let $\gamma \in K_1 K_2 = F(\alpha, \beta)$. Then $\sigma(\gamma) \in F(\sigma(\alpha), \sigma(\beta))$, and $\sigma(\alpha) \in K_1, \sigma(\beta) \in K_2$ since $F \subset K_1$ and $F \subset K_2$ are normal extensions. Therefore $\sigma(\gamma) \in K_1 K_2$.

Consequently

$$\sigma(K_1 K_2) \subset K_1 K_2.$$

Applying this result to σ^{-1}, we obtain $\sigma^{-1}(K_1 K_2) \subset K_1 K_2$, therefore $K_1 K_2 \subset \sigma(K_1 K_2)$, and so

$$\forall \sigma \in \mathrm{Gal}(M/F),\ \sigma(K_1 K_2) = K_1 K_2.$$

By Theorem 7.2.5, we conclude that $K_1 K_2$ is a Galois extension of F. □

8.3 SOLVABLE EXTENSIONS AND SOLVABLE GROUPS

Ex. 8.3.1 *Let m be a positive integer, and let L be a field of characteristic 0. Then let $L \subset M$ be the splitting field of $x^m - 1 \in L[x]$.*

(a) Prove that $x^m - 1$ is separable.

(b) Prove that the roots of $x^m - 1$ lying in M form a group under multiplication.

Proof. (a) Let $f = x^m - 1,\ m \in \mathbb{N}^*$. Then $f' = mx^{m-1}$ is relatively prime with f. Indeed $m \neq 0$ in L since the characteristic of L is not 0, and $-f + m^{-1}xf' = -x^m + 1 + 1x^m = 1$ is a Bézout's relation between f et f'. Therefore (Prop. 5.3.2), f is a separable polynomial, and $x^m - 1$ has so m distinct roots in M, the splitting field of f over L.

(b) We show that $\mathbb{U}_m = \{\alpha \in M \mid \alpha^m = 1\}$, the set of the m roots of f in M, is a subgroup of M^*.

- $1^m = 1$, donc $1 \in \mathbb{U}_m \neq \emptyset$.
- Si $\alpha, \beta \in \mathbb{U}_m$, alors $(\alpha\beta^{-1})^m = \alpha^m(\beta^m)^{-1} = 1$, donc $\alpha\beta^{-1} \in \mathbb{U}_m$.

The roots of $x^m - 1$ in M form a group under multiplication, subgroup of the multiplicative group of a field, so it is cyclic.

□

Ex. 8.3.2 *Assume that $F \subset L$ is a Galois extension and that F has characteristic 0. Also, consider the extension $L \subset L(\zeta)$ obtained by adjoining a primitive mth root of unity. Prove that $F \subset L(\zeta)$ is Galois.*

Proof. Let ζ a primitive root of $f = x^m - 1$, in other words a generator of $\mathbb{U}_m$.

As the characteristic of F is 0, by Exercise 1, f is a separable polynomial, and $f = (x-1)(x-\zeta)\dots(x-\zeta)^{m-1}$

$F(\zeta) = F(1, \zeta, \cdots, \zeta^{m-1})$ is the splitting field over F of the separable polynomial f, so $F \subset F(\zeta)$ is a Galois extension. By hypothesis, $F \subset L$ is also a Galois extension. By the Theorem of the Primitive Element, there exists $\alpha \in L$ such that $L = F(\alpha)$. Then the compositum of $L = F(\alpha)$ and $F(\zeta)$ is $F(\alpha, \zeta) = L(\zeta)$. By Exercise 8.2.7, this is a Galois extension of F.

$$F \subset L(\zeta) \text{ is a Galois extension.}$$

□

Ex. 8.3.3 *Prove (8.9), where ζ is a primitive pth root of unity and $1 \leq i \leq p-1$.*

Proof. As $\zeta^p = 1, \zeta^i \neq 1 (1 \leq i \leq p-1)$,

$$1 + \zeta^{-i} + \zeta^{-2i} + \cdots + \zeta^{-(p-1)i} = \frac{1 - \zeta^{-ip}}{1 - \zeta^{-i}} = 0.$$

□

Ex. 8.3.4 *Consider the extension $F_{i-1} \subset F_i$ of (8.11). In the discussion following (8.11), we showed that this extension is Galois. We now describe its Galois group.*

(a) Let $\sigma \in \mathrm{Gal}(F_i/F_{i-1})$. Show that there is a unique integer $0 \leq l \leq m_i - 1$ such that $\sigma(\gamma_i) = \zeta_i^l \gamma_i$.

(b) Show that $\sigma \mapsto [l]$ defines a one-to-one homomorphism $\mathrm{Gal}(F_i/F_{i-1}) \to \mathbb{Z}/m_i\mathbb{Z}$, where $[l]$ is the congruence class of l modulo m_i.

(c) Conclude that $\mathrm{Gal}(F_i/F_{i-1})$ is cyclic.

Proof. Recall the context: the extension $F_{i-1} \subset F_i$ is a Galois extension, where $F_i = F_{i-1}(\gamma_i) = F(1, \gamma_i, \zeta^i\gamma_i, \cdots, \zeta^{m_i-1}\gamma_i)$ is the splitting field of $x^{m_i} - a_i$ over F_i, $a_i = \gamma_i^{m_i} \in F_{i-1}$ and ζ_i is a m_ith primitive root of unity.

(a) Let $\sigma \in \mathrm{Gal}(F_i/F_{i-1})$. As γ_i is a root of $x^{m_i} - a_i \in F_{i-1}(x)$, $\sigma(\gamma_i)$ is another root, so

$$\sigma(\gamma_i) = \zeta_i^l\gamma_i, \qquad 0 \leq l \leq m_i - 1.$$

Such an l is unique, since $\zeta_i^l\gamma_i = \zeta_i^{l'}\gamma_i,\ 1 \leq l, l' \leq m_i$ implies $\zeta_i^l = \zeta_i^{l'}$, thus $m_i \mid l'-l$, so $l \equiv l' \pmod{m_i}$. As $|l' - l| \leq m_i - 1$, then $l' - l = 0$.

(b) Let

$$\varphi : \begin{cases} \mathrm{Gal}(F_i/F_{i-1}) & \to & \mathbb{Z}/m_i\mathbb{Z} \\ \sigma & \mapsto & [l] : \sigma(\gamma_i) = \zeta_i^l\gamma_i \end{cases}$$

This mapping is well defined, since l is known modulo m_i.

• We verify that φ is a group homomorphism.

Let $\sigma, \tau \in \mathrm{Gal}(F_i/F_{i-1})$. Then $\sigma(\gamma_i) = \zeta_i^l\gamma_i, \tau(\gamma_i) = \zeta_i^k\gamma_i$.

Thus $(\sigma\tau)(\gamma_i) = \sigma(\zeta_i^k\gamma_i) = \sigma(\zeta_i)^k\sigma(\gamma_i) = \zeta_i^k\sigma(\gamma_i)$, since $\zeta_i \in F$, therefore $\zeta_i \in F_{i-1}$.

$(\sigma\tau)(\gamma_i) = \zeta_i^k\zeta_i^l\gamma_i = \zeta_i^{l+k}\gamma_i$, so $\varphi(\sigma\tau) = [l+k] = [l] + [k] = \varphi(\sigma) + \varphi(\tau)$.

• φ is an injective homomorphism:

if $\sigma \in \ker(\varphi)$, $[l] = [0]$, so $\sigma(\gamma_i) = \sigma_i^l\gamma_i = \gamma_i$. As σ fixes the elements of F_{i-1} and also γ_i, this is the identity on $F_i = F_{i-1}(\gamma_i)$. $\ker(\varphi) = \{e\}$, and φ is injective.

(c) Therefore $\mathrm{Gal}(F_i/F_{i-1})$ is isomorphic to a subgroup H de $\mathbb{Z}/m_i\mathbb{Z}$. As every subgroup of a cyclic group is cyclic, H is cyclic, so

$$\mathrm{Gal}(F_i/F_{i-1}) \text{ is a cyclic group.}$$

□

Ex. 8.3.5 *Suppose that we have extensions $F \subset F_{i-1} \subset F_i \subset L$ such that L is Galois over F and F_i is Galois over F_{i-1}. Prove that $|\mathrm{Gal}(F_i/F_{i-1})|$ divides $|\mathrm{Gal}(L/F)|$.*

Proof. $F \subset F_{i-1} \subset F_i \subset L$.

As $F \subset L$ is a Galois extension, $F_i \subset L$ and $F_{i-1} \subset L$ are also Galois, therefore

$$[L : F_i] = |\mathrm{Gal}(L/F_i)|, \qquad [L : F_{i-1}] = |\mathrm{Gal}(L/F_{i-1}|.$$

$\mathrm{Gal}(F_i/F_{i-1}) \simeq \mathrm{Gal}(L/F_{i-1})/\mathrm{Gal}(L/F_i)$, thus $|\mathrm{Gal}(F_i/F_{i-1})|$ divides $|\mathrm{Gal}(L/F_{i-1}| = [L/F_{i-1}]$.

As $|\mathrm{Gal}(L/F)| = [L : F] = [L : F_{i-1}][F_{i-1} : F]$,

$$|\mathrm{Gal}(F_i/F_{i-1})| \text{ divides } |\mathrm{Gal}(L/F)|.$$

□

Ex. 8.3.6 *Let L be a field containing a primitive mth root of unity ζ and let n be a positive divisor of m. Prove that $\zeta^{m/n}$ is a primitive nth root of unity.*

Proof. For all $k \in \mathbb{Z}$,

$$(\zeta^{m/n})^k = 1 \iff \zeta^{mk/n} = 1 \iff m \mid mk/n \iff n \mid k.$$

The order of $\zeta^{m/n}$ is so n. In other words, $\zeta^{m/n}$ is a primitive nth root of unity. □

Ex. 8.3.7 *Let $F \subset L$ be Galois and solvable (with F of characteristic 0). This exercise will consider a variation of Corollary 8.3.4. Let $p_1, \ldots, p_r$ be the distinct primes dividing $[L : F]$.*

(a) Show that F contains a primitive $(p_1 \cdots p_r)$th root of unity if and only if F contains a primitive p_ith root of unity for $i = 1, \ldots, r$.

(b) Prove that $F \subset L$ is radical when F contains a primitive $(p_1 \cdots p_r)$th root of unity.

(c) Prove that $F \subset L(\zeta)$ is radical, where ζ is a primitive $(p_1 \cdots p_r)$th root of unity.

Proof. $F \subset L$ a solvable Galois extension, with F of characteristic 0. $p_1, \cdots, p_r$ are the distinct prime numbers which divide $[L : F]$.

(a) **Lemma 1.** *Suppose that two elements a, b of an Abelian group G are of respective order p, q, where p, q are relatively prime. Then the order of ab is pq.*

Proof of Lemma 1:

$a^p = b^q = e$, therefore $(ab)^{pq} = (a^p)^q (b^q)^p = e$.

For all $k \in \mathbb{Z}$, since $p \wedge q = 1$,

$$(ab)^k = e \Rightarrow (ab)^{qk} = e \Rightarrow a^{qk} b^{qk} = e \Rightarrow a^{qk} = e \Rightarrow p \mid qk \Rightarrow p \mid k.$$

Similarly

$$(ab)^k = e \Rightarrow (ab)^{pk} = e \Rightarrow a^{pk} b^{pk} = e \Rightarrow b^{pk} = e \Rightarrow q \mid pk \Rightarrow q \mid k.$$

Consequently, using again $p \wedge q = 1$,

$$(ab)^k = e \Rightarrow (p \mid k \text{ and } q \mid k) \Rightarrow pq \mid k.$$

To conclude,

$$\forall k \in \mathbb{Z},\ (ab)^k = e \iff pq \mid k,$$

The order of ab is so pq. □

Lemma 2. *If G is an Abelian group and $c_1, \cdots, c_r \in G$ are of respective order $p_1, \cdots, p_r$, where $p_1, \cdots, p_r$ are pairwise relatively prime, then the order of $c = c_1 \cdots c_r$ is $p_1 \cdots p_r$.*

Proof of Lemma 2: Using the induction hypothesis $|c_1 \cdots c_k| = p_1 \cdots p_k,\ k < r$, and applying Lemma 1 to $a = c_1 \cdots c_k$ of order $p_1 \cdots p_k$, and $b = c_{k+1}$ of order p_{k+1}, where $p_1 \cdots p_k \wedge p_{k+1} = 1$, then $|c_1 \cdots c_{k+1}| = p_1 \cdots p_{k+1}$. □

• Suppose that F contains a root of unity c of order $n = p_1 \cdots p_r$. Write $c_i = c^{n/p_i},\ i = 1, \cdots r$. Then $c_i \in F$ and Exercise 6 proves that c_i is of order p_i.

• Conversely, suppose that F contains some elements c_i of order p_i, for all $i, 1 \leq i \leq r$. The p_i are distinct prime numbers, so are pairwise relatively prime.

Let $c = c_1 \cdots c_r$. Lemma 2 applied in the Abelian group $G = F^*$ shows that the order of $c_1 \cdots c_r$ is $p_1 \cdots p_r$.

Conclusion: if $p_1, \cdots, p_r$ are distinct prime numbers, F contains a primitive $(p_1 \cdots p_r)$th of unity if and only if it contains primitive p_ith roots of unity for all $i = 1, \cdots, r$.

(b) Suppose that F contains a primitive $p_1 \cdots p_r$th root of unity $\zeta_{p_1 \cdots p_r}$. By part (a), F contains also p_ith primitive roots of unity ζ_{p_i} for $i = 1, \cdots, r$.

So the condition 8.11 is satisfied: F contains a pth primitive root of unity for all p dividing $\mathrm{Gal}(L/F) = [L : F]$. The part $(b) \Rightarrow (a)$ (special case) in the proof of Theorem 8.3.3 shows that $F \subset L$ is a radical extension.

(c) Let ζ a $p_1 \cdots p_r$th primitive root of unity.

As proven in the text, there exists an injective group homomorphism (8.13)

$$\mathrm{Gal}(L(\zeta)/F(\zeta)) \to \mathrm{Gal}(L/F)$$

thus $|\mathrm{Gal}(L/F)|$ is a multiple of $|\mathrm{Gal}(L(\zeta)/F(\zeta))|$.

So $F(\zeta)$ contains a pth primitive root of unity for all p dividing $|\mathrm{Gal}(L(\zeta)/F(\zeta))|$, and then the part (b) proves that $F(\zeta) \subset L(\zeta)$ is a radical extension. As $F \subset F(\zeta)$ is radical, by Lemma 8.2.7(a), $F \subset L(\zeta)$ is a radical extension.

□

Ex. 8.3.8 *This exercise concerns the details of our derivation of Cardan's formulas.*

(a) Use the computational methods of Section 2.3 the formulas for α_1^3 and β_1 stated in the text.

(b) Prove (8.15).

Proof. (a) We know that $\alpha_1 = x_1 + \omega^2 x_2 + \omega x_3$, so

$$\begin{aligned}\alpha_1^3 &= (x_1 + \omega^2 x_2 + \omega x_3)^3 \\ &= \quad x_1^3 + x_2^3 + x_3^3 \\ &\quad + 3\omega\,(x_1^2 x_3 + x_2^2 x_1 + x_3^2 x_2) \\ &\quad + 3\omega^2 (x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1) \\ &\quad + 6 x_1 x_2 x_3.\end{aligned}$$

Thus α_1^3 is of the form

$$\alpha_1^3 = p + 3\omega r + 3\omega^2 s + 6q,$$

where

$$\begin{aligned}p &= x_1^3 + x_2^3 + x_3^3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3, \\ q &= x_1 x_2 x_3 = \sigma_3, \\ r &= x_1^2 x_3 + x_2^2 x_1 + x_3^2 x_2, \\ s &= x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1.\end{aligned}$$

Since r, s are fixed by the permutations of A_3, they must be of the form $A + B\sqrt{\Delta},\ A, B \in K = \mathbb{Q}(\sigma_1, \sigma_2, \sigma_3)$, where we choose

$$\begin{aligned}\sqrt{\Delta} &= (x_2 - x_1)(x_3 - x_2)(x_3 - x_1) \\ &= (x_1^2 x_3 + x_2^2 x_1 + x_3^2 x_2) - (x_1^2 x_3 + x_2^2 x_1 + x_3^2 x_2) \\ &= r - s.\end{aligned}$$

The pair (r, s) is so the solution of the system

$$\begin{aligned} r - s &= \sqrt{\Delta}, \\ r + s &= \sigma_1\sigma_2 - 3\sigma_3. \end{aligned}$$

Therefore

$$\begin{aligned} r &= \frac{1}{2}(\sigma_1\sigma_2 - 3\sigma_3 + \sqrt{\Delta}), \\ s &= \frac{1}{2}(\sigma_1\sigma_2 - 3\sigma_3 - \sqrt{\Delta}). \end{aligned}$$

Then

$$\begin{aligned} \alpha_1^3 &= (x_1 + \omega^2 x_2 + \omega x_3)^3 \\ &= + \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3 \\ &\quad + \frac{3}{2}\omega\,(\sigma_1\sigma_2 - 3\sigma_3 + \sqrt{\Delta}) \\ &\quad + \frac{3}{2}\omega^2(\sigma_1\sigma_2 - 3\sigma_3 - \sqrt{\Delta}) \\ &\quad + 6\sigma_3 \\ &= \sigma_1^3 - 3\sigma_1\sigma_2 + 9\sigma_3 - \frac{3}{2}(\sigma_1\sigma_2 - 3\sigma_3) + \frac{3}{2}(\omega - \omega^2)\sqrt{\Delta} \\ &= \sigma_1^3 - \frac{9}{2}\sigma_1\sigma_2 + \frac{27}{2}\sigma_3 + \frac{3\sqrt{3}}{2}i\sqrt{\Delta} \end{aligned}$$

Therefore

$$\begin{aligned} \alpha_1^3 &= -\frac{27}{2}q + \frac{3\sqrt{3}}{2}i\sqrt{\Delta} \\ &= \frac{27}{2}\left(-q + \sqrt{\frac{-\Delta}{27}}\right) \end{aligned}$$

where

$$q = -\frac{2}{27}\sigma_1^3 + \frac{1}{3}\sigma_1\sigma_2 - \sigma_3.$$

So

$$\begin{aligned} \alpha_1 &= x_1 + \omega^2 x_2 + \omega x_3 \\ &= 3\sqrt[3]{\frac{1}{2}\left(-q + \sqrt{\frac{-\Delta}{27}}\right)}, \end{aligned}$$

and

$$\begin{aligned} \beta_1 &= (23)\cdot\alpha_1 \\ &= x_1 + \omega^2 x_3 + \omega x_2 \\ &= 3\sqrt[3]{\frac{1}{2}\left(-q - \sqrt{\frac{-\Delta}{27}}\right)}. \end{aligned}$$

Indeed the same calculation gives β_1, by the exchange of x_2 with x_3, which sends $\sqrt{\Delta}$ on $-\sqrt{\Delta}$.

(b) The system of equations

$$\begin{aligned}\sigma_1 &= x_1 + x_2 + x_3\\ \alpha_1 &= x_1 + \omega^2 x_2 + \omega x_1\\ \beta_1 &= x_1 + \omega x_2 + \omega^2 x_3,\end{aligned}$$

has for solution

$$\begin{aligned}x_1 &= \frac{1}{3}(\sigma_1 + \alpha_1 + \beta_1)\\ x_2 &= \frac{1}{3}(\sigma_1 + \omega\alpha_1 + \omega^2\beta_1)\\ x_3 &= \frac{1}{3}(\sigma_1 + \omega^2\alpha_1 + \omega\beta_1)\end{aligned}$$

And these are the Cardan's formula for the roots of $\tilde{f} = x^3 - \sigma_1 x^2 + \sigma_2 x - \sigma_3$.

□

8.4 SIMPLE GROUPS

Ex. 8.4.1 *Let G be a non trivial finite Abelian group. Prove that G is simple if and only if $G \simeq \mathbb{Z}/p\mathbb{Z}$ for some prime p.*

Proof. Let G be a non trivial finite Abelian group.

- If $G \simeq \mathbb{Z}/p\mathbb{Z}$, G is cyclic of order p. Every subgroup H of G has a cardinality dividing p, so its order is 1 or p, therefore $H = \{e\}$ or $H = G$. The only subgroups of G, normal or not, are $\{e\}$ or G. So G is simple.
- Suppose that G is a non trivial finite Abelian simple group. As G is Abelian, every subgroup of G is normal in G, thus G has no other subgroup that $\{e\}$ or G. As G is not trivial, there exists $x \in G, x \neq e$. Then $\langle x\rangle$ is a subgroup of G with cardinality greater than 1, therefore $G = \langle x\rangle$. G being cyclic, it is isomorphic to $\mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{N}, n > 1$. If n was not prime, n would be divisible by some integer $d, 1 < d < n$. Then $\langle [d]_n\rangle$ is a subgroup of $\mathbb{Z}/n\mathbb{Z}$ of order $n/d, 1 < n/d < n$, so $\mathbb{Z}/n\mathbb{Z}$ would have a non trivial subgroup. This is a contradiction, so $n = p$ is prime:

$$G \simeq \mathbb{Z}/p\mathbb{Z},\ p \text{ prime.}$$

□

Ex. 8.4.2 *Prove that A_n is generated by 3-cycles when $n \geq 3$.*

Proof. As every permutation in A_n is the product of an even number of permutations, it is sufficient to prove that the product of $(ij)(kl), i \neq j, k \neq l$, is a product of 3-cycles.

- If $\{i, j\}, \{k, l\}$ are disjointed, then i, j, k, l are distincts, so

$$(ij)(kl) = (kil)(ijk).$$

Indeed, by applying first (ijk), then (kil), we obtain

$$\begin{aligned} i &\mapsto j \mapsto j, \\ j &\mapsto k \mapsto i, \\ k &\mapsto i \mapsto l, \\ l &\mapsto l \mapsto k, \end{aligned}$$

and the other elements are unchanged.

• If $\{i,j\},\{k,l\}$ have one common element, say $i=k, i\neq l$, then

$$(i\,j)(k\,l) = (i\,j)(i\,l) = (i\,l\,j)$$

is a 3-cycle.

• If $\{i,j\} = \{k,l\}$, alors $(i\,j)(k\,l) = (i\,j)^2 = () = e$ is the empty product.

Conclusion: A_n is generated by 3-cycles. □

Ex. 8.4.3 *This exercise is concerned with the proof of Theorem 8.4.3.*

(a) Prove (8.17).

(b) Verify the identities (8.18), (8.19) and (8.20).

(c) Verify the conjugation identity (8.21).

Theorem. *The alternating group A_n is simple for all $n \geq 5$.*

Proof. Let $H \neq \{e\}$ a normal subgroup of A_n. It is sufficient to prove that $H = A_n$. We show first that H contains a 3-cycle. As $H \neq \{e\}$, H contains an even permutation $\sigma \neq e$. For any 3-cycle $(j_1 j_2 j_3)$, $(j_1 j_2 j_3) \in A_n$, and $H \lhd A_n$, so

$$\sigma^{-1}(j_1\,j_2\,j_3)^{-1}\sigma\,(j_1\,j_2\,j_3) \in H.$$

(a) Suppose that $j \notin \{j_1,j_2,j_3\}$ and $\sigma(j) \notin \{j_1,j_2,j_3\}$.

We show then that $\sigma^{-1}(j_1\,j_2\,j_3)^{-1}\sigma\,(j_1\,j_2\,j_3)$ fixes j.

As $j \notin \{j_1,j_2,j_3\}$, then $(j_1\,j_2\,j_3)\cdot j = j$, and $[\sigma(j_1\,j_2\,j_3)]\cdot j = \sigma(j)$.

As $\sigma(j) \notin \{j_1,j_2,j_3\}$, and $(j_1\,j_2\,j_3)^{-1} = (j_3 j_2 j_1)$,

$$[(j_1\,j_2\,j_3)^{-1}\sigma\,(j_1\,j_2\,j_3)]\cdot j = (j_1\,j_2\,j_3)^{-1}\cdot\sigma(j) = \sigma(j).$$

Therefore

$$[\sigma^{-1}(j_1\,j_2\,j_3)^{-1}\sigma\,(j_1\,j_2\,j_3)]\cdot j = \sigma^{-1}(\sigma(j)) = j.$$

This proves that this commutator is a permutation in H that move at most 6 elements of $\{1,\ldots,n\}$, the elements $j_1,j_2,j_3,\sigma^{-1}(j_1),\sigma^{-1}(j_2),\sigma^{-1}(j_3)$.

(b) • **Case 1.** First suppose that one of the cycles in the cycle decomposition of σ has a length ≥ 4, say

$$\sigma = (i_1\,i_2\,i_3\,i_4\cdots)(\cdots)\cdots.$$

In this case we claim that

$$\lambda = \sigma^{-1}(i_2\,i_3\,i_4)^{-1}\sigma\,(i_2\,i_3\,i_4) = (i_1\,i_3\,i_4).$$

We already know that λ fixes every element k which is not in

$$A = \{i_2,i_3,i_4,\sigma^{-1}(i_2),\sigma^{-1}(i_3),\sigma^{-1}(i_4)\} = \{i_1,i_2,i_3,i_4\}.$$

- If $k \notin A$, then $\lambda(k) = k = (i_1\, i_3\, i_4) \cdot k$.
- If $k = i_1$, $\lambda(i_1) = [\sigma^{-1}(i_2\, i_3\, i_4)^{-1}\sigma\,(i_2\, i_3\, i_4)] \cdot i_1 = [\sigma^{-1}(i_2\, i_3\, i_4)^{-1}] \cdot i_2 = \sigma^{-1}(i_4) = i_3 = (i_1\, i_3\, i_4) \cdot i_1$.
- If $k = i_2$, $\lambda(i_2) = [\sigma^{-1}(i_2\, i_3\, i_4)^{-1}\sigma\,(i_2\, i_3\, i_4)] \cdot i_2 = [\sigma^{-1}(i_2\, i_3\, i_4)^{-1}] \cdot i_4 = i_2 = (i_1\, i_3\, i_4) \cdot i_2$
- If $k = i_3$, $\lambda(i_3) = [\sigma^{-1}(i_2\, i_3\, i_4)^{-1}\sigma\,(i_2\, i_3\, i_4)] \cdot i_3 = [\sigma^{-1}(i_2\, i_3\, i_4)^{-1}] \cdot \sigma(i_4) = \sigma^{-1}(\sigma(i_4)) = i_4 = (i_1\, i_3\, i_4) \cdot i_3$ (since $\sigma(i_4) \notin \{i_2, i_3, i_4\}$).
- If $k = i_4$, $\lambda(i_4) = [\sigma^{-1}(i_2\, i_3\, i_4)^{-1}\sigma\,(i_2\, i_3\, i_4)] \cdot i_4 = [\sigma^{-1}(i_2\, i_3\, i_4)^{-1}] \cdot i_3 = \sigma^{-1}(i_2) = i_1 = (i_1\, i_3\, i_4) \cdot i_4$.

$\forall k \in \{1, \ldots, n\},\ \lambda \cdot k = (i_1\, i_3\, i_4) \cdot k$, so $\lambda = (i_1\, i_3\, i_4)$.

In this case, H contains the 3-cycle $(i_1\, i_3\, i_4)$.

- **Case 2.** Next suppose that σ has a 3-cycle. If σ is a 3-cycle, then we are done. Hence we may assume that

$$\sigma = (i_1\, i_2\, i_3)(i_4 i_5 \cdots) \cdots .$$

We show that

$$\mu = \sigma^{-1}(i_2\, i_3\, i_5)^{-1}\sigma\,(i_2\, i_3\, i_5) = (i_1\, i_4\, i_2\, i_3\, i_5).$$

We know that μ fixes every element not in the set

$$B = \{i_2, i_3, i_5, \sigma^{-1}(i_2), \sigma^{-1}(i_3), \sigma^{-1}(i_5)\} = \{i_1, i_2, i_3, i_4, i_5\}.$$

- If $k \notin B$, $\mu(k) = k = (i_1\, i_4\, i_2\, i_3\, i_5) \cdot k$.
- If $k = i_4$, $[\sigma^{-1}(i_2\, i_3\, i_5)^{-1}\sigma\,(i_2\, i_3\, i_5)] \cdot i_4 = [\sigma^{-1}(i_2\, i_3\, i_5)^{-1}] \cdot i_5 = \sigma^{-1}(i_3) = i_2 = (i_1\, i_4\, i_2\, i_3\, i_5) \cdot i_4$
- If $k = i_1$, $[\sigma^{-1}(i_2\, i_3\, i_5)^{-1}\sigma\,(i_2\, i_3\, i_5)] \cdot i_1 = [\sigma^{-1}(i_2\, i_3\, i_5)^{-1}] \cdot i_2 = \sigma^{-1}(i_5) = i_4 = (i_1\, i_4\, i_2\, i_3\, i_5) \cdot i_1$
- If $k = i_2$, $[\sigma^{-1}(i_2\, i_3\, i_5)^{-1}\sigma\,(i_2\, i_3\, i_5)] \cdot i_2 = [\sigma^{-1}(i_2\, i_3\, i_5)^{-1}] \cdot i_1 = \sigma^{-1}(i_1) = i_3 = (i_1\, i_4\, i_2\, i_3\, i_5) \cdot i_2$
- If $k = i_3$, $[\sigma^{-1}(i_2\, i_3\, i_5)^{-1}\sigma\,(i_2\, i_3\, i_5)] \cdot i_3 = [\sigma^{-1}(i_2\, i_3\, i_5)^{-1}] \cdot \sigma(i_5) = \sigma^{-1}(\sigma(i_5)) = i_5 = (i_1\, i_4\, i_2\, i_3\, i_5) \cdot i_3$ (since $\sigma(i_5) \notin \{i_2, i_3, i_5\}$).

Hence $\mu = (i_1\, i_4\, i_2\, i_3\, i_5)$.

As H contains a 5-cycle, by case 1, it contains also a 3-cycle.

- **Case 3.** Finally suppose that σ is a product of disjoint 2-cycles. There must be at least two since $\sigma \in H \subset A_n$:

$$\sigma = (i_1\, i_2)(i_3\, i_4)(\cdots)(\cdots) \cdots .$$

This time, we have

$$\nu = \sigma^{-1}(i_2\, i_3\, i_4)^{-1}\sigma\,(i_2\, i_3\, i_4) = (i_1\, i_3)(i_2\, i_4).$$

Every element not in

$$C = \{i_2, i_3, i_4, \sigma^{-1}(i_2), \sigma^{-1}(i_3), \sigma^{-1}(i_4)\} = \{i_1, i_2, i_3, i_4\}$$

is fixed by ν.

- If $k \notin C$, $\nu(k) = k = (i_1\, i_3)(i_2\, i_4) \cdot k$
- If $k = i_1$, $\nu(i_1) = [\sigma^{-1}(i_2\, i_3\, i_4)^{-1}\sigma\,(i_2\, i_3\, i_4)] \cdot i_1 = [\sigma^{-1}(i_2\, i_3\, i_4)^{-1}] \cdot i_2 = \sigma^{-1}(i_4) = i_3 = (i_1\, i_3)(i_2\, i_4) \cdot i_1$.
- If $k = i_2$, $\nu(i_2) = [\sigma^{-1}(i_2\, i_3\, i_4)^{-1}\sigma\,(i_2\, i_3\, i_4)] \cdot i_2 = [\sigma^{-1}(i_2\, i_3\, i_4)^{-1}] \cdot i_4 = \sigma^{-1}(i_3) = i_4 = (i_1\, i_3)(i_2\, i_4) \cdot i_2$.
- If $k = i_3$, $\nu(i_3) = [\sigma^{-1}(i_2\, i_3\, i_4)^{-1}\sigma\,(i_2\, i_3\, i_4)] \cdot i_3 = [\sigma^{-1}(i_2\, i_3\, i_4)^{-1}] \cdot i_3 = \sigma^{-1}(i_2) = i_1 = (i_1\, i_3)(i_2\, i_4) \cdot i_3$.
- If $k = i_4$, $\nu(i_4) = [\sigma^{-1}(i_2\, i_3\, i_4)^{-1}\sigma\,(i_2\, i_3\, i_4)] \cdot i_4 = [\sigma^{-1}(i_2\, i_3\, i_4)^{-1}] \cdot i_1 = \sigma^{-1}(i_1) = i_2 = (i_1\, i_3)(i_2\, i_4) \cdot i_4$.

Hence $\nu = (i_1\, i_3)(i_2\, i_4)$, so $(i_1\, i_3)(i_2\, i_4) \in H$. To turn this into a 3-cycle, let $i_5 \notin \{i_1, i_2, i_3, i_4\}$ (this is where we use $n \geq 5$).
Then

$$((i_1\, i_3)(i_2\, i_4))^{-1}(i_1\, i_3\, i_5)^{-1}(i_1\, i_3)(i_2\, i_4)(i_1\, i_3\, i_5) = (i_1\, i_5\, i_3).$$

We verify this with more simple notations,

$$((1\,3)(2\,4))^{-1}(1\,3\,5)^{-1}(1\,3)(2\,4)(1\,3\,5) = (1\,5\,3)$$

by computing the successive images of 1 2 3 4 5:

1 2 3 4 5	
3 2 5 4 1	by $(1\,3\,5)$
1 4 5 2 3	by $(1\,3)(2\,4)$
5 4 3 2 1	by $(1\,3\,5)^{-1} = (1\,5\,3)$
5 2 1 4 3	by $((1\,3)(2\,4))^{-1} = (1\,3)(2\,4)$

This is the permutation $(1\,5\,3)$.
Hence H contains in this case the 3-cycle $(i_1\, i_5\, i_3)$.

As every $\sigma \neq e$ in H satisfies one of these three cases, we can conclude that H contains always a 3-cycle, say$(i\, j\, k)$.

(c) We prove then that H contains all 3-cycles.

If $(i'\ j'\ k')$ (where i', j', k' are distincts) is any 3-cycle, there exists a permutation $\theta \in S_n$ such that $\theta(i) = i', \theta(j) = j', \theta(k) = k'$.

Recall the following property, which is true for all cycle $(i_1\, i_2 \cdots i_l)$:

$$\theta(i_1\, i_2 \cdots i_l)\theta^{-1} = (\theta(i_1)\, \theta(i_2) \cdots \theta(i_l)).$$

Indeed,

- if $1 \leq k < l, (\theta(i_1\, i_2 \cdots i_l)\theta^{-1})(\theta(i_k)) = \theta(i_{k+1})$,
- if $k = l, (\theta(i_1\, i_2 \cdots i_l)\theta^{-1})(\theta(i_l)) = \theta(i_1)$,
- if $x \notin \{\theta(i_1), \cdots, \theta(i_l)\}$, then $\theta^{-1}(x) \notin \{i_1, \cdots, i_l\}$, hence $(\theta(i_1\, i_2 \cdots i_l)\theta^{-1})(x) = \theta(\theta^{-1}(x)) = x$.

This implies that

$$\theta(i\,j\,k)\theta^{-1} = (i'\,j'\,k') \in H.$$

H contains all 3-cycles, and the 3-cycles generate A_n (Exercise 2), so $H = A_n$. The group $A_n, n \geq 5$ is simple.

□

Ex. 8.4.4 *Let H_1 and H_2 be subgroups of a group G and assume that H_1 is normal in G. Prove that $H_1 \cap H_2$ is normal in H_2.*

Proof. We assume that $H_1 \lhd G, H_2 \subset G$. Let $x \in H_1 \cap H_2$. If $y \in H_2$, then $y \in G$. As $H_1 \lhd G$, $yxy^{-1} \in H_1$. Moreover $x \in H_1 \cap H_2$, thus $x \in H_2$, and by hypothesis $y \in H_2$, hence $yxy^{-1} \in H_2$. Consequently $yxy^{-1} \in H_1 \cap H_2$.

$$\forall x \in H_1 \cap H_2,\ \forall y \in H_2,\ yxy^{-1} \in H_1 \cap H_2.$$

Conclusion: if H_1 is a subgroup of G , and if H_2 is normal in G, then $H_1 \cap H_2$ is a normal subgroup of H_2. □

Ex. 8.4.5 *Suppose that $H \subset S_n$ is a subgroup such that $H \neq \{e\}$ and $H \cap A_n = \{e\}$. Prove that $H = \{e, \sigma\}$, where σ is a product of an odd number of disjoint 2-cycles.*

Proof. As $H \neq \{e\}$, there exists a permutation $\sigma \in H, \sigma \neq e$. Then $\sigma^2 \in H \cap A_n$, so $\sigma^2 = e$. Moreover σ is an odd permutation, otherwise $\sigma \in H \cap A_n$, and then $\sigma = e$.

Let τ any permutation in $H \setminus \{e\}$. With the same reasoning, τ is an odd permutation, and so is σ. Hence $\sigma^{-1}\tau \in H \cap A_n$, hence $\sigma^{-1}\tau = e$, so $\tau = \sigma$. H has no other element than e, σ.

$$H = \{e, \sigma\},\ \sigma^2 = e.$$

The order of σ is 2, so in the decomposition of σ in disjoint cycles, since the order of σ is the lcm of the orders of these cycles, all the cycles have order 2.

As $\sigma \notin A_n$, σ is a product of an odd number of disjoint 2-cycles. □

Ex. 8.4.6 *Let G be a finite group.*

(a) Among all normal subgroups of G different from G itself, pick one of maximal order and call it H. Prove that G/H is a simple group.

(b) Use part (a) and complete induction on $|G|$ to prove that G has a composition series.

Proof. (a) Let G be a finite group, and $H \neq G$ a normal subgroup of G of maximal order. We show that G/H is a simple group.

If G/H was not simple, G/H would have a normal subgroup $\overline{K}$,

$$\{\overline{e}\} \subsetneq \overline{K} \subsetneq G/H,$$

where $\overline{e} = eH$ is the indentity of G/H. Let $\pi = G \to G/H, g \mapsto gH$ the canonical projection, and $K = \pi^{-1}(\overline{K})$.

As $\{\overline{e}\} \subsetneq \overline{K} \subsetneq G/H$, then $\pi^{-1}(\{\overline{e}\}) \subsetneq \pi^{-1}(\overline{K}) \subsetneq \pi^{-1}(G/H)$, so

$$H \subsetneq K \subsetneq G.$$

We show that $K \lhd G$. Let $y \in G, x \in K$. Then $\overline{y} = yH \in G/H$ and $\overline{x} = xH \in \overline{K}$, where $\overline{K} \lhd G/H$, hence $\pi(yxy^{-1}) = \overline{y}\,\overline{x}\,\overline{y}^{-1} \in \overline{K}$, so $yxy^{-1} \in K = \pi^{-1}(\overline{K})$.

$H \subsetneq K \subsetneq G$ and $K \lhd G$ is in contradiction with the definition of H as normal subgroup of G of maximal order, so such a subgroup $\overline{K}$ of G/H doesn't exists.

$$G/H \text{ is a simple group.}$$

(b) The trivial group $\{e\}$ has a composition series with a unique element. Reasoning by induction, we suppose that every group of order less that n has a composition series, and let G be a group of order n.

G has a normal subgroup H of maximal order such that

$$\{e\} \subset H \subsetneq G, \qquad H \lhd G.$$

By part (a), G/H is simple.

As $|H| < n$, the induction hypothesis gives a composition series for H, that we write

$$\{e\} = G_l \subset G_{l-1} \subset \cdots \subset G_1 = H,$$

where $G_i \lhd G_{i-1},\ 2 \leq i \leq l$, and G_{i-1}/G_i is simple.

Then

$$\{e\} = G_l \subset G_{l-1} \subset \cdots \subset G_1 = H \subset G_0 = G$$

is a composition series for G, and the induction is done.

Every finite group has a composition series.

□

Ex. 8.4.7 *Show that the Feit-Thomson Theorem (Theorem 8.1.9) is equivalent to the assertion that every non Abelian finite simple group has even order.*

Proof. We show the equivalence between the two following properties:
(FT) Every group of odd order is solvable.
(H) Every non Abelian finite simple group has even order.

(FT) ⇒ (H) Let G a non Abelian finite simple group. If G was solvable, it would have a normal subgroup $H \subsetneq G$, with G/H cyclic of prime order. G being simple, $H = \{e\}$, hence $G \simeq G/\{e\} = G/H$ would be cyclic, a fortiori Abelian, which is in contradiction with the hypothesis made on G.

Therefore, every non Abelian finite simple group G is not solvable.

If the order of G was odd, G would be solvable by (FT), hence $|G|$ is even. Every non Abelian finite simple group has even order.

(H) ⇒ (FT) Suppose (H). Let G a group of odd order. By Exercise 6, as any finite group, it has a composition series

$$\{e\} = G_m \subset G_{m-1} \subset \cdots \subset G_1 \subset G_0 = G,$$

with G_{i-1}/G_i simple, $i = 1, \cdots, m$.

Then

$$|G| = (G : \{e\}) = (G_0 : G_1)(G_1 : G_2) \cdots (G_{i-1} : G_i) \cdots (G_{m-1} : G_m).$$

As $|G|$ is odd, $(G_{i-1} : G_i)$ is odd for all $i,\ i = 1, \cdots, m$.

So G_{i-1}/G_i is a simple group of odd order. By hypothesis (H), it is then Abelian, and simple, therefore G_{i-1}/G_i is cyclic of prime order (Exercise 8.1.8). So G is solvable, and this shows that (H) $\Rightarrow$ (FT).

□

Ex. 8.4.8 *Prove that $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ are non isomorphic groups with the same composition factors.*

Proof.

$$\{\dot{0}\} \subset \{\dot{0}, \dot{2}\} \subset \mathbb{Z}/4\mathbb{Z}$$
$$\{(\dot{0}, \dot{0})\} \subset \{(\dot{0}, \dot{0}), (\dot{0}, \dot{1})\} \subset \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

are composition series whose factors are of order 2, so are isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Yet the two groups $\mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ are not isomorphic, since $\mathbb{Z}/4\mathbb{Z}$ has one element of order 2, and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ has 3 such elements. □

8.5 SOLVING POLYNOMIALS BY RADICALS

Ex. 8.5.1 *Let $F \subset L_1$ and $F \subset L_2$ be splitting fields of $f \in F[x]$. Prove that $F \subset L_1$ is solvable if and only if $F \subset L_2$ is solvable.*

Proof. The characteristic of F is 0 in this section.

Let L_1, L_2 two splitting fields of $f \in F[x]$ over F. Then there exists an isomorphism $\varphi : L_1 \to L_2$ which is the identity on F.

Suppose that $F \subset L_1$ is a solvable extension.

As L_1 is a splitting field of f over F, $F \subset L_1$ is a normal extension, and as the characteristic of F is 0, this is a separable extension, so $F \subset L_1$ is a Galois extension.

Let ζ be a mth primitive root of unity, where $m = [L_1 : F]$. Write $M_1 = L_1(\zeta)$. As $F \subset L_1$ is a solvable Galois extension, by Corollary 8.3.4, $F \subset M_1$ is a radical extension, so there exist fields $F_i, i = 1, \cdots, m$ such that

$$F_0 = F \subset F_1 \subset \cdots \subset F_{m-1} \subset F_m = M_1 = L_1(\zeta),$$

and $F_i = F_{i-1}(\gamma_i), \gamma_i \in F_i, \gamma_i^{m_i} \in F_{i-1}, m_i > 0$ $(i = 1, \cdots, m)$.

Moreover, $M_1 = L_1(\zeta)$ is the splitting field of $x^m - 1$ over L_1. Let $M_2 = L_2(\zeta')$ the splitting field of $x^m - 1$ over L_2. By theorem 5.1.6, there exists an isomorphism $\overline{\varphi} : M_1 \to M_2$ such that $\varphi = \overline{\varphi}|_{L_1}$. Then M_2 is such that $F \subset L_2 \subset M_2$.

Write $F_i' = \overline{\varphi}(F_i)$. Then

$$F_0' = F \subset F_1' \subset \cdots \subset F_{m-1}' \subset F_m' = M_2,$$

and $F_i' = F_{i-1}'(\gamma_i')$, where $\gamma_i' = \overline{\varphi}(\gamma_i) \in F_i'$ satisfies $\gamma_i'^{m_i} = \overline{\varphi}(\gamma_i)^{m_i} = \overline{\varphi}(\gamma_i^{m_i}) \in \overline{\varphi}(F_{i-1}) = F_{i-1}'$.

So $F \subset M_2$ is radical, and $F \subset L_2$ is solvable.

By exchanging L_1, L_2, we show similarly that $F \subset L_2$ is solvable implies $F \subset L_1$ is solvable, so

$F \subset L_1$ is solvable if and only if $F \subset L_2$ is solvable. □

Ex. 8.5.2 *Let $f \in F[x]$ be separable and irreducible, and assume that we have an extension $F \subset F(\alpha)$ where α is a root of f. Prove that the Galois closure of this extension (as defined in Section 7.1) is the splitting field of f over F.*

Proof. Let L the splitting field of f over F, then

$$L = F(\alpha_1, \cdots, \alpha_n),$$

where $\alpha_1 = \alpha, \alpha_2, \cdots, \alpha_n$ are the roots of f in L.

• L is a Galois extension of F, since L is the splitting field of a separable polynomial $f \in F[x]$ (Theorem 7.1.1).

• Let M be any extension of $F(\alpha)$ such that M is Galois over F. As α is a root of the irreducible polynomial $f \in F[x]$, and $\alpha \in M$, where M is a normal extension of F, the polynomial f splits completely over F and its distinct roots $\beta_1 = \alpha = \alpha_1, \beta_1, \cdots, \beta_n$ are in M. Let $L' = F(\beta_1, \cdots, \beta_n)$. L' is a splitting field of f over F, hence there exists an isomorphism $\varphi : L \to L'$ which is the identity on F, that is an embedding of L in M which is the identity on F.

So, by definition, L is a Galois closure of $F \subset F(\alpha)$, unique up to isomorphism. □

Ex. 8.5.3 *Let F have characteristic 0 and suppose that $f \in F[x]$ has degree ≤ 4 and is not separable. Prove that f is solvable by radicals over F.*

Proof. By Proposition 5.3.8, f has the same roots as $g = f/\text{pgcd}(f, f')$. The splitting field L of f over F is so the splitting field of the separable polynomial g. As $\deg(g) \leq \deg(d) \leq 4$, L is solvable over F by Proposition 8.5.4. We can conclude that all polynomial $f \in F[x]$ of degree $n \leq 4$, separable or not, is solvable by radicals over F. □

Ex. 8.5.4 *Let f be the minimal polynomial over $\mathbb{Q}$ of $\sqrt[5]{\sqrt[3]{17} + \sqrt[4]{37}}$ over $\mathbb{Q}$, where all of the indicated radicals are real. Prove that f is solvable by radicals over $\mathbb{Q}$.*

Proof. Let f the minimal polynomial over $\mathbb{Q}$ of

$$\alpha = \sqrt[5]{\sqrt[3]{17} + \sqrt[4]{37}}.$$

$\alpha \in K = \mathbb{Q}(\sqrt[5]{\sqrt[3]{17} + \sqrt[4]{37}})$, and we obtain the inclusion chain

$$F_0 = \mathbb{Q} \subset F_1 = \mathbb{Q}(\sqrt[3]{17}) \subset F_2 = \mathbb{Q}(\sqrt[3]{17}, \sqrt[4]{37}) \subset F_3 = \mathbb{Q}\left(\sqrt[3]{17}, \sqrt[4]{37}, \sqrt[5]{\sqrt[3]{17} + \sqrt[4]{37}}\right);$$

that is

$$F_0 \subset F_1 = F_0(\gamma_1) \subset F_2 = F_1(\gamma_2) \subset F_3 = F_3(\gamma_3) = K,$$

where $\gamma_1 = \sqrt[3]{17} \in F_1, \gamma_2 = \sqrt[4]{37} \in F_2, \gamma_3 = \sqrt[5]{\sqrt[3]{17} + \sqrt[4]{37}}$ satisfy

$$\gamma_1^3 = 17 \in \mathbb{Q} = F_0, \gamma_2^4 = 37 \in \mathbb{Q} \subset F_1, \gamma_3^5 = \gamma_1 + \gamma_2 \in F_2.$$

This proves that $\mathbb{Q} \subset K$ is a radical extension, with α in K, so α is expressible by radicals over $\mathbb{Q}$ according to Definition 8.5.1. By Proposition 8.5.2, as the irreducible polynomial f has a root expressible by radicals over $\mathbb{Q}$, f is solvable by radicals. So all the roots of f are expressible by radicals over $\mathbb{Q}$. □

Ex. 8.5.5 *Let F have characteristic 0, and assume that we have fields $F \subset K \subset L$. Also suppose that $\alpha \in L$ is expressible by radicals over K and that the extension $F \subset K$ is a solvable extension. Prove carefully that the minimal polynomial of α over F is solvable by radicals over F.*

Proof. F has characteristic 0, and $F \subset K \subset L$.

$\alpha \in L$ is expressible by radicals over K, so there exist by definition a radical extension $K \subset N$ such that $\alpha \in N$.

By hypothesis $F \subset K$ is solvable, so there exists a radical extension $F \subset M$ such that $K \subset M$.

As $K \subset N$ is radical (and $K \subset M$), then $M \subset MN$ is also radical by Lemma 8.2.7(b).

So $F \subset M$ and $M \subset MN$ are radical extensions, so $F \subset MN$ is a radical extension (Lemma 8.2.7(a)).

As $\alpha \in N \subset MN$, with $F \subset MN$ radical, by definition α is expressible par radicals over F and by Proposition 8.5.2, it minimal polynomial f over F is solvable by radicals over F. □

Ex. 8.5.6 *The proof of Theorem 8.5.9 used the Theorem of the Primitive Element to show that $\mathbb{R}$ has no extension of odd degree > 1. Prove this without using primitive elements.*

Proof. We show that $\mathbb{R}$ has no extension L of odd degree $d = [L : \mathbb{R}] > 1$, knowing that every polynomial with an odd degree has a real root by the Intermediate value Theorem.

As $[L : \mathbb{R}] > 1$, there exists $\alpha \in L, \alpha \notin \mathbb{R}$. Let p the minimal polynomial of α over $\mathbb{R}$. By the Tower Theorem,

$$[L : \mathbb{R}] = [L : \mathbb{R}(\alpha)][\mathbb{R}(\alpha) : \mathbb{R}],$$

hence $\deg(p) = [\mathbb{R}(\alpha) : \mathbb{R}]$ divides the odd integer $d = [L : \mathbb{R}]$, so $\deg(p)$ is odd. Therefore p has a real root. As p is irreducible over $\mathbb{R}$, its degree is $\deg(p) = 1$, which implies $[\mathbb{R}(\alpha) : \mathbb{R}] = 1$, so $\alpha \in \mathbb{R}$, in contradiction with the definition of α.

Conclusion: $\mathbb{R}$ has no extension of odd degree greater than 1. □

8.6 THE CASUS IRREDUCIBILIS (OPTIONAL)

Ex. 8.6.1 *Here are some details from the proof of Proposition 8.6.4.*

(a) Prove (8.27):

$$[KL : K] = [L : M] = p.$$

(b) Prove that $KL = K$ if and only if $L \subset K$.

Proof. To achieve the induction in part (a), it is necessary, in the situation of diagram 8.24, to prove that $M(\gamma) \subset L(\gamma)$ is a Galois extension, knowing that the extension $L \subset M$ is a Galois extension. This is done in Exercise 4.

(a) As the extension $M \subset K$ is radical, there exist $\gamma_1, \ldots, \gamma_n \in K \subset \mathbb{R}$ such that the subfields $M_k = M(\gamma_1, \ldots, \gamma_k),\ k = 0, \ldots, n$ of K satisfy

$$M_0 = M \subset M_1 \subset \cdots \subset M_n = K,$$

and $M_i = M_{i-1}(\gamma_i), \gamma_i \in M_i, \gamma_i^{m_i} \in M_{i-1}, m_i > 0$, with m_i prime (Lemma 8.6.2).

Let $L_0 = L, L_i = L(\gamma_1, \ldots, \gamma_i)$. Then $M_0 = M \subset L_0 = L$ and $M_i \subset L_i$.

$[L_0 : M_0] = [L : M] = p$. Reasoning by induction for $i = 1, \ldots, n$, we suppose that $M_{i-1} \subset L_{i-1}$ is a Galois extension and $[L_{i-1} : M_{i-1}] = p$ (where p is the odd prime $[L : M]$). As $L_i = L_{i-1}(\gamma_i), M_i = M_{i-1}(\gamma_i),\ i = 1, \cdots, n$, the Exercise 8.6.4(a) shows that $M_i \subset L_i$ is Galois, and the proof of Proposition 8.6.4 shows that $[L_i : M_i] = [L_{i-1}(\gamma_i) : M_{i-1}(\gamma_i)] = p$, and the induction is done. Therefore $[L(\gamma_1, \ldots, \gamma_n) : K] = [L_n : M_n] = [L_0 : M_0] = [L : M]$, so

$$[L(\gamma_1, \ldots, \gamma_n) : K] = [L : M] = p.$$

Moreover, $M \subset L$, and $K = M(\gamma_1, \cdots, \gamma_n)$, hence $KL = L(\gamma_1, \ldots, \gamma_n)$. Indeed $\mathbb{R}$ is a field which contains K and L, and $L(\gamma_1, \cdots, \gamma_n)$ is the smallest subfield of $\mathbb{R}$ containing K and L, so $KL = L(\gamma_1, \ldots, \gamma_n)$.

$$[KL : K] = [L : M] = p.$$

(b) We show that

$$KL = K \iff L \subset K.$$

($\Leftarrow$) If $L \subset K$, K is the smallest subfield of $\mathbb{R}$ containing L and K, so $KL = K$.

($\Rightarrow$) If $KL = K$, then $L \subset KL = K$, so $L \subset K$.

□

Ex. 8.6.2 *Let $F \subset K$ be a real radical extension and suppose that $F \subset M \subset \mathbb{R}$. Prove that $M \subset MK$ is a real radical extension.*

Proof. As the extension $F \subset K$ is radical, there exist $\gamma_1, \ldots, \gamma_n \in K \subset \mathbb{R}$ such that the subfields $K_i = F(\gamma_1, \ldots, \gamma_i),\ i = 0, \ldots, n$ of K satisfy

$$K_0 = F \subset K_1 \subset \cdots \subset K_n = K,$$

and $K_i = K_{i-1}(\gamma_i), \gamma_i \in K_i, \gamma_i^{m_i} \in K_{i-1}, m_i > 0$.

Let $M_0 = M, M_i = M(\gamma_1, \ldots, \gamma_i)$. Then $K_0 = F \subset M_0 = M$ and $K_i \subset M_i$. Moreover

$$M_0 = M \subset M_1 \subset \cdots \subset M_n = M(\gamma_1, \ldots, \gamma_n),$$

and $M_i = M_{i-1}(\gamma_i), \gamma_i^{m_i} \in K_{i-1} \subset M_{i-1}$, so

$$M \subset M(\gamma_1, \ldots, \gamma_n) = M_n \text{ is a real radical extension.}$$

Moreover, as $F \subset M$, $K = F(\gamma_1, \ldots, \gamma_n)$ and $K \subset M_n = M(\gamma_1, \ldots, \gamma_n)$, then $M_n = MK$, so

$$M \subset MK \text{ is a real radical extension.}$$

□

Ex. 8.6.3 *Show that the polynomial $f = x^4 - 4x^2 + x + 1$ of Example 8.6.7 is irreducible over $\mathbb{Q}$ and has four real roots.*

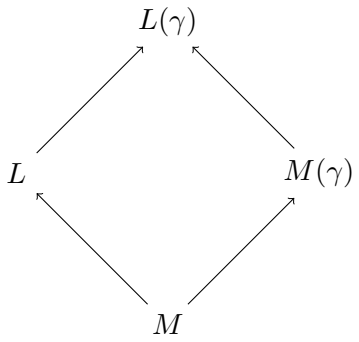
Proof. By Gauss Lemma (Theorem A.3.2), it is sufficient to prove that f has no non trivial factorization in $\mathbb{Z}[x]$. Since the reduction modulo 2 of f is $\overline{f} = x^4 + x + 1$ is of the same degree, it is sufficient to prove that $\overline{f}$ is irreducible in $\mathbb{F}_2[x]$ (a non trivial factorization in $\mathbb{Z}[x]$ would give a factorisation in $\mathbb{F}_2[x]$ by projection). This is the case if $\overline{f}$ has no root in $\mathbb{F}_4 \supset \mathbb{F}_2$ (an irreducible factor $\overline{g}$ of $\overline{f}$ of degree 2 would give a root of g in $\mathbb{F}_2[x]/\langle g \rangle \simeq \mathbb{F}_4$).

As any element $\alpha \in \mathbb{F}_4$ satisfies $\alpha^4 = \alpha = -\alpha$, $\overline{f}(\alpha) = \alpha^4 + \alpha + 1 = 1 \neq 0$, so $\overline{f}$ is irreducible over $\mathbb{F}_2$. Therefore

$$x^4 - 4x^2 + x + 1 \text{ is irreducible over } \mathbb{Q}$$

$f(-3) = 43 > 0, f(-2) = -1 < 0, f(0) = 1 > 0, f(1) = -1 < 0, f(2) = 3 > 0$. As f is continuous, the Intermediate Value Theorem shows the existence of the roots $x_1 \in]-3, -2[, x_2 \in]-2, 0[, x_3 \in]0, 1[, x_4 \in]1, 3[$. As $\deg(f) = 4$, f has no other root, so all the roots of f are real. □

Ex. 8.6.4 *Complete the proof of Proposition 8.6.10.*
diagram (8.24):



Proof. (a) We show that in the situation of diagram (8.24), where $M \subset L$ is Galois, and $[L : M] = n < \infty$, then $M(\gamma) \subset L(\gamma)$ is also a Galois extension.

By the Theorem of the Primitive Element (Theorem 5.4.1), as $M \subset L$ is Galois, there exists a separable element $\delta \in L$ such that $L = M(\delta)$. Let f be the minimal polynomial of δ over M. Then $f \in M[x]$ is a separable polynomial, and as $M \subset L$ is normal, f splits completely over L. Write $\delta_1 = \delta, \delta_2, \ldots, \delta_n$ the roots of f in L.

Then

$$L(\gamma) = M(\delta, \gamma) = M(\gamma)(\delta).$$

Moreover, as $\delta_i \in L \subset L(\gamma) = M(\gamma)(\delta)$, with $\delta = \delta_1$, then $M(\gamma)(\delta) = M(\gamma)(\delta_1, \ldots \delta_n)$, so

$$M(\gamma) \subset L(\gamma) = M(\gamma)(\delta_1, \ldots \delta_n)$$

is the splitting field of the separable polynomial $f \in M[x] \subset M(\gamma)[x]$ over $M(\gamma)$.

This implies that $M(\gamma) \subset L(\gamma)$ is a Galois extension.

(b) We show that L lies in no radical extension of M, as in the proof of Proposition 8.6.4. and Exercise 1.

As the extension $M \subset K$ is radical, there exist $\gamma_1, \ldots, \gamma_n \in K$ such that the subfields $M_k = M(\gamma_1, \ldots, \gamma_k),\ k = 0, \ldots, n$, of K satisfy

$$M_0 = M \subset M_1 \subset \cdots \subset M_n = K,$$

and $M_i = M_{i-1}(\gamma_i), \gamma_i \in M_i, \gamma_i^{m_i} \in M_{i-1}, m_i > 0$, with m_i prime (Lemma 8.6.2).

Let $L_0 = L$ and $L_i = L(\gamma_1, \ldots, \gamma_i)$. Then $M_0 = M \subset L_0 = L$ and $M_i \subset L_i$.

$[L_0 : M_0] = [L : M] = p$. Reasoning by induction, we suppose that $M_{i-1} \subset L_{i-1}$ is a Galois extension and $[L_{i-1} : M_{i-1}] = p$ (where p is the odd prime $[L : M]$). As $L_i = L_{i-1}(\gamma_i), M_i = M_{i-1}(\gamma_i),\ i = 1, \cdots, n$, the part (a) shows that $M_i \subset L_i$ is Galois, and the proof of Proposition 8.6.10 shows that

$$[L_i : M_i] = [L_{i-1}(\gamma_i) : M_{i-1}(\gamma_i)] = p, \qquad i = 1, \ldots, n,$$

therefore $[L(\gamma_1, \ldots, \gamma_n) : K] = [L_n : M_n] = [L_0 : M_0] = [L : M]$, so

$$[L(\gamma_1, \ldots, \gamma_n) : K] = [L : M].$$

Moreover, $M \subset L$, and $K = M(\gamma_1, \cdots, \gamma_n)$, hence $KL = L(\gamma_1, \cdots, \gamma_n)$ in a fixed extension Ω of K and L. Indeed $L(\gamma_1, \cdots, \gamma_n)$ is the smallest subfield of Ω containing K and L, so $KL = L(\gamma_1, \ldots, \gamma_n)$.

$$[KL : K] = [L : M] = p.$$

It follows that $KL \neq K$, so $L \not\subset K$ (see Exercise 1). Since $M \subset K$ is an arbitrary real radical extension of M, we conclude that L cannot lie in a radical extension, so the extension $M \subset L$ is not solvable

□

Ex. 8.6.5 *This exercise will consider the polynomial $f = x^p - x + t$ from Example 8.6.11. Let $\alpha \in L$ a root of f.*

(a) Show that the roots of f are $\alpha, \alpha + 1, \ldots, \alpha + p - 1$.

(b) Let $\sigma \in \mathrm{Gal}(L/M)$. By part (a), $\sigma(\alpha) = \alpha + i$ for some i. Prove that $\sigma \mapsto [i]$ gives the desired one-to-one homomorphism (8.29).

Proof. (a) Already done in Exercise 5.3.16:

$M = k(t)$ has characteristic p and $f = x^p - x + t \in M[x]$.

$f' = -1$, thus $f \wedge f' = 1$, so f is separable.

As α is a root of f, $f(\alpha) = \alpha^p - \alpha + t = 0$, thus

$$\begin{aligned} f(\alpha + 1) &= (\alpha + 1)^p - (\alpha + 1) + a \\ &= \alpha^p + 1 - \alpha - 1 + a \\ &= 0 \end{aligned}$$

$\alpha + 1 \in L$ is also a root of f.

So $\alpha, \alpha+1, \ldots, \alpha+p-1$ are roots of f. These roots are distinct since $0, 1, \ldots, p-1$ are the p distinct elements of the prime subfield of F, isomorphic to $\mathbb{F}_p$, and identified with $\mathbb{F}_p$.

Thus f is divisible by $(x-\alpha)\cdots(x-\alpha-p+1)$, of degree $p = \deg(f)$. As both polynomials are monic,

$$f = (x-\alpha)(x-\alpha-1)\cdots(x-\alpha-p+1) \tag{1}$$

so the roots of f are $\alpha, \alpha+1, \ldots, \alpha+p-1$, and $L = M(\alpha)$.

(b) Let

$$\varphi : \begin{cases} \mathrm{Gal}(L/M) & \to & \mathbb{Z}/p\mathbb{Z} \\ \sigma & \mapsto & [i] : \sigma(\alpha) = \alpha + i \end{cases}$$

Here $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ is the prime field of M, so $[i] \in \mathbb{F}_p \subset M$. φ is well defined: if $\alpha + i = \alpha + j$, then $[i] = [j]$. Moreover φ is a group homomorphism: if $\sigma, \tau \in \mathrm{Gal}(L/M)$, then $\sigma(\alpha) = \alpha + i, \tau(\alpha) = \alpha + j$ for integers i, j, and

$$(\sigma\tau)(\alpha)) = \sigma(\alpha + j) = \alpha + i + j.$$

Hence

$$\varphi(\sigma\tau) = [i+j] = [i] + [j] = \varphi(\sigma) + \varphi(\tau).$$

Moreover, if $\sigma \in \ker(\varphi)$, $\sigma(\alpha) = \alpha$. As $L = M(\alpha)$, and σ fixes M, $\sigma = e$, so $\ker(\varphi) = \{e\}$ and φ is injective. □

Ex. 8.6.6 *Let k be a field and let $M = k(t)$, where t is a variable. The goal of this exercise is to prove that if $n > 1$, then there is no element $\beta \in M$ such that $\beta^n - \beta + t = 0$.*

(a) Write $\beta = A/B$, where $A, B \in k[t]$ are relatively prime polynomials. Prove that $\beta^n - \beta + t = 0$ implies that $B \mid A$ and hence B is constant.

(b) Show that $A^n - A + t \neq 0$ for all polynomials $A \in k[t]$.

Proof.

(a) We assume that

$$\beta^n - \beta + t = 0, \qquad \beta = \frac{A}{B},$$

where $A, B \in k[t]$ are relatively prime polynomials. Then

$$\frac{A^n}{B^n} - \frac{A}{B} + t = 0,$$

$$A^n - AB^{n-1} + tB^n = 0.$$

Hence $B \mid A^n$, and $B \wedge A = 1$, so $B \wedge A^n = 1$, therefore $B \mid 1$, so B is a constant, and $\beta = A/B$ is a polynomial.

(b) By part (a), if $\beta \in M$ satisfies $\beta^n - \beta + t = 0$, then $\beta \in k[t]$. Write $\beta = A \in k[t]$, then

$$A^n - A + t = 0.$$

Then $A \mid t$. As any polynomial of degree 1, t is irreducible in $k[t]$, so

$$A = \lambda \text{ or } A = \lambda t, \text{ where } \lambda \in k^*.$$

If $A = \lambda$ then $t \in k$, in contradiction with $\deg(t) = 1$.

If $A = \lambda t,\ \lambda \in k^*$, then $\lambda^n t^n + (1-\lambda)t = 0,\ n > 1$, shows that t is algebraic over k, in contradiction with the definition of t as a transcendental variable over k.

Conclusion: $x^n - x + t,\ n > 1$ has no root in $M = k(t)$. □

Ex. 8.6.7 *Suppose that F is a field of characteristic p and that $F \subset L$ is a Galois extension. Also assume that* $\mathrm{Gal}(L/F)$ *is solvable and that $p \nmid [L : F]$. Prove that $F \subset L$ is solvable.*

Proof. We follow the proof of (b) $\Rightarrow$ (a) in the proof of Theorem 8.3.3. The part "A Special Case" is unchanged.

Assume that $\mathrm{Gal}(L/F)$ is solvable and that $p \nmid [L : F]$.

A Special Case. Assume first that F satisfies the following special hypothesis:

(8.12) F has a primitive qth root of unity for every prime q dividing $|\mathrm{Gal}(L/F)|$.

We will prove that $F \subset L$ is radical in this situation. Since $\mathrm{Gal}(L/F)$ is solvable, we have subgroups $\{1_L\} = G_n \subset \cdots \subset G_0 = \mathrm{Gal}(L/F)$ as in Definition 8.1.1. Then consider the fixed fields

$$F_i = L_{G_i} \subset L.$$

Since the Galois correspondence is inclusion-reversing, this gives the fields

$$F = L_{\mathrm{Gal}(L/F)} = L_{G_0} = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n = L_{G_n} = L_{\{1_L\}} = L.$$

Furthermore, since G_i is normal in G_{i-1}, the Galois correspondance together with Theorem 7.2.7 implies that

$$G_{i-1}/G_i \simeq \mathrm{Gal}(F_i/F_{i-1}).$$

Since $[G_{i-1} : G_i]$ is prime, $\mathrm{Gal}(F_i/F_{i-1}) \simeq \mathbb{Z}/q\mathbb{Z}$ for a prime q. By Exercise 5, we know that $q = |\mathrm{Gal}(F_i/F_{i-1})$ divides $\mathrm{Gal}(L/F)|$. By (8.12), F and hence F_{i-1} contain a primitive qth root of unity.

It follows that $F_{i-1} \subset F_i$ satisfies the conditions of Lemma 8.3.2. Thus F_i is obtained from F_{i-1} by adjunction of a qth root of an element of F_{i-1}:

$$F_i = F_{i-1}(\theta_i), \qquad \theta_i \in F_i \setminus F_{i-1}, \quad \theta_i^q \in F_{i-1}.$$

This proves that $F \subset L$ is a radical extension when F satisfies (8.12).

The General Case. Finally, we consider what happens when we only assume that $F \subset L$ is a Galois extension with solvable Galois group.

Write $m = [L : F] = |\mathrm{Gal}(L/F)|$, then m, p are relatively prime, so m is invertible in F.

If $h = x^m - 1$, then $h' = mx^{m-1}$, where m is invertible in F, so the Bézout's relation $m^{-1}h' + hq^{-1} = x(mx^{m-1}) - (x^m - 1) = 1$ proves that $h \wedge h' = 1$, so h is separable. Let K a splitting field of h over L. Let

$$\mathbb{U}_m = \{\xi \in K \mid \xi^m = 1\}$$

the set of the roots of h in K. Then $\mathbb{U}_m$ is a subgroup of K^*, so $\mathbb{U}_m$ is cyclic (Proposition A.5.3), and as h is separable, $|\mathbb{U}_m| = m$, hence $\mathbb{U}_m \simeq \mathbb{Z}/m\mathbb{Z}$, so $\mathbb{U}_m$ has a generator ζ, i.e. a mth primitive root of unity, and

$$\mathbb{U}_m = \{1, \zeta, \zeta^2, \ldots, \zeta^{m-1}\}.$$

(this is Exercise 8.3.1 in characteristic p, where $p \nmid m$.)

Thus $K = L(\zeta)$ is the splitting field of ζ over L, and the proof of Exercise 8.3.2 remains unchanged in characteristic p, so Lemma 8.3.1 is also valid in characteristic p.

So $F \subset L(\zeta)$ is a Galois extension and $\mathrm{Gal}(L(\zeta)/F(\zeta)$ is solvable since $\mathrm{Gal}(L/F)$ is, and

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

This isomorphisms comes from the homomorphism

$$\varphi : \mathrm{Gal}(L(\zeta)/F) \to \mathrm{Gal}(L/F)$$

given by restricting an automorphism of $L(\zeta)$ to L. Since $\mathrm{Gal}(L(\zeta)/F(\zeta))$ is a subgroup of $\mathrm{Gal}(L(\zeta)/F)$, we have a homomorphism

$$\mathrm{Gal}(L(\zeta)/F(\zeta) \to \mathrm{Gal}(L/F)$$

also given by restriction to L. But the kernel of this map is the identity, since elements of the kernel are the identity on both L and $F(\zeta)$. Thus φ is injective, which by Lagrange's Theorem implies that

$$m = |\mathrm{Gal}(L/F)| \text{ is a multiple of } |\mathrm{Gal}(L(\zeta)/F(\zeta))|.$$

Now let q be a prime dividing $|\mathrm{Gal}(L(\zeta)/F(\zeta))|$. Then q divides m, so $q \neq p$. Since ζ is a primitive mth root of unity, $\zeta^{m/p}$ is a primitive pth root of unity (see Exercise 8.3.6).

Since $\zeta^{m/p} \in F(\zeta)$, we conclude that $F(\zeta) \subset L(\zeta)$ satisfies (8.12) with F and L replaced by $F(\zeta)$ and $L(\zeta)$, respectively. It follows that $F(\zeta) \subset L(\zeta)$ is radical by the Special Case. But $F \subset F(\zeta)$ is obviously radical ($\zeta^m = 1 \in F$), so that $F \subset L(\zeta)$ is radical by part (a) of Proposition 8.2.7. Hence

$$F \subset L \text{ is solvable.}$$

□