

# Solutions to David A.Cox "Galois Theory"

Richard Ganaye

February 11, 2020

## 6 Chapter 6 : THE GALOIS GROUP

### 6.1 DEFINITION OF THE GALOIS GROUP

**Ex. 6.1.1** Let  $L = F(\alpha_1, \dots, \alpha_n)$ , and let  $p_i \in F[x]$  be a nonzero polynomial vanishing at  $\alpha_i$ . Explain why the proof of Corollary 6.1.5 implies that  $|\text{Gal}(L/F)| \leq \deg(p_1) \cdots \deg(p_n)$ .

*Proof.*  $L = F(\alpha_1, \dots, \alpha_n)$ , where  $\alpha_i$  is algebraic over  $F$ .  $\alpha_i$  is the root of a polynomial  $p_i \in F[x]$ .

By Proposition 6.1.4, every  $\sigma \in \text{Gal}(L/F)$  is uniquely determined by the images of  $\alpha_i, i = 1, \dots, n$ .  $\alpha_i$  being a root of  $p_i \in F[x]$ ,  $\sigma(\alpha_i)$  is also a root of  $p_i$ . So there exist only  $\deg(p_i)$  possibilities for the choice of  $\sigma(\alpha_i)$ .

More formally, write  $R_i$  the set of the roots of  $p_i$  in  $L$ , then  $\sigma(\alpha_i) \in R_i$ , with  $|R_i| \leq \deg(p_i)$ , and the map

$$\begin{cases} \text{Gal}(L/F) & \rightarrow & R_1 \times \cdots \times R_n \\ \sigma & \mapsto & (\sigma(\alpha_1), \dots, \sigma(\alpha_n)) \end{cases}$$

is injective (one-to-one), since  $\sigma \in \text{Gal}(L/F)$  is uniquely determined by the images of  $\alpha_i, i = 1, \dots, n$ .

Therefore

$$|\text{Gal}(L/F)| \leq |R_1| \times \cdots \times |R_n| \leq \deg(p_1) \cdots \deg(p_n).$$

□

**Ex. 6.1.2** Consider the extension  $\mathbb{Q} \subset L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ . In Exercise 13 of Section 5.1, you used Proposition 5.1.8 to construct an automorphism of  $L$  that takes  $\sqrt{3}$  to  $-\sqrt{3}$  and is the identity on  $\mathbb{Q}(\sqrt{2})$ . By interchanging the roles of 2 and 3 in this construction, explain why all possible signs in (6.1) can occur. This shows that  $|\text{Gal}(L/\mathbb{Q})| = 4$ .

*Proof.* As  $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$  is the splitting field of  $x^2 - 3$  over  $\mathbb{Q}(\sqrt{2})$ , and as  $x^2 - 3$  is irreducible over  $\mathbb{Q}(\sqrt{2})$  (see Exercise 5.1.13), there exists by Proposition 5.1.8 a field isomorphism  $\sigma : L \rightarrow L$  which is identity on  $\mathbb{Q}(\sqrt{2})$  and which takes  $\sqrt{3}$  on  $-\sqrt{3}$ . As  $\sigma$  is identity on  $\mathbb{Q}(\sqrt{2})$ , we have also  $\sigma(\sqrt{2}) = \sqrt{2}$ . As the restriction of  $\sigma$  to  $\mathbb{Q}(\sqrt{2})$  is identity, the restriction of  $\sigma$  to  $\mathbb{Q}$  is the identity on  $\mathbb{Q}$ , so  $\sigma \in \text{Gal}(L/\mathbb{Q})$ .

Similarly  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  is the splitting field of  $x^2 - 2$  over  $\mathbb{Q}(\sqrt{3})$ , and  $x^2 - 2$  is irreducible over  $\mathbb{Q}(\sqrt{3})$  by the Reciprocity Theorem (see Exercise 4.3.6), so there exists by Proposition 5.1.8 a field isomorphism  $\tau : L \rightarrow L$  which is identity on  $\mathbb{Q}(\sqrt{3})$  and which takes  $\sqrt{2}$  on  $-\sqrt{2}$ . As  $\tau$  is identity on  $\mathbb{Q}(\sqrt{3})$ , we have also  $\tau(\sqrt{3}) = \sqrt{3}$ , and  $\tau \in \text{Gal}(L/\mathbb{Q})$ .

Moreover  $1_L(\sqrt{2}) = \sqrt{2}, 1_L(\sqrt{3}) = \sqrt{3}$ , avec  $1_L \in \text{Gal}(L/\mathbb{Q})$ .

Finally  $\sigma\tau = \sigma \circ \tau \in \text{Gal}(L/\mathbb{Q})$  satisfies  $(\sigma\tau)(\sqrt{2}) = -\sqrt{2}, (\sigma\tau)(\sqrt{3}) = -\sqrt{3}$ .

All possibilities in Example 6.1.10 can occur. Consequently  $|\text{Gal}(L/\mathbb{Q})| \geq 4$ . As it is proved in Example 6.1.10 that  $|\text{Gal}(L/\mathbb{Q})| \leq 4$ , then  $|\text{Gal}(L/\mathbb{Q})| = 4$ , and

$$\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \{1_L, \sigma, \tau, \sigma\tau\}.$$

□

**Ex. 6.1.3** This exercise will prove a generalizes form of Proposition 6.1.11.

(a) Let  $\varphi : L_1 \rightarrow L_2$  be an isomorphism of fields. Given a subfield  $F_1 \subset L_1$ , set  $F_2 = \varphi(F_1)$ , which is a subfield of  $L_2$ . Prove that the map sending  $\sigma \in \text{Gal}(L_1/F_1)$  to  $\varphi \circ \sigma \circ \varphi^{-1}$  induces an isomorphism  $\text{Gal}(L_1/F_1) \simeq \text{Gal}(L_2/F_2)$ .

(b) Explain why Proposition 6.1.11 follows from part (a).

*Proof.* (a) If  $\varphi : L_1 \rightarrow L_2$  is a field isomorphism, and  $\sigma \in \text{Gal}(L_1/F_1)$ , then  $\sigma : L_1 \rightarrow L_1$ , and so  $\varphi \circ \sigma \circ \varphi^{-1}$  is a map from  $L_2$  to  $L_2$ , composed of three field isomorphisms, is an automorphism of  $L_2$ .

Moreover, if  $\alpha \in F_2$ , then  $\varphi^{-1}(\alpha) \in F_1$ , since  $F_2 = \varphi(F_1)$ . As  $\sigma \in \text{Gal}(L_1/F_1)$ ,  $\sigma$  is identity on  $F_1$ , thus  $\sigma(\varphi^{-1}(\alpha)) = \varphi^{-1}(\alpha)$ , and  $(\varphi \circ \sigma \circ \varphi^{-1})(\alpha) = \alpha$ . Consequently

$$\varphi \circ \sigma \circ \varphi^{-1} \in \text{Gal}(L_2/F_2).$$

Let

$$\chi : \begin{cases} \text{Gal}(L_1/F_1) & \rightarrow & \text{Gal}(L_2/F_2) \\ \sigma & \mapsto & \varphi \circ \sigma \circ \varphi^{-1} \end{cases}$$

If  $\sigma, \tau \in \text{Gal}(L_1/F_1)$ ,

$$\chi(\sigma)\chi(\tau) = \varphi \circ \sigma \circ \varphi^{-1} \circ \varphi \circ \tau \circ \varphi^{-1} = \varphi \circ \sigma \circ \tau \circ \varphi^{-1} = \chi(\sigma \circ \tau).$$

$\chi$  is so a group homomorphism.

Moreover, if  $\chi(\sigma) = \text{id}$ , alors  $\varphi \circ \sigma \circ \varphi^{-1} = \text{id}$ , then  $\sigma = \varphi^{-1} \circ \varphi = \text{id} : \ker(\chi) = \{\text{id}\}$ , so  $\chi$  is injective.

If  $\tau \in \text{Gal}(L_2/F_2)$ , let  $\sigma = \varphi^{-1} \circ \tau \circ \varphi$ , then  $\sigma \in \text{Gal}(L_1/F_1)$  with the same arguments, and  $\chi(\sigma) = \tau$ , thus  $\chi$  is surjective.

Conclusion :  $\chi : \text{Gal}(L_1/F_1) \rightarrow \text{Gal}(L_2/F_2)$  is a group isomorphism.

(b) Suppose as in Proposition 6.1.11 that the restriction of  $\varphi$  to  $F$  is identity, and let  $F_1 = F$ . Then  $F_2 = \varphi(F_1) = F_1 = F$ , and part (a) shows that

$\chi : \text{Gal}(L_1/F) \rightarrow \text{Gal}(L_2/F), \sigma \mapsto \varphi \circ \sigma \circ \varphi^{-1}$  is a group isomorphism : this is Proposition 6.1.11.

□

**Ex. 6.1.4** In the Historical Notes, we saw that Dedekind defined a "permutation"  $\alpha \rightarrow \alpha'$  to be a map  $\Omega \rightarrow \Omega'$  satisfying  $(\alpha + \beta)' = \alpha' + \beta'$  and  $(\alpha\beta)' = \alpha'\beta'$  for all  $\alpha, \beta \in \Omega$ . Dedekind also assumes that  $\Omega' = \{\alpha' \mid \alpha \in \Omega\}$  and that the  $\alpha'$  are not all zero.

- (a) Show that  $1 \in \Omega$  maps to  $1 \in \Omega'$ . Once this is proved, it follows that  $\alpha \mapsto \alpha'$  is a ring homomorphism (Recall that sending 1 to 1 is part of the definition of ring homomorphism given in Appendix A.)
- (b) Show that the map  $\alpha \rightarrow \alpha'$  is one-to-one. This shows that Dedekind's definition of field is equivalent to ours.

*Proof.* Let  $\varphi : \alpha \rightarrow \alpha'$ . By hypothesis, for all  $\alpha, \beta \in \Omega$ ,

$$\varphi(\alpha + \beta) = \varphi(\alpha) + \varphi(\beta), \varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta).$$

- (a) By hypothesis, there exists  $\alpha \in \Omega$  such that  $\alpha' = \varphi(\alpha) \neq 0$ . Then  $\varphi(\alpha) = \varphi(\alpha \cdot 1) = \varphi(\alpha)\varphi(1)$ , and since  $\varphi(\alpha) \neq 0$ ,  $\alpha' = \varphi(\alpha)$  has an inverse in  $\Omega'$ , thus

$$\varphi(1) = 1.$$

$\varphi$  is so a ring homomorphism between two fields.

- (b) We show that  $\varphi$  is injective:

If  $a \neq 0$ , there exists an inverse  $b$  of  $a$  :  $ab = 1$ , thus  $\varphi(a)\varphi(b) = \varphi(ab) = \varphi(1) = 1$ , therefore  $\varphi(a) \neq 0$ . The kernel of  $\varphi$  is null, thus  $\varphi$  is injective.

As  $\Omega' = \{\varphi(\alpha), \alpha \in \Omega\}$ ,  $\varphi$  is surjective. So  $\varphi : \Omega \rightarrow \Omega'$  is a field isomorphism.

□

**Ex. 6.1.5** Prove the following inequalities:

- (a)  $|\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q})| \leq 8$
- (b)  $|\text{Gal}(\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})/\mathbb{Q})| \leq 2^n$ , where  $p_1, \dots, p_n$  are the first  $n$  primes. In each case, one can show that these are actually equalities.

*Proof.* (a) As  $\sqrt{2}$  is a root of  $f_1 = x^2 - 2$ ,  $\sqrt{3}$  a root of  $f_2 = x^2 - 3$ , and  $\sqrt{5}$  a root of  $f_3 = x^2 - 5$ , Exercise 1 shows that

$$|\text{Gal}(F(\sqrt{2}, \sqrt{3}, \sqrt{5})/F)| \leq \deg(f_1) \deg(f_2) \deg(f_3) = 8.$$

- (b) As  $\sqrt{p_i}$  is a root of  $f_i = x^2 - p_i$ , the same Exercise 1 shows that

$$|\text{Gal}(F(\sqrt{p_1}, \dots, \sqrt{p_n})/F)| \leq \deg(f_1) \cdots \deg(f_n) = 2^n.$$

□

**Ex. 6.1.6** If we apply Exercise 1 to the extension  $\mathbb{Q} \subset L = \mathbb{Q}(\sqrt{6}, \sqrt{10}, \sqrt{15})$ , we get the inequality  $|\text{Gal}(L/\mathbb{Q})| \leq 8$ . Show that  $|\text{Gal}(L/\mathbb{Q})| \leq 4$ .

*Proof.*  $L = \mathbb{Q}(\sqrt{6}, \sqrt{10}, \sqrt{15})$ .

$\sqrt{15} = \sqrt{3 \cdot 5} = 3\frac{\sqrt{10}}{\sqrt{6}} \in \mathbb{Q}(\sqrt{6}, \sqrt{10})$ , therefore

$$L = \mathbb{Q}(\sqrt{6}, \sqrt{10}, \sqrt{15}) = \mathbb{Q}(\sqrt{6}, \sqrt{10}).$$

Then Exercise 1 shows that

$$|\text{Gal}(L/\mathbb{Q})| \leq 4$$

Note : moreover,  $x^2 - 10$  is irreducible over  $\mathbb{Q}(\sqrt{6})$ , otherwise the roots  $\pm\sqrt{10}$  of  $f$  would be in  $\mathbb{Q}(\sqrt{6})$ , and then

$$\sqrt{10} = a + b\sqrt{6}, \quad a, b \in \mathbb{Q}(\sqrt{6}).$$

By squaring, we obtain  $10 = a^2 + 6b^2 + 2ab\sqrt{6}$ . The irrationality of  $\sqrt{6}$  shows that  $ab = 0$ ,  $a^2 + 6b^2 = 10$ . Since  $\sqrt{10}$  and  $\sqrt{\frac{5}{3}}$  are irrational, this system has no solution in  $\mathbb{Q} \times \mathbb{Q}$ .

$x^2 - 10$  is irreducible over  $\mathbb{Q}(\sqrt{6})$ , thus

$$[\mathbb{Q}(\sqrt{6}, \sqrt{10}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{6}, \sqrt{10}) : \mathbb{Q}(\sqrt{6})] \cdot [\mathbb{Q}(\sqrt{6}) : \mathbb{Q}] = 4.$$

Using section 6.2, as  $L$  is the splitting field of the separable polynomial  $(x^2 - 6)(x^2 - 10)$  over  $\mathbb{Q}$ , we obtain

$$|\text{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}] = 4.$$

□

**Ex. 6.1.7** Let  $F \subset L$  be a finite extension, and let  $\sigma : L \rightarrow L$  be a ring homomorphism that is the identity on  $F$ . This exercise will show that  $\sigma$  is an automorphism.

(a) Show that  $\sigma$  is one-to-one.

(b) Show that  $\sigma$  is onto.

*Proof.* (a) Let  $a \in L, a \neq 0$ . Then  $a$  has an inverse  $b$  in the field  $L$ , so  $ab = 1$ ,  $\sigma(a)\sigma(b) = \sigma(1) = 1$ ,  $\sigma(a) \neq 0$ . Therefore  $\ker(\sigma) = \{0\}$ , thus  $\sigma$  is injective.

$\sigma : L \rightarrow L$  is an injective field homomorphism.

(b) As  $K \subset L$  is a finite extension,  $L$  is a finite dimensional vector space over  $F$ . As  $\sigma$  is identity on  $F$ ,  $\sigma : L \rightarrow L$  is an injective linear application on a finite dimensional vector space, thus  $\sigma$  is also surjective :

$$\sigma \in \text{Gal}(L/F).$$

□

## 6.2 GALOIS GROUPS OF SPLITTING FIELDS

**Ex. 6.2.1** Complete Example 6.2.2 by showing that  $\text{Gal}(L/\mathbb{Q}) = \{1_L, \sigma, \tau, \sigma\tau\}$  and that  $\text{Gal}(L/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .

*Proof.* We proved in Exercise 6.1.2 that

$$G := \text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \{1_L, \sigma, \tau, \sigma\tau\}.$$

Every group of order 4 is abelian, and isomorphic to  $\mathbb{Z}/4\mathbb{Z}$  or  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .

As  $G$  has at least 2 elements of order 2, since  $\sigma^2 = \tau^2 = 1_L$ . This is not the case in  $\mathbb{Z}/4\mathbb{Z}$ . Thus

$$\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

□

**Ex. 6.2.2** Consider  $\mathbb{Q} \subset L = \mathbb{Q}(\omega, \sqrt[3]{2})$ , where  $\omega = e^{2\pi i/3}$ .

(a) Explain why  $\sigma \in \text{Gal}(L/\mathbb{Q})$  is uniquely determined by  $\sigma(\omega) \in \{\omega, \omega^2\}$  and  $\sigma(\sqrt[3]{2}) \in \{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\}$ .

(b) Explain why all possible combinations for  $\sigma(\omega)$  and  $\sigma(\sqrt[3]{2})$  actually occur.

In the next section we will show that  $\text{Gal}(L/\mathbb{Q}) \simeq S_3$ .

*Proof.* (a) As  $L = \mathbb{Q}(\omega, \sqrt[3]{2})$ , Proposition 6.1.4(b) shows that  $\sigma \in \text{Gal}(L/\mathbb{Q})$  is uniquely determined by  $\sigma(\omega), \sigma(\sqrt[3]{2})$ .

Moreover, by theorem 6.1.4 (a),  $\sigma(\omega)$  is a root of  $f = x^2 + x + 1$ , whose roots are  $\omega, \omega^2$ , and  $\sigma(\sqrt[3]{2})$  is a root of  $g = x^3 - 2$  whose roots are  $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$ .

Then Exercise 6.1.1 shows that

$$|\text{Gal}(L/\mathbb{Q})| \leq \deg(f) \deg(g) = 6.$$

(b)  $L$  is the splitting field of the separable irreducible polynomial  $g = x^3 - 2 \in \mathbb{Q}[x]$ . Indeed,  $g$  is irreducible over  $\mathbb{Q}$  since  $\deg(g) = 3$  and  $g$  has no root in  $\mathbb{Q}$ , and separable since its roots in  $\mathbb{C}$  are  $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$  which are distinct.

By theorem 6.2.1,  $|\text{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}]$ , and by Exercise 5.1.8,  $[L : \mathbb{Q}] = 2 \times 3 = 6$ , therefore

$$|\text{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}] = 6.$$

If all possible combinations for  $\sigma(\omega)$  and  $\sigma(\sqrt[3]{2})$  don't actually occur, then  $|\text{Gal}(L/\mathbb{Q})| < 6$ , which is false, so all possible combinations occur.

□

**Ex. 6.2.3** Consider  $\mathbb{Q} \subset L = \mathbb{Q}(\zeta_5, \sqrt[5]{2})$ , where  $\zeta_5 = e^{2\pi i/5}$ . By proposition 4.2.5, the minimal polynomial of  $\zeta_5$  over  $\mathbb{Q}$  is  $x^4 + x^3 + x^2 + x + 1$ .

(a) Show that  $[L : \mathbb{Q}] = 20$ .

(b) Show that  $L$  is the splitting field of  $x^5 - 2$  over  $\mathbb{Q}$ , and conclude that  $\text{Gal}(L/\mathbb{Q})$  is a group of order 20.

We will describe the structure of this Galois group in section 6.4.

*Proof.* Write  $\zeta = \zeta_5$ .

(a) as  $L = \mathbb{Q}(\zeta, \sqrt[5]{2})$ , Proposition 6.1.4(b) shows that  $\sigma \in \text{Gal}(L/\mathbb{Q})$  is uniquely determined by  $\sigma(\zeta), \sigma(\sqrt[5]{2})$ .

Moreover by Proposition 6.4.1(a),  $\sigma(\zeta)$  is a root of  $f = x^4 + x^3 + x^2 + x + 1$ , whose roots are  $\zeta^i$ ,  $1 \leq i \leq 4$ , and  $\sigma(\sqrt[5]{2})$  is a root of  $g = x^5 - 2$ , whose roots are  $\zeta^j \sqrt[5]{2}$ ,  $0 \leq j \leq 4$ .

Then Exercise 6.1.1 shows that

$$|\text{Gal}(L/\mathbb{Q})| \leq \deg(f) \deg(g) = 20.$$

(b)  $L$  is the splitting field of the separable irreducible polynomial  $g = x^5 - 2 \in \mathbb{Q}[x]$  over  $\mathbb{Q}$ . Indeed,  $g$  is irreducible over  $\mathbb{Q}$  by Schönemann-Eisenstein Criterion with  $p = 2$ , and separable since its roots in  $\mathbb{C}$  are  $\sqrt[5]{2}, \zeta \sqrt[5]{2}, \zeta^2 \sqrt[5]{2}, \zeta^3 \sqrt[5]{2}, \zeta^4 \sqrt[5]{2}$  which are distinct.

By theorem 6.2.1,  $|\text{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}]$ , and by Exercise 5.1.8,  $[L : \mathbb{Q}] = 4 \times 5 = 20$ , therefore

$$|\text{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}] = 20.$$

□

**Ex. 6.2.4** Consider the  $n$ th root of unity  $\zeta_n = e^{2\pi i/n}$ . We call  $\mathbb{Q} \subset \mathbb{Q}(\zeta_n)$  a cyclotomic extension of  $\mathbb{Q}$ .

(a) Show that  $\mathbb{Q} \subset \mathbb{Q}(\zeta_n)$  is a splitting field of a separable polynomial.

(b) Given  $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ , show that  $\sigma(\zeta_n) = \zeta_n^i$  for some integer  $i$ .

(c) Show that the integer  $i$  in part (b) is relatively prime to  $n$ .

(d) The set of congruence classes modulo  $n$  relatively prime to  $n$  form a group under multiplication, denoted  $(\mathbb{Z}/n\mathbb{Z})^*$ . Show that the map  $\sigma \mapsto [i]$ , where  $\sigma(\zeta_n) = \zeta_n^i$ , define a one-to-one group homomorphism  $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \rightarrow (\mathbb{Z}/n\mathbb{Z})^*$ .

(e) The order of  $(\mathbb{Z}/n\mathbb{Z})^*$  is  $|(\mathbb{Z}/n\mathbb{Z})^*| = \phi(n)$ , where  $\phi(n)$  is the Euler  $\phi$ -function from number theory. Prove that the homomorphism of part (d) is an isomorphism if and only if  $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$ .

(f) Let  $p$  be prime. Use part (e) and Proposition 4.2.5 to show that  $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^*$ .

In chapter 9 we will prove that  $[Q(\zeta_n) : \mathbb{Q}] = \phi(n)$ . By part (e), this will imply that there is an isomorphism  $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$  for all  $n$ .

*Proof.* (a)  $\zeta_n$  is a root of  $x^n - 1 \in \mathbb{Q}[x]$ . Write  $\mathbb{U}_n$  the set of  $n$ th roots of unity in  $\mathbb{C}$  :

$$\mathbb{U}_n = \{\zeta_n^k, 0 \leq k \leq n-1\}$$

and  $|\mathbb{U}_n| = n$ .

As  $x^n - 1 = \prod_{\zeta \in \mathbb{U}_n} (x - \zeta)$ ,  $x^n - 1$  is separable, and the splitting field of  $x^n - 1$  over  $\mathbb{Q}$  is  $\mathbb{Q}(\zeta, \dots, \zeta^{n-1}) = \mathbb{Q}(\zeta)$

Conclusion :  $\mathbb{Q}(\zeta_n)$  is the splitting field of the separable polynomial  $x^n - 1 \in \mathbb{Q}[x]$  over  $\mathbb{Q}$ .

(b) Soit  $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q})$ .

As  $\zeta_n$  is a root of  $x^n - 1 \in \mathbb{Q}[x]$ , by Proposition 6.1.4(a)  $\sigma(\zeta_n)$  is a root of  $x^n - 1$ , thus  $\sigma(\zeta_n) \in \mathbb{U}_n$ , so

$$\sigma(\zeta_n) = \zeta_n^i, i \in \mathbb{N}.$$

(c) Note that  $\zeta_n = e^{2i\pi/n}$  is an element of order  $n$  in the group  $\mathbb{U}_n$ . Indeed, for all  $k \in \mathbb{Z}$ ,

$$\zeta_n^k = 1 \iff e^{2i\pi k/n} = 1 \iff k/n \in \mathbb{Z} \iff n \mid k.$$

$\sigma$  being a field isomorphism,  $\sigma(\zeta_n) \in \mathbb{U}_n$  is also of order  $n$ . Indeed, for all  $k \in \mathbb{Z}$ ,

$$\sigma(\zeta_n)^k = 1 \iff \sigma(\zeta_n^k) = 1 \iff \zeta_n^k = 1 \iff n \mid k.$$

If the order of an element  $\zeta$  is  $|\zeta| = n$ , then for all integer  $j$ , the order of  $\zeta^j$  in  $\mathbb{U}_n$  is

$$|\zeta^j| = \frac{n}{n \wedge j}.$$

Indeed for all  $k \in \mathbb{Z}$ ,

$$(\zeta^j)^k = 1 \iff n \mid jk \iff \frac{n}{n \wedge j} \mid \frac{j}{n \wedge j} k \iff \frac{n}{n \wedge j} \mid k \text{ (since } \frac{n}{n \wedge j} \wedge \frac{j}{n \wedge j} = 1).$$

If we apply this result to  $\zeta_n^i = \sigma(\zeta_n)$ , on obtient

$$\frac{n}{n \wedge i} = |\zeta_n^i| = |\sigma(\zeta_n)| = n,$$

thus

$$n \wedge i = 1.$$

(d) Let

$$\varphi : \begin{cases} \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) & \rightarrow & (\mathbb{Z}/n\mathbb{Z})^* \\ \sigma & \mapsto & [i] : \sigma(\zeta_n) = \zeta_n^i \end{cases}$$

We show that  $\varphi$  is a group homomorphism.

If  $\sigma, \tau \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ , and  $\varphi(\sigma) = [i], \varphi(\tau) = [j]$ , then  $\sigma(\zeta_n) = \zeta_n^i, \tau(\zeta_n) = \zeta_n^j$ , thus

$$(\sigma \circ \tau)(\zeta_n) = \sigma((\zeta_n)^j) = (\sigma(\zeta_n))^j = (\zeta_n^i)^j = \zeta_n^{ij},$$

therefore

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

$\varphi$  is injective :

If  $\varphi(\sigma) = [1]$ , then  $\sigma(\zeta_n) = \zeta_n$ . Since  $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ ,  $\sigma$  is uniquely determined by the image of  $\zeta_n$ , thus  $\sigma = 1_{\mathbb{Q}(\zeta_n)}$ . The kernel of  $\varphi$  is trivial, thus  $\varphi$  is injective.

Conclusion : there exist an injective group homomorphism

$$\varphi : \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \rightarrow (\mathbb{Z}/n\mathbb{Z})^*.$$

(e) As  $\mathbb{Q}(\zeta_n)$  is the splitting field of a separable polynomial over  $\mathbb{Q}$ ,

$$|\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = [\mathbb{Q}(\zeta_n) : \mathbb{Q}].$$

If we suppose that  $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$ ,  $\varphi$  is an injection between two set of same cardinality, thus  $\varphi$  is a bijection, and so  $\varphi$  is a group isomorphism. Reciprocally, if  $\varphi$  is a group isomorphism, then  $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = |\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = \phi(n)$

Conclusion :  $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$  if and only if  $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$ .

(f) If  $p$  is prime, we know that  $f = 1 + x + \dots + x^{p-1}$  is irreducible over  $\mathbb{Q}$ , so  $f$  is the minimal polynomial of  $\zeta_p$  over  $\mathbb{Q}$ . This implies that  $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1 = \phi(p)$ .

By part (e), we know then that  $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^*$  (and so this group is cyclic).

□

**Ex. 6.2.5** Let  $F$  have characteristic  $p$ , and assume that  $f = x^p - x + a \in F[x]$  is irreducible over  $F$ . Then let  $L = F(\alpha)$ , where  $\alpha$  is a root of  $f$  in some splitting field. In Exercise 16 of Section 5.3, you showed that  $F \subset L$  is a normal extension.

(a) Show that  $|\text{Gal}(L/F)| = p$ , and use this to prove that  $|\text{Gal}(L/F)| \simeq \mathbb{Z}/p\mathbb{Z}$ .

(b) Exercise 15 of Section 5.3 showed that  $\alpha + 1$  is a root of  $f$ . For  $i = 0, \dots, p - 1$ , show that there is a unique element of  $\text{Gal}(L/F)$  that takes  $\alpha$  to  $\alpha + i$ .

(c) Use part (b) to describe an explicit isomorphism  $\text{Gal}(L/F) \simeq \mathbb{Z}/p\mathbb{Z}$ .

*Proof.* (a)  $L = F(\alpha)$  and  $\alpha$  has for minimal polynomial  $f = x^p - x + a$ , thus  $[L : F] = p$ .

By Exercise 5.3.16, we know that  $L = F(\alpha) = F(\alpha, \alpha + 1, \dots, \alpha + p - 1)$  is the splitting field of

$$f = x^p - x - a = (x - \alpha)(x - \alpha - 1) \cdots (x - \alpha - p + 1).$$

Therefore  $F(\alpha)$  is the splitting field of a separable polynomial  $f \in F[x]$ , and by theorem 6.2.1

$$|\text{Gal}(L/F)| = [L : F] = p.$$

Every group of order  $p$ , where  $p$  is prime, is cyclic and isomorphic to  $\mathbb{Z}/p\mathbb{Z}$  :

$$\text{Gal}(L/F) \simeq \mathbb{Z}/p\mathbb{Z}.$$



- (b)  $F \subset L$  is by part (a) a normal extension, and  $f \in F[x]$  is irreducible over  $F$  by hypothesis. The roots of  $f$  in  $L$  are  $\alpha, \alpha + 1, \dots, \alpha + p - 1$ . By Proposition 5.1.8, there exists a field isomorphism  $\sigma_i : L \rightarrow L$  which is identity on  $F$  and which takes  $\alpha$  on  $\alpha + i, i \in \mathbb{F}_p$ . Then  $\sigma_i \in \text{Gal}(L/F), \sigma(\alpha) = \alpha + i$ . As  $L = F(\alpha)$ ,  $\sigma$  is uniquely determined by the image of  $\alpha$ .

Conclusion:  $\alpha$  being a fixed root of  $f$ , and  $i \in \mathbb{F}_p$ , there exist a unique  $\sigma_i \in \text{Gal}(L/F)$  such that  $\sigma_i(\alpha) = \alpha + i$ .

- (c) Let

$$\varphi \begin{cases} \text{Gal}(L/F) & \rightarrow \mathbb{F}_p \\ \sigma & \mapsto \sigma(\alpha) - \alpha \end{cases}$$

- For all  $\sigma \in \text{Gal}(L/F)$ ,  $\varphi(\sigma) \in \mathbb{F}_p$  since  $\sigma(\alpha)$  is a root of  $f$ , so  $\sigma(\alpha) - \alpha = i \in \mathbb{F}_p$ .
- $\varphi$  is bijective by part(b), since for all  $i \in \mathbb{F}_p$ , there exists a unique  $\sigma \in \text{Gal}(L/F)$  such that  $\varphi(\sigma) = \sigma(\alpha) - \alpha = i$ .
- $\varphi$  is a group homomorphism : if  $\sigma, \tau \in \text{Gal}(L/F)$ , and  $\varphi(\sigma) = i, \varphi(\tau) = j$ , then  $\sigma(\alpha) = \alpha + i, \tau(\alpha) = \alpha + j$  ( $i, j \in \mathbb{F}_p$ ).

$(\sigma \circ \tau)(\alpha) = \sigma(\alpha + j) = \sigma(\alpha) + \sigma(j) = (\alpha + i) + j = \alpha + (i + j)$  ( $\sigma(j) = j$  since  $\sigma$  is identity on  $F$ , a fortiori on  $\mathbb{F}_p \subset F$ ).

As  $(\sigma \circ \tau)(\alpha) = \alpha + (i + j)$ ,  $\varphi(\sigma \circ \tau) = i + j = \varphi(\sigma) + \varphi(\tau)$ .

$\varphi : \text{Gal}(L/F) \rightarrow \mathbb{F}_p$  is so a group isomorphism.

□

**Ex. 6.2.6** Let  $f \in F[x]$  be irreducible and separable of degree  $n$ , and let  $F \subset L$  be a splitting field of  $f$ . Prove that  $n$  divides  $|\text{Gal}(L/F)|$ .

*Proof.* Let  $L$  a splitting field of  $f$  over  $F$ , where  $f$  is a separable irreducible polynomial. By Proposition 6.2.1 (using the separability of  $f$ ) :

$$|\text{Gal}(L/F)| = [L : F].$$

Let  $\alpha$  a root of  $f$  in  $L$ . As  $f$  is irreducible,  $f$  is the minimal polynomial of  $\alpha$  over  $F$ , thus  $[F(\alpha) : F] = \deg(f) = n$ , and

$$[L : F] = [L : F(\alpha)] [F(\alpha) : F] = n[L : F(\alpha)] :$$

So  $n$  divides  $|\text{Gal}(L/F)|$ .

□

### 6.3 PERMUTATION OF THE ROOTS

**Ex. 6.3.1** Consider  $\text{Gal}(L/\mathbb{Q})$ , where  $L = \mathbb{Q}(\omega, \sqrt[3]{2}), \omega = e^{2\pi i/3}$ . By Exercise 2 of section 6.2, there are  $\sigma, \tau \in \text{Gal}(L/\mathbb{Q})$  such that

$$\sigma(\sqrt[3]{2}) = \omega \sqrt[3]{2}, \sigma(\omega) = \omega \quad \text{and} \quad \tau(\sqrt[3]{2}) = \sqrt[3]{2}, \tau(\omega) = \omega^2.$$

Find the permutations in  $S_3$  corresponding to  $\sigma$  and  $\tau$ .

*Proof.*  $L = \mathbb{Q}(\omega, \sqrt[3]{2})$  is the splitting field over  $\mathbb{Q}$  of  $f = x^3 - 2$ .

By Exercise 6.2.2, there exist  $\sigma, \tau \in \text{Gal}(L/\mathbb{Q})$  such that

$$\sigma(\sqrt[3]{2}) = \omega\sqrt[3]{2}, \sigma(\omega) = \omega \quad \text{and} \quad \tau(\sqrt[3]{2}) = \sqrt[3]{2}, \tau(\omega) = \omega^2.$$

Number the roots of  $f$  by  $\alpha_1 = \sqrt[3]{2}, \alpha_2 = \omega\sqrt[3]{2}, \alpha_3 = \omega^2\sqrt[3]{2}$ .

Then  $\sigma(\alpha_1) = \alpha_2, \sigma(\alpha_2) = \alpha_3, \sigma(\alpha_3) = \alpha_1$ . If we write  $\tilde{\sigma} = (1, 2, 3)$ , then for  $i = 1, 2, 3, \sigma(\alpha_i) = \alpha_{\tilde{\sigma}(i)}$ , so the 3-cycle  $\tilde{\sigma} = (1, 2, 3)$  corresponds to  $\sigma$ .

$\tau(\alpha_1) = \alpha_1, \tau(\alpha_2) = \alpha_3, \tau(\alpha_3) = \alpha_2$ , so  $\tilde{\tau} = (2, 3)$  corresponds to  $\tau$ .

As  $S_3$  is generated by  $\tilde{\sigma}, \tilde{\tau}$ ,  $\text{Gal}(L/\mathbb{Q})$  is generated by  $\sigma, \tau$ .  $\square$

**Ex. 6.3.2** For each of the following Galois groups, find an explicit subgroup of  $S_4$  that is isomorphic to the group. Also, the Galois group is isomorphic to which known group?

(a)  $\text{Gal}(\mathbb{Q}(i, \sqrt{2})/\mathbb{Q})$ .

(b)  $\text{Gal}(\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q})$ .

*Proof.* (a)  $\text{Gal}(\mathbb{Q}(i, \sqrt{2})/\mathbb{Q}) = \{1_{\mathbb{Q}}, \sigma, \tau, \sigma\tau\}$ , where

$$\sigma(i) = -i, \sigma(\sqrt{2}) = \sqrt{2},$$

$$\tau(i) = i, \tau(\sqrt{2}) = -\sqrt{2}.$$

As every  $g \in \text{Gal}(\mathbb{Q}(i, \sqrt{2})/\mathbb{Q})$  satisfies  $g^2 = 1_{\mathbb{Q}}$ ,

$$\text{Gal}(\mathbb{Q}(i, \sqrt{2})/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

(ViertelGruppe de Klein : cf Exercise 6.2.1 and example 6.2.2 for more details).

If we number the roots by  $\alpha_1 = i, \alpha_2 = -i, \alpha_3 = \sqrt{2}, \alpha_4 = -\sqrt{2}$ , then  $(1, 2)$  corresponds to  $\sigma$ , and  $(3, 4)$  to  $\tau$ .

As subgroup of  $S_4$ ,  $\text{Gal}(\mathbb{Q}(i, \sqrt{2})/\mathbb{Q})$  is represented by

$$\{(), (1, 2), (3, 4), (1, 2)(3, 4)\} = \langle (1, 2), (3, 4) \rangle \simeq \text{Gal}(\mathbb{Q}(i, \sqrt{2})/\mathbb{Q}).$$

(b)

$$\begin{aligned} f &= x^4 - 2 \\ &= (x^2 - \sqrt{2})(x^2 + \sqrt{2}) \\ &= (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x + i\sqrt[4]{2})(x - i\sqrt[4]{2}) \end{aligned}$$

The splitting root of  $f$  over  $\mathbb{Q}$  is so  $L = \mathbb{Q}(i, i\sqrt[4]{2}) = \mathbb{Q}(i, \sqrt[4]{2})$ .  $f$  is separable, since  $f$  has simple roots in its splitting field.  $L$  is so the splitting field over  $\mathbb{Q}$  of a separable polynomial, therefore by Theorem 6.2.1,

$$|\text{Gal}(L : \mathbb{Q})| = [L : \mathbb{Q}].$$

$f$  is irreducible over  $\mathbb{Q}$  by the Schönemann-Eisenstein Criterion with  $p = 2$ . As  $f$  is irreducible over  $\mathbb{Q}$ ,

$$[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = \deg(f) = 4,$$

and  $x^2 + 1$  is irreducible over  $\mathbb{Q}(\sqrt[4]{2})$ , since it is of degree 2, without root in  $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$ , thus

$$[\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}(\sqrt[4]{2})] = 2.$$

Consequently,

$$[\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}] = [\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}(\sqrt[4]{2})] [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 8,$$

and so

$$|\text{Gal}(L : \mathbb{Q})| = 8.$$

If  $\sigma \in \text{Gal}(L/\mathbb{Q})$ , as  $i$  is a root of  $x^2 + 1 \in \mathbb{Q}[x]$ , and  $\sqrt[4]{2}$  a root of  $x^4 - 2 \in \mathbb{Q}[x]$ , then  $\sigma(i) = \pm i$ , et  $\sigma(\sqrt[4]{2}) = i^k \sqrt[4]{2}$ ,  $k = 0, 1, 2, 3$ . as  $\sigma$  is uniquely determined by the images of  $i, \sqrt[4]{2}$ , and as  $|\text{Gal}(L : \mathbb{Q})| = 8$ , these 8 possibilities occur, thus  $G = \text{Gal}(L/\mathbb{Q}) = \{\sigma_{j,k} \mid 0 \leq j \leq 1, 0 \leq k \leq 3\}$ , where  $\sigma_{j,k}$ , which is identity on  $\mathbb{Q}$ , is determined by

$$\sigma_{j,k}(i) = (-1)^j i, \sigma_{j,k}(\sqrt[4]{2}) = i^k \sqrt[4]{2}.$$

Write  $\tau : L \rightarrow L, z \mapsto \bar{z}$  the complex conjugation restricted to  $L$ .  $\tau$  is a ring homomorphism and an involution, thus  $\tau$  is a field automorphism of  $L$ , which is identity on  $\mathbb{Q}$ , so  $\tau \in G$ . Moreover

$$\tau(i) = -i, \tau(\sqrt[4]{2}) = \sqrt[4]{2},$$

Let  $\sigma \in \text{Gal}(L/\mathbb{Q})$  defined by

$$\sigma(i) = i, \sigma(\sqrt[4]{2}) = i\sqrt[4]{2}.$$

Then  $\tau = \sigma_{1,0}, \sigma = \sigma_{0,1}$ .

As  $\tau^2 = 1_L$  and  $\tau \neq e$ , the order of  $\tau$  is 2.

$\sigma^4(i) = i$  and  $\sigma^4(\sqrt[4]{2}) = \sqrt[4]{2}$ , thus  $\sigma^4 = e$ . As  $\sigma^2(\sqrt[4]{2}) = i^2 \sqrt[4]{2} = -\sqrt[4]{2}, \sigma^2 \neq e$ , thus the order of  $\sigma$  is 4.

$$|\tau| = 2, \quad |\sigma| = 4.$$

As  $\tau(i) = -i, \tau \notin \langle \sigma \rangle$ . Thus the subgroup  $\langle \sigma, \tau \rangle$  of  $G$  contains at least 5 elements, so is equal to  $G$  by Lagrange's Theorem :

$$G = \langle \sigma, \tau \rangle.$$

As the index of  $H = \langle \sigma \rangle$  in  $G$  is 2, and  $\tau \notin H, G = H \cup \tau H$  :

$$G = \text{Gal}(L/\mathbb{Q}) = \{1_L, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3\}.$$

If we number the roots of  $f$  by  $\alpha_k = i^{k-1} \sqrt[4]{2}$ , for  $k = 1, 2, 3, 4$ , then  $\tau$  corresponds to the transposition  $(2, 4)$ , and  $\sigma$  to the cycle  $(1, 2, 3, 4)$  :

$$G \simeq \langle (1, 2, 3, 4), (2, 4) \rangle \subset S_4.$$

If we number the 4 summits of a square by 1,2,3,4 in the direct orientation, then  $\sigma$  corresponds to a rotation of angle  $\pi/2$ , and  $\tau$  to a symmetry with respect to the

diagonal  $[1, 3]$ . They generate the group of isometry of the square, which is the dihedral group  $D_8$ , defined also by generators and relations :

$$G = \langle \sigma, \tau \rangle, \sigma^4 = \tau^2 = e, \tau\sigma = \sigma^{-1}\tau.$$

(En effet,  $\tilde{\sigma}^{-1}\tilde{\tau} = (1, 4, 3, 2)(2, 4) = (4, 3, 2, 1) = (2, 4)(1, 2, 3, 4) = \tilde{\tau}\tilde{\sigma}$ .)

As a verification, the following GAP instruction confirm the result  $D_8$  :

```
G:= Group((1,2,3,4),(2,4));
StructureDescription(G);
"D8"
```

□

**Ex. 6.3.3** In the terminology of Exercise 2,  $\text{Gal}(\mathbb{Q}(i, \sqrt{2}, \sqrt{3})/\mathbb{Q})$  is isomorphic to which known group? Explain your reasoning in detail.

*Proof.* We have already proved (Ex. 5.1.13) that  $f = x^2 - 3$  is irreducible over  $\mathbb{Q}[\sqrt{2}]$ .  $f$  is so the minimal polynomial of  $\sqrt{3}$  over  $\mathbb{Q}(\sqrt{2})$ , thus  $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = \deg(f) = 2$ .

As  $g = x^2 - 2$  is irreducible over  $\mathbb{Q}$ ,  $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = \deg(g) = 2$ , therefore

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4.$$

Moreover,  $h = x^2 + 1$  has no real root, a fortiori  $h$  has no root in  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ . As  $\deg(h) = 2$ ,  $h$  is irreducible over  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ ,  $h$  is the minimal polynomial of  $i$  over  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ , thus  $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, i) : \mathbb{Q}(\sqrt{2}, \sqrt{3})] = 2$ , and by the Tower Theorem, and the equality  $\mathbb{Q}(\sqrt{2}, \sqrt{3}, i) = \mathbb{Q}(i, \sqrt{2}, \sqrt{3})$ ,

$$[\mathbb{Q}(i, \sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 8.$$

$L = \mathbb{Q}(i, \sqrt{2}, \sqrt{3})$  is the splitting field of  $p = (x^2 + 1)(x^2 - 2)(x^2 - 3)$  over  $\mathbb{Q}$ , and  $p = (x - i)(x + i)(x - \sqrt{2})(x + \sqrt{2})(x - \sqrt{3})(x + \sqrt{3})$  is separable. By theorem 6.2.1, we obtain

$$|\text{Gal}(L : \mathbb{Q})| = [L : \mathbb{Q}] = 8.$$

If  $\sigma \in \text{Gal}(L : \mathbb{Q})$ ,  $\sigma(i) = \pm i, \sigma(\sqrt{2}) = \pm\sqrt{2}, \sigma(\sqrt{3}) = \pm\sqrt{3}$ . As  $|\text{Gal}(L : \mathbb{Q})| = 8$ , all of these possibilities occur: there exist 8  $\mathbb{Q}$ -automorphisms of  $L$  satisfying these equalities. As  $L = \mathbb{Q}(i, \sqrt{2}, \sqrt{3})$ ,  $\sigma \in \text{Gal}(L : \mathbb{Q})$  is uniquely determined by the images of these 3 elements.

In particular, there exist  $\sigma_1, \sigma_2, \sigma_3 \in \text{Gal}(L : \mathbb{Q})$  defined by

$$\begin{aligned} \sigma_1(i) &= -i, & \sigma_1(\sqrt{2}) &= \sqrt{2}, & \sigma_1(\sqrt{3}) &= \sqrt{3} \\ \sigma_2(i) &= i, & \sigma_2(\sqrt{2}) &= -\sqrt{2}, & \sigma_2(\sqrt{3}) &= \sqrt{3} \\ \sigma_3(i) &= i, & \sigma_3(\sqrt{2}) &= \sqrt{2}, & \sigma_3(\sqrt{3}) &= -\sqrt{3} \end{aligned}$$

and  $1_L, \sigma_1, \sigma_2, \sigma_3, \sigma_1\sigma_2, \sigma_1\sigma_3, \sigma_2\sigma_3, \sigma_1\sigma_2\sigma_3$  give distinct images to  $i, \sqrt{2}, \sqrt{3}$ , thus

$$G := \text{Gal}(L : \mathbb{Q}) = \{1_L, \sigma_1, \sigma_2, \sigma_3, \sigma_1\sigma_2, \sigma_1\sigma_3, \sigma_2\sigma_3, \sigma_1\sigma_2\sigma_3\}.$$

Therefore

$$G = \langle \sigma_1, \sigma_2, \sigma_3 \rangle.$$

Note that  $\sigma_1\sigma_2 = \sigma_2\sigma_1$  since they give the same images to  $i, \sqrt{2}, \sqrt{3}$ . Similarly  $\sigma_1\sigma_3 = \sigma_3\sigma_1$  and  $\sigma_2\sigma_3 = \sigma_3\sigma_2$ . Thus  $G$  is abelian, generated by 3 elements of order 2, with  $\sigma_2 \notin \langle \sigma_1 \rangle, \sigma_3 \notin \langle \sigma_1, \sigma_2 \rangle$ . Therefore  $G$  is the direct sum of the 3 subgroups  $\{e, \sigma_i\}$ ,  $i = 1, 2, 3$ , d'ordre 2 :

$$\text{Gal}(L : \mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^3.$$

Some instructions Sage and Gap to verify these results :

```
f=(x-i-sqrt(2)-sqrt(3))*(x-i-sqrt(2)+sqrt(3))*(x+i-sqrt(2)-sqrt(3))
*(x-i+sqrt(2)+sqrt(3))*(x+i-sqrt(2)-sqrt(3))*(x+i-sqrt(2)+sqrt(3))
*(x+i+sqrt(2)-sqrt(3))*(x+i+sqrt(2)+sqrt(3));f
(x + sqrt(3) + sqrt(2) + i)(x + sqrt(3) + sqrt(2) - i)(x + sqrt(3) - sqrt(2) + i)(x + sqrt(3) - sqrt(2) - i)
(x - sqrt(3) + sqrt(2) + i)(x - sqrt(3) + sqrt(2) - i)(x - sqrt(3) - sqrt(2) + i)(x - sqrt(3) - sqrt(2) - i)

g=f.expand();g
x^8 - 16x^6 + 88x^4 + 192x^2 + 144

g.factor()
x^8 - 16x^6 + 88x^4 + 192x^2 + 144

x=polygen(QQ,'x')
K.<z> = NumberField(x^8-16*x^6+88*x^4+192*x^2+144)
G = K.galois_group();G
<((1,2)(3,4)(5,6)(7,8),(1,3)(2,4)(5,7)(6,8),(1,5)(2,6)(3,7)(4,8))>
```

With Gap :

```
G:=Group((1,2)(3,4)(5,6)(7,8),(1,3)(2,4)(5,7)(6,8),(1,5)(2,6)(3,7)(4,8));
StructureDescription(G);
C2 x C2 x C2
```

As  $x^8 - 16x^6 + 88x^4 + 192x^2 + 144$  is irreducible over  $\mathbb{Q}$ ,  $[\mathbb{Q}(i + \sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 8 = [L : \mathbb{Q}]$ , and since  $\mathbb{Q}(i + \sqrt{2} + \sqrt{3}) \subset L$ ,  $L = \mathbb{Q}(i + \sqrt{2} + \sqrt{3})$ .

These results imply that  $L = \mathbb{Q}(i, \sqrt{2}, \sqrt{3})$  is the splitting field of the irreducible polynomial  $x^8 - 16x^6 + 88x^4 + 192x^2 + 144$ , that  $i + \sqrt{2} + \sqrt{3}$  is a primitive element of  $\mathbb{Q} \subset L$ , and that  $\text{Gal}(L : \mathbb{Q}) \simeq C_2 \times C_2 \times C_2$ .  $\square$

**Ex. 6.3.4** Consider the extension  $\mathbb{Q} \subset L = \mathbb{Q}(\alpha)$ , where  $\alpha = \sqrt{2 + \sqrt{2}}$ . In Exercise 6 of Section 5.1, you showed that  $f = x^4 - 4x^2 + 2$  is the minimal polynomial of  $\alpha$  over  $\mathbb{Q}$  and that  $L$  is the splitting field of  $f$  over  $\mathbb{Q}$ . Show that  $\text{Gal}(L/\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$ .

*Proof.*  $L = \mathbb{Q}(\alpha)$ ,  $\alpha = \sqrt{2 + \sqrt{2}}$ . We have already proved (Ex. 5.1.6) that

$$\begin{aligned} f &= x^4 - 4x^2 + 2 \\ &= \left(x - \sqrt{2 + \sqrt{2}}\right) \left(x + \sqrt{2 + \sqrt{2}}\right) \left(x - \sqrt{2 - \sqrt{2}}\right) \left(x + \sqrt{2 - \sqrt{2}}\right) \end{aligned}$$

is the minimal polynomial of  $\alpha$  over  $\mathbb{Q}$ , and that  $L = \mathbb{Q}(\alpha)$  is the splitting field of  $f$  over  $\mathbb{Q}$ .

$L = \mathbb{Q}(\alpha)$  is so the splitting field of the irreducible separable polynomial  $f$ . By theorem 6.2.1,

$$|\text{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}] = 4.$$

Write  $\beta = \sqrt{2 - \sqrt{2}}$ . If  $\sigma \in \text{Gal}(L/\mathbb{Q})$ ,  $\sigma(\alpha)$  is a root of  $f$ , thus

$$\sigma(\alpha) \in \{\alpha, \beta, -\alpha, -\beta\}.$$

Moreover, since  $L = \mathbb{Q}(\alpha)$ , an automorphism of  $\text{Gal}(L/\mathbb{Q})$  is uniquely determined by the image of  $\alpha$ , and since  $|\text{Gal}(L/\mathbb{Q})| = 4$ , all of these possibilities occur, so there exist one and only one  $\sigma \in \text{Gal}(L/\mathbb{Q})$  such that  $\sigma(\alpha) = \gamma$ , where  $\gamma \in \{\alpha, \beta, -\alpha, -\beta\}$  (alternatively, since  $f$  is irreducible over  $\mathbb{Q}$ , we can use Theorem 5.1.8).

$$\text{Gal}(L/\mathbb{Q}) = \{\sigma_0 = e, \sigma_1, \sigma_2, \sigma_3\}, \sigma_1(\alpha) = \beta, \sigma_2(\alpha) = -\alpha, \sigma_3(\alpha) = -\beta.$$

In particular, there exists so  $\sigma(= \sigma_1) \in \text{Gal}(L/\mathbb{Q})$  defined by  $\sigma(\alpha) = \beta$ .

Recall that  $\alpha\beta = \sqrt{2}$ ,  $\alpha^2 = 2 + \sqrt{2}$ ,  $\beta^2 = 2 - \sqrt{2}$  (see Ex. 5.1.6), thus

$$\alpha^2 - \beta^2 = 2\alpha\beta.$$

From this equality we obtain

$$\alpha^2 - \frac{2}{\alpha^2} = 2\alpha\beta, \quad \frac{2}{\beta^2} - \beta^2 = 2\alpha\beta,$$

therefore

$$\beta = \frac{1}{2} \left( \alpha - \frac{2}{\alpha^3} \right), \quad \alpha = -\frac{1}{2} \left( \beta - \frac{2}{\beta^3} \right).$$

As  $\sigma(\alpha) = \beta$ ,

$$\begin{aligned} \sigma(\beta) &= \frac{1}{2} \left( \sigma(\alpha) - \frac{2}{\sigma(\alpha)^3} \right) \\ &= \frac{1}{2} \left( \beta - \frac{2}{\beta^3} \right) \\ &= -\alpha \end{aligned}$$

Finally  $\sigma(-\alpha) = \sigma(-1)\sigma(\alpha) = -\sigma(\alpha) = -\beta$ , so

$$\sigma(\alpha) = \beta, \sigma^2(\alpha) = -\alpha, \sigma^3(\alpha) = -\beta.$$

As every element in  $\text{Gal}(L/\mathbb{Q})$  is uniquely determined by the image of  $\alpha$ ,

$$\sigma^0 = e = \sigma_0, \sigma^1 = \sigma_1, \sigma^2 = \sigma_2, \sigma^3 = \sigma_3,$$

and

$$\text{Gal}(L/\mathbb{Q}) = \{e, \sigma, \sigma^2, \sigma^3\} = \langle \sigma \rangle.$$

$\text{Gal}(L/\mathbb{Q})$  is so cyclic, generated by  $\sigma$  :

$$\text{Gal}(L/\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}.$$

□

**Ex. 6.3.5** Let  $f \in F[x]$  be separable, where  $f = g_1 \cdots g_s$  for  $g_i \in F[x]$  of degree  $d_i > 0$ , and let  $L$  be the splitting field of  $f$  over  $F$ . Show that  $\text{Gal}(L/F)$  is isomorphic to a subgroup of the product group  $S_{d_1} \times \cdots \times S_{d_s}$ .

*Proof.* We show the proposition for  $s = 2$  to have lighter notations.

Suppose that  $f = gh \in F[x]$  is separable, with  $g, h \in F[x]$ ,  $\deg(g) = r$ ,  $\deg(h) = s$ . Then  $g, h$  are separable.

Write  $\alpha_1, \dots, \alpha_r$  the roots of  $g$  in  $M$ , and  $\beta_1, \dots, \beta_s$  the roots of  $h$  in  $N$ .

Let  $M = F(\alpha_1, \dots, \alpha_r)$ ,  $N = F(\beta_1, \dots, \beta_s)$ , then  $M$  is a splitting field of  $g$  over  $F$ ,  $N$  a splitting field of  $h$  over  $F$ , and  $L = F(\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_s)$  is a splitting field of  $f$  over  $F$ . As  $f$  is separable, the  $d = r + s$  roots of  $f$ ,  $\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_s$  are distinct.

Write  $A$  the set of the roots of  $g$  in  $L$ ,  $B$  the set of roots of  $h$  in  $L$  :  $|A| = r$ ,  $|B| = s$ , and write  $S(A)$  the set of bijections of  $A$  (and the same for  $B$ ) :  $S(A) \simeq S_r$ ,  $S(B) \simeq S_s$ .

Let  $\sigma \in \text{Gal}(L/F)$ . As  $g, h \in F[x]$ ,  $\sigma$  induce a permutation of the roots of  $g$  and of the roots of  $h$ , so the maps

$$\sigma_1 : \begin{cases} A & \rightarrow & A \\ \alpha & \mapsto & \sigma(\alpha) \end{cases} \quad \text{and} \quad \sigma_2 : \begin{cases} B & \rightarrow & B \\ \beta & \mapsto & \sigma(\beta) \end{cases}$$

restrictions of  $\sigma$  à  $A, B$ , satisfy  $\sigma_1 \in S(A)$ ,  $\sigma_2 \in S(B)$ .

The map

$$\varphi : \begin{cases} \text{Gal}(L/F) & \rightarrow & S(A) \times S(B) \\ \sigma & \mapsto & (\sigma_1, \sigma_2) \end{cases}$$

is a group homomorphism : if  $\varphi(\sigma) = (\sigma_1, \sigma_2)$  and  $\varphi(\tau) = (\tau_1, \tau_2)$  (with  $\sigma, \tau \in \text{Gal}(L/F)$ ), and also  $\eta = \sigma \circ \tau$ ,  $\varphi(\eta) = (\eta_1, \eta_2)$ , then for all  $\alpha$  in  $A$  and  $\beta \in B$ ,

$$\eta_1(\alpha) = \eta(\alpha) = (\sigma\tau)(\alpha) = (\sigma_1\tau_1)(\alpha), \eta_2(\beta) = \eta(\beta) = (\sigma\tau)(\beta) = (\sigma_2\tau_2)(\beta),$$

thus  $\eta_1 = \sigma_1\tau_1$ ,  $\eta_2 = \sigma_2\tau_2$ . Consequently

$$\varphi(\sigma \circ \tau) = \varphi(\eta) = (\eta_1, \eta_2) = (\sigma_1\tau_1, \sigma_2\tau_2) = (\sigma_1, \sigma_2)(\tau_1, \tau_2) = \varphi(\sigma)\varphi(\tau).$$

$\varphi$  is injective : if  $\varphi(\sigma) = (\sigma_1, \sigma_2) = (1_A, 1_B)$ , then

$$\sigma(\alpha_i) = \alpha_i, \quad i = 1, \dots, r \quad \text{et} \quad \sigma(\beta_j) = \beta_j, \quad j = 1, \dots, s.$$

Comme  $L = F(\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_s)$ ,  $\sigma = 1_L$ .

$\text{Gal}(L/F)$  is isomorphic to a subgroup of  $S(A) \times S(B)$ , and as  $S(A) \times S(B) \simeq S_r \times S_s$ ,  $\text{Gal}(L/F)$  is isomorphic to a subgroup of  $S_r \times S_s$ .

We can generalize to  $s$  polynomials similarly, or by induction. □

**Ex. 6.3.6** Let  $H$  be a transitive subgroup of  $S_n$ . Prove that  $|H|$  is a multiple of  $n$ .

*Proof.* A subgroup  $H$  of  $S_n$  defines an action on  $[1, n]$  by  $h \cdot x = h(x)$ ,  $h \in H$ ,  $x \in [1, n]$ . By definition  $H$  is a transitive subgroup of  $S_n$  if this action is transitive, i.e. if the only orbit is  $\mathcal{O}_i = [1, n]$ ,  $i = 1, \dots, n$ . If we write  $H_i = \text{Stab}_H(i)$  the stabilizer in  $H$  of a fixed element  $i$ , then  $(H : H_i) = |\mathcal{O}_i| = n$ , thus  $|H| = |H_i| \times n$  :

$$n \text{ divides } |H|.$$

□

**Ex. 6.3.7** Let  $f \in F[x]$  be irreducible and separable of degree  $n$  and let  $F \subset L$  be a splitting field of  $f$  over  $F$ . Use Exercise 6 and Proposition 6.3.7 to prove that  $n$  divides  $|\text{Gal}(L/F)|$ . This gives an alternate proof of Exercise 6 of Section 6.2.

*Proof.* We define a left action of the Galois group  $G = \text{Gal}(L/F)$  on the set  $S$  of the roots of  $f$  by  $\sigma \cdot \alpha = \sigma(\alpha)$ , where  $\sigma \in G, \alpha \in S$  (we know that  $\sigma(\alpha) \in S$ ).

For a fixed  $\alpha \in S$ , define  $G_\alpha = \text{Stab}_G(\alpha) = \{\sigma \in G \mid \sigma(\alpha) = \alpha\}$  the stabilizer of  $\alpha$  in  $G$ , and  $\mathcal{O}_\alpha = \{\sigma \cdot \alpha \mid \sigma \in G\}$  its orbit.

As  $f$  is irreducible, by proposition 5.8.1, if  $\alpha, \beta$  are two roots of  $f$ , there exists a field isomorphism  $\sigma : L \rightarrow L$ , which is identity on  $F$  (so  $\sigma \in \text{Gal}(L/F)$ ), and such that  $\sigma(\alpha) = \beta$ .

Therefore the action of  $G$  on  $S$  is transitive, so there exists a unique orbit : for all  $\alpha \in S$ ,  $\mathcal{O}_\alpha = S$ , thus

$$|\mathcal{O}_\alpha| = |S| = n.$$

Indeed the separability of  $f$  implies that  $f$  has  $n = \deg(f)$  distinct roots in  $L$ .

As  $(G : G_\alpha) = |\mathcal{O}_\alpha|$ , we obtain

$$|G| = |\text{Gal}(L/F)| = n \times |G_\alpha|.$$

So  $n = \deg(f)$  divides  $|\text{Gal}(L/F)|$ . □

## 6.4 EXAMPLES OF GALOIS GROUPS

**Ex. 6.4.1** Given  $a, b \in \mathbb{F}_p$ , define  $\gamma_{a,b} : \mathbb{F}_p \rightarrow \mathbb{F}_p$  by  $\gamma_{a,b}(u) = au + b$ .

- (a) Prove that  $\gamma_{a,b}$  is one-to-one and onto if and only if  $a \neq 0$ .
- (b) Suppose that  $a \neq 0$ . Prove that the inverse function of  $\gamma_{a,b}$  is  $\gamma_{a^{-1}, -a^{-1}b}$ .
- (c) Show that

$$\text{AGL}(1, \mathbb{F}_p) = \{\gamma_{a,b} \mid (a, b) \in \mathbb{F}_p^* \times \mathbb{F}_p\}$$

is a group under composition.

*Proof.* Let  $a, b \in \mathbb{F}_p$ , and  $\gamma_{a,b} : \mathbb{F}_p \rightarrow \mathbb{F}_p, u \mapsto \gamma_{a,b}(u) = au + b$ .

- (a) If  $a = 0$ ,  $\gamma_{a,b}$  is the constant function  $b$ , thus  $\gamma_{0,b}$  is not a bijection.

Suppose that  $a \neq 0$ . Then, for all  $u, v \in \mathbb{F}_p$ ,

$$v = au + b \iff u = a^{-1}v - a^{-1}b.$$

So every  $v \in \mathbb{F}_p$  has a unique antecedent, therefore  $\gamma_{a,b}$  est bijective.

- (b) If  $a \neq 0$ , by part (a),  $\gamma_{a,b}$  is bijective, and the unique antecedent  $u$  of any  $v \in \mathbb{F}_p$  is given by  $u = a^{-1}v - a^{-1}b = \gamma_{a^{-1}, -a^{-1}b}(v)$ . Consequently

$$\gamma_{a,b}^{-1} = \gamma_{a^{-1}, -a^{-1}b}.$$

- (c) We show that  $\text{AGL}(1, \mathbb{F}_p)$  is a subgroup of  $(S(\mathbb{F}_p), \circ)$ .

- By part (a), if  $f \in \text{AGL}(1, \mathbb{F}_p)$ , then  $f = \gamma_{a,b}$ , where  $a \neq 0$ , thus  $f$  est bijective :  $\text{AGL}(1, \mathbb{F}_p) \subset S(\mathbb{F}_p)$ , and  $1_{\mathbb{F}_p} = \gamma_{1,0} \in \text{AGL}(1, \mathbb{F}_p)$ , so  $\text{AGL}(1, \mathbb{F}_p) \neq \emptyset$ .
- If  $f, g \in \text{AGL}(1, \mathbb{F}_p)$ , then  $f = \gamma_{a,b}, g = \gamma_{c,d}$ ,  $a, b, c, d \in \mathbb{F}_p, a \neq 0, c \neq 0$ .



For all  $u \in \mathbb{F}_p$ ,

$$(g \circ f)(u) = \gamma_{c,d}(\gamma_{a,b}(u)) = \gamma_{c,d}(au + b) = c(au + b) + d = acu + (bc + d) = \gamma_{ac,bc+d}.$$

Therefore  $g \circ f = \gamma_{c,d} \circ \gamma_{a,b} = \gamma_{ac,bc+d}$  and  $ac \neq 0$ , so  $g \circ f \in \text{AGL}(1, \mathbb{F}_p)$ .

• If  $f \in \text{AGL}(1, \mathbb{F}_p)$ ,  $f = \gamma_{a,b}$ ,  $a \neq 0$ , then  $f^{-1} = \gamma_{a^{-1}, -a^{-1}b} \in \text{AGL}(1, \mathbb{F}_p)$ .

$\text{AGL}(1, \mathbb{F}_p)$  is a group under composition.

□

**Ex. 6.4.2** Consider the map  $\text{AGL}(1, \mathbb{F}_p) \rightarrow \mathbb{F}_p^*$  defined by  $\gamma_{a,b} \mapsto a$ .

(a) Show that this map is an onto group homomorphism with kernel  $T = \{\gamma_{1,b} \mid b \in \mathbb{F}_p\}$ . Then use this to prove (6.6).

(b) Show that  $T \simeq \mathbb{F}_p$ .

*Proof.* Let  $\varphi : \text{AGL}(1, \mathbb{F}_p) \rightarrow \mathbb{F}_p^*$ ,  $\gamma_{a,b} \mapsto \varphi(\gamma_{a,b}) = a$ .

(a) This map is well defined, since

$$f = \gamma_{a,b} = \gamma_{c,d} \in \text{AGL}(1, \mathbb{F}_p) \Rightarrow \forall u \in \mathbb{F}_p, au + b = cu + d \Rightarrow a = c.$$

$\varphi$  is a group homomorphism: if  $f = \gamma_{a,b}$ ,  $g = \gamma_{c,d} \in \text{AGL}(1, \mathbb{F}_p)$ , then

$$\varphi(g \circ f) = \varphi(\gamma_{c,d} \circ \gamma_{a,b}) = \varphi(\gamma_{ac,bc+d}) = ac = \varphi(g)\varphi(f).$$

This homomorphism is surjective, since every  $a \in \mathbb{F}_p^*$  satisfies  $a = \varphi(\gamma_{a,0})$ , with  $\gamma_{a,0} \in \text{AGL}(1, \mathbb{F}_p)$ .

$\gamma_{a,b} \in \ker(\varphi) \iff a = 1$ : the kernel of  $\varphi$  is  $T = \{\gamma_{1,b} \mid b \in \mathbb{F}_p\}$ , so  $T$  is a normal subgroup.

As the image of the group homomorphism  $\varphi$  is  $\mathbb{F}_p^*$ , and its kernel  $T$ , the Isomorphism Theorem shows that

$$\text{AGL}(1, \mathbb{F}_p)/T \simeq \mathbb{F}_p^*.$$

(b) The map  $\psi : T \rightarrow \mathbb{F}_p$ ,  $\gamma_{1,b} \mapsto b$  is bijective, and satisfies

$$\psi(\gamma_{1,b} \circ \gamma_{1,d}) = \psi(\gamma_{1,b+d}) = b + d = \psi(\gamma_{1,b}) + \psi(\gamma_{1,d}),$$

So  $\psi$  is a group homomorphism:  $T \simeq \mathbb{F}_p$ .

□

**Ex. 6.4.3** This exercise is concerned with the proof of (6.7). Given  $\tau \in S_n$ , observe that  $f \mapsto \tau \cdot f$  can be regarded as the evaluation map from  $F[x_1, \dots, x_n]$  to itself that evaluates  $f(x_1, \dots, x_n)$  at  $(x_{\tau(1)}, \dots, x_{\tau(n)})$ .

(a) Explain why Theorem 2.1.2 implies that  $f \mapsto \tau \cdot f$  is a ring homomorphism. This proves the first two bullets of (6.7).

(b) Prove the third bullet of (6.7).

*Proof.* (a) Let  $\tau \in S_n$ . As  $f \mapsto \tau.f$  is the evaluation map that evaluates  $f(x_1, \dots, x_n)$  at  $(x_{\tau(1)}, \dots, x_{\tau(n)})$ , Theorem 2.1.2 shows that this application is a ring homomorphism, thus

$$\begin{aligned}\tau.(f + g) &= \tau.f + \tau.g \\ \tau.(fg) &= (\tau.f)(\tau.g)\end{aligned}$$

(b) Let  $f = f(x_1, \dots, x_n) \in F(x_1, \dots, x_n)$ , and  $\tau, \gamma \in S_n$ . Define  $g$  by

$$g(x_1, \dots, x_n) = \gamma.f = f(x_{\gamma(1)}, \dots, x_{\gamma(n)}).$$

Then  $\tau \cdot (\gamma \cdot f) = \tau \cdot g = g(x_{\tau(1)}, \dots, x_{\tau(n)})$  is obtained by substituting each  $x_i$  in the expression of  $g$  by  $x_{\tau(i)}$ , thus  $x_{\gamma(j)}$  becomes  $x_{\tau(\gamma(j))} = x_{(\tau\gamma)(j)}$ :

$$\tau \cdot (\gamma \cdot f) = f(x_{(\tau\gamma)(1)}, \dots, x_{(\tau\gamma)(n)}) = (\tau\gamma) \cdot f.$$

Conclusion :

$$\tau \cdot (\gamma \cdot f) = (\tau\gamma) \cdot f.$$

□

**Ex. 6.4.4** Let  $\tau \in S_n$ . Prove that  $f \mapsto \tau \cdot f$  is a ring isomorphism from  $F[x_1, \dots, x_n]$  to itself.

*Proof.* We know (Exercise 6.4.3 (a)) that  $\varphi : f \mapsto \tau \cdot f$  is a ring isomorphism. As  $\tau \in S_n$ ,  $\tau$  is bijective and so  $\tau^{-1}$  exists. Let  $\psi : f \mapsto \tau^{-1} \cdot f$ . Then for all  $f \in F[x_1, \dots, x_n]$ , by Exercise 6.4.3 (b)

$$\begin{aligned}(\psi \circ \varphi)(f) &= \tau^{-1} \cdot (\tau \cdot f) = (\tau^{-1}\tau) \cdot f = 1_{[1,n]} \cdot f = f \\ (\varphi \circ \psi)(f) &= \tau \cdot (\tau^{-1} \cdot f) = (\tau\tau^{-1}) \cdot f = 1_{[1,n]} \cdot f = f\end{aligned}$$

Therefore  $\psi \circ \varphi = \varphi \circ \psi = 1_{F[x_1, \dots, x_n]}$ , so  $\varphi$  is a bijection.

Conclusion :  $\varphi$  is a ring isomorphism.

□

**Ex. 6.4.5** Let  $R$  be an integral domain, and let  $K$  be its field of fractions. Prove that every ring isomorphism  $\phi : R \rightarrow R$  extends uniquely to an automorphism  $\tilde{\phi} : K \rightarrow K$ .

*Proof.* If  $f = p/q \in K$ , then the fraction  $\phi(p)/\phi(q)$  doesn't depend of the choice of the representent  $(p, q)$  of the fraction: if  $f = p/q = r/s$ , then  $ps = qr$ , thus  $\phi(p)\phi(s) = \phi(ps) = \phi(qr) = \phi(q)\phi(r)$ , and so  $\phi(p)/\phi(q) = \phi(r)/\phi(s)$ . Therefore there exists a map  $\tilde{\phi} : K \rightarrow K$  defined for all  $p/q \in K$  by

$$\tilde{\phi}(p/q) = \phi(p)/\phi(q).$$

In particular, if  $p \in R$ ,  $\tilde{\phi}(p) = \tilde{\phi}(p/1) = \phi(p)/\phi(1) = \phi(p)$  :  $\tilde{\phi}$  extends  $\phi$ .

$\tilde{\phi}$  is a ring homomorphism:  $\tilde{\phi}(1) = 1$  since  $1 \in R$  and  $\phi(1) = 1$ .

$$\begin{aligned}\tilde{\phi}\left(\frac{p}{q}\frac{r}{s}\right) &= \tilde{\phi}\left(\frac{pr}{qs}\right) = \frac{\phi(pr)}{\phi(qs)} = \frac{\phi(p)\phi(r)}{\phi(q)\phi(s)} \\ &= \tilde{\phi}\left(\frac{p}{q}\right)\tilde{\phi}\left(\frac{r}{s}\right). \\ \tilde{\phi}\left(\frac{p}{q} + \frac{r}{s}\right) &= \tilde{\phi}\left(\frac{ps + qr}{qs}\right) = \frac{\phi(ps + qr)}{\phi(qs)} \\ &= \frac{\phi(p)\phi(s) + \phi(q)\phi(r)}{\phi(q)\phi(s)} = \frac{\phi(p)}{\phi(q)} + \frac{\phi(r)}{\phi(s)} \\ &= \tilde{\phi}\left(\frac{p}{q}\right) + \tilde{\phi}\left(\frac{r}{s}\right)\end{aligned}$$

If  $\tilde{\phi}(p/q) = 0$ , then  $\phi(p)/\phi(q) = 0$ , thus  $\phi(p) = 0$ ,  $p = 0$ ,  $p/q = 0$  :  $\tilde{\phi}$  is injective.

If  $g = u/v \in K$ , as  $\phi$  is surjective,  $u = \phi(p)$ ,  $v = \phi(q)$ ,  $p, q \in R$ . Then  $g = \phi(p)/\phi(q) = \tilde{\phi}(p/q)$ ,  $p/q \in K$  :  $\tilde{\phi}$  est surjective.

$\tilde{\phi} : K \rightarrow K$  is a field automorphism.

If  $\psi : K \rightarrow K$  is any field automorphism which extends  $\phi$ , then for any fraction  $p/q \in K$ ,

$$\psi\left(\frac{p}{q}\right) = \frac{\psi(p)}{\psi(q)} = \frac{\phi(p)}{\phi(q)} = \tilde{\phi}\left(\frac{p}{q}\right),$$

so  $\psi = \tilde{\phi}$ :

every ring isomorphism  $\phi : R \rightarrow R$  extends uniquely to an automorphism of  $K$ .  $\square$

**Ex. 6.4.6** As in the text, let  $f = x^5 - 6x + 3$ .

(a) Use the hints given in the text to show that every element of  $S_5$  of order 5 is a 5-cycle.

(b) Use curve graphing from calculus to show that  $f$  has exactly three real roots.

*Proof.* Let  $f = x^5 - 6x + 3$ .

(a) Let  $\sigma \in S_5$  a permutation of order 5. Write  $\sigma = \sigma_1 \cdots \sigma_r$  ( $\sigma_i \neq e$ ) the cycle decomposition of  $\sigma$ . Let  $d_i = |\sigma_i|$  the order of  $\sigma_i$  in  $S_n$ . As the cycles are disjoint, for all integer  $k$ ,  $\sigma^k = \sigma_1^k \cdots \sigma_r^k$  and

$$\begin{aligned}\sigma^k = e &\iff \sigma_1^k = \cdots = \sigma_r^k = e \\ &\iff d_1 \mid k, d_2 \mid k, \dots, d_r \mid k \\ &\iff \text{lcm}(d_1, \dots, d_r) \mid k\end{aligned}$$

So the order of  $\sigma$  is the lcm of the orders  $d_i$ .

$$5 = \text{lcm}(d_1, \dots, d_r).$$

As  $d_i \mid 5$ ,  $i = 1, \dots, r$ , and  $d_i \neq 1$ , where 5 is prime,  $d_i = 5$ . The cycles  $\sigma_i$  being disjoint, as  $d_i = |\sigma_i| = \text{length}(\sigma_i)$ ,  $d_1 + \cdots + d_r \leq 5$ , thus  $rd_1 = 5r \leq 5$ , so  $r = 1$ .

Conclusion :  $\sigma = \sigma_1$  is a 5-cycle.

(b) Let  $f : \mathbb{R} \rightarrow \mathbb{R}, x \mapsto f(x) = x^5 - 6x + 3$ .

If  $x \in \mathbb{R}, f'(x) = 5x^4 - 6 < 0 \iff x^4 < \frac{6}{5} \iff -x_0 < x < x_0$ , where  $x_0 = \sqrt[4]{\frac{6}{5}}$ .

$f$  is so strictly increasing on  $]-\infty, -x_0]$ , strictly decreasing on  $[-x_0, x_0]$ , and strictly increasing on  $[x_0, +\infty[$ .

$f(x_0) = x_0(x_0^4 - 6) + 3 = x_0(\frac{6}{5} - 6) + 3 = -\frac{24}{5}x_0 + 3 = \frac{3}{5}(5 - 8x_0) < 0$ : indeed  $x_0 = \sqrt[4]{\frac{6}{5}} > 1 > \frac{5}{8}$ , so  $5 - 8x_0 < 0$ .

$f(-x_0) = -x_0(x_0^4 - 6) + 3 = \frac{24}{5}x_0 + 3 > 0$ .

As  $f$  is continuous,  $\lim_{x \rightarrow -\infty} f(x) = -\infty, f(-x_0) > 0$ , and  $f$  is strictly increasing on  $]-\infty, -x_0]$ , the Intermediate Values Theorem shows that  $f$  has a unique root in  $]-\infty, -x_0]$ .

With a similar reasoning on  $[-x_0, x_0]$  and on  $[x_0, +\infty[$ , with  $f(-x_0) < 0, f(x_0) > 0, \lim_{x \rightarrow +\infty} f(x) = +\infty$ , we prove that  $f$  has a unique root in  $[-x_0, x_0]$ , and also in  $[x_0, +\infty[$ .

Conclusion :  $f$  has exactly three real roots.

□

**Ex. 6.4.7** Show that  $S_n$  is generated by the transposition  $(1\ 2)$  and the  $n$ -cycle  $(1\ 2\ \dots\ n)$ .

*Proof.* Let  $G_n$  the subgroup of  $S_n$  generated by the transpositions  $(1, 2), (2, 3), \dots, (n-1, n)$ :

$$G_n = \langle (1, 2), (2, 3), \dots, (n-1, n) \rangle$$

For all  $i \in \{1, \dots, n\}$ , there exists  $g \in G_n$  such that  $g(n) = i$ .

Indeed, if  $g = (i, i+1) \circ (i+1, i+2) \circ \dots \circ (n-1, n) = (i, i+1)(i+1, i+2) \dots (n-1, n)$  (with the convention  $g = e$  if  $i = n$ ).

Then  $g \in G_n$  and  $g(n) = i$  (as  $\mathcal{O}_n = [1, n]$ ,  $G_n$  is a transitive subgroup of  $S_n$ ).

Conclusion: for all  $i \in \{1, \dots, n\}$ , there exists  $g \in G_n$  tel que  $g(n) = i$ .

We show that  $G_n = S_n$ .

$S_2 = \{e, (1, 2)\}$  is equal to  $G_2 = \langle (1, 2) \rangle$ .

By induction, we suppose that  $S_{n-1} = G_{n-1}$  ( $n \geq 3$ ).

The subgroup of  $S_n$  of the permutations fixing  $n$  is identified with  $S_{n-1}$ , so

$$\text{Stab}_{S_n}(n) = S_{n-1}.$$

Let  $\sigma \in S_n$  and  $i = \sigma(n)$ . By part (a), there exist  $g \in G_n$  such that  $g(n) = i$ . Then

$$(g^{-1} \circ \sigma)(n) = n : g' = g^{-1} \circ \sigma \in S_{n-1}.$$

Thus  $\sigma = g \circ g'$ , where  $g \in G_n, g' \in G_{n-1} \subset G_n$ , therefore  $\sigma \in G_n$ . So  $S_n \subset G_n$ , and by definition  $G_n \subset S_n$ , thus  $G_n = S_n$ .

Conclusion : for all  $n \geq 2$ ,  $S_n = \langle (1, 2), (2, 3), \dots, (n-1, n) \rangle$

We recall the following lemma :

**Lemma :** If  $g = (a_1, \dots, a_k)$  is a cycle in  $S_n$ , and  $\sigma \in S_n$ , then

$$\sigma \circ g \circ \sigma^{-1} = (\sigma(a_1), \dots, \sigma(a_k)).$$

Indeed,

- If  $1 \leq i < k$ ,  $(\sigma \circ g \circ \sigma^{-1})(\sigma(a_i)) = \sigma(g(a_i)) = \sigma(a_{i+1})$ .
- If  $i = k$ ,  $(\sigma \circ g \circ \sigma^{-1})(\sigma(a_k)) = \sigma(g(a_k)) = \sigma(a_1)$ .
- if  $x \notin \{\sigma(a_1), \dots, \sigma(a_k)\}$ , then  $\sigma^{-1}(x) \notin \{a_1, \dots, a_k\}$ , therefore  $g(\sigma^{-1}(x)) = \sigma^{-1}(x)$ ,  $(\sigma \circ g \circ \sigma^{-1})(x) = x$ .  $\square$

Let  $\tau = (1, 2)$ ,  $\sigma = (1, 2, \dots, n)$ .

We apply the Lemma to  $\tau$  and  $\sigma^{k-1}$ ,  $1 \leq k < n$  :

$$\sigma^{k-1} \circ \tau \circ \sigma^{-(k-1)} = (\sigma^{k-1}(1), \sigma^{k-1}(2)) = (k, k+1).$$

Thus  $\langle \sigma, \tau \rangle \supset G_n = S_n$ .

Conclusion :  $S_n$  is generated by the transposition  $(1, 2)$  and the  $n$ -cycle  $(1, 2, \dots, n)$ .  $\square$

**Ex. 6.4.8** Let  $G$  and  $H$  be groups where  $G$  acts on  $H$  by group homomorphisms. As in the text, we let  $H \rtimes G$  denote the set  $H \times G$  with the binary operation given by (6.9).

- (a) Prove that  $H \rtimes G$  is a group.
- (b) Prove that the map  $H \rtimes G \rightarrow G$  defined by  $(h, g) \mapsto g$  is an onto homomorphism with kernel  $H \times \{e\}$ .
- (c) Prove that  $h \mapsto (h, e)$  defines an isomorphism  $H \simeq H \times \{e\}$  (where the group structure on  $H \times \{e\}$  comes from  $H \rtimes G$ ).

*Proof.* By definition of an action by group homomorphisms, there exists a group homomorphism  $\varphi : G \rightarrow \text{Aut}(H)$  such that for all  $(g, h) \in G \times H$ ,

$$g \cdot h = \varphi(g)(h),$$

so  $h \mapsto g \cdot h$  is a group automorphism of  $H$  for all  $g \in G$ .

- (a) I If  $h, h' \in H, g, g' \in G$ , then  $g \cdot h' \in H$ , thus  $(h(g \cdot h'), gg') \in H \times G$ , so this law defines a binary operation on  $H \times G$ .
- A Let  $(h, g), (h', g'), (h'', g'') \in H \times G$ . Then

$$\begin{aligned} ((h, g) \cdot (h', g')) \cdot (h'', g'') &= (h(g \cdot h'), gg') \cdot (h'', g'') \\ &= (h(g \cdot h')((gg') \cdot h''), gg'g'') \\ &= (h(g \cdot h')(g \cdot (g' \cdot h'')), gg'g''). \end{aligned}$$

The last equality is true because  $G$  acts on  $H$ .

$$\begin{aligned} (h, g) \cdot ((h', g') \cdot (h'', g'')) &= (h, g)((h'(g' \cdot h''), g'g'')) \\ &= (h(g \cdot (h'(g' \cdot h''))), gg'g'') \\ &= (h(g \cdot h')(g \cdot (g' \cdot h'')), gg'g''). \end{aligned}$$

The last equality is true because  $G$  acts on  $H$  by group homomorphism.

Therefore  $((h, g) \cdot (h', g')) \cdot (h'', g'') = (h, g) \cdot ((h', g') \cdot (h'', g''))$ : the law is associative.

$\boxed{N}$  Write  $e_H, e_G$  the identity of  $H$  and the identity of  $G$ .

$$\begin{aligned}(f, g) \cdot (e_H, e_G) &= (f(g \cdot e_H), ge_G) = (fe_H, ge_G) = (f, g), \\ (e_H, e_G) \cdot (f, g) &= (e_H(e_G \cdot f), e_Gg) = (e_Hf, e_Gg) = (f, g).\end{aligned}$$

So  $(e_H, e_G)$  is the identity of  $H \rtimes G$ , which we will write now  $(1, 1)$ .

$\boxed{S}$

Analysis : if  $(h', g')$  is the inverse of  $(h, g)$ , then  $(h(g \cdot h'), gg') = (1, 1)$ . Thus  $g' = g^{-1}$ , and  $g \cdot h' = h^{-1}$ , therefore  $h' = g^{-1} \cdot (h^{-1})$ .

Synthesis : we show that  $(g^{-1} \cdot (h^{-1}), g^{-1})$  is the inverse of  $(h, g)$  :

$$\begin{aligned}(h, g) \cdot (g^{-1} \cdot (h^{-1}), g^{-1}) &= (h(g \cdot (g^{-1} \cdot (h^{-1}))), gg^{-1}) \\ &= (h(gg^{-1} \cdot (h^{-1})), 1) \\ &= (hh^{-1}, 1) = (1, 1) \\ (g^{-1} \cdot (h^{-1}), g^{-1}) \cdot (h, g) &= ((g^{-1} \cdot (h^{-1}))(g^{-1} \cdot h), g^{-1}g) \\ &= (g^{-1} \cdot (h^{-1}h), 1) \\ &= (g^{-1} \cdot 1, 1) = (1, 1)\end{aligned}$$

Every element of  $H \rtimes G$  has an inverse.

$H \rtimes G$  is a group.

(b) Let  $\psi : \begin{cases} H \rtimes G & \rightarrow G \\ (h, g) & \mapsto g \end{cases}$ .

$\psi((h, g) \cdot (h', g')) = \psi(h(g \cdot h'), gg') = gg' = \psi(h, g)\psi(h', g')$ .  $\psi$  is so a group homomorphism.

As every  $g$  in  $G$  is the image of  $(1, g) \in H \rtimes G$  by  $\psi$ ,  $\psi$  is surjective.

$$\ker(\psi) = \{(h, g) \in H \rtimes G \mid g = e\} = H \times \{e\}.$$

(c) Let  $\chi : \begin{cases} H & \rightarrow H \times \{e\} \\ h & \mapsto (h, e) \end{cases}$ .

$\chi(h)\chi(h') = (h, e)(h', e) = (h(e \cdot h'), e) = (hh', e) = \chi(hh')$  :  $\chi$  is a group homomorphism from  $H$  on the subgroup  $H \times \{e\}$  of  $H \rtimes G$ .

$\chi(h) = (e, e) \iff h = e$ , thus  $\chi$  est injective, and surjective since every element of  $H \times \{e\}$  is of the form  $(h, e) = \chi(h)$  :  $H \simeq H \times \{e\}$ .

Therefore the sequence  $\{e\} \rightarrow H \rightarrow H \rtimes G \rightarrow G \rightarrow \{e\}$  is a short exact sequence, so  $H \rtimes G$  is an extension of  $H$  by  $G$ .

□

**Ex. 6.4.9** Explain how (6.6) and (6.10) relate to the last paragraph of the discussion of semidirect products in the Mathematical Notes.

*Proof.* The group homomorphism  $\psi$  of Exercise 8 shows that  $(H \rtimes G)/(H \times \{e\}) \simeq G$ .

Moreover the isomorphism (6.10)  $\phi : \begin{cases} \text{AGL}(1, \mathbb{F}_p) & \rightarrow \mathbb{F}_p \rtimes \mathbb{F}_p^* \\ \gamma_{a,b} & \mapsto (b, a) \end{cases}$

maps  $T = \{\gamma_{1,b} \mid b \in \mathbb{F}_p\}$  on  $\mathbb{F}_p \times \{1\}$ .

Therefore  $\text{AGL}(1, \mathbb{F}_p)/T \simeq (\mathbb{F}_p \rtimes \mathbb{F}_p^*)/(\mathbb{F}_p \times \{1\}) \simeq \mathbb{F}_p^*$  : we obtain so (6.6) :

$$\text{AGL}(1, \mathbb{F}_p)/T \simeq \mathbb{F}_p^*.$$

□

**Ex. 6.4.10** Let  $p \geq 3$  be prime, and let  $\mathbb{F}_p \rtimes \mathbb{F}_p^*$  be the semidirect product described in the Mathematical Notes.

- (a) Show that  $\mathbb{F}_p \rtimes \mathbb{F}_p^*$  is not Abelian.
- (b) Show that the product group  $\mathbb{F}_p \times \mathbb{F}_p^*$  is Abelian.
- (c) Show that  $\mathbb{F}_p \times \mathbb{F}_p^*$  is an extension of  $\mathbb{F}_p$  by  $\mathbb{F}_p^*$ .

Since we already know that  $\mathbb{F}_p \rtimes \mathbb{F}_p^*$  is an extension of  $\mathbb{F}_p$  by  $\mathbb{F}_p^*$ , we see that (a) and (b) give nonisomorphic extensions.

*Proof.* (a) As  $p \geq 3$ , there exist in  $\mathbb{F}_p$  an element 2 with  $2 \neq 0, 2 \neq 1$ , so  $(0, 2) \in \mathbb{F}_p \rtimes \mathbb{F}_p^*$ , and also  $(1, 1) \in \mathbb{F}_p \rtimes \mathbb{F}_p^*$ .

$$\begin{aligned} (0, 2) \cdot (1, 1) &= (0 + 2 \times 1, 2 \times 1) = (2, 2) \\ (1, 1) \cdot (0, 2) &= (1 + 1 \times 0, 1 \times 2) = (1, 2) \end{aligned}$$

Since  $2 \neq 1$ ,  $(0, 2) \cdot (1, 1) \neq (1, 1) \cdot (0, 2)$ . So if  $p \geq 3$ , then  $\mathbb{F}_p \rtimes \mathbb{F}_p^*$  is not Abelian.

- (b) By definition of the product in  $\mathbb{F}_p \times \mathbb{F}_p^*$ ,  $(a, b)(c, d) = (ac, bd) = (ca, db) = (c, d)(a, b)$ :  $\mathbb{F}_p \times \mathbb{F}_p^*$  is Abelian.
- (c) The sequence

$$\{0\} \rightarrow \mathbb{F}_p \rightarrow \mathbb{F}_p \times \mathbb{F}_p^* \rightarrow \mathbb{F}_p^* \rightarrow \{1\}$$

is a short exact sequence (the first arrow is the injective map  $x \mapsto (x, 1)$ , and the second one is the surjective map  $(x, y) \mapsto y$ ). Actually, a direct product is a special case of semidirect product, where  $\varphi : G \rightarrow \text{Aut}(H)$  is the trivial action defined by  $\phi(g) = 1_H$  for all  $g \in G$ , so  $\varphi(g)(h) = g \cdot h = h$  for all  $h \in H$ . By part (a) and (b), these two extensions are not isomorphic.

□

**Ex. 6.4.11** The goal of this exercise is to show that the group  $G$  of permutations (6.11) is metacyclic in the sense that  $G$  has a normal subgroup  $H$  such that  $H$  and  $G/H$  are cyclic. Show that this follows from  $G \simeq \text{AGL}(1, \mathbb{F}_p)$  together with (6.6) and proposition A.5.3.

*Proof.* If  $L = \mathbb{Q}(\zeta_p, \sqrt[p]{2})$ , and  $G = \text{Gal}(L/\mathbb{Q})$ , then by (6.4),  $G \simeq \text{AGL}(1, \mathbb{F}_p)$ . By (6.6) and Exercise 9,  $\text{AGL}(1, \mathbb{F}_p)/T \simeq \mathbb{F}_p^*$ , and  $T \simeq \mathbb{F}_p$ . As  $\mathbb{F}_p$  is a cyclic (additive) group, and  $\mathbb{F}_p^*$  a cyclic (multiplicative) group by Proposition A.5.3,  $G = \text{Gal}(L/\mathbb{Q})$  is metacyclic. □

**Ex. 6.4.12** Let  $p$  be prime. Generalize part (a) of Exercise 6 by showing that every element of  $S_p$  of order  $p$  is a  $p$ -cycle.

*Proof.* Let  $\sigma \in S_p$  a permutation of order  $p$ . Write  $\sigma = \sigma_1 \cdots \sigma_r$  ( $\sigma_i \neq e$ ) the cycle decomposition of  $\sigma$ . Let  $d_i = |\sigma_i|$  the order of  $\sigma_i$  in  $S_n$ . The order of  $\sigma$  is the lcm of the orders  $d_i$  (see Ex. 6).

$$p = \text{lcm}(d_1, \dots, d_r).$$

As  $d_i \mid p$ ,  $i = 1, \dots, r$ , and  $d_i \neq 1$ , where  $p$  is prime,  $d_i = p$ . The cycles  $\sigma_i$  being disjoint, as  $d_i = |\sigma_i| = \text{length}(\sigma_i)$ ,  $d_1 + \dots + d_r \leq p$ , thus  $rd_1 = pr \leq p$ , so  $r = 1$ .

Conclusion :  $\sigma = \sigma_1$  is a  $p$ -cycle.  $\square$

**Ex. 6.4.13** Let  $L$  be the splitting field of  $2x^5 - 10x + 5$  over  $\mathbb{Q}$ . Prove that  $\text{Gal}(L/\mathbb{Q}) \simeq S_5$ .

**Lemma :** Let  $p$  be a prime number. Let  $\alpha = (i, j) \in S_p$  a transposition, and  $\beta \in S_p$  a  $p$ -cycle. Then  $S_p = \langle \alpha, \beta \rangle$ .

*Proof of lemma.*  $\beta \in S_p$  is a  $p$ -cycle, so  $\beta = (a_1, a_2, \dots, a_p) = (a, \beta(a), \dots, \beta^{p-1}(a))$ , where  $1 \leq a = a_1 \leq p$  is fixed.

The  $\beta^i(a)$  are distinct, otherwise  $\beta^i(a) = \beta^j(a)$ ,  $i < j$  implies  $\beta^{j-i}(a) = a$ , so the cycle would have an order at most equal to  $j - i < p$ , thus not equal to  $p$ .

The support of  $\beta$ ,  $\text{Supp}(\beta) = \{a_1, \dots, a_p\}$  has so  $p$  elements, therefore

$$\text{Supp}(\beta) = \{1, 2, \dots, p\}.$$

So there exists  $r < p, s < p$  such that  $i = \beta^r(a), j = \beta^s(a)$ , thus  $j = \beta^{s-r}(i)$ .

Let  $k$  the remainder of the division of  $s - r$  by  $p$ . Then  $\beta^k(i) = j, 0 \leq k \leq p - 1$ , and as  $i \neq j$  since  $\alpha = (ij)$  is a transposition,  $k \neq 0$ , so

$$\beta^k(i) = j, 1 \leq k \leq p - 1.$$

As  $p$  is prime, and  $1 \leq k \leq p - 1$ ,  $\beta^k$  is also a  $p$ -cycle.

Indeed,  $H = \{n \in \mathbb{Z} \mid (\beta^k)^n(a) = a\}$  is a subgroup of  $\mathbb{Z}$ , therefore it is of the form  $H = d\mathbb{Z}, d > 0$ .

As  $p \in H$ ,  $d$  divides  $p$ , and  $d \neq 1$  (otherwise  $\beta^k(a) = a, k < p$ ), thus  $d = p$ .

Consequently  $\beta^k = (a, \beta^k(a), \beta^{2k}(a), \dots, \beta^{(p-1)k}(a))$  is a  $p$ -cycle, thus  $i$  is in the support of  $\beta^k$ .

$\alpha = (i, j), \beta^k = (i, j = \beta^k(i), \dots, \beta^{(p-1)k}(i))$  generate  $S_n$  as in Exercice 7 where we have proved that  $\sigma = (1, 2, \dots, p)$  and  $\tau = (1, 2)$  generate  $S_p$ .

There is a simple relabeling of the roots. More formally, let

$$\gamma = \begin{pmatrix} 1 & 2 & \dots & p \\ i & j = \beta^k(i) & \dots & \beta^{k(p-1)}(i) \end{pmatrix}.$$

Let  $g$  be any permutation in  $S_n$ . Then  $\gamma^{-1}g\gamma \in S_n = \langle \sigma, \tau \rangle$ .

So  $\gamma^{-1}g\gamma = \sigma_1\sigma_2 \cdots \sigma_l$ , where  $\sigma_i = \tau$ , or  $\sigma_i = \sigma$  (we can avoid negative powers since each element is of finite order).

Then  $g = (\gamma\sigma_1\gamma^{-1})(\gamma\sigma_2\gamma^{-1}) \cdots (\gamma\sigma_l\gamma^{-1})$ , and  $\gamma\sigma_i\gamma^{-1} \in \{\alpha, \beta^k\}$ , since by the Lemma of Exercise 6.4.1:  $\gamma\tau\gamma^{-1} = \alpha, \gamma\sigma\gamma^{-1} = \beta^k$ .

$S_n$  is generated by  $\alpha, \beta^k$ , a fortiori by  $\alpha, \beta$ .

Conclusion: if  $p$  is prime, a  $p$ -cycle  $\beta$ , and any transposition  $(i, j)$  generate  $S_n$ .  $\square$



*Proof.* Let  $f = 2x^5 - 10x + 5 \in \mathbb{Q}[x]$ , and  $L$  the splitting field of  $f$ ,  $G = \text{Gal}(L/\mathbb{Q})$ , and  $G' \subset S_5$  the corresponding subgroup of  $S_5$  isomorphic to  $G$ .

The Schönemann-Eisenstein Criterion with  $p = 5$  shows that  $f$  is irreducible over  $\mathbb{Q}$  (if  $f = \sum_{k=0}^5 a_k x^k$ ,  $5 \nmid a_5 = 2$ ,  $5 \mid a_i$ ,  $i = 0, \dots, 4$ ,  $5^2 \nmid a_0 = 5$ ).

Thus  $G$  acts transitively on the roots of  $f$  (Proposition 6.3.7). By Exercise 6.3.6, 5 divides  $|G|$ .

By Cauchy's Theorem, there exists an element  $\sigma$  of order 5 in  $G$ , thus an element  $\tilde{\sigma}$  of order 5 in  $G' \subset S_5$ . Exercise 6.4.6(a) shows that  $\tilde{\sigma}$  is a 5-cycle.

For all  $t \in \mathbb{R}$ ,  $f'(t) < 0 \iff |t| < 1$ ,  $f$  is strictly decreasing on  $[-1, 1]$ , strictly increasing on  $]-\infty, -1]$  and on  $[1, +\infty[$ . As  $f$  is continuous,  $f(1) = -3 < 0$ ,  $f(-1) = 13 > 0$ , and  $\lim_{+\infty} f = +\infty$ ,  $\lim_{-\infty} f = -\infty$ , the Intermediate Values Theorem shows that the polynomial  $f$  has exactly 3 real roots, thus 2 non real conjugate complex roots. The restriction  $\tau$  of complex conjugation to  $L$  is a  $\mathbb{Q}$ -automorphism of  $L$  (thus  $\tau \in G$ ) who fixes three roots and exchanges the two others. The corresponding element  $\tilde{\tau}$  in  $G' \subset S_5$  is so a transposition. By the above Lemma,  $G' = S_5$ , and so

$$G = \text{Gal}(L/\mathbb{Q}) \simeq S_5.$$

□

**Ex. 6.4.14** Let  $L = \mathbb{Q}(\zeta_p, \sqrt[p]{2})$ . Prove that  $L = \mathbb{Q}(\sqrt[p]{2}, \zeta_p \sqrt[p]{2})$ , i.e. the splitting field of  $x^p - 2$  over  $\mathbb{Q}$  can be generated by two of its roots.

*Proof.* Let  $L = \mathbb{Q}(\zeta_p, \sqrt[p]{2})$ .

$\sqrt[p]{2} \in L$ , and  $\zeta_p \sqrt[p]{2} \in L$ , thus  $\mathbb{Q}(\sqrt[p]{2}, \zeta_p \sqrt[p]{2}) \subset L$ .

$\zeta_p = \zeta_p \sqrt[p]{2} / \sqrt[p]{2} \in \mathbb{Q}(\sqrt[p]{2}, \zeta_p \sqrt[p]{2})$ , and  $\sqrt[p]{2} \in \mathbb{Q}(\sqrt[p]{2}, \zeta_p \sqrt[p]{2})$ . As  $L$  is the smallest subfield of  $\mathbb{C}$  containing  $\mathbb{Q}$ ,  $\zeta_p$ ,  $\sqrt[p]{2}$ , then  $L \subset \mathbb{Q}(\sqrt[p]{2}, \zeta_p \sqrt[p]{2})$ .

Conclusion :

$$\mathbb{Q}(\zeta_p, \sqrt[p]{2}) = \mathbb{Q}(\zeta_p, \zeta_p \sqrt[p]{2}).$$

The splitting field of  $x^p - 2$  over  $\mathbb{Q}$  is generated by two of its roots. □

**Ex. 6.4.15** Let  $L = \mathbb{Q}(\zeta_p, \sqrt[p]{2})$ . The description of  $\text{Gal}(L/\mathbb{Q})$  given in the text enables one to construct some elements of  $\text{Gal}(L/\mathbb{Q}(\zeta_p))$ . Use these automorphisms and Proposition 6.3.7 to prove that  $x^p - 2$  is irreducible over  $\mathbb{Q}(\zeta_p)$ .

*Proof.* Let  $L = \mathbb{Q}(\zeta_p, \sqrt[p]{2})$ , the splitting field of  $f = x^p - 2$  over  $\mathbb{Q}$ . Then  $\text{Gal}(L/\mathbb{Q}) \simeq \text{AGL}(1, \mathbb{F}_p)$ .

We show that  $x^p - 2$  is irreducible over  $\mathbb{Q}(\zeta_p)$ .

$\Phi_p = 1 + x + \dots + x^{p-1}$  is irreducible over  $\mathbb{Q}$ , thus  $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$ .

$[L : \mathbb{Q}] = p(p - 1)$  by Section 6.4. We deduce of  $[L : \mathbb{Q}] = [L : \mathbb{Q}(\zeta_p)] [(\mathbb{Q}(\zeta_p) : \mathbb{Q})]$  that

$$[\mathbb{Q}(\zeta_p, \sqrt[p]{2}) : \mathbb{Q}(\zeta_p)] = p.$$

If  $g$  is the minimal polynomial of  $\sqrt[p]{2}$  over  $\mathbb{Q}(\zeta_p)$ , then  $\deg(g) = [\mathbb{Q}(\zeta_p, \sqrt[p]{2}) : \mathbb{Q}(\zeta_p)] = p$ . Moreover  $\sqrt[p]{2}$  is a root of  $f = x^p - 2 \in \mathbb{Q}[x] \subset \mathbb{Q}(\zeta_p)[x]$ , thus  $g \mid f$  in  $\mathbb{Q}(\zeta_p)[x]$ , where  $f, g$  are of the same degree  $p$  and monic, thus  $g = f = x^p - 2$ .

Conclusion :  $x^p - 2$  is irreducible over  $\mathbb{Q}(\zeta_p)$ . □

## 6.5 ABELIAN EQUATION (OPTIONAL)

**Ex. 6.5.1** Assume that  $f \in F[x]$  is nonconstant and has roots  $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$  in a splitting field  $L$ . Prove that  $L = F(\alpha)$  if and only if there are rational functions  $\theta_i \in F(x)$  such that  $\alpha_i = \theta_i(\alpha)$ . Can we assume that the  $\theta_i$  are polynomials?

*Proof.* • Suppose that  $L = F(\alpha)$ . As  $\alpha_i \in L$ ,  $\alpha_i \in F(\alpha)$ . By definition of  $F(\alpha)$ , there exist  $\theta_i \in F(x)$  such that  $\alpha_i = \theta_i(\alpha)$ .

• Reciprocally, suppose that for all  $i$ ,  $1 \leq i \leq n$ ,  $\alpha_i = \theta_i(\alpha)$ ,  $\theta_i \in F(x)$ . Thus  $\alpha_i \in F(\alpha)$ . Consequently  $L = F(\alpha_1, \dots, \alpha_n) \subset F(\alpha)$ .

As  $F(\alpha) = F(\alpha_1) \subset F(\alpha_1, \dots, \alpha_n)$ ,  $L = F(\alpha_1, \dots, \alpha_n) = F(\alpha)$ .

Conclusion :  $L = F(\alpha) \iff \alpha_i = \theta_i(\alpha), \theta_i \in F(x) \ (1 \leq i \leq n)$ .

Moreover, as  $\alpha$  is algebraic over  $F$ ,  $F(\alpha) = F[\alpha]$ , therefore every  $\alpha_i \in F(\alpha) = F[\alpha]$  is of the form  $\alpha_i = \theta_i(\alpha)$ , where the  $\theta_i \in F[x]$  are polynomials.  $\square$

**Ex. 6.5.2** Show that the equation  $x^4 - 10x^2 + 1 = 0$  discussed in Example 6.5.1 is Abelian.

*Proof.* As in Example 6.5.1, let  $\theta_1(x) = x, \theta_2(x) = -x, \theta_3(x) = 10x - x^3, \theta_4(x) = -10x + x^3$ , so the solutions of the equations are  $\alpha_i = \theta_i(\alpha)$ ,  $i = 1, 2, 3, 4$ .

The roots of  $f$  being polynomials in  $\alpha$ , the splitting field of  $f$  is  $F(\alpha)$  (See Exercise 1).

Moreover, as  $\theta_1 = x, \theta_2 = -x, \theta_4 = -\theta_3$  and  $\theta_3, \theta_4$  are odd functions,

$\theta_1(\theta_i(\alpha)) = \theta_i(\alpha) = \theta_i(\theta(\alpha))$ ,  $i = 2, 3, 4$ .

$\theta_2(\theta_i(\alpha)) = -\theta_i(\alpha) = \theta_i(-\alpha) = \theta_i(\theta_2(\alpha))$ ,  $i = 3, 4$ .

$\theta_3(\theta_4(\alpha)) = \theta_3(-\theta_3(\alpha)) = -\theta_3^2(\alpha) = -\theta_4^2(\alpha) = \theta_4(-\theta_4(\alpha)) = \theta_4(\theta_3(\alpha))$ .

Thus  $\theta_i(\theta_j(\alpha)) = \theta_j(\theta_i(\alpha))$ , for  $1 \leq i < j \leq 4$ , thus also for  $1 \leq i, j \leq 4$ .

$x^4 - 10x^2 + 1 = 0$  is an Abelian equation.  $\square$

**Ex. 6.5.3** Complete the proof of theorem 6.5.3.

*Proof.* We show that the Galois group  $G$  of an Abelian equation is Abelian.

Let  $L = F(\alpha_1, \dots, \alpha_n)$  a splitting field of  $f \in F[x]$ , et  $\alpha = \alpha_1$ .

By definition of an Abelian equation, there exists  $\theta_i \in F(x)$  tels que  $\alpha_i = \theta_i(\alpha)$  ( $i = 1, \dots, n$ ), so  $L = F(\alpha)$  (see Exercise 1).

•  $\sigma \in \text{Gal}(L/F)$ , et  $f \in F[x]$ , thus  $\sigma(\alpha)$  is also a root  $\alpha_i, 1 \leq i \leq n$  of  $f$ :

$\sigma(\alpha) = \alpha_i = \theta_i(\alpha)$ . Similarly  $\tau(\alpha) = \theta_j(\alpha), 1 \leq j \leq n$ .

• if  $\sigma\tau = \tau\sigma$ , then  $\sigma(\tau(\alpha)) = (\sigma\tau)(\alpha) = (\tau\sigma)(\alpha) = \tau(\sigma(\alpha))$ .

Réciproquement, si  $\sigma(\tau(\alpha)) = \tau(\sigma(\alpha))$ , then  $(\sigma\tau)(\alpha) = (\tau\sigma)(\alpha)$ .

As  $L = F(\alpha)$ , and as  $\sigma\tau$  and  $\tau\sigma$  are identity over  $F$  and send  $\alpha$  on the same element,  $\sigma\tau = \tau\sigma$ .

$$\sigma\tau = \tau\sigma \iff \sigma(\tau(\alpha)) = \tau(\sigma(\alpha)).$$

•  $\sigma(\tau(\alpha)) = \sigma(\theta_j(\alpha))$ . Moreover  $\sigma$  is a  $F$ -automorphism of fields, et  $\theta_j \in F(x)$  a polynomial, thus  $\sigma(\theta_j(\alpha)) = \theta_j(\sigma(\alpha)) = \theta_j(\theta_i(\alpha))$ . Therefore  $\sigma(\tau(\alpha)) = \theta_j(\theta_i(\alpha))$ . Similarly  $\tau(\sigma(\alpha)) = \theta_i(\theta_j(\alpha))$ .

The equation  $f = 0$  being Abelian,  $\theta_j(\theta_i(\alpha)) = \theta_i(\theta_j(\alpha))$ , thus  $\sigma(\tau(\alpha)) = \tau(\sigma(\alpha))$ , so  $\sigma\tau = \tau\sigma$ , and this is true for all  $\sigma, \tau \in \text{Gal}(L/F)$  :  $\text{Gal}(L/F)$  is Abelian.

Conclusion: the Galois group of an Abelian equation is Abelian.  $\square$

**Ex. 6.5.4** Show that  $x^n - 1$  is an Abelian equation over  $\mathbb{Q}$ .

*Proof.* The roots of  $f = x^n - 1$  in  $\mathbb{C}$  are  $\zeta^k, 0 \leq k < n$ , where  $\zeta = e^{2i\pi/n}$ .

The splitting field of  $f$  over  $\mathbb{Q}$  is  $\mathbb{Q}(1, \zeta, \dots, \zeta^{n-1}) = \mathbb{Q}(\zeta)$ . Moreover, every root  $\zeta^k$  is of the form  $\zeta^k = \theta_k(\zeta)$ , where  $\theta_k = x^k, 0 \leq k \leq n-1$ .

$$\theta_i(\theta_j(\zeta)) = (\zeta^j)^i = \zeta^{ji} = (\zeta^i)^j = \theta_j(\theta_i(\zeta)), \quad 0 \leq i, j \leq n-1,$$

so by definition  $x^n - 1 = 0$  is an Abelian equation.  $\square$

**Ex. 6.5.5** Let  $f$  the minimal polynomial of  $\sqrt{2 + \sqrt{2}}$  over  $\mathbb{Q}$ . Show that  $f = 0$  is an Abelian equation.

*Proof.* By Exercises 5.1.6 and 6.3.4,

$$\begin{aligned} f &= x^4 - 4x^2 + 2 \\ &= \left(x - \sqrt{2 + \sqrt{2}}\right) \left(x + \sqrt{2 + \sqrt{2}}\right) \left(x - \sqrt{2 - \sqrt{2}}\right) \left(x + \sqrt{2 - \sqrt{2}}\right) \\ &= (x - \alpha)(x + \alpha)(x - \beta)(x + \beta) \end{aligned}$$

where  $\beta = \frac{1}{2} \left(\alpha - \frac{2}{\alpha^3}\right) = \alpha^3 - 3\alpha$ .

The 4 roots of  $f$  are of the form  $\alpha = \theta_1(\alpha), -\alpha = \theta_2(\alpha), \beta = \theta_3(\alpha), -\beta = \theta_4(\alpha)$ , where

$$\theta_1(x) = x, \theta_2(x) = -x, \theta_3(x) = x^3 - 3x, \theta_4(x) = -x^3 + 3x.$$

As  $\theta_1 = x, \theta_2 = -x, \theta_4 = -\theta_3$  and  $\theta_3, \theta_4$  are odd functions, as in Exercise 2,

$$\theta_1(\theta_i(\alpha)) = \theta_i(\alpha) = \theta_i(\theta_1(\alpha)), \quad i = 2, 3, 4.$$

$$\theta_2(\theta_i(\alpha)) = -\theta_i(\alpha) = \theta_i(-\alpha) = \theta_i(\theta_2(\alpha)), \quad i = 3, 4.$$

$$\theta_3(\theta_4(\alpha)) = \theta_3(-\theta_3(\alpha)) = -\theta_3^2(\alpha) = -\theta_4^2(\alpha) = \theta_4(-\theta_4(\alpha)) = \theta_4(\theta_3(\alpha)).$$

Thus  $\theta_i(\theta_j(\alpha)) = \theta_j(\theta_i(\alpha))$ , for  $1 \leq i < j \leq 4$ , thus also for  $1 \leq i, j \leq 4$ .

$$\theta_i(\theta_j(\alpha)) = \theta_j(\theta_i(\alpha)), \quad 1 \leq i, j \leq 4.$$

$$x^4 - 4x^2 + 2 = 0 \text{ is an Abelian equation.}$$

$\square$

**Ex. 6.5.6** In this exercise, you will prove a partial converse to Theorem 6.5.3. Suppose that a finite extension  $F \subset L$  is normal and separable and has an Abelian Galois group.

(a) Explain why  $F \subset L$  has a primitive element.

(b) By part (a), we can find  $\alpha \in L$  such that  $L = F(\alpha)$ . Let  $f$  be the minimal polynomial of  $\alpha$ . Prove that  $f = 0$  is an Abelian equation over  $f$ .

*Proof.* Suppose that  $F \subset L$  is normal and separable and that  $G = \text{Gal}(L/F)$  is an Abelian group.

(a) As  $F \subset L$  is separable, the Theorem of the Primitive Element shows that there exists a separable element  $\alpha \in L$  such that  $L = F(\alpha)$ .

- (b) Let  $f$  the minimal polynomial of  $\alpha$  over  $F$ . Then  $f$  is irreducible and separable. As  $F \subset L$  is normal, the roots  $\alpha_1 = \alpha, \dots, \alpha_n$  of  $f$  are all in  $L$ , so  $L = F(\alpha) = F(\alpha_1, \dots, \alpha_n)$  is the splitting field of  $f$ . By Exercise 1, there exist polynomials  $\theta_i \in F[x]$  such that  $\alpha_i = \theta_i(\alpha)$ ,  $i = 1, \dots, n$ .

Let  $1 \leq i, j \leq n$ . As  $f$  is separable and irreducible, by Proposition 6.3.7, the Galois group  $G$  acts transitively on the set of the roots of  $f$ : so there exists  $\sigma, \tau \in G$  such that  $\theta_i(\alpha) = \sigma(\alpha)$  and  $\theta_j(\alpha) = \tau(\alpha)$ .

Exercise 3 shows that  $(\sigma\tau)(\alpha) = \theta_j(\theta_i(\alpha))$  and  $(\tau\sigma)(\alpha) = \theta_i(\theta_j(\alpha))$ . As  $G$  is Abelian by hypothesis,  $\sigma\tau = \tau\sigma$ , so

$$\theta_j(\theta_i(\alpha)) = \theta_i(\theta_j(\alpha)), 1 \leq i, j \leq n.$$

The equation  $f = 0$  is Abelian.

Conclusion: if the finite extension  $F \subset L$  is normal and separable and has an Abelian Galois group, and if  $f$  is the minimal polynomial of a primitive element  $\alpha$ , then  $f = 0$  is an Abelian equation. □

**Ex. 6.5.7** Show that the implication (a)  $\Rightarrow$  (b) of Theorem 6.5.5 is equivalent to Kronecker's assertion that the roots of an Abelian equation over  $\mathbb{Q}$  can be expressed rationally in terms of a root of unity.

*Proof.* Suppose that the implication (a) $\Rightarrow$ (b) of Theorem 6.5.5 is true.

Let  $f \in \mathbb{Q}[x]$  such that the equation  $f = 0$  is Abelian. Then  $f$  has a root  $\alpha$  such that  $L = F(\alpha)$  is the splitting field of  $F$ , so the extension  $F \subset L$  is normal. By Theorem 6.5.3 (and Exercise 3), as the equation  $f = 0$  is Abelian,  $\text{Gal}(L/\mathbb{Q})$  is an Abelian group. The hypothesis (a) is so satisfied, and (b) follows:  $L \subset \mathbb{Q}(\zeta_n)$ , where  $\zeta_n = e^{2i\pi/n}$ . As the roots of  $f$  are in  $L$ , these roots can be expressed rationally in terms of a root of unity.

Conversely, suppose that the roots  $\alpha_1, \dots, \alpha_n$  of any Abelian equation  $f = 0$  in the splitting field of  $f$  can be expressed rationally in terms of a root of unity  $\zeta_n$ , and suppose also (a):  $\mathbb{Q} \subset L \subset \mathbb{C}$ , the extension  $\mathbb{Q} \subset L$  is normal, and  $\text{Gal}(L/\mathbb{Q})$  is an Abelian group.

As the characteristic of  $\mathbb{Q}$  is 0,  $\mathbb{Q} \subset L$  is also separable, and there exists a primitive element  $\alpha$  for the extension  $\mathbb{Q} \subset L$ . Let  $f$  the minimal polynomial of  $\alpha$  over  $\mathbb{Q}$ . By Exercise 6, since  $\mathbb{Q} \subset L$  is normal and separable, the equation  $f = 0$  is Abelian. By hypothesis, the roots  $\alpha_1 = \alpha, \dots, \alpha_n$  of  $f$  can be expressed rationally in terms of a root of unity  $\zeta_n$ , therefore  $\alpha_i \in \mathbb{Q}(\zeta_n)$ ,  $1 \leq i \leq n$ . In particular  $\alpha \in \mathbb{Q}(\zeta_n)$ , thus  $L = \mathbb{Q}(\alpha) \subset \mathbb{Q}(\zeta_n)$ . (b) is so proved under the hypothesis (a).

Conclusion: (a) $\Rightarrow$ (b) is equivalent to the assertion of Kronecker: the roots of an Abelian equation over  $\mathbb{Q}$  can be expressed rationally in terms of a root of unity. □