Solutions to David A.Cox "Galois Theory"

Richard Ganaye

August 26, 2022

9   Chapter 9 : CYCLOTOMIC EXTENSIONS

9.1   CYCLOTOMIC POLYNOMIALS

Ex. 9.1.1   *Prove that a congruence class $[i] \in \mathbb{Z}/n\mathbb{Z}$ has a multiplicative inverse if and only if $\gcd(i, n) = 1$. Conclude that $(\mathbb{Z}/n\mathbb{Z})^*$ has order $\phi(n)$. Be sure you understand what happens when $n = 1$.*

Proof. If $[i]$ has a multiplicative inverse in the ring $\mathbb{Z}/n\mathbb{Z}$, then there exists $[j] \in \mathbb{Z}/n\mathbb{Z}$ such that $[i][j] = [ij] = 1$, so $ij \equiv 1 \ [n]$. Thus there exists $k \in \mathbb{Z}$ such that $ij - kn = 1$. This Bézout's relation between i and n shows that $i \wedge n = 1$.

Conversely, if $i \wedge n = 1$, by Bézout's Theorem, there exist integers j, k such that $ij - kn = 1$, so $[i][j] = [1]$, and $[i]$ has a multiplicative inverse $\mathbb{Z}/n\mathbb{Z}$.

$$[i] \in (\mathbb{Z}/n\mathbb{Z})^* \iff i \wedge n = 1.$$

The mapping

$$\begin{cases} \{i \in \mathbb{N} \mid 0 \leq i < n, i \wedge n = 1\} & \to & (\mathbb{Z}/n\mathbb{Z})^* \\ i & \mapsto & [i] \end{cases}$$

obtained by restriction of the bijection $[\![0, n[\![\to \mathbb{Z}/n\mathbb{Z}, \ i \mapsto [i]$, is well defined, and this is a bijection.

Therefore

$$|(\mathbb{Z}/n\mathbb{Z})^*| = \text{Card}(\{i \in \mathbb{N} \mid 0 \leq i < n, i \wedge n = 1\} = \phi(n).$$

If $n = 1$, the ring $\mathbb{Z}/1\mathbb{Z}$ is the trivial ring $\{[0]\}$, where $[0] = [1]$, so the multiplicative group $(\mathbb{Z}/1\mathbb{Z})^* = \{[1]\}$ has one element, and the set of integers i such that $0 \leq i < 1 = n$ is reduced to $\{0\}$, which satisfies $0 \wedge 1 = 1$, so $\phi(1) = 1$. $\square$

Ex. 9.1.2   *Assume that $\gcd(n, m) = 1$. By Lemma A.5.2, we have a ring isomorphism $\alpha : \mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ that sends $[a]_{nm}$ to $([a]_n, [a]_m)$. Prove that α induces a group isomorphism $(Z/nm\mathbb{Z})^* \simeq (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$.*

Proof. Let A, B are commutative rings (with unity). Then

$$(A \times B)^* = A^* \times B^*.$$

Indeed, let $(a, b) \in A \times B$.

$$(a, b) \in (A \times B)^* \iff \exists (c, d) \in A \times B, \ (a, b)(c, d) = (1, 1)$$
$$\iff \exists c \in A, \exists d \in B, \ ac = 1, bd = 1$$
$$\iff a \in A^*, b \in B^*$$
$$\iff (a, b) \in A^* \times B^*.$$

Moreover, if $\varphi : A \to B$ is a ring isomorphism, then for all $a \in A^* \Rightarrow \varphi(a) \in A^*$, since $ab = 1_A \Rightarrow \varphi(a)\varphi(b) = \varphi(1_A) = 1_B$. So we can define $\psi : A^* \to B^*$ by restriction with $a \mapsto \psi(a) = \varphi(a)$.

ψ is a group homomorphism: if $u, v \in A^*, \psi(uv) = \varphi(uv) = \varphi(u)\varphi(v) = \psi(u)\psi(v)$, and ψ is bijective:

- φ is injective, so its restriction ψ if also injective.
- If $b \in B^*$, then there exists $d \in B$ such that $bd = 1$. If we write $a = \varphi^{-1}(b), c = \varphi^{-1}(d)$, then $b = \varphi(a), d = \varphi(c), 1 = bd = \varphi(ac)$, so $ac = 1, a \in A^*$, thus $b = \psi(a)$, so ψ is surjective.

$$A \simeq B \Rightarrow A^* \simeq B^*.$$

If we apply these two results to the rings $\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}$, we obtain

$$(\mathbb{Z}/nm\mathbb{Z})^* \simeq (\mathbb{Z}/n\mathbb{Z} \times Z/m\mathbb{Z})^* = (\mathbb{Z}/nZ)^* \times (\mathbb{Z}/m\mathbb{Z})^*.$$

$\square$

Ex. 9.1.3 *Let $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$. Prove that ζ_n^i for $0 \le i < n$ and $\gcd(i, n) = 1$ are the primitive nth roots of unity in $\mathbb{C}$.*

Proof. Let $\mathbb{U}_n$ be the group of n-th roots of unity in $\mathbb{C}$. Then $\mathbb{U}_n = \langle \zeta_n \rangle$, where $\zeta_n = e^{2i\pi/n}$. Write $o(x)$ the order of an element $x \in G$. Then $o(x) = |\langle x \rangle|$.

Recall that if $d > 0$, $o(x) = d \iff (\forall k \in \mathbb{Z}, \ x^k = e \iff d \mid k)$.

For all $i \in \mathbb{Z}$,
$$o(\zeta_n^i) = \frac{n}{n \wedge i}.$$

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

$$(\zeta_n^i)^k = 1 \iff \zeta_n^{ik} = 1 \iff n \mid ik \iff \frac{n}{n \wedge i} \mid \frac{i}{n \wedge i} k \iff \frac{n}{n \wedge i} \mid k$$

(since $\frac{n}{n \wedge i} \wedge \frac{i}{n \wedge i} = 1$). So $o(\zeta_n^i) = \frac{n}{n \wedge i}$.

By definition, ζ is a primitive nth root of unity if and only if ζ is a generator of $\mathbb{U}_n$, if and only if $o(\zeta) = n$, so

$$\mathbb{U}_n = \langle \zeta_n^i \rangle \iff o(\zeta_n^i) = n \iff \frac{n}{n \wedge i} = n \iff n \wedge i = 1.$$

$\square$

Ex. 9.1.4 *Let R be an integral domain, and let $f, g \in R[x]$, where $f \ne 0$. If K is the field of fractions of R, then we can divide g by f in $K[x]$ using the division algorithm of Theorem A.1.14. This gives $g = qf + r$, though $q, r \in K[x]$ need not lie in $R[x]$.*

(a) *Show that dividing x^2 by $2x + 1$ in $\mathbb{Q}[x]$ gives $x^2 = q \cdot (2x + 1) + r$, where $q, r \in \mathbb{Q}[x]$ are not in $\mathbb{Z}[x]$, even though x^2 and $2x + 1$ lie in $\mathbb{Z}[x]$.*

(b) Show that if f is monic, then the division algorithm gives $g = qf + r$, where $q, r \in R[x]$. Hence the division algorithm works over R provides we divide by monic polynomials.

Proof. (a) $x^2 = (\frac{1}{2}x - \frac{1}{4})(2x + 1) + \frac{1}{4}$. The quotient $q(x) = \frac{1}{2}x - \frac{1}{4}$ is not in $\mathbb{Z}[x]$.

(b) Let $f = x^m + b_{m-1}x^{m-1} + \cdots + b_0$ be a fixed monic polynomial in $R[x]$.

We show by induction on the degree n the proposition

$P(n) : \forall g \in R[x], \deg(g) = n \Rightarrow \exists(q, r) \in R^2, \; g = qf + r, \; \deg(r) < \deg(f)$

(with the convention $\deg(0) = -\infty$).

We suppose that $P(k)$ is true for all $k < n$, and we prove $P(n)$. Let g any polynomial in $R[x]$.

- If $\deg(g) < m = \deg(f)$, then the pair $(q, r) = (0, g)$ is an answer.

- Suppose that $\deg(g) \geq m$. Write $g = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$, with $\deg(g) = n \geq m$ and $a_i \in R, i = 0, \ldots, n$.

The polynomial $g_1 = g - a_nx^{n-m}f \in R[x]$ satisfies $\deg(g_1) < n$. We can then apply to it the induction hypothesis:

$g_1 = q_1f + r, q_1 \in R[x], \; r \in R[x], \; \deg(r) < \deg(f)$.

Then $g = (a_nx^{n-m} + q_1)f + r$.

If we write $q = a_nx^{n-m} + q_1$, then $q \in R[x]$ and $g = fq + r, \; (q, r) \in R[x]^2, \deg(r) < \deg(f)$. The pair (q, r) is an answer, and the induction is done.

In particular, if $g, f \in \mathbb{Z}[x]$, and $g = fq$, the unicity of the Euclidean division in $\mathbb{Q}[x]$ and the preceding result shows that $q \in \mathbb{Z}[x]$.

$\square$

Ex. 9.1.5 *Verify the formula for $\Phi_{105}(x)$ given in Example 9.1.7.*

Proof. The factors of $105 = 3 \times 5 \times 7$ are $105, 35, 21, 15, 7, 5, 3, 1$, thus

$$x^{105} - 1 = \Phi_{105}\, \Phi_{35}\, \Phi_{21}\, \Phi_{15}\, \Phi_7\, \Phi_5\, \Phi_3\, \Phi_1.$$

As $x^{35} - 1 = \Phi_{35}\, \Phi_7\, \Phi_5\, \Phi_1$, we obtain

$$x^{105} - 1 = (x^{35} - 1)\Phi_{105}\, \Phi_{21}\, \Phi_{15}\, \Phi_3,$$

that is

$$x^{70} + x^{35} + 1 = \Phi_{105}\, \Phi_{21}\, \Phi_{15}\, \Phi_3.$$

Moreover $x^{21} - 1 = \Phi_{21}\, \Phi_7\, \Phi_3\, \Phi_1$, so

$$\begin{aligned}
\Phi_{21} &= (x^{21} - 1)\frac{x - 1}{x^7 - 1}\frac{x - 1}{x^3 - 1}\frac{1}{x - 1} \\
&= \frac{x^{21} - 1}{(x^7 - 1)(x^2 + x + 1)} \\
&= \frac{x^{14} + x^7 + 1}{x^2 + x + 1} \\
&= x^{12} - x^{11} + x^9 - x^8 + x^6 - x^4 + x^3 - x + 1.
\end{aligned}$$

Similarly $x^{15} - 1 = \Phi_{15}\,\Phi_5\,\Phi_3\,\Phi_1$, so

$$\begin{aligned}
\Phi_{15} &= \frac{x^{15} - 1}{(x^5 - 1)(x^2 + x + 1)} \\
&= \frac{x^{10} + x^5 + 1}{x^2 + x + 1} \\
&= x^8 - x^7 + x^5 - x^4 + x^3 - x + 1.
\end{aligned}$$

Therefore

$$\begin{aligned}
\Phi_{105} &= \frac{x^{70} + x^{35} + 1}{\Phi_{21}\Phi_{15}\Phi_3} \\
&= \frac{x^{70} + x^{35} + 1}{x^{22} - x^{21} + x^{19} - x^{18} + x^{17} + x^{12} - x^{11} + x^{10} + x^5 - x^4 + x^3 - x + 1} \\
&= \ x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2\,x^{41} - x^{40} - x^{39} + x^{36} + x^{35} + x^{34} + x^{33} + x^{32} \\
&\quad + x^{31} - x^{28} - x^{26} - x^{24} - x^{22} - x^{20} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} - x^9 - x^8 \\
&\quad - 2\,x^7 - x^6 - x^5 + x^2 + x + 1
\end{aligned}$$

$\square$

Ex. 9.1.6 *This exercise is concerned with the proof of Lemma 9.1.8.*

(a) *Let $f \in \mathbb{Z}[x_1, \ldots, x_n]$ be symmetric. Prove that f is a polynomial in $\sigma_1, \ldots, \sigma_n$ with integer coefficients.*

(b) *Let p be prime and let $h \in \mathbb{F}_p[x_1, \ldots, x_n]$. Prove that $h(x_1, \ldots, x_n)^p = h(x_1^p, \ldots, x_n^p)$.*

Proof.   (a) The algorithm in the proof of Theorem 2.2.2 consists to replace the symmetric polynomial f, here with coefficients in $\mathbb{Z}$, by $f_1 = f - cg$, $f_2 = f - cg - c_1 g_1, \cdots$, until we obtain 0. The coefficient c is the leading coefficient of f, so it is an integer, and $g = \sigma_1^{a_1 - a_2} \cdots \sigma_{n-1}^{a_{n-1} - a_n} \sigma_n^{a_n} \in \mathbb{Z}[\sigma_1, \ldots, \sigma_n]$, so $f_1 \in \mathbb{Z}[x_1, \ldots, x_n]$. The same reasoning applied to f_1 and to the following terms shows that $c_i \in \mathbb{Z}$ for all i. Therefore
$$f = cg + c_1 g_1 + \cdots + c_{m-1} g_{m-1} \in \mathbb{Z}[\sigma_1, \cdots, \sigma_n].$$

In particular, the symmetric polynomial $\sigma_i(x_1^p, \cdots, x_r^p) - \sigma_i(x_1, \cdots, x_r)^p$ is a polynomial in $\sigma_1, \ldots, \sigma_r$ with integer coefficients:

$$\sigma_i(x_1^p, \cdots, x_r^p) - \sigma_i(x_1, \cdots, x_r)^p = S(\sigma_1, \cdots, \sigma_r) \in \mathbb{Z}[\sigma_1, \cdots, \sigma_r].$$

(b) Let $h \in \mathbb{F}_p[x_1, \ldots, x_n]$. Write

$$h = \sum_{(i_1, \ldots, i_n) \in A} a_{i_1, \ldots, i_n} x_1^{i_1} \cdots x_n^{i_n},$$

where $A \subset \mathbb{N}^n$ is finite, and the coefficients $a_{i_1, \ldots, i_n} \in \mathbb{F}_p$. As the characteristic of the field $\mathbb{F}_p(x_1, \cdots, x_r)$ is p, using the Little Fermat's Theorem: $a^p = a$ for all

$a \in \mathbb{F}_p$,

$$f(x_1, \ldots, x_n)^p = \left(\sum_{(i_1,\ldots,i_n) \in A} a_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n} \right)^p$$

$$= \sum_{(i_1,\ldots,i_n) \in A} a_{i_1,\ldots,i_n}^p x_1^{pi_1} \cdots x_n^{pi_n}$$

$$= \sum_{(i_1,\ldots,i_n) \in A} a_{i_1,\ldots,i_n} x_1^{pi_1} \cdots x_n^{pi_n}$$

$$= f(x_1^p, \ldots, x_n^p)$$

In particular, write $\overline{\sigma}_i$ the projection of σ_i in $\mathbb{F}_p[x_1, \cdots, x_r]$, and $\overline{S}$ the projection of S. As the characteristic of the field $\mathbb{F}_p(x_1, \cdots, x_r)$ is p,

$$\overline{\sigma}_i(x_1, \cdots, x_r)^p = \left(\sum_{1 \le j_1 < j_2 < \cdots < j_i \le r} x_{j_1} \cdots x_{j_i} \right)^p$$

$$= \sum_{1 \le j_1 < j_2 < \cdots < j_i \le r} x_{j_1}^p \cdots x_{j_i}^p$$

$$= \overline{\sigma}_i(x_1^p, \cdots, x_r^p)$$

Hence $\overline{S}(\overline{\sigma}_1, \ldots, \overline{\sigma}_r) = \overline{\sigma}_i(x_1^p, \cdots, x_r^p) - \overline{\sigma}_i^p = 0$. Since $\overline{\sigma}_1, \ldots, \overline{\sigma}_r$ are algebraically independant over $\mathbb{F}_p$ (see Ex. 2.2.5), $\overline{S} = 0$, so $S \equiv 0 \pmod{p}$. Therefore p divides all the coefficients of S.

$\square$

Ex. 9.1.7 *This exercise is concerned with the proof of Theorem 9.1.9.*

(a) *Let ζ be a primitive nth root of unity, and let i be relatively prime to n. Prove that ζ^i is a primitive nth root of unity and that every primitive nth root of unity is of this form.*

(b) *Let $\gamma_1, \ldots, \gamma_r$ be distinct primitive nth roots of unity and let i be relatively prime to n. Prove that $\gamma_1^i, \ldots, \gamma_r^i$ are distinct.*

Proof. Let ζ be a primitive nth root of unity, so $o(\zeta) = n$ (where we write $o(x)$ the order of an element x in a group G). We have proved in Exercise 3 that for all $i \in \mathbb{Z}$,

$$o(\zeta^i) = \frac{n}{n \wedge i}$$

In particular, if i and n are relatively prime ($n \wedge i = 1$), then $o(\zeta^i) = n$, so ζ^i is a primitive nth root of unity.

If ξ is any primitive nth root of unity, as ζ is a generator of $\mathbb{U}_n$, $\xi = \zeta^i, 0 \le i < n$. As ζ^i is a primitive nth root of unity, $o(\zeta^i) = n = \frac{n}{n \wedge i}$, so $n \wedge i = 1$.

(b) Let $i \in \mathbb{Z}$ relatively prime to n. Consider

$$\varphi : \begin{cases} \mathbb{U}_n & \to & \mathbb{U}_n \\ \lambda & \mapsto & \lambda^i \end{cases}$$

φ is a group homomorphism.

If $\lambda \in \ker(\varphi)$, then $\lambda = \zeta^k$, $k \in \mathbb{Z}$, and $1 = \lambda^i = \zeta^{ki}$, thus $n \mid ki$. Since $n \wedge i = 1$, $n \mid k$, hence $\lambda = \zeta^k = 1$, so $\ker(\varphi) = \{1\}$.

The group homomorphism φ is injective, so the images of the distinct $\gamma_1, \cdots, \gamma_r \in \mathbb{U}_n$ are distinct.

Conclusion: if $i \wedge n = 1$, $\zeta \mapsto \zeta^i$ is a bijection from the set of primitive nth roots of unity on itself.

$\square$

Ex. 9.1.8 *This exercise will present an alternate proof of (9.8) that doesn't use symmetric polynomials.*

$$(9.8) \qquad \text{If } \zeta \text{ is a root of } f, \text{ then so is } \zeta^p.$$

where f is an irreducible factor of Φ_n, and p a prime number such that $p \nmid n$.

Assume that ζ is a root of f such that $f(\zeta^p) \neq 0$. As in the text, $q(x) \in \mathbb{Z}[x]$ maps to the polynomial $\overline{q}(x) \in \mathbb{F}_p[x]$. Let $g(x)$ be as in (9.7), i.e. $\Phi_n(x) = f(x)g(x)$.

(a) *Prove that ζ is a root of $g(x^p)$, and conclude that $f(x) \mid g(x^p)$.*

(b) *Use Gauss's Lemma to explain why $f(x)$ divides $g(x^p)$ in $\mathbb{Z}[x]$, and conclude that $\overline{f}(x)$ divides $\overline{g}(x^p)$ in $\mathbb{F}_p[x]$.*

(c) *Use Exercise 7 to prove that $\overline{g}(x)^p = \overline{g}(x^p)$, and conclude that $\overline{f}(x)$ divides $\overline{g}(x)^p$.*

(d) *Now let $h(x) \in \mathbb{F}_p[x]$ be an irreducible factor of $\overline{f}(x)$. Show that $h(x)$ divides $\overline{g}(x)$, so that $h(x)^2$ divides $\overline{f}(x)\overline{g}(x)$.*

(e) *Conclude that $h(x)^2$ divides $x^n - 1 \in \mathbb{F}_p[x]$.*

(f) *Use separability to obtain a contradiction.*

Proof. As in the proof of Theorem 9.1.9, the Gauss's Lemma in the form of Corollary 4.2.1 allows us to assume that there exists a polynomial $f(x) \in \mathbb{Z}[x]$ of $\Phi_n(x)$ such that $\Phi_n(x) = f(x)g(x)$, $f(x), g(x) \in \mathbb{Z}[x]$, where f is monic and irreducible over $\mathbb{Q}$. Let p be a prime number such that $p \nmid n$.

Reasoning by contradiction, we suppose that ζ is a root of f such that $f(\zeta^p) \neq 0$.

(a) As ζ is the root of f, where f divides Φ_n, ζ is a nth primitive root of unity. Since $p \nmid n, p \wedge n = 1$, hence ζ^p is also a nth primitive root of unity by Exercise 7(a), therefore $0 = \Phi(\zeta^p) = f(\zeta^p)g(\zeta^p)$. As $f(\zeta^p) \neq 0$, $g(\zeta^p) = 0$, so

$$\zeta \text{ is a root of } g(x^p).$$

As f is irreducible, f is the minimal polynomial of ζ over $\mathbb{Q}$, and ζ is a root of $g(x^p) \in \mathbb{Q}[x]$, hence

$$f(x) \mid g(x^p).$$

(b) As f is monic, the refined division algorithm of Exercise 4 show that the quotient $q(x)$ of $g(x^p)$ by $f(x)$ lies in $\mathbb{Z}[x]$, so $f(x)$ divides $g(x^p)$ in $\mathbb{Z}[x]$.

The projection homomorphism on $\mathbb{F}_p[x]$ gives $\overline{g}(x^p) = \overline{f}(x)\overline{q}(x)$, thus $\overline{f}(x)$ divides $\overline{g}(x^p)$ in $\mathbb{F}_p[x]$.

(c) As the characteristic of $\mathbb{F}_p(x)$ is p, writing $\overline{g}(x) = \sum_{i=0}^{r} a_i x^i \in \mathbb{F}_p[x]$, then (as in Exercise 7)

$$\overline{g}(x)^p = \left(\sum_{i=0}^{r} a_i x^i\right)^p = \sum_{i=0}^{r} a_i^p x^{ip} = \sum_{i=0}^{r} a_i x^{ip} = \overline{g}(x^p).$$

Therefore $\overline{f}(x)$ divides $\overline{g}(x)^p$ in $\mathbb{F}_p[x]$.

(d) Let $h(x) \in \mathbb{F}_p[x]$ an irreducible factor of $\overline{f}(x)$. Then $h(x) \mid \overline{g}(x)^p$. Since h is irreducible (hence prime) in $\mathbb{F}_p[x]$, then $h \mid \overline{g}$.

$h(x) \mid \overline{f}(x), h(x) \mid \overline{g}(x)$, so $h(x)^2 \mid \overline{f}(x)\overline{g}(x)$.

(e) Therefore $h^2 \mid \overline{\Phi}_n$, and $\overline{\Phi}_n \mid x^n - 1$, thus $h^2 \mid x^n - 1 \in F_p[x]$.

(f) As $\deg(h) > 1$, every root of h in the splitting root of $x^n - 1 \in \mathbb{F}_p[x]$ is not a simple root, thus $x^n - 1$ would not be separable.

But n is relatively prime to p, so $(x^n - 1)' = nx^{n-1}$ is relatively prime to $x^n - 1$, and so $x^n - 1 \in \mathbb{F}_p[x]$ is separable: this is a contradiction, therefore.

$$f(\zeta) = 0 \Rightarrow f(\zeta^p) = 0.$$

We conclude that Φ_n is irreducible as in the conclusion of the proof of Theorem 9.1.9.

$\square$

Ex. 9.1.9 *In proving Fermat's Little Theorem $a^p \equiv a$ (mod p), recall from the proof of Lemma 9.1.2 that we first proved $a^{p-1} \equiv 1$ (mod p) when a is relatively prime to p. For general $n > 1$, Euler showed that $a^{\phi(n)} \equiv 1$ (mod n) when a is relatively prime to n. Prove this. What basic fact from group theory do you use?*

Proof. If $a \wedge n = 1$, $[a] \in (\mathbb{Z}/n\mathbb{Z})^*$. By Lagrange Theorem, the order of $[a]$ divides the order of the group $(\mathbb{Z}/n\mathbb{Z})^*$, therefore the order of a divides $\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$, and so $[a]^{\phi(n)} = [1]$.

$$a \wedge n = 1 \Rightarrow a^{\phi(n)} \equiv 1 \quad (\text{mod } n).$$

$\square$

Ex. 9.1.10 *Prove that a cyclic group of order n has $\phi(n)$ generators.*

Proof. More generally, we prove that a cyclic group G of order n has $\phi(d)$ elements of order d if $d \mid n$ (0 otherwise !).

Let ζ a generator of G: $G = \langle \zeta \rangle$.

Every element $\alpha \in G$ is of the form $\zeta^k, 0 \leq k < n$. Recall (see Exercise 3), that

$$o(\zeta^k) = \frac{n}{n \wedge k}.$$

If $d \nmid n$, there is no element of order d by Lagrange's Theorem, and if $d \mid n$,

$$o(\zeta^k) = d \iff \frac{n}{n \wedge k} = d$$
$$\iff \frac{n}{d} = n \wedge k$$
$$\iff \exists \lambda \in \mathbb{Z}, \ k = \lambda \frac{n}{d}, \ 0 \le \lambda < d, \ \lambda \wedge d = 1$$

Indeed, if $\delta = \frac{n}{d} = n \wedge k$, then there exists λ, μ, with $\lambda \wedge \mu = 1$, such that

$$\begin{cases} n &= \mu\delta \\ k &= \lambda\delta \end{cases}.$$

$\mu = n/\delta = d$, so $\lambda \wedge d = 1$. As $0 \le k < n$, $0 \le \lambda < n/\delta = d$.
Conversely, if $k = \lambda \frac{n}{d}$, $\lambda \wedge d = 1$, then

$$n \wedge k = d\frac{n}{d} \wedge \lambda\frac{n}{d} = (d \wedge \lambda)\frac{n}{d} = \frac{n}{d}.$$

The elements of order d in G are so the elements ζ^k, where

$$k = \lambda\frac{n}{d}, \ 0 \le \lambda < d, \ \lambda \wedge d = 1.$$

The mapping $\varphi : \{\lambda \in \mathbb{Z} \mid 0 \le \lambda < d, \lambda \wedge d = 1\} \to \{\alpha \in G \mid o(\alpha) = d\}$ defined by $\varphi(\lambda) = \zeta^{\lambda\frac{n}{d}}$ is so a bijection.

Hence there exist exactly $\phi(d)$ elements of order d in G, for every factor d of $n = |G|$. In particular, there exist $\phi(n)$ elements of order $n = |G|$ in G, hence $\phi(n)$ generators in a cyclic group G of order n. $\qquad\square$

Ex. 9.1.11 *Prove that $n = \sum_{d \mid n} \phi(d)$.*

Proof. Let G a fixed cyclic group of order n, by example $G = \mathbb{U}_n$. If A_d is the set of elements of order d in G, then G is the disjoint union of the A_n, so $|G| = \sum_{d=0}^{n} |A_d|$.

By the proof of Exercise 10, $|A_d| = \phi(d)$ if $d \mid n$, and $|A_d| = 0$ if $d \nmid n$, so

$$n = \sum_{d \mid n} \phi(d).$$

Note: as an alternative proof, we can take the degrees in the formula $x^n - 1 = \prod_{d \mid n} \Phi_d(n)$.
$\qquad\square$

Ex. 9.1.12 *Here are some further properties of cyclotomic polynomials.*

(a) *Given n, let $m = \prod_{p \mid n} p$. Prove that $\Phi_n(x) = \Phi_m(x^{n/m})$. This shows that we can reduce computing $\Phi_n(x)$ to the case when n is squarefree.*

(b) *Let $n > 1$ be an odd integer. Prove that $\Phi_{2n}(x) = \Phi_n(-x)$.*

(c) *Let p be a prime not dividing an integer $n > 1$. Prove that $\Phi_{pn}(x) = \Phi_n(x^p)/\Phi_n(x)$.*

Lemma. *Let $f(x), g(x) \in \mathbb{C}[x]$ be two monic polynomials in $\mathbb{Q}[x]$, of same degree d, and f separable.*

If every root of f in $\mathbb{C}$ is a root of g, then $f = g$.

Proof of the Lemma. As $f(x)$ is monic separable of degree d, the decomposition in irreducible factors of $f(x)$ in $\mathbb{C}[x]$ is

$$f(x) = \prod_{\alpha \in S} (x - \alpha)$$

The hypothesis implies that for all $\alpha \in S$, $x - \alpha \mid g(x)$, hence $f(x) \mid g(x)$. As $\deg(f) = \deg(g)$, and as f, g are monic, then $f = g$. $\qquad\square$

Proof. (a) $n = p_1^{\nu_1} p_2^{\nu_2} \cdots p_r^{\nu_r}$. Write $m = p_1 \cdots p_r$. Then

$\deg(\Phi_n(x)) = \phi(n) = p_1^{\nu_1 - 1} p_2^{\nu_2 - 1} \cdots p_r^{\nu_r - 1} (p_1 - 1)(p_2 - 1) \cdots (p_r - 1)$.

$\deg(\Phi_m(x))) = \phi(p_1 p_2 \cdots p_n) = (p_1 - 1)(p_2 - 1) \cdots (p_r - 1)$, therefore

$\deg(\Phi_m(x^{n/m})) = p_1^{\nu_1 - 1} p_2^{\nu_2 - 1} \cdots p_r^{\nu_r - 1} (p_1 - 1)(p_2 - 1) \cdots (p_r - 1) = \deg(\Phi_n(x))$.

Moreover these polynomials are monic and Φ_n is separable. It remains to show that every root ζ of $\Phi_n(x)$ is a root of $\Phi_m(x^{n/m})$.

Such a root ζ has order $n = p_1^{\nu_1} p_2^{\nu_2} \cdots p_r^{\nu_r}$ in the group $\mathbb{C}^*$.

Write $\xi = \zeta^{n/m} = \zeta^{p_1^{\nu_1 - 1} p_2^{\nu_2 - 1} \cdots p_r^{\nu_r - 1}}$.

Then the order of ξ is $m = p_1 p_2 \cdots p_r$. Indeed, for all $k \in \mathbb{Z}$,

$\xi^k = 1 \iff \zeta^{k p_1^{\nu_1 - 1} p_2^{\nu_2 - 1} \cdots p_r^{\nu_r - 1}} = 1 \iff p_1^{\nu_1} p_2^{\nu_2} \cdots p_r^{\nu_r} \mid k p_1^{\nu_1 - 1} p_2^{\nu_2 - 1} \cdots p_r^{\nu_r - 1}$

$\iff p_1 p_2 \cdots p_r \mid k$.

Therefore, by definition of Φ_m, $\Phi_m(\zeta^{n/m}) = \Phi_m(\xi) = 0$.

The hypotheses of the lemma are satisfied, thus

$$\Phi_n(x) = \Phi_m(x^{n/m})$$

(b) We show that $\Phi_{2n}(x) = \Phi_n(-x)$ ($n > 1, n$ odd, so $n \geq 3$).

Note first that $\deg(\Phi_{2n}(x)) = \phi(2n) = \phi(2)\phi(n) = \phi(n) = \deg(\Phi_n(-x))$.

If $n > 2$, then $\phi(n)$ is even. Indeed, we can group in pairs the elements of $(\mathbb{Z}/n\mathbb{Z})^*$, with the pairs $\{[d], -[d]\}$, where $d \wedge n = 1$ and $[d] \neq -[d]$ since $(n \mid 2d, d \wedge n = 1) \Rightarrow n \mid 2$, which is impossible if $n > 2$. Hence

$$(-1)^{\phi(n)} = 1 \qquad (n > 2).$$

$\Phi_{2n}(x)$ is monic by definition, and the leading coefficient of $\Phi_n(-x)$ is $(-1)^{\phi(n)} = 1$, so $\Phi_n(-x)$ is also monic.

Let α be any root of $\Phi_n(-x)$. Then $\alpha = -\zeta$, where ζ is a nth primitive root of unity , so ζ is an element of order n in the group $\mathbb{C}^*$.

Then the order of $\alpha = -\zeta$ is $2n$. Indeed, for all $k \in \mathbb{Z}$,

$(-\zeta)^k = 1$, that is $(-1)^k \zeta^k = 1$, implies $\zeta^{2k} = 1$, thus $n \mid 2k$, so $n \mid k$ (since n is odd), therefore $\zeta^k = 1, (-1)^k = 1$ and so $2 \mid k$.

As $n \wedge 2 = 1, 2n \mid k$.

Conversely, if $2n \mid k$, $(-\zeta)^{2n} = [(-1)^2]^n [\zeta^n]^2 = 1$.

Conclusion: $(-\zeta)^k = 1 \iff 2n \mid k$, so the order of $\alpha = -\zeta$ is $2n$, hence $x = -\zeta$ is a root of Φ_{2n}.

Every root of $\Phi_n(-x)$ in $\mathbb{C}$ is a root of $\Phi_{2n}(x)$. Moreover $\Phi_n(-x)$ is a separable polynomial, and $\deg(\Phi_{2n}(x)) = \deg(\Phi_n(-x))$. Then the lemma gives the conclusion, for all odd n, $n > 1$,

$$\Phi_{2n}(x) = \Phi_n(-x)$$

(c) We show first that $\Phi_n(x)$ divides $\Phi_n(x^p)$. As $\Phi_n(x)$ is separable, it is sufficient to verify that every root ζ of $\Phi_n(x)$ is a root of $\Phi_n(x^p)$. Such a root ζ is a nth primitive root of unity, so its order is n. Then the order of ζ^p is also n. Indeed, for all $k \in \mathbb{Z}$, as $n \wedge p = 1$,

$$(\zeta^p)^k = 1 \iff \zeta^{pk} = 1 \iff n \mid pk \iff n \mid k.$$

Therefore ζ^p is a root of Φ_n, so $\Phi_n(\zeta^p) = 0$ and ζ is a root of $\Phi_n(x^p)$.

$$\Phi_n(x) \mid \Phi_n(x^p) \quad (p \nmid n).$$

We compare the degrees:

$\deg(\Phi_{pn}(x)) = \phi(pn) = \phi(p)\phi(n) = (p-1)\phi(n)$,

$\deg(\Phi_n(x^p)/\Phi_n(x)) = p\phi(n) - \phi(n) = (p-1)\phi(n)$, thus

$$\deg(\Phi_n(x^p)/\Phi_n(x)) = \deg(\Phi_{pn}(x)).$$

Moreover, these two polynomials are monic, and Φ_{pn} is separable.

We show that every root ζ of $\Phi_{pn}(x)$ is a root of $\Phi_n(x^p)/\Phi_n(x)$.

If ζ is a root of $\Phi_{pn}(x)$, then $o(\zeta) = pn$, therefore $o(\zeta^p) = n$

(indeed, for all $k \in \mathbb{Z}$, $(\zeta^p)^k = 1 \iff \zeta^{pk} = 1 \iff pn \mid pk \iff n \mid k$).

So ζ^p is a root of $\Phi_n(x)$, which is equivalent to ζ is a root of $\Phi_n(x^p)$.

As $o(\zeta) = pn$, $\zeta^n \neq 1$, $\Phi_n(\zeta) \neq 0$, therefore ζ is a root of $\Phi_n(x^p)/\Phi_n(x)$.

The hypotheses of the lemma are so satisfied, so

$$\Phi_{pn}(x) = \Phi_n(x^p)/\Phi_n(x) \qquad (p \nmid n).$$

$\square$

Ex. 9.1.13 *We know $\Phi_p(x)$ when p is prime. Use this and Exercise 12 to compute $\Phi_{15}(x)$ and $\Phi_{105}(x)$.*

Proof. (a) By Exercise 12(c),

$$\begin{aligned}
\Phi_{15}(x) &= \frac{\Phi_3(x^5)}{\Phi_3(x)} \\
&= \frac{x^{10} + x^5 + 1}{x^2 + x + 1} \\
&= x^8 - x^7 + x^5 - x^4 + x^3 - x + 1.
\end{aligned}$$

(b)

$$\Phi_{105}(x) = \frac{\Phi_{15}(x^7)}{\Phi_{15}(x)}$$

$$= \frac{x^{56} - x^{49} + x^{35} - x^{28} + x^{21} - x^7 + 1}{x^8 - x^7 + x^5 - x^4 + x^3 - x + 1}$$

$$= \quad x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2\,x^{41} - x^{40} - x^{39} + x^{36} + x^{35} + x^{34} + x^{33} + x^{32}$$

$$+ \, x^{31} - x^{28} - x^{26} - x^{24} - x^{22} - x^{20} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} - x^9 - x^8$$

$$- \, 2\,x^7 - x^6 - x^5 + x^2 + x + 1$$

$\square$

Ex. 9.1.14 *The Möbius function is defined for integers $n \geq 1$ by*

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^s, & \text{if } n = p_1 \cdots p_s \text{ for distinct primes } p_1, \ldots, p_s \\ 0, & \text{otherwise} \end{cases}$$

Prove that $\sum_{d|n} \mu\left(\frac{n}{d}\right) = 0$ when $n > 1$.

Proof. Suppose $n > 1$. Write $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ its decomposition in prime factors. The factors d of n such that $\mu(d) \neq 0$ are the integers $d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ where $\beta_i = 0, 1$. If exactly r exponents β_i are non zero, then $\mu(d) = (-1)^r$, and there are $\binom{k}{r}$ such integers d.

Therefore

$$\sum_{d|n} \mu(d) = \sum_{r=0}^{k} (-1)^r \binom{k}{r} = (1-1)^k = 0$$

(since $k \neq 0$)

Conclusion: if $n \geq 1$,

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) = \begin{cases} 0, & \text{if } n > 1, \\ 1, & \text{if } n = 1. \end{cases}$$

$\square$

Ex. 9.1.15 *Let μ be the Möbius function defined in Exercise 14. Prove that*

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}.$$

Proof. Our starting point is

$$F(n) = x^n - 1 = \prod_{d|n} \Phi_d \qquad (n \geq 1).$$

It is sufficient to copy the proof of the Möbius Inversion Formula in multiplicative notations:

$$\prod_{d|n}(x^d - 1)^{\mu\left(\frac{n}{d}\right)} = \prod_{e|n}(x^{\frac{n}{e}} - 1)^{\mu(e)}$$

$$= \prod_{e|n}\prod_{d|\frac{n}{e}}\Phi_d^{\mu(e)}$$

$$= \prod_{d|n}\prod_{e|\frac{n}{d}}\Phi_d^{\mu(e)} \qquad \left(\text{since } e|n \text{ and } d|\frac{n}{e} \iff d|n \text{ and } e|\frac{n}{d}\right)$$

$$= \prod_{d|n}\Phi_d^{\sum_{e|\frac{n}{d}}\mu(e)}$$

$$= \Phi_n,$$

since by Exercise 14, $\sum_{e|\frac{n}{d}}\mu(e) \neq 0$ only if $\frac{n}{d} = 1$, that is $d = n$, so the product is Φ_n.

Conclusion :

$$\Phi_n(x) = \prod_{d|n}(x^d - 1)^{\mu\left(\frac{n}{d}\right)} \quad (n \geq 1).$$

$\square$

Ex. 9.1.16 *Let n and m be relatively prime positive integers.*

(a) *Prove that $\mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_{nm})$.*

(b) *Prove that $\Phi_n(x)$ is irreducible over $\mathbb{Q}(\zeta_m)$.*

Proof. Here we write $\zeta_k = e^{2i\pi/k}$ for all subscript k.

(a) $\zeta_n = (\zeta_{nm})^m \in \mathbb{Q}(\zeta_{nm})$, and $\zeta_m = (\zeta_{nm})^n \in \mathbb{Q}(\zeta_{nm})$, therefore

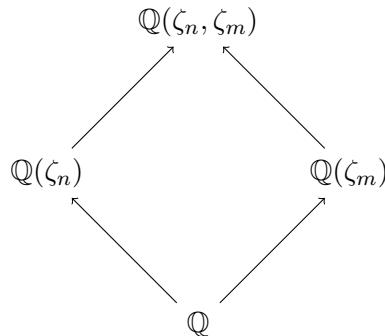$$\mathbb{Q}(\zeta_n, \zeta_m) \subset \mathbb{Q}(\zeta_{nm}).$$

As $n \wedge m = 1$, there exists integers u, v such that $1 = un + vm$.

Therefore $\zeta_{nm} = (\zeta_{nm}^n)^u(\zeta_{nm}^m)^v = \zeta_m^u\zeta_n^v \in \mathbb{Q}(\zeta_n, \zeta_m)$, hence

$$\mathbb{Q}(\zeta_{nm}) \subset \mathbb{Q}(\zeta_n, \zeta_m)$$

We have proved

$$\mathbb{Q}(\zeta_{nm}) = \mathbb{Q}(\zeta_n, \zeta_m)$$

(b) By Corollary 9.1.10, $[\mathbb{Q}(\zeta_{nm}) : \mathbb{Q}] = \phi(nm)$. As $n \wedge m = 1, \phi(nm) = \phi(n)\phi(m)$ (Lemma 9.1.1), so $[\mathbb{Q}(\zeta_{nm}) : \mathbb{Q}] = \phi(n)\phi(m)$, and by part (a), this is equivalent to

$$[\mathbb{Q}(\zeta_n, \zeta_m) : \mathbb{Q}] = \phi(n)\phi(m).$$

Using the Tower Theorem,

$$\phi(n)\phi(m) = [\mathbb{Q}(\zeta_n, \zeta_m) : \mathbb{Q}] = [\mathbb{Q}(\zeta_n, \zeta_m) : \mathbb{Q}(\zeta_m)] \, [\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \phi(m)[\mathbb{Q}(\zeta_n, \zeta_m) : \mathbb{Q}(\zeta_m)],$$

thus

$$\phi(n) = [\mathbb{Q}(\zeta_m)(\zeta_n) : \mathbb{Q}(\zeta_m)].$$

Let f be the minimal polynomial of ζ_n over $\mathbb{Q}(\zeta_m)$. Then

$$\deg(f) = [\mathbb{Q}(\zeta_m)(\zeta_n) : \mathbb{Q}(\zeta_m)] = \phi(n).$$

ζ_n is a root of $\Phi_n(x) \in \mathbb{Q}[x] \subset \mathbb{Q}(\zeta_m)[x]$, therefore $f \mid \Phi_n$ in $\mathbb{Q}(\zeta_m)[x]$. Moreover these two polynomials are monic of same degree $\phi(n)$, so they are identical. $\Phi_n = f$ is so irreducible over $\mathbb{Q}(\zeta_m)$.

$\square$

9.2 GAUSS AND ROOTS OF UNITY (OPTIONAL)

Ex. 9.2.1 *Let G be a cyclic group of order n and let g be a generator of G.*

(a) *Let f be a positive divisor of n and set $e = n/f$. Prove that $H_f = \langle g^e \rangle$ has order f and hence is the unique subgroup of order f.*

(b) *Let f and f' be positive divisors of $p - 1$. Prove that $H_f \subset H_{f'}$ if and only if $f \mid f'$.*

Proof. (a) • Let G be a cyclic group of order n and let g be a generator of G. If f is a positive divisor of n, write $e = n/f$, and $H = \langle g^e \rangle$.

The order of g is $n = ef$, hence the order of g^e is $\frac{n}{n \wedge e} = \frac{n}{e} = f$, therefore the set $A = \{(g^e)^0, \cdots, (g^e)^{f-1}\} \subset \langle g^e \rangle$ has f distinct elements: $|A| = f$.

Conversely, if $h \in \langle g^e \rangle$, then $h = (g^e)^k, k \in \mathbb{Z}$. The Euclidean division of k by f gives $k = qf + r, 0 \leq r < f$, thus $h = (g^{ef})^q g^{er} = (g^e)^r, 0 \leq r < f$, therefore $h \in A$.

Hence $H_f = \langle g^e \rangle = A$ has order f.

$$|H_f| = |\langle g^e \rangle| = f.$$

• Let K be any subgroup of order f. We must prove that $K = H$.

The set E of integers $m > 0$ such that $g^m \in K$ is non empty, since $g^n = e \in K$. Set

$$k = \min(E) = \min\{m \in \mathbb{N}^* \mid g^m \in K\},$$

so k is the least positive integer such that $g^k \in K$. We show that $K = \langle g^k \rangle$.

As $g^k \in K, \langle g^k \rangle \subset K$.

Conversely, if $h \in K$, then h is an element of G of the form $h = g^l$, $l \in \mathbb{Z}$. The Euclidean division of l by k gives $l = qk + r$, $0 \leq r < k$.

Then $g^r = g^l(g^k)^{-q} = h(g^k)^{-q} \in K$ and $0 \le r < k$. If r was not zero, it would lie in E and would be less than the minimum of E. This is a contradiction, so $r = 0$, and $h = g^l = (g^k)^q \in \langle g^k \rangle$. Therefore $K \subset \langle g^k \rangle$. Finally,

$$K = \langle g^k \rangle.$$

We show first that $k \mid n$. Write $d = k \wedge n$. There exist integers u, v such that $d = uk + vn$, therefore $g^d = (g^k)^u(g^n)^v = (g^k)^u \in K$, so $d \in E$, and $1 \le d \le k$, therefore $d = k$ by definition of $k = \min(E)$. So $k = k \wedge n$, hence $k \mid n$.

$K = \langle g^k \rangle$ is cyclic, and its cardinality is the order of g^k, $k \mid n$, so

$$|K| = \langle g^k \rangle = o(g^k) = \frac{n}{k},$$

by the first part of the proof.

By hypothesis the order of K is f, so $f = |K| = n/k$, and $k = n/f = e$.

$$K = \langle g^e \rangle = H.$$

Conclusion:

A cyclic group with generator g, of order $n = ef$, contains a unique subgroup of order f, written H_f, which is cyclic, generated by g^e.

(b) Let f, f' be positive divisors of $p - 1 = |(\mathbb{Z}/p\mathbb{Z})^*|$, and let g a generator of $(\mathbb{Z}/p\mathbb{Z})^*$. As in the text, write H_f the unique subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$ of order f.

If $H_f \subset H'_f$, then H_f is a subgroup of H'_f. By Lagrange's Theorem $|H_f|$ divides $|H_{f'}|$, so $f \mid f'$.

Conversely, if $f \mid f'$, $f' = qf$, $q \in \mathbb{N}$. Moreover $H_f = \langle g^e \rangle$, $H_{f'} = \langle g^{e'} \rangle$, where $n = ef = e'f'$ by part (a). Therefore $e = e'q$, and $g^e = (g^{e'})^q \in H_{f'}$, hence $H_f = \langle g^e \rangle \subset H_{f'}$.

$$f \mid f' \iff H_f \subset H_{f'}.$$

$\square$

Ex. 9.2.2 *Prove Proposition 9.2.1.*

Proof. Write $\tilde{H}_f$ the subgroup corresponding to H_f by the isomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^*$. Then

$$\sigma \in \tilde{H}_f \iff \exists [i] \in H_f, \ \sigma(\zeta_p) = \zeta_p^i,$$

and

$$L_f = \{\alpha \in \mathbb{Q}(\zeta_p) \mid \forall \sigma \in \tilde{H}_f, \ \sigma(\alpha) = \alpha\}$$

is the fixed field of $\tilde{H}_f$, with $\mathbb{Q} \subset L_f \subset \mathbb{Q}(\zeta_p)$.

(a) As $G = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is Abelian (G is cyclic since $(\mathbb{Z}/p\mathbb{Z})^* \simeq G$ is cyclic for prime p), so every subgroup of G is normal, therefore $\mathbb{Q} \subset L_f$ is a Galois extension (Theorem 7.3.2).

Moreover, by the Galois correspondence (Theorem 7.3.1), $[L_f : \mathbb{Q}] = (G : \tilde{H}_f)$, and $(G : \tilde{H}_f) = ((\mathbb{Z}/p\mathbb{Z})^* : H_f) = (p-1)/f = e$, so

$$[L_f : \mathbb{Q}] = e.$$

L_f is a Galois extension of $\mathbb{Q}$ of degree e.

(b) By Exercise 1, $f \mid f' \iff H_f \subset H_{f'}$. As the Galois correspondence is order reversing,

$$f \mid f' \iff H_f \subset H_{f'} \iff \tilde{H}_f \subset \tilde{H}_{f'} \iff L_f \supset L_{f'}.$$

(c) Let f, f' be positive divisors of $p-1$ such that $f \mid f'$. Since G is Abelian, $L_{f'} \subset L_f$ is a Galois extension, and by Theorem 7.3.2,

$$\mathrm{Gal}(L_f/L_{f'}) \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_p)/L_{f'})/\mathrm{Gal}(\mathbb{Q}(\zeta_p)/L_f) = \tilde{H}_{f'}/\tilde{H}_f \simeq H_{f'}/H_f.$$

As $H_{f'}$ is cyclic of order f', the quotient group $H_{f'}/H_f$ is itself cyclic, of order f'/f.

Conclusion:

$$\mathrm{Gal}(L_f/L_{f'}) \text{ is cyclic of order } f'/f.$$

$\square$

Ex. 9.2.3 *Let η_1, η_2, η_3 be as in Example 9.2.2.*

(a) *We know that ζ_7 is a root of $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 0$. Dividing by x^3 gives*
$$x^3 + x^2 + x + 1 + x^{-1} + x^{-2} + x^{-3} = 0.$$
Use this to show that η_1, η_2, η_3 are roots of $y^3 + y^2 - 2y - 1$.

(b) *Prove that $[\mathbb{Q}(\eta_1) : \mathbb{Q}] = 3$, and conclude that $\mathbb{Q}(\eta_1)$ is the fixed field of the subgroup $\{e, \tau\} \subset \mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q})$, where τ is the complex conjugation.*

(c) *Prove (9.10).*

Proof.   (a) Let ζ be any 7th primitive root of unity (i.e. $\zeta = \zeta_7^i$, $i = 1, \cdots, 6$).

Then $1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6 = 0$, and division by ζ^3 gives

$$\zeta^{-3} + \zeta^3 + \zeta^{-2} + \zeta^2 + \zeta + \zeta^{-1} + 1 = 0. \tag{1}$$

Write $\eta = \zeta + \zeta^{-1}$. Then

$$\eta^2 = \zeta^2 + \zeta^{-2} + 2,$$
$$\eta^3 = \zeta^3 + \zeta^{-3} + 3(\zeta + \zeta^{-1}).$$

Therefore

$$\zeta^2 + \zeta^{-2} = \eta^2 - 2,$$
$$\zeta^3 + \zeta^{-3} = \eta^3 - 3\eta.$$

15

By (3), $(\eta^3 - 3\eta) + (\eta^2 - 2) + \eta + 1 = 0$, so

$$\eta^3 + \eta^2 - 2\eta - 1 = 0. \tag{2}$$

Applying the equality (2) to $\zeta_7, \zeta_7^2, \zeta_7^3$, we obtain that $\eta_1 = \zeta_7 + \zeta_7^{-1}, \eta_2 = \zeta_7^2 + \zeta_7^{-2}, \eta_3 = \zeta_7^3 + \zeta_7^{-3}$ are roots of

$$f = x^3 + x^2 - 2x - 1.$$

As the minimal polynomial of ζ_7 over $\mathbb{Q}$ is Φ_7 of degree 6, the list $(1, \zeta_7, \zeta_7^2, \zeta_7^3, \zeta_7^4, \zeta_7^5)$ is linearly independent over $\mathbb{Q}$, thus also the list obtained by multiplication by ζ_7, so $(\zeta_7, \zeta_7^2, \zeta_7^3, \zeta_7^4, \zeta_7^5, \zeta_7^6)$ is a linearly independent list, therefore $\eta_1 = \zeta_7 + \zeta_7^6, \eta_2 = \zeta_7^2 + \zeta_7^5, \eta_3 = \zeta_7^3 + \zeta_7^4$ are linearly independent, so are a fortiori distinct. Therefore

$$f = x^3 + x^2 - 2x - 1 = (x - \eta_1)(x - \eta_2)(x - \eta_3).$$

η_1, η_2, η_3 are the three distinct roots of f.

(b) f has no root in $\mathbb{Q}$. Indeed, if $\alpha = p/q, p \wedge q = 1$ was such a root, we would have the equality

$$p^3 + p^2 q - 2pq^2 - q^3 = 0,$$

which implies, since $p \wedge q = 1$, that $p \mid 1, q \mid 1$, so $\alpha = \pm 1$, but neither 1, nor -1 is a root of f.

Since f has no root in $\mathbb{Q}$ and $\deg(f) = 3$, f is irreducible over $\mathbb{Q}$. So f is the minimal polynomial of η_1 over $\mathbb{Q}$, and also of η_2, η_3, which are so conjugate of η_1 over $\mathbb{Q}$. Moreover

$$[\mathbb{Q}(\eta_1) : \mathbb{Q}] = \deg(f) = 3.$$

Let τ be the complex conjugation restricted to $\mathbb{Q}(\zeta_7)$. As $\tau(\zeta_7) = \bar{\zeta}_7 = \zeta_7^{-1} \in \mathbb{Q}(\zeta_7)$, τ is an automorphism of $\mathbb{Q}(\zeta_7)$ which fixes the elements of $\mathbb{Q}$, so $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q})$, and $\tau^2 = e$, therefore $\{e, \tau\} = \tilde{H}_2$ is the unique subgroup of $G = \mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q})$ of order 2.

Let $L_2 = L_{\langle \tau \rangle}$ be the fixed field of $\tilde{H}_2$. By the Galois Correspondence (see Proposition 9.2.1 and Exercise 2),

$$[L_2 : \mathbb{Q}] = (G : H_2) = 3.$$

As $\eta_1 \in \mathbb{R}, \tau(\eta_1) = \eta_1$, hence $\eta_1 \in L_2$, and so $\mathbb{Q}(\eta_1) \subset L_2$.

Since $[L_2 : \mathbb{Q}] = [\mathbb{Q}(\eta_1) : \mathbb{Q}] = 3$, then $[L_2 : \mathbb{Q}(\eta_1)] = 1$, hence $L_2 = \mathbb{Q}(\eta_1)$.

The fixed field L_2 of $\tilde{H}_2 = \{e, \tau\}$ is $\mathbb{Q}(\eta_1)$.

(c) $\eta_1 = 2\cos(2\pi/7), \eta_2 = 2\cos(4\pi/7), \eta_3 = 4\cos(6\pi/7)$ are the roots of $f = x^3 + x^2 - 2x - 1$. We compute these roots with the Cardan's Formula.

The substitution $x = y - 1/3$ in f gives

$$\begin{aligned}
g(y) &= f\left(y - \frac{1}{3}\right) \\
&= \left(y - \frac{1}{3}\right)^3 + \left(y - \frac{1}{3}\right)^2 - 2\left(y - \frac{1}{3}\right) - 1 \\
&= y^3 - y^2 + \frac{1}{3}y - \frac{1}{27} + y^2 - \frac{2}{3}y + \frac{1}{9} - 2y + \frac{2}{3} - 1 \\
&= y^3 - \frac{7}{3}y - \frac{7}{27}
\end{aligned}$$

(Note: if Δ is the discriminant of f or g, then $\Delta = -4p^3 - 27q^2 = -4\left(-\frac{7}{3}\right)^3 - 27\left(\frac{7}{27}\right)^2 = \frac{1372}{27} - \frac{49}{27} = \frac{1323}{27} = 49 = 7^2$ is the square of an element of $\mathbb{Q}$, hence the Galois group of f is $A_3 \simeq \mathbb{Z}/3\mathbb{Z}$. This shows again that

$$|\mathrm{Gal}(\mathbb{Q}(\eta_1)/\mathbb{Q})| = [L_2 : \mathbb{Q}] = 3.)$$

Let α a root of g (that is to say $\alpha - 1/3$ is a root of f). There exist two complex numbers u, v such that $\alpha = u + v, uv = 7/9$. Then

$$0 = (u + v)^3 - \frac{7}{3}(u + v) - \frac{7}{27}$$

$$= u^3 + v^3 + \left(3uv - \frac{7}{3}\right)(u + v) - \frac{7}{27}$$

$$= u^3 + v^3 - \frac{7}{27}$$

So (u, v), which satisfies the condition $uv = 7/9$, is a solution of the system

$$u^3 + v^3 = \frac{7}{3^3}$$

$$u^3 v^3 = \frac{7^3}{3^6}$$

u^3, v^3 are so the roots of the equation $x^2 - \frac{7}{3^3}x + \frac{7^3}{3^6}$, of discriminant

$$\delta = \frac{7^2}{3^6} - 4\frac{7^3}{3^6} = \frac{7^2(-27)}{3^6} = -\frac{7^2}{3^3} = -\frac{49}{27}.$$

$$u^3 = \frac{1}{2}\left(\frac{7}{27} + i\sqrt{\frac{49}{27}}\right) = \frac{1}{27} \times \frac{7}{2}\left(1 + 3i\sqrt{3}\right)$$

$$v^3 = \frac{1}{2}\left(\frac{7}{27} - i\sqrt{\frac{49}{27}}\right) = \frac{1}{27} \times \frac{7}{2}\left(1 - 3i\sqrt{3}\right)$$

As $u^3 = \overline{v}^3$, and $uv = 7/9 \in \mathbb{R}$, then $v = \omega^k \overline{u}$, $k = 0, 1, 2$, and so $uv = u\overline{u}\omega^k \in \mathbb{R}$, therefore $\omega^k \in \mathbb{R}$, so $k = 0$, which gives $v = \overline{u}$. The set $\{\eta_1, \eta_2, \eta_3\}$ of the three roots of f is so the set $\{-1/3 + u + \overline{u}, -1/3 + \omega u + \omega^2\overline{u}, -1/3 + \omega^2 u + \omega\overline{u}\}$.

To identify each root, we must define the determination of $3u = \sqrt[3]{\frac{7}{2}\left(1 + 3i\sqrt{3}\right)}$. Choose for this cubic root the one which lies in the first quadrant (there exists one and only one such a cubic root since $\mathrm{Arg}(1 + 3i\sqrt{3}) \in [0, \pi/2]$), and write $3\overline{u} = \sqrt[3]{\frac{7}{2}\left(1 - 3i\sqrt{3}\right)}$ its conjugate.

Then

$$-\frac{1}{3} + u + \overline{u} = \frac{1}{3}(-1 + 3u + 3\overline{u})$$

$$= \frac{1}{3}\left(-1 + \sqrt[3]{\frac{7}{2}\left(1 + 3i\sqrt{3}\right)} + \sqrt[3]{\frac{7}{2}\left(1 - 3i\sqrt{3}\right)}\right)$$

As $\left| \frac{7}{2} \left(1 + 3i\sqrt{3} \right) \right| = \frac{7}{2}\sqrt{28} = (\sqrt{7})^3$, then $|3u| = \sqrt{7}$, and $\mathrm{Arg}(3u) \in [0, \pi/6]$, therefore $\mathrm{Re}\,(3u) \geq \sqrt{7}\cos(\pi/6) = \sqrt{7}\sqrt{3}/2$, so $2\,\mathrm{Re}\,(3u) \geq \sqrt{21}$.

Therefore $\mathrm{Re}\,(-1 + 3u + 3\overline{u}) \geq \sqrt{21} - 1 > 0$.

As $\eta_1 = 2\cos(2\pi/7)$ is the only positive root of f,

$$\eta_1 = \zeta_7 + \zeta_7^{-1} = 2\cos(2\pi/7) = \frac{1}{3}\left(-1 + \sqrt[3]{\frac{7}{2}\left(1 + 3i\sqrt{3}\right)} + \sqrt[3]{\frac{7}{2}\left(1 - 3i\sqrt{3}\right)} \right)$$

where $\sqrt[3]{\frac{7}{2}\left(1 + 3i\sqrt{3}\right)}$ is chosen such that

$$\mathrm{Re}\left(\sqrt[3]{\frac{7}{2}\left(1 + 3i\sqrt{3}\right)} \right) > 0, \ \mathrm{Im}\left(\sqrt[3]{\frac{7}{2}\left(1 + 3i\sqrt{3}\right)} \right) > 0$$

and $\sqrt[3]{\frac{7}{2}\left(1 - 3i\sqrt{3}\right)}$ is its conjugate.

As ζ_7 is a root of $x^2 - \eta_1 x + 1$, with positive imaginary part, then $\zeta_7 = \frac{1}{2}\left(\eta_1 + i\sqrt{4 - \eta_1^2} \right)$, so

$$
\begin{aligned}
\zeta_7 &= -\frac{1}{6} + \frac{1}{6}\sqrt[3]{\frac{7}{2}(1 + 3i\sqrt{3})} + \frac{1}{6}\sqrt[3]{\frac{7}{2}(1 - 3i\sqrt{3})} \\
&\quad + \frac{i}{2}\sqrt{4 - \left(\frac{1}{3} - \frac{1}{3}\sqrt[3]{\frac{7}{2}(1 + 3i\sqrt{3})} - \frac{1}{3}\sqrt[3]{\frac{7}{2}(1 - 3i\sqrt{3})} \right)^2} \\
&= -\frac{1}{6} + \frac{1}{6}\sqrt[3]{\frac{7}{2}(1 + 3i\sqrt{3})} + \frac{1}{6}\sqrt[3]{\frac{7}{2}(1 - 3i\sqrt{3})} \\
&\quad + i\sqrt{1 - \left(\frac{1}{6} - \frac{1}{6}\sqrt[3]{\frac{7}{2}(1 + 3i\sqrt{3})} - \frac{1}{6}\sqrt[3]{\frac{7}{2}(1 - 3i\sqrt{3})} \right)^2}
\end{aligned}
$$

with the same cube roots.

(It seems that there is a misprint in (9.11)).

$\square$

Ex. 9.2.4 *Let $A \subset B$ be subgroups of a group G, and assume that A has index d in B. Prove that every left coset of B in G is a disjoint union of d left cosets of A in G.*

Proof. Let $\{b_1 \cdots, b_d\}$ a complete system of representatives of left cosets of A in B, where $d = (B : A)$. Then

$$B = \biguplus_{1 \leq i \leq d} b_i A.$$

If cB, $c \in G$ is any left coset of B in G, then

$$cB = \biguplus_{1 \leq i \leq d} cb_i A.$$

Indeed,

- $b_i A \subset B$, thus $cb_i A \subset cB$, $i = 1, \ldots, d$, therefore $\bigcup_{1 \leq i \leq d} cb_i A \subset cB$.

- If $g \in cB$, then $g = ch$, $h \in B$, and $h \in b_i A$ for some i, $1 \leq i \leq d$, so $h = b_i a, a \in A$, hence $g = cb_i A \in \bigcup_{1 \leq i \leq d} cb_i A$. Therefore $cB \subset \bigcup_{1 \leq i \leq d} cb_i A$.

$$cB = \bigcup_{1 \leq i \leq d} cb_i A.$$

- The union is a disjoint union: if $g \in cb_i A$ and $g \in cb_j A$, then $c^{-1} g \in b_i A \cap b_j A$, which is possible only if $i = j$. Thus $i \neq j \Rightarrow cb_i A \cap cb_j A = \emptyset$.

Conclusion: every left coset of B in G is the disjoint union of $d = (B : A)$ left cosets of A in G. $\qquad \square$

Ex. 9.2.5 *Complete the proof of Proposition 9.2.8.*

Proof. By Exercise 4 , we obtain (9.12):

$$[\lambda] H_{f'} = [\lambda_1] H_f \cup \cdots \cup [\lambda_d] H_f, \qquad \lambda = \lambda_1.$$

We must prove that every period (f, λ_j), $j = 1, \ldots, d$, is of the form $(f, \lambda_j) = \sigma(\eta) = \sigma((f, \lambda))$, where $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/L_{f'})$.
   Write $[i] = [\lambda]^{-1}[\lambda_j]$. As $[\lambda_j] \in [\lambda] H_{f'}$, then $[i] = [\lambda]^{-1}[\lambda_j] \in H_{f'}$.
   Since $[\lambda_j] = [i\lambda]$,
$$(f, \lambda_j) = (f, i\lambda), \qquad i \in H_{f'}.$$
Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/L_{f'})$ be defined by $\sigma(\zeta_p) = \zeta_p^i$, where $[i] \in H_{f'}$, so by Lemma 9.2.4(c),

$$(f, \lambda_j) = (f, i\lambda) = \sigma(\eta), \ \sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/L_{f'}).$$

Every (f, λ_j), $j = 1, \ldots, d$, is a conjugate of (f, λ) over $L_{f'}$. $\qquad \square$

Ex. 9.2.6 *Prove that the sum of the distinct f-periods equals -1.*

Proof. With a fixed divisor f of n, and $e = n/f$,

$$(\mathbb{Z}/p\mathbb{Z})^* = \biguplus_{1 \leq i \leq e} \lambda_i H_f,$$

where $\lambda_1, \cdots, \lambda_e$ are distinct representatives of the cosets of H_f in $(\mathbb{Z}/p\mathbb{Z})^*$.
   The e distinct f-periods are the (f, λ_i), $i = 1, \cdots, e$, thus

$$\sum_{i=1}^{e} (f, \lambda_i) = \sum_{i=1}^{e} \sum_{a \in [\lambda_i] H_f} \zeta_p^a = \sum_{a \in \bigcup_{1 \leq i \leq e} [\lambda_i] H_f} \zeta_p^a = \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^*} \zeta_p^a = -1,$$

since $\sum_{a \in (\mathbb{Z}/p\mathbb{Z})} \zeta_p^a = 0$. $\qquad \square$

Ex. 9.2.7 *This exercise is concerned with the details of Examples 9.2.10, 9.2.11, 9.2.12, and 9.2.13.*

(a) *Show that 2 is a primitive root modulo 19.*

(b) *Use the methods of Example 9.2.10 to obtain formulas for $(6,2)^2$ and $(6,4)^2$.*

(c) *Show that the formulas of part (b) follow from $(6,1)^2 = 4 - (6,2)$ and part (d) of Lemma 9.2.4.*

(d) *Prove (9.15) and use this and Exercise 6 to show that $(6,1)(6,2)(6,4) = 7$.*

(e) *Find the minimal polynomial of $(3,2)$ and $(3,4)$ over the field L_6 considered in Example 9.2.12.*

(f) *Show that (9.18) is the minimal polynomial of ζ_{19} over the field L_3 considered in Example 9.2.13.*

Proof. (a) $2^2 = 4 \not\equiv 1 \pmod{19}$, and $2^9 = 512 = 19 \times 26 + 18 \equiv -1 \pmod{19}$. Therefore the order of $[2]$ in $(\mathbb{Z}/19\mathbb{Z})^*$ is 18, so 2 is a primitive root modulo 19.

(b) In Example 9.2.10, we obtained

$$H_6 = \{1, 7, 8, 11, 12, 18\},$$
$$2H_6 = \{2, 3, 5, 14, 16, 17\},$$
$$4H_6 = \{4, 6, 9, 10, 13, 15\}.$$

By Proposition 9.2.9,

$$(6,1)^2 = \sum_{\lambda' \in H_6} (6, \lambda' + 1), \ (6,2)^2 = \sum_{\lambda' \in 2H_6} (6, \lambda' + 2), \ (6,4)^2 = \sum_{\lambda' \in 4H_6} (6, \lambda' + 4).$$

$$\begin{aligned}
(6,1)^2 &= (6,2) + (6,8) + (6,9) + (6,12) + (6,13) + 6 \\
&= 2(6,1) + (6,2) + 2(6,4) + 6 \\
&= (6,1) + (6,4) + 5 \\
&= 4 - (6,2),
\end{aligned}$$

$$\begin{aligned}
(6,2)^2 &= (6,4) + (6,5) + (6,7) + (6,16) + (6,18) + 6 \\
&= 2(6,1) + 2(6,2) + (6,4) + 6 \\
&= (6,1) + (6,2) + 5 \\
&= 4 - (6,4),
\end{aligned}$$

$$\begin{aligned}
(6,4)^2 &= (6,8) + (6,10) + (6,13) + (6,14) + (6,17) + 6 \\
&= (6,1) + 2(6,2) + 2(6,4) + 6 \\
&= (6,2) + (6,4) + 5 \\
&= 4 - (6,1).
\end{aligned}$$

$$(6,1)^2 = 4 - (6,2), \quad (6,2)^2 = 4 - (6,4), \quad (6,4)^2 = 4 - (6,1).$$

If we write $\eta_1 = (6,1), \eta_2 = (6,2), \eta_3 = (6,4)$, then

$$\eta_1^2 = 4 - \eta_2, \quad \eta_2^2 = 4 - \eta_3, \quad \eta_3^2 = 4 - \eta_1.$$

(c) The similarity of these results has an explanation. If $\sigma \in G = \mathrm{Gal}(\mathbb{Q}(\zeta_{19})/\mathbb{Q})$ is determined by $\sigma(\zeta_{19}) = \zeta_{19}^2$, then by Lemma 9.2.4(d), $\sigma((6,1)) = (6,2), \sigma((6,2)) = (6,4)$ and $\sigma((6,4)) = (6,8) = (6,1)$, so

$$\sigma(\eta_1) = \eta_2, \quad \sigma(\eta_2) = \eta_3, \quad \sigma(\eta_3) = \eta_1.$$

Therefore $\eta_1^2 = 4 - \eta_2$ implies $\eta_2^2 = 4 - \eta_3$ and $\eta_3^2 = 4 - \eta_1$.

By Proposition 9.2.6 and Corollary 9.2.7, $L_6 = \mathbb{Q}(\eta_1) = \mathbb{Q}(\eta_1, \eta_2, \eta_3) = \mathrm{Vect}_{\mathbb{Q}}(\eta_1, \eta_2, \eta_3)$, and so σ sends L_6 on itself. The restriction $\tilde{\sigma}$ of σ to $\mathbb{Q}(\eta_1)$ is so a $\mathbb{Q}$-automorphism of $\mathbb{Q}(\eta_1)$ of order 3, since $\tilde{\sigma}^3(\eta_1) = \eta_1$. Moreover, the extension $\mathbb{Q} \subset \mathbb{Q}(\eta_1)$ is Galois (since $G = \mathrm{Gal}(\mathbb{Q}(\zeta_{19}/\mathbb{Q})$ is Abelian, every subgroup of G is normal), so

$$\mathrm{Gal}(\mathbb{Q}(\eta_1)/\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_{19})/\mathbb{Q})/\mathrm{Gal}(\mathbb{Q}(\zeta_{19})/\mathbb{Q}(\eta_1)),$$

thus
$$|\mathrm{Gal}(\mathbb{Q}(\eta_1)/\mathbb{Q})| = [\mathbb{Q}(\eta_1) : \mathbb{Q}] = (G : \tilde{H}_6) = ((\mathbb{Z}/19\mathbb{Z})^* : H_6) = 3,$$

therefore
$$\mathrm{Gal}(\mathbb{Q}(\eta_1)/\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}, \quad \mathrm{Gal}(\mathbb{Q}(\eta_1)/\mathbb{Q}) = \langle \tilde{\sigma} \rangle.$$

(d)

$$\begin{aligned}
(6,1)(6,2) &= \sum_{\lambda' \in H_6} (6, \lambda' + 2) \\
&= (6,3) + (6,9) + (6,10) + (6,13) + (6,14) + (6,1) \\
&= (6,2) + (6,4) + (6,4) + (6,4) + (6,2) + (6,1) \\
&= (6,1) + 2(6,2) + 3(6,4).
\end{aligned}$$

If we apply σ, σ^2 to this equality, we obtain (9.15) :

$$\begin{aligned}
(6,1)(6,2) &= (6,1) + 2(6,2) + 3(6,4), \\
(6,2)(6,4) &= 3(6,1) + (6,2) + 2(6,4), \\
(6,4)(6,1) &= 2(6,1) + 3(6,2) + (6,4).
\end{aligned}$$

It follows

$$\begin{aligned}
(6,1)(6,2)(6,4) &= (6,1)(3(6,1) + (6,2) + 2(6,4)) \\
&= 3(6,1)^2 + (6,1)(6,2) + 2(6,1)(6,4) \\
&= [12 - 3(6,2)] + [(6,1) + 2(6,2) + 3(6,4)] + 2[2(6,1) + 3(6,2) + (6,4)] \\
&= 12 + 5(6,1) + 5(6,2) + 5(6,4) \\
&= 7
\end{aligned}$$

We have so obtained

$$\eta_1 + \eta_2 + \eta_3 = -1, \ \eta_1\eta_2 + \eta_2\eta_3 + \eta_3\eta_1 = -6, \ \eta_1\eta_2\eta_3 = 7.$$

Hence the minimal polynomial of η_1 over $\mathbb{Q}$ (and also of η_2, η_3) is

$$f = (x - \eta_1)(x - \eta_2)(x - \eta_3) = x^3 + x^2 - 6x - 7.$$

The splitting field of f is $L_6 = \mathbb{Q}(\eta_1)$ generated by the 6-periods.

(e) Since

$$H_6 = \{1, 7, 11\} \cup \{8, 12, 18\} = H_3 \cup 8H_3,$$
$$2H_6 = \{2, 3, 14\} \cup \{5, 16, 17\} = 2H_3 \cup 16H_3,$$
$$4H_6 = \{4, 6, 9\} \cup \{10, 13, 15\} = 4H_3 \cup 13H_3,$$

we obtain

$$(6, 1) = (3, 1) + (3, 8),$$
$$(6, 2) = (3, 2) + (3, 16),$$
$$(6, 4) = (3, 4) + (3, 13).$$

In Example 9.2.12, we have proved that the minimal polynomial of $(3, 1)$ and $(3, 8)$ over L_6 is

$$(x - (3, 1))(x - (3, 8)) = x^2 - (6, 1)x + (6, 4) + 3 = x^2 - \eta_1 x + \eta_2 + 3.$$

If $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is determined by $\sigma(\zeta_{19}) = \zeta_{19}^2$ then $\sigma((3,1)) = (3,2), \sigma((3,8)) = (3,16), \sigma((6,1)) = (6,2), \sigma(6,4) = (6,8) = (6,1)$, so the minimal polynomial of $(3, 2)$ is

$$(x - (3, 2))(x - (3, 16)) = x^2 - (6, 2)x + (6, 1) + 3.$$

Similarly, applying σ^2, we obtain

$$(x - (3, 4))(x - (3, 13)) = x^2 - (6, 4)x + (6, 2) + 3.$$

(f) The extension $L_1/L_3 = \mathbb{Q}(\zeta_{19})/\mathbb{Q}((3,1))$ is an extension of degree $d = 3$.

Here $[1]H_3 = \{[1], [7], [11]\} = [1]H_1 \cup [7]H_1 \cup [11]H_1$ (with $H_1 = \{1\}$). Proposition 9.2.8 shows that the minimal polynomial of ζ_{19} over L_3 is

$$(x - (1, 1))(x - (1, 7))(x - (1, 11)) = (x - \zeta_{19})(x - \zeta_{19}^7)(x - \zeta_{19}^{11}).$$

Without Proposition 9.2.8, note that $\mathrm{Gal}(L_1/L_3) = \tilde{H}_3 = \langle \sigma^6 \rangle = \{e, \sigma^6, \sigma^{12}\}$, where σ^6 takes ζ_{19} to $\zeta_{19}^{2^6} = \zeta_{19}^7$, so the minimal polynomial of ζ_{19} over L_3 is

$$(x - \zeta_{19})(x - \sigma^6(\zeta_{19}))(x - \sigma^{12}(\zeta_{19})) = (x - \zeta_{19})(x - \zeta_{19}^7)(x - \zeta_{19}^{11}).$$

As

$$\zeta_{19} + \zeta_{19}^7 + \zeta_{19}^{11} = (3, 1),$$
$$\zeta_{19}\zeta_{19}^7\zeta_{19}^{11} = \zeta_{19}^{19} = 1,$$
$$\zeta_{19}\zeta_{19}^7 + \zeta_{19}^7\zeta_{19}^{11} + \zeta_{19}\zeta_{19}^{11} = \zeta_{19}^8 + \zeta_{19}^{18} + \zeta_{19}^{12} = (3, 8),$$

we obtain that the minimal polynomial of ζ_{19} over L_3 is

$$(x - \zeta_{19})(x - \zeta_{19}^7)(x - \zeta_{19}^{11}) = x^3 - (3, 1)x^2 + (3, 8)x - 1.$$

$\square$

Ex. 9.2.8 *In this exercise and the next, you will derive Gauss's radical formula (9.19) for* $\cos(2\pi/17)$.

(a) *Show that* 3 *is a primitive root modulo* 17.

(b) *Show that*

$$H_8 = \{1, 2, 4, 8, 9, 13, 15, 16\},$$
$$H_4 = \{1, 4, 13, 16\},$$
$$H_2 = \{1, 16\}.$$

(c) *Use Propositions 9.2.8 and 9.2.9 to compute the following minimal polynomials:*

Extension	Primitive Elements	Minimal Polynomial
$\mathbb{Q} \subset L_8$	$(8,1), (8,3)$	$x^2 + x - 4$
$L_8 \subset L_4$	$(4,1), (4,2)$	$x^2 - (8,1)x - 1$
	$(4,3), (4,6)$	$x^2 - (8,3)x - 1$
$L_4 \subset L_2$	$(2,1), (2,4)$	$x^2 - (4,1)x + (4,3)$

The resulting quadratic equations are easy to solve using quadratic formula. But how do the roots correspond to the periods? For example, the roots $(8,1), (8,3)$ *of* $x^2 + x - 4$ *are* $(-1 \pm \sqrt{17})/2$. *How do these match up? The answer will be given in the next exercise.*

Proof. (a) By Exercise 1, $3^8 \equiv 9^4 = 81^2 \equiv (-4)^2 \equiv -1 \not\equiv 1 \pmod{17}$, therefore the order of $[3]$ in $(\mathbb{Z}/17\,\mathbb{Z})^*$ is 16, so 3 is a primitive root modulo 17.

(b)

$$H_8 = \langle 3^2 \rangle = \{1, 9, 9^2, 9^3, -1, -9, -9^2, -9^3\}$$
$$= \{1, 9, -4, -2, -1, -9, 4, 2\}$$
$$= \{1, 9, 13, 15, 16, 8, 4, 2\},$$

$H_4 = \langle 3^4 \rangle = \{1, 13, 16, 4\}$, and $H_2 = \langle 3^8 \rangle = \{1, 16\}$, so

$$H_8 = \{1, 2, 4, 8, 9, 13, 15, 16\},$$
$$H_4 = \{1, 4, 13, 16\},$$
$$H_2 = \{1, 16\}.$$

(c) • Extension $\mathbb{Q} \subset L_8$.
   The cosets of H_8 in $(\mathbb{Z}/17\,\mathbb{Z})^*$ are

$$H_8 = \{1, 2, 4, 8, 9, 13, 15, 16\},$$
$$3H_8 = \{3, 6, 12, 7, 10, 5, 11, 14\}.$$

L_8 is generated over $\mathbb{Q}$ by the 8-periods $(8,1), (8,3)$, where $(8,1)+(8,3) = -1$, and

$$(8,1)(8,3) = \sum_{\lambda \in H_8} (8, \lambda + 3)$$
$$= (8,4) + (8,5) + (8,7) + (8,11) + (8,12) + (8,16) + (8,1) + (8,2)$$
$$= 4(8,1) + 4(8,3)$$
$$= -4.$$

The minimal polynomial over $\mathbb{Q}$ of the 8-p¬ériods $(8,1),(8,3)$ isso $(x-(8,1))(x-(8,3)) = x^2 + x - 4$.

- Extension $L_8 \subset L_4$.

$$H_8 = \{1,4,13,16\} \cup \{2,8,9,15\} = H_4 \cup 2H_4,$$
$$3H_8 = \{3,5,12,14\} \cup \{6,7,10,11\} = 3H_4 \cup 6H_4.$$

The 4-periods are so $(4,1),(4,2)$, and $(4,3),(4,6)$, where

$$(4,1) + (4,2) = (8,1),$$
$$(4,1) \times (4,2) = \sum_{\lambda \in H_4} (4, \lambda + 2)$$
$$= (4,3) + (4,7) + (4,15) + (4,1)$$
$$= -1.$$

The minimal polynomial of $(4,1)$ and $(4,2)$ over L_8 is so

$$(x - (4,1))(x - (4,2)) = x^2 - (8,1)x - 1.$$

Applying $\sigma : \zeta_{17} \mapsto \zeta_{17}^3$, we obtain the minimal polynomial of $(4,3)$ and $(4,6)$

$$(x - (4,3))(x - (4,6)) = x^2 - (8,3)x - 1.$$

- Extension $L_4 \subset L_2$.

$$H_4 = \{1,16\} \cup \{4,13\} = H_2 \cup 4H_2,$$
$$3H_4 = \{3,14\} \cup \{5,12\} = 3H_2 \cup 5H_2,$$
$$\dots$$

The 2-periods $(2,1),(2,4)$ satisfy

$$(2,1) + (2,4) = (4,1),$$
$$(2,1) \times (2,4) = \sum_{\lambda \in H_2} (2, \lambda + 4)$$
$$= (2,5) + (2,3)$$
$$= (4,3).$$

The minimal polynomial of $(2,1)$ and $(2,4)$ over L_4 is so

$$(x - (2,1))(x - (2,4)) = x^2 - (4,1)x + (4,3).$$

$\square$

Ex. 9.2.9 *In this exercise, you will use numerical computations and the previous exercise to find radical expressions for various f-periods when $p = 17$.*

(a) Show that

$$(8,1) = 2\cos(2\pi/17) + 2\cos(4\pi/17) + 2\cos(8\pi/17) + 2\cos(16\pi/17)$$
$$(4,1) = 2\cos(2\pi/17) + 2\cos(8\pi/17)$$
$$(4,3) = 2\cos(6\pi/17) + 2\cos(10\pi/17)$$
$$(2,1) = 2\cos(2\pi/17)$$

Then compute each of these periods to five decimal places.

(b) *Use the numerical computations of part (a) and the quadratic polynomials of Exercise 8 to show that*

$$(8,1) = \frac{1}{2}\left(-1 + \sqrt{17}\right)$$

$$(8,3) = \frac{1}{2}\left(-1 - \sqrt{17}\right)$$

$$(4,1) = \frac{1}{4}\left(-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}}\right)$$

$$(4,2) = \frac{1}{4}\left(-1 + \sqrt{17} - \sqrt{34 - 2\sqrt{17}}\right)$$

$$(4,3) = \frac{1}{4}\left(-1 - \sqrt{17} + \sqrt{34 + 2\sqrt{17}}\right)$$

(c) *Use the quadratic polynomial $x^2 - (4,1)x + (4,3)$ and part (b) to derive (9.19).*

Proof. Recall (see Exercise 8) that

$$H_8 = \{1, 2, 4, 8, 9, 13, 15, 16\}$$
$$H_4 = \{1, 4, 13, 16\}$$
$$3H_4 = \{3, 5, 12, 14\}$$
$$H_2 = \{1, 16\}$$

Write $\zeta = \zeta_{17}$.

(a) Using these results, and $\zeta^{-k} = \zeta^{17-k}$, $k = 1, 2, 4, 8$, and also $\zeta^k + \zeta^{-k} = 2\cos(2k\pi/17)$,

we obtain

$$(8,1) = \sum_{[a]\in H_8} \zeta^a$$
$$= \zeta + \zeta^2 + \zeta^4 + \zeta^8 + \zeta^9 + \zeta^{13} + \zeta^{15} + \zeta^{16}$$
$$= (\zeta + \zeta^{-1}) + (\zeta^2 + \zeta^{-2}) + (\zeta^4 + \zeta^{-4}) + (\zeta^8 + \zeta^{-8})$$
$$= 2\cos(2\pi/17) + 2\cos(4\pi/17) + 2\cos(8\pi/17) + 2\cos(16\pi/17)$$

$$(4,1) = \sum_{[a]\in H_4} \zeta^a$$
$$= \zeta + \zeta^4 + \zeta^{13} + \zeta^{16}$$
$$= (\zeta + \zeta^{-1}) + (\zeta^4 + \zeta^{-4})$$
$$= 2\cos(2\pi/17) + 2\cos(8\pi/17)$$
$$(4,3) = \sum_{[a]\in 3H_4} \zeta^a$$
$$= \zeta^3 + \zeta^5 + \zeta^{12} + \zeta^{14}$$
$$= (\zeta^3 + \zeta^{-3}) + (\zeta^5 + \zeta^{-5})$$
$$= 2\cos(6\pi/17) + 2\cos(10\pi/17)$$

$$(2,1) = \sum_{[a]\in H_2} \zeta^a$$
$$= \zeta + \zeta^{16}$$
$$= \zeta + \zeta^{-1}$$
$$= 2\cos(2\pi/17)$$

$(2,1) = 2\cos(2\pi/17) \simeq 0.93247$,

$(4,1) \simeq 2.04948, (4,3) \simeq 0.34415$,

$(8,1) \simeq 1.56155$.

As $(4,1) + (4,2) = (8,1)$, we obtain $(4,2) \simeq -0.48792 < 0$.

(b) By Exercise 8, $(8,1), (8,3)$ are the roots of $x^2 + x - 4$, and by part (a) $(8,1) > 0$. The only positive root of $x^2 + x - 4$ is $(-1 + \sqrt{17})/2$, therefore

$$(8,1) = \frac{1}{2}\left(-1 + \sqrt{17}\right),$$
$$(8,3) = \frac{1}{2}\left(-1 - \sqrt{17}\right).$$

$(4,1), (4,2)$ are the roots of $x^2 - (8,1)x - 1$, with discriminant

$$\Delta = \frac{1}{4}(-1 + \sqrt{17})^2 + 4 = \frac{1}{4}(34 - 2\sqrt{17}),$$

therefore

$$\{(4,1), (4,2)\} = \left\{ \frac{1}{4}\left(-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}}\right), \frac{1}{4}\left(-1 + \sqrt{17} - \sqrt{34 - 2\sqrt{17}}\right) \right\}.$$

By part (a) $(4, 2) < 0 < (4, 1)$, so

$$(4, 1) = \frac{1}{4}\left(-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}}\right),$$

$$(4, 2) = \frac{1}{4}\left(-1 + \sqrt{17} - \sqrt{34 - 2\sqrt{17}}\right).$$

$(4, 3), (4, 6)$ are the roots of $x^2 - (8, 3)x - 1$, with discriminant

$$\Delta = \frac{1}{4}(-1 - \sqrt{17})^2 + 4 = \frac{1}{4}(34 + 2\sqrt{17}),$$

therefore

$$\{(4, 3), (4, 6)\} = \left\{\frac{1}{4}\left(-1 - \sqrt{17} + \sqrt{34 + 2\sqrt{17}}\right), \frac{1}{4}\left(-1 - \sqrt{17} - \sqrt{34 + 2\sqrt{17}}\right)\right\}.$$

As $(4, 3) > 0$,

$$(4, 3) = \frac{1}{4}\left(-1 - \sqrt{17} + \sqrt{34 + 2\sqrt{17}}\right),$$

$$(4, 6) = \frac{1}{4}\left(-1 - \sqrt{17} - \sqrt{34 + 2\sqrt{17}}\right).$$

(c) $(2, 1) = 2\cos(2\pi/17)$, and also $(2, 4)$, is root of $x^2 - (4, 1)x + (4, 3)$, with discriminant

$$\Delta = (4, 1)^2 - 4(4, 3).$$

As

$$(4, 1)^2 = \sum_{\lambda \in H_4} (4, \lambda + 1)$$
$$= (4, 2) + (4, 5) + (4, 14) + 4$$
$$= (4, 2) + 2(4, 3) + 4,$$

then

$$\Delta = (4, 2) - 2(4, 3) + 4$$
$$= \frac{1}{4}\left(-1 + \sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\left(-1 - \sqrt{17} + \sqrt{34 + 2\sqrt{17}}\right) + 16\right)$$
$$= \frac{1}{4}\left(17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}\right).$$

The roots of $x^2 - (4, 1)x + (4, 3)$ are so $\frac{1}{2}((4, 1) \pm \sqrt{\Delta})$

$$= \frac{1}{8}\left(-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}}\right) \pm \frac{1}{4}\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}.$$

As $(2, 4) = 2\cos(4\pi/17) < 2\cos(2\pi/17) = (2, 1)$, we can conclude that

$$\cos\left(\frac{2\pi}{17}\right) = -\frac{1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34 - 2\sqrt{17}}$$
$$+ \frac{1}{8}\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}.$$

$\square$

Ex. 9.2.10 *Let $p = 11$. Prove that $y^5 + y^4 - 4y^3 - 3y^2 + 3y + 1$ is the minimal polynomial of the 2-period $(2, 1) = 2\cos(2\pi/11)$.*

Proof. Let $\zeta = \zeta_{11} = e^{2i\pi/11}$, and $\eta = (2, 1) = \zeta + \zeta^{-1} = 2\cos(2\pi/11)$. The powers of 2 modulo 11 are $1, 2, 2^2 = 4, 2^3 = 8, 2^4 = 5, 2^5 = -1$, so the order of $[2]$ in $(\mathbb{Z}/11\,\mathbb{Z})^*$ is 10, so 2 is a primitive root modulo 11.

As $\Phi_{11}(\zeta) = 1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6 + \zeta^7 + \zeta^8 + \zeta^9 + \zeta^{10} = 0$, we obtain by multiplication by ζ^{-5} :

$$(\zeta^{-5} + \zeta^5) + (\zeta^{-4} + \zeta^4) + (\zeta^{-3} + \zeta^3) + (\zeta^{-2} + \zeta^2) + (\zeta^{-1} + \zeta) + 1 = 0. \qquad (3)$$

Write $u_n = \zeta^n + \zeta^{-n}$. As

$$\zeta^{n+2} + \zeta^{-n-2} = (\zeta + \zeta^{-1})(\zeta^{n+1} + \zeta^{-n-1}) - (\zeta^n + \zeta^{-n}),$$

we obtain for all $n \in \mathbb{N}$

$$u_{n+2} = \eta\, u_{n+1} - u_n, \ u_0 = 2, u_1 = \eta.$$

Therefore

$$\begin{aligned}
\zeta + \zeta^{-1} &= \eta, \\
\zeta^2 + \zeta^{-2} &= \eta^2 - 2, \\
\zeta^3 + \zeta^{-3} &= \eta(\eta^2 - 2) - \eta = \eta^3 - 3\eta, \\
\zeta^4 + \zeta^{-4} &= \eta(\eta^3 - 3\eta) - (\eta^2 - 2) = \eta^4 - 4\eta^2 + 2, \\
\zeta^5 + \zeta^{-5} &= \eta(\eta^4 - 4\eta^2 + 2) - (\eta^3 - 3\eta) = \eta^5 - 5\eta^3 + 5\eta.
\end{aligned}$$

The equality (3) gives

$$\begin{aligned}
0 &= (\eta^5 - 5\eta^3 + 5\eta) + (\eta^4 - 4\eta^2 + 2) + (\eta^3 - 3\eta) + (\eta^2 - 2) + \eta + 1 \\
&= \eta^5 + \eta^4 - 4\eta^3 - 3\eta^2 + 3\eta + 1.
\end{aligned}$$

So η is a root of $f = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1 \in \mathbb{Q}[x]$.

By Proposition 9.2.6 (b), the fixed field L_2 of $\tilde{H}_2$ corresponding to $H_2 = \{-1, 1\}$ is $L_2 = \mathbb{Q}(\eta)$, and $[L_2 : \mathbb{Q}] = 5$ by Proposition 9.2.1. (as $\mathbb{Q} \subset \mathbb{Q}(\zeta)$ is a Galois extension, $[\mathbb{Q}(\eta) : \mathbb{Q}] = |\mathrm{Gal}(\mathbb{Q}(\eta)/\mathbb{Q})| = (G : \tilde{H}_2) = ((\mathbb{Z}/11\mathbb{Z})^* : \{-1, 1\}) = 5)$.

The minimal polynomial g of η over $\mathbb{Q}$ divides f, and has degree 5, so $g = f$.

Using the other form of the minimal polynomial given in Proposition 9.2.6(a), we obtain that

$$\begin{aligned}
&(x - \zeta - \zeta^{-1})(x - \zeta^2 - \zeta^{-2})(x - \zeta^3 - \zeta^{-3})(x - \zeta^4 - \zeta^{-4})(x - \zeta^5 - \zeta^{-5}) \\
&= x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1
\end{aligned}$$

is the minimal polynomial of $\eta = \zeta_{11} + \zeta_{11}^{-1}$ over $\mathbb{Q}$. $\qquad \square$

Ex. 9.2.11 *Let $L_{fq} \subset L_f$ be the extension studied in Theorem 9.2.14. Thus f and fq divide $p - 1$, and q is prime. As usual, $ef = p - 1$ and g is a primitive root modulo p. Finally, let ω be a primitive qth root of unity.*

(a) *Let $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ satisfy $\tau(\zeta_p) = \zeta_p^{g^{e/q}}$, and let $\sigma' = \tau|_{L_f}$ be the restriction of τ to L_f. Prove that σ' generates $\mathrm{Gal}(L_f/L_{fq})$.*

(b) Prove that $\operatorname{Gal}(L_f(\omega)/L_{fq}(\omega)) \simeq \operatorname{Gal}(L_f/L_{fq})$, where the isomorphism is defined by restriction to L_f.

(c) Let $\sigma \in \operatorname{Gal}(L_f(\omega)/L_{fq}(\omega))$ map to the element $\sigma' \in \operatorname{Gal}(L_f/L_{fq})$ constructed in part (a). Prove that σ satisfies (9.21).

(d) Prove the coset decomposition of H_{fq} given in (9.23).

Proof. (a) Let $f' = fq$, and $e' = n/f'$. Then $p - 1 = ef = e'f'$, and $e = e'q$.

By section 9.2,

$$L_f \text{ is the fixed field of } \tilde{H}_f = \langle \sigma \rangle, \text{ where } \sigma(\zeta_p) = \zeta_p^{g^e}.$$

$\tilde{H}_f$ is the set of automorphisms ξ such that $\zeta_p \mapsto \xi(\zeta_p) = \zeta_p^i$, $i \in H_f = \{1, g^e, g^{2e}, \cdots, g^{(f-1)e}\}$. This result applied to f' gives:

$$L_{fq} \text{ is the fixed field of } \tilde{H}_{fq} = \langle \tau \rangle, \text{ where } \tau(\zeta_p) = \zeta_p^{g^{e'}} = \zeta_p^{g^{e/q}}.$$

By the Galois correspondence, $\operatorname{Gal}(\mathbb{Q}(\zeta_p)/L_{fq}) = \tilde{H}_{fq} = \langle \tau \rangle$.

As $\mathbb{Q} \subset L_f$ is a Galois extension, $\tau L_f = L_f$ (Theorem 7.2.5).

If $\sigma' : L_f \to L_f$ is the restriction of τ to L_f, then $\sigma' \in \operatorname{Gal}(L_f/L_{fq})$.

The restriction mapping $\psi : \operatorname{Gal}(\mathbb{Q}(\zeta_p)/L_{fq}) \to \operatorname{Gal}(L_f/L_{fq})$ is a surjective mapping by the proof of Theorem 7.2.7, so every element of $\operatorname{Gal}(L_f/L_{fq})$ is of the form $\psi(\tau^k) = \sigma'^k$, $k \in \mathbb{Z}$, therefore

$$\operatorname{Gal}(L_f/L_{fq}) = \langle \sigma' \rangle.$$

Since $|\operatorname{Gal}(L_f/L_{fq})| = q$ (Proposition 9.2.1), the order of σ' is q.

Note: as $\tau(\zeta_p) = \zeta_p^{g^{e/q}}, \tau((f, \lambda)) = (f, g^{e/q}\lambda)$, for every period (f, λ) (Lemma 9.2.4(d)), and $(f, \lambda) \in L_f$, so

$$\sigma'((f, \lambda)) = (f, g^{e/q}\lambda).$$

(b) Since $q \mid p - 1, p \wedge q = 1$, therefore $\Phi_q(x) = \frac{x^q - 1}{x - 1}$ is irreducible over $\mathbb{Q}(\zeta_p)$ by Exercise 9.1.16. Hence Φ_q is a fortiori irreducible over the subfields L_f, L_{fq} of $\mathbb{Q}(\zeta_p)$. Consequently

$$[L_f(\omega) : L_f] = [L_{fq}(\omega) : L_{fq}] = \deg(\Phi_q) = q - 1.$$

$L_f(\omega)$ is the splitting field of Φ_q over L_f, $L_f \subset L_f(\omega)$ is so a Galois extension, and similarly $L_{fq} \subset L_{fq}(\omega)$ is Galois.

By Exercises 8.3.2 and 8.2.7, $L_f(\omega)$ is a Galois extension of L_{fq}, a fortiori of $L_{fq}(\omega)$.

Let

$$\varphi : \begin{cases} \operatorname{Gal}(L_f(\omega)/L_{fq}(\omega)) & \to & \operatorname{Gal}(L_f/L_{fq}) \\ \sigma & \mapsto & \sigma|_{L_f} \end{cases}$$

This mapping is well defined since L_f is a normal extension of L_{fq}, so $\sigma L_f = L_f$, and σ fixes the elements of $L_{fq}(\omega)$, a fortiori the elements of L_{fq}.

φ is a group homomorphism, and φ is injective:

if $\sigma \in \ker(\varphi)$, then $\sigma(\omega) = \omega$, and σ is the identity on L_f, thus σ is the identity on $L_f(\omega)$, so $\sigma = e$, therefore $\ker(\varphi) = \{e\}$.

Moreover, $[L_f : L_{fq}] = q$ and $[L_f(\omega) : L_f] = [L_{fq}(\omega) : L_{fq}] = q - 1$, therefore, by the Tower Theorem, $[L_f(\omega) : L_{fq}(\omega)] = q$. Hence $|\mathrm{Gal}(L_f(\omega)/L_{fq}(\omega))| = |\mathrm{Gal}(L_f, L_{fq})| = q$, so φ is a group isomorphism.

(c) Let $\sigma = \varphi^{-1}(\sigma')$. Then σ is a generator of $\mathrm{Gal}(L_f(\omega)/L_{fq}(\omega))$, and $\varphi(\sigma) = \sigma'$.

As $\sigma|_{L_f} = \sigma'$, by the note in part (a),

$$\sigma((f, \lambda)) = \sigma'((f, \lambda)) = (f, g^{e/q}\lambda).$$

(d) $H_f = \langle g^e \rangle$, and $H_{fq} = \langle g^{e/q} \rangle$.

We show first that $g^{k(e/q)} \notin H_f$ if $1 \le k \le q - 1$. If not, there would exist an integer j such that $g^{k(e/q)} = g^{je}$. As the order of g is $p - 1 = ef$, $ef \mid k\frac{e}{q} - je$, so $\lambda efq = ke - jeq, \lambda \in \mathbb{Z}$, therefore $\lambda fq = k - jq$, and so $q \mid k$. It is impossible since $1 \le k \le q - 1$.

If $0 \le i < j \le q - 1$, by the preceding result, $(g^{i(e/q)})^{-1}g^{j(e/q)} = g^{(j-i)(e/q)} \notin H_f$, therefore $g^{i(e/q)}H_f \neq g^{j(e/q)}H_f$.

The q left cosets $H_f, g^{e/q}H_f, g^{2e/q}H_f, \cdots, g^{(q-1)e/q}H_f$ are so distinct. Since $(H_{fq} : H_f) = q$, the set of left cosets is reduced to these q cosets, which give a partition of H_{fq}:

$$H_{fq} = H_f \cup g^{e/q}H_f \cup g^{2e/q}H_f \cup \cdots \cup g^{(q-1)e/q}H_f.$$

$\square$

Ex. 9.2.12 *Let p be an odd prime, and let m be a positive integer relatively prime to p.*

(a) *Prove that $1, \zeta_p, \ldots, \zeta_p^{p-2}$ are linearly independent over $\mathbb{Q}(\zeta_m)$.*

(b) *Explain why part (a) implies that $\zeta_p, \ldots, \zeta_p^{p-1}$ are linearly independent over $\mathbb{Q}(\zeta_m)$.*

(c) *Let $f \mid p - 1$. Prove that the f-periods are linearly independent over $\mathbb{Q}(\zeta_m)$.*

Proof. (a) As $p \wedge m = 1$, $\Phi_p(x) = x^{p-1} + \cdots + x + 1$ is irreducible over $\mathbb{Q}(\zeta_m)$ by Exercise 9.1.16. Therefore the minimal polynomial of ζ_p over $\mathbb{Q}(\zeta_m)$ is $\Phi_p(x)$, of degree $p - 1$, so $1, \zeta_p, \zeta_p^2, \cdots, \zeta_p^{p-2}$ are linearly independent over $\mathbb{Q}(\zeta_m)$.

(b) If $a_1, \cdots, a_{p-1} \in \mathbb{Q}(\zeta_m)$, as $\zeta_p \neq 0$,

$$a_1\zeta_p + a_2\zeta_p^2 + \cdots + a_{p-1}\zeta_p^{p-1} = 0 \Rightarrow a_1 + a_2\zeta_p + \cdots + a_{p-1}\zeta_p^{p-1} = 0 \Rightarrow a_1 = a_2 = \cdots = a_{p-1} = 0,$$

so $\zeta_p, \zeta_p^2, \cdots, \zeta_p^{p-1}$ are linearly independent over $\mathbb{Q}(\zeta_m)$.

(c) Suppose that $\sum_{i=1}^{e} a_i(f, \lambda_i) = 0$, where $a_i \in \mathbb{Q}(\zeta_m)$. Let $\{[\lambda_1], \cdots, [\lambda_e]\}$ be a complete system of representatives of the cosets $[\lambda]H_f$, then

$$\sum_{i=1}^{e} a_i \sum_{a \in [\lambda_i]H_f} \zeta_p^a = 0.$$

30

As $(\lambda_i H_f)_{1 \leq i \leq e}$ is a partition of $(\mathbb{Z}/p\mathbb{Z})^*$, this equality is equivalent to

$$\sum_{[k] \in (\mathbb{Z}/p\mathbb{Z})^*} b_k \zeta_p^k = \sum_{k=0}^{p-1} b_k \zeta_p^k = 0,$$

where b_k is a constant on every coset $[\lambda_i]H_f$, equal to a_i.

Since $\zeta_p, \zeta_p^2, \cdots, \zeta_p^{p-1}$ are linearly independent over $\mathbb{Q}(\zeta_m)$, all the b_k are zero, so $a_1 = \cdots = a_e = 0$.

Thus f-periods are linearly independent over $\mathbb{Q}(\zeta_m)$.

$\square$

Ex. 9.2.13 *Prove (9.24):*

$$\sum_{a=0}^{17} \left(\frac{a}{17}\right) \zeta_{17}^a = \sqrt{17}.$$

Proof. By Exercise 8 (b), we have proved for $p = 17$, that

$$(8,1) = \frac{1}{2}\left(-1 + \sqrt{17}\right),$$
$$(8,3) = \frac{1}{2}\left(-1 - \sqrt{17}\right).$$

So

$$\sqrt{17} = (8,1) - (8,3) = \sum_{a \in H_8} \zeta^a - \sum_{a \in 3H_8} \zeta^a.$$

Let

$$\varphi : \begin{cases} (\mathbb{Z}/p\mathbb{Z})^* & \to & (\mathbb{Z}/p\mathbb{Z})^* \\ x & \mapsto & x^2. \end{cases}$$

φ is a group homomorphism.

As $x^2 = 1 \iff (x-1)(x+1) = 0 \iff x \in \{-1, 1\}$, $\ker(\varphi) = \{-1, 1\} \subset (\mathbb{Z}/p\mathbb{Z})^*$. Write $C = \text{im}(\varphi)$ the set of square elements in $(\mathbb{Z}/p\mathbb{Z})^*$. Then $\text{im}(\varphi) \simeq (\mathbb{Z}/p\mathbb{Z})^*/\ker(\varphi)$, so $|C| = |\text{im}(\varphi)| = (p-1)/2 = 8$. Moreover $H_8 = \langle 3^2 \rangle$ (Exercise 1), so $H_8 \subset C$, and $|H_8| = 8 = |C|$, therefore $H_8 = C$ is the set of squares in $(\mathbb{Z}/17\mathbb{Z})^*$. Its complement $3H_8$ is the set of non squares in $(\mathbb{Z}/17\mathbb{Z})^*$.

Therefore, for all $a \in (\mathbb{Z}/17\mathbb{Z})^*$.

$$\left(\frac{a}{17}\right) = 1 \iff a \in H_8,$$

$$\left(\frac{a}{17}\right) = -1 \iff a \in 3H_8,$$

and $\left(\frac{a}{17}\right) = 0$ if $a = 0$ or $a = 17$ (where we write for all integer k, $\left(\frac{[k]}{17}\right) = \left(\frac{k}{17}\right)$). Hence

$$\sum_{a=0}^{17} \left(\frac{a}{17}\right) \zeta_{17}^a = \sqrt{17}.$$

$\square$

Ex. 9.2.14 *Consider the quotation from Galois given at the end of the Historical Notes.*

(a) *Show that the permutations obtained by mapping the first line in the displayed table to the other lines give a cyclic group of order $n - 1$. Also explain how these permutations relate to the Galois group.*

(b) *Explain what Galois is saying in the last sentence of the quotation.*

Proof. This group of permutations is generated by the cycle

$$(a, b, c, \cdots, k) = (r, r^g, r^{g^2}, \cdots, r^{g^{n-2}}).$$

It is a cyclic subgroup of order $n - 1$ in the group of permutation of the $n - 1$ roots of $\Phi_n(x)$. The Galois group of $\Phi_n(x)$, as a permutation group of the roots, is indeed a cyclic group of order $n - 1$, if n is prime:

$$\mathrm{Gal}_{\mathbb{Q}}(\Phi_n) = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^* \simeq C_{n-1}.$$

For such a Galois extension,

$$|\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = n - 1 = \deg(\Phi_n(x)).$$

(b) If all the roots are rational function of one fixed root α of f, then the extension $\mathbb{Q} \subset \mathbb{Q}(\alpha)$ is Galois, so the equality $|\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})| = [\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f)$ is true for the minimal polynomial f of α over $\mathbb{Q}$. □

Ex. 9.2.15 *What are the 1-periods?*

Proof. $H_1 = \{[1]\}$, and the coset of $[a] \in (\mathbb{Z}/p\mathbb{Z})^*$ is $[a]H_1 = \{[a]\}$, so the 1-periods $(1, a)$ are the powers of ζ_p:

$$(1, a) = \zeta_p^a.$$

□

Ex. 9.2.16 *Redo Exercise 3 using periods.*

Proof. If $p = 7$, and $\zeta = e^{2i\pi/7}$, the 2-periods corresponding to $H_2 = \{-1, 1\} = \{1, 6\}$ are $(2, 1) = \zeta + \zeta^{-1}, (2, 2) = \zeta^2 + \zeta^{-2}, (2, 3) = \zeta^3 + \zeta^{-3}$. By Proposition 9.2.6, they are the roots of the irreducible polynomial

$$f = (x - (2, 1))(x - (2, 2))(x - (2, 3))$$

$$(2, 1) + (2, 2) + (2, 3) = -1,$$
$$(2, 1)^2 = \sum_{\lambda \in H_2} (2, \lambda + 1) = (2, 2) + 2,$$
$$(2, 1)(2, 2) = \sum_{\lambda \in H_2} (2, \lambda + 2) = (2, 3) + (2, 1).$$

3 is a primitive root modulo 7. Let σ the $\mathbb{Q}$-automorphism determined by $\sigma(\zeta) = \zeta^3$. Then σ gives the chain $(2, 1) \mapsto (2, 3) \mapsto (2, 2) \mapsto (2, 1)$, so

$$(2, 1)(2, 2) = (2, 3) + (2, 1), \quad (2, 3)(2, 1) = (2, 2) + (2, 3), \quad (2, 2)(2, 3) = (2, 1) + (2, 2).$$

By summation of these equalities,

$$(2,1)(2,2) + (2,3)(2,1) + (2,2)(2,3) = 2(2,3) + 2(2,1) + 2(2,2) = -2.$$

Finally

$$(2,1)(2,2)(2,3) = (2,1)[(2,1)+(2,2)] = (2,1)^2 + (2,1)(2,2) = (2,2)+2+(2,3)+(2,1) = 1.$$

Therefore $f = x^3 + x^2 - 2x - 1$ is the minimal polynomial of $(2,1) = 2\cos(2\pi/7)$ over $\mathbb{Q}$ (and also of $(2,2), (2,3)$).

The fixed field L_2 of $\tilde{H}_2$ corresponding to H_2 is $\mathbb{Q}(\zeta + \zeta^{-1})$, of degree 3 over $\mathbb{Q}$, and $\tilde{H}_2 = \{e, \tau\}$, where $\tau(\zeta) = \zeta^{-1} = \bar{\zeta}$, so τ is the restriction of the complex conjugation to L_2. The end of the proof is the same as in Exercise 3. $\qquad\square$

Ex. 9.2.17 *Let f be an even divisor of $p-1$ where p is an odd prime. Prove that every f-period (f, λ) lies in $\mathbb{R}$.*

Proof. As $2 \mid f$ is even, $H_2 \subset H_f$ (Exercise 1), so every coset $[\lambda]H_f$ is a disjoint union of $[\mu]H_2$ (Exercise 4), so

$$[\lambda]H_f = \bigcup_{[\mu]\in A} [\mu]H_2.$$

Therefore

$$(f,\lambda) = \sum_{a\in[\lambda]H_f} \zeta_p^a = \sum_{\mu\in A}\sum_{a\in[\mu]H_2} \zeta_p^a = \sum_{\mu\in A}(\zeta_p^\mu + \zeta_p^{-\mu}) \in \mathbb{R}.$$

$\qquad\square$