Galois theory - Problem Set 5

To be solved on Monday 17.04

Problem 1. Let $n \in \mathbb{Z}$, $n \geq 1$. Show that the following hold.

(a) For every $m \in \mathbb{Z}_n$ we have that the order of m is $o(m) = \frac{n}{\gcd(m,n)}$. In particular, $m \in \mathbb{Z}_n$ is a generator of $\mathbb{Z}_n$ if and only if $\gcd(m,n) = 1$.

(b) The number of generators of the cyclic group $\mathbb{Z}_n$ is $\phi(n)$.

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

Solution.

(a) Recall that $\gcd(n,m)\,\mathrm{lcm}(n,m) = nm$. Then

$$\frac{n}{\gcd(n,m)} m \equiv \mathrm{lcm}(n,m) \equiv 0 \mod n,$$

and so $o(m) \mid \frac{n}{\gcd(n,m)}$. It is enough to show that $\frac{n}{\gcd(n,m)} \mid o(m)$ too. We have that

$$o(m)m \equiv 0 \mod n,$$

and so $n \mid o(m)m$. Since $n \mid o(m)n$, we obtain that $n \mid \gcd(o(m)m, o(m)n)$. It follows that $n \mid o(m)\gcd(n,m)$ or that $\frac{n}{\gcd(n,m)} \mid o(m)$, as required.

(b) Since $|\mathbb{Z}_n| = n$ is a cyclic group, an element $m \in \mathbb{Z}_n$ is a generator if and only if $o(m) = n$. By part (b) this is equivalent to $\gcd(m,n) = 1$. Hence there are as many generators of $\mathbb{Z}_n$ as elements m with $1 \leq m \leq n$ and $\gcd(m,n) = 1$. Since there are precisely $\phi(n)$ such elements, the claim follows.

(c) Let d be a divisor of n. Recall that $\mathbb{Z}_n$ has exactly one subgroup of order d, that is $H_d = \langle \frac{n}{d} \rangle$ (see Theorem 4.4.4 in the book). In particular, we have $H_d \cong \mathbb{Z}_d$. Now let $x \in \mathbb{Z}_n$ be an element of order d. Then $\langle x \rangle$ is a subgroup of $\mathbb{Z}_n$ of order d and hence $\langle x \rangle = H_d$ and x is a generator of H_d. Since $x \in \mathbb{Z}_n$ was arbitrary, it follows that every element of order d in $\mathbb{Z}_n$ is a generator of $H_d \cong \mathbb{Z}_d$. Since by part (b) we have that $\mathbb{Z}_d$ has $\phi(d)$ generators, we conclude that there are exactly $\phi(d)$ elements of order d in $\mathbb{Z}_n$. Since the order of any element in $\mathbb{Z}_n$ divides $|\mathbb{Z}_n| = n$, we have

$$n = |\mathbb{Z}_n| = \sum_{d|n} |\{\text{elements of order } d \text{ in } \mathbb{Z}_n\}| = \sum_{d|n} \phi(d),$$

as required.

Problem 2. (Exam May 2013, Problem 1)

(a) Let E be the splitting field of $f(x) = x^{14} - 1$ over $\mathbb{Q}$. Show that the Galois group $G = \mathrm{Gal}(E/\mathbb{Q})$ is abelian.

(b) Let $\tilde{E}$ be the splitting field of $g(x) = x^7 + 1$ over $\mathbb{Q}$. Show that the Galois group $\tilde{G} = \mathrm{Gal}(\tilde{E}/\mathbb{Q})$ is abelian.

Solution.

(a) By Theorem 14.12(1) we have that $E = \mathbb{Q}(\omega)$ where ω is a primitive 14-th root of unity. By Theorem 14.12(4) we have $G = \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong \mathbb{Z}_{14}^{\times}$, which is an abelian group.

(b) We have that $x^{14} - 1 = (x^7 + 1)(x^7 - 1)$. Hence $x^7 + 1$ splits in $E = \mathbb{Q}(\omega)$. It follows that the splitting field $\tilde{E}$ of $x^7 + 1$ is a subfield of E. Since $\tilde{E}$ is the splitting field of $x^7 + 1$, the extension $\mathbb{Q} \subseteq \tilde{E}$ is normal. Since $\mathbb{Q} \subseteq \tilde{E} \subseteq E$, we obtain by the FTGT(6) that

$$\tilde{G} = \mathrm{Gal}(\tilde{E}/\mathbb{Q}) \cong \mathrm{Gal}(E/\mathbb{Q})/\,\mathrm{Gal}(E/\tilde{E}).$$

Therefore, $\tilde{G}$ is isomorphic to a quotient group of the abelian group $G = \mathrm{Gal}(E/\mathbb{Q})$. Since quotient groups of abelian groups are abelian, it follows that $\tilde{G}$ is abelian.

Problem 3. (Exam May 2004, Problem 3) Let p be a prime. Let E be the splitting field of $x^p - 1 \in \mathbb{Q}[x]$ over $\mathbb{Q}$.

(a) Prove that $\mathrm{Gal}(E/\mathbb{Q})$ is abelian of order $p - 1$.

(b) Let $\omega = e^{\frac{2\pi i}{31}}$. Prove that there exists a subfield F of $\mathbb{C}$ such that $[F(\omega) : F] = 5$.

Solution.

(a) Let $f(x) = x^p - 1$ and $\omega = e^{\frac{2\pi i}{p}}$. Then ω is a primitive p-th root of unity and $\{\omega^i \mid 1 \le i \le\}$ are the roots of $x^p - 1$. Hence $E = \mathbb{Q}(\omega)$. Since the minimal polynomial of ω over $\mathbb{Q}$ is $\Phi_p(x) = 1 + x + \cdots + x^{p-1}$, it follows that $[\mathbb{Q}(\omega) : \mathbb{Q}] = p - 1$ and $\{1, \omega, \ldots, \omega^{p-2}\}$ is a $\mathbb{Q}$-basis of E. Then an element $\sigma \in \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ is determined completely by its value $\sigma(\omega)$. Since $\Phi_p(\sigma(\omega)) = \sigma(\Phi_p(\omega)) = 0$, we have that $\sigma(\omega)$ is a root of $\Phi_p(x)$. Hence $\sigma(\omega) = \omega^i$ with $1 \le i \le p - 1$. Therefore

$$\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) = \{\sigma_i : \mathbb{Q}(\omega) \to \mathbb{Q}(\omega) \mid 1 \le i \le p-1, \sigma_i(\omega) = \omega^i, \text{ and } \sigma_i\big|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}\}$$

Then the map

$$\begin{aligned} \Psi : \mathbb{Z}_p^{\times} &\to \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \\ \bar{i} &\mapsto \sigma_i \end{aligned}$$

is well-defined and is clearly injective. Since both sets have $p-1$ elements, Ψ is also bijective. Moreover we claim that Ψ is a group homomorphism. Indeed, for $\bar{i}, \bar{j} \in \mathbb{Z}_p^{\times}$ we have

$$\sigma_{ij}(\omega) = \omega^{ij} = \sigma_i \circ \sigma_j(\omega).$$

Hence

$$\Psi(\overline{ij}) = \sigma_{ij} = \sigma_i \circ \sigma_j = \Psi(\bar{i}) \circ \Psi(\bar{j}).$$

Hence $\mathrm{Gal}(E/\mathbb{Q})$ is isomorphic to $\mathbb{Z}_p^{\times}$ which is an abelian group of order $p - 1$.

(b) Consider the subgroup $\{1, 2, 4, 8, 16\}$ of $\mathbb{Z}_{31}^{\times}$. By the map Ψ in part (a) it corresponds to the subgroup $H = \{\sigma_1, \sigma_2, \sigma_4, \sigma_8, \sigma_{16}\}$ of $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$. By the FTGT the field E_H satisfies

$$[\mathbb{Q}(\omega) : E_H] = |\mathrm{Gal}(\mathbb{Q}(\omega)/E_H)| = |H| = 5.$$

Since $\mathbb{Q} \subseteq E_H \subseteq \mathbb{Q}(\omega)$ we have $\mathbb{Q}(\omega) \subseteq E_H(\omega) \subseteq \mathbb{Q}(\omega)$ and so $E_H(\omega) = \mathbb{Q}(\omega)$. Therefore, by setting $F = E_H$ we have

$$[F(\omega) : F] = [E_H(\omega) : E_H] = [\mathbb{Q}(\omega) : E_H] = 5,$$

as required.

Problem 4. (Exam May 2009, Problem 5.) Let $F \subseteq K$ be a Galois extension such that $G(K/F)$ is cyclic of order n and let σ be a generator for $G(K/F)$. Assume that F contains a primitive n-th root ω of unity. Let $\alpha \in K \setminus F$ and let $(\omega, \alpha) \neq 0$ be the Lagrange resolvent defined by

$$(\omega, \alpha) = \alpha + \omega\sigma(\alpha) + \cdots + \omega^{n-1}\sigma^{n-1}(\alpha).$$

(a) Show that $a = \alpha + \sigma(\alpha) + \cdots + \sigma^{n-1}(\alpha)$ is an element in F.

(b) Show that $K = F((\omega, \alpha))$.

(c) Let $b = (\omega, \alpha)^n$. Show that $b \in F$ and that K is the splitting field of $x^n - b \in F[x]$ over F.

(d) Give an argument why $x^n - b$ is an irreducible polynomial over F.

Solution.

(a) Since $G(K/F)$ is cyclic of order n and $\sigma \in G(K/F)$ is a generator, we have that $\sigma^n = \mathrm{id}_K$. Hence

$$\begin{aligned}\sigma(a) &= \sigma(\alpha + \sigma(\alpha) + \cdots + \sigma^{n-2}(\alpha) + \sigma^{n-1}(\alpha)) \\ &= \sigma(\alpha) + \sigma^2(\alpha) + \cdots + \sigma^{n-1}(\alpha) + \sigma^n(\alpha) \\ &= \sigma(\alpha) + \sigma^2(\alpha) + \cdots + \sigma^{n-1}(\alpha) + \alpha = a.\end{aligned}$$

Hence $\sigma(a) = a$. It follows that $\sigma^i(a) = a$ for all $1 \leq i \leq n$. Since $\langle\sigma\rangle = G(K/F)$, it follows that $\tau(a) = a$ for any $\tau \in G(K/F)$. Hence $a \in E_{G(K/F)} = F$, where the last equality follows by the FTGT(1).

(b) Set $H = G(K/F((\omega, \alpha)))$. Since $F \subseteq F((\omega, \alpha)) \subseteq K$, we have that $H < G(K/F) = \langle\sigma\rangle$. Hence there exists $I \subseteq \{1, \ldots, n\}$ such that $H = \{\sigma^i \mid i \in I\}$. Since $\sigma\big|_F = \mathrm{id}_F$ and since $\omega \in F$, we have $\sigma(\omega) = \omega$. Then we compute

$$\sigma((\omega, \alpha)) = \sigma(\alpha) + \sigma(\omega)\sigma^2(\alpha) + \cdots + \sigma(\omega^{n-1})\sigma^n(\alpha) = \sigma(\alpha) + \omega\sigma^2(\alpha) + \cdots + \omega^{n-1}\alpha = \omega^{n-1}(\omega, \alpha),$$

where the last equality follows since $\omega^n = 1$. Therefore, for $i \in I$ we have $\sigma^i \in H$ and so

$$(\omega, \alpha) = \sigma^i((\omega, \alpha)) = (\omega^{n-1})^i(\omega, \alpha).$$

We obtain that $(\omega^{n-1})^i = 1$ for all $i \in I$. Equivalently, we have that $n \mid i(n-1)$ since ω has order n. Since $\gcd(n-1, n) = 1$, we have that $n \mid i$. Since $1 \leq i \leq n$ we conclude that $i = n$. Hence $I = \{n\}$ and so $H = \{\sigma^n\} = \{\mathrm{id}_K\}$. But then by the FTGT(3) we have

$$[K : F((\omega, \alpha))] = |G(K/F((\omega, \alpha)))| = |H| = 1,$$

and so $F((\omega, \alpha)) = K$.

(c) We compute

$$\sigma(b) = \sigma((\omega, \alpha)^n) = (\sigma((\omega, \alpha)))^n = (\omega^{n-1}(\omega, \alpha))^n = \omega^{(n-1)n}(\omega, \alpha)^n = 1 \cdot b = b.$$

Therefore, $\sigma^i(b) = b$ for all $i \geq 1$. Since σ generates $G(K/F)$, it follows that $\tau(b) = b$ for all $\tau \in G(K/F)$. Hence $b \in E_{G(K/F)} = F$, where the last equality follows by the FTGT(1).

The roots of $x^n - b$ are $(\omega, \alpha), \omega(\omega, \alpha), \cdots, \omega^n(\omega, \alpha)$. By part (b) we have that they all belong to K. Hence $x^n - b$ factors into linear factors in K. Moreover, assume to a contradiction that $F \subseteq X \subsetneq K$ is an intermediate field and that $x^n - b$ factors into linear factors in X. Then $(\omega, \alpha) \in X$ and so $K = F((\omega, \alpha)) \subseteq X \subsetneq K$ is a contradiction. Hence $x^n - b$ does not factor into linear factors in any strict subfield of K and so K is the splitting field of $x^n - b$.

(d) Since $F \subseteq K$ is a Galois extension, and since $K = F((\omega, \alpha))$ by part (b), we have that $F \subseteq F((\omega, \alpha))$ is Galois. In particular, $F \subseteq F((\omega, \alpha))$ is finite and has degree equal to the degree of the minimal polynomial of (ω, α). Assume to a contradiction that $x^n - b$ is not irreducible. Since (ω, α) is a root of $x^n - b$, this implies that there exists an irreducible monic polynomial $g(x)$ with (ω, α) as a root and $\deg(g(x)) < \deg(x^n - b) = n$. By the FTGT(3) we have

$$n > \deg(g(x)) = [F((\omega, \alpha)) : F] = [K : F] = |G(K/F)| = n,$$

which is a contradiction. Hence $x^n - b$ is irreducible.

Problem 5. (Exam June 2014, Problem 2.) Let $F \subseteq E$ where $F = \mathrm{GF}(5^3)$ and $E = \mathrm{GF}(5^{24})$. Describe the Galois group $G = \mathrm{Gal}(E/F)$ and list the fields K such that $F \subseteq K \subseteq E$.

Solution. By Theorem 10.8 and uniqueness of finite fields we have $[\mathrm{GF}(5^{24}) : \mathrm{GF}(5^3)] = \frac{24}{3} = 8$. Another way to see this is to use the tower of field extensions $\mathrm{GF}(5) \subseteq \mathrm{GF}(5^3) \subseteq \mathrm{GF}(5^{24})$. This gives

$$[\mathrm{GF}(5^{24}) : \mathrm{GF}(5)] = [\mathrm{GF}(5^{24}) : \mathrm{GF}(5^3)] \cdot [\mathrm{GF}(5^3) : \mathrm{GF}(5)].$$

Since $[\mathrm{GF}(p^n) : \mathrm{GF}(p)] = n$, we conclude that

$$24 = [\mathrm{GF}(5^{24}) : \mathrm{GF}(5^3)] \cdot 3$$

and so $[\mathrm{GF}(5^{24}) : \mathrm{GF}(5^3)] = 8$. By Theorem 10.8 we also have that $\mathrm{GF}(5^{24})$ is the splitting field of $x^{5^{24}} - x$ over $\mathrm{GF}(5^3)$ (the way to see this is to notice that every element of $\mathrm{GF}(5^{24})$ is a root of $x^{5^{24}} - x$, and since $x^{5^{24}} - x$ can have at most 5^{24} roots, it follows that $\mathrm{GF}(5^{24})$ is the smallest field which contains all its roots). Hence the extension $\mathrm{GF}(5^3) \subseteq \mathrm{GF}(5^{24})$ is normal. Since it is also finite of degree 8 and separable because $\mathrm{GF}(5^3)$ is a perfect field (as it is finite), we conclude that $\mathrm{GF}(5^3) \subseteq \mathrm{GF}(5^{24})$ is a Galois extension. By the FTGT(3) we obtain that

$$|G| = |\mathrm{Gal}(\mathrm{GF}(5^{24})/\mathrm{GF}(5^3))| = [\mathrm{GF}(5^{24}) : \mathrm{GF}(5^3)] = 8.$$

By Example 15.2(2) we have that G is a cyclic group as it is the Galois group of an extension of a finite field. Hence $G \cong \mathbb{Z}_8$. The subgroups of $\mathbb{Z}_8$ are

$$\{0\} < \{0, 4\} < \{0, 2, 4, 6\} < \mathbb{Z}_8.$$

By the FTGT these subgroups H correspond to intermediate fields between F and E via the map $H \mapsto E_H$. We have

$$E_{\mathbb{Z}_8} = E_G = E_{\mathrm{Gal}(E/F)} = F = \mathrm{GF}(5^3),$$

and

$$E_{\{0\}} = E_{\mathrm{id}_E} = E = \mathrm{GF}(5^{24}).$$

For the subgroup $H_1 = \{0, 4\}$, we have by the FTGT(2) and (3) that

$$2 = |H_1| = |\mathrm{Gal}(E/E_{H_1})| = [E : E_{H_1}].$$

Hence if $E_{H_1} = \mathrm{GF}(5^m)$, then $2 = [E : E_{H_1}] = \frac{24}{m}$. Therefore, $E_{H_1} = \mathrm{GF}(5^{12})$. Similarly, if $H_2 = \{0, 2, 4, 6\}$, then $E_{H_2} = \mathrm{GF}(5^6)$. Therefore we obtain the tower of subfields

$$F = \mathrm{GF}(5^3) \subseteq \mathrm{GF}(5^6) \subseteq \mathrm{GF}(5^{12}) \subseteq \mathrm{GF}(5^{24}) = E.$$

Problem 6. (Exercise 18.2.4 in the book.) Let E be a finite separable normal extension over F and let $G(E/F) = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$. If $\alpha \in E$ we define

$$T_{E/F}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha) \text{ and } N_{E/F}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$$

and call these respectively the *trace* and *norm* of α in E over F. Show:

(a) $T_{E/F}(\alpha) \in F$, $N_{E/F}(\alpha) \in F$.

(b) $T_{E/F}$ is an F-linear map of the vector space E over F.

(c) $N_{E/F}$ is a group homomorphism from the group $E^* = E \setminus \{0\}$ to the group $F^* = F \setminus \{0\}$.

(d) If $G(E/F)$ is a cyclic group generated by σ, then $N_{E/F}(\alpha) = 1$ if and only if there exists $b \in E$ such that $\alpha = (\sigma(b))^{-1}b$. (*Hint*: Generalize Lemma 2.4 (Lemma 15.3 in our notes).)

Solution.

(a) Recall that for any group G and any $g \in G$, the map

$$\begin{aligned}\lambda_g : G &\to G\\ h &\mapsto \lambda_g(h) = gh\end{aligned}$$

is a bijection. Therefore, for every $\sigma_j \in \mathrm{Gal}(E/F)$, we have that

$$\{\sigma_1, \sigma_2, \ldots, \sigma_n\} = \mathrm{Gal}(E/F) = \{\sigma_j\sigma_1, \sigma_j\sigma_2, \ldots, \sigma_j\sigma_n\} = .$$

Then for every $\sigma_j \in \mathrm{Gal}(E/F)$ we have

$$\sigma_j(T_{E/F}(\alpha)) = \sigma_j\left(\sum_{i=1}^{n} \sigma_i(\alpha)\right) = \sum_{i=1}^{n} \sigma_j\sigma_i(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha) = T_{E/F}(\alpha).$$

Since σ_j is arbitrary, it follows that $T_{E/F}(\alpha) \in E_{\mathrm{Gal}(E/F)} = F$, where the last equality follows by the FTGT(1) since $F \subseteq E$ is Galois. Similarly, we have

$$\sigma_j(N_{E/F}(\alpha)) = \sigma_j\left(\prod_{i=1}^{n} \sigma_i(\alpha)\right) = \prod_{i=1}^{n} \sigma_j\sigma_i(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) = N_{E/F}(\alpha),$$

and so $N_{E/F}(\alpha) \in E_{\mathrm{Gal}(E/F)} = F$.

(b) Let $\alpha, \beta \in E$ and $f, g \in F$. Then for every $\sigma_i \in \mathrm{Gal}(E/F)$ we have $\sigma_i(f) = f$ and $\sigma_i(g) = g$. Using this we compute

$$\begin{aligned}T_{E/F}(f\alpha + g\beta) &= \sum_{i=1}^{n} \sigma_i(f\alpha + g\beta)\\ &= \sum_{i=1}^{n} (\sigma_i(f)\sigma_i(\alpha) + \sigma_i(g)\sigma_i(\beta))\\ &= \sum_{i=1}^{n} (f\sigma_i(\alpha) + g\sigma_i(\beta))\\ &= f\sum_{i=1}^{n} \sigma_i(\alpha) + g\sum_{i=1}^{n} \sigma_i(\beta)\\ &= fT_{E/F}(\alpha) + gT_{E/F}(\beta),\end{aligned}$$

which shows that $T_{E/F} : E \to F$ is an F-linear map.

(c) Let $\alpha \in E$. Then $N_{E/F}(\alpha) = 0$ implies that $\prod_{i=1}^{n} \sigma_i(\alpha) = 0$ and so $\sigma_i(\alpha) = 0$ for some $\sigma_i \in \mathrm{Gal}(E/F)$. Since σ_i is a ring morphism between fields, it follows that $\alpha = 0$. Since $N_{E/F}$ is a map from E to F by part (a), it follows that $N_{E/F} : E^* \to F^*$. Then for every $\alpha, \beta \in E$ we have

$$N_{E/F}(\alpha\beta) = \prod_{i=1}^{n} \sigma_i(\alpha\beta) = \prod_{i=1}^{n} \sigma_i(\alpha)\sigma_i(\beta) = \prod_{i=1}^{n} \sigma_i(\alpha) \prod_{i=1}^{n} \sigma_i(\beta) = N_{E/F}(\alpha)N_{E/F}(\beta),$$

which shows that $N_{E/F}$ is a group homomorphism.

(d) Let $\alpha \in E$. We may write $\mathrm{Gal}(E/F) = \{\sigma^0 = \mathrm{id}_E, \sigma, \sigma^2, \dots, \sigma^{n-1}\}$. Assume first that $\alpha = (\sigma(b))^{-1}b$ for some $b \in E$ and we show that $N_{E/F}(\alpha) = 1$. We claim that for $i \geq 0$ we have $\sigma^i(\alpha) = \sigma^{i+1}(b)^{-1}\sigma^i(b)$. We use induction on i. For $i = 0$ the claim is immediate. Assume that the claim is true for $i-1$ and we show it for i. We have

$$\sigma^i(\alpha) = \sigma(\sigma^{i-1}(\alpha)) = \sigma(\sigma^i(b)^{-1}\sigma^{i-1}(b)) = \sigma^{i+1}(b)^{-1}\sigma^i(b),$$

as required. Therefore, we can compute

$$\begin{aligned} N_{E/F}(\alpha) = \prod_{i=1}^{n} \sigma^i(\alpha) &= \sigma^2(b)^{-1}\sigma(b)\sigma^3(b)^{-1}\sigma^2(b)\cdots\sigma^n(b)^{-1}\sigma^{n-1}(b)\sigma^{n+1}(b)^{-1}\sigma^n(b) \\ &= \sigma^2(b)^{-1}\sigma(b)\sigma^3(b)^{-1}\sigma^2(b)\cdots b^{-1}\sigma^{n-1}(b)\sigma(b)^{-1}b = 1, \end{aligned}$$

where the last equality follows since the terms cancel each other.

For the other direction assume that $N_{E/F}(\alpha) = 1$ and we show that there exists $b \in E$ such that $\alpha = (\sigma(b))^{-1}b$. Since $N_{E/F}(\alpha) = 1$, we have that

$$\alpha\sigma(\alpha)\sigma^2(\alpha)\cdots\sigma^{n-1}(\alpha) = 1.$$

By Lemma 15.3 we obtain that there exists $z \in E^*$ such that $\alpha = \sigma(z)z^{-1}$. Setting $b = z^{-1}$ we obtain $\alpha = \sigma(b^{-1})b = \sigma(b)^{-1}b$, as required.

Problem 7. (Exam June 2014, Problem 4.)

(a) Let $F \subseteq F(\theta)$ and $F \subseteq F(\gamma)$ be two Galois extensions of the field F, where $\mathrm{char}(F) = 0$. Show that $F \subseteq F(\theta, \gamma)$ is a Galois extension of F.

(b) Assume $\mathrm{Gal}(F(\theta)/F)$ and $\mathrm{Gal}(F(\gamma)/F)$ are both abelian groups. Show that $\mathrm{Gal}(F(\theta,\gamma)/F))$ is an abelian group.

Solution.

(a) We need to show that $F \subseteq F(\gamma, \theta)$ is finite, normal and separable.

Since $F \subseteq F(\gamma)$ is finite, we have that γ is algebraic over F. Hence γ is algebraic over $F(\theta)$. Then $F \subseteq F(\theta, \gamma)$ is finitely-generated and θ and γ are algebraic over F. Hence $F \subseteq F(\theta,\gamma)$ is a finite extension.

We have that $F \subseteq F(\gamma, \theta)$ is a normal extension by Problem 3 in Problem Set 3. Here is another way to show this. Since $F \subseteq F(\theta)$ is normal and finite, we have that $F(\theta)$ is the splitting field of a polynomial $f(x) \in F[x]$ by Proposition 8.4. Similarly, $F(\gamma)$ is the splitting field of a polynomial $g(x) \in F[x]$. Let $h(x) = f(x)g(x)$ and we claim that its splitting field is $F(\theta,\gamma)$. Clearly $h(x)$ factors into linear factors in $F(\theta,\gamma)$ since $f(x)$ factors into linear factors in $F(\theta)$ and $g(x)$ factors into linear factors in $F(\gamma)$. Let $F \subseteq K \subsetneq F(\theta,\gamma)$ be an intermediate field and assume to a contradiction that $h(x)$ factors into linear factors in K. Then $f(x)$ factors into linear factors in K and so $F(\theta) \subseteq K$. Similarly, $F(\gamma) \subseteq K$. But then $F(\theta,\gamma) \subseteq K$, contradicting $K \subsetneq F(\theta,\gamma)$. This shows that $F(\theta,\gamma)$ is the splitting field of $h(x)$ and hence $F \subseteq F(\theta,\gamma)$ is normal.

Since $\mathrm{char}\, F = 0$, we have that $F \subseteq F(\theta,\gamma)$ is a separable extension.

(b) Define a map

$$\begin{aligned} \Psi : \mathrm{Gal}(F(\theta,\gamma)/F) &\to \mathrm{Gal}(F(\theta)/F) \times \mathrm{Gal}(F(\gamma)/F) \\ \sigma &\mapsto (\sigma\big|_{F(\theta)}, \sigma\big|_{F(\gamma)}). \end{aligned}$$

We claim that σ is well defined. That is, we need to show that $\sigma\big|_{F(\theta)} \in \mathrm{Gal}(F(\theta)/F)$ and $\sigma\big|_{F(\gamma)} \in \mathrm{Gal}(F(\gamma)/F)$. We only show the first claim as the other is similar. Since

$$\left(\sigma\big|_{F(\theta)}\right)\Big|_F = \sigma\big|_F = \mathrm{id}_F,$$

we only need to show that $\sigma\big|_{F(\theta)} : F(\theta) \to F(\theta)$ is a field isomorphism. Let $p(x) \in F[x]$ be the minimal polynomial of θ and assume that $\deg(p(x)) = d$. Then

$$0 = \sigma(p(\theta)) = p(\sigma(\theta))$$

implies that $\sigma(\theta)$ is a root of $p(x)$. By Theorem 8.5 and since $F \subseteq F(\theta)$ is a normal extension, we have that all roots of $p(x)$ are in $F(\theta)$. Hence $\sigma(\theta) \in F(\theta)$. Since $\{1, \theta, \ldots, \theta^{d-1}\}$ is a basis of $F(\theta)$ over F, we have that if $a_0 + a_1\theta + \cdots + a_{d-1}\theta^{d-1} \in F(\theta)$ with $a_i \in F$, then

$$\sigma(a_0 + a_1\theta + \cdots + a_{d-1}\theta^{d-1}) = a_0 + a_1\sigma(\theta) + \cdots + a_{d-1}\sigma(\theta)^{d-1} \in F(\theta).$$

Hence $\sigma(F(\theta)) \subseteq F(\theta)$. Moreover, similarly we obtain that $\sigma^i(\theta)$ is a root of $p(x)$ for all $i \geq 0$ and that $\sigma^i(\theta) \in F(\theta)$. Since $p(x)$ has at most d roots, we obtain that $\sigma^i(\theta) = \sigma^j(\theta)$ for some $i < j$. Since σ is injective, we have $\theta = \sigma^{j-i}(\theta) \in \sigma(F(\theta))$. Since $\theta \in \sigma(F(\theta))$ and $\sigma(F(\theta)) \subseteq F(\theta)$, we conclude that $\sigma(F(\theta)) = F(\theta)$. This shows that Ψ is well-defined.

Now we claim that Ψ is a group homomorphism. Indeed, for any $\sigma, \rho \in \mathrm{Gal}(F(\theta,\gamma)/F)$ we have that

$$(\sigma \circ \rho)\big|_{F(\theta)} = \sigma\big|_{F(\theta)} \circ \rho\big|_{F(\theta)},$$

since $\rho(F(\theta)) \subseteq F(\theta)$. Then

$$\Psi(\sigma\circ\rho) = ((\sigma \circ \rho)\big|_{F(\theta)}, (\sigma \circ \rho)\big|_{F(\gamma)}) = (\sigma\big|_{F(\theta)}\circ\rho\big|_{F(\theta)}, \sigma\big|_{F(\gamma)}\circ\rho\big|_{F(\gamma)}) = (\sigma\big|_{F(\theta)}, \sigma\big|_{F(\gamma)})\circ(\rho\big|_{F(\theta)}, \rho\big|_{F(\gamma)})$$

and so Ψ is a group homomorphism.

Now we claim that Ψ is injective. For this assume that $\Psi(\sigma) = (\mathrm{id}_{F(\theta)}, \mathrm{id}_{F(\gamma)})$ and we show that $\sigma = \mathrm{id}_{F(\theta,\gamma)}$. Since

$$(\sigma\big|_{F(\theta)}, \sigma\big|_{F(\gamma)} = \Psi(\sigma) = (\mathrm{id}_{F(\theta)}, \mathrm{id}_{F(\gamma)}),$$

we have $\sigma\big|_{F(\theta)} = \mathrm{id}_{F(\theta)}$ and $\sigma\big|_{F(\gamma)} = \mathrm{id}_{F(\gamma)}$. A basis of $F(\theta)$ over F is given by $\{1, \theta, \ldots, \theta^{d-1}\}$ and if $q(x)$ is the minimal polynomial of γ over $F(\theta)$ and $\deg(q(x)) = t$, then a basis of $F(\theta, \gamma)$ over $F(\theta)$ is given by $\{1, \gamma, \ldots, \gamma^{t-1}\}$. It follows that a basis of $F(\gamma, \theta)$ over F is given by the set

$$B = \{\theta^i\gamma^j \mid 0 \leq i \leq d-1, 0 \leq j \leq t-1\}.$$

Since

$$\sigma(\theta) = \sigma\big|_{F(\theta)}(\theta) = \mathrm{id}_{F(\theta)}(\theta) = \theta$$

and similarly $\sigma(\gamma) = \gamma$, we have that σ acts as the identity on the F-basis B of $F(\theta, \gamma)$. Since by assumption we have that σ acts as the identity on F, we conclude that $\sigma = \mathrm{id}_{F(\theta,\gamma)}$.

We have shown that Ψ is an injective group homomorphism. By assumption the groups $\mathrm{Gal}(F(\theta)/F)$ and $\mathrm{Gal}(F(\gamma)/F)$ are abelian, and so their product $\mathrm{Gal}(F(\theta)/F) \times \mathrm{Gal}(F(\gamma)/F)$ is abelian. Hence $\Psi(\mathrm{Gal}(F(\theta,\gamma)/F))$ is abelian as it is the subgroup of an abelian group. Since Ψ is injective, we obtain that $\mathrm{Gal}(F(\theta,\gamma)/F) \cong \Psi(\mathrm{Gal}(F(\theta,\gamma)))$ is abelian as required.

Problem 8. (Exercise 18.2.3 in the book.) Let p be a prime and let F be a field. Prove that $x^p - b \in F[x]$ is reducible if and only if its splitting field is F or $F(\omega)$ according to whether $\mathrm{char}(F) = p$ or $\mathrm{char}(F) \neq p$, where ω is a primitive p-th root of unity.

Solution. Let E be the splitting field of $x^p - b$ over F. Let $\alpha \in E$ be a root of $x^p - b$. We consider the cases $\mathrm{char}(F) = p$ and $\mathrm{char}(F) \neq p$ separately.

Case $\mathrm{char}(F) = p$. Then $b = \alpha^p$ and so $x^p - b = x^p - \alpha^p = (x - \alpha)^p$ since $\mathrm{char}(F) = p$. Hence if $E = F$ we have that $x - \alpha \in F[x]$ divides $x^p - b$ and so $x^p - b$ is reducible. For the other direction assume that $x^p - b \in F[x]$ is reducible. Since $x^p - b = (x - \alpha)^r$ in $E[x]$ and $x^p - b$ is reducible over F, we conclude that $(x - \alpha)^r$ divides $\big|$ $x^p - b$ in $F[x]$ for some $1 \leq r < p$. Then $(x - \alpha)^r \in F[x]$. The constant term of $(x - \alpha)^r$ is $-r\alpha$ and so $-r\alpha \in F[x]$. Since $1 \leq r < p = \mathrm{char}(F)$, we conclude that $\alpha \in F$. Therefore F contains all the roots of $x^p - b$ and hence $E = F$ is the splitting field of $x^p - b$.

Case $\text{char}(F) \neq p$. Assume first that $E = F(\omega)$ and we show that $x^p - b$ is reducible. Assume to a contradiction that $x^p - b$ is irreducible. Since $E = F(\omega)$ is the splitting field of $x^p - b$, we have that $F(\sqrt[p]{b}) \subseteq F(\omega)$, since $\sqrt[p]{b}$ is a root of $x^p - b$. On the other hand, since $x^p - b$ is irreducible and monic and $\sqrt[p]{b}$ is a root of $x^p - b$, we have that $x^p - b$ is the minimal polynomial of b over F. Then

$$[F(\sqrt[p]{b}) : F] = \deg(x^p - b) = p.$$

On the other hand, since $x^p - 1 = (x-1)(x^{p-1} + \cdots + x + 1)$, we have that ω is a root of $x^{p-1} + \cdots + x + 1$. It follows that

$$[F(\omega) : F] \leq \deg(x^{p-1} + \cdots + x + 1) \leq p - 1.$$

Now, using $F \subseteq F(\sqrt[p]{b}) \subseteq F(\omega)$, we get

$$p - 1 \geq [F(\omega) : F] = [F(\omega) : F(\sqrt[p]{b})][F(\sqrt[p]{b}) : F] \geq 1 \cdot p = p,$$

which is a contradiction. Hence $x^p - b$ is reducible.

Now assume that $x^p - b$ is reducible and let ω be a primitive p-th root of unity. We show that $E = F(\omega)$. Let $\alpha = \sqrt[p]{b}$ be a root of $x^p - b$. Then the roots of $x^p - b$ are $\alpha, \omega\alpha, \ldots, \omega^{p-1}\alpha$. In particular we have that $F(\omega) \subseteq E$. Hence to show that $E = F(\omega)$ it is enough to show that $x^p - b$ splits in $F(\omega)$. Since $x^p - b$ is reducible, there exists a polynomial $f(x) \in F[x]$ with $\deg(f(x)) = k \geq 1$ and $f(x) \mid (x^p - b)$. Since

$$x^p - b = \prod_{i=0}^{p-1} (x - \omega^i \alpha),$$

it follows that there exist $i_1, \ldots, i_k \in \{0, 1, \ldots, p-1\}$ such that

$$f(x) = (x - \omega^{i_1}\alpha)(x - \omega^{i_2}\alpha) \cdots (x - \omega^{i_k}\alpha).$$

In particular the constant term of $f(x)$ is

$$u = (-1)^k \alpha^k \omega^{i_1 + i_2 + \cdots + i_k}$$

and we have $u \in F$ since $f(x) \in F[x]$. Then $\omega^{i_1 + i_2 + \cdots + i_k} = \omega^d$ for some $d \in \{0, \ldots, p-1\}$. Therefore $u = \alpha^k \omega^d$ and so

$$u^p = (\alpha^k \omega^d)^p = (\alpha^p)^k (\omega^p)^d = b^k.$$

Now let $s, t \in \mathbb{Z}$ be such that $ks + pt = 1$. Then

$$b = b^{ks+pt} = u^{ps} b^{pt} = (u^s b^t)^p.$$

Since $u \in F$ and $b \in F$ we have that $u^s b^t \in F$. But then $u^s b^t$ is a root of $x^p - b$ and so there exists a $j \in \{0, \ldots, p-1\}$ such that $u^s b^t = \omega^j \alpha$. Hence $\omega^j \alpha \in F$. Since $F(\omega)$ contains all the roots of $x^p - b$, it follows that $x^p - b$ splits in $F(\omega)$ as required.

Extra problems

The following problems may be a bit more challenging, in case you feel like you need something more.

Problem 9. (a) Show that for every $n \in \mathbb{Z}$, $n \geq 1$ we have

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x),$$

where $\Phi_d(x)$ is the d-th cyclotomic polynomial. Conclude that the constant term of $\Phi_n(x)$ is ± 1.

(b) Let $n \in \mathbb{Z}$, $n \geq 1$. Let $p \geq 2$. Show that if $p \mid \Phi_n(\alpha)$, then $p \nmid \alpha$.

(c) Let $n \in \mathbb{Z}$, $n \geq 1$. Let $\alpha \in \mathbb{Z}$ and let p be a prime such that $\gcd(p, n) = 1$. Show that p divides $\Phi_n(\alpha)$ if and only if the order of $\overline{\alpha} \in \mathbb{Z}_p^\times$ is n.

(d) (Special case of Dirichlet's theorem) Show that for any $n \geq 1$ there are infinitely many prime numbers p such that $n \mid (p-1)$.

(e) Let G be a finite abelian group. Show that there exists a Galois extension E of $\mathbb{Q}$ such that $\mathrm{Gal}(E/\mathbb{Q}) \cong G$.

Solution.

(a) For $n = 1$ the claim is clear. Assume $n \geq 2$. We first show the equality of the two polynomials. Since both polynomials $x^n - 1$ and $\prod_{d|n} \Phi_d(x)$ are monic, it is enough to show that they have exactly the same roots. Let α be a root of $x^n - 1$ and we show that α is a root of $\prod_{d|n} \Phi_d(x)$. Since α is a root of $x^n - 1$, it follows that α is an n-th root of unity. Let d be the smallest positive integer such that $\alpha^d = 1$. Then α is a primitive d-th root of unity, and so α is a root of $\Phi_d(x)$. For the other direction, let ω be a root of $\prod_{d|n} \Phi_d(x)$. Then ω is a root of $\Phi_d(x)$ for some $d \mid n$. In particular, $\omega^n = 1$ and so ω is a root of $x^n - 1$ as well.

We now show that the constant term of $\Phi_n(x)$ is ± 1. We use induction on the number of prime factors of n. If there is only one prime factor, then the claim follows by Example 14.10(2). For the induction step, we have

$$x^n - 1 = \prod_{d|n} \Phi_d(x) = \Phi_n(x) \prod_{d|n, d<n} \Phi_d(x).$$

If $d \mid n$ and $d < n$, then d has strictly less prime factors than n. Hence the terms $\Phi_d(x)$ with $d \mid n$ and $d < n$ have constant coefficient ± 1 by induction assumption. If a is the constant coefficient of $\Phi_n(x)$, then the constant coefficient of the right hand side in the above equality is $\pm a$ and the constant coefficient on the left hand side is -1. It follows that $a = \pm 1$.

(b) Assume to a contradiction that $p \mid \alpha$. Since by part (a) we have that the constant term of $\Phi_n(\alpha)$ is 1, we conclude that p divides $\Phi_n(\alpha) - 1$. But then $p \mid \Phi_n(\alpha)$ and $p \mid (\Phi_n(\alpha) - 1)$ implies that $p \mid \gcd(\Phi_n(\alpha), \Phi_n(\alpha) - 1) = 1$, which is a contradiction since $p \geq 2$.

(c) Notice first that if $p \mid \Phi_n(\alpha)$ then $\overline{\alpha} \in \mathbb{Z}_p^\times$ by part (a). Now let l be the order of $\overline{\alpha} \in \mathbb{Z}_p^\times$. Set $f(x) = x^n - 1$ and $g(x) = x^l - 1$. We write $\overline{f}(x)$ for the polynomial $f(x)$ as a polynomial in $\mathbb{Z}_p[x]$ and similarly for other polynomials. Then

$$\overline{f}(x)' = (x^n - \overline{1})' = \overline{n}x^{n-1}$$

and since p does not divide n, we have that $\overline{f}(x)'$ is nonzero for $x \neq 0$. Since 0 is not a root of $\overline{f}(x)$, it follows by Theorem 9.3 that $\overline{f}(x)$ has only simple roots. By part (a) we have that

$$\overline{f}(x) = \prod_{d|n} \overline{\Phi_d}(x) \text{ and } \overline{g}(x) = \prod_{d|l} \overline{\Phi_d}(x). \tag{1}$$

Now assume first that $\overline{\Phi_n}(\overline{\alpha}) = 0$. Hence $\overline{\alpha}$ is a root of $\overline{f}(x)$ and so $\overline{\alpha}^n = \overline{1}$. Since the order of $\overline{\alpha} \in \mathbb{Z}_p^\times$ is l, we obtain that $l \mid n$. On the other hand, since the order of $\overline{\alpha} \in \mathbb{Z}_p^\times$ is l, we have that $\overline{\alpha}^l = \overline{1}$. In particular, $\overline{\alpha}$ is a root of $\overline{g}(x) \in \mathbb{Z}_p[x]$. By (1) we have that there exists some $d' \mid l$ such that $\overline{\alpha}$ is a root of $\overline{\Phi_{d'}}(x)$. Hence $\overline{\alpha}$ is a root of both $\overline{\Phi_n}(x)$ and of $\overline{\Phi_{d'}}(x)$ and moreover $d' \mid n$ since $d' \mid l$ and $l \mid n$. Hence by (1) we have that if $d' < n$, then $\overline{\alpha}$ is a double root of $\overline{f}(x)$. Since $\overline{f}(x)$ has only simple roots, we obtain $d' = n$. Then $n = d' \leq l \leq n$ implies $l = n$, as required.

Now assume that $l = n$. Then $\overline{\alpha}$ is a root of $\overline{f}(x)$ and so by (1) we have that $\overline{\alpha}$ is a root of $\overline{\Phi_{d'}}(x)$ for some $d' \mid n$. Set $h(x) = x^{d'} - 1$. Then $\overline{\alpha}$ is also a root of $\overline{h}(x) = \prod_{d|d'} \overline{\Phi_d}(x)$. Hence $\overline{\alpha}^{d'} = \overline{1}$, which implies that $n \mid d'$ since the order of $\overline{\alpha}$ is n. Since both $d' \mid n$ and $n \mid d'$ hold, we conclude that $n = d'$. Since $\overline{\alpha}$ is a root of $\overline{\Phi_{d'}}(x) = \overline{\Phi_n}(x)$, we conclude that $p \mid \Phi_n(\alpha)$.

(d) For $n = 1$ there is nothing to show. Let $n \geq 2$. Assume to a contradiction that there exist only finitely many such primes, say $p_1, \ldots, p_k$. Set $P = p_1 \cdots p_k$. Since $\Phi_n(x)$ is a monic polynomial, we have

$$\lim_{t \to \infty} \Phi_n(tnP) = \infty.$$

Hence there exists t such that $\Phi_n(tnP) > 1$. Since $\Phi_n(tnP) > 1$, there exists a prime number p such that $p \mid \Phi_n(tnP)$. By part (b) we have that $p \nmid tnP$. In particular, we have that $p \nmid n$. Then it follows by part (c) that the order of $\overline{\Phi(ntP)} \in \mathbb{Z}_p^\times$ is n. Since the order of $\mathbb{Z}_p^\times$ is $p-1$, we obtain that $n \mid p-1$. Hence $p = p_j$ for some $j \in \{1, \ldots, k\}$. But then $p \mid tnP$, which contradicts $p \nmid tnP$.

(e) Since G is a finite abelian group, by the fundamental theorem of finite abelian groups (Theorem 8.3.1 in the book) we have that there exist positive integers $m_1, \cdots, m_k \in \mathbb{Z}$ such that

$$G \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_t}.$$

By part (d) there exist distinct prime numbers $p_1, \ldots, p_t$ such that $m_i \mid (p_i - 1)$. Write $k_i = \frac{p_i - 1}{m_i}$. Since p_i is a prime number, the multiplicative group of units $\mathbb{Z}_{p_i}^\times$ is cyclic of order $p_i - 1$. Hence

$$\mathbb{Z}_{p_i}^\times \cong \mathbb{Z}_{p_i - 1}.$$

We pick an isomorphism $\phi_i : \mathbb{Z}_{p_i}^\times \to \mathbb{Z}_{p_i-1}$. Since k_i divides $p_i - 1$, it follows that there exists a subgroup H_i of $\mathbb{Z}_{p_i-1}$ of order k_i (Theorem 4.4.4. in the book). Then $\mathbb{Z}_{p_i-1}/H_i$ is isomorphic to $\mathbb{Z}_{\frac{p_i-1}{k_i}} = \mathbb{Z}_{m_i}$. Set $V_i \coloneqq \phi_i^{-1}(H_i)$. Then V_i is a subgroup of $\mathbb{Z}_{p_i}^\times$ and we have

$$\mathbb{Z}_{p_i}^\times / V_i \cong \mathbb{Z}_{p_i-1}/H_i \cong \mathbb{Z}_{m_i}. \tag{2}$$

On the other hand, notice that for any rings R_1, R_2 we have that $(R_1 \times R_2)^\times \cong R_1^\times \times R_2^\times$. Hence we have

$$\mathbb{Z}_{p_1}^\times \times \cdots \times \mathbb{Z}_{p_t}^\times \cong (\mathbb{Z}_{p_1} \times \cdots \mathbb{Z}_{p_t})^\times \cong \mathbb{Z}_{p_1 \cdots p_t}^\times, \tag{3}$$

where the last isomorphism follows since all of the primes $p_1, \ldots, p_t$ are distinct. Set $m = p_1 \cdots p_t$ and pick an isomorphism $\psi_i : \mathbb{Z}_{p_1}^\times \times \cdots \times \mathbb{Z}_{p_t}^\times \to \mathbb{Z}_m^\times$. Set $U \coloneqq \psi(V_1 \times \cdots \times V_t)$. Using (2) and (3) we have

$$\begin{aligned} G &\cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_t} \\ &\cong (\mathbb{Z}_{p_1}^\times / V_1) \times \cdots \times (\mathbb{Z}_{p_t}^\times / V_t) \\ &\cong (\mathbb{Z}_{p_1}^\times \times \cdots \times \mathbb{Z}_{p_t}^\times)/(V_1 \times \cdots \times V_t) \\ &\cong \mathbb{Z}_m^\times / U. \end{aligned}$$

Now let ω be a primitive m-th root of unity. By Theorem 14.12 we know that $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong \mathbb{Z}_m^\times$. We pick an isomorphism $\chi : \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \to \mathbb{Z}_m^\times$. Set $W \coloneqq \chi^{-1}(U)$. Since $\mathbb{Z}_m^\times$ is abelian, the subgroup $U < \mathbb{Z}_m^\times$ is a normal subgroup. Hence $W \lhd \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}))$ is a normal subgroup as well. Since $\mathbb{Q} \subseteq \mathbb{Q}(\omega)$ is a Galois extension, we may apply the FTGT. By the FTGT(2) we have that $W = \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}(\omega)_W)$. By the FTGT(5) it follows that $\mathbb{Q} \subseteq \mathbb{Q}(\omega)_W$ is a normal extension and hence a Galois extension. We set $E = \mathbb{Q}(\omega)_W$. Then by the FTGT(6) we have

$$\mathrm{Gal}(E/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\omega)_W/\mathbb{Q}) \cong \frac{\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})}{\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}(\omega)_W)} \cong \frac{\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})}{W} \cong \frac{\mathbb{Z}_m^\times}{U} \cong G,$$

as required.

Problem 10. Let $F \subseteq E$ be a Galois extension with Galois group G. As in Problem 6, for any $\alpha \in E$ define the norm of α in E over F via

$$N_{E/F}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha).$$

(a) Find $n \in \mathbb{Z}$ such that $i \in \mathbb{Q}(\omega)$, where $\omega \in \mathbb{C}$ is a primitive n-th root of unity.

(b) Show that $\sqrt{2} \in \mathbb{Q}(\omega)$ where $\omega \in \mathbb{C}$ is a primitive 8-th root of unity.

(c) Let $p \geq 3$ be a prime number. Let $\omega \in \mathbb{C}$ be a primitive p-th root of unity.

  (i) Show that $N_{\mathbb{Q}(\omega)/\mathbb{Q}}(-1) = 1$, $N_{\mathbb{Q}(\omega)/\mathbb{Q}}(p) = p^{p-1}$, $N_{\mathbb{Q}(\omega)/\mathbb{Q}}(\omega) = 1$ and $N_{\mathbb{Q}(\omega)/\mathbb{Q}}(1-\omega) = p$.

  (ii) Show that $N_{\mathbb{Q}(\omega)/\mathbb{Q}}(\Phi_p'(\omega)) = p^{p-2}$.

  (iii) Show that the *discriminant* $\Delta := \prod_{1 \leq i < j \leq p-1} (\omega^i - \omega^j)^2$ satisfies $\Delta = (-1)^{\frac{p-1}{2}} p^{p-2}$.

  (iv) Show that if $p \equiv 1 \mod 4$, then $\sqrt{p} \in \mathbb{Q}(\omega)$, while if $p \equiv 3 \mod 4$, then $i\sqrt{p} \in \mathbb{Q}(\omega)$.

(d) Let $n, m \geq 1$. Let $\omega_n \in \mathbb{C}$ be a primitive n-th root of unity and $\omega_m \in \mathbb{C}$ be a primitive m-th root of unity. Let $l = \operatorname{lcm}(n, m)$ and let $\omega_l \in \mathbb{C}$ be a primitive l-th root of unity. Show that $\mathbb{Q}(\omega_n, \omega_m) = \mathbb{Q}(\omega_l)$.

(e) Let $k \in \mathbb{Z}$ be an integer. Show that there exists an $n \in \mathbb{Z}$, $n \geq 1$ such that $\sqrt{k} \in \mathbb{Q}(\omega_n)$ where ω_n is a primitive n-th root of unity.

Solution.

(a) Notice that $i^4 = 1$. Hence i is a primitive 4-th root of unity and hence $i \in \mathbb{Q}(i)$.

(b) We have that $\omega = e^{\frac{2\pi i}{8}} = e^{\frac{\pi i}{4}}$. In particular we have

$$\omega^2 = e^{\frac{\pi i}{2}} = \cos\tfrac{\pi}{2} + i \sin\tfrac{\pi}{2} = i.$$

Then

$$\omega = e^{\frac{\pi i}{4}} = \cos\tfrac{\pi}{4} + i\sin\tfrac{\pi}{4} = \frac{1}{\sqrt{2}} + i\frac{\sqrt{2}}{2} = \sqrt{2}\left(\frac{1+i}{2}\right) = \sqrt{2}\left(\frac{1+\omega^2}{2}\right).$$

Hence

$$\sqrt{2} = \frac{2\omega}{1+\omega^2} \in \mathbb{Q}(\omega),$$

as required.

(c) Recall that the set $\{\omega^i \mid 1 \leq i \leq p-1\}$ is the set of all primitive p-th roots of unity. Moreover, by Theorem 14.2 we have that $\operatorname{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) = \{\sigma_i \mid 1 \leq i \leq p-1\}$ where $\sigma_i(\omega) = \omega^i$.

  (i) We have

$$N_{\mathbb{Q}(\omega)/\mathbb{Q}}(-1) = \prod_{i=1}^{p-1} \sigma_i(-1) = \prod_{i=1}^{p-1}(-1) = (-1)^{p-1} = 1,$$

since p is odd. Similarly we have

$$N_{\mathbb{Q}(\omega)/\mathbb{Q}}(p) = \prod_{i=1}^{p-1} \sigma_i(p) = \prod_{i=1}^{p-1} p = p^{p-1}.$$

Moreover we compute

$$N_{\mathbb{Q}(\omega)/\mathbb{Q}}(\omega) = \prod_{i=1}^{p-1} \sigma_i(\omega) = \prod_{i=1}^{p-1} \omega^i = \omega^{\sum_{i=1}^{p-1} i} = \omega^{\frac{p(p-1)}{2}} = 1.$$

Recall that by the definition of $\Phi_p(x)$ we have

$$\Phi_p(x) = \prod_{i=1}^{p-1}(x - \omega^i).$$

Notice that since p is prime, we have in particular by Example 14.10(2) that

$$\Phi_p(x) = 1 + x + x^2 + \cdots + x^{p-1}.$$

Hence we can compute

$$\prod_{i=1}^{p-1}(1-\omega^i) = \Phi_p(1) = 1 + 1 + 1^2 + \cdots + 1^{p-1} = p.$$

Therefore, we have

$$N_{\mathbb{Q}(\omega)/\mathbb{Q}}(1-\omega) = \prod_{i=1}^{p-1}\sigma_i(1-\omega) = \prod_{i=1}^{p-1}(1-\sigma_i(\omega)) = \prod_{i=1}^{p-1}(1-\omega^i) = p.$$

(ii) We have $\Phi_p(x) = \frac{x^p-1}{x-1}$. Therefore, we have $(x-1)\Phi_p(x) = x^p - 1$. By taking derivatives we obtain

$$\Phi_p(x) + (x-1)\Phi_p'(x) = px^{p-1}.$$

Then evaluating at ω we have

$$\Phi_p(\omega) + (\omega-1)\Phi_p'(\omega) = p\omega^{p-1}.$$

Notice that $\Phi_p(\omega) = 0$. By applying $N_{\mathbb{Q}(\omega)/\mathbb{Q}}$ in both sides and using the fact that $N_{\mathbb{Q}(\omega)/\mathbb{Q}}$ is multiplicative by Problem 6(c), we obtain

$$N_{\mathbb{Q}(\omega)/\mathbb{Q}}(-1)N_{\mathbb{Q}(\omega)/\mathbb{Q})}(1-\omega)N_{\mathbb{Q}(\omega)/\mathbb{Q}}(\Phi_p'(\omega)) = N_{\mathbb{Q}(\omega)/\mathbb{Q}}(p)N_{\mathbb{Q}(\omega)/\mathbb{Q}}(\omega)^{p-1}.$$

Using part (c)(i) we have

$$1 \cdot p \cdot N_{\mathbb{Q}(\omega)/\mathbb{Q}}(\Phi_p'(\omega)) = p^{p-1} \cdot 1^{p-1}$$

and so

$$N_{\mathbb{Q}(\omega)/\mathbb{Q}}(\Phi_p'(\omega)) = p^{p-2}.$$

(iii) We have

$$\prod_{1\le i<j\le p-1}(\omega^i-\omega^j)^2 = \prod_{1\le i<j\le p-1}(\omega^i-\omega^j)(\omega^i-\omega^j) = \prod_{1\le i<j\le p-1}(-1)(\omega^i-\omega^j)(\omega^j-\omega^i)$$
$$= (-1)^{\frac{(p-2)(p-1)}{2}}\prod_{1\le i<j\le p-1}(\omega^i-\omega^j)(\omega^j-\omega^i) = (-1)^{\frac{p-1}{2}}\prod_{i\neq j}(\omega^i-\omega^j).$$

Hence it is enough to show that $\prod_{i\neq j}(\omega^i-\omega^j) = p^{p-2}$. Since

$$\Phi_p(x) = \prod_{i=1}^{p-1}(x-\omega^i),$$

we have

$$\Phi_p'(x) = \prod_{\substack{i=1\\ i\neq 1}}^{p-1}(x-\omega^i) + \prod_{\substack{i=1\\ i\neq 2}}^{p-1}(x-\omega^i) + \cdots + \prod_{\substack{i=1\\ i\neq p-1}}^{p-1}(x-\omega^i).$$

Then evaluating at ω^k for $1 \le k \le p-1$ we have

$$\Phi_p'(\omega^k) = \prod_{\substack{i=1\\ i\neq k}}^{p-1}(\omega^k-\omega^i).$$

Hence

$$\prod_{k=1}^{p-1} \Phi_p'(\omega^k) = \prod_{k=1}^{p-1} \prod_{\substack{i=1 \\ i \neq k}}^{p-1} (\omega^k - \omega^i) = \prod_{i \neq j} (\omega^j - \omega^i)$$

Hence it is enough to show that $\prod_{k=1}^{p-1} \Phi_p'(\omega^k) = p^{p-2}$. By part (c)(ii) and since $\Phi_p'(x) \in \mathbb{Q}[x]$ we have

$$p^{p-2} = N_{\mathbb{Q}(\omega)/\mathbb{Q}}(\Phi_p'(\omega)) = \prod_{k=1}^{p-1} \sigma_k(\Phi_p'(\omega)) = \prod_{k=1}^{p-1} \Phi_p'(\sigma_k(\omega)) = \prod_{k=1}^{p-1} \Phi_p'(\omega^k),$$

as required.

(iv) First notice that we have

$$\sqrt{\Delta} = \sqrt{\prod_{1 \le i < j \le p-1} (\omega^i - \omega^j)^2} = \prod_{1 \le i < j \le p-1} \sqrt{(\omega^i - \omega^j)^2} = \prod_{1 \le i < j \le p-1} (\omega^i - \omega^j) \in \mathbb{Q}(\omega).$$

Moreover, notice that since $p \ge 3$ is odd, $p^{\frac{p-3}{2}}$ is an integer. In particular $p^{\frac{p-3}{2}} \in \mathbb{Q}(\omega)$.
Assume now that $p \equiv 1 \mod 4$. Then $\frac{p-1}{2}$ is even and so by (c)(iii) we have $\Delta = p^{p-2}$. Then

$$\sqrt{p} = p^{\frac{1}{2}} = \frac{p^{\frac{p-2}{2}}}{p^{\frac{p-3}{2}}} = \frac{\sqrt{\Delta}}{p^{\frac{p-3}{2}}}$$

which is in $\mathbb{Q}(\omega)$ since both $\sqrt{\Delta} \in \mathbb{Q}(\omega)$ and $p^{\frac{p-3}{2}} \in \mathbb{Q}(\omega)$ hold.
Assume now that $p \equiv 3 \mod 4$. Then $\frac{p-1}{2}$ is odd and so by (c)(iii) we have $\Delta = -p^{p-2}$. In particular, we have $\sqrt{\Delta} = i\sqrt{p^{p-2}}$ and so

$$i\sqrt{p} = ip^{\frac{1}{2}} = \frac{ip^{\frac{p-2}{2}}}{p^{\frac{p-3}{2}}} = \frac{\sqrt{\Delta}}{p^{\frac{p-3}{2}}},$$

which similarly is in $\mathbb{Q}(\omega)$.

(d) We have

$$\omega_n^l = \omega_n^{n\frac{l}{n}} = (\omega_n^n)^{\frac{l}{n}} = 1^{\frac{l}{n}} = 1,$$

and so ω_n is an l-th root of unity. Hence $\omega_n \in \mathbb{Q}(\omega_l)$. Similarly we obtain $\omega_m \in \mathbb{Q}(\omega_l)$ and so we have $\mathbb{Q}(\omega_n, \omega_m) \subseteq \mathbb{Q}(\omega_l)$.

For the other inclusion, by Bezout's identity there exist $x, y \in \mathbb{Z}$ such that $xn + ym = \gcd(n, m)$. Using the identity $nm = \operatorname{lcm}(n, m)\gcd(n, m)$, we obtain

$$\frac{1}{l} = \frac{1}{\operatorname{lcm}(n, m)} = \frac{\gcd(n, m)}{nm} = \frac{xn + ym}{nm}.$$

We may choose $\omega_n = e^{\frac{2\pi i}{n}}$, $\omega_m = e^{\frac{2\pi i}{m}}$ and $\omega_l = e^{\frac{2\pi i}{l}}$. Then

$$\omega_n^y \omega_m^x = e^{\frac{2\pi i y}{n}} e^{\frac{2\pi i x}{m}} = e^{2\pi i\left(\frac{y}{n} + \frac{x}{m}\right)} = e^{2\pi i \frac{ym + xn}{nm}} = e^{\frac{2\pi i}{l}} = \omega_l$$

is a primitive l-th root of unity. Hence $\omega_l = \omega_n^y \omega_m^x \in \mathbb{Q}(\omega_n, \omega_m)$, and so $\mathbb{Q}(\omega_l) \subseteq \mathbb{Q}(\omega_n, \omega_m)$, which proves the claim.

(e) Let us first assume that $k \geq 0$. If $k = 0$ or $k = 1$ the claim is clear. Assume that $k \geq 2$. We use induction on the number M of prime factors of k. For the base case $M = 1$ we have that $k = p$ is prime. If $p = 2$, then we have that $\sqrt{p} \in \mathbb{Q}(\omega_8)$ by part (b). If $p \equiv 1 \mod 4$, then we have that $\sqrt{p} \in \mathbb{Q}(\omega_p)$ by part (c)(iv). If $p \equiv 3 \mod 4$, then we have that $i\sqrt{p} \in \mathbb{Q}(\omega_p)$ and so $\sqrt{p} = -i^2\sqrt{p} \in \mathbb{Q}(\omega_p, i)$. Since $i = \omega_4$ is a primitive 4-th root of unity and since $\text{lcm}(4, p) = 4p$, we have by part (d) that $\mathbb{Q}(\omega_p, i) = \mathbb{Q}(\omega_{4p})$. Hence in this case $\sqrt{p} \in \mathbb{Q}(\omega_{4p})$ and so the base case is proved.

For the induction step assume that k has M prime factors. Then $k = Kp$ where K has $M - 1$ prime factors and p is a prime number. By induction assumption we have that $\sqrt{K} \in \mathbb{Q}(\omega_N)$ for some $N \in \mathbb{Z}$ and also that $\sqrt{p} \in \mathbb{Q}(\omega_{N'})$ for some $N' \in \mathbb{Z}$. Then by part (d) we have

$$\sqrt{k} = \sqrt{Kp} = \sqrt{K}\sqrt{p} \in \mathbb{Q}(\omega_N, \omega_{N'}) = \mathbb{Q}(\omega_{\text{lcm}(N,N')}),$$

which proves the induction step.

Finally assume that $k < 0$. Then $-k > 0$ and so there exists an $N \in \mathbb{Z}$ such that $\sqrt{-k} \in \mathbb{Q}(\omega_N)$. Then again by part (d) we have

$$\sqrt{k} = i\sqrt{-k} \in \mathbb{Q}(i, \omega_N) = \mathbb{Q}(\omega_4, \omega_N) = \mathbb{Q}(\omega_{\text{lcm}(4,N)}),$$

which completes the proof.