Q1 Prove the following statements.

(a) $\overline{\mathbb{Q}}/\mathbb{Q}$ is Galois.

Proof. Since $\operatorname{char}\mathbb{Q} = 0$, then every algebraic extension of $\mathbb{Q}$ is separable; in particular, $\overline{\mathbb{Q}}/\mathbb{Q}$ is separable. Given any $\alpha \in \overline{\mathbb{Q}}$,

$$m_{\alpha,\mathbb{Q}}(x) \in \mathbb{Q}[x] \subseteq \overline{\mathbb{Q}}[x].$$

Since $\overline{\mathbb{Q}}$ is algebraically closed, $m_{\alpha,\mathbb{Q}}(x)$ splits completely over $\overline{\mathbb{Q}}[x]$. Therefore, $\overline{\mathbb{Q}}/\mathbb{Q}$ is normal, hence, Galois.

□

(b) If F is a finite field, then every algebraic extension of F is Galois.

Proof. Let K/F be an algebraic extension. Given $\alpha \in K$, $F(\alpha)/F$ is a finite extension.

Since finite fields are perfect, then $F(\alpha)/F$ is separable. So α is separable over F, implying K/F is separable.

Since F is finite, then $F \cong \mathbb{F}_{p^n}$ for some prime p and positive integer n. Likewise, $F(\alpha) \cong \mathbb{F}_{p^m}$ for some multiple m of n. Then $\mathbb{F}_{p^m}/\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^n}/\mathbb{F}_p$ are algebraic extensions, with $\mathbb{F}_{p^m}$ defined to be the splitting field of $x^{p^m} - x$ over $\mathbb{F}_p$. Therefore, $\mathbb{F}_{p^m}/\mathbb{F}_p$ is a normal extension, implying that $\mathbb{F}_{p^m}/\mathbb{F}_{p^n}$ is also normal (by Q2(a)). Correspondingly, $F(\alpha)/F$ is normal, which means that $m_{\alpha,F}(x)$ splits completely over $(F(\alpha))[x] \subseteq K[x]$. Hence, K/F is normal.

As a separable and normal extension, K/F is Galois.

□

(c) $\overline{\mathbb{F}_p(t)}/\mathbb{F}_p(t)$ is not Galois.

Proof. We claim that $\overline{\mathbb{F}_p(t)}/\mathbb{F}_p(t)$ is not separable; in particular, that $x^p - t$ is irreducible in $(\mathbb{F}_p(t))[x]$, yet is not separable. Clearly, $x^p - t$ is not separable, since if $\alpha \in \overline{\mathbb{F}_p(t)}$ is a root, then

$$x^p - t = x^p - \alpha^p = (x - \alpha)^p.$$

We can consider $\mathbb{F}_p(t)$ to be the field of fractions for the UFD $\mathbb{F}_p[t]$. Then $x^p - t \in (\mathbb{F}_p[t])[x]$ and the gcd of its coefficients is 1, implying that $x^p - t$ is irreducible in $(\mathbb{F}_p(t))[x]$ if and only if it is irreducible in $(\mathbb{F}_p[t])[x]$. And indeed, Eisenstein's criterion tells us that $x^p - t$ is irreducible in $(\mathbb{F}_p[t])[x]$, since all the coefficients are in the prime ideal (t) of $\mathbb{F}_p[t]$, but $t \notin (t)^2$. Hence, $x^p - t$ is a monic irreducible polynomial in $(\mathbb{F}_p(t))[x]$, so it is the minimal polynomial of α over $\mathbb{F}_p(t)$. Thus, $\overline{\mathbb{F}_p(t)}/\mathbb{F}_p(t)$ is not Galois.

□

Q2 Let K/F and L/K be algebraic extensions.

(a) Show that if L/F is normal, then L/K is normal.

Proof. Assume L/F is normal. Given $\alpha \in L$, consider $m_{\alpha,K}(x) \in K[x]$. Since $m_{\alpha,F}(x) \in F[x] \subseteq K[x]$ and has α as a root, then $m_{\alpha,K}(x)$ divides $m_{\alpha,F}(x)$. Since $m_{\alpha,F}(x)$ splits completely in $L[x]$, then L contains all the roots of $m_{\alpha,F}(x)$, which includes all the roots of $m_{\alpha,K}(x)$. Therefore, $m_{\alpha,K}(x)$ splits completely in $L[x]$, implying L/K is normal.

□

(b) Show that if L/F is Galois, then L/K is Galois.

Proof. Assume L/F is Galois. In particular, L/F is normal, so Q1(a) gives L/K is normal. Moreover, L/F is separable, which is the case if and only if L/K and K/F are separable. Therefore, L/K is separable and normal, hence, Galois.

□

Q3 Let $\zeta_p = e^{2\pi i/p}$, a primitive p-th root of unity. Show that $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is Galois and $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$.

Proof. Since $\mathbb{Q}(\zeta_p)$ is the splitting field of the separable polynomial $x^p - 1$ over $\mathbb{Q}$, then $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is Galois, so

$$|\operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})| = [\mathbb{Q}(\zeta_p) : \mathbb{Q})] = p - 1.$$

An automorphism of $\mathbb{Q}(\zeta_p)$ fixing $\mathbb{Q}$ is completely determined by the image of ζ_p, which must be another primitive root of unity. Consider the map

$$\begin{aligned} \varphi : (\mathbb{Z}/p\mathbb{Z})^\times &\to \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \\ \overline{n} &\mapsto (\sigma_n : \zeta_p \mapsto \zeta_p^n). \end{aligned}$$

We check that this map is well-defined on the equivalence classes. If $\overline{n} = \overline{m}$, then $n = m + pq$ for some integer q. Then

$$\zeta_p^n = \zeta_p^{m+pq} = e^{2\pi im/p + 2\pi ipq/p} = \zeta_p^m,$$

so $\varphi(\overline{n}) = \sigma_n = \sigma_m = \varphi(\overline{m})$. This map is also well-defined in the codomain, since ζ_p^n is a primitive root of unity for $1 \le n \le p-1$, which is the case if and only if $\overline{n} \in (\mathbb{Z}/p\mathbb{Z})^\times$; that is, each σ_n does in fact define an automorphism on $\mathbb{Q}(\zeta_p)$ fixing $\mathbb{Q}$. We claim φ is an isomorphism of groups.

First, φ is a bijection. As previously mentioned, an element of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is completely determined by the image of ζ_p, which must be another primitive root of unity. All primitive roots of unity are of the form ζ_p^n for $n = 1, \dots, p-1$, and the corresponding automorphism is given by $\varphi(\overline{n})$. Hence, φ is surjective. Since both sets are finite and of the same size, then in fact φ is a bijection.

Lastly, φ is a group homomorphism:

$$\varphi(nm) = \varphi(mn) = \left(\sigma_{mn} : \zeta_p \mapsto \zeta_p^{mn}\right) = \left(\sigma_n \circ \sigma_m : \zeta_p \mapsto (\zeta_p^m)^n\right) = \varphi(n) \circ \varphi(m).$$

Thus, φ is in fact an isomorphism of groups.

□

Q4 Show that $\mathbb{Q}(\sqrt{2}+\sqrt{5})/\mathbb{Q}$ is Galois and $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}+\sqrt{5})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Proof. Let $K = \mathbb{Q}(\sqrt{2}+\sqrt{5})$. Since $K = \mathbb{Q}(\sqrt{2},\sqrt{5})$ is the splitting fields of the separable polynomial $(x^2-2)(x^2-5)$ over $\mathbb{Q}$, then $K/\mathbb{Q}$ is Galois. Any automorphism on K fixing $\mathbb{Q}$ is completely determined by the images of $\sqrt{2}$ and $\sqrt{5}$, which must map to $\pm\sqrt{2}$ and $\pm\sqrt{5}$, respectively; there are four such maps. Define the map

$$\begin{aligned}\varphi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} &\to \mathrm{Gal}(K/\mathbb{Q}) \\ (\overline{a},\overline{b}) &\mapsto \sigma_{a,b} : \begin{cases} \sqrt{2} \mapsto (-1)^a\sqrt{2} \\ \sqrt{3} \mapsto (-1)^b\sqrt{3} \end{cases}\end{aligned}$$

Then φ is well-defined with respect to both the equivalence classes and the codomain. This map is surjective, as all possible automorphisms of K fixing $\mathbb{Q}$, as described above, are attained. And since the both sets are of the same size, φ is a bijection. Lastly, φ is a group homomorphism:

$$\begin{aligned}\varphi((a,b)+(c,d)) &= \varphi((c+a,d+b)) \\ &= \sigma_{c+a,d+b} : \begin{cases} \sqrt{2} \mapsto (-1)^{c+a}\sqrt{2} \\ \sqrt{3} \mapsto (-1)^{d+b}\sqrt{3} \end{cases} \\ &= \sigma_{a,b} \circ \sigma_{c,d} : \begin{cases} \sqrt{2} \mapsto (-1)^c(-1)^a\sqrt{2} \\ \sqrt{3} \mapsto (-1)^d(-1)^b\sqrt{3} \end{cases} \\ &= \varphi((a,b)) \circ \varphi((c,d)).\end{aligned}$$

Hence, φ is an isomorphism of groups.

□

Q5 Problem 14.2.13 Prove that if the Galois group of the splitting field of a cubic over $\mathbb{Q}$ is the cyclic group of order 3, then all the roots of the cubic are real.

Proof. Suppose K is the splitting field of a cubic polynomial in $\mathbb{Q}[x]$, then $K = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$, where the α's (not necessarily distinct) are the roots of the cubic polynomial. Assume, for contradiction, that not all the α's are real, yet $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$. Then without loss of generality we can assume α_1 is real and α_2, α_3 are complex conjugates (in particular not entirely real). Then $\mathbb{Q}(\alpha_1)$ is a strict subfield of K and a nontrivial field extension of $\mathbb{Q}$. By the fundamental theorem of Galois theory, $\mathbb{Q}(\alpha_1)$ corresponds to a strict nontrivial subgroup of $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$. But $\mathbb{Z}/3\mathbb{Z}$ has no such subgroups, so this is a contradiction.

□