Peize Liu
St. Peter's College
University of Oxford

Problem Sheet 3

B3.1: Galois Theory

A⁻ Great work!
Just a couple of oversights.

16 November, 2020

In these problems K denotes an arbitrary field, $K[x]$ denotes the ring of polynomials in one variable x over K and $K(x)$ the ring of rational functions in the variable x (i.e. the fraction field of $K[x]$). If p is a prime number, then $\mathbb{F}_p$ denotes the field of integers modulo p.

Question 1

Let $\Phi_m(x) \in \mathbb{C}[x]$ be the m-th cyclotomic polynomial, the monic polynomial whose roots are the primitive m-th roots of 1 in $\mathbb{C}$. Show that

(a) $\Phi_1(x) = x-1$; $\Phi_2(x) = x+1$; $\Phi_3(x) = x^2+x+1$; $\Phi_4(x) = x^2+1$.

(b) $\prod_{d|m} \Phi_d(x) = x^m - 1$

(c) $\Phi_m(x) \in \mathbb{Z}[x]$. [Hint: prove first that $\Phi_m(x) \in \mathbb{Q}[x]$ by induction on m.]

(d) If p is prime then $\Phi_p(x) = 1 + x + x^2 + \cdots + x^{p-1}$ and $\Phi_{p^n}(x) = \Phi_p\left(x^{p^{n-1}}\right)$.

(e) $\deg \Phi_{nm} = \deg \Phi_m \deg \Phi_n$ if (m,n) are relatively prime.

Proof. By definition, $\Phi_m(x) = \prod\{(x-\omega) : \omega \text{ is a primitive } m\text{-th root of unity}\}$. We say that ω is a primitive m-th root of unity, if ω generates the cyclic group $\mu_m(\mathbb{C}) := \{\rho \in \mathbb{C} : \rho^m = 1\}$.

(a) The primitive first root of unity is 1. So $\Phi_1(x) = x-1$.

The primitive second root of unity is -1. So $\Phi_2(x) = x+1$.

The primitive third roots of unity are $\omega = \dfrac{-1+\mathrm{i}\sqrt{3}}{2}$ and ω^2. They satisfy

$$x^3 - 1 = (x-1)(x-\omega)(x-\omega^2)$$

So $\Phi_3(x) = (x-\omega)(x-\omega^2) = \dfrac{x^3-1}{x-1} = x^2+x+1$.

The primitive fourth roots of unity are $\pm\mathrm{i}$. So $\Phi_4(x) = (x-\mathrm{i})(x+\mathrm{i}) = x^2+1$. ✓

(b) For $\rho \in \mu_m(\mathbb{C})$, by Lagrange's Theorem $d = \mathrm{ord}(\rho) \mid m$. And ρ is a primitive d-th root of unity. Hence $(x-\rho) \mid \prod_{d|m} \Phi_d(x)$. Hence

$$x^m - 1 = \prod_{\rho \in \mu_m(\mathbb{C})} (x-\rho) \,\Bigg|\, \prod_{d|m} \Phi_d(x)$$

On the other hand, since $\mathbb{C}$ is algebraically closed, $\prod_{d|m} \Phi_d(x)$ splits over $\mathbb{C}$. For every linear factor $(x-\rho)$ of $\prod_{d|m} \Phi_d(x)$, $(x-\rho)$ is a linear factor of $\Phi_d(x)$ for some $d \mid m$. Hence ρ is a primitive d-th root.

$$\rho^d = 1 \implies \rho^m = 1 \implies \rho \in \mu_m(\mathbb{C})$$

Hence $(x-\rho) \mid (x^m-1)$. We deduce that

$$\prod_{d|m} \Phi_d(x) \,\Big|\, (x^m - 1)$$

Hence $\prod_{d|m} \Phi_d(x) = x^m - 1$. ✓

(c) (I follow the proof in Lemma 5.3 and Proposition 5.5).

Let ω be a primitive m-th root of unity. Then $\mathbb{Q}(\omega) \mid \mathbb{Q}$ is a Galois extension. Let $\omega_1, \ldots, \omega_k$ be all the primitive m-th roots of unity. By Vieta's Theorem we have

$$\Phi_m(x) = \prod_{i=1}^{k} (x-\omega_i) = \sum_{i=0}^{k} (-1)^{k-i} s_{k-i}(\omega_1, \ldots, \omega_k) x^i$$

where $s_i(\omega_1, \ldots, \omega_k)$ is the i-th symmetric function in $\omega_1, .., \omega_k$. Note that for $\gamma \in \mathrm{Gal}(\mathbb{Q}(\omega) \mid \mathbb{Q})$, $\gamma(s_i(\omega_1, \ldots, \omega_k)) = s_i(\omega_1, \ldots, \omega_k)$ because γ only permutes the primitive m-th roots of unity. Hence $s_i(\omega_1, \ldots, \omega_k) \in \mathbb{Q}$ and $\Phi_m(x) \in \mathbb{Q}[x]$.

Next we show that $\Phi_m \in \mathbb{Z}[x]$. By (b) there exists $\Psi \in \mathbb{Q}[x]$ such that $x^m - 1 = \Phi_m(x)\Psi(x)$. By Gauss' Lemma, $1 = \mathrm{c}(x^m-1) = \mathrm{c}(\Psi)\,\mathrm{c}(\Phi_m)$. Hence $\mathrm{c}(\Phi_m) = 1$ and $\Phi_m \in \mathbb{Z}[x]$. ✓

(d) If p is prime, then $\mu_p(\mathbb{C}) \cong \mathbb{Z}/p\mathbb{Z}$. In particular every non-trivial element of $\mu_p(\mathbb{C})$ generates $\mu_p(\mathbb{C})$. Hence

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

By (b) we have

$$x^{p^n} - 1 = \prod_{d \mid p^n} \Phi_d(x) = \Phi_1(x)\Phi_p(x)\cdots\Phi_{p^n}(x) = \left(x^{p^{n-1}} - 1\right)\Phi_{p^n}(x)$$

Hence

$$\Phi_{p^n}(x) = \frac{x^{p^n}-1}{x^{p^{n-1}}-1} = 1 + x^{p^{n-1}} + x^{2p^{n-1}} + \cdots + x^{(p-1)p^{n-1}} = \Phi_p(x^{p^{n-1}})$$ ✓

(e) By Chinese Remainder Theorem, $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z}$ for $\gcd(m,n) = 1$. Hence $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/mn\mathbb{Z})^\times$. We know that

$$\deg \Phi_m = |\mu_m(\mathbb{C})^\times| = |(\mathbb{Z}/m\mathbb{Z})^\times|$$

Hence

$$\deg \Phi_m \deg \Phi_n = |(\mathbb{Z}/m\mathbb{Z})^\times| \cdot |(\mathbb{Z}/n\mathbb{Z})^\times| = |(\mathbb{Z}/mn\mathbb{Z})^\times| = \deg(\Phi_m\Phi_n)$$ ✓ Great Ⓐ □

Question 2

Let n be a positive integer and $f = x^{p^n} - x \in \mathbb{F}_p[x]$. Let M be the splitting field of f over $\mathbb{F}_p$. Show that M consists exactly of the set of roots of f. Show that $[M:\mathbb{F}_p] = n$ Explain why this fact also shows the existence of an irreducible polynomial of degree n in $\mathbb{F}_p[x]$.

Proof. In Question 6 of Sheet 1, we have shown that the roots of $f(x) = x^{p^n} - x$ in splitting field M form a subfield K of M. On the other hand, for $a \in \mathbb{F}_p$, by Fermat's Little Theorem we have $a^p = a$. Then $a^{p^2} = a^p = a$. Inductively we have $a^{p^n} = a$. Hence $a \in K$. Then $\mathbb{F}_p \subseteq K$. Since K contains all roots of f, by the definition of splitting field we have $M \subseteq K$. Hence $M = K$.

We have also shown that f has no multiple roots. Hence we have $|K| = |M| = p^n$. And

$$[M:\mathbb{F}_p] = \log_{|\mathbb{F}_p|} |M| = \log_p(p^n) = n$$

Since f is separable, $M \mid \mathbb{F}_p$ is a separable extension. By the theorem of primitive element, $M \mid \mathbb{F}_p$ is a simple extension. There exists $\alpha \in M$ such that $M = \mathbb{F}_p(\alpha)$. Therefore the minimal polynomial m_α of α over $\mathbb{F}_p$ is an irreducible polynomial of degree n. ✓ Nice Ⓐ □

Question 3

(a) Prove that $\Phi_{12}(x) = x^4 - x^2 + 1$, and that it is irreducible over $\mathbb{Q}$. Factorise it into irreducibles over $\mathbb{F}_p$ when $p = 2, 3, 5, 13$.

(b) If p is any prime with $p > 3$ show that $p^2 - 1$ is divisible by 12, and deduce that Φ_{12} is reducible over $\mathbb{F}_p$ for every prime p.

Proof. (a) By Part (b) of Question 1, we have

$$x^{12} - 1 = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_4(x)\Phi_6(x)\Phi_{12}(x) = (x^6-1)\Phi_4(x)\Phi_{12}(x) = (x^6-1)(x^2+1)\Phi_{12}(x)$$

Hence

$$\Phi_{12}(x) = \frac{x^{12}-1}{(x^6-1)(x^2+1)} = \frac{x^6+1}{x^2+1} = x^4 - x^2 + 1$$

We can invoke Proposition 5.5 to assert that Φ_{12} is irreducible over $\mathbb{Q}$. Otherwise, we can also directly verify this:

We factorise Φ_{12} over $\mathbb{C}$:

$$x^4 - x^2 + 1 = 0 \implies (x^2)_{1,2} = \frac{1 \pm \mathrm{i}\sqrt{3}}{2} \implies x_{1,2,3,4} = \pm\sqrt{\frac{1 \pm \mathrm{i}\sqrt{3}}{2}}$$

Hence Φ_{12} has no root in $\mathbb{Q}$. Suppose that it has a quadratic factor in $\mathbb{Q}[x]$. Then there exists $a, b \in \mathbb{Q}$ such that

$$x^4 - x^2 + 1 = (x^2 + ax \pm 1)(x^2 + bx \pm 1)$$

which implies that

$$a + b = 0, \qquad ab \pm 2 = -1 \tag{$*$}$$

Clearly no rational numbers satisfy $(*)$. We deduce that Φ_{12} is irreducible in $\mathbb{Q}[x]$.

Factorisation of Φ_{12} over $\mathbb{F}_2$: We note that $a = b = 1$ solves the equation $(*)$ in $\mathbb{F}_2$. So

$$\Phi_{12}(x) = x^4 - x^2 + 1 = (x^2 + x + 1)^2$$

Φ_{12} has no linear factors in $\mathbb{F}_2$ since $\mathbb{F}_2$ contains no primitive 12th roots of unity.

Factorisation of Φ_{12} over $\mathbb{F}_3$: We note that $a = b = 0$ solves $(*)$ in $\mathbb{F}_3$. Hence

$$\Phi_{12}(x) = x^4 - x^2 + 1 = (x^2 + 1)^2$$

Φ_{12} has no linear factors in $\mathbb{F}_3$ since $\mathbb{F}_3$ contains no primitive 12th roots of unity.

Factorisation of Φ_{12} over $\mathbb{F}_5$: We note that $a = 3$ and $b = -3$ solve $(*)$ in $\mathbb{F}_5$. Hence

$$\Phi_{12}(x) = x^4 - x^2 + 1 = (x^2 + 3x - 1)(x^2 - 3x - 1)$$

Φ_{12} has no linear factors in $\mathbb{F}_5$ since $\mathbb{F}_5$ contains no primitive 12th roots of unity.

Factorisation of Φ_{12} over $\mathbb{F}_{13}$: Note that $\mathbb{F}_{13}^\times \cong \mathbb{Z}/12\mathbb{Z}$ contains all primitive 12th roots of unity. Hence Φ_{12} splits over $\mathbb{F}_{13}$. Moreover we note that 2 generates $\mathbb{F}_{13}^\times$:

$$2^1 = 2 \quad 2^2 = 4 \quad 2^3 = -5 \quad 2^4 = 3 \quad 2^5 = 6 \quad 2^6 = -1 \quad 2^7 = -2 \quad 2^8 = -4 \quad 2^9 = 5 \quad 2^{10} = -3 \quad 2^{11} = -6 \quad 2^{12} = 1$$

We also read from this table that the generators of $\mathbb{F}_{13}^\times$ are $2, 6, -2, -6$. Hence we have

$$\Phi_{12}(x) = x^4 - x^2 + 1 = (x - 2)(x + 2)(x - 6)(x + 6)$$

✓

(b) For a prime number $p > 3$, p is odd. So $(p+1)$ and $(p-1)$ are even. In addition one of them is divisible by 4. Hence $p^2 - 1 = (p+1)(p-1)$ is divisible by 8. One of the consecutive numbers $p-1$, p, $p+1$ must be divisible by 3. Since $p > 3$ is prime, either $(p-1)$ or $(p+1)$ is divisible by 3. Hence $p^2 - 1$ is divisible by 3. We deduce that $24 \mid (p^2 - 1)$.

Suppose that Φ_{12} is irreducible over $\mathbb{F}_p$ for some prime p. By (a) we may assume that $p > 5$. Then the splitting extension of Φ_{12} over $\mathbb{F}_p$ has degree at least $\deg \Phi_{12} = 4$. But we also note that Φ_{12} splits over $\mathbb{F}_{p^2}$: We have $\mathbb{F}_{p^2}^\times \cong \mathbb{Z}/(p^2-1)\mathbb{Z}$. Since $12 \mid (p^2 - 1)$, $\mathbb{F}_{p^2}$ contains all primitive 12th roots of unity. But $[\mathbb{F}_{p^2} : \mathbb{F}_p] = 2$, which is a contradiction. We conclude that Φ_{12} is reducible over $\mathbb{F}_p$ for all prime p. □

✓ Excellent Ⓐ

Question 4

For this exercise recall the definition of a group action on a set. Let $f \in K[x]$ be a separable degree n polynomial, let M be its splitting field and $G = \Gamma(M : K)$ be the Galois group of M. Let $A = \{\alpha_1, \dots \alpha_n\} \subseteq M$ be the set of roots of f. Let $S(A)$ be the set of permutations of the roots of f.

(a) Show that G acts faithfully on A (this is equivalent to showing that there is an injective group homomorphism between G and $S(A)$).

(b) Show that if f is irreducible, then G acts transitively on A (this is equivalent to show that for any $\alpha_i, \alpha_j \in A$ there exists $\sigma \in G$ such that $\sigma(\alpha_i) = \alpha_j$).

Proof. (a) Firstly, we note that for $\gamma \in \mathrm{Gal}(M \mid K)$, $\gamma(\alpha_i)$ is a root of f because

$$0 = \gamma(f(\alpha_i)) = \gamma\left(\sum_{k=0}^{n} c_n \alpha_i^n\right) = \sum_{k=0}^{n} c_n \gamma(\alpha_i)^n = f(\gamma(\alpha_i))$$

Since γ is a field automorphism, γ maps $\{\alpha_1,...,\alpha_k\}$ bijectively to itself. This defines a group homomorphism $\varphi : \mathrm{Gal}(M \mid K) \to S(A)$. Note that $M = K(\alpha_1,...,\alpha_n)$ by definition of the splitting field. Hence $\varphi(\gamma) \in S(A)$ is uniquely determined by the image $\gamma(\alpha_1),...,\gamma(\alpha_n)$. Hence φ is a group monomorphism. $\mathrm{Gal}(M \mid K)$ acts faithfully on $\{\alpha_1,...,\alpha_k\}$. ✓

(b) Since M is the splitting field of the separable polynomial f over K, by Theorem 3.8 $M \mid K$ is a Galois extension. For $\alpha_i, \alpha_j \in A$, note that f is both the minimal polynomial of α_i and α_j, we have the field automorphism $\sigma : K[\alpha_i] \to K[\alpha_j]$ with $\sigma(\alpha_i) = \alpha_j$ given by the composition:

$$K[\alpha_i] \xrightarrow{\sim} K[x]/\langle f(x)\rangle \xrightarrow{\sim} K[\alpha_j]$$ ✓

Then σ extends to a automorphism $\tilde{\sigma} \in \mathrm{Gal}(M \mid K)$ by letting $\tilde{\sigma}(\alpha_k) = \alpha_k$ for all $k \neq i, j$. Hence $\mathrm{Gal}(M \mid K)$ acts transitively on $\{\alpha_1,...,\alpha_k\}$. □ AB

We can extend σ to M by using uniqueness of splitting fields (for example), but cannot ensure $\tilde{\sigma}(\alpha_k) = \alpha_k$. What if $\alpha_k = \alpha_i^2$?

Question 5

Find the Galois groups of the following polynomials and for each subgroup identify the corresponding subfield of the splitting field:

(a) $x^2 + 1$ over $\mathbb{R}$

(b) $x^3 - 1$ over $\mathbb{Q}$

(c) $x^3 - 5$ over $\mathbb{Q}$

(d) $x^6 - 3x^3 + 2$ over $\mathbb{Q}$

(e) $x^5 - 1$ over $\mathbb{Q}$

(f) $x^6 + x^3 + 1$ over $\mathbb{Q}$.

Find the Galois group of the polynomial $x^{p^n} - x - t$ over $\mathbb{F}_{p^n}(t)$ (you can assume that this polynomial is irreducible over $\mathbb{F}_{p^n}(t)$; you need not determine the subfield subgroup correspondence here).

Proof. From (a) to (f) all base fields have characteristic 0. So all splitting extensions are separable.

(a) The splitting field of $x^2 + 1$ over $\mathbb{R}$ is $\mathbb{R}(\mathrm{i}) = \mathbb{C}$. We have $|\mathrm{Gal}(\mathbb{C} \mid \mathbb{R})| = [\mathbb{C} : \mathbb{R}] = 2$. Hence $\mathrm{Gal}(\mathbb{C} \mid \mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$. In fact the elements of $\mathrm{Gal}(\mathbb{C} \mid \mathbb{R})$ are the identity map and the conplex conjugation $z \mapsto \overline{z}$. ✓

(b) The splitting field of $x^3 - 1$ over $\mathbb{Q}$ is $\mathbb{Q}(\omega)$, where $\omega = \dfrac{-1 + \mathrm{i}\sqrt{3}}{2}$. ω has minimal polynomial $x^2 + x + 1$ over $\mathbb{Q}$. Hence $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$. $\mathrm{Gal}(\mathbb{Q}(\omega) \mid \mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$. ✓

(c) The splitting extension of $x^3 - 5$ over $\mathbb{Q}$ is a Kummer extension. Let ω be a third root of a unity (given by (b)). Then by Lemma 5.6 the splitting field of $x^3 - 5$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{3}\mathrm{i}, \sqrt[3]{5})$. Similar to Question 4 in Sheet 2 we have $[\mathbb{Q}(\sqrt{3}\mathrm{i}, \sqrt[3]{5}) : \mathbb{Q}] = 6$. Note that $x^3 - 5$ is irreducible. By Question 2.(b) we have $\mathrm{Gal}\left(\mathbb{Q}(\sqrt{3}\mathrm{i}, \sqrt[3]{5}) \mid \mathbb{Q}\right) \cong H \leqslant S_3$. But $|S_3| = 6$. We deduce that $\mathrm{Gal}\left(\mathbb{Q}(\sqrt{3}\mathrm{i}, \sqrt[3]{5}) \mid \mathbb{Q}\right) \cong S_3$.

The non-trivial subgroups of S_3 are $\langle(12)\rangle$, $\langle(13)\rangle$, $\langle(23)\rangle$ and $\langle(123)\rangle$. Correspondingly, $\mathbb{Q}(\sqrt{3}\mathrm{i}, \sqrt[3]{5})$ has 3 subfields which are degree 3 over $\mathbb{Q}$: $\mathbb{Q}(\sqrt[3]{5})$, $\mathbb{Q}(\omega\sqrt[3]{5})$ and $\mathbb{Q}(\omega^2\sqrt[3]{5})$, and 1 subfield which is degree 2 over $\mathbb{Q}$: $\mathbb{Q}(\sqrt{3}\mathrm{i})$. ✓

(d) Note that $x^6 - 3x^3 + 2$ is reducible over $\mathbb{Q}$:

$$x^6 - 3x^3 + 2 = (x-1)(x^5 + x^4 + x^3 - 2x^2 - 2x - 2) = (x-1)(x^3 - 2)(x^2 + x + 1)$$

The root of the polynomial are $1, \omega, \omega^2, \sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$. Hence the splitting field is $\mathbb{Q}(\omega, \sqrt[3]{2})$ and $[\mathbb{Q}(\omega, \sqrt[3]{2}) : \mathbb{Q}] = 6$. The Galois group $\mathrm{Gal}\left(\mathbb{Q}(\omega, \sqrt[3]{2}) \mid \mathbb{Q}\right)$ is isomorphic to either $\mathbb{Z}/6\mathbb{Z}$ or S_3.

Any $\mathbb{Q}$-automorphism σ is uniquely determined by its image of ω and $\sqrt[3]{2}$. Let $\alpha \in \mathrm{Gal}\left(\mathbb{Q}(\omega, \sqrt[3]{2}) \mid \mathbb{Q}\right)$ given by $\alpha(\omega) = \omega^2$ and $\alpha(\sqrt[3]{2}) = \sqrt[3]{2}$. Then $\alpha^2 = \mathrm{id}$. Let $\beta \in \mathrm{Gal}\left(\mathbb{Q}(\omega, \sqrt[3]{2}) \mid \mathbb{Q}\right)$ given by $\beta(\omega) = \omega$ and $\beta(\sqrt[3]{2}) = \omega\sqrt[3]{2}$. Then $\beta^3 = \mathrm{id}$. Note that

$$\alpha \circ \beta(\omega\sqrt[3]{2}) = \alpha(\omega^2\sqrt[3]{2}) = \omega\sqrt[3]{2}, \qquad \beta \circ \alpha(\omega\sqrt[3]{2}) = \beta(\omega^2\sqrt[3]{2}) = \sqrt[3]{2}$$

Hence $\alpha \circ \beta \neq \beta \circ \alpha$. In particular $\mathrm{Gal}\left(\mathbb{Q}(\omega, \sqrt[3]{2}) \mid \mathbb{Q}\right)$ is not Abelian. Hence $\mathrm{Gal}\left(\mathbb{Q}(\omega, \sqrt[3]{2}) \mid \mathbb{Q}\right) \cong S_3$.

The non-trivial subgroups of $\mathrm{Gal}\left(\mathbb{Q}(\omega, \sqrt[3]{2}) \mid \mathbb{Q}\right)$ are $\langle\alpha\rangle$, $\langle\beta\alpha\rangle$, $\langle\beta^2\alpha\rangle$ and $\langle\beta\rangle$.

Or just use same proof as in (c), in fact rest of (d) is verbatim.

Since $\alpha(\sqrt[3]{2}) = \sqrt[3]{2}$, the fixed field of $\langle\alpha\rangle$ is $\mathbb{Q}(\sqrt[3]{2})$.

Since $\beta\circ\alpha(\omega^2\sqrt[3]{2}) = \beta(\omega\sqrt[3]{2}) = \omega^2\sqrt[3]{2}$, the fixed field of $\langle\beta\alpha\rangle$ is $\mathbb{Q}(\omega^2\sqrt[3]{2})$.

Since $\beta^2\circ\alpha(\omega\sqrt[3]{2}) = \beta^2(\omega^2\sqrt[3]{2}) = \omega\sqrt[3]{2}$, the fixed field of $\langle\beta\alpha\rangle$ is $\mathbb{Q}(\omega\sqrt[3]{2})$.

Since $\beta(\omega) = \omega$, the fixed field of $\langle\beta\rangle$ is $\mathbb{Q}(\omega)$. ✓

(e) The splitting extension of x^5-1 over $\mathbb{Q}$ is a cyclotomic extension. Let ζ be a primitive fifth root of unity. Then the splitting field is $\mathbb{Q}(\zeta)$. By Proposition 5.4 we have

$$\mathrm{Gal}(\mathbb{Q}(\zeta)\mid\mathbb{Q}) \cong \mathrm{Aut}(\mathbb{Z}/5\mathbb{Z}) \cong \mathbb{Z}/4\mathbb{Z}$$

(since $\Phi_5(x) = x^4+x^3+x^2+x+1$ is irreducible).

We note that $\mathrm{Gal}(\mathbb{Q}(\zeta)\mid\mathbb{Q})$ is generated by σ which maps ζ to ζ^2. The only non-trivial subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta)\mid\mathbb{Q})$ is $\langle\sigma^2\rangle$. Then σ^2 maps ζ to ζ^4, ζ^2 to ζ^3, ζ^3 to ζ^2, and ζ^4 to ζ. The fixed field of $\langle\sigma^2\rangle$ is $\mathbb{Q}(\zeta+\zeta^4) = \mathbb{Q}(\cos\frac{2\pi}{5})$. ✓

(f) By Question 2 of Sheet 2 we know that x^6+x^3+1 is irreducible over $\mathbb{Q}$. We have shown that the 6 roots of x^6+x^3+1 are exactly the primitive 9th roots of unity, which means $\Phi_9(x) = x^6+x^3+1$. So the splitting extension of x^6+x^3+1 is a cyclotomic extension. Let ρ be a primitive 9th roots of unity. Then the splitting field is $\mathbb{Q}(\rho)$. By Proposition 5.4 we have

$$\mathrm{Gal}\big(\mathbb{Q}(\rho)\mid\mathbb{Q}\big) \cong \mathrm{Aut}(\mathbb{Z}/9\mathbb{Z}) \cong (\mathbb{Z}/9\mathbb{Z})^\times \cong \mathbb{Z}/6\mathbb{Z}$$

$\mathrm{Gal}\big(\mathbb{Q}(\rho)\mid\mathbb{Q}\big)$ is generated by γ, which maps ρ to ρ^2. The action of γ on the roots is given by

$$\gamma : \rho \mapsto \rho^2 \mapsto \rho^4 \mapsto \rho^8 \mapsto \rho^7 \mapsto \rho^5 \mapsto \rho$$

$\rho(1+\rho^3+\rho^6) = \frac{\rho(\rho^9-1)}{\rho^3-1} = 0$

The non-trivial subgroups of $\mathrm{Gal}\big(\mathbb{Q}(\rho)\mid\mathbb{Q}\big)$ are $\langle\gamma^2\rangle$ and $\langle\gamma^3\rangle$. The fixed field of $\langle\gamma^2\rangle$ is $\mathbb{Q}(\rho+\rho^4+\rho^7)$. The fixed field of $\langle\gamma^3\rangle$ is $\mathbb{Q}(\rho+\rho^8) = \mathbb{Q}(\cos\frac{2\pi}{9})$.

↑ is actually $\mathbb{Q}(\rho^3)$

Let K be the splitting field of $f(x) := x^{p^n}-x-t$ over $\mathbb{F}_{p^n}(t)$. Let α be a root of f in K. Note that for $k\in\mathbb{F}_{p^n}$,

$$f(\alpha+k) = (\alpha+k)^{p^n}-(\alpha+k)-t = \alpha^{p^n}+k-(\alpha+k)-t = 0$$

where we used the Frobenius automorphism $x\mapsto x^{p^n}$ and the fact that $k^{p^n} = k$. Hence $\alpha+k$ is also a root of f. The roots of f are exactly $\{\alpha+k\in K : k\in\mathbb{F}_p\}$. In particular we have $K = F_{p^n}(t)(\alpha)$. So $\big|\mathrm{Gal}\big(K\mid F_{p^n}(t)\big)\big| = p^n$. Any $\gamma\in\mathrm{Gal}\big(K\mid F_{p^n}(t)\big)$ is uniquely determined by its action on α. We deduce that $\mathrm{Gal}\big(K\mid F_{p^n}(t)\big)\cong\mathbb{Z}/p^n\mathbb{Z}$. ✓ □

↑ Could do with little bit more detail here

AB Good, but need to be more rigorous proving the fixed field, else may cause mistakes.

Question 6

Prove that $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ is Galois over $\mathbb{Q}$, and find its Galois group.

Proof. Let $u = \sqrt{2+\sqrt{2}}$. Then

$$u^2 = 2+\sqrt{2} \implies (u^2-2)^2 = 2 \implies u^4-4u^2+2 = 0$$

Let $f(x) = x^4-4x^2+2\in\mathbb{Q}[x]$. By Eisenstein's criterion with $p=2$, it is irreducible over $\mathbb{Q}$. Hence f is the minimal polynomial of $\sqrt{2+\sqrt{2}}$ over $\mathbb{Q}$. The field extension $\mathbb{Q}(\sqrt{2+\sqrt{2}}\mid\mathbb{Q})$ is separable because $\mathrm{char}\,\mathbb{Q} = 0$. We shall prove that the extension is also normal. The all four roots of f are $\pm\sqrt{2\pm\sqrt{2}}$. Note that

$$\left(\sqrt{2+\sqrt{2}}\right)^2 = 2 = \sqrt{2}$$

So $\sqrt{2}\in\mathbb{Q}(\sqrt{2+\sqrt{2}})$. Next note that

$$\sqrt{2+\sqrt{2}}\cdot\sqrt{2-\sqrt{2}} = \sqrt{2^2-2} = \sqrt{2}$$

So $\sqrt{2-\sqrt{2}}\in\mathbb{Q}(\sqrt{2+\sqrt{2}})$. It is clear that $-\sqrt{2+\sqrt{2}}$ and $-\sqrt{2-\sqrt{2}}$ are in $\mathbb{Q}(\sqrt{2+\sqrt{2}})$. We deduce that $\mathbb{Q}(\sqrt{2+\sqrt{2}}\mid\mathbb{Q}$ is normal. By Theorem 3.18, $\mathbb{Q}(\sqrt{2+\sqrt{2}})\mid\mathbb{Q}$ is a Galois extension. ✓

Next we have $\left|\mathrm{Gal}\left(\mathbb{Q}(\sqrt{2+\sqrt{2}})\mid\mathbb{Q}\right)\right| = \left[\mathbb{Q}(\sqrt{2+\sqrt{2}}):\mathbb{Q}\right] = 4$. The only groups of order 4 are $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$. Let

$\gamma \in \mathrm{Gal}\left(\mathbb{Q}(\sqrt{2+\sqrt{2}}) \mid \mathbb{Q}\right)$ such that $\gamma(\sqrt{2+\sqrt{2}}) = \sqrt{2-\sqrt{2}}$. Then

$$\gamma(2+\sqrt{2}) = 2-\sqrt{2} \implies \gamma(\sqrt{2}) = -\sqrt{2}$$

And

$$\gamma^2\left(\sqrt{2+\sqrt{2}}\right) = \gamma\left(\sqrt{2-\sqrt{2}}\right) = \gamma\left(\frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}}\right) = \frac{\gamma(\sqrt{2})}{\gamma(\sqrt{2+\sqrt{2}})} = \frac{-\sqrt{2}}{\sqrt{2-\sqrt{2}}} = -\sqrt{2+\sqrt{2}} \neq \sqrt{2+\sqrt{2}}$$

Then $\gamma^2 \neq \mathrm{id}$. So γ has order 4 in the Galois group. We deduce that

$$\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right) \,\middle|\, \mathbb{Q}\right) \cong \mathbb{Z}/4\mathbb{Z}$$ ✓ Good work Ⓐ □