Solutions Single Choice 12

1. Let K be the splitting field of $x^{49} - 1$ over $\mathbb{Q}$. Then $[K : \mathbb{Q}]$ is equal to

(a) 7
(b) 42
(c) 48
(d) 49

Solution: The correct answer is (d). Let ζ denote the 49-th primitive root of unity. We have seen in the lecture that

$$[K : \mathbb{Q}] = [\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(49),$$

where φ is Euler's totient function. We have seen in Algebra I that for a prime number p and a positive integer k we have

$$\varphi(p^k) = (p-1)p^{k-1},$$

so $[K : \mathbb{Q}] = 6 \cdot 7 = 42$.

2. Let $r \in \mathbb{Z}_{>1}$ and let $L : K$ be a Galois extension such that $\mathrm{Gal}(L : K)$ is cyclic of order 2^r. What is the number of the subfields M such that $K \subsetneq M \subsetneq L$?

(a) $r - 1$
(b) r
(c) $r + 1$
(d) $r + 2$

Solution: Let σ be a generator of $G := \mathrm{Gal}(L : K)$, so that $\sigma^{2^r} = 1$. For $0 \leqslant m \leqslant r$ let H_m be the subgroup generated by σ^{2^m}, which is cyclic of order 2^{r-m}. Then we have

$$1 = H_r < H_{r-1} < \cdots < H_0 = G,$$

and since G is cyclic, are these all the subgroups of G.

Write $M_m := L^{H_m}$. Then by the Galois correspondence we obtain the intermediate fields:

$$L = M_r : M_{r-1} : \cdots : M_0 = K.$$

Hence there are $r - 1$ subfields M such that $K \subsetneq M \subsetneq L$.

3. Let K be the splitting field of $x^{42} - 1$ over $\mathbb{Q}$. What is the number of the subfields M such that $\mathbb{Q} \subsetneq M \subsetneq K$?

(a) 3
(b) 4
(c) 6

(d) 8

Solution: The correct answer is (d). By Theorem 6.7 we have

$$\mathrm{Gal}(K:\mathbb{Q}) \cong (\mathbb{Z}/42\mathbb{Z})^\times,$$

and

$$(\mathbb{Z}/42\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z})^\times \times (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/7\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z}).$$

The group $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$ has precisely 8 proper non-trivial subgroups, so by the Galois correspondence there are also 8 subfields M such that $\mathbb{Q} \subsetneq M \subsetneq K$.

Alternatively, we can determine the group $G := \mathrm{Gal}(K:\mathbb{Q})$ more explicitly by looking at its automorphisms. Automorphisms in G are determined by the image of the 42-th root of unity ζ. Consider the automorphisms $\varphi : \zeta \mapsto \zeta^5$ and $\sigma : \zeta \mapsto \zeta^{13}$. Then φ has order 6, while σ has order 2. Also $\varphi\sigma = \sigma\varphi$, which gives $G \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$, since $\langle\sigma\rangle$ is not a subgroup of $\langle\varphi\rangle$.

4. Let $f \in \mathbb{Q}[X]$ be irreducible and let K denote its splitting field. If $\mathrm{Gal}(K:\mathbb{Q}) = D_4$ (the dihedral group of order 8), what are the possibilities for the degree of f?

(a) Only the degree 4 is possible.

(b) Only the degree 8 is possible.

(c) Only the degrees 4 and 8 are possible.

(d) The degrees 2, 4 and 8 are all possible.

Solution: The correct answer is (c). The polynomial f has to have degree greater than 2, since otherwise the Galois group would be C_2. For degree 4 note that $x^4 - 2$ is a polynomial of degree 4 over $\mathbb{Q}$, which has Galois group isomorphic to D_4. The splitting field is given by $\mathbb{Q}(\sqrt[4]{2}, i)$ and considering the automorphisms $\varphi : \sqrt[4]{2} \mapsto \sqrt[4]{2}, i \mapsto -i$ and $\sigma : \sqrt[4]{2} \mapsto i\sqrt[4]{2}, i \mapsto i$, we can compute

$$\mathrm{Gal}(K:\mathbb{Q}) = \langle \sigma, \varphi : \sigma^4 = \varphi^2 = 1, \varphi\sigma\varphi^{-1} = \sigma^{-1} \rangle \cong D_4.$$

Also, note that $\mathbb{Q}(\sqrt[4]{2}, i) = \mathbb{Q}(\sqrt[4]{2} + i)$, and the element $\sqrt[4]{2} + i$ has minimal polynomial $x^8 + 4x^6 + 2x^4 + 28x^2 + 1$ over $\mathbb{Q}$, which has degree 8.

5. Which of the following statements is **false**?

(a) There exists a primitive root of unity ζ such that $\mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\zeta)$.

(b) Let $K:\mathbb{Q}$ be a finite normal extension. If $\mathrm{Gal}(K:\mathbb{Q})$ is solvable, then there exists an extension $L:K$ such that $L:\mathbb{Q}$ is radical.

(c) The Galois group of the polynomial $X^4 + X^2 + 1$ over $\mathbb{Q}$ is solvable.

(d) Each radical extension is normal.

Solution: Part (a) is the Kronecker-Weber theorem, since $\mathrm{Gal}(\mathbb{Q}(\sqrt{5}):\mathbb{Q}) = C_2$ is an abelian group. From Theorem 7.5 we obtain part (b).

Part (c) follows from Theorem 7.6: since $X^4 + X^2 + 1$ is solvable by radicals. More precisely,

$$X^4 + X^2 + 1 = (X^2 + X + 1)(X^2 - X + 1),$$

which has zeros $\pm\frac{1}{2} \pm \frac{i\sqrt{3}}{2}$.

Part (d) is false: consider the radical extension $\mathbb{Q}(\sqrt[3]{3}):\mathbb{Q}$.