Solutions 08

P8.1. Prove that

$$|\mathrm{Gal}(\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_n}) \,/\, \mathbb{Q})| = 2^n$$

where $p_1, p_2, \dots, p_n$ are the first n primes in the ring $\mathbb{Z}$ of integers.

Solution. Let $L := \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_n})$. Since $x^2 - p_j \in \mathbb{Q}[x]$ has $\pm\sqrt{p_j}$ as roots, each automorphism $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ is uniquely determined by

$$\sigma(\sqrt{p_j}) = \pm\sqrt{p_j} \quad \text{for all } 1 \leqslant j \leqslant n.$$

This gives the inequality $|\mathrm{Gal}(L/\mathbb{Q})| \leqslant 2^n$.

On the other hand, L is the splitting field of the separable polynomial

$$f := (x^2 - p_1)(x^2 - p_2) \cdots (x^2 - p_n) \in \mathbb{Q}[x]\,.$$

It follows that $|\mathrm{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}]$. Hence, it suffices to show that the set

$$\left\{ \sqrt{\prod_{j \in X} p_j} \;\middle|\; X \subset [n] := \{1, 2, \dots, n\} \right\}$$

is a $\mathbb{Q}$-basis for L.

We prove a stronger statement. Let $\mathcal{A}_n := \{a_1, a_2, \dots, a_n\}$ be a set of positive integers such that no element is the square of any integer and every pair of elements is relatively prime. We claim that set

$$\left\{ \sqrt{\prod_{j \in X} a_j} \;\middle|\; X \subset [n] := \{1, 2, \dots, n\} \right\}$$

is a $\mathbb{Q}$-basis for $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_n})$. We proceed by induction on n.

The case $n = 0$ holds because 1 is a $\mathbb{Q}$-basis for $\mathbb{Q}$. Suppose that a is a positive integer that is not a perfect square. The polynomial $x^2 - a \in \mathbb{Q}[x]$ is irreducible and $\sqrt{a}$ is a root, so $\{1, \sqrt{a}\}$ is a $\mathbb{Q}$-basis for $\mathbb{Q}(\sqrt{a})$. Thus, the case $n = 1$ holds.

For the induction step, set $K_j := \mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \dots, \sqrt{a_j})$ for all $0 \leqslant j \leqslant n$. By the Tower Theorem, it is enough to show that $[K_j : K_{j-1}] = 2$ for all $1 \leqslant j \leqslant n$. Suppose otherwise and let m be the smallest integer such that $[K_m : K_{m-1}] = 1$. It follows that $K_m = K_{m-1}$ and $\sqrt{a_m} \in K_{m-1}$. Since $\{1, \sqrt{a_{m-1}}\}$ is a K_{m-2}-basis for K_{m-1}, there exists $b, c \in K_{m-2}$ such that

$$b + c\sqrt{a_{m-1}} = \sqrt{a_m} \qquad \Longrightarrow \qquad b^2 + 2bc\sqrt{a_{m-1}} + c^2 a_{m-1} = a_m\,.$$

If $bc \neq 0$, then this would imply that $\sqrt{a_{m-1}} \in K_{m-2}$ contradicting our choice of m. Thus, we deduce that either $b = 0$ or $c = 0$. We consider these cases separately.

($b = 0$) If $b = 0$, then we have $ba_{m-1} = \sqrt{a_m a_{m-1}}$, which implies that $\sqrt{a_m a_{m-1}} \in K_{m-2}$. However, $a_m a_{m-1}$ is not the square of any integer because a_m and a_{m-1} are relatively prime, so this contradicts the induction hypothesis when applied to $\mathcal{A}_{n-1} = \{a_1, a_2, \dots, a_{n-2}, a_n a_{n-1}\}$.

($c = 0$) If $b = 0$, then $\sqrt{a_m} \in K_{m-2}$ which contradicts the induction hypothesis when applied to $\mathcal{A}_{n-1} = \{a_1, a_2, \dots, a_{n-2}, a_n\}$.

Therefore, the given set indexed by the subsets of $[n]$ is a $\mathbb{Q}$-basis.q □

P8.2. Find a subgroup of the symmetric group $\mathfrak{S}_4$ that is isomorphic to the Galois group

$$\mathrm{Gal}\Big(\mathbb{Q}(\mathrm{i}, \sqrt[4]{2}) \,/\, \mathbb{Q}\Big).$$

Can you name this group?

Solution. Let $\beta := \sqrt[4]{2} \in \mathbb{R}$ and $L := \mathbb{Q}(\mathrm{i}, \beta)$. Since the polynomial $x^4 - 2$ is irreducible by the Eisenstein criterion (where $p = 2$), it follows that $[\mathbb{Q}(\beta) : \mathbb{Q}] = 4$. The inclusion $\mathbb{Q}(\beta) \subset \mathbb{R}$ shows that $\mathrm{i} \notin \mathbb{Q}(\beta)$, so $x^2 + 1$ is the minimal polynomial of i over $\mathbb{Q}(\beta)$. Hence, the Tower Theorem gives $[L : \mathbb{Q}] = [L : \mathbb{Q}(\beta)][\mathbb{Q}(\beta) : \mathbb{Q}] = (2)(4) = 8$.

The factorization $x^4 - 2 = (x^2 - \sqrt{2})(x^2 + \sqrt{2}) = (x - \beta)(x + \beta)(x - \mathrm{i}\beta)(x + \mathrm{i}\beta)$ establishes that $\mathbb{Q}(\mathrm{i}, \mathrm{i}\beta)$ is the splitting field for $x^4 - 2$. Since $(-\mathrm{i})(\mathrm{i}\beta) = \beta$, we see that $L \subseteq \mathbb{Q}(\mathrm{i}, \mathrm{i}\beta)$ and $L = \mathbb{Q}(\mathrm{i}, \mathrm{i}\beta)$, so L is also the splitting field for the separable polynomial $x^4 - 2 \in \mathbb{Q}[x]$. Hence, there exists $\sigma, \tau \in \mathrm{Gal}(L/\mathbb{Q})$ such that

$$\sigma(\beta) = \mathrm{i}\beta\,, \qquad \sigma(\mathrm{i}) = \mathrm{i}\,, \qquad \tau(\beta) = \beta\,, \qquad \tau(\mathrm{i}) = -\mathrm{i}\,.$$

Setting $\alpha_1 := \beta$, $\alpha_2 := -\beta$, $\alpha_3 := \mathrm{i}\beta$, and $\alpha_4 := -\mathrm{i}\beta$, we have

$$\begin{aligned}
\sigma(\alpha_1) &= \sigma(\beta) = \mathrm{i}\beta = \alpha_3\,, & \sigma(\alpha_3) &= \sigma(\mathrm{i}\beta) = \sigma(\mathrm{i})\sigma(\beta) = -\beta = \alpha_2\,,\\
\sigma(\alpha_2) &= \sigma(-\beta) = -\sigma(\beta) = -\mathrm{i}\beta = \alpha_4\,, & \sigma(\alpha_4) &= \sigma(-\mathrm{i}\beta) = -\sigma(\mathrm{i})\sigma(\beta) = \beta = \alpha_1\,,\\
\tau(\alpha_1) &= \tau(\beta) = \beta = \alpha_1\,, & \tau(\alpha_3) &= \tau(\mathrm{i}\beta) = \tau(\mathrm{i})\tau(\beta) = -\mathrm{i}\beta = \alpha_4\,,\\
\tau(\alpha_2) &= \tau(-\beta) = -\beta = \alpha_2\,, & \tau(\alpha_4) &= \tau(-\mathrm{i}\beta) = -\tau(\mathrm{i})\tau(\beta) = \mathrm{i}\beta = \alpha_3\,.
\end{aligned}$$

When $\rho : \mathrm{Gal}(L/\mathbb{Q}) \to \mathfrak{S}_4$ is the corresponding permutation group homomorphism, we see that $\rho(\sigma) = (4\ \ 1\ \ 3\ \ 2)$ and $\rho(\tau) = (4\ \ 3)$. Thus, we deduce that

$$\mathrm{Gal}(L/\mathbb{Q}) \cong \langle (4\ \ 1\ \ 3\ \ 2), (4\ \ 3) \rangle \subset \mathfrak{S}_4\,.$$

In particular, this Galois group is the Dihedral group of order 8 because

$$(4\ \ 1\ \ 3\ \ 2)^4 = \mathrm{id}_{[4]}\,, \quad (4\ \ 3)^2 = \mathrm{id}_{[4]}\,, \quad (4\ \ 3)(4\ \ 1\ \ 3\ \ 2)(4\ \ 3) = (4\ \ 2\ \ 3\ \ 1) = (4\ \ 1\ \ 3\ \ 2)^{-1}\,. \square$$

P8.3. Let L be the splitting field of $f := 2x^5 - 10x + 5$ over $\mathbb{Q}$. Prove that $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathfrak{S}_5$.

Solution. We first claim that the image of the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ in $\mathfrak{S}_5$ contains a 5-cycle. Since 5 does not divide 2, 5 divides -10 and 5, and $5^2 = 25$ does not divide 5, the Eisenstein criterion with $p = 5$ implies that the polynomial f is irreducible over $\mathbb{Q}$. When β is a root of f, it follows that $[\mathbb{Q}(\beta) : \mathbb{Q}] = 5$. Hence, the Tower Theorem gives $[L : \mathbb{Q}] = [L : \mathbb{Q}(\beta)][\mathbb{Q}(\beta) : \mathbb{Q}]$. Since every irreducible polynomial is separable over a field of characteristic zero, the field extension $\mathbb{Q} \subseteq L$ is separable. Because L is the splitting field of f over $\mathbb{Q}$, this field extension is also Galois. Hence, the equation $|\mathrm{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}]$ implies that 5 divides the order of the Galois group $|\mathrm{Gal}(L/\mathbb{Q})|$. The Cauchy theorem from group theory implies that $\mathrm{Gal}(L/\mathbb{Q})$ contains an element of order 5. Because the order of a permutation is the least common multiple of the lengths of its disjoint cycles, the image of the Galois group in $\mathfrak{S}_5$ contains a 5-cycle.

We next claim that the image of the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ in $\mathfrak{S}_5$ contains a 2-cycle. Observe that $f' = 10x^4 - 10 = 10(x^4 - 1)$, and

$$f(-1) = -2 + 10 + 5 = 13 > 0\,, \qquad f(1) = 2 - 10 + 5 = -3 < 0\,,$$
$$\lim_{x\to-\infty} f(x) = -\infty\,, \lim_{x\to\infty} f(x) = \infty\,.$$

Since $f'(x) = 0$ only at $x = \pm 1$, the polynomial f has exactly two critical points. From the sign changes above, it follows that f has exactly three real roots and two nonreal complex roots. Complex conjugation fixes the real roots and interchanges the two nonreal roots. Thus, the image of the Galois group in $\mathfrak{S}_5$ contains a 2-cycle.

We finally claim that the Galois group contains all adjacent transpositions. By relabeling the roots if necessary, we may assume that the image of the Galois group in $\mathfrak{S}_5$ contains the 5-cycle $(5\ \ 1\ \ 2\ \ 3\ \ 4)$ and the 2-cycle $(a\ \ 1)$ for some $a \in \{2, 3, 4, 5\}$. For every permutation $\sigma \in \mathfrak{S}_5$ and every $k \in \mathbb{N}$, we have $\sigma^k\ (a\ \ 1)\ \sigma^{-k} = (\sigma^k(a)\ \ \sigma^k(1))$. In particular, m the 2-cycle $(a\ \ 1)$ produces the 2-cycles $(a + k\ \ 1 + k)$ for all $k \in \mathbb{N}$, because the kth power of the 5-cycle satisfies $j \mapsto j + k \mod 5$ for all $j \in [5]$. When $a \in \{2, 5\}$, it follows that the image of the Galois group contains $(2\ \ 1)$. Similarly, when $a \in \{3, 4\}$, it follows that the image of the Galois group contains $(3\ \ 1)$ and $(4\ \ 1)$, so $(3\ \ 1)(4\ \ 1)(3\ \ 1) = (4\ \ 3)$. In either case, the image contains an adjacent transposition. Conjugating by the 5-cycle, the image contains all adjacent transpositions. We conclude that $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathfrak{S}_5$ because the symmetric group is generated by the adjacent 2-cycles. □