Problems Galois Theory

Adapted from `https://irma.math.unistra.fr/~guillot/`.

Warm-up exercise. Let K be the splitting field of $x^3 - 2$ over $\mathbb{Q}$. Show that $\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$.

1 Problem 1

1. Let K/F be a finite extension. Show that $|\mathrm{Gal}(K/F)|$ divides $[K : F]$.
2. Let K be a field of cardinality 49.
   (a) Explain why there exists $A \in K$ such that $K = \{0, 1, A, A^2, \cdots, A^{48}\}$.
   (b) Show that $K = \{x + yA,\ x, y \in \mathbb{F}_7\}$.
   (c) How many elements $B \in K$ satisfy the same property than A (*ie*, $K = \{0, 1, B, B^2, \cdots, B^{48}\}$) ? Are they of the form $\sigma(A)$ for $\sigma \in \mathrm{Gal}(K/\mathbb{F}_7)$?
3. Consider the following matrix with coefficients in $\mathbb{F}_7$:

$$A = \begin{pmatrix} 0 & 2 \\ 1 & 2 \end{pmatrix}.$$

   (a) Compute A^2 and show that $A^2 = 2I + 2A$.
   (b) Compute A^4 and A^8. Show that $A^{48} = I$ and $A^k \neq I,\ \forall 1 \leq k \leq 48$.
   (c) Show that $\{0, 1, A, A^2, \cdots, A^{48}\} = \{xI + yA,\ x, y \in \mathbb{F}_7\}$.
   (d) Denote K the set described in two different ways previous question. Show that K is a field of cardinality 49.
4. *(Harder)* Let p prime and let K be a field of cardinality p^2. Show that K can be seen as a subring of $M_2(\mathbb{F}_p)$.

2 Problem 2

1. Let $p > 2$ prime and let $\omega = e^{\frac{2i\pi}{p}}$. Let $L = \mathbb{Q}(\omega)$ and $F = L \cap \mathbb{R}$.
   (a) Show that $L/\mathbb{Q}$ is Galois and describe the Galois group.
   (b) Using the polynomial $(X - \omega)(X - \omega^{-1})$, show that $[L : F] = 2$.
   (c) Show that $F/\mathbb{Q}$ is Galois.
2. Let $a \in \mathbb{Q}_{>0}$ such that a does not admit any p^{th}-root in $\mathbb{Q}$, and let $\alpha = \sqrt[p]{a} \in \mathbb{R}$. Let $K = F(\alpha)$ and $N = L(\alpha) = \mathbb{Q}(\alpha, \omega)$. Draw a diagram describing the situation.
3. (a) Let f be the minimal polynomial of α over $\mathbb{Q}$. Show that f admits exactly one real root, and at least one non-real root.
   (b) Deduce that $\alpha \notin L$ *(use 1(c))*.
   (c) An extension is called *cyclic* if the corresponding Galois group is cyclic. Show that N/L is a cyclic extension and that $[N : L] = p$.
   (d) Deduce that $f = X^p - a$ and that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p$.
   (e) Show that $[N : K] \leq 2$ and $[K : F] \leq p$, then show that those are actually equalities.
4. We will describe $G = \mathrm{Gal}(N/F)$.
   (a) Show that N/F is Galois.
   (b) Show that there exists $\sigma \in G$ such that $\sigma(\alpha) = \alpha\,\omega$ and $\sigma(\omega) = \omega$.
   (c) Show that there exists $\tau \in G$ such that $\tau(\alpha) = \alpha$ and $\tau(\omega) = \omega^{-1}$.
   (d) Deduce the full description of G.

3 Problem 3

Let k be a field and $K = k(X)$ the field of fractions with coefficients in k. Let $\sigma \in \mathrm{Gal}(K/k)$ such that $\sigma(X) = 1/X$ and let $\tau \in \mathrm{Gal}(K/k)$ such that $\tau(X) = 1 - X$.

1. (a) Show that $\sigma^2 = I$, that $\tau^2 = I$ and that $\tau\sigma\tau = \sigma\tau\sigma$. Deduce $(\sigma\tau)^3 = I$.
   (b) Let $\rho = \sigma\tau$. Show that $\rho^3 = I$ and that $\sigma\rho = \rho^2\sigma$.
2. Let G the group generated by σ and τ. Deduce that G contains exactly 6 elements, that is, $I, \sigma, \tau, \sigma\tau, \tau\sigma, \tau\sigma\tau$. Deduce that $G \cong S_3$.
3. *(long and boring)* For every $g \in G$, compute $g(1 + X)$. Show that

$$u := \prod_{g \in G} g(1 + X) = -\frac{(X-2)^2(2X-1)^2(X+1)^2}{(X-1)^2X^2}.$$

4. Let $\mathfrak{g}$ be the smallest field containing G. Show that $\mathfrak{g} = k(u)$.

4 Problem 4

Let p be a prime number and $q = p^s$, let $\mathbb{F}_q$ be a field of cardinality q and let $\overline{\mathbb{F}_q}$ be the algebraic closure of $\mathbb{F}_q$.

1. Show that there exists a field K satisfying $\mathbb{F}_q \subset K \subset \overline{\mathbb{F}_q}$ and $[K : \mathbb{F}_q] \leq 2$ such that every equation of the form $aX^2 + bX + c = 0, \quad a, b, c \in \mathbb{F}_q$, admits a solution in K.
2. (a) Suppose $p > 2$. Show that there exists an element in $\mathbb{F}_q$ which doesn't admit any square root in $\mathbb{F}_q$.
   (b) Suppose $p = 2$. Show that there exists an element in $\mathbb{F}_q$ which is not of the form $X^2 + X$.
   (c) Deduce that there always exists an explicit irreducible polynomial of $\mathbb{F}_q[X]$ of degree 2.
3. Show that, for all $n \geq 1$, there exists an irreducible polynomial of degree n of $\mathbb{F}_q[X]$ *(it is not advised to use the previous question)*.

5 Problem 5

In this problem, we will compute the Galois group of $\mathbb{Q}\left(\sqrt{5}, \sqrt{11}, \sqrt{4+\sqrt{5}}\right)/\mathbb{Q}$.

1. Let $K = \mathbb{Q}(\sqrt{5}, \sqrt{11})$. Show that $K/\mathbb{Q}$ is Galois and that there exists $\sigma, \tau \in \mathrm{Gal}(K/\mathbb{Q})$ such that
$$\sigma(\sqrt{5}) = -\sqrt{5}; \quad \sigma(\sqrt{11}) = \sqrt{11}; \quad \tau(\sqrt{5}) = \sqrt{5}; \quad \tau(\sqrt{11}) = -\sqrt{11}.$$
2. Let $\alpha = 4 + \sqrt{5} \in K$. Compute $\alpha\sigma(\alpha)$, then show that for all $g \in \mathrm{Gal}(K/\mathbb{Q})$, it is possible to find $x \in K$ such that $g(\alpha) = \alpha x^2$.
3. Let $L = K(\sqrt{\alpha})$. Let $\phi : L \to \overline{\mathbb{Q}}$ be an homomorphism, where $\overline{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$. Show that $\phi(K) = K$ and $\phi(L) = L$. Deduce that $L/\mathbb{Q}$ is Galois.
4. We denote by $\tilde{\sigma}$ (resp. $\tilde{\tau}$) the element of $\mathrm{Gal}(L/\mathbb{Q})$ such that $\tilde{\sigma}|_K = \sigma$ (resp. $\tilde{\tau}|_K = \tau$). Show that $\tilde{\sigma}^2 = \tilde{\tau}^2 = I$ and that $\tilde{\sigma}\tilde{\tau}\tilde{\sigma}\tilde{\tau}$ is not the identity.
5. Show that $\mathrm{Gal}(L/\mathbb{Q})$ is a non-abelian group of order 8.
6. Deduce the full description of $\mathrm{Gal}(L/\mathbb{Q})$.

6 Problem 6

1. Let $p_1, \cdots, p_s$ be distinct odd primes and $k_1, \cdots k_s$ integers ≥ 0. Show that there exists a Galois extension $K/\mathbb{Q}$ such that
$$\mathrm{Gal}(K/\mathbb{Q}) \cong \prod_{i=1}^{s} \mathbb{Z}/p_i^{k_i}(p_i-1)\,\mathbb{Z}\,.$$
Adapt the previous formula in the case where there exists i such that $p_i = 2$.
2. Let $n \in \mathbb{Z}$. Show that there exists a Galois extension $L/\mathbb{Q}$ such that $\mathrm{Gal}(L/\mathbb{Q})$ is cyclic of order n.
3. Let s be an integer ≥ 1. Show that here exists a Galois extension $L/\mathbb{Q}$ such that
$$\mathrm{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/2\,\mathbb{Z})^s.$$
4. In this last question, we will use the following result, known as Dirichlet Theorem :

   Theorem 1. *For all $n \in \mathbb{Z}$ there exists infinitely many primes of the form $1 + dn$, with $d \in \mathbb{Z}$.*

   Show that for all finite abelian group A, there exists a Galois extension $L/\mathbb{Q}$ such that $\mathrm{Gal}(L/\mathbb{Q}) \cong A$.