Review problems

Problem 1. (1) Let $K = \mathbb{Q}[\sqrt{2}]$.

(a) Recall the definition of the norm $N : K \to \mathbb{Q}$ and justify why it has values in $\mathbb{Q}$.

(b) Show that if $x \in K$ is a square in K, then $N(x)$ is a square in $\mathbb{Q}$. Is $4 + 2\sqrt{2}$ a square in K ?

(2) Let $L = \mathbb{Q}[\sqrt{4 + 2\sqrt{2}}]$.

(a) Compute $[L : \mathbb{Q}]$. What is the minimal polynomial of $\sqrt{4 + 2\sqrt{2}}$ over K ? Over $\mathbb{Q}$?

(b) Show that $L/\mathbb{Q}$ is Galois. What is the cardinality of its Galois group G.

(c) Show that there is a unique $g \in G$ such that $g(\sqrt{4 + 2\sqrt{2}}) = \sqrt{4 - 2\sqrt{2}}$. What is the order of g ?

(d) What are the subfields of L ?

Problem 2. (On cyclic extensions) Let k be a perfect field, $n \geq 2$. We suppose that the set

$$\mu_n(k) = \{x \in k,\ x^n = 1\}$$

has cardinality n. In particular, it implies that the characteristic of k does not divide n.

(1) Show that $\mu_n(k)$ is a cyclic group of cardinality n. How many generators does it have ?

(2) Let $a \in k$ and K the stem field of $P := X^n - a$. It is generated over k by an element α such that $\alpha^n = a$. Show that K is also the splitting field of P.

Let G be the Galois group of K/k. We define the map

$$\kappa : G \to \mu_n(k),\ g \mapsto g(\alpha)/\alpha.$$

It is a morphism of groups.

(3) Show that κ is injective and $|G|$ divides n.

(4) Show that P is irreducible over k if and only if $[K : k] = n$ if and only if κ is surjective if and only if G is a cyclic group of order n.

(5) Suppose that P is not irreducible and let $|G| = d$ where d divides n strictly. Show that $\alpha^d \in k$.

(6) Show that P is irreducible over k if and only if « $\alpha^d \in k$ for $d|n$ » implies « $d = n$ ». *(Introduce a generator of $\mu_n(k)$ and $g \in G$ such that $\kappa(g) = \zeta$).*

(7) Show that P is irreducible over k if and only if the only divisor δ of n such that $X^\delta - a$ has a root in k is 1 (that is to say a is not a δ-power in k except for $\delta = 1$).

***Problem* 3.** Let $n \geq 1$ and ℓ a prime number. We say that $m \in \mathbb{Z}$ is not a ℓ-power in a subring A of $\mathbb{C}$ if the equation $x^\ell - m$ has no solution $x \in A$. We suppose that n is not a ℓ-power in $\mathbb{Z}$.

Let $\zeta := e^{2i\pi/\ell}$ and K the splitting field of $P = X^\ell - n$ over $\mathbb{Q}$.

(1) Show that $K = \mathbb{Q}(\zeta, \sqrt[\ell]{n})$.
(2) Let $x, y \in \mathbb{Q}$ such that $x^{\ell-1} = y^\ell$. Show that x is a ℓ-power in $\mathbb{Q}$. If $x \in \mathbb{Z}$, show that x is a ℓ-power in $\mathbb{Z}$.
(3) Suppose that n is a ℓ-power in $\mathbb{Q}[\zeta]$. Compute $N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(n)$ in two different ways and find a contradiction.
(4) Show that P is irreducible over $\mathbb{Q}[\zeta]$. (Use the result of Problem 2)
(5) Let G be the Galois group of K over $\mathbb{Q}$. Show that we have an exact sequence of groups
$$0 \to \mathbb{Z}/\ell\mathbb{Z} \to G \to (\mathbb{Z}/\ell\mathbb{Z})^\times \to 0.$$

***Problem* 4.** Let $n \geq 1$ and $G = \mathbb{Z}/n\mathbb{Z}$. Let $K/\mathbb{Q}$ a Galois extension with Galois group G and $x \in K$ generating $K/\mathbb{Q}$. Le P be the minimal polynomial of x over $\mathbb{Q}$.

(1) Why does x exist ?
(2) How many subfields L such that $[K : L] = 2$ does K contain ? Is L/K Galois ? If yes what is its Galois group ?
(3) How many subfields L such that $[L : \mathbb{Q}] = 2$ does K contain ? Is $K/\mathbb{Q}$ Galois ? If yes what is its Galois group ?

Let $\sigma \in \mathrm{Aut}(\mathbb{C})$ be the complex conjugation.

(4) Show that $\sigma(K) = K$.
(5) Suppose that n is odd. Show that in the natural embedding $G \hookrightarrow \mathfrak{S}_n$, the group G injects in $\mathfrak{A}_n$.
(6) Suppose that n is odd. Show that the restriction of σ to K is the identity.
(7) Suppose that $n = 4$, that $K \not\subset \mathbb{R}$ and let L be the unique subfield of K of degree 2 over $\mathbb{Q}$. Let $L' = K^\sigma$ be the subfield of K of the elements fixed by σ. Show that $L = L'$ and $L \subset \mathbb{R}$. Deduce that if $m \in \mathbb{Q}$ satisfies $\sqrt{m} \in K$ then $m \geq 0$.

***Problem* 5.** Write the Galois group of $X^{16} - 1$ over $\mathbb{Q}$ as a product of cyclic groups.

***Problem* 6.** Let $a \in \mathbb{Z}$. We want to show that the quadratic extension $\mathbb{Q}(\sqrt{a})$ of $\mathbb{Q}$ is contained in a cyclotomic extension of $\mathbb{Q}$.

(1) Show that it is true if $a = -1$ and $a = 2$.
(2) Let p be an odd prime number, $\zeta := e^{2i\pi/p}$ and $K = \mathbb{Q}(\zeta)$. We identify the Galois group of K with $(\mathbb{Z}/p\mathbb{Z})^\times$.
   (a) Show that $\sum_{1\leq i<p} \zeta^i = -1$ and that $\mathcal{B} := \{\zeta^k\}_{1\leq k\leq p-1}$ is a basis for the $\mathbb{Q}$-vector space K.
   (b) Show that the subset H of the squares in $(\mathbb{Z}/p\mathbb{Z})^\times$ is a subgroup of index 2.

(c) Let $x := \sum_{h\in H} h(\zeta)$. Show that x has degree 2 over $\mathbb{Q}$ and give a formula for its unique $\mathbb{Q}$-conjugate x'.

(d) Show that $x + x' = -1$ and $x^2 + x \in \mathbb{Q}$. We want to compute this element explicitly. Show that

$$x^2 + x = \sum_{g\in H} g(\zeta) + \sum_{g,g'\in H} g(\zeta)g'(\zeta)$$

and that $g(\zeta) \in \mathcal{B}$. Under which condition do we have $g(\zeta)g'(\zeta) = 1$?

(i) Suppose that $-1 \in H$. Show that there is a family $(a_i)_{1\le i<p}$ of elements in $\mathbb{Q}$ such that

$$x^2 + x = \frac{p-1}{2} + \sum_{1\le i<p} a_i\zeta^i$$

and $\sum_{1\le i<p} a_i = (p-1)^2/4$. Using (2)(a) show that $x^2 + x = (p-1)/4$ and find the value of x. What is $\mathbb{Q}(x)$?

(ii) Suppose that $-1 \notin H$. Show that there is a family $(a_i)_{1\le i<p}$ of elements in $\mathbb{Q}$ such that

$$x^2 + x = \sum_{1\le i<p} a_i\zeta^i$$

and $\sum_{1\le i<p} a_i = (p-1)(p+1)/4$. Using (2)(a) show that $x^2 + x = -(p+1)/4$ and find the value of x. What is $\mathbb{Q}(x)$?.

(3) For $n, m \ge 1$ show that $\mathbb{Q}(e^{2i\pi/n}, e^{2i\pi/m}) \subset \mathbb{Q}(e^{\frac{2i\pi}{nm}})$.

(4) Conclude.