Midterm Exam

You don't need to solve all the questions to get an excellent grade. Write your answers carefully and clearly to get full credit, use a scratch paper.

Problem 1. (1) Consider the Galois group G of $\mathbb{Q}(e^{2i\pi/35})/\mathbb{Q}$. How many subgroups of order 2 does G have ? Is G cyclic ? Justify.

(2) How many subfields of degree 12 over $\mathbb{Q}$ does $\mathbb{Q}(e^{2i\pi/35})$ contain ? Justify.

Problem 2. Let $P = X^5 + 20X + 16 \in \mathbb{Z}[X]$.

(1) Let $\bar{P} = P \mod 7 \in \mathbb{F}_7[X]$.
  (a) Find the roots in $\mathbb{F}_7$ of $\bar{P}$.
  (b) Show that the Galois group of $\bar{P}$ over $\mathbb{F}_7$ contains a 3-cycle.

(2) Let $\bar{P} = P \mod 3 \in \mathbb{F}_3[X]$.
  (a) Let $x \in \mathbb{F}_9$. Show that $x^5 = x$ or $x^5 = -x$.
  (b) Show that $\bar{P}$ has no root in $\mathbb{F}_9$.
  (c) Show that $\bar{P} \in \mathbb{F}_3[X]$ is irreducible.

Problem 3. (1) Let k be a perfect field with characteristic different from 2. Let $\bar{k}$ be an algebraic closure of k. For $P \in k[X]$ a separable polynomial with degree n, with roots $\{x_1, \ldots, x_n\}$ in $\bar{k}$, and Galois group G, we set

$$\mathrm{disc}(P) = (-1)^{n(n-1)/2} \prod_{i \neq j} (x_i - y_j) \text{ and } \delta = \prod_{i<j} (x_i - x_j).$$

We recall that $\delta^2 = \mathrm{disc}(P)$. We also recall the following result : when G is seen as a subgroup of $\mathfrak{S}_n$, we have

$$\sigma(\delta) = \epsilon(\sigma)\delta$$

for any $\sigma \in G$ where $\epsilon : \mathfrak{S}_n \to \{\pm 1\}$ denotes the signature.

  (a) Show that $\mathrm{disc}(P)$ is a square in k if and only if G is contained in the alternate group $\mathfrak{A}_n$.
  (b) We **admit** that $\mathrm{disc}(P) = (-1)^{n(n-1)/2} \prod_{i=1}^{n} P'(x_i)$. (It is not hard to prove).
  (c) For q an odd prime number, we choose $P = X^q - 1$. Let $q^* := \mathrm{disc}(X^q - 1)$.
    (i) At which condition on k is P separable ?
    (ii) Show, using (1)(b) that

$$q^* = (-1)^{q(q-1)/2} q^q.$$

(2) Let p and q be two distinct odd prime numbers. Let G be the Galois group of $X^q - 1$ over $\mathbb{Q}$.
  (a) We see G as a subgroup of $\mathfrak{S}_q$. Show that G is not contained in the alternate group $\mathfrak{A}_q$.
  (b) Show that G is cyclic.

END OF THE EXAM

The following questions are not to be solved for the exam.

We identify G with the group $(\mathbb{Z}/q\mathbb{Z})^*$. We denote by 1 the unit element in G. Since q is odd, we have $-1 \not\equiv 1 \mod q$ and we denote the element $-1 \bmod q$ of G simply by -1.

(c) Show that the map

$$\begin{aligned} \Psi : G &\longrightarrow \{\pm 1\} \\ g &\longmapsto g^{(q-1)/2} \end{aligned}$$

is a well defined surjective morphism of groups. For $g \in G$ we use the following notation :

$$\left(\frac{g}{q}\right) := \Psi(g)$$

.

(d) Show that the kernel H of Ψ is the unique subgroup of G of index 2 (that is to say such that $|G| = 2|H|$).

(e) Show that H is the image of the morphism of groups $G \to G$, $g \mapsto g^2$.

(f) What is the kernel of

$$G \hookrightarrow \mathfrak{S}_q \xrightarrow{\epsilon} \{\pm 1\}?$$

(g) Show that for any $g \in G$ seen as an element of $\mathfrak{S}_q$ we have $\epsilon(g) = \left(\frac{g}{q}\right)$.

(h) Let $\zeta := e^{2i\pi/q}$. Show that there is a unique $f \in G$ such that $f(\zeta) = \zeta^p$.

(i) Why can p be seen as an element of G ? Check that

$$\left(\frac{p}{q}\right) = 1 \text{ if and only if } p \text{ is a square mod } q.$$

(j) Show that $f \in H$ if and only if p is a square mod q. Show that $\epsilon(f) = \left(\frac{p}{q}\right)$.

(k) Let $A = \mathbb{Z}[\zeta]$. We recall that there is $\mathcal{P}$ a maximal ideal of A such that $\mathcal{P} \cap \mathbb{Z} = p\mathbb{Z}$.

(i) Recall why $K := A/\mathcal{P}$ is a finite field of characteristic p.

(ii) We know that the decomposition subgroup $D := \{g \in G,\ g(\mathcal{P}) = \mathcal{P}\}$ of G is isomorphic to $\mathrm{Gal}(K/\mathbb{F}_p)$. Show that in this isomorphism, the element $f \in G$ corresponds to the Frobenius of $K/\mathbb{F}_p$ (show first that $f \in D$).

(iii) Why is there an embedding of $\mathrm{Gal}(K/\mathbb{F}_p)$ in $\mathfrak{S}_q$ which is compatible with the embedding of G in $\mathfrak{S}_q$ via the isomorphism of the previous question ?
Show that the Frobenius of $K/\mathbb{F}_p$ is in $\mathfrak{A}_q$ if and only if q^* is a square modulo p if and only if $((-1)^{(q-1)/2}q)^{(p-1)/2} = 1$.

(iv) Prove the quadratic reciprocity law :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

(3) Prove the result of Question (1)(b).