Field and Galois Theory
Semestral Exam
Nov. 2023

Time: 3 hours

Max score: 50

Answer any **5** questions.

1. (a) Show that the extension $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$ is a simple extension, for every prime p and for every $n \in \mathbb{Z}^+$.
(b) Show that the polynomial $x^{p^n} - x$ is precisely the product of all the distinct monic irreducible polynomials in $\mathbb{F}_p[x]$ of degree d, where d runs over all divisors of n. (5+5)

2. (a) Show that a finite extension K/F is a simple extension if and only if there are only finitely many subfields of K containing F.
(b) Let p be a prime. Let $K = \mathbb{F}_p(X, Y)$ be the field of rational functions in two variables X and Y, and $F = \mathbb{F}_p(X^p, Y^p) \subset K$. Using part (a) above, or otherwise, show that K/F is not a simple extension. $(5 + 5)$

3. (a) Prove that there exists a subfield E of a cyclotomic field such that $\mathrm{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}_{14}$
(b) Let $K = \mathbb{Q}(\zeta)$, where $\zeta = \cos(\frac{2\pi}{17}) + \sin(\frac{2\pi}{17})i$. Then
(i) Prove that K contains a unique subfield L such that $[L : \mathbb{Q}] = 8$.
(ii) Prove that L is a Galois extension of $\mathbb{Q}$.
(iii) Find an element $\alpha \in L$ such that $L = \mathbb{Q}(\alpha)$. $(5 + 5)$

4. (a) Let $f(x) \in F[x]$ be a separable polynomial of degree n, where $char(F) \neq 2$. Show that the Galois group of $f(x)$ is a subgroup of the alternating group A_n if and only if the discriminant of $f(x)$ is the square of an element of F.
(b) Show that the Galois group of $f(x) = x^5 - 6x + 3$ over $\mathbb{Q}$ is S_5. $(5 + 5)$

5. Let $n \in \mathbb{Z}^+$. Let F be a field such that of $\mathrm{char}(F)$ does not divide n and F contains the nth roots of unity.
(a) Show that for any $a \in F$, the extension $F(\sqrt[n]{a})$ over F is a cyclic extension of degree dividing n.
(b) Prove that any cyclic extension of degree n over F is of the form $F(\sqrt[n]{a})$ for some $a \in F$. $(4 + 6)$

6. Find a polynomial $f(x)$ of degree 7 whose Galois group over $\mathbb{Q}$ is S_7. (10)

****