B3.1 Galois Theory Sheet 4 (MT 2018)

In these problems K denotes an arbitrary field and $K[x]$ denotes the ring of polynomials in one variable x over K. If p is a prime number, then $\mathbb{F}_p$ denotes the field of integers modulo p.

1. Find the Galois groups of the following polynomials over $\mathbb{Q}$:

   (a) $x^5 - 2x^3 - x^2 + 2$;

   (b) $x^5 - 2$;

   (c) $x^5 - 4x + 2$.

2. In this exercise you will complete the characterization of finite fields. Let L be a finite field. Recall that there exists a prime number p, and a positive integer n such that $|L| = p^n$. Recall that $(L^*, \cdot)$ is a cyclic group.

   (a) Show that there exists an irreducible polynomial $g(x) \in \mathbb{F}_p[x]$ such that $L \cong \mathbb{F}_p[x]/(g(x))$

   (b) Show that L is a Galois extension of $\mathbb{F}_p$.

   (c) Show that, up to isomorphism, there exists a unique finite field of cardinality p^n. This finite field is denoted by $\mathbb{F}_{p^n}$.

   (d) Show that the map $\varphi : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$ defined by $\varphi(y) := y^p$ is an automorphism of $\mathbb{F}_{p^n}$. This map is called the *Frobenius automorphism*.

   (e) Show that $\Gamma(\mathbb{F}_{p^n} : \mathbb{F}_p) \cong (\mathbb{Z}/n\mathbb{Z}, +)$.

   (f) Deduce that there is exactly one subfield of $\mathbb{F}_{p^n}$ for any divisor d of n.

   (g) Let $f \in \mathbb{F}_p[x]$ be an irreducible polynomial. Show that f splits into linear factors in $\mathbb{F}_{p^{\deg(f)}}$.

3. Let p be an odd prime, $K = \mathbb{F}_p(t)$, and $f = x^4 - t \in K[x]$.

   (a) Find the splitting field E of f distinguishing the cases $p \equiv 1 \mod 4$ and $p \equiv 3 \mod 4$. (Hint: if α is a root of f, find $c \in E$ such that $c\alpha$ is a root of f).

   (b) Write down a set of generators for $\Gamma(E : K)$ distinguishing the cases $p \equiv 1 \mod 4$ and $p \equiv 3 \mod 4$.

   (c) In the case $p \equiv 1 \mod 4$ write down the Galois correspondence for $E : K$ and $\Gamma(E : K)$.

4. Let L/K be a finite separable extension of field. Define a *Galois Closure* M of L/K as a minimal degree extension of L for which M/K is Galois. Show that the Galois Closure of L/K exists and is unique up to isomorphism. Show that the set of K-invariant embeddings $\hom_K(L, M)$ of L in M is in natural bijection with the set of right cosets of $\Gamma(M : L)$ in $\Gamma(M : K)$.

5. Let ℓ be a positive integer, p be a prime number, and $f_\ell = x^{2^\ell} + 1 \in \mathbb{F}_p[x]$. If $N > 1$ is an integer, we denote by $U(\mathbb{Z}/N\mathbb{Z})$ the set of invertible elements of the ring $\mathbb{Z}/N\mathbb{Z}$. Recall that $(U(\mathbb{Z}/N\mathbb{Z}), \cdot)$ is a multiplicative group.

   (a) Show that any polynomial of degree 2 in $\mathbb{F}_p[x]$ splits in $\mathbb{F}_{p^2}[x]$.

   (b) Show that for $p = 3$ the polynomial f_1 is irreducible in $\mathbb{F}_3[x]$ and give a construction of the field $\mathbb{F}_{3^2}$.

   (c) Show that the splitting field of f_ℓ is isomorphic to the splitting field of $x^{2^{\ell+1}} - 1 \in \mathbb{F}_p[x]$.

   (d) Prove that for $p = 5$ the polynomial $f_2 \in \mathbb{F}_5[x]$ is reducible.

   (e) Show that there exists an integer ℓ such that for any prime number p, the polynomial f_ℓ is reducible in $\mathbb{F}_p[x]$. (Hint: show first that $(U(\mathbb{Z}/2^n\mathbb{Z}), \cdot)$ is not a cyclic group if $n \geq 3$).