# MAT 5210 Homework 3

1. Let $\Phi_m(x) \in \mathbb{C}[x]$ be the $m$-th cyclotomic polynomial, the monic polynomial whose roots are the primitive $m$-th roots of 1 in $\mathbb{C}$. Show that

   (a) $\Phi_1(x) = x - 1$; $\Phi_2(x) = x + 1$; $\Phi_3(x) = x^2 + x + 1$; $\Phi_4(x) = x^2 + 1$.

   (b) $\prod_{d|m} \Phi_d(x) = x^m - 1$.

   (c) $\Phi_m(x) \in \mathbb{Z}[x]$. [Hint: prove first that $\Phi_m(x) \in \mathbb{Q}[x]$ by induction on $m$].

   (d) If $p$ is prime then $\Phi_p(x) = 1 + x + x^2 + \cdots + x^{p-1}$ and $\Phi_{p^n}(x) = \Phi_p(x^{p^{n-1}})$.

   (e) $\deg \Phi_{nm} = \deg \Phi_m \deg \Phi_n$ if $(m, n)$ are relatively prime.

2. Find the Galois groups of the following polynomials and for each subgroup identify the corresponding subfield of the splitting field:

   (a) $x^2 + 1$ over $\mathbb{R}$;

   (b) $x^3 - 1$ over $\mathbb{Q}$;

   (c) $x^3 - 5$ over $\mathbb{Q}$;

   (d) $x^6 - 3x^3 + 2$ over $\mathbb{Q}$;

   (e) $x^5 - 1$ over $\mathbb{Q}$;

   (f) $x^6 + x^3 + 1$ over $\mathbb{Q}$.

3. Prove that $\mathbb{Q}(\sqrt{2 + \sqrt{2}})$ is Galois over $\mathbb{Q}$, and find its Galois group.

4. Find the Galois group of the polynomial $x^{p^n} - x - t$ over $\mathbb{F}_{p^n}(t)$ (you can assume that this polynomial is irreducible over $\mathbb{F}_{p^n}(t)$).

5. 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 $p \equiv 1 \bmod 4$ and $p \equiv 3 \bmod 4$. (Hint: if $\alpha$ 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 $Gal(E/K)$ distinguishing the cases $p \equiv 1 \bmod 4$ and $p \equiv 3 \bmod 4$.

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

6. 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 $Gal(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong (\mathbb{Z}/n\mathbb{Z}, +)$.

7. Let $\ell$ 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 $(\mathbb{Z}/N\mathbb{Z})^*$ the set of invertible elements of the ring $\mathbb{Z}/N\mathbb{Z}$. Recall that $((\mathbb{Z}/N\mathbb{Z})^*, \cdot)$ 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 $f_\ell$ 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 $\ell$ such that for any prime number $p$, the polynomial $f_\ell$ is reducible in $\mathbb{F}_p[x]$. (Hint: show first that $((\mathbb{Z}/2^n\mathbb{Z})^*, \cdot)$ is not a cyclic group if $n \geq 3$).