

Math 5031 - Homework 12

Due 12/05/05

- Splitting fields and Galois groups of polynomials.** For each of the following polynomials (i) find the splitting field, K , over \mathbb{Q} , (ii) determine the degree of the extension, $[K : \mathbb{Q}]$, (iii) find the Galois group $G(K : \mathbb{Q})$, and (iv) find all the intermediate fields between \mathbb{Q} and K .
 - $X^2 - 4X + 4$;
 - $X^2 - 2X + 4$;
 - $X^4 - 2$;
 - $X^3 - 2$;
 - $X^6 - 3x^3 + 2$.
- Finite fields.** Recall that if K is any field, the kernel of the ring homomorphism $\eta : \mathbb{Z} \rightarrow K$ sending n to $n \cdot 1$, where 1 is the unity in K , is either 0 or the maximal ideal $(p) \subseteq \mathbb{Z}$ for some prime p . Suppose that K is a finite field. Then the kernel of η is non-zero and K is said to have characteristic p . The image $\eta(\mathbb{Z})$ is isomorphic to $\mathbb{Z}/(p)$, which we also denote by \mathbb{F}_p . We can regard \mathbb{F}_p as a subfield of K and write $n = [K : \mathbb{F}_p]$.
 - If K is a finite field, show that K has cardinality $q = p^n$, and that $a^q - a = 0$ for all $a \in K$.
 - For any given prime p and positive integer n , show that a field with cardinality $q = p^n$ exists and is unique up to isomorphism. We denote this field by \mathbb{F}_q . (Define \mathbb{F}_q as a splitting field of $X^q - X$.)
 - Show that the multiplicative group of units, \mathbb{F}_q^* , is cyclic. (More generally, show that if K is any field, then every finite subgroup of K^* is cyclic.)
 - Show that the Galois group $G(K : \mathbb{F}_p)$, for $K \cong \mathbb{F}_q$, is cyclic of order n , where $q = p^n$. A generating element is given by the *Frobenius map* $\phi_p : K \rightarrow K$, $\phi_p(a) = a^p$. (Check that ϕ_p is indeed a \mathbb{F}_p -automorphism for any field K of characteristic p .)
 - If L is a field extension of k and both L and k are finite fields, show that L is a Galois extension of k . If $k \cong \mathbb{F}_q$ and $L \cong \mathbb{F}_{q'}$, show that $\sigma(a) = a^q$ is a generator for the Galois group $G(L : k)$.