

Math 536 Homework 11
Spring 2008
Due: Friday, April 18

1. Let p be a prime number. The goal of this exercise is to show that for each integer $n \geq 1$ there exists a field F with p^n elements. On the last homework we already showed that such a field, if it exists, is unique up to isomorphism.
 - (a) Let $q = p^n$, and let F be a splitting field of the polynomial $f(X) = X^q - X \in \mathbb{F}_p[X]$. Show that every element of F is a root of $f(X)$.
(Hint: We know that F is generated by the roots of f over \mathbb{F}_p , so one of the things you have to show is that anything “generated by roots α, β ” is again a root.)
 - (b) Show that $f(X)$ has no multiple roots. Deduce that F has exactly $q = p^n$ elements.
2. Let α be a complex root of $X^6 + X^3 + 1$. Find all homomorphisms $\sigma : \mathbb{Q}(\alpha) \rightarrow \mathbb{C}$. (Hint: The polynomial is a factor of $X^9 - 1$. Also, we have already discussed some properties of this polynomial on Homework 8.)
3. Let E, F be two finite extensions of a field k , contained in a larger field K . Show that

$$[EF : k] \leq [E : k][F : k].$$

Here EF denotes the compositum of E and F in K .

If $[E : k]$ and $[F : k]$ are relatively prime, show that one has an equality sign in the above relation.

4. Describe the splitting fields of the following polynomials over \mathbb{Q} , and find the degree of each such splitting field.
 - (a) $X^2 - 2$
 - (b) $X^3 - 2$
 - (c) $(X^3 - 2)(X^2 - 2)$
 - (d) $X^2 + X + 1$
 - (e) $X^6 + X^3 + 1$
5. Let ζ be a primitive 7-th root of unity, say $\zeta = e^{2\pi i/7}$. In this exercise we will analyze the extension $\mathbb{Q}[\zeta]/\mathbb{Q}$.
 - (a) Show that the extension $\mathbb{Q}[\zeta]/\mathbb{Q}$ is a Galois extension. What is $\text{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$?
 - (b) Show that the automorphism σ of E which sends ζ to ζ^3 generates $\text{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$.
 - (c) What is the subfield of $\mathbb{Q}[\zeta]$ that is fixed by the subgroup $\langle \sigma^2 \rangle$ of $\text{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$?