PROBLEM SET 8 – DUE THURSDAY AUGUST 5.

Degree of a field extension

Let F be a field and let K be a larger field containing F. We will say that some elements, $x_1, x_2, \ldots, x_m$ are a ***basis*** for K over F if every element y of K can be written in exactly one way as $\sum a_i x_i$ for coefficients a_i in F.

Problem 1. (1) Give a basis for $\mathbb{Q}[\sqrt{2}]$ over $\mathbb{Q}$.
(2) Give a basis for $\mathbb{Q}[\sqrt[3]{2}]$ over $\mathbb{Q}$.
(3) Give a basis for $\mathbb{Q}[\omega]$ over $\mathbb{Q}$, where ω is a primitive cube root of unity.
(4) Give a basis for $\mathbb{Q}[\omega, \sqrt[3]{2}]$. You may assume (but it is even better to prove it!) that $x^3 - 2$ remains irreducible over $\mathbb{Q}[\omega]$.

Problem 2. Let $x_1, x_2, \ldots, x_m$ and $y_1, y_2, \ldots, y_n$ be two bases for K over F. In this problem, we will show that $m = n$.

(1) Show that there are constants A_{ij} in F such that $y_j = \sum_i A_{ij} x_i$.

Suppose, for the sake of contradiction, that $m < n$. By the Key Lemma of Linear Algebra (Problem Set 6), there are constants $(c_1, c_2, \ldots, c_n)$, not all zero, such that $\sum_j A_{ij} c_j = 0$ for $1 \leq i \leq m$.

(2) Show that $\sum_j c_j y_j = 0$.
(3) Explain why this contradicts the assumption that the y_j are a basis.

Thus, any two bases of K over F have the same cardinality. We define the ***degree of K over F*** to be the cardinality for a basis of K over F. We are deliberately omitting the question of whether every field has a basis in order to avoid issues with the Axiom of Choice, but the next two problems will cover any case we need.

Problem 3. Let F be a field and let K be a larger field containing F. Suppose that there is an element θ in K such that $K = F(\theta)$, let $m(x)$ be the degree of the minimal polynomial of θ over F, and let n be the degree of $m(x)$. Show that $1, \theta, \theta^2, \ldots, \theta^{n-1}$ is a basis for K over F.

Problem 4. Let $F \subset K \subset L$ be a chain of fields. Suppose that $x_1, x_2, \ldots, x_m$ is a basis of K over F and $y_1, y_2, \ldots, y_n$ is a basis of L over K. Show that the mn numbers $x_i y_j$ are a basis for L over F.

Problem 5. Let F be a field and let $f(x)$ be an irreducible polynomial in $F[x]$. Suppose that K is a larger field containing F and that $f(x)$ has a root in K. Show that, if K has a basis over F, then the degree of K over F is divisible by the degree of $f(x)$.

Finite fields – part one

Problem 6. Let F be a field with finitely many elements.

(1) Show that there is a positive integer n such that $n = 0$ in F
(2) Let p be the least positive integer which is 0 in F (WOP!). Show that p is prime.

The integer p is called the ***characteristic of F***.

Problem 7. Let p be a prime number and let q be a power of p. Let F be a field of characteristic p. Show that the set of solutions to $x^q = x$ in F is a subfield of F.