PROBLEM SET 9 – DUE MONDAY AUGUST 9.

Finite fields – part two

Let F be a field with finitely many elements. In this problem set, you will show that $\#(F)$ is a prime power and that, for each prime power, there is exactly one field of that size.

Problem 1. Back on Problem Set 8, we learned that there was a prime number p, called the characteristic of F, such that $p = 0$ in F, so $\mathbb{Z}_p$ is a subfield of F.

(1) Show that F has a basis over $\mathbb{Z}_p$.
(2) Letting n be the degree of F over $\mathbb{Z}_p$. Show that $|F| = p^n$.

Problem 2. Let p be prime and let $q = p^n$ be a power of p. Let $\mathbb{F}_q$ be the splitting field of the polynomial $x^q - x$. Show that $\mathbb{F}_q$ has q elements, all of which are roots of $x^q - x$.

Problem 3. Let p be prime, let $q = p^n$ be a power of p and let F be a field with q elements.

(1) Let u be any element of F. Show that $u^q = u$. (Hint: Think about how we proved Fermat's Little Theorem.)
(2) Show that there is an isomorphism $\mathbb{F}_q \to F$.

Commutators

Recall that, if G is a group and g_1, g_2 are two elements of G, the ***commutator*** of g_1 and g_2 is $g_1 g_2 g_1^{-1} g_2^{-1}$. The ***commutator subgroup*** of G is the subgroup of G generated by the commutators of G.

Problem 4. Compute the commutator subgroups of the following groups:

$$S_3, \quad A_3, \quad S_4, \quad A_4, \quad S_5 \quad \text{and} \quad A_5.$$

Problem 5. Let G be a group and let H be its commutator subgroup.

(1) Show that H is a normal subgroup (see Problem Set 3) of G.
(2) Show that G/H (see Problem Set 5) is abelian.

The fixed field of the automorphism group

Problem 6. Let $F \subseteq L$ be fields and let L be a splitting field of some polynomial in $F[x]$. Let ρ be an element of L. Suppose that every element of $\mathrm{Aut}(L/F)$ fixes ρ.

(1) Show that the minimal polynomial of ρ over F is of the form $(x-\rho)^n$ for some positive integer n. This is just about quoting the right result from class.
(2) Suppose that, in the field F, we have $n \neq 0$ for all positive integers n. Conclude that ρ is in F.

Here is an example to show that we needed the hypothesis on the characteristic of F in the previous part. Let L be the field of rational functions $\mathbb{F}_p(t)$ and let F be the subfield $\mathbb{F}_p(t^p)$.

(3) Show that L is the splitting field of $x^p - t^p$ over F.
(4) Show that $\mathrm{Aut}(L/F)$ is the trivial group, and, in particular, it fixes t.

We have not actually used the word "Galois group" in this class. A field extension $F \subseteq L$ is called ***Galois*** if L is a splitting field and F is the fixed field of $\mathrm{Aut}(L/F)$, as this problem shows, in characteristic zero, the second condition follows from the first. In this case, $\mathrm{Aut}(L/F)$ is called the ***Galois group*** of L over F.