Homework Assignment 1

Assigned Mon 01/10. Due Fri 01/14.

1. Suppose F (with binary operations $+$, $\cdot$) is some field, and assume all quantities referenced in this problem are elements of F. Do this problem using *only* the basic field axioms.
   (a) Show that the additive (and multiplicative) identity in a field is unique. [To help you get started, here's what you should do: Suppose 0 and $0'$ were two (additive) identities. Show that $0 = 0'$.]
   (b) Show that $-a = (-1)a$. [To explain the notation, the left hand side is the additive inverse of a. The right hand side is the additive inverse of 1 multiplied by a.]
   (c) If $a \neq 0$, and $ab = ac$ then show $b = c$.
   (d) Show that $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$, provided $b, d \neq 0$. [We *define* $\frac{a}{b} = a \cdot b^{-1}$, where b^{-1} is the (unique) multiplicative inverse of b.]

2. Suppose the set $F = \{0, 1, \alpha, \beta\}$ with binary operations $+$ and $\cdot$ form a field. Construct the addition and multiplication for F (i.e. draw two tables – one showing how to add all possible pairs of elements in F, and the other showing how to multiply all possible pairs of elements in F). [It turns out that there is exactly one way to do this. You don't have to justify your steps or work for this question. Just the final answer will suffice.]

3. Let F be a field, and $n \in \mathbb{N}$. We define $n! \in F$ by

$$n! = \underbrace{(1 + 1 + \cdots + 1)}_{n\text{-times}}(n-1)!$$

   and $0! = 1$. Notice that the standard definition $n! = n(n-1)!$ can't really be used here, since there is no reason for any given natural number n to be an element of the filed F. However, no matter what the field F is, we are guaranteed $1 \in F$, so our definition makes sense (and further $n! \in F$). Now if $n, m \in \mathbb{N}$ with $m \leqslant n$, we define the binomial coefficient $\binom{n}{m}$ by $\binom{n}{m} = \frac{n!}{m!(n-m)!} \in F$. If $a, b \in F$ and $n \in \mathbb{N}$ show that

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

   Here we use the convention that for any $a \in F$, $n \in \mathbb{N}$, $a^n = \underbrace{a \cdot a \cdots a}_{n\text{-times}}$, and $a^0 = 1$ by definition.

4. (a) Suppose F is a field with an even number of elements (i.e. the cardinality of the set F is both finite and even). Show that $1 + 1 = 0$ in F. [Hint: Show first that $\exists a \in F$ such that $a \neq 0$ and $a + a = 0$.]
   (b) Suppose now F is a field with an odd number of elements. Show that $1 + 1 \neq 0$ in F.

[$\star$] 5. *(Optional. Do, but don't turn this in. Read the policy on optional HW for more info.)*
   (a) Suppose F is a *finite* set, and that $+, \cdot$ are two binary operations on F which satisfy all the field axioms *except* (possibly) the existence of multiplicative inverses. Suppose further, $\forall a, b \in F$, $ab = 0$ implies that $a = 0$ or $b = 0$. Show that F must in fact be a field.
   (b) Let p be prime, and $F = \{0, 1, \dots, p-1\}$. Define $+$ and $\cdot$ to be addition and multiplication (respectively) modulo p. (That is, for $a, b \in F$ define $a + b$ to be the remainder of the sum of a and b when divided by p.) Show that F is a field. [The only field axiom you should explicitly check is the existence of multiplicative inverses.]