Yale University Department of Mathematics
**Math 225 Linear Algebra and Matrix Theory**
Spring 2015

Problem Set # 2 (due in class Thursday 5 February, postponed due to Nor'easter Juno!)

**Notation:** Let $F$ be a field, $0_F$ its (unique) additive identity, and $1_F$ its unique multiplicative identity. Recall that $\mathbb{Z} = \{\dots, -2, -1, 0, 1, \dots\}$ is the set of integers. There is a natural map $\iota : \mathbb{Z} \to F$ defined as follows: if $n = 0$ then $\iota(0) = 0_F$; if $n > 0$ then $\iota(n) = 1_F + \cdots + 1_F$ is the sum of $1_F$ with itself taken $n$ times; if $n < 0$, then $\iota(n) = -\iota(|n|)$.

We say that the field $F$ has **characteristic zero** if $\iota(n) = 0_F$ is only possible when $n = 0$. However, this can fail. For a prime number $p$, we say that $F$ has **characteristic** $p$ if $\iota(p) = 0_F$. For example, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ have characteristic zero, while $\mathbb{F}_p$ has characteristic $p$. It is a theorem from abstract algebra that a field either has characteristic zero or it has characteristic $p$ for a unique prime number $p$.

Let $S$ and $T$ be sets and $f : S \to T$ be a map. We say that $f$ is **injective** (or **one-to-one**) if $f(x) = f(y) \Rightarrow x = y$ (i.e., no two elements in $S$ get mapped to the same element). We say that $f$ is **surjective** (or **onto**) if for every $y \in T$ there exists an element $x \in S$ with $f(x) = y$ (i.e., every element in $T$ gets mapped to). We say that $f$ is **bijective** (or **one-to-one and onto**) if $f$ is injective and surjective. The **cardinality** of a finite set $S$ is the number of elements in $S$.

**Pigeon Hole Principle.** *If $n$ pigeons are put into $m$ pigeonholes, and $n > m$, then there is at least one pigeonhole with more than one pigeon.*

A variant of the pigeonhole principle is the following useful theorem.

**Theorem.** *Let $S$ and $T$ be finite sets of the same cardinality. Then a function $f : S \to T$ is injective if and only if it is surjective.*

**Reading:** FIS 1.4–1.6

**Problems:**

**1.** FIS 1.4 Exercises 1 (Either cite, prove, or provide a counterexample), 3bc (Show your work), 5h (Show your work), 11, 13, 15.

**2.** FIS 1.5 Exercises 1 (Either cite, prove, or provide a counterexample), 2bcd, 3 (Just stare at it, you do not need to show your work), 8 (In part a, the book writes $R$ for $\mathbb{R}$), 9, 10, 11 (The book writes $Z_2$ for $\mathbb{F}_2$), 12, 18 , 20.

**3.** FIS 1.6 Exercises 1 (If true, then either cite or prove it, it false then provide a counterexample), 2bd (Show your work), 14, 19, 24.

**4.** Let $F$ be a field. Prove that two vectors $(a, b)$ and $(c, d)$ in $F^2$ are linearly dependent if $ad-bc = 0$ and are linearly independent if $ad - bc \neq 0$ (**Hint.** Try using the contrapositive and §1.5 #9).

**5.** In this problem, you will prove that $\mathbb{F}_p$ really is a field. The outstanding issue was the existence of multiplicative inverses. You can proceed by proving the following multiple lemmas.

**Lemma 0.1.** *Prove that for $a, b \in \mathbb{F}_p$, if $ab = 0$ then either $a = 0$ or $b = 0$.*

**Hint.** You can use the following fact about prime numbers: if $a$ and $b$ are integers not divisible by a prime number $p$, then $ab$ is not divisible by $p$ (this is a consequence of "prime factorization").

**Lemma 0.2.** *For $a \in \mathbb{F}_p$, consider the map $f_a : \mathbb{F}_p \to \mathbb{F}_p$ defined by $f_a(x) = ax$. Prove that if $a \neq 0$ then $f_a$ is injective.*

Finally, use pigeons (and pigeon holes) to conclude with a proof of:

**Theorem 0.3.** *Each nonzero element of $\mathbb{F}_p$ has a multiplicative inverse.*

Yale University, Department of Mathematics, 10 Hillhouse Ave, New Haven, CT 06511
*E-mail address*: asher.auel@yale.edu