Yale University Department of Mathematics
Math 225 Linear Algebra and Matrix Theory
Spring 2014

Problem Set # 3 (due 4 pm Wednesday 5 February 2014)

Notation: 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 1.6, 2.1

Problems:

1. 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.

2. FIS 2.1 Exercises 1 (If true, then either cite or prove it, it false then provide a counterexample), 3, 5, 9, 11, 16, 21.

3. Let F be a field and $V = F^3$. Let $W \subseteq V$ be the subspace of vectors with zero component sum, i.e., vectors (a, b, c) such that $a + b + c = 0$. Let $S = \{(1, 1, 0),\ (1, 0, 1),\ (0, 1, 1)\} \subseteq V$.

(1) Prove that if the characteristic of V is not 2, then S is a basis for V.
(2) Prove that if the characteristic of V is 2, then S generates W. Find a subset of S that is a basis for W.

4. 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 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 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 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