LINEAR ALGEBRA HOMEWORK 1

LECTURER: BONG H. LIAN

This homework offers warm-up exercises on sets: you will work with various set notions like memberships, subsets, intersections, unions, disjointness, and partitions. You will also work with maps of various kinds: injective, surjective, and bijective.

Exercise 0.1. *WRITE UP This exercise will show that 'fractions' is a way to break up a particular set*

$$\mathcal{P} \equiv \widetilde{\mathbb{Z}^2} := \{(a,b) \in \mathbb{Z}^2 | b \neq 0\}$$

into smaller subsets – namely fractions. A fraction is of the form

$$a/b := \{(m,n) \in \mathcal{P} | an = bm\}.$$

Prove that two fractions are either equal or disjoint. For this reason, we say that the fractions form a **partition** *of* $\mathcal{P}$*.*

(1) *Prove that* $a/b = a'/b'$ *iff* $ab' = ba'$*.*
(2) *Prove that* $a/b \cap a'/b' = \emptyset$ *(i.e. the two sets have no members in common) iff* $ab' \neq ba'$*.*

(3) *Prove that the map* $\iota : \mathbb{Z} \to \mathbb{Q}$*,* $n \mapsto n/1$ *is injective. Therefore, we can treat* $\mathbb{Z}$ *as a subset of* $\mathbb{Q}$ *by treating set* $n/1$ *as the integer* n*.*
(4) *Prove that this map is not surjective, i.e. there is a fraction* $b/a \in \mathbb{Q}$ *which is not* $\iota(c)$ *for any* $c \in \mathbb{Z}$*.*

Exercise 0.2. *Verify that the multiplication rule given by*

$$\times : \mathbb{Q}^2 \to \mathbb{Q}, \ (a/b, a'/b') \mapsto a/b \times a'/b' := (aa')/(bb')$$

is well-defined. Note that this rule generalizes the usual rule for multiplying integers, i.e. grouping apples. Therefore, the multiplication rule for $\mathbb{Z}$ *remains the same after we treat it as a subset of* $\mathbb{Q}$*. (See next exercise.)*

(1) *Prove using this multiplication rule, that* a/b *is a solution to the equation* $bx = a$*. That is,* $b \times a/b = a$*.)*
(2) *Prove that this is the only solution. That is, if* a'/b' *is another solution, then* $a'/b' = a/b$*.*

Exercise 0.3. *Write For* $n \in \mathbb{Z}$*, put* $\iota(n) = n/1$*. Verify the identities*

$$\iota(1) = 1/1, \quad \iota(nn') = \iota(n)\iota(n'), \quad n, n' \in \mathbb{Z}.$$

Also express $\iota(n + n')$ *in terms of* $\iota(n)$*,* $\iota(n')$*.*

Exercise 0.4. *Let F be a field. For $X, Y, Z \in F^2$ and $\lambda, \mu \in F$, verify that*
V1. $(X + Y) + Z = X + (Y + Z)$
V2. $X + Y = Y + X$
V3. $X + 0 = X$
V4. $X + (-X) = 0$
V5. $\lambda(X + Y) = \lambda X + \lambda Y$
V6. $(\lambda + \mu)X = \lambda X + \mu X$
V7. $(\lambda\mu)X = \lambda(\mu X)$
V8. $1X = X$.
Here $\lambda(x_1, x_2) := (\lambda x_1, \lambda x_2)$. The same holds true for F^n, the n-times Cartesian product $F^n = F \times \cdots \times F$.
Suggestion: *Think about exactly what facts about F you need to use to prove each of these statements.*

Exercise 0.5. *WRITE UP Recall that for a given field F, we have a* **characteristic map** *defined by*

$$\iota_F : \mathbb{Z} \to F, \quad n \mapsto n \cdot 1_F.$$

We say that F has characteristics p if there exists a smallest positive integer p such that $\iota_F(p) = 0_F$. If such a p does not exists, we say that F has characteristics 0.

- *(1) What is the characteristics of the field $\mathbb{Q}$? Prove your answer.*
- *(2) Prove that if F is finite then p exists and it must be a prime number.*
- *(3) Fix a prime number p. For each integer, put*

  $$\bar{a} = a + p\mathbb{Z} := \{a + pn | n \in \mathbb{Z}\} = \{..., a - p, a, a + p, a + 2p, ...\}.$$

  Define the set

  $$\mathbb{Z}/p := \{a + p\mathbb{Z} | a \in \mathbb{Z}\}.$$

  Consider the map

  $$f_p : [p] := \{0, 1, ..., p - 1\} \to \mathbb{Z}/p, \quad a \mapsto \bar{a} := a + p\mathbb{Z}.$$

  Show that f_p is a bijection, hence $\#\mathbb{Z}/p = p$.
- *(4) Show that the set $\mathbb{Z}/p$ can be made a field with distinguished members $\bar{0}, \bar{1}$, by giving it 4 operations $+, \times, -, 1/\cdot$. Therefore, for every prime number p, you have constructed a* **finite field** *$\mathbb{F}_p$ with p members.*