EXTRA CREDIT #3

MATH 217 – SECTION 4

We've recently been introduced to abstract *real* vector spaces. The *real* means that we use real numbers ($\mathbb{R}$) as our scalar set. In this extra credit assignment, we'll introduce other sets of scalars we can use instead of the real numbers. To do this, we need to introduce the notion of a field.

A field K is a set of elements satisfying the following properties.

(i) For every two elements $r, s \in K$, there is a way to add them to get another element $r + s \in K$. (Recall, the expression $a \in A$ means that a is an element in the set A).
(ii) For every two elements $r, s \in K$, there is a way to multiply them to get another element $rs \in K$.
(iii) For every $r, s \in K$, we have $r + s = s + r$.
(iv) For every $r, s, t \in K$, we have $r + (s + t) = (r + s) + t$.
(v) There is an element $0 \in K$ such that $r + 0 = r$ for every $r \in K$.
(vi) For every element $r \in K$, there is an element $-r \in K$ such that $(-r) + r = 0$.
(vii) For every two elements $r, s \in K$, $rs = sr$.
(viii) For every two elements $r, s, t \in K$, $r(st) = (rs)t$.
(ix) There is an element $1 \in K$ such that $1r = r$ for every element $r \in K$.
(x) For every non-zero element $r \in K$, there is an element $\frac{1}{r} in K$ such that $r(\frac{1}{r}) = 1$.
(xi) For every elements $r, s, t \in K$, we have $r(s + t) = rs + rt$.

The first example of a field you've run across is the real numbers, but there are many others.

For example, consider the set of fractions $\frac{a}{b}$ where a and b are integers and $b \neq 0$ (integers are whole numbers that can be positive or negative). The set of these numbers (thought of as a subset of the real numbers) form a field under the usual addition and multiplication. This field is denoted by $\mathbb{Q}$ and is called the *rational numbers* or simply the *rationals*.

Exercise 0.1. Prove that the "zero" element whose existence is guaranteed by (v) is unique. That is, suppose that $0'$ is another element that also satisfies the property of (v), prove that $0' = 0$. (1 point)

In a similar way, one can prove that the 1 element from property (ix) is unique.

Exercise 0.2. Prove that multiplicative inverses are unique, that is, prove that if r is an element and s is any other element such that $rs = 1$, then $s = \frac{1}{r}$. (1 point)

Exercise 0.3. Suppose that L is a field and that $f \in L$. Prove that $0f = 0$ and $f0 = 0$. Hint: What is $0 + 0$? (1 point)

Exercise 0.4. Suppose that L is a field and that $f, g \in K$. If $fg = 0$, prove that either $f = 0$ or $g = 0$ (it's also possible that they are both zero). (1 point)

We are now going to construct another field besides $\mathbb{R}$ and $\mathbb{Q}$. Let K be the set of all real numbers that can be expressed as $u + v\sqrt{2}$ where $u, v \in Q$.

Exercise 0.5. Prove that K is a field. (2 points) Hint: Pay particular attention to how to satisfy property (x). Let $u + v\sqrt{2} \in K$, consider $u - v\sqrt{2}$. Is the product of these two elements in $\mathbb{Q}$? Can the product of these two elements be zero? (2 points)

The field K constructed above usually denoted by $\mathbb{Q}[\sqrt{2}]$.

The set of complex numbers $\mathbb{C}$ is also a field. In particular, let $\mathbb{C}$ be set of all elements $r + si$ where $r, s \in R$. We define $i^2 = -1$ (i is thought of as the square root of -1). Using this, we say that $(r + si)(u + vi) = ru + rvi + usi - sv = (ru - sv) + (rv + us)i$. And so we have defined how the multiplication works.

Exercise 0.6. Prove that $\mathbb{C}$ is a field. (2 points)

Given any field K, one can define a *K-vector space* to be a set of objects satisfying the properties in the book, but we use the "scalar set" K instead of $\mathbb{R}$.

Exercise 0.7. Explain why $\mathbb{C}$ is a $\mathbb{R}$-vector space (a real vector space). What is it's dimension? Explain why $\mathbb{R}$ and $\mathbb{Q}[\sqrt{2}]$ are both $\mathbb{Q}$ vector spaces. What is the dimension of $\mathbb{Q}[\sqrt{2}]$ as a $\mathbb{Q}$ vector space? (2 points)

We conclude with a more exotic sort of field, a finite field.

Let $\mathbb{Z}$ be the set of integers and let p be a prime positive integer. Consider the set of numbers $\{0, 1, 2, 3, \ldots, p - 2, p - 1\}$. We add and multiply these numbers using modular (clock) arithmetic.

So suppose that $p = 7$ and we want to add the numbers 5 and 6. We would normally get $5 + 6 = 11$, but using modular arithmetic, we would call this sum 4 (after you get to 7 you loop around to zero, 4 is also the remainder you get when you divide 11 by 7). When we multiply, we get the same thing, $(5)(6) = 30$ usually, but we would interpret this number as $(5)(6) = 2$ (the remainder when you divide 30 by 7 is 2). Another way of saying this is that 30 mod 7 is the same as 2 mod 7 (it's also the same as 9 mod 7 and -5 mod 7. This set of these numbers with these operations is denoted by $\mathbb{Z}/(p)$.

First we do a couple exercises just to introduce you to modular (clock) arithmetic.

Exercise 0.8. Suppose p is a prime and that a mod p is the same as b mod p. Show that $a - b$ is a multiple of p. (1 point)

Exercise 0.9. In some sense, it doesn't really matter how you represent your numbers. Suppose p is a prime and that a mod p is the same as b mod p. If c is any number such that $0 \leq c < p$, show that $a + c$ mod p is the same as $b + c$ mod p. Likewise show that ac mod p is the same as bc mod p. (1 point)

The final problem of this extra credit set is to prove that $\mathbb{Z}/(p)$ is a field.

Exercise 0.10. Prove that $\mathbb{Z}/(p)$ is a field. (3 points).