NOTES ON FIELDS

SANTIAGO CAÑEZ

Fields are the objects which provide us with the scalars we use in linear algebra. Here we give the full definition of a field, and review the examples we have seen and will see in class.

Definition 1. *A field is a set $\mathbb{F}$ together with an addition operation*

$$(a, b) \mapsto a + b$$

and a multiplication operation

$$(a, b) \mapsto ab$$

such that the following hold:

- *(Associativity) For all $a, b, c \in \mathbb{F}$, $(a + b) + c = a + (b + c)$ and $(ab)c = a(bc)$,*
- *(Commutativity) For all $a, b \in \mathbb{F}$, $a + b = b + a$ and $ab = ba$,*
- *(Distributivity) For all $a, b, c \in \mathbb{F}$, $a(b + c) = ab + ac$,*
- *(Identities) There exist elements $0 \in \mathbb{F}$ and $1 \in \mathbb{F}$ such that $0 \neq 1$ and for any $a \in \mathbb{F}$, $0 + a = a$ and $1a = a$,*
- *(Inverses) For any $a \in \mathbb{F}$, there exists an element $-a \in \mathbb{F}$ such that $a+(-a) = 0$; if further $a \neq 0$, there exists an element $a^{-1} \in \mathbb{F}$ such that $aa^{-1} = 1$.*

Of course, it is implicitly assumed that adding two elements of $\mathbb{F}$ still gives something in $\mathbb{F}$ and similarly for multiplication. Fields are a fundamental object of study in Math 114, but we will only need to know about a few basic examples.

Example 1. The set, $\mathbb{Q}$, of rational numbers is a field; explicitly, it is given by

$$\mathbb{Q} := \left\{ \frac{p}{q} \;\middle|\; p, q \in \mathbb{Z} \text{ and } q \neq 0 \right\}.$$

The field operations are just the usual addition and scalar multiplication, and the inverse of p/q is q/p. In fact, $\mathbb{Q}$ is an example of a "subfield" of $\mathbb{R}$.

Example 2. Let $\mathbb{F}$ be a field. Then we can form a new field $\mathbb{F}(x)$, called the field of rational functions over $\mathbb{F}$, by setting

$$\mathbb{F}(x) := \left\{ \frac{p(x)}{q(x)} \;\middle|\; p, q \in P(\mathbb{F}) \text{ and } q \neq 0 \right\},$$

where $P(\mathbb{F})$ denotes the space of polynomials with coefficients in $\mathbb{F}$. So, $\mathbb{F}(x)$ simply consists of fractions of such polynomials. The addition and multiplication operations are the usual ones for fractions, keeping in mind that whenever we have to add or multiply coefficients we use the operations of $\mathbb{F}$. Again, the inverse of $p(x)/q(x)$ is $q(x)/p(x)$.

Example 3. Let p be a prime number — that is, a positive integer greater than 1 whose only factors are itself and 1. Then we can form a field called the *integers mod* p and denoted by $\mathbb{Z}_p$ as follows.

The elements of $\mathbb{Z}_p$ are the possible remainders you can get when dividing an integer by p:

$$\mathbb{Z}_p := \{0, 1, 2, \dots, p-1\}.$$

Actually, you should think that $\mathbb{Z}_p$ consists of all integers, but two integers are declared to be the same in $\mathbb{Z}_p$ if they give the same remainder when dividing by p. For example, since the remainder when dividing 9 by 7 is 2, we say that

$$9 = 2 \text{ in } \mathbb{Z}_7.$$

Addition and multiplication are defined as the usual operations for integers, with the extra caveat that you have to take the remainder of the result when dividing by p to get an element of $\mathbb{Z}_p$. So, for example, since $3 \cdot 3 = 9$, we have that

$$3^2 = 2 \text{ in } \mathbb{Z}_7.$$

The phrase "in $\mathbb{Z}_p$" is so common that we usually just replace it by "mod p"; so for example, $3^2 = 2 \bmod 7$.

The only property which may seem non-obvious is the existence of multiplicative inverses. Recall that the multiplicative inverse of an element $a \in \mathbb{Z}_p$ should be an element $a^{-1} \in \mathbb{Z}_p$ so that

$$aa^{-1} = 1.$$

In $\mathbb{Z}_7$, since $3 \cdot 5 = 15 = 1 \bmod 7$, we have that

$$3^{-1} = 5 \bmod 7.$$

One can show, using properties of prime numbers, that any nonzero element of $\mathbb{Z}_p$ has a multiplicative inverse, so that $\mathbb{Z}_p$ is in fact a field.

It may be helpful to consider what happens when p is not prime, for example, why is $\mathbb{Z}_4$ not a field? We have the following equations in $\mathbb{Z}_4$:

$$2 \cdot 0 = 0$$
$$2 \cdot 1 = 2$$
$$2 \cdot 2 = 0$$
$$2 \cdot 3 = 2.$$

Hence we see that 2 does not have a multiplicative inverse in $\mathbb{Z}_4$, so $\mathbb{Z}_4$ is not a field. In any $\mathbb{Z}_m$ with m not prime, there always exists a nonzero element without a multiplicative inverse; indeed, if m is not prime and n is a factor of m, then n does not have a multiplicative inverse in $\mathbb{Z}_m$. Thus $\mathbb{Z}_m$ is a field if and only if m is prime

In this course, $\mathbb{R}$ and $\mathbb{C}$ are the most important fields we will work with. However, as I have said, from time to time we will use some other fields to illustrate a few points. It is important to realize that most of the theorems about abstract vector spaces we cover in this class also hold for vector spaces over arbitrary fields