1. Sep. 3, 2013, first class

We shall discuss linear algebra this semester and the object of study is a vector space. The simplest vector spaces are $\mathbb{R}^n$, $n = 1, 2, 3$. These are “real” vector spaces, or vector spaces defined over the real number field $\mathbb{R}$. Most of the vector spaces we shall discuss are real vector spaces, but we will briefly encounter “complex” vector spaces later in this course. In general, a vector space can be defined over a field. So let me start with a brief introduction of “field” and properties of real numbers. I shall assume that you are familiar with natural numbers $\mathbb{N}$, integers $\mathbb{Z}$, and rational numbers $\mathbb{Q}$. We can perform addition and multiplication in $\mathbb{N}$ but not subtraction or division. In $\mathbb{Z}$, we can do both addition and subtraction and we can take the “negative” of an element in $\mathbb{Z}$. For rational numbers $\mathbb{Q}$, we can perform “addition”, “multiplication”, “subtraction”, and “division” and make sense of the “negative” and the “reciprocal” of an element in $\mathbb{Q}$. Recall that as a set

$$\mathbb{Q} = \{ \frac{p}{q} : p, q \in \mathbb{Z}, q > 0, \text{ and } p, q \text{ are coprime} \}.$$ 

$\mathbb{Q}$ is a “field” and here is the definition:

**Definition 1.** A field is a set that is equipped with two operations “addition +” and “multiplication ·” such that the following nine axioms hold:

1. Commutative law for addition.
2. Associative law for addition.
3. Existence of identity element for addition (or existence of “0”).
5. Commutative law for multiplication.
6. Associative law for multiplication.
7. Existence of identity element for multiplication (or existence of “1”).
8. Existence of reciprocals.

*Date: September 5, 2013.*
It is easy to check that $\mathbb{Q}$ is a field and $\mathbb{Z}$ is not. The simplest field is $\mathbb{Z}_p$ for a (positive) prime number $p$. The set consists of equivalence classes of integers defined by the following equivalence relation $\sim_p$: for $a, b \in \mathbb{Z}$, $a \sim_p b$ if $a - b$ is divisible by $p$.

We recall the definition of “equivalence relation”:

**Definition 2.** An equivalence relation on a set is a binary relation that is reflexive, symmetric, and transitive.

These properties allow us to define equivalence classes and each element of the set belongs to one and only one equivalence class. It is not hard to check that the relation $\sim_p$ is an equivalence relation in $\mathbb{Z}$. The quotient space is the set of equivalence classes. For example, in $\mathbb{Z}_2$, the equivalence class of 0, $[0]$ consists of all even integers and the equivalence class of 1, $[1]$ consists of all odd integers. There are only two elements in $\mathbb{Z}_2 = \{[0], [1]\}$.

We can then define “addition” and “multiplication” in $\mathbb{Z}_p$ by $[a] + [b] = [a + b]$ and $[a] \cdot [b] = [a \cdot b]$. Whenever an operation is defined on the quotient set by an equivalence relation, it is important to check that the operation is well-defined, or is independent of the choice of representative in each equivalence class. For example, if $a_1 \sim_p a_2$ and $b_1 \sim_p b_2$, is $a_1 + b_1 \sim_p a_2 + b_2$?

**Proposition 1.** Both addition and multiplication are well-defined on $\mathbb{Z}_p$.

**Proof.**

**Exercise 1.** Write down the multiplication table for $\mathbb{Z}_5$ and find the reciprocal of each non-zero element.

To show that $\mathbb{Z}_p$ is a field, we show that all nine axioms hold. In particular, we need to identify the zero and identity elements in $\mathbb{Z}_p = \{[0], [1], \cdots , [p-1]\}$. The most difficult axiom to check is the existence of reciprocals. It suffices to show if $[x] \neq [0]$, then there exists a $[y]$ such that $[x] \cdot [y] = [1]$, or

**Proposition 2.** Given an integer $x$ not divisible by $p$, there exists an integer $y$ such that $x \cdot y = 1 + k \cdot p$ for some $k \in \mathbb{Z}$.

**Proof.** We prove by contradiction.
(1) Check that $\sim_p$ is an equivalence relation on $\mathbb{Z}$ so that each element $a$ of $\mathbb{Z}$ belongs to one and only one equivalence class $[a]$.

(2) Define addition and multiplication on $\mathbb{Z}/\sim_p = \mathbb{Z}/\sim_p$ by $[a] + [b] = [a+b]$ and $[a] \cdot [b] = [a\cdot b]$ and check that both operations are well-defined (i.e. independent of choice of representatives from each equivalence class).

(3) Given any $[x] \neq [0]$, show that there exists a $[y]$ such that $[x] \cdot [y] = [1]$. This corresponds to the existence of reciprocals axiom.

(4) Check that $+$, $\cdot$, $[0]$, and $[1]$ satisfy all nine axioms of a field.

We shall see that the real number system is also a field. Before that, we need to define real numbers $\mathbb{R}$. We know that there are real numbers that are not rational numbers, for example, the solution(s) of $x^2 = 2$.

**Proposition 3.** There is no rational number that solves the equation $x^2 = 2$

**Proof.** We prove by contradiction.

This shows that if we want to solve the quadratic equation $x^2 = 2$, we need to go beyond rational numbers. In contrast, if we just want to solve a linear equation of integer coefficients such as $ax + b = 0$ for $a, b \in \mathbb{Z}$, we can stay in rational numbers. Notice that we cannot solve $x^2 = 2$ in $\mathbb{Z}_3$ either.

Even we cannot solve $x^2 = 2$ in rational numbers, we can still approximate the solution by rational numbers and this is often how we solve a problem in reality. For example, we know that the solution is between 1.4 and 1.5 because $(1.4)^2 < 2$ and $(1.5)^2 > 2$ and we know that the solution is between 1.41 and 1.42 because $(1.41)^2 < 2$ and $(1.42)^2 > 2$. In this way, we get a sequence of approximate (lower) solutions: $a_1 = 1.4, a_2 = 1.41, a_3 = 1.414, a_4 = 1.4142, \cdots$ that will eventually “converge” to an actual solution. Notice that each member of the sequence is a rational number, but we do not expect the “limit” to be rational. We can write the sequence in the following form

$$a_n = 1 + \sum_{j=1}^{n} \frac{d_j}{10^j},$$

where $d_1 = 4, d_2 = 1, d_3 = 4, d_4 = 2, \cdots$ are all digits. At the $n$-th step, we choose the largest integer $d_n$ with $0 \leq d_n \leq 9$ such that $a_n^2 \leq 2$. Notice that $a_{n+1} - a_n = \frac{d_{n+1}}{10^{n+1}} \leq \frac{1}{10^n}$. In fact, we have $|a_m - a_n| \leq \frac{1}{10^n}$ if $m \geq n$ because we do not alter the $n$-th digit after the $n$-step.

The above example shows there are “gaps” in rational numbers, and real numbers fill these “gaps”. We shall consider $\mathbb{R}$ as an extension of $\mathbb{Q}$ through a limiting process and thus a real number is considered as a
Definition 3. A sequence \( \{a_n\}_{n \in \mathbb{N}} \) of rational numbers is said to be a Cauchy sequence if for every \( \epsilon > 0 \), there exists an \( N_0 \in \mathbb{N} \) such that if both \( n, m \geq N_0 \), then \( |a_n - a_m| < \epsilon \).

Proposition 4. An infinite decimal expansion is a Cauchy sequence. Let \( d_n \) be a sequence of integers with \( 0 \leq d_n \leq 9 \) for each \( n \in \mathbb{N} \), define \( a_n = \sum_{j=1}^{n} \frac{d_j}{10^j} \). Then \( \{a_n\} \) is a Cauchy sequence.

Proof. We do a preliminary estimate of \( |a_n - a_m| \) before the formal proof. Suppose \( n \geq m \), we compute
\[
a_n - a_m = \sum_{j=m+1}^{n} \frac{d_j}{10^j}.
\]
Since \( d_j \leq 9 \), we have
\[
a_n - a_m \leq 9 \sum_{j=m+1}^{n} \frac{1}{10^j} = 9 \left( \frac{1}{10^{m+1}} + \cdots + \frac{1}{10^n} \right) = \frac{9}{10^{m}} \left( \frac{1}{10} + \cdots + \frac{1}{10^{n-m}} \right).
\]
Recall the formula
\[
r + \cdots + r^k = r \left( \frac{1 - r^k}{1 - r} \right)
\]
if \( |r| < 1 \).
Thus \( a_n - a_m = \frac{9}{10^{m}} \left( \frac{1 - \frac{1}{10^{n-m}}}{1 - \frac{1}{10}} \right) \) Since \( 1 - \frac{1}{10^{n-m}} < 1 \), taking the absolute value and simplifying the expression, we obtain
\[
|a_n - a_m| < \frac{1}{10^m}
\]
for any \( n \geq m \).

Here is the formal proof: Given any \( \epsilon > 0 \), there exists an \( N_0 \) such that \( \frac{1}{10^{N_0}} < \epsilon \) (this comes from the Archimedean property). Now if both \( n \) and \( m \) are \( \geq N_0 \), we claim that \( |a_n - a_m| < \epsilon \). Suppose \( n \geq m \), by the above estimate we have \( |a_n - a_m| < \frac{1}{10^m} \) but \( m \geq N_0 \) and thus \( |a_n - a_m| < \frac{1}{10^{N_0}} < \epsilon \). If \( m \geq n \), we get \( |a_n - a_m| < \frac{1}{10^m} \) but \( n \geq N_0 \) and thus \( |a_n - a_m| < \frac{1}{10^{N_0}} < \epsilon \).

Definition 4. A sequence \( \{a_n\}_{n \in \mathbb{N}} \) of rational numbers is said to converge to a rational number \( L \) if for every \( \epsilon > 0 \), there exists an \( N_0 \in \mathbb{N} \) such that if \( n \geq N_0 \) then \( |a_n - L| < \epsilon \). Such a sequence is called a convergent sequence of rational numbers and we write \( \lim_{n \to \infty} a_n = L \).
Proposition 5. Any convergent sequence of rational numbers is a Cauchy sequence.

Proof. Suppose \( \{a_n\} \) is a sequence that converges to \( L \), we need to show that for every \( \epsilon > 0 \), there exists an \( N_0 \) such that if both \( n, m \geq N_0 \), then \( |a_n - a_m| < \epsilon \). By assumption, for any given \( \epsilon > 0 \), we can find an \( N_0 \) such that \( n \geq N_0 \) implies \( |a_n - L| < \frac{\epsilon}{2} \). We claim this \( N_0 \) satisfies the desired property. Suppose both \( n, m \geq N_0 \), we have \( |a_n - L| < \frac{\epsilon}{2} \) and \( |a_m - L| < \frac{\epsilon}{2} \). By the triangle inequality, \( |a_n - a_m| = |a_n - L + L - a_m| \leq |a_n - L| + |a_m - L| < \frac{\epsilon}{2} + \frac{\epsilon}{2} \). Therefore \( |a_n - a_m| < \epsilon \) as long as both \( n, m \geq N_0 \).

\[ \square \]

The converse of the statement is not true and not every Cauchy sequence of rational numbers converges to a rational number. We can show that sequence \( a_1 = 1.4, a_2 = 1.41, a_3 = 1.414, a_4 = 1.4142, \cdots \), if ever converges, must converge to a root of \( x^2 = 2 \), but we know the root cannot be a rational number. The rational number system is incomplete in this sense. We complete the rational numbers by adding all Cauchy sequences of rational numbers. However, there are some redundancy that we need to take care of first.

Definition 5. We say two Cauchy sequences \( \{a_n\} \) and \( \{b_n\} \) of rational numbers are equivalent, or \( \{a_n\} \sim \{b_n\} \), if the sequence \( \{a_n - b_n\} \) converges to zero.

It is not hard to show that \( \sim \) is an equivalence relation of Cauchy sequences of rational numbers.

Example 1. For example, the sequences,

\[ 100, 1, 1, 1, \cdots \]

and

\[ 0.9, 0.99, 0.999, \cdots \] (a repeating decimal)

are equivalent Cauchy sequences.