Fields besides the Real Numbers
Math 130 Linear Algebra

D Joyce, Fall 2015

Most of the time in linear algebra, our vectors will have coordinates that are real numbers, that is to say, our scalar field is **R**, the real numbers.

But linear algebra works over other fields, too, like **C**, the complex numbers. In fact, when we discuss eigenvalues and eigenvectors, we'll need to do linear algebra over **C**. Some of the applications of linear algebra such as solving linear differential equations require **C** as as well.

Some applications in computer science use linear algebra over a two-element field $\mathbf{Z}_2$ (described below). That's appropriate because the unit of storage in a computer is a bit, and a bit can have only have two values, 0 and 1.

In number theory and algebraic geometry other finite fields besides $\mathbf{Z}_2$ come in handy.

In general, if you have what's called a *field*, you can form vectors with coordinates in that field, and most everything that you can say about real matrices and real vectors also holds for matrices and vectors over that field, Not everything, however. In particular, things related to eigenvalues and eigenvectors depend on the field.

Fields. Informally, a field is a set equipped with four operations—addition, subtraction, multiplication, and division that have the usual properties. (They don't have to have the other operations that the field of real numbers **R** has, like powers, roots, logs, and the myriad functions like $\sin x$.) Here's an informal definition for fields.

Definition 1 (Field)**.** A *field* is a set equipped with two binary operations, one called *addition* and the other called *multiplication*, denoted in the usual manner, which are both commutative and associative, both have identity elements (the additive identity denoted 0 and the multiplicative identity denoted 1), addition has inverse elements (the additive inverse of x denoted $-x$ as usual), multiplication has inverses of nonzero elements (the multiplicative inverse of x denoted $\frac{1}{x}$ or x^{-1}), multiplication distributes over addition, and $0 \neq 1$.

Of course, one example of a field is the field of real numbers **R**. What are some others?

Example 2 (The field of rational numbers, **Q**)**.** Another example is the field of rational numbers. A rational number is the quotient of two integers a/b where the denominator is not 0. The set of all rational numbers is denoted **Q**. We're familiar with the fact that the sum, difference, product, and quotient (when the denominator is not zero) of rational numbers is another rational number, so **Q** has all the operations it needs to be a field, and since it's part of the field of the real numbers **R**, its operations have the the properties necessary to be a field. We say that **Q** is a *subfield* of **R** and that **R** is an *extension* of **Q**. But **Q** is not all of **R** since there are irrational numbers like $\sqrt{2}$.

Example 3 (The field of complex numbers, **C**)**.** Yet another example is the field of complex numbers **C**. A complex number is a number of the form $a + bi$ where a and b are real numbers and $i^2 = -1$. The field of real numbers **R** is a subfield of **C**. We'll review complex numbers before we use them. See my *Dave's Short Course on Complex Numbers* at `http://www.clarku.edu/∼djoyce/complex/`

Finite fields Finite fields are studied in number theory, and the field of two elements is useful in logic and computer science. Finite fields are based on the concept of congruence modulo n, where n is a positive integer.

Definition 4. Fix n, a positive integer. We say that two integers x and y are *congruent modulo n* if n divides the difference $x - y$ with no remainder. We'll use the standard notation from number theory

$$x \equiv y \pmod{n}$$

to indicate that x is congruent to y modulo n, and the notation $n|m$ to indicate that the integer n divides the integer m (with no remainder). Then

$$x \equiv y \pmod{n} \quad \text{iff} \quad n\big|(x-y).$$

When n doesn't divide the difference $x-y$, we say a is not congruent to b, denoted $x \not\equiv y \pmod{n}$.

You're familiar with congruence modulo 12; it's what 12-hour clocks use. For example,

$$11 + 2 \equiv 1 \pmod{12}$$

since 2 hours after 11 o'clock is 1 o'clock.

The set of integers modulo n is denoted $\mathbf{Z}/n\mathbf{Z}$, or more simply $\mathbf{Z}_n$, and it has operations of addition, subraction, and multiplication that it inherits from the integers. In the special case when n is prime, and and in that case we'll denote it p, then $\mathbf{Z}_p$ turns out to be a field, called the Galois field of characteristic p and denoted $GF(p)$.

Example 5. We'll be most interested in the field $\mathbf{Z}_2$ of two elements. Note that there is only one nonzero element, namely 1, and it is its own inverse. The addition and multiplication tables for $\mathbf{Z}_2$ are particularly simple.

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Note that subtraction is the same as addition in $\mathbf{Z}_2$ since $x - y \equiv x + y \pmod{2}$.

Each entry in a matrix over $\mathbf{Z}_2$ is either 0 or 1.

A vector over $\mathbf{Z}_2$ is often called a *bitstring.* For example, $(1,0,0,1,1,0)$ is a vector in ${\mathbf{Z}_2}^6$. Bitstrings are often denoted more simply without parentheses and commas, e.g., 100110.

Example 6. $\mathbf{Z}_3$. Here, there are two nonzero elements, namely 1 and 2, but, for symmetry's sake, we'll call the two nonzero elements 1 and -1. Note that each of these two are their own inverses. The addition and multiplication tables are still pretty simple.

$+$	-1	0	1
-1	1	-1	0
0	-1	0	1
1	0	1	-1

$\cdot$	-1	0	1
-1	1	0	-1
0	0	0	0
1	-1	0	1

Usually we'll use the letter F to denote a generic field. As most of linear algebra applies to vector spaces over any field F, we'll state our theorems relative to a generic field F. Typically, however, for examples, the field F will be the field of real numbers $\mathbf{R}$.

Math 130 Home Page at
`http://math.clarku.edu/~ma130/`