Math 24
Winter 2010
Monday, January 4

In class today we discussed fields, which are defined in Appendix C of your textbook. All you really need to know about fields for this course is the following:

Important examples of fields are the real numbers $\mathbb{R}$, the complex numbers $\mathbb{C}$, and the rational numbers $\mathbb{Q}$.

Two other, rather different, examples of fields are the two-element field $\mathbb{Z}/2\mathbb{Z}$ (also denoted F_2) and the three-element field $\mathbb{Z}/3\mathbb{Z}$ (also denoted F_3). These are the integers modulo 2 and modulo 3 respectively. If you are not familiar with modular arithmetic, you can define these fields as follows.

The elements of F_2 are $\overline{0}$ and $\overline{1}$ (which you can think of as "even" and "odd"). The operations are given by the following tables.

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

The elements of F_3 are $\overline{0}$, $\overline{1}$ and $\overline{2}$. The operations are given by the following tables.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

These fields differ from each other in their *characteristic*. The fields $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Q}$ are all of characteristic zero, which means that

$$1 + 1 + \cdots + 1 \neq 0.$$

The fields F_2 and F_3 are of finite characteristic, which means that adding 1 to itself a finite number of times will eventually yield zero. Specifically, in F_2 we have $1 + 1 = 0$; we say that F_2 has characteristic 2. Similarly, in F_3 we have $1 + 1 + 1 = 0$; we say that F_3 has characteristic 3.

Now, here are some things about fields that you do not need to know for this course, but may be interested in.

For any integer $n \geq 2$ we can define the integers modulo n, or $\mathbb{Z}/n\mathbb{Z}$. (The notation $\mathbb{Z}/n\mathbb{Z}$ will make a little more sense to you when we encounter a similar notation in our study of vector spaces.) The elements of $\mathbb{Z}/n\mathbb{Z}$ are $\overline{0}$, $\overline{1}$, $\ldots$, $\overline{n-1}$. To add and multiply modulo n, add and multiply as usual, divide by n and take the remainder. For example, in $\mathbb{Z}/5\mathbb{Z}$, we have $\overline{2}+\overline{2}=\overline{4}$ but $\overline{3}+\overline{3}=\overline{1}$, because $3+3=6$ and when 6 is divided by 5 the remainder is 1.

However, $\mathbb{Z}/n\mathbb{Z}$ is not always a field, because it is not always the case that all elements have multiplicative inverses. For example, in $\mathbb{Z}/4\mathbb{Z}$, the element $\overline{2}$ has no multiplicative inverse. We can see this because any multiple of 2 is even, and when divided by 4 has remainder 0 or 2; therefore, in $\mathbb{Z}/4\mathbb{Z}$, any multiple of $\overline{2}$ is either $\overline{0}$ or $\overline{2}$, *not* $\overline{1}$. (We could also check this by directly computing all the multiples of $\overline{2}$; there are only four of them.)

It turns out that $\mathbb{Z}/n\mathbb{Z}$ is a field exactly in case n is prime. If you are up for a challenge, try proving that. (Hints available.) The field $\mathbb{Z}/p\mathbb{Z}$, for p a prime number, is also denoted F_p.

In Appendix C of the textbook, it is claimed that the set of real numbers of the form $a+b\sqrt{2}$, where a and b are rational numbers, forms a field. You might try checking this. Most of the axioms are not too hard to check; the existence of multiplicative inverses is the one that needs a little cleverness.