18.704 Supplementary Notes
February 2, 2005

Fields

This seminar is going to be about several kinds of abstract mathematical structure. One point of defining such a structure is to help you recognize that some of the work you've done can apply in more places than you thought. Often it's best to think of an abstract structure not in terms of the list of axioms that defines it, but in terms of a list of examples. So you should think of a field not as something satisfying the eleven axioms I'll write in a moment, but as something like $\mathbb{R}$, or $\mathbb{Z}/2\mathbb{Z}$, or $\mathbb{Q}[i]$. Similarly, a group should be something like the symmetric group S_n, or $GL(n, \mathbb{C})$, or the non-zero quaternions. (Most of these examples may be unfamiliar to you, but you'll learn about them soon.)

The first structure is a *field*.

Definition 1. A *field* is a set F equipped with two binary operations $+$ and $\cdot$ (called *addition* and *multiplication*) satisfying the following axioms.

$(F, +)$ IS AN ABELIAN GROUP

(1) (commutative law) For all elements a and b in F, we have

$$a + b = b + a.$$

(2) (associative law) For all elements a, b, and c in F, we have

$$(a + b) + c = a + (b + c).$$

(3) (identity element) There is an element $0_F \in F$ such that for every element a in F, we have

$$0_F + a = a + 0_F = a.$$

(4) (additive inverses) For every element a in F there is an element $-a$ in F such that

$$a + (-a) = (-a) + a = 0_F.$$

$(F, \cdot)$ IS A MONOID

(5) (associative law) For all elements a, b, and c in F, we have

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

(6) (identity element) There is an element $1_F \in F$ such that for every element a in F, we have

$$1_F \cdot a = a \cdot 1_F = a.$$

MULTIPLICATION IS DISTRIBUTIVE OVER ADDITION

(7) (left distributive law) For all elements a, b, and c in F, we have

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c).$$

(8) (right distributive law) For all elements a, b, and c in F, we have

$$(b + c) \cdot a = (b \cdot a) + (c \cdot a).$$

Define $F^\times = F \setminus 0_F$, the collection of non-zero elements of F.

$(F^\times, \cdot)$ IS A GROUP

Since F is already assumed to be a monoid under multiplication, this imposes only two more requirements.

(9) (identity element) The multiplicative identity 1_F is not equal to the additive identity 0_F.

(10) (multiplicative inverses) For every non-zero element a in F there is a non-zero element a^{-1} so that

$$a \cdot a^{-1} = a^{-1} \cdot a = 1_F.$$

MULTIPLICATION IS COMMUTATIVE

(11) (commutative law) For all elements a and b in F, we have

$$a \cdot b = b \cdot a.$$

The numbered items in Definition 1 are the *axioms* for a field. To make an example of a field, we need to describe the set F, describe the operations $+$ and $\cdot$, and check that all of the axioms are satisfied. There is some redundancy in the axioms: since multiplication is supposed to be commutative, the right distributive law is redundant. (That is, if all the axioms except the right distributive law are satisfied, then that law must be satisfied as well.) There are various other ways that the axioms could be made shorter. One reason for stating them in this way is that sometimes we'll be interested in systems that satisfy only some of the axioms. For example, a system satisfying axioms (1)–(8) is called a *ring*; if axiom (11) holds, then it's a *commutative ring*. If axioms (1)–(10) are satisfied, then F is called a *division ring*.

I said that what mattered about these abstract definitions was the examples, so here are some examples (and, equally important, some non-examples).

Example 1. The rational numbers. Write $\mathbb{Q}$ for the collection of all rational numbers n/m, with n and m integers and $m \neq 0$. I won't recall how you tell when two rational numbers are equal, and how you add and multiply rational numbers; but you should know for example that $6/1 = 12/2$ (six of one and half a dozen of the other, as we say in algebraic number theory). With the familiar operations $+$ and $\cdot$, $\mathbb{Q}$ is a field.

Example 2. The real numbers. Write $\mathbb{R}$ for the collection of all real numbers. There are lots of ways to define $\mathbb{R}$ precisely, which you might learn in 18.100. I won't worry about the details too much; but if you think of real numbers as given by decimal expansions, then you should know that $.999\ldots = 1.000\ldots$. With the familiar operations $+$ and $\cdot$, $\mathbb{R}$ is a field.

Non-example 3. The integers. Write $\mathbb{Z}$ for the integers $0, \pm 1, \pm 2, \ldots$. There are familiar operations of addition and multiplication, and these satisfy axioms (1)–(9) and (11) of Definition 1. The integers are therefore a commutative ring. Axiom (10) is *not* satisfied, however: the non-zero element 2 of $\mathbb{Z}$ has no multiplicative inverse in $\mathbb{Z}$. That is, there is no integer m such that $2 \cdot m = 1$. So $\mathbb{Z}$ is *not* a field.

These are (some of) the examples you should already know. When you see a new abstract definition, it's a good idea to try to make the simplest possible examples of it. Here are two tries.

Non-example 4. The zero ring. Suppose that F consists of the single element 0. Since there is only one element, the addition and multiplication tables are easy to write:

$$0 + 0 = 0, \qquad 0 \cdot 0 = 0.$$

The axioms in Definition 1 are easy to check: (1)-(5) are all true. (6) may not look true at first, but the axiom only says that there is *some* element 1 that behaves in a certain way (not that you were already calling it 1. In our example $1_F = 0$ is a multiplicative identity, because $0 \cdot a = a \cdot 0 = a$ for every element (namely 0) of F. So (6) is true. The distributive laws (7) and (8) are true, and so is the commutative law for multiplication (11). So far this means that F is a commutative ring. But (9) is not true: $F^\times$ is the empty set, and that's not a group. So 0 is a commutative ring, but not a field.

Sometimes an example 5. The integers modulo n. Suppose n is a positive integer (that is, 1 or 2 or 3 ...). Two integers a and b are said to be *congruent modulo n* if $a - b$ is divisible by n. We write this condition as $a \equiv b \pmod{n}$. For example, $11 \equiv 25 \pmod{7}$.

Write $\overline{a}$ for the equivalence class of the integer a. For example, if $n = 3$

$$\overline{4} = \{\ldots - 5, -2, 1, 4, 7, 10 \ldots\}.$$

The set of *integers modulo n* is the set of all equivalence classes for this equivalence relation, and is written $\mathbb{Z}/n\mathbb{Z}$. If $n = 3$, then $\mathbb{Z}/n\mathbb{Z}$ has exactly three elements:

$$\begin{aligned} \overline{0} &= \{\ldots - 6, -3, 0, 3, 6, 9 \ldots\} \\ \overline{1} &= \{\ldots - 5, -2, 1, 4, 7, 10 \ldots\} \\ \overline{2} &= \{\ldots - 4, -1, 2, 5, 8, 11 \ldots\} \end{aligned}$$

In general $\mathbb{Z}/n\mathbb{Z}$ has exactly n elements:

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1} \ldots \overline{n-1}\}.$$

It makes sense to add and multiply equivalence classes: if $a_1 \equiv a_2 \pmod{n}$ and $b_1 \equiv b_2 \pmod{n}$, then $a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$ and $a_1 b_1 \equiv a_2 b_2 \pmod{n}$. The class $\overline{0}$ is an additive identity, and $\overline{1}$ is a multiplicative identity. Properties (1)–(8) and (11) are inherited from $\mathbb{Z}$, so $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring having exactly n elements.

Property (9) (that $1_F \neq 0_F$) amounts to requiring that $overline 0 \neq \overline{1}$. This means that 0 should not be equivalent to 1, or (by definition of $\equiv$) that $1 - 0$ should not be divisible by n. Since n is a positive integer, 1 is not divisible by n unless $n = 1$. To summarize: property (9) is true in $\mathbb{Z}/n\mathbb{Z}$ if and only if $n > 1$. (The case $n = 1$ gives the zero ring of Example 4.)

Suppose now that $n > 1$, so that properties (1)–(9) and (11) are satisfied. Then $\mathbb{Z}/n\mathbb{Z}$ will be a field if and only if every non-zero element has a multiplicative inverse. Deciding when this is true requires enough ideas to be labelled a theorem.

Theorem 1. *Suppose n is a positive integer. Then the commutative ring $\mathbb{Z}/n\mathbb{Z}$ (Example 5 above) is a field if and only if n is a prime number.*

Proof. If $n = 1$, then n is not a prime, and $\mathbb{Z}/n\mathbb{Z}$ is not a field; so we may assume $n > 1$. Suppose first that n is not a prime. We need to show that $\mathbb{Z}/n\mathbb{Z}$ is not a field; the only hope is to show that property (10) of Definition 1 fails. Since n is not prime, there are positive integers a and b, both greater than 1, so that $n = ab$. From this equation it follows that a and b are both strictly smaller than n:

$$1 < a, b < n - 1.$$

In particular, neither a nor b is divisible by n, so

(A) $$\overline{a} \neq \overline{0}, \qquad \overline{b} \neq \overline{0}$$

in $\mathbb{Z}/n\mathbb{Z}$. But the equation $ab = n$ means that

(B) $$\overline{a} \cdot \overline{b} = \overline{0}.$$

If $\overline{a}$ had a multiplicative inverse, then multiplying (B) by that inverse would give $\overline{b} = \overline{0}$, which contradicts (A). So $\overline{a}$ has no multiplicative inverse, which means that property (10) fails and $\mathbb{Z}/n\mathbb{Z}$ is not a field.

Next, suppose that $n = p$ *is* a prime number. (Changing the name of the number to p isn't logically necessary, but it makes me more comfortable.) We have to show that property (10) is satisfied, and therefore that $\mathbb{Z}/p\mathbb{Z}$ is a field. So suppose $\overline{a} \neq \overline{0}$; that is, that a is not divisible by p. We have to find a multiplicative inverse for $\overline{a}$. That is, we have to find $\overline{x}$ so that

(C) $$\overline{a} \cdot \overline{x} = \overline{1}.$$

Let's be explicit about what C means: we're given an integer a that's not divisible by p, and we're supposed to find another integer x so that $ax - 1$ is divisible by p. This is a bit tricky. Suppose for instance that $p = 59$ and $a = 13$; how do you find x? It turns out that $x = 50$ works: $ax = 650 = 11 \cdot 59 + 1$. But finding this x by trial and error is tedious work. On the course web site you can find another handout describing a systematic way to find x, but I don't want to get into that here.

How can I get away with "not getting into that?" if I'm supposed to find an $\overline{x}$? The answer is that I don't really need to *find* $\overline{x}$, but only to prove that it exists; and that's much easier. Here is an argument.

Lemma. *Suppose p is a prime number, and that a is an integer not divisible by p.*

1. *If b is an integer not divisible by p, then ab is not divisible by p.*
2. *If b_1 and b_2 are integers, and $b_1 - b_2$ is not divisible by p, then $ab_1 - ab_2$ is not divisible by p.*
3. *If $\overline{b_1} \neq \overline{b_2}$ in $\mathbb{Z}/p\mathbb{Z}$, then $\overline{a}\overline{b_1} \neq \overline{a}\overline{b_2}$.*
4. *The p classes $\overline{a}\overline{0}, \overline{a}\overline{1} \ldots \overline{a}\overline{p-1}$ in $\mathbb{Z}/p\mathbb{Z}$ are all distinct.*
5. *Every element of $\mathbb{Z}/p\mathbb{Z}$ is of the form $\overline{ax}$, for some $\overline{x} \in \mathbb{Z}/p\mathbb{Z}$.*
6. *$\overline{a}$ has a multiplicative inverse in $\mathbb{Z}/p\mathbb{Z}$.*

Proof. Part (1) is part of the statement that every positive integer has a unique prime factorization. Part (2) is (1) applied to $b = b_1 - b_2$. Part (3) is exactly the same as (2), written using the definition of $\mathbb{Z}/p\mathbb{Z}$. Part (4) is an immediate consequence of (3). Part (5) follows: we have p distinct elements of a p-element set, so we must have all of them. Part (6) is a special case of (5): if every element shows up, then $\overline{1}$ must show up. Part (7) is just a reformulation of (6). □

This argument proves that multiplicative inverses exist, and therefore that $\mathbb{Z}/p\mathbb{Z}$ is a field. □

We've now got one finite field $\mathbb{Z}/p\mathbb{Z}$ for each prime number p. The teaser for the future is this: for every prime *power* $q = p^m$, there is a finite field with q elements. It's natural to guess that this field ought to be $\mathbb{Z}/q\mathbb{Z}$, but that's not right: $\mathbb{Z}/p^m\mathbb{Z}$ is not a field unless $m = 1$. Since we'll need these fields to work with, we'll need to find them somewhere else.