Mathematics 262
Homework 1 solutions

1. Can you find a field with three elements? With 4 elements? [**Extra credit**: for which integers $n > 1$ can you find a field with N elements?]

ANSWER: Yes, there is a field with three elements; there is also a field with 4 elements. If you want to know the answer to the extra credit problem, let me know. I won't give the answer here, in case any of you want to keep working on it.

The integers modulo 3 form a field with three elements. I'll give the addition and multiplication tables.

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Since addition and multiplication of integers satisfy most of the appropriate properties (commutativity, associativity, distributivity), then the same is true here. The only thing you have to check is that every nonzero element has a multiplicative inverse, and that's clear from the multiplication table.

It may be harder to find a field with 4 elements, because the integers modulo 4 don't work, and also because there are more possibilities for addition and multiplication. In any case, here are the tables:

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

×	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

To verify that these operations define a field, you have to check commutativity for + and × (clear since both tables are symmetric), associativity for + and ×, and distributivity. (It is clear from the tables that 0 and 1 work as they should, that every element has an additive inverse, and that every nonzero element has a multiplicative inverse.)

Associativity for +: you have to see if $x + (y + z) = (x + y) + z$. If any of x, y, or z is 0, then this is clear, so assume that they are all nonzero. If any two of them are equal, say $x = y$, then since $x + x = 0$ for every x under consideration, this is also not too hard to check. This leaves the case in which they are all different. Because of commutativity, this reduces to checking that $1 + (a + b) = (1 + a) + b$.

Associativity for ×: check that $x(yz) = (xy)z$. If any of x, y, or z is either

0 or 1, this is easy. It is also easy if $x = y = z$. So you only have to check

$$\begin{aligned} a(ab) &= (aa)b, \\ a(bb) &= (ab)b, \\ a(ba) &= (ab)a, \\ b(ab) &= (ba)b, \\ b(aa) &= (ba)a, \\ b(ba) &= (ba)b. \end{aligned}$$

Most of these follow from commutativity. For example, the third one holds because

$$a(ba) = a(ab) = (ab)a.$$

You only have to use the tables to check the first two, and these are easy to verify.

Distributivity: This is similarly tedious, and I'm not going to work it out.

---

2. Let $\mathbf{R}$ denote the field of real numbers. Let $\mathbf{R}^{\infty\times\infty}$ denote the set of all "infinite matrices" with entries in $\mathbf{R}$; this is the set of all arrays of real numbers of the form:

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & \dots \\ a_{21} & a_{22} & a_{23} & \dots \\ a_{31} & a_{32} & a_{33} & \dots \\ \vdots & \vdots & \vdots & \end{bmatrix}$$

You can add these the way you would expect, but I claim that the standard matrix multiplication law has problems in this setting. Explain. Can you find a subset of $\mathbf{R}^{\infty\times\infty}$ that forms a ring?

ANSWER: The problem with the multiplication is convergence. If I try to multiply using ordinary matrix multiplication, I have to take the dot product of two vectors from $\mathbf{R}^{\infty}$. If the ith row of the infinite matrix A is $(1, 1, 1, \dots)$, and the jth column of the infinite matrix B is the same, then the (i, j)-entry of the product AB is the dot product of this vector with itself, $\sum_{i=1}^{\infty} 1$, which doesn't converge.

There are various ways to avoid this. One of them is to restrict your attention to infinite matrices in which every row and every column has only finitely many nonzero entries. Then when you take the dot product of a row $(a_{i1}, a_{i2}, \dots)$ with a column $(b_{1j}, b_{2j}, \dots)$, the answer

$$\sum_{k=1}^{\infty} a_{ik} b_{kj}$$

has only finitely many nonzero terms, and therefore converges. (You have to check that this set of matrices is closed under addition and multiplication, but this is not very hard. Neither are associativity, distributivity, etc.)

As a special case, you can just use diagonal matrices. There are other options, too. If you want to get fancy, then you can consider all infinite matrices whose rows and columns are the terms of absolutely convergent series. These form a ring; I'll let you check the details. (The main thing you have to check is that the term-by-term product of absolutely convergence series is absolutely convergent. In other words, if $\sum a_k$ and $\sum b_k$ converge absolutely, then so does $\sum a_k b_k$.) Come to think of it, you can probably get away with matrices whose rows are the terms of an absolutely convergent series, and whose columns are the terms of any convergent series. (Or you can switch the roles of row and column: look at all matrices whose columns give absolutely convergent series, and whose rows give convergence series.)

---

3. Write down addition and multiplication tables for the ring $\mathbf{Z}/6\mathbf{Z}$.

ANSWER: You perform ordinary addition and multiplication, and then take remainders upon division by 6. Here's the answer:

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Note that this is not a field: the element 2 does not have a multiplicative inverse (and neither do 3 or 4).

From Section 5.2 in the book:

3. I'm going to get tired of writing subscripts, so instead I'll write the matrix A as $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then the adjoint of A is $\operatorname{adj} A = \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$.

3(a) Multiply $\operatorname{adj} A$ by A using ordinary matrix multiplication:

$$(\operatorname{adj} A)A = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ad - bc & 0 \\ 0 & ad - bc \end{pmatrix} = (\det A)I.$$

The same sort of computation works for the product $A(\operatorname{adj} A)$.

3(b) Compute the determinant of $\operatorname{adj} A$ using the standard formula for a 2×2 determinant to get $da - (-b)(-c) = ad - bc = \det A$.

3(c) Since $A^t = \left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right)$, then

$$\operatorname{adj}(A^t) = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} = (\operatorname{adj} A)^t.$$

---

12. I will assume that $D(A)$ is not 0 for some A, and prove that $D(I) = 1$. Indeed, suppose that $D(A) = c \neq 0$. Then $c = D(A) = D(AI) = D(A)D(I) = cD(I)$. Now multiply both sides by c^{-1}: $1 = D(I)$.

Now, if A is invertible with inverse B, then

$$1 = D(I) = D(AB) = D(A)D(B).$$

Therefore $D(A)$ is nonzero (if $D(A) = 0$, then $D(A)D(B) = 0$ no matter what $D(B)$ is).