MATH30010: Field Theory
Homework 1: Solutions

1. Prove the uniqueness of multiplicative inverses in any field F; i.e., let $a \in F$ and let $b, c \in F$ satisfy

$$a \cdot b = a \cdot c = 1.$$

Using the field axioms, show that $b = c$.

Solution: We have $c = 1 \cdot c = (b \cdot a) \cdot c = b \cdot (a \cdot c) = b \cdot 1 = b$.

2. Let F be a field. Using the field axioms, prove that $0 \cdot a = 0$ for every $a \in F$.

Solution: We have $0 = 0 + 0$ and hence

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0.$$

Thus

$$\begin{aligned} 0 &= a \cdot 0 + (-a \cdot 0) \\ &= (a \cdot 0 + a \cdot 0) + (-a \cdot 0) \\ &= a \cdot 0 + (a \cdot 0 + (-a \cdot 0)) \\ &= a \cdot 0 + 0 \\ &= a \cdot 0. \end{aligned}$$

3. Let F be any field.

(a) If $a, b, c \in F$ with $b, c \neq 0$, show that

$$\frac{a}{b} = \frac{ac}{bc}.$$

(b) If $a, b, c, d \in F$ with $b, d \neq 0$ show that

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

Solution:

(a) First observe that for any $x, y \in F$, $(xy)^{-1} = y^{-1}x^{-1}$ since

$$(xy)(y^{-1}x^{-1}) = x(y \cdot y^{-1})x^{-1} = x \cdot 1 \cdot x^{-1} = x \cdot x^{-1} = 1.$$

Thus

$$\frac{ac}{bc} = (ac)(bc)^{-1} = (ac)(c^{-1}b^{-1}) = a(c \cdot c^{-1})b^{-1} = ab^{-1} = \frac{a}{b}.$$

(b) Recall from class that if $x, yz \in F$ and $z \neq 0$, then

$$\frac{x}{z} + \frac{y}{z} = \frac{x+y}{z}.$$

We have

$$\begin{aligned} \frac{a}{b} + \frac{c}{d} &= \frac{ad}{bd} + \frac{bc}{bd} \text{ (using (a))} \\ &= \frac{ad+bc}{bd}. \end{aligned}$$

4. Let F be a field and let $a, b \in F$. Suppose that $ab = 0$. Prove that either $a = 0$ or $b = 0$ (possibly both).

   Solution: Suppose that $ab = 0$. If $a = 0$ we're done. The other possibility is that $a \neq 0$, and in this case we must show that this forces $b = 0$:

   Now $a \neq 0 \implies a^{-1}$ exists. Thus, multiplying both sides of $ab = 0$ by a^{-1} give $a^{-1}ab = a^{-1} \cdot 0 = 0$ (by problem 2). But $a^{-1}ab = 1 \cdot b = b$. So $b = 0$ and we're done.

5. Let F be a field with exactly 3 elements. $0 \neq 1$ are necessarily two of the elements. Denote the third by a. Using the field axioms, prove that we must have

$$a + 1 = 0, \qquad 1 + 1 = a \text{ and } a^2 = a + a = 1.$$

   Solution: $a + 1$ is equal to either $0, 1$ or a. We eliminate the last two possibilities, thus proving the first:

   We can't have $a + 1 = 1$, for adding -1 to both sides gives $a = 0$, and we have assumed 0, 1 and a are distinct.

   Similarly, we can't have $a + 1 = a$, since adding $-a$ to both sides would imply $1 = 0$, which is impossible.

   So we can conclude that $a + 1 = 1 + a = 0$, and thus $a = -1$ and $1 = -a$.

   Next we can eliminate the possibilities $1 + 1 = 0$ (which implies $1 = -1 = a$) and $1 + 1 = 1$ (which implies $1 = 0$) to deduce that $1 + 1 = a$. Thus $a = 2 = -1$ in our field.

   Finally, in view of the above, we have $a^2 = 2a = 2 \cdot (-1) = -2 = -a = 1$.

6. Let F be the set of all 2×2 matrices of the form

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

   where $a, b \in \mathbb{R}$.

(a) If $X, Y \in F$, show that $X + Y \in F$ (where $+$ denotes matrix addition).

(b) If $X, Y \in F$, show that $X \cdot Y \in F$.

(c) Is F a field? If so, prove it. If not, determine which of the nine field axioms fail to hold for $(F, +, \cdot)$.

[Note: You may assume, without proving it, that matrix addition and multiplication are associative.]

Solution:

(a) Let

$$X = \begin{bmatrix} x & -y \\ y & x \end{bmatrix}, Y = \begin{bmatrix} z & -w \\ w & z \end{bmatrix} \in F.$$

Then

$$X+Y = \begin{bmatrix} x+z & -y-w \\ y+w & x+z \end{bmatrix} = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \text{ with } a = x+z,\ b = y+w.$$

So $X + Y \in F$.

(b) Again, let

$$X = \begin{bmatrix} x & -y \\ y & x \end{bmatrix}, Y = \begin{bmatrix} z & -w \\ w & z \end{bmatrix} \in F.$$

Then

$$X \cdot Y = \begin{bmatrix} xz - yw & -xw - yz \\ yz + xw & xz - yw \end{bmatrix} = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \text{ with } a = xz-yw,\ b = xw+yz.$$

so that $X \cdot Y \in F$. Observe also that $X \cdot Y = Y \cdot X$.

(c) $(F, +, \cdot)$ is a field:

The addition is commutative and associative since this is in general true of matrix addition. (Axioms (1) and (2)).

The Zero matrix belongs to F (take $a = b = 0$) and is an additive identity (Axiom (3)).

If $X \in F$, then $-X \in F$; just replace a by $-a$ and b by $-b$ (Axiom (4)).

The multiplication in F is commutative, as observed above (Axiom (5)).

The multiplication is associative, since this is in general true for matrix multiplication (Axiom (6)).

The 2×2 identity matrix I belongs to F; take $a = 1, b = 0$ (Axiom (7)).

Now let

$$0 \neq X = \begin{bmatrix} x & -y \\ y & x \end{bmatrix} \in F$$

Since $X \neq 0$, not both of x, y are 0 and thus $\det(X) = x^2+y^2 > 0$. Hence

$$X^{-1} = \frac{1}{x^2+y^2} \begin{bmatrix} x & y \\ -y & x \end{bmatrix} = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

with

$$a = \frac{x}{x^2+y^2}, b = \frac{-y}{x^2+y^2}.$$

Thus $X^{-1} \in F$ and axiom (8) holds.

Finally, since matrix multiplication generally distributes over matrix addition, axiom (9) also holds.

7. Show that 5 is a fourth power in the field $\mathbb{F}_{11}$.

   Solution: $2^4 = 5$ in $\mathbb{F}_{11}$.

8. Find *all* roots of the polynomial $x^3 - 6$ in the field $\mathbb{F}_7$.

   Solution: In $\mathbb{F}_7$, we have $3^3 = 27 = 6$, $5^3 = (-2)^3 = -8 = 6$ and $6^3 = (-1)^3 = -1 = 6$, while $0^3 = 0$, $1^3 = 1$, $2^3 = 1$ $4^3 = (2^3)^2 = 1$. So 3, 5 and 6 are the roots of $x^3 - 6$ in $\mathbb{F}_7$.

9. Find *all* roots of the polynomial $x^3+x+1 = 0$ in the field $\mathbb{F}_9 := \mathbb{F}_3(i)$.

   Solution: Observe that for all $a \in \mathbb{F}_3$ we have $a^3 = a$. Suppose that $a + bi \in \mathbb{F}_3(i)$. Then

   $$(a+bi)^3 = a^3 + 3a^2bi - 3ab^2 - b^3i = a - bi$$

   (since $a^3 = a$, $b^3 = b$ and $3 = 0$).

   Thus, if $x = a + bi$, then $x^3 + x + 1 = a - bi + a + bi + 1 = 2a + 1$. So $x^3 + x + 1 = 0$ if and only if $2a + 1 = 0$ in $\mathbb{F}_3$. Solving this for a gives $a = -1/2 = -2 = 1$. Thus the three roots are $x = 1$, $x = 1 + i$ and $x = 1 + 2i$.