Problem 1

1. Provide the definition of a field. List out and name all the field axioms.[a]

2. List out all the fields you know.

Solution

1. A field F is a set with the operations $+$ and $-$, distinguished elements 0 and 1 (with $0 \neq 1$), in which the following axioms hold:

   (a) $x + y, x \cdot y \in F$ for any $x, y \in F$ (**closure** under addition and multiplication).

   (b) $x + (y + z) = (x + y) + z$ and $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ for any $x, y, z \in F$ (**associativity** of addition and multiplication).

   (c) $x+y = y+x$ and $x \cdot y = y \cdot x$ for any $x, y \in F$ (**commutativity** of addition and multiplication).

   (d) $x + 0 = x$ and $x \cdot 1 = x$ for all $x \in F$ (where 0 and 1 are called the **additive identity** and **multiplicative identity** respectively).

   (e) For any $x \in F$, there is a $w \in F$ such that $x + w = 0$ (existence of **negatives**). Moreover, if $x \neq 0$, then there is also an $r \in F$ such that $x \cdot r = 1$ (existence of **reciprocals**). We denote $w = -x$ and $r = x^{-1}$.

   (f) $x \cdot (y + z) = x \cdot y + x \cdot z$ for any $x, y, z \in F$ (**distributivity** of addition over multiplication).

2. $\mathbb{R}$ (with usual addition and multiplication), $\mathbb{Q}$ (with usual addition and multiplication), the field of two elements (addition and multiplication defined in the book), et cetera.

[a] Consult Definition 5.13 in the Course Notes if needed.

Problem 2

Let $F = \{0, 1, a\}$. Complete the following addition and multiplication tables for F.

+	0	1	a
0			
1			
a			

·	0	1	a
0			
1			
a			

Solution

First of all, we have the following facts:

- $0 + x = 0$ for all $x \in F$.
- $0 \cdot x = 0$ for all $x \in F$.
- $1 \cdot x = x$ for all $x \in F$.

This forces us to fill out the tables in the following manner:

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

·	0	1	a
0	0	0	0
1	0	1	a
a	0	a	

Now if $a \cdot a = 0$ or $a \cdot a = a$, then a (which is $\neq 0$) will not have a multiplicative inverse. So we are forced to put $a \cdot a = 1$.

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

·	0	1	a
0	0	0	0
1	0	1	a
a	0	a	1

Let us now consider what $1+a$ is. If $1+a=1$, then adding -1 on both sides, we get $a=0$ which is impossible. If $1+a=a$, then $1=0$ which is impossible. Thus, we are forced to have $1+a=0$.

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

·	0	1	a
0	0	0	0
1	0	1	a
a	0	a	1

Now we consider $1+1$: if $1+1=0$, then $1+1=1+a$ so $1=a$ which is impossible; if $1+1=1$ then $1=0$ which is impossible. So we are forced to have $1+1=a$.

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

·	0	1	a
0	0	0	0
1	0	1	a
a	0	a	1

Lastly, $a+a=0$ produces $a+a=a+1$ or $a=1$ which is impossible; $a+a=a$ produces $a=0$ which is impossible. So $a+a=1$.

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

·	0	1	a
0	0	0	0
1	0	1	a
a	0	a	1

Problem 3

Let F be a field, and $a, b \in F$.

1. Suppose $ab=0$. Show that $a=0$ or $b=0$.[a] You may use Claim 2.3.2.
2. Show that $a^2-b^2=(a+b)(a-b)$.
3. Suppose $a^2=b^2$. Show that $a=-b$ or $a=b$.

Solution

1. To show that $a=0$ or $b=0$, we assume $a\neq 0$ and show that $b=0$.

   Suppose $a\neq 0$. Then a^{-1} exists. Thus

$$
\begin{aligned}
& ab=0 \\
\Rightarrow & a^{-1}(ab)=a^{-1}(0) && \text{multiplying both sides on the left by } a^{-1} \\
\Rightarrow & (a^{-1}a)b=a^{-1}(0) && \text{associativity of } \cdot \\
\Rightarrow & 1b=a^{-1}(0) && a \text{ and } a^{-1} \text{ are multiplicative inverses} \\
\Rightarrow & b=a^{-1}(0) && 1 \text{ is the multiplicative identity} \\
\Rightarrow & b=0a^{-1} && \text{commutativity of } \cdot \\
\Rightarrow & b=0 && \text{Claim 2.3.2: } 0x=0 \text{ for any } x\in F
\end{aligned}
$$

   The proof is complete. □

2. We prove a lemma:

   Lemma. $-x = (-1)x$ for all $x \in F$. *Proof.*

$$\begin{aligned}
&0 = 0 \\
\Rightarrow &0 = 0x && \text{Claim 2.3.2} \\
\Rightarrow &0 = (1 + -1)x && -1 \text{ is the additive inverse of } 1 \\
\Rightarrow &0 = 1x + (-1)x && \text{distributivity} \\
\Rightarrow &0 = x + (-1)x && 1 \text{ is the multiplicative identity} \\
\Rightarrow &-x + 0 = -x + (x + (-1)x) && \text{adding } -x \text{ to the left of both sides} \\
\Rightarrow &-x = -x + (x + (-1)x) && 0 \text{ is the additive identity} \\
\Rightarrow &-x = (-x + x) + (-1)x && \text{associativity} \\
\Rightarrow &-x = 0 + (-1)x && x \text{ is the additive inverse of } -x
\end{aligned}$$

$$\Rightarrow -x = (-1)x 0 \text{ is the additive identity}$$

   Now we can prove the original statement $a^2 - b^2 = (a+b)(a-b)$. We have

$$\begin{aligned}
(a+b)(a-b) &= (a+b)a + (a+b)(-b) && \text{distributivity} \\
&= a^2 + ba + a(-b) + b(-b) && \text{distributivity} \\
&= a^2 + ba + a(-1)b + b(-1)b && \text{Lemma} \\
&= a^2 + ab + (-1)ab + (-1)b^2 && \text{commutativity} \\
&= a^2 + ab + (-ab) + (-b^2) && \text{Lemma} \\
&= a^2 + (-b^2) && \text{additive inverse} \\
&= a^2 - b^2 && \text{“}-x\text{” is just shorthand for “}+(-x)\text{”}
\end{aligned}$$

   The proof is complete. □

3. If $a^2 = b^2$, then $a^2 - b^2 = 0$, which by part 2 means $(a+b)(a-b) = 0$. By part 1, this means either $a + b = 0$ (so $a = -b$), or $a - b = 0$ (so $a = b$).

[a] This is known as the **zero-product property**.

Problem 4

Define $F = \mathbb{R} \times \mathbb{R}$. We define addition $+$ and multiplication $\cdot$ over F in the following way:

- $(a, b) + (c, d) = (a + b, c + d)$ (where $a + b$ and $c + d$ is just addition of real numbers).
- $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$ (where again the operations are over real numbers).

1. Show that F is a field. *Hint: The multiplicative inverse of* (a, b) *is* $\left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2}\right)$.
2. Show that there is $(a, b) \in F$ such that $(a, b) \cdot (a, b) = -1$ (where -1 is the additive inverse of the additive identity 1 in F).

Comment. F is the *complex numbers*; (a, b) corresponds with $a + bi$. This problem asks you to show that the complex numbers form a field.

Solution

1. We verify all the field axioms. The additive identity in F will is set to $(0, 0)$, while the multiplicative identity in F is set to $(1, 0)$.

(a) If $(a,b),(c,d) \in \mathbb{R}\times\mathbb{R}$, then $(a+b, c+d)$ and $(ac-bd, ad+bc)$ are both in $\mathbb{R}\times\mathbb{R}$.

(b)
$$((a,b)+(c,d))+(e,f) = (a+b+c, d+e+f) = (a,b)+((c,d)+(e,f)).$$

$$\begin{aligned}((a,b)\cdot(c,d))\cdot(e,f) &= (ac-bd, ad+bc)\cdot(e,f)\\ &= ((ac-bd)e-(ad+bc)f, (ac-bd)f+(ad+bc)e)\\ &= (ace-bde-adf-bcf, acf-bdf+ade-bce),\\ (a,b)\cdot((c,d)\cdot(e,f)) &= (a,b)\cdot(ce-df, cf+de)\\ &= (a(ce-df)-b(cf+de), a(cf+de)-b(ce-df))\\ &= (ace-adf-bcf-bde, acf-ade-bce-bdf).\end{aligned}$$

(c)
$$(a,b)+(c,d) = (a+c, b+d) = (c,d)+(a,b).$$
$$(a,b)\cdot(c,d) = (ac-bd, ad+bc) = (c,d)\cdot(a,b).$$

(d) $(a,b)+(0,0) = (a,b)$ and $(a,b)\cdot(1,0) = (a(1)-b(0), a(0)+b(1)) = (a,b)$, which are the additive and multiplicative identities we have respectively defined.

(e) Given $(a,b)\in F$, we have $(-a,-b)\in F$, and $(a,b)+(-a,-b) = (0,0)$.

Given $(a,b)\in F$, we have $\left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2}\right)\in F$, and

$$\begin{aligned}&(a,b)\cdot\left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2}\right)\\ =&\left(a\left(\frac{a}{a^2+b^2}\right)-b\left(-\frac{b}{a^2+b^2}\right), a\left(-\frac{b}{a^2+b^2}\right)+b\left(\frac{a}{a^2+b^2}\right)\right)\\ =&\left(\frac{a^2+b^2}{a^2+b^2}, \frac{-ab+ab}{a^2+b^2}\right)+b\left(\frac{a}{a^2+b^2}\right)\\ =&(1,0).\end{aligned}$$

(f)

$$\begin{aligned}&(a,b)\cdot((c,d)+(e,f))\\ =&(a,b)\cdot(c+e, d+f)\\ =&(a(c+e)-b(d+f), a(d+f)+b(c+e))\\ =&(ac+ae-bd-bf, ad+af+bc+be),\\ &(a,b)\cdot(c,d)+(a,b)\cdot(e,f)\\ =&(ac-bd, ad+bc)+(ae-bf, af+be)\\ =&(ac+ae-bd-bf, ad+af+bc+be).\end{aligned}$$

Problem 5

Suppose $F\subseteq\mathbb{R}$ is a field with addition and multiplication inherited from the real numbers.[a]

1. Show that $\mathbb{N}\subseteq F$.
2. Show that $\mathbb{Z}\subseteq F$.
3. Show that $\mathbb{Q}\subseteq F$.[b]

Solution

Let 0_F and 1_F denote the additive and multiplicative identities of F respectively. First, we show that 0_F is the real number 0. We know that $0_F + 1_F = 1_F$ (by property of 0_F being the additive identity). Thus

$$0_F + (1_F - 1_F) = 1_F - 1_F.$$

But notice that in "$1_F - 1_F$" we are performing subtraction of real numbers; since $x - x = 0$ for any real number x, we have $1_F - 1_F = 0$ (the real number). So

$$0_F + 0 = 0.$$

In "$0_F + 0$" we are performing real addition; since $x + 0 = 0$ for any $x \in \mathbb{R}$, we get

$$0_F = 0.$$

Next, we show $1_F = 1$. Similarly, $1_F \cdot 1_F = 1_F$ (by property of 1_F being the multiplicative identity). Thus 1_F satisfies the equation of real numbers $x^2 = x$; the only solutions to $x^2 = x$ are $x = 0$ or $x = 1$. Thus $1_F = 0$ or $1_F = 1$; since $1_F \neq 0_F = 0$, we conclude $1_F = 1$.

1. Notice that since 1_F is the real number 1, $1 \in F$. For any natural number $n \in \mathbb{N}$, we have

   $$n = \underbrace{1 + \ldots + 1}_{n \text{ times}}.$$

   Since F is closed under addition, $\underbrace{1 + \ldots + 1}_{n \text{ times}}$ is in F. This shows $n \in F$. Thus $\mathbb{N} \subseteq F$.

2. Let $n \in \mathbb{Z}$. We split into cases.

   - $n > 0$: then $n \in \mathbb{N}$, and in part 1 we've shown $n \in F$.
   - $n = 0$: $0 = 0_F \in F$.
   - $n < 0$: then $-n > 0$, so $-n \in F$. Because F must be closed under additive inverses, $-(-n) = n \in F$ as well.

   In all cases, $n \in F$. Thus $\mathbb{Z} \subseteq F$.

3. Let $\frac{p}{q} \in \mathbb{Q}$, with $p, q \in \mathbb{Z}, q \neq 0$. In part 2 we've shown $p, q \in F$. Since F is closed under multiplicative inverses, $q^{-1} \in F$; since F is closed under multiplication, $\frac{p}{q} = pq^{-1} \in F$.

[a] In other words, to add or multiply any two elements $a, b \in F$, treat a and b as real numbers.
[b] This is Exercise 2.5.52 from the Course Notes.