MAT 240 - Algebra I

Fields

Definition. A *field* is a set F, containing at least two elements, on which two operations $+$ and $\cdot$ (called *addition* and *multiplication*, respectively) are defined so that for each pair of elements x, y in F there are unique elements $x+y$ and $x \cdot y$ (often written xy) in F for which the following conditions hold for all elements x, y, z in F:

(i) $x+y=y+x$ (commutativity of addition)

(ii) $(x+y)+z=x+(y+z)$ (associativity of addition)

(iii) There is an element $0 \in F$, called zero, such that $x+0=x$. (existence of an additive identity)

(iv) For each x, there is an element $-x \in F$ such that $x+(-x)=0$. (existence of additive inverses)

(v) $xy=yx$ (commutativity of multiplication)

(vi) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ (associativity of multiplication)

(vii) $(x+y) \cdot z = x \cdot z + y \cdot z$ and $x \cdot (y+z) = x \cdot y + x \cdot z$ (distributivity)

(viii) There is an element $1 \in F$, such that $1 \neq 0$ and $x \cdot 1 = x$. (existence of a multiplicative identity)

(ix) If $x \neq 0$, then there is an element $x^{-1} \in F$ such that $x \cdot x^{-1} = 1$. (existence of multiplicative inverses)

Remark: The axioms (F1)–(F-5) listed in the appendix to Friedberg, Insel and Spence are the same as those above, but are listed in a different way. Axiom (F1) is (i) and (v), (F2) is (ii) and (vi), (F3) is (iii) and (vii), (F4) is (iv) and (ix), and (F5) is (vii).

Proposition. *Let F be a field.*

(1) The additive identity in F is unique.

(2) The additive inverse of an element of F is unique.

(3) The multiplicative identity of F is unique.

(4) The multiplicative inverse of a nonzero element of F is unique.

PROOF. (3) Suppose that $1 \in F$ and $\alpha \in F$ are multiplicative identities. Since 1 is a multiplicative identity, by property (viii), $x \cdot 1 = x$ for all $x \in F$. Setting $x = \alpha$, we get $\alpha \cdot 1 = \alpha$. On the other hand, since α is a multiplicative identity, by property (viii), $x \cdot \alpha = x$ for all $x \in F$. If we take $x = 1$, we get $1 \cdot \alpha = 1$. But $1 \cdot \alpha = \alpha \cdot 1$ by property (v). So we have

$$\alpha = \alpha \cdot 1 = 1 \cdot \alpha = 1.$$

The proofs of (1), (2) and (4) are left as exercises.

Examples. The rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$ and the complex numbers $\mathbb{C}$ (discussed below) are examples of fields. The set $\mathbb{Z}$ of integers is not a field. In $\mathbb{Z}$, axioms (i)-(viii) all hold, but axiom (ix) does not: the only nonzero integers that have multiplicative inverses that are integers are 1 and -1. For example, 2 is a nonzero integer.

If 2 had a multiplicative inverse in $\mathbb{Z}$, there would be an integer n such that $2n = 1$, which is impossible, since 1 is an odd integer, and not an even integer.

Example. Let F be a field. Using the axioms in the definition of field, prove that $(-1) \cdot x = -x$ for all $x \in F$. State which axioms are used in your proof.

Solution: We must show that $(-1) \cdot x$ is an additive inverse of x, that is, $x + (-1) \cdot x = 0$.

$$\begin{aligned}
x + (-1) \cdot x &= x + x \cdot (-1) \text{ by (v)} \\
&= x \cdot 1 + x \cdot (-1) \text{ by (viii)} \\
&= x \cdot (1 + (-1)) \text{ by (vii)} \\
&= x \cdot 0 \text{ by (iv)} \\
&= x \cdot 0 + 0 \text{ by (iii)} \\
&= x \cdot 0 + (x \cdot 0 + -(x \cdot 0)) \text{ by (iv)} \\
&= (x \cdot 0 + x \cdot 0) + -(x \cdot 0) \text{ by (ii)} \\
&= x \cdot (0 + 0) + -(x \cdot 0) \text{ by (vii)} \\
&= x \cdot 0 + -(x \cdot 0) \text{ by (iii)} \\
&= 0 \text{ by (iv)}
\end{aligned}$$

Associativity of addition (ii), existence of an additive identity (iii), existence of additive inverses (iv), commutativity of multiplication (v), distributivity (vii), and existence of a multiplicative identity (viii), were the properties used in the proof.

Theorem(Cancellation Laws). *Let a, b, and c be elements of a field F.*
(1) If $a + b = c + b$, then $a = c$.
(2) If $ab = cb$ and $b \neq 0$, then $a = c$.

PROOF. The proof of part (1) is left as an exercise. For part (2), suppose that $b \neq 0$. Then, according to axiom (ix), there exists $b^{-1} \in F$ such that $b \cdot b^{-1} = 1$. Multiplying both sides of $ab = cb$ on the right by b^{-1}, we get $(ab)b^{-1} = (cb)b^{-1}$. Applying axiom (vi) to both sides, we get $a(bb^{-1}) = c(bb^{-1})$, that is, $a \cdot 1 = c \cdot 1$. Now applying axiom (viii), we obtain $a = c$, and part (2) is proved.

Proposition. *Let a and b be elements of a field F. Then*
(1) $a \cdot 0 = 0$
(2) $(-a)b = a(-b) = -ab$
(3) $(-a)(-b) = ab$

PROOF. Part (1) was proved in an example above. For part (2), using the example above, then axiom (vi), followed by the example one more time, we have

$$(-a)b = (-1 \cdot a)b = -1(ab) = -(ab).$$

Next, using the example again, as well as axioms (vi) and (v), we have

$$a(-b) = a(-1 \cdot b) = (a \cdot -1)b = (-1 \cdot a) \cdot b = (-a)b.$$

Part (3) is proved similarly.

Definition. The set of *complex numbers*, denoted $\mathbb{C}$, is the set of ordered pairs of real numbers (a, b), with the operations of addition and multiplication defined by:

$$(a, b) + (c, d) = (a + c, b + d) \quad \text{and} \quad (a, b) \cdot (c, d) = (ac - bd, ad + bc).$$

Note that $(0, 1) \cdot (0, 1) = (-1, 0)$, so $(0, 1)$ is a complex number whose square is -1. We usually write i for $(0, 1)$, and $a + ib$ or $a + bi$ for (a, b). In that case, the multiplication is $(a + ib)(c + id) = ac - bd + i(ad + bc)$. The real numbers a and b are called the *real* and *imaginary* parts of $a + ib$, respectively.

Lemma. *With the above multiplication and addition, $\mathbb{C}$ is a field.*

The proof of the lemma will be disussed in class. The additive identity is $0 = 0 + 0i$, the multiplicative identity is $1 = 1 + 0i$, and the multiplicative inverse of a nonzero complex number $a + ib$ is $(a + ib)^{-1} = a/(a^2 + b^2) + i(-b/(a^2 + b^2))$.

Definition. The *complex conjugate* of the complex number $z = a + ib$ is the complex number $\overline{z} = a - ib$.

If c is a positive real number, the symbol $\sqrt{c}$ will be used to denote the positive (real) square root of c. Also $\sqrt{0} = 0$. Notice that if $z = a + ib$ is a nonzero complex number, then $a^2 + b^2$ is a positive real number.

Definition. The *absolute value* of the complex number $z = a+ib$ is $|z| = \sqrt{z\overline{z}} = \sqrt{a^2 + b^2}$.

Note that $z = a + ib \neq 0$ is equivalent to $|z| \neq 0$. Viewing $z = a + ib$ as a point $(a, b) \in \mathbb{R}^2$, the length of the line segment joining $(0, 0)$ and (a, b) is $\sqrt{a^2 + b^2} = |z|$. If θ is the angle that this segment makes with the positive first coordinate axis, then $a = |z| \cos\theta$ and $b = |z| \sin\theta$. (Here we have the usual convention that positive angles are measured counterclockwise from the positive first coordinate axis). So we can write $z = |z|(\cos\theta + i \sin\theta)$. Note that if θ is replace by $\theta \pm 2\pi k$, $k \in \mathbb{Z}$, we have defined the same complex number z. For example, $i = i \sin(\pi/2 + 2\pi)$.

Let $c \in \mathbb{R}$ be such that $c > 0$. If $z = a + ib$ satisfies $|z| = c$, then $a^2 + b^2 = c^2$. That is, $z = (a, b)$ lies on the circle of radius c centered at $(0, 0)$. So, contrary to the case of real numbers, the equation $|z| = c$ has infinitely many complex solutions (for $c \in \mathbb{R}$, $c > 0$.)

Suppose that $z_j = |z_j|(\cos(\theta_j) + i \sin(\theta_j))$, $j = 1, 2$ are two complex numbers. Using trigonometric identities, we obtain

$$\begin{aligned}
z_1 z_2 &= |z_1||z_2| \left(\cos(\theta_1)\cos(\theta_2) - \sin(\theta_1)\sin(\theta_2)\right) + i \left(\cos(\theta_1)\sin(\theta_2) + \cos(\theta_2)\sin(\theta_1)\right) \\
&= |z_1||z_2|(\cos(\theta_1 + \theta_2) + i \sin(\theta_1 + \theta_2)) \\
&= |z_1 z_2|(\cos(\theta_1 + \theta_2) + i \sin(\theta_1 + \theta_2)) \quad \text{using } |z_1||z_2| = |z_1 z_2|.
\end{aligned}$$

It follows that

$$\begin{aligned}
z^{-1} &= |z|^{-1}(\cos(-\theta) + i \sin(-\theta)) = |z|^{-1}(\cos(\theta) - i \sin(\theta)), \quad \text{if } z \neq 0, \\
z^n &= |z|^n(\cos(n\theta) + i \sin(n\theta)), \qquad n \in \mathbb{Z}.
\end{aligned}$$

The second formula above is called *de Moivre's formula* and can be proved using induction on the integer n. De Moivre's formula can be used to find roots of complex numbers. Note that the first formula above can be expressed, for $z = a + ib \neq 0$, as

$$z^{-1} = (a + ib)^{-1} = (a - ib)/(\sqrt{a^2 + b^2})^2 = \bar{z}/|z|^2.$$

Suppose we are given a nonzero complex number z_0 and a positive integer n. To find nth roots of z_0, we must solve $z^n = z_0$. Write $z_0 = |z_0|(\cos\theta_0 + i\sin\theta_0)$. From DeMoivre's formula, we see that $z = |z|(\cos\theta + i\sin\theta)$ must satisfy

$$|z|^n = |z_0| \ \text{ and } \ n\theta = \theta_0 + 2\pi k,\ k \in \mathbb{Z}.$$

Since both $|z_0|$ and $|z|$ are positive real numbers, we have $|z| = |z_0|^{1/n}$ (that is, $|z|$ is the unique positive nth root of $|z_0|$). The angle θ is of the form $\theta = \theta_0/n + 2\pi k/n$ for k an integer. The values $k = 0, 1, \ldots, n-1$ determine n distinct values for θ. Any other value of k would yield one of the n values for θ obtained from $0, 1, \ldots, n-1$. Therefore the nth roots of the nonzero complex number z_0 are

$$|z_0|^{1/n}(\cos(\theta_0/n + 2\pi k/n) + i\sin(\theta_0/n + 2\pi k/n)), \qquad k = 0, 1, \ldots, n-1.$$