MATH 2135 Linear Algebra
Fields

Alyssa Motas

February 16, 2021

Contents

1 What is Abstract Algebra?

In algebra, which is a broad division of mathematics, abstract algebra (occasionally called modern algebra) is the study of algebraic structures. Algebraic structures include groups, rings, fields, modules, vector spaces, lattices, and algebras. [1]

Arithmetic involves $2 + 3 = 5$, and basic algebra involves using laws in $2 + x = 5$. For abstract algebra, we use laws $(x + y = y + x)$ *without* any arithmetic.

Example. Let $\mathbb{Z}_2 = \{0, 1\}$, the integers modulo 2. We can define the following addition and multiplication rules:

$$\begin{aligned} 0 + 0 &= 0 & 0 \cdot 0 &= 0 \\ 0 + 1 &= 1 & 0 \cdot 1 &= 0 \\ 1 + 0 &= 1 & 1 \cdot 0 &= 0 \\ 1 + 1 &= 0 & 1 \cdot 1 &= 1. \end{aligned}$$

Examples of laws. For all x, y, $x + y = y + x$

x	y	$x + y$	$y + x$
0	0	0	0
0	1	1	1
1	0	1	1
1	1	0	1

$$xy = yx \qquad (x + y) + z = x + (y + z)$$

...plus many additional laws.

[1] Definition taken from Wikipedia.

2 Fields

Definition. A *field* is a set F, with distinct elements $0, 1 \in F$, and together with two binary operations

$$+ : F \times F \to F \qquad \cdot : F \times F \to F,$$

called *addition* and *multiplication*, respectively, and satisfying the following nine axioms:

(A1) *Commutativity of addition.* For all $a, b \in F$, we have

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

(A2) *Associativity of addition.* For all $a, b, c \in F$, we have

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

(A3) *Additive identity.* For all $a \in F$, we have

$$0 + a = a.$$

(A4) *Additive inverse.* For all $a \in F$, there exists $b \in F$ such that

$$a + b = 0.$$

(FM1) *Commutativity of multiplication.* For all $a, b \in F$,

$$ab = ba.$$

(FM2) *Associativity of multiplication.* For all $a, b, c \in F$,

$$(ab)c = a(bc).$$

(FM3) *Multiplicative identity.* For all $a \in F$,

$$1a = a.$$

(FM4) *Multiplicative inverse.* For all $a \in F$, if $a \neq 0$, then there exists $b \in F$ such that

$$ab = 1.$$

In $\mathbb{R}$, it would look like

$$b = \frac{1}{a}.$$

(D) *Distributivity.* For all $a, b, c \in F$, we have

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

Note. There are many additional laws of fields besides the above 9. But they are all consequences of the 9 axioms stated above.

Examples of fields.

1. The set $\mathbb{R}$ of real numbers, with the "usual" addition and multiplication, is a field.

2. The set $\mathbb{C}$ of complex numbers is a field.

3. The set $\mathbb{Q}$ of rational numbers is a field.

4. The set $\mathbb{Z}$ of integers is *not* a field. It only satisfies 8 of the 9 axioms and the one that fails is (FM4).

5. The set $\mathbb{N}$ of natural numbers is *not* a field. It only satisfies 7 of the 9 axioms and the ones that fail are (A4) and (FM4).

6. The set $\mathbb{Z}_2$ of integers modulo 2 is a field (with the above addition and multiplication).

7. Let $n \geq 2$, and let $\mathbb{Z}_n$ be the integers modulo n, with addition and multiplication taken modulo n. Then, there are two cases:

   (a) If n is prime, then $\mathbb{Z}_n$ is a field.

   (b) If n is not prime, then $\mathbb{Z}_n$ is not a field. The only failed axiom is (FM4).

3 Elementary Properties of Fields

3.1 Cancellation of addition

For all $x, y, a \in F$, if $x + a = y + a$, then $x = y$.

Proof. Take arbitrary[2] elements $x, y, a \in F$. Assume[3] $x + a = y + a$ and we need to show that $x = y$. By (A4), a has an additive inverse. So, let b be its additive inverse, $a + b = 0$.

$$\begin{aligned}
x &= 0 + x && \text{by (A3)} \\
&= x + 0 && \text{by (A1)} \\
&= x + (a + b) && \text{because } b \text{ is the additive inverse of } a \\
&= (x + a) + b && \text{by (A2)} \\
&= (y + a) + b && \text{by assumption} \\
&= y + (a + b) && \text{by (A2)} \\
&= y + 0 && \text{because } b \text{ is the additive inverse of } a \\
&= 0 + y && \text{by (A1)} \\
&= y && \text{by (A3).}
\end{aligned}$$

Therefore, $x = y$, which is what we had to show. □

3.2 Cancellation of multiplication

For all elements x, y, a of a field, if $xa = ya$ and $x \neq 0$, then $x = y$.

Proof. Assume both $xa = ya$ and $a \neq 0$ are true, and we need to show that $x = y$. Let b be the multiplicative inverse of a, where $ab = 1$. By (FM3),

[2] When we need to prove a "for all" statement, we do it by taking arbitrary elements and prove it.

[3] When we need to prove an "if-then" statement, we do it by assuming the if-part then proving the else-part.

we can rewrite x as

$$
\begin{aligned}
x &= 1 \cdot x \\
&= (ab)x \\
&= \left(a \cdot \frac{1}{a}\right) x && \text{since } b = \frac{1}{a} \\
&= \frac{1}{a}(a \cdot x) && \text{by (FM1)} \\
&= \frac{1}{a}(xa) \\
&= \frac{1}{a}(ya) && \text{since } xa = ya \\
&= \frac{1}{a}(a \cdot y) \\
&= \left(\frac{1}{a} \cdot a\right) y \\
&= (ab)y \\
&= 1 \cdot y = y.
\end{aligned}
$$

Therefore, $xa = ya \Leftrightarrow x = y$ if and only if $a \neq 0$, as shown above. □

3.3 $0a = 0$

For all elements a of a field F, we have

$$0a = 0.$$

Proof. Consider an arbitrary element $a \in F$. We must show that $0a = 0$.

$$
\begin{aligned}
0 + 0a &= 0a && \text{by (A3)} \\
&= (0 + 0)a && \text{by (A3)} \\
&= a(0 + 0) && \text{by (FM1)} \\
&= a0 + a0 && \text{by (D)} \\
&= 0a + 0a && \text{by (FM1)}
\end{aligned}
$$

Therefore, by cancellation of addition (Proposition 3.1), it follows that

$$0 = 0a.$$

□

3.4 $ab = 0$

In any field F, for all $a, b \in F$, if $ab = 0$, then $a = 0$ or $b = 0$.[4]

Proof. Take arbitrary $a, b \in F$ and assume that $ab = 0$. We need to show that $a = 0$ or $b = 0$.

Case 1. When $a = 0$, then the conclusion holds.
Case 2. When $a \neq 0$, by (FM4), a has a multiplicative inverse. Let c be such an inverse, i.e. $ac = 1$. Then

$$\begin{aligned}
b &= 1b && \text{by (FM3)}\\
&= (ac)b && \text{by definition of } c\\
&= (ca)b && \text{by (FM1)}\\
&= c(ab) && \text{by (FM2)}\\
&= c0 && \text{by assumption}\\
&= 0c && \text{by (FM1)}\\
&= 0 && \text{by Proposition 3.3}
\end{aligned}$$

So $b = 0$ as desired. □

3.5 $z + a = a$

In any field F, if $z \in F$ is an element that acts like a zero, i.e. such that for all $a \in F$, $z + a = a$, then $z = 0$.

Proof. Let $z \in F$ be such an element. Assume that $z + a = a$. Then we have

$$\begin{aligned}
z &= 0 + z && \text{by (A3)}\\
&= z + 0 && \text{by (A1)}\\
&= 0 && \text{by assumption.}
\end{aligned}$$

□

3.6 Unique additive inverse

Let F be a field. For every $a \in F$, the element $b \in F$ in axiom (A4) is *uniquely* determined. In other words, if $b, c \in F$ are two additive inverses of a, then $b = c$.

[4] We use this all the time when solving equations such as $x^2 + 3x + 2 = 0 \Rightarrow x = -1, -2$.

Proof. Because b is an additive inverse of a, we have

$$a + b = 0. \tag{1}$$

Similar to c, we also have

$$a + c = 0. \tag{2}$$

From (1) and (2), we get

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

From (A1), we get

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

By Proposition 3.1 (cancellation of addition), we get

$$b = c.$$

□

Definition. Since the additive inverse of a is unique, we can introduce a notation for it. We write $b = (-a)$ when b is the additive inverse of a.

From now on, we can write

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

We define *subtraction* as $a - b$ which is an abbreviation for $a + (-b)$.

All of the "usual" laws of negative and subtraction follow from the field axioms.

3.7 Unique multiplicative identity

In a field, the element 1 is uniquely determined by axiom (FM3).

Proof. Suppose we represent b, c as multiplicative identities of a, where $a, b, c \in F$. By (FM3), we have

$$a \cdot b = a \quad \text{and} \quad a \cdot c = a.$$

Then we have

$$\begin{aligned} a \cdot b &= a \cdot c \\ \Rightarrow b &= c \qquad \text{by Proposition 3.2} \end{aligned}$$

This implies that the multiplicative identity of a is unique and there can be no more than one of it. □

3.8 Unique multiplicative inverse

For any element $a \neq 0$ of a field, the element b in axiom (FM4) is uniquely determined.

Proof. Suppose b, c are multiplicative inverses of a, where $a \neq 0$ and $a, b, c \in F$. By the definition of (FM4), we have

$$a \cdot b = 1 \quad \text{and} \quad a \cdot c = 1.$$

It follows that, since both equations are equal to 1, we can use the axiom (FM3) to prove that $b = c$.

$$\begin{aligned} b &= 1 \cdot b \\ &= (c \cdot a)b \\ &= c(a \cdot b) \\ &= c \cdot 1 \\ &= c. \end{aligned}$$

Hence, we get $b = c$, which implies that the multiplicative inverse of any element is unique. □

3.9 Right Distributivity

Distributivity also holds on the right: $(b + c)a = ba + ca$.

Proof. This is a direct consequence of (D) and (FM1). □

3.10 Laws of Negative

(a) $-(-a) = a$

(b) $-(ab) = (-a)b = a(-b)$
$(-a)(-b) = ab$

(c) $-a = (-1)a$

Proof. (a) By definition of $(-a)$, we have $a+(-a) = 0$. Also, by definition of $-(-a)$ (and commutativity), we have $(-(-a)) + (-a) = 0$. By cancellation, it follows that $a = -(-a)$.

(b) To show that $-(ab) = (-a)b$, we need to show that $(-a)b$ is the negative of ab, in other words, that $ab + (-a)b = 0$. This follows from the axioms:

$$\begin{aligned} ab + (-a)b &= (a + (-a))b && \text{by distributivity} \\ &= 0b && \text{by (A4)} \\ &= 0 && \text{by Proposition 3.3} \end{aligned}$$

The proof of $-(ab) = a(-b)$ is similar.
(c) By (FM3) and (b), we have $-a = -(1a) = (-1)a$. $\square$

3.10.1 Laws of subtraction

1. $(a - b)(c - d) = ac - ad - bc + bd$