More algebraic structures

Casey Blacker
Math 300

Section 1

Rings

Definition

A *ring* $(R, +, \cdot)$ comprises a set R and two binary operations $+, \cdot : R \times R \to R$, such that

i. $(R, +)$ is an abelian group,
ii. $(R, \cdot)$ is a monoid,
iii. the operation $\cdot$ *distributes* over $+$, that is, for all $a, b, c \in R$,

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$
$$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$$

Remarks

i. We typically call $+$ *addition* and $\cdot$ *multiplication*.
ii. The additive identity of R is conventionally denoted $0 \in R$ and called *zero, and the multiplicative identity by* $1 \in R$ *and called one.*

Remarks

i. If the multiplication $\cdot$ is commutative, then $(R, +, \cdot)$ is called a *commutative ring*.

ii. If $(R, +, \cdot)$ satisfies all the conditions of a ring except for the existence of a multiplicative identity $1 \in R$, then it is called a *rng*.

Challenge! Is it a ring?

Is it a ring?

$$(\mathbb{Z}, +, \cdot)$$

Yes!

Is it a ring?

$$(\mathbb{R}, +, \cdot)$$

Yes!

Is it a ring?

$$(\mathbb{N}, +, \cdot)$$

No!

Is it a ring?

$$(2\mathbb{Z}, +, \cdot)$$

No!

Is it a ring?

$$(\{0\}, +, \cdot)$$

Yes! The *zero ring*

Definition

A *zero divisor* in a commutative ring $(A, +, \cdot)$ is an element $a \in A$ for which there exists a nonzero $b \in A$ with $ab = 0$.

Definition

A commutative ring $(R, +, \cdot)$ is called an *integral domain* when

i. it does not contain any nonzero zero divisor,
ii. $0 \neq 1$.

Is it an integral domain?

$$(\mathbb{Z}, +, \cdot)$$

Yes!

Is it an integral domain?

$$(\{0\}, +, \cdot)$$

No!

Is it an integral domain?

$$(\mathbb{Z}_4, +, \cdot)$$

No!

Section 2

Fields

Definition

An integral domain $(R, +, \cdot)$ is called a *field* when every nonzero element $a \in R\backslash\{0\}$ has a multiplicative inverse $a^{-1} \in R$.

Is it a field?

$$(\mathbb{Z}, +, \cdot)$$

No!

Is it a field?

$$(\mathbb{R}, +, \cdot)$$

Yes!

Is it a field?

$$(\{0\}, +, \cdot)$$

No!

Is it a field?

$$(\mathbb{Z}_2, +, \cdot)$$

Yes!

Section 3

Vector spaces

Definition

Let k be field. A *k-vector space* $(V, +, \cdot)$ comprises a set V together with operations

$$+ : V \times V \to V$$
$$\cdot : k \times V \to V$$

such that

i. $(V, +)$ is an abelian group
ii. *scalar multiplication* $\cdot$ and *vector addition* $+$ satisfy

$$1 \cdot u = u$$
$$(a + b) \cdot u = (a \cdot u) + (b \cdot u)$$
$$a \cdot (b \cdot u) = (a \cdot b) \cdot u$$
$$a \cdot (u + v) = (a \cdot u) + (a \cdot v)$$

Is it a vector space?

$$k = \mathbb{R},\ V = \mathbb{R}$$

Yes!

Is it a vector space?

$$k = \mathbb{R}, \; V = \mathbb{C}$$

Yes!

Is it a vector space?

$$k = \mathbb{Z},\ V = \mathbb{R}$$

No!

Is it a vector space?

$$k = \mathbb{R}, \ V = \mathbb{R}^n$$

Yes!

Section 4

Modules

Fix a ring R.

Definition

An *R-module* $(V, +, \cdot)$ comprises a set V together with operations

$$+ : V \times V \to V$$

and

$$\cdot : k \times V \to V$$

that together satisfy the familiar vector space conditions.

Remark

That is, an R-module is a vector space with a ring of scalars R rather than a field of scalars k.

Is it a module?

k-vector space V

Yes!

Is it a module?

$$R = \mathbb{Z},\ V = \mathbb{Z}^n$$

Yes!

Is it a module?

$$R = \{0\},\ V = \{0\}$$

Yes!