

MATH 415  
Modern Algebra I

**Lecture 20:**  
**Rings.**

# Groups

*Definition.* A **group** is a binary structure  $(G, *)$  that satisfies the following axioms:

**(G0: closure)**

for all elements  $g$  and  $h$  of  $G$ ,  $g * h$  is an element of  $G$ ;

**(G1: associativity)**

$(g * h) * k = g * (h * k)$  for all  $g, h, k \in G$ ;

**(G2: existence of identity)**

there exists an element  $e \in G$ , called the **identity** (or **unit**) of  $G$ , such that  $e * g = g * e = g$  for all  $g \in G$ ;

**(G3: existence of inverse)**

for every  $g \in G$  there exists an element  $h \in G$ , called the **inverse** of  $g$ , such that  $g * h = h * g = e$ .

The group  $(G, *)$  is said to be **commutative** (or **abelian**) if it satisfies an additional axiom:

**(G4: commutativity)**  $g * h = h * g$  for all  $g, h \in G$ .

# Semigroups

*Definition.* A **semigroup** is a binary structure  $(S, *)$  that satisfies the following axioms:

**(S0: closure)**

for all elements  $g$  and  $h$  of  $S$ ,  $g * h$  is an element of  $S$ ;

**(S1: associativity)**

$(g * h) * k = g * (h * k)$  for all  $g, h, k \in S$ .

The semigroup  $(S, *)$  is said to be a **monoid** if it satisfies an additional axiom:

**(S2: existence of identity)** there exists an element  $e \in S$  such that  $e * g = g * e = g$  for all  $g \in S$ .

Optional useful properties of semigroups:

**(S3: cancellation)**  $g * h_1 = g * h_2$  implies  $h_1 = h_2$  and  $h_1 * g = h_2 * g$  implies  $h_1 = h_2$  for all  $g, h_1, h_2 \in S$ .

**(S4: commutativity)**  $g * h = h * g$  for all  $g, h \in S$ .

# Rings

*Definition.* A **ring** is a set  $R$ , together with two binary operations usually called **addition** and **multiplication** and denoted accordingly, such that

- $R$  is an abelian group under addition,
- $R$  is a semigroup under multiplication,
- multiplication distributes over addition.

The complete list of axioms is as follows:

**(A0)** for all  $x, y \in R$ ,  $x + y$  is an element of  $R$ ;

**(A1)**  $(x + y) + z = x + (y + z)$  for all  $x, y, z \in R$ ;

**(A2)** there exists an element, denoted  $0$ , in  $R$  such that  $x + 0 = 0 + x = x$  for all  $x \in R$ ;

**(A3)** for every  $x \in R$  there exists an element, denoted  $-x$ , in  $R$  such that  $x + (-x) = (-x) + x = 0$ ;

**(A4)**  $x + y = y + x$  for all  $x, y \in R$ ;

**(M0)** for all  $x, y \in R$ ,  $xy$  is an element of  $R$ ;

**(M1)**  $(xy)z = x(yz)$  for all  $x, y, z \in R$ ;

**(D)**  $x(y+z) = xy+xz$  and  $(y+z)x = yx+zx$  for all  $x, y, z \in R$ .

## Examples of rings

Informally, a ring is a set with three arithmetic operations: addition, subtraction and multiplication. Subtraction is defined by  $x - y = x + (-y)$ .

- Real numbers  $\mathbb{R}$ .
- Integers  $\mathbb{Z}$ .
- $2\mathbb{Z}$ : even integers.
- $\mathbb{Z}_n$ : congruence classes modulo  $n$ .
- $\mathcal{M}_{n,n}(\mathbb{R})$ : all  $n \times n$  matrices with real entries.
- $\mathcal{M}_{n,n}(\mathbb{Z})$ : all  $n \times n$  matrices with integer entries.
- $\mathbb{R}[X]$ : polynomials in variable  $X$  with real coefficients.
- All functions  $f : S \rightarrow \mathbb{R}$  on a nonempty set  $S$ .
- **Zero ring**: any additive abelian group with trivial multiplication:  $xy = 0$  for all  $x$  and  $y$ .
- Trivial ring  $\{0\}$ .

## Multiplication modulo $n$

We have an isomorphism of additive groups  $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$ . Oftentimes,  $\mathbb{Z}_n$  is identified with  $\mathbb{Z}/n\mathbb{Z}$ .

We can define multiplication on  $\mathbb{Z}_n$  in two ways. Directly, given  $x, y \in \{0, 1, 2, \dots, n-1\}$ , we let  $x \cdot_n y$  to be the remainder under division of  $xy$  by  $n$  (**multiplication modulo  $n$** ).

Alternatively, we define multiplication on  $\mathbb{Z}/n\mathbb{Z}$  by  $(x + n\mathbb{Z})(y + n\mathbb{Z}) = xy + n\mathbb{Z}$  for all  $x, y \in \mathbb{Z}$ .

Then  $\mathbb{Z}_n$  becomes a ring.

**Example.** Let  $M$  be the set of all  $2 \times 2$  matrices of the form  $\begin{pmatrix} x & -y \\ y & x \end{pmatrix}$ , where  $x, y \in \mathbb{R}$ .

$$\begin{aligned} \begin{pmatrix} x & -y \\ y & x \end{pmatrix} + \begin{pmatrix} x' & -y' \\ y' & x' \end{pmatrix} &= \begin{pmatrix} x + x' & -(y + y') \\ y + y' & x + x' \end{pmatrix}, \\ - \begin{pmatrix} x & -y \\ y & x \end{pmatrix} &= \begin{pmatrix} -x & -(-y) \\ -y & -x \end{pmatrix}, \\ \begin{pmatrix} x & -y \\ y & x \end{pmatrix} \begin{pmatrix} x' & -y' \\ y' & x' \end{pmatrix} &= \begin{pmatrix} xx' - yy' & -(xy' + yx') \\ xy' + yx' & xx' - yy' \end{pmatrix}. \end{aligned}$$

Hence  $M$  is closed under matrix addition, taking the negative, and matrix multiplication. Also, the multiplication is commutative on  $M$ . The associativity and commutativity of the addition, the associativity of the multiplication, and the distributive law hold on  $M$  since they hold for all  $2 \times 2$  matrices. Thus  $M$  is a commutative ring.

*Remark.*  $M$  is the ring of complex numbers  $x + yi$  “in disguise”.

## Basic properties of rings

Let  $R$  be a ring.

- The zero  $0 \in R$  is unique.
- For any  $x \in R$ , the negative  $-x$  is unique.
- $-(-x) = x$  for all  $x \in R$ .
- $x0 = 0x = 0$  for all  $x \in R$ .
- $(-x)y = x(-y) = -xy$  for all  $x, y \in R$ .
- $(-x)(-y) = xy$  for all  $x, y \in R$ .
- $x(y - z) = xy - xz$  for all  $x, y, z \in R$ .
- $(y - z)x = yx - zx$  for all  $x, y, z \in R$ .



## Divisors of zero

**Theorem** Let  $R$  be a ring. Then  $x0 = 0x = 0$  for all  $x \in R$ .

*Proof:* Let  $y = x0$ . Then  $y + y = x0 + x0 = x(0 + 0) = x0 = y$ . It follows that  $(-y) + y + y = (-y) + y$ , hence  $y = 0$ . Similarly, one shows that  $0x = 0$ .

A nonzero element  $x$  of a ring  $R$  is a **left zero divisor** if  $xy = 0$  for another nonzero element  $y \in R$ . The element  $y$  is called a **right zero divisor**.

*Examples.* • In the ring  $\mathbb{Z}_6$ , the zero divisors are congruence classes of 2, 3 and 4, as  $2 \cdot 3 \equiv 4 \cdot 3 \equiv 0 \pmod{6}$ .

• In the ring  $\mathcal{M}_{n,n}(\mathbb{R})$ , the zero divisors (both left and right) are nonzero matrices with zero determinant. For instance,

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

• In any zero ring, all nonzero elements are zero divisors.

## Integral domains

A ring  $R$  is called a **domain** if it has no zero divisors.

**Theorem** Given a nontrivial ring  $R$ , the following are equivalent:

- $R$  is a domain,
- $R \setminus \{0\}$  is a semigroup under multiplication,
- $R \setminus \{0\}$  is a semigroup with cancellation under multiplication.

*Idea of the proof:* No zero divisors means that  $R \setminus \{0\}$  is closed under multiplication. Further, if  $a \neq 0$  then  $ab = ac \implies a(b - c) = 0 \implies b - c = 0 \implies b = c$ .

A ring  $R$  is called **commutative** if the multiplication is commutative.  $R$  is called a **ring with unity** if there exists an identity element for multiplication (denoted 1).

An **integral domain** is a nontrivial commutative ring with unity and no zero divisors.