

MATH 433  
Applied Algebra

**Lecture 23:**  
**Rings.**  
**Fields.**

# Groups

*Definition.* A **group** is a set  $G$ , together with a binary operation  $*$ , that satisfies the following axioms:

**(G1: closure)**

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

**(G2: associativity)**

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

**(G3: 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  $g \in G$ ;

**(G4: 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:

**(G5: commutativity)**  $g * h = h * g$  for all  $g, h \in G$ .

# Semigroups

*Definition.* A **semigroup** is a nonempty set  $S$ , together with a binary operation  $*$ , that satisfies the following axioms:

**(S1: closure)**

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

**(S2: 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:

**(S3: existence of identity)** there exists an element  $e \in S$  such that  $e * g = g * e = g$  for all  $g \in S$ .

Additional useful properties of semigroups:

**(S4: 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  $g, h_1, h_2 \in S$ .

**(S5: 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:

**(R1)** for all  $x, y \in R$ ,  $x + y$  is an element of  $R$ ;

**(R2)**  $(x + y) + z = x + (y + z)$  for all  $x, y, z \in R$ ;

**(R3)** there exists an element, denoted  $0$ , in  $R$  such that  $x + 0 = 0 + x = x$  for all  $x \in R$ ;

**(R4)** for every  $x \in R$  there exists an element, denoted  $-x$ , in  $R$  such that  $x + (-x) = (-x) + x = 0$ ;

**(R5)**  $x + y = y + x$  for all  $x, y \in R$ ;

**(R6)** for all  $x, y \in R$ ,  $xy$  is an element of  $R$ ;

**(R7)**  $(xy)z = x(yz)$  for all  $x, y, z \in R$ ;

**(R8)**  $x(y+z) = xy+xz$  and  $(y+z)x = yx+zx$  for all  $x, y, z \in R$ .

## Examples of rings

In most examples, addition and multiplication are naturally defined and verification of the axioms is straightforward.

- Real numbers  $\mathbb{R}$ .
- Integers  $\mathbb{Z}$ .
- $2\mathbb{Z}$ : even integers.
- $\mathbb{Z}_n$ : congruence classes modulo  $n$ .
- $\mathcal{M}_n(\mathbb{R})$ : all  $n \times n$  matrices with real entries.
- $\mathcal{M}_n(\mathbb{Z})$ : all  $n \times n$  matrices with integer entries.
- $\mathbb{R}[X]$ : polynomials in variable  $X$  with real coefficients.
- $\mathbb{R}(X)$ : rational functions 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  $\{0\}$ .

**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”.

## Zero-divisors

**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  $[2]_6$ ,  $[3]_6$ , and  $[4]_6$ , as  $[2]_6[3]_6 = [4]_6[3]_6 = [0]_6$ .

• In the ring  $\mathcal{M}_n(\mathbb{R})$ , 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 identity** if there exists an identity element for multiplication (denoted 1).

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



# Fields

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

- $F$  is an Abelian group under addition,
- $F \setminus \{0\}$  is an Abelian group under multiplication,
- multiplication distributes over addition.

In other words, the field is a commutative ring with identity ( $1 \neq 0$ ) such that any nonzero element has a multiplicative inverse.

*Examples.* • Real numbers  $\mathbb{R}$ .

- Rational numbers  $\mathbb{Q}$ .
- Complex numbers  $\mathbb{C}$ .
- $\mathbb{Z}_p$ : congruence classes modulo  $p$ , where  $p$  is prime.
- $\mathbb{R}(X)$ : rational functions in variable  $X$  with real coefficients.

## Quotient field

**Theorem** A ring  $R$  with identity can be extended to a field if and only if it is an integral domain.

If  $R$  is an integral domain, then there is a smallest field  $F$  containing  $R$  called the **quotient field** of  $R$ . Any element of  $F$  is of the form  $b^{-1}a$ , where  $a, b \in R$ .

- Examples.*
- The quotient field of  $\mathbb{Z}$  is  $\mathbb{Q}$ .
  - The quotient field of  $\mathbb{R}[X]$  is  $\mathbb{R}(X)$ .