MATH 3022 Algebra II **Lecture 2**
LECTURE JOE TRAN

Recall: We introduced the definition of a ring, and we mentioned how we require *two* binary operations for a ring, namely an "addition" operation $+$ and a "multiplication" operator $\cdot$.

Definition 1. Let R be a set and let $+$ and $\cdot$ be operations of "addition" and "multiplication". Then R is said to be a *ring*, if

(1) $(R, +)$ is an abelian group.
(2) For every $x, y, z \in R$, $x(yz) = (xy)z$
(3) For every $x, y, z \in R$, $x(y+z) = xy + xz$ and $(x+y)z = xz + yz$

Example 1. The following are examples of rings:

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_n$, and $n\mathbb{Z}$, which are typical examples rings.
- $\mathbb{F}[x]$
- $\mathcal{M}_n(\mathbb{F})$ which is the set of all $n \times n$ matrices with $\mathbb{F}$ entries.
- $\mathbb{H}$ which is the set of quaternions, where

$$\mathbb{H} = \left\{ \begin{bmatrix} \alpha & \beta \\ -\overline{\beta} & -\overline{\alpha} \end{bmatrix} : \alpha = a + \mathbf{i}d, \beta = b + \mathbf{i}b \in \mathbb{C} \right\} = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} : a, b, c, d \in \mathbb{R}\}$$

Proposition 1. *Let R be a ring and let $x, y \in R$. Then*

(1) $x0 = 0x = 0$
(2) $x(-y) = (-x)y = -xy$
(3) $(-x)(-y) = xy$

Proof. To prove (1), using the distributive property,

$$x0 = x(0+0) = x0 + x0$$

and so $x0 = 0$. In a similar approach, it can be shown that $0x = 0$.

To show that (2) is true, observe that

$$x(-y) + xy = x(-y + y) = x0 = 0$$

and similarly, $(-x)y = -xy$ as well.

Finally, to see that (3) is true, note that by (2), and using the associative property of "multiplication"

$$(-x)(-y) = -(x(-y)) = -(-xy) = xy$$

as desired. □

There are various types of rings that we will look at.

Definition 2. A ring R is said to be a *commutative ring* if for every $x, y \in R$, $xy = yx$. That is, multiplication is also commutative.

Example 2. $\mathbb{Z}$, $\mathbb{F}$, $\mathbb{Z}_n$, $n\mathbb{Z}$, and $\mathbb{F}[x]$ are examples of commutative rings, but $\mathcal{M}_n(\mathbb{F})$ and $\mathbb{H}$ are not.

Definition 3. A ring R is said to be a *ring with identity* if there exists $1 \in R$ with $1 \neq 0$ such that $x1 = 1x = x$ for all $x \in R$.

Example 3. $\mathbb{Z}$, $\mathbb{F}$, $\mathbb{Z}_n$, $R[x]$ (where R is a ring), $\mathcal{M}_n(\mathbb{F})$ and $\mathbb{H}$ are examples of rings with identity, but $n\mathbb{Z}$ is not a ring with an identity whenever $n \geq 2$. In particular, the identity of $R[x]$ is $1 = 1 + 0x$, and the identity for $\mathcal{M}_n(\mathbb{F})$ is the identity matrix I_n.

Before we introduce the integral domain, we introduce the zero divisor.

Definition 4. Let R be a commutative ring. A nonzero element $x \in R$ is called a zero divisor if there exists a nonzero element $y \in R$ such that $xy = yx = 0$.

Example 4. Consider $\mathbb{Z}_8$ and take $2, 4 \in \mathbb{Z}_8$, which are both nonzero elements in $\mathbb{Z}_8$. Then

$$2 \cdot_8 4 = 2 \cdot 4 \textbf{ mod } 8 = 8 \textbf{ mod } 8 = 0$$

Also, if we take $4, 6 \in \mathbb{Z}_8$, which are also both nonzero, then

$$4 \cdot_8 6 = 4 \cdot 6 \textbf{ mod } 8 = 24 \textbf{ mod } 8 = 0$$

Definition 5. A commutative ring R with identity is called an *integral domain* if it does not contain nonzero divisors. Alternatively, R is said to be an *integral domain* if for every $x, y \in R$ such that $xy = 0$, then either $x = 0$ or $y = 0$.

Example 5. $\mathbb{F}$ and $\mathbb{H}$ are examples of integral domains. However, because $\mathcal{M}_n(\mathbb{F})$ is not commutative, then it cannot be an integral domain.

Example 6. Consider $\mathbb{Z}_n$ for $n \geq 2$ such that n is not a prime number. Then $n = xy$ for some $x, y \in \mathbb{Z}$, so

$$x \cdot_n y = x \cdot y \textbf{ mod } n = n \textbf{ mod } n = 0$$

so $\mathbb{Z}_n$ is not an integral domain. Consider if n is prime, i.e. $n = p$. Then $\mathbb{Z}_p$ is both commutative and contains the identity. Suppose $x \cdot_p y = x \cdot y \textbf{ mod } p = 0$ in $\mathbb{Z}_p$. Then by definition, $p \mid xy$, so by Euclid's Lemma, either $p \mid x$ or $p \mid y$. That is, either $x = 0$ or $y = 0$. Therefore, $\mathbb{Z}_p$ has no zero divisors, and thus, is an integral domain.

Proposition 2. *$\mathbb{Z}_n$ is an integral domain whenever n is prime.*

Example 7. Let R be a ring that is either $\mathbb{Z}$, $\mathbb{Z}_n$ or $\mathbb{F}$. Is $R[x]$ an integral domain? For sure, the set $R[x]$ is a commutative ring with identity. So we check if it is an integral domain. Let $p(x)$ and $q(x)$ be polynomials in $R[x]$ such that $p(x)q(x) = 0$. [...]