MATH 3022 Algebra II **Lecture 7**
LECTURE JOE TRAN

Recall in the previous lecture:

(1) The characteristic of an integral domain is either prime or zero.

(2) If R has characteristic zero, then $|R|$ is not finite.

(1) + (2) The characteristic of a finite field is a prime p.

(3) If R is a commutative ring with no zero divisors, then every nonzero elements have the same additive order.

- This implies that every nonzero element in an infinite field has additive order p.

From point •, this would imply that the field $(F, +)$ is a p-group.

Definition 1. A group $(G, *)$ is said to be a p-group if $|G| = p^m$.

Corollary 1 (15.2)**.** *Let G be a finite group. Then G is a p-group if and only if $|G| = p^m$.*

Corollary 2. *Let F be a finite field with characteristic p (prime), then $|F| = p^m$ for some $m \in \mathbb{Z}$.*

1 Ring Homomorphisms

Definition 2. Let $(R, +_R, \cdot_R)$ and $(S, +_S, \cdot_S)$[1] be two rings with respect to their own operations. Then the mapping $\phi : R \to S$ is said to be a *ring homomorphism* if for all $x, y \in R$,

$$\phi(x +_R y) = \phi(x) +_S \phi(y)$$
$$\phi(x \cdot_R y) = \phi(x) \cdot_S \phi(y)$$

Observe that for $n \in \mathbb{N}$ and for all $x \in R$,

$$\begin{aligned}\phi(nx) &= \phi(x +_R x +_R \cdots +_R x) \\ &= \phi(x) +_S \phi(x) +_S + \cdots +_S \phi(x) \\ &= n\phi(x)\end{aligned}$$

[1] I will use triplets to denote the ring $(R, +, \cdot)$, where R is the ring, and $+$ and $\cdot$ are the operations of addition and multiplication, respectively.

Also observe that $\phi(x^n) = \phi^n(x)$ and also, $\phi(0_R) = 0_S$[2].

Taking the first observation and the third observation, if $nx = 0_R$, then $n\phi(x) = 0_S$, and furthermore, if the additive order of x i n, then the additive order of $\phi(x) \mid n$.

Also on Assignment: If R and S are rings with identity and ϕ is onto, then $\phi(1_R) = 1_S$.

Question 1. *Give an example where ϕ is not onto and $\phi(1_R) \neq 1_S$.*

Example 1.
- Let $\phi : \mathbb{Z} \to \mathbb{Z}_n$ given by $\phi(x) = x \bmod n$ for all $x \in \mathbb{Z}$ is a ring homomorphism.
- Let $\phi : \mathbb{C} \to \mathbb{C}$ be defined by $\phi(a + ib) = a - ib$ for all $a, b \in \mathbb{R}$ is a ring homomorphism.

Definition 3. A ring homomorphism $\phi : R \to S$ is said to be a ring isomorphism if ϕ is a bijection.

Example 2. For a fixed $a \in R$, define $\phi : R[x] \to R$ given by

$$\phi_a(f(x)) = f(a)$$

This is called the *evaluation homomorphism*. Indeed,

$$\phi_a(f(x) + g(x)) = f(a) + g(x) = \phi_a(f(x)) + \phi_a(g(x))$$

and

$$\phi_a(f(x)g(x)) = f(a)g(a) = \phi_a(f(x))\phi_a(g(x))$$

Question 2. *Is the mapping $\phi : \mathbb{R} \to \mathbb{R}$ given by $\phi(a) = -a$ a ring homomorphism?*

No it is not. Take $2, 3 \in \mathbb{R}$ and observe that

$$\phi(2 \cdot 3) = -6 = 6 == -2 \cdot -3 = \phi(2)\phi(3)$$

which is absurd.

Example 3. Determine all ring homomorphisms from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{30}$.

Let $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_{30}$ be a mapping and let $\phi(x \bmod 12) = y \bmod 30$. Then

$$\phi(12 \cdot 1 \bmod 12) = 12 \cdot y \bmod 30$$

[2] Question 8 on Assignment 1

would imply that $12y \bmod 30 = 0 \bmod 30$, and so $12y \equiv 0 \pmod{30}$, i.e. all y such that $30 \mid 12y$. So $y \bmod 30 = 0, 5, 10, 15, 20, 25$.

Observe that $\phi(1 \bmod 12) = y \bmod 30$ implies that

$$\phi(x \bmod 12) = \phi(\underbrace{1 +_{12} + \cdots +_{12} 1}_{x\ times}) = x(y \bmod 30) = xy \bmod 30$$

Thus, it determines the map ϕ.

To complete the proof, we need to work with multiplication now. Observe for any $a \in \mathbb{Z}_{12}$,

$$\phi(1 \bmod 12) = \phi(1 \cdot 1 \bmod 12) = \phi(1 \bmod 12)\phi(1 \bmod 12) = \phi(1 \bmod 12)$$

which implies that

$$(x \bmod 30)^2 = x \bmod 30$$

So we have 0 mod 30, 10 mod 30, 15 mod 30 and 25 mod 30.