MATH 427 10/17/2022

22.1

<u>Last time:</u> Defined rings and polynomial rings (with coefficients in a commutative ring). Defined <u>degree</u> of a polynomial.

<u>Definition</u> A subset S of a ring R is a <u>subring</u> iff

1) S is a subgroup of $(R, +, 0)$
2) $\forall a, b \in S$, $ab \in S$ (ie S is "closed under multiplication.")

<u>Ex</u>
- For a commutative ring R, R is a subring of $R[x]$ (as polynomials of degree ≤ 0
- we usually think of $\mathbb{Z}$ as subring of $\mathbb{Q}$, of $\mathbb{Q}$ as a subring of $\mathbb{R}$, of $\mathbb{R}$ as a subring of $\mathbb{C}$.

<u>Definition</u> Let R, R' be two rings. A map $f: R \to R'$ is a (ring) homomorphism iff f preserves $+$ and $\cdot$:

$$f(a+b) = f(a) + f(b) \quad \forall a, b \in R$$
$$f(ab) = f(a) f(b) \quad \forall a, b \in R$$

A ring homomorphism $f: R \to R'$ is <u>unital</u> if $f(1_R) = 1_{R'}$.

<u>Ex</u> $\pi: \mathbb{Z} \to \mathbb{Z}_n$, $\pi(k) = [k]$ is a unital homomorphism $\forall n$.

<u>Ex</u> $f: \mathbb{R} \to M_2(\mathbb{R})$, $f(a) = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ is a homomorphism

since $f(a) + f(b) = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a+b & 0 \\ 0 & 0 \end{pmatrix} = f(a+b)$

$f(a) \cdot f(b) = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} = f(ab)$

f is <u>not</u> unital since

$$1_{M_2(\mathbb{R})} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = f(1).$$

<u>Proposition 22.1</u> ("substitution principle")

Let $\varphi: R \to R'$ be a homomorphism between two comm. rings

For any $\alpha \in R'$, there is a unique homomorphism $\varphi_\alpha : R[x] \to R'$
so that (1) $\varphi_\alpha(r) = \varphi(r) \quad \forall r \in R \subseteq R[x]$ and
(2) $\varphi_\alpha(x) = \alpha$

[Aside: if R is not unital then $x := 1_R \cdot x \in R[x]$ does not make sense]

Proof (Uniqueness) Suppose $\psi : R[x] \to R'$ is another homomorphism so that (1) & (2) hold. Then $\forall\, p(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$

$$\psi(p) = \psi(a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n) = \psi(a_0) + \psi(a_1)\psi(x) + \psi(a_2)(\psi(x))^2 + \cdots$$
$$+ \psi(a_n)(\psi(x))^n = \varphi(a_0) + \varphi(a_1)\alpha + \varphi(a_2)\alpha^2 + \cdots + \varphi(a_n)\alpha^n$$
$$\cdots = \varphi_\alpha(a_0 + a_1 x + \cdots + a_n x^n) = \varphi_\alpha(p).$$

$\therefore \quad \psi = \varphi_\alpha$ and φ_α with these properties is unique.

(existence)

Define $\varphi_\alpha : R[x] \to R'$ by $\varphi_\alpha(a_0 + \cdots + a_n x^n) := \varphi(a_0) + \varphi(a_1)\alpha + \cdots + \varphi(a_n)\alpha^n$.

Then

$$\varphi_\alpha\left((\Sigma a_i x^i)(\Sigma b_j x^j)\right) = \varphi_\alpha\left(\sum_k \left(\sum_{i+j=k} a_i b_j\right) x^k\right) = \sum_k \varphi\left(\sum_{i+j=k} a_i b_j\right)\alpha^k$$

$$= \sum_k \left(\sum_{i+j=k} \varphi(a_i)\varphi(b_j)\alpha^i\alpha^j\right) = \left(\sum_i \varphi(a_i)\alpha^i\right)\left(\sum_j \varphi(b_j)\alpha^j\right)$$

$$= \varphi_\alpha(\Sigma a_i x^i) \cdot \varphi_\alpha(\Sigma b_j x^j) \Rightarrow \varphi_\alpha \text{ preserves } \cdot$$

Similarly φ_α preserves $+$. $\square$

Note: If φ is unital then so is φ_α since
$\varphi_\alpha(1_R) = \varphi(1_R) = 1_{R'}$.

Special case: $R' = R$, $\varphi = \mathrm{id}_R$. Then $\varphi_\alpha : R[x] \to R$ is given by
$\varphi_\alpha(\Sigma a_i x^i) = \Sigma a_i \alpha^i$

This map is called "evaluation at α". One usually writes
$p(\alpha)$ for $\varphi_\alpha(p) \quad \forall p \in R[x]$.

Occasionally we'll write ev_α for φ_α

Thus $ev_\alpha\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} a_i \alpha^i$.

Note: $ev_\alpha : R[x] \to R$ is a unital homomorphism.

Special case: Let $\varphi : R \to S$ be a ring homomorphism. The inclusion $i : S \hookrightarrow S[x]$ $i(a_0) = a_0$ is also a ring homomorphism.

Hence $i \circ \varphi : R \to S[y]$ is a ring homomorphism.

Exercise If $f : A \to B$, $g : B \to C$ are two ring homomorphisms Then so is $g \circ f : A \to C$.

Let $\alpha = y = 1_S \cdot y \in S[y]$. Then $\varphi_\alpha : R[x] \to S[y]$ is given by $\varphi_\alpha\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} \varphi(a_i) y^i \quad \forall \sum a_i x^i \in R[x]$.

Again, if φ is unital, so is this φ_α

Example $R = \mathbb{Z}$, $S = \mathbb{Z}_n$ $\varphi = \pi : \mathbb{Z} \to \mathbb{Z}_n$, $\pi(k) = [k]$

We then have a unital homomorphism

$$\psi : \mathbb{Z}[x] \to \mathbb{Z}_n[x], \quad \psi\left(\sum_{i=0}^{k} a_i x^i\right) = \sum_{i=0}^{k} [a_i] x^i$$

This homomorphism ψ is called "reduction of scalars modulo n."

The analogues of normal subgroups in ring theory are called ideals. Ideals are not (sub) rings.

Definition An ideal I in a ring R is a subgroup of $(R, +, 0)$ (i.e. $I \neq \emptyset$ and $\forall a, b \in I$, $a - b \in I$) and $\forall i \in I$, $\forall r \in R$ $ir \in I$ and $ri \in I$.

Example $\forall n$, $n\mathbb{Z} \subseteq \mathbb{Z}$ is an ideal.

We know $n\mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +, 0)$ Additionally $\forall a \in \mathbb{Z}$ $i \in n\mathbb{Z}$ $ai = ia \in n\mathbb{Z}$.

For any ring R, $0 := \{0\}$ and R are ideals in R

<u>Remark</u> if R is commutative, then $ir = ri$ $\forall r, i \in R$
So one condition in the def of ideal is redundant.

<u>Ex</u> R comm. ring. Then $\langle x \rangle = \{x\, p(x) \mid p(x) \in R[x]\}$
is an ideal in $R[x]$: $\langle x \rangle \neq \emptyset$ since $x \in \langle x \rangle$
$\forall p, q \in R[x]$, $x\,p(x) - x\,q(x) = x \cdot (p(x) - q(x)) \in \langle x \rangle$. $\Rightarrow \langle x \rangle$ is a subgroup
$\forall p, q \in R[x]$ $(x\,p(x)) \cdot q(x) \in \langle x \rangle$.
$\Rightarrow \langle x \rangle$ is an ideal.

<u>Definition</u> The <u>kernel</u> of a ring homomorphism $f: R \to S$ is
$\ker f := \{r \in R \mid f(r) = 0\}$.

<u>Lemma 22.3</u> The kernel of a ring homomorphism $f: R \to S$ is an ideal.

<u>Proof</u> Since $f: (R, +, 0) \to (S, +, 0)$ is a group homomorphism,
$\ker f \leq R$ is a subgroup.
Moreover, $\forall r \in R$, $\forall i \in \ker f$
$f(ri) = f(r) f(i) = f(r) \cdot 0 = 0$ $\Rightarrow ri \in \ker f$.
$f(ir) = f(i) f(r) = 0\, f(r) = 0$ $\Rightarrow ir \in \ker f$.

<u>Ex</u> $\left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in M_2(\mathbb{R}) \,\middle|\, a, b \in \mathbb{R} \right\}$ is a subring of $M_2(\mathbb{R})$.
It is <u>not</u> an ideal in $M_2(\mathbb{R})$.

In fact, in any ring if $I \subseteq R$ is an ideal and $1 \in I$
then $I = R$. [why?]