10/19/2022
We

23.1

Last time: • Proved the substitution principle: $\varphi: R \to S$ unital homomorphism of commutative rings, $\alpha \in S$. $\Rightarrow \exists!$ homomorphism $\varphi_\alpha: R[x] \to S$ s.t. $\varphi_\alpha(a_0 + a_1 x + \cdots + a_n x^n) = \varphi(a_0) + \varphi(a_1)\alpha + \cdots + \varphi(a_n)\alpha^n$.

• Defined ideals in a ring

• $\ker(f: R \to S) := \{ r \in R \mid f(r) = 0 \}$ is an ideal in R.

"Ex" $\pi: \mathbb{Z} \to \mathbb{Z}_n$, $\pi(k) = [k]$ is a ring homomorphism. $\Rightarrow$
$\ker \pi = n\mathbb{Z}$ is an ideal in $\mathbb{Z}$.

"Ex" $ev_\alpha: R[x] \to R$ $ev_\alpha(\sum a_i x^i) = \sum a_i \alpha^i$ is a homomorphism
$\Rightarrow \ker(ev_\alpha) = \{ p(x) \in R[x] \mid p(\alpha) := ev_\alpha(p) = 0 \}$
is an ideal.

Definition Let R be a commutative ring. $\alpha \in R$ is a root of $p(x) \in R[x]$ if $p(\alpha) = 0$ (ie iff $p \in \ker ev_\alpha$)

Ex $\sqrt{-1} \in \mathbb{C}$ is a root of $x^2 + 1 \in \mathbb{C}[x]$

Ex Let p be a prime. Then $\forall\, a \in \mathbb{Z}_p$ $a^p = a$
$\Rightarrow \forall\, a \in \mathbb{Z}_p$ is a root of $q(x) = x^p - x$ $(= [1]x^p + [-1]x)$

Note The function $f: \mathbb{Z}_p \to \mathbb{Z}_p$ $f(a) = a^p - a$ is the zero function, but $q_f(x) = x^p - x \in \mathbb{Z}_p[x]$ is a non zero polynomial.

We have seen:

Lemma 23.1 Let I be an ideal in a ring R.
$1_R \in I \iff I = R$.

Corollary 23.2 Let $I \subseteq R$ be an ideal. I contains a unit $\iff$

$\Leftrightarrow \quad I = R.$

Proof ($\Leftarrow$) if $I = R$, $\pm 1 \in I$, which are both units.

($\Rightarrow$) if u is a unit, $\exists\, v \in R$ s.t. $1 = uv$.

So if $u \in I$, $1 = uv \in I$ as well. $\Rightarrow I = R$. □

Corollary 23.3 The only ideals in a field F are 0 and F.

Proof Let $I \subseteq F$ be an ideal. If $I \neq 0$, $\exists\, u \in I$ s.t. $u \neq 0$.

Since F is a field, u is a unit. $\Rightarrow I = F$. □

Theorem 23.4 Let R be a ring, $I \subseteq R$ an ideal. The quotient group $(R/I, +, 0+I)$ has a well-defined multiplication $\cdot$ which is given by

$$(a+I)\cdot(b+I) = (ab)+I \qquad \forall\, a+I, b+I \in R/I.$$

With this multiplication $(R/I, +, 0+I, 1+I)$ is a ring and $\pi: R \to R/I$, $\pi(a) = a+I$ is a surjective ring homomorphism.

Sketch of proof • We check that $\cdot$ is well-defined.

Suppose $a+I = a'+I$, $b+I = b'+I$ for some $a, a', b, b' \in R$. Then $a = a' + i_1$, $b = b' + i_2$ for some $i_1, i_2 \in I$. And then

$$ab = (a'+i_1)(b'+i_2) = a'b' + i_1 b' + a' i_2 + i_1 i_2$$

Since I is an ideal, $i_1, i_2 \in I$, $i_1 b', a' i_2, i_1 i_2 \in I \Rightarrow i_1 b' + a' i_2 + i_1 i_2 \in I$.

$\Rightarrow \quad ab - a'b' \in I$

$\Rightarrow \quad ab + I = a'b' + I$

$\Rightarrow \cdot$ is well-defined

• It's easy to check that $\cdot$ distributes over $+$:

$$((a+I)+(b+I))\cdot(c+I) = ((a+b)+I)(c+I) = (a+b)c + I$$
$$= (ac+bc)+I = (ac+I)+(bc+I) = (a+I)(c+I)+(b+I)(c+I)$$

Similarly

$$(c+I)\cdot((a+I)+(b+I)) = (c+I)\cdot(a+I)+(c+I)\cdot(b+I)$$

and so on... □

Exercise For any unital homomorphism $\varphi: R \to S$ the image $\varphi(R) := \{\varphi(r) \mid r \in R\}$ is a subring of S.

Theorem (1^{st} isomorphism theorem for rings) Let $\varphi: R \to S$ be a (unital) ring homomorphism, and $I = \ker\varphi$. Then

$$\overline{\varphi}: R/I \to S, \quad \overline{\varphi}(a+I) = \varphi(a)$$

is a well defined injective ring homomorphism. In particular

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ \downarrow & & \uparrow \\ R/I & \xrightarrow[\overline{\varphi}]{} & \varphi(R) \end{array}$$

commutes and $\overline{\varphi}: R/I \to \varphi(R)$ is an iso.

Proof We know that $\overline{\varphi}: R/I \to \varphi(R)$, $\overline{\varphi}(a+I) = \varphi(a)$, is a well-defined isomorphism of abelian groups making the diagram above commute. Remains to check that $\overline{\varphi}$ preserves multiplication. This is easy:

$$\overline{\varphi}((a+I)(b+I)) = \overline{\varphi}(ab+I) = \varphi(ab) = \varphi(a)\varphi(b) = \overline{\varphi}(a+I)\,\overline{\varphi}(b+I). \quad \square$$

& Let $R = \left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a,b,c \in \mathbb{R}\right\}$, R is a subring of $M_2(\mathbb{R})$:

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\cdot\begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} = \begin{pmatrix} aa' & ab'+bc' \\ 0 & cc' \end{pmatrix}.$$

So is closed under matrix multiplication. Also $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} - \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} = \begin{pmatrix} a-a' & b-b' \\ 0 & c-c' \end{pmatrix}$

$\therefore$ R is a (unital) subring of $M_2(\mathbb{R})$.

Consider $\varphi: R \to \mathbb{R}$, $\varphi\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\right) = a$. It's easy to see that φ preserves $+$ and $\cdot$, hence is a homomorphism.

$$\ker\varphi = \left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a = 0\right\} = \left\{\begin{pmatrix} 0 & b \\ 0 & c \end{pmatrix} \mid b,c \in \mathbb{R}\right\}.$$

$\varphi: R \to \mathbb{R}$ is clearly onto. Hence

$$\overline{\varphi}: R/\ker\varphi \to \mathbb{R}, \quad \overline{\varphi}\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} + \ker\varphi\right) = a$$

is a well-defined isomorphism of rings.

Lemma 23.5 Let R be a commutative ring. For any $a \in R$ the set

$$aR = \{ar \mid r \in R\}$$

is an ideal in R.

Proof Since $0 = a \cdot 0$, $0 \in \langle a \rangle$. In particular $\langle a \rangle \neq \emptyset$.

$\forall\, x_1, x_2 \in \langle a \rangle$ $\exists\, r_1, r_2 \in R$ s.t. $x_1 = ar_1$, $x_2 = ar_2$.

And then $x_1 - x_2 = ar_1 - ar_2 = a(r_1 - r_2) \in \langle a \rangle$.

Finally $\forall\, q \in R$, $ar \in \langle a \rangle$ $\quad qar = qra \in \langle a \rangle$

and $(ar)q = a(rq) \in \langle a \rangle$.

$\therefore$ $\langle a \rangle$ is an ideal in R. D

Remark R is not commutative, aR need not be an ideal.

Ex $R = M_2(\mathbb{R})$, $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} b_{21} & b_{22} \\ 0 & 0 \end{pmatrix} \Rightarrow aR = \left\{\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} \mid x, y \in \mathbb{R}\right\}.$$

But

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} a = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \notin aR.$$

Remark If I is an ideal in $\mathbb{Z}$, then I is a subgroup of $\mathbb{Z}$.

$\Rightarrow \exists\, n \in \mathbb{Z}$ s.t. $I = n\mathbb{Z}$ and $n\mathbb{Z}$ is an ideal in $\mathbb{Z}$.

$\therefore$ all ideals in $\mathbb{Z}$ are of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$.

Recall To prove that any subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some n we used the division algorithm.

We'll prove: Let F be a field, $f, g \in F[x]$, $g \neq 0$. Then there exist unique $q, r \in F[x]$ s.t. $f = qg + r$ and $\deg r < \deg g$

From this fact one can deduce: if $I \subset F[x]$ is an ideal then

$$I = aF[x] \quad \text{for some } a \in F[x]$$