(16)
2/6/2019>

§11.3, 11.4 Ideals and quotient rings

Recall for a group homomorphism $G \xrightarrow{\varphi} G'$

one has (i) $K := \ker\varphi$ a normal subgroup ($gKg^{-1} \subset K$ $\forall g \in G$), $\operatorname{im}\varphi$ a subgroup

and in fact (ii) {normal subgroups $K \trianglelefteq G$} = {kernels of homoms $G \to G'$}

since $K = \ker(G \xrightarrow{\pi} G/K)$ (quotient group), $g \mapsto gK$

and (iii) Noether's 1st Isomorphism theorem:

One has an isomorphism $G/K \xrightarrow{\sim} \operatorname{im}\varphi$ ($K = \ker\varphi$), $gK \mapsto \varphi(g)$

There's a parallel story for rings....

PROPOSITION: For any ring homom. $R \xrightarrow{\varphi} R'$,

- $\operatorname{im}\varphi$ is a subring of R'
- $\ker\varphi$ is an ideal of R

DEFN: $I \subset R$ a ring is an ideal if $I^+ < R^+$ is an additive subgroup and every $x \in I$, $r \in R$ have $rx \in I$

proof: If $a', b' \in \operatorname{im}\varphi$, say $\varphi(a)=a'$, $\varphi(b)=b'$ then $a'+b' = \varphi(a)+\varphi(b) = \varphi(a+b) \in \operatorname{im}\varphi$

$a'b' = \varphi(a)\varphi(b) = \varphi(ab) \in \operatorname{im}\varphi$

$1 = \varphi(1) \in \operatorname{im}\varphi$

If $x \in \ker\varphi$ and $r \in R$ then $\varphi(rx) = \varphi(r)\varphi(x) = \varphi(r)\cdot 0 = 0 \Rightarrow rx \in \ker\varphi$

$y \in \ker\varphi$ $\varphi(x+y) = \varphi(x)+\varphi(y) = 0+0 = 0$ ∎

EXAMPLES:

(1) $n\mathbb{Z} \overset{\text{ideal}}{\subset} \mathbb{Z}$, and every ideal $I \subset \mathbb{Z}$ is of the form $I = n\mathbb{Z}$ for some $n \in \mathbb{Z}$, since $I^+ < \mathbb{Z}^+$ is an additive subgroup

$= \ker(\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z})$, $a \mapsto \bar{a}$ mod n

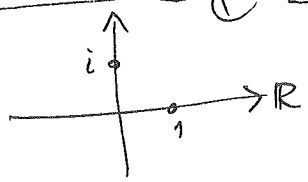
(2) We've seen that the substitution homom. $R[x] \xrightarrow[x \mapsto \alpha]{\varphi} R$ has $\ker\varphi = (x-\alpha) := \{\text{all multiples } (x-\alpha)f(x) : f(x) \in R[x]\}$

(3) The substitution homom. "$x = i$"

$\mathbb{R}[x] \xrightarrow{\varphi} \mathbb{C}$

extending $\mathbb{R} \xrightarrow[\text{inclusion}]{} \mathbb{C}$

and $x \longmapsto i$



we claim has $\ker(\varphi) = (x^2+1) := \{\text{all multiples } (x^2+1)f(x) : f(x) \in \mathbb{R}[x]\}$

DEF'N: In a ring R, the principal ideal $I = (r_0)$ generated by $r_0 \in R$ is

$:= \{rr_0 : r \in R\} = \{\text{all multiples of } r_0 \text{ in } R\}$

More generally, given $\{r_1, r_2, \dots\} \subset R$

the ideal $I = (r_1, r_2, \dots)$ generated by $\{r_1, r_2, \dots\}$ in R

$:= \{\underbrace{s_1r_1 + s_2r_2 + \dots + s_kr_k}_{\text{finite sums}} : s_i \in R\}$

To see the claim, note $x^2+1 \in \ker(\varphi)$ since $i^2+1 = -1+1 = 0$ in $\mathbb{C}$

so $(x^2+1) \subseteq \ker(\varphi)$

Conversely, given $f(x) \in \ker(\varphi)$, write $f(x) = (x^2+1)g(x) + \underbrace{r(x)}_{ax+b}$

$x^2+1 \overline{)\, f(x)}$ quotient $g(x)$, remainder $ax+b$

and substitute $x = i$: $0 = \varphi(f) = f(i) = \underbrace{(i^2+1)}_{0}g(i) + ai + b$

$0 = ai + b$ i.e. $r = 0$, so $f(x) = (x^2+1)g(x) \in (x^2+1)$

Thus $\ker(\varphi) = (x^2+1)$

Later we'll see every ideal $I \subset \mathbb{F}[x]$ for a field $\mathbb{F}$ has $I = (f(x))$ principal.

④ Let's analyze $\ker\varphi$ for $\mathbb{Z}[x] \xrightarrow{\varphi} \mathbb{F}_5$

$x \longmapsto \bar{2}$

(and $\mathbb{Z} \xrightarrow[a \longmapsto \bar{a}]{} \mathbb{F}_5$)

Certainly $\ker\varphi$ contains $x-2$ and 5,

so $I := (5, x-2)$ $\left(= \{ 5f_1(x) + (x-2)f_2(x) : f_1, f_2 \in \mathbb{Z}[x] \}\right)$

$\subseteq \ker\varphi$

We claim that's all of $\ker\varphi$:

$$x-2 \,\big)\, f(x) \quad \text{quotient } q(x), \text{ remainder } r$$

Given $f(x) \in \ker\varphi$, write $f(x) = (x-2)\underbrace{q(x)}_{\in\mathbb{Z}[x]} + \underbrace{r}_{\in\mathbb{Z}}$

and apply φ: $\bar{0} = \varphi(f) = (\bar{2}-\bar{2})q(\bar{2}) + \bar{r}$ in $\mathbb{F}_5$

$= \bar{r}$

$\Rightarrow r \in 5\mathbb{Z}$, i.e. $r = 5m$ for some $m \in \mathbb{Z}$

$\Rightarrow f(x) = (x-2)q(x) + 5m \in (5, x-2)$

Thus $\ker(\varphi) = (5, x-2) = I$

EXERCISE: Convince yourself $I = (5, x-2) \neq (f(x))$ i.e. it's not a principal ideal in $\mathbb{Z}[x]$

DEFN-PROP (THM. 11.4.1): Given any ideal $I \subset R$ a ring, the (additive) cosets

$$R/I = \{ r + I : r \in R \} \quad \left(= R^+/I^+ \text{ as groups}\right)$$

form a ring, using the multiplication

$$(a+I)(b+I) := ab + I.$$

The canonical surjection homomorphism $R \xrightarrow[r \longmapsto r+I]{\pi} R/I$

becomes a ring homomorphism, with $\ker\pi = I$

Hence $\{\text{ideals } I \text{ of } R\} = \{\text{kernels of homoms. } R \to R'\}$.

(19)

proof: Same as for why $\overset{R}{\mathbb{Z}}/\overset{I}{n\mathbb{Z}}$ was a ring;

check $\times$ is well-defined, i.e. if $a+I=a'+I$ i.e. $a'=a+i_1$
$b+I=b'+I$ $b'=b+i_2$ with $i_1,i_2\in I$

then $(a'+I)(b'+I) \overset{?}{=} (a+I)(b+I)$

$\|$ $\|$

$a'b'+I$ $ab+I$

$= (a+i_1)(b+i_2)+I$

$= ab + \underbrace{ai_2}_{\in I} + \underbrace{bi_1}_{\in I} + \underbrace{i_1 i_2}_{\in I} + I$

$\in I$

$= ab+I$ ✓

The rest is all easy. ∎

EXAMPLES: (1) Since every ideal $I \subset \mathbb{Z}$ is $I = \overset{=(n)}{n\mathbb{Z}}$ (principal) for some n (maybe $n=0$)

every quotient ring of $\mathbb{Z}$ is either $\mathbb{Z}/n\mathbb{Z}$

or $\mathbb{Z}/\{0\} = \mathbb{Z}$ itself.

(2) Something similar happens for $\mathbb{F}[x]$, $\mathbb{F}$ a field...

PROP (11.3.22 / 11.5.5) (a) Every nonzero ideal $I \subset \mathbb{F}[x]$ for a field $\mathbb{F}$

is principal, $I = (f(x))$

generated by any nonzero monic polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$

of lowest degree in I.

(b) In this case, the quotient ring $\mathbb{F}[x]/(f(x)) = \mathbb{F}[x]/I$

is isomorphic as an $\mathbb{F}$-vector space to $\mathbb{F}^n$,

with $\mathbb{F}$-basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ where $\alpha = x+I = \bar{x}$ in $\mathbb{F}[x]/I$