Lecture 29

Tuesday, March 17, 2015 10:00 AM

Group rings

R a commutative ring w/ 1

G a finite group

The group ring $RG = \left\{ \sum_{g \in G} a_g g \mid a_g \in R \right\}$

$$\left(\sum a_g g\right) + \left(\sum b_g g\right) = \sum (a_g + b_g) g$$

$$(ag)\cdot(bh) = \underbrace{(a\cdot b)}_{\in R}\underbrace{(gh)}_{\in G} \in RG$$

$h, g \in G$, $b, a \in R$

We can extend this product so that distribution works.

Ring homomorphisms

R, S rings

Defn A ring homomorphism $\varphi : R \to S$ is a fn satisfying

(i) $\varphi(a+b) = \varphi(a) + \varphi(b)$

(ii) $\varphi(ab) = \varphi(a)\varphi(b)$

$\forall a, b \in R$

[so φ is a gp hom $(R,+) \to (S,+)$]

The <u>kernel</u> of a ring hom $\varphi: R \to S$ is

$$\ker(\varphi) = \{ r \in R \mid \varphi(r) = 0 \}$$

A bijective ring hom is called a (ring) <u>isomorphism</u>.

<u>e.g.</u> $\text{red}: \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$, $\ker(\text{red}) = n\mathbb{Z}$

$\qquad a \longmapsto \bar{a} = a + n\mathbb{Z}$

$\psi: \mathbb{Q}[x] \longrightarrow \mathbb{Q}$, $\ker(\psi) = \{ p \in \mathbb{Q}[x] \mid$ const term of p is $0 \}$

$\qquad p \longmapsto p(0)$

$= x \cdot \mathbb{Q}[x]$

$= \{ x\, p(x) \mid p(x) \in \mathbb{Q}[x] \}$

<u>Prop</u> For any ring hom $\varphi: R \to S$,

1. $\operatorname{im}(\varphi)$ is a subring of S
2. $\ker(\varphi)$ is a subring of R; moreover,

$\forall r \in R$, $\alpha \in \ker(\varphi)$, $r\alpha$, $\alpha r \in \ker(\varphi)$.

I.e. $R \cdot (\ker \varphi)$, $(\ker \varphi) \cdot R \subseteq \ker \varphi$.

Pf ① Take $r_1, r_2 \in R$. $\varphi(r_1 - r_2) = \varphi(r_1) - \varphi(r_2)$
so differences of elts of $\mathrm{im}(\varphi)$ are still in $\mathrm{im}(\varphi)$.
Also, $\varphi(r_1)\varphi(r_2) = \varphi(r_1 r_2) \in \mathrm{im}(\varphi)$ so $\mathrm{im}(\varphi)$ is closed under mult.

② For $\alpha, \beta \in \ker(\varphi)$, $\varphi(\alpha - \beta) = \varphi(\alpha) - \varphi(\beta) = 0 - 0 = 0$
$\Rightarrow \alpha - \beta \in \ker(\varphi)$.
For $r \in R$, $\varphi(r\alpha) = \varphi(r)\varphi(\alpha) = \varphi(r) \cdot 0 = 0$
$\Rightarrow r\alpha \in \ker\varphi$. Sim, $\varphi(\alpha r) = 0 \cdot \varphi(r) = 0$
so $\alpha r \in \ker \varphi$. $\square$

Given $\varphi : R \to S$ w/ $\ker(\varphi) = I$, we have

$$R/I \cong \mathrm{im}(\varphi) \quad \text{as additive abelian gps.}$$

$$r + I \mapsto \varphi(r)$$

Thus it makes sense to define $(r+I)(s+I) = (rs) + I$ for $r, s \in R$. (Because $\varphi(rs) = \varphi(r)\varphi(s)$.)
Thus R/I has a natural ring structure $\cong \mathrm{im}(\varphi)$.

Moral: We can do "ring quotients" as long as I is the kernel of a ring hom.

Q: What typifies such subrings $I \subseteq R$?

A: They're ideals.

$$\boxed{\text{groups} : \text{normal subgps} :: \text{rings} : \text{ideals}}$$

Defn: R a ring, $I \subseteq R$, $r \in R$.

1. $rI = \{ra \mid a \in I\}$, $Ir = \{ar \mid a \in I\}$
2. $I \subseteq R$ is a left ideal of R if
   - (i) I is a subring of R, and
   - (ii) $rI \subseteq I \quad \forall r \in R$

   $I \subseteq R$ is a right ideal of R if (i) holds and
   - (ii′) $Ir \subseteq I \quad \forall r \in R$
3. $I \subseteq R$ is a (two-sided) ideal if it is both a left & right ideal of R.

The conditions for being an ideal are more than just being a subring.

being a substring!"

<u>Prop</u> R a ring, $I \subseteq R$ an ideal. Then the additive group R/I is a ring under the ops

$$(r+I)+(s+I) = (r+s)+I$$

$$(r+I)\cdot(s+I) = (rs)+I$$

for $r,s \in R$. In this case, I is the kernel of the ring hom
$$\begin{aligned} R &\longrightarrow R/I \\ r &\longmapsto r+I. \end{aligned}$$

<u>Pf</u> The additive parts of the prop are clear b/c $I \trianglelefteq (R,+)$. Mult is well-defined b/c for $\alpha,\beta \in I$, $r,s \in R$

$$(r+\alpha+I)\cdot(s+\beta+I)$$
$$= ((r+\alpha)(s+\beta))+I$$
$$= (rs + \underbrace{\underbrace{r\beta}_{\in I} + \underbrace{\alpha s}_{\in I} + \underbrace{\alpha\beta}_{\in I}}_{\in I}) + I$$
$$= rs+I.$$

Associativity & distributivity: check. $\square$

First Isomorphism Thm If $\varphi : R \to S$ is a ring hom w/ $\ker(\varphi) = I$, then $R/I \cong \operatorname{im}(\varphi)$

$$r + I \longmapsto \varphi(r).$$ $\square$

Examples

- $\underbrace{0 = \{0\}}_{\text{trivial ideal}}$, $R \subseteq R$ are ideals of R.

- $n\mathbb{Z} \subseteq \mathbb{Z}$ is an ideal

Comment If R is a commutative ring, then left ideals = right ideals = ideals.

- $x^2 \cdot \mathbb{Z}[x] = \{ x^2 \cdot f(x) \mid f(x) \in \mathbb{Z}[x] \}$

$= \{ \deg \geq 2 \text{ elts of } \mathbb{Z}[x] \} \cup \{0\}$

$\subseteq \mathbb{Z}[x]$.

$\bar{r} = r + I \in R/I$

$\deg(f+g) \geq \deg(f), \deg(g)$ for $f \neq -g$

$\deg(f \cdot g) = \deg(f) + \deg(g)$

$\mathbb{Z}[x] / x^2 \cdot \mathbb{Z}[x]$: $(\overline{1+x}) \cdot (\overline{2-3x}) = \overline{(2 - x - 3x^2)}$

$= \overline{2-x}$.

G finite gp, R comm ring w/ 1.

$$\varepsilon : RG \longrightarrow R \qquad \sum_{g\in G} a_g g \longmapsto \sum_{g \in G} a_g$$

is called the augmentation hom.

This has kernel $\ker(\varepsilon)$, the augmentation ideal of RG.

By 1st iso thm: $RG / \ker(\varepsilon) \cong R$.

Why bother?

Q Are there integer sol'ns to $x^2 + y^2 \overset{(*)}{=} 3z^2$?

Tactic Reduce mod $4\mathbb{Z}$.

Since $\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z}$ is a ring hom, the rel'n $(*)$ is preserved in $\mathbb{Z}/4\mathbb{Z}$: $\bar{x}^2 + \bar{y}^2 \overset{(**)}{=} 3\bar{z}^2 \in \mathbb{Z}/4\mathbb{Z}$

$\bar{0}^2 = \bar{0}$, $\bar{1}^2 = \bar{1}$, $\bar{2}^2 = \bar{0}$, $\bar{3}^2 = \bar{1}$

Thus sol'ns to $(**)$ look like

$$(\bar{0} \text{ or } \bar{1}) + (\bar{0} \text{ or } \bar{1}) = 3 \cdot (\bar{0} \text{ or } \bar{1})$$
$$= (\bar{0} \text{ or } \bar{3})$$

The only sol'n is all $\bar{0}$'s $\Rightarrow \bar{x} = \bar{y} = \bar{z} = \bar{0} \in \mathbb{Z}/4\mathbb{Z}$.

Tuesday, March 17, 2015 10:52 AM

Thus $x = y = z = 0$ (b/c x, y, z are all infinitely divisible by 4).

<u>Read</u> 2^{nd}, 3^{rd}, 4^{th} iso thms. $\square$