~~Alg~~ Algebra I Lecture 14: Ring homomorphisms / quotients.

Def: R, S rings.
A ring hom is a fn $\varphi: R \to S$ s.t.
$$\varphi(a+b) = \varphi(a) + \varphi(b)$$
$$\varphi(ab) = \cancel{\varphi(b)}\, \varphi(a)\cdot\varphi(b).$$

(respects both + and ·).

$\ker(\varphi) = \{r \in R \mid \varphi(r) = 0\}$
(i.e., $\ker(\varphi) = \ker(\varphi)$ as a hom of additive gps).

A ring isomorphism is a bijective ring hom. (respects set structure too...)

Lemma: $\varphi: R \to S$ hom.
1). $\mathrm{im}(\varphi)$ is a subring of S
2). $\ker(\varphi)$ is a subring of R
~~(show closed under~~ $-, \cdot$).

Pf: 1). If $s_1, s_2 \in \mathrm{im}(\varphi)$, say $s_i = \varphi(r_i)$.

Then $\varphi(r_1 - r_2) = s_1 - s_2 \in \mathrm{im}(\varphi)$
$\varphi(r_1 \cdot r_2) = s_1 \cdot s_2 \in \mathrm{im}(\varphi)$ $\Rightarrow$ $\mathrm{im}(\varphi)$ closed under $-, \cdot$ ✓

2). If $\varphi(r_1) = \varphi(r_2) = 0$, then
~~$\varphi(r_1) + \varphi(r_2) =$~~
$\varphi(r_1 - r_2) = 0 - 0 = 0$
$\varphi(r_1 \cdot r_2) = 0 \cdot 0 = 0$ $\Rightarrow$ $\ker(\varphi)$ closed under $-, \cdot$ ✓

Extra structure:
Moreover, If $\alpha \in \ker(\varphi)$, and $r \in R$, then $\alpha r, r\alpha \in \ker(\varphi)$ too!
(1)

(as $\varphi(r\cdot\alpha) = r\cdot 0 = 0$
$\varphi(\alpha\cdot r) = 0\cdot r = 0$).

Subrings with this added structure are called ideals.

Defn: A left ~~l~~ ideal of R is a subring $I \leq R$ which is closed under left mult by elts of R:
$$rI \subseteq I \quad \forall r \in I.$$

An (two-sided ideal) is a subring closed under ~~the~~ mult by elts of R on the ~~l~~ left and right.

Quotient ring:

If I is an ideal of R, define equivalence ~~classes~~ rel^n
$$a \sim b \Leftrightarrow a - b \in I.$$

Classes: $r + I$.

~~Then~~ The set of classes is R/I.

Prop: R/I is a ring under
$$\cancel{a+b)}\ (a+I)+(b+I) = (a+b)+I$$
$$(a+I)\cdot(b+I) = (a\cdot b)\cdot I$$

Pf: Main pt. (as with ~~gps~~ quotient gps, ~~is~~ well-definedness).

If $x_1 + I = x_2 + I$,
$y_1 + I = y_2 + I$

Then $x_1 - x_2 \in I$ (these are cosets in $(R,+)$.)
$y_1 - y_2 \in I$.

$\Rightarrow$ $(x_1 - x_2)y_1 \in I$

(I is an ideal) $x_2(y_1 - y_2) \in I$

$\Rightarrow (x_1 - x_2)y_1 + x_2(y_1 - y_2) \in I$

$(I,+)$ is a gp) $\Rightarrow x_1 y_1 - x_2 y_2 \in I$

$\Rightarrow (x_1 y_1) + I = (x_2 y_2) + I$

Addition :

Under the same hypotheses, ($x_1 + I = x_2 + I$
$y_1 + I = y_2 + I$)

want $(x_1 + y_1) + I = (x_2 + y_2) + I$.

well-defined if $(I,+) \trianglelefteq (R,+)$
as we saw before.
This is true as $(R,+)$ is abelian for any ring.

Ring properties of R/I:

As $(I,+) \trianglelefteq (R,+)$,
$(R/I,+)$ is a gp. by gp. theory

Closure under $\cdot$ is clear.

Associativity of $\cdot$:

$(x+I)((y+I)(z+I))$
$= (x+I)(yz+I) = xyz + I$
$= (xy+I)(z+I) = ((x+I)(y+I))(z+I)$

Distributive prop: e.g.:
$((x+I)+(y+I))(z+I) = (x+y+I)(z+I)$
$= (xz+yz)+I = \bar{x}\bar{z} + \bar{y}\bar{z}$

As expected, the rest follow "for free" from ring props of R.

Converse: R/I ring $\Rightarrow I$ an ideal: Exercise

Natural map:

$$\pi : R \twoheadrightarrow R/I.$$
$$r \longmapsto r+I.$$

clearly surjective.

ring hom: $r \cdot s \mapsto rs+I = (r+I)(s+I)$

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

by ~~above~~ def of $+, \cdot$ in R/I.

$\ker(\pi) = \{r \in R \mid r+I = I\}$

$= I.$ } Pause.

Thus, (as expected), I is an ideal $\Leftrightarrow$ it is the kernel of a ring hom.

1st Iso. Thm:

If $\varphi : R \to S$ ring hom, then
$R/\ker(\varphi) \cong \mathrm{im}(\varphi)$.

Pf: Map: $\Psi : R/\ker(\varphi) \longrightarrow \mathrm{im}(\varphi)$
$r+\ker(\varphi) \longmapsto \varphi(r)$.

well-defined: If $r+\ker(\varphi) = r'+\ker(\varphi)$,

then $r-r' \in \ker(\varphi)$

$\Rightarrow \varphi(r-r') = 0$

$\Rightarrow \varphi(r) = \varphi(r')$ ✓.

Let $I = \ker(\varphi)$.

hom: $\Psi(r_1+I+r_2+I) = \Psi(r_1+r_2+I) = \varphi(r_1+r_2) = \varphi(r_1)+\varphi(r_2)$ $\underset{\varphi\ \text{hom}}{=} \Psi(r_1+I) + \Psi(r_2+I)$

$\Psi(r_1I \cdot r_2I) = \Psi(r_1r_2I) = \varphi(r_1r_2)$
$= \varphi(r_1)\cdot\varphi(r_2) = \Psi(r_1I)\cdot\Psi(r_2I)$.

~~Pf~~ Isomorphism:

surjective is clear:

$\varphi(r) \leftarrow\!\shortmid\; r + I.$

injective: $\psi(r+I) = 0 \Leftrightarrow \varphi(r) = 0 \Leftrightarrow r \in I$

$\Leftrightarrow r + I = I = 0$ in R/I ∎

(Could also save a few steps using 1st Iso thm for gps. -- but easy enough).

Examples:

- ~~$R, \{0\}$~~ $R, \{0\}$ are always ideals.

  ↑ trivial ideal

A proper ideal is one which $\neq R$.

- Ideals of $\mathbb{Z}$: $\{n\mathbb{Z} \mid n \geq 0\}$. (Pause).

  $\pi : \mathbb{Z} \twoheadrightarrow$ ~~$n\mathbb{Z}$~~ $\mathbb{Z}/n\mathbb{Z}$ natural projection. (reduction mod n)

- If I is an ideal containing a unit u, then $uv = 1$ some v.

  $\Rightarrow uv = 1 \in$ ~~R~~ I

  $\Rightarrow r \cdot 1 = r \in I \;\; \forall r \in I$.

In particular, in a field, F, the only ideals are $\{0\}$, F.

This means that every ~~ring hom~~ nontrivial ring hom $\varphi : F \to S$ is injective

(ker = nothing or all)

- $\mathbb{R} \hookrightarrow \mathbb{R}[x] \xrightarrow{\text{eval}_a} \mathbb{R}$
  $f \longmapsto f(a)$ is surjective
  with kernel
  $I_a = \{ f \in \mathbb{R}[x] \mid f(a) = 0 \}$

Thus, $\mathbb{R}[x]/I \cong \mathbb{R}$.

~~Ex: R comm. ring w/ $1 \neq 0$.~~

~~$G = \{g_1, \dots, g_n\}$ finite gp. under.~~

~~Group ring: $RG = \{a_1 g_1 + \dots + a_n g_n \mid a_1, \dots, a_n \in R\}$.~~
~~(of G with coeffs. in R). formal sums.~~

~~Addition: $(a_1 g_1 + \dots + a_n g_n) + (b_1 g_1 + \dots + b_n g_n)$~~
~~$= (a_1 + b_1) g_1 + \dots + (a_n + b_n) g_n$~~

~~Multiplication; use: $(a g_i)(b g_j) = (ab)(g_i g_j)$~~
~~extend linearly.~~

Cut

~~$RG \xrightarrow{\pi} R$~~
~~$\sum a_i g_i \longmapsto \sum a_i$ augmentation hom.~~
~~ker = augmentation ideal $= \{ \sum a_i g_i \mid \sum a_i = 0 \}$.~~
~~$RG / \ker(\pi) \cong R$.~~

Ex of one-sided ideal: in non-comm. ring. $M_n(R)$.
(R comm. ring w/ $1 \neq 0$). $n \geq 2$.

$L = \{ A = (a_{ij}) \in M_n(R) \mid a_{ij} = 0 \text{ if } j \neq 1 \}$.

If $B \in M_n(R)$, $A \in L$, then $BA \in L$.
However, may not have $AB \in L$.

ex: $n=2$: $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} * & 0 \\ * & 0 \end{pmatrix} = \begin{pmatrix} * & 0 \\ * & 0 \end{pmatrix}$

$\begin{pmatrix} * & 0 \\ * & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} * & * \\ * & * \end{pmatrix}$

So L is a Left ideal not a right ideal.

To Here.

Ex: $x^2+y^2=3z^2$ has no non-zero integer sol^{ns}.

Pf: Look at over $\mathbb{Z}/4\mathbb{Z}$. (natural reduction map).
Look at primitive sol^{ns} (no common factor)

$\square$'s are 0,1 mod 4.

$0,1 + 0,1 \equiv 0,3 \Rightarrow 0,0,0$
all 0 mod 4
Contradicts primitive!
(infinite descent!) $\square$

2nd Isom thm (rings): $A \subseteq B$ subring, B ideal.
Then $A+B$ is a subring, $A \cap B$ is an ideal, and
$(A+B)/B \cong A/(A\cap B)$.

3rd isom thm: I, J ideals with $I \subseteq J$.
Then J/I is an ideal of R/I, and
$(R/I)/(J/I) \cong R/J$.

write on board ahead of time

4th isom thm: I ideal of R. There are 1-1 correspondences
{subrings of R/I} $\longleftrightarrow$ {subrings of R containing I},
{ideals of R/I} $\longleftrightarrow$ {ideals of R containing I}

given by $A \longrightarrow \bar{A} = A/I$

$\pi^{-1}(\bar{A}) \longleftarrow \bar{A}$

to prove these, use the Isom. thm for gps. and then check multiplication (E-Z.).

to here

Defn: I, J ideals of R.

1). $I + J = \{a+b \mid a \in I, b \in J\}$ = smallest ideal containing both I and J.

2). $IJ = \{\sum_{i=1}^{k} a_i b_i \mid a_i \in I, b_i \in J\}$ = smallest ideal containing $\{ab \mid a \in I, b \in J\}$.

3) $I^n = \{$ all finite sums of elts of the form $a_1 \cdots a_n$, with $a_i \in I$ $\forall i \}$.

"ideal generated by": ...