2/25/14

Exam 1 Thursday
Today Review
Next Week : NO CLASS
(But I will assign HW 3).

Review for Exam 1

~~(1) Properties of general rings~~
(2) Properties of $\mathbb{Z}$ & $K[x]$

(1) Definitions of

ring / homomorphism / subring / ideal.

We say $(R, +, \times, 0, 1)$ is a ring if

- $(R, +, 0)$ is abelian group
- $(R, \times, 1)$ is commutative semigroup
- For all $a, b, c \in R$ we have

$$a(b+c) = ab + ac$$

- $0 \neq 1$.

Given rings R, S we say $\varphi : R \to S$
is a ring homomorphism if

- $\varphi(a+b) = \varphi(a) + \varphi(b)$
- $\varphi(ab) = \varphi(a)\varphi(b)$
- $\varphi(1_R) = 1_S$.

If $\varphi : R \to S$ is a ring hom then

$$\operatorname{im}\varphi := \{\varphi(r) : r \in R\} \subseteq S$$

is a <u>subring</u> and

$$\ker\varphi := \{r \in R : \varphi(r) = 0_S\} \subseteq R$$

is <u>not</u> a subring. What is it?

<u>Def</u>: We say $I \subseteq R$ is an <u>ideal</u> if

- I is a subgroup of $(R, +, 0)$
- For all $a \in I$, $b \in R$ we have

$$ab \in I.$$

☆ <u>Theorem</u>: Given <u>subset</u> $I \subseteq R$ we have

I is an ideal $\iff$ $\exists$ ring R' and hom $\varphi : R \to R'$ with $I = \ker\varphi$.

Proof $\Leftarrow$ Easy

$\Rightarrow$ We must construct the ring R' and the map φ. Given an ideal $I \leq R$ we define a relation on R by.

$$a \sim b \iff a - b \in I.$$

Prove that this is an equivalence

(• $a \sim a$
• $a \sim b \Rightarrow b \sim a$
• $a \sim b$ & $b \sim c \Rightarrow a \sim c$)

with equivalence classes given by cosets

$$\begin{aligned} [a] &= \{ b \in R : a \sim b \} \\ &= \{ b \in R : a - b \in I \} \\ &= \{ b \in R : a - b = x \in I \\ &= \{ a + x : x \in I \} \\ &= a + I. \end{aligned}$$

Prove that we have

$$a + I = b + I \iff a \sim b.$$

Consider the set of cosets

$$R/I := \{ a+I \; ; \; a \in R \}.$$

Define addition and multiplication by

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

Show that these are well-defined and make R/I into a ring. Show that the map

$$\varphi : R \longrightarrow R/I$$
$$a \longmapsto a+I.$$

is a ring homomorphism with $\ker\varphi = I$.

///

☆ First Isomorphism Theorem:
Given a ring homomorphism

$$\varphi : R \to S$$

$\downarrow$

the function

$$\overline{\varphi} : R/\ker\varphi \to \operatorname{im}\varphi$$
$$a+\ker\varphi \mapsto \varphi(a)$$

is a ring isomorphism.

Proof: It's a surjective ring map (easy). To see that it's well defined and injective note that

$$\begin{aligned} a+\ker\varphi = b+\ker\varphi &\iff a-b \in \ker\varphi \\ &\iff \varphi(a-b) = 0 \\ &\iff \varphi(a)-\varphi(b) = 0 \\ &\iff \varphi(a) = \varphi(b). \end{aligned}$$

$\Rightarrow$ well-defined ✓

$\Leftarrow$ injective ✓ ///

☆ Correspondence Theorem

Given ideals $I \leq J \leq R$ note that

$$J/I := \{a+I : a \in J\}$$

is an ideal of R/I.

then the map $J \mapsto J/I$ defines an isomorphism of lattices

$$\begin{array}{ccc} R & & R/I \\ \vee\!| & & \vee\!| \\ J & \longleftrightarrow & J/I \\ \vee\!| & & \vee\!| \\ I & & I/I = 0 \end{array}$$

Proof omitted. //

Applications:

- classify subgroups of $\mathbb{Z}/n\mathbb{Z}$.
- prove that

$$I \leq R \text{ maximal } \Longleftrightarrow R/I \text{ field}.$$

Recall the Diamond Isomorphism from HW 2:

If $S \subseteq R$ is a subring and $I \subseteq R$ is an ideal, then

- $S + I \subseteq R$ is a subring
- $I \subseteq S + I$ is an ideal
- $S \cap I \subseteq S$ is an ideal
- We have an isomorphism

$$\frac{S}{S \cap I} \cong \frac{S + I}{I}.$$

Picture:

$$\begin{tikzcd}[column sep=small]
 & R \arrow[d, dash] & \\
 & S + I \arrow[dl, dash] \arrow[dr, dash] & \\
S \arrow[dr, dash] & & I \arrow[dl, dash] \\
 & S \cap I \arrow[d, dash] & \\
 & 0 &
\end{tikzcd}$$

See the Diamond?

(2) Properties of $\mathbb{Z}$ and $K[x]$

We say ring R is a <u>domain</u> if

$$ab = 0 \implies a = 0 \text{ or } b = 0.$$

We say domain R is <u>Euclidean</u> if we have $\delta : R - 0 \to \mathbb{N}$ such that for all $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ such that

- $a = qb + r$
- $r = 0$ or $\delta(r) < \delta(b)$.

☆ Theorem: Euclidean $\implies$ PID.

<u>Proof</u>: Let $I \leq R$ be an ideal. If $I = (0)$ we're done so suppose $I \neq (0)$ and choose $0 \neq a \in I$ with $\delta(a)$ minimal. Show that $I = (a)$. ///

<u>Corollary</u>: $\mathbb{Z}$ and $K[x]$ are PIDs.

This follows from the fact that $\mathbb{Z}$ is Euclidean with $\delta(n) = |n|$ and $K[x]$ is Euclidean with $\delta(f) = \deg(f)$. //

[Given a ring R and $f(x), g(x) \in R[x]$, recall that if $g(x)$ is <u>monic</u> then $\exists\ q, r \in R[x]$ such that

- $f(x) = q(x)g(x) + r(x)$
- $r = 0$ or $\deg(r) < \deg(g)$.

If $R = K$ a field then every nonzero $g \in K[x]$ is monic, hence $K[x]$ is Euclidean.]

Since $\mathbb{Z}$ is a PID, every ideal looks like (n) for $n \in \mathbb{Z}$.

Recall that

$$(a) + (b) = (d)$$
$$(a) \cap (b) = (m)$$

where $d = \gcd(a,b)$ & $m = \operatorname{lcm}(a,b)$.

Thus given ideals $I, J \leq R$ we think

$$I + J \approx \gcd(I, J)$$
$$I \cap J \approx \operatorname{lcm}(I, J).$$

If $I + J = (1)$ (i.e. if I, J are "coprime") then we have

$$I \cap J = IJ \quad \text{and}$$

$$\frac{R}{IJ} \approx \frac{R}{I} \times \frac{R}{J}.$$

When $R = \mathbb{Z}$ and $a, b \in \mathbb{Z}$ are coprime this says that

$$\mathbb{Z}/(ab) \approx \mathbb{Z}/(a) \times \mathbb{Z}/(b).$$

"Chinese Remainder Theorem"

This gives an isomorphism of groups of units:

$$(\mathbb{Z}/(ab))^\times \approx (\mathbb{Z}/(a))^\times \times (\mathbb{Z}/(b))^\times$$

and this implies that

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

φ = Euler's totient function.

We use this to compute

$$\varphi(n) = n \prod_{\substack{p \mid n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right)$$

E.g. $\varphi(100) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)$

$= 40.$

Then applying Lagrange's Theorem to $(\mathbb{Z}/(n))^\times$ gives Euler's Theorem

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

for all a, n with $\gcd(a,n) = 1$.

Application: Compute the last two digits of 73^{402}.

$$73^{402} = 73^{10\cdot 40 + 2}$$

$$= (73^{40})^{10}\, 73^2$$

$$\equiv (1)^{10} \cdot 73^2 \pmod{100}$$

$$\equiv 73^2 \pmod{100}$$

$$\equiv 5329 \pmod{100}$$

$$\equiv 29 \pmod{100}$$

MAGIC.

$$\begin{array}{r} {}^{2}73 \\ \times\ 73 \\ \hline 219 \\ 5110 \\ \hline 5329 \end{array}$$