LECTURE 25

Nov. 14/2003.

Recall def'n of ring ((R,+) ab gp, (R, ×) assoc. operation w/ 1, distrib.)

- last time we didn't assume multiplicat. is commutative
- From now on, all our rings will be <u>commutative</u>.

Recall also:

Ring homomorphisms:

$f: R \to R'$ (gp homo (R,+) that preserve 1 & mult.)

lead to kernels

$I = \ker f$ (defined as for grps)

& these subsets I satisfy properties making them "<u>ideals</u>" (subgroups for + stable under

In fact: given any ideal I, it is the kernel of the ring homomorphism

$$R \longrightarrow R' := R/I$$
$$a \longmapsto a + I$$

where R/I is "quotient ring" defined as quotient group for + & with mult. operation

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

Can verify that this indeed defines a good ring structure on R/I.

Two obvious ideals $\subset R$:

$I = \{0\}$ $\quad R' = R/I = R$ (f = id.)

$I = R$ $\quad R' = R/I = \{0\}$ $f(1) = 0_{R'}$ "0-ring"

Recall also that we have notion of "principal ideal": $(0)=\{0\}$ & $(1)=R$, and more generally $(a)=\{a\cdot r : r\in R\}\subset R$.

If $R\neq\{0\}$, these 2 ideals are distinct ($1\neq 0$) → i.e. $(0)\neq(1)$.

Prop If R has only one ideal, $R=\{0\}$.
R has exactly two ideals (namely R & $\{0\}$) $\iff$ R is a field (i.e. a ring where every nonzero $a\in R$ has a mult. inverse $a^{-1}\in R$, $a a^{-1}=a^{-1}a=1_R$)

Pf) ($\Leftarrow$) Assume R field, $I\neq 0$ ideal.
Want to show $I=R$.
Take $a\in I$ with $a\neq 0$.
Since a has inverse $a^{-1}\in R$,
$1=a\cdot a^{-1}\in I$ (by def'n of ideal)
Since $1\in I$, for any $r\in R$,
$r=1\cdot r\in I$ (again, def'n of ideal)
$\therefore$ $I=R$.
($\Rightarrow$) let $a\in R$, $a\neq 0$, consider the principal ideal (a). Now,
$(0)\neq(a)$ so $(a)=R$.
But $1\in R$ so $\exists r\in R$ s.t. $ar=1$.
$\boxtimes$.

Ex.: • $R=\mathbb{Z}/4\mathbb{Z}=\{0,1,2,3\}$
$I=(0),(1),(2)$

$$(0)=\{0\},\quad (1)=R,\quad (2)=\{0,2\}.$$

- $R = (\mathbb{Z}/n\mathbb{Z})$ have ideals (d), e.g. for $d \mid n$ (not nec. distinct.
- $R = (\mathbb{Z}/p^k\mathbb{Z})$: have descending chain of ideals:

$$(1) \supset (p) \supset (p^2) \supset (p^3) \supset \cdots \supset (p^k) = (0).$$

- $R = \mathbb{Z}$ has infinite # of distinct ideals. They are of the form $I = (n) = n\mathbb{Z}$ $n \geq 0$.

(this is the full list of subgroups & all are stable under mult. by $\mathbb{Z}$)

Note: $(n) \supset (n') \iff n$ divides n'.

So: lattice of ideals in $\mathbb{Z}$ = lattice of nonnegative integers under the divisibility rel'n.

$\mathbb{Z}/(n) = \mathbb{Z}/n\mathbb{Z}$ quotient rings.

- Another important ring where we know all ideals

F = field $\rightarrow$ $R = F[X] = \{a_n X^n + \cdots + a_1 X + a_0 \mid a_i \in F\}$ (n arb.)

"ring of polynoms. / F"

$p(X) \in R[X]$ is monic if $a_n = 1$.

If $q(x)$ is any polynomial of degree n (i.e. $q(x) = a_n x^n + \cdots + a_0$ & $a_n \neq 0$) then $\exists!\, c \in F^\times$ s.t. $c \cdot q(x)$ is monic of degree n $(c = a_n^{-1})$.

Note: In general: the highest power of X w/ nonzero coeff. is called the degree of the polynomial.

Prop Every ideal $I \subset R = F[X]$ is principal, generated $I = (f)$ by the monic poly f in I of least degree.

So: {ideals} $\longleftrightarrow$ {monic polys}

& $(f) \supset (g) \Longleftrightarrow$ f divides polynom. g

$g(x) = f(x)q(x)$

Pf) Analogue of Euclidean algorithm for polynoms. / a field:

If f & g are 2 polys. w/ $\deg(f) \geq \deg(g)$

($\deg(f)$: a degree of f)

then $f(x) = g(x) \cdot q(x) + r(x)$

where $\deg(r) < \deg(g)$

e.g.: take $f(x) = x^3 + 2x^2 + 3x + 7$

$g(x) = x^2 + x + 1$

then find $q(x) = (x+1)$

$r(x) = (x+6)$

If $I \neq 0$, take $f \in I$, $f \neq 0$, of minimal degree n. Scale by $c = a_n^{-1}$ to make f monic (note this doesn't change $f \in I$).

Let h be another poly in I.

$$h(x) = q(x) f(x) + r(x)$$

by Euclidean algorithm.

$$q(x) f(x) \in I \Rightarrow h(x) - q(x) f(x) \in I$$

& $\deg(r) < \deg(f) = n$.

But $r(x) = h(x) - q(x) f(x)$ & so unless $r = 0$, we have contradiction of $f \neq 0$ having minimal degree. So $r = 0$ &

$$h = q \cdot f \in (f). \quad \boxtimes$$

Fix $c \in F$ & Consider map $R = F[X] \xrightarrow{h} F$

$$f(x) \longmapsto f(c)$$

This is a ring homomorphism.

Note: poly $f(x) = X - c$ is monic, of degree 1, with $f(c) = 0$. By argument above, then <u>any</u> $f \in I = \ker(h)$ is a multiple of $X - c$.

<u>Cor</u> $\#\{\text{roots of poly } f \text{ over } F \text{ (field)}\} \leq (\text{degree of } f)$

Note: This doesn't work if F isn't field.

e.g.: $\mathbb{Z}/8\mathbb{Z}[X]$

X^2-1 has 4 roots,

but $\deg(X^2-1) = 2$.

Example of non-principal ideal:

$R = F[X,Y]$. $I = (X, Y)$.

$$h: R \longrightarrow F$$
$$f(x,y) \longmapsto f(0,0)$$

$I = \ker(h)$ is not generated by one element

$X \in I$, $y \in I$ & these can't both be multiples of some element other than a constant; but $I \neq (\text{const}) = R$.

For any group G, have a subgroup $\{e\} \longrightarrow G$; but this is not such an interesting subgroup.

For any ring (comm.) R, there is a natural ring hom.:

$$h: \mathbb{Z} \longrightarrow R$$
$$0 \longmapsto 0_R$$
$$1 \longmapsto 1_R$$
$$n \longmapsto \underbrace{1_R + \cdots + 1_R}_{n \text{ times}}.$$

Warning: h is not necessarily injective.

$I = \ker h = n\mathbb{Z}$ for some $n \geq 0$.

Think about this: If R is a field, either $\ker h = 0$ or $\ker h = p\mathbb{Z}$, p prime.