LECTURE 24 Nov. 12/2003

Rings

Examples: $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{C}$, F = field, $M_n(F)$

Rough def'n:
- ab. gp. under $+$
  identity denoted 0
- mult. operation $\times$
  identity denoted $\underline{1}$
  operation not necessarily commutative
  don't nec. have inverses
- distributive props. $a(b+c) = ab+ac$
  $(b+c)a = ba+ca$

Subring $R' \subset R$ (subset which is ring under same operations)

e.g. $\mathbb{Z} \subset \mathbb{Q}$

NOTE: After today, we will assume our rings are commutative (so $M_n(F)$ will not be an example). But for now, we will not assume commutativity.

Subrings of $R = \mathbb{C} \leftarrow$ complex #'s:
$\mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{Z}+\mathbb{Z}i = \{a+bi : a,b \in \mathbb{Z}\}$, etc...

usually denoted $\mathbb{Z}[i]$
& called "Gaussian integers"

A ring not contained in $\mathbb{C}$:
R = all polynomials in 1 variable X with coeffs. in $\mathbb{C}$

$= \{a_n X^n + \text{—} + a_1 X + a_0 : a_i \in \mathbb{C}\}$

denoted $\mathbb{C}[X]$

Polynomials in multiple variables:
e.g. $\mathbb{C}[X,Y] = \mathbb{C}[X][Y]$.

Or more generally, if R is a commutative ring, have ring $R[X]$ of polynoms. w/ coeffs in R.

E.g. if $R = \mathbb{Z}/2$, in $R[X]$
$$(X+1)(X+1) = X^2+2X+1 = X^2+1$$

The smallest ring is $R=\{0\}$ $(1=0)$.
But:

<u>Prop</u> If $R \neq \{0\}$ then $1 \neq 0$ in R

<u>Pf)</u> Let $a \in R$ and suppose $1=0$
Then $a = 1 \cdot a = 0 \cdot a$
But $0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a$
$\Rightarrow 0 \cdot a = 0$ $\binom{=1a}{=a}$ (cancelling)
hence $R = \{0\}$. $\boxtimes$

Have rings of every size: $\mathbb{Z}/n\mathbb{Z}$ ring with n elements.

A very useful way to construct rings is to start with an abelian group $(A,+,0)$, and let

$$R = \mathrm{End}(A) = \{f : A \to A \text{ homomorphisms}\}$$

operations:
- $f+g$ defined by $(f+g)(a) = f(a)+g(a)$
  0_R defined by $0_R(a) = 0_A$
  $-f$ defined by $(-f)(a) = -(f(a))$
- $f \times g$ defined by $(f\times g)(a) = f(g(a))$ (composition)
  1_R defined by $1_R(a) = a$
  need not have inverses! (f is invertible $\Leftrightarrow$ it is an isomorphism)

E.g.:
- $R = \mathrm{End}(\{e\}) = \{0\}$.
- $\mathbb{Z}$ as a ring $= \mathrm{End}(\underbrace{\mathbb{Z},+,0}_{\text{the group}})$

Note that $f(k) = k \cdot f(1) \quad \forall f \in \mathrm{End}(\mathbb{Z})$

Thus the map $\mathrm{End}(\mathbb{Z},+,0) \longrightarrow \mathbb{Z}$
$f \longmapsto f(1)$

is a bijection & the ring structure on $\mathrm{End}(\mathbb{Z})$ induces one on $\mathbb{Z}$.

<u>But</u>: this is just the <u>usual</u> operations of addition and multiplication on $\mathbb{Z}$!

- similarly $\mathbb{Z}/n\mathbb{Z} = \mathrm{End}(\mathbb{Z}/n, +, 0)$
  $f(1) \longleftarrow\!\shortmid\; f$
- $A = (\mathbb{Z}/p\mathbb{Z})^2 = \{(a_1, a_2) : a_i \in \mathbb{Z}/p\mathbb{Z}\}$
  $\mathrm{End}(A) = M_2(\mathbb{Z}/p\mathbb{Z})$
  ↖ noncomm. ring.
- more generally, $A = (\mathbb{Z}/p\mathbb{Z})^n$
  $\Rightarrow \mathrm{End}(A) = M_n(\mathbb{Z}/p\mathbb{Z})$

FROM NOW ON: We will assume our rings are commutative

Ring homomorphism $f : R \longrightarrow R'$
is map of sets which is gp hom. for $+$,
maps $1_R \longmapsto 1_{R'}$ and $f(a *_R b) = f(a) *_{R'} f(b)$

E.g.: If $R \subset R'$ is a subring, the inclusion
$f : R \hookrightarrow R'$ is a ring hom.

$\ker(f) = \{a \in R : f(a) = 0_{R'}\}$

Properties of $\ker(f)$: 1) A subgroup under $+$
2) If $a \in R$, $b \in \ker(f)$,
then $f(a \times b) = f(a) \times 0 = 0$
So $a \cdot b \in \ker(f)$.

Defn: A subset $I \subset R$ which is a subgroup under $+$, and closed under $\times$ by any $a \in R$ is called an ideal.

Examples: 1) $\ker(f)$ (f any ring hom)
2) $\{0\}$ $(= \ker(\mathrm{id} : R \to R))$
3) R $(= \ker(0 : R \to \{0\}))$
4) Given $r \in R$, $I = \{ar : a \in R\}$

is an ideal

<u>Def'n</u> This I is called the <u>principal ideal</u> generated by r.
(often denoted $I = (r)$ or $I = rR = Rr$)

<u>In fact</u>:
Any ideal I is the kernel of a natural ring hom.

$$\begin{aligned} R &\longrightarrow R/I \\ a &\longmapsto a+I \end{aligned}$$

completely analogously to groups.
We define a ring structure on R/I by

$$(a+I)+(b+I) = (a+b)+I$$
$$(a+I)\times(b+I) = (a\times b)+I$$

This works because I is an ideal.
We will return to this in greater detail later.

<u>Fact</u> The only ideals in $\mathbb{Z}$ have the form $I = (n) = n\mathbb{Z}$.
The quotient ring is $\mathbb{Z}/n\mathbb{Z}$.

(<u>Recall</u>: these are the only subgroups of $\mathbb{Z}$.)

<u>Important fact</u>: There are rings in which there are ideals which are <u>not principal</u>.

Another important notion:

<u>Units</u> in R: $a \in R$ s.t. $\exists b \in R$ w/ $ab = 1$

(i.e. a^{-1} <u>exists</u>)

Given any ring R,

$R^\times :=$ units of R

$= \{a \in R : a \text{ is a unit}\}$

is a group, called the <u>unit group of</u> R.

(gp op.: multiplication)

<u>E.g.</u>:

- $R = F$, a field
  $R^\times = R - \{0\}$
- $R = \mathbb{Z}$
  $R^\times = \{\pm 1\}$
- $R = \mathbb{Z}/n\mathbb{Z}$
  $R^\times = \{a + n\mathbb{Z} : \gcd(a,n) = 1\}$
- $R = M_n(F)$
  $R^\times = GL_n(F)$.