4/12/17

Recall: if R is a ring, and $a \in R$, we define

$$(a) = aR = \{ar : r \in R\}$$

<u>Claim</u> aR is an ideal of R, the <u>principal ideal generated by</u> a.

<u>Pf</u> Let $I = aR$.

1) $(I, +)$ is a subgp. of $(R, +)$:

- $0 = a0 \in I$
- $ar_1, ar_2 \in I \Rightarrow ar_1 + ar_2 = \underbrace{a(r_1 + r_2)}_{\in I}$

[$\cancel{x = ar \in I, s \in R \Rightarrow (ar)s = a(rs)}$ $\in I$.]

- $ar \in I \Rightarrow -ar = a(-r) \in I$

2) $IR \subseteq I$:

$ar \in I, s \in R \Rightarrow (ar)s = a(rs) \in I$. //

<u>Defn</u> If $\phi : R \to R'$ is a homomorphism, <u>kernel</u>

$$\mathrm{Ker}(\phi) = \{x \in R : \phi(x) = 0\}.$$

<u>Prop 20.1</u> Let $\phi : R \to R'$ homom.

1) $\mathrm{Ker}(\phi)$ is an ideal of R.

2) $\mathrm{Im}(\phi)$ is a subring of R'.

Pf. 1) Let $K = \ker(\phi)$.

- $(K, +)$ is a subgp of $(R, +)$ (group hom)
- $a \in \ker(\phi)$, $r \in R$

$\Rightarrow \phi(ar) = \phi(a)\phi(r)$
$= 0 \cdot \phi(r) = 0$

$\Rightarrow ar \in \ker(\phi)$.

So K is an ideal.

2) $(\mathrm{Im}(\phi), +)$ is a subgp of $(R', +)$ (gp hom), and $\mathrm{Im}(\phi)$ is closed under mult, as $\phi(a)\phi(b) = \phi(ab) \in \mathrm{Im}(\phi)$. //

Eg. 1) $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}_n$,

$$\phi(x) = [x] \quad \forall x \in \mathbb{Z}$$

Here $\ker(\phi) = \{x \in \mathbb{Z} : [x] = 0\}$
$= n\mathbb{Z}$,

a principal ideal of $\mathbb{Z}$.

2) $\phi : F[x] \longrightarrow F$,

$$\phi(f(x)) = f(0) \quad \forall f \in F[x]$$

is a homom., and

$\ker(\phi) = \{f(x) : f(0) = 0\}$
$= \{\text{polys. } a_r x^r + \dots + a_1 x\}$
$= (x)$, principal ideal.

3) Define $\phi : \mathbb{Z}[i] \to \mathbb{Z}_5$ by

$$\phi(a+bi) = [a-2b]_5$$

Ex: Show ϕ is a homom.

Here

$$\operatorname{Ker}(\phi) = \{a+bi : a \equiv 2b \bmod 5\}$$

an ideal of $\mathbb{Z}[i]$.

<u>Quotient Rings</u>

R ring (commutative with 1).

Let I be an ideal of R.

For $r \in R$, define the coset

$$I + r = \{i + r : i \in I\},$$

(coset of $(I,+)$ in $(R,+)$).

Define $+, \times$ of cosets by

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

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

We need to check these are well-defined.

Well, $+$ is well-defined (group theory).

What about $\times$?

Well,

$$I+r = I+r', \quad I+s = I+s'$$

$$\Rightarrow r-r',\ s-s' \in I$$

$$\Rightarrow (r-r')s + (s-s')r' \in I \quad \text{(ideal)}$$

$$\Rightarrow rs - r's' \in I$$

$$\Rightarrow I+rs = I+r's'.$$

So $+, \times$ of cosets are well-defined.

<u>Theorem 20.2</u> Let $\frac{R}{I}$ be the set of all cosets $I+r$ $(r \in R)$. With $+, \times$ as above, $\frac{R}{I}$ is a ring, commutative with 1.

<u>Pf.</u> Need to check

1) $\left(\frac{R}{I}, +\right)$ abelian gp
2) $\left(\frac{R}{I}, \times\right)$ associative (& commutative with 1)
3) Distributivity

1) is done, by group theory.

2) Check:

$$(I+r)\big((I+s)(I+t)\big)$$
$$= (I+r)(I+st)$$
$$= I + r(st)$$
$$= I + (rs)t$$
$$= (I+rs)(I+t)$$
$$= \big((I+r)(I+s)\big)(I+t).$$

Commutative: $(I+r)(I+s) = I+rs$
$$= I+sr$$
$$= (I+s)(I+r)$$

Elt 1: this is $I+1$.

3) Distributivity: ex. //

Eg. 1) $\dfrac{\mathbb{Z}}{5\mathbb{Z}} = \dfrac{\mathbb{Z}}{I}$

$= \{I, I+1, I+2, I+3, I+4$

Easy check: map

$$I+r \longrightarrow [r]_5$$

is an isomorphism

$$\frac{\mathbb{Z}}{5\mathbb{Z}} \longrightarrow \mathbb{Z}_5.$$

2) Let $R = \mathbb{Q}[x]$, and

$$I = (x^2 - 2)$$

<u>Claim 1</u> $\frac{R}{I}$ = set of cosets

$$\{I + ax + b : a, b \in \mathbb{Q}\}$$

<u>Pf</u> Consider a coset

$$I + f(x) \qquad (f(x) \in \mathbb{Q}[x])$$

Write

$$f(x) = (x^2-2)\,q(x) + r(x)$$

where $r = 0$ or $\deg(r) < 2$.

Now $(x^2-2)\,q(x) \in I$, so

$$I + f(x) = I + (x^2-2)q(x) + r(x)$$

$$= I + r(x)$$

$$= I + ax + b.$$

<u>Claim 2</u> In $\frac{R}{I}$,

$$(I + x)^2 = I + 2$$

<u>Pf.</u> $(I + x)^2 = I + x^2$

$$= I + 2.$$

<u>Thm. 20.3</u> (1st Iso Thm. for Rings)

Let R, S be rings (commutative with $\mathbb{1}$). Suppose $\phi : R \to S$ is a homom. Then $\mathrm{Ker}(\phi)$ is an ideal of R, $\mathrm{Im}(\phi)$ is a subring of S, and

$$\frac{R}{\mathrm{Ker}(\phi)} \cong \mathrm{Im}(\phi).$$

Pf ~~Define~~ Let $K = \mathrm{ke}(\phi)$. Define $\alpha : \frac{R}{K} \longrightarrow \mathrm{Im}(\phi)$ by

$$\alpha(K+r) = \phi(r) \quad \forall r \in R.$$

We'll prove α is an isomorphism.

1) <u>Well-defined</u>:

$$K+r = K+s \implies r-s \in K$$
$$\implies \phi(r-s) = 0$$
$$\implies \phi(r) = \phi(s).$$
$$\implies \alpha(K+r) = \alpha(K+s).$$

2) <u>Homom.</u>

$$\alpha\big((K+r)+(K+s)\big) = \alpha(K+r+s)$$

$$= \phi(r+s)$$

$$= \phi(r)+\phi(s)$$

$$= \alpha(K+r)+\alpha(K+s).$$

Similarly $\alpha\big((K+r)(K+s)\big) = \alpha(K+r)\alpha(K+s)$.

3) <u>α bijection</u>:

Injective: $\alpha(K+r) = \alpha(K+s)$

$$\Longrightarrow \phi(r) = \phi(s)$$

$$\Longrightarrow \phi(r-s) = 0$$

$$\Longrightarrow r-s \in \ker(\phi) = K$$

$$\Longrightarrow K+r = K+s.$$

<u>Surjective</u> $x \in \mathrm{Im}(\phi)$

$$\Longrightarrow x = \phi(r), \text{ some } r \in R$$

$$\Longrightarrow x = \alpha(K+r).$$

//

<u>5/12/17</u>

<u>Examples</u>

1) Homom. $\phi : \mathbb{Z} \to \mathbb{Z}_n$

sending $x \longrightarrow [x]$.

$Ker(\phi) = n\mathbb{Z}$

$Im(\phi) = \mathbb{Z}_n$

So Thm 20.3 says

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$$

Isomorphism is

$$n\mathbb{Z} + r \longrightarrow [r] \qquad (r \in \mathbb{Z})$$

2) Let

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$$

This is a <u>field</u>:

Subgroup of $(\mathbb{R}, +)$: easy check

Subgroup of $(\mathbb{R}^*, \times)$:

- $1 \in \mathbb{Q}(\sqrt{2})$
- closed under mult ✓
- inverses :

$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} \in \mathbb{Q}(\sqrt{2}).$$

Define $\phi : \mathbb{Q}[x] \longrightarrow \mathbb{Q}(\sqrt{2})$ by

$$\phi(f(x)) = f(\sqrt{2}) \quad \forall f(x) \in \mathbb{Q}[x]$$

(e.g. $\phi(x^3 - x + 1) = (\sqrt{2})^3 - \sqrt{2} + 1 \in \mathbb{Q}(\sqrt{2})$)

Then ϕ is a homom of rings,

and

$$\mathrm{Ker}(\phi) = \{ f(x) \in \mathbb{Q}[x] : f(\sqrt{2}) = 0 \}.$$

If $f(x) \in \mathbb{Q}[x]$ has a root $\sqrt{2}$,

then it also has $-\sqrt{2}$ as a root,

so $f(x)$ is ~~divide~~ ~~dis~~ ~~dis~~ divisible by $x^2 - 2$. Hence

$$\mathrm{Ker}(\phi) = \text{principal ideal } (x^2-2).$$

Also

$$\mathrm{Im}(\phi) = \mathbb{Q}(\sqrt{2}).$$

So by Thm 20.3,

$$\frac{\mathbb{Q}[x]}{I \leftarrow (x^2-2)} \cong \mathbb{Q}(\sqrt{2})$$

(Isomorphism

$$I + ax + b \longrightarrow a\sqrt{2} + b,)$$

$$I + x \longrightarrow \sqrt{2}$$

See previous example.

21. Ideals in ED's

Recall: ideal I of R means

$(I,+)$ abelian gp

$IR \subseteq I$

Eg. Principal ideals aR $(=(a))$.

Defn Call R a Principal Ideal Domain (PID) if every ideal of R is principal ideal.

Theorem 21.1 Every ED is a PID.

Pf. Let R be an ED with Euclidean function $\delta : R \setminus 0 \longrightarrow \mathbb{Z}_{\geq 0}$.

Let I be an ideal of R.

If $I = \{0\}$ then $I = (0)$ is principal.

So now assume $I \neq (0)$.

Choose $a \in I$ s.t. $a \neq 0$ and $\delta(a)$ is as small as possible.

<u>Claim</u> $I = aR$.

Pf. Let $x \in I$. As R is an ED, $\exists\, q, r \in R$ s.t.

$$x = qa + r \text{ and } r = 0 \text{ or } \delta(r) < \delta(a).$$

Now $r = x - qa \in I$ since $x \in I$ and $qa \in I$. Hence by the choice of a, we must have $r = 0$. Therefore

$$x = qa \in aR.$$

So $I \subseteq aR$.

As $a \in I$, $aR \subseteq I$.

Therefore

$$I = aR,$$

a principal ideal. //

Eg. 1) $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\sqrt{2}]$, $F[x]$ (F field) ~~all~~ are all ED's, hence PID's.

2) By a previous example,

$$I = \{a+bi \in \mathbb{Z}[i] : a \equiv 2b \bmod 5\}$$

is an ideal of $\mathbb{Z}[i]$.

By above, it must be principal.

Generator? Ans By above proof,

$I = aR$, where $a \in I$ ~~is~~ has smallest $\delta(a)$.

Check smallest possible $\delta(a)$ is 5, so generator is $2+i$.

3) $R = \mathbb{Z}[\sqrt{-3}]$ is not a PID

Pf. For $a, b \in R$ define

$$aR + bR$$

$$= \{ar_1 + br_2 : r_i \in R\}$$

This is an ideal of R (Sheet 9, Q2).

Now let

$$I = 2R + (1+\sqrt{-3})R$$

Claim I is non-principal

Pf. Suppose $I = aR$, principal.

Then

$$2 = ar \qquad (r, s \in R).$$
$$1+\sqrt{-3} = as.$$

Then

$$4 = |a|^2|r|^2 = |a|^2|s|^2$$

Let

$$a = x + y\sqrt{-3} \qquad (x, y \in \mathbb{Z}).$$

Then $|a|^2 = x^2 + 3y^2 = 1, 2$ or 4.

Clearly 2 is not possible.

If $|a|^2 = 4$ then

$|r|^2 = |s|^2 = 1$, so

$r, s = \pm 1$ hence by

$$1+\sqrt{-3} = \pm 2 \quad \#$$

Therefore

$$|a|^2 = 1$$

hence $a = \pm 1$. Hence

$$I = R.$$

However, a general elt. of I is

$$2t + (1+\sqrt{-3})u \quad (t, u \in R)$$

Check: this has form

$$v + w\sqrt{-3}, \quad v \equiv w \bmod 2$$

So in fact $I \neq R$

Therefore I is non-principal.

4) $\mathbb{Z}[\sqrt{-d}]$, $d \geq 3$ is not a ~~RNB~~ PID (Sh 9 qn).

22. Maximal Ideals

R ring (commutative with 1) ID

I an ideal of R.

Basic Qn When is the quotient ring $\frac{R}{I}$ a field?

<u>Defn</u> I is a <u>maximal</u> ideal if

1) $I \neq R$, and

2) $I \subsetneq J \subseteq R$ (J ideal)
$\Longrightarrow J = R$.

(i.e. I is contained in no larger ideal, apart from R itself).

Eg. $R = \mathbb{Z}$

<u>Claim</u> For p prime, $p\mathbb{Z}$ is a maximal ideal.

Pf Suppose

$$p\mathbb{Z} \subsetneq J, \text{ ideal}$$

As $\mathbb{Z}$ is a PID, $\exists d \in \mathbb{Z}$ s.t. $J = d\mathbb{Z}$.

Then

$$p \in d\mathbb{Z} \Rightarrow d \text{ divides } p$$
$$\Rightarrow d = \pm 1 \text{ or } \pm p$$
$$\Longrightarrow J = \mathbb{Z} \text{ or } \cancel{p\mathbb{Z}}$$

$\therefore J = \mathbb{Z}$.

Theorem 22.1 $\frac{R}{I}$ is a field iff I is a maximal ideal of R.

Ex $\frac{\mathbb{Z}}{p\mathbb{Z}} \cong \mathbb{Z}_p$, a field ✓.

Proof of Thm 22.1 **POSTPONE**

Maximal ideals in PID's

Prop 22.4 Suppose R is a PID, and let $a \in R$. Then the ideal aR is maximal iff the elt $a \in R$ is an irreducible elt.

Pf. ($\Rightarrow$) Suppose $I = aR$ is maximal. ~~[illegible]~~ Let

$$a = bc \quad (b, c \in R).$$

Then $a \in bR$, hence

$$aR \subseteq bR.$$

As aR is maximal, this implies

$$bR = aR \text{ or } R.$$

If $bR = R$ then b is a unit.

If $bR = aR$, then

$$b = au, \quad a = bv \quad (u, v \in R)$$

Then $a = auv$, hence $uv = 1$,

so u, v are units, so c is a unit.

Hence b or c is a unit, so

a is <u>irreducible</u>.

($\Longleftarrow$) Suppose a irreducible.

Let

$$aR \subseteq J \subseteq R$$

(J ideal). As R is a PID,

$J = dR$. Then

$$a = de \quad (e \in R).$$

As a is irreducible,

d or e is a unit.

If d is ~~am~~ a unit,

then

$$J = dR = R.$$

If e is a unit then

$$aR = deR = dR = J.$$

Hence $J = aR$ or R.

Therefore aR is maximal. //.

Eg. Recall any ED is a PID, eg. $\mathbb{Z}$, $\mathbb{Z}[i]$, $F[x]$ (F field).

By 22.4,

max. ideals of $\mathbb{Z}$ are $p\mathbb{Z}$ (p prime)

max. ideals of $F[x]$ are principal ideals $(p(x))$, where $p(x) \in F[x]$ is an <u>irreducible</u> polynomial.

23. <u>Finite fields</u>

By Thm 22.1,

I maxl. ideal of R

$\Longrightarrow$ $\frac{R}{I}$ is a field

And by 22.4, if R is a PID and $a \in R$ is irred. elt. then aR is a maxl. ideal.

<u>Conclude</u> R a PID $\Rightarrow$.

If $a \in R$ is irreducible, the

$$\frac{R}{aR}$$

is a field.

Eg. 1) $R = \mathbb{Z}$:

$$\frac{\mathbb{Z}}{p\mathbb{Z}} \cong \mathbb{Z}_p \text{ , field.}$$

2) Here's a new finite field

Let

$$R = \mathbb{Z}_2[x]$$

The quadratic poly

$$x^2 + x + 1 \in \mathbb{Z}_2[x]$$

is irreducible. Therefore the quotient ring

$$\frac{\mathbb{Z}_2[x]}{(x^2+x+1)} = F$$

is a field.

<u>Elts of F</u> Writing $I = (x^2+x+1)$ elts of F are of form

$$I + ax + b \quad (a, b \in \mathbb{Z}_2)$$

So

$$F = \{I, I+1, I+x, I+x+1\},$$

$|F| = 4$. Write

$$\alpha = I + x$$

and

$$\bar{0} = I$$

$$\bar{1} = I + 1.$$

So

$$F = \{\bar{0}, \bar{1}, \alpha, \alpha+\bar{1}\}.$$

Observe that

$$\alpha^2 + \alpha + \bar{1} = I + x^2 + x + 1$$

$$= I = \bar{0}$$

So F is a field of 4 elements, ~~the~~ with $+, \times$

$(F, +)$

	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

$(F^*, \times)$

	1	α	$\alpha+1$
1	1	α	$\alpha+1$
α	α	$\alpha+1$	1
$\alpha+1$	$\alpha+1$	1	α

Note $(F, +) \cong C_2 \times C_2$

$(F^*, \times) \cong C_3$.

<u>Prop. 23.1</u> F field.

Let $p(x) \in F[x]$ be an irreducible poly. of degree $n \geq 1$. Let $I = (p(x))$. Then

1) $\frac{F[x]}{I}$ is a field.

2) Elts. of $\frac{F[x]}{I}$ are of form

$$I + f(x), \quad \deg(f) < n.$$

3) If $F = \mathbb{Z}_p$, then

$$\left| \frac{F[x]}{I} \right| = p^n$$

4) If $\alpha = I + x \in \frac{F[x]}{I}$ then

$$p(\alpha) = 0.$$

5) The map $\phi : F \to \frac{F[x]}{I}$ given by

$$\phi(a) = I + a \quad (a \in F)$$

is an injective homom.

Hence $\phi(F) = \{ I + a : a \in F \} \cong F$ so $\frac{F[x]}{I}$ has a subfield isomorphic to F.

Pf 1) Already done

2) Let $I + h(x) \in \frac{F[x]}{I}$.

Write

$$h(x) = q(x)\,p(x) + r(x),$$

$$\deg(r) < \deg(p) = n$$

Then

$$I + h(x) = I + r(x).$$

3) By (2), the elts of $\frac{F[x]}{I}$ are

$$\{ I + a_{n-1}x^{n-1} + \dots + a_0 : a_i \in F \}$$

and all these cosets are distinct.

So if $F = \mathbb{Z}_p$, no. of cosets is p^n.

4) If $\alpha = I + x$, then

$$p(\alpha) = I + p(x)$$

$$= I = \bar{0}.$$

5) ϕ is a homom, and is injective as for $a, b \in F$

$$\phi(a) = \phi(b) \Rightarrow I + a = I + b$$

$$\Rightarrow a - b \in I = (p(x))$$

$$\Rightarrow a = b. \quad //$$