3/12/19

Defn For a homom. $\phi : R \to R'$, the <u>kernel</u> is

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

Prop. 23.1 Let $\phi : R \to R'$ be a homom. Then

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

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

Pf. 1) First, $(\mathrm{Ker}(\phi), +)$ is a subgp of $(R, +)$ (by group theory).

Also

$a \in \mathrm{Ker}(\phi)$, $r \in R$

$\Longrightarrow \phi(a) = 0$

$\Longrightarrow \phi(ar) = \phi(a)\phi(r) = 0$

$\Longrightarrow ar \in \mathrm{Ker}(\phi)$.

Hence $\mathrm{Ker}(\phi)$ is an ideal.

2) $(\mathrm{Im}(\phi), +)$ is a subgp of $(R', +)$ (gp. theory). Also $\mathrm{Im}(\phi)$ is closed under mult, since

$$\phi(a)\phi(b) = \phi(ab) \in \mathrm{Im}(\phi). \quad //$$

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

sending

$$x \longrightarrow [x] \qquad (x \in \mathbb{Z})$$

Here $\ker(\phi) = \{na : a \in \mathbb{Z}\}$

$= $ principal ideal $n\mathbb{Z}$.

2) $\phi : F[x] \to F$ (F field), sending

$$p(x) \longrightarrow p(0) \qquad \forall p(x) \in F[x].$$

Here

$$\ker(\phi) = \{p(x) : p(0) = 0\}$$

$= $ principal ideal $x F[x]$.

Quotient Rings

Let I be an ideal of R, and for $r \in R$, define the coset

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

Define addition & mult. of cosets by

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

Need to check these operations are well-defined. The addition of cosets is well-defined (group theory, working in the group $(R,+)$).

To check mult. of cosets well-def: need to check

$$\left.\begin{array}{l} I+r = I+r' \\ I+s = I+s' \end{array}\right\} \Rightarrow I+rs = I+r's'$$

Pf. Well,

$$\text{LHS} \Rightarrow r-r' \in I,\ s-s' \in I$$

$$\Rightarrow (r-r')s + (s-s')r' \in I$$

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

$$\Rightarrow I+rs = I+r's' \quad \checkmark$$

Theorem 23.2 Let $\frac{R}{I}$ be the set of all cosets $I+r$ $(r\in R)$. With $+,\times$ of cosets defined as above in $(*)$, $\frac{R}{I}$ is a ring, commutative with 1.

Pf. Need to check:

- $\left(\frac{R}{I},+\right)$ abelian gp

(true by group theory for gp $(R,+)$).

- $\left(\frac{R}{I},\times\right)$ associative, commutative with 1

- distributive laws

This is routine (Ex.) //.

<u>Defn</u> We call $\frac{R}{I}$ the <u>quotient ring</u> of R by I.

<u>Eg.</u> 1) Let $R = \mathbb{Z}$, $I = 5\mathbb{Z}$.

Here

$$\frac{R}{I} = \{I, I+1, I+2, I+3, I+4\}$$

Check the map

$$I + x \longrightarrow [x] \in \mathbb{Z}_5$$

is an isomorphism $\frac{\mathbb{Z}}{5\mathbb{Z}} \to \mathbb{Z}_5$.

2) Let

$$R = \mathbb{Q}[x],$$

$$I = (x^2+1)R$$

What can we say about the quotient ring R/I?

<u>Claim</u> The elements of $\frac{R}{I}$ are just the cosets

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

Pf. Take any coset

$$I + p(x) \in \frac{R}{I}$$

(where $p(x) \in \mathbb{Q}[x]$).

Divide x^2+1 into $p(x)$:

$$p(x) = q(x)(x^2+1) + r(x)$$

where $q(x), r(x) \in \mathbb{Q}[x]$, $\deg(r) < 2$.

Then

$$\begin{aligned} I + p(x) &= I + q(x)(x^2+1) + r(x) \\ &= I + r(x) \quad (\text{as } q(x)(x^2+1) \in I) \\ &= I + ax + b, \end{aligned}$$

proving Claim.

One more fact about $\frac{R}{I}$: let

$$\alpha = I + x \in \frac{R}{I}$$

Then

$$\begin{aligned} \alpha^2 &= I + x^2 \\ &= I - 1. \end{aligned}$$

So can think of

$$\frac{R}{I} = \{ a\alpha + b : a \in \mathbb{Q} \}$$

where $\alpha^2 = -1$.

To be continued....

<u>Theorem 23.3</u> (First Iso Thm for rings)

If $\phi : R \to S$ is a homom (of rings), then

$$\frac{R}{\ker(\phi)} \cong \operatorname{Im}(\phi)$$

<u>Pf.</u> Let $I = \ker(\phi)$, ideal of R.

Define

$$\alpha : \frac{R}{I} \longrightarrow \operatorname{Im}(\phi)$$

by

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

1) <u>α is well-defined</u> (by group theory for $(R,+)$ – checked in pf of 1st Iso thm for groups)

2) <u>α is a homom</u>:

$$\begin{aligned} \alpha\big((I+r) + (I+s)\big) &= \alpha(I+r+s) \\ &= \phi(r+s) \\ &= \phi(r) + \phi(s) \\ &= \alpha(I+r) + \alpha(I+s) \end{aligned}$$

Similarly

$$\alpha\big((I+r)(I+s)\big) = \alpha(I+r) \cdot \alpha(I+s).$$

3) α <u>bijection</u>: proved in pf of First Iso Thm for gps. //.

<u>Eg.</u> 1) Homom $\phi : \mathbb{Z} \to \mathbb{Z}_5$ sending $x \to [x]$.

Has $\ker(\phi) = 5\mathbb{Z}$,

$\operatorname{Im}(\phi) = \mathbb{Z}_5$.

So 1st Iso thm says

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

2) Define

$$\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}.$$

Check this is a field (subfield of $\mathbb{C}$).

Define $\phi : \mathbb{Q}[x] \to \mathbb{Q}(i)$ by

$$\phi(p(x)) = p(i) \quad \forall p(x) \in \mathbb{Q}[x]$$

This is a homom. (ex),

and

$$\ker(\phi) = \{p(x) \in \mathbb{Q}[x] : p(i) = 0\},$$

the set of rational polys have i as a root.

If $p(x) \in \mathbb{Q}[x]$ has root i, then $-i$ is also a root, so $p(x)$ is divisible by $(x-i)(x+i) = x^2+1$. Hence

$$\operatorname{Ker}(\phi) = \text{ideal } (x^2+1)\,\mathbb{Q}[x].$$

So 1st Iso thm

$$\frac{\mathbb{Q}[x]}{(x^2+1)\,\mathbb{Q}[x]} \cong \operatorname{Im}(\phi) = \mathbb{Q}(i).$$

<u>5/12/19</u>

1) Typo on Sh 9, Q2

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

2) Given a field F, and a subset $H \subseteq F$, how to check that H is a <u>subfield</u> of F.

<u>Ans</u> The axioms of a field:

- $(F, +)$ an abelian group
- $(F \backslash 0, \times)$ an abelian group
- distributive laws

So to check H is a subfield:

1) Check $(H, +)$ is a subgp of $(F, +)$

2) Check $(H \backslash 0, \times)$ is a subgp of $(F \backslash 0, \times)$.

(3) All our rings will be commutative (under $\times$) with mult. identity 1.

24. Ideals in EDs

Defn R is a principal ideal domain (PID) if every ideal of R is a principal ideal aR.

Theorem 24.1 Every ED is a PID.

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

Let I be an ideal of R, $I \neq \{0\}$.

Choose $0 \neq a \in I$ with $\delta(a)$ as small as possible.

Claim $I = aR$.

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

$$x = qa + r$$

where $r = 0$ or $\delta(r) < \delta(a)$.

Then
$$r = x - qa \in I.$$

If $r \neq 0$, then $\delta(r) < \delta(a)$ contradicts the minimal choice of $\delta(a)$.

Hence $r = 0$, so
$$x = qa \in aR$$

So $I \subseteq aR$.

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

so $I = aR$. //

Eg. 1) $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-2}]$, $F[x]$ (F field) are all PIDs.

2) Here is an example of a non-PID:

<u>Claim</u> $\mathbb{Z}[\sqrt{-3}]$ is <u>not</u> a PID.

Pf. For $a, b \in R$ (ring), define
$$aR + bR$$
$$= \{ar_1 + br_2 : r_1, r_2 \in R\}$$

Then $aR+bR$ is an ideal of R

In $R = \mathbb{Z}[\sqrt{-3}]$, define

$$I = \underset{\substack{\uparrow \\ a}}{2}R + (\underset{\substack{\uparrow \\ b}}{1+\sqrt{-3}})R$$

<u>Subclaim</u> I is not a principal ideal of R.

Pf. First observe that for $x, y \in \mathbb{Z}$,

$$x + y\sqrt{-3} \in I \Rightarrow x \equiv y \bmod 2$$

(Ex.) [In particular, this shows that $I \neq R$].

Suppose ~~that~~ I is principal, say

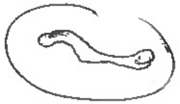
$$I = aR$$

where $a = x + y\sqrt{-3} \in R$.

Then $\exists\, r, s \in R$ s.t.

$$\underline{2 = ar, \quad 1+\sqrt{-3} = as}$$ 

Taking $(\text{modulus})^2$ of both sides, get

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

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

Now

$$|a|^2 = x^2 + 3y^2$$

By , this divides 4.

It can't be 2, so

$$|a|^2 = 1 \text{ or } 4.$$

If $|a|^2 = 1$ then $x = \pm 1, y = 0$

so $a = \pm 1$ and $I = aR = R$ $\#$

Therefore $|a|^2 = 4$.

By , this implies

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

$$r, s = \pm 1.$$

By  this implies

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

Therefore I is non-principal

25 Maximal ideals

Let R be an ID, and I an ideal of R.

Qn When is the quotient ring R/I a *field*?

Defn I is a *maximal* ideal of R if

1) $I \neq R$, and

(2) If J is an ideal s.t.

$$I \subsetneqq J \subseteq R$$

then $J = R$.

Answer to qn:

Thm 25.1 $\frac{R}{I}$ is a field iff I is a maximal ideal of R.

Pf. Later. (Sec 27).

Maximal ideals in PID's:

These are very easy to classify:

Prop 25.2 Let R be a PID and let $0 \neq a \in R$. Then the ideal aR is a maximal ideal iff a is an irreducible elt. of R.

Eg. In $\mathbb{Z}$ (a PID), max ideals are $p\mathbb{Z}$ (p prime)

In $R = F[x]$, max. ideals are $p(x)R$, where $p(x)$ is an irreducible poly.

Pf ($\Rightarrow$) Suppose $I = aR$ is maximal. Let

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

Then $a \in bR$, so

$$aR \subseteq bR \leq R$$

hence (as aR maxl),

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

If $bR = R$ then b is a <u>unit</u>.

If $bR = aR$ then

$$a = bc, \quad b = ad$$

(some $d \in R$). Hence

$$a = bc = adc$$

$\Rightarrow$ $cd = 1$ (as R is ID)

$\Rightarrow$ c a unit.

Hence b or c is a unit, proving a irreducible.

($\Leftarrow$) Suppose $a \in R$ is irreducible. Let J be an ideal s.t.

$$aR \subsetneq J \subseteq R.$$

As R is a PID, $\exists\, d \in R$ s.t.

$$J = dR.$$

As $a \in J$, $\exists\, e \in R$ s.t.

$$a = de.$$

Now a is irreducible, so

d or e is a unit.

If e a unit, then

$$aR = deR = dR = J$$

Hence d is a unit and so

$$J = dR = R.$$

So aR is a maximal ideal.

Friday 6th December

Corollary 26.3 Let R be a principal ideal domain (PID). Let $a \in R$ be an irreducible element. Then R/aR is a field.

Proof 26.2 says that aR is a maximal ideal. 26.1 says that the quotient ring by a max. ideal is a field. ∎

Example $R = \mathbb{Q}[x]$ $a = x^2+1$

Then $\mathbb{Q}[x]/(x^2+1)\mathbb{Q}[x]$ is a field.

We'll seen soon that this field is $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$

It is the set $\{a + b\sqrt{-1} \mid a, b \in \mathbb{Q}\}$.

27. Finite fields

We know $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p$ is an example of a finite field.

Example $R = \mathbb{Z}_2[x]$ $a = x^2+x+1$ $I = aR$

This is an irreducible polynomial.

Then ~~*~~ let's call $F = \mathbb{Z}_2[x]/(x^2+x+1)\mathbb{Z}_2[x]$

The elements of F are the cosets

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

Write $\alpha = I + x$. Then $F = \{0, 1, \alpha, \alpha+1\}$.

We have $\boxed{\alpha^2 + \alpha + 1 = 0}$

$$\alpha^2 = (I + x)(I + x) = I + x^2 = I + x + 1 = \alpha + 1$$

(because $x^2 - x - 1 = x^2 + x + 1 = 0$ in R/I)

Thus F contains four elements

$(F, +)$

$+$	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

$(F, \times)$

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

$$(\alpha+1)^2 = \alpha^2 + 1 = \alpha \qquad \alpha(\alpha+1) = \alpha^2 + \alpha = 1$$

Prop. 27.1 Let F be a field. Let $p(x)$ be an irreducible polynomial of degree $n \geq 1$. Let I be the ideal $p(x)F(x)$. Let $F_0 = F[x]/I$.

Then we have the following statements:

1) F_0 is a field
2) $F_0 = \{ I + r(x) \mid r(x) \in F[x],\ \deg r(x) \leq n-1 \}$
3) If $F = \mathbb{Z}_p$, then $|F_0| = p^n$.
4) Write $\alpha = I + x \in F_0$. Then $p(\alpha) = 0$ in F_0.
5) The map $\varphi : F \to F_0$ sending a to $I + a$ is an injective homomorphism.

<u>Proof</u> (1) $p(x)$ is irreducible $\Rightarrow$ I is maximal

$\Rightarrow F_0$ is a field by 26.3.

(2) Let $I + f(x)$ be any element in F_0

A priori $f(x)$ is any polynomial in $F[x]$.

$$f(x) = q(x)\,p(x) + r(x) \quad , \quad r(x) \text{ is zero or } \deg r(x) \leq n-1.$$

Hence $I + f(x) = I + r(x)$

Such a representative is unique.

(3) $|F_0|$ equals the number of polynomials of degree $\leq n-1$ $\quad a_0 + a_1 x + \dots + a_{n-1} x^{n-1}$

$a_i \in F$, so there are p^n such polynomials.

Hence $|F_0| = p^n$.

(4) $p(\alpha) = I + p(x) = I$. This is $0 \in R/I$.

but $p(x) \in I$

(5) $\varphi(a) = I + a \qquad \varphi(b) = I + b$

$a \in F \qquad \varphi(a+b) = I + (a+b) = (I+a) + (I+b)$

$\varphi(ab) = I + ab = (I+a)(I+b)$ So φ is a homomorphism

Suppose $\varphi(a) = I + a = I \Leftrightarrow a \in I$. This implies that $a = p(x)\,f(x)$ for some $f(x) \in F[x]$.

a is a polynomial of degree 0, whereas $\deg(p(x) f(x)) \geq \deg(p(x)) = n$. ($n \geq 1$ otherwise $p(x)$ is a constant but then it's not an irreducible.) $\blacksquare$

Cor. 27.2. Let F be a field, $p(x) \in F[x]$ an irreducible polynomial. Then there exists a field F_0 containing F and such that $p(x)$ has a root in F_0.

Example $F = \mathbb{Z}_2 = \{0, 1\}$. $p(x) = x^3 + x + 1$

This is irreducible. Hence by 27.1(3) we have a field with 8 elements:

$$F_8 = \mathbb{Z}_2[x] / (x^3 + x + 1)\mathbb{Z}_2[x]$$

$$\alpha = I + x \Rightarrow \alpha^3 + \alpha + 1 = 0$$

Calculations in F_8: $\alpha^2(\alpha^2 + 1) = \alpha^4 + \alpha^2 = \alpha$

$$\alpha^4 + \alpha^2 + \alpha = 0$$

Remark This can be done for any prime p. So we can construct field with p^2 and p^3 elements.