Alg-26

H & K are two subgroups of a finite group G.

Assume $(|H|, |K|) = 1$

$\Rightarrow H \cap K = \{e\}$

$x \in H \cap K \Rightarrow x^{|H|} = e = x^{|K|}$

e is unique

$\Rightarrow x = e$

$H \cap K$ is a subgroup of H & a subgp of K

$|H \cap K| \mid |H|$ and

$|H \cap K| \mid |K|$

$\Rightarrow |H \cap K| = 1$

Prob $(|H|, |K|) = 1$

$\Rightarrow |H \cap K| = 1 \Rightarrow$

$H \cap K = \{e\}$

Def

R is a rng (need not be commutative) and has identity.

$\phi \neq J \subseteq R$

(1) J is a left ideal of R iff

(i) $a - b \in J \quad \forall a, b \in J$

(ii) $ra \in J, \quad \forall r \in R, a \in J$

(2) J is a right ideal of R

iff (i) $a - b \in J \quad \forall a, b \in J$

(ii) $ar \in J \quad \forall a \in J$ and $\forall r \in R$

(3) J is two-sided or simply an ideal iff it is both a left ideal and a right ideal.

Note. In a commutative ring R with 1

Note. In a commutative ring R every left ideal is also a right ideal, hence two sided ideal of the ring R.

Ex 1- $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}$ are commutative rings with 1.

2- $M_{n\times n}(K) = R$ is a ring with $1_R = I_n$

Ex $n \in \mathbb{N}$, $n\mathbb{Z} \subseteq \mathbb{Z}$ is an ideal of $\mathbb{Z}$. And have seen that any $I \neq \{0\}$ of $\mathbb{Z}$, $\exists\, n \in \mathbb{N}\setminus\{0\}$ s.t. $I = n\mathbb{Z}$.

Let I, J are two ideals of a commutative ring R with 1.

1- $I + J \overset{\text{def}}{=} \{a + b : \forall\, a \in I$ ...

$$LM \overset{\text{def}}{=} \left\{ \sum_{i=1}^{n} a_i b_i : \forall n \in \mathbb{N} \; \forall a_1 \ldots a_n \in L \; \& \; b_1 \ldots b_n \in M \right\}$$

$$L+M = \{ l+m \in R : l \in L, m \in M \}$$

then LM & $L+M$ are ideals of R

Note: two sided ideal of a ring with 1 correspond to normal subgroup of a group.

FACT. Let I_α be a left (right, two sided) ideal of a ring R with 1 for each $\alpha \in I \neq \emptyset$. Then

$J = \bigcap_{\alpha \in} I_\alpha$ is a left (right, two sided) ideal of R.

Prop Let R be a ring with 1. $S \subseteq R$. Then there is a [illegible] containing S s.t.

$S \subseteq R$. The ... left ideal J containing S s.t. if J_1 is another left ideal containing S, then $J \subseteq J_1$

i.e. there is a smallest left ideal J containing S

$J = (S)$, S is called a set of generators of J

$S = \phi$, $J = \{0\}$

Ex $S = \{a_1 \dots a_n\} \subseteq R$, $|S| = n$

$L = \{r_1 a_1 + r_2 a_2 + \dots + r_n a_n : r_1 \dots r_n \in R\}$

Then L is a left ideal of R and $a_1 \dots a_n$ are generators of L

write $L = (a_1 \dots a_n)_l$ — left ideal generated $S = \{a_1 \dots a_n\}$

$L = (a_1, \ldots a_n)_r$, right ideal

$L = (a_1, \ldots a_n)$. two-sided ideal

Def R is a commutative ring with 1
L is an ideal of R. L is called
a principal ideal iff $L = (a)$,
i.e. L is generated by a single
element of R.

Def. A commutative ring R with 1
is called a principal ideal
ring iff every ideal is
principal ideal

Def. An integral domain R is
called a principal ideal
domain (PID) iff every ideal
of R is principal ideal of R

Ex. $\mathbb{Z}$ is an integral domain

Ex 1. $\mathbb{Z}$ is an integral domain

$I \subseteq \mathbb{Z}$ is an ideal, $\Rightarrow \exists n \in \mathbb{N}$ s.t. $I = n\mathbb{Z} = (n) = \{nm : m \in \mathbb{Z}\}$

- $\mathbb{Z}[t]$ is an integral dom
- $\mathbb{Z}[i]$ - - - -
- $\mathbb{Z}/p\mathbb{Z}$ - - - for p prime

- $\mathbb{Z}/p\mathbb{Z}$ is a field $\equiv \mathbb{F}_p$ a finite field $|\mathbb{F}_p| = p$

Def Let R & R' be two rings

$f : R \to R'$ is a ring homo

if (1) $f(a+b) = f(a) + f(b)$

(2) $f(ab) = f(a) f(b)$

iff (1) $f(a+b) = f(a) + f(b)$

(2) $f(ab) = f(a) f(b)$

If R & R' have identities 1_R & $1_{R'}$ respectively, then, in addition, we require

$$f(1_R) = 1_{R'}$$

Prop $\ker f = \{ a \in R : f(a) = 0_{R'} \}$ is a two sided ideal of R

$a, b \in \ker f$, $r \in R$, then

$f(a-b) = f(a) - f(b) = 0 - 0 = 0$

$\Rightarrow a - b \in \ker f$

$f(ra) = f(r) f(a) = f(r) 0 = 0$

& $f(ar) = f(a) f(r) = 0 f(r) = 0$

$\Rightarrow ar, ra \in \ker f$.

$f(R)$ is a subring of R'

$\supset$ under f.

$f(R)$ is a ... of R under f.
(image of R under f.)

Let R be a ring & let M be a two sided ideal of R
for $a, b \in R$, define $a \equiv b \bmod M$
or $a \underset{M}{\sim} b \iff a - b \in M$

Then $\underset{R}{\sim}$ or $\equiv$ is an equivalence rel on R.

(1) $a \equiv a \bmod M$
(2) $a \equiv b \bmod M \Rightarrow b \equiv a \bmod M$
(3) $a \equiv b \bmod M$, $b \equiv c \bmod M$
$\Rightarrow a \equiv c \bmod M$
(4) $a \equiv a' \bmod M$, $b \equiv b' \bmod M$
then (i) $a + a' \equiv b + b' \bmod M$
(ii) $aa' \equiv bb' \bmod M$
(5) $a \equiv b \bmod M$ & $c \in R$
then $ac \equiv bc \bmod M$ & $ca \equiv cb \bmod M$

then $ac \equiv bc \bmod M$ $\Rightarrow$ $a \equiv b \bmod M$

$\bar{R} = \{\bar{a} : a \in R\}$ where

$\bar{a} = [a] = \{b \in R : b \equiv a \bmod M\}$

$= a + M$, called coset

of M in $\bar{R}$

$\bar{R} = R/M$

Thm M is a two-sided ideal of R with 1, then R/M is a ring

$(a+M)+(b+M) = \bar{a}+\bar{b} \overset{\text{def}}{=} \overline{a+b}$

$= a+b+M$

sum

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

Moreover (i) R/M has identity $1_R + M$ if R has 1_R, always

$1_{R/M} = 1_R + M.$

(ii) R is commutative with 1_R
then R/M is commutative

$$\begin{aligned}(a+M)(b+M) &= ab+M \\ &= ba+M \\ &= (b+M)(a+M)\end{aligned}$$

$\Rightarrow R/M$ is commutative

$\mathbb{Z}/n\mathbb{Z}$ in mind for quotient or factor ring

Thm. Let R & R' be rings with 1_R & $1_{R'}$ respectively & $f: R \to R'$ a ring homo. Then there is ring homo $\bar{f}: R/\ker f \longrightarrow f(R)$ which is an iso of rings

Proof $\bar{f}(a+\ker f) = f(a)$

Proof $\bar{f}(a+\ker f) = f(a)$

$a+\ker f = b+\ker f \Rightarrow a-b \in \ker f$

$\Rightarrow f(a-b) = 0$

$\Rightarrow f(a) = f(b)$

well defined.

$\bar{f}\left((a+\ker f)+(b+\ker f)\right)$

$= f(a+b+\ker f) = f(a+b)$

$= f(a)+f(b)$

$= \bar{f}(a+\ker f) + \bar{f}(b+\ker f)$

$R \xrightarrow{\pi} R/M$

The map $a \longmapsto a+M$

$\pi(a) = a+M$

π is called the canonical ring homo where M is a two sided ideal of R, a

ring with 1_R

Let R be a ring with $1_R = 1 = e$

Assume $R \neq \{0\}$, $e = 1 \neq 0$

$f : \mathbb{Z} \longrightarrow R$ by

$f(m) = me$

f is a ring homo

(1) $f(r+s) = (r+s)e$
$= re + se$
$= f(r) + f(s)$

(2) $f(rs) = rse$
$= (re)(se)$
$= f(r) f(s)$

(3) $f(1) = e$

me is defined inductively:
$1 \cdot e = e$
$ne \in R$
$(n+1)e = ne + e$
$= e + ne$,

$n = 0$, $0e = 0$
$n < 0$, $ne = (-n)(-e)$

Case 1 $\ker f = \{0\} \Rightarrow R$ has characteristic

Case 1 $\ker f = \{0\} \Rightarrow$ zero characteristic

write $\mathrm{ch}\, R = 0$

$n \cdot e = 0 \Rightarrow n = 0$

Case 2 $\ker f \neq \{0\} \subseteq \mathbb{Z}$

$\| \; n\mathbb{Z}$, $n \in \mathbb{N}$ is smallest element of $\ker f$

$n = \mathrm{ch}\, R$, characteristic of R.

$R = \mathbb{Z}$, $\mathrm{ch}\, \mathbb{Z} = 0$

$R = \mathbb{Z}/m\mathbb{Z}$, $\mathrm{ch}(\mathbb{Z}/m\mathbb{Z}) = m$

$m(1_{\mathbb{Z}/m\mathbb{Z}}) = 0_{\mathbb{Z}/m\mathbb{Z}} = m\mathbb{Z}$

$m(1+m\mathbb{Z})$

$= m + m\mathbb{Z} = m\mathbb{Z} \Rightarrow ch(\mathbb{Z}/m\mathbb{Z})$

$= m.$

$ch(R[x]) = m$ where $R = \mathbb{Z}/m\mathbb{Z}$.

$ch(\mathbb{Z}_2[x]) = 2$, $\boxed{\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}}$

$ch(\mathbb{Z}_p[x]) = p$, p - prime.

$\mathbb{Z}_p \equiv \mathbb{Z}/p\mathbb{Z}$

Note. R is a ring with 1_R

$ch\, R = 0$, then R contains a copy of $\mathbb{Z}$ and hence R is infinite as

$m \longmapsto m1.$

$\mathbb{Z}$ is embedded in R

↑ the homo

"

injective"

2 $\mathrm{ch}R = n > 0$ integer

Then R contains a copy of $\mathbb{Z}_n \equiv \mathbb{Z}/n\mathbb{Z}$

$$\mathbb{Z} \longrightarrow R$$
$$m \longmapsto m\,1.$$

$\ker f = n\mathbb{Z}$

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\ker f \xrightarrow{\sim} f(\mathbb{Z}) \subseteq R$$

1. $\mathbb{Z}_2 \subseteq \mathbb{Z}_2[x]$

Thm R is an integral domain then either $\mathrm{ch}R = 0$ or if $\mathrm{ch}R = n$, then $n = p$, a prime.

proof $n = rs$, $1 < r, s < n$

$0 = n1 = (rs)1 = (r1)(s1) = 0$

$r1 = 0$ or $s1 = 0$

$f: R \to R'$, R & R' are rings

is (1) iso iff f is ring homo & bijection

$\Rightarrow f^{-1}: R' \to R$ is also a ring homo.

(2) $f: R \to R$ is ring auto iff f is iso of ring.

Thm Let G be a cyclic group of order N. (group operation is product)

$(m, N) = 1$, $m \in \mathbb{N}$

$\sigma_m: G \to G$ given by $\sigma_m(x) = x^m$

$\sigma_m \in \mathrm{Aut}(G)$

...

then $\sigma_m \in Aut(G)$

Moreover $\sigma : (\mathbb{Z}/N\mathbb{Z})^* \to Aut(G)$

$\sigma(m) = \sigma_m$ is well def

where $(\mathbb{Z}/N\mathbb{Z})^*$ = the group of units in $\mathbb{Z}/N\mathbb{Z}$

$$= \{ m \in \mathbb{N} : (m, N) = 1 \}$$

$$|(\mathbb{Z}/N\mathbb{Z})^*| = \varphi(N)$$ called

$N = p$, prime, $Aut(\mathbb{Z}_p) \cong (\mathbb{Z}/p\mathbb{Z})^*$

$= \mathbb{Z}_p^* = \mathbb{Z}_p - \{0\}$ is a commutative group under product

$$|Aut(\mathbb{Z}_p)| = p - 1$$

$|\mathbb{Z}_p^*| = p-1$

$a \in \mathbb{Z}_p^* \Rightarrow a^{p-1} = 1$

$a \not\equiv 0 \bmod p \Rightarrow a^p = a \bmod p$

$a \in \mathbb{Z}$ (Fermat's little thm)

$U(\mathbb{Z}/n\mathbb{Z})$ = units in $\mathbb{Z}/n\mathbb{Z}$

$U(R) = \{r \in R : rs = sr = 1\}$

R is a ring with 1

↑

a group called the group of units in R, a ring with 1.

field.

$U(M_{n\times n}(K)) = GL(n, K)$

$U(M_{2\times 2}(\mathbb{Z})) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$

$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2\times 2}(\mathbb{Z})$

$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2\times 2}(\mathbb{Z})$

A is invertible $\iff \det(A) \neq 0$

$\mathbb{Z} \ni ad - bc \neq 0$

$A^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

Def Let R be a commutative ring with $1 \neq 0$

(1) $P \subsetneq R$ is an ideal. P is called a prime ideal of R iff $ab \in P \Rightarrow a \in P$ or $b \in P$

(2) $M \subsetneq R$ ideal of R. M is called a maximal ideal of R iff J is an ideal of R $M \subseteq J$, then $M = J$ or $J = R$

Thm. R is a commutative ring with $1 \neq 0$

(1) P is a prime ideal of R

R/P is an

(1) P is a prime ideal of R $\iff$ R/P is an integral domain

(2) M is a maximal ideal of R $\iff$ R/M is a field

(3) M is maximal $\Rightarrow$ M is prime

$\not\Leftarrow$

FACTS: 1 $f: K \to R$ is ring homo where K is a field & R is a ring. Then f is injective.

2 K is a field & $\mathrm{ch} K = p$, a prime.

Then the map $\varphi_p : K \to K$ s.t. $\varphi(a) = a^p$

defn' $\varphi_p(a) = a^p$
is an auto

hmm $\varphi_p(a+b) = \varphi_p(a) + \varphi_p(b)$

$(a+b)^p = a^p + b^p$

$(ab)^p = a^p b^p$ (!)

Freshman's dream thm. → in 1981