M2PM2 Algebra II

3/10/19

<u>Webpage</u>: Me (M. Liebeck)

Will upload all lecture notes, sheets, but <u>not</u> solutions.
(Solutions handed out at lectures).

Recommended books on webpage

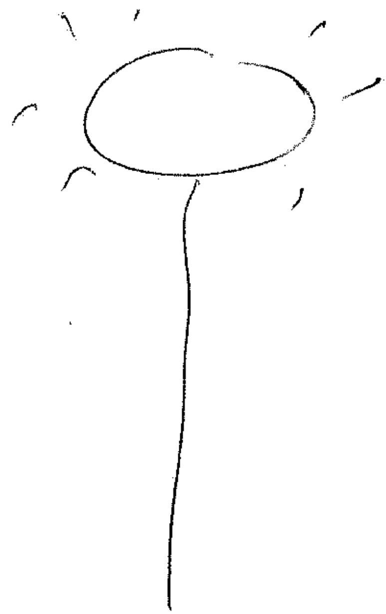
<u>Office hour</u> Tuesday 12.00
(Room 665).

<u>Algebra I</u>: Groups
Linear Alg.
Rings

Algebra II

1) More groups
2) More linear alg.
3) More rings.

Highlights from course:



2) <u>Linear alg highlight</u>

Recall: $n \times n$ matrix A is **diagonalisable** if $\exists$ invertible matrix P s.t.

$$P^{-1}AP = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}.$$

Highly desirable.

But many matrices are not diagonalisable, eg.

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

[Pf: evalues are 1, 1, so if A is diagble then $\exists P$ s.t.

$$P^{-1}AP = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$$

Then $A = PIP^{-1}$

$= I$ ⨳].

Substitute for diagonalisation:

Jordan Canonical Form Theorem

For any $n \times n$ matrix A over $\mathbb{C}$, $\exists$ invertible P s.t.

$$P^{-1}AP = \begin{pmatrix} \boxed{\begin{matrix} \lambda_1 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda_1 \end{matrix}} & & & \text{\Large 0} \\ & \boxed{\begin{matrix} \lambda_2 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda_2 \end{matrix}} & & \\ \text{\Large 0} & & \ddots & \end{pmatrix}$$

This is the <u>unique</u> JCF of the matrix A (apart from swapping the order of the blocks).

(1) Groups

Recall examples of groups from Algebra I :

A) Number systems :

$(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$,

$(\mathbb{Q}^*,\times)$ $(\mathbb{Q}^* = \mathbb{Q}\setminus 0)$

$(\mathbb{Z}_n,+)$ $(\mathbb{Z}_n = \{[0],[1],\dots[n-1]\}$, with addition modulo$)$

$(\mathbb{Z}_p^*,\times)$ (p prime)

(B) Symmetric group S_n, group of all permutations of $\{1,\dots,n\}$

General linear group

$GL(n,\mathbb{C})$, group of all invertible $n\times n$ matrices over $\mathbb{C}$

Cyclic groups:

Finite: $C_n = \{z \in \mathbb{C} : z^n = 1\}$

$= \{1, \omega, \omega^2, \ldots, \omega^{n-1}\}$

$(\omega = e^{2\pi i/n})$

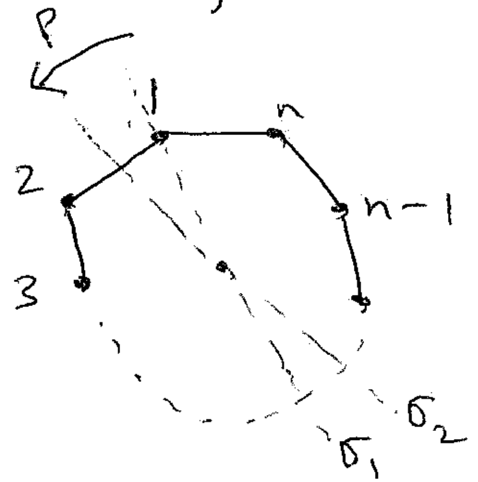
$= \langle \omega \rangle.$

Infinite: $(\mathbb{Z}, +) = \langle 1 \rangle$,

infinite cyclic.

Dihedral groups

D_{2n} = symmetry group of regular n-gon



Elts of D_{2n}:

n rotations: $e, \rho, \rho^2, \ldots, \rho^{n-1}$

n reflections: $\sigma_1, \sigma_2, \ldots, \sigma_n$

Highlights:

1) More examples:

<u>Alternating groups</u> A_n

(subgroup of S_n)

<u>Finite general linear groups</u>

$GL(n, \mathbb{Z}_p)$

2) Classification of "small" groups, i.e. groups of order ≤ 15.

3) "<u>Structure theory</u>" of groups:

given a "normal" subgp N of G, can define the <u>factor group</u> $\frac{G}{N}$.

If G has no normal subgps, say G is a <u>simple</u> group.

Examples of simple groups:

C_p, A_n, ...

(3) Rings

Ring is $(R, +, \times)$ with axioms

Field is a ring where $(R^*, \times)$ form an abelian group

Some fields: $\mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}_p$

Rings (not fields):

$$\mathbb{Z}$$

Poly. ring $F[x]$, ring of polys. over a field F

$$\mathbb{Z}[i] = \{a+bi : a, b \in \mathbb{Z}\}$$

Motivating example

Consider the **Diophantine equation**: fix $k \in \mathbb{Z}$, eqn.

$$x^2 - y^3 = k$$

to be solved for $x, y \in \mathbb{Z}$.

Called **Mordell's eqn**.

<u>Eg 1</u>: Let $\underline{K=1}$. Eqn is

$$x^2 - y^3 = 1.$$

Some solns: $x, y = 0, -1$

$\pm 1, 0$

$\pm 3, 2$

$\vdots$

Can we find all solns?

<u>Soln</u> Rewrite as

$$y^3 = x^2 - 1$$
$$= (x+1)(x-1).$$

<u>Suppose x even</u>:

Then $x+1$, $x-1$ are odd so

$$\text{hcf}(x+1, x-1) = 1.$$

So the product of two coprime integers $x+1$, $x-1$ is the cube y^3.

By <u>unique prime factn</u> for the ring $\mathbb{Z}$ this implies both $x+1$ and $x-1$ are cubes: so

$$x+1 = m^3$$
$$x-1 = n^3 \qquad (m, n \in \mathbb{Z}).$$

So $m^3 - n^3 = 2$. List of cubes

$$\ldots -27, -8, -1, 0, 1, 8, \ldots$$

Only poss. is

$$m^3 = 1, \quad n^3 = -1.$$

Hence only soln. of

with x even is

$$\underline{x = 0, \quad y = -1}$$

Case x odd... more complicated.

Eg 2 $k = -1$: eqn

$$x^2 - y^3 = -1.$$

Cleverly rewrite:

$$y^3 = x^2 + 1$$
$$= (x+i)(x-i),$$

fact. in the ring $\mathbb{Z}[i]$.

To solve as before, need unique fact. property for the ring $\mathbb{Z}[i]$.

4/10/19

Chapter 1: Groups

1. Isomorphism

Eg. Let $G = C_2 = (\{1,-1\}, \times)$ and $H = S_2 = \{e, a\}$ (where $a = (1\,2)$).

Mult. tables:

G

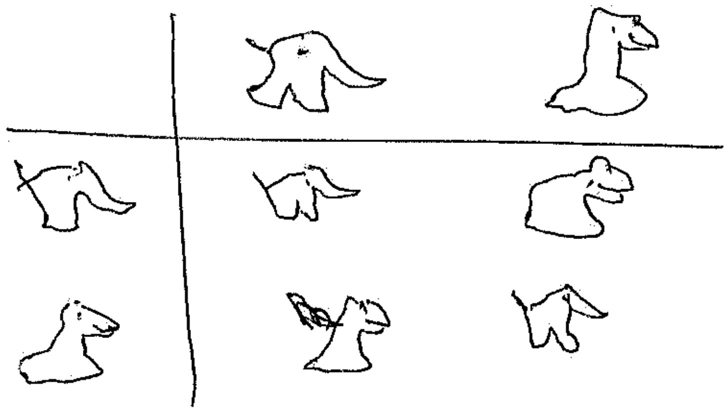
	1	-1
1	1	-1
-1	-1	1

H

	e	a
e	e	a
a	a	e

Tables are identical, except that the elements have different labels.

Another group K:



In these examples, $\exists$ bijection $\phi : G \to H$ s.t. if $g_1 \xrightarrow{\phi} h_1$, $g_2 \xrightarrow{\phi} h_2$ then $g_1 g_2 \xrightarrow{\phi} h_1 h_2$

<u>Defn</u> Let G, H be groups. Say $\phi : G \to H$ is an <u>isomorphism</u> if

1) ϕ is a bijection
2) $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$ $\forall g_1, g_2 \in G$.

If $\exists$ isomorphism $\phi : G \to H$, we say G is <u>isomorphic</u> to H, and write

$$G \cong H.$$

Eg. $C_2 \cong S_2$

<u>Remark</u> The relation on all groups:

$$G \sim H \iff G \cong H$$

is an equivalence relation

ie.

- $G \cong G$
- $G \cong H \Rightarrow H \cong G$
- $G \cong H,\ H \cong K \Rightarrow G \cong K$

(Qn on Sheet 1).

<u>Question</u>: Given two groups G, H how can we tell whether they are isomorphic?

Often very hard.

Here's our strategy:

a) If you think $G \not\cong H$ try to prove it using <u>Prop. 1.1</u> below.

b) If you think $G \cong H$, try to find an isomorphism $\phi: G \to H$.

<u>Recall</u> In group theory, we use the word "order" in two ways:

- the <u>order</u> of a group G is $|G|$, the no. of elts of G
- the <u>order</u> of an element $x \in G$ is the smallest positive integer k s.t. $x^k = e$. Write as
  $o(x)$.

<u>Prop 1.1</u> Let G, H be gps.

1) If $|G| \neq |H|$ then $G \ncong H$.

2) If G is abelian and H is non-abelian, then $G \ncong H$.

3) Suppose $\exists\, k \in \mathbb{N}$ s.t. G and H have different numbers of elts of order k. Then $G \ncong H$.

Before proof ~~of~~ of this, some examples of how it can be applied.

<u>Eg.</u> a) Is C_8 isomorphic to D_8?

<u>Ans</u> Both have order 8, so 1.1(1) does not apply. However C_8 is abelian, but D_8 is not ($\rho\sigma_1 \neq \sigma_1\rho$). So by 1.1(2),

$$C_8 \ncong D_8.$$

b) Is D_8 isomorphic to S_4?

<u>Ans</u> $|D_8| = 8$, $|S_4| = 24$,

so $D_8 \ncong S_4$ by 1.1(1).

c) Is S_4 isomorphic to D_{24}?

<u>Ans</u> Both have order 24

and are non-abelian (so 1.1(1) & 1.1(2) don't apply).

We apply 1.1(3) taking

$K = 12$.

No. of elts of order 12

in S_4 is $\underline{\underline{0}}$

[cycle-shapes e, (12), (123), (1234), $(12)(34)$, orders $1, 2, 3, 4, 2$]

No. of elts of order 12

in D_{24} is > 0

(eg. $o(\rho) = 12$).

Hence by 1.1(3),

$$S_4 \ncong D_{24}.$$

d) Let

$G = S_3$, all perms. of $\{1,2,3\}$

$H = D_6$, symmetry gp of $\triangle$

Is $G \cong H$?

Well,

$|G| = |H| = 6$ so 1.1(1) doesn't apply

G & H are non-abelian so 1.1(2) doesn't apply

Elts of D_6:

	e	ρ	ρ^2	σ_1	σ_2	σ_3
order	1	3	3	2	2	2

Elts of S_3:

e	(123)	(132)	(12)	(13)	(23)
1	3	3	2	2	2

So D_6, S_3 have same nos. of elts of each order.

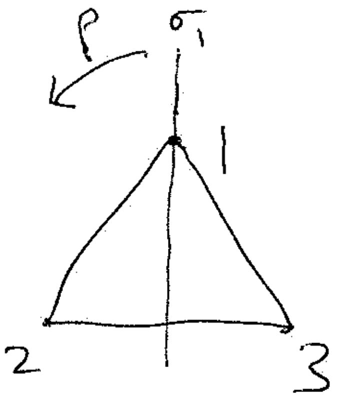
So 1.1(3) doesn't apply.

Just because 1.1. doesn't apply does <u>not</u> imply $G \cong H$. But it perhaps suggest this might be true...

<u>Claim</u> $D_6 \cong S_3$.

<u>Pf.</u> Define

$$\phi : D_6 \to S_3$$



to send each symmetry in D_6 to the perm. of the corners 1, 2, 3 it gives.

So

$$\phi : \quad e \to e$$
$$\rho \to (1\,2\,3)$$
$$\rho^2 \to (1\,3\,2)$$
$$\sigma_1 \to (2\,3)$$
$$\sigma_2 \to (1\,3)$$
$$\sigma_3 \to (1\,2).$$

Then ϕ is a bijection and

$$\phi(g_1 g_2) = \phi(g_1)\phi(g_2) \quad \forall g_1, g_2 \in D_6$$

Since the binary ops. in G and H are both composition of functions.

Hence

$$D_6 \cong S_3.$$

<u>Proof of Prop 1.1</u>

Need

<u>Lemma 1.2</u> If $\phi : G \to H$ is a isomorphism, then

$$\phi(e_G) = e_H.$$

<u>Pf</u> Now

$$e_G e_G = e_G.$$

So

$$\phi(e_G) = \phi(e_G e_G)$$
$$= \phi(e_G)\,\phi(e_G).$$

So if we write $h = \phi(e_G)$, then

$$h = h^2.$$

Hence

$$h^{-1}h = h^{-1}h^2$$

so $$e_H = h = \phi(e_G).$$ //

<u>Pf. of Prop 1.1</u>

1) Obvious. If $|G| \neq |H|$, then there cannot be a bijection $G \to H$, so $G \not\cong H$.

2) We show

<u>if G is abelian and $G \cong H$, then H is abelian.</u>

So suppose G abelian, & $G \cong H$. Let $h_1, h_2 \in H$, and $\phi : G \to H$ isomorphism.

As ϕ bijection, $\exists\, g_1, g_2 \in G$ s.t

$$h_1 = \phi(g_1), \quad h_2 = \phi(g_2).$$

So

$$\begin{aligned} h_2 h_1 &= \phi(g_2)\phi(g_1) \\ &= \phi(g_2 g_1) \\ &= \phi(g_1 g_2) \quad \text{as } G \text{ abelian} \\ &= \phi(g_1)\phi(g_2) \\ &= h_1 h_2. \end{aligned}$$

Hence H abelian.