8/10/19

Prob. Sheet 1 : paper copy + website.

Proof of Prop 1.1 (3)

Fix $n \in \mathbb{N}$. Define

$$G_n = \{x \in G : o(x) = n\},$$

$$H_n = \{y \in H : o(y) = n\}.$$

We'll prove

$$G \cong H \Rightarrow |G_n| = |H_n|.$$

(This implies (3)).

Let $\phi : G \to H$ be an isomorphism.

Claim ϕ sends $G_n \to H_n$.

Pf. Let $x \in G_n$. This means

$$x^n = e_G$$

and

$$x^i \neq e_G \text{ for } 1 \leq i \leq n-1$$

Now for $i \geq 1$,

$$\phi(x^i) = \phi(\overbrace{x\,x\ldots x}^{i})$$

$$= \phi(x)\,\phi(x)\ldots\phi(x)$$

$$= \phi(x)^i.$$

Hence

$$\phi(x)^k = \phi(x^k)$$

$$= \phi(e_G)$$

$$= e_H \quad \text{(by 1.2)}$$

and for $1 \leq i \leq k-1$,

$$\phi(x)^i = \phi(x^i)$$

$$\neq \phi(e_G)$$

(as $x^i \neq e_G$ and ϕ is injective)

Hence

$\phi(x)$ has order k

So

ϕ sends $G_k \to H_k$,

as claimed.

Since ϕ is injective,

this implies

$$|H_n| \geq |G_n|.$$

Also ϕ^{-1} is an isomorphism $H \to G$ (see your (brilliant) solution to sheet 1, Q3),

so ϕ^{-1} sends $H_n \longrightarrow G_n$.

Hence also

$$|G_n| \geq |H_n|.$$

Therefore $|G_n| = |H_n|$. ✓

Cyclic groups

Prop 1.3

1) If G is a cyclic group of order n, then

$$G \cong C_n.$$

2) If G is an infinite cyclic group, then

$$G \cong (\mathbb{Z}, +).$$

Remark This prop. says that if we count isomorphic groups as being the same, then there is only one cyclic group of each order. We say: up to isomorphism, the only cyclic groups are C_n and $(\mathbb{Z}, +)$.

Proof of Prop 1.3

1) Let $G = \langle x \rangle$ be a cyclic group of order n. Then

$$G = \{e, x, x^2, \ldots, x^{n-1}\}$$

where $x^n = e$.

Recall

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

where $w = e^{2\pi i/n}$ (so $w^n = 1$)

Define $\phi : G \to C_n$ by

$$\phi(x^j) = \omega^j \quad \forall j.$$

Then ϕ is a bijection and

$$\begin{aligned}\phi(x^i x^j) &= \phi(x^{i+j}) \\ &= \omega^{i+j} \\ &= \omega^i \omega^j \\ &= \phi(x^i)\phi(x^j).\end{aligned}$$

Hence ϕ is an isomorphism, so $G \cong C_n$.

2) Let $G = \langle x \rangle$ be an infinite cyclic group, so $o(x) = \infty$ and

$$\begin{aligned}G &= \{x^n : n \in \mathbb{Z}\} \\ &= \{\ldots, x^{-2}, x^{-1}, e, x, x^2, \ldots\}\end{aligned}$$

Define $\phi : G \to (\mathbb{Z}, +)$ by

$$\phi(x^n) = n \quad \forall n \in \mathbb{Z}.$$

Ex: ϕ is an isomorphism, so $G \cong (\mathbb{Z}, +)$. //

2. Groups of permutations

Aim to define the alternating groups A_n (subgroups of S_n).

Key is to define "even" and "odd" permutations.

Eg. $n = 3$

Let x_1, x_2, x_3 be variables and define polynomial

$$\triangle = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$$

Let each permutation in S_3 permute the variables x_1, x_2, x_3 in the same way it permutes $1, 2, 3$.

Eg. Permutation $(1\ 3)$ sends

$$x_1 \to x_3$$
$$x_2 \to x_2$$
$$x_3 \to x_1$$

We apply the perms. in S_3 to the poly. Δ.

Eg. a) (13) sends

$$\Delta \longrightarrow (x_3-x_2)(x_3-x_1)(x_2-x_1)$$
$$= -\Delta.$$

b) (123) sends

$$\Delta \longrightarrow (x_2-x_3)(x_2-x_1)(x_3-x_1)$$
$$= +\Delta.$$

Each perm. in S_3 will send $\Delta \to \pm\Delta$.

Those sending $\Delta \to \Delta$ we call <u>even</u> perms, and those sending $\Delta \to -\Delta$ <u>odd</u> perms.

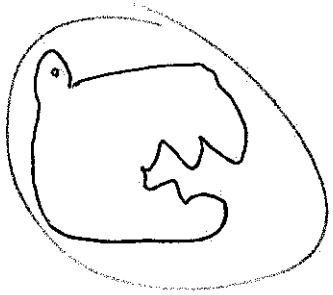
Eg. In S_3, <u>(12), (13), (23) are odd</u> <u>e, (123), (132) are even</u>

General defn. for S_n $(n \geq 2)$

Let $x_1, \ldots, x_n$ be variables and define poly

$$\Delta = \prod_{i<j} (x_i - x_j)$$

$$= (x_1 - x_2)(x_1 - x_3) \cdots (x_1 - x_n)$$
$$\times (x_2 - x_3) \cdots (x_2 - x_n)$$
$$\times \quad \vdots$$
$$(x_{n-1} - x_n)$$



Let each perm. $g \in S_n$ permute the variables $x_1, \ldots, x_n$ in the same way it permutes $1, \ldots, n$.

[Formally,

$$g : x_i \longrightarrow x_{g(i)} \quad \forall i \,].$$

Every $g \in S_n$ sends

$$\Delta \longrightarrow \pm \Delta.$$

Defn For $g \in S_n$, the signature of g, written $s(g)$ is the number ± 1 such that

$$g(\Delta) = s(g)\Delta.$$

Call g an even perm if $s(g) = +1$, and an odd perm if $s(g) = -1$.

Eg. Let $g = (125)(713)(86) \in S_{13}$

What is $s(g)$?

Aim: to easily compute $s(g)$ for any $g \in S_n$.

Key:

Prop 2.1

1) For any $x, y \in S_n$,

$$s(xy) = s(x)\,s(y)$$

2) $s(e) = +1$ and

$$s(x^{-1}) = s(x) \quad \forall x \in S_n.$$

3) For any 2-cycle (ij),

$$s(ij) = -1.$$

10/10/19

Proof of Prop 2.1

1) By defn, $x(\Delta) = s(x)\Delta$.

So

$$xy(\Delta) = x(s(y)\Delta)$$
$$= s(y) \cdot x(\Delta)$$
$$= s(y)s(x)\Delta$$

Also by defn

$$xy(\Delta) = s(xy)\Delta$$

Hence

$$s(xy) = s(y)s(x)$$
$$= s(x)s(y).$$

2) As $e(\Delta) = \Delta$,

$$s(e) = +1.$$

Hence

$$1 = s(e) = s(xx^{-1})$$
$$= s(x)s(x^{-1}) \quad \text{by (1)}$$

Hence $s(x^{-1}) = s(x)$.

(3) Let $t = (ij)$, and assume $i < j$.

We list the terms in Δ (expression) that

t sends to terms $(x_r - x_s)$ with $r > s$: these are

$$x_i - x_j,$$

$$x_i - x_{i+1}, \cdots, x_i - x_{j-1}$$

$$x_{i+1} - x_j, \cdots, x_{j-1} - x_j$$

Total number of these terms is

$$2(j-i-1)+1,$$

which is odd. Hence

$$t(\Delta) = -\Delta.$$

Therefore $s(t) = s(ij) = -1$.

Recipe for computing $s(x)$ for an arbitrary perm. x:

1) express x as a product of 2-cycles

2) use part (1) of 2.1.

For part (1):

Prop 2.2 Let c be an r-cycle in S_n, say

$$c = (a_1 a_2 \dots a_r)$$

Then c can be expressed as a product of $r-1$ 2-cycles.

Pf. Check

$$c = (a_1 a_r)(a_1 a_{r-1}) \cdots (a_1 a_2)$$

since RHS sends

$$a_1 \longrightarrow a_2 \longrightarrow a_3 \longrightarrow \cdots$$

$$\longrightarrow a_r \longrightarrow a_1. \quad //$$

Corollary 2.3 Every elt. x of S_n can be expressed as a product of 2-cycles.

Pf. We know

$$x = c_1 \cdots c_m,$$

a product of disjoint cycles $c_1, \ldots, c_m$. By 2.2, each c_i is a product of 2-cycles. //

Cor. 2.4 If $c = (a_1 \ldots a_r)$ is an r-cycle, then the signature

$$s(c) = (-1)^{r-1}$$

Pf. By 2.2, can express

$$c = t_1 \cdots t_{r-1}$$

where each t_i is a 2-cycle. Then ✡

$$s(c) = s(t_1) \ldots s(t_{r-1})$$

(by 2.1(1))

$$= (-1)^{r-1} \quad \text{(by 2.1(3))}.$$

//

Finally:

<u>Prop. 2.5</u> Let $x \in S_n$,

and let

$$x = c_1 \cdots c_m,$$

a product of disjoint cycles $c_1, \ldots, c_m$ of lengths $r_1, \ldots, r_m$. Then

$$s(x) = \prod_{i=1}^{m} (-1)^{r_i - 1}$$

Pf. ~~[illegible]~~

By 2.1(1)

$$s(x) = \prod_{i=1}^{m} s(c_i)$$

$$\overset{2.4}{=} \prod (-1)^{r_i - 1}.$$

//

Using this result, can ~~work~~ compute $s(x)$ in our little heads for any perm. x.

Ex. $x = (1\ 3\ 9\ 2)(4\ 5\ 7)(6\ 8)$ in S_n.

Then
$$s(x) = +1$$

A major reason for this theory is

Defn Define

$$A_n = \{x \in S_n : s(x) = +1\},$$

the set of all even perms in S_n.

Prop. 2.6

1) A_n is a subgroup of S_n.

2) The order of A_n is

$$|A_n| = \frac{1}{2} n!$$

Pf (1) Check the three properties needed for a subgp:

- $e \in A_n$ as $s(e) = +1$
- $x, y \in A_n$

$\Rightarrow s(x) = s(y) = +1$

$\Rightarrow s(xy) = s(x)\,s(y)$ (2.1(1))

$= +1$

$\Rightarrow xy \in A_n$

- $x \in A_n \Rightarrow s(x) = 1$

$\Rightarrow s(x^{-1}) = 1$ (2.1(2))

$\Rightarrow x^{-1} \in A_n$.

Hence A_n is a subgp.

2) Consider the <u>right cosets</u> $A_n g$ $(g \in S_n)$. Two of these are

A_n $(= A_n e)$

$A_n(12)$.

Claim $A_n \cup A_n(12) = S_n$

Pf. Let $x \in S_n$.

If x is even then $x \in A_n$.

If x is odd, then

$$s(x \cdot (12)) = s(x)\, s(12)$$
$$= (-1)^2 = 1$$

$$\Longrightarrow x \cdot (12) \in A_n$$

$$\Longrightarrow x \in A_n(12).$$

Claim is proved.

& Since left/right (distinct) cosets are disjoint and have the same size (Alg I), the Claim gives

$$|S_n| = 2\,|A_n|$$

hence

$$|A_n| = \tfrac{1}{2}\,|S_n|$$
$$= \tfrac{1}{2}\, n!$$

Eg. 1) $A_2 = \{e\}$

2) $A_3 = \{e, (123), (132)\}$

$= \langle (123) \rangle \cong C_3$

3) Elts of A_4:

cycle-shape	e	(2)	(3)	(4)	(2,2)
in A_4?	✓	×	✓	×	✓
number of elts	1		8		3

Total $= |A_4| = 12 = \frac{1}{2} 4!$

11/10/19

4) How many elements of order 2 are there in A_6?

Ans Cycle-types of elements of order 2 in S_6 are

(2), $(2,2)$, $(2,2,2)$

Of these, only $(2,2)$ gives even perms.

So the elements of order 2 in A_6 are the perms. of cycle-shape $(2,2)$, say $(ij)(kl)$.

No. of such elts is

$$\frac{\binom{6}{2}\times\binom{4}{2}}{2} = 45$$

($\binom{6}{2}$: choose i,j; $\binom{4}{2}$: choose k,l)

$\uparrow$ because $(ij)(kl) = (kl)(ij)$

3. Direct Products

This chapter gives a way of exaples of constructing new groups.

Let $G_1, \ldots, G_n$ be groups.

The Cartesian product

$G_1 \times G_2 \times \ldots \times G_n$ is the set

$$\{ (x_1, \ldots, x_n) : x_i \in G_i \}$$

Define multiplication on $G_1 \times \ldots \times G_n$ by

$$(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n)$$

$$= (x_1 y_1, \ldots, x_n y_n)$$

(where $x_i y_i$ is the product of x_i and y_i in the group G_i).

Prop 3.1 Under this mult., $G_1 \times \cdots \times G_n$ is a group, called the direct product of the groups $G_1, \ldots, G_n$.

Pf We check the group axioms for $G_1 \times \cdots \times G_n$:

Closure Follows from closure in each group G_i.

Associativity Need to check

$$\Big((x_1,\ldots,x_n)(y_1,\ldots,y_n)\Big)(z_1,\ldots,z_n) = (x_1,\ldots,x_n)\Big((y_1,\ldots,y_n)(z_1,\ldots,z_n)\Big)$$

Well,

$$\text{LHS} = (x_1y_1,\ldots,x_ny_n)(z_1,\ldots,z_n)$$

$$= \big((x_1y_1)z_1,\ldots,(x_ny_n)z_n\big)$$

$$= \big(x_1(y_1z_1),\ldots,x_n(y_nz_n)\big)$$

(by assoc. in each G_i)

$= (x_1, \dots, x_n)(y_1 z_1, \dots, y_n z_n)$

$= (x_1, \dots, x_n)\left((y_1, \dots, y_n)(z_1, \dots, z_n)\right)$

$=$ RHS.

Identity is $(e_1, \dots, e_n)$, where e_i is the identity of G_i.

Inverse of $(x_1, \dots, x_n)$ is $(x_1^{-1}, \dots, x_n^{-1})$. //

Eg. We can now write down lots of new groups:

1) $C_2 \times C_2$,

$C_2 \times C_2 \times C_2$,

$S_{97} \times D_{138} \times (\mathbb{Q}, +)$

2) The group

$C_2 \times C_2$

Since $C_2 = \{1, -1\}$,

the elts. of $C_2 \times C_2$ are

e a b c

$(1,1), (1,-1), (-1,1), (-1,-1)$.

Mult table:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Note $C_2 \times C_2$ is abelian and $x^2 = e \quad \forall x \in C_2 \times C_2$.

Prop 3.2 Let $G_1, \ldots, G_n$ be groups.

1) Order of $G_1 \times \cdots \times G_n$ is $|G_1||G_2| \cdots |G_n|$.

2) $G_2 \times G_1 \cong G_1 \times G_2$, and

$(G_1 \times G_2) \times G_3 \cong G_1 \times (G_2 \times G_3)$

3) If every G_i is abelian, then $G_1 \times \dots \times G_n$ is also abelian.

4) If $x = (x_1, \dots, x_n) \in G_1 \times \dots \times G_n$ then the order of x is

$$o(x) = \operatorname{lcm}\left(o(x_1), \dots, o(x_n)\right).$$

Pf. 1) Clear.

2) Ex on Sheet 2.

3) Assume every G_i is abelian. Then

$$(x_1, \dots, x_n)(y_1, \dots, y_n)$$

$$= (x_1 y_1, \dots, x_n y_n)$$

$$= (y_1 x_1, \dots, y_n x_n)$$

(as each G_i abelian)

$$= (y_1, \dots, y_n)(x_1, \dots, x_n).$$

Hence $G_1 \times \dots \times G_n$ is abelian

4) Let

$$x = (x_1, \ldots, x_n)$$

and let $r_i = o(x_i)$.

Recall from Alg I,

$$x_i^k = e_i \iff r_i \mid k.$$

Let

$$r = \operatorname{lcm}(r_1, \ldots, r_n).$$

Then

$$x^r = (x_1^r, \ldots, x_n^r)$$

$$= (e_1, \ldots, e_n)$$

(as $r_i \mid r \ \forall i$)

Also, if $1 \leq k < r$,

then $\exists i$ s.t. $r_i \nmid k$,

so

$$x^k = (\ldots, x_i^k, \ldots)$$

and $x_i^k \neq e_i$, hence

$$x^k \neq (e_1, \ldots, e_n).$$

This shows that

$$o(x) = r. \quad //$$

Eg. 1. Lots of new abelian groups $C_{n_1} \times C_{n_2} \times \dots \times C_{n_r}$.

Eg. Some abelian groups of order 8:

$$C_8, \quad C_4 \times C_2, \quad C_2 \times C_2 \times C_2$$

Are these all non-isomorphic?

Ans Yes: use Prop 1.11(3):

G	C_8	$C_4 \times C_2$	$C_2 \times C_2 \times C_2$
no. of elts of order 8	4	0	0
no. of elts of order 4	2	4	0
no. of elts of order 2	1	3	7