Queen Mary
University of London

QP_LS-JA (Campus M)

Group Theory

Week 4, Lecture 1, 2 & 3

ahw811@qmul.ac.uk

Dr Lubna Shaheen

Assessment 1: Week 1 - Week 5

Deadline : Friday 15th Nov
17:00 (Week 8)

Table of Contents

Thursday

1:00 – 2:00

@ learning cafe

Monday

after 12:30 pm

office Hours.

Thursday in Morning.

Definition of Cosets

Definition

Let H be a subgroup of the group G whose operation is written multiplicatively (juxtaposition denotes the group operation). Given an element g of G, the left cosets of H in G are the sets obtained by multiplying each element of H by a fixed element g of G (where g is the left factor).

$gH = \{gh : \text{ h an element of H}\}$ for g in G.

The right cosets are defined similarly, that is,

$Hg = \{hg : \text{ h an element of H}\}$ for g in G.

gH, Hg

left Right

$D_6 = \{1, r, r^2, s, sr, sr^2\}$

Cosets: Example

$D_6 = \{1, r, r^2, s, rs, r^2 s\}$ ✓

Example: Let G be the dihedral group of order six. Its elements may be represented by $\{I, a, a^2, b, ab, a^2b\}$. In this group, $a^3 = b^2 = I$ and $ba = a^2b$. This is enough information to fill in the entire Cayley table:

$a = r, \quad b = s \quad H = \{1, s\}$

*	I	a	a²	b	ab	a²b
I	I	a	a^2	b	ab	a^2b
a	a	a^2	I	ab	a^2b	b
a²	a^2	I	a	a^2b	b	ab
b	b	a^2b	ab	I	a^2	a
ab	ab	b	a^2b	a	I	a^2
a²b	a^2b	ab	b	a^2	a	I

$T = \{1, s\}$ ✓ $\quad rT, \quad r^2T, \quad Tr, \quad Tr^2$

Let **T** be the subgroup $\{I, b\}$. The left cosets of T are: $IT = T = \{I, b\}$, $aT = \{a, ab\}$, and $a^2T = \{a^2, a^2b\}$. The right cosets of T are: $TI = T = \{I, b\}$, $Ta = \{a, ba\} = \{a, a^2b\}$ and $Ta^2 = \{a^2, ba^2\} = \{a^2, ab\}$.

$\{1, r, r^2\}$

Let **H** be the subgroup $\{I, a, a^2\}$. The left cosets of H are $IH = H$ and $bH = \{b, ba, ba^2\}$. The right cosets of H are $HI = H$ and $Hb = \{b, ab, a^2b\} = \{b, ba^2, ba\}$. In this case, every left coset of H is also a right coset of H? Why?

Cosets: Example

$rT = \{r, rs\}$ $\quad r^2T = \{r^2, r^2s\}$

Example: Take $G = \mathcal{S}_3$, $H = <(12)> = \{id, (12)\}$ and $g = (23)$. Then $Hg = \{(23), (123)\}, gH = \{(23), (132)\}$.

Remark:
(i) H is always a right coset of itself, since

$$H1 = \{h1 | h \in H\} = \{h | h \in H\} = H.$$

(ii) We can have $Hf = Hg$ even when $f \neq g$.

For example, let $G = \mathcal{C}_6 = \{1, z, z^2, z^3, z^4, z^5\}$. Then $H = \{1, z^3\}$ is a subgroup. We have $Hz = \{z, z^4\}$, and also $Hz^4 = \{z, z^4\}$. We can see that $Hf = Hg$.

$\mathcal{S}_3$

Cosets: Proposition

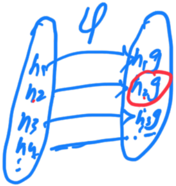
Proposition Subgroup

Suppose G is a group, $H \leq G$ and $f, g \in G$.

1. $|Hg| = |H|$.
2. If $f \in Hg$, then $Hf = Hg$. ✓
3. Each element of G is contained in exactly one right coset of H.

1) $\varphi : H \longrightarrow Hg$, $\varphi(h) = hg$ well-defined

φ is a bijection



One-one: $\varphi(h) = \varphi(h_2)$

$$hg = h_2 g$$

$$hgg^{-1} = h_2 g \cdot g^{-1} \Rightarrow h = h_2$$

Onto: for every hg, $\exists\, h \in H$, s. that

Cosets: Proposition

$\varphi(h) = hg$

2) $f \in Hg \Rightarrow Hf = Hg$

$f = hg$, $h \in H$. $\longrightarrow$ $g = h^{-1}f$

$kf \in Hf$, $\quad kf = khg = \underset{\substack{\Uparrow \\ H}}{kh}g \in Hg$

$Hf \subseteq Hg$

$lg \in Hg \quad lg = \underset{\substack{\Uparrow \\ H}}{lh^{-1}}f \in Hf$

3) $f \in G$, $\quad 1 \in H$

$\Rightarrow Hg \subseteq Hf \quad f = 1 \cdot f \in Hf$

Suppose $f \in Hg$, $\Rightarrow \boxed{Hf = Hg}$

Cosets: Proposition

$D_8 = \{1, r, r^2, r^3, s, rs, r^2 s, r^3 s\}$

Example

Take $G = D_8$ and $H = \{1, rs\}$. Then the right cosets are

$G = D_8$

$s \cdot r = r^{-1} s$ ✓

$$H1 = \{1, rs\}$$ ✓

$$Hr = \{r, s\}$$ ✓

$$Hr^2 = \{r^2, r^3 s\}$$ ✓

$$Hr^3 = \{r^3, r^2 s\}$$

$H \cdot r = \{1, rs\} \cdot r = \{r, rsr\} = \{r, s\}$

$rsr = r \cdot r^{-1} s = s$

$H \cdot r^2 = \{1, rs\} \cdot r^2 = \{r^2, rsr^2\}$

$= r^3 s$

$r \underline{s \cdot r} \cdot r = r \cdot r^{-1} \underline{s \cdot r} = s \cdot r = r^{-1} s$ ✓

Cosets: Coset Lemma

Coset lemma

Suppose G is a group, $H \leq G$ and $f, g \in G$. Then:
(i) Hf = Hg if and only if $fg^{-1} \in H$; 2nd
(ii) fH = gH if and only if $f^{-1}g \in H$. 1st

Sol $Hf = Hg$ $(\Longrightarrow)$

$f = 1 \cdot f \in Hf = Hg$

$f = hg \Longrightarrow fg^{-1} = h \in H$

$(\Longleftarrow)$ $fg^{-1} \in H$ $\quad f = fg^{-1}g \in Hg$

from above $\quad Hf = Hg$

Cosets

Proposition

If G is a group and $H \leq G$, then the number of right cosets of H is equal to the number of left cosets of H.

θ : Set of left cosets $\longrightarrow$ Right cosets

θ : $gH \longmapsto Hg$

$\theta(gH) = Hg^{-1}$ ✓

well-define

$fH = gH$ ✓

$\Rightarrow f^{-1}g \in H$, by coset Lemma

$Hf^{-1} = Hg^{-1}$

Again by coset Lemma

Cosets

Injection: One-one.

$Hf^{-1} = Hg^{-1}$

$\varphi(gH) = \varphi(fH)$

$Hg^{-1} = Hf^{-1}$

by coset lemma

$f^{-1}g \in H$

$fH = gH$

by coset lemma

One-one.

Surjective,

by definition

Lagrange's Theorem

Definition

Suppose G is a group and $H \leq G$. The index of H in G is the number of right cosets of H in G, written as $|G : H|$.

Lagrange's Theorem

Suppose G is a group and $H \leq G$. Then $|G| = |H||G : H|$. In particular, if G is finite then $|H|$ divides $|G|$.

Proof: $|G:H|$ is the no of right cosets of H in G, they have size $|H|$.

Proof of Lagrange's Theorem

So total size of cosets together

is $|H| \cdot |G:H| = |G|$.

Because each element of G lives

exactly in one coset so,

The number of elements of G

must be $|H| \cdot |G:H|$

Lagrange's Theorem

$3\mathbb{Z} = \{0, \pm 3, \pm 6, \pm 9, \cdots\}$

Example: $G = \mathbb{Z}$, $H = 3\mathbb{Z}$.

$$[G : H] = [\mathbb{Z} : 3\mathbb{Z}] = 3$$

The cosets of H in $\mathbb{Z}$ are of the form:

$$g + H = \{g + h | h \in H\} = \{g + 3k | k \in \mathbb{Z}\}$$

where $g \in \mathbb{Z}$.

Thus the distinct cosets of $3\mathbb{Z}$ in $\mathbb{Z}$ are:

(i) $0 + 3\mathbb{Z} = \{0, 3, 6, 9, \cdots\}$

(ii) $1 + 3\mathbb{Z} = \{1, 4, 7, 10, \cdots\}$

(iii) $2 + 3\mathbb{Z} = \{2, 5, 8, 11, \cdots\}$

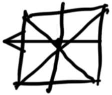
$|G| = \underset{\text{(infinite)}}{|H|}\ \underset{(3)}{|G:H|}$

countably infinite

$[G : H| = |\mathbb{Z} : 3\mathbb{Z}| = 3$

$D_8 = \{1, r, r^2, r^3, s, rs, r^2s, r^3s\}$

Lagrange's Theorem



$r = 90°$ rs

s – Reflection

Example Dihedral group $\mathcal{D}_8$:

Consider the dihedral group $\mathcal{D}_8$, which represents the symmetries of a square. The order of 8. The elements of $\mathcal{D}_8$ consist of 4 rotations and 4 reflections.

Let $H = \{e, r, r^2, r^3, \}$, where e is the identity and r, r^2, r^3 are the rotations by 90°, 180°, and 270°. This is a subgroup of $\mathcal{D}_8$ (the group of rotations), and its order is 4 Since 4 divides 8, Lagrange's Theorem holds for this example.

No of cosets of H in $\mathcal{D}_8$ are 2, which are

$$H = \{1, r, r^2, r^3\} \text{ and } Hs = \{s, rs, r^2s, r^3s\}$$

Symmetric Group $\mathcal{S}_3$: Consider the symmetric group $\mathcal{S}_3$, which is the group of all permutations of 3 elements. The order of $\mathcal{S}_3$ is 6. The elements of $\mathcal{S}_3$ are:

$\mathcal{S}_3 = \{e, (12), (13), (23), (123), (132)\}$. Now, consider the subgroup $H = \{e, (12)\}$. This is a subgroup of $\mathcal{S}_3$, and the order of H is 2. According to Lagrange's Theorem, the order of H must divide the order of S_3, which is true. The list of right cosets of H is

$|\mathcal{S}_3| = 6$ $|H| = 2$, $\Rightarrow$ 3 distinct cosets.

$$H = \{e, (12)\}, \{(13), (132)\}, \text{ and } \{(23), (123)\}$$

Corollary

$(12)\cdot(13) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132)$ Right cosets

Corollary

Suppose G is a finite group and $g \in G$. Then ord(g) divides $|G|$.

Proof

$H = \langle g \rangle, \quad H \leq G$

$|H| = |\langle g \rangle|$, by Langrange's Theorem

$\text{ord}(g) \mid |G|$

$H = \{e, (12)\}$

$H\cdot(13)$

$= \{(13), (132)\}$

$H\cdot(23)$

$= \{(23), (123)\}$

Euler's Theorem

Invertible residuals mod(n)

Applications in Number Theory

$$\mathcal{U}_n = (\mathbb{Z}/n\mathbb{Z})^\times$$ co-prime to n

Invertible residues mod n.

$|\mathcal{U}_n| = \Phi(n) =$ no of residues coprime to n.

$\mathcal{U}_n = \{ \quad \}$

Pick a residues $x \in \mathcal{U}_n$ it generates a cyclic subgroup

$$\langle x \rangle = \{1, x, x^2, \cdots x^{ord(x)-1}\}$$

of order ord(g).

Ord(g) $|\Phi(n) \implies x^{\Phi(n)} = 1.$ mod(n).

In other words

If x is coprime to n, then $x^{\Phi(n)} \equiv 1 \, mod(n)$.

Euler's Theorem

$\varphi(8) = |\{1, 3, 5, 7\}| = 4$

Example:

$$3^4 = 81 \equiv 1 \bmod (8)$$

$$\varphi(8) = |\{1, 3, 5, 7, \}| = 4$$

If $n = p$ is prime, then $\varphi(n) = p - 1$, $X^{p-1} \equiv 1 \text{mod } p \Leftrightarrow X^P - X$ is divisible by p.

For example $X^7 - X$ is divisible by 7, $2^7 - 2 = 128 - 2 = 126 = 7.18$.

$U_8 = \{1, 2, 3, 5, 7\}$

Lagrange's Theorem

Corollary: If $g \in G$ then $or(g) || G|$.

Important

$|S_n| = n!$ A_n : set of all even permutation

Example

S_n is symmetric group. $|S_n| = n!$. , $\mathcal{A}_n =< \mathcal{S}_n$ group of even permutation.

$$[\mathcal{S}_n : \mathcal{A}_n] = 2$$

$A_n \leq S_n$

Which right cosets do we know. $\{A_n, A_n(12)\}$

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

$[A_n : S_n] = 2$

$\mathcal{A}_n$ all the even permutation

$|A_n : S_n| |A_n| = n!$

Coset of $\mathcal{A}_n(12) =$ odd permutations

$\Rightarrow \frac{n!}{2} \cdot \underline{\underline{2}} = n!$

$$[\mathcal{S}_n : \mathcal{A}_n] = \frac{|\mathcal{S}_n|}{|\mathcal{A}_n|}$$

Index.

Conjugacy

BF-BB-AR (Campus M)

Definition

Suppose G is a group and $f, g \in G$. We say that f is conjugate to g in G (written $f \sim_G g$) if there is $k \in G$ such that $kfk^{-1} = g$.

Notation

$kfk^{-1} = g$

Page 25 Sn.

Lemma

Suppose G is a group then $\sim_G$ is an equivalence relation.

$\sim_G$

$l^{-1} g l = f$

Proof.

$x \sim_G x$

1. Reflexive: $x = exe^{-1}$

(x, y) $\quad x = gyg^{-1}$ $\quad g^{-1}x = yg^{-1}$

2. Symmetric: $x = gyg^{-1} \implies y = g^{-1}xg$.

$g^{-1}xg = y$

3. Transitive: $x = gyg^{-1}$ and $y = hzh^{-1} \implies x = (gh)z(gh)^{-1}$

$(x \sim_G y$ and $y \sim_G z)$ $\quad (y, x)$

$\square$

$x = gyg^{-1} = g(hzh^{-1})g^{-1}$

Conjugacy

$$= (gh)\, z\, h^{-1} g^{-1}$$

$$= (gh)\, z\, (gh)^{-1}$$

$$x = b\, z\, b^{-1}$$

$$(x, z)$$

$$x \sim_G z$$

Conjugacy in $\mathcal{D}_8$

Example: **Dehidral group of order 8** In this case the conjugacy classes

correspond to "types of symmetry":

- r and r^3 are both 90° rotations;
- r^2 is the only 180° rotation;
- s and r^2s are both reflections in axes parallel to the sides of the square;
- rs and r^3s are both reflections in diagonals of the square.

Conjugacy classes in D_8

Conjugacy classes in $\mathcal{D}_8$ are $= \{1, r, r^2, r^3, s, rs, r^2s, r^3s\}$

$$\big\{\{1\}, \{r, r^3\}, \{r^2\}, \{s, r^2s\}, \{rs, r^3s\}\big\}$$

The elements r and r^3 are conjugate to each other. Reflections s and sr conjugate r to r^3, but r and r^3 are not conjugate to other elements of the group.

Conjugacy

$$\boxed{sr = r^{-1}s}$$

$s^2 = 1$

$r^4 = 1$

$rrr^{-1} = r^3$

$r \sim_{D_8} r^3$ ✓

$srs^{-1} = r^3$

$rsr^{-1} = sr^2$ ✓

$\cancel{rsr^{-1}} = \cancel{sr^3}$

$r\,rs \cdot r^{-1} = r^3 s$

The element r^2 is in its own conjugacy class.

$srs^{-1} = r^{-1}s \cdot s^{-1} = r^{-1} \cdot e = r^{-1} = r^3$

✓ $sr^2s^{-1} = s \cdot r \cdot r \cdot s^{-1} = r^{-1} \cdot s \cdot r \cdot s^{-1}$

$= r^{-1} r^{-1} s \cdot s^{-1}$

$= r^{-2} = r^2$

$s \cdot \boxed{rs} \cdot s^{-1} = r^{-1} \cdot s \cdot s \cdot s^{-1} = r^{-1} \cdot s = \boxed{r^3 s}$

Conjugacy

$$rsr^{-1} = rsr^{-1}s \cdot s^{-1} = rs \cdot sr \cdot s^{-1} = r^2 \cdot s^{-1} = r^2 s.$$

Conjugacy classes in $\mathcal{D}_{10}$

Exercise: Find the conjugacy classes of $\mathcal{D}_{10}$.

Elements of $\mathcal{D}_{10}$ can be written as:

Rotations: $\{e, r, r^2, r^3, r^4\}$ where r represents a rotation by $2\pi/5(72^\circ)$ degree, and e is the identity (rotation by 0 degrees).

Reflections: $\{s, rs, r^2s, r^3s, r^4s\}$ where each s represents a reflection across a line of symmetry through a vertex or an edge.

$$\mathcal{D}_{10} = \{1, r, r^2, r^3, r^4, s, rs, r^2s, r^3s, r^4s\}$$

W can write $\mathcal{D}_{10} = \left\{\{e\}, \{r^2\}, \{r, r^3\}, \{s, r^2s\}, \{r, r^3s\}\right\}$

$$s \cdot r^2 s^{-1} = s \cdot r \cdot r \cdot s^{-1} = r^{-1} s \cdot r \cdot s^{-1} = r^{-1} \cdot r^{-1} s \cdot s^{-1}$$
$$= r^{-2} \cdot e$$
$$= r^2$$

$$s \cdot r \cdot s^{-1} = r^{-1} \cdot s \cdot s^{-1}$$
$$= r^{-1} \cdot e = r^3$$

$$r^5 = 1$$
$$r^4 = r^{-1}$$

Conjugacy

$rs \cdot r^{-1} = rs \cdot r^{-1} \cdot s \cdot s^{-1} = rs \cdot s \cdot r \cdot s^{-1} = r \cdot e \cdot r \cdot s^{-1} = r^2 s^{-1} = r^2 s$ $\quad (s \sim_{D_{10}} r^2 s)$

It turns out that:
Conjugacy class of $r = \{r, r^4\}$, $srr^{-1} = r^4$
Conjugacy class of $r^2 = \{r^2, r^3\}$, $sr^2s^{-1} = r^4$
The rotations split into two conjugacy classes: $\{r, r^2\}$ and $\{r^2, r^3\}$ as the as the elements r and r^4 are conjugate to each other, and similarly r^2 and r^3 are conjugate to each other. $r^2 \cdot s \cdot r^{-2} = r \cdot (r \cdot s \cdot r^{-1}) r^{-1} = r \cdot r^2 s \cdot r^{-1}$

Reflections: All reflections in $\mathcal{D}_{10}$ are conjugate to each other. Conjugating any reflection by a rotation produces another reflection:
Conjugacy class of reflections $= \{s, sr, sr^2, sr^3, sr^4\}$
This means all 5 reflections form a single conjugacy class.
Thus, the group $\mathcal{D}_{10}$ has four distinct conjugacy classes.

$= r^3 s \cdot r^{-1} \cdot s \cdot s^{-1} = r^3 \cdot s \cdot sr \cdot s^{-1} = r^3 r s^{-1} = r^4 s^{-1} = r^4 s.$

1) $\{e\}$ (the identity element), 2) $\{r, r^4\}$ (rotations by 72° and 288°), 3) $\{r^2, r^3\}$ (rotations by 144° and 216°
4) $\{s, rs, r^2s, r^3s, r^4s\}$ (all reflections) verify this

Centre of a Group

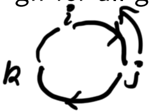
Definition

If G is a group, the **centre** of G is

$$Z(G) = \left\{ g \in G \middle| hg = gh \text{ for all } h \in G \right\}.$$

$ab = ba$

- Suppose G is abelian. Then $hg = gh$ for all g, h, so $Z(G) = G$.
- Let's find the centre of
  $$\mathcal{Q}_8 = \left\{ 1, -1, i, -i, j, -j \right\}. \quad k, -k$$



$i \cdot j = k \quad j \cdot i = -k$

$j \cdot k = i$

Certainly $1 \in Z(\mathcal{Q}_8)$, because $1g = g = g1$ for all g. Also $-1 \in Z(\mathcal{Q}_8)$, because -1 changes the sign of everything whether we multiply it from the left or the right.

$1 \cdot i = i \cdot 1 \qquad 1 \cdot j = j \cdot 1$

$ij \neq ji$, which means that neither i nor j is in $Z(\mathcal{Q}_8)$. Similarly we can show $-i, -j, k, -k \notin Z(\mathcal{Q}_8)$. So $Z(\mathcal{Q}_8) = \{1, -1\}$.

$-1 \cdot i = -i = i \cdot (-1)$

$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\} \qquad Z(Q_8) = \{\pm 1\}$

Centre of a Group

$i \cdot j = k \neq j \cdot i = -k$

Proposition

If G is a group, then $Z(G) \leq G$.

$i \cdot k \neq k \cdot i$

Given is that $Z(G)$ a set.

Solution:

- For any $h \in G$ we have
$$h1 = h = 1h,$$
so $1 \in Z(G)$. $1 \in Z(G) \neq \phi$

$fg^{-1} \in Z(G)$

- Suppose $f, g \in Z(G)$. Then for any $h \in G$
$$hfg^{-1} = fhg^{-1} = fg^{-1}ghg^{-1} = fg^{-1}hgg^{-1} = fg^{-1}h,$$
so $fg^{-1} \in Z(G)$.

$\therefore f \in Z(G)$ $hf = fh$.

$h \cdot fg^{-1} = f \cdot h\, g^{-1} = f \cdot g^{-1} g h g^{-1} = f g^{-1} h g g^{-1}$

$= f g^{-1} h \cdot e$

$= fg^{-1} h.$

$fg^{-1} \in Z(G)$

Centre of a Group

Lemma

Suppose G is a group and $x \in G$. Then $x \in Z(G)$ if and only if x lies in a conjugacy class of itself.

Proof.

Suppose x is in its own conjugacy class. This means that

$$gxg^{-1} = x, \quad \forall g \in G \Leftrightarrow gx = xg, \quad \forall g \in G \leftrightarrow x \in Z(G)$$

□

$\Leftarrow \quad gxg^{-1} = x \Rightarrow gx = xg \Rightarrow x \in Z(G)$

$\Rightarrow \quad x \in Z(G) \Rightarrow hx = xh$ for any $h \in G$

$x = h^{-1}xh \Rightarrow x \sim_G x$

Conjugacy in $\mathcal{S}_n$

Proposition

Suppose $n \geq 3$. Then $Z(\mathcal{S}_n) = \{id\}$.

Proof:

We know id $\in Z(\mathcal{S}_n)$, so we just need to show that if $g \in \mathcal{S}_n$ and $g \neq$ id then $g \notin Z(\mathcal{S}_n)$, i.e. there is some $h \in \mathcal{S}_n$ such that $gh \neq hg$.

Since $g \neq$ id, we can find $a \neq b \in \{1, \ldots, n\}$ such that $g \cdot a = b$. Let $c \in \{1, \ldots, n\}$ be different from a and b, and let $h = (b\, c)$. Then Transposition

$$gh \cdot a = g \cdot a = b, \qquad hg \cdot a = h \cdot b = c,$$

so $\boxed{gh \neq hg}$.

$h(b) = c$ $\quad$ $h(a) = a$

$h(c) = b$ $\quad$ $h(1) = 1$

$h(2) = 2$

$g \cdot h(a) = g \cdot a = b$ ✓

$hg(a) = h \cdot b = c$ ✓

Conjugacy in $\mathcal{S}_n$

Page (25)

Definition

Suppose $f \in \mathcal{S}_n$, written in disjoint cycle notation. The **cycle type** of f is the list of the lengths of the cycles of f, written in decreasing order.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 8 & 1 & 3 & 5 & 2 & 7 & 9 & 6 \end{pmatrix} = (143)(2896) = (4\ 3\ 1\ 1)$$

Example:

In $\mathcal{S}_9$, the permutation $(1\,4\,3)(2896)$ has cycle type $(4, 3, 1, 1)$. Notice in particular that the cycle lengths must be written in decreasing order, and we include cycles of length 1 (even though we usually don't write them when we're writing down the permutation).

Theorem

Suppose $f, g \in \mathcal{S}_n$. Then $f \sim_{\mathcal{S}_n} g$ if and only if f and g have the same cycle type.

Big Idea

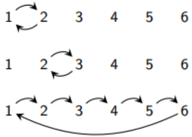
Conjugate permutations have the same structure. Such permutations are the same up to renumbering.

Conjugacy in $\mathcal{S}_n$

$6! = 6 \times 5 \times 4 \times 3 \times 2$

Consider the following permutations in $G = S_6$:

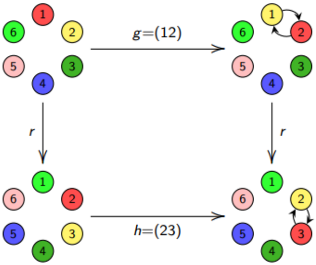
$$g = (1\ 2) \qquad h = (2\ 3) \qquad r = (1\ 2\ 3\ 4\ 5\ 6)$$



Since g and h have the same cycle type, they are conjugate:

$$\overset{h}{(1\ 2\ 3\ 4\ 5\ 6)}\,\overset{g}{(2\ 3)}\,\overset{h^{-1}}{(1\ 6\ 5\ 4\ 3\ 2)} = (1\ 2)\,.$$

Here is a visual interpretation of $g = rhr^{-1}$:



Conjugacy in $\mathcal{S}_n$

Theorem $\Longrightarrow$

Suppose $f, g \in \mathcal{S}_n$. Then $f \sim_{\mathcal{S}_n} g$ if and only if f and g have the same cycle type.

Proof: Suppose f and g are conjugate, $\exists\, h \in S_n$

s. that $\underline{g = hfh^{-1}}$. $\Longrightarrow$ $\underline{h^{-1} g h} = f$ ✓

Let $(a_1, \dots a_n)$ is the cycle type of f.

$f \cdot a_1 = a_2, \quad f \cdot a_2 = a_3, \quad \dots \quad , \quad f \cdot a_n = a_1$

this gives

$\underline{h^{-1} \cdot g\, h} \cdot a_1 = a_2 \quad h^{-1} \cdot g \cdot h \cdot a_2 = a_3 \quad \dots \dots$

$h^{-1} \cdot g\, h \cdot a_n = a_1$

Apply h on both sides of all

Conjugacy in S_n

we have

$$g(h\cdot a_1) = ha_2 \quad g(h\cdot a_2) = ha_3 \quad \dots, \quad g(h\cdot a_n) = ha_1$$

$\Rightarrow$ $(h\cdot a_1, ha_2 \dots, ha_n)$ is a cycle type of g.

This means for every cycle type of f, there is a corresponding cycle of g of same length.

$\Leftarrow$ conversely, if f, g have same cycle type, we paired up the cycle $(a_1, \dots a_r)$ of f with the cycle $(b_1, b_2, \dots, b_r)$ of g, and define $\boxed{h\cdot a_i = b_i}$ for each i.

$g(b_1) = b_2 \quad g(b_2) = b_3$

$$hfh^{-1}\cdot b_i = hf\cdot a_i$$

Exams Style Questions

$= h a_{i+1} = b_{i+1} = g \cdot b_i$

Conjugacy classes of $\mathcal{S}_3$:

$h : \{1 \ldots n\} \longrightarrow \{1, \ldots n\}$

because each no appears once $\longrightarrow$ bijection

$$\left\{ id, \{(12),(23),(13)\}, \{(123),(213)\} \right\}$$

$h f h^{-1} \cdot b = g b$ for all g

$b \in \{1, \ldots n\}$

so

$h f h^{-1} = g.$

xmxma

Conjugacy classes of $\mathcal{S}_4$:

$$\left\{ id, \{(12),(23),(13),(14)\}, \{(123),(213), 413\} \cdots \right\}$$

id, transpositions, (12)(34) , 3 -cycles, 4 -cylces

Exams Style Questions

Example: In $\mathcal{S}_3$ the elements (1 2 3) and (1 3 2) are conjugate.

Transpositions are conjugate: $\{(12), (13), (23)\}$.

Identity element is a conjugate class.

(12)
(13)
$h = (23)$ } from page 25 of Lecture Notes.

Solution:

$\underset{f}{(12)} \sim_{S_3} \underset{g}{(13)}$ find out h?

$hfh^{-1} = g$

$(23)(12)(23)^{-1} = (23)(12)(23) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (13) \Rightarrow h = (23)$

$\left.\begin{matrix} f = (123) \\ g = (132) \end{matrix}\right\}$ $h = (23)$ $(23)(123)(23) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132)$

So $h = (23)$ Remember that $h^{-1} = (23)$

Exams Style Questions

Example: In $\mathcal{S}_9$, find g such that $g = kfk^{-1}$

$f = (1356)(28)(497)$ and

$$k = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ & \downarrow & \downarrow & \downarrow & \downarrow & & & & \\ 4 & 1 & 6 & 3 & 8 & 2 & 7 & 5 & 9 \end{pmatrix}$$

$$g = kfk^{-1} = (4682)(15)(397)$$

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ & \downarrow & \downarrow & & & & & & \\ 5 & 4 & 9 & 6 & 1 & 8 & 3 & 2 & 7 \end{pmatrix}$$

Exams Style Questions

What are the conjugacy classes of $\mathcal{Q}_8 = \{1, -1, i, -i, j, -j, k, -k\}$.

Solution:

1. $\{1\}$
2. $\{-1\}$
3. $\{i, -i\}$
4. $\{j, -j\}$
5. $\{k, -k\}$

$i \cdot j = k$

$j \cdot k = -i$

$i^2 = j^2 = k^2 = -1$

$j \cdot i = -k$

$-j \times -i = k$

$k \times -i = -k \times i$
$= -j$

$\cdot$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$					
i	i	$-i$	-1					
$-i$	$-i$	i	1					
j	j	$-j$	$-k$					
$-j$	$-j$	j	k					
k	k	$-k$	j					
$-k$	$-k$	k	$-j$					

Exams Style Questions

Question: Write few elements of Conjugacy class of (13)(4679) in $\mathcal{S}_9$

Solution: Here is the list of some elements that belong to conjugacy class of (13)(4679).

1. (2 4)(5781) transposition (24) and 4 -cycle (5781)
2. (56)(2983)
3. (18)(2347)

Exams Style Questions

Question: In this question we work with the group
$\mathcal{U}_{21} = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$.

1. Find order of 5.
2. Hence find an element of order 3, and a subgroup H of order 3.
3. Find all the right cosets of H in $\mathcal{U}_{21}$.

Exams Style Questions

Solution:

1. We calculate $5^2 = 4$, $5^3 = 20$, $5^4 = 16$, $5^5 = 17$, $5^6 = 1$, so order of $5 = 6$.
2. Since 5 has order 6, $5^2 = 4$ has order 3. So $H = \langle 4 \rangle = \{1, 4, 16\}$ is a subgroup of order 3.
3. $$\begin{aligned} H1 &= \{1, 4, 16\}, \\ H5 &= \{5, 20, 17\}, \\ H2 &= \{2, 8, 11\}, \\ H10 &= \{10, 19, 13\}. \end{aligned}$$

   (We know we've found all the right cosets because we've written each element of $\mathcal{U}_{21}$ once.)

Exams Style Questions

Question:

Consider the following permutations:

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 8 & 4 & 3 & 6 & 7 & 5 & 1 \end{pmatrix}, \qquad b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 7 & 1 & 3 & 2 & 5 & 6 & 8 & 4 \end{pmatrix}.$$

Write down the disjoint cycle notation for a and b, and also for ab, ba, a^{-1}, b^{-1}, $(aba)^{-1}$ and $b^{-1}ab$. Which of these permutations lie in $\mathcal{A}_8$?

$$\begin{aligned} a &= (128)(34)(567) \\ b &= (17842) \\ ab &= (1567)(348) \\ ba &= (243)(5687) \\ a^{-1} &= (182)(34)(576) \\ aba^{-1} &= (13825) \\ b^{-1} &= (12487) \\ b^{-1}ab &= (156)(247)(38). \end{aligned}$$

QMplus Quiz

Attempt Quiz 4 at QMplus page

Some Useful Notations

Throughout this course, we use the following notation.

- $\mathcal{C}_n$ denotes the cyclic group of order n.
- Klein group often symbolized by the letter $\mathcal{V}_4$ or as $K_4 = \mathbb{Z}_4 \times \mathbb{Z}_4$ denotes the group $\{1, a, b, c\}$, with group operation given by

$$a^2 = b^2 = c^2 = 1, \qquad ab = ba = c, \; ac = ca = b, \; bc = cb = a.$$

- $\mathcal{U}_n$ is the set of integers between 0 and n which are prime to n, with the group operation being multiplication modulo n.

Some Useful Notations

- $\mathcal{D}_{2n}$ is the group with $2n$ elements

$$1,\ r,\ r^2,\ \dots,\ r^{n-1},\ s,\ rs,\ r^2s,\ \dots,\ r^{n-1}s.$$

  The group operation is determined by the relations $r^n = s^2 = 1$ and $sr = r^{n-1}s$.
- $\mathcal{S}_n$ denotes the group of all permutations of $\{1,\dots,n\}$, with the group operation being composition.
- $GL_n(\mathbb{R})$ is the group of $n \times n$ invertible matrices with entries in $\mathbb{R}$, with the group operation being matrix multiplication.
- $\mathcal{Q}_8$ is the group $\{1,-1,i,-i,j,-j,k,-k\}$, in which

$$i^2 = j^2 = k^2 = -1, \qquad ij = k,\ jk = i,\ ki = j,\ ji = -k,\ kj = -i,\ ik = -j.$$