# COSETS

# Cosets

Now we begin our study of the internal structure of gps. We present a way to split any group into distinct parts.

Def$^n$ Let $H$ be a subgp of $G$. (We often write $H < G$.) Let $g \in G$. Then

$$gH = \{gh \mid h \in H\} \ \& \ Hg = \{hg \mid h \in H\}$$

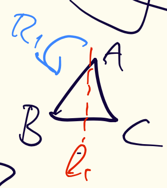
are called left & right cosets respectively of $H$ by $g$.

[ Aside: Something we haven't spoken of yet is the fact that in a gp the binary operation need not be commutative. Recall the gp of symmetries of $\Delta$, $S_3$ from the Cayley table

$$r_1 f_3 = f_2$$
$$f_3 r_1 = f_1$$

A gp $G$ in which $g_1 g_2 = g_2 g_1 \ \forall g_1, g_2 \in G$ is called <u>abelian</u>, in honour of Niels Abel. Abel was, among other things, the first person to show the quintic $a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0$ has no closed form sol$^n$ in terms of surds. We discuss abelian & non abelian gps in more detail later. ]

<u>Example</u>: Recall the gp $S_3$ of symmetries of




Consider the subgps $\langle f_1 \rangle = \{f_1, f_1^2\} = \{e, f_1\}$

& $\langle R_1 \rangle = \{R_1, R_1^2, R_1^3\} = \{e, R_1, R_1^2\}$

First note $e \cdot e = e$, $e \cdot f_1 = f_1$, $f_1 \cdot e = f_1$, $f_1 \cdot f_1 = e$

So $e \cdot \langle f_1 \rangle = f_1 \cdot \langle f_1 \rangle = \langle f_1 \rangle$

$$f_2 \cdot \langle f_1 \rangle = \{f_2 \cdot e = f_2, \ f_2 \cdot f_1 = r_2\} = \{f_2, r_2\}$$

$f_3 \cdot \langle f_1 \rangle = \{f_3, f_3 \cdot f_1\} = \{f_3, r_1\}$

$r_1 \cdot \langle f_1 \rangle = \{r_1, r_1 \cdot f_1\} = \{r_1, f_3\}$

$r_2 \cdot \langle f_1 \rangle = \{r_2, r_2 \cdot f_1\} = \{r_2, f_2\}$

No identity
Sets but not
nec. gps !!!

HW: Find cosets of $\langle R_1 \rangle$

Note every elt. appears in some coset of $\langle f_1 \rangle$.

Lemma 1: Let $H$ be a subgp of $G$. Let $g_1, g_2, g \in G$.
Then $g \in g_1 H$ & $g \in g_2 H$ iff $g_1 \in g_2 H$.

| | $e$ | $r_1$ | $r_2$ | $f_1$ | $f_2$ | $f_3$ |
|---|---|---|---|---|---|---|
| $e$ | $e$ | $r_1$ | $r_2$ | $f_1$ | $f_2$ | $f_3$ |
| $r_1$ | $r_1$ | $r_2$ | $e$ | $f_3$ | $f_1$ | $f_2$ |
| $r_2$ | $r_2$ | $e$ | $r_1$ | $f_2$ | $f_3$ | $f_1$ |
| $f_1$ | $f_1$ | $f_2$ | $f_3$ | $e$ | $r_1$ | $R_2$ |
| $f_2$ | $f_2$ | $f_3$ | $f_1$ | $r_2$ | $e$ | $R_1$ |
| $f_3$ | $f_3$ | $f_1$ | $f_2$ | $r_1$ | $r_2$ | $e$ |

Proof: If $g\in g_1H$ & $g_1\in g_2H$ then $g_1=g_2h_2$ for some $h_2\in H$
$g=g_1h_1$ some $h_1\in H$. Then $g=g_2h_2h_1$, $h_2h_1\in H$ so
$g\in g_2H$

If $g\in g_1H$ & $g\in g_2H$ then $g=g_1h_1=g_2h_2$
$g_1=g_2\underbrace{h_2h_1^{-1}}_{\in H}$ so $g_1\in g_2H$ □

Moreover:

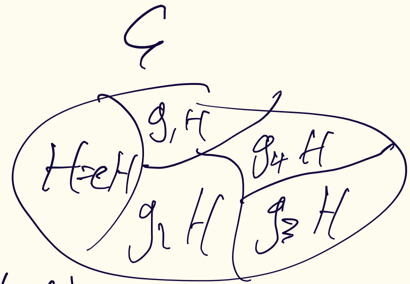
Lemma 2: If $H<G$ & $g_1\in g_2H$ then $g_1H=g_2H$.

Proof: if $h\in H$ then $g_1h\in g_1H$ & $g_1=g_2h_2$, some $h_2\in H$
$g_1h=g_2h_2h\in g_2H$ So $g_1H\subseteq g_2H$.
Consider $g_2h\in g_2H$. Then $g_1=g_2h_2$, some $h_2\in H$
$g_2h=(g_1h_2^{-1})h\in g_1H$ So $g_2H\subseteq g_1H$ □

Lemma 3: Let $H<G$ & $g\in G$. Then $g$ is in some coset of $H$.

Proof: Trivial: $g=g\cdot e\in gH$ □

So cosets partition the gp.




We can infer an important relation between the order of a group ($\#G=|G|$) & order of a subgroup from this partitioning.

Let $H<G$ & $h_1\neq h_2$, $h_1,h_2\in H$.

Note $h_1\neq h_2$ implies $gh_1\neq gh_2$ $\forall g\in G$.

Hence every coset of $H$ has the same # of elts, the same # as $H$ itself, i.e. every elt in $H$ contributes precisely once to each coset of $H$.

If $|G|=m$, $|H|=n$, & $r=\#$ of left cosets of $H$,

then $m = n \cdot r$.
In other words, we have just proven:

**Lagrange's thm**: The order of a subgp of $G$ divides the order of $G$!

From this we can also infer information about orders of elts ($\min\{n \mid g^n = e\}$):
**Corollary**: The order of an elt divides the order of a finite group.

Proof: HW

Q. Is the same true for inf. gps assuming $\infty / \infty$?

All questions 84-92

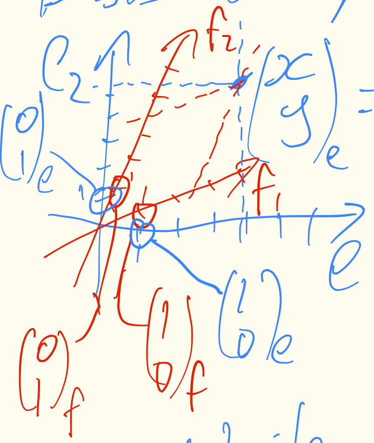
The same construction can be made for right cosets, we omit it here.
An important class of subgroups appears when comparing left & right cosets. While we could define it here we will prepare its defn w/ some extra study.
Finally, a word on nomenclature: $H < G$ & $|G| = |H| \cdot r$, some $r \in \mathbb{Z}_{>0}$. $r$ is called the 'index' of $H$ in $G$ & is denoted $[G : H]$, i.e. # copies of $H$ in $G$.

# INNER AUTOMORPHISM

Digression into Linear Algebra

Basis transformation of points – multiplication

Basis transformation of transformation – conjugation




$$\begin{pmatrix}x\\y\end{pmatrix}_e = \begin{pmatrix}z\\w\end{pmatrix}_f$$

How to convert coordinates?

$$\begin{pmatrix}x\\y\end{pmatrix}_e = x\cdot\begin{pmatrix}1\\0\end{pmatrix}_e + y\begin{pmatrix}0\\1\end{pmatrix}_e$$

$$\begin{pmatrix}z\\w\end{pmatrix}_f = z\begin{pmatrix}1\\0\end{pmatrix}_f + w\begin{pmatrix}0\\1\end{pmatrix}_f$$

Write basis vectors in terms of one another, as they are just points!

So $\begin{pmatrix}1\\0\end{pmatrix}_e = \begin{pmatrix}a\\c\end{pmatrix}_f \qquad \begin{pmatrix}0\\1\end{pmatrix}_e = \begin{pmatrix}b\\d\end{pmatrix}_f$

Then: $\begin{pmatrix}x\\y\end{pmatrix}_e = x\cdot\begin{pmatrix}1\\0\end{pmatrix}_e + y\begin{pmatrix}0\\1\end{pmatrix}_e = x\begin{pmatrix}a\\c\end{pmatrix}_f + y\begin{pmatrix}b\\d\end{pmatrix}_f$

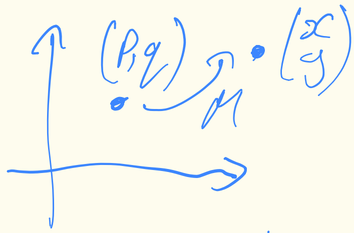
$$= \begin{pmatrix}ax+by\\cx+dy\end{pmatrix}_f = \begin{pmatrix}a & b\\c & d\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}_e = \begin{pmatrix}z\\w\end{pmatrix}_f$$

$\begin{pmatrix}a & b\\c & d\end{pmatrix}$ sends the e basis to the f basis. This works for every pt.

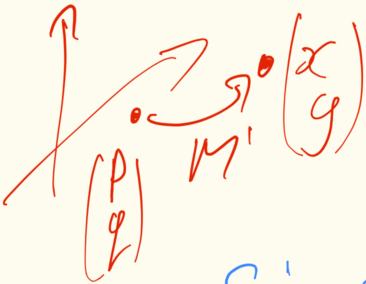
It acts by multiplication.

It may also be thought of as a transformation of points.

---

Now consider such a basis transformation $\begin{pmatrix}a & b\\c & d\end{pmatrix}$. And consider another transformation M sending  The basis transformation sends $\begin{pmatrix} p \\ q \end{pmatrix}$ & $\begin{pmatrix} x \\ y \end{pmatrix}$ to $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} p \\ q \end{pmatrix}$ & $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$

But what matrix $M'$ sends $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} p \\ q \end{pmatrix}$ to $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$?



$$M'\begin{pmatrix} p \\ q \end{pmatrix} = M'\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} p \\ q \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$$

Simple! $$\underbrace{\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} M' \begin{pmatrix} a & b \\ c & d \end{pmatrix}}_{M} \begin{pmatrix} p \\ q \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$$

Hence $M' = \begin{pmatrix} a & b \\ c & d \end{pmatrix} M \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}$ !!!

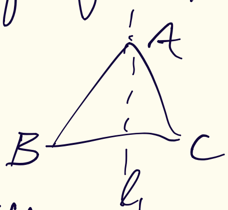
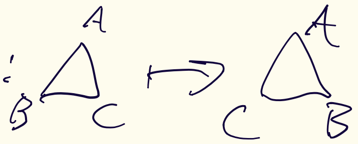
This transformation is called conjugation of $M$ by $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

So basis transformation of points — multiplication
Basis transformation of transformations — conjugation
$P^{-1}AP$ — Similar matrices
$P^TAP$ — Congruent matrices

— DIGRESSION END ————

# Inner automorphisms

Start w/ an example translating the notion of basis change into language of groups.

<u>Ex</u>: Consider  & flip $F_1$: 

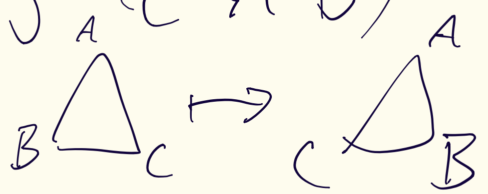
$F_1$ may be written as $\begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}$. We have seen the equivalence of symmetry preserving transf. of $\Delta$ & permutations on 3 letters $A, B, C$. i.e. $\exists$ an isomorphism

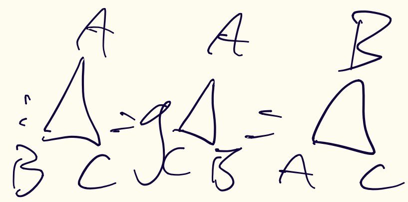
$$\left\{ \begin{matrix} \text{symmet. transf.} \\ \text{of } \Delta \end{matrix} \right\} \longrightarrow \{\text{Perms of } A, B, C\}.$$

This isomorphism is not unique: Any relabelling of vertices, which is itself a permutation of $A, B, C$, provides a different isomorphism.

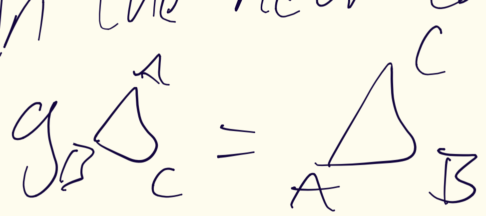
Let $g$ be a change of labelling (basis change) & let $h$ be a symmetric transf. of $\Delta$

eg $g = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}$

$h$: 

In the new coordinates this is $gh$: 

In the new coordinates the 'base' $\Delta$ is



Q: How to get to $gh$ in the new coords?

i.e. We want to reach $gh_B\Delta^A{}_C = {}_A\Delta^B{}_C$

starting from $g_B\Delta^A{}_C = {}_A\Delta^C{}_B$

Simple: transform back into base coords, then apply $h$, then go to new coords once again

$$(gh)(g^{-1})\,{}_A\Delta^C{}_B = (gh)(g^{-1}g_B\Delta^A{}_C) = gh_B\Delta^A{}_C$$

So $ghg^{-1}$ performs the $h$ transformation in the coordinates obtained by $g$.

Coordinates transform by $g$

transformations (gp elts) transform by $ghg^{-1}$

Def$^n$ Let $G$ be a gp & $g \in G$. Define a map $\Phi_g : G \to G : h \mapsto ghg^{-1}$. This is called the <u>inner</u> or <u>internal automorphism</u> of $G$ generated by $g$.

Let us show $\Phi_g$ is actually an automorphism.

Let $h \in G$. Then $g^{-1}hg \in G$. So $\Phi_g(g^{-1}hg) = gg^{-1}hgg^{-1} = h$

So $\Phi_g$ surjective

Let $h_1, h_2 \in G$. Then $\Phi_g(h_1) = \Phi_g(h_2)$ iff $gh_1g^{-1} = gh_2g^{-1}$

iff $h_1 = h_2$

So $\Phi_g$ injective, so a bijection from $G$ to $G$.
Finally let $h_1, h_2 \in G$. Then $\Phi_g(h_1 h_2) = g h_1 h_2 g^{-1} =$
$= g h_1 e h_2 g^{-1} = g h_1 g^{-1} g h g^{-1} = \Phi_g(h_1) \cdot \Phi_g(h_2)$ So
$\Phi_g$ is a hom. Hence $\Phi_g$ is an auto. of $G$.

Clearly in a gp w/ a commutative operation
$\Phi_g =$ identity map $\quad (\Phi_g(h) = ghg^{-1} = gg^{-1}h = h)$
Moreover, consider $g, h \in G$. Then $\Phi_g(h) = ghg^{-1}$

Note $\Phi_g(h)^n = g h \underbrace{g^{-1} \cdot g}_{e} h g^{-1} \cdots g h g^{-1} = g h^n g^{-1}$
So $\operatorname{ord}(h) = \Phi_g(h)$.
Let $\operatorname{ord}(hg) = m$ so $\overbrace{hghg \ldots hg}^{m} = e$
Then $\Phi_g((hg)^m) = ghghg \ldots hg \underbrace{g^{-1}}_{e} = \underbrace{ghghgh \ldots gh}_{m}$
$= \Phi_g(e) = geg^{-1} = gg^{-1} = e$
So $\operatorname{ord}(gh) = m$

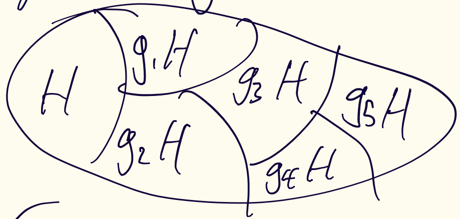
---

Now consider $H < G$ & the image of
$H$ under $\Phi_g$ for any $g \in G$. If $G$ is abelian
then clearly $\Phi_g(H) = H$, but in general this is
not true... But when is it true?

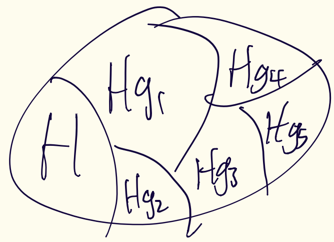
# GROUP STRUCTURE (NORMALITY)

# Normal Subgps

Recall the partitioning of a gp $G$ into cosets by its subgp $H$




We omitted discussion, but we can also consider the partition by the right cosets




We ask: When are these partitions precisely the same?

Clearly if $ab = ba$ $\forall\, a, b \in G$, then this is true, But this is non trivial in general. In fact it tells us much about the gp's structure.

Def$^n$. A subgp $H < G$ is called normal if
$$gH = Hg \quad \forall g \in G.$$

Def$^n$. A subgp $H < G$ is called normal if
$$\Phi_g(H) = H \quad \forall g \in G.$$
We write $H \triangleleft G$.

HW show equivalence of these definitions

A normal subgp is one that admits the same partiong & for both left & right cosets

A normal subgp is one that is unchanged by coordinate transformations i.e. they are the most symmetric w.r.t. commutativity of the gp operation.

Example: Consider $S_3 = \{\text{symm transf. of } \triangle\}$

Consider the subgps of rotations & flips

$R = \{e, r_1, r_2\}$ Are these normal?

$F_i = \{e, f_i\}$ Recall the Cayley table

($\{e, f_1, f_2, f_3\}$ not a gp)

| | $e$ | $r_1$ | $r_2$ | $f_1$ | $f_2$ | $f_3$ |
|---|---|---|---|---|---|---|
| $e$ | $e$ | $r_1$ | $r_2$ | $f_1$ | $f_2$ | $f_3$ |
| $r_1$ | $r_1$ | $r_2$ | $e$ | $f_3$ | $f_1$ | $f_2$ |
| $r_2$ | $r_2$ | $e$ | $r_1$ | $f_2$ | $f_3$ | $f_1$ |
| $f_1$ | $f_1$ | $f_2$ | $f_3$ | $e$ | $r_1$ | $R_2$ |
| $f_2$ | $f_2$ | $f_3$ | $f_1$ | $r_2$ | $e$ | $R_1$ |
| $f_3$ | $f_3$ | $f_1$ | $f_2$ | $r_1$ | $r_2$ | $e$ |

$f_i^{-1} = f_i$

So $f_i r_1 f_i^{-1} = f_i r_1 f_i$

$$\left.\begin{aligned} f_1 r_1 f_1 &= f_1 f_3 \\ f_2 r_1 f_2 &= f_2 f_1 \\ f_3 r_1 f_3 &= f_3 f_2 \end{aligned}\right\} \in R$$

& $f_i e f_i = f_i f_i = e \in R$

Since $R$ is a subgp $r_i R r_i^{-1} = R$

So $R \triangleleft S_3$

What about $F_1 = \{e, f_1\}$? $f_2 f_1 f_2 = f_2 r_1 = f_3 \notin F_1$

So $F_i$ not normal.

**Theorem**: Let $H < G$ & $|H| = |G|/2$

Then $H \triangleleft G$

**Proof**: Lagrange's Thm says # left cosets = 2 = # right.
But one of these cosets is $e \cdot H = H = H \cdot e$
The other coset is $G \setminus H$, which is both a left & right coset. Hence left & right cosets are the same & so $H \triangleleft G$.

**Corollary**: $A_n \triangleleft S_n$

Recall that $g$ & $h \in G$ are said to commute if
$gh = hg$

We can consider the set of elements in $G$ that commute w/ every element in $G$.

Defn. The centre of $G$, $Z(G)$, is the set of elements that commute w/ every elt of $G$, ie.

$$Z(G) = \{g \in G \mid gh = hg \ \forall h \in G\}$$

In fact, the centre is a subgp.

HW Show $Z(G) < G$

In fact, it is normal!

HW Show $Z(G) \triangleleft G$

HW Show $G \triangleleft G$
& $\{e\} \triangleleft G$
(trivial subgps)

# QUOTIENTS

# Quotients

Recall that $\mathbb{Z}_n = \{0,1,2,\dots,n-1\}$, is a gp w/ addition modulo $n$.

The numbers here represent equivalence classes

$i = [i] = \{i + nk \mid n \in \mathbb{Z}\}$

$0 = [0] = \{0, 6, 12, 18, \dots, -6, -12, \dots\}$

$4 = [4] = \{\dots, -8, -2, 4, 10, \dots\}$

Note: These are all cosets of $6\mathbb{Z} \leq \mathbb{Z}$, $6\mathbb{Z} = \{\dots -12, -6, 0, 6, \dots\} = [0]$

Recall the gp operation is addition,

So $1[0] = 1 + [0] = \{\dots, -11, -5, 1, 7, 13, \dots\}$

$2 + [0] = \{\dots, -10, -4, 2, 8, \dots\}$

etc.

We mirror this construction for general gps.

Defn Let $H \trianglelefteq G$ & let $\{eH, g_1H, g_2H, \dots\}$ be the collection of left cosets of $H$. Define a binary operation $* : (g_1H, g_2H) \mapsto (g_1 \cdot g_2)H$. We call $(\{H, g_1H, \dots\}, *)$ the <u>quotient gp</u> of $H$ in $G$ & denote it $G/H$.

Firstly we must show this operation $*$ is well defined.

i.e. if $x \in gH$ ($xH = gH$) & $y \in hH$ ($yH = hH$)
Then $xyH = ghH$

To see this: $xyH = x(yH) = x(hH) = x(Hh)$
$= (xH)h = (gH)h = g(Hh) = ghH$

This works only as $H$ is normal.
Recall that $(\mathbb{Z}, +)$ is abelian, so every subgp is normal.

Next we must show this is a gp.

$(eH) * (gH) = (e \cdot g)H = gH$, so $e \cdot H$ is an identity elt.
$gH * g^{-1}H = g \cdot g^{-1} H = eH$, so inverses are inherited
Check associativity is inherited also (HW)
Show $G/G \cong \{e\}$ & $G/\{e\} \cong G$
Show $|G/H| = |G|/|H|$

Typically normal subgps of $G$ are denoted $N$, not $H$.
Consider $G = S_3$ & $N = \{e, r_1, r_2\}$

Then $G/N = \{e \cdot N, f_1 \cdot N, f_2 \cdot N, f_3 \cdot N\} = \left\{\begin{matrix} \{e, r_1, r_2\} \\ \{f_1, f_2, f_3\} \\ \{f_2, f_3, f_1\} \\ \{f_3, f_1, f_2\} \end{matrix}\right\} = \left\{\begin{matrix} \{e, r_1, r_2\} \\ \{f_1, f_2, f_3\} \end{matrix}\right\}$

$e \cdot N * f_1 N = \{f_1, f_2, f_3\}$
$f_1 N * f_2 N = f_1 \cdot f_2 N = r_1 N = eN$

This has the structure of $C_2 = \{e, a\} \cong \mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$

HW Show construction is the same w/ right cosets.