Cosets and Lagrange's Thm

Def: Let G be a group and let $H \leq G$ be a subgp of G. A left coset (resp right coset) of H in G is a subset of G of the form

$$aH := \{ah : h \in H\} \quad (\text{resp } Ha := \{ha : h \in H\})$$

We say that aH (resp Ha) is the left (resp right) coset represented by a and that a is a representative for the coset aH (resp Ha).

Note: Take $1_G \in H$, we see that $a \in aH$ and $a \in Ha$.

Prop: Let G be a gp, let $H \leq G$ be a subgp of G, and let a, b be elements of G.

(a) One has $aH = H$ iff $a \in H$.

(b) One has either $aH = bH$ or $aH \cap bH = \emptyset$. Moreover

$$aH = bH \text{ iff } b^{-1}a \in H \text{ iff } a^{-1}b \in H$$

(c) One has $Ha = H$ iff $a \in H$.

(d) One has either $Ha = Hb$ or $Ha \cap Hb = \emptyset$. Moreover

$$Ha = Hb \text{ iff } ab^{-1} \in H \text{ iff } ba^{-1} \in H$$

proof: (a) $(\Rightarrow)$ Assume $aH = H$. Then $a \cdot 1_G = a \in H$.

$(\Leftarrow)$ Assume $a \in H$. Since $a \in H$, $x = ah \in H$.

Let $x \in aH$, then $x = ah$ for some $h \in H$.

Let $x \in H$. Then since $a \in H$, $a^{-1} \in H$, so

$$x = aa^{-1}x \in aH.$$

(b) First we show $aH = bH$ iff $b^{-1}a \in H$ iff $a^{-1}b \in H$.

($\Rightarrow$) Assume $aH = bH$. Then $\exists h, k \in H$ s.t. $ah = bk$. Then

$$b^{-1}a = kh^{-1} \in H \quad \text{and}$$
$$a^{-1}b = hk^{-1} \in H$$

because H is a subgp of G.

($\Leftarrow$) Assume $a^{-1}b \in H$. Then since H is a subgp

$$(a^{-1}b)^{-1} = b^{-1}a \in H$$

Let $x \in aH$, so $x = ah$ for some $h \in H$. Then

$$x = bb^{-1}ah$$

and since $b^{-1}a \in H$, $b^{-1}ah \in H$, so $x \in bH$.

Let $x \in bH$, so $x = bh$ for some $h \in H$. Then

$$x = aa^{-1}bh$$

and since $a^{-1}b \in H$, $a^{-1}bh \in H$, so $x \in bH$.

~~[illegible]~~

~~Now we show that if $aH \neq bH$, then $aH \cap bH \neq \phi$.~~

~~$aH \neq bH$ implies $\exists x \in bH$ s.t. $x \notin aH$ or $\exists x \in aH$ s.t. $x \notin bH$.~~

~~WLOG, let $x \in aH$ s.t. $x \notin bH$.~~

We show that if $aH \cap bH \neq \phi$, then $aH = bH$. Let $x \in aH \cap bH$, so $\exists h, k \in H$ s.t. $x = ah = bk$. Then

$$a^{-1}b = hk^{-1} \in H$$

so $aH = bH$. (c), (d) similar. $\square$

Remarks:

1. From now on, we will only talk about left cosets, but the analogous statements all hold for right cosets. See the notes for statements and notation about ~~left~~ ~~right~~ right cosets.

2. The proposition says that the set of left cosets of H in G form a partition of G:

$$G = \bigcup_{a \in G} aH \quad \text{because } a \in aH$$

$$\text{either } aH = bH \text{ or } aH \cap bH = \emptyset$$

The equivalence relation for this partion is defined as: For $x, y \in G$,

$$x \sim y \quad \text{iff} \quad x^{-1}y \in H$$

The equivalence classes are the left cosets of H in G.

Def: Let G be a group and $H \leq G$ a subgp. The set of left cosets of G in H is denoted G/H. We have in set notation

$$G/H = \{aH : a \in G\}$$

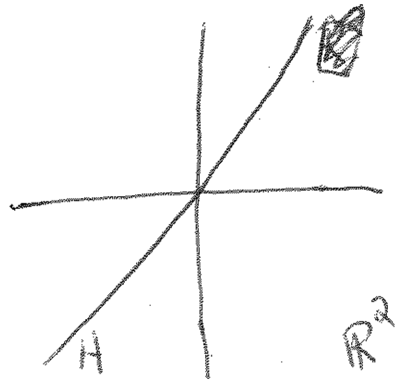
Examples: 1. Let $G = \mathbb{Z}$ and $H = m\mathbb{Z}$. Then

$$\begin{aligned} a + m\mathbb{Z} = b + m\mathbb{Z} \quad &\text{iff} \quad -a + b \in m\mathbb{Z} \\ &\text{iff} \quad m \text{ divides } b - a \\ &\text{iff} \quad a \equiv b \mod m \end{aligned}$$

$\mathbb{Z}/m\mathbb{Z} \equiv$ set of left cosets of $m\mathbb{Z}$ in $\mathbb{Z}$. These notions agree with our earlier notation.

2. $G = \mathbb{R}^2$ with addition

$H = \operatorname{Span}((1,1)) = \{ (\lambda,\lambda) : \lambda \in \mathbb{R} \}$

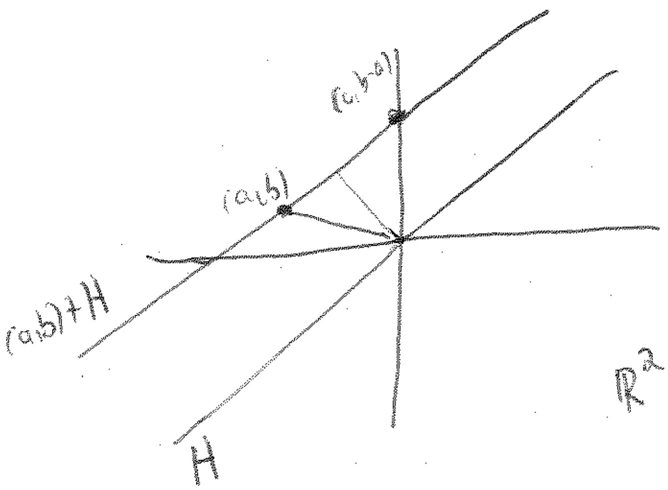


Given $(a,b) \in \mathbb{R}^2$,

$\lambda + b = a + \lambda + (b-a)$

$$(a,b) + H = \{ (a+\lambda, b+\lambda) : \lambda \in \mathbb{R} \}$$

line $y = x + b - a$



<u>Def</u>: Let $H \leq G$ be a subgp of a gp G. If $|G/H| < \infty$, then we say that H has <u>finite index</u> in G and we write $[G:H] = |G/H|$.

Examples: 1. $|\mathbb{Z}/m\mathbb{Z}| = m$, so $m\mathbb{Z}$ has index m in $\mathbb{Z}$.

2. $|\mathbb{R}^2/H|$ is not finite, when $H \subseteq \mathbb{R}^2$ is from previous example.

Prop: G-gp, $H \subseteq G$ subgp. For all $a \in G$ the function

$$\varphi_a : H \longrightarrow aH$$
$$h \longmapsto ah$$

is a bijection.

proof: Define $\psi_a : aH \longrightarrow H$, $x \longmapsto a^{-1}x$. ψ_a is a function from aH to H because if $x \in aH$, then $x = ah$ for some $h \in H$, so

$\psi_a(x) = a^{-1}x = a^{-1}ah = h \in H$.

We claim that φ_a and ψ_a are inverse functions to each other:

$$\psi_a \circ \varphi_a(h) = \psi_a(ah) = a^{-1}ah = h \quad \text{for all } h \in H$$
$$\varphi_a \circ \psi_a(x) = \varphi_a(a^{-1}x) = aa^{-1}x = x \quad \text{for all } x \in aH$$

Therefore $\psi_a \circ \varphi_a = Id_H$, $\varphi_a \circ \psi_a = Id_{aH}$, so φ_a and ψ_a are bijections. $\square$

Thm (Lagrange's Thm): Let G be a finite gp and $H \subseteq G$ a subgp. Then $|H|$ divides $|G|$. Furthermore $|G| = [G:H] \cdot |H|$.

proof: By definition, $[G:H]$ is the number of left cosets of H in G. By the previous prop, $\forall a \in G$, $|aH| = |H|$, so all the left cosets of H in G have the same size. Finally because $G = \bigcup_{a \in G} aH$, ~~we'll get that~~ and either $aH = bH$ or $aH \cap bH = \emptyset$, we get $|G| = [G:H] \cdot |H|$. $\square$

Point: There are $[G:H]$ cosets of H in G. They all have the same size, $|H|$, and they partition G. Therefore $|G| = [G:H] \cdot |H|$.

Cor: Let G be a finite gp and let $a \in G$. Then $o(a)$ divides $|G|$.

proof: $o(a) = |\langle a \rangle|$ and by Lagrange's Thm $|\langle a \rangle|$ divides $|G|$. $\square$

Cor: Let p be a prime number and let G be a gp of order p. Then $G \cong \mathbb{Z}/p\mathbb{Z}$.

proof: $p > 1$, so $\exists\, a \in G$ s.t. $a \neq 1_G$. Consider $\langle a \rangle \leq G$. By Lagrange's Thm $|\langle a \rangle|$ divides $|G| = p$. Because p is prime $|\langle a \rangle| = 1$ or p. Since $a \neq 1_G$, $\langle a \rangle \neq \{1_G\}$, so $|\langle a \rangle| \neq 1$. Hence $|\langle a \rangle| = p$, so $\langle a \rangle = G$, and G is a cyclic gp of order p. Hence $G \cong \mathbb{Z}/p\mathbb{Z}$. $\square$