Subgrupo

·) El centro de G: $Z(G)$

$$Z(G) = \{a \in G : ab = ba \quad \forall b \in G\}$$

es subgrupo

dem.·) $eb = be = b \quad \forall b \in G \Rightarrow e \in Z(G)$

·) $a, c \in Z(G)$ como $c \in Z(G)$

$\Rightarrow \forall b \in G \quad cb = bc$

$\Leftrightarrow c^{-1}cb = c^{-1}bc$

$ebc^{-1} = c^{-1}be$

$bc^{-1} = c^{-1}b \Rightarrow c^{-1} \in Z(G)$

$\Rightarrow c^{-1}, c, a \in Z(G)$

$ac^{-1}b = abc^{-1} = bac^{-1}$

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

$\Rightarrow G(Z)$ subgrupo

(~~de~~ es abeliano)

Ejemplo·) $G = GL(n, \mathbb{R})$, $Z(G) = \{cId : c \in \mathbb{R}^*\}$

·) G abeliano $\Leftrightarrow Z(G) = G$

·) $n \geq 3 \quad Z(D_n) = \{e\}$

$Z(D_n) \ni \delta : \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & & \sigma(n) \end{pmatrix}$

ejercicio: Ver que $\delta \in Z(G)$ conmuta con todas:

las trasposiciones $(i\,j)$ ¡¡¡

$$\begin{pmatrix} 1 & 2 & \cdots & i & \cdots & j & \cdots & n \\ 1 & 2 & \cdots & i & & j & & n \end{pmatrix}$$

que son ciclos de longitud 2

Lema Sea G grupo y sea $(S_i)_{i\in I}$ una familia de subgrupos de G. Entonces $\bigcap_{i\in I} S_i$ es subgrupo de G

demo) Como $e \in S_i$ $\forall i$

$\Rightarrow e \in \bigcap_{i\in I} S_i = S \Rightarrow S \neq \emptyset$

) $a, b \in \bigcap S_i \Rightarrow a, b \in S_i \ \forall i \in I$

$\Rightarrow ab^{-1} \in S_i \ \forall i \in I$ (subgrupo)

$\Rightarrow ab^{-1} \in \bigcap S_i$

obs en general la unión de subgrupos no es subgrupo

eg $GL(n,\mathbb{R}) \supseteq SL(n,\mathbb{R})$, $Z = \{cI : c \in \mathbb{R}^\times\}$

pero $Z \cup SL(n,\mathbb{R})$ no es subgrupo

$2I \in Z$ $\quad A = \begin{pmatrix} 1 & 1 & & \\ & 1 & & 0 \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix} \in SL(n,\mathbb{R})$

$AB^{-1} = \frac{1}{2}A \notin SL(n,\mathbb{R}) \cup Z$

Prop Ser G grupo y ser $X \subseteq G$
ent $\exists!$ subgrupo de G que denotamos
~~$\langle X \rangle$~~ H tq

a) $X \subseteq \langle X \rangle_H$

b) Si $S \leq G$ tq $X \subseteq S$
$\Rightarrow \langle X \rangle_H \subseteq S$

a este único lo denotamos $\langle X \rangle$

) es decir $\langle X \rangle$ es el menor subgrupo de G que contiene a X. $\langle X \rangle$ se llama subgrupo generado por X

Dem Ser $\langle X \rangle_H = \bigcap_{X \subseteq S \leq G} S$. Por lema anterior $\langle X \rangle_H$ subgrupo y $X \subseteq \langle X \rangle_H$ pues cierto en cada $S \Rightarrow$ a) ✓
(obs: la familia $\neq \emptyset$ pues $G \supseteq X$)

Si $S_0 \leq G$ y $X \subseteq S_0$

$\Rightarrow S_0$ es un miembro de la familia

$\Rightarrow \langle X \rangle_H = \bigcap_{X \subseteq S \leq G} S \subseteq S_0$

$\therefore \langle X \rangle_H$ cumple b)

Ahora sea $S, \tilde{S}$ son subgrupos que cumplen a), b) $\forall X$

como $X \subseteq S \Rightarrow \tilde{S} \subseteq S$ (pues $\tilde{S}$ cumple b))

$X \subseteq \tilde{S} \Rightarrow S \subseteq \tilde{S}$ (pues $\tilde{S}$ cumple b))

$\forall$ "X" $\Rightarrow \tilde{S} = S$ (es único)

Prop Sea $X \subseteq G$, $X \neq \emptyset$ ent:

$$\langle X \rangle = \{ x_1^{n_1} \cdots x_r^{n_r} \quad r \in \mathbb{N},\ x_i \in X,\ n_i \in \mathbb{Z} \}$$

den llamemos $H = \{ x_1^{n_1} \cdots x_r^{n_r} : r \in \mathbb{N} \cdots \}$

I) $H \leq G$ veámoslo: Notar $X \subseteq H \Rightarrow H \neq \emptyset$

ψ

$x = x^1 \in H$

$$a = x_1^{n_1} \cdots x_r^{n_r}, \quad b = y_1^{m_1} \cdots y_k^{m_k} \in H$$

$$\Rightarrow a b^{-1} = x_1^{n_1} \cdots x_r^{n_r} y_k^{-m_k} \cdots y_1^{-m_1} \in H \Rightarrow H \leq G$$

II) H cumple a) (trivial) de la prop anterior (contener a X)

III) Si $S \leq G$ / $X \subseteq S$ como S cerrado para la operación de G

$$\Rightarrow x_1^{n_1} \cdots x_r^{n_r} \in S \quad \forall x_i \in S,\ n_i \in \mathbb{Z},\ r \in \mathbb{N}$$

$\Rightarrow H \subseteq S \Rightarrow H$ cumple 2) $\Rightarrow$ por unicidad

$\therefore H = \langle X \rangle$ □

*) Cuando $X=\{a\}$ $(a \in G)$ $\langle X \rangle = \langle a \rangle$

se llama al subgrupo cíclico generado por a por la propiedad anterior

$$\langle a \rangle = \langle X \rangle = \{ a^n : n \in \mathbb{Z} \}$$

*) Diremos que un subconjunto $X \subseteq G$ es un conjunto de generadores de G

$$\rightsquigarrow \quad \langle X \rangle = G$$

*) $a \in G$ $\quad a^k, a^m \in \langle a \rangle \quad a^n \cdot a^k = a^{n+k}$

$$= a^{k+n} = a^k \cdot a^n$$

$\langle a \rangle$ es siempre abeliano

Ejemplo Generadores de $GL(n,K)$

$A \in GL(n,K) \Leftrightarrow E_k \cdots E_1 A = I$

$\Leftrightarrow A = E_1^{-1} \cdots E_k^{-1}$ producto de matrices elementales

$\Rightarrow GL(n,K) = \langle E \mid E$ matriz elemental $n \times n \}$

Ej) $GL(2,K)$ generado por $a \in K$ $c \in K^*$

$$\left\langle \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix} \begin{pmatrix} c & 0 \\ 0 & 1 \end{pmatrix} \right\rangle$$

*) $D_n = \{ r^k s^j : j = 1, 0 \quad 0 \le k \le n-1 \}$ $\quad |D_n| = 2n$

$\Rightarrow D_n = \langle r, s \rangle$

$srs^{-1} = srs \quad$ pues $\quad s^2 = e$
$\quad\quad = r^{-1} \quad\quad\quad\quad r^n = e$

$\Leftrightarrow sr = r^{-1}s \Rightarrow D_n$ no es abeliano
y $r^{-1} \neq r$ (si $n > 3$)

(y como lo pruebo)

*) El subgrupo conmutador (o derivado) de un grupo G se define como

$$[G, G] = \langle [a, b] : a, b \in G \rangle$$

$$[a, b] = abab^{-1}b^{-1}$$

obs G abeliano $\Leftrightarrow [G, G] = \{e\}$

Notación aditiva (caso G abeliano)

$a \cdot b$	$a + b$
e	0
a^{-1}	$-a$
a^n	na

$$\langle X \rangle = \{ x_1^{n_1} \cdots x_r^{n_r} \}$$

$$\langle X \rangle = \{ \sum_{\text{distintos}} n_i x_i \mid x_i \in X \}$$

* Ejemplo subgrupos de $\mathbb{Z}$: $\{0\}, \mathbb{Z}, \underbrace{2\mathbb{Z}}_{\text{pares}}$

$$2\mathbb{Z} = \{n \in \mathbb{Z} : 2 \mid n\} \leq \mathbb{Z}$$

1) Vemos que todos son de esta forma

Tomamos $H \leq \mathbb{Z}$ y suponemos $H \neq \{0\}$

4 Como H es cerrado por $x \mapsto -x$ (subgrupo) H contiene un entero positivo. Sea

$$a = \min\{k > 0 \mid k \in H\} \quad b)$$

2) Vemos $\langle a \rangle = H$. Como $a \in H \Rightarrow \langle a \rangle \subseteq H$

3) Sea $h \in H$: $h = ma + r$ $\quad 0 \leq r \leq a-1$ $\quad m \in \mathbb{Z}$

$$r = h - ma \in H \quad (H \text{ subgrupo})$$
$$\in H \quad \in H \Rightarrow$$

Como $a = \min\{k > 0 : k \in H\} \Rightarrow r \geq 0$

$\Rightarrow h = ma \in a\mathbb{Z}$

(abeliano)

$(\underbrace{a+a \cdots + a}_{m\text{-veces}})$

Luego $H \subseteq \langle a \rangle = a\mathbb{Z}$

$\Rightarrow H = a\mathbb{Z}$

$\therefore$ todo subgrupo de $\mathbb{Z}$ es cíclico

en particular $\mathbb{Z} = 1\mathbb{Z} = (-1)\mathbb{Z}$

def $a \in G$, el orden de a se define como $|a| = |\langle a \rangle| = |\{a^m : m \in \mathbb{Z}\}|$

(a lo numerable)

Proposición G grupo, $a \in G$. Son equivalentes

i) $|a| = n$

ii) $n = \min\{r \in \mathbb{N} \mid a^r = e\}$

iii) $a^k = e \Leftrightarrow n \mid k$

iv) $a^r = a^s \Leftrightarrow r \equiv s \ (n)$

v) $\langle a \rangle = \{e, a, a^2, \dots a^{n-1}\}$

demo i) $\Rightarrow$ ii) por i) $\langle a \rangle$ finito

$\therefore$ La función $\mathbb{Z} \to \langle a \rangle$, $k \mapsto a^k$

no puede ser inyectiva

$\Rightarrow \exists\, k < m \Rightarrow a^k = a^m \Leftrightarrow a^{m-k} = e$

Luego $\{r \in \mathbb{N} : a^r = e\} \neq \emptyset$

Sea $h = \min\{r \in \mathbb{N} \mid a^r = e\}$

En primer lugar los elementos

$a^0 = e, a, a^2, \dots, a^{h-1}$

son distintos entre sí

Se fosse $a^i = a^j$ $0 \le i < j \le n-1$

$\Rightarrow a^{j-i} = e$ e $1 \le j-i \le n$ absurdo.

n mínimo

Além disso se $m \in \mathbb{Z}$, $m = nt + r$ $0 \le r \le n-1$
$\ge n-1$ $r, t \in \mathbb{Z}$

$$\Rightarrow a^m = (a^n)^t a^r = e^t a^r = a^r$$

$$\therefore \langle a \rangle = \{ e = a^0, a^1, \dots a^{n-1} \}$$

$$\therefore n = |\langle a \rangle| = n = \min \{ r \in \mathbb{N} \mid a^r = e \}$$

ii) $\Rightarrow$ iii) $k \in \mathbb{Z}$ $k = nq + r$ $0 \le r < n$

$$a^k = (a^n)^q a^r = a^r = e \Leftrightarrow r = 0$$

pois n mínimo

(hipótese $a^n = e$)

$$\Leftrightarrow k = nq \Leftrightarrow n \mid k$$

iii) $\Rightarrow$ iv) $a^r = a^s \Leftrightarrow a^{r-s} = e$

iii) $\Leftrightarrow n \mid r-s$

$\Leftrightarrow r \equiv s \pmod{n}$

iv) $\Rightarrow$ v) Sea $m \in \mathbb{N}$ / $a^r = a^s \Leftrightarrow r \equiv s \pmod{m}$

$\Rightarrow \{a^k : k \in \mathbb{Z}\} = \{a^k : 0 \leq k \leq m-1\}$

porque $\forall k \; \exists! \; 0 \leq \tilde{k} \leq m-1 \mid k \equiv \tilde{k} \pmod{m}$

Como las potencias a^k, $0 \leq k \leq m-1$
son distintas $\Rightarrow n = |\langle a \rangle| = m$

(pq $k \not\equiv \tilde{k} \pmod{m}$ si $k \leq m-1$)

v) $\Rightarrow$ i) Como $\langle a \rangle = \{a, a^2, \ldots a^{n-1}\}$

$\Rightarrow |a| = n$

Proposición G grupo, $a \in G$. Son equivalentes

i) $|a|$ es infinito

ii) $a^k = e \Leftrightarrow k = 0$

iii) $a^r = a^s \Leftrightarrow r = s$

Tarea ejercicio

i) $\Rightarrow$ ii) ($\Rightarrow$) Supongo $K \neq 0$

$\Rightarrow a^k = e$

$\Rightarrow |a| = K$ absurdo

$\Rightarrow k = 0$

($\Leftarrow$) por def

ii) $\Rightarrow$ iii) ($\Rightarrow$) $a^r = a^s$

$\Rightarrow a^{r-s} = e$

ii) $\Rightarrow r - s = 0 \Rightarrow r = s$

($\Leftarrow$) Trivial

iii) $\Rightarrow$ i) Supongo $|a| = n$

$\Rightarrow \langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$

$\Rightarrow a^n \in \langle a \rangle$ si no $|a| = n+1$

$\Rightarrow$ $a^n = a^j$ com $j \leq n-1$

Pois! $(n > n-1 \geq j \Rightarrow n \neq j)$