Grupos

I) Semigrupos y monoides.

Def. Sea G un conjunto no vacío dotado de una operación binaria "$\cdot$", y $e \in G$. Decimos que e es una identidad izquierda (resp. derecha) de G, si $e \cdot a = a$ (resp. $a \cdot e = a$) $\forall\, a \in G$.
Diremos que e es identidad ó elemento neutro si e es identidad izquierda y derecha a la vez, es decir, $\forall\, a \in G$,

$$e \cdot a = a \cdot e = a$$

Ejemplo:

a) Sea $G = \{a, b\}$, con $\cdot : G^2 \to G$ una operación binaria dada por la siguiente tabla:

$\cdot$	a	b
a	a	b
b	a	b

Es claro que a y b son dos identidades izquierdas, no necesariamente iguales. La siguiente proposición muestra que no podemos tener dos identidades, una izquierda y otra derecha, que sean diferentes.

Prop.
Sea G un conjunto no vacío dotado de una operación. Si $e \in G$ es identidad izquierda y e' es identidad derecha, entonces $e = e'$.

Dem:

$$e = e \cdot e' = e'$$

q.e.d.

Corolario:
Sea G un conjunto no vacío dotado de una operación. Entonces toda identidad $e \in G$ es única.

Def. Sea G un conjunto no vacío dotado de una operación. Decimos que G es semigrupo si dicha operacion es asociativa, i.e:

$$\forall x,y,z \in G, \quad x\cdot(y\cdot z) = (x\cdot y)\cdot z$$

Def. Todo semigrupo con identidad es llamado monoide.

Sea G un conjunto no vacío dotado de una operación, con $a_1, a_2, \ldots, a_n \in G$. Definimos el producto $a_1\cdot a_2\cdot \ldots \cdot a_n$ de manera inductiva.

- Para $n=3$:

$$a_1\cdot a_2\cdot a_3 = (a_1\cdot a_2)\cdot a_3$$

- Para $n>3$:

$$a_1\cdot a_2\cdot \ldots \cdot a_n = (a_1\cdot a_2\cdot \ldots \cdot a_{n-1})\cdot a_n$$

Proposición:

Sea G un semigrupo, entonces $\forall a_1, a_2, \ldots, a_n \in G$, $n \geq 3$ se tiene que, $\forall\ 1 \leq m < n$, $m \in \mathbb{N}$:

$$a_1\cdot a_2\cdot \ldots \cdot a_n = (a_1\cdot a_2\cdot \ldots \cdot a_m)\cdot(a_{m+1}\cdot \ldots \cdot a_n)$$

Dem:

Procederemos por inducción sobre n.

- Para $n=3$:

$$\forall a_1, a_2, a_3 \in G, \quad a_1\cdot a_2\cdot a_3 = (a_1\cdot a_2)\cdot a_3 = a_1\cdot(a_2\cdot a_3)$$

La afirmación se cumple para $m=1,2$.

- Suponga que se cumple para $n=K$.
- Probaremos que se cumple para $n=K+1$.

Si $m=K$, la afirmación se cumple por definición. Para $m<K$:

$$\forall a_1, a_2, \ldots, a_{K+1} \in G, \quad a_1\cdot a_2\cdot \ldots \cdot a_{K+1} = (a_1\cdot a_2\cdot \ldots \cdot a_K)\cdot a_{K+1}$$

Por la hipótesis de inducción:

$$
\begin{aligned}
a_1 \cdot a_2 \cdot \ldots \cdot a_{K+1} &= [(a_1 \cdot a_2 \cdot \ldots \cdot a_m) \cdot (a_{m+1} \cdot \ldots \cdot a_K)] \cdot a_{K+1} \\
&= (a_1 \cdot a_2 \cdot \ldots \cdot a_m) \cdot [(a_{m+1} \cdot \ldots \cdot a_K) \cdot a_{K+1}] \\
&= (a_1 \cdot a_2 \cdot \ldots \cdot a_m) \cdot (a_{m+1} \cdot \ldots \cdot a_{K+1})
\end{aligned}
$$

Teniendo lo deseado.

Aplicando inducción, se cumple $\forall\, n \in \mathbb{N}$, $n \geq 3$.

q.e.d.

Si $a_1, a_2, \ldots, a_n \in G$, G con una operación binaria, y suponemos que $a_i = a$ $\forall\, i \in \{1, \ldots, n\}$, entonces, el producto:

$$a_1 \cdot a_2 \cdot \ldots \cdot a_n = a \cdot a \cdot \ldots \cdot a$$

se denota por a^n.

Proposición:

Si G es semigrupo, entonces, $\forall\, a \in G$:

i) $a^{m+n} = a^m \cdot a^n$

ii) $a^{mn} = (a^m)^n$

$\forall\, m, n \in \mathbb{N}$. Si G es un monoide se define $a^0 = e$ $\forall\, a \in G$.

Dem:

De (i): Procederemos por inducción sobre n:

- Sea $m \in \mathbb{N}$. Claramente:

$$a^{m+1} = \underbrace{a \cdot a \cdot \ldots \cdot a}_{m\text{-veces}} \cdot a = a^m \cdot a = a^m \cdot a^1$$

por tanto, el resultado se tiene para $n = 1$.

- Suponga que se tiene el resultado para $n = K$.
- Probaremos que se cumple el resultado para $n = K+1$. En efecto:

$$a^{m+K+1} = a^{(m+K)+1} = a^{(m+K)} \cdot a^1 = (a^m \cdot a^K)\, a^1 = a^m (a^K \cdot a^1) = a^m \cdot a^{K+1}$$

Con lo que se cumple para $n=K+1$.

Por inducción, se cumple $\forall\, n\in\mathbb{N}$.

De (ii): Sea $m\in\mathbb{N}$. Procederemos por inducción sobre n.

· Para $n=1$ el resultado es claro, pues:

$$a^{m\cdot 1}=a^{m}=(a^{m})^{1}$$

· Suponga que el resultado se cumple para $n=K$.

· Probaremos que se cumple para $n=K+1$. En efecto:

$$a^{m(K+1)}=a^{mK+m}=a^{mK}\cdot a^{m}=(a^{m})^{K}\cdot a^{m}=(a^{m})^{K+1}$$

Aplicando inducción, se cumple $\forall\, n\in\mathbb{N}$.

q.e.d.

Def. Sea G un conjunto no vacío dotado de una operación. Se dice que la operación binaria es conmutativa si:

$$a\cdot b=b\cdot a$$

$\forall\, a,b\in G$. Cuando esto ocurre, se dice que G es abeliano.

Proposición:

Sea G un semigrupo abeliano y $a_1,a_2,\ldots,a_n\in G$, y φ una permutación del conjunto $\underbrace{\{1,2,\ldots,n\}}_{N}$ (φ es una función biyectiva de N en N)

Denotamos a φ como:

$$\varphi:=\begin{pmatrix}1 & 2 & \cdots & n\\ \varphi(1) & \varphi(2) & \cdots & \varphi(n)\end{pmatrix} \quad y$$

$$\varphi^{-1}:=\begin{pmatrix}\varphi(1) & \varphi(2) & \cdots & \varphi(n)\\ 1 & 2 & \cdots & n\end{pmatrix}$$

Entonces:

$$a_1\cdot a_2\cdot\ldots\cdot a_n=a_{\varphi(1)}\cdot a_{\varphi(2)}\cdot\ldots\cdot a_{\varphi(n)}$$

Dem:

Procederemos por inducción sobre n.

- Para $n=2$, el resultado se sigue del hecho que G es semigrupo abeliano, y φ tiene dos posibilidades:

$$\varphi = id_{\{1,2\}} \quad o \quad \varphi = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

teniendo así:

$$a_1 \cdot a_2 = a_1 \cdot a_2 \quad o \quad a_1 \cdot a_2 = a_2 \cdot a_1$$

en ambos casos se cumple la afirmación.

- Suponga que se cumple para $n=K$.
- Probaremos que se cumple para $n=K+1$. En este caso tenemos 3 posibilidades:

1) $\varphi(K+1)=K+1$. Entonces:

$$a_{\varphi(1)} \cdot a_{\varphi(2)} \cdot \ldots \cdot a_{\varphi(K+1)} = (a_{\varphi(1)} \cdot a_{\varphi(2)} \cdot \ldots \cdot a_{\varphi(K)}) \cdot a_{K+1}$$

Tomando a $\varphi: J_K \to J_K$, se tiene por la hip. de inducción:

$$= (a_1 \cdot a_2 \cdot \ldots \cdot a_K) \cdot a_{K+1}$$
$$= a_1 \cdot a_2 \cdot \ldots \cdot a_{K+1}.$$

2) $\varphi(1)=K+1$.

$$a_{\varphi(1)} \cdot a_{\varphi(2)} \cdot \ldots \cdot a_{\varphi(K+1)} = a_{K+1} \cdot (a_{\varphi(2)} \cdot \ldots \cdot a_{\varphi(K+1)})$$

Tomando a $\varphi: \{2, \ldots, K+1\} \to J_K$, se tiene por hip.

$$= a_{K+1} \cdot (a_1 \cdot \ldots \cdot a_K)$$
$$= (a_1 \cdot \ldots \cdot a_K) \cdot a_{K+1}$$
$$= a_1 \cdot a_2 \cdot \ldots \cdot a_{K+1}$$

3) $K+1 = \varphi(i)$ para algún $i \in \mathbb{N}$, $1 < i < K+1$:

$$a_{\varphi(1)} \cdot a_{\varphi(2)} \cdot \ldots \cdot a_{\varphi(K+1)} = a_{\varphi(1)} \cdot \ldots \cdot a_{\varphi(i-1)} \cdot a_{\varphi(i)} \cdot a_{\varphi(i+1)} \cdot \ldots \cdot a_{\varphi(K+1)}$$

$$= (a_{\varphi(1)} \cdot \ldots \cdot a_{\varphi(i-1)}) \cdot (a_{k+1} \cdot [a_{\varphi(i+1)} \cdot \ldots \cdot a_{\varphi(k+1)}])$$
$$= [(a_{\varphi(1)} \cdot \ldots \cdot a_{\varphi(i-1)}) \cdot (a_{\varphi(i+1)} \cdot \ldots \cdot a_{\varphi(k+1)})] \cdot a_{k+1}$$
$$= a_1 \cdot a_2 \cdot \ldots \cdot a_{k+1}.$$

Aplicando inducción se tiene lo deseado.

q.e.d.

Def. Sea G un monoide y $a \in G$. Decimos que un elemento $b \in G$ es un inverso izquierdo (resp. derecho) de a si $ba = e$ (resp. $ab = e$), donde e es la identidad de G. Si b es inverso tanto izquierdo como derecho, entonces b es un inverso de a.

Proposición:

Sea G un monoide, y $a \in G$. Suponga que $b, c \in G$ son tales que $ba = e = ac$. Entonces $b = c$.

Dem:

$$b = be = b(ac) = (ba)c = e \cdot c = c$$

q.e.d.

Corolario

Si G es un monoide y $a \in G$ es tal que tiene un inverso, entonces dicho inverso es único.

Si G es un monoide y $a \in G$ tiene un inverso en G, por la unicidad este se denota por a^{-1}.

Def. Sea G un conjunto no vacío con una operación. Se dice que G es grupo si es un monoide tal que todo elemento tiene inverso en G.

Proposición:

Si G es grupo, entonces en G se cumplen las Leyes de cancelación, es decir, $\forall a,b,c \in G$:

$$ab = ac \Rightarrow b = c$$
$$ba = ca \Rightarrow b = c$$

Dem:

Sean $a,b,c \in G$ tales que $ab = ac$. Veamos que

$$b = e \cdot b = (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot (ac) = (a^{-1}a)c = ec = c$$

Para la otra igualdad el caso es análogo.

q.e.d.

Corolario:

Sea G un grupo. Para cada $a,b,c \in G$ se tiene:

i) $ab = e \Rightarrow b = a^{-1}$. ($\&$ $a = b^{-1}$).

ii) $ab = c \Rightarrow b = a^{-1}c$ ($\&$ $a = cb^{-1}$).

iii) $(a^{-1})^{-1} = a$.

iv) $(ab)^{-1} = b^{-1}a^{-1}$.

Dem:

De i):

$$b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}e = a^{-1}. \quad \&$$
$$a = a \cdot e = a(b \cdot b^{-1}) = (ab)b^{-1} = eb^{-1} = b^{-1}$$

De ii):

$$b = eb = (a^{-1}a)b = a^{-1}(ab) = a^{-1}c \quad \&$$
$$a = ae = a(bb^{-1}) = (ab)b^{-1} = cb^{-1}.$$

De iii):

Como $a \cdot a^{-1} = e$, por i): $a = (a^{-1})^{-1}$.

De iv):

$$(ab)(b^{-1}a^{-1}) = a(b(b^{-1}a^{-1})) = a((bb^{-1})a^{-1}) = a(ea^{-1}) = aa^{-1} = e$$

luego, como $(ab)(ab)^{-1}=e$, entonces $(ab)^{-1}=b^{-1}a^{-1}$.

q.e.d.

Proposición:

Si G es un grupo y $a_0, a_1, \ldots, a_n \in G$, entonces

$$(a_0 a_1 \ldots a_n)^{-1} = a_n^{-1} \ldots a_1^{-1} a_0^{-1}$$

Dem:

Procederemos por inducción sobre n.

- Para $n=1$, el caso se cumple por el corolario anterior.
- Suponga que se cumple para $n=K$.
- Probaremos que se cumple para $n=K+1$. En efecto

$$\begin{aligned}(a_0 a_1 \cdot \ldots \cdot a_K \cdot a_{K+1})^{-1} &= ((a_0 a_1 \ldots a_K) \cdot a_{K+1})^{-1} \\ &= a_{K+1}^{-1} \cdot (a_0 a_1 \ldots a_K)^{-1} \\ &= a_{K+1}^{-1} a_K^{-1} \cdot \ldots \cdot a_1^{-1} \cdot a_0^{-1}\end{aligned}$$

Aplicando inducción se cumple $\forall\, n \in \mathbb{N}$.

q.e.d.

Sea G un grupo y $a \in G$, definimos las potencias de a: $\forall\, m \in \mathbb{Z}$:

$$a^m := \begin{cases} a^m & \text{si } m > 0 \\ a^0 & \text{si } m = 0 \\ (a^{-1})^{-m} & \text{si } m < 0 \end{cases}$$

Proposición:

Sea G un grupo y $a, b \in G$. Entonces:

i) $a^{m+n} = a^m \cdot a^n$

ii) $a^{mn} = (a^m)^n$

iii) $a^n = (a^{-1})^{-n}$

$\forall\, m, n \in \mathbb{Z}$.

iv) Si G es abeliano: $(ab)^n = a^n b^n$.

Dem:

De (i): Sean $m, n \in \mathbb{Z}$. Si $m \geq 0$ y $n < 0$, entonces:

$$a^m \cdot a^n = a^m \cdot (a^{-1})^{-n}$$

Def. Sea G un grupo. Decimos que G es de orden finito, o simplemente finito, si G como conjunto es finito.
En caso contrario, decimos que G es infinito.

En algunas ocasiones escribimos $|G| < \infty$ o $|G| = \infty$ para establecer la condición de que G sea finito o infinito.
El símbolo $|G|$ representa el cardinal de G.
Si $n \in \mathbb{N}$ y $|G| = n$, entonces G tiene n-elementos. Si $|G| = \aleph_0$, G es numerable, y si $|G| = \mathfrak{c} = c = \aleph_1$, G es no numerable.

Def. Sea G un grupo y $a \in G$. Decimos que a es de orden finito, a lo que se escribe $|a| < \infty$ o $o(a) < \infty$, si existe $m \in \mathbb{N}$ $\ni$ $a^m = e$.

Nota: $|G| = o(G)$, donde "o" denota la cantidad de elementos de G.

Si lo anterior ocurre, entonces al menor entero positivo n tal que $a^n = e$ se le llama el orden de a, y se expresa como:

$$n = |a| = o(a)$$

Si tal entero no existe, decimos que a es de orden infinito, y se expresa como

$$|a| = o(a) = \infty$$

Proposición.

Sea G un grupo y $a \in G$ tal que $|a| < \infty$. Si $m \in \mathbb{Z}$ es tal que $a^m = e$, entonces $|a| \mid m$ (ó $o(a) \mid m$).

Dem:

Sea $n = |a| = o(a)$. Por el algoritmo de la división $\exists!$ $q, r \in \mathbb{Z}$ tales que:

$$m = nq + r, \quad 0 \leq r < n$$

probaremos que $r = 0$. En efecto:

$$e=a^m=a^{nq+r}=a^{nq}\cdot a^r=(a^n)^q\cdot a^r=e^q\cdot a^r=e\cdot a^r=a^r$$

Si $r>0$, entonces $a^r=e \cancel{\ast c}$, pues $|a|=n$ y $r<n$. Por tanto, $r=0$.

De esta forma:

$$m=nq \Rightarrow n|m$$
$$\Rightarrow |a|\,|m$$

q.e.d.

Sea G un grupo y $a\in G$ tal que $n=|a|<\infty$. Si $n=1$, entonces $a=a^1=e$, si $n\geqslant 2$ entonces $a\neq e$. En este último caso, denotamos por

$$A=\{a^m \mid m\in\mathbb{Z}\}$$

Afirmamos que A es finito y tiene n elementos; más aún:

$$A=\{e,a,a^2,\dots,a^{n-1}\}, \text{ donde}$$
$$a^i\neq a^j \ \forall\, i,j\in J_{n-1}\cup\{0\},\ i\neq j.$$

Claramente $\{e,a,\dots,a^{n-1}\}\subset A$, probaremos la otra contención.

Sea $x\in A$, entonces $\exists\, m\in\mathbb{Z} \ni x=a^m$. Por el algoritmo de la división $\exists!\ q,r\in\mathbb{Z}$ tales que:

$$m=nq+r,\ 0\leqslant r<n$$

Entonces:

$$x=a^m=a^{nq+r}=a^{nq}\cdot a^r=(a^n)^q\cdot a^r=e^q\cdot a^r=ea^r=a^r,\ 0\leqslant r\leqslant n-1$$

por tanto, $x\in\{e,a,a^2,\dots,a^{n-1}\}$, así

$$A=\{e,a,a^2,\dots,a^{n-1}\}$$

Además $|A|=n$.

Finalmente, probaremos que $a^i\neq a^j\ \forall\, i,j\in J_{n-1}\cup\{0\}$, $i\neq j$. Sean $i,j\in\mathbb{Z}$, $0\leqslant i<j\leqslant n-1$. Suponga que $a^i=a^j$, entonces:

$$a^i=a^j\Rightarrow a^{j-i}=e$$

donde $0<j-i<j\leqslant n-1$, luego $j-i\in J_{n-1}\cup\{0\}$ y $a^{j-i}=e$ con $j-i<n$

$\neq c$, pues $|a| = n$, por tanto $a^i \neq a^j$.

q.e.d.

Si $|a| = \infty$ y $A = \{\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots\}$. Se tiene que $\forall i, j \in \mathbb{N}$, $i < j \Rightarrow a^i \neq a^j$ (de manera similar a lo anterior). Así $|A| = \aleph_0$.