Lista 5.

1. Sea G un grupo. Pruebe que G es abeliano si, y sólo si la función de G en sí mismo dada por la correspondencia $a \longmapsto a^{-1}$ es un automorfismo de G.

Dem:

$\Rightarrow$) Suponga que G es abeliano. Probaremos que $f: G \to G$ dada como:

$$\forall a \in G,\ f(a) = a^{-1}$$

es automorfismo. Claramente f está bien definida.

a) f es homomorfismo.

Sean $a, b \in G$, entonces

$$f(ab) = (ab)^{-1}, \text{ como } G \text{ es abeliano, } (ab)^{-1} = a^{-1}b^{-1}$$

$$\Rightarrow f(ab) = a^{-1}b^{-1} = f(a)f(b)$$

b) f es monomorfismo.

Sean $a, b \in G$ m $f(a) = f(b)$:

$$f(a) = f(b) \Rightarrow a^{-1} = b^{-1} \Rightarrow a = b$$

c) f es epimorfismo.

Sea $g \in G$, $\exists$ $g^{-1} \in G$ tal que

$$f(g^{-1}) = (g^{-1})^{-1} = g$$

Por a) – c), f es automorfismo, luego $f \in \mathrm{Aut}(G)$.

$\Leftarrow$) Suponga que $f(a) = a^{-1}$, $\forall a \in G$ es un automorfismo de G. Sean $x, y \in G$, entonces

Como f es automorfismo:

$$f(xy) = f(x)f(y)$$

$$\Rightarrow (xy)^{-1} = x^{-1}y^{-1}$$

por un problema, lo anterior implica que G es abeliano.

q.e.d.

2. Pruebe que no existe un isomorfismo entre los grupos $\mathbb{K}$ y $\mathbb{K}^*$, donde $\mathbb{K}$ es el campo de los racionales, reales ó complejos.

Dem:

$(\mathbb{K},+)$ y $(\mathbb{K}^*,\cdot)$ son isomorfos. En efecto, sea $f:\mathbb{K}\to\mathbb{K}^*$ dada como:

$$\forall x\in\mathbb{K},\ f(x)=e^x$$

f es isomorfismo.

q.e.d.

racionales, reales ó complejos.

3. Sean f un automorfismo de un grupo G y $a \in G$. Pruebe que a y $f(a)$ son del mismo orden.

4. Sean G un grupo cíclico generado por $a \in G$ y G_1 cualquier grupo. Pruebe que todo homo-

Dem:

Sea $a\in G \ni |a|=m$. Entonces:

$$f(a)^m = f(a)\cdots f(a) = f(a^m) = f(e) = e$$

$\forall f\in \mathrm{Aut}(G)$. Así $|f(a)|=n\leq m$. Suponga que $n<m$. Como $f^{-1}\in\mathrm{Aut}(G)$:

$$a^n = f^{-1}(f(a))^n = f^{-1}(f(a)^n) = f^{-1}(e) = e \ \#c$$

pues $|a|=n$. Por tanto, $|f(a)|=m$.

q.e.d.

4. Sean G un grupo cíclico generado por $a \in G$ y G_1 cualquier grupo. Pruebe que todo homomorfismo $f : G \longrightarrow G_1$ está completamente determinado por $f(a) \in G_1$. Más precisamente, pruebe que $f(G) = \langle f(a)\rangle$.

Dem:

$G=\langle a\rangle$. Probaremos que $f(G)=\langle f(a)\rangle$.

a) Sea $x\in f(G)$, entonces $\exists\, m\in\mathbb{Z} \ni x=f(a^m)=f(a)^m \Rightarrow x\in\langle f(a)\rangle$.

b) Sea $x\in\langle f(a)\rangle$, entonces $\exists\, m\in\mathbb{Z}\ni x=f(a)^m=f(a^m)\in f(G)$.

Por a) y b), $f(G)=\langle f(a)\rangle$.

q.e.d.

5. Sea G un grupo cíclico. Pruebe que el grupo $\mathrm{Aut}(G)$ de los automorfismos de G es isomorfo a $\mathbb{Z}/2\mathbb{Z}$ si G es grupo cíclico infinito, y que $\mathrm{Aut}(G)$ es isomorfo a $(\mathbb{Z}/n\mathbb{Z})^*$ si G es grupo cíclico finito de n elementos.

Dem:

Tenemos 2 casos:

a) G es infinito. Como G es grupo cíclico infinito, si a es generador de G, a^{-1} también lo es y, a, a^{-1} son los únicos generadores de G.

Claramente $id \in Aut(G)$. Sea ahora $f \in Aut(G)$, $f \neq id$. Probaremos el resultado:

Si $f'(a) = a \Leftrightarrow f' = id$.

Sea $m \in \mathbb{Z}$, entonces $f'(a^m) = f'(a)^m = a^m$. Por tanto $f' = id$.

Como a es generador de G, $G = \langle a \rangle = \langle a^{-1} \rangle$ y, a, a^{-1} son los únicos generadores (por ser G infinito). Por ④, $G = \langle f(a) \rangle$, pero $f(a) \neq a$, pues $f \neq id$.

Por tanto, $f(a) = a^{-1}$.

Sea $m \in \mathbb{Z}$, entonces: $f(a^m) = f(a)^m = a^{-m} = (a^m)^{-1}$. Por tanto, $f = inv$, donde $\forall x \in G$, $inv(x) = x^{-1}$.

De esta forma, $Aut(G) = \{id, inv\}$. Sea $H : Aut(G) \to \mathbb{Z}/2\mathbb{Z}$ dada como:

$$H(id) = [0], \quad H(inv) = [1]$$

claramente H es biyectiva, y

$$H(id \circ id) = H(id) = [0] = [0] + [0]$$
$$H(inv \circ id) = H(inv) = [1] = [1] + [0]$$
$$H(id \circ inv) = H(inv) = [1] = [0] + [1]$$
$$H(inv \circ inv) = H(id) = [0] = [1] + [1]$$

por tanto, H es isomorfismo, así $Aut(G) \cong \mathbb{Z}/2\mathbb{Z}$.

b) G es finito de orden $n \in \mathbb{N}$. Como $G = \langle a \rangle$ con $a \in G$, G tiene $\varphi(n)$ generadores, a saber $G = \langle a^m \rangle$ si $m \in \mathbb{N}$ ~~m~~ $1 \leq m \leq n-1$ y $(m,n) = 1$. Asumiremos $n \geq 2$.

Sea $f \in Aut(G)$, por ④:

$$G = \langle f(a) \rangle$$

Así, $f(a)$ puede tener $\varphi(n)$ opciones diferentes. Si $f(a) = a^l$ con $l \in \mathbb{N}$, $1 \leq l \leq$

$n-1$, $(l,n)=1$, entonces:

$$\forall m \in \mathbb{Z},\ f(a^m) = f(a)^m$$
$$= a^{lm}$$
$$= (a^m)^l$$

por tanto, $\forall x \in G$, $f(x) = x^l$. Así f queda univocamente determinada por $f(a)$, i.e f tiene $\varphi(n)$ opciones. Por tanto:

$$Aut(G) = \{ f_m : G \to G \mid f_m(x) = x^m, \forall x G \text{ y } m \in \mathbb{N} \text{ ∍ } 1 \leq m \leq n-1,\ (m,n) = 1 \}$$

Considere el grupo $(\mathbb{Z}/n\mathbb{Z})^*$. Tomemos $H: Aut(G) \to (\mathbb{Z}/n\mathbb{Z})^*$ como:

$$\forall f_m \in Aut(G),\ H(f_m) = [m].$$

H está bien definida. Veamos que es isomorfismo:

a) Sean $f_m, f_l \in Aut(G)$ ∍ $H(f_m) = H(f_l)$, entonces:

$$[m] = [l] \Rightarrow [0] = [l-m]$$
$$\Rightarrow n \mid l-m$$

Pero $1 \leq l, m \leq n-1 \Rightarrow 0 < l, m < n \Rightarrow -n < l-m < n$. Así, si $n \mid l-m \Rightarrow$ $l-m = 0$. Por tanto $l = m \Rightarrow f_n = f_m$.

b) Sea $[m] \in (\mathbb{Z}/n\mathbb{Z})^*$. Por el algoritmo de la división, $\exists\, q, r \in \mathbb{Z}$ ∍

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

por resultados previos, $1 \leq r \leq n-1$, $(r,n) = 1$, y $[m] = [r]$. Así $\exists\, f_r \in Aut(G)$ tal que:

$$H(f_r) = [r] = [m].$$

c) Sean $f_m, f_l \in Aut(G)$, entonces:

$$f_m \circ f_l(x) = x^{ml},\ \forall x \in G.$$

Por el alg. de la div $\exists\, q, r \in \mathbb{Z}$ ∍

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

Como $(m,n)=(l,n)=1$. Como $n \geq 2 \Rightarrow n \nmid ml \Rightarrow r \neq 0$. Por tanto:

$$1 \leq r \leq n-1, \text{ como } (m,n)=(l,n)=1,$$

entonces $(r,n)=1$. Por lo tanto $f_r \in \mathrm{Aut}(G)$, y además:

$$\forall x \in G,\ f_{ml}(x) = x^{ml} = x^{nq+r} = (x^n)^q \cdot x^r \text{. como } |G| = n$$
$$= e^q \cdot x^r = x^r = f_r(x)$$

Por tanto, $f_{ml} = f_r$. Por lo tanto:

$$\begin{aligned} H(f_m \circ f_l) &= H(f_{ml}) \\ &= H(f_r) \\ &= [r] \\ &= [ml] \\ &= [m]\cdot[l] \\ &= H(f_m)\cdot H(f_l) \end{aligned}$$

Luego, H es homomorfismo.

Por a) - c), $\mathrm{Aut}(G) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

q.e.d.

6. Pruebe que $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$, $\mathrm{Aut}(\mathbb{Z}/6\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$, $\mathrm{Aut}(\mathbb{Z}/8\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ y $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/(p-1)\mathbb{Z}$ (p número primo).

Dem:

Por 5, $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$, pues $\mathbb{Z} = \langle 1 \rangle$ y $|\mathbb{Z}| = \aleph_0$. Probaremos que $(\mathbb{Z}/n\mathbb{Z})^* \cong \mathbb{Z}/\varphi(n)\mathbb{Z}$.

8. Pruebe que los únicos grupos de orden 4 (salvo isomorfismos) son $\mathbb{Z}/4\mathbb{Z}$ y $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

9. *a*) Pruebe que si se tienen dos grupos del tipo D_4, entonces éstos son isomorfos.

Dem:

Sea G un grupo m $|G|=4$. Tenemos 2 casos:

a) G es cíclico.

Si G es cíclico, $\exists\, a \in G$ m $G=\langle a \rangle$, como $|G|=4 \Rightarrow |a|=4$. Así $G=\{e,a,a^2,a^4\}$. Sea $h: G \to \mathbb{Z}/4\mathbb{Z}$ dada como:

$$\forall\, m \in \mathbb{Z},\ h(a^m)=[m]$$

h está bien definida: Sean $m,n \in \mathbb{Z}$ m $a^m=a^n \Rightarrow a^{m-n}=e \Rightarrow 4 \mid m-n \Rightarrow m \equiv n \bmod 4 \Rightarrow [m]=[n] \Rightarrow h(a^m)=h(a^n)$.

i) h es homomorfismo

Sean $m,n \in \mathbb{Z}$. Entonces

$$h(a^m \cdot a^n) = h(a^{m+n}) = [m+n] = [m]+[n] = h(a^m)+h(a^n)$$

ii) h es inyectiva.

Sean $m,n \in \mathbb{Z}$ m $[m]=[n] \Rightarrow m \equiv n \bmod 4 \Rightarrow 4 \mid m-n \Rightarrow a^{m-n}=e \Rightarrow a^m=a^n$.

iii) h es biyectiva

$\forall\, [m] \in \mathbb{Z}/4\mathbb{Z}\ \exists\, m \in \mathbb{Z}$ m $h(a^m)=[m]$.

Por i)–iii), h es isomorfismo, así $G \cong \mathbb{Z}/4\mathbb{Z}$.

b) G no es cíclico.

Como G no es cíclico, $\forall\, g \in G$, $|\langle g \rangle| = 1$ ó 2. Si $|g|=1 \Rightarrow g=e$. Así $|g|=2$, $\forall\, g \neq e$.

Digamos que $G=\{e,a,b,c\}$, donde $|a|=|b|=|c|=2$. Veamos que

- $ab \neq e$, pues en tal caso, $b=a^{-1}=a$ $\#_c$, pues $a \neq b$.
- $ab \neq a$, pues en tal caso $b=aa^{-1}=e$ $\#_c$ pues $b \neq e$
- $ab \neq b$, pues en tal caso, $a=e$ $\#_c$ pues $a \neq e$.

Por tanto, $ab=c$. Por ser G de orden $4=2^2$ y ser 2 primo, G es abeliano, así $ab=ba$.
En resumen, $G=\{e,a,b,ab\}$. Sea $h: G \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ dada como:

$$h(e)=([0],[0]),\ h(a)=([1],[0]),\ h(b)=([0],[1]),\ h(ab)=([1],[1])$$

Claramente h es biyectiva. Veamos que es homomorfismo:

q.e.d.

9. a) Pruebe que si se tienen dos grupos del tipo D_4, entonces éstos son isomorfos.
   b) Haga lo mismo que en (a) para Q_8.

Dem:

La prueba de b) es igual que la de a). Por tanto, basta con probar a):
Sean D_4 y D_4' dos grupos, dados como:

$$D_4=\{a^i b^j \mid i=0,1,\ j=0,\dots,3\},\ \text{con } a^2=b^4=e,\ ab=b^{-1}a.$$
$$D_4'=\{c^i d^j \mid i=0,1,\ j=0,\dots,3\}\ \text{con } c^2=d^4=e,\ cd=d^{-1}c.$$

$\forall\, a^i b^j \in D_4$, $i=0,1$ y $j=0,\dots,3$. $h(a^i b^j)=c^i d^j$ es un isomorfismo.

q.e.d.

10. Sean f un epimorfismo de un grupo G en un grupo G_1, y K el kernel de f. Pruebe que para cada $a \in G$, $Ka = f^{-1}(\{f(a)\})$.

Dem:

Sea $a \in G$.

a) $x \in Ka \Rightarrow x = ka$, con $k \in \operatorname{Ker} f \Rightarrow f(x)=f(ka)=f(a) \Rightarrow x \in f^{-1}(f(a))$.

b) $x \in f^{-1}(\{f(a)\}) \Rightarrow f(x)=f(a) \Rightarrow f(xa^{-1})=e \Rightarrow xa^{-1} \in K \Rightarrow x \in Ka$.

Por a) y b), $Ka = f^{-1}(\{f(a)\})$.

q.e.d.

11. Sea G un grupo abeliano finito de orden n, y sea $m \in \mathbb{N}$ tal que $(m,n)=1$. Pruebe que para todo $g \in G$ existe $x \in G$ tal que $g = x^m$. (Sugerencia: considere la función $f: G \longrightarrow G$ dada por $f(x)=x^m$ para cada $x \in G$, y pruebe que $f \in \operatorname{Aut}(G)$).

Dem:

Probaremos que $f: G \to G$ dada como: $f(x) = x^m$, $\forall x \in G$ es un automorfismo de G. Claramente f está bien definida.

a) Sean $a, b \in G$, entonces:

$$\begin{aligned} f(ab) &= (ab)^m, \text{ como } G \text{ es abeliano} \\ &= a^m b^m \\ &= f(a) f(b) \end{aligned}$$

b) Sea $a \in G$:

$a \in \operatorname{Ker} f \Rightarrow f(a) = e = a^m$, como G es finito, el orden de a es $|a| = l$, donde l es tal que $l \mid n$ (pues, $a^{|G|} = e$). Pero $a^m = e$, luego $l \mid m$. Por tanto, $l \leq (m, n) = 1$. Como $l \in \mathbb{N} \Rightarrow l = 1$. Así $a = e$.

Por tanto, $\operatorname{Ker} f = \{e\} \Rightarrow f$ es inyectiva.

c) Sea $g \in G$. Como $(m,n) = 1$, $\exists\ q, s \ \ni\ mq + ns = 1 \Rightarrow mq = 1 - ns$. Por tanto, $\exists\ g^q \in G \ \ni$

$$\begin{aligned} f(g^q) &= g^{mq} \\ &= g^{1-ns} \\ &= g \cdot (g^n)^{-s} \\ &= g \end{aligned}$$

Por a)–c), $f \in \operatorname{Aut}(G)$. Luego $\forall g \in G\ \exists\ x \in G \ \ni\ f(x) = g \Rightarrow g = x^m$.

q.e.d.

12. Sean $a, b \in \mathbb{R}$ con $a \neq 0$, y defina $T_{ab} : \mathbb{R} \longrightarrow \mathbb{R}$ dada por $T_{ab}(x) = ax + b$. Sea $G = \{T_{ab} \mid a, b \in \mathbb{R} \text{ y } a \neq 0\}$ y $N = \{T_{1b} \mid b \in \mathbb{R}\}$. Pruebe que G es un grupo con la operación de composición de funciones tal que $N \lhd G$, y que $G/N \cong \mathbb{R}^*$.

Dem:

Claramente G es grupo. Veamos que $N \lhd G$.

a) Sean $b_1, b_2 \in \mathbb{R}$, entonces:

$$T_{1b_1} \circ T_{1-b_2}(x) = T_{1b_1}(x - b_2) = x + b_2 - b_1 = T_{1b_1 - b_2}(x), \ \forall x \in \mathbb{R}$$

por tanto, $T_{1b_1} \circ T_{1-b_2} \in N$. Así $N < G$.

b) Sean $a,b,c \in \mathbb{R}$, $a \neq 0$. Entonces:

$$\forall\, x \in \mathbb{R}, \quad T_{ab} \circ T_{1c} \circ (T_{ab})^{-1}(x) = T_{ab} \circ T_{1c} \circ T_{\frac{1}{a}-b}(x)$$
$$= T_{ab} \circ T_{1c}\left(\tfrac{1}{a}x - b\right)$$
$$= T_{ab}\left(\tfrac{1}{a}x - b + c\right)$$
$$= x - ab + ac + b$$
$$= T_{1-ab+ac+b}(x)$$

Luego $T_{ab} \circ T_{1c} \circ (T_{ab})^{-1} \in N$. Así $N \lhd G$.

Por lo anterior:

$$G/N = \{ T_{a0} \circ N \mid a \in \mathbb{R}^* \}$$

Sea $f: \mathbb{R}^* \to G/N$ dada como:

$$f(a) = T_{a0} \circ N, \ \forall\, a \in \mathbb{R}^*$$

Claramente f está bien definida. Veamos que:

c) $\forall\, a,b \in \mathbb{R}^*$:

$$f(ab) = T_{(ab)0} \circ N, \text{ como } T_{a0} \circ T_{b0} = T_{(ab)0}, \text{ entonces}$$
$$= T_{a0} \circ T_{b0} \circ N$$
$$= T_{a0} \circ N \circ T_{b0} \circ N, \text{ por ser } N \text{ normal}$$
$$= f(a) \circ f(b)$$

d) Sean $a,b \in \mathbb{R}$ $\ni$ $f(a) = f(b)$, entonces $T_{a0} \circ N = T_{b0} \circ N \Rightarrow T_{a0} \circ T_{\frac{1}{b}0} \in N \Rightarrow \exists\, c \in \mathbb{R}$ $\ni$ $T_{a0} \circ T_{\frac{1}{b}0} = T_{1c} \Rightarrow \frac{a}{b}x + 0 = x + c$, $\forall\, x \in \mathbb{R}$. Si lo anterior sucede $\forall\, x \in \mathbb{R} \Rightarrow$ $c = 0 \Rightarrow \frac{a}{b}x = x, \forall\, x \in \mathbb{R} \Rightarrow \frac{a}{b} = 1 \Rightarrow a = b$.

e) $\forall\, T_{a0} \circ N \ \exists\ a \in \mathbb{R}^*$ $\ni$ $f(a) = T_{a0} \circ N$.

Por c) – e), f es isomorfismo $\Rightarrow G/N \cong \mathbb{R}^*$.

q.e.d.

de funciones tal que $N \lhd G$, y que $G/N \cong \mathbb{R}^*$.

13. Sea D_n el grupo diédrico de grado n tal que $D_n = \{a^i b^j \mid i = 0, 1 \text{ y } j = 0, \ldots, n-1\}$, donde $a, b \in D_n$ con $a^2 = e = b^n$ y $ab = b^{-1}a$. Sea $N = \{e, b, \ldots, b^{n-1}\}$. Pruebe que:

    a) $N \lhd D_n$; y

    b) $D_n/N \cong \{-1, 1\}$.

Dem:

14. Pruebe que todo grupo de orden 9 es abeliano.

15. Sea G un grupo no abeliano de orden 6. Pruebe que $G \cong S_3$.

Dem:

Como $9 = 3^2$ y 3 es primo, entonces G es abeliano.

q.e.d.

14. Pruebe que todo grupo de orden 9 es abeliano.

15. Sea G un grupo no abeliano de orden 6. Pruebe que $G \cong S_3$.

Dem:

Podemos suponer que $G = \{e, a, b, c, d, f\}$. Como G no es abeliano, no puede ser cíclico. Asi $|g| = 1, 2$ ó 3, $\forall g \in G$, más aún, $|g| = 2, 3$, $\forall g \in G \setminus \{e\}$.

Si $|g| = 2$, $\forall g \in G \setminus \{e\} \Rightarrow g^2 = e$, $\forall g \in G$. Por un ejercicio G sería abeliano #c.

Por tanto, $\exists\, g_0 \in G \ni |g_0| = 3$, digamos $g_0 = a$.