PRODUCTOS DIRECTOS

Sean G_1 y G_2 grupos. El producto cartesiano

$$G_1 \times G_2 = \{(g_1, g_2) / g_1 \in G_1 \wedge g_2 \in G_2\}$$

Definimos la operación:

$$(g_1, g_2) \cdot (g_1', g_2') = (g_1 g_1', g_2 g_2')$$

Con esta operación $G_1 \times G_2$ adquiere estructura de grupo.

- Elemento neutro: $(1, 1) = (1_{G_1}, 1_{G_2})$
- Inverso de (g_1, g_2): $(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$

PROPIEDADES

1) $|G_1 \times G_2| = |G_1| |G_2|$

2) $G_1 \times \{1\}$ (resp. $\{1\} \times G_2$) son subgrupos de $G_1 \times G_2$

Además son subgrupos normales

Para comprobarlo tenemos que ver que

$$(g_1, g_2) \cdot (G_1 \times \{1\}) (g_1, g_2)^{-1} \leq G_1 \times \{1\}$$

para todo $(g_1, g_2) \in G_1 \times G_2$.

Veámoslo:

sea $(g, 1) \in G_1 \times \{1\}$ arbitrario,

$$(g_1, g_2)(g, 1)(g_1^{-1}, g_2^{-1}) = (g_1 g g_1^{-1}, g_2 \cdot 1 \cdot g_2^{-1}) =$$

$$= (g_1 g g_1^{-1}, 1) \in G_1 \times \{1\}$$

C.Q.D.

OBSERVACIÓN:

Como $G_1 \times \{1\} \trianglelefteq G_1 \times G_2$ tiene sentido hacer el cociente:

$$\frac{G_1 \times G_2}{G_1 \times \{1\}} \simeq G_2$$

¿Y por qué?

$$\pi: G_1 \times G_2 \longrightarrow G_2 \quad \text{es hom. suprayectivo}$$
$$(g_1, g_2) \longmapsto g_2$$

<u>1er T. de isomorfía</u>:

$$\cancel{G_1 \times G_2 / \ker \pi} = \frac{G_1 \times G_2}{\underline{\underline{G_1 \times \{1\}}}} \simeq \operatorname{Im}\pi = \underline{\underline{G_2}}$$

<u>Ejemplo</u>: $G_1 = \mathbb{Z}/2\mathbb{Z} = \mathbb{Z}/(2) = C_2$; $G_2 = \mathbb{Z}/3\mathbb{Z}$

$$f: \mathbb{Z}/6\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$
$$\overline{m}^6 \longmapsto (\overline{m}^2, \overline{m}^3)$$
$$\overline{3} \longmapsto (\overline{1}, \overline{0})$$

¿ Quién es f^{-1}?

$$f^{-1}: \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \longmapsto \mathbb{Z}/6\mathbb{Z}$$
$$(\overline{a}, \overline{b}) \longmapsto \overline{c}\ ? = 3a+4b$$

Es más difícil, esto es el T. chino del resto.

T. chino dice que $\exists\, c \in \mathbb{Z} \mid \begin{cases} c \equiv a \mod 2 \\ c \equiv b \mod 3 \end{cases}$

En nuestro caso (2,3) podemos tomar

$$c = 3a + 4b$$

efectivamente: $f(c) = (\overline{c}^2, \overline{c}^3) = (\overline{a}^2, \overline{b}^3)$

<u>Ejemplo 2</u>: $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \overset{?}{\xrightarrow{\sim}} \mathbb{Z}/24\mathbb{Z}$

No son isomorfos porque $\mathbb{Z}/24\mathbb{Z}$ tiene un elemento de orden 24 y $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ no.

(el par $(\overline{1}, \overline{1})$ tiene orden 12)

El elemento $(3,5)$ tiene un orden que divide a 12.

• De hecho $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ es el único grupo abeliano de orden 6.

¿Por qué?

Si G es abeliano y $|G|=6$ ha de tener un elemento a, $\mathrm{ord}(a)=2$ y un elemento b, $\mathrm{ord}(b)=3$. entonces

$$(ab)^k \underset{\text{abeliano}}{=} a^k b^k = 1 \Rightarrow k \text{ es un múltiplo de } 6$$

$$\Rightarrow G = \langle ab \rangle$$

De hecho los elementos de G son:

ab, $\cancel{a^2} b^2$, $a^3 \cancel{b^3} = a$, $\cancel{a^4} b^4 = b$, $a^5 b^5 = a b^2$, $a^6 b^6 = 1$

$$\Longrightarrow \quad G \simeq \mathbb{Z}/6\mathbb{Z}.$$

Ejemplos ¿Y no abelianos de orden 6?

Tenemos al menos $S_3 \simeq D_6$

De hecho S_3 es el único no abeliano de orden 6 (salvo isomorfismo)

Veamos por qué.

Sea G no abeliano con $|G|=6$.

Por la misma razón que antes, deben existir elementos $a, b \in G$ con $\mathrm{ord}(a)=2$ y $\mathrm{ord}(b)=3$.

Debe ocurrir que $G=\langle a,b \rangle$ porque $\langle a,b \rangle$ contiene al menos los elementos $1, a, b, b^2$ y su orden $|G|=6$ debe ser un múltiplo de $|\langle a,b \rangle|$

De hecho $G = \{1, a, b, b^2, ab, ab^2\}$
(pues, claramente, estos 6 elementos son distintos)

Además $\langle b \rangle$ es el único 3-grupo de Sylow de orden 3
(puesto que $n_3 = 1, 4, 7, \dots$ y $n_3 | 6$)

Así que debemos tener:

$$ab \neq ba \Leftrightarrow aba^{-1} \neq b \Rightarrow aba^{-1} = b^2$$

($ab = ba \Rightarrow G$ abel.)

b y b^2 son los únicos elementos de orden 3

Luego $G = \langle a, b : a^2 = b^3 = 1, aba^{-1} = b^2 \rangle \Rightarrow$

$\Rightarrow G \simeq D_6 \cong S_3$ C.Q.D.

A partir de los ejemplos anteriores podemos enunciar la siguiente

PROPOSICIÓN: Salvo isomorfismo, sólo hay dos grupos G con $|G| = 6$:

1) $G \cong \mathbb{Z}/6\mathbb{Z}$ (si G es abeliano)
2) $G \cong S_3$ (si G no es abeliano)

Del mismo modo podemos definir el producto directo de cualquier número finito de grupos:

Definition 5.1. For any finite collection of groups $G_1, \dots, G_n$ we define their direct product to be the group

$$\prod_{i=1}^{i=n} G_i = G_1 \times \dots \times G_n,$$

defined through the binary operation

$$(g_1, \dots, g_n)(g'_1, \dots, g'_n) = (g_1 g'_1, \dots, g_n g'_n).$$

Exercise 5.2. Prove that $\prod_{i=1}^{i=n} G_i$ is a group, and determine its identity element and the inverse of each of its elements. Prove that it is abelian of and only if each group G_i is abelian. Prove that

$$|\prod_{i=1}^{i=n} G_i| = \prod_{i=1}^{i=n} |G_i|,$$

and in particular that $\prod_{i=1}^{i=n} G_i$ is finite if and only if each group G_i is finite.

Lemma 5.5. *Let $G_1, \dots, G_n$ be groups. Fix j with $1 \leq j \leq n$.*

(i) *The subgroup*

$$\{(1, 1, \dots, 1, g_j, 1, \dots, 1) : g_j \in G_j\} \tag{31}$$

is normal in $\prod_{i=1}^{i=n} G_i$, and is also canonically isomorphic to G_j. By abuse of notation we denote the subgroup (31) by G_j.

(ii) *In the notation of claim (i) we have a canonical isomorphism*

$$(\prod_{i=1}^{i=n} G_i)/G_j \cong \prod_{i \neq j} G_i$$

(with i running over the integers from 1 to n that are different from j).

(iii) *The surjective homomorphism*

$$\pi_j : \prod_{i=1}^{i=n} G_i \to G_j$$

defined by

$$\pi_j((g_1, \dots, g_n)) := g_j$$

has

$$\ker(\pi_j) \cong \prod_{i \neq j} G_i.$$

(iv) *In the notation of claim (i), if x belongs to the subgroup G_j of $\prod_{i=1}^{i=n} G_i$ and y belongs to the subgroup G_k of $\prod_{i=1}^{i=n} G_i$ for some $k \neq j$, then $xy = yx$.*

En el caso particular en el que H, K son subgrupos de un mismo grupo G, tenemos una aplicación

$$f : H \times K \longmapsto G$$
$$(h, k) \longmapsto hk$$

En principio f no tiene por qué ser un homomorfismo

¿Recordáis quién es $\operatorname{Im} f$?.

Se denotaba por HK

Definition 3.47. Let G be a group and let H and K be subgroups of G. We define a set

$$HK := \{hk : h \in H, k \in K\}.$$

Como f no tiene por qué ser un homomorfismo, su $\operatorname{Im} f = HK$ no tiene por qué ser un subgrupo

Teníamos:

Proposition 3.51. *Let G be a group and let H and K be subgroups of G. Then HK is a subgroup of G if and only if $HK = KH$.*

Corollary 3.53. *If H and K are subgroups of G for which K is contained in $N_G(H)$, the set HK is a subgroup of G.*

In particular, given a normal subgroup H of G, the subset HK is a subgroup of G for every subgroup K of G.

El siguiente caso es particularmente interesante:

Lema: Sean H, K subgrupos de G con $H \trianglelefteq G$ (de forma que HK es un subgrupo de G)

Supongamos que i) $H \cap K = \{1\}$

ii) $G = HK$

entonces la aplicación anterior

$$f : H \times K \longrightarrow G \quad (\mathrm{Im} f = HK)$$
$$(h, k) \longmapsto hk$$

es biyectiva.

Demostración

Por hipótesis es suprayectiva

¿e inyectiva?

Veamos que $\ker f = \{(1,1)\}$

Sea $(h,k) \in \ker f \Rightarrow f(h,k) = hk = 1 \Rightarrow$

$\Rightarrow h = k^{-1} \in H \cap K = \{1\} \Rightarrow h = k = 1 \Rightarrow$

$\Rightarrow \ker f = \{(1,1)\}$

¿Algún problema? Nadie nos ha dicho que f sea un homomorfismo

(e.g.: $f : \mathbb{Z} \longrightarrow \mathbb{Z}$, $0 \longmapsto 0$, $x \longmapsto 5, \forall x \neq 0$ $\quad f^{-1}(\{0\}) = \{0\} \not\Rightarrow f$ se inyectiva)

Inyectividad (ahora, bien)

$f(h,k) = f(h',k') \Rightarrow \underline{(h,k) = (h',k')}$

$f(h,k) = f(h',k') \Rightarrow hk = h'k' \Rightarrow \underbrace{(h')^{-1}h}_{H} = \underbrace{k'k^{-1}}_{K}$

$$\Rightarrow (h')^{-1} h = k' k^{-1} \in H \cap K = \{1\} \Rightarrow$$

$$\Rightarrow \begin{cases} (h')^{-1} h = 1 \\ k' k^{-1} = 1 \end{cases} \Rightarrow \left.\begin{matrix} h = h' \\ k = k' \end{matrix}\right\} \Rightarrow (h,k) = (h',k')$$

Observación: En el caso de grupos finitos una condición para que se cumpla $G = HK$ es pedir $|H||K| = |G|$ porque al ser f inyectiva se tiene $|\operatorname{Im} f| = |HK| = |H \times K| = |H||K| = |G|$

• otra forma de decir que f es inyectiva es:

Exercise 5.11. Let H and K be subgroups of a group G and assume that $H \cap K = \{1\}$. Show that every element of HK has a unique expression as a product hk with $h \in H$ and $k \in K$.

Observ. Si $f: H \times K \longmapsto G$ fuera un homomorfismo no sólo tendríamos una forma (un poco) más fácil de probar la inyectividad sino que tendríamos

$$f: H \times K \xrightarrow{\sim} G \text{ (isomorfismo)}$$

(i.e. que G sería el producto directo de sus subgrupos H y K)

¡Esto va a ocurrir cuando no sólo H es normal, sino que también $K \trianglelefteq G$!

Corollary 5.14. *Let G be a group and let H and K be normal subgroups of G which satisfy both*

$$H \cap K = \{1\}$$

and

$$HK = G.$$

Then G is isomorphic to $H \times K$.

Demostración Tenemos que ver que $f: H\times K \to G = HK$, $(h,k) \mapsto hk$ es un homomorfismo.

- $f(h,k)f(h',k') = hk\,h'k'$
- $f((h,k)(h',k')) = f(hh', kk') = hh'kk'$

Tenemos que convencernos de que

$$\cancel{h}k\,h'\cancel{k'} = \cancel{h}h'k\cancel{k'} \Leftrightarrow kh' = h'k \Leftrightarrow$$

$$1 = (h'k)^{-1}kh' \Leftrightarrow 1 = \underbrace{k^{-1}h'^{-1}k}_{H}h' \in H \cap K = \{1\} \quad ✓$$

$$1 = k^{-1}\underbrace{h'^{-1}kh'}_{K}$$

— o —

Observación: Hemos visto que en esta situación $hk = kh$ $\forall k \in K, \forall h \in H$ (lo cual es mucho más que decir que $KH = HK$ y mucho menos que decir que K y H están contenidos en el centro de G)

. Como en otras situaciones, este resultado se generaliza al caso de un número finito de subgrupos:

Theorem 5.12. *Let G be a group and let $H_1, \ldots, H_n$ be* **normal** *subgroups of G with the property that*

$$H_j \cap (H_1 \ldots H_{j-1} H_{j+1} \ldots H_n) = \{1\} \tag{33}$$

for each $1 \leq j \leq n$. Then

$$H_1 \ldots H_n \cong H_1 \times \ldots \times H_n. \tag{34}$$

Lo importante es que si $H \trianglelefteq G \Rightarrow HK$ es un grupo y si, además, $K \trianglelefteq G \Rightarrow$
$\Rightarrow HK \cong H \times K$ y el isomorfismo viene dado por

$$\begin{aligned} H \times K &\xrightarrow{f} HK \\ (h,k) &\longmapsto hk \end{aligned}$$

¿Y qué pasa si K no es normal? ¿es todavía cierto que $HK \simeq H \times K$?

$\Updownarrow$

¿es todavía cierto que f es un homom?

Nos estamos preguntando si en el caso $K \ntrianglelefteq G$ se verifica todavía:

$$\underbrace{f(h,k)f(h',k')}_{\substack{\| \\ hkh'k' \\ \| \\ hkh'k^{-1}kk' \,=\, f(h\cdot kh'k^{-1},\, kk')}} = f((h,k)(h',k')) = \underbrace{f(hh', kk')}_{\substack{\| \\ hh'kk'}}$$

Esto lo que me dice es que $f(h,k)f(h',k')$ no coincide con $f(hh',kk')$ sino con $f(h\cdot kh'k^{-1}, kk')$

Entonces f sería un homomorfismo si

hubiéramos definido la operación en $H \times K$ de la siguiente manera:

$$(h,k) * (h',k') = (h \cdot \underbrace{kh'k^{-1}}_{\tau(k)(h')}, kk')$$

Pero, claro, esta operación no parece que vaya a definir una estructura de grupo

• Sin embargo sí que lo va a ser

y el correspondiente grupo se va a llamar producto semidirecto de H y K

y se va a denotar por $\boxed{H \rtimes K}$

Una vez que lo probemos vamos a tener:

Theorem 5.29. *Let G be a group. Let H be a normal subgroup of G. Let K be a subgroup of G. Assume that*

$$H \cap K = \{1\}.$$

Let

$$\tau : K \to \mathrm{Aut}(H)$$

be given by

$$\tau(k)(h) := khk^{-1}.$$

Then $HK \cong H \rtimes_\tau K$.

If in particular $G = HK$ then $G \cong H \rtimes_\tau K$, via the isomorphism $f : H \rtimes K \xrightarrow{\sim} G = HK$, $(h,k) \longmapsto hk$

Pero falta ver que esta operación define una estructura de grupo

$$(h,k) * (h',k') = (h \circ \tau(k)(h'), kk')$$

donde $\tau(k)(h') = kh'k^{-1}$

observación $\tau : K \longrightarrow \mathrm{Aut}(H)$ homom

$k \longmapsto \tau(k) : H \longrightarrow khk^{-1}$

Más generalmente vamos a tener:

PRODUCTOS SEMIDIRECTOS

Theorem 5.20. *Let H and K be groups and let*

$$\rho : K \to \mathrm{Aut}(H)$$ (e.g. nuestro τ anterior)

be a group homomorphism. We define a binary operation $\star_\rho$ on the set $H \times K$ by

$$(h,k) \star_\rho (h',k') := (h \cdot (\rho(k)(h')), k \cdot k').$$

(luego si $\rho(k) \equiv id$, este es el producto usual)

Then the following claims are valid.

(i) *The pair $(H \times K, \star_\rho)$ is a group of order $|H||K|$* que se denota por $H \rtimes_\rho K$.

(ii) *The sets*

$$\tilde{H} := \{(h,1) : h \in H\} \text{ and } \tilde{K} := \{(1,k) : k \in K\}$$

are subgroups of $(H \rtimes_\rho K, \cancel{\star_\rho})$ and the maps $h \mapsto (h,1)$ for $h \in H$ and $k \mapsto (1,k)$ for $k \in K$ define isomorphisms

$\left(\begin{array}{l} H \longrightarrow \tilde{H} \\ h \longmapsto (h,1) \end{array} \right)$

$$H \cong \tilde{H} \text{ and } K \cong \tilde{K}.$$

(iii) *The subgroup $\tilde{H}$ is normal in $(H \times K, \star_\rho) =: H \rtimes_\rho K$.*

(iv) *$\tilde{H} \cap \tilde{K} = \{1\}$* ~~and $\tilde{H} \star_\rho \tilde{K} = (H \times K, \star_\rho)$~~. En particular. $H \rtimes_\rho K = \tilde{H}\tilde{K}$.

(v) *For $x = (h,1) \in \tilde{H}$ and $y = (1,k) \in \tilde{K}$ one has*

$$\tau(y)(x) := y \star_\rho x \star_\rho y^{-1} = (\rho(k)(h), 1).$$

vi) La aplicación $f : \tilde{H} \rtimes \tilde{K} = \tilde{H} \rtimes_\rho \tilde{K} \longrightarrow H \rtimes_\rho K$ es un isomorfismo.

$$((h,1),(1,k)) \longmapsto (h,1) \star_\rho (1,k) = (h,k)$$

Proof. We first show $\star_\rho$ is associative. Let $a,b,c \in H$ and $x,y,z \in K$. Then

$$\begin{aligned}
((a,x) \star_\rho (b,y)) \star_\rho (c,z) =& (a(\rho(x)(b)), xy) \star_\rho (c,z) \\
=& (a(\rho(x)(b))(\rho(xy)(c)), xyz) \\
=& (a(\rho(x)(b))(\rho(x)(\rho(y)(c))), xyz) \\
=& (a(\rho(x)(b(\rho(y)(c)))), xyz) \\
=& (a,x) \star_\rho (b(\rho(y)(c)), yz) \\
=& (a,x) \star_\rho ((b,y) \star_\rho (c,z)).
\end{aligned}$$

The element $(1,1)$ is the identity because

$$\rho : K \xrightarrow{\text{homom.}} \mathrm{Aut}(H), \quad 1 \longmapsto id$$

$$\begin{aligned}
(h,k) \star_\rho (1,1) = (h\underbrace{(\rho(k)(1))}_{1}, k1) = (h1, k1) = (h,k) \\
= (\underbrace{\rho(1)}_{id}(h), k) = (1(\underbrace{\rho(1)}_{id}(h)), 1k) = (1,1) \star_\rho (h,k).
\end{aligned}$$

Given $(h,k) \in H \times K$ the inverse element is

$$(h,k)^{-1} := (\rho(k^{-1})(h^{-1}), k^{-1}).$$

Indeed,

$$
\begin{aligned}
(h,k) \star_\rho (h,k)^{-1} =& (h,k) \star_\rho (\rho(k^{-1})(h^{-1}), k^{-1})\\
=& (h(\rho(k)(\rho(k^{-1})(h^{-1})), kk^{-1}) = (h\,\underbrace{\rho(kk^{-1})}_{id}(h^{-1}), kk^{-1})\\
& \cancel{= (h(\rho(k)(\rho(k)^{-1}(h^{-1})), kk^{-1})}\\
=& (hh^{-1}, kk^{-1})\\
=& (1,1)\\
=& (\rho(k^{-1})(1), 1)\\
=& (\rho(k^{-1})(h^{-1}h), k^{-1}k =\\
=& ((\rho(k^{-1})(h^{-1}))(\rho(k^{-1})(h)), k^{-1}k)\\
=& (\rho(k^{-1})(h^{-1}), k^{-1}) \star_\rho (h,k)\\
=& (h,k)^{-1} \star_\rho (h,k).
\end{aligned}
$$

The order of the group $(H \times K, \star_\rho)$ is just the cardinality of $H \times K$ which is just $|H||K|$. This completes the proof of claim (i).

ii) We have $\tilde{H} = \{(h,1)\}$ es un subgrupo de $H \rtimes H$ $\quad (\rho : K \to Aut(H),\ 1 \mapsto id)$

(40) $$(h,1) \star_\rho (h',1) = (h(\rho(1)(h')), 11) = (hh', 1)$$

and

$$(h,1)^{-1} = (\rho(1)(h^{-1}), 1) = (h^{-1}, 1)$$

so $\tilde{H}$ is a subgroup of G. Moreover the function $f_H : H \to \tilde{H}$ given by $f_H(h) = (h,1)$ is a homomorphism because (40) implies that

$$f_H(hh') = (hh',1) = (h,1) \star_\rho (h',1) = f_H(h) \star_\rho f_H(h').$$

Since f_H is clearly a bijection, it is an isomorphism $H \cong \tilde{H}$.

We have

(41) $$(1,k) \star_\rho (1,k') = (1(\rho(k)(1)), kk') = (11, kk') = (1, kk')$$

and

$$(1,k)^{-1} = (\rho(k^{-1})(1), k^{-1}) = (1, k^{-1})$$

so $\tilde{K}$ is a subgroup of G. Moreover the function $f_K : K \to \tilde{K}$ given by $f_K(k) = (1,k)$ is a homomorphism because (41) implies that

$$f_K(kk') = (1,kk') = (1,k) \star_\rho (1,k') = f_K(k) \star_\rho f_K(k').$$

Since f_K is clearly a bijection, it is an isomorphism $K \cong \tilde{K}$. This completes the proof of claim (ii).

iv) It is clear that $\tilde{H} \cap \tilde{K} = \{1\}$ ~~and also that $\tilde{H} \rtimes_\rho \tilde{K} = (H \times K, \star_\rho)$~~, so (iv) is valid.

Además vimos que en esta situación $f : \tilde{H} \times \tilde{K} \to H \rtimes_\rho K = G$, $(x,y) \mapsto xy$ era inyectiva. Luego:

$$
\left.
\begin{array}{l}
|\tilde{H} \times \tilde{K}| = |\mathrm{Im} f| = |\tilde{H} \cdot \tilde{K}| \\
\quad \| \\
|H \times K| = |H||K| = |H \rtimes_\rho K|
\end{array}
\right\} \Rightarrow \underbrace{\tilde{H} \cdot \tilde{K}}_{\mathrm{Im} f} = H \rtimes K.
$$

We prove claim (v) before proving claim (iii). We have

$$\begin{aligned}(1,k)\star_\rho(h,1)\star_\rho(1,k)^{-1} &= (1(\rho(k)(h)),k1)\star_\rho(1,k)^{-1}\\ &= (\rho(k)(h),k)\star_\rho(1,k^{-1})\\ &= ((\rho(k)(h))(\rho(k)(1)),kk^{-1})\\ &= (\rho(k)(h)1,kk^{-1})\\ &= (\rho(k)(h),1).\end{aligned}$$

$(H\times K, \star_\rho) =: H \rtimes_\rho K$

This proves claim (v).

iii) Now claim (v) implies in particular that $\tilde{K} \subseteq N_{(H\times K,\star_\rho)}(\tilde{H})$. Since [redacted] obviously $\tilde{H} \subseteq N_{(H\times K,\star_\rho)}(\tilde{H})$, [redacted] and $\tilde{H}\tilde{K} = H\rtimes_\rho K$

it follows that [redacted] $N_{H\rtimes_\rho K}(\tilde{H}) = H\rtimes_\rho K$

This means that $\tilde{H}$ is normal in $(H\times K,\star_\rho)$, which proves claim (iii) [redacted]

vi) follows from Th. 5.29 (el anterior a éste). □

Definition 5.21. Let H and K be groups and let

$$\rho : K \to \mathrm{Aut}(H)$$

be a group homomorphism. The group $(H\times K,\star_\rho)$ is the 'semidirect product of H and K with respect to ρ' and is denoted by $H \rtimes_\rho K$, or simply by $H \rtimes K$ when ρ is clear from context. y especialmente cuando $\rho(k)$ = conjugación por k, como en los casos anteriores,

$H \rtimes_\rho K$

Notation 5.22. We use the canonical isomorphisms described in Theorem 5.20 (ii) to identify both H of K with subgroups of $H\rtimes_\rho K$, and so we henceforth drop the notation $\tilde{H}$, $\tilde{K}$ and simply write H and K in their place. As usual, we often drop the binary operation $\star_\rho$ from all notation.

Remark 5.23. The symbol $H\rtimes K$ reminds us that, under the identifications of Notation 5.22, H is a normal subgroup of $H\rtimes K$, while K is not necessarily normal in $H\rtimes K$. Unlike the direct product $\times$, the semidirect product $\rtimes$ is certainly not symmetric.

El caso $K \trianglelefteq H\rtimes K$ sólo ocurre cuando $H\rtimes K \cong H\times K$

pues ya vimos que $H\rtimes K = \tilde{H}\cdot\tilde{K} \cong \tilde{H}\times\tilde{K} = H\times K$

(si $\tilde{K}$ es también normal)

Ejemplo 1: $\mathbb{Z}/3\mathbb{Z} \rtimes_\rho \mathbb{Z}/2\mathbb{Z} \cong D_6 \cong S_3$

$\rho(1): \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$, $x \mapsto -x$

$\rho(1+1) = \rho(2) = \rho(0) = Id$

$(\rho(1)\circ\rho(1))x = \rho(1)(\rho(1)(x)) =$

$= \rho(1)(-x) = x$

i.e. $\rho(1)\circ\rho(1) = Id$

(ii) Let

$$\rho : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$$

be given by $\rho(0)(x) = x$ and by $\rho(1)(x) = -x$ for $x \in \mathbb{Z}/3\mathbb{Z}$. It is easy to see that ρ is a homomorphism. Then the group $\mathbb{Z}/3\mathbb{Z} \rtimes_\rho \mathbb{Z}/2\mathbb{Z}$ is a non-abelian group of order 6 and therefore it's going to be isomorphic to $S_3 \cong D_6$.

$(0,1)*(1,0) = (0+\rho(1)(1), 1+0) = (0+(-1), 1) = (-1,1) = (2,1)$

$(1,0)*(0,1) = (1+\rho(0)(0), 0+1) = (1+0, 1) = (1,1)$ $\Rightarrow$ no es abel $\Rightarrow$ es S_3.

De hecho, la aplicación

$$\mathbb{Z}/3\mathbb{Z} \rtimes_\rho \mathbb{Z}/2\mathbb{Z} \to D_6$$

given by

$$(0,0) \mapsto 1, \quad (1,0) \mapsto r, \quad (2,0) \mapsto r^2, \quad (0,1) \mapsto s, \quad (1,1) \mapsto sr, \quad (2,1) \mapsto sr^2$$

is an isomorphism.

$(0,1)*(0,1) = (0+\rho(1)0, 1+1) = (0,2) = (0,0) \Rightarrow (0,1)$ es de orden 2

$(1,0)*(1,0) = (1+\rho(0)1, 0+0) = (1+1,0) = (2,0) \Rightarrow (1,0)$ tiene que ser de orden 3

$\underset{s}{(0,1)} * \underset{r}{(1,0)} * \underset{s^{-1}}{(0,1)} = (2,1)*(0,1) = (2+\rho(1)0, 1+1) = \underbrace{(2,0)}_{r^2} \Rightarrow \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \cong D_6$

Ejemplo 2

(iii) More generally, let

$$\rho : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$$

be given by $\rho(0)(x) = x$ and by $\rho(1)(x) = -x$ for $x \in \mathbb{Z}/n\mathbb{Z}$. It is easy to see that ρ is a homomorphism. Then the group $\underline{\mathbb{Z}/n\mathbb{Z} \rtimes_\rho \mathbb{Z}/2\mathbb{Z}}$ is a non-abelian group of order $2n$

$(\underset{\text{II}}{H} \cong \mathbb{Z}/n\mathbb{Z})$

and contains $H = \{(0,0), (1,0), (2,0), \ldots, (n-1,0)\}$ as a normal subgroup. In fact, as a straightforward generalisation of part (ii), one sees that

$$\mathbb{Z}/n\mathbb{Z} \rtimes_\rho \mathbb{Z}/2\mathbb{Z} \to D_{2n}.$$

$\left\{ \begin{array}{l} \rho(x) : \mathbb{Z}/2\mathbb{Z} \longmapsto \mathbb{Z}/2\mathbb{Z} \\ \quad 0 \longmapsto 0 \\ \quad 1 \longmapsto 1 \end{array} \right.$ $\Rightarrow \left\{ \begin{array}{l} \rho : \mathbb{Z}/n\mathbb{Z} \longmapsto \mathrm{Aut}(\mathbb{Z}/2\mathbb{Z}) \\ \quad x \longmapsto \rho(x) = id \end{array} \right. \Rightarrow$

i.e. $\mathrm{Aut}(\mathbb{Z}/2\mathbb{Z}) = \{id\}$

$\Rightarrow \mathbb{Z}/2\mathbb{Z} \rtimes_\rho \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

¡importa el orden!

Ejemplo 3 $\mathbb{Z}/3\mathbb{Z} \rtimes_\rho \mathbb{Z}/4\mathbb{Z}$, $\rho : \mathbb{Z}/4\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$

$\rho : \mathbb{Z}/4\mathbb{Z} \longmapsto \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$

$k = 0, 1, 2, 3$

$$\begin{cases} \rho(k)(x) = (-1)^k x \quad \text{hom.} \\ \rho(1+2)x = \rho(3)\,x = -x \\ (\rho(1)\circ\rho(2))x = \rho(1)(\rho(2)x) = \rho(1)x = -x \end{cases}$$

(v) More generally, for any abelian group H, let

$$\rho : \mathbb{Z}/2n\mathbb{Z} \to \mathrm{Aut}(H)$$

be given by $\rho(k)(x) = (-1)^k x$ for $0 \le k \le 2n-1$ and for $x \in H$. It is easy to see that ρ is a homomorphism.

As an example we consider the case $H = \mathbb{Z}/3\mathbb{Z}$ and $n = 2$. The group ~~$\mathbb{Z}/4\mathbb{Z} \ltimes_\rho \mathbb{Z}/3\mathbb{Z}$~~ $\mathbb{Z}/3\mathbb{Z} \rtimes_\rho \mathbb{Z}/4\mathbb{Z}$ has order 12 and we claim that it is non-abelian, so for instance it cannot have isomorphism class C_{12}, or isomorphism class $C_2 \times C_6$. We also claim that it is not isomorphic to D_{12} or to A_4. In this way, we have used the semidirect product to construct a genuinely new group that we had not encountered previously.

We have

$$(1,1)(2,0) = (1 + \rho(1)(2), 1 + 0) = (1 - 2, 1) = (2,1) \qquad = (-1,1)$$

while

$$(2,0)(1,1) = (2 + \rho(0)(1), 0 + 1) = (2 + 1, 1) = (0,1), \qquad = (3,1) =$$

} no abel,

so $\mathbb{Z}/3\mathbb{Z} \rtimes_\rho \mathbb{Z}/4\mathbb{Z}$ is non-abelian.

In addition D_{12} and A_4 do not have any elements of order 4, but $\mathbb{Z}/3\mathbb{Z} \rtimes_\rho \mathbb{Z}/4\mathbb{Z}$ contains the cyclic subgroup $\mathbb{Z}/4\mathbb{Z}$ of order 4 (~~which in fact~~ • THERE IS A ~~is the~~ unique Sylow 3-subgroup) because it is normal. Therefore $\mathbb{Z}/3\mathbb{Z} \rtimes_\rho \mathbb{Z}/4\mathbb{Z}$ cannot be isomorphic to either D_{12} or A_4.

$$\left.\begin{cases} (0,1) * (0,1) = (0,2) \\ (0,1) * (0,1) * (0,1) = (0,3) \\ (0,1) * (0,1) * (0,1) * (0,1) = (0,4) = (0,0) \end{cases}\right\} \Rightarrow \mathrm{ord}\,(0,1) = 4$$

· A_4 no tiene elementos de orden 4: los únicos elementos de orden 4 de $S_4 \supset A_4$ son de la forma $\underbrace{(a,b,c,d)}_{\text{sign} = -1} \notin A_4$

luego $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z} \not\cong A_4$

· Lo mismo para D_{12}: tampoco tiene elementos de orden 4:

$$D_{12} = D_{2\cdot 6} = \left\{ \begin{matrix} \overbrace{1, r, r^2, r^3, r^4, r^5}^{|\langle r\rangle| = 6} \\ \underbrace{s, sr, sr^2, sr^3, sr^4, sr^5}_{\text{orden } 2 \neq 4} \end{matrix} \right\} \qquad \text{ord} \neq 4$$