Definición 0.1. Una sucesión de grupos G_i y homomorfismos de grupos f_i es

$$G_0 \xrightarrow{f_1} G_1 \xrightarrow{f_2} G_2 \xrightarrow{f_3} \cdots \xrightarrow{f_n} G_n \xrightarrow{f_{n+1}} \cdots$$

se dice que es exacta si $Ker(f_{i+1}) = Im(f_i)$. Diremos que es una sucesión exacta corta cuando es de la forma

$$1 \to G_1 \xrightarrow{f_2} G_2 \xrightarrow{f_3} G_3 \to 1 \tag{1}$$

Observación 0.2. Una sucesión exacta corta como (1) es equivalente a decir que f_2 es inyectiva, f_3 sobreyectiva y que $G_2/f_2(G_1) \cong G_3$

Demostración. $Ker(f_2) = Im(f_1) = \{1\} \implies f_2$ es inyectiva.

$Im(f_3) = Ker(f_4) = G_3 \implies f_3$ es sobreyectiva.

$Ker(f_3) = Im(f_2) \cong G_1 \implies G_2/G_1 \cong G_3$ por el Primer Teorema de Isomorfía. ∎

Proposición 0.3. *Dos extensiones equivalentes son isomorfas*

Demostración. Sea $x_2 \in E$ tal que $f(x_2) = 1$, por la conmutatividad de f, $\pi(x_2) = \pi'(f(x_2)) = \pi'(1) = 1$. $x_2 \in Ker(\pi) = Im(i)$, por tanto existe $x_1 \in N$ tal que $i(x_1) = x_2$, utilizando que $f \circ i = i'$, $i'(x_1) = f(i(x_1)) = 1$ y como i es inyectiva, x_2 es único y f es inyectiva.

Sea $x'_2 \in E'$, como π es sobreyectiva existe $x_2 \in E$ tal que $\pi'(x'_2) = \pi(x_2) = \pi'(f(x_2))$. Por tanto, $x'_2 f(x_2)^{-1} \in Ker(\pi') = Im(i')$ y existe $x_1 \in N$ tal que $f(i(x_1)) = i'(x_1) = x'_2 f(x_2)^{-1}$, $x'_2 = f(i(x_1)x_2)$ y f es sobreyectiva. ∎

Proposición 0.4. *La equivalencia de extensiones, como su nombre indica, es una relación de equivalencia.*

Demostración.

1. Reflexiva: E es equivalente a sí misma tomando $f = 1_E$
2. Simétrica: Si $f\colon E_1 \to E_2$ es una equivalencia, por (0.3), $f^{-1}\colon E_2 \to E_1$ es una equivalencia.
3. Transitiva: Si $f\colon E_1 \to E_2$ y $g\colon E_2 \to E_3$ son equivalencias, es trivial comprobar que $g \circ f \circ i_1 = i_3$ y que $\pi_1 \circ g \circ f = \pi_3$ entonces $g \circ f\colon E \to E''$ es una equivalencia.

∎

Definición 0.5. Denotamos por $Ext_\phi(Q, A)$ a las clases de extensiones equivalentes que dan lugar a la acción ϕ de Q en A.

Observación 0.6. El producto semidirecto se corresponde con el elemento trivial de $H^2(Q, A)$.

Demostración. ∎

Proposición 0.7. *Sean $[E_1], [E_2] \in Ext(Q, A)$ dos extensiones y $[c_1], [c_2] \in H^2(Q, A)$ sus cociclos asociados, podemos definir la suma $[E_1] + [E_2]$ como la clase de extensiones equivalentes asociada a $[c1 + c2] \in H^2(Q, A)$. Es decir, $Ext(Q, A)$ tiene una estructura de grupo heredada de $H^2(Q, A)$.*

Demostración. ∎

Proposición 0.8. *Podemos expresar la suma de extensiones anterior a partir de las extensiones* $1 \to A \xrightarrow{i_j} E_j \xrightarrow{\pi_j} Q \to 1$, *para* $j = 1, 2$, *como prueba el siguiente diagrama conmutativo.*

$$\begin{tikzcd}
1 \arrow[r] & A \times A \arrow[r, hook, "i_1 \times i_2"] \arrow[d, equal] & E_1 \times E_2 \arrow[r, two heads, shift left, "\pi_1 \times \pi_2"] & Q \times Q \arrow[l, hook', shift left, "s_1 \times s_2"] \arrow[r] & 1 \\
1 \arrow[r] & A \times A \arrow[r, hook, "\tilde{\imath}"] \arrow[d, two heads, "+"'] & E_1 \times_Q E_2 \arrow[u, hook, "i"'] \arrow[d, two heads, "\pi_{Ker(+)}"'] \arrow[r, two heads, shift left, "\tilde{\pi}"] & Q \arrow[u, hook, "\Delta"'] \arrow[d, equal] \arrow[l, hook', shift left, "\tilde{s}"] \arrow[r] & 1 \\
1 \arrow[r] & A \arrow[r, hook, "i_3"] & \frac{E_1 \times_Q E_2}{Ker(+)} \arrow[r, two heads, shift left, "\pi_3"] & Q \arrow[l, hook', shift left, "s_3"] \arrow[r] & 1
\end{tikzcd}$$

Demostración. A partir de las extensiones E_1 y E_2 se construye la extensión del producto directo tomando la inclusión y proyección coordenada a coordenada. El objetivo será utilizar los cociclos c_1 y c_2 para construir una sucesión exacta $1 \to A \xrightarrow{i_3} E_3 \xrightarrow{\pi_3} Q \to 1$ cuyo cociclo asociado sea $c_3 = c_1 + c_2$.

$$1 \to A \times A \xrightarrow{i_1 \times i_2} E_1 \times E_2 \xrightarrow{\pi_1 \times \pi_2} Q \times Q \to 1 \tag{2}$$

La sección $s_1 \times s_2$ de $\pi_1 \times \pi_2$ tiene como cociclo asociado

$$(c_1 \times c_2)\colon (Q \times Q) \times (Q \times Q) \to A \times A \tag{3}$$
$$((q_{11}, q_{12}), (q_{21}, q_{22})) \mapsto (c_1(q_{11}, q_{12}), c_2(q_{21}, q_{22})) \tag{4}$$

Proyectando $A \times A$ sobre A y haciendo la suma de componentes en A movemos $(c_1 \times c_2)((q_{11}, q_{12}), (q_{21}, q_{22}))$ a $c_1(q_{11}, q_{12}) + c_2(q_{21}, q_{22})$. Basta identificar q_{11} con q_{21} y q_{12} con q_{22} mediante $\Delta\colon Q \to Q \times Q$ definido por $\Delta(q) = (q, q)$. Notese que el morfismo diagonal está definido para las secciones s_1 y s_2, por tanto, para los cociclos estará definido de $Q \times Q$ en $(Q \times Q) \times (Q \times Q)$.

$$Q \times Q \xrightarrow{\Delta} (Q \times Q) \times (Q \times Q) \xrightarrow{c_1 \times c_2} A \times A \xrightarrow{+} A \tag{5}$$

El cociclo que buscamos es $c_3 = + \circ (c_1 \times c_2) \circ \Delta = c_1 + c_2$

Completando el diagrama de Δ y $\pi_1 \times \pi_2$ con $i\colon \tilde{E} \to E_1 \times E_2$ y $\tilde{\pi}\colon E \to Q$, para $x \in \tilde{E}$ $(\pi_1(i(x)), \pi_2(i(x))) = (\tilde{\pi}(x), \tilde{\pi}(x))$ lo que implica que $\pi_1(i(x)) = \pi_2(i(x))$ y por tanto $i(x) \in E_1 \times_Q E_2$. Lo natural es tomar $\tilde{E} = E_1 \times_Q E_2$, i la inclusión y $\tilde{\pi}(e_1, e_2) = \pi_1(e_1) = \pi_2(e_2)$.

$$\begin{tikzcd}
E_1 \times E_2 \arrow[r, "\pi_1 \times \pi_2"] & Q \times Q \\
\tilde{E} \arrow[u, "i"] \arrow[r, "\tilde{\pi}"] & Q \arrow[u, "\Delta"']
\end{tikzcd}$$

$Ker(\tilde{\pi}) = \{(e_1, e_2) \in E_1 \times_Q E_2 \colon \tilde{\pi}(e_1, e_2) = 0\} = \{(e_1, e_2) \in E_1 \times_Q E_2 \colon \pi_1(e_1) = \pi_2(e_2) = 0\} = A \times A$

Por tanto, la sucesión $1 \to A \times A \xrightarrow{\tilde{\imath}} E_1 \times_Q E_2 \xrightarrow{\tilde{\pi}} Q \to 1$ es exacta.

El cociclo correspondiente a la extensión es por tanto $c_1 + c_2$ y por la proposición **??** la suma está bien definida en clases de extensiones equivalentes. ■

Capítulo 1

Extensiones de grupos

Definición 1.1. Una extensión de un grupo Q por un grupo N es una sucesión exacta corta

$$1 \to N \to G \to Q \to 1$$

Decimos que otra extensión $1 \to N \to G' \to Q \to 1$ es equivalente si existe un homomorfismo $f\colon G \to G'$ tal que el siguiente diagrama conmuta:

$$\begin{tikzcd}
& & G \arrow[dd, "f"'] \arrow[dr] & & \\
1 \arrow[r] & N \arrow[ur] \arrow[dr] & & Q \arrow[r] & 1 \\
& & G' \arrow[ur] & &
\end{tikzcd}$$

1.1. Extensiones separables

Definición 1.2. Sea $\pi\colon A \to B$ un homomorfismo de grupos, decimos que s es una sección de π cuando $\pi \circ s = id$

Definición 1.3. Decimos que una extensión E de Q por N es separable cuando existe una sección $s\colon Q \to E$ que es un homomorfismo.

Teorema 1.4. *Una extensión E de Q por N es separable sí y solo sí $G \cong N \ltimes_\varphi Q$, donde $\varphi\colon Q \to Aut(N)$ es una acción de grupos de Q en N.*

Demostración. Como E es separable, existe una sección s que es homomorfismo. Al ser una inversa a la derecha, es inyectiva y, por tanto, $Q \cong s(Q) \leq E$. $\pi(i(N)) = \{0\}$ y $s(q) \in i(N) \iff q = 0$, por lo que $s(Q) \cap i(N) = 0_E$ y E es isomorfo a un producto semidirecto externo de Q por N

En la otra dirección, definiendo para $n \in N$, $q \in Q$ $i(n) = (1_Q, n)$ y $\pi((n, q)) = qN$ ∎

1.2. Extensiones con kernel abeliano

A continuación estudiaremos el caso en que N es un grupo abeliano que a partir de ahora denotaremos por A. Si consideramos la acción de G por conjugación sobre $i(A)$, la acción restringida a $i(A)$ es trivial y por tanto está contenida en el kernel de la acción. Esto induce una acción en el cociente $G/i(A) \cong Q$, haciendo a A un Q-módulo.

Observación 1.5. Dos extensiones E y E' equivalentes vienen dadas por una misma acción de Q a A. Por ello, para estudiar las extensiones salvo equivalencia podemos fijar un Q-módulo A y estudiar las extensiones que dan lugar a ese módulo.

Demostración. $f\left(i(a)^{s(q)}\right) = f(i(a))^{f(s(q))} = i'(a)^{s'(q)}$. ■

$$1 \to A \xrightarrow{i} E \xrightarrow{\pi} Q \to 1 \tag{1.1}$$

$$\varphi \colon Q \to Aut(A) \tag{1.2}$$

Para estudiar esta extensión, consideramos una sección de π, esto es, una función $s \colon Q \to E$ tal que $\pi \circ s = id$. Como $Q \cong E/i(A)$, dados $g, h \in Q$, $\pi\left(s(g)s(h)s(gh)^{-1}\right) = 1_Q$ por ser π homomorfismo. Por tanto, $s(gh)$ y $s(g)s(h)$ distan en un elemento de $i(A)$ y podemos definir una función $c \colon Q \times Q \to A$ que mide cuánto dista s de ser un homomorfismo:

$$s(g)s(h) = s(gh)i\left(c(g,h)\right) \tag{1.3}$$

Podemos recuperar la extensión (1.1) a partir de la acción φ que hemos fijado y de la función c. Como $E = \bigcup_{q \in Q} s(q)i(A) = s(Q)i(A)$ es una unión disjunta, podemos expresar unívocamente cada elemento de E como un producto de elementos de $s(Q)$ e $i(A)$. Es decir, tenemos una biyección $Q \times A \to E$. A partir del producto en E, podemos definir una operación de grupo en $Q \times A$, que denotaremos por E_c. Dados $a_1, a_2 \in A,\ q_1, q_2 \in Q$ tenemos:

$$\begin{aligned} s(q_1)i(a_1)s(q_2)i(a_2) &= s(q_1)s(q_2)i(a_1 \cdot q_2)i(a_2) \\ &= s(q_1q_2)i(c(q_1,q_2) + a_1 \cdot q_2 + a_2) \end{aligned} \tag{1.4}$$

Por tanto, la operación en E_c viene dada por:

$$(q_1, a_1)(q_2, a_2) = (q_1q_2, c(q_1, q_2) + a_1 \cdot q_2 + a_2) \tag{1.5}$$

Notese que este producto no depende directamente de la sección s escogida. Por ello, supondremos que la sección s es normalizada

$$s(1) = 1 \tag{1.6}$$

de donde obtenemos que

$$c(1, q) = 0 = c(q, 1) \tag{1.7}$$

De esta forma el isomorfismo $f \colon E \to E_c$ viene dado por $q \in Q,\ a \in A$ $s(q)i(a) \mapsto (q, a)$. La inclusión de A a E_c y la proyección a Q son las canónicas, haciendo a la extensión E_c equivalente a (1.1).

Proposición 1.6. *Sea φ una acción de Q en A y $c\colon Q \times Q \to A$ una función que verifica la condición de normalización* (1.7)*. Entonces, la operación* (1.5) *define una extensión de Q por A cuando c es un 2-cociclo.*

Demostración. Para ver que la funcion define una operación de grupo comprobamos la asociatividad y la existencia de identidad e inversos.

Imponiendo que $[(q_1, a_1)(q_2, a_2)](q_3, a_3) = (q_1, a_1)[(q_2, a_2)(q_3, a_3)]$ llegamos a la siguiente condición que garantiza que la operación sea asociativa

$$c(q_1, q_2) \cdot q_3 - c(q_1, q_2q_3) + c(q_1q_2, q_3) - c(q_2, q_3) = 0 \tag{1.8}$$

Identidad: $(1, 0)$
Sea $(q, a) \in Q \times A$,
$(1, 0)(q, a) = (q, c(1, q) + 0 \cdot q + a) = (q, a)$
$(q, a)(1, 0) = (q, c(q, 1) + a \cdot 1 + 0) = (q, a)$
Inverso de $(q, a) \in Q \times A$: $(q^{-1}, -c(q, q^{-1}) - a \cdot q)$

A continuación, comprobamos que la inclusión de A a $A \times Q$ y la proyección a Q definen homomorfismos y hacen a la sucesión exacta.
$i(a_1)i(a_2) = (1, a_1)(1, a_2) = (1, c(1, 1)+a_1 \cdot 1+a_2) = (1, a_1 +a_2) = i(a_1 +a_2)$
$\pi((q_1, a_1)(q_2, a_2)) = \pi((q_1q_2, -)) = q_1q_2 = \pi((q_1, -))\pi((q_2, -))$
$\pi(i(a)) = \pi(1, a) = 1$ ∎

Proposición 1.7. *Sea E una extensión de Q por A y s, s' dos secciones de Q a E y c, c' los cociclos asociados a s y s'. Entonces, c y c' se diferencian en un 2-coborde. Esto es, la extensión E determina la clase $[c] \in H^2_\varphi(Q, A)$.*

Demostración. La diferencia de s y s' es una función $e\colon Q \to A$, $s'(q) = s(q)i(e(q))$

$$\begin{aligned} s'(gh)i(c'(g, h)) &= s'(g)s'(h) \\ &= s(g)i(e(g))s(h)i(e(h)) \\ &= s(g)s(h)i(e(g) \cdot h + e(h)) \\ &= s(gh)i(c(g, h) + e(g) \cdot h + e(h)) \end{aligned} \tag{1.9}$$

De donde obtenemos $c'(g, h) - c(g, h) = e(g) \cdot h + e(h) - e(gh)$. ∎

Teorema 1.8. *Sea A un Q-módulo definido por una acción $\varphi\colon Q \to Aut(A)$ y sea $Ext_\varphi(Q, A)$ el conjunto de clases de equivalencia de extensiones que dan lugar a la acción φ. Entonces*

$$Ext_\varphi(Q, A) \cong H^2_\varphi(Q, A)$$

Como consecuencia de este resultado podemos demostrar el caso abeliano del Teorema de Schur-Zassenhaus.

Teorema 1.9. *Sea G un grupo finito y sea $N \trianglelefteq G$ abeliano, $|N| = n$ y $|G : N| = m$ con $\operatorname{mcd}(n, m) = 1$. Entonces G contiene subgrupos de orden m y dos cualesquiera son conjugados.*

Demostración. Tomamos una sección s y su cociclo asociado c. Definimos la función $d(x) = \prod_{t \in Q} c(t, x)$ y hacemos el producto en $t \in Q$ de (1.8), de donde obtenemos

$$mc(x, y) = d(x) \cdot y + d(y) - d(xy) \tag{1.10}$$

Como $\operatorname{mcd}(m, n) = 1$, existe un $k \in \mathbb{Z}$ tal que $km \equiv 1 \mod n$. Multiplicando (1.10) por k llegamos a

$$c(x, y) = kd(x) \cdot y + kd(y) - kd(xy) \tag{1.11}$$

Por tanto, c verifica la ecuación de un coborde para la función kd y $H^2(Q, A)$ es trivial.

% TODO conjugación ■

1.2.1. Extensiones centrales

Un caso particular de (1.1) es cuando la acción de Q en A es trivial

Teorema 1.10 (Schur-Zassenhaus)**.** *Sea G un grupo finito y $N \trianglelefteq G$, $|N| = n$ y $|G : N| = m$ con $\operatorname{mcd}(n, m) = 1$. Entonces G contiene subgrupos de orden m y son conjugados.*

Demostración. (i) Existencia: N abeliano. Sea $Q = G/N$. Construimos una sección $s' \colon Q \to G$ que manda cada $x \in Q$ a un elemento de x. En principio la sección no es un homomorfismo y tenemos que $s'(xy)N = s'(x)s'(y)N$. Podemos definir una función $c \colon Q \times Q \to N$ de tal forma que $s'(x)s'(y) = s'(xy)c(x, y)$.

Si tomamos otra sección $s \colon Q \to N$, tenemos $s(x)N = s'(x)N$ y por tanto $s(x) = s'(x)e(x)$, con $e \colon Q \to N$. Imponiendo que s sea un homomorfismo:

$$\begin{aligned} s'(xy)e(xy) = s(xy) = s(x)s(y) &= s'(x)e(x)s'(y)e(y) \\ &= s'(x)s'(y)e(x)^{s'(y)}e(y) \\ &= s'(xy)c(x,y)e(x)^{s'(y)}e(y) \end{aligned}$$

$$c(x, y)^{-1} = e(xy)^{-1}e(x)^{s'(y)}e(y) \tag{1.12}$$

Aplicando la propiedad asociativa a $(s'(t)s'(x))s'(y) = s'(t)(s'(x)s'(y))$

$$\begin{aligned} (s'(t)s'(x))s'(y) &= s'(tx)c(t,x)s'(y) \\ &= s'(tx)s'(y)c(t,x)^{s'(y)} \\ &= s'(txy)c(tx,y)c(t,x)^{s'(y)} \\ s'(t)(s'(x)s'(y)) &= s'(t)s'(xy)c(x,y) \\ &= s'(txy)c(t,xy)c(x,y) \end{aligned}$$

$$c(x, y) = c(t, xy)^{-1}c(t, x)^{s'(y)}c(tx, y) \tag{1.13}$$

Podemos definir $d(x) = \prod_{t \in Q} c(t, x)$ y hacer el producto en (1.13) sobre t para relacionarlo con (1.12). Obtenemos $c(x, y)^m = d(xy)^{-1}d(x)^{s'(y)}d(y)$. Como $\operatorname{mcd}(n, m) = 1$, existe un $k \in \mathbb{Z}$ tal que $km \equiv 1 \pmod{n}$. Elevando esta última ecuación a $-k$:

$$c(x, y)^{-1} = d(xy)^k \left(d(x)^{-k}\right)^{s'(y)} d(y)^{-k} \tag{1.14}$$

Finalmente podemos igualar $e(x) = d(x)^{-k}$ y escribir explícitamente s en términos de s':

$$s(x) = s'(x) \prod_{t \in Q} c(t, x)^{-k} = s'(x) \prod_{t \in Q} \left(s'(t)s'(x)s'(tx)^{-1}\right)^{-k} \tag{1.15}$$

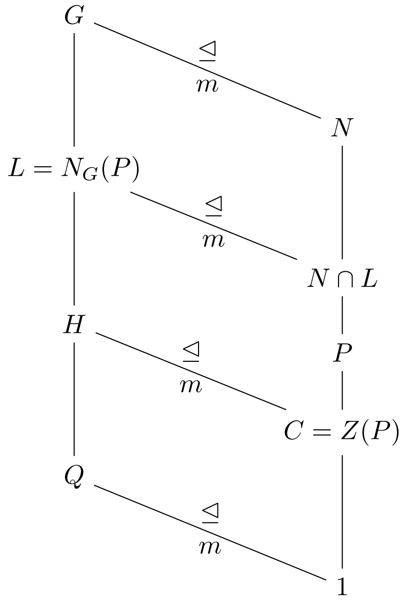
A partir de una sección cualquiera s', hemos conseguido definir una sección s que es un homomorfismo. Las secciones son inyectivas y por tanto $s(Q)$ es un subgrupo de G de orden m. A continuación, veremos que cualesquiera dos subgrupos de orden m son conjugados.

Sean H y H^* dos subgrupos de orden m. **TODO**

(ii) Existencia: Caso general. Lo demostramos por inducción fuerte sobre $|G|$. Podemos tomar como caso base C_p, que como es abeliano se cumple el resultado. Sea p un divisor primo de n y $P \in Syl_p(N)$. Sean $L = N_G(P)$ y $C = Z(P)$. Como C es característico en P, tenemos que $C \trianglelefteq L$. Por el argumento de Frattini $G = LN$. Observamos que $|L : N \cap L| = |G : N| = m$ y $N \cap L \trianglelefteq L$ por el Segundo Teorema de Isomorfía. Podemos aplicar la inducción sobre el grupo L/C ya que $C \neq 1$ por ser P un p-subgrupo.

Por inducción, existe $H/C \leq L/C$ de orden m y volviendo a G tenemos el subgrupo H de índice m en C.

Podemos aplicar el caso abeliano a H y C y concluir que existe un subgrupo Q de orden m.



$\blacksquare$