Resumen

Este trabajo trata sobre *racks, quandles y conjuntos cruzados* finitos. Se da las principales propiedades algebraicas de los mismos junto con una gran cantidad de ejemplos. Se introduce la noción de rack *simple* y se los clasifica en término de teoría de grupos. Dicha clasificación se divide en dos casos distintos, cuando el cardinal del rack es divisible por la potencia de un número primo o no. Se considera, luego, el grupo de trenzas y las ecuaciones *conjuntistas* de trenzas y se ve que están en correspondencia biyectiva con las soluciones *conjuntistas* de la *ecuación cuántica de Yang-Baxter* (QYBE). Finalmente, se da una manera completa de cómo construir soluciones de la QYBE a partir de los racks finitos.

Índice

1. Introducción. **3**

2. Racks, quandles y conjuntos cruzados. **5**

2.1. **Definiciones.** 5

2.2. **Nociones básicas.** 9

3. Ejemplos. **23**

3.1. **Contraejemplos.** 23

3.2. **Sumas amalgamadas.** 23

3.3. **Ejemplos geométricos.** 25

3.4. **Conjuntos cruzados afines.** 29

3.5. **Conjuntos cruzados involutivos.** 37

3.6. **El quandle libre de un conjunto.** 40

4. Extensiones. **43**

5. Racks simples. **47**

5.1. **Conjuntos cruzados indescomponibles exactos.** 47

5.2. **Clasificación de racks simples.** 52

6. Ecuación cuántica de Yang-Baxter. **64**

6.1. **El grupo de Trenzas.** 64

6.2. **La ecuación cuántica de Yang-Baxter (QYBE).** 65

1. Introducción.

La *ecuación cuántica de Yang-Baxter* (QYBE) es una de las ecuaciones básicas de la física matemática y yace en la fundamentación de la teoría de grupos cuánticos. Esta ecuación involucra a un operador lineal $R : V \otimes V \to V \otimes V$, donde V es un espacio vectorial, y tiene la forma

$$R^{12}R^{13}R^{23} = R^{23}R^{13}R^{23} \tag{1.1}$$

en $\mathrm{End}(V \otimes V \otimes V)$, donde R^{ij} es el operador R actuando en las componentes i, j.

En los últimos veinte años, se han encontrado soluciones a esta ecuación y las estructuras algebraicas relacionadas (Álgebras de Hopf) han sido intensamente estudiadas. Sin embargo, estas soluciones eran usualmente deformaciones de la solución identidad.

Cabe destacar, que la ecuación (1.1) tiene aún sentido si R no es un operador lineal $V \otimes V \to V \otimes V$, sino también cuando es una función $V \times V \to V \times V$, con X un conjunto. En efecto, a cada solución *conjuntista* de (1.1) le corresponde una solución *lineal*, considerando el funtor de X al módulo libre generado por X.

Ahora bien, en [Dr], Drinfeld sugiere estudiar las soluciones conjuntistas a la QYBE además de las lineales, afirmando a partir del Ejemplo 2 (B.B. Venkov) que la QYBE es equivalente a la condición de racks. Un *rack* es un conjunto con una operación binaria tal que la multiplicación a izquierda es un automorfismo. De esta manera, es importante tener una clasificación de los mismos. Nos interesa, en particular, los racks finitos. En este sentido, la determinación de todos los racks finitos es una tarea para nada sencilla. No obstante, sabemos que cualquier rack finito es una unión de componentes (subracks) *indescomponibles* (Proposición 2.31). Sin embargo, los racks indescomponibles pueden ser combinados de muchas maneras distintas como sumas amalgamadas y la descripción de todas las formas de hacerlo es nuevamente difícil.

La teoría de racks está fuertemente conectada con la teoría de grupos, módulos cruzados y presentaciones de grupos. También aparecen en el estudio de espacios topológicos. En [FR], se menciona que un rack es un conjunto con una operación binaria satisfaciendo dos leyes sencillas que son la destilación algebraica de dos de los movimientos de Reidemeister (Ω_1 y Ω_2). Además, los racks proveen un contexto algebraico completo y elegante para el estudio de vínculos (links) y nudos (knots) en 3-variedades y también para el estudio de las 3-variedades mismas. En este contexto topológico, la teoría de racks da la posibilidad práctica de encontrar una sucesión completa de invariantes para vínculos y 3-variedades. Por ejemplo, cualquier subvariedad de codimensión tiene un rack fundamental, el cual es un invariante para vínculos irreducibles de cualquier 3-variedad, que contiene más información que el grupo fundamental.

Los racks han sido estudiados por muchos autores bajo una gran variedad de nombres usando diferentes notaciones y terminología. Los primeros trabajos en los que se ha utilizado este concepto son debido a Conway y Wraith, en forma de correspondencias no pubicadas. Ellos usaron el nombre **wrack** y se lo ha adoptado no solamente por ser el nombre original,

sino también por ser una palabra inglesa sencilla sin otro significado matemático. Además, rack es usado en el mismo sentido que en la expresión inglesa "rack and ruin". El contexto de los trabajos de Conway y Wraith es la operación conjugación en un grupo y se recuerda a un rack como los "restos"de un grupo después de que la operación de grupo es olvidada y sólo permanece la noción de conjugación. Luego, por degeneración de la palabra wrack ha quedado rack. Otro trabajo que trata con este concepto es dado por Joyce en [J1], y el nombre que se utiliza es el de **quandle**. Aquí, Joyce establece el álgebra básica de quandles, dando varios ejemplos, y define quandles aumentados y sus grupos asociados. Este trabajo de Joyce ha sido muy estudiado, entre otros, por Matveev. Éste último desarrolló el concepto independientemente de Joyce dándole el nombre de **grupoide distributivo**. Notar que un rack no es un grupoide en el sentido usual. Por último en un trabajo de Kauffman se estudian racks bajo el nombre de **cristales**, pero dado que esta terminología se utiliza en otra área de la matemática se decidió no usarla.

La noción de conjunto cruzado aparece en la tesis de Graña, [G], introducida por consideraciones originadas en problemas de clasificación de Álgebras de Hopf punteadas.

Este trabajo está basado en [AG], donde se estudia la estructura fina de los racks. Los resultados de las secciones 4 y 5 son extraídos de [AG].

Se describe ha continuación el contenido de este trabajo.

En la sección 2, se dan las definiciones y nociones básicas de *racks, quandles y conjuntos cruzados*. Se estudian algunas propiedades de morfismos de racks y la descomposición de un rack como unión disjunta de subracks *indescomponibles*.

En la sección 3, se exhibe una gran cantidad de ejemplos. Se ve, mediante las *sumas amalgamadas*, cómo se puede formar un nuevo rack a partir de ciertos racks dados. Además, se estudian los conjuntos cruzados *afines* y se dan algunas consideraciones categóricas acerca de quandles.

En la sección 4, se tratan las *extensiones* de un rack por un conjunto no vacío, y se prueba que todo rack finito indescomponible es una extensión de un conjunto cruzado indescomponible *exacto*.

En la sección 5, se estudian los racks *simples*. Se dice que un rack no trivial es simple si no tiene cocientes propios. Entonces cualquier rack finito indescomponible con cardinalidad mayor que uno es una extensión de un rack simple. Uno de los principales resultados es la clasificación explícita de todos los racks simples finitos, Teoremas 5.31 y 5.33, cuyas pruebas están basadas en la teoría de grupos.

En la sección 6, se presenta el grupo de trenzas como así también las ecuaciones de trenzas y de Yang-Baxter. Se muestra que las soluciones de la ecuación de trenzas están en correspondencia biyectivas con las soluciones de la QYBE. Se exhibe una manera de dar soluciones de la ecuación de trenzas, Teorema 6.13, y se caracterizan a las soluciones no degeneradas de la misma, Teorema 6.20.

2. Racks, quandles y conjuntos cruzados.

2.1. Definiciones.

Definición 2.1. Un *rack* es un par $(X, \triangleright)$ donde X es un conjunto no vacío y $\triangleright : X \times X \to X$ es una función, tal que

$$\phi_i : X \to X, \quad \phi_i(j) = i \triangleright j, \quad \text{es una biyección para todo } i \in X, \tag{2.2}$$
$$i \triangleright (j \triangleright k) = (i \triangleright j) \triangleright (i \triangleright k) \ \forall i, j, k \in X. \tag{2.3}$$

Un *quandle* es un rack $(X, \triangleright)$ que verifica

$$i \triangleright i = i, \text{ para todo } i \in X. \tag{2.4}$$

Un *conjunto cruzado* es un quandle $(X, \triangleright)$ que verifica además

$$j \triangleright i = i \text{ siempre que } i \triangleright j = j. \tag{2.5}$$

Definición 2.6. Sean $(X, \triangleright)$ e $(Y, \triangleright)$ racks. Se dice que $\psi : (X, \triangleright) \to (Y, \triangleright)$ es un *morfismo de racks* si

$$\psi(i \triangleright j) = \psi(i) \triangleright \psi(j)$$

para todo $i, j \in X$.

Morfismos de quandles (resp. conjuntos cruzados) son morfismos de racks entre quandles (resp. conjuntos cruzados).

Definición 2.7. Un *subrack* de un rack $(X, \triangleright)$ es un subconjunto Y no vacío, tal que $y \triangleright Y = Y$, para todo $y \in Y$

Es claro que todo subrack de un quandle (resp. conjunto cruzado) es un quandle (resp. conjunto cruzado). Cabe destacar que si X es finito Y es un subrack si y sólo si $y \triangleright Y \subset Y$, para todo $y \in Y$.

Ejemplo 2.8. Sea G un grupo cualquiera y $X \subseteq G$ un subconjunto no vacío de G. Si definimos $\triangleright : X \times X \to X$ por $i \triangleright j := iji^{-1}$ entonces

(I) si X es estable por conjugación en todos los elementos de G entonces $(G, \triangleright)$ es un rack ya que

  (i) $\triangleright$ está bien definido pues X es estable por conjugación.

(ii) si $i \in X$ y $\phi : X \to X$ con $\phi_i(j) = i \triangleright j$ entonces ϕ_i es biyección pues si $\phi_i(j) = \phi_i(j')$ implica que $iji^{-1} = ij'i^{-1}$, o sea $j = j'$ y si $k \in X$ se tiene que $iki^{-1} \in X$ y $\phi_i(iki^{-1}) = k$, por lo que ϕ_i es suryectiva.

(iii) $i \triangleright (j \triangleright k) = ijkj^{-1}i^{-1} = iji^{-1}iki^{-1}(iji^{-1})^{-1} = (i \triangleright j) \triangleright (i \triangleright k)$, para todo $i, j \in X$. Más aún, $(X, \triangleright)$ es un conjunto cruzado puesto que

(iv) $i \triangleright i = iii^{-1} = i$, para todo $i \in X$.

(v) si $i \triangleright j = j$ implica que $iji^{-1} = j$, es decir $i = jij^{-1} = j \triangleright i$.

Al conjunto cruzado X se lo llama *conjunto cruzado estándar*.

(II) si X es estable por conjugación en sus propios elementos y X es finito entonces ϕ_i resulta suryectiva y $(X, \triangleright)$ es un rack.

Por otra parte, si X no es finito puede ocurrir que ϕ_i no sea suryectiva para todo $i \in X$ como se ve en el siguiente ejemplo.

Ejemplo 2.9. Sean

$$G := \mathbb{S}_{\mathbb{R}} = \{f : \mathbb{R} \to \mathbb{R} / \text{ f es biyectiva } \},$$
$$X := \{f \in \mathbb{S}_{\mathbb{R}} \ / \ f(x) = ax + b, \ \forall x \in \mathbb{R} \text{ con } a \in \mathbb{Z} - \{0, 1, -1\} \text{ y } b \in \mathbb{Z} \ \}.$$

Notemos que si $f \in X$, con $f(x) = ax + b$ para todo $x \in X$, donde $a \in \mathbb{Z} - \{0, 1, -1\}$ y $b \in \mathbb{Z}$, entonces $f^{-1}(x) = a^{-1}x - ba^{-1}$, para todo $x \in \mathbb{R}$ y $f^{-1} \notin X$, pues $a^{-1} \notin \mathbb{Z} - \{0, 1, -1\}$. Si definimos ahora

$$\triangleright : X \times X \to X, \quad f \triangleright g := fgf^{-1}$$

tenemos que $\triangleright$ está bien definido ya que si $f, g \in X$, con $f(x) = ax + b$ y $g(x) = cx + d$, donde $a, c \in \mathbb{Z} - \{0, 1, -1\}$ y $b, d \in \mathbb{Z}$, se tiene que

$$(f \triangleright g)(x) = cx - bc + ad + b, \quad x \in \mathbb{Z}.$$

Además, si $\phi_f : X \to X$, $\phi_f(g) = f \triangleright g$ resulta que ϕ_f es inyectiva, pues si $\phi_f(g) = \phi_f(g')$ entonces $fgf^{-1} = fg'f^{-1}$ y $g = g'$, pero ϕ no es suryectiva pues si $f \in X$, con $f(x) = 2x + 3$ para todo $x \in \mathbb{R}$ y sea $h \in X$ tal que $h(x) = 4x + 6$ y supongamos que existe g con $g(x) = ax + b$ tal que $\phi_f(g) = h$ entonces se tiene que $\phi_f(g) = ax - 3a + 2b + 3$; así $a = 4 \in \mathbb{Z} - \{0, 1, -1\}$, pero $b \notin Z$ y $g \notin X$. Luego $(X, \triangleright)$ no es un rack.

Definición 2.10. Sea $(X, \triangleright)$ un rack y sea $\mathbb{S}_X$ el grupo de simetrías de X. Por (2.2) tenemos una función $\phi : X \to \mathbb{S}_X$. Se define

$$\text{Aut}_{\triangleright}(X) := \{g \in \mathbb{S}_X \ / \ g(i \triangleright j) = g(i) \triangleright g(j)\},$$
$$\text{Inn}_{\triangleright}(X) := \text{ el subgrupo de } \mathbb{S}_X \text{ generado por } \phi(X).$$

Por (2.3), $\mathrm{Inn}_{\triangleright}(X)$ es un subgrupo de $\mathrm{Aut}_{\triangleright}(X)$. Por otro lado, es fácil ver que

$$g\phi_x g^{-1} = \phi_{g(x)}, \qquad \forall g \in \mathrm{Aut}_{\triangleright}(X), x \in X. \tag{2.11}$$

Por lo tanto, $\phi(X) \subset \mathrm{Aut}_{\triangleright}(X)$ es un conjunto cruzado estándar, $\phi : X \to \mathrm{Aut}_{\triangleright}(X)$ es un morfismo de racks e $\mathrm{Inn}_{\triangleright}(X)$ es un subgrupo normal de $\mathrm{Aut}_{\triangleright}(X)$. En general, no es verdadero que $\mathrm{Inn}_{\triangleright}(X) = \mathrm{Aut}_{\triangleright}(X)$, como lo muestra el siguiente ejemplo.

Ejemplo 2.12. Sea $X = \{\pm i, \pm j\}$ un subconjunto estándar del grupo de unidades de los cuaterniones. Entonces $\mathrm{Inn}_{\triangleright}(X) \neq \mathrm{Aut}_{\triangleright}(X)$.

Demostración. Sale por computación directa. □

Veremos ahora como se relacionan entre sí racks, quandles y conjuntos cruzados.

De racks a quandles.

Sea X un rack y sea $C_{\triangleright}(X)$ el centralizador en $\mathrm{Aut}_{\triangleright}(X)$ de $\mathrm{Inn}_{\triangleright}(X)$. Para $\psi \in C_{\triangleright}(X)$ definimos $\triangleright^{\psi}$ por

$$a \triangleright^{\psi} b = a \triangleright \psi(b) = \psi(a \triangleright b) = \psi(a) \triangleright \psi(b).$$

Luego, $(X, \triangleright^{\psi})$ es un rack pues

(i) si $\phi_x^{\psi} : X \to X$ dada por $\phi_x^{\psi}(y) = x \triangleright^{\psi} y = x \triangleright \psi(y) = \psi(x \triangleright y) = \psi(x) \triangleright \psi(y)$ se tiene que $\phi_x^{\psi} = \phi_x \psi$ y por lo tanto es una biyección ya que $\phi_x, \psi \in \mathrm{Aut}_{\triangleright}(X) \subseteq \mathbb{S}_X$.

(ii) ver que $x \triangleright^{\psi} (y \triangleright^{\psi} z) = (x \triangleright^{\psi} y) \triangleright^{\psi} (x \triangleright^{\psi} z)$, para todo $x, y, z \in X$. Tenemos que

$$\begin{aligned} x \triangleright^{\psi} (y \triangleright^{\psi} z) &= x \triangleright^{\psi} (\psi(y) \triangleright \psi(z)) = \psi(x) \triangleright \psi(\psi(y) \triangleright \psi(z)) = \\ &= \psi(x) \triangleright (\psi^2(y) \triangleright \psi^2(z)) = (\psi(x) \triangleright \psi^2(y)) \triangleright (\psi(x) \triangleright \psi^2(z)). \end{aligned}$$

Mientras que por otro lado se tiene que

$$\begin{aligned} (x \triangleright^{\psi} y) \triangleright^{\psi} (x \triangleright^{\psi} z) &= (x \triangleright \psi(y)) \triangleright^{\psi} (x \triangleright \psi(z)) = \psi(x \triangleright \psi(y)) \triangleright \psi(x \triangleright \psi(z)) = \\ &= (\psi(x) \triangleright \psi^2(y)) \triangleright (\psi(x) \triangleright \psi^2(z)). \end{aligned}$$

A $(X, \triangleright^{\psi})$ se lo llama el *conjugado* a $(X, \triangleright)$ respecto de ψ.

Sea ahora $\iota : X \to X$ dada por $a \triangleright \iota(a) = a$, la cual está bien definida por (2.2). Entonces por (2.3)

$$a \triangleright b = a \triangleright (b \triangleright \iota(b)) = (a \triangleright b) \triangleright (a \triangleright \iota(b)),$$

luego $a \triangleright \iota(b) = \iota(a \triangleright b)$, pues como $(a \triangleright b) \triangleright \iota(a \triangleright b) = a \triangleright b = (a \triangleright b) \triangleright (a \triangleright \iota(b))$ se tiene que $\phi_{a \triangleright b}(\iota(a \triangleright b)) = \phi_{a \triangleright b}(a \triangleright \iota(b))$ y como $\phi_{a \triangleright b}$ es biyectiva resulta que $\iota(a \triangleright b) = a \triangleright \iota(b)$. En particular, $a = \iota(a \triangleright b)$ por lo que ι es suryectiva. También

$$a \triangleright (\iota(a) \triangleright \iota(b)) = (a \triangleright \iota(a)) \triangleright (a \triangleright \iota(b)) = a \triangleright (a \triangleright \iota(b)),$$

así que por (2.2) $\iota(a) \triangleright \iota(b) = a \triangleright \iota(b) = \iota(a \triangleright b)$, es decir $\iota \in \mathrm{Aut}_{\triangleright}(X)$. Supongamos que $\iota(a) = \iota(b)$, entonces

$$a = a \triangleright \iota(a) = \iota(a) \triangleright \iota(a) = \iota(b) \triangleright \iota(b) = b \triangleright \iota(b) = b.$$

Esto es, ι es inyectiva y pertenece a $C_{\triangleright}(X)$. Podemos entonces considerar el quandle $(X, \triangleright^{\iota})$ pues $a \triangleright^{\iota} a = a \triangleright \iota(a) = a$. En conclusión, cualquier rack $(X, \triangleright)$ es conjugado a un único quandle llamado el *quandle asociado* a $(X, \triangleright)$.

Observación 2.13. Si $F : X \to Y$ es un morfismo de racks, entonces

$$F\iota = \iota F$$

ya que $F(x) \triangleright \iota(F(x)) = F(x)$, para todo $x \in X$. Además, como $x \triangleright \iota(x) = x$ se tiene que $F(x \triangleright \iota(x)) = F(x)$, es decir $F(x) \triangleright F(\iota(x)) = F(x)$; con esto se tiene que

$$\phi_{F(x)}(\iota(F(x))) = \phi_{F(x)}(F(\iota(x)))$$

y como ϕ_x es biyectiva para todo x en X resulta que $\iota(F(x)) = F(\iota(x))$, para todo $x \in X$. Por otra parte,

$$F(x \triangleright^{\iota} x') = F(x \triangleright \iota(x')) = F(x) \triangleright F((\iota(x')) = F(x) \triangleright \iota(F(x')) = F(x) \triangleright F(x').$$

Por lo tanto, F es un morfismo de los quandles asociados.

Observación 2.14. Por la Observación anterior se puede ver que $\mathrm{Aut}_{\triangleright}(X) \simeq \mathrm{Aut}_{\triangleright^{\iota}}(X)$, pero $\mathrm{Inn}_{\triangleright}(X)$ y $\mathrm{Inn}_{\triangleright^{\iota}}(X)$ pueden ser muy diferentes. Para ver esto tomemos X un conjunto cualquiera y $f \in \mathbb{S}_X$. Sea $x \triangleright y := f(y)$. Así $(X, \triangleright)$ es un rack ya que las funciones $\phi_x : X \to X$ dadas por $\phi_x(y) = x \triangleright y$ son biyectivas para todo x en X y

$$x \triangleright (y \triangleright z) = f(f(z)) = f(y) \triangleright f(z) = (x \triangleright y) \triangleright (x \triangleright z).$$

Pero si $f \neq \mathrm{id}$ entonces $(X, \triangleright)$ no es un quandle pues si lo fuera tendríamos que $x \triangleright x = x$, para todod $x \in X$, es decir $f(x) = x$ para todo $x \in X$, entonces $f = \mathrm{id}$ contra lo supuesto. A $(X, \triangleright)$ se lo llama *rack de permutación*. De esta manera, se tiene que si X es no vacío y $f \in \mathbb{S}_X$, con $f \neq \mathrm{id}$ entonces el rack de permutación satisface $\mathrm{Inn}_{\triangleright^{\iota}}(X) = \langle \phi_x / x \in X \rangle = \mathrm{id}$ mientras que $\mathrm{Inn}_{\triangleright}(X) = \langle f \rangle$.

De quandles a conjuntos cruzados.

Sea $(X, \triangleright)$ un quandle finito y sea $\sim$ la relación de equivalencia generada por

$$x \sim x' \text{ si existe } y \text{ tal que } x \triangleright y = y \text{ e } y \triangleright x = x'. \tag{2.15}$$

Se ve que $\sim$ coincide con la relación identidad si y sólo si X es un conjunto cruzado. Para ver esto supongamos que $\sim$ es la relación identidad, esto ocurre si y sólo si $x \sim x'$ con $x' = x$ para todo x en X. Sean $x, y \in X$ tales que $x \triangleright y = y$. Luego, $x \sim y \triangleright x$, o sea, $x = y \triangleright x$. Por lo tanto, X es un conjunto cruzado. Recíprocamente, si X es un conjunto cruzado y sean $x, x' \in X$ que satisfacen que existe $y \in X$ con $x \triangleright y = y$ e $y \triangleright x = x'$. Como $x \triangleright y = y$ se tiene que $y \triangleright x = x$. Luego, $x = x'$; por lo que $\sim$ resulta la relación identidad en X. Sea $X_1 := X/\sim$. Supongamos que x, x', y son como en (2.15). Entonces

$$x' \triangleright y = (y \triangleright x) \triangleright (y \triangleright y) = y \triangleright (x \triangleright y) = y.$$

Ahora, para $z \in X$ tenemos

$$y \triangleright (x' \triangleright z) = (x' \triangleright y) \triangleright (x' \triangleright z) = x' \triangleright (y \triangleright z) = (y \triangleright x) \triangleright (y \triangleright z) y = y \triangleright (x \triangleright z),$$

de ahí que $x' \triangleright z = x \triangleright z$, para todo $z \in X$, es decir que $\phi_x = \phi_{x'}$ y entonces $\phi_x = \phi_{x''}$ para algún x'' con $x'' \sim x$. De esta manera, tiene sentido considerar $\triangleright : X_1 \times X \to X$. Finalmente, tenemos para $z \in X$

$$\begin{aligned}(z \triangleright x) \triangleright (z \triangleright y) &= z \triangleright (x \triangleright y) = z \triangleright y \\ (z \triangleright y) \triangleright (z \triangleright x) &= z \triangleright (y \triangleright x) = z \triangleright x'.\end{aligned}$$

lo cual implica que $(z \triangleright x) \sim (z \triangleright x')$, y tiene sentido considerar $\triangleright : X_1 \times X_1 \to X_1$. Con esto se ve que X_1 hereda la estructura de quandle de X. Observar que por lo visto anteriormente $\operatorname{card}(X) \geq \operatorname{card}(X_1)$ y se da la igualdad si y sólo si $\sim$ es la relación identidad, es decir, si y sólo si X_1 es un conjunto cruzado. Si X_1 no es un conjunto cruzado entonces tomamos $X_2 := X_1/\sim$ y así siguiendo. De esta forma,construimos una sucesión X_k que se estabiliza en $k = n$ para algún n, pues X es finito; X_n resulta un conjunto cruzado. De esta manera, hemos exhibido un functor Q de la categoría de quandles finitos a la de conjuntos cruzados, el cual asigna a un quandle X un conjunto cruzado cociente $Q(X)$ que tiene la propiedad universal: cualquier morfismo de quandles $X \to Y$ se factoriza de manera única a través de $Q(X)$ siempre y cuando Y sea un conjunto cruzado.

2.2. Nociones básicas.

Definición 2.16. Sea $(X, \triangleright)$ un rack. Se dice que X es *trivial* si $i \triangleright j = j$, para todo $i, j \in X$.

Lema 2.17. *Sean $(X, \triangleright)$ un rack, H un grupo y $\varphi : X \to H$ un morfismo inyectivo de racks tal que la imagen es invariante por conjugación en H. Entonces $(X, \triangleright)$ es un conjunto cruzado y el mapa $\widetilde{\varphi} : H \to \mathbb{S}_X$, dado por*

$$\widetilde{\varphi}_h(x) = \varphi^{-1}(h\varphi(x)h^{-1})$$

es un homomorfismo de grupo cuya imagen está contenida en $\mathrm{Aut}_{\triangleright}(X)$.

Demostración. Sea $x \in X$. Luego, $\varphi(x \triangleright x) = \varphi(x) \triangleright \varphi(x) = \varphi(x)\varphi(x)\varphi(x)^{-1} = \varphi(x)$ y como φ es inyectiva se tiene que $x \triangleright x = x$. Además, si $x, y \in X$ con $x \triangleright y = y$ resulta que

$$\varphi(y) = \varphi(x \triangleright y) = \varphi(x) \triangleright \varphi(y) = \varphi(x)\varphi(y)\varphi(x)^{-1}$$

y esto implica que

$$\varphi(x) = \varphi(y)\varphi(x)\varphi(y)^{-1} = \varphi(y \triangleright x),$$

entonces $y \triangleright x = x$ y $(X, \triangleright)$ resulta un conjunto cruzado. Sean $h, h' \in H$. Veamos que $\widetilde{\varphi}_{hh'} = \widetilde{\varphi}_h\widetilde{\varphi}_{h'}$. Tomemos $x \in X$, luego

$$\begin{aligned}(\widetilde{\varphi}_h\widetilde{\varphi}_{h'})(x) &= \widetilde{\varphi}_h(\varphi^{-1}(h'\varphi(x)h'^{-1})) = \varphi^{-1}(h\varphi(\varphi^{-1}(h'\varphi(x)h'^{-1}))h^{-1}) = \\ &= \varphi^{-1}(hh'\varphi(x)h'^{-1}h^{-1}) = \widetilde{\varphi}_{hh'}(x)\end{aligned}$$

por lo que $\widetilde{\varphi} : H \to \mathbb{S}_X$ es un homomorfismo de grupos. Por otro lado, sean $h \in H$ y $x, y \in X$. Luego

$$\begin{aligned}\varphi(\widetilde{\varphi}_h(x) \triangleright \widetilde{\varphi}_h(y)) &= \varphi\widetilde{\varphi}_h(x) \triangleright \varphi\widetilde{\varphi}_h(y) = h\varphi(x)h^{-1} \triangleright h\varphi(y)h^{-1} = \\ &= h\varphi(x)h^{-1}h\varphi(y)h^{-1}(h\varphi(x)h^{-1})^{-1} = h\varphi(x)\varphi(y)(\varphi(x))^{-1}h^{-1} = \\ &= h(\varphi(x) \triangleright \varphi(y))h^{-1} = h(\varphi(x \triangleright y))h^{-1} = \varphi(\widetilde{\varphi}_h(x \triangleright y)).\end{aligned}$$

Como φ es inyectiva se tiene que

$$\widetilde{\varphi}_h(x \triangleright y) = \widetilde{\varphi}_h(x) \triangleright \widetilde{\varphi}_h(y)$$

con lo que se ve que $\widetilde{\varphi}_h \in \mathrm{Aut}_{\triangleright}(X)$, para todo $h \in H$. □

La asignación $X \to \mathrm{Inn}_{\triangleright}(X)$, en general, no es funtorial. Tomar $i \in X$ con $\phi_i \neq \mathrm{id}$, la inclusión $\{i\} \subset X$ no se extiende a un morfismo $\mathrm{Inn}_{\triangleright}(\{i\}) \to \mathrm{Inn}_{\triangleright}(X)$. Sin embargo, se tiene el siguiente Lema.

Lema 2.18. *Sea $(X, \triangleright)$ un rack finito. Si $\pi : X \to Y$ es un morfismo suryectivo de racks entonces se extiende a un homomorfismo de grupos* $\mathrm{Inn}_{\triangleright}(\pi) : \mathrm{Inn}_{\triangleright}(X) \to \mathrm{Inn}_{\triangleright}(Y)$.

Demostración. Observemos que como X es finito entonces $\mathbb{S}_X$ es finito y, por lo tanto, $\mathrm{Inn}_\triangleright(X)$ es finito. Luego, se cumple para y en X que

$$\phi_y^{-1} = \phi_{y_1} \dots \phi_{y_r}$$

con $y_1, \dots, y_r \in X$. Sea $\varphi \in \mathrm{Inn}_\triangleright(X)$, con $\varphi = \phi_{x_1} \dots \phi_{x_s}$ definimos

$$\mathrm{Inn}_\triangleright(\pi)(\varphi) := \phi_{\pi(x_1)} \dots \phi_{\pi(x_s)}.$$

Está bien definida pues si $\phi = \phi_{x_1} \dots \phi_{x_s} = \varphi = \phi_{y_1} \dots \phi_{y_r}$ ocurre que

$$\phi_{\pi(x_1)} \dots \phi_{\pi(x_s)} = \phi_{\pi(y_1)} \dots \phi_{\pi(y_r)},$$

ya que π es suryectiva, esto es

$$\begin{aligned}\phi_{\pi(x_1)} \dots \phi_{\pi(x_s)}(z) &= \pi(x_1) \triangleright (\pi(x_2) \triangleright (\dots (\pi(x_s) \triangleright z) \dots)) = \pi(x_1 \triangleright (x_2 \triangleright (\dots (x_s \triangleright z') \dots) = \\ &= \pi(y_1 \triangleright (y_2 \triangleright (\dots (y_r \triangleright z') \dots))) = \pi(y_1) \triangleright (\pi(y_2) \triangleright (\dots (\pi(y_r) \triangleright z) \dots)) = \\ &= \phi_{\pi(y_1)} \dots \phi_{\pi(y_r)}(z),\end{aligned}$$

donde $z \in X$ y $\pi(z') = z$. Por otra parte, $\mathrm{Inn}_\triangleright(\pi)$ es un homomorfismo por definición. □

Determinaremos ahora la estructura de $\mathrm{Inn}_\triangleright(X)$ cuando X es estándar.

Lema 2.19. *Sea H un grupo y sea $X \subset H$ un subconjunto estándar.*

(a) $\mathrm{Inn}_\triangleright(X) \simeq C/Z(C)$*, donde $C = \langle X \rangle$ es el subgrupo de H generado por X, el cual es claramente normal.*

(b) Si X genera H entonces $\mathrm{Inn}_\triangleright(X) \simeq H/Z(H)$.

(c) Si H es simple, no abeliano y $X \neq \{e\}$ entonces $H = \mathrm{Inn}_\triangleright(X)$.

Demostración. (a) Se sigue de (b).

(b) Consideremos la función $\varphi : H \to \mathbb{S}_X$, dada por $\varphi_h(x) = hxh^{-1}$. Como X es estándar entonces φ está bien definida y resulta obvio que es un homomorfismo de grupos. Además, si $y \in X$ se tiene que $\varphi_y(x) = yxy^{-1} = y \triangleright x = \phi_y(x)$, para todo $x \in X$; es decir $\langle \varphi(X) \rangle = \mathrm{Im}\,\varphi = \mathrm{Inn}_\triangleright(X)$. Por otro lado

$$\begin{aligned}\ker(\varphi) &= \{h \in H \ / \ \varphi_h = \mathrm{id}\} = \{h \in H \ / \ hxh^{-1} = x, \ \forall x \in X\} = \\ &= Z(X) = Z(\langle X \rangle) = Z(H).\end{aligned}$$

Luego, $H/Z(H) \simeq \mathrm{Inn}_\triangleright(X)$.

(c) Como $X \neq \{e\}$ y H es simple se tiene que $\langle X \rangle = H$. Luego, por (b) $\mathrm{Inn}_\triangleright(X) \simeq H/Z(H)$. Ahora bien como H no es abeliano tenemos que $Z(H) \neq H$, entonces $Z(H) = \{e\}$. Por lo tanto, $\mathrm{Inn}_\triangleright(X) \simeq H$. □

Corolario 2.20. *Sean $(X, \triangleright)$ un rack, H un grupo y $\psi : X \to H$ un morfismo de racks. Si $Z(\langle \psi(X) \rangle)$ es trivial entonces ψ se extiende a un morfismo de grupos $\Psi : \mathrm{Inn}_{\triangleright}(X) \to H$.*

Demostración. Sea H' el subgrupo de H generado por $Y = \psi(X)$. Ahora bien, si $h \in H'$ entonces $h = \psi(x_1) \dots \psi(x_n)$, donde $x_1, \dots, x_n \in X$. Luego, si $x \in X$ se tiene que

$$h\psi(x)h^{-1} = \psi(x_1) \dots \psi(x_n)\psi(x)\psi(x_n)^{-1} \dots \psi(x_1)^{-1} = \psi(x_1 \triangleright (\dots (x_n \triangleright x) \dots)) \in Y.$$

De esta manera, Y es estable por conjugación en H', es decir Y es un conjunto cruzado estándar de H'. Por los Lemas 2.18 y 2.19 existe un homomorfismo

$$\widetilde{\Psi} := \mathrm{Inn}_{\triangleright}(\psi) : \mathrm{Inn}_{\triangleright}(X) \to \mathrm{Inn}_{\triangleright}(Y) \simeq H'/Z(H') = H'.$$

Ahora si $\iota : H' \to H$ es el mapa inclusión entonces $\Psi = \iota\widetilde{\Psi}$ es el morfismo buscado. □

El mapa $\phi : X \to \mathrm{Inn}_{\triangleright}(X)$, en general, no es inyectivo, pues si $\mathrm{card}(X) > 1$ y $(X, \triangleright_f)$ es un rack de permutación tenemos que $\phi_x = f$ para todo x en X, por lo que ϕ no es inyectiva.

Definición 2.21. Se dice que el rack $(X, \triangleright)$ es *exacto* si la función ϕ correspondiente es inyectiva.

Observación 2.22. Si X es un rack exacto entonces X es un conjunto cruzado ya que

(i) $\phi_{x \triangleright x} = \phi_x \phi_x \phi_x^{-1} = \phi_x$ lo que implica que $x \triangleright x = x$.

(ii) si $x \triangleright y = y$ se tiene que $\phi_{x \triangleright y} = \phi_x \phi_y \phi_x^{-1} = \phi_y$ lo que implica $\phi_x = \phi_y \phi_x \phi_y^{-1} = \phi_{y \triangleright x}$ y como ϕ es inyectiva tenemos que $x = y \triangleright x$.

Observación 2.23. Si $(X, \triangleright)$ es exacto entonces el centro de $\mathrm{Inn}_{\triangleright}(X)$ es trivial. Más generalmente, si $\varphi \in Z(\mathrm{Inn}_{\triangleright}(X))$ entonces $\phi_{\varphi(x)} = \phi_x$, para todo $x \in X$.

Demostración. Tomemos $x \in X$ y $\varphi \in Z(\mathrm{Inn}_{\triangleright}(X))$; luego

$$\phi_x(\varphi(y)) = \phi_x \varphi(y) = \varphi \phi_x(y) = \varphi(x \triangleright y) = \varphi(x) \triangleright \varphi(y) = \phi_{\varphi(x)}(\varphi(y)),$$

y como $\varphi \in \mathbb{S}_X$ se tiene que $\phi_x = \phi_{\varphi(x)}$. □

Veamos ahora cuándo se puede escribir un rack como unión disjunta de algunos de sus subracks.

Definición 2.24. Una *descomposición* de un rack $(X, \triangleright)$ es una unión disjunta $X = Y \cup Z$ tal que Y y Z son subracks de X.

En particular, Y y Z son conjuntos no vacíos.

Definición 2.25. Un rack $(X, \triangleright)$ se dice *descomponible* si admite una descomposición e *indescomponible* en caso contrario.

La imagen de un rack indescomponible X por un morfismo $\pi : X \to Y$ es indescomponible puesto que si $\pi(X)$ es descomponible existen subconjuntos no vacíos Y_1, Y_2 de Y, disjuntos, que son subracks, tales que $\pi(X) = Y_1 \cup Y_2$. Luego, $X = X_1 \cup X_2$ donde $X_1 = \pi^{-1}(Y_1)$ y $X_2 = \pi^{-1}(Y_2)$ con X_1, X_2 subconjuntos no vacíos, que son subracks de X y disjuntos lo cual contradice la hipótesis de indescomponibilidad de X.

Denotaremos $i^n \triangleright j := \phi_i^n(j)$, para todo n en $\mathbb{Z}$.

Definición 2.26. La *órbita* de un elemento $x \in X$ es el subconjunto

$$\mathcal{O}_x := \{i_s^{\pm 1} \triangleright (i_{s-1}^{\pm 1} \triangleright (\dots (i_1^{\pm 1} \triangleright x) \dots)) \ / \ i_1, \dots, i_s \in X\}.$$

Es decir, $\mathcal{O}_x$ es la órbita de x bajo la acción natural del grupo $\mathrm{Inn}_{\triangleright}(X)$. Si X es finito, entonces

$$\mathcal{O}_x = \{i_s \triangleright (i_{s-1} \triangleright (\dots (i_1 \triangleright x) \dots)) \ / \ i_1, \dots, i_s \in X\}.$$

Lema 2.27. *Sean $(X, \triangleright)$ un rack finito, $Y \neq X$ un subconjunto no vacío de X y $Z = X - Y$. Entonces, las siguientes afirmaciones son equivalentes*

(a) $X = Y \cup Z$ es una descomposición de X.

(b) $Y \triangleright Z \subseteq Z$ y $Z \triangleright Y \subseteq Y$.

(c) $X \triangleright Y \subseteq Y$.

Demostración. (a)⇒(b). Sean $y \in Y$, $z \in Z$. Como Y es un subrack de X se tiene que $\phi_y : Y \to Y$ es una biyección. Luego, si $y \triangleright z \in Y$ entonces existe un único $y' \in Y$ tal que $\phi_y(y') = y \triangleright y' = y \triangleright z$, y como $\phi_y : X \to X$ es biyectiva entonces $y' = z \in Y$ lo cual es absurdo pues $Y \cap Z = \emptyset$. Por lo tanto, $y \triangleright z \in Z$ para todo $y \in Y, z \in Z$. De manera análoga se prueba que $Z \triangleright Y \subseteq Y$.

(b)⇒(c). Sea $x \in X$. Si $x \in Z$ se tiene que $x \triangleright y \in Y$ para todo $y \in Y$, por hipótesis. Ahora bien, si $x \in Y$ sabemos que $\phi_x : X \to X$ es biyectiva y $\phi_x(Z) \subseteq Z$ y como X es finito entonces $\phi_x(Z) = Z$ y $\phi_x(Y) = Y$, para todo $x \in X$. Luego, $X \triangleright Y \subseteq Y$.

(c)⇒(a). Basta ver que Y y Z son subracks de X. Y es subrack de X pues $Y \triangleright Y \subseteq X \triangleright Y \subseteq Y$ por hipótesis. Sea $z \in Z$; luego $\phi_z : X \to X$ es biyectiva y $\phi_z(Y) \subseteq Y$ y como X es finito implica que $\phi_z(Y) = Y$ y por lo tanto $\phi_z(Z) \subseteq Z$ y Z resulta un subrack. □

Lema 2.28. *Sea $(X, \triangleright)$ un rack finito. Entonces las siguientes afirmaciones son equivalentes*

(a) X es indescomponible.

(b) $X = \mathcal{O}_x$ para todo (o para algún) $x \in X$.

Demostración. (a)⇒(b). Supongamos, por el absurdo, que existe $x \in X$ tal que $\mathcal{O}_x \neq X$. Tenemos que $\mathcal{O}_x \neq \emptyset$ y $Z = X - \mathcal{O}_x \neq \emptyset$. Sea $z \in X$ y sea $w \in \mathcal{O}_x$; luego $z \triangleright w = \phi_z(w) \in \mathcal{O}_x$. Entonces $X \triangleright \mathcal{O}_x \subseteq \mathcal{O}_x$. Por Lema 2.27 se tiene que X es descomponible, contra lo supuesto. Por lo tanto, $X = \mathcal{O}_x$, para todo $x \in X$.

(b)⇒(a). Si X fuera descomponible entonces existen subconjuntos de X, no vacíos, disjuntos, Y y Z tales que $X = Y \cup Z$. Sea $y \in Y$; luego

$$\mathcal{O}_y = \{i_s \triangleright (i_{s-1} \triangleright (\dots (i_1 \triangleright y) \dots)) \ / \ i_1, \dots, i_s \in X\}$$

por ser X finito y por Lema 2.27 $\mathcal{O}_y \subseteq Y \neq X$ lo cual es absurdo. □

Observación 2.29. Sea H un grupo no trivial. Si consideramos a H como un conjunto estándar entonces no es indescomponible. En efecto, si $\mathcal{C} \subset H$ es una clase de conjugación entonces $\mathcal{C}$ es un subrack. Por lo tanto, $H = \mathcal{C} \cup (H - \mathcal{C})$ es una descomposición de H. En particular, $H = \{e\} \cup (H - \{e\})$.

Sea X un conjunto estándar de un grupo no trivial H. Se puede ver, a partir de la observación anterior, que si X es indescomponible entonces X es una clase de conjugación en H. La recíproca solamente es cierta si $X = \{e\}$, la clase de conjugación de la identidad en H (ver Ejemplo 2.30). Sin embargo, si H es simple y X es una clase de conjugación entonces X es indescomponible. En efecto, si $X \neq \{e\}$ se tiene, por Lema 2.19, que $\mathcal{O}_x = X$, para todo $x \in X$, es decir, X es indescomponible. Mientras que si $X = \{e\}$ la afirmación es obvia.

Ejemplo 2.30. Sea A un grupo abeliano y G el grupo de isomorfismos de A. Consideremos $H = A \rtimes G$ y sea $X = \{(g(a), 1)/g \in G\}$. Con la identificación $a \leftrightarrow (a, 1)$ se ve que X es la órbita de a por la acción de G. Entonces X es trivial ya que

$$(f(a), 1) \triangleright (g(a), 1) = (f(a), 1)(g(a), 1)(f(a), 1)^{-1} = (g(a), 1)$$

para todo $f, g \in G$.

Proposición 2.31. *Todo rack finito X es unión disjunta de sus subracks indescomponibles maximales.*

Demostración. Dado $x \in X$ sea $A_x = \{x^n \triangleright x \ / \ n \in \mathbb{Z}\}$. Luego, A_x es un subrack indescomponible que contiene a x pues si $y, z \in A_x$ con $y = x^n \triangleright x$ y $z = x^m \triangleright x$ se tiene que

$$\begin{aligned} y \triangleright z = (x^n \triangleright x) \triangleright (x^m \triangleright x) = \phi_x^n(x) \triangleright \phi_x^m(x) = \phi_x^n(x \triangleright \phi_x^{m-n}(x)) = \\ = \phi_x^n(\phi_x(\phi_x^{m-n}(x))) = \phi_x^{m+1}(x) \in A_x \end{aligned}$$

y A_x resulta un subrack de X. Es indescomponible pues si $y \in A_x$ con $y = x^n \triangleright x$ entonces $A_x = \mathcal{O}_y$; ya que si $z \in A_x$ con $z = x^m \triangleright x$ tenemos que

$$z = \phi_x^m(x) = \phi_x^{m-n}(\phi_x^n(x)) = \phi_x^{m-n}(y) \in \mathcal{O}_y,$$

y por Lema 2.28 se tiene que A_x es indescomponible.

Sea $Y \subseteq X$, un subconjunto cualquiera de X. Definimos

$$Y' := Y \cup (Y \triangleright Y) \cup (Y^{-1} \triangleright Y),$$

donde $Y^{-1} \triangleright Y = \{\phi_y^{-1}(z) \ / \ y, z \in Y\}$. Es obvio que $Y \subseteq Y'$ y es fácil ver que todo subrack de X que contiene a Y contiene a Y', pues si Z es subrack de X que contiene a Y entonces

$$Y \triangleright Y \subseteq Z \triangleright Z \subseteq Z$$

$$Y^{-1} \triangleright Y = \{\phi_y^{-1}(z)/y, z \in Y\} \subseteq \{\phi_y^{-1}(z)/y, z \in Z\} \subseteq Z^{-1} \triangleright Z \subseteq Z.$$

Luego, si definimos que el subrack generado por Y, $\langle Y \rangle$, es el subrack de X más pequeño que contiene a Y entonces

$$\langle Y \rangle = \cup_{n \in \mathbb{N}} Y^n, \text{ donde } Y^{n+1} = (Y^n)' \text{ e } Y^1 = Y \ .$$

Para ver esto, tomemos Z subrack de X que contiene a Y. Luego, $Y' \subseteq Z$ por lo visto anteriormente. Como $Y^2 = (Y^1)' = Y'$ entonces $Y^2 \subseteq Z$; así siguiendo $(Y^n)' \subseteq Z$, para todo $n \in \mathbb{N}$. Luego, $\cup_{n \in \mathbb{N}} Y^n \subseteq Z$. Es fácil ver que $\cup_{n \in \mathbb{N}} Y^n$ es un subrack de X. Esto implica que $\cup_{n \in \mathbb{N}} Y^n$ es el subrack de X más pequeño que contiene a Y.

Sean $y_1, y_2 \in Y$. Diremos que y_1 e y_2 son *conectables* (o que están *conectados*) si existen $u_1, \ldots, u_n \in Y$ tales que

$$y_2 = u_1^{\pm 1} \triangleright (u_2^{\pm 1} \triangleright (\ldots (u_n^{\pm 1} \triangleright y_1) \ldots)).$$

Diremos que Y es *conexo* si y_1 e y_2 son conectables, para todo $y_1, y_2 \in Y$.

A continuación verificamos por casos que si Y es conexo entonces Y' es conexo. Sean $y_1, y_2 \in Y' = Y \cup (Y \triangleright Y) \cup (Y^{-1} \triangleright Y)$

(1) si $y_1, y_2 \in Y$ entonces y_1 e y_2 están conectados pues Y es conexo.

(2) si $y_1 \in Y$ e $y_2 \in Y \triangleright Y$, donde $y_2 = y_{21} \triangleright y_{22}$ con $y_{21}, y_{22} \in Y$. Como Y es conexo existen $u_1, \dots, u_n \in Y$ tales que $y_{22} = u_1^{\pm 1} \triangleright (u_2^{\pm 1} \triangleright (\dots (u_n^{\pm 1} \triangleright y_1) \dots))$. Luego,

$$y_2 = y_{21} \triangleright (u_1^{\pm 1} \triangleright (u_2^{\pm 1} \triangleright (\dots (u_n^{\pm 1} \triangleright y_1) \dots)))$$

resultando y_1 e y_2 conectables.

(3) si $y_1 \in Y$ e $y_2 \in Y^{-1} \triangleright Y$ con $y_2 = y_{21}^{-1} \triangleright y_{22}$ se tiene que y_1 e y_2 están conectados de la misma manera que en caso anterior.

(4) si $y_1, y_2 \in Y \triangleright Y$ con $y_1 = y_{11} \triangleright y_{12}$ e $y_2 = y_{21} \triangleright y_{22}$ con $y_{ij} \in Y$. Como y_{11} e y_{12} están conectados con y_{21} e y_{22}, respectivamente, existen $u_1, \dots, u_r, v_1, \dots, v_s \in Y$ tales que

$$\begin{aligned} y_{21} &= u_1^{\pm 1} \triangleright (u_2^{\pm 1} \triangleright (\dots (u_r^{\pm 1} \triangleright y_{11}) \dots)) \\ y_{22} &= v_1^{\pm 1} \triangleright (v_2^{\pm 1} \triangleright (\dots (v_s^{\pm 1} \triangleright y_{12}) \dots)). \end{aligned}$$

Luego,

$$\begin{aligned} y_2 = y_{21} \triangleright y_{22} &= \phi_{y_{21}}(y_{22}) = \phi_{u_1^{\pm 1} \triangleright (u_2^{\pm 1} \triangleright (\dots (u_r^{\pm 1} \triangleright y_{11}) \dots))}(y_{22}) = \\ &= \phi_{u_1}^{\pm 1} \dots \phi_{u_r}^{\pm 1} \phi_{y_{11}} \phi_{u_r}^{\mp 1} \dots \phi_{u_1}^{\mp 1} \phi_{v_1}^{\pm 1} \dots \phi_{v_s}^{\pm 1} \phi_{y_{11}}^{-1}(\phi_{y_{11}}(y_{12})) = \\ &= u_1^{\pm 1} \triangleright (\dots (u_n^{\pm 1} \triangleright (y_1 \triangleright (u_r^{\mp 1} \triangleright (\dots (u_1^{\mp 1} \triangleright (v_1^{\pm 1} \triangleright (\dots (v_s^{\pm 1} \triangleright (y_{11}^{-1} \triangleright (y_{11} \triangleright y_{12}))) \dots) \end{aligned}$$

con lo que y_1 e y_2 están conectados.

Los demás casos son análogos.

Además, $\langle Y \rangle$ es conexo pues si $y_1, y_2 \in \langle Y \rangle$, digamos que $y_1 \in Y^r$ e $y_2 \in Y^s$ y suponiendo que $r \geq s$ entonces $y_2 \in Y^r$. Como Y^r es conexo se tiene que

$$y_2 = u_1^{\pm 1} \triangleright (u_2^{\pm 1} \triangleright (\dots (u_s^{\pm 1} \triangleright y_1) \dots))$$

donde $u_1, \dots, u_s \in Y^r \subseteq \langle Y \rangle$. De esta manera, $\langle Y \rangle$ es un subrack indescomponible por 2.28.

Por último afirmamos que si $\{Y_i\}_{i \in I}$ es una familia de subracks de X, indescomponibles tales que $\cap_{i \in I} Y_i \neq \emptyset$ entonces $\cup_{i \in I} Y_i$ es conexo; para ver esto tomemos $y_1, y_2 \in \cup_{i \in I} Y_i$, con $y_1 \in Y_{i_1}$ e $y_2 \in Y_{i_2}$. Sea $x \in \cap_{i \in I} Y_i$. Como y_1, y_2 están conectados con x tenemos que

$$\begin{aligned} y_1 &= u_1^{\pm 1} \triangleright (u_2^{\pm 1} \triangleright (\dots (u_r^{\pm 1} \triangleright x) \dots)) \\ x &= v_1^{\pm 1} \triangleright (v_2^{\pm 1} \triangleright (\dots (v_s^{\pm 1} \triangleright y_2) \dots)) \end{aligned}$$

con $u_1, \dots, u_r, v_1, \dots, v_s \in \cup_{i \in I} Y_i$. Luego,

$$y_1 = u_1^{\pm 1} \triangleright (u_2^{\pm 1} \triangleright (\dots (u_r^{\pm 1} \triangleright (v_1^{\pm 1} \triangleright (v_2^{\pm 1} \triangleright (\dots (v_s^{\pm 1} \triangleright y_2) \dots)))) \dots))$$

con lo que y_1 e y_2 resultan conectados.

Sea $x \in X$. Definimos

$$M_x = \langle \bigcup_{\substack{x \in Y \subset X \\ Y \text{indescomponible}}} Y \rangle.$$

Luego, M_x es un subrack indescomponible y maximal (el subrack indescomponible más grande que contiene a x). Es obvio que $X = \cup_{x \in X} M_x$. Ahora bien si $M_x \cap M_{x'} \neq \emptyset$ entonces $\langle M_x \cup M_{x'} \rangle$ es un subrack indescomponible que contiene a x y x'. Por lo tanto,

$$M_x, M_{x'} \subseteq M_x \cup M_{x'} \subseteq \langle M_x \cup M_{x'} \rangle \subseteq M_{x'}, M_x;$$

y por maximalidad de M_x y M'_x esto implica que $M_x = M_x \cup M_{x'} = M_{x'}$. Llamamos a M_x la *componente indescomponible* de x. Así, X es la unión disjunta de componentes indescomponibles, las cuales son subracks indescomponibles maximales. Además, si M es un subrack indescomponible maximal entonces $M = M_x$ para algún $x \in M$. Con esto se finaliza la prueba. □

Salvo la situación del Lema 2.27 las componentes indescomponibles pueden no ser estables bajo la acción de X.

El caso de dos componentes es más satisfactorio porque podemos describir cómo pegar dos racks.

Lema 2.32. *(a). Sean Y, Z dos racks y $X = Y \sqcup Z$ la unión disjunta. Las siguientes afirmaciones son equivalentes*

(i) X tiene una estructura de rack tal que $X = Y \cup Z$ es una descomposición.

(ii) Existe un par (σ, τ) $\sigma : Y \to \mathrm{Aut}_{\triangleright}(Z)$, $\tau : Z \to \mathrm{Aut}_{\triangleright}(Y)$ de morfismos de racks tales que

$$y \triangleright \tau_z(u) = \tau_{\sigma_y(z)}(y \triangleright u), \qquad \forall y, u \in Y, \quad z \in Z, \qquad \textit{i.e.,}\ \phi_y \tau_z = \tau_{\sigma_y(z)} \phi_y, \tag{2.33}$$

$$z \triangleright \sigma_y(w) = \sigma_{\tau_z(y)}(z \triangleright w), \qquad \forall y \in Y, \quad z, w \in Z, \qquad \textit{i.e.,}\ \phi_z \sigma_y = \sigma_{\tau_z(y)} \phi_z. \tag{2.34}$$

(b) Supongamos que Y y Z son conjuntos cruzados y se cumplen (2.33) *y* (2.34)*. Entonces X es un conjunto cruzado exactamente cuando*

$$\sigma_y(z) = z \quad \textit{ si y sólo si } \quad \tau_z(y) = y, \quad \forall y \in Y, \quad z \in Z. \tag{2.35}$$

Demostración. (a). (i)⇒(ii). Supongamos que X tiene estructura de rack tal que $X = Y \cup Z$ es una descomposición de X. Notemos que esto dice que $\triangleright_X|_{Y \times Y} = \triangleright_Y$ y que $\triangleright_X|_{Z \times Z} = \triangleright_Z$, donde $\triangleright_X = \triangleright$, $\triangleright_Y$ y $\triangleright_Z$ denotan la operación $\triangleright$ en X, Y y Z, respectivamente. Definimos $\sigma : Y \to \mathrm{Aut}_{\triangleright}(Z)$ y $\tau : Z \to \mathrm{Aut}_{\triangleright}(Y)$ por

$$\sigma_y(z) := y \triangleright z$$
$$\tau_z(y) := z \triangleright y,$$

para todo $y \in Y$, $z \in Z$. Por Lema 2.27 se tiene que $\sigma_y(z) \in Z$ y como $\sigma_y = \phi_y|_Z$ entonces $\sigma_y \in \mathrm{Aut}_{\triangleright}(Z)$, para todo $y \in Y$ y por lo tanto σ está bien definida. Por otra parte, como $\phi : X \to \mathrm{Aut}_{\triangleright}(X)$ es un morfismo de racks resulta que $\widetilde{\sigma} = \phi|_Y : Y \to \mathrm{Aut}_{\triangleright}(X)$ es un morfismo de rack, entonces σ también lo es. De manera análoga se puede ver que τ está bien definida y es un morfismo de racks. Ahora bien

$$y \triangleright \tau_z(u) = y \triangleright (z \triangleright u) = (y \triangleright z) \triangleright (y \triangleright u) = \sigma_y(z) \triangleright (y \triangleright u) = \tau_{\sigma_y(z)}(y \triangleright u),$$

$$z \triangleright \sigma_y(w) = z \triangleright (y \triangleright w) = (z \triangleright y) \triangleright (z \triangleright w) = \tau_z(y) \triangleright (z \triangleright w) = \sigma_{\tau_z(y)}(z \triangleright w),$$

para todo $y, u \in Y$, $w, z \in Z$. Luego, se satisfacen (2.33) y (2.34).

(ii)⇒(i). Definimos $\triangleright : X \to X$ por

$$\begin{aligned} y \triangleright z &:= \sigma_y(z), \\ z \triangleright y &:= \tau_z(y), \end{aligned}$$

para todo $y \in Y$, $z \in Z$; mientras que

$$\begin{aligned} \triangleright &:= \triangleright_Y \quad \text{en } Y \times Y, \\ \triangleright &:= \triangleright_Z \quad \text{en } Z \times Z\ . \end{aligned}$$

Sea $x \in X$ y supongamos que $x \in Y$; luego $\phi_x : X \to X$ dada por $\phi_x(x') = x \triangleright x'$ es biyectiva puesto que $\phi_x|_Y : Y \to Y$ lo es y $\phi_x|_Z : Z \to Z$ cumple que $\phi_x|_Z = \sigma_x$ que es biyectiva ya que $\sigma_x \in \mathrm{Aut}_{\triangleright}(Z)$. Si $x \in Z$ se procede de la misma manera. Resta mostrar la propiedad (2.3), que se verifica por casos. Hay que ver que $a \triangleright (b \triangleright c) = (a \triangleright b) \triangleright (a \triangleright c)$, para todo $a, b, c \in X$.

(1) Si $a, b, c \in Y$ se satisface dicha propiedad pues Y es un rack. Lo mismo ocurre si $a, b, c \in Z$.

(2) Si $a, b \in Y$ y $c \in Z$ entonces

$$a \triangleright (b \triangleright c) = a \triangleright \sigma_b(c) = (\sigma_a\sigma_b)(c) = (\sigma_a\sigma_b\sigma_a^{-1})(\sigma_a(c)) = (\sigma_a \triangleright \sigma_b)(\sigma_a(c)) =$$

$$= \sigma_{a \triangleright b}(\sigma_a(c)) = (a \triangleright b) \triangleright \sigma_a(c) = (a \triangleright b) \triangleright (a \triangleright c).$$

(3) Si $a \in Y$ y $b, c \in Z$ se tiene

$$a \triangleright (b \triangleright c) = \sigma_a(b \triangleright c) = \sigma_a(b) \triangleright \sigma_a(c) = (a \triangleright b) \triangleright (a \triangleright c).$$

(4) Si $a, c \in Y$ y $b \in Z$ resulta

$$a \triangleright (b \triangleright c) = a \triangleright \tau_b(c) = \tau_{\sigma_a(b)}(a \triangleright c) = \sigma_a(b) \triangleright (a \triangleright c) = (a \triangleright b) \triangleright (a \triangleright c).$$

Los demás casos son similares a estos.

(b). Supongamos que se cumple (2.35). Como Y, Z son conjuntos cruzados entonces $x \triangleright x = x$, para todo $x \in X$. Ahora bien, sean $x, x' \in X$ tales que $x \triangleright x' = x'$.

1) Si $x, x' \in Y$ entonces $x' \triangleright x = x$ pues Y es un conjunto cruzado.

2) Si $x, x' \in Z$ ocurre lo mismo que antes.

3) Si $x \in Y$ y $x' \in Z$, $x \triangleright x' = x'$ implica $\sigma_x(x') = x'$ entonces por suposición $\tau_{x'}(x) = x$, es decir $x' \triangleright x = x$.

4) Si $x \in Z$ y $x' \in Y$, $x \triangleright x' = x'$ implica $\tau_x(x') = x'$ lo cual implica que $\sigma_{x'}(x) = x$, o sea $x' \triangleright x = x$.

Por lo tanto, X es un conjunto cruzado. La recíproca es obvia. □

Si las condiciones del Lema son satisfechas, diremos que X es la *suma amalgamada* de Y y Z. Si σ y τ son triviales decimos que X es la *suma disjunta* de Y y Z. Análogamente, se puede definir la suma de cualquier familia de racks (resp. quandles, conjuntos cruzados). Sea $\{Y_i\}_{i\in I}$ una familia de racks tales que para cada par $(i,j) \in I \times I$ existe un morfismo de racks $\sigma^{ij} : Y^i \to \mathrm{Aut}_{\triangleright}(Y^j)$, dado por $x \mapsto \sigma_x^{ij}$, que satisface

$$\sigma_x^{ik}\sigma_y^{jk} = \sigma^{jk}_{\sigma_x^{ij}(y)}\sigma_x^{ik}$$

para todo $i, j, k \in I$, distintos entre sí y para todo $x \in Y_i$, $y \in Y_j$. Si consideramos $X = \bigsqcup_{i\in I} Y_i$, la unión disjunta de dicha familia de racks, y $\sigma^{ii} : Y^i \to \mathrm{Aut}_{\triangleright}(Y^i)$, dada por $\sigma_x^{ii}(y) = x \triangleright_{Y_i} y$, definimos $\triangleright$ por

$$x \triangleright y := \sigma_x^{ij}(y)$$

si $x \in Y_i$, $y \in Y_j$. Resulta sencillo verificar que $(X, \triangleright)$ es un rack y X es la suma amalgamada de la familia $\{Y_i\}_{i\in I}$.

Por otro lado, sea X un rack (resp. quandle, conjunto cruzado) y sea $2X = X \times \{1, 2\}$. Luego, es fácil ver que $2X$ es un rack (resp. quandle, conjunto cruzado) con

$$(x, i) \triangleright (y, j) := (x \triangleright y, j).$$

Además $2X$ no es indescomponible ya que $2X = X_1 \cup X_2$, con $X_i = X \times \{i\}$, es una descomposición; y no es exacto pues $\phi : 2X \to \mathrm{Inn}_{\triangleright}(2X)$ no es inyectiva puesto que $\phi_{(x,1)} = \phi_{(x,2)}$. En forma análoga, se define el conjunto cruzado nX para cualquier entero positivo.

Podemos enunciar esto de manera más general.

Ejemplo 2.36. Sean X, Y dos racks (resp. quandles, conjuntos cruzados). Entonces $X \times Y$ es un rack (resp. quandle, conjunto cruzado) con $(x, y) \triangleright (u, v) := (x \triangleright u, y \triangleright v)$. Esto es el producto directo de X e Y en la categoría de racks (resp. quandles, conjuntos cruzados).

Lema 2.37. *Sean X, Y dos racks.*

(a) Si $X \times Y$ es indescomponible entonces X e Y son indescomponibles.

(b) Si X, Y son indescomponibles y X ó Y es quandle entonces $X \times Y$ es indescomponible.

Demostración. (a). Como las proyecciones $X \times X \to X$, $Y \times Y \to Y$ son morfismos suryectivos de racks entonces X e Y resultan indescomponibles.

(b). Supongamos que X es quandle. Sean $(x_1, y_1), (x_2, y_2) \in X \times Y$ entonces existen $u_1, \dots, u_n \in X$ y $v_1, \dots, v_m \in Y$ tales que

$$x_2 = u_1^{\epsilon_1} \triangleright (u_2^{\epsilon_2} \triangleright (\dots (u_n^{\epsilon_n} \triangleright x_1) \dots)),$$

$$y_2 = v_1^{\epsilon'_1} \triangleright (v_2^{\epsilon'_2} \triangleright (\dots (v_m^{\epsilon'_m} \triangleright y_1) \dots)),$$

donde $\epsilon_i, \epsilon'_j \in \{\pm 1\}$. Agregando, si es necesario, y_1, y_1^{-1} al final de la sucesión en Y podemos suponer que $m \geq n$. Luego, agregando al final de la sucesión en X elementos x_1 podemos suponer que $m = n$. Entonces,

$$(x_2, y_2) = (u_1^{\epsilon_1}, v_1^{\epsilon'_1}) \triangleright ((u_2^{\epsilon_2}, v_1^{\epsilon'_2}) \triangleright (\dots ((u_n^{\epsilon_n}, v_n^{\epsilon'_n}) \triangleright (x_1, y_1)) \dots)),$$

con lo que $X \times Y$ resulta indescomponible. □

Como un contraejemplo de 2.37(b) citamos los rack de permutación dados por $X = \mathbb{Z}_2$, $Y = \mathbb{Z}_4$ y $f_i : \mathbb{Z}_i \to \mathbb{Z}_i$, $f(\text{clase de } n) := \text{clase de } (n+1)$, $i = 2, 4$. Luego,

$$\mathcal{O}_x = \{f_2^r(x) \ / \ r \in \mathbb{Z}\} = X,$$

$$\mathcal{O}_y = \{f_4^r(x) \ / \ r \in \mathbb{Z}\} = Y,$$

para todo $x \in X$, $y \in Y$; por lo tanto X, Y son indescomponibles. Pero $X \times Y$ no lo es ya que

$$\mathcal{O}_{(0,0)} = \{(f_2^r(0), f_4^r(0)) \ / \ r \in \mathbb{Z}\} = \{(0,0); (1,1); (0,2); (1,3)\} \neq X \times Y.$$

Sea X un rack y tomemos $\phi : X \to \mathrm{Inn}_{\triangleright}(X)$ como antes. Denotaremos $F_y := \phi^{-1}(y)$, una *fibra* de ϕ. Si X es un quandle entonces cualquier fibra F_y es un subquandle trivial ya que si $x, x' \in F_y$ se tiene que $\phi_{x \triangleright x'} = \phi_x \phi_{x'} \phi_x^{-1} = yyy^{-1} = y$, lo que implica que $x \triangleright x' \in F_y$; además

$$y(x \triangleright x') = \phi_{x'}(x \triangleright x') = (x' \triangleright x) \triangleright (x' \triangleright x') = (x' \triangleright x) \triangleright x' = y(x'),$$

y por lo tanto $x \triangleright x' = x'$, para todo $x, x' \in X$.

Lema 2.38. *Sea $f : X \to Y$ un morfismo suryectivo de racks. Si denotamos por G_y a la fibra $f^{-1}(y)$, para todo $y \in Y$, entonces*

(a) las fibras G_y y $G_{u \triangleright y}$ tienen la misma cardinalidad para todo $u, y \in Y$.

(b) si X es indescomponible entonces todas las fibras de f tienen la misma cardinalidad.

Demostración. (a). Sean $u, y \in Y$, donde $u = f(i)$ e $y = f(j)$. Definimos $\Phi : G_y \to G_{u \triangleright y}$ por

$$\Phi(k) := i \triangleright k = \phi_i(k).$$

Notemos que $f(i \triangleright k) = f(i) \triangleright f(k) = u \triangleright y$, es decir $\Phi(k) \in G_{u \triangleright y}$, lo que nos dice que Φ está bien definida. Además, Φ es morfismo inyectivo de racks pues ϕ_i lo es. Finalmente, sea $k' \in G_{u \triangleright y}$; sabemos que existe $k \in X$ tal que $i \triangleright k = k'$ y aplicando f tenemos que

$$u \triangleright y = f(k') = f(i \triangleright k) = f(i) \triangleright f(k) = u \triangleright f(k).$$

Como Y es rack resulta que $f(k) = y$, o sea, $k \in G_y$. Por lo tanto, G_y y $G_{u \triangleright y}$ tienen la misma cardinalidad. De manera análoga, podemos ver que dicha afirmación también se cumple para las fibras G_y y $G_{u^{-1} \triangleright y}$.

(b). Si X es indescomponible entonces Y es indescomponible. Sean $u, y \in Y$. Luego, existen $u_1, \dots, u_n \in Y$ tales que

$$u = u_1^{\epsilon_1} \triangleright (u_2^{\epsilon_2} \triangleright (\dots (u_n^{\epsilon_n} \triangleright y) \dots)),$$

con $\epsilon_i \in \{\pm 1\}$. Por (a) tenemos que

$$G_y, G_{u_n^{\epsilon_n} \triangleright y)}, \dots, G_{u_1^{\epsilon_1} \triangleright (u_2^{\epsilon_2} \triangleright (\dots (u_n^{\epsilon_n} \triangleright y) \dots))} = G_u$$

tienen la misma cardinalidad, como queríamos mostrar. □

Observación 2.39. En el caso particular en que $Y = \mathrm{Inn}_{\triangleright}(X)$ y $f = \phi$, y si denotamos por F_y a una fibra de ϕ, entonces las fibras F_y y $F_{u \triangleright y}$ tienen la misma cardinalidad para todo $u, y \in \phi(X)$.

Corolario 2.40. *Sea X un rack finito indescomponible y $f : X \to Y$ un morfismo suryectivo de racks. Si denotamos por G_y a la fibra $f^{-1}(y)$ entonces*

$$\mathrm{card}(X) = \mathrm{card}(Y)\,\mathrm{card}(G_y),$$

para todo $y \in Y$.

Demostración. Dado que X es igual a la unión disjunta $\cup_{y \in Y} G_y$ tenemos que $\mathrm{card}(X) = \sum_{y \in Y} \mathrm{card}(G_y)$. Por Lema 2.38 la afirmación se satisface trivialmente. □

Definición 2.41. Sea $(X, \triangleright)$ un quandle. Se dice que X es *involutivo* si $\phi_x^2 = \mathrm{id}$ para todo $x \in X$.

Definición 2.42. Se dice que X es *abeliano* si

$$(x \triangleright w) \triangleright (y \triangleright z) = (x \triangleright y) \triangleright (w \triangleright z)$$

para todo $w, x, y, z \in X$.

3. Ejemplos.

3.1. Contraejemplos.

De rack que no es quandle.

Sea X un conjunto no vacío. Si $f \in \mathbb{S}_X$ con $f \neq \mathrm{id}$ entonces el rack de permutación asociado no es un quandle.

De quandle que no es conjunto cruzado.

Sea $X = \{a, b, c\}$ con

$$a \triangleright a = a,\ a \triangleright b = c,\ a \triangleright c = b$$

y $\phi_b, \phi_c = \mathrm{id}$. Es fácil ver que, $(X, \triangleright)$ es un quandle, pero no es un conjunto cruzado ya que $b \triangleright a = a$ y $a \triangleright b = c \neq b$.

3.2. Sumas amalgamadas.

Sea Z un rack. Describiremos todas las sumas amalgamadas $X = Y \cup Z$ para el rack trivial $Y = \{0, 1\}$. Denotamos $\mathrm{Aut}(Y) = \{+ = \mathrm{id}, -\}$. Sean $\sigma : Y \to \mathrm{Aut}_{\triangleright}(Z)$ y $\tau : Z \to \{+, -\}$ morfismos de racks como en el Lema 2.32. Podemos ver que Z se descompondría como una unión disjunta de subracks $Z = Z_+ \cup Z_-$, donde $\tau(Z_\pm) = \pm$. Ahora bien la condición (2.33)

$$y \triangleright \tau_z(u) = \tau_{\sigma_y(z)}(y \triangleright u),\ \forall y, u \in Y; z \in Z$$

es equivalente a que $Z_\pm$ permanezcan estables por σ_0 y σ_1. Para ver esto supongamos que se satisface tal condición, entonces

$$y \triangleright \tau_z(u) = \tau_z(u)$$

y

$$\tau_{\sigma_y(z)}(y \triangleright u) = \tau_{\sigma_y(z)}(u),$$

pues Y es un rack trivial. Ahora, (2.33) dice que $\tau_z = \tau_{\sigma_y(z)}$, para todo $y \in Y$, $z \in Z$. Sea $z \in Z_+$; como $\tau_z = + = \tau_{\sigma_y(z)}$ entonces $\sigma_y(z) \in Z_+$, para todo $y \in Y$. Esto implica que Z_+ permanece estable por σ_0 y σ_1. De la misma manera, se puede ver que Z_- es estable por σ_0 y σ_1. La recíproca es clara.

Por otro lado, la condición (2.34)

$$z \triangleright \sigma_y(w) = \sigma_{\tau_z(y)}(z \triangleright w),\ \forall y \in Y;\ z, w \in Z$$

es equivalente a

$$\phi_z\sigma_0 = \sigma_0\phi_z, \quad \phi_z\sigma_1 = \sigma_1\phi_z, \quad \forall z \in Z_+, \tag{3.1}$$

$$\phi_z\sigma_0 = \sigma_1\phi_z, \quad \phi_z\sigma_1 = \sigma_0\phi_z, \quad \forall z \in Z_-. \tag{3.2}$$

Supongamos que (2.34) se satisface y sea $z \in Z$. Si $z \in Z_+$ entonces $\phi_z\sigma_0(w) = \sigma_0\phi_z(w)$, para todo $w \in Z$,$y = 0, 1$ mientras que si $z \in Z_-$ e $y = 0$ entonces $\tau_z(0) = 1$ lo cual implica que $\phi_z\sigma_0(w) = \sigma_1\phi_z(w)$, para todo $w \in Z$ y si $y = 1$ se tiene que $\tau_z(1) = 0$ y $\phi_z\sigma_1(w) = \sigma_0\phi_z(w)$, para todo $w \in Z$, como queríamos probar. La recíproca es obvia.

Otra manera de describir la situación es considerar $Z = Z_+ \cup Z_-$ una unión disjunta. Tomemos $C_+ = \langle\{\phi_x/x \in Z_+\}\rangle$ el subgrupo generado por ϕ_{Z_+}, $C_- = \langle\{\phi_x\phi_y/x, y \in Z_-\}\rangle$ y sea $C = \langle C_+ \cup C_-\rangle$. Entonces

$$[\sigma_0, C] := \{[\sigma_0, \varphi] = \sigma_0\varphi\sigma_0^{-1}\varphi^{-1}/\varphi \in C\} = 1 \in \mathbb{S}_Z, \tag{3.3}$$

$$\sigma_1 = \phi_x\sigma_0\phi_x^{-1} \ \forall x \in Z_-. \tag{3.4}$$

Para ver esto, tomemos primero $x \in Z_+$. Luego, por (3.1) $\phi_x\sigma_0 = \sigma_0\phi_x$ lo cual implica que $[\sigma_0, \phi_x] = \sigma_0\phi_x\sigma_0^{-1}\phi_x^{-1} = 1$. Ahora, si $x, y \in Z_-$ entonces por (3.2)

$$[\sigma_0, \phi_x\phi_y] = \sigma_0\phi_x\phi_y\sigma_0^{-1}(\phi_x\phi_y)^{-1} = \phi_x\sigma_1\phi_y\sigma_0^{-1}\phi_y^{-1}\phi_x^{-1} = \phi_x\phi_y\sigma_0\sigma_0^{-1}\phi_y^{-1}\phi_x^{-1} = 1$$

como queríamos mostrar. Por otra parte, (3.4) es (3.2).

Proposición 3.5. *Sean Y, Z, X como antes.*

(a) Si Z es un quandle entonces X es un quandle.

(b) Si Z es un conjunto cruzado entonces X es un conjunto cruzado si y sólo si

$$Z_+ = Z^{\sigma_i} = \{z \in Z/\sigma_i(z) = z\}$$

con $i = 0, 1$.

Demostración. (a). Sea $x \in X$. Si $z \in Z$ entonces $x \triangleright x = x$ por hipótesis, mientras que si $x \in Y$ se tiene que $x \triangleright x = x$, trivialmente.

(b) Supongamos que X es un conjunto cruzado y sea $z \in Z_+$. Luego, $z \triangleright 0 = 0$ y $z \triangleright 1 = 1$ entonces $0 \triangleright z = z$ y $1 \triangleright z = z$ lo cual implica que $z \in Z^{\sigma_0}$ y $z \in Z^{\sigma_1}$. Ahora, tomemos $z \in Z^{\sigma_0}$ entonces $\sigma_0(z) = z$ lo que implica $z \triangleright 0 = 0$. Como $\tau_z \in \mathrm{Aut}_{\triangleright}(Y) \subseteq \mathbb{S}_Y$ resulta que $z \triangleright 1 = 1$, o sea $\tau_z = +$ y $z \in Z_+$. De manera análoga se ve que $Z^{\sigma_1} \subseteq Z_+$. Para ver la recíproca, consideremos $x, x' \in X$ con $x \triangleright x' = x'$ y verifiquemos por casos.

(1) Si x, x' están ambos en Y o en Z entonces $x' \triangleright x = x$ pues éstos son conjuntos cruzados.

(2) Si $x \in Y$ y $x' \in Z$ entonces $x \triangleright x' = \sigma_x(x') = x'$ lo que implica que $x' \in Z^{\sigma_x} = Z_+$, o sea $\tau_{x'} = +$, por lo que $x' \triangleright x = x$.

(3) Si $x \in Z$ y $x' \in Y$ entonces $x \triangleright x' = \tau_x(x') = x'$ lo que implica que $\tau_x = +$, es decir $x \in Z_+ = Z^{\sigma_0} = Z^{\sigma_1}$, o sea $\sigma_{x'}(x) = x$, con $x' = 0, 1$.

Luego, $x' \triangleright x = x$ como queríamos ver. □

3.3. Ejemplos geométricos.

Conjuntos cruzados poliedrales.

Sea $P \subset \mathbb{R}$ un poliedro regular con vértices $X = \{x_1, \ldots, x_n\}$ y centro 0. Para $1 \leq i \leq n$, sea T_i el mapa lineal ortogonal que fija a x_i y rota el plano ortogonal en un ángulo de $2\pi/r$ con la regla de la mano derecha (dirigiendo el pulgar hacia x_i), donde r es el número de aristas que salen de cada vértice. Definimos $\triangleright : X \times X \to X$ por

$$x_i \triangleright x_j := T_i(x_j).$$

Entonces $(X, \triangleright)$ es un conjunto cruzado. Para ver esto consideramos $\mathcal{G}$ el grupo de las transformaciones ortogonales con determinante 1 y notamos que $\{T_1, \ldots, T_n\}$ es una clase de conjugación de $\mathcal{G}$ cuyo conjunto subyacente es un conjunto cruzado estándar e isomorfo a X.

Es claro que a cada poliedro también le corresponde un conjunto cruzado análogo dado por las caras, que resulta isomorfo al conjunto cruzado dado por los vértices del poliedro dual.

Se puede ver,por computación directa, que el conjunto cruzado dado por los vértices del tetraedro, el octaedro, el dodecaedro y el icosaedro son indescomponibles.

Caso 1: Tetraedro.

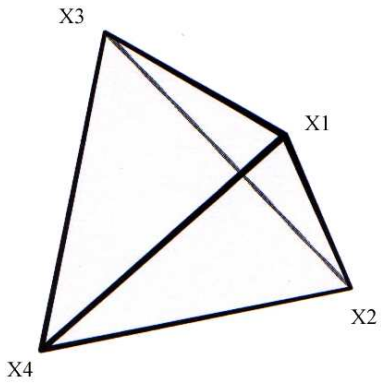


Figura 1: El tetraedro.

Vemos que $x_2 = \phi_3(x_1)$, $x_3 = \phi_4(x_1)$ y $x_4 = \phi_2(x_1)$. Luego, $\mathcal{O}_{x_1} = X_T$, lo que dice que $X_T = \{x_1, x_2, x_3, x_4\}$ es indescomponible.

Caso 2: Octaedro.

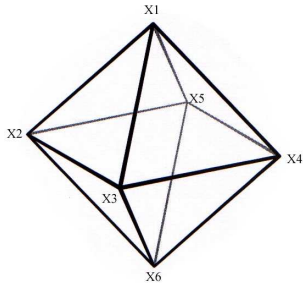


Figura 2: El octaedro.

De la figura vemos que $x_2 = \phi_3(x_1)$, $x_3 = \phi_4(x_1)$, $x_4 = \phi_5(x_1)$, $x_5 = \phi_2(x_1)$ y $x_6 = \phi_3\phi_3(x_1)$, con lo que $\mathcal{O}_{x_1} = X_O$ y resulta X_O indescomponible.

Caso 3: Icosaedro.

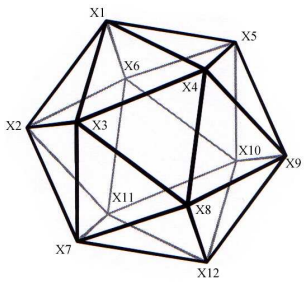


Figura 3: El icosaedro.

De acuerdo a la Figura 3 es fácil chequear que $x_2 = \phi_1\phi_2(x_1)$, $x_3 = \phi_2^4(x_1)$, $x_4 = \phi_5(x_1)$, $x_5 = \phi_1\phi_5(x_1)$, $x_6 = \phi_2(x_1)$, $x_7 = \phi_2^3(x_1)$, $x_8 = \phi_9\phi_5(x_1)$, $x_9 = \phi_5^2(x_1)$, $x_{10} = \phi_5^3(x_1)$, $x_{11} = \phi_2^2(x_1)$, $x_{12} = \phi_9^2\phi_5(x_1)$. Luego,$\mathcal{O}_{x_1} = X_I$ y entonces X_I es indescomponible.

Caso 4: Dodecaedro.

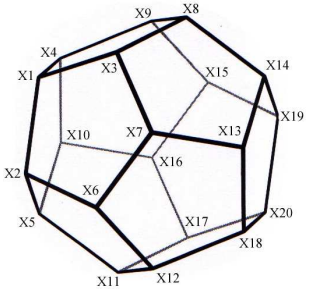


Figura 4: El dodecaedro.

De la figura, se puede chequear que $x_2 = \phi_5^2\phi_4^2(x_1)$, $x_3 = \phi_7^2\phi_2^2(x_1)$, $x_4 = \phi_{10}\phi_2(x_1)$, $x_5 = \phi_2(x_1)$, $x_6 = \phi_2^2(x_1)$, $x_7 = \phi_3(x_1)$, $x_8 = \phi_3^2(x_1)$, $x_9 = \phi_4(x_1)$, $x_{10} = \phi_4^2(x_1)$, $x_{11} = \phi_5\phi_4^2(x_1)$, $x_{12} = \phi_{11}^2\phi_2(x_1)$, $x_{13} = \phi_7\phi_2^2(x_1)$, $x_{14} = \phi_8\phi_7^2\phi_2^2(x_1)$, $x_{15} = \phi_9\phi_3^2(x_1)$, $x_{16} = \phi_{10}^2\phi_2^2(x_1)$, $x_{17} = \phi_{11}\phi_2(x_1)$, $x_{18} = \phi_{20}^2\phi_{11}\phi_2(x_1)$, $x_{19} = \phi_{20}\phi_{11}\phi_2(x_1)$, $x_{20} = \phi_{17}\phi_{10}^2\phi_2(x_1)$.

Entonces $\mathcal{O}_{x_1} = X_D$ como queríamos mostrar.

En el caso del cubo tenemos que si d es la *distancia de Hamming* [1] sobre el cubo entonces $d(x_j, T_i(x_j)) = 2$ si x_i no es ni x_j ni el vértice opuesto (por el centro del cubo) a x_j. Luego, $\mathcal{O}_{x_j} = \{x_k \in X_C \ / \ d(x_j, x_k) = 2 \text{ o } 0\ \}$, y $\text{card}(\mathcal{O}_{x_j}) = 4$.

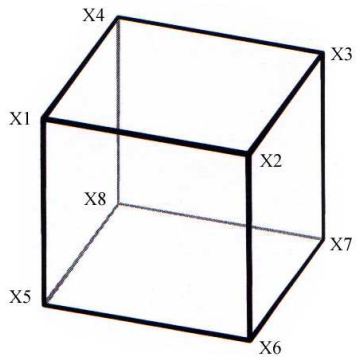


Figura 5: El cubo.

Luego, $X_C = X_1 \cup X_2$, con $X_1 = \{x_1, x_3, x_6, x_8\}$ y $X_2 = \{x_2, x_4, x_5, x_7\}$, es una descomposición. Es fácil ver que cada una de estas componentes es isomorfa al conjunto cruzado dado por los vértices del tetraedro.

Por otra parte, resulta claro que en los casos indescomponibles $\text{Inn}_{\triangleright}(X) \simeq \mathcal{G}$.

Racks de Coxeter.

Sea $(V, <>)$ un espacio vectorial sobre un cuerpo k, provisto de una forma bilineal simétrica no isotrópica, es decir si $v \in V$ y $v \neq 0$ entonces $< v, v > \neq 0$. Definimos para $u, v \in V - \{0\}$

$$v \triangleright u := u - \frac{2 < u, v >}{< v, v >} v.$$

Vemos que $v \triangleright u \in V - \{0\}$ pues si $v \triangleright u = 0$ entonces $< u, v >= 0$ y resulta que $u = 0$, contra lo supuesto.

[1] La *distancia de Hamming* es una función $d : X_C \times X_C \to \{0, 1, 2, 3\}$, dada por $d(x_i, x_j)$:=cantidad mínima de aristas necesarias para ir de x_ia x_j.

Afirmamos que $(V-\{0\}, \triangleright)$ es un rack. Para ver esto tomemos $v \in V-\{0\}$ y consideremos $\phi_v : V - \{0\} \to V - \{0\}$ dada por $\phi_v(u) = v \triangleright u$. Si $\phi_v(u) = \phi_v(u')$ entonces

$$u - \frac{2 < u, v >}{< v, v >} v = u' - \frac{2 < u', v >}{< v, v >} v$$

lo que implica que

$$(u - u') - \frac{2 < u - u', v >}{< v, v >} v = 0,$$

por lo tanto, $u - u' = 0$ y ϕ_v resulta inyectiva. Para ver que ϕ_v es suryectiva tomemos $w \in V - \{0\}$; sea $u = v \triangleright w = w - \frac{2<w,v>}{<v,v>} v$, luego

$$v \triangleright u = w - \frac{2 < w, v >}{< v, v >} v - 2\frac{< w, v > -2 < w, v >}{< v, v >} v = w - \frac{2 < w, v >}{< v, v >} v + \frac{2 < w, v >}{< v, v >} v = w.$$

Veamos que se satisface la condición (2.3). Sean $u, v, w \in V - \{0\}$; entonces

$$\begin{aligned} u \triangleright (v \triangleright w) &= w - \frac{2 < w, v >}{< v, v >} v - 2\frac{< w, u > - \frac{2<w,v>}{<v,v>} < v, u >}{< u, u >} u = \\ &= w - \frac{2 < w, v >}{< v, v >} v - \frac{2 < w, u >}{< u, u >} u + 4\frac{< w, v >< v, u >}{< v, v >< u, u >} u \end{aligned}$$

mientras que, por otro lado

$$(u \triangleright v) \triangleright (u \triangleright w) = w - \frac{2 < w, u >}{< u, u >} u - 2\frac{< u \triangleright w, u \triangleright v >}{< u \triangleright v, u \triangleright v >} (u \triangleright v).$$

Pero como $<, >$ es simétrico se tiene que

$$\begin{aligned} < u \triangleright v, u \triangleright v > &=< v - \frac{2 < v, u >}{< u, u >} u, v - \frac{2 < v, u >}{< u, u >} u > = \\ &=< v, v > -2\frac{< v, u >}{< u, u >} < v, u > -2\frac{< v, u >}{< u, u >} < u, v > +4\frac{< v, u >}{< u, u >} < v, u > = \\ &=< v, v > \end{aligned}$$

y además

$$\begin{aligned} < u \triangleright w, u \triangleright v > &=< w - \frac{2 < w, u >}{< u, u >} u, v - \frac{2 < v, u >}{< u, u >} u > = \\ &=< w, v > -2\frac{< v, u >}{< u, u >} < w, u > -2\frac{< w, u >}{< u, u >} < u, v > +4\frac{< w, u >}{< u, u >} < v, u > = \\ &=< w, v > . \end{aligned}$$

Por lo tanto

$$(u \triangleright v) \triangleright (u \triangleright w) = w - \frac{2 < w, u >}{< u, u >} u - \frac{2 < w, v >}{< v, v >} (v - \frac{2 < v, u >}{< u, u >} u)$$

como queríamos mostrar.

Para convertir esto en un quandle se puede tomar el cociente por la relación $v \sim -v$ ya que $v \triangleright v = -v$. También se puede tomar el quandle conjugado $(V - \{0\}, \triangleright^\iota)$ como en la subsección 1.1. Dado que ι satisface $u = u \triangleright \iota(u) = \iota(u \triangleright u) = \iota(-u)$ se tiene que

$$v \triangleright^\iota u = \iota(u) - \frac{2 < \iota(u), v >}{< v, v >} v = -u + \frac{2 < u, v >}{< v, v >} v.$$

Además, si $v \triangleright^\iota u = u$ entonces $u = \frac{<u,v>}{<v,v>} v$ por lo que

$$u \triangleright^\iota v = -v + \frac{2 < v, u >}{< u, u >} u = -v + 2\frac{< v, u >< u, u >}{< u, u >< v, v >} v = -v + 2v = v$$

con lo que $(V - \{0\}, \triangleright^\iota)$ es también un conjunto cruzado.

Ejemplo 3.6. Consideramos el sistema de raíces de un álgebra de Lie semisimple compleja con respecto a una subálgebra de Cartan $\mathfrak{h}$. Si $V = \mathfrak{h}_0^*$ y consideramos $\triangleright$ como antes se obtiene que $(V - \{0\}, \triangleright)$ es un rack donde la acción ϕ_α coincide con la acción de $w_\alpha \in W$, el grupo de Weyl.

3.4. Conjuntos cruzados afines.

Conjuntos cruzados homogéneos.

Sea G un grupo finito y sea $\Phi : \mathbb{S}_G \to \mathrm{Fun}(G, \mathbb{S}_G)$ una función dada por

$$\Phi_x^s(y) = s(yx^{-1})x, \qquad s \in \mathbb{S}_G, x, y \in G.$$

Entonces

$$\Phi_x^{st}(y) = s(t(yx^{-1}))x = s(t(yx^{-1})xx^{-1})x = \Phi_x^s(t(yx^{-1})x) = \Phi_x^s \Phi_x^t(y)$$

es decir que si consideramos a $\mathrm{Fun}(G, \mathbb{S}_G)$ como un grupo con la multiplicación punto a punto, Φ resulta un morfismo de grupo. Si además, $s : G \to G$ es un automorfismo de grupo se define

$$x \triangleright y := \Phi_x^s(y) = s(yx^{-1})x.$$

Vamos a mostrar que $(G, \triangleright)$ es un conjunto cruzado. Para ver esto, tomemos $x \in G$ y sea $\phi_x : G \to G$ dada por $\phi_x(y) := x \triangleright y = \Phi_x^s(y)$. Como $\Phi_x^s \in \mathbb{S}_G$ entonces ϕ_x es biyectiva. También podemos ver que si $x, y, z \in G$ se tiene que

$$\begin{aligned} x \triangleright (y \triangleright z) &= \Phi_x^s(\Phi_y^s(z)) = s(s(zy^{-1})yx^{-1})x = s^2(zy^{-1})s(yx^{-1})x = \\ &= s^2(zx^{-1})s^2(zy^{-1})s(yx^{-1})x = s(s(zx^{-1})x(s(yx^{-1})x)^{-1})s(yx^{-1})x = \\ &= \Phi_x^s(y) \triangleright \Phi_x^s(z) = (x \triangleright y) \triangleright (x \triangleright z), \end{aligned}$$

pues s es un automorfismo de G. Con esto vemos que $(G, \triangleright)$ es un rack. Por otra parte, $x \triangleright x = s(xx^{-1})x = x$ para todo $x \in G$ y si $x \triangleright y = y$ se tiene que $s(yx^{-1})x = y$, o sea $s(yx^{-1})x = y$ lo cual implica que $s(xy^{-1}) = xy^{-1}$, es decir $s(xy^{-1})y = x$ como queríamos mostrar. Luego, decimos que $(G, \triangleright)$ es un conjunto cruzado *homogéneo principal* y lo denotamos por (G, s).

Sea $t : G \to G$ dada por $t(x) = s(x^{-1})x$. Luego, $x \triangleright y = s(y)t(x)$ y es claro que $\phi_x = \phi_z$ si y sólo si $t(x) = t(z)$; por consiguiente las fibras de ϕ como conjunto cruzado son las mismas que las fibras de t. Notar que t es un homomorfismo de grupo si y sólo si $Im(t) \subset Z(G)$, el centro de G. Esto es cierto ya que

$$t(xy) = t(x)t(y) \iff s(y^{-1}x^{-1})xy = t(x)s(y^{-1})y \iff s(y^{-1})t(x) = t(x)s(y^{-1})$$

para todo $x, y \in G$, y como s es biyectiva se tiene que la última condición es equivalente a $t(x) \in Z(G)$.

Más generalmente, sea $H \subset G^s$ un subgrupo, donde G^s es el subgrupo de elementos de G fijos por S. Entonces $H\backslash G$ es un conjunto cruzado con

$$Hx \triangleright Hy := Hs(yx^{-1})x$$

llamado conjunto cruzado *homogéneo*. Además, se puede ver en [J1] que un conjunto cruzado es homogéneo si y sólo si es una órbita bajo la acción de $\mathrm{Aut}_{\triangleright}(X)$.

Conjuntos cruzados homogéneos torcidos.

Sea G un grupo como antes y sea $s \in \mathrm{Aut}(G)$. Si consideramos a G con $x \triangleright y = xs(yx^{-1})$ entonces $(G, \triangleright)$ es un conjunto cruzado que, en general, es distinto al anterior. A una órbita cualquiera de éste la llamamos un conjunto cruzado *homogéneo torcido*.

Conjuntos cruzados afines.

Sea A un grupo abeliano finito y sea $g : A \to A$ un automorfismo de grupo. Al conjunto cruzado homogéneo principal correspondiente lo llamamos conjunto cruzado *afín* y lo denotamos por (A, g). Luego,

$$x \triangleright y = x + g(y - x) = f(x) + g(y),$$

donde $f = \mathrm{id} - g$. Por otra parte, como $g = \mathrm{id} - f$ se tiene que $x \triangleright y = f(x - y) + y$ con lo cual se puede ver por inducción que

$$x_1 \triangleright (x_2 \triangleright (\dots (x_n \triangleright y) \dots)) \in y + f(A),$$

y mostrar de esta manera que $\mathcal{O}_y = y + \mathrm{Im}\, f$. De esta forma, tenemos que (A, g) es indescomponible si y sólo si es exacto puesto que si (A, g) es indescomponible entonces $x + \mathrm{Im}\, f = A$; luego $\mathrm{Im}\, f = A$ y como A es finito f resulta inyectiva, y si $\phi_x = \phi_y$ entonces

$z + f(x - z) = z + f(y - z)$ para todo $z \in A$ lo que implica que $f(x) = f(y)$, es decir $x = y$ y (A, g) resulta exacto. La recíproca es inmediata.

Veamos ahora cuándo dos conjuntos cruzados indescomponibles afines son isomorfos.

Lema 3.7. *Dos conjuntos cruzados indescomponibles afines (A, g) y (B, h) son isomorfos si y sólo si existe un isomorfismo de grupo $T : A \to B$ tal que $Tg = hT$. Si esto sucede, cualquier isomorfismo de conjunto cruzado $U : (A, g) \to (B, h)$ puede ser escrito de manera única como $U = \tau_b T$, donde $\tau_b : B \to B$ es la translación $\tau_b(x) = x + b$ y $T : A \to B$ es un isomorfismo de grupo.*

Demostración. Supongamos que existe un isomorfismo de conjuntos cruzados $U : (A, g) \to (B, h)$ y consideremos $\tau_b : B \to B$ dada por $\tau_b(x) = x + b$ la translación por b. Entonces, τ_b es isomorfismo de conjuntos cruzados ya que

$$\tau_b(x \triangleright x') = x + h(x' - x) + b = (x + b) \triangleright (x' + b) = \tau_b(x) \triangleright \tau_b(x').$$

Definimos ahora, $T := \tau_b^{-1} U$ con $b = U(0)$. Luego, T es un isomorfismo de conjuntos cruzados y $T(0) = 0$. Sean $f = \mathrm{id} - g$ y $k = \mathrm{id} - h$; entonces

$$T(f(x) + g(y)) = T(x \triangleright y) = T(x) \triangleright T(y) = k(T(x)) + h(T(y))$$

para todo $x, y \in A$. Tomando $x = 0$ vemos que $Tg = hT$ lo que implica que $Tf = kT$. Por lo tanto,

$$T(f(x) + g(y)) = T(f(x)) + T(g(y)).$$

Como (A, g) es indescomponible entonces f es biyectiva y T resulta morfismo de grupo. Para ver la recíproca tomamos $T : A \to B$ un isomorfismo lineal tal que $Tg = hT$. Luego,

$$T(x \triangleright y) = T(f(x) + g(y)) = T(f(x)) + T(g(y)) = k(T(x)) + h(T(y)) = T(x) \triangleright T(y)$$

y T es un isomorfismo de conjuntos cruzados. □

Corolario 3.8. *Si (A, g) es un conjunto cruzado indescomponible afín entonces $\mathrm{Aut}_{\triangleright}(A, g)$ es el producto semidirecto $A \rtimes \mathrm{Aut}(A)^g$ donde $\mathrm{Aut}(A)^g$ es el subgrupo de todos los automorfismo lineales de A tales que $Tg = gT$.*

Demostración. Definimos $\Phi : A \rtimes \mathrm{Aut}(A)^g \to \mathrm{Aut}_{\triangleright}(A, g)$ dada por

$$\Phi(a, T) := \tau_a T.$$

Así, Φ está bien definida y es biyectiva. Pues si $\tau_a T = \tau_{a'} T'$ entonces $\tau_{a'}^{-1} \tau_a = T' T^{-1}$ y evaluando en 0 tenemos que $-a' + a = 0$, o sea $a = a'$ y por lo tanto $T = T'$; luego, Φ es inyectiva. Para ver que Φ es suryectiva tomemos $U \in \mathrm{Aut}_{\triangleright}(A, g)$ entonces $U = \tau_b T$ como vimos en el Lema 3.7. Por otra parte, Φ es morfismo de grupo ya que

$$\begin{aligned}\Phi((a, T)(a', T'))(x) &= \Phi(a + T(a'), TT')(x) = \tau_{a+T(a')} TT'(x) = T(T'(x)) + a + T(a') = \\ &= \tau_a T \tau_{a'} T'(x) = \Phi(a, T)\Phi(a', T')(x)\end{aligned}$$

para todo $x \in A$. □

Observación 3.9. Si (A, g) no es indescomponible el Corolario puede no ser cierto. Por ejemplo, si $g = \mathrm{id}$ entonces $f = 0$ y (A, g) es trivial. Por lo tanto,

$$\mathrm{Aut}_{\triangleright}(A, g) = \mathbb{S}_A \not\simeq A \rtimes \mathrm{Aut}(A)^g.$$

Observación 3.10. El grupo $\mathrm{Inn}_{\triangleright}(A, g)$ es usualmente pequeño ya que $\mathrm{Inn}_{\triangleright}(A, g) \simeq \mathrm{Im}\, f \rtimes \langle g \rangle$.

Demostración. Solamente hay que mostrar que $\Phi(\mathrm{Im}\, f \rtimes \langle g \rangle) = \mathrm{Inn}_{\triangleright}(A, g)$, donde Φ es la del Lema anterior. Dado que

$$\phi_a = \tau_{f(a)} g = \Phi(f(a), g),$$

entonces $\mathrm{Inn}_{\triangleright}(A, g) \subset \Phi(\mathrm{Im}\, f \rtimes \langle g \rangle)$. Por otro lado, teniendo en cuenta que $\phi_0 = g$, se tiene que

$$\Phi(f(a), g^j)(b) = \tau_{f(a)} g^j(b) = \phi_a(g^{j-1}(b)) = \phi_a \phi_0^{j-1}(b),$$

para todo $j \in \mathbb{N}$ y $b \in A$. Esto implica que $\Phi(f(a), g^j) \in \mathrm{Inn}_{\triangleright}(A, g)$. □

En particular, $\mathrm{Inn}_{\triangleright}(A, g)$ es soluble ya que si $G = \mathrm{Im}\, f \rtimes \langle g \rangle$ y

$$G^{(1)} = \langle \{[x, y] = xyx^{-1}y^{-1} / x, y \in G\} \rangle.$$

Entonces $G^{(1)} \subset \mathrm{Im}\, f \rtimes \{\mathrm{id}\} = H$ y por lo tanto $G^{(2)} \subset H^{(1)} = \{\mathrm{id}\}$ pues A es abeliano.

Observación 3.11. Un conjunto cruzado estándar $\mathcal{O}$ donde $\mathcal{O}$ es una órbita no trivial de un grupo finito no abeliano simple G no puede ser afín ya que por Lema 2.19 $\mathrm{Inn}_{\triangleright}(\mathcal{O}) \simeq G$ y si $\mathcal{O}$ fuera afín, por lo visto anteriormente, se tiene que $G \simeq \mathrm{Im}\, f \rtimes \langle g \rangle$ que no es simple.

De la misma manera, discutimos si los conjuntos cruzados poliedrales son afines.

El conjunto cruzado de los vértices del tetraedro es afín e isomorfo a

$$(A = \mathbb{Z}_2 \times \mathbb{Z}_2, g = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}).$$

Por su parte, el conjunto cruzado dado por los vértices del cubo no es afín ya que los posibles grupos subyacentes serían: $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$ y $\mathbb{Z}_2^3$.

(i) $\mathbb{Z}_8$ no puede ser pues $\mathrm{Aut}(\mathbb{Z}_8) = \{\bar{1} = \mathrm{id}, \bar{3}, \bar{5}, \bar{7}\}$, donde $\bar{x}$ denota la clase de x en $\mathbb{Z}_8$. Luego, para cualquier elección de $g \in \mathrm{Aut}(\mathbb{Z}_8)$ y $a \in \mathbb{Z}_8$ se tiene que

$$\phi_a^2(b) = a - g^2(a) + g^2(b) = b,$$

para todo $b \in \mathbb{Z}_8$. Esto dice que $\phi_a^2 = \mathrm{id}$, para todo $a \in \mathbb{Z}_8$, mientras que las rotaciones T_i, en el cubo, satisfacen que $T_i^2 \neq \mathrm{id}$. Por lo tanto, no puede ocurrir este caso.

(ii) $\mathrm{Aut}_{\triangleright}(\mathbb{Z}_2 \times \mathbb{Z}_4)$ tiene orden 8 mientras que $\mathrm{Inn}_{\triangleright}(X)$ contiene elementos de orden 3,por lo que no puede darse este caso.

(iii) Mientras que $\mathbb{Z}_2^3$ puede ser excluido mirando los automorfismos $g \in \mathrm{Aut}(A)$ tales que $g^3 = \mathrm{id}$.

Para el caso del octaedro tenemos que $\mathrm{Inn}_{\triangleright}(X)$ es $\mathbb{S}_4$ mientras que para el icosaedro y el dodecaedro es $\mathbb{A}_5$. Por lo tanto, el conjunto cruzado dado por los vértices de ellos no es afín, por Corolario 3.8.

Ejemplo 3.12. Sea $A = \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ y sea $q \in \mathbb{Z}_n^\times = \{p \in \mathbb{Z}_n \ / \ (p,n) = 1\}$ tal que $(1-q) \in \mathbb{Z}_n^\times$. Entonces tenemos una estructura de rack sobre $\mathbb{Z}_n$ dada por

$$x \triangleright^q y = (1-q)x + qy.$$

Más aún, este rack, que es denotado por $(\mathbb{Z}_n, \triangleright^q)$ es un conjunto cruzado indescomponible porque es exacto y se puede ver que

$$(\mathbb{Z}_n, \triangleright^q) \simeq (\mathbb{Z}_n, \triangleright^{q'}) \iff q = q'.$$

Para ver esto suponemos que $(\mathbb{Z}_n, \triangleright^q) \simeq (\mathbb{Z}_n, \triangleright^{q'})$, luego por Lema 3.7 existe $T : \mathbb{Z}_n \to \mathbb{Z}_n$ isomorfismo lineal tal que

$$Tg_q = g_{q'}T = Tg_{q'} \iff T(g_q - g_{q'}) = 0 \iff g_q - g_{q'} = 0 \iff q = q'$$

ya que $\mathrm{Aut}(\mathbb{Z}_n)$ es abeliano.

Ejemplo 3.13. Se tiene que $(\mathbb{Z}_3, \triangleright^2)$ es el único conjunto cruzado indescomponible con tres elementos y que cualquier conjunto cruzado con tres elementos es o bien trivial o bien isomorfo a $(\mathbb{Z}_3, \triangleright^2)$. Para ver esto, sea $X = \{a, b, c\}$ un conjunto cruzado; luego $a \triangleright a = a$ y tenemos dos posibilidades para $a \triangleright b$

(i) si $a \triangleright b = b$ entonces $a \triangleright c = c$ pues ϕ_a es biyectiva. Como X es un conjunto cruzado resulta que $b \triangleright a = a$ y $c \triangleright a = a$. Por último, dado que ϕ_b es biyectiva se tiene que $b \triangleright c = c$. Por lo tanto, X es trivial.

(ii) si $a \triangleright b = c$ entonces $a \triangleright c = b$ y como no puede ocurrir que $b \triangleright a = a$ se tiene que $b \triangleright a = c$ y $b \triangleright c = a$. De manera similar se puede ver que $c \triangleright a = b$ y $c \triangleright b = a$. Por lo tanto, X es isomorfo a $(\mathbb{Z}_2, \triangleright^2)$ vía la identificación

$$a \longleftrightarrow 0, \ b \longleftrightarrow 1, \ c \longleftrightarrow 2.$$

En [EGS] está probado que cualquier rack indescomponible de orden primo p es o bien isomorfo a $(\mathbb{Z}_p, \triangleright^q)$ para algún $q \in \mathbb{Z}_p^\times$ o bien es isomorfo al rack de permutación $(\mathbb{Z}_p, \triangleright)$ con $x \triangleright y = y + 1$.

En [G] están clasificados los racks indescomponibles de orden p^2; en particular se prueba que cualquier quandle indescomponible de orden p^2 es afín.

Racks afines.

Éstos son una generalización de los conjuntos cruzados afines. Sean A un grupo abeliano, $g \in \mathrm{Aut}(A)$, $f \in \mathrm{End}(A)$ tales que $fg = gf$ y $f(\mathrm{id} - g - f) = 0$. Definimos, $x \triangleright y := f(x) + g(y)$ para todo $x, y \in A$. Luego, $(A, \triangleright)$ es un rack pues

(I) ϕ_x es biyectiva para todo $x \in A$

(i) $\phi_x(y) = \phi_x(y')$ si y sólo si $f(x) + g(y) = f(x) + g(y')$ si y sólo si $g(y) = g(y')$ si y sólo si $y = y'$, pues $g \in \mathrm{Aut}(A)$.

(ii) sea $z \in A$. Como g es biyectiva se tiene que existe $y \in A$ tal que $g(y) = z - f(x)$ lo que implica que ϕ_x es suryectiva.

(II) la propiedad (2.3) se cumple ya que

$$\begin{aligned} x \triangleright (y \triangleright z) &= f(x) + g(f(y)) + g^2(z) = f^2(x) + f(g(y)) + g(f(x)) + g^2(z) = \\ &= (f(x) + g(y)) \triangleright (f(x) + g(z)) = (x \triangleright y) \triangleright (x \triangleright z) \end{aligned}$$

pues $f - fg - f^2 = 0$ y por lo tanto $f(x) = f(g(x)) + f^2(x)$.

Es claro que A es un quandle si y sólo si $f = \mathrm{id} - g$ pues $a \triangleright a = a$ si y sólo si $f(a) + g(a) = a$ para todo $a \in A$ si y sólo si $f(a) = (id - g)(a)$ para todo $a \in A$. Se puede observar que como $f(\mathrm{id} - g - f) = 0$ entonces

$$0 = g^{-1} f(\mathrm{id} - g - f) = f(g^{-1} - \mathrm{id} - g^{-1} f)$$

y por lo tanto

$$(\mathrm{id} - f)(\mathrm{id} + g^{-1} f) = \mathrm{id} - f + g^{-1} f - f g^{-1} f = \mathrm{id}\,.$$

Luego, $\mathrm{id} - f$ es un automorfismo de A. De esta manera, se puede considerar el quandle afín $(A, \mathrm{id} - f)$. Es fácil ver que este quandle es el quandle asociado al rack. Para ver esto consideremos que

$$(A, g) = (A, \triangleright) \quad \text{y} \quad (A, \mathrm{id} - f) = (A, \triangleright')$$

Tenemos que ver que $(A, \triangleright') = (A, \triangleright^\iota)$ donde $\iota \in C_\triangleright(X)$ y cumple que $a \triangleright \iota(a) = a$, es decir $\iota(a) = \phi_a^{-1}(a) = g^{-1}(a) - g^{-1}(f(a))$ para todo $a \in A$. Luego,

$$x \triangleright' y = f(x) + y - f(y) = f(x) + g(\iota(y)) = x \triangleright^\iota y$$

como queríamos ver.

Ejemplo 3.14. Como caso particular de la construcción anterior, podemos tomar $A = \mathbb{Z}_{p^2}$, $g = \mathrm{id}$ y $f(x) = px$.

Uniones amalgamadas de conjuntos cruzados afines.

Sean (A, g) y (A, h) dos conjuntos cruzados indescomponibles afines y definamos $f = \mathrm{id} - g$, $k = \mathrm{id} - h$. Buscamos $\sigma : (A, g) \to \mathrm{Aut}_{\triangleright}(A, h)$, $\tau : (A, h) \to \mathrm{Aut}_{\triangleright}(A, g)$ morfismos de racks que sean de la forma

$$\begin{aligned} \sigma_x &= \alpha(x) + \beta, && \text{i.e. } \sigma_x(y) = \alpha(x) + \beta(y), \\ \tau_y &= \gamma + \delta(y), && \text{i.e. } \tau_y(x) = \gamma(x) + \delta(y), \end{aligned}$$

donde $\alpha, \delta \in \mathrm{End}(A)$ y $\beta, \gamma \in \mathrm{Aut}(A)$. Ahora bien

$$\sigma_x(y \triangleright y') = \alpha(x) + \beta(k(y)) + \beta(h(y'))$$

es igual a

$$\begin{aligned} \sigma_x(y) \triangleright \sigma_x(y') &= (\alpha(x) + \beta(y)) \triangleright (\alpha(x) + \beta(y')) = \\ &= k(\alpha(x)) + k(\beta(y)) + h(\alpha(x)) + h(\beta(y')), \end{aligned}$$

para todos $x, y, y' \in A$ si y sólo si $\beta h = h\beta$, y por lo tanto $\beta \in \mathrm{Aut}(A)^h$. De manera análoga, se ve que τ es un morfismo de rack si y sólo si $\gamma \in \mathrm{Aut}(A)^g$. Queremos construir una suma amalgamada usando σ y τ. Para ello debemos establecer bajo qué condiciones se satisfacen (2.33) y (2.34). La condición (2.33)

$$x \triangleright \tau_y(x') = \tau_{\sigma_x(y)}(x \triangleright x'),$$

para todo $x, x' \in (A, g)$, $y \in (A, h)$, es equivalente a

$$f(x) + g(\gamma(x')) + g(\delta(y)) = \gamma(f(x)) + \gamma(g(x')) + \delta(\alpha(x)) + \delta(\beta(y)),$$

para todo $x, x' \in (A, g)$, $y \in (A, h)$. Tomando $x' = y = 0$ se tiene que $f - f\gamma - \delta\alpha = 0$ mientras que si tomamos $x = x' = 0$ resulta que $\delta\beta - g\delta = 0$. Por otra parte, la condición (2.34)

$$y \triangleright \sigma_x(y') = \sigma_{\tau_y(x)}(y \triangleright y'),$$

para todo $x \in (A, g)$, $y, y' \in (A, h)$, es equivalente a

$$k(y) + h(\alpha(x)) + h(\beta(y')) = \alpha(\gamma(x)) + \alpha(\delta(y)) + \beta(k(y)) + \beta(h(y'))$$

para todo $x \in (A, g)$, $y, y' \in (A, h)$. Tomando $y' = x = 0$ tenemos que $k - k\beta - \alpha\delta = 0$ y si tomamos $y = y' = 0$ obtenemos $\alpha\gamma - h\alpha = 0$. De la misma manera podemos obtener una condición equivalente a la (2.35). En conclusión

$$\begin{aligned} &(2.33) && \text{es equivalente a} && f - f\gamma - \delta\alpha = 0, \quad \delta\beta - g\delta = 0, && (3.15) \\ &(2.34) && \text{es equivalente a} && k - k\beta - \alpha\delta = 0, \quad \alpha\gamma - h\alpha = 0, && (3.16) \\ &(2.35) && \text{es equivalente a} && \alpha(x) + \beta(y) = y \iff \gamma(x) + \delta(y) = x. && (3.17) \end{aligned}$$

Si (3.15), (3.16) y (3.17) se satisfacen entonces la unión disjunta $X = (A, g) \sqcup (A, h)$ adquiere una estructura de conjunto cruzado descomponible.

Ejemplo 3.18. Supongamos que f es inversible y consideramos $h = -gf^{-1} = \mathrm{id} - f^{-1}$ y definimos σ y τ tomando $\alpha = \mathrm{id}$, $\beta = g$, $\gamma = h$, $\delta = \mathrm{id}$. Entonces es fácil ver que σ y τ son morfismos de rack y satisfacen (3.15), (3.16) y (3.17).

Ejemplo 3.19. Sea $A = \mathbb{Z}_p$ y sea $q \in \mathbb{Z}_p^\times$ tal que $(1-q) \in \mathbb{Z}_p^\times$. Consideremos $g \in \mathrm{Aut}(A)$ dada por la multiplicación por q. Luego, $f = \mathrm{id} - g$ es inversible. Si $h = -gf^{-1} = \mathrm{id} - f^{-1}$ entonces los conjuntos cruzados afines (A, g) y (A, h) son isomorfos si y sólo si $(1-q)^2 = 1$.

Demostración. Por Ejemplo 3.12 tenemos que (A, g) y (A, h) son indescomponibles. Ahora bien, por Lema 3.7 (A, g), (A, h) son isomorfos si y sólo si existe un isomorfismo de grupos $T : A \to B$ tal que $Tg = hT$; y esto ocurre si y sólo si

$$Tg = -gf^{-1}T \iff T - Tf = T - f^{-1}T \iff Tf = f^{-1}T,$$

y esta última condición es equivalente a $(1-q)^2 = 1$. □

Lema 3.20. *Si (A, g) es un conjunto cruzado afín entonces sus órbitas son isomorfas como conjuntos cruzados.*

Demostración. Sabemos que $\mathcal{O}_x = x + \mathrm{Im}(f)$ para cualquier $x \in A$. Sea entonces

$$\{x_0 = 0, x_1, \dots, x_n\}$$

un conjunto completo de representantes de las coclases en $A/\mathrm{Im}(f)$. Si definimos $\varphi_i : x_i + \mathrm{Im}(f) \to \mathrm{Im}(f)$ dada por $\varphi_i(y) = y - x_i$ tenemos que φ_i es un isomorfismo de conjuntos cruzados pues φ_i es claramente biyectiva y como ocurre que

$$\varphi_i(y \triangleright y') = \varphi_i(f(y) + g(y')) = f(y) + g(y') - x_i = f(y) + g(y') - f(x_i) - g(x_i) =$$

$$= f(y - x_i) + g(y' - x_i) = (y - x_i) \triangleright (y' - x_i) = \varphi_i(y) \triangleright \varphi_i(y')$$

entonces φ_i resulta un morfismo de rack. □

Como una consecuencia de esto podemos decir que si (A, g) y (B, h) son dos conjuntos cruzados indescomponibles afines no isomorfos entonces cualquier suma amalgamada $X = A \sqcup B$ no es afín. Esto es cierto ya que las únicas órbitas en X son A y B; pues si $x \in X$, digamos $x \in A$, entonces

$$\mathcal{O}_x = \{\phi_{x_1} \dots \phi_{x_n}(x) \ / \ x_1, \dots, x_n \in X\} \supseteq \{\phi_{x_1} \dots \phi_{x_n}(x) \ / \ x_1, \dots, x_n \in X\} = A,$$

y como $\mathcal{O}_x \subseteq A$ se tiene que $\mathcal{O}_x = A$.

3.5. Conjuntos cruzados involutivos.

Sea S un conjunto con una colección de funciones $\{\gamma_i\}_{i\in I}$, donde I es un conjunto cualquiera de índices, tal que $\gamma_i : \mathbb{Z} \to S$ y para todo $x, y \in S$ existe $i \in I$ tal que $x, y \in \mathrm{Im}(\gamma_i)$. A las γ_i las llamaremos *geodésicas*.

Consideremos $g : \mathbb{Z} \to \mathbb{Z}$ dada por $g(n) = -n$. Si definimos

$$n \triangleright m := (\mathrm{id} - g)(n) + g(m) = 2n - m,$$

entonces $(\mathbb{Z}, \triangleright)$ es un conjunto cruzado afín que denotamos por $(\mathbb{Z}, -1)$.

Supongamos que S satisface que dados $x, y \in S$ que pertenecen a dos geodésicas γ y γ', o sea $x = \gamma(n) = \gamma'(n')$, $y = \gamma(m) = \gamma'(m')$, con $n, n', m, m' \in \mathbb{Z}$, entonces $\gamma(n \triangleright m) = \gamma'(n' \triangleright m')$. Podemos definir sobre S una única operación binaria $\triangleright$ de forma tal que las geodésicas respeten a $\triangleright$, y de la siguiente manera

$$x \triangleright y := \gamma(n \triangleright m) = \gamma(2n - m),$$

para cualquier geodésica γ tal que $\gamma(n) = x$ y $\gamma(m) = y$. Notemos que $\triangleright$ está bien definida por la suposición anterior.

Afirmamos que $(S, \triangleright)$ es un quandle involutivo si $x \triangleright \gamma$ es una geodésica para todo $x \in S$ y para toda γ geodésica, ya que

(i) Sea $\phi_x : S \to S$ dada por $\phi_x(y) = x \triangleright y$. Notemos que si $x = \gamma(n)$, $y = \gamma(m)$ entonces

$$x \triangleright (x \triangleright y) = \gamma(n) \triangleright (\gamma(n \triangleright m)) = \gamma(n \triangleright (n \triangleright m)) = \gamma(2n - (2n - m)) = \gamma(m) = y.$$

Luego, $\phi_x^2 = \mathrm{id}$ y por lo tanto ϕ_x es biyectiva.

(ii) Sean $x, y, z \in S$ y supongamos que $y = \gamma(n)$, $z = \gamma(m)$. Entonces

$$x \triangleright (y \triangleright z) = x \triangleright \gamma(n \triangleright m) = (x \triangleright \gamma(n)) \triangleright (x \triangleright \gamma(m)) = (x \triangleright y) \triangleright (x \triangleright z),$$

pues $x \triangleright \gamma$ es una geodésica.

(iii) Sea $x \in S$ y γ una geodésica que pasa por x, digamos $x = \gamma(n)$. Luego, $x \triangleright x = \gamma(n \triangleright n) = \gamma(n) = x$.

Por lo visto en (i) se tiene que $(S, \triangleright)$ es involutivo. Más aún, se puede ver en [J1] que cualquier quandle involutivo se origina de esta manera.

Corazón de un grupo.

Sea G un grupo. Si definimos $x \triangleright y := xy^{-1}x$ entonces $(G, \triangleright)$ es un conjunto cruzado involutivo pues

(i) sea $x \in G$. Luego, $\phi_x^2(y) = \phi_x(xy^{-1}x) = xx^{-1}yx^{-1}x = y$ por lo que ϕ_x resulta biyectiva.

(ii) se cumple (2.3) ya que

$$x \triangleright (y \triangleright z) = xy^{-1}zy^{-1}x = xy^{-1}xx^{-1}zx^{-1}xy^{-1}x = (x \triangleright y) \triangleright (x \triangleright z).$$

(iii) $x \triangleright x = xx^{-1}x$.

(iv) si $x \triangleright y = y$ entonces $xy^{-1}x = y$. Luego, $x = yx^{-1}y = y \triangleright x$.

A $(G, \triangleright)$ lo llamamos el *corazón* de G. Si G es abeliano entonces $(G, \triangleright)$ es el conjunto cruzado afín dado por $g = -\operatorname{id}$. Como un ejemplo particular veremos el corazón de un loop de Moufang.

Loops de Moufang.

Definición 3.21. Un *loop* es un par $(L, \cdot)$ donde L es un conjunto no vacío con una operación binaria $\cdot$ sobre L tal que

(i) dados $a, b \in L$ las ecuaciones

$$a \cdot x = b, \quad y \cdot a = b \tag{3.22}$$

tienen soluciones únicas en L.

(ii) existe un elemento identidad $1 \in L$ que satisface

$$1 \cdot x = x \cdot 1 = x, \quad \forall x \in L. \tag{3.23}$$

Definición 3.24. Un *loop de Moufang* es un loop que satisface

$$x \cdot (y \cdot (x \cdot z)) = ((x \cdot y) \cdot x) \cdot z. \tag{3.25}$$

Notaremos xy por $x \cdot y$.

Proposición 3.26. *Sea $(L, \cdot)$ un loop de Moufang. Entonces:*

(i) si $x \in L$ existe un único elemento x^{-1} en L tal que

$$xx^{-1} = x^{-1}x = 1.$$

(ii) $x(yx) = (xy)x$ para todo $x, y \in L$.

Demostración. (i) Sea $x \in L$ y sean $x', x'' \in L$ las soluciones a las ecuaciones $xa = 1$ y $bx = 1$, respectivamente. Luego, $xx' = 1$ y $x''x = 1$. Ahora bien, sea $w \in L$ tal que $x' = x''w$. Luego,

$$x'' = x''1 = x''(xx') = x''(x(x''w)) = ((x''x)x'')w = (1x'')w = x''w,$$

por lo que $w = 1$ y $x' = x''$.

(ii) Se obtiene de (3.25) tomando $z = 1$. □

Proposición 3.27. *Si $(L,\cdot)$ es un loop de Moufang entonces*

(i) $(L,\cdot)$ tiene la propiedad de inverso a izquierda, o sea

$$x^{-1}(xy) = y, \quad \forall x, y \in L. \tag{3.28}$$

(ii) $(L,\cdot)$ tiene la propiedad de inverso a derecha

$$(xy)y^{-1} = x, \quad \forall x, y \in L. \tag{3.29}$$

Demostración. (i)Como

$$x(x^{-1}(xy)) = ((xx^{-1})x)y = xy,$$

entonces, por (3.22), se tiene que $x^{-1}(xy) = y$.

(ii) Sabemos que $xy = (y(y^{-1}x))y = y(y^{-1}x)y)$ y que $xy = y(y^{-1}(xy))$. Luego, por (3.22) se tiene que $(y^{-1}x)y = y^{-1}(xy)$. Ahora

$$y^{-1}(xy) = y^{-1}((xy)(y^{-1}y)) = (y^{-1}(xy)y^{-1})y,$$

y por (3.23) resulta que $y^{-1}(xy)y^{-1} = y^{-1}x$. Por lo tanto, $(xy)y^{-1} = x$ por (3.22). □

Proposición 3.30. *Si $(L,\cdot)$ es un loop de Moufang entonces $(xy)^{-1} = y^{-1}x^{-1}$ para todo $x, y \in L$.*

Demostración. Sea $z = xy$. Luego, $x^{-1}z = y$ e $yz^{-1} = x^{-1}$. Por lo tanto, $y^{-1}x^{-1} = z^{-1} = (xy)^{-1}$. □

Definición 3.31. Sea $(L,\cdot)$ un loop de Moufang. Se define $Cor(L) := (L, \triangleright)$, el corazón de L, donde $\triangleright : L \times L \to L$ está dada por

$$x \triangleright y := xy^{-1}x.$$

Proposición 3.32. *Si $(L,\cdot)$ es un loop de Moufang entonces $Cor(L)$ es un conjunto cruzado involutivo.*

Demostración. Para $x \in L$, sea $\phi_x : L \to L$ dada por $\phi_x(y) = x \triangleright y$.

(i) Sea $x \in L$. Luego,

$$x \triangleright (x \triangleright y) = x(xy^{-1}x)^{-1}x = x(x^{-1}yx^{-1})x = (x(x^{-1}(yx^{-1})))x = yx^{-1} = y,$$

para todo $y \in L$, o sea $\phi_x^2 = \mathrm{id}$ y por lo tanto ϕ_x es biyectiva para todo $x \in L$.

(ii) Veamos que $x \triangleright (y \triangleright z) = (x \triangleright y) \triangleright (x \triangleright z)$ para todo $x, y, z \in L$.

$$\begin{aligned}(x \triangleright y) \triangleright (x \triangleright z) &= (xy^{-1}x)(xz^{-1}x)^{-1}(xy^{-1}x) = (xy^{-1}x)(x^{-1}zx^{-1})(xy^{-1}x) = \\ &= (xy^{-1}x)(((x^{-1}z)x^{-1})(xy^{-1}x)) = (xy^{-1}x)(x^{-1}(z(x^{-1}(xy^{-1}x)))) = \\ &= (xy^{-1}x)(x^{-1}(z(y^{-1}x))) = x(y^{-1}(x(x^{-1}(z(y^{-1}x))))) = \\ &= x(y^{-1}(z(y^{-1}x))) = x(((y^{-1}z)y^{-1})x) = x((y^{-1}z)y^{-1})x = \\ &= x(y^{-1}zy^{-1})x = x(y^{-1}zy^{-1}x = x \triangleright (yz^{-1}y) = x \triangleright (y \triangleright z).\end{aligned}$$

(iii) Sea $x \in L$. Luego, $x \triangleright x = xx^{-1}x = x$.

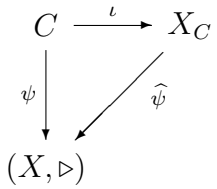
(iv) Sea $x, y \in L$ y supongamos que $x \triangleright y = y$, es decir $xy^{-1}x = y$. Por (3.29) $xy^{-1} = yx^{-1}$, y nuevamente por (3.29) $x = yx^{-1}y = y \triangleright x$.

Por lo tanto, $Cor(L)$ es un conjunto cruzado involutivo. □

3.6. El quandle libre de un conjunto.

Sea C un conjunto cualquiera y sea $F(C)$ el grupo libre generado por C. Para $c \in C$ denotamos por $\mathcal{O}_c$ a la órbita de c en $F(C)$, o sea $\mathcal{O}_c = \{ucu^{-1} \ / \ u \in F(C)\}$. Definimos $X_C := \bigcup_{c \in C} \mathcal{O}_c$. Luego, X_C es un conjunto cruzado ya que cada $\mathcal{O}_c$ es estable por conjugación en $F(C)$ y X_C resulta estándar.

Afirmamos que X_C es el quandle libre sobre el conjunto C, es decir si $(X, \triangleright)$ es un quandle y $\psi : C \to (X, \triangleright)$ es una función cualquiera entonces existe un único $\widehat{\psi} : X_C \to X$ morfismo de rack tal que el siguiente diagrama es conmutativo



es decir $\widehat{\psi}\iota = \psi$, con ι la inclusión de C en el grupo libre $F(C)$.

Sea $(X, \triangleright)$ un quandle y sea $\psi : C \to (X, \triangleright)$ una función cualquiera. Definimos $\widetilde{\psi} : C \to \mathrm{Inn}_{\triangleright}(X)$ dada por $\widetilde{\psi}(c) := \phi_{\psi(c)}$. Como $F(C)$ es un objeto libre sobre C en la categoría de grupos entonces existe un único morfismo de grupo $\Phi : F(C) \to \mathrm{Inn}_{\triangleright}(X)$ tal que $\Phi\iota = \widetilde{\psi}$. Ahora definimos $\widehat{\psi} : X_C \to X$ dada por

$$\widehat{\psi}(y) = \Phi(u)(\psi(c)),$$

donde $y = ycu^{-1}$, con $c \in C$ y $u \in F(C)$. Veamos que $\widehat{\psi}$ está bien definida. Para ver esto usaremos los siguientes resultados que probaremos más adelante

(a) si $c, d \in C$ y $\mathcal{O}_c = \mathcal{O}_d$ entonces $c = d$.

(b) sea $c \in C$, el centralizador de c en $F(C)$ es $\langle c \rangle$.

Sea $y \in X_C$ y supongamos que $y = ucu^{-1} = vdv^{-1}$, con $c, d \in C$ y $u, v \in F(C)$. Luego, $c = u^{-1}vdv^{-1}u$ por lo que $\mathcal{O}_c \subset \mathcal{O}_d$ y como $d = v^{-1}ucu^{-1}v$ se tiene que $\mathcal{O}_d \subset \mathcal{O}_c$. Así, $\mathcal{O}_c = \mathcal{O}_d$. Por (a) tenemos que $c = d$. Además, $cv^{-1}u = v^{-1}uc$, es decir $v^{-1}u \in Z_{F(C)}(c) = \langle c \rangle$ por lo que

$$u = c_1 \dots c_k c^n \quad \text{y} \quad v = c_1 \dots c_k c^m,$$

con $c_1, \dots, c_k \in C$ y $n, m \in \mathbb{N} \cup \{0\}$. Luego,

$$\begin{aligned}
\Phi(u)(\psi(c)) &= \psi(c_1) \triangleright (\psi(c_2) \triangleright (\dots (\psi(c_n)(\triangleright(\psi(c)^n \triangleright \psi(c))) \dots)) = \\
&= \psi(c_1) \triangleright (\psi(c_2) \triangleright (\dots (\psi(c_n) \triangleright \psi(c)) \dots)) = \\
&= \psi(c_1) \triangleright (\psi(c_2) \triangleright (\dots (\psi(c_n)(\triangleright(\psi(c)^m \triangleright \psi(c))) \dots)) = \\
&= \Phi(v)(\psi(c)),
\end{aligned}$$

pues $(X, \triangleright)$ es un quandle. De esta manera, hemos visto que $\widehat{\psi}$ está bien definida.

Probemos (a). Como $\mathcal{O}_c = \mathcal{O}_d$ se tiene que $d = ucu^{-1}$ para algún $u \in F(C)$. Entonces, $u = c_1^{\epsilon_1} \dots c_n^{\epsilon_n}$, con $c_i \in C$, $\epsilon_i \in \{1, -1\}$ y $c_i^{\epsilon_i} c_{i+1}^{\epsilon_{i+1}} \neq 1$ para todo i. Luego

$$d = c_1^{\epsilon_1} \dots c_n^{\epsilon_n} c c_n^{-\epsilon_n} \dots c_1^{-\epsilon_1}.$$

Por lo tanto, $c_n^{\epsilon_n} c c_n^{-\epsilon_n} = c$ ya que, o bien $c_n^{\epsilon_n} = c^{-1}$ o bien $c_n^{-\epsilon_n} = c^{-1}$ pues la manera de escribir a d en $F(C)$ es única y de no ser así el miembro de la derecha no sería un elemento en C. Siguiendo de esta manera se tiene que $u = c^n$ o $u = c^{-n}$; entonces $d = c$.

Probemos (b). Sea $c \in C$ y $u \in Z_{F(C)}(c)$. Luego, $c = ucu^{-1}$. Por lo visto anteriormente $u = c^n$ o $u = c^{-n}$. Luego $u \in \langle c \rangle$.

A continuación mostraremos que

(i) $\widehat{\psi} : X_C \to X$ es un morfismo de quandles.

(ii) $\widehat{\psi} : X_C \to X$ extiende a ψ, es decir $\widehat{\psi}\iota = \psi$.

(iii) $\widehat{\psi}$ es única satisfaciendo (i) y (ii).

Demostración. (i) Sean $x, y \in X_C$, digamos $x = ucu^{-1}$, $y = vdv^{-1}$, con $c, d \in C$ y $u = c_1^{\epsilon_1} \dots c_n^{\epsilon_n}, v \in F(C)$. Entonces

$$\begin{aligned}
\widehat{\psi}(x \triangleright y) &= \widehat{\psi}((ucu^{-1}v)d(ucu^{-1}v)^{-1}) = \Phi(ucu^{-1}v)(\psi(d)) = \Phi(ucu^{-1})(\Phi(v)(d)) = \\
&= \phi_{\psi(c_1)} \dots \phi_{\psi(c_n)} \phi_{\psi(c)} \phi_{\psi(c_n)}^{-1} \dots \phi_{\psi(c_1)}^{-1}(\Phi(v)(\psi(d))) = \\
&= \phi_{\psi(c_1)} \dots \phi_{\psi(c_n)}(\psi(c)) \triangleright \Phi(v)(\psi(d)) = \Phi(u)(\psi(c)) \triangleright \Phi(v)(\psi(d)) = \widehat{\psi}(x) \triangleright \widehat{\psi}(y).
\end{aligned}$$

(ii) Sea $c \in C$. Luego

$$(\widehat{\psi}\iota)(c) = \widehat{\psi}(c) = \Phi(1)(\psi(c)) = \psi(c),$$

ya que $\Phi(1) = \mathrm{id}$ por ser Φ un morfismo de grupos.

(iii) Supongamos que existe $\bar{\psi} : X_C \to X$ tal que $\bar{\psi}$ es morfismo de quandles y que $\bar{\psi}\iota = \psi$. Veamos que $\bar{\psi}(x) = \widehat{\psi}(x)$ para todo $x \in X_C$. Sea $x \in X_C$. Luego, existe $c \in C$ y $u \in F(C)$ tales que $x = ucu^{-1}$. Si $u = 1$ entonces $x = c$ y tenemos que $(\bar{\psi}\iota)(c) = \bar{\psi}(c) = \psi(c) = \widehat{\psi}(c)$; mientras que si $u = c_1^{\epsilon_1} \dots c_n^{\epsilon_n}$, con $c_i \in C$ y $\epsilon_i \in \{1, -1\}$, para todo i se tiene que

$$\begin{aligned}
\bar{\psi}(x) &= \bar{\psi}(ucu^{-1}) = \bar{\psi}(c_1^{\epsilon_1} \triangleright (c_2^{\epsilon_2} \triangleright (\dots (c_n^{\epsilon_n} \triangleright c) \dots))) = \\
&= \bar{\psi}(c_1^{\epsilon_1}) \triangleright (\bar{\psi}(c_2^{\epsilon_2}) \triangleright (\dots (\bar{\psi}(c_n^{\epsilon_n}) \triangleright \bar{\psi}(c)) \dots)) = \\
&= (\bar{\psi}(c_1))^{\epsilon_1} \triangleright ((\bar{\psi}(c_2))^{\epsilon_2} \triangleright (\dots ((\bar{\psi}(c_n))^{\epsilon_n} \triangleright \bar{\psi}(c)) \dots)) = \\
&= (\widehat{\psi}(c_1))^{\epsilon_1} \triangleright ((\widehat{\psi}(c_2))^{\epsilon_2} \triangleright (\dots ((\widehat{\psi}(c_n))^{\epsilon_n} \triangleright \widehat{\psi}(c)) \dots)) = \\
&= \widehat{\psi}(c_1^{\epsilon_1}) \triangleright (\widehat{\psi}(c_2^{\epsilon_2}) \triangleright (\dots (\widehat{\psi}(c_n^{\epsilon_n}) \triangleright \widehat{\psi}(c)) \dots)) = \widehat{\psi}(c_1^{\epsilon_1} \triangleright (c_2^{\epsilon_2} \triangleright (\dots (c_n^{\epsilon_n} \triangleright c) \dots))) = \\
&= \widehat{\psi}(ucu^{-1}) = \widehat{\psi}(x).
\end{aligned}$$

Con esto se finaliza la prueba. □

Observación 3.33. X_C no es un rack libre pues puede fallar la buena definición de la $\widehat{\psi}$.

4. Extensiones.

En esta sección mostraremos cómo se relacionan los racks finitos con los conjuntos cruzados indescomponibles exactos.

Lema 4.1. *Sea X un rack y S un conjunto no vacío. Sea $\alpha : X \times X \to \mathrm{Fun}(S \times S, S)$ una función tal que para cada $i, j \in X$ y $s, t \in S$ se tiene un elemento $\alpha_{i,j}(s,t) \in S$. Escribimos $\alpha_{i,j}(s) : S \to S$ como la función $\alpha_{i,j}(s)(t) = \alpha_{i,j}(s,t)$. Entonces*

(I) $X \times S$ es un rack con la operación

$$(i,s) \triangleright (j,t) := (i \triangleright j, \alpha_{i,j}(s,t))$$

si y sólo si se satisfacen las siguientes condiciones

$$\alpha_{i,j}(s) \text{ es una biyección;} \tag{4.2}$$

$$\alpha_{i,j\triangleright k}(s, \alpha_{j,k}(t,u)) = \alpha_{i\triangleright j, i\triangleright k}(\alpha_{i,j}(s,t), \alpha_{i,k}(s,u)), \quad \text{para todo } i,j,k \in X;\ s,t,u \in S. \tag{4.3}$$

En otras palabras, $\alpha_{i,j\triangleright k}(s)\alpha_{j,k}(t) = \alpha_{i\triangleright j, i\triangleright k}(\alpha_{i,j}(s,t))\alpha_{i,k}(s)$.

(II) Si X es un quandle, entonces $X \times S$ es un quandle si y sólo si se satisfacen (4.2), (4.3) *y*

$$\alpha_{i,i}(s,s) = s, \tag{4.4}$$

para todo $i \in X$, $s \in S$.

(III) Si X es un conjunto cruzado, entonces $X \times S$ es un conjunto cruzado si y sólo si se satisfacen (4.2), (4.3), (4.4) *y*

$$\alpha_{j,i}(t,s) = s \quad \text{siempre que } i \triangleright j = j \text{ y } \alpha_{i,j}(s,t) = t, \tag{4.5}$$

para todo $i, j \in X$, $s, t \in S$

Demostración. Se obtiene directamente de las definiciones básicas. □

Definición 4.6. Si se satisfacen estas condiciones decimos que α es un *cociclo dinámico* y que $X \times S$ es una *extensión* de X por S, y lo denotamos por $X \times_\alpha S$.

Sea X un quandle y supongamos que la extensión de X por S, $X \times_\alpha S$, es también un quandle. Para $i \in X$ definimos

$$s \triangleright_i t := \alpha_{i,i}(s,t).$$

Es fácil ver que $(S, \triangleright_i)$ es un quandle para todo $i \in X$. Entonces, cuando $j = k$ la condición (4.3) dice que

$$\alpha_{i,j}(s, t \triangleright_j u) = \alpha_{i,j}(s,t) \triangleright_{i\triangleright j} \alpha_{i,j}(s,u), \tag{4.7}$$

para todo $s, t, u \in S$, es decir, el mapa $\alpha_{i,j}(s) : (S, \triangleright_j) \to (S, \triangleright_{i\triangleright j})$ es un morfismo de quandles.

Por otro lado, la proyección $X \times_\alpha S \to X$ es claramente un morfismo.

Lema 4.8. *Sea $(X, \triangleright)$ un quandle el cual es una unión disjunta $X = \sqcup_{i\in Y} X_i$, tal que existe $\bar{\triangleright} : Y \times Y \to Y$ que satisface $X_i \triangleright X_j = X_{i\bar{\triangleright}j}$, para todo $i, j \in Y$. Supongamos que $\mathrm{card}(X_i) = \mathrm{card}(X_j)$, para todo $i, j \in Y$ (esto sucede, por ejemplo, si X es indescomponible). Entonces $(Y, \bar{\triangleright})$ es un quandle.*

Más aún, sea S un conjunto tal que $\mathrm{card}(S) = \mathrm{card}(X_i)$ y para cada $i \in Y$ sea $g_i : X_i \to S$ una biyección. Consideremos $\alpha : Y \times Y \to \mathrm{Fun}(S \times S, S)$ dada por

$$\alpha_{i,j}(s,t) := g_{i\bar{\triangleright}j}(g_i^{-1}(s) \triangleright g_j^{-1}(t)).$$

Entonces α es un cociclo dinámico y $X \simeq Y \times_\alpha S$.

Demostración. Veamos que $(Y, \bar{\triangleright})$ es un quandle.

Sea $i \in Y$. Consideremos $\bar{\phi}_i : Y \to Y$, dada por $\bar{\phi}_i(j) := i\bar{\triangleright}j$.

(I) $\bar{\phi}_i$ es biyectiva ya que

(i) si $\bar{\phi}_i(j) = \bar{\phi}_i(j')$ se tiene que $X_i \triangleright X_j = X_i \triangleright X_{j'}$. Supongamos que $j \neq j'$ entonces $X_j \cap X_{j'} = \emptyset$. Sean $x \in X_i$, $y \in X_j$. Luego, $x \triangleright y \in X_i \triangleright X_{j'}$. Como $\phi_x : X \to X$ es biyectiva y $\mathrm{card}(X_{j'}) = \mathrm{card}(X_i \triangleright X_{j'})$ entonces $\phi_x|_{X_{j'}} : X_{j'} \to X_i \triangleright X_j$ es biyectiva. Luego, existe $z \in X_{j'}$ tal que $x \triangleright z = x \triangleright y$ y esto implica $y = z \in X_j \cap X_{j'}$; lo cual es una contradicción. Por lo tanto, $j = j'$ y $\bar{\phi}_i$ resulta inyectiva.

(ii) sean $k \in Y$, $x \in X_i$ y $z \in X_k$. Luego, existe $y \in X$ tal que $x \triangleright y = z$. Suponiendo que $y \in X_j$ se tiene que $X_i \triangleright X_j = X_k$. Luego, $X_{i\bar{\triangleright}j} = X_k$, o sea $i\bar{\triangleright}j = k$.

(II) Sean $i, j, k \in Y$. Luego

$$X_{i\bar{\triangleright}(j\bar{\triangleright}k)} = X_i \triangleright (X_j \triangleright X_k) = (X_i \triangleright X_j) \triangleright (X_i \triangleright X_k) = X_{i\bar{\triangleright}j} \triangleright X_{i\bar{\triangleright}k} = X_{(i\bar{\triangleright}j)\bar{\triangleright}(i\bar{\triangleright}k)},$$

lo que inplica que $i\bar{\triangleright}(j\bar{\triangleright}k) = (i\bar{\triangleright}j)\bar{\triangleright}(i\bar{\triangleright}k)$.

(III) Sea $i \in Y$. Como X es un quandle se tiene que

$$X_i = \{x \triangleright x \ / \ x \in X_i\} \subseteq X_i \triangleright X_i.$$

Entonces, $X_i \triangleright X_i = X_i$, es decir $i\bar{\triangleright}i = i$.

Ahora bien, si S es un conjunto no vacío tal que $\mathrm{card}(S) = \mathrm{card}(X_i)$ y para cada $i \in Y$ existe una biyección $g_i : X_i \to S$ entonces

(i) para cada $i, j \in Y$, $s \in S$ la función $\alpha_{i,j}(s) : S \to S$, dada por

$$\alpha_{i,j}(s)(t) = \alpha_{i,j}(s,t) = g_{i\bar{\triangleright}j}(g_i^{-1}(s) \triangleright g_j^{-1}(t)) = g_{i\bar{\triangleright}j}\phi_{g_i^{-1}(s)}g_j^{-1}(t),$$

es biyectiva pues es composición de biyecciones.

(ii) sean $i,j,k \in Y$ y $s,t,u \in S$; luego

$$\begin{aligned}
\alpha_{i,j\bar{\triangleright}k}(s,\alpha_{j,k}(t,u)) &= g_{i\bar{\triangleright}(j\bar{\triangleright}k)}(g_i^{-1}(s) \triangleright g_{j\bar{\triangleright}k}^{-1}(g_{j\bar{\triangleright}k}(g_j^{-1}(t) \triangleright g_k^{-1}(u)))) = \\
&= g_{i\bar{\triangleright}(j\bar{\triangleright}k)}(g_i^{-1}(s) \triangleright (g_j^{-1}(t) \triangleright g_k^{-1}(u))) = \\
&= g_{(i\bar{\triangleright}j)\bar{\triangleright}(i\bar{\triangleright}k)}((g_i^{-1}(s) \triangleright g_j^{-1}(t)) \triangleright (g_i^{-1}(s) \triangleright g_k^{-1}(u))) = \\
&= g_{(i\bar{\triangleright}j)\bar{\triangleright}(i\bar{\triangleright}k)}(g_{i\bar{\triangleright}j}^{-1}(g_{i\bar{\triangleright}j}(g_i^{-1}(s) \triangleright g_j^{-1}(t))) \triangleright \\
&\qquad \triangleright g_{i\bar{\triangleright}k}^{-1}(g_{i\bar{\triangleright}k}(g_i^{-1}(s) \triangleright g_k^{-1}(u)))) = \\
&= g_{(i\bar{\triangleright}j)\bar{\triangleright}(i\bar{\triangleright}k)}(g_{i\bar{\triangleright}j}^{-1}(\alpha_{i,j}(s,t)) \triangleright g_{i\bar{\triangleright}k}^{-1}(\alpha_{i,k}(s,u))) = \\
&= \alpha_{i\bar{\triangleright}j,i\bar{\triangleright}k}(\alpha_{i,j}(s,t),\alpha_{i,k}(s,u)),
\end{aligned}$$

lo que muestra que se cumple la condición (4.3) del Lema 4.1 y α resulta un cociclo dinámico.

Más aún, como Y es un quandle entonces $Y \times_\alpha S$ resulta un quandle ya que

$$\alpha_{i,i}(s,s) = g_{i\bar{\triangleright}i}(g_i^{-1}(s) \triangleright g_i^{-1}(s)) = g_i(g_i^{-1}(s)) = s,$$

para todo $i \in Y$, $s \in S$.

Finalmente, sea $\Phi : Y \times_\alpha S \to X$ dada por $\Phi(i,s) := g_i^{-1}(s)$. Luego,

(I) Φ es biyectiva, ya que

(i) si $\Phi(i,s) = \Phi(i',s')$ entonces $g_i^{-1}(s) = g_{i'}^{-1}(s') \in X_i \cap X_{i'}$; luego $i = i'$, lo que implica que $s = s'$.

(ii) sea $x \in X$. Luego, existe $i \in Y$ tal que $x \in X_i$. De esta manera, $\Phi(i, g_i(x)) = g_i^{-1}(g_i(x)) = x$, y Φ resulta suryectiva.

(II) Dado que

$$\begin{aligned}
\Phi((i,s) \triangleright (j,t)) &= \Phi(i\bar{\triangleright}j, \alpha_{i,j}(s,t)) = g_{i\bar{\triangleright}j}^{-1}(g_{i\bar{\triangleright}j}(g_i^{-1}(s) \triangleright g_j^{-1}(t))) = \\
&= g_i^{-1}(s) \triangleright g_j^{-1}(t) = \Phi(i,s) \triangleright \Phi(j,t),
\end{aligned}$$

se tiene que Φ es morfismo de racks.

Por lo tanto, $X \simeq Y \times_\alpha S$. $\square$

Observación 4.9. (1) Supongamos que se satisfacen las condiciones del Lema anterior. Si X es indescomponible entonces Y también lo es.

(2) El Lema anterior puede enunciarse en término de racks.

(3) Para enunciar el Lema en término de conjuntos cruzados es necesario suponer que $(Y, \bar{\triangleright})$ es un conjunto cruzado.

Corolario 4.10. *Sean $(X, \triangleright)$ y $(Y, \bar{\triangleright})$ quandles (resp. racks, conjuntos cruzados). Sea $f : X \to Y$ un morfismo suryectivo de racks tal que las fibras $f^{-1}(y)$ tienen todas la misma cardinalidad (lo que sucede, por ejemplo, si X es indescomponible). Entonces $X = Y \times_\alpha S$ es una extensión.*

Demostración. Sabemos que $X = \sqcup_{y \in Y} X_y$, donde $X_y = f^{-1}(y)$. Por hipótesis $\mathrm{card}(X_y) = \mathrm{card}(X_{y'})$, para todo $y, y' \in Y$.

Además, si $x \in X_y$, $x' \in X_{y'}$ entonces $x \triangleright x' \in X_{y \bar{\triangleright} y'}$, ya que $f(x \triangleright x') = f(x) \bar{\triangleright} f(x') = y \bar{\triangleright} y'$. Por otro lado, si $z \in X_{y \bar{\triangleright} y'}$ entonces $f(z) = y \bar{\triangleright} y'$. Como f es suryectiva tenemos que $y = f(x)$. Dado que ϕ_x es biyectiva existe $x'' \in X$ tal que $z = x \triangleright x''$. Luego, $y \bar{\triangleright} y' = y \bar{\triangleright} f(x'')$, por lo que $y' = f(x'')$, es decir $z \in X_y \triangleright X_{y'}$. Con esto se ve que $X_y \triangleright X_{y'} = X_{y \bar{\triangleright} y'}$.

Se define $S := X_{y_0}$, con $y_0 \in Y$ fijo. Luego, $\mathrm{card}(S) = \mathrm{card}(X_y)$, para todo $y \in Y$. Esto implica que existe una biyección $g_y : X_y \to S$. Por Lema 4.8 $X = Y \times_\alpha S$ es una extensión. □

Proposición 4.11. *Sea X un rack finito indescomponible. Entonces X es isomorfo a una extensión $Y \times_\alpha S$, donde Y es un conjunto cruzado indescomponible exacto. Más aún, Y es único con la propiedad que cualquier morfismo suryectivo de racks $X \to Z$, con Z exacto, se factoriza a través de Y.*

Demostración. Consideremos la sucesión

$$X \to X_1 := \phi(X) \to X_2 := \phi(X_1) \dots;$$

como X es finito la sucesión se estabiliza, digamos en $Y = X_n$, el cual es claramente exacto e indescomponible. Por ser exacto Y resulta un conjunto cruzado. Sea $f : X \to X_n$ el morfismo suryectivo dado por la sucesión anterior. Como X es indescomponible las fibras $f^{-1}(y)$ tienen la misma cardinalidad. Por Corolario 4.10 se tiene que $X = Y \times_\alpha S$.

Sea ahora $\psi : X \to Z$ un morfismo suryectivo con Z exacto. Por Lema 2.18 se tiene un morfismo suryectivo $\psi_1 : X_1 \to Z$, y así siguiendo. Luego, $\psi : X \to Z$ se factoriza a través de Y por el morfismo $\psi_n : X_n \to Z$. □

5. Racks simples.

5.1. Conjuntos cruzados indescomponibles exactos.

Los conjuntos cruzados indescomponibles exactos pueden ser caracterizados como sigue.

Proposición 5.1. *(1) Si X es un conjunto cruzado indescomponible exacto entonces existe un grupo G y un morfismo inyectivo de conjuntos cruzados $\varphi : X \to G$ tal que $Z(G)$ es trivial y $\varphi(X)$ es una sola órbita que genera a G como grupo. Más aún, G es único con estas condiciones, salvo isomorfismo.*

(2) Si X es una sola órbita en un grupo G con $Z(G)$ trivial y X genera G como grupo entonces X es un conjunto cruzado indescomponible exacto.

(3) Existe una equivalencia de categorías entre

(a) $\mathfrak{C}$; la categoría de conjunto cruzados indescomponibles exactos, con morfismos suryectivos.

(b) $\mathfrak{P}$; la categoría de pares $(G, \mathcal{O})$, donde G es un grupo con $Z(G)$ trivial y $\mathcal{O}$ es una órbita que genera G y un morfismo $f : (G, \mathcal{O}) \to (K, \mathcal{U})$ es un homomorfismo de grupo $f : G \to K$ tal que $f(\mathcal{O}) = \mathcal{U}$.

Demostración. (1). Tomamos $G = \mathrm{Inn}_{\triangleright}(X)$ y $\varphi = \phi : X \to \mathrm{Inn}_{\triangleright}(X)$. Luego, φ es morfismo inyectivo y $\varphi(X) = \phi(X)$ es una sola órbita que genera a G como grupo, por definición. Además, $Z(G)$ es trivial por Observación 2.23. Para ver unicidad supongamos que existen G' y $\varphi' : X \to G'$ que cumplen con estas condiciones. Si consideramos $X' = \varphi'(X)$ entonces $\varphi' : X \to X'$ es un isomorfismo de racks. Por Lema 2.18 la función $h := \mathrm{Inn}_{\triangleright}(\varphi') : \mathrm{Inn}_{\triangleright}(X) \to \mathrm{Inn}_{\triangleright}(X')$ es un isomorfismo de grupos; mientras que por Lema 2.19 (b) $\mathrm{Inn}_{\triangleright}(X') \simeq G'$. Por lo tanto, $\mathrm{Inn}_{\triangleright}(X) \simeq G'$.

(2). Como X es una órbita existe $x \in G$ tal que $X = \{gxg^{-1} \ / \ g \in G\}$, entonces es estable por conjugación, lo que implica que X es un conjunto cruzado. Además, $\mathcal{O}_x = X$ pues si $y \in X$, con $y = gxg^{-1}$, se tiene que

$$y = x_1 \triangleright (x_2 \triangleright (\dots (x_n \triangleright x) \dots)) \in \mathcal{O}_x.$$

Por otro lado, si $\phi_x = \phi_y$ entonces $xzx^{-1} = yzy^{-1}$ para todo $z \in X$; luego $x^{-1}y \in Z(G)$, es decir $x = y$. Con esto se ve que X es un conjunto cruzado indescomponible exacto.

(3). Sea $S : \mathfrak{C} \to \mathfrak{P}$ el funtor que a cada objeto X en $\mathfrak{C}$ le asocia el objeto $(\mathrm{Inn}_{\triangleright}(X), \phi(X))$ en $\mathfrak{P}$. Usando (2) podemos definir un funtor $T : \mathfrak{P} \to \mathfrak{C}$. A partir de esto y (1) es fácil ver que existe una equivalencia de categorías entre $\mathfrak{C}$ y $\mathfrak{P}$. □

Definición 5.2. Sean X, Y racks y sea $\pi : X \to Y$ una proyección de racks, es decir, un morfismo suryectivo de racks. Decimos que π es *trivial* si $\mathrm{card}(Y) = 1$ o $\mathrm{card}(X)$.

Definición 5.3. Un rack X es *simple* si X no es un rack trivial y cualquier proyección de racks $\pi : X \to Y$ es trivial.

Observación 5.4. Sea X un rack descomponible, digamos $X = X_1 \cup X_2$ y sea $Y = \{0, 1\}$, el rack trivial. Luego, $f : X \to Y$ dada por $f(X_1) = 0$ y $f(X_2) = 1$ es un morfismo suryectivo de racks.

Por lo tanto, todo rack simple Z es indescomponible. Para ver esto notamos que si $\text{card}(Z) = 2$ entonces es indescomponible por ser no trivial. Ahora bien, si $\text{card}(Z) \neq 2$ y supongamos que Z es descomponible entonces, por lo anterior, existe $\pi : Z \to Y = \{0, 1\}$ morfismo suryectivo de racks. Como Z es simple y $\text{card}(Y) \neq 1$ se tiene que $\text{card}(Z) = 2$ contra lo supuesto.

Observación 5.5. Sea X un rack simple con n elementos. Como $\phi(X)$ es un rack y $\phi : X \to \phi(X)$ es una proyección de racks entonces $\text{card}(X) = 1$ o n. Si $\text{card}(\phi(X)) = n$ se tiene que X es exacto y, por lo tanto, es un conjunto cruzado. También notamos que en este caso $\text{card}(X) > 2$. Por otra parte, si $\text{card}(\phi(X)) = 1$ entonces $\phi(X) = \{\varphi\}$ e

$$\text{Inn}_{\triangleright}(X) = \{\varphi^k \ / \ k \in \mathbb{N} \cup \{0\}\}.$$

Como X es simple entonces X es indescomponible. Luego, si $x \in X$

$$X = \mathcal{O}_x = \{\varphi^k(x) \ / \ k \in \mathbb{Z}\} = \{\varphi^k(x) \ / \ k \in \mathbb{N} \cup \{0\}\} = \{\varphi^k(x) \ / \ 0 \leq k \leq m-1\},$$

pues X es finito y orden de φ es igual a m. Sea M el mínimo entero positivo entre los j tales que

$$X = A_j := \{\varphi^k(x) \ / \ 0 \leq k \leq j\}.$$

Luego, $M = n$, pues si $M < n$ entonces $\text{card}(A_M) \neq n$ lo cual contradice el hecho de que $X = A_M$. Así, X es un rack de permutación definido por un ciclo de longitud n.

Proposición 5.6. *Sea X un rack indescomponible, con* $\text{card}(X)$ *primo, entonces X es simple.*

Demostración. Sean Y un rack y $f : X \to Y$ un morfismo suryectivo de racks. Por Corolario 2.40 se tiene que $\text{card}(X) = \text{card}(Y)\,\text{card}(G_y)$, para todo $y \in Y$, donde G_y es una fibra de f. Ahora bien, como $\text{card}(X)$ es primo entonces $\text{card}(Y) = 1$ ó $\text{card}(X)$. Por lo tanto, X es simple. □

Proposición 5.7. *Sea X un rack de permutación con n elementos definido por un ciclo de longitud n. Entonces X es simple si y sólo si n es primo.*

Demostración. Supongamos que X es simple. Sabemos que $X = \{x, \varphi(x), \dots, \varphi^{n-1}(x)\}$ donde φ es el ciclo que define al rack y x es un elemento cualquiera de X. Sea d un divisor de n. Consideramos en X la siguiente relación de equivalencia

$$\varphi^i(x) \sim \varphi^j(x) \iff i \equiv j \mod d.$$

Luego, definimos $Y := X/\sim$. Entonces, $\text{card}(Y) = d$ y notamos que

$$Y = \{[x], [\varphi(x)], \dots, [\varphi^{d-1}(x)]\},$$

donde $[\varphi^j(x)]$ es la clase de $\varphi^j(x)$. Además Y tiene estructura de rack con

$$[\varphi^i(x)] \triangleright [\varphi^j(x)] := [\varphi^{j+1}(x)].$$

Notar que $\triangleright$ está bien definido ya que si $\varphi^i(x) \sim \varphi^k(x)$ y $\varphi^j(x) \sim \varphi^h(x)$ entonces $\varphi^{j+1}(x) \sim \varphi^{h+1}(x)$, lo que nos dice que

$$[\varphi^i(x)] \triangleright [\varphi^j(x)] = [\varphi^k(x)] \triangleright [\varphi^h(x)].$$

Ahora bien, la proyección al cociente $\pi : X \to Y$ es un morfismo de racks. Como X es simple se tiene que $\text{card}(Y) = 1$ o n. Por lo tanto, n es primo.

Recíprocamente, supongamos que n es primo. Como $n \neq 1$, X es no trivial. Sea Y un rack y sea $f : X \to Y$ un morfismo suryectivo de racks. Luego,

$$\begin{aligned} f(\varphi^i(x)) &= f(x \triangleright (x \triangleright (\dots (x \triangleright x) \dots))) = f(x) \triangleright (f(x) \triangleright (\dots (f(x) \triangleright f(x)) \dots)) = \\ &= \psi^i(f(x)), \end{aligned}$$

donde $\psi = \phi_{f(x)}$. Ahora bien, como f es suryectiva se tiene que $1 \leq \text{card}(Y) \leq n$. Si $\text{card}(Y) < n$ existen i, j con $i \neq j$ y $0 \leq i, j \leq n-1$, tales que

$$f(\varphi^i(x)) = f(\varphi^j(x)),$$

o equivalentemente existe r con $1 \leq r \leq n-1$, tal que

$$f(x) = f(\varphi^r(x)).$$

De esta manera, $f(x) = \psi^r(f(x))$ lo que implica que $\psi^{rk}(f(x)) = f(x)$, para todo $k \in \mathbb{N}$. Como n y r son coprimos entonces $f(x) = \psi^j(f(x))$, para todo j con $1 \leq j \leq n-1$. Luego, $\text{Im}(f) = \{f(x)\}$, es decir $\text{card}(Y) = 1$. Por lo tanto, X es simple. □

Proposición 5.8. *Sea X un conjunto cruzado indescomponible exacto, el cual corresponde al par $(G, \mathcal{O})$. Entonces, X es simple si sólo si cualquier cociente de G, distinto de G, es cíclico.*

Demostración. Supongamos que X es simple y sea $\pi : G \to K$ epimorfismo de grupos. Dado que por Proposición 5.1 $G \simeq \mathrm{Inn}_{\triangleright}(X)$ entonces tenemos que $\psi := \pi\phi : X \to \pi(\phi(X))$ es un morfismo suryectivo de conjuntos cruzados y como π es homomorfismo de grupos entonces $\psi(X)$ genera a K como grupo. Por la Observación 5.5 se tiene que o bien $\psi(X)$ es un solo punto o bien ψ es biyectiva. Si $\psi(X)$ es un solo punto entonces K es cíclico. Mientras que si ψ es biyectiva tomamos $g \in Ker(\pi)$; luego,

$$\pi(g\phi_x g^{-1}) = \pi\phi_x,$$

y como $g\phi_x g^{-1} \in \phi(X)$, pues $\phi(X)$ es estándar, entonces $g\phi_x g^{-1} = \phi_y$, para algún $y \in X$. Esto implica que $\psi(x) = \psi(y)$ y, por ser ψ biyectiva, $x = y$, es decir $\phi_x = \phi_y$. De esta manera, se tiene que $g\phi_x = \phi_x g$, para todo $x \in X$, o sea $g \in Z(G)$, que es trivial. Por lo tanto, π es isomorfismo de grupo y K no es un cociente propio de G.

Recíprocamente, supongamos que cualquier cociente no trivial de G es cíclico. Sea $\pi : X \to Y$ un morfismo suryectivo de conjuntos cruzados. Luego, $\Phi = \mathrm{Inn}_{\triangleright}(\pi) : \mathrm{Inn}_{\triangleright}(X) \to \mathrm{Inn}_{\triangleright}(Y)$ es un epimorfismo de grupo. Como $G \simeq \mathrm{Inn}_{\triangleright}(X)$ se tiene que o bien Φ es una biyección, en cuyo caso $X \simeq Y$ y $\mathrm{card}(Y) = \mathrm{card}(X)$, o bien $\mathrm{Inn}_{\triangleright}(Y)$ es cíclico, digamos $\mathrm{Inn}_{\triangleright}(Y) = \langle\varphi\rangle$. En este último caso, como $\phi(Y)$ es un conjunto cruzado indescomponible dentro de un grupo abeliano entonces $\phi(Y)$ es un punto. Ahora bien, si $y \in Y$ entonces

$$\begin{aligned} Y = \mathcal{O}_y &= \{i_1^{\pm 1} \triangleright (i_2^{\pm 1} \triangleright (\dots (i_s^{\pm 1} \triangleright y)\dots)) \ / \ i_1, \dots, i_s \in Y\} = \\ &= \{\phi_{i_1}^{\pm 1} \dots \phi_{i_s}^{\pm 1}(y) \ / \ i_1, \dots, i_s \in Y\} \\ &= \{\phi_y^{\pm n}(y) \ / \ n \in \mathbb{N}\} = \{y\}, \end{aligned}$$

lo que implica que Y tiene un solo elemento. Por lo tanto, X es simple. □

Observación 5.9. Notar que si X es conjunto cruzado indescomponible exacto y $\pi : X \to Y$ es un morfismo suryectivo de racks entonces Y, y por ende $\phi(Y)$, son conjuntos cruzados indescomponibles.

Ejemplo 5.10. Sea X el conjunto cruzado de las caras del cubo (que es el mismo que el dado por los vértices del tetraedro). Podemos realizar X como la órbita dada por 4-ciclos de $\mathbb{S}_4$ ya que X es exacto e $\mathrm{Inn}_{\triangleright}(X) \simeq \mathbb{S}_4$. Considerando el cociente

$$\mathbb{S}_4 \to \mathbb{S}_4/K \simeq \mathbb{S}_3,$$

donde K es el subgrupo de Klein, podemos ver que X no es simple puesto que $\mathbb{S}_3$ no es cíclico.

Veamos a continuación algunos resultados de grupos finitos, por completitud.

Proposición 5.11. *Sea n un entero positivo,con $n \neq 4$. Luego*

(1) Si N es un subgrupo normal no trivial de $\mathbb{S}_n$ entonces $N = \mathbb{A}_n$ ó $N = \mathbb{S}_n$.

(2) Si C es un cociente de $\mathbb{S}_n$, distinto de $\mathbb{S}_n$, entonces $C \simeq \mathbb{Z}_2$ ó $C \simeq \{\mathrm{id}\}$.

Demostración. (1). Se tiene que $N \cap \mathbb{A}_n$ es un subgrupo normal de $\mathbb{A}_n$. Como $\mathbb{A}_n$ es simple tenemos que

$$N \cap \mathbb{A}_n = \mathbb{A}_n \quad \text{ó} \quad N \cap \mathbb{A}_n = \{\mathrm{id}\},$$

Si $N \cap \mathbb{A}_n = \mathbb{A}_n$ entonces $\mathbb{A}_n \subset N \subset \mathbb{S}_n$ lo que implica que

$$2 = [\mathbb{S}_n : \mathbb{A}_n] = [\mathbb{S}_n : N][N : \mathbb{A}_n],$$

por lo tanto, $[\mathbb{S}_n : N] = 1$ ó 2. Si es 1 entonces $N = \mathbb{S}_n$ y si es 2 entonces $N = \mathbb{A}_n$.

Veamos ahora que el segundo caso no puede ocurrir. Supongamos que $N \cap \mathbb{A}_n = \{\mathrm{id}\}$. Como $N \neq \{\mathrm{id}\}$ existe $\sigma \in N$, con $\sigma \neq \mathrm{id}$. Luego, $\sigma^2 \in N$ y $\sigma^2 \in \mathbb{A}_n$, pues es el producto de una cantidad par de transposiciones. Entonces $\sigma^2 = \mathrm{id}$. Sea $\sigma = (a_1b_1)(a_2b_2)\dots(a_rb_r)$ la descomposición de σ como producto de 2-ciclos disjuntos.

(I) Si $r = 1$ entonces $\sigma = (a_1b_1)$.

(i) Si $1 < a_1 < b_1$ entonces $(1b_1)(a_1b_1)(1b_1) = (1a_1)$ y $(1a_1)(a_1b_1)(1a_1) = (1b_1)$, y como N es normal se tiene que $(1a_1), (1b_1) \in N$. Luego, $(1a_1)(1b_1) = (1a_1b_1) \in N \cap \mathbb{A}_n$, lo cual es absurdo pues $(1a_1b_1) \neq \mathrm{id}$.

(ii) Si $a_1 = 1 < b_1$ tomemos a, con $a \neq 1$ y $a \neq b_1$. Entonces $(1a)(1b_1)(1a) = (ab_1) \in N$, y por (i) tenemos que $(1ab_1) \in \mathbb{A}_n$, absurdo.

(II) Si $r > 1$ entonces $(b_1a_2)\sigma(b_1a_2) \in N$ entonces $(b_1a_2)\sigma(b_1a_2) \neq \mathrm{id}$, ya que $\sigma \neq \mathrm{id}$; por lo tanto $(a_1b_1)(a_2b_2) = (a_1a_2)(b_1b_2)$, lo cual es absurdo.

(2). Es claro a partir de (1). □

Ejemplo 5.12. Sea n un entero positivo distinto de 4. Si X es una órbita no trivial de $\mathbb{S}_n$, digamos $X = \{\varphi\sigma\varphi^{-1} \ / \ \varphi \in \mathbb{S}_n\}$, entonces $N := \langle X \rangle$, el subgrupo de $\mathbb{S}_n$ generado por X, es normal en $\mathbb{S}_n$. Por la Proposición 5.11 se tiene que $N = \mathbb{A}_n$ o $N = \mathbb{S}_n$.

Si $N = \mathbb{S}_n$ tenemos que como X es una órbita de $\mathbb{S}_n$ entonces es indescomponible. Además, si $\phi_x = \phi_y$ se tiene que $x^{-1}y \in Z(\mathbb{S}_n)$, que es trivial. Por lo tanto, X es exacto. Por Lema 2.19 (b) resulta que

$$\mathrm{Inn}_{\triangleright}(X) \simeq \mathbb{S}_n/Z(\mathbb{S}_n) = \mathbb{S}_n,$$

que satisface que los únicos cocientes propios son cíclicos. Luego, por Proposición 5.8 se tiene que X es simple.

Si $N = \mathbb{A}_n$ puede ocurrir que X no sea una órbita en $\mathbb{A}_n$. En rigor, X no es una órbita en $\mathbb{A}_n$ si y sólo si los centralizadores de los elementos de X están en $\mathbb{A}_n$, pues el orden de la órbita es el orden del grupo dividido el orden del subgrupo centralizador de X.En este caso, X se descompone como una unión de dos órbitas las cuales son isomorfas vía conjugación por cualquier elemento de $\mathbb{S}_n \setminus \mathbb{A}_n$ (un ejemplo de este caso aparece para $n = 5$ y X los 5-ciclos). Por otra parte, si los centralizadores de los elementos de X no están en $\mathbb{A}_n$ entonces X resulta una órbita en $\mathbb{A}_n$ y de manera análoga al caso anterior se puede ver que X es indescomponible; por lo tanto X resulta simple por la Proposición 5.8.

5.2. Clasificación de racks simples.

Caracterizaremos a los racks simples en términos de teoría de grupos. Para ello, primero clasificamos los grupos finitos G tales que $Z(G)$ es trivial y G/N es cíclico para cualquier N, subgrupo normal no trivial de G.

Notaremos: si G actúa sobre H, el producto semidirecto $H \rtimes G$ tiene estructura de grupo dada por $(h, g)(h', g') = (hg \cdot h', gg')$.

Teorema 5.13 (Guralnick)**.** *Sea G un grupo finito, no trivial, tal que $Z(G)$ es trivial y G/H es cíclico para cualquier subgrupo normal, no trivial H. Entonces existe un grupo simple L, un entero positivo t y un grupo finito cíclico $C = \langle x \rangle$, donde $x \in \mathrm{Aut}(N)$ y $N := L^t = L \times \cdots \times L$ (t veces), tales que se satisface una de las siguientes posibilidades*

(1) L es abeliano, así N es abeliano de orden p^t, x es no trivial y actúa irreduciblemente sobre N. Más aún, $G \simeq N \rtimes C$.

(2) L es no abeliano, $G = NC \simeq N \rtimes C/Z(N \rtimes C)$ y x actúa por

$$x \cdot (l_1, \ldots, l_t) = (\theta(l_t), l_1, \ldots, l_{t-1}), \tag{5.14}$$

para algún $\theta \in \mathrm{Aut}(L)$.

Recíprocamente, todos los grupos que satisfacen (1) o (2) tienen las propiedades deseadas. Más aún, dos grupos en una de las listas son isomorfos si y sólo si los correspondientes grupos L son isomorfos, los correspondientes enteros t son iguales y los correspondientes automorfismos x definen, salvo conjugación, el mismo elemento en $\mathrm{Out}(N) = \mathrm{Aut}(N)/\mathrm{Int}(N)$.

Veremos algunos resultados previos que nos serán útiles para probar este Teorema.

Lema 5.15. *Si G es un grupo entonces*

(i) $[G, G] := \langle \{[a, b] = aba^{-1}b^{-1} / a, b \in G\} \rangle$ es un subgrupo normal.

(ii) $G/[G, G]$ es abeliano.

(iii) Si N es un subgrupo normal de G entonces G/N es abeliano si y sólo si $[G,G] \subset N$.

Demostración. (i) Si $a, b, g \in G$ entonces

$$g[a,b]g^{-1} = gaba^{-1}b^{-1}g^{-1} = [gag^{-1}, gbg^{-1}] \in [G,G].$$

Luego, $[G,G]$ es subgrupo normal de G.

(ii) Sean $g, h \in G$. Luego,

$$(g[G,G])(h[G,G]) = (h[G,G])(g[G,G]) \iff gh(hg)^{-1} \in G,$$

pero $gh(hg)^{-1} = ghg^{-1}h^{-1} = [g,h]$ que pertenece a $[G,G]$. Así, $G/[G,G]$ es abeliano.

(iii) Sean $g, h \in G$. Si G/N es abeliano de la misma manera que en (ii) se tiene que $gh(hg)^{-1} \in N$, es decir $[G,G] \subset N$. La recíproca es fácil. □

Observación 5.16. Si G es un grupo no abeliano tal que G/H es abeliano para cualquier subgrupo normal no trivial H, entonces G tiene un único subgrupo normal no trivial minimal, que es $[G,G]$.

Lema 5.17. *Si G es un grupo no trivial tal que G/N es cíclico para todo subgrupo normal no trivial N entonces G es no abeliano si y sólo si $Z(G)$ es trivial.*

Demostración. Supongamos que G es no abeliano y que $Z(G)$ es no trivial. Sea $x \in Z(G)$, con $x \neq e$, y sea $N := \langle x \rangle$. Luego, N es un subgrupo normal no trivial de G; esto implica que G/N es cíclico, digamos $G/N = \langle yN \rangle$, con $y \in G - N$. Por lo tanto, todo elemento g de G se puede escribir como $g = y^r x^s$, con $r, s \in \mathbb{Z}$, resultando G abeliano, contra lo supuesto. La recíproca es obvia. □

Observación 5.18. El caso (2) del Teorema 5.13 contempla el caso en el que G es simple no abeliano tomando $L = G$, $C = \mathrm{id}$ y $t = 1$.

Observación 5.19. En el caso (1), identificamos L con $\mathbb{F}_p$ y el automorfismo x con $T \in \mathrm{GL}(t, \mathbb{F}_p)$. Entonces x actúa irreduciblemente si y sólo si el polinomio característico de T es irreducible, y por lo tanto, igual al polinomio minimal de T. En este caso, si n es igual al orden de x y si d divide a n, con $d \neq 1$ y $d \neq n$, entonces $\ker(T^d - \mathrm{id}) = 0$. Esto implica que $N - \{0\}$ es una unión de copias de C. Por lo tanto, $|C|$ divide a $p^t - 1$. Claramente, podemos asumir que x actúa por la matriz compañera de un polinomio mónico irreducible en $\mathbb{F}_p[X]$ de grado t.

Observación 5.20. Sean N, C dos grupos, donde C actúa sobre N por automorfismos. Si $(n,c) \in Z(N \rtimes C)$ entonces $(n,c)(m,d) = (m,d)(n,c)$, es decir

$$(n\ c \cdot m, cd) = (m\ d \cdot n, dc),$$

para todo $(m,d) \in N \rtimes C$. Esto implica que $c \in Z(C)$ y $n\ c \cdot m = m\ d \cdot n$. Tomando $d = e$ se tiene que $c \cdot m = n^{-1}mn$ y tomando $m = e$ obtenemos que $d \cdot n = n$, para todo $d \in C$, es decir $n \in N^C := \{m \in N / C \cdot m = m\}$. Por lo tanto,

$$Z(N \rtimes C) = \{(n,c)/c \in Z(C), n \in N^C, c \cdot m = n^{-1}mn, \forall m \in N\}.$$

En particular, si $\pi : N \rtimes C \to N \rtimes C/Z(N \rtimes C)$ es la proyección canónica al cociente entonces

$$\pi(N) \simeq N/Z(N)^C. \tag{5.21}$$

Lema 5.22. *Si G es un grupo entonces*

(i) si P y M son subgrupos tales que $[P,M] = \{e\}$ entonces $\varphi : P \times M \to G$, $\varphi(x,y) = xy$ es un homomorfismo de grupos.

(ii) si P y M son subgrupos normales y $P \cap M = \{e\}$ entonces $[P,M] = \{e\}$, y PM es un subgrupo normal de G.

Demostración. Directa. □

Lema 5.23. *Sea A un grupo y sean $A_1, \ldots, A_n$ subgrupos normales no triviales de A entonces $A_1 \ldots A_n$ es un subgrupo normal de A.*

Demostración. Por inducción en n y el Lema anterior. □

Demostración. (Del Teorema 5.13)

Paso I. Sea G un grupo finito y sea N un subgrupo normal no trivial minimal tal que G/N es cíclico.

Entonces existe $x \in G$ tal que $[x]$, la clase de x, genera G/N. Definimos $C := \langle x \rangle$. Luego, $G = NC$ ya que si $g \in G$ entonces $gN = x^j N$ para algún j, o sea $gx^{-j} \in N$ y, por lo tanto, $g \in NC$. Sea L un subgrupo normal no trivial y minimal de N. Se define

$$L_i := x^{i-1} L x^{-i+1},$$

para todo $i \in \mathbb{N}$. Luego, afirmamos que

(i) L_i es un subgrupo normal minimal de N.

(ii) $(L_1 \dots L_j) \cap L_{j+1}$ es trivial ó es L_{j+1}.

Para ver (i) tenemos que

$$nx^{i-1}Lx^{-i+1}n^{-1} = x^{i-1}(x^{-i+1}nx^{i-1})l(x^{-i+1}n^{-1}x^{i-1})x^{-i+1} \in L_i,$$

para todo $n \in N$ y $l \in L$. Además, L_i es minimal pues L lo es. Por otro lado, (ii) es cierto ya que $L_1 \dots L_j$ es un subgrupo normal de N, por Lema 5.23; lo que implica que $(L_1 \dots L_j) \cap L_{j+1}$ es un subgrupo normal de N contenido en L_{j+1}. Como L_{j+1} es minimal se tiene que $(L_1 \dots L_j) \cap L_{j+1}$ es trivial ó L_{j+1}. Consideremos t el entero positivo más pequeño tal que

$$(L_1 \dots L_t) \cap L_{t+1} = L_{t+1}.$$

Entonces

$$L_1 \dots L_t \simeq L_1 \times \cdots \times L_t.$$

Primero veámoslo para el caso $t = 2$. Sea $\Phi : L_1 \times L_2 \to L_1L_2$ dada por

$$\Phi(l_1l_2) := l_1l_2.$$

Es obvio que Φ es suryectiva; además si $l_1l_2 = l_1'l_2'$ entonces

$$(l_1')^{-1}l_1 = l_2'l_2^{-1} \in L_1 \cap L_2 = \{e\},$$

pues $t = 2$. Por lo tanto, $l_1 = l_1'$ y $l_2 = l_2'$ resultando Φ inyectiva. Ahora bien,

$$l_1l_2 = l_1l_2l_1^{-1}l_1 \in L_2L_1,$$

$$l_1l_2 = l_2l_2^{-1}l_1l_2 \in L_2L_1,$$

por lo que $l_2 = l_1l_2l_1^{-1}$, es decir $l_2l_1 = l_1l_2$. De esta forma

$$\Phi((l_1, l_2)(l_1', l_2')) = \Phi(l_1l_1', l_2l_2') = l_1l_1'l_2l_2' = l_1l_2l_1'l_2' = \Phi(l_1l_2)\Phi(l_1'l_2'),$$

con lo que Φ resulta un isomorfismo de grupos. Luego, se procede por inducción en j, $1 \leq j \leq t$. Por otra parte, $L_1 \dots L_t \simeq L_1 \times \cdots \times L_t$ es un subgrupo normal de G ya que es normal en N y es estable por conjugación por x. Por lo tanto, $N = L_1 \dots L_t$. Si S es subgrupo normal de L entonces

$$S \simeq S \times e \times \cdots \times e$$

y $S \times e \times \cdots \times e$ es normal en

$$N = L_1 \times \cdots \times L_t \simeq L \times \cdots \times L.$$

Como L es minimal se tiene que $S = \{e\}$ ó $S = L$, por lo tanto L es simple.

Paso II. Ahora, mostramos que cualquier grupo G que satisface los requerimientos del Teorema es o bien como en el caso (1) o bien como en el caso (2). Supongamos que G no es

simple (ver Observación 5.18). Mantenemos la notación del Paso (I) y suponemos que $Z(G)$ es trivial y que cualquier cociente propio de G es cíclico. Sea $N = [G, G]$, subgrupo normal no trivial minimal por Observación 5.16. Por el paso I, $N = L \times \cdots \times L$ (t veces).

(A). Si L es abeliano entonces N es abeliano y se tiene que $N \cap C \subset Z(G)$, que es trivial por hipótesis. Si consideramos ahora a $N \rtimes C$, donde C actúa por conjugación sobre N, y a la proyección $p : N \rtimes C \to G$ dada por $p(n, c) = nc$ se tiene que p es un epimorfismo de grupos. Luego,

$$Z(N \rtimes C) \subseteq p^{-1}(Z(G)) = p^{-1}(e) = \ker(p). \tag{5.24}$$

Por otra parte, si $(n, c) \in \ker(p)$ entonces $c = n^{-1}$, lo que implica que c actúa por conjugación sobre N por n^{-1}. Además, $c = n^{-1} \in N \cap C = \{e\}$. Luego, $(n, c) = e$ y ,por lo tanto, $Z(N \rtimes C) = \{e\}$. Con esto se ve que

$$G \simeq N \rtimes C.$$

Más aún, x actúa irreduciblemente ya que si P es un subgrupo de N x-estable entonces P es normal en G lo que implica que $P = \{e\}$ ó $P = N$. Por lo tanto, G es como en el caso (1).

(B). Si L es no abeliano y $t > 1$ tenemos que

$$[xL_tx^{-1}, L_i] = x[L_t, L_{i-1}]x^{-1} = e, \tag{5.25}$$

para todo $1 < i \leq t$. La primera igualdad es cierta ya que

$$\begin{aligned} w \in [xL_tx^{-1}, L_i] \Leftrightarrow w &= (xx^{t-1}l_tx^{-t+1}x^{-1})(x^{i-1}l_ix^{-i+1})(xx^{t-1}l_t^{-1}x^{-t+1}x^{-1})(x^{i-1}l_i^{-1}x^{-i+1}) = \\ &= x[(x^{t-1}l_tx^{-t+1})(x^{i-2}l_ix^{-i+2})(x^{t-1}l_t^{-1}x^{-t+1})(x^{i-2}l_i^{-1}x^{-i+2})]x^{-1} = \\ &= w' \in x[L_t, L_{i-1}]x^{-1}, \end{aligned}$$

mientras que la segunda igualdad sale del Lema 5.22. De aquí sacamos que x lleva L_t isomórficamente a L_1 y x actúa como en el caso (2) del enunciado. Para ver esto, recordamos que $N = L \times \cdots \times L$ (t veces). Sean

$$\begin{aligned} u &= (u_1, \ldots, u_t) \in xL_tx^{-1}, \\ v_l &= (e, \ldots, l, \ldots, e) \in L_i. \end{aligned}$$

Por (5.25) se tiene que $[u, v_l] = e$, para todo $l \in L$. Entonces $[u_i, l] = e$, para todo $l \in L$, $1 < i \leq t$. Como L es simple no abeliano, esto implica que $u_i \in Z(G) = \{e\}$, para todo $1 < i \leq t$. Luego, $u = (u_1, e, \ldots, e)$, o sea $xL_tx^{-1} \subseteq L_1$. Más aún, $xL_tx^{-1} = L_1$.

Ahora bien, sea $u = (e, \ldots, e, l) \in L_t$, con $l \in L$. Por lo visto anteriormente

$$x \cdot u_l = xu_lx^{-1} = (\theta(l), e, \ldots, e),$$

donde $\theta \in \mathrm{Aut}(L)$. Por otro lado, si $i < t$ tenemos que $xL_ix^{-1} = L_{i+1}$ por definición, lo que dice que si $v_i = (e, \ldots, l, \ldots, e) \in L_i$ entonces

$$x \cdot u_i = x \cdot (e, \ldots, l, \ldots, e) = (e, \ldots, e, l, \ldots, e) \in L_{i+1}.$$

Por último, si consideramos la proyección p como en (A), entonces por (5.24) se tiene que $Z(N \rtimes C) \subseteq \ker(p)$. Ahora bien, si $(n, c) \in \ker(p)$ entonces $c = n^{-1}$, lo que implica que c actúa por conjugación sobre N por n^{-1}. Por Observación 5.20 tenemos que $(n, c) \in Z(N \rtimes C)$. De esta manera, $Z(N \rtimes C) = \ker(p)$. Por lo tanto

$$G \simeq N \rtimes C/Z(N \rtimes C).$$

Paso III. Unicidad. N es único pues, como observamos, $N = [G, G]$. Por su parte, L es único por Jordan-Hölder, entonces t es único. Puesto que x fue elegido módulo N se tiene que x y x' generan al mismo grupo si conciden en $\mathrm{Out}(N)$. Además, como cualquier automorfismo $G \to G$ debe dejar invariante a N entonces x es único salvo conjugación en $\mathrm{Out}(N)$.

Paso IV. Mostramos ahora que los grupos descriptos en el Teorema tienen las propiedades deseadas.

Sean L, N, C, G como en el caso (1). Por la irreducibilidad de la acción de C, siendo x no trivial, se ve que $Z(G)$ es trivial pues por la Observación 5.20 si $(n, c) \in Z(N \rtimes C)$ entonces $x \cdot n = n$ y $c \cdot m = m$, para todo $m \in N$, lo que implica que $c = e$ y $n = e$, ya que si $n \neq e$ se tendría que $x \cdot \langle n \rangle \subseteq \langle n \rangle$ y x no actuaría irreduciblemente. Afirmamos que cualquier subgrupo normal no trivial M de G contiene a

$$\widetilde{N} := N \rtimes \{e\}.$$

Como $\widetilde{N}$ es subgrupo normal de G entonces $M \cap \widetilde{N}$ es subgrupo normal en G y como $M \cap \widetilde{N} \subseteq \widetilde{N}$ se tiene que

$$M \cap \widetilde{N} = N' \rtimes \{e\},$$

con N' subgrupo de N. Ahora bien, sea $(m, c) \in M \cap \widetilde{N}$, digamos $(m, c) = (m, e)$ con $m \in N'$. Luego,

$$(e, x)(m, e)(e, x^{-1}) = (x \cdot m, e) \in N' \rtimes \{e\},$$

lo que implica que $x \cdot m \in N'$, para todo $m \in N'$. Por lo tanto, N' es un subgrupo de N x-estable y dado que x actúa irreduciblemente sobre N se tiene que $N' = \{e\}$ ó $N' = N$, es decir

$$M \cap \widetilde{N} = \{e\} \quad \text{ó} \quad M \cap \widetilde{N} = \widetilde{N}.$$

Si $a \in G$ y $m \in M$, $m \neq e$, entonces

$$[a, m] \in M \cap [G, G] \subseteq M \cap \widetilde{N}.$$

Si $M \cap \widetilde{N} = \{e\}$ se tendría que $am = ma$, o sea $m \in Z(G) = \{e\}$ contra lo supuesto. Por otro lado, si G/M es un cociente de G, existe un epimorfismo de grupos

$$C \simeq G/N \to G/M,$$

con lo cual G/M resulta un cociente de C y por lo tanto es cíclico, como queríamos mostrar.

Sean L, N, C, G como en el caso (2). Identificamos a N con su imagen en G, por (5.21). Afirmamos que $Z(G)$ es trivial. Para ver esto consideramos la proyección $p : N \rtimes C \to G$ y sea (n, c) tal que $p(n, c) = nc \in Z(G)$. Esto implica que

$$ncmd = mdnc,$$

para todo $m \in N, d \in C$, y tomando $m = e$, $d = x$ vemos que $n \in N^x$ mientras que si tomamos $d = e$ vemos que c actúa sobre N por conjugación por n^{-1}. Luego, $(n, c) \in Z(N \rtimes C) = \ker(p)$ y $nc = e$ en G.

Veamos finalmente que todo cociente de G es cíclico. Cualquier subgrupo normal P de N es de la forma

$$\prod_{j \in J} L_j$$

para algún subconjunto J de $\{1, \dots, t\}$. Si P es x-estable entonces o bien P es trivial o bien es igual a N pues x permuta las copias de L. Como en el caso (1), concluimos que cualquier subgrupo normal no trivial M de G contiene a N, por lo tanto cualquier cociente no trivial de G es cíclico. Con esto se finaliza la prueba. □

Teorema 5.26 (Etingof-Guralnik-Soloviev)**.** *Sea G un grupo finito y sea $x \in G$. Sea $\mathcal{C}_x$ la clase de conjugación de x y $N = \langle \mathcal{C}_x \rangle$ el subgrupo de G generado por $\mathcal{C}_x$. Si el cardinal de $\mathcal{C}_x$ es la potencia de un primo entonces N es soluble.*

Demostración. Ver [EGS], Lema 8. □

Observación 5.27. Sean N y C grupos finitos con C actuando sobre N por automorfismos de grupo y sea $G = N \rtimes C$. Si $(m, z), (n, y) \in G$ entonces

$$(m, z)(n, y)(m, z)^{-1} = (m(z \cdot n)(zyz^{-1} \cdot m^{-1}), zyz^{-1}).$$

Consideremos la acción de N sobre sí mismo dada por

$$m \rightharpoonup_y n := mn(y \cdot m^{-1}). \tag{5.28}$$

y denotemos por $\mathcal{O}_y$ a la órbita bajo esta acción. Luego, si C es abeliano se tiene que

$$\mathcal{C}(n, y) = \{(m(z \cdot n)(y \cdot m^{-1}), y) \ / \ z \in C, m \in N\} = \bigcup_{z \in C} \mathcal{O}_y(z \cdot n) \times \{y\}, \tag{5.29}$$

donde $\mathcal{C}(n, y)$ es la clase de conjugación en $N \rtimes C$. Además, $n^{-1} \rightharpoonup_y n = y \cdot n$, lo que implica que

$$m \rightharpoonup_y y \cdot n = m \rightharpoonup_y (n^{-1} \rightharpoonup_y n) = mn^{-1} \rightharpoonup_y n \in \mathcal{O}_y(n)$$

y $\mathcal{O}_y(y \cdot n) \subseteq \mathcal{O}_y(n)$. Ahora bien, como

$$m \rightharpoonup_y y^2 \cdot n = m \rightharpoonup_y ((y \cdot n)^{-1} \rightharpoonup_y y \cdot n) = m(y \cdot n)^{-1} \rightharpoonup_y y \cdot n \in \mathcal{O}_y(y \cdot n),$$

entonces se tiene que

$$\mathcal{O}_y(y^2 \cdot n) \subseteq \mathcal{O}_y(n),$$

y así siguiendo. De esta manera, vemos que

$$\bigcup_{z \in <y>} \mathcal{O}_y(z \cdot n) = \mathcal{O}_y(n). \tag{5.30}$$

Podemos ahora enunciar la clasificación de racks simples. Comenzamos dando el siguiente teorema importante.

Teorema 5.31. *Sea $(X, \triangleright)$ un conjunto cruzado simple y sea p un número primo. Entonces las siguientes afirmaciones son equivalentes*

(1) X tiene p^t elementos, para algún $t \in \mathbb{N}$.

(2) $\mathrm{Inn}_{\triangleright}(X)$ es soluble.

(3) $\mathrm{Inn}_{\triangleright}(X)$ es como en el caso (1) del Teorema 5.13.

(4) X es un conjunto cruzado afín $({\mathbb{F}_p}^t, T)$ donde $T \in \mathrm{GL}(t, \mathbb{F}_p)$ actúa irreduciblemente.

Demostración. (1) $\implies$ (2). Como $(X, \triangleright)$ es simple entonces ϕ es una biyección, es decir $\phi(X)$ tiene p^t elementos. Por Teorema 5.26, $\mathrm{Inn}_{\triangleright}(X)$ es soluble.

(2) $\implies$ (3). Si $G = \mathrm{Inn}_{\triangleright}(X)$ es soluble entonces sus factores de composición en la serie de Jordan-Hölder son abelianos. Por lo tanto, G es como en el caso (1) del Teorema 5.13.

(3) $\implies$ (4). Se obtiene a partir de la Observación 5.19. Por otro lado, como $\phi(X) \subset \mathrm{Inn}_{\triangleright}(X)$ es una clase de conjugación entonces, por (5.29), se tiene que $\phi(X) = N \times \{x^r\}$, donde N y x son como en el caso (1) del Teorema 5.13. Dado que $\phi(X)$ genera a $\mathrm{Inn}_{\triangleright}(X)$, r debe ser coprimo con el orden de x. Tomamos $y = x^r$ y llamamos $T \in \mathrm{GL}(t, \mathbb{F}_p)$ a la acción de y, la cual es también irreducible. Entonces

$$(m, y) \triangleright (n, y) = (m, y)(n, y)(m, y)^{-1} = (Tn + (\mathrm{id} - T)m, y),$$

da una estructura de conjunto cruzado afín a X.

(4) $\implies$ (1). Es obvio. $\square$

Corolario 5.32. *La clasificación de racks simples con p^t elementos, para algún número primo p y $t \in \mathbb{N}$ es la siguiente*

(a) el rack de permutación correspondiente al ciclo $(1, 2, \ldots, p)$ si $t = 1$.

(b) *conjuntos cruzados afines* $(\mathbb{F}_p{}^t, T)$ *donde* T *es la matriz compañera de un polinomio mónico irreducible en* $\mathbb{F}_p[X]$ *distinto de los polinomios* X *y* $X-1$.

Demostración. Por Observación 5.5 ocurre que $\phi(X)$ tiene un solo elemento o ϕ es una biyección. En el primer caso, X es un rack de permutación definido por un ciclo de longitud p^t. Como X es simple, por Proposición 5.7, se tiene que $t = 1$. Mientras que en el segundo caso X resulta un conjunto cruzado (con $\operatorname{card}(X) > 2$), y por el Teorema 5.31 y la Observación 5.19, X es como en (b). Luego, x actúa por la matriz compañera de un polinomio mónico irreducible f en $\mathbb{F}_p[X]$. Ahora bien, si χ_T y m_T son el polinomio característico y minimal de T, respectivamente, entonces

$$\chi_T = m_T = f.$$

Por lo tanto, si $f = X$ se tiene que $m_T(T) = T = 0$, lo cual es absurdo; mientras que si $f = X - 1$ entonces $m_T(T) = T - \mathrm{id} = 0$, es decir $T = \mathrm{id}$, contradiciendo la hipótesis de que x es no trivial. □

Teorema 5.33. *Sea* $(X, \triangleright)$ *un conjunto cruzado cuyo cardinal es divisible por al menos dos números primos distintos. Entonces las siguientes afirmaciones son equivalentes*

(i) X *es simple.*

(ii) *Existe un grupo simple no abeliano* L*, un entero positivo* t *y* $x \in \operatorname{Aut}(L^t)$ *donde* x *actúa por* (5.14)*, para algún* $\theta \in \operatorname{Aut}(L)$*, tal que* $X = \mathcal{O}_x(n)$ *es una órbita de la acción* $\rightharpoonup_x$ *de* $N = L^t$ *en sí mismo como en* (5.28) *(*$n \neq m^{-1}$ *si* $t = 1$ *y* x *es interior,* $x(u) = mum^{-1}$*). Más aún,* L *y* t *son únicos, y* x *solamente depende de su clase de conjugacíon en* $\operatorname{Out}(L^t)$*. Si* $m, u \in X$ *entonces*

$$m \triangleright u = mx(um^{-1}). \tag{5.34}$$

Demostración. (i) $\implies$ (ii). Como X no tiene p^t elementos, con p primo y $t \in \mathbb{N}$, entonces, por Teorema 5.31, $\operatorname{Inn}_{\triangleright}(X)$ no es como en el caso (1) del Teorema 5.13; luego, ocurre el caso (2). De esta manera, existen un grupo simple no abeliano L, un entero positivo t y $x \in \operatorname{Aut}(L^t)$. Denotamos $N = L^t$ y $C = \langle x \rangle$. Luego,

$$G := N \rtimes C / Z(N \rtimes C) \simeq \operatorname{Inn}_{\triangleright}(X). \tag{5.35}$$

Sean $\widetilde{G} := N \rtimes C$ y $\pi : \widetilde{G} \to G$ la proyección canónica, y denotamos por $\widetilde{\mathcal{C}}$ y $\mathcal{C}$ las clases de conjugación en $\widetilde{G}$ y G, respectivamente. Ahora bien, si $\widetilde{\mathcal{C}}(n, y)$ es una clase de conjugación en $\widetilde{G}$ entonces, por ser π un homomorfismo suryectivo de grupos, se tiene que $\pi(\widetilde{\mathcal{C}}(n, y))$ es una clase de conjugación en G; más aún

$$\pi(\widetilde{\mathcal{C}}(n, y)) = \mathcal{C}(\pi(n, y)).$$

Además, $\widetilde{\mathcal{C}}(n, y)$ y $\mathcal{C}(\pi(n, y))$ son conjuntos cruzados estándares en $\widetilde{G}$ y G, respectivamente; y no es difícil ver que $\pi : \widetilde{\mathcal{C}}(n, y) \to \mathcal{C}(\pi(n, y))$ es un isomorfismo de conjuntos cruzados.

Por otro lado, por (5.29), se puede ver que $\widetilde{\mathcal{C}}(n,y)$ y $\bigcup_{z\in C}\mathcal{O}_y(z\cdot n)$ son isomorfos como conjuntos cruzados, donde $\mathcal{O}_y$ es la órbita en N dada por (5.28). Notar que $\bigcup_{z\in C}\mathcal{O}_y(z\cdot n)$ tiene estructura de conjunto cruzado dada por

$$m \triangleright m' = m\ y\cdot m'\ y\cdot m^{-1},$$

para todo $m, m' \in \bigcup_{z\in C}\mathcal{O}_y(z\cdot n)$.

Como $\phi(X)$ es una órbita en $\mathrm{Inn}_{\triangleright}(X)$ se tiene que, por (5.35), $\phi(X)$ es de la forma $\mathcal{C}(\pi(n,y)) = \pi(\widetilde{\mathcal{C}}(n,y))$, para algún $(n,y)\in N\rtimes C$. Por lo visto anteriormente, resulta que X tiene la estructura de $\bigcup_{z\in C}\mathcal{O}_y(z\cdot n)$.

Ahora, $ny\in G$ debe ser tal que $\pi(\widetilde{\mathcal{C}}(n,y))$ genere a G. Como el subgrupo generado por ny es invariante sabemos, por la prueba del Teorema 5.13, que es trivial o contiene a N. Es trivial si $(n,y)\in Z(N\rtimes C)$, es decir $t=1$ e y actúa sobre N por conjugación por n^{-1}; así que debemos excluir este caso. Con este caso excluido, y debe generar C, y entonces podemos tomar $y=x$ en la prueba del Teorema 5.13. Por lo tanto,

$$\bigcup_{z\in C}\mathcal{O}_y(z\cdot n) = \bigcup_{z\in C}\mathcal{O}_x(z\cdot n) = \mathcal{O}_x(n),$$

por (5.30). Con esto se ve que X tiene la estructura de $\mathcal{O}_x(n)$, como queríamos probar.

(ii) $\implies$ (i). Es análoga a la anterior. $\square$

Conclusiones.

Podemos enunciar la clasificación de los racks simples de la siguiente manera: si X es un rack simple entonces puede ocurrir

(1) $\mathrm{card}(X) = p$, con p primo, $X\simeq \mathbb{F}_p$ un rack de permutación dado por $x\triangleright y = y+1$.

(2) $\mathrm{card}(X) = p^t$, con p primo, $X\simeq ({\mathbb{F}_p}^t, T)$ es afín como en el Corolario 5.32 (1).

(3) $\mathrm{card}(X)$ es divisible por al menos dos primos distintos y X es un conjunto cruzado homogéneo torcido como en Teorema 5.33.

Los conjuntos cruzados simples en (2) pueden ser alternativamente descriptos como $(X, \triangleright^a)$ donde $X\simeq\mathbb{F}_q$, con $q=p^t$ y $a\in\mathbb{F}_q$ que genera a $\mathbb{F}_q$ sobre $\mathbb{F}_p$ y

$$x\triangleright^a y = (1-a)x + ay.$$

Por Corolario 3.8 se sigue fácilmente que $\mathrm{Aut}(X,\triangleright^a)$ es el producto semidirecto $\mathbb{F}_q\rtimes\mathbb{F}_q^{\times}$.

Es natural preguntarse cuántos conjuntos cruzados simples diferentes con $q = p^t$ elementos existe. Este es un resultado elemental bien conocido que utiliza la función de Möbius.

La *función de Möbius* es una función $\mu : \mathbb{N} \to \{-1, 0, 1\}$ dada por

(1) $\mu(n) = 0$, si n es divisible por el cuadrado de un número primo.

(2) $\mu(n) = (-1)^k$, si n no es divisible por el cuadrado de un número primo y k es la cantidad de divisores primos de n.

Proposición 5.36. *(i) La función μ es la única aplicación de $\mathbb{N}$ en $\mathbb{Z}$ tal que $\mu(1) = 1$ y*

$$\sum_{d|n} \mu(d) = 0, \tag{5.37}$$

para todo $n \in \mathbb{N}$.

(ii) Sean s y t dos aplicaciones de $\mathbb{N}$ sobre un grupo conmutativo notado aditivamente. Entonces

$$s(n) = \sum_{d|n} t(d) \iff t(n) = \sum_{d|n} \mu(d) s(\frac{n}{d}),$$

para todo $n \in \mathbb{N}$.

Demostración. (i). Tenemos que $\mu(1) = (-1)^0 = 1$. Por otro lado, sea $n \in \mathbb{N}$ tal que $n > 1$. Sea $P = \{p \in \mathbb{N} \,/\, p \text{ es primo, } p|n\}$ y sea $n = \prod_{p \in P} p^{d_p(n)}$, la descomposición de n en factores primos. Luego, si d es un divisor de n entonces $\mu(d) = 0$ salvo que $d = \prod_{p \in H} p$, donde H es un subconjunto de P. Por lo tanto,

$$\sum_{d|n} \mu(d) = \sum_{H \subset P} (-1)^{\mathrm{card}(H)} = \sum_{k=0}^{\mathrm{card}(P)} \left(\begin{array}{c} \mathrm{card}(P) \\ k \end{array} \right) (-1)^k = (1-1)^{\mathrm{card}(P)} = 0.$$

Para ver la unicidad supongamos que existe $\tau : \mathbb{N} \to \mathbb{Z}$ tal que $\tau(1) = 1$ y $\sum_{d|n} \tau(d) = 0$, para todo $n > 1$. Veamos por inducción que $\mu(n) = \tau(n)$, para todo $n \in \mathbb{N}$. Por definición $\mu(1) = \tau(1)$. Supongamos ahora que existe $k \in \mathbb{N}$ tal que para todo $j \leq k$ se cumple que $\mu(j) = \tau(j)$. Luego, como

$$\sum_{d|k+1} \mu(d) = 0 = \sum_{d|k+1} \tau(d),$$

se tiene que

$$0 = \sum_{d|k+1, d \neq k+1} (\mu(d) - \tau(d)) + \mu(k+1) - \tau(k+1) = \mu(k+1) - \tau(k+1),$$

como queríamos mostrar.

(ii). Supongamos que $s(n) = \sum_{d|n} t(d)$. Luego,

$$\sum_{d|n} \mu(d)s(\frac{n}{d}) = \sum_{d|n} \mu(d) \sum_{\delta|\frac{n}{d}} t(\delta) = \sum_{d|n} \sum_{\delta|\frac{n}{d}} \mu(d)t(\delta) =$$
$$= \sum_{d\delta|n} \mu(d)t(\delta) = \sum_{\delta|n} t(\delta) \sum_{d|\frac{n}{\delta}} \mu(d) = t(n),$$

ya que si $\frac{n}{\delta} \neq 1$ entonces $\sum_{d|\frac{n}{\delta}} \mu(d) = 0$, por (5.37).

Recíprocamente, si $t(n) = \sum_{d|n} \mu(d)s(\frac{n}{d})$ entonces

$$\sum_{d|n} t(d) = \sum_{d|n} \sum_{\delta|d} \mu(\delta)s(\frac{d}{\delta}) = \sum_{d|n} s(d) \sum_{\delta|\frac{n}{d}} \mu(\delta) =$$
$$= s(n),$$

pues si $\frac{n}{d} \neq 1$ entonces $\sum_{\delta|\frac{n}{d}} \mu(\delta) = 0$, por (5.37). Con esto finaliza la prueba. □

Observación 5.38. Si $I_p(n)$ denota el número de polinomios mónicos irreducibles en $\mathbb{F}_p[X]$ de grado n entonces

$$I(n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d,$$

donde μ es la función de Möbius.

Demostración. Sabemos que $p^n = \sum_{d|n} dI_p(d)$ es la cantidad de polinomios mónicos en $\mathbb{F}_p[X]$ de grado n. Luego, considerando las funciones $s, t : \mathbb{N} \to \mathbb{R}$ dadas por

$$s(n) = p^n,$$
$$t(n) = nI_p(n),$$

se tiene que $s(n) = \sum_{d|n} t(d)$. Por Proposición 5.36 (ii) obtenemos que

$$nI_p(n) = \sum_{d|n} \mu(d)p^{\frac{n}{d}} = \sum_{\delta|n} \mu(\frac{n}{\delta})p^{\delta}.$$

Por lo tanto,

$$I_p(n) = \frac{1}{n} \sum_{d|n} \mu(\frac{n}{d})p^d,$$

como queríamos mostrar. □

Una consecuencia importante de esto es la siguiente: si p es un número primo entonces, por Corolario 5.32 (b), se tiene que

(1) existen $p - 2$ conjuntos cruzados simples con p elementos, esto es la cantidad de polinomios mónicos irreducibles en $\mathbb{F}_p[X]$ distintos de X y $X - 1$.

(2) existen $I_p(n)$ conjuntos cruzados simples con p^n elementos, donde $n \neq 1$.

6. Ecuación cuántica de Yang-Baxter.

6.1. El grupo de Trenzas.

Sabemos que el grupo simétrico $\mathbb{S}_n$, $n \in \mathbb{N}$, podemos definirlo a través de generadores y relaciones de la siguiente manera

$$\mathbb{S}_n \simeq F/N,$$

donde F es el grupo libre sobre el conjunto de las transposiciones $\{\sigma_1, \ldots, \sigma_{n-1}\}$, con $\sigma_i = (i, i+1)$, y N es el subgrupo normal de F generado por las siguientes relaciones

(L) Local	$\sigma_i\sigma_j = \sigma_j\sigma_i,$	si $\lvert i-j\rvert \geq 2$
(T) Trenza	$\sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j,$	si $\lvert i-j\rvert = 1$
(I) Idempotencia	$\sigma_i^2 = \mathrm{id},$	para todo i,

(ver [Bou]).

De manera análoga, podemos definir el *grupo de trenzas* $\mathbb{B}_n$ como

$$\mathbb{B}_n := F/M$$

donde F es el grupo libre sobre un conjunto de generadores $\{s_1, \ldots, s_{n-1}\}$ y M es el subgrupo normal generado por

(L)	$s_is_j = s_js_i,$	si $\lvert i-j\rvert \geq 2,$
(T)	$s_is_js_i = s_js_is_j,$	si $\lvert i-j\rvert = 1$.

Claramente, se tiene un epimorfismo canónico

$$\rho_n : \mathbb{B}_n \to \mathbb{S}_n \quad \text{dado por} \quad \rho_n(s_i) := \sigma_i.$$

Además notamos que $\mathrm{card}(\mathbb{S}_n) = n!$ mientras que $\mathrm{card}(\mathbb{B}_n) = \infty$.

Definición 6.1. Sea V un espacio vectorial y sea $c \in \mathrm{Aut}(V \otimes V)$. Se dice que c satisface la *ecuación de trenzas* si vale la siguiente igualdad de morfismos de $V \otimes V \otimes V$ en sí mismo

$$(c \otimes \mathrm{id})(\mathrm{id} \otimes c)(c \otimes \mathrm{id}) = (\mathrm{id} \otimes c)(c \otimes \mathrm{id})(\mathrm{id} \otimes c). \tag{6.2}$$

Observación 6.3. Sea $c : V \otimes V \to V \otimes V$ isomorfismo y tomemos un entero $n \geq 2$. Definimos $c_i \in \mathrm{Aut}(V^{\otimes n})$ dado por

$$c_i := \mathrm{id}_{V^{\otimes(i-1)}} \otimes c \otimes \mathrm{id}_{V^{\otimes(n-i-1)}},$$

para cada i. Afirmamos que c satisface (6.2) si y sólo si la función $\varphi : \mathbb{B}_n \to \mathrm{GL}(V^{\otimes n})$ dada por $\varphi(s_i) := c_i$ define una representación.

Definición 6.4. Sea X un conjunto no vacío y $S : X \times X \to X \times X$ una biyección. Se dice que S satisface la ecuación de trenzas *conjuntista* si

$$(S \times \mathrm{id})(\mathrm{id} \times S)(S \times \mathrm{id}) = (\mathrm{id} \times S)(S \times \mathrm{id})(\mathrm{id} \times S), \tag{6.5}$$

como funciones de $X \times X \times X$ en sí mismo.

Al par (X, S) se lo llama un *conjunto trenzado* mientras que a S se la llama una *solución conjuntista* de la ecuación de trenzas o, brevemente, una *solución*.

Ejemplo 6.6. Sea $\tau : X \times X \to X \times X$ la transposición $\tau(x, y) = (y, x)$. Entonces, aplicando solamente las definiciones, se obtiene que τ es una solución de (6.5).

Observación 6.7. Sea X un conjunto no vacío, k un cuerpo y $V := kX$ (el espacio vectorial de base $(x)_{x \in X}$). Sea $S : X \times X \to X \times X$ una biyección con $S(x, y) = (S_1(x, y), S_2(x, y))$ y $S_1, S_2 : X \times X \to X$, y consideremos $c : V \otimes V \to V \otimes V$ donde

$$c(x \otimes y) = S_1(x, y) \otimes S_2(x, y).$$

Entonces resulta sencillo mostrar, por computación directa, que

$$S \text{ es solución de (6.5) y sólo si } c \text{ es solución de (6.2) .}$$

Observación 6.8. Sea X un conjunto no vacío y $S : X \times X \to X \times X$. Entonces si (X, S) es un conjunto trenzado se tienen morfismos de grupos $\rho_n : \mathbb{B}_n \to \mathbb{S}_{X^n}$ donde

$$\rho_n(s_i) = \mathrm{id}_{X^{i-1}} \times S \times \mathrm{id}_{X^{n-i-1}} =: S^{i,\ i+i}.$$

6.2. La ecuación cuántica de Yang-Baxter (QYBE).

Definición 6.9. Sea X un conjunto no vacío y $R : X \times X \to X \times X$ una biyección. Se dice que R satisface la QYBE conjuntista si

$$R^{12} R^{13} R^{23} = R^{23} R^{13} R^{12} \tag{6.10}$$

como funciones de $X \times X \times X$ en sí mismo, donde

$$\begin{aligned} R^{12}(x, y, z) &= (R(x, y), z) \\ R^{23}(x, y, z) &= (x, R(y, z)) \\ R^{13}(x, y, z) &= (R_1(x, z), y, R_2(x, z)) \end{aligned}$$

para todo $x, y, z \in X$ y donde $R(u, v) = (R_1(u, v), R_2(u, v))$.

Proposición 6.11. *Sea X un conjunto no vacío, $S : X \times X \to X \times X$ una biyección y τ la transposición del Ejemplo 6.6. Entonces S es una solución de la ecuación de trenzas conjuntista si y sólo si $R = \tau S$ es una solución de QYBE conjuntista.*

Demostración. Por cálculo directo. □

Observación 6.12. Si (X, S) es un conjunto trenzado existe una acción del grupo de trenzas $\mathbb{B}_n$ sobre X^n, donde los generadores s_i actúan por $S^{i,\ i+i}$.

En particular, un conjunto trenzado finito origina cocientes finitos de $\mathbb{B}_n$ para todo n, a saber, la imagen del homomorfismo de grupo $\rho_n : \mathbb{B}_n \to \mathbb{S}_{X^n}$ inducida por la acción anterior.

Finalizamos el trabajo caracterizando a las soluciones de la ecuación de trenzas conjuntista a partir de los racks.

Teorema 6.13 (Brieskorn)**.** *Sea X un conjunto no vacío y sea $\triangleright : X \times X \to X$ una función. Consideramos*

$$c : X \times X \to X \times X, \qquad c(x, y) := (x \triangleright y, x). \tag{6.14}$$

Entonces, c es una solución si y sólo si $(X, \triangleright)$ es un rack.

Demostración. Supongamos que c es una solución. Para $x \in X$, definimos $\phi_x : X \to X$ dada por $\phi_x(y) := x \triangleright y$. Luego, ϕ_x es biyectiva pues

(i) si $\phi_x(y) = \phi_x(y')$ entonces $x \triangleright y = x \triangleright y'$, lo que implica que $c(x, y) = c(x, y')$. Como c es biyectiva se tiene que $y = y'$.

(ii) si $z \in X$ entonces existe $y \in X$ tal que $c(x, y) = (z, x)$. Esto nos dice que $z = \phi_x(y)$.

Por otro lado, como c es solución entonces

$$(c \times \mathrm{id})(\mathrm{id} \times c)(c \times \mathrm{id})(x, y, z) = (\mathrm{id} \times c)(c \times \mathrm{id})(\mathrm{id} \times c)(x, y, z), \tag{6.15}$$

para todo $x, y, z \in X$. Efectuando la evaluación se tiene que la expresión (6.15) es equivalente a

$$x \triangleright (y \triangleright z) = (x \triangleright y) \triangleright (x \triangleright z).$$

Con esto se ve que $(X, \triangleright)$ es un rack.

La recíproca es obvia. □

Definición 6.16. Sean X, $\widetilde{X}$ dos conjuntos no vacíos y sean $S : X \times X \to X \times X$ y $\widetilde{S} : \widetilde{X} \times \widetilde{X} \to \widetilde{X} \times \widetilde{X}$ dos biyecciones. Se dice que (X, S) y $(\widetilde{X}, \widetilde{S})$ son *equivalentes* si existe una familia de biyecciones $T^n : X^n \to \widetilde{X}^n$ tales que

$$T^n S^{i,\ i+1} = \widetilde{S}^{i,\ i+1} T^n,$$

para todo $n \geq 2$, $1 \leq i \leq n - 1$.

Observación 6.17. Si (X, S) y $(\widetilde{X}, \widetilde{S})$ son equivalentes y (X, S) es una solución entonces $(\widetilde{X}, \widetilde{S})$ es también una solución y las biyecciones T^n entrelazan las correspondientes acciones del grupo de trenzas.

Demostración. Como (X, S) y $(\widetilde{X}, \widetilde{S})$ son equivalentes entonces existe una biyección $T^3 : X^3 \to \widetilde{X}^3$ tal que $T^3 S^{i,\ i+1} = \widetilde{S}^{i,\ i+1} T^3$, para $i = 1, 2$. Dado que S es solución se tiene que

$$S^{1,2} S^{2,3} S^{1,2} = S^{2,3} S^{1,2} S^{2,3}.$$

Aplicando T^3 a esta última igualdad obtenemos

$$\widetilde{S}^{1,2} \widetilde{S}^{2,3} \widetilde{S}^{1,2} T^3 = \widetilde{S}^{2,3} \widetilde{S}^{1,2} \widetilde{S}^{2,3} T^3,$$

lo que implica que

$$\widetilde{S}^{1,2} \widetilde{S}^{2,3} \widetilde{S}^{1,2} = \widetilde{S}^{2,3} \widetilde{S}^{1,2} \widetilde{S}^{2,3}.$$

Por lo tanto, $(\widetilde{X}, \widetilde{S})$ es una solución. □

Definición 6.18. Sea (X, S) una solución y sean $f, g : X \to \mathrm{Fun}(X, X)$ tales que

$$S(x, y) = (g_x(y), f_y(x)). \tag{6.19}$$

Se dice que la solución S (o el conjunto trenzado (X, S)) es *no degenerada* si las imágenes de f y g están dentro de $\mathbb{S}_X$.

Teorema 6.20. *[So, LYZ1] Sea S una solución no degenerada, con la notación de 6.18, y definamos $\triangleright$ por*

$$x \triangleright y := f_x \left(g_{f_y^{-1}(x)}(y) \right). \tag{6.21}$$

Entonces:

(1) se cumple que

$$f_x f_y = f_{f_x(y)} f_{g_y(x)}, \qquad \forall x, y \in X. \tag{6.22}$$

$$f \text{ preserva } \triangleright, \text{ i.e. } f_x(y \triangleright z) = f_x(y) \triangleright f_x(z); \tag{6.23}$$

(2) Si c está dada por (6.13) *entonces c es una solución, que llamamos* solución derivada *de S. Las soluciones S y c son equivalentes, y $(X, \triangleright)$ es un rack.*

(3) Sea $(X, \triangleright)$ un rack y sea $f : X \to \mathbb{S}_X$. Definimos $g : X \to \mathbb{S}_X$ por

$$g_x(y) = f^{-1}_{f_y(x)}(f_y(x) \triangleright y). \tag{6.24}$$

Sea $S : X \times X \to X \times X$ dada por (6.19)*. Entonces S es una solución si y sólo si se satisface* (6.22) *y* (6.23)*. Si esto sucede, las soluciones S y c son equivalentes, y S es no degenerada.*

Demostración. (1). Como S es solución tenemos que

$$(S \times \mathrm{id})(\mathrm{id} \times S)(S \times \mathrm{id})(x, y, z) = (\mathrm{id} \times S)(S \times \mathrm{id})(\mathrm{id} \times S)(x, y, z),$$

para todo $x, y, z \in X$. Efectuando la evaluación se tiene que la expresión anterior es equivalente a

$$f_z f_y(x) = f_{f_z(y)} f_{g_y(z)}(x), \tag{6.25}$$
$$g_x g_y(z) = g_{g_x(y)} g_{f_y(x)}(z), \tag{6.26}$$
$$f_{g_{f_y(x)}(z)} g_x(y) = g_{f_{g_y(z)}(x)} f_z(y), \tag{6.27}$$

para todo $x, y, z \in X$.

(i). Por (6.25) se tiene que $f_x f_y = f_{f_x(y)} f_{g_y(x)}$, para todo $x, y, z \in X$.

(ii). Sean $x, y, z \in X$. Luego,

$$f_x(y \triangleright z) = f_x f_y g_{f_z^{-1}(y)}(z) = f_{f_x(y)} f_{g_y(x)} g_{f_z^{-1}(y)}(z).$$

Por otro lado,

$$f_x(y) \triangleright f_x(z) = f_{f_x(y)} g_{f_{f_x(z)}^{-1}(f_x(y))} f_x(z).$$

Como S es no degenerada se tiene que $f_{f_x(y)} \in \mathbb{S}_X$. Por lo tanto, $f_x(y \triangleright z) = f_x(y) \triangleright f_x(z)$ si y sólo si

$$f_{g_y(x)} g_{f_z^{-1}(y)}(z) = g_{f_{f_x(z)}^{-1}(f_x(y))} f_x(z). \tag{6.28}$$

Eligiendo adecuadamente los elementos x, y, z en (6.27) el miembro de la izquierda de la igualdad anterior es

$$g_{f_{g_z(x)}(f_z^{-1}(y))} f_x(z).$$

Luego, (6.28) es cierta si y sólo si vale la siguiente igualdad

$$f_{g_z(x)} f_z^{-1}(y) = f_{f_x(z)}^{-1} f_x(y). \tag{6.29}$$

Por (i) tenemos que $f_u f_v = f_{f_u(v)} f_{g_v(u)}$, para todo $u, v \in X$. Entonces

$$f_{f_u(v)}^{-1} f_u = f_{g_v(u)} f_v^{-1},$$

para todo $u, v \in X$. Eligiendo $u = x$ y $v = z$ se tiene que (6.29) es cierta. Luego, vale (6.28), y f preserva $\triangleright$ como queríamos probar.

(2). Es suficiente mostrar que S y c son equivalentes; automáticamente, c es solución y, por lo tanto, $(X, \triangleright)$ es un rack.

Sea c dada por (6.14). Definimos $Q : X \times X \to X \times X$,

$$Q(x, y) := (f_y(x), y).$$

Es fácil verificar que Q es biyectiva. Además,

$$\begin{aligned} QS(x,y) &= Q(g_x(y), f_y(x)) = (f_{f_y(x)}(g_x(y)), f_y(x)) = (f_{f_y(x)}(g_{f_y^{-1}(f_y(x))}(y)), f_y(x)) = \\ &= (f_y(x) \triangleright y, f_y(x)) = c(f_y(x), y) = cQ(x,y), \end{aligned}$$

para todo $x, y \in X$. Luego, $c = QSQ^{-1}$ y c es una biyección.

Ahora bien, sean $T^n : X^n \to X^n$ definidas inductivamente por

$$T^2 := Q, \qquad T^{n+1} := Q_n(T^n \times \mathrm{id}),$$

donde $Q_n(x_1, \dots, x_{n+1}) := (f_{x_{n+1}}(x_1), \dots, f_{x_{n+1}}(x_n), x_{n+1})$. Resulta sencillo mostrar que $Q_n : X^{n+1} \to X^{n+1}$ es una biyección, para todo $n \geq 1$. Además, si T^k es biyectiva entonces $T^k \times \mathrm{id}$ es biyectiva. Por lo tanto, las funciones T^n son biyecciones.

Veamos ahora que

$$T^n S^{i,\ i+1} = c^{i,\ i+1} T^n,$$

para todo $n \geq 1$, $1 \leq i \leq n-1$. Si $n = 2$ dicha igualdad ya está probada. Supongamos que la afirmación vale para un cierto $n > 2$; vamos a ver que la afirmación es válida para $n+1$.

(i). Sea i tal que $1 \leq i \leq n-1$. Entonces

$$\begin{aligned} Q_n c^{i,\ i+1}(x_1, \dots, x_{n+1}) &= Q_n(x_1, \dots, c(x_i, x_{i+1}), \dots, x_{n+1}) = \\ &= (f_{x_{n+1}}(x_1), \dots, f_{x_{n+1}}(x_i \triangleright x_{i+1}), \dots, f_{x_{n+1}}(x_n), x_{n+1}). \end{aligned}$$

Por otro lado,

$$\begin{aligned} c^{i,\ i+1} Q_n(x_1, \dots, x_{n+1}) &= c^{i,\ i+1}(f_{x_{n+1}}(x_1), \dots, f_{x_{n+1}}(x_n), x_{n+1}) = \\ &= (f_{x_{n+1}}(x_1), \dots, c(f_{x_{n+1}}(x_i), f_{x_{n+1}}(x_{i+1})), \dots, f_{x_{n+1}}(x_n), x_{n+1}) = \\ &= (f_{x_{n+1}}(x_1), \dots, f_{x_{n+1}}(x_i) \triangleright f_{x_{n+1}}(x_{i+1})), f_{x_{n+1}}(x_i), \dots, f_{x_{n+1}}(x_n), x_{n+1}). \end{aligned}$$

Luego, por (6.23) se tiene que

$$Q_n c^{i,\ i+1} = c^{i,\ i+1} Q_n.$$

Usando la igualdad anterior podemos escribir

$$\begin{aligned} T^{n+1} S^{i,\ i+1} &= Q_n(T^n \times \mathrm{id}) S^{i,\ i+1} = Q_n(T^n S^{i,\ i+1} \times \mathrm{id}) = Q_n(c^{i,\ i+1} T^n \times \mathrm{id}) = \\ &= Q_n c^{i,\ i+1}(T^n \times \mathrm{id}) = c^{i,\ i+1} Q_n(T^n \times \mathrm{id}) = c^{i,\ i+1} T^{n+1}. \end{aligned}$$

(ii). Sea $i = n$. Notamos que se puede ver por inducción que

$$\begin{aligned} T^{n+1}(x_1, \dots, x_{n+1}) = (&f_{x_{n+1}} f_{x_n} \dots f_{x_2}(x_1), f_{x_{n+1}} f_{x_n} \dots f_{x_3}(x_2), \dots, f_{x_{n+1}} f_{x_n}(x_{n-1}), \\ &, f_{x_{n+1}}(x_n), x_{n+1}). \end{aligned}$$

Por la igualdad anterior podemos escribir

$$\begin{aligned}T^{n+1}S^{n,\ n+1}(x_1,\ldots,x_{n+1}) &= T^{n+1}(x_1,\ldots,x_{n-1},S(x_n,x_{n+1})) = \\ &= T^{n+1}(x_1,\ldots,x_{n-1},g_{x_n}(x_{n+1}),f_{x_{n+1}}(x_n)) = \\ &= (f_{f_{x_{n+1}}(x_n)}f_{g_{x_n}(x_{n+1})}f_{x_{n-1}}\ldots f_{x_2}(x_1),\ldots,f_{f_{x_{n+1}}(x_n)}f_{g_{x_n}(x_{n+1})}(x_{n-1}),\\ &\quad ,f_{f_{x_{n+1}}(x_n)}(g_{x_n}(x_{n+1})),f_{x_{n+1}}(x_n)).\end{aligned}$$

Por (6.22) tenemos que $f_{f_{x_{n+1}}(x_n)}f_{g_{x_n}(x_{n+1})} = f_{x_{n+1}}f_{x_n}$. Entonces

$$\begin{aligned}T^{n+1}S^{n,\ n+1}(x_1,\ldots,x_{n+1}) &= (f_{x_{n+1}}f_{x_n}f_{x_{n-1}}\ldots f_{x_2}(x_1),\ldots,f_{x_{n+1}}f_{x_n}(x_{n-1}),\\ &\quad ,f_{x_{n+1}}(x_n)\triangleright x_{n+1},f_{x_{n+1}}(x_n)) = \\ &= (f_{x_{n+1}}f_{x_n}f_{x_{n-1}}\ldots f_{x_2}(x_1),\ldots,f_{x_{n+1}}f_{x_n}(x_{n-1}),c(f_{x_{n+1}}(x_n),x_{n+1})) = \\ &= c^{n,\ n+1}(f_{x_{n+1}}f_{x_n}f_{x_{n-1}}\ldots f_{x_2}(x_1),\ldots,f_{x_{n+1}}f_{x_n}(x_{n-1}),f_{x_{n+1}}(x_n),x_{n+1}) = \\ &= c^{n,\ n+1}T^n(x_1,\ldots,x_{n+1}).\end{aligned}$$

De esta manera, hemos visto que S y c son equivalentes. Como S es solución se tiene que, por Observación 6.17, c es solución; y por Teorema 6.13, $(X,\triangleright)$ es un rack.

(3). Dado que

$$g_x(y) = f^{-1}_{f_y(x)}\phi_{f_y(x)}(y),$$

se tiene que $g_x \in \mathbb{S}_X$, para todo $x \in X$, o sea $g : X \to \mathbb{S}_X$ está bien definida.

Ahora bien, supongamos que S es solución. Luego, S es no degenerada y es fácil ver que el $\triangleright$ definido por (6.21) coincide con el $\triangleright$ en X. Por lo tanto, por (1) se satisfacen (6.22) y (6.23).

Recíprocamente, supongamos que se satisfacen (6.22) y (6.23). Veamos que S es solución. En primer lugar, S es biyectiva ya que

(a) si $S(x,y) = S(x',y')$ entonces $(g_x(y),f_y(x)) = (g_{x'}(y'),f_{y'}(x'))$. La igualdad en la primer componente nos dice que

$$f^{-1}_{f_y(x)}\phi_{f_y(x)}(y) = f^{-1}_{f_{y'}(x')}\phi_{f_{y'}(x')}(y'),$$

lo que implica que $y = y'$, y por ende, $x = x'$.

(b) Sea $(x,y) \in X \times X$. Luego, es fácil verificar que

$$(x,y) = S(f^{-1}_{y^{-1}\triangleright f_y(x)}(y),y^{-1}\triangleright f_y(x)).$$

Por otro lado, si consideramos $c : X \times X \to X \times X$, como en (6.14), se tiene que c es solución. Pero, por (2), sabemos que c y S son equivalentes y, por lo tanto, S es solución. Más aún, S es no degenerada. Con esto finalizamos la prueba. □

Referencias

[AG] N. Andruskiewitsch y M. Graña, *From racks to pointed Hopf algebras*. Advances in Mathematics, por aparecer.

[B] E. Brieskorn, *Automorphic sets and singularities*, Contemp. Math. **78** (1988), 45–115.

[Bou] N. Bourbaki, *Eléments de Mathématique, Groupes et Algèbres de Lie: Chapitres 4, 5 et 6*, Actualités scientifiques et industrielles **1337**, Hermann, Paris (1968).

[Dr] V. G. Drinfeld , *On some unsolved problems in quantum group theory*, in Quantum groups (Leningrad, 1990), Lecture Notes in Math. **1510**, Springer, Berlin, (1992), 1–8.

[EGS] P. Etingof, R. Guralnik y A. Soloviev, *Indecomposable set-theoretical solutions to the Quantum Yang–Baxter Equation on a set with prime number of elements*, J. Algebra **242** (2001), 709-719.

[ESS] P. Etingof, T. Schedler y A. Soloviev, *Set-theoretical solutions to the Quantum Yang–Baxter Equation*, Duke Math. J. **100** (1999), 169–209.

[FR] R. Fenn y C. Rourke, *Racks and links in codimension two*, J. of Knot Th. and Its Ramifications **1**, 4 (1992), 343-406.

[G] M. Graña, *Indecomposable racks of order p^2*, `math.QA/0203157`

[H] T. W. Hungerford, *Algebra*, Springer-Berlag, New York (1974).

[J1] D. Joyce, *A Classifying Invariant of Knots, The Knot Quandle*, J. Pure Appl. Alg. **23** (1982), 37–65.

[J2] D. Joyce, *Simples quandles*, J. Algebra **79** 2 (1982), 307–318.

[LYZ1] Jiang-Hua Lu, Min Yan & Yong-Chang Zhu, *On Set-theoretical Yang–Baxter equation*, Duke Math. J. **104** (2000), pp. 1–18.

[Ne] S. Nelson, *Classification of finite Alexander quandles*, `math.GT/0202281`.

[So] A. Soloviev, *Non-unitary set-theoretical solutions to the quantum Yang–Baxter equation*, `math.QA/0202281`.