Rewriting Group Products with Transversals

Gabriel Zapata

Abstract

For any group G with subgroup H and a set of representatives T from the set of cosets G/H, we develop a rewriting system from G that bequeaths a product into the set decomposition $T \times H$ of G, converting it into a group. In return the rewriting system also describes any product between elements in G in terms of elements from T and H, while we gain a new universal group-isomorphism between G and $T \times H$. From this framework we develop the concept of Diffracted Groups.

1   Introduction

Let H be a subgroup of a group G and T be a set of *representatives* from the set of cosets G/H. The set T, under the product of G, is generally a semigroup and not a group. Therefore, our objective is to develop a rewriting process in G bequeathing a group product for the set $T \times H$, which is bijective to G, cf. [7] chapter III. From the rewriting process we also demonstrate how the bijection between $T \times H$ and G lifts to a universal group-isomorphism.

To formally design the rewriting process, we begin by defining Set and Grp to be the small category of sets and groups, respectively. Given any objects H and G from $\mathsf{C} \in \{\mathsf{Set}, \mathsf{Grp}\}$, we write $\mathrm{Hom}_{\mathsf{C}}(H, G)$ to denote the set of morphisms from H to G. We also let S_H be the group of permutation (or, the symmetric group) with underlying set H. We can then express the well-known, natural set-isomorphism

$$\mathrm{Hom}_{\mathsf{Grp}}(G, \mathrm{S}_H) \;\cong\; \mathrm{Hom}_{\mathsf{Set}}(G \times H, H) \tag{1}$$

between *group-representations* and *group-actions* on H. This bridge will allow us to transverse between G's local "representative" structure and its global "bundle" action on H. Moreover, while also using the basic but powerful *Cayley's representation*, we will go from the internal multiplicative structure of G to the set-theoretic decomposition $T \times H$ with respect to a subgroup H and its representatives T of G/H. We will then develop a representation of G bequeathing a multiplicative rewriting process for group elements in the decomposition $T \times H$:

Definition 1 The *Cayley's representation* is the monomorphism defined as

$$\varrho : G \longrightarrow \mathrm{S}_G \quad \text{such that} \quad \forall_{g,h\, \in\, G} \;\; \big[\;\; \varrho : g \longmapsto \big(\, g^\varrho : h \longrightarrow gh \, \big) \;\; \big], \tag{2}$$

where the element $g^\varrho \in \mathrm{S}_G$ symbolizes the image of g under ϱ.

To be more precise, Cayley's representation $\varrho \in \mathrm{Hom}_{\mathsf{Grp}}(G, \mathrm{S}_G)$ shows us a decomposition of the product of G by way of its associated (left) action $\hat{\varrho} \in \mathrm{Hom}_{\mathsf{Set}}(G \times G, G)$, i.e., via the commutative diagram

$$
\begin{array}{ccc}
G \times G & \xrightarrow{\text{``}\bullet\text{''}} & G \\
{\scriptstyle \mathbb{1}_G \times \mathbb{1}_G} \big\downarrow & & \big\uparrow {\scriptstyle \mathbb{1}_G} \\
G \times G & \xrightarrow{\hat{\varrho}} & G,
\end{array}
\tag{3}
$$

where "$\bullet$" and $\mathbb{1}_G$ denote the multiplicative operation and the identity automorphism of G, respectively. In the following sections, we develop representations that engender the replacement of the pair $G \times G$, from Cayley's action $\hat{\varrho}$, by the pair $(T \times H) \times (T \times H)$. From the latter decomposition we will obtain a rewriting process describing the product of elements from G in terms of elements from T and H. This rewriting process will also endow a multiplicative group structure for the set $T \times H$, and it will induce a universal group-isomorphism between G and the group structure developed for $T \times H$.

2 The Frobenius Representation

This section reviews a method that offers an intuitive path for describing a decomposition of G—a codification using a subgroup H and G/H.

Definition 2 Given a group G with $H \leq G$ and its set of left cosets G/H, let

$$
\Lambda \; := \; \{\, \tau : G/H \longrightarrow \bigcup_{g \in G} (gH) \mid \forall_{g \in G} \; [\, \tau(gH) \in gH \,] \,\}.
\tag{4}
$$

A set of (left) *representatives* T of G/H is the image of a coordinate $\tau \in \Lambda$, i.e., $T := \mathrm{Im}\,\tau$. Moreover, a set of representatives T is termed a *transversal* if the identity element $1 \in G$ is also in T.

Intuitively, a set of representatives T consists of one chosen element from each coset of G/H. The didactic definition is not an accident, it is suitable for visualizing and extrapolating crucial representative properties: each coordinate point $\tau \in \Lambda$ contains a codification of G, modulo H. Given τ and the canonical projection $p : G \longrightarrow G/H$, there is a unique map $\bar{\tau} : G \longrightarrow T$ such that the following diagrams

$$
\begin{array}{ccc}
G & \xdashrightarrow{\;\bar{\tau}\;} & T \\
& {\scriptstyle p} \searrow \quad \big\uparrow {\scriptstyle \tau} & \\
& G/H &
\end{array}
\quad , \text{ i.e.,} \quad
\begin{array}{ccc}
g & \xdashmapsto{\;\bar{\tau}\;} & \tau(\,g\,H\,) \\
& {\scriptstyle p} \nwarrow \quad \big\uparrow {\scriptstyle \tau} & \\
& g\,H &
\end{array}
$$

commute, for any $g \in G$. In particular $\bar{\tau} : G \longrightarrow T$ systematically maps G onto T (cf. [5] classical construction.)

2

Definition 3 Let $p : G \longrightarrow G/H$ be a canonical projection and $\tau \in \Lambda$. Given its set of representatives T of G/N, a *representative map* is the map

$$\bar{\tau} : G \longrightarrow T \quad \text{such that} \quad \forall_{g \in G} \left[\ g \xmapsto{\bar{\tau}} \bar{g} := \tau(gH)\ \right].$$

Moreover any element of the form $\bar{g} \in T$ is termed a *representative of g* (from gH.)

Lemma 1 *If T is a set of representatives of G/H of G, then*

i. $\quad \forall_{g \in G} \left[\ g\,H = \bar{g}\,H\ \right]$

ii. $\quad \forall_{g_1, g_2 \in G} \left[\ \overline{g_1\overline{g_2}} = \overline{g_1\,g_2}\ \right]$

Proof: Let T be a set of representative of G/H and τ a map of its representatives.

i. Given $g \in G$, then $gH = \bar{g}\,H$ since its representative $\bar{g}$ satisfies

$$g \in \bar{g}\,H \iff \exists!_{h \in H} \left[\ \bar{g} = g\,h^{-1}\ \right] \iff \bar{g} \in gH.$$

ii. By the above argument $g_2 H = \overline{g_2}H$ for any $g_2 \in G$. Then $g_1 g_2\,H = g_1\overline{g_2}\,H$ for any $g_1 \in G$. Therefore $\overline{g_1\overline{g_2}} = \overline{g_1 g_2}$ since $\bar{\tau}$ is well defined. $\qquad\qquad\square$

Definition 4 Given a set of representatives T of G/H, the *Frobenius representation* is the representation

$$\gamma : G \longrightarrow S_T \quad \text{definied as} \quad \forall_{g \in G}\ \forall_{t \in T} \left[\ g \longmapsto (\ g^\gamma : t \longmapsto \overline{g\,t}\ )\ \right]. \qquad (5)$$

To see that γ is a representation, let T be a set of representatives of G/H and g_1 and g_2 be elements of G. Then

$$(\,g_1 g_2\,)^\gamma(t) = \overline{g_1 g_2\,t} = \overline{g_1\overline{g_2\,t}} = \overline{g_1 g_2^\gamma(t)} = g_1^\gamma \circ g_2^\gamma(t),$$

which follows from lemma 1. Therefore $(\,g_1 g_2\,)^\gamma = g_1^\gamma \circ g_2^\gamma$. Last, if t is in T, then $\gamma : 1 \longmapsto 1^\gamma$ satisfies $1^\gamma(t) = \overline{1t} = \bar{t} = t$ by definition, i.e., $1^\gamma = 1$ is in S_T. cf. [3].

3   The Diffraction and T-Fibration Maps

The Frobenius representation is fruitful in many branches of group theory, yet for us, it will give us the pivotal tools used to derive the mechanisms essential for our rewriting process. To exploit it, we begin with the standard representative system T of G/H for G. Now any group G is bijective to $T \times H$:

$$G = \bigsqcup_{t \in T} tH \simeq_{\text{Set}} \bigsqcup_{t \in T} \{\,t\,\} \times H = T \times H.$$

Since, any $g \in G$, has a unique $t \in T$ so that $g \in tH$. And, if $g = t\,h$ and $t\,h = t\,h'$ for $h, h' \in H$, then $h' = h$. i.e., the map $g \longmapsto \langle t, h \rangle$ is a well-defined bijection. For additional details see [6].

Definition 5 Given a set of representatives T of G/H, the *diffraction map* of G by T is the set-isomorphism

$$\nabla : G \longrightarrow T \times H \quad \text{is defined by} \quad \nabla : g \longmapsto \langle t, h \rangle \tag{6}$$

If we think of the above bijection metaphorically, any element g from its source G can be witnessed with a "prism" T as having a unique "spectrum" $\langle t, h \rangle$ from its "diffraction" $T \times H$. Essentially, ∇ diffracts the group G into the set $T \times H$. Viewing G internally, through the bijection, any element $g \in G$ can also be uniquely decomposed as $g = th$, where $\langle t, h \rangle \in T \times H$.

The set of representatives T under the product of G is a sub-semigroup of G, and it is not a subgroup in general; this is why our goal is to "diffract" G as $T \times H$ such that it fosters a multiplicative group structure on itself. Therefore, to achieve this objective, consider the action $\hat{\varrho} \in \mathrm{Hom}_{\mathsf{Set}}(G \times G, G)$ restricted to T, induced by Cayley's representation ϱ (cf. Definition 1). Then, rewrite the action as

$$\hat{\varrho} : \langle g, t \rangle \longmapsto gt =: \overline{gt}\,(\overline{gt})^{-1}gt \tag{7}$$

for any of $g \in G$ and $t \in T$. In the left-hand side of assignment (7) we have rewritten the effect of Cayley's action over the pair $\langle g, t \rangle \in G \times T$ using the Frobenius representation. Notice that $\overline{gt} \in T$ by definition, and $(\overline{gt})^{-1}gt \in H$ because for any $t \in T$ and $g \in G$

$$\overline{1} = \overline{(\overline{gt})^{-1}(\overline{gt})} = \overline{(\overline{gt})^{-1}gt} \implies H = \overline{1}H = \overline{(\overline{gt})^{-1}gt}\,H = (\overline{gt})^{-1}gt\,H\,,$$

which follows from lemma 1. Hence, assignment (7) renders the following tool:

Definition 6 A *T-fibration* of G, for a representatives T of G/H, is the map

$$\delta : G \times T \longrightarrow H \quad \textit{defined by} \quad \forall_{\langle g, t \rangle \,\in G \times T} \left[\, \delta(g, t) := (\overline{gt})^{-1}g\,t \,\right].$$

A T-fibration δ is an abstract generalization of a fiber bundle, at its core. To see an analogous construction of δ, consult [1]. For us, δ will allow a canonical description of the diffraction set-isomorphism $\nabla : G \longrightarrow T \times H$.

Theorem 1 *If T is a transversal of G/H and $\delta : G \times T \longrightarrow H$ its T-fibration, then the diffraction map $\nabla : G \longrightarrow T \times H$ uniquely decomposes into the pair*
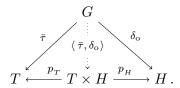
$$\nabla = \langle\, \bar{\tau}\,,\, \delta_{\mathrm{o}}\,\rangle \quad \textit{such that} \quad \forall_{g \,\in G} \left[\, \langle\, \bar{\tau}\,,\, \delta_{\mathrm{o}}\,\rangle\,(g) = \langle\, \bar{g}\,, (\bar{g})^{-1}g \rangle \,\right],$$

where δ_{o} is $\delta(-, 1) : G \longrightarrow H$, and $\bar{\tau}$ is the representative map (cf. definition 3).

Proof: Let $\delta : G \times T \longrightarrow H$ be the T-fibration of G/H and let $\nabla : G \longrightarrow T \times H$ be the diffraction map of G by T. If T is a transversal with $1 \in T$, Cayley's action for any $g \in G$ on the identity is just $\hat{\varrho}(g, 1) = g$. Then

$$\nabla(g) = \nabla \circ \hat{\varrho}\,(g, 1) = \langle \bar{g}, (\bar{g})^{-1}g \rangle = \langle\, \bar{\tau}(g), \delta(g, 1)\,\rangle = \langle \bar{\tau}, \delta_{\mathrm{o}} \rangle\,(g)\,,$$

4

where δ_o is $\delta(-,1) : G \longrightarrow H$. Now given the projection maps $p_H : T \times H \longrightarrow H$ and $p_T : T \times H \longrightarrow T$, the pair $\langle\, \bar{\tau}, \delta_o \,\rangle$ satisfies the commutative diagram

$$
\begin{array}{ccc}
 & G & \\
\bar{\tau} \swarrow & \downarrow {\scriptstyle \langle\, \bar{\tau}, \delta_o \,\rangle} & \searrow \delta_o \\
T \xleftarrow{\ p_T\ } & T \times H & \xrightarrow{\ p_H\ } H\,.
\end{array}
$$

Therefore ∇ is uniquely decomposable into the pair $\langle\, \bar{\tau}, \delta_o \,\rangle$ by uniqueness of the universal property of direct products. $\qquad\square$

4   The Diffraction Representation

In this penultimate section, we gather the tools we have built to describe a *faithful* representation from G into $\mathrm{S}_{T \times H}$, in exchange for Cayley's representation. Then, in the following last section, this representation will enable us to rewrite the product of G as a product in its canonical set $T \times H$ for a transversal T of G/H. We do this by first examining the general natural isomorphism

$$
\mathrm{Hom}_{\mathsf{set}}\,(G \times T, H\,) \cong \mathrm{Hom}_{\mathsf{Grp}}\,(G, H^T\,),
$$

where $H^T := \mathrm{Hom}_{\mathsf{set}}\,(T, H\,)$ is the group of maps from G to H^T under functional point-wise multiplication, i.e.

$$
\forall_{f_1, f_2\, \in H^T}\ \big[\ f_1 \cdot f_2\ := \{\, \langle\, t, f_1(t)\, f_2(t)\, \rangle\ \mid t \in T\, \}\ \big]. \tag{8}
$$

Notice the dual $\hat{\delta} \in \mathrm{Hom}_{\mathsf{set}}\,(G, H^T\,)$ of a T-fibration $\delta : G \times T \longrightarrow H$, from the set of maps $\mathrm{Hom}_{\mathsf{set}}\,(G \times T, H\,)$, is described as

$$
\hat{\delta} : G \longrightarrow\ H^T\ \ \text{such that}\ \ \ \forall_{g\, \in G}\, \forall_{t\, \in T}\ \Big[\ \hat{\delta} : g \longmapsto \big(\, \delta_g :\ t \longmapsto \delta(g,t)\, \big)\ \Big],
$$

where δ_g is the map $\delta(g,-) : T \longrightarrow H$ in H^T. Moreover, the group structure of the image $\hat{\delta}(G) := \{\, \delta_g \mid g \in G\, \}$, of the dual of δ acts on the partition $T \times H$ of G. In general, any $f \in H^T$ can act as a permutation on the cartesian set $T \times H$, e.g.

$$
\forall_{\langle t,h \rangle\, \in T \times H}\ \Big[\ f \curvearrowright \langle t, h \rangle := \langle\, t,\, f(t)\, h\, \rangle\ \Big]. \tag{9}
$$

Proposition 1 *Given the group $\hat{\delta}(G)$, from the image of the dual $\hat{\delta}$ of a T-fibration δ, the assignment $\beta : \hat{\delta}(G) \longrightarrow \mathrm{S}_{T \times H}$ defined as*

$$
\forall_{\delta_g\, \in\, \hat{\delta}(G)}\ \forall_{\langle t,h \rangle\, \in T \times H}\ \Big[\ \delta_g \xmapsto{\ \beta\ } \big(\, (\delta_g)^\beta :\langle t,h \rangle \longmapsto \langle\, t,\, \delta(g,t)\, h\, \rangle \big)\ \Big] \tag{10}
$$

is an injective permutation representation of $\hat{\delta}(G)$ into $\mathrm{S}_{T \times H}$.

Proof. The assignment $\beta : \hat{\delta}(G) \longrightarrow S_{T \times H}$ is a well-defined map by way of δ. Now let for any $\langle t, h \rangle \in T \times H$, by *a priori* $(\delta_1)^\beta \langle t, h \rangle = \langle t, \delta_1(t) h \rangle = \langle t, h \rangle$. Then β is a homomorphism since

$$\left(\delta_{g_1} \cdot \delta_{g_2}\right)^\beta \langle t, h \rangle = \langle t, \delta(g_1, t)\delta(g_2, t) h \rangle = \left(\delta_{g_1}\right)^\beta \langle t, \delta(g_2, t) h \rangle = \left(\delta_{g_1}\right)^\beta \circ \left(\delta_{g_2}\right)^\beta \langle t, h \rangle$$

for any $g_1, g_2 \in G$. To see that β is injective, let $\delta_g \in \mathrm{Ker}\,\beta$. Then

$$(\delta_g)^\beta \langle t, h \rangle = \langle t, h \rangle = \langle t, \delta(g, t)h \rangle. \tag{11}$$

Equation (11) above is satisfiable if and only if $\delta_g(t) = 1$, i.e., $g = 1$. Therefore β is an injective permutation representation of $\hat{\delta}(G)$ into $S_{T \times H}$. □

From proposition 1 it follows that the group structure of $\hat{\delta}(G)$ acts on the decomposition $T \times H$ of G. This result, along with the assistance of the Frobenius representation, grants us our sought out extension of Cayley's representation to our permutation representation of G into $S_{T \times H}$.

Definition 7 The *diffraction representation* of G, by a set of representatives T of G/H, is the assignment $\alpha : G \longrightarrow S_{T \times H}$ defined by

$$\forall_{g \in G} \forall_{\langle t,h \rangle \in T \times H} \left[g \xmapsto{\ \alpha\ } \left((g^\gamma \times \mathbb{1}_H) \circ (\delta_g)^\beta : \langle t, h \rangle \longmapsto \langle g^\gamma(t), \delta(g, t) h \rangle \right) \right],$$

where β is the permutation representation described in proposition 1.

Lemma 2 A T-fibration δ, for a set of representatives T of G/H, satisfies

$$\forall_{t \in T} \forall_{g_1, g_2 \in G} \left[\delta(g_1 g_2, t) = \delta\big(g_1, g_2^\gamma(t)\big) \delta(g_2, t) \right]$$

Proof: If $\delta : G \times T \longrightarrow H$ is the T-fibration associated to the representative T, then

$$\delta\big(g_1, g_2^\gamma(t)\big) \delta(g_2, t) = (\overline{g_1\,\overline{g_2\,t}})^{-1} g_1\,\overline{g_2\,t}\,(\overline{g_2\,t})^{-1} g_2\,t = (\overline{g_1 g_2\,t})^{-1} g_1 g_2\,t = \delta(g_1 g_2, t)$$

for any $g_1, g_2 \in G$ and $t \in T$, since $\overline{g t} := g^\gamma(t)$. □

Theorem 2 The diffraction representation $\alpha : G \longrightarrow S_{T \times H}$ is an injective permutation representation of G into $S_{T \times H}$.

Proof: Let $g \in G$ and $\langle t, h \rangle \in T \times H$. Then $(g^\gamma \times \mathbb{1}_H) \in S_{T \times H}$ since it acts as

$$\langle t, h \rangle \xmapsto{\ g^\gamma \times \mathbb{1}_H\ } \langle g^\gamma(t), h \rangle,$$

which is permutation induced by the Frobenius representation γ. From Proposition 1, the map $\delta_g \in \hat{\delta}(G)$ acts on the diffraction $T \times H$ as $(\delta_g)^\beta : \langle t, h \rangle \longmapsto \langle t, \delta(t, g) h \rangle$. Thus $(g^\gamma \times \mathbb{1}_H) \circ (\delta_g)^\beta \in S_{T \times H}$ is a permutation on the set $T \times H$ described as

$$(g^\gamma \times \mathbb{1}_H) \circ (\delta_g)^\beta : \langle t, h \rangle \longmapsto \langle g^\gamma(t), \delta(g, t) h \rangle.$$

6

Now the action of the identity $1 \in G$ induced by α on $\langle h, t \rangle$ is given as

$$\alpha(1)\,\langle t, h \rangle \;:=\; (1^\gamma \times \mathbb{1}_H) \circ (\delta_1)^\beta\,\langle t, h \rangle \;=\; \langle\, 1^\gamma(t)\,,\, \delta(1,t)\,h\,\rangle \;=\; \langle\, \bar{t}\,,\, (\bar{t})^{-1}\,t\,h\,\rangle \;=\; \langle t, h \rangle$$

since $\bar{t} = t$. Therefore $\alpha(1) = 1$ in $S_{T \times H}$. Moreover, given $g_1, g_2 \in G$, the action of g_2 followed by the action of g_1 on $\langle t, h \rangle$ by way of α is

$$\begin{aligned}
\alpha(g_1) \circ \alpha(g_2)\,\langle t, h \rangle \;&=\; \big((g_1^\gamma \times \mathbb{1}_H) \circ (\delta_{g_1})^\beta \big) \circ \big((g_2^\gamma \times \mathbb{1}_H) \circ (\delta_{g_2})^\beta \big)\,\langle t, h \rangle \\
&=\; \big((g_1^\gamma \times \mathbb{1}_H) \circ (\delta_{g_1})^\beta \big)\,\langle\, g_1^\gamma(t)\,,\, \delta(g_2, t)\,h\,\rangle \\
&=\; \langle\, g_1^\gamma \circ g_2^\gamma(t)\,,\, \delta(g_1\,,\, g_2^\gamma(t))\,\delta(g_2, t)\,h\,\rangle\,.
\end{aligned}$$

But $g_1^\gamma \circ g_2^\gamma(t) = (g_1\,g_2)^\gamma(t)$ and $\delta\big(g_1\,,\, g_2^\gamma(t)\big)\,\delta(g_2, t) = \delta(g_1\,g_2\,, t)$ by the Frobenius representation γ and lemma 2, respectively. Therefore, putting these together, we get

$$\begin{aligned}
\alpha(g_1) \circ \alpha(g_2)\,\langle t, h \rangle \;&=\; \langle\, (g_1 g_2)^\gamma(t)\,,\, \delta(g_1 g_2, t)\,h\,\rangle \;=\; \big((g_1 g_2)^\gamma \times \mathbb{1}_H \big) \circ (\delta_{g_1 g_2})^\beta\,\langle t, h \rangle \\
&=\; \alpha(g_1 g_2)\,\langle t, h \rangle\,,
\end{aligned}$$

i.e., $\alpha(g_1 g_2) = \alpha(g_1) \circ \alpha(g_2)$. Hence α is a representation of G into $S_{T \times H}$. Last, α is injective if $\langle\, g^\gamma(t)\,,\, \delta_g(t)\,h\,\rangle = \langle t, h \rangle$, i.e., $\overline{g t} = t$ and $\delta_g(t) = 1$ if and only if $g = 1$. Therefore, α is injective as well. $\qquad\square$

5 Rewriting in a Diffracted Group

Given a transversal set T of G/H for a group G, in this last section, we describe the group structure for the set $T \times H$ that emerges from the bijection of the diffraction map $\nabla : G \longrightarrow T \times H$ and its diffraction representation $\alpha : G \longrightarrow S_{T \times H}$. Moreover, we will also show that ∇ can be lifted to a universal group-isomorphism $G \simeq_{\mathsf{Grp}} T \times H$. We begin by applying a group-action isomorphism on sets, cf. [4].

Definition 8 Given a group G, the category G-Set of (left) *group actions of G on* Set consists of the following objects and morphisms:

- Objects in G-Set are pairs $\langle \hat{\varrho}, X \rangle$, where $X \in \mathsf{Set}$ and $\hat{\varrho} \in \mathrm{Hom}_{\mathsf{Set}}(G \times X, X)$ satisfy

i. $\forall_{x \in X}\ \big[\ \hat{\varrho}(1, x) = x\ \big]$

ii. $\forall_{g_1, g_2 \in G}\ \forall_{x \in X}\ \big[\ \hat{\varrho}(g_1 g_2, x) = \hat{\varrho}\big(g_1, \hat{\varrho}(g_2, x)\big)\ \big]$

We refer to objects $\langle \hat{\varrho}, X \rangle$ from G-Set as (left) *actions* of G on sets.

- Morphisms in G-Set are arrows between any two actions $\nabla : \langle \hat{\varrho}, X \rangle \longrightarrow \langle \hat{\alpha}, Y \rangle$ such that $\nabla \in \mathrm{Hom}_{\mathsf{Set}}(X, Y)$ and the following diagram commutes:

$$\begin{CD}
G \times X @>{\hat{\varrho}}>> X \\
@V{\mathbb{1} \times \nabla}VV @VV{\nabla}V \\
G \times Y @>{\hat{\alpha}}>> Y
\end{CD}$$

A morphism ∇ in G-Set is said to be a G-Set *isomorphism* if ∇ is also a bijective map.

Theorem 3 *The diffraction map $\nabla : G \longrightarrow T \times H$ is a G-Set isomorphism between the actions induced by Cayley's representation $\varrho : G \longrightarrow S_G$ and the diffracted representation $\alpha : G \longrightarrow S_{T \times H}$, for a transversal T of G/H.*

Proof: Let $\hat{\varrho} : G \times G \longrightarrow G$ and $\hat{\alpha} : G \times (T \times H) \longrightarrow T \times H$ be the actions induced by Cayley's representation ϱ and the diffraction representation α from Theorem 2, respectively. Then our bijection $\nabla : G \longrightarrow T \times H$ satisfies the commutative diagrams

$$\begin{CD}
G \times G @>{\hat{\varrho}}>> G \\
@V{\mathbb{1}_G \times \nabla}VV @VV{\nabla}V \\
G \times (T \times H) @>{\hat{\alpha}}>> (T \times H)
\end{CD}
\qquad \text{since} \qquad
\begin{CD}
\langle g, k \rangle @>{\hat{\varrho}}>> \overline{gt}\,(\overline{g\,t})^{-1} g\,t\,h \\
@V{\mathbb{1}_G \times \nabla}VV @VV{\nabla}V \\
\langle g, \langle t, h \rangle \rangle @>{\hat{\alpha}}>> \langle \overline{gt}, (\overline{g\,t})^{-1} g\,t\,h \rangle
\end{CD}$$

for any $g, k \in G$ and $k = t\,h$, where $\langle t, h \rangle \in T \times H$. i.e., ∇ is a G-Set isomorphism. $\square$

Theorem 3 not only stipulates that G and $T \times H$ are G-Set isomorphic, but that the diffracted representation α expresses Cayley's representation when G decomposes as $\nabla(G) = T \times H$ as a set. Fortunately, this relationship is more than happenstance; the diffraction $T \times H$ of G borrows the group structure of G through the diffraction representation α since Cayley's representation ϱ exposes the product structure of G. As a consequence, following the commutativity of the diagram in (3) from the introduction, the product "$\bullet$" in G can be reconstructed as

$$\begin{CD}
G \times G @>{\text{``}\bullet\text{''}}>> G \\
@V{\mathbb{1} \times \nabla}VV @AA{\nabla^{-1}}A \\
G \times (T \times H) @>{\hat{\alpha}}>> T \times H
\end{CD} \qquad (12)$$

Theorem 4 *If δ is the T-fibration associated to Frobenius representation γ for a transversal T of G/H, then $T \times H$ becomes a group under the product defined by*

$$\forall_{\langle t_1, h_1 \rangle, \langle t_2, h_2 \rangle \in T \times H} \left[\ \langle t_1, h_1 \rangle \cdot \langle t_2, h_2 \rangle \ := \ \langle t_1^\gamma \circ h_1^\gamma (t_2), \delta(t_1 h_1, t_2) h_2 \rangle \ \right] \qquad (13)$$

Proof. Given the diffraction map $\nabla : G \longrightarrow T \times H$ of G with respect to a transversal T and the diffraction representation $\alpha : G \longrightarrow T \times H$ of G by T, it follows from diagram (12) by mean of theorem 3 that the following diagram commutes:

$$
\begin{array}{ccc}
G \times G & \xrightarrow{\ \ "\bullet"\ \ } & G
\end{array}
$$

Diagram:

$G \times G \xrightarrow{\ "\bullet"\ } G$, with $\nabla^{-1} \times \nabla^{-1}$, ∇, $\mathbb{1} \times \nabla$, $(T \times H)^2 \xrightarrow{\ "\cdot"\ } T \times H$, ∇^{-1}, $(\nabla^{-1}) \times \mathbb{1}$, $\mathbb{1}$, $G \times (T \times H) \xrightarrow{\ \hat{\alpha}\ } T \times H$.

Moreover, letting $g_1 = t_1 h_1$ and $g_2 = t_2 h_2$ in G where $\langle t_1, h_1 \rangle, \langle t_2, h_2 \rangle \in T \times H$, then chasing the central arrow "$\cdot$" through $\hat{\alpha}$ describes the product in $T \times H$ from G as

$$
\big\langle\, \langle t_1, h_1 \rangle, \langle t_2, h_2 \rangle \,\big\rangle \xmapsto{\ \ "\cdot"\ \ } \big\langle\, t_1^\gamma \circ h_1^\gamma (t_2)\,,\, \delta(t_1 h_1, t_2)\, h_2 \,\big\rangle .
$$

Therefore the set $T \times H$ becomes a group under formulation (13) since G is a group. $\square$

Definition 9 Let T be a transversal of G/H for G. The *diffracted group of G by T*, denoted by $T \triangledown H$, is the group structure on $T \times H$ described by the product in formulation (13). And, the product in $T \triangledown H$ is termed the (*external*) *bequeath product*.

Theorem 4 also allows us to use the Frobenius representation γ and its T-fibration δ to rewrite the product of any two elements $g_1, g_2 \in G$ in terms of a transversal T and its associated subgroup H. More precisely, given any two elements $g_1 = t_1 h_1$ and $g_2 = t_2 h_2$ in G of the form $\langle t_1, h_1 \rangle, \langle t_2, h_2 \rangle \in T \times H$, we can use the bequeathed rewriting process to express their internal product in terms of elements in T and H as

$$
g_1 g_2 = t_1^\gamma \circ h_1^\gamma (t_2)\, \delta(t_1 h_1, t_2)\, h_2 = \overline{t_1 h_1 t_2}\, \delta(t_1 h_1, t_2)\, h_2 ,
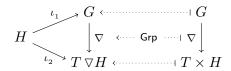$$

which is $g_1 g_2 = t_1 h_1 t_2 h_2$; nevertheless, elucidating $\overline{t_1 h_1 t_2} \in T$ and $\delta(t_1 h_1, t_2)\, h_2 \in H$.

Definition 10 Let T be a transversal of G/H for G and $g_1, g_2 \in G$ such that $g_1 = t_1 h_1$ and $g_2 = t_2 h_2$, where $t_1, t_2 \in T$ and $h_1, h_2 \in H$. The (*internal*) *bequeathed product* of g_1 and g_2 is the rewriting of $g_1 g_2$ in terms of elements from T and H defined by

$$
g_1 g_2 := \overline{t_1 h_1 t_2}\, \delta(t_1 h_1, t_2)\, h_2 .
$$

Furthermore, Theorem 4 not only dispenses the essential framework to convert the set $T \times H$ into a group, but it also assists in the lifting of the diffraction bijection $\nabla : G \longrightarrow T \times H$ to a group-isomorphism $\nabla : G \longrightarrow T \triangledown H$.

Theorem 5 *If G is a group with a subgroup H and an embedding $\iota_1 : H \longrightarrow G$, then for any transversal T of G/H with an embedding $\iota_2 : H \longrightarrow T \triangledown H$, there is a unique isomorphism $\nabla : G \longrightarrow T \triangledown H$ such that $\nabla \circ \iota_1 = \iota_2$, i.e., the diagram commutes:*

Proof: Let T be a transversal of G/H, and $\nabla : G \longrightarrow T \times H$ be its diffraction bijection. Given the identity $1 \in G$, then $\nabla(1) = \langle 1, 1 \rangle$. Now let g_1, g_2 be elements in G such that each has a unique decomposition $g_1 = t_1\, h_1$ and $g_2 = t_2\, h_2$, where $t_1, t_2 \in T$ and $h_1, h_2 \in H$. Then ∇ extends to a homomorphism from G into $T \,\nabla H$ since

$$
\begin{aligned}
\nabla(g_1 g_2) &= \langle\, \overline{t_1 h_1\, t_2 h_2}\,,\, \delta(t_1 h_1\, t_2 h_2, 1)\,\rangle \quad = \langle\, \overline{t_1 h_1\, t_2 \overline{h_2}}\,,\, \delta(t_1 h_1,\, \overline{t_2 \overline{h_2}})\,\delta(t_2 h_2, 1)\,\rangle \\
&= \langle\, t_1^{\gamma} \circ h_1^{\gamma}(t_2)\,,\, \delta(t_1 h_1,\, t_2)\, h_2\,\rangle \;=\; \langle t_1, h_1 \rangle \cdot \langle t_2, h_2 \rangle \\
&= \nabla(g_1) \cdot \nabla(g_2)
\end{aligned}
$$

by Lemma 1, Lemma 2 and Theorem 4. Moreover ∇ is an isomorphism since any $g \in \operatorname{Ker} \nabla$ must satisfy $g = 1$. The universal mapping property $\nabla \circ \iota_1 = \iota_2$ follows by composition, where the existence and uniqueness of ∇ is provided by Theorem 1. $\square$

References

[1] G. Baumslag, *Topics in combinatorial group theory*, Lectures in Mathematics, ETH Zürich, 1993.

[2] T. W. Hungerford, *Algebra*, Springer Graduate Texts in Mathematics, vol. 73, 1989

[3] R. C. Lyndon and P. E. Schupp, *Combinatorial Group Theory*, Ergebnisse der Mathematik, band 89, Springer 1977. Reprinted in the Springer Classics in Mathematics series, 2000.

[4] S. Mac Lane, (1971) *Categories for the Working Mathematician*, Springer, 2nd ed. 1998.

[5] W. Magnus, A. Karrass and D. Solitar, *Combinatorial Group Theory*, Wiley, New York, 1966 (also corrected Dover reprint 1976).

[6] J. J. Rotman, *An introduction to the theory of groups* (4th edition), Springer Graduate Texts in Mathematics 148, Springer-Verlag, Berlin- Heidleberg-New York, 1995.

[7] G. Zapata, *Rewriting Methods in Groups with Applications to Cryptography* (2017). CUNY Academic Works. https://academicworks.cuny.edu/gc_etds/2030

Mathematics Department, New York City College of Technology, Brooklyn NY 11201

e-mail : nyzapata@gmail.com