Decomposition of Groups into Twisted Subgroups and Subgroups

Tuval Foguel
and
Abraham A. Ungar

Department of Mathematics
North Dakota State University
Fargo, ND 58105
USA

e-mail: foguel@prairie.Nodak.edu
e-mail: ungar@plains.Nodak.edu

Suggested running title: **Twisted Subgroups**

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

Abstract. This article is subsequent to our previous one, entitled *Involutory decomposition of groups into twisted subgroups and subgroups* [7]. The twisted subgroups resulting from the involutory decomposition of groups into twisted subgroups and subgroups in [7] turn out to be *gyrocommutative gyrogroups.* In contrast, the twisted subgroups resulting from the (non-involutory) decomposition of groups into twisted subgroups and subgroups that we present in this article need not be gyrocommutative. Twisted subgroups arise in the study of problems in computational complexity [1] and in the study of gyrogroups [7]. Gyrogroups are grouplike structures that first arose in the study of Einstein's velocity addition in the special theory of relativity [23, 24]. We showed in [7] that any gyrogroup is an extension of a group by a gyrocommutative gyrogroup. The gyrogroups that we construct in this article demonstrate that this extension is not trivial.

§1. Introduction

Gyrogroup theory is an algebraic theory modelled on the groupoid of all relativistically admissible velocities with their Einstein velocity composition law and Thomas prcssion [23]. In our previous article [7] we have shown that any gyrogroup is an extension of a group by a gyrocommutative gyrogroup. In Remark 4.2 we show in this article that this extension need not be trivial. In fact, we present in the Remark an extension of a group by another group that gives a nonassociative structure, that is, a nongyrocommutative gyrogroup. Left gyrogroup is a structure slightly weaker than gyrogroup. We show that any given group can be turned into a left gyrogroup which is, in turn, a gyrogroup if and only if the given group is central by a 2-Engel group. The importance of left gyrogroups stems from the fact that they form twisted subgroups in specified groups.

Twisted subgroups are subsets of groups, introduced by Aschbacher [1], which under general conditions are near subgroups. The concept of near subgroup of a finite group was introduced by Feder and Vardi [6] as a tool to study problems in computational complexity involving the class NP. In the previous article [7] we have shown that every gyrogroup is a twisted subgroup in some specified group, and introduced the involutory decomposition of groups into twisted subgroups and subgroups, demonstrating that the resulting twisted subgroups are gyrocommutative gyrogroups. Gyrogroups are grouplike objects which share analogies with groups. In particular, gyrogroups are classified into gyrocommutative and non-gyrocommutative ones in full analogy with groups, thus offering a broader context for the study of groups. Gyrogroups are structures which first arose in the study of Einstein's relativistic velocity addition law. Gyrogroup theory captures the mathematical regularity that has seemingly been lost in the transition from ordinary vector addition (which is a group operation) to Einstein's relativistic velocity addition (which, being nonassociative, is not a group operation).

Following the involutory decomposition that we presented in [7], we present in this article a non-involutory decomposition of groups into twisted subgroups and subgroups. The resulting twisted subgroups, in this case, turn out to be gyrogroups that need not be gyrocommutative.

In Section 2 we present the basic definitions and properties that will be used in Section 3. In particular, we present the definition of gyrogroups and left gyrogroups. The decomposition of groups into subgroups and gyrogroups result, in Section 3, from diagonal transversals. We show in Theorem 3.3 that any group can be turned into the diagonal transversal of a specified group. But, by Theorem 2.12, any transversal groupoid is a left gyrogroup. Hence, by Theorem 3.4, any group can be turned into a left gyrogroup. We then characterize in Theorem 3.7 the groups that their associated left gyrogroups are gyrogroups. Finally, two examples of nongyrocommutative gyrogroups, one finite and one infinite, are presented in Section 4.

§2. Gyrotransversals, the transversals that give rise to gyrogroups

Definition 2.1. (Groupoids or Magmas, and Automorphism Groups of Groupoids)
A groupoid [3] or a magma [2] is a nonempty set with a binary operation. An automorphism of the groupoid $(S, \cdot)$ is a bijection of S that respects the binary operation $\cdot$ in S. The set of all automorphisms of $(S, \cdot)$ forms a group denoted by $Aut(S, \cdot)$.

An important subcategory of the category of groupoids is the category of loops, which are defined below.

Definition 2.2. (Loops [3]) A *loop* is a magma $(S, \cdot)$ with an identity element in which each of the two equations $a \cdot x = b$ and $y \cdot a = b$ for the unknowns x and y possesses a unique solution ($a \cdot x$ is the product of a and x in S. Subsequently we will omit the dot and write ax).

Definition 2.3. (Transversals, the Transversal Operation, the Transversal Map, and Transversal Groupoids) A set B is a transversal in a group G (all transversals in this article are left transversals) of a subgroup H of G if every $g \in G$ can be written uniquely as $g = bh$ where $b \in B$ and $h \in H$. Let $b_1, b_2 \in B$ be any two elements of B, and let

$$b_1 b_2 = (b_1 \odot b_2) h(b_1, b_2) \tag{2.1}$$

be the unique decomposition of the element $b_1 b_2 \in G$, where $b_1 \odot b_2 \in B$ and $h(b_1, b_2) \in H$, determining (i) a binary operation, $\odot$, in B, called the *transversal operation of B induced by G,* and (ii) a map $h : B \times B \to H$, called the *transversal map.* The element $h(b_1, b_2) \in H$ is called the element of H determined by the two elements b_1 and b_2 of its transversal B in G (its importance stems from the fact that it gives rise to gyrations in Definition 2.5. Gyrations, in turn, result from the abstraction of the Thomas precession of the special theory relativity into the Thomas gyration). A *transversal groupoid* $(B, \odot)$ of H in G is a groupoid formed by a transversal B of H in G with its transversal operation $\odot$.

Definition 2.4. (Gyrotransversals, Gyrotransversal Groupoids, Gyrodecompositions of Groups) A transversal groupoid $(B, \odot)$ of a subgroup H in a group G is a *gyrotransversal* of H in G if

(i) $1_G \in B$, 1_G being the identity element of G;

(ii) $B = B^{-1}$; and

(iii) B is normalized by H, $H \subseteq N_G(B)$, that is, $hBh^{-1} \subseteq B$ for all $h \in H$.

A *gyrotransversal groupoid* is a groupoid formed by a gyrotransversal with its transversal operation. The decomposition $G = BH$ where $H < G$ and where B is a transversal of H in G is a *gyrodecomposition* if B is a gyrotransversal of H in G. The gyrodecomposition $G = BH$ is *reduced* if $C_H(B) = \{1_G\}$

Definition 2.5. (Gyrations of a Gyrotransversal) Let B be a gyrotransversal of a subgroup H in a group G, let $b_1, b_2 \in B$ be any two elements of B, and let $h(b_1, b_2)$ be the element of H determined by b_1 and b_2. Then the *gyration* $gyr[b_1, b_2]$ of B generated by b_1 and b_2 is the map of B into itself given by

$$gyr[b_1, b_2] = \alpha_{h(b_1, b_2)}$$

where α_h, $h \in H$, denotes conjugation by h, that is, for any $h \in H$ and $b \in B$

$$\alpha_h(b) = b^h = hbh^{-1}$$

It follows from Definition 2.5 that a gyration of B generated by $b_1, b_2 \in B$ is given in terms of its effects on $x \in B$ by the equation

$$gyr[b_1, b_2]x = h(b_1, b_2)x(h(b_1, b_2))^{-1} \tag{2.2a}$$

or, equivalently, by the equation

$$gyr[b_1, b_2]x = x^{h(b_1, b_2)} \tag{2.2b}$$

The conjugation operations α_h, $h \in H$, are bijections of B since B is normalized by H. Hence, in particular, the gyrations $gyr[b_1, b_2]$ are bijections of B for all $b_1, b_2 \in B$. Moreover, these gyrations are automorphisms of the gyrotransversal $(B, \odot)$ as shown in Theorem 2.11 of [7], following which gyrations $gyr[a, b]$ of a gyrotransversal groupoid are also called *gyroautomorphisms* of the gyrotransversal groupoid.

In general, a transversal groupoid need not be a group. Some non-group gyrotransversal groupoids possess an important grouplike structure called a gyrogroup. The importance of gyrogroups is indicated by the fact that the first known gyrogroup is the Einstein gyrogroup, whose gyrogroup operation is the Einstein velocity addition (of velocities that need not be parallel), and whose gyration operation is the well known Thomas precession (or, gyration) of the special theory of relativity [17, 21]. The gyrogroup definition, abstracted from the Einstein groupoid of relativistically admissible velocities with (i) their Einstein velocity addition law and (ii) their Thomas precessions (or, gyrations) [18, 19], therefore follows.

Definition 2.6. (Gyrogroups [23]) The magma $(G, \odot)$ is a *gyrogroup* if its binary operation satisfies the following axioms. In G there is at least one element, 1, called a left identity, satisfying

(G1) $1 \odot a = a$ Left Identity

for all $a \in G$. There is an element $1 \in G$ satisfying axiom $(G1)$ such that for each a in G there is an x in G, called a left inverse of a, satisfying

(G2) $x \odot a = 1$ Left Inverse

Moreover, for any $a, b, z \in G$ there exists a unique element $gyr[a, b]z \in G$ such that

(G3) $a \odot (b \odot z) = (a \odot b) \odot gyr[a, b]z$ Left Gyroassociative Law

If $gyr[a, b]$ denotes the map $gyr[a, b] : G \to G$ given by $z \mapsto gyr[a, b]z$ then

(G4) $gyr[a, b] \in Aut(G, \odot)$ Gyroautomorphism

and $gyr[a, b]$ is called the *Thomas gyration*, or the *gyroautomorphism* of G, *generated* by $a, b \in G$. Finally, the gyroautomorphism $gyr[a, b]$ generated by any $a, b \in G$ satisfies

(G5) $gyr[a, b] = gyr[a \odot b, b]$ Left Loop Property

Definition 2.7. (Gyrocommutative Gyrogroups) The gyrogroup $(G, \oplus)$ is *gyrocommutative* if for all $a, b \in G$

(G6) $a \oplus b = gyr[a,b](b \oplus a)$ Gyrocommutative Law

As it is customary with groups, we use additive notation, $\oplus$, with gyrocommutative gyrogroups, and multiplicative notation, $\odot$, with general gyrogroups.

Definition 2.8. (Gyrations, Gyroautomorphisms, Gyroautomorphism Groups) The automorphisms $gyr[a,b]$ of a gyrogroup are called *gyroautomorphisms*. The action of the gyroautomorphism $gyr[a,b]$ on G is called a gyration. The set of all gyroautomorphisms of a gyrogroup $(G, \odot)$ need not form a group. A *gyroautomorphism group* of $(G, \odot)$ is any subgroup $Aut_o(G, \odot)$ (not necessarily the smallest one) of $Aut(G, \odot)$ containing all the gyroautomorphisms of $(G, \odot)$.

Properties of gyrogroups have been studied in [23].

Theorem 2.9. *Each of the two equations*

$$a \odot x = b \tag{2.3a}$$

$$y \odot a = b \tag{2.4a}$$

for the unknowns x and y in a gyrogroup $(P, \odot)$ possesses a unique solution,

$$x = a^{-1} \odot b \tag{2.3b}$$

$$y = b \odot (gyr[b,a]a)^{-1} \tag{2.4b}$$

The proof of Theorem 2.9 may be found in [23] and in [22]. Theorem 2.9 implies that a gyrogroup is a loop.

The substitution of (2.3b) in (2.3a), with a replaced by a^{-1}, reveals the left cancellation law

$$a^{-1} \odot (a \odot b) = b \tag{2.5}$$

Eq. (2.3a) can therefore be solved by the left cancellation law (2.5), which gyrogroups obey. To solve Eq. (2.4a), on the other hand, one must use the loop property, as explained in [23] and in [22]. Suggestively, we define a *left gyrogroup* as a "gyrogroup with a weak loop property", so that in a left gyrogroup Eq. (2.3a) is uniquely solved by a left cancellation, while Eq. (2.4a) need not have a unique solution.

Definition 2.10. (Left Gyrogroups) A magma $(G, \odot)$ is a left gyrogroup if it satisfies Axioms $(G1) - (G4)$ of the gyrogroup axioms in Definition 2.6, and

(G5') $gyr[a, a^{-1}] = 1_{Aut(G)}$ Weak Loop Property

A left gyrogroup is, thus, a gyrogroup in which the loop property (G5) has been weakend into (G5'). Left gyrogroups possess the left cancellation law (2.5). Hence, Eq. (2.3a) possesses a unique solution in a left gyrogroup. In contrast, Eq. (2.4a) in a left gyrogroup may have no solution, a single solution or several solutions. Examples of left gyrogroups which are not gyrogroups are mentioned in Remark 3.10. We clearly have the following Lemma (whose proof is obvious) and Theorem (which is Theorem 2.13 in [7]):

Lemma 2.11.
(i) A left gyrogroup is a group if and only if its binary operation is associative.
(ii) A left gyrogroup G is a group if and only if its gyrations vanish, that is, if and only if $gyr[a,b] = I$ is the identity automorphism of G for all $a, b \in G$.

Theorem 2.12. [7] *Any gyrotransversal groupoid is a left gyrogroup.*

Since any gyrotransversal groupoid is a left gyrogroup, and since a left gyrogroup is a gyrogroup without the loop property, we have

Corollary 2.13. *A gyrotransversal groupoid is a gyrogroup if and only if it possesses the loop property.*

To verify the converse of Theorem 2.12, in Theorem 2.16 below, we need the following Definition and Lemma.

Definition 2.14. (Gyrosemidirect Product Groups) Let $P = (P, \odot)$ be a left gyrogroup, and let $Aut_o(P) = Aut_o(P, \odot)$ be any gyroautomorphism group of P (Definition 2.8). The *gyrosemidirect product group*

$$P \rtimes Aut_o(P) \tag{2.6}$$

of the left gyrogroup P and a gyroautomorphism group $Aut_o(P)$ is a group of pairs (x, X), where $x \in P$ and $X \in Aut_o(P)$, with group operation given by the *gyrosemidirect product*

$$(x, X)(y, Y) = (x \odot Xy, gyr[x, Xy]XY). \tag{2.7}$$

It is anticipated in Definition 2.14 that the gyrosemidirect product group (2.6) is a group with group operation given by the gyrosemidirect product (2.7). This is indeed the case as we show in the following

lemma 2.15. *Let $(P, \odot)$ be a left gyrogroup, and let $Aut_o(P, \odot)$ be any of its gyroautomorphism groups. Then the gyrosemidirect product $P \rtimes Aut_o(P)$ is a group.*

Proof. We view the elements (x, X) of $P \times Aut_o(P)$ as bijections of P according to the equation

$$(x, X)g = x \odot Xg$$

for any $x, g \in P$ and $X \in Aut_o(P)$, where the identity bijection is the pair $(0, I)$, and the inverse of (x, X) is $(x, X)^{-1} = ((X^{-1}x)^{-1}, X^{-1})$. To show that the elements of $P \times Aut_o(P)$ indeed act bijectively on P we employ the left cancellation law (2.5), which is valid in any left gyrogroup. As such, the set $P \times Aut_o(P)$ forms a group of bijections with group operation given by bijection composition,

$$\begin{aligned}
(x, X)(y, Y)g &= (x, X)(y \odot Yg) \\
&= x \odot X(y \odot Yg) \\
&= x \odot (Xy \odot XYg) \\
&= (x \odot Xy) \odot gyr[x, Xy]XYg \\
&= (x \odot Xy, gyr[x, Xy]XY)g.
\end{aligned}$$

The bijection composition turns out to be the gyrosemidirect product (2.7) in $P \rtimes Aut_o(P)$ thus verifying that (2.7) is indeed a group operation in the gyrosemidirect product group (2.6). $\square$

Theorem 2.16. *(The Converse of Theorem 2.12) Every left gyrogroup $P = (P, \odot)$ is a gyrotransversal of its gyroautomorphism group $Aut_o(P)$ in its gyrosemidirect product group $P \rtimes Aut_o(P)$.*

Proof. Let $H = Aut_o(P)$ be any gyroautomorphism group of the left gyrogroup $(P, \odot)$, and let $G = P \rtimes H$ be the resulting gyrosemidirect product group. Identifying elements $h \in H$ with pairs $(1, h) \in G$, H is isomorphic with a subgroup of G. Similarly, identifying elements $p \in P$ with their corresponding pairs $(p, 1_H) \in G$, P is a subset of G. The left gyrogroup P and the two groups H and G share their identity elements which are respectively denoted by 1_P, 1_H and 1_G. We note that in any left gyrogroup $(P, \odot)$ the gyroautomorphisms $gyr[p, 1_P]$ and $gyr[1_P, p]$ are the identity automorphism of P, as shown in [23].

The left gyrogroup P, considered as a set, is the transversal of H in $G = P \rtimes H$ by Definition 2.14. In order to show that $(P, \odot)$ is a gyrotransversal of H in G it remains to verify that the transversal operation in P equals its left gyrogroup operation $\odot$, and establish the validity of properties (i), (ii) and (iii) in Definition 2.4 of gyrotransversals.

Let $(x, 1_H), (y, 1_H) \in P \subset G$ be any two elements of P. Their product in G, Definition 2.14, has the unique decomposition

$$\begin{aligned}(x, 1_H)(y, 1_H) &= (x \odot y, gyr[x, y]) \\ &= (x \odot y, 1_H)(1_P, gyr[x, y])\end{aligned}$$

indicating that the transversal binary operation in P is the gyrogroup operation, $\odot$, in P.

Clearly, P contains the identity element $(1_P, 1_H)$ of G. Moreover, since in G, $(p, 1_H)^{-1} = (p^{-1}, 1_H)$ for any $p \in P$, we have $(p, 1_H)^{-1} \in P$ so that $P = P^{-1}$, thus establishing properties (i) and (ii) of Definition 2.4.

To show that H normalizes P in G, property (iii) in Definition 2.4, we note that for all $p \in P$ and $h \in H$ we have by Definition 2.14,

$$\begin{aligned}(1_P, h)(p, 1_H)(1_P, h^{-1}) &= (1_P \odot p^h, gyr[1_P, p^h]h1_H)(1_P, h^{-1}) \\ &= (p^h, h)(1_P, h^{-1}) \\ &= (p^h \odot 1_P^h, gyr[p^h, 1_P^h]hh^{-1}) \\ &= (p^h, 1_H) \in P\end{aligned}$$

and the proof is thus complete. $\square$

Theorem 2.17. *Let $(B, \odot)$ be a gyrotransversal groupoid of a subgroup H in a group G and let h be its transversal map. Then $(B, \odot)$ is a group if and only if $h(a, b) \in C_G(B)$ for all $a, b \in B$. Equivalently, $(B, \odot)$ is a group if and only if $gyr[a, b]$ vanishes (that is, it is the identity automorphism of B) for all $a, b \in B$.*

Proof. By Theorem 2.12, the pair $(B, \odot)$ is a left gyrogroup. Hence, by Lemma 2.11, it is a group if and only if its binary operation $\odot$ is associative. The binary operation $\odot$, in turn, is associative if and only if $gyr[a, b]c = c$ for all $a, b, c \in B$ or, equivalently, by Definition 2.5, if and only if $c^{h(a,b)} = c$ for all $a, b, c \in B$. But, the latter is satisfied if and only if $h(a, b) \in C_G(B)$ for all $a, b \in B$. $\square$

§3. Diagonal Transversals

Definition 3.1. (Diagonal Transversals)

Let K be a group and let $G = K \rtimes Inn(K)$ be the semidirect product group of K and $Inn(K)$, where $Inn(K)$ is the inner automorphism group of K whose generic element α_k denotes conjugation by $k \in K$. Then, the *diagonal transversal* D generated by K (in G) is a subset of G given by

$$D = \{(k, \alpha_k) | k \in K\} \subset G$$

Any element $(k, \alpha_k) \in D$ is determined by a corresponding element $k \in K$. We therefore use the notation

$$D(k) = (k, \alpha_k)$$

to denote the elements of D.

We may note that if K is commutative then $Inn(K) = \{1_K\}$ is the trivial group, and the transversal of $Inn(K)$ in G is isomorphic with the group G.

It is anticipated in Definition 3.1 that diagonal transversals are transversals. In the following theorem we will show that this is indeed the case. In fact, we will show that diagonal transversals are special transversals; they are gyrotransversals.

Theorem 3.2. *A diagonal transversal with its transversal operation, is a gyrotransversal groupoid.*

Proof. Let D be a diagonal transversal generated by a group K, and let $G = K \rtimes Inn(K)$. Any element (k, α_h) of G, where $k, h \in K$, can be uniquely written as a product

$$(k, \alpha_h) = (k, \alpha_k)(1_K, \alpha_{k^{-1}h}) = D(k)(1_K, \alpha_{k^{-1}h}) \tag{3.1}$$

of an element in D and an element in $Inn(K)$. Hence, D is a transversal of $Inn(K)$ in G.

In order to find the transversal operation $\odot$ of the transversal D let us consider the product decomposition

$$(k_1, \alpha_{k_1})(k_2, \alpha_{k_2}) = (k_1 k_2^{k_1}, \alpha_{k_1 k_2}) = (k_1 k_2^{k_1}, \alpha_{k_1 k_2^{k_1}})(1_K, \alpha_{(k_2^{-1})^{k_1} k_2}) \tag{3.2a}$$

which can be written as

$$D(k_1)D(k_2) = D(k_1 k_2^{k_1})(1_K, \alpha_{[k_1, k_2^{-1}]}) \tag{3.2b}$$

for any $k_1, k_2 \in K$, where $[k_1, k_2] = k_1 k_2 k_1^{-1} k_2^{-1}$ is the commutator of k_1 and k_2 [15, p. 92]. It follows from the product decomposition (3.2) that the transversal operation is given by

$$D(k_1) \odot D(k_2) = D(k_1 k_2^{k_1}) \tag{3.3}$$

As a byproduct we also find from the product decomposition (3.2) that the element $h \in Inn(K) \subset G$ determined by any two elements $D(k_1)$ and $D(k_2)$ of the transversal D, Definition 2.3, is

$$h(D(k_1), D(k_2)) = (1_K, \alpha_{[k_1, k_2^{-1}]}) \in Inn(K) \tag{3.4}$$

h being the transversal map $D \times D \to Inn(K)$. To show that the transversal groupoid $(D, \odot)$ is a gyrotransversal groupoid, we will verify the validity of properties (i)-(iii) in Definition 2.4.

(i) The identity $(1_K, \alpha_{1_K})$ of G is the identity element $D(1_K)$ in D.

(ii) In D, $D(k_1)^{-1} = D(k^{-1})$ so $D = D^{-1}$.

(iii) $Inn(K) \subseteq N_G(D)$ since

$$(1_K, \alpha_h)D(k)(1_K, \alpha_{h^{-1}}) = (1_K, \alpha_h)(k, \alpha_k)(1_K, \alpha_{h^{-1}}) = (k^h, \alpha_{k^h}) = D(k^h) \in D \tag{3.5}$$

and the proof is complete. $\square$

Theorem 3.3. *Let K be a group, let $G = K \rtimes Inn(K)$ be the semidirect product group of K and $Inn(K)$, and let D be the diagonal transversal formed by K in G. Then, G can be written as a gyrosemidirect product group $G = D \rtimes\!\!\mid Inn(K)$.*

Proof. By Theorems 3.2 and 2.12, D is a left gyrogroup. By Definition 2.5, $Inn(K)$ contains all the gyrations of the left gyrogroup D thus giving rise to the gyrosemidirect product $\bar{G} = D \rtimes\!\!\mid Inn(K)$ of the left gyrogroup D and its gyroautomorphism group $Inn(K)$. It is clear from Eq. (3.1) that every element of G (of $\bar{G}$) is contained in $\bar{G}$ (in G) so that $G = \bar{G}$, as desired. $\square$

Following Definition 3.1, any group $(K, \cdot)$ generates a diagonal transversal

$$D = \{D(k) = (k, \alpha_k) | k \in K\}$$

whose elements $D(k) \in D$ are identified with the elements $k \in K$. By Theorem 3.2, the diagonal transversal D forms a gyrotransversal groupoid whose binary operation is given by Eq. (3.3), and whose gyrations are derived from Eq. (3.4) by means of Eq. (2.2). By Theorem 2.12, any gyrotransversal groupoid is a left gyrogroup. Under the obvious identification of the set D of the left gyrogroup $(D, \odot)$ with the set K of the group $(K, \odot)$, this group is turned into the left gyrogroup $(K, \odot)$

(i) where the left gyrogroup operation is given by

$$a \odot b = ab^a \tag{3.6}$$

as we see from Eq. (3.3), and

(ii) when the gyrations of K are the automorphisms

$$gyr[a, b] = \alpha_{[a, b^{-1}]} \tag{3.7}$$

of K as we see from Eq. (3.4). These suggest the following theorem and definition.

Theorem 3.4. *Any group $(K, \cdot)$ can be turned into an associated left gyrogroup $(K, \odot)$ by introducing into $(K, \cdot)$ the left gyrogroup operation $\odot$ which is given in terms of the group operation $\cdot$ by*

$$a \odot b = ab^a \tag{3.8}$$

The gyroautomorphisms of the resulting left gyrogroup $(K, \odot)$ are given by the equation

$$gyr[a, b] = \alpha_{[a, b^{-1}]} \tag{3.9}$$

for all $a, b \in K$.

Definition 3.5. (Associated Left Gyrogroups) The associated left gyrogroup of a group $(K, \cdot)$ is the left gyrogroup $(K, \odot)$ whose left gyrogroup operation $\odot$ is given in terms of the group operation $\cdot$ by $a \odot b = ab^a$ for all $a, b \in K$.

Theorem 3.6. *The associated left gyrogroup $(K, \odot)$ of a group $(K, \cdot)$ is a group if and only if $(K, \cdot)$ is nilpotent of class 2.*

Proof. By Lemma 2.11 the left gyrogroup $(K, \odot)$ is a group if and only if $gyr[a, b] = I$ is the identity automorphism of K for all $a, b \in K$. But, by Eq. (3.7), $gyr[a, b^{-1}] = I$ for all $a, b \in K$ if and only if $\alpha_{[a,b]} = I$ for all $a, b \in K$. The latter is equivalent to the condition $[a, b] \in Z(K)$ for all $a, b \in K$, that is, the condition that K is nilpotent of class 2 is equivalent to the condition that $(K, \odot)$ is a group, as desired. □

A 2-Engel group E is a group satisfying $[[a, b], b] = 1$. Engel groups are useful in various studies of nilpotency; see e.g. [14]. It becomes evident from the following Theorem that these are useful in the study of gyrogroups as well.

Theorem 3.7. *Let $(K, \odot)$ be the left gyrogroup associated with a group $(K, \cdot)$. Then $(K, \odot)$ is a gyrogroup if and only if $(K, \cdot)$ is central by a 2-Engel group.*

Proof. A left gyrogroup is a gyrogroup if and only if it possesses the loop property, by Definition 2.10. We thus have to characterize the loop property identity

$$gyr[a \odot b, b] = gyr[a, b] \tag{3.10}$$

in $(K, \odot)$ in terms of a characterization of 2-Engel groups. Identity (3.10) in $(K, \odot)$ is equivalent to the identity

$$\alpha_{[ab^a, b^{-1}]} = \alpha_{[a,b^{-1}]} \tag{3.11}$$

in $(K, \cdot)$. Identity (3.11), viewed in $(K, \cdot)/Z(K)$, is equivalent to the identity

$$[ab^a, b^{-1}] = [a, b^{-1}] \tag{3.12}$$

in $(K, \cdot)/Z(K)$. This, in turn, is equivalent to the more revealing identity

$$[a, b] = [b^{-1}, a] \tag{3.13}$$

in $(K, \cdot)/Z(K)$, as we see from the following chain of equivalent identities.

$$\begin{aligned} [ab^a, b^{-1}] = [a, b^{-1}] &\Leftrightarrow a^2ba^{-1}b^{-1}ab^{-1}a^{-2}b = ab^{-1}a^{-1}b \\ &\Leftrightarrow b^{-1} = aba^{-1}b^{-1}ab^{-1}a^{-1} \\ &\Leftrightarrow 1 = aba^{-1}bab^{-1}a^{-1}b^{-1} \\ &\Leftrightarrow [[a, b], b] = 1 \end{aligned} \tag{3.14}$$

Finally, the identity (3.14) characterizes the 2-Engel groups [14]. Hence, the loop property identity (3.11) in the group $(K, \cdot)$ is equivalent to the identity (3.14) in the quotient group $(K, \cdot)/Z(K)$. The latter, in turn, is equivalent to the condition that $(K, \cdot)/Z(K)$ is a 2-Engel group, as desired. □

Corollary 3.8. *The left gyrogroup $(K, \odot)$ associated with any nilpotent group $(K, \cdot)$ of class 3 is a gyrogroup.*

Proof. Any nilpotent group of class 3 is central by a 2-Engel group [14]. The result thus follows from Theorem 3.7. □

Following Corollary 3.8, gyrogroup formalism can be applied to nilpotent groups of class 3 (or, more generally, to any group which is central by a 2-Engel group). Gyrogroup formalism, proved useful in the special theory of relativity and in hyperbolic geometry [23], is presently being found useful in group theory as well.

As an example of the application of gyrogroup formalism to nilpotent groups of class 3, let us realize the equation (2.4a)

$$x \odot a = b \tag{3.15}$$

and its unique solution for x,

$$x = b \odot (gyr[b, a]a)^{-1} \tag{3.16}$$

in the abstract gyrogroup $(G, \odot)$ by an equation and its solution in a nilpotent group $(K, \cdot)$ of class 3. Let $(K, \odot)$ be the gyrogroup generated by $(K, \cdot)$ according to Definition 3.5.

According to Eq. (3.8), Equation (3.15) in $(K, \odot)$ takes the form

$$xa^x = b$$

in $(K, \cdot)$, and according to both Eqs. (3.9) and (3.8) its unique solution (3.16) in $(K, \odot)$ takes in $(K, \cdot)$ the form

$$\begin{aligned} x &= b \odot (a^{[b,a^{-1}]})^{-1} \\ &= b \odot (a^{-1})^{[b,a^{-1}]} \\ &= b((a^{-1})^{[b,a^{-1}]})^b \\ &= b(a^{-1})^{b[b,a^{-1}]} \end{aligned}$$

By means of gyrogroup theory we have thus obtained in the following Corollary a group theoretic identity that would be very tedious to obtain otherwise.

Corollary 3.9. *Let G be a group which is central by a 2-Engel group. Then the equation*

$$xa^x = b \tag{3.17}$$

for x in G possesses the unique solution

$$x = b(a^{-1})^{b[b,a^{-1}]} \tag{3.18}$$

Remark 3.10. It can readily be shown by induction on the nilpotency class that equation (3.17) for the unknown x in any nilpotent group $(G, \cdot)$ possesses a unique solution. It is true when $(G, \cdot)$ is abelian, and an induction on the class (divide out the center) does the rest. Hence, for any nilpotent group $(G, \cdot)$ the associated groupoid $(G, \odot)$ is a left gyrogroup that forms a loop. Consequently, there are loops which are left gyrogroups but are not gyrogroups.

Remark 3.11. Any loop $(L, *)$ has an associativity correction C satisfying $a*(b*c) = (a*b)*C[a,b]c$ for all $a, b \in L$. The loop L is a left gyrogroup if and only if $C[a,b]$ is an automorphism of L for any $a, b \in L$. Examples of loops which are non-gyrogroup left gyrogroups are provided in Remark 3.10.

§4. Examples

Example 4.1. (A gyrogroup multiplication table) The lowest order of nongroup gyrogroups generated from nilpotent groups of class 3 which are not of class 2 is 16. Using the software package MAGMA and its library [4] we found three nonisomorphic nilpotent groups of order 16 which are of class 3 but are not of class 2 (see Lemma 3.4). They generate three non-gyrocommutative gyrogroups of order 16, denoted by K_{16}, L_{16}, and M_{16}. The gyrogroup multiplication table of one of them, K_{16}, calculated by employing Eq. (3.8), is presented in Table I, where the elements $k_i \in K_{16}$, $i = 1, 2, \ldots, 16$, are denoted by their subscripts.

Table I *(The gyrogroup K_{16})*

$\circ$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	2	1	4	3	6	5	8	7	10	9	12	11	14	13	16	15
3	3	4	2	1	7	8	6	5	12	11	9	10	16	15	13	14
4	4	3	1	2	8	7	5	6	11	12	10	9	15	16	14	13
5	5	6	7	8	4	3	1	2	16	15	13	14	10	9	12	11
6	6	5	8	7	3	4	2	1	15	16	14	13	9	10	11	12
7	7	8	6	5	1	2	3	4	14	13	16	15	11	12	10	9
8	8	7	5	6	2	1	4	3	13	14	15	16	12	11	9	10
9	9	10	11	12	13	14	15	16	1	2	3	4	5	6	7	8
10	10	9	12	11	14	13	16	15	2	1	4	3	6	5	8	7
11	11	12	10	9	15	16	14	13	4	3	1	2	8	7	5	6
12	12	11	9	10	16	15	13	14	3	4	2	1	7	8	6	5
13	13	14	15	16	12	11	9	10	7	8	6	5	1	2	3	4
14	14	13	16	15	11	12	10	9	8	7	5	6	2	1	4	3
15	15	16	14	13	9	10	11	12	5	6	7	8	4	3	1	2
16	16	15	13	14	10	9	12	11	6	5	8	7	3	4	2	1

The gyroautomorphisms of K_{16} are calculated by means of Eq. (3.9). There is only one non-identity gyroautomorphism, A, whose transformation table is given in Table II.

Table II *(The automorphism A of K_{16})*

$1 \to 1$	$5 \to 5$	$9 \to 10$	$13 \to 14$
$2 \to 2$	$6 \to 6$	$10 \to 9$	$14 \to 13$
$3 \to 3$	$7 \to 7$	$11 \to 12$	$15 \to 16$
$4 \to 4$	$8 \to 8$	$12 \to 11$	$16 \to 15$

The gyroautomorphism $gyr[a, b]$ generated by any $a, b \in K_{16}$ is either A or the identity automorphism 1. The gyroautomorphism table for $gyr[a, b]$ is presented in Table III.

Table III *(The gyroatomorphisms $gyr[a, b]$ of K_{16})*

gyr	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
4	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
5	1	1	1	1	1	1	1	1	A	A	A	A	A	A	A	A
6	1	1	1	1	1	1	1	1	A	A	A	A	A	A	A	A
7	1	1	1	1	1	1	1	1	A	A	A	A	A	A	A	A
8	1	1	1	1	1	1	1	1	A	A	A	A	A	A	A	A
9	1	1	1	1	A	A	A	A	1	1	1	1	A	A	A	A
10	1	1	1	1	A	A	A	A	1	1	1	1	A	A	A	A
11	1	1	1	1	A	A	A	A	1	1	1	1	A	A	A	A
12	1	1	1	1	A	A	A	A	1	1	1	1	A	A	A	A
13	1	1	1	1	A	A	A	A	A	A	A	A	1	1	1	1
14	1	1	1	1	A	A	A	A	A	A	A	A	1	1	1	1
15	1	1	1	1	A	A	A	A	A	A	A	A	1	1	1	1
16	1	1	1	1	A	A	A	A	A	A	A	A	1	1	1	1

The set of all automorphisms of K_{16}, $\{I, A\}$, is a group of order 2. In general, the set of all gyroautomorphisms of a gyrogroup need not form a group. Thus, for instance, the gyroautomorphisms of the Einstein 2-dimensional gyrogroup $(\Re_c^2, \oplus_E)$ are all rotations of the Euclidean plane $\Re^2$ about its origin, but there is no gyroautomorphism that rotates the plane about its origin by π radians [21].

As an example illustrating the use of Tables I-III, let us corroborate the left gyroassociative law

$$a \odot (b \odot c) = (a \odot b) \odot gyr[a, b]c$$

for the special case when $a = 6$, $b = 9$, and $c = 12$ in K_{16}. On one hand

$$a \odot (b \odot c) = 6 \odot (9 \odot 12) = 6 \odot 4 = 7$$

and on the other

$$\begin{aligned} (a \odot b) \odot gyr[a, b]c &= (6 \odot 9) \odot gyr[6, 9]12 \\ &= 15 \odot A(12) \\ &= 15 \odot 11 \\ &= 7 \end{aligned}$$

as expected.

Remark 4.2. The 4×4 upper left corner of Table I forms a multiplication table of a group, H. The group H is a normal subgroup of the gyrogroup K_{16} (see Definitions 4.7 and 4.8 in [7]). The quotient gyrogroup K_{16}/H turns out to be an Abelian group. Hence, we have in hand an example of an extension of a group by another group that gives a nonassociative structure (that is, the gyrogroup K_{16}). It is an extension which is far from being trivial, where H and K_{16}/H are groups while K_{16} is a non-gyrocommutative gyrogroup.

Example 4.3. (A non-group, non-gyrocommutative matrix gyrogroup) The matrix group $(T_4, \cdot)$ of all 4×4 real or complex upper triangular matrices with diagonal elements 1,

$$M(x) = \begin{pmatrix} 1 & x_1 & x_2 & x_3 \\ 0 & 1 & x_4 & x_5 \\ 0 & 0 & 1 & x_6 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

under matrix multiplication is nilpotent of nilpotency class 3. Hence, by Corollary 3.8 the pair $(T_4, \odot)$ is a gyrogroup whose gyrogroup operation is given by

$$M(x) \odot M(y) = (M(x))^2 M(y) (M(x))^{-1}$$

The gyroautomorphisms $gyr[M(a), M(b)]$ of the gyrogroup $(T_4, \odot)$ are given in terms of their effects on $M(z)$ by the equation

$$gyr[M(a), M(b)]M(z) = (M(a) \odot M(b))^{-1} \odot (M(a) \odot (M(b) \odot M(z)))$$

for all $M(a), M(b), M(z) \in (T_4, \odot)$.

Acknowledgments. We have been assisted by Jeremy Dover of NSA in the use of the software package MAGMA [4]. We wish to thank him, and Michael Kinyon of Indiana University South Bend for helpful suggestions about the paper. During a seminar that Joseph Rotman gave about the present paper at the University of Illinois, Sergei Ivanov made Remark 3.10, thus providing us with examples of left gyrogroups which are loops but fail to be gyrogroups. This and other useful remarks made during the seminar were e-mailed to us by Joseph Rotman. We are pleased to acknowledge financial support fron ND EPSCoR grants #OSR-9452892 (awarded to TF) and #OSE-9452892 (awarded to AU).

References

1. Michael Aschbacher. Near subgroups of finite groups. *J. Group Theory* **1** (1998), 113-129.
2. Nicolas Bourbaki. *Algebra* (Addison-Wesley, 1974).
3. Richard H. BrucK. *A Survey of Binary Systems* (Springer-Verlag, 1966).
4. J. Cannon and C. Playoust. *An introduction to MAGMA* (University of Sydney, Sydney, 1993).
5. O. Chein, Hala O. Pflugfelder, and Jonathan D.H. Smith (eds.). *Quasigroups and Loops Theory and Applications* (Sigma Series in Pure Mathematics, Vol. 8, Heldermann Verlag, Berlin, 1990).
6. T. Feder and M. Vardi. The computational structure of monotone monadic SNP and constraint satisfaction: a study through Datalog and group theory. *SIAM J. Comput.* **28** (1999), no. 1, 57-104.
7. Tuval Foguel and Abraham A. Ungar. Involutory decomposition of groups into twisted subgroups and subgroups. *J. Group Theory* To appear.
8. Tomas Kepka and Jon D. Phillips. Connected transversals to subnormal subgroups. *Comm. Math. Univ. Carolinae* **38** (1997), 223-230.
9. Markku Niemenmaa. On multiplication groups of loops. *J. Algebra* **135** (1990), 112-122.
10. Markku Niemenmaa. On the structure of the inner mapping groups of loops. *Comm. Algebra* **24** (1996), 135-142.
11. Markku Niemenmaa and Tomas Kepka. On connected transversals to Abelian subgroups in finite groups. *Bull. London Math. Soc.* **24** (1992), 343-346.
12. Markku Niemenmaa and Ari Vesanen. On connected transversals in the projective special linear group PSL(2,7). *J. Algebra* **166** (1994), 455-460.
13. Hala O. Pflugfelder. *Quasigroups and Loops: Introduction* (Heldermann Verlag, Berlin, 1990).
14. Derek J.S. Robinson. *A Course in the Theory of Groups* (Springer, New York, 1995).
15. Joseph J. Rotman. *An Introduction to the Theory of Groups* (Springer, New York, 1995).
16. Lev V. Sabinin. On the equivalence of categories of loops and homogeneous spaces. *Soviet Math. Dokl.* **13** (1972), 970-974.
17. Abraham A. Ungar. Thomas rotation and the parametrization of the Lorentz transformation group. *Found. Phys. Lett.* **1** (1988), 57-89.
18. Abraham A. Ungar. Axiomatic approach to the nonassociative group of relativistic velocities. *Found. Phys. Lett.* **2** (1989), 199-203.
19. Abraham A. Ungar. The relativistic noncommutative nonassociative group of velocities and the Thomas rotation. *Results Math.* **16** (1989), 168-179.
20. Abraham A. Ungar. Weakly associative groups. *Results Math.* **17** (1990), 149-168.
21. Abraham A. Ungar. Thomas precession and its associated grouplike structure. *Amer. J. Phys.* **59** (1991), 824-834.
22. Abraham A. Ungar. The holomorphic automorphism group of the complex disk. *Aequat. Math.* **47** (1994), 240-254.
23. Abraham A. Ungar. Thomas precession: its underlying gyrogroup axioms and their use in hyperbolic geometry and relativistic physics. *Found. Phys.* **27** (1997), 881-951.
24. Abraham A. Ungar. From Pythagoras to Einstein: the hyperbolic Pythagorean theorem. *Found. Phys.* **28** (1998), 1283-1321.