Quasigroups and Related Systems **22** (2014), 283 – 294

Lagrange's theorem for gyrogroups and the Cauchy property

Teerapong Suksumran and Keng Wiboonton

Abstract. We prove a version of Lagrange's theorem for gyrogroups and use this result to prove that gyrogroups of particular orders have the strong Cauchy property.

1. Introduction

Lagrange's theorem (that the order of any subgroup of a finite group Γ divides the order of Γ) is well known in group theory and has impact on several branches of mathematics, especially finite group theory, combinatorics, and number theory. Lagrange's theorem proves useful for unraveling mathematical structures. For instance, it is used to prove that any finite field must have prime power order. Certain classification theorems of finite groups arise as an application of Lagrange's theorem [9, 10, 17]. Further, Fermat little's theorem and Euler's theorem may be viewed as a consequence of this theorem. Also relevant are the orbit-stabilizer theorem and the Cauchy-Frobenius lemma (or Burnside's lemma). A history of Lagrange's theorem on groups can be found in [15].

In loop theory, the Lagrange property becomes a nontrivial issue. For example, whether Lagrange's theorem holds for Moufang loops was an open problem in the theory of Moufang loops for more than four decades [5, p. 43]. This problem was answered in the affirmative by Grishkov and Zavarnitsine [11]. In fact, not every loop satisfies the Lagrange property as one can construct a loop of order five containing a subloop of order two. Nevertheless, some loops satisfy the Lagrange property.

Baumeister and Stein [1] proved a version of Lagrange's theorem for Bruck loops by studying in detail the structure of a finite Bruck loop. Foguel et al. [7] proved that left Bol loops of *odd* order satisfy the strong Lagrange property. It is, however, still an open problem whether or not Bol loops satisfy the Lagrange property [6, p. 592]. In the same spirit, we focus on the Lagrange property for *gyrogroups* or *left Bol loops with the* A_ℓ*-property* in the loop literature. In [18], we proved that the order of an *L-subgyrogroup* of a finite gyrogroup G divides the order of G. In this paper, we extend this result by proving that the order of *any* subgyrogroup of G divides the order of G, see Theorem 5.7.

2010 Mathematics Subject Classification: 20N05, 18A32, 20A05.
Keywords: gyrogroup, Lagrange's theorem, Cauchy property, Bol loop, A_ℓ-loop.

A gyrogroup is a group-like structure, introduced by Ungar, arising as an algebraic structure that the set of relativistically admissible vectors in $\mathbb{R}^3$ with Einstein addition encodes [19]. The origin of a gyrogroup is described in [22, Chapter 1]. There are two prime examples of gyrogroups, namely the *Einstein gyrogroup*, which consists of the relativistic ball in $\mathbb{R}^3$ with Einstein addition [19], and the *Möbius gyrogroup*, which consists of the complex unit disk with Möbius addition [21].

In this paper, we prove that Lagrange's theorem holds for gyrogroups and apply this result to show that finite gyrogroups of particular orders have the Cauchy property. Our results are strongly based on results by Foguel and Ungar [8] and Baumeister and Stein [1]. For basic terminology and definitions in loop theory, we refer the reader to [2, 12, 14].

2. Gyrogroups

In this section, we summarize definitions and basic properties of gyrogroups. Much of this section can be found in [20].

Let $(G, \oplus)$ be a magma. Denote the group of automorphisms of G with respect to $\oplus$ by $\mathrm{Aut}\,(G, \oplus)$.

Definition 2.1 ([20]). A magma $(G, \oplus)$ is a *gyrogroup* if its binary operation satisfies the following axioms:

(G1) $\exists 0 \in G\, \forall a \in G,\ 0 \oplus a = a$; (left identity)

(G2) $\forall a \in G\, \exists b \in G,\ b \oplus a = 0$; (left inverse)

(G3) $\forall a, b \in G\, \exists \mathrm{gyr}[a, b] \in \mathrm{Aut}\,(G, \oplus)\, \forall c \in G,$

$$a \oplus (b \oplus c) = (a \oplus b) \oplus \mathrm{gyr}[a, b]c; \qquad \text{(left gyroassociative law)}$$

(G4) $\forall a, b \in G,\ \mathrm{gyr}[a, b] = \mathrm{gyr}[a \oplus b, b]$. (left loop property)

The following theorem gives a characterization of a gyrogroup.

Theorem 2.2 ([8]). *Suppose that $(G, \oplus)$ is a magma. Then $(G, \oplus)$ is a gyrogroup if and only if $(G, \oplus)$ satisfies the following properties:*

(g1) $\exists 0 \in G \forall a \in G, 0 \oplus a = a$ *and* $a \oplus 0 = a$; (two-sided identity)

(g2) $\forall a \in G \exists b \in G, b \oplus a = 0$ *and* $a \oplus b = 0$. (two-sided inverse)
For $a, b, c \in G$, define

$$\mathrm{gyr}[a, b]c = \ominus(a \oplus b) \oplus (a \oplus (b \oplus c)), \qquad \text{(gyrator identity)}$$

then

(g3) $\mathrm{gyr}[a, b] \in \mathrm{Aut}\,(G, \oplus)$; (gyroautomorphism)

(g3a) $a \oplus (b \oplus c) = (a \oplus b) \oplus \mathrm{gyr}[a, b]c$; (left gyroassociative law)

(g3b) $(a \oplus b) \oplus c = a \oplus (b \oplus \mathrm{gyr}[b, a]c)$; (right gyroassociative law)

(g4a) $\mathrm{gyr}[a, b] = \mathrm{gyr}[a \oplus b, b]$; (left loop property)

(g4b) $\mathrm{gyr}[a, b] = \mathrm{gyr}[a, b \oplus a]$. (right loop property)

Definition 2.3 ([20]). A gyrogroup G having the additional property that

$$a \oplus b = \mathrm{gyr}[a, b](b \oplus a) \qquad \text{(gyrocommutative law)}$$

for all $a, b \in G$ is called a *gyrocommutative gyrogroup*.

The *gyrogroup cooperation*, $\boxplus$, is defined by the equation

$$a \boxplus b = a \oplus \mathrm{gyr}[a, \ominus b]b, \qquad a, b \in G. \tag{1}$$

Theorem 2.4 ([20]). *Let G be a gyrogroup and let $a, b \in G$. The unique solution of the equation $a \oplus x = b$ in G for the unknown x is $x = \ominus a \oplus b$, and the unique solution of the equation $x \oplus a = b$ in G for the unknown x is $x = b \boxplus (\ominus a)$.*

By Theorem 2.4, the following cancellation laws hold in gyrogroups.

Theorem 2.5 ([20]). *Let G be a gyrogroup. For all $a, b, c \in G$,*

(1) $a \oplus b = a \oplus c$ *implies* $b = c$; (general left cancellation law)

(2) $\ominus a \oplus (a \oplus b) = b$; (left cancellation law)

(3) $(b \ominus a) \boxplus a = b$; (right cancellation law I)

(4) $(b \boxplus (\ominus a)) \oplus a = b$. (right cancellation law II)

Let G be a gyrogroup. For $a \in G$, the *left gyrotranslation by a*, $L_a \colon x \mapsto a \oplus x$, and the *right gyrotranslation by a*, $R_a \colon x \mapsto x \oplus a$, are permutations of G. Further, one has the following composition law

$$L_a \circ L_b = L_{a \oplus b} \circ \mathrm{gyr}[a, b]. \tag{2}$$

From this it can be proved that every gyrogroup forms a left Bol loop with the A_ℓ-property, where the gyroautomorphisms correspond to *left inner mappings* or *precession maps*. In fact, gyrogroups and left Bol loops with the A_ℓ-property are equivalent, see for instance [16].

3. Subgyrogroups

Let G be a gyrogroup. A nonempty subset H of G is called a *subgyrogroup* if it is a gyrogroup under the operation inherited from G and the restriction of $\mathrm{gyr}[a,b]$ to H becomes an automorphism of H for all $a,b \in H$. If H is a subgyrogroup of G, we write $H \leqslant G$. We have the following subgyrogroup criterion, as in the group case.

Proposition 3.1 ([18]). *A nonempty subset H of G is a subgyrogroup if and only if* (1) *$a \in H$ implies $\ominus a \in H$ and* (2) *$a,b \in H$ implies $a \oplus b \in H$.*

Subgyrogroups that arise as groups under gyrogroup operation are of great importance in the study of gyrogroups.

Definition 3.2 ([8]). A nonempty subset X of a gyrogroup $(G,\oplus)$ is a *subgroup* if it is a group under the restriction of $\oplus$ to X.

The following proposition shows that any subgroup of a gyrogroup is simply a subgyrogroup with trivial gyroautomorphisms.

Proposition 3.3. *A nonempty subset X of a gyrogroup G is a subgroup if and only if it is a subgyrogroup of G and $\mathrm{gyr}[a,b]\big|_X = \mathrm{id}_X$ for all $a,b \in X$.*

Just as in group theory, we obtain the following results.

Proposition 3.4. *Let G be a gyrogroup and let $\mathcal{H}$ be a nonempty collection of subgyrogroups of G. Then the intersection $\bigcap_{H\in\mathcal{H}} H$ forms a subgyrogroup of G.*

Proof. This follows directly from the subgyrogroup criterion. □

Proposition 3.5. *Let A be a nonempty subset of a gyrogroup G. There exists a unique subgyrogroup of G, denoted by $\langle A\rangle$, such that*

(1) *$A \subseteq \langle A\rangle$ and*

(2) *if $H \leqslant G$ and $A \subseteq H$, then $\langle A\rangle \subseteq H$.*

Proof. Set $\mathcal{H} = \{H : H \leqslant G \text{ and } A \subseteq H\}$. Then $\langle A\rangle := \bigcap_{H\in\mathcal{H}} H$ is a subgyrogroup of G satisfying the two conditions. The uniqueness follows from condition (2). □

The subgyrogroup generated by one-element set $\{a\}$ is called the *cyclic subgyrogroup generated by a*, which will be denoted by $\langle a\rangle$. Next, we will give an explicit description of $\langle a\rangle$.

Let G be a gyrogroup and let $a \in G$. Define recursively the following notation:

$$0\cdot a = 0, \quad m\cdot a = a \oplus ((m-1)\cdot a),\ m \geqslant 1, \quad m\cdot a = (-m)\cdot(\ominus a),\ m < 0. \tag{3}$$

We also define the right counterparts:

$$a\cdot 0 = 0, \quad a\cdot m = (a\cdot(m-1)) \oplus a,\ m \geqslant 1, \quad a\cdot m = (\ominus a)\cdot(-m),\ m < 0. \tag{4}$$

Lemma 3.6. *Let G be a gyrogroup. For any element a of G,*

$$\mathrm{gyr}[a \cdot m, a] = \mathrm{gyr}[m \cdot a, a] = \mathrm{gyr}[a, m \cdot a] = \mathrm{gyr}[a, a \cdot m] = \mathrm{id}_G$$

for all $m \in \mathbb{Z}$.

Proof. By induction, $\mathrm{gyr}[a, a \cdot m] = \mathrm{id}_G$ and $\mathrm{gyr}[a \cdot m, a] = \mathrm{id}_G$ for all $a \in G$ and all $m \geqslant 0$. By the right gyroassociative law, $a \cdot m = m \cdot a$ for all $m \in \mathbb{Z}$. If $m < 0$, the left and right loop properties and the left cancellation law together imply $\mathrm{gyr}[a, a \cdot m] = \mathrm{id}_G$. □

By induction,

$$(m \cdot a) \oplus (k \cdot a) = (m + k) \cdot a \tag{5}$$

for all $m, k \geqslant 0$. In fact, we have the following proposition.

Proposition 3.7. *Let a be an element of a gyrogroup. For all $m, k \in \mathbb{Z}$,*

$$(m \cdot a) \oplus (k \cdot a) = (m + k) \cdot a.$$

Proof. The proof is routine, using (5) and induction. □

Theorem 3.8. *Let G be a gyrogroup and let $a \in G$. Then $\langle a \rangle = \{m \cdot a \colon m \in \mathbb{Z}\}$. In particular, $\langle a \rangle$ forms a subgroup of G.*

Proof. Set $H = \{m \cdot a \colon m \in \mathbb{Z}\}$. For all $m, n \in \mathbb{Z}$, Proposition 3.7 implies that $\ominus(m \cdot a) = (-m) \cdot a \in H$ and $(m \cdot a) \oplus (k \cdot a) = (m + k) \cdot a \in H$. This proves $H \leqslant G$. Since $a \in H$, we have $\langle a \rangle \subseteq H$ by the minimality of $\langle a \rangle$. By the closure property of subgyrogroups, $H \subseteq \langle a \rangle$ and so equality holds.

Note that $(m \cdot a) \oplus [(n \cdot a) \oplus (k \cdot a)] = (m + n + k) \cdot a = [(m \cdot a) \oplus (n \cdot a)] \oplus (k \cdot a)$ for all $m, n, k \in \mathbb{Z}$. Thus, $\mathrm{gyr}[m \cdot a, n \cdot a]\big|_{\langle a \rangle} = \mathrm{id}_{\langle a \rangle}$ for all $m, n \in \mathbb{Z}$ and hence $\langle a \rangle$ forms a subgroup of G by Proposition 3.3. □

Theorem 3.8 suggests us to define the *order* of an element in a gyrogroup as follows.

Definition 3.9. Let G be a gyrogroup and let $a \in G$. The *order* of a, denoted by $|a|$, is defined to be the cardinality of $\langle a \rangle$ if $\langle a \rangle$ is finite. In this case, we will write $|a| < \infty$. If $\langle a \rangle$ is infinite, the order of a is defined to be infinity, and we will write $|a| = \infty$.

Proposition 3.10. *Let G be a gyrogroup and let $a \in G$. For all $m, n \in \mathbb{Z}$,*

$$\mathrm{gyr}[m \cdot a, n \cdot a] = \mathrm{id}_G.$$

Proof. By induction, $L_{m \cdot a} = L_a^m$ for all $a \in G$ and all $m \in \mathbb{Z}$. Since $L_a^{-1} = L_{\ominus a}$, we have from (2) that

$$\mathrm{gyr}[m \cdot a, n \cdot a] = L_{-(m+n) \cdot a} \circ L_{m \cdot a} \circ L_{n \cdot a} = L_a^{-(m+n)} \circ L_a^m \circ L_a^n = \mathrm{id}_G$$

for all $m, n \in \mathbb{Z}$. □

In light of the proof of Proposition 3.10, gyrogroups are *left power alternative*. Further, the following proposition implies that gyrogroups are *power associative*.

Proposition 3.11. *If a is an element of a gyrogroup, then $\langle a\rangle$ forms a cyclic group with generator a under gyrogroup operation.*

Proof. By Theorem 3.8, $\langle a\rangle$ is a group under gyrogroup operation. By induction, $m \cdot a = a^m$ for all $m \geqslant 0$, where the notation a^m is used as in group theory. If $m < 0$, one obtains similarly that $m \cdot a = a^m$. Hence, $\langle a\rangle$ forms a cyclic group with generator a. □

Corollary 3.12. *Any gyrogroup generated by one element is a cyclic group.*

Because the *group* order of a and the *gyrogroup* order of a are the same, we obtain the following results.

Proposition 3.13. *Let G be a gyrogroup and let $a \in G$.*

(1) *If $|a| < \infty$, then $|a|$ is the smallest positive integer such that $|a| \cdot a = 0$.*

(2) *If $|a| = \infty$, then $m \cdot a \neq 0$ for all $m \neq 0$ and $m \cdot a \neq k \cdot a$ for all $m \neq k$ in $\mathbb{Z}$.*

Corollary 3.14. *Let a be an element of a gyrogroup. If $|a| = n < \infty$, then*

$$\langle a\rangle = \{0 \cdot a, 1 \cdot a, \ldots, (n-1) \cdot a\}.$$

Corollary 3.15. *Let a be an element of a gyrogroup and let $m \in \mathbb{Z} \setminus \{0\}$.*

(1) *If $|a| = \infty$, then $|m \cdot a| = \infty$.*

(2) *If $|a| < \infty$, then $|m \cdot a| = \dfrac{|a|}{\gcd(|a|, m)}$.*

4. Gyrogroup homomorphisms

A *gyrogroup homomorphism* is a map between gyrogroups that preserves the gyrogroup operations. A bijective gyrogroup homomorphism is called a *gyrogroup isomorphism*. We say that gyrogroups G and H are *isomorphic*, written $G \cong H$, if there exists a gyrogroup isomorphism from G to H.

Suppose that $\varphi\colon G \to H$ is a gyrogroup homomorphism. The kernel of φ is defined to be the inverse image of the trivial subgyrogroup $\{0\}$ under φ. Since $\ker\varphi$ is invariant under all the gyroautomorphisms of G, the operation

$$(a \oplus \ker\varphi) \oplus (b \oplus \ker\varphi) := (a \oplus b) \oplus \ker\varphi, \qquad a, b \in G, \tag{6}$$

is independent of the choice of representatives for the left cosets. The system $(G/\ker\varphi, \oplus)$ forms a gyrogroup, called a *quotient gyrogroup*. This results in the first isomorphism theorem for gyrogroups.

Theorem 4.1 ([18], The First Isomorphism Theorem). *If φ is a gyrogroup homomorphism of G, then $G/\ker\varphi \cong \varphi(G)$ as gyrogroups.*

A subgyrogroup N of a gyrogroup G is *normal in* G, denoted by $N \trianglelefteq G$, if it is the kernel of a gyrogroup homomorphism of G. By Theorem 4.1, every normal subgyrogroup N gives rise to the quotient gyrogroup G/N, along with the *canonical projection* $\Pi\colon a \mapsto a \oplus N$.

We state the second isomorphism theorem for gyrogroups for easy reference; its proof can be found in [18].

Theorem 4.2 (The Second Isomorphism Theorem). *Let G be a gyrogroup and let $A, B \leqslant G$. If $B \trianglelefteq G$, then $A \oplus B \leqslant G$, $A \cap B \trianglelefteq A$, and $(A \oplus B)/B \cong A/(A \cap B)$ as gyrogroups.*

5. The Lagrange property

Throughout this section, all gyrogroups are finite. A version of the Lagrange property for loops can be found in [5]. In terms of gyrogroups, the Lagrange property can be restated as follows.

Definition 5.1. A gyrogroup G is said to have the *Lagrange property* if for each subgyrogroup H of G, the order of H divides the order of G.

A version of the following proposition for loops was proved by Bruck in [2]. As the first isomorphism theorem and the second isomorphism theorem hold for gyrogroups, we also have the following proposition:

Proposition 5.2. *Let H be a subgyrogroup of a gyrogroup G and let B be a normal subgyrogroup of H. If B and H/B have the Lagrange property, then so has H.*

Corollary 5.3. *Let N be a normal subgyrogroup of a gyrogroup G. If N and G/N have the Lagrange property, then so has G.*

Proof. Taking H = G in the proposition, the corollary follows. □

Proposition 5.4. *Let X be a subgroup of a gyrogroup G. If $H \leqslant X$, then $|H|$ divides $|X|$. In other words, every subgroup of G has the Lagrange property.*

Proof. Suppose that $H \leqslant X$. Since $\mathrm{gyr}[a,b]\big|_H = \mathrm{id}_H$ for all $a, b \in H$, H forms a subgroup of G. By definition, X forms a group and H becomes a subgroup of X. By Lagrange's theorem for groups, $|H|$ divides $|X|$. □

Lagrange's theorem holds for *all* gyrocommutative gyrogroups, as shown by Baumeister and Stein in [1, Theorem 3] in the language of Bruck loops.

Theorem 5.5. *In a gyrocommutative gyrogroup G, if $H \leqslant G$, then $|H|$ divides $|G|$. In other words, every gyrocommutative gyrogroup has the Lagrange property.*

Proof. Let G be a gyrocommutative gyrogroup and let $H \leqslant G$. Then G is a Bruck loop and H becomes a subloop of G. By Theorem 3 of [1], $|H|$ divides $|G|$, which completes the proof. □

The next theorem, due to Foguel and Ungar, enables us to extend Lagrange's theorem to all finite gyrogroups.

Theorem 5.6 ([8], Theorem 4.11). *If G is a gyrogroup, then G has a normal subgroup N such that G/N is a gyrocommutative gyrogroup.*

Theorem 5.7 (Lagrange's Theorem). *If H is a subgyrogroup of a gyrogroup G, then $|H|$ divides $|G|$. That is, every gyrogroup has the Lagrange property.*

Proof. Let G be a gyrogroup. By Theorem 5.6, G has a normal subgroup N such that G/N is gyrocommutative. Because $N = \ker \Pi$, where $\Pi\colon G \to G/N$ is the canonical projection, N is a normal subgyrogroup of G. By Proposition 5.4 and Theorem 5.5, N and G/N have the Lagrange property. By Corollary 5.3, G has the Lagrange property. □

6. Applications

In this section, we provide some applications of Lagrange's theorem. Throughout this section, all gyrogroups are finite.

Proposition 6.1. *Let G be a gyrogroup and let $a \in G$. Then $|a|$ divides $|G|$. In particular, $|G| \cdot a = 0$.*

Proof. By definition, $|a| = |\langle a \rangle|$. By Lagrange's theorem, $|a|$ divides $|G|$. Write $|G| = |a|k$ with $k \in \mathbb{N}$, so $|G| \cdot a = (|a|k) \cdot a = \underbrace{|a| \cdot a \oplus \cdots \oplus |a| \cdot a}_{k \text{ copies}} = 0$. □

Although we know that a left Bol loop of prime order is a cyclic group by a result of Burn [3, Corollary 2], we present the following theorem as an application of Lagrange's theorem.

Theorem 6.2. *If G is a gyrogroup of prime order p, then G is a cyclic group of order p under gyrogroup operation.*

Proof. Let a be a nonidentity element of G. Then $|a| \neq 1$ and $|a|$ divides p. It follows that $|a| = p$, which implies $G = \langle a \rangle$ since G is finite. By Proposition 3.11, $\langle a \rangle$ is a cyclic group of order p, which completes the proof. □

The Cauchy property

In the loop literature, it is known that left Bol loops of odd order satisfy the Cauchy property [7, Theorem 6.2]. However, Bol loops fail to satisfy the Cauchy property as Nagy proves the existence of a simple right Bol loop of exponent 2 and of order 96 [13, Corollary 3.7]. This also implies that gyrogroups fail to satisfy the Cauchy property since any Bol loop of exponent 2 is necessarily a Bruck loop, hence a gyrocommutative gyrogroup.

In this subsection, we apply Lagrange's theorem and results from loop theory to establish that some finite gyrogroups satisfy the Cauchy property.

Definition 6.3 (The Weak Cauchy Property, WCP). A finite gyrogroup G is said to have the *weak Cauchy property* if for every prime p dividing $|G|$, G has an element of order p.

Definition 6.4 (The Strong Cauchy Property, SCP). A finite gyrogroup G is said to have the *strong Cauchy property* if every subgyrogroup of G has the weak Cauchy property.

The Cauchy property is an invariant property of gyrogroups, as shown in the following proposition.

Proposition 6.5. *Let G and H be gyrogroups and let $\phi\colon G \to H$ be a gyrogroup isomorphism.*

(1) *If G has the weak Cauchy property, then so has H.*

(2) *If G has the strong Cauchy property, then so has H.*

Proof. (1) It suffices to prove that $|\phi(a)| = |a|$ for all $a \in G$. By induction, $\phi(n \cdot a) = n \cdot \phi(a)$ for all $a \in G$ and all $n \in \mathbb{N}$. Let $a \in G$. Since $|a| \cdot a = 0$, we have $|a| \cdot \phi(a) = \phi(|a| \cdot a) = \phi(0) = 0$. If there were a positive integer $m < |a|$ for which $m \cdot \phi(a) = 0$, then we would have $\phi(m \cdot a) = 0$ and would have $m \cdot a = 0$, contradicting the minimality of $|a|$. Hence, $|a|$ is the smallest positive integer such that $|a| \cdot \phi(a) = 0$, which implies $|\phi(a)| = |a|$ by Proposition 3.13 (1).

(2) Let $B \leqslant H$. Set $A = \phi^{-1}(B)$. Then $A \leqslant G$ and A has the WCP. Since $\phi\big|_A$ is a gyrogroup isomorphism from A onto B, B has the WCP by Item 1. □

Corollary 6.6. *Let G and H be gyrogroups. If $G \cong H$, then G has the weak (resp. strong) Cauchy property if and only if H has the weak (resp. strong) Cauchy property.*

Theorem 6.7. *Let H be a subgyrogroup of a gyrogroup G and let B be a normal subgyrogroup of H.*

(1) *If B and H/B have the weak Cauchy property, then so has H.*

(2) *If B and H/B have the strong Cauchy property, then so has H.*

Proof. (1) Suppose that p is a prime dividing $|H|$. Since $|H| = [H\colon B]|B|$, p divides $|H/B|$ or $|B|$. If p divides $|B|$, then B has an element of order p and we are done. We may therefore assume that $p \nmid |B|$. Hence, p divides $|H/B|$. By assumption, H/B has an element of order p, say $a \oplus B$. By induction, $n \cdot (a \oplus B) = (n \cdot a) \oplus B$ for all $n \geqslant 0$. Hence, by Proposition 3.13 (1), p is the smallest positive integer such that $p \cdot a \in B$. In particular, $a \notin B$. Note that $\gcd(|a|, p) = 1$ or p. If $\gcd(|a|, p) = 1$ were true, we would have $|p \cdot a| = \dfrac{|a|}{\gcd(|a|, p)} = |a|$, and would have $a \in \langle a \rangle = \langle p \cdot a \rangle \leqslant B$, a contradiction. Hence, $\gcd(|a|, p) = p$, which implies p divides $|a|$. Write $|a| = mp$. Then $|m \cdot a| = \dfrac{|a|}{\gcd(|a|, m)} = p$, which finishes the proof of (1).

(2) Suppose that B and H/B have the SCP. Let $A \leqslant H$. By assumption, $A \cap B$ has the WCP. Since $A \oplus B/B \leqslant H/B$, $A \oplus B/B$ has the WCP. Since $A/A \cap B \cong A \oplus B/B$, $A/A \cap B$ has the WCP. By Item 1, A has the WCP. □

Corollary 6.8. *Let N be a normal subgyrogroup of a gyrogroup G. If N and G/N have the weak (strong) Cauchy property, then so has G.*

Consider a gyrogroup G of order pq, where p and q are primes. If pq is odd, by a result of Foguel, Kinyon, and Phillips [7, Theorem 6.2], G has the weak Cauchy property. Since any subgyrogroup of G is of order $1, p, q$ or pq, every subgyrogroup of G has the weak Cauchy property as well. This implies that G has the strong Cauchy property. If pq is even, at least one of p or q must be 2. Hence, G is of order $2\tilde{p}$, where $\tilde{p}$ is a prime. By a result of Burn [3, Theorem 4], G is a group, hence has the strong Cauchy property. This proves the following theorem.

Theorem 6.9 (Cauchy's Theorem). *Let p and q be primes. Every gyrogroup of order pq has the strong Cauchy property.*

Theorem 6.10. *Let p and q be primes and let G be a gyrogroup of order pq. If $p = q$, then G is a group. If $p \neq q$, then G is generated by two elements; one has order p and the other has order q.*

Proof. In the case $p = q$, G is a left Bol loop of order p^2, hence must be a group by Burn's result [3, Theorem 5].

Suppose that $p \neq q$. Let a and b be elements of order p and q, respectively. By Lagrange's theorem, $\langle a \rangle \cap \langle b \rangle = \{0\}$. For all $m, n, s, t \in \mathbb{Z}$, if $(m \cdot a) \oplus (n \cdot b) = (s \cdot a) \oplus (t \cdot b)$, then $\ominus(s \oplus a) \oplus (m \cdot a) = (t \cdot b) \boxplus (\ominus(n \cdot b)) = (t \cdot b) \ominus (n \cdot b)$ belongs to $\langle a \rangle \cap \langle b \rangle$. Hence, $\ominus(s \oplus a) \oplus (m \cdot a) = 0$ and $(t \cdot b) \ominus (n \cdot b) = 0$ and so $m \cdot a = s \cdot a$ and $n \cdot b = t \cdot b$. This proves $\{(m \cdot a) \oplus (n \cdot b)\colon 0 \leq m < p, 0 \leq n < q\}$ contains pq distinct elements of G. Since G is finite, it follows that

$$G = \{(m \cdot a) \oplus (n \cdot b)\colon 0 \leq m < p, 0 \leq n < q\} = \langle a, b \rangle. \qquad \square$$

In general, gyrogroups of order pq, where p and q are distinct primes not equal to 2, need not be groups. This is a situation where gyrogroups are different from

Moufang loops. As Moufang loops are *diassociative*, every Moufang loop generated by two elements must be a group. This implies that Moufang loops of order pq are groups [4, Proposition 3].

Let G be a finite *nongyrocommutative* gyrogroup. By Theorem 5.6, G has a normal subgroup N such that G/N is gyrocommutative. Because G is nongyrocommutative, we have N is nontrivial, since otherwise $\Pi\colon G \to G/N$ would be a gyrogroup isomorphism and G and G/N would be isomorphic gyrogroups. From this we can deduce the following results.

Theorem 6.11. *Let p be a prime. Every nongyrocommutative gyrogroup of order p^3 has the strong Cauchy property.*

Proof. Let G be a nongyrocommutative gyrogroup of order p^3. As noted above, G has a nontrivial normal subgroup N. By Lagrange's theorem, $|N| = p, p^2$ or p^3. If $|N| = p^3$, then $G = N$ is a group, hence has the SCP. If $|N| \in \{p, p^2\}$, then $|N| \in \{p, p^2\}$. In any case, N and G/N form groups. Hence, N and G/N have the SCP and by Corollary 6.8, G has the SCP. □

Theorem 6.12. *Let p, q and r be primes. Every nongyrocommutative gyrogroup of order pqr has the strong Cauchy property.*

Proof. The proof follows the same steps as in the proof of Theorem 6.11. □

Acknowledgment. This work was completed with the support of Development and Promotion of Science and Technology Talents Project (DPST), Institute for Promotion of Teaching Science and Technology (IPST), Thailand.

References

[1] **B. Baumeister and A. Stein**, *The finite Bruck loops*, J. Algebra **330** (2011), 206 – 220.

[2] **R. H. Bruck**, *A survey of binary systems*, Springer, Berlin Heidelberg, 1971.

[3] **R. P. Burn**, *Finite Bol loops*, Math. Proc. Cambridge Philos. Soc. **84** (1978), 377 – 386.

[4] **O. Chein**, *Moufang loops of small order I*, Trans. Amer. Math. Soc. **188** (1974), 31 – 51.

[5] **O. Chein, M. K. Kinyon, A. Rajah, and P. Vojtěchovský**, *Loops and the Lagrange property*, Results. Math. **43** (2003), 74 – 78.

[6] **T. Foguel and M. K. Kinyon**, *Uniquely 2-divisible Bol loops*, J. Algebra Appl. **9** (2010), 591 – 601.

[7] **T. Foguel, M. K. Kinyon, and J. D. Phillips**, *On twisted subgroups and Bol loops of odd order*, Rocky Mountain J. Math. **36** (2006), 183 – 212.

[8] **T. Foguel and A. A. Ungar**, *Involutory decomposition of groups into twisted subgroups and subgroups*, J. Group Theory **3** (2000), 27 – 46.

[9] **J. A. Gallian**, *The classification of groups of order* $2p$, Math. Mag. **74** (2001), $60-61$.

[10] **J. A. Gallian and D. Moulton**, *On groups of order* pq, Math. Mag. **68** (1995), $287-288$.

[11] **A. N. Grishkov and A. V. Zavarnitsine**, *Lagrange's theorem for Moufang loops*, Math. Proc. Cambridge Philos. Soc. **139** (2005), $41-57$.

[12] **H. Kiechle**, *Theory of K-Loops*, Springer, Berlin, 2002.

[13] **G. P. Nagy**, *A class of finite simple Bol loops of exponent* 2, Trans. Amer. Math. Soc. **361** (2009), $5331-5343$.

[14] **H. O. Pflugfelder**, *Quasigroups and Loops: An Introduction*, Heldermann Verlag, Berlin, 1991.

[15] **R. L. Roth**, *A history of Lagrange's theorem on groups*, Math. Mag. **74** (2001), $99-108$.

[16] **L. V. Sabinin, L. L. Sabinina, and L. V. Sbitneva**, *On the notion of gyrogroup*, Aequat. Math. **56** (1998), $11-17$.

[17] **A. Sinefakopoulos**, *On groups of order* p^2, Math. Mag. **70** (1997), $212-213$.

[18] **T. Suksumran and K. Wiboonton**, *Isomorphism theorems for gyrogroups and L-subgyrogroups*, to appear in J. Geom. Symmetry Phys.

[19] **A. A. Ungar**, *Einstein's velocity addition law and its hyperbolic geometry*, Comput. Math. Appl. **53** (2007), $1228-1250$.

[20] **A. A. Ungar**, *Analytic Hyperbolic Geometry and Albert Einstein's Special Theory of Relativity*, World Scientific, Hackensack, 2008.

[21] **A. A. Ungar**, *From Möbius to gyrogroups*, Amer. Math. Monthly **115** (2008), $138-144$.

[22] **A. A. Ungar**, *A Gyrovector Space Approach to Hyperbolic Geometry*, Morgan & Claypool, San Rafael, 2009.

Received November 2, 2014

Department of Mathematics and Computer Science
Faculty of Science, Chulalongkorn University
Thailand
E-mails: teerapong.su@student.chula.ac.th (T. Suksumran)
keng.w@chula.ac.th (K. Wiboonton)