Journal of Mathematical Extension
Vol. 11, No. 3, (2017), 77-86
ISSN: 1735-8299
URL: http://www.ijmex.com

Some Generalizations of Lagrange Theorem and Factor Subsets for Semigroups

M. H. Hooshmand
Young Researchers and Elite Club
Shiraz Branch, Islamic Azad University

Abstract. It is well known that every group is equal to the direct product of its subgroup and related left and right transversal sets (in the sense of direct product of subsets). Therefore, every subgroup of a group is its left and right factor and one of its consequence is the Lagrange's theorem for finite groups. This paper generalizes the results for semigroups and proves a necessary and sufficient condition for a subgroup of a semigroup to be a factor. Also, by using the conception upper periodic subsets of semigroups and groups (introduced by the author as a generalization of the conception ideals) we prove some sufficient conditions for a vast class of subsets of semigroups to be factors and Lagrange subsets.

AMS Subject Classification: 20M99; 20M10
Keywords and Phrases: Factor subset, factor sub-semigroup and group, periodic and upper periodic subset, Lagrange subset

1. Introduction and Preliminaries

In 1942 G. Hajôs, in order to solve a geometric problem posed by Minkowski, introduced the notion of the direct product of subsets (see [1,4]). He said that the group G is the direct product of two of its subsets, A and B, if each element of G is uniquely expressible in the form

Received: September 2016; Accepted: May 2017

the sets is a group. Also, factoring (groups, semigroups and quasigroups) by subsets is used by the author for studying periodic subsets and functional equations on algebraic structures in [2,3], and their projections and some of their properties are considered. For semigroups (and even quasigroups) direct product of two subsets can be stated as follows:

If Δ and Ω are subsets of a semigroup $(S, \cdot)$, then the product $\Delta\Omega$ is called direct and it is denoted by $\Delta \cdot \Omega$ ($\Delta \dot{+} \Omega$ for additive notation) if the restricted binary map $\cdot|_{\Delta\times\Omega}$ is injective (equivalently, $\delta\Omega \cap \delta'\Omega = \emptyset$ for all distinct elements $\delta, \delta' \in \Delta$). By the notation $S = \Delta \cdot \Omega$, we mean $S = \Delta\Omega$ and the product $\Delta\Omega$ is direct and we say S is a *direct product* of (subsets) Δ and Ω. In this case we call Δ [resp. Ω] a left [resp. right] factor of S. It is easy to see that if Δ, Ω are non-empty subsets of a group G then

$$\Delta\Omega = \Delta \cdot \Omega \Leftrightarrow \Delta^{-1}\Delta \cap \Omega\Omega^{-1} = \{1\}.$$

If Δ and Ω are finite subsets of S, then $\Delta\Omega = \Delta \cdot \Omega$ if and only if $|\Delta\Omega| = |\Delta||\Omega|$.

Those have close relations to decomposer functions [2], and they also appear in the direct representation of periodic and upper periodic subsets of semigroups [3].

Example 1.1. Every subgroup of a group is a left and right factor. If Δ is a sub-semigroup of a group G but not a subgroup, then Δ is not a left or right factor of G (see Lemma 2.9 (a)). Hence $\mathbb{N}$ is not a factor of additive groups $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$. For every real number $b \neq 0$, $\mathbb{R}_b := b[0, 1)$ [resp. $b\mathbb{Z} = \langle b\rangle$] is a factor [resp. cyclic subgroup factor] of $\mathbb{R}$. If $|S| = p$, for a prime number p, and A is a non-singleton proper subset of S, then A is not a left or right factor.

Definition 1.2. *We call a subset A of finite semigroup (or groupoid) S a Lagrange subset if $|A|$ divides $|S|$.*

If S is finite then every left and right factor of S is a Lagrange subset. Since every subgroup of a (finite) group is a left and right factor then it is a Lagrange subset, and we arrive at the Lagrange theorem for groups.

2. Factors, Lagrange Subsets and Main Results

Now, we recall the upper periodic subsets of semigroups and some of their related definitions from [3], and then introduce a necessary and sufficient condition for a subgroup of a semigroup to be a factor. Also, we introduce a vast class of factors of cancelative semigroups.

In continuation S, X and G denotes a semigroup, groupoid and group (with the identity element e_G) respectively. Suppose A and B are subsets of S. A subset A is called *left [resp. right] upper B-periodic* if $BA \subseteq A$ [resp. $AB \subseteq A$]. If $A \subseteq BA$ [resp. $A \subseteq AB$], then we call it *left [resp. right] lower B-periodic.* If A is both left [resp. right] upper and lower B-periodic (i.e. $BA = A$ [resp. $AB = A$]), then we call it left [resp. right] B-periodic. Also we call A (two sided) upper [resp. lower] B-periodic if is both left and right upper [resp. lower] B-periodic (equivalently $BA \cup AB \subseteq A$ [resp. $A \subseteq BA \cap AB$]).

When we use the notation $H \dot{\leqslant} K$ [resp. $H \leqslant K$] it means that K is a semigroup or group and H is its sub-semigroup [resp. subgroup]. If $\Omega \subseteq X$, then we say X is right Ω-cancelative or Ω has right cancellation property in X if $\cdot|_{X\times\Omega}$ is injective with respect to the first variable, i.e. the map $r_\omega : X \to X$; $r_\omega(x) = \cdot(x, \omega) = x\omega$ is injective for every $\omega \in \Omega$.

Example 2.1. If $B^2 \subseteq B$ [resp. $B \subseteq B^2$] then BC [resp. CB] is left [resp. right] upper (resp. lower) B-periodic, for every $C \in 2^S$. For every subset A and B of X we put

$$Prd^{\ell}_B(A) := \{b \in B | bA = A\} \quad : \text{ The set of left periods of } A \text{ in } B$$

$$Uprd^{\ell}_B(A) := \{b \in B | bA \subseteq A\} \quad : \text{ The set of left upper periods of } A \text{ in } B$$

$$Lprd^{\ell}_B(A) := \{b \in B | A \subseteq bA\} \quad : \text{ The set of left lower periods of } A \text{ in } B$$

If $B = S$ then we may omit B in the notation.

It is clear that $Prd^{\ell}_B(A) = Uprd^{\ell}_B(A) \cap Lprd^{\ell}_B(A)$. If $B \dot{\leqslant} S$ then every non empty case of the above sets is a sub-semigroup of S. Especially if S is a monid, then $Uprd^{\ell}(A)$, $Lprd^{\ell}(A)$ and $Prd^{\ell}(A)$ are sub-monids of S, for every $A \subseteq S$. If $\emptyset \neq A \subseteq G$ then $Prd^{\ell}_A(A) = A$ if and only if $A \leqslant G$ if and only if $Prd^{r}_A(A) = A$.

Theorem 2.2. *(A necessary and sufficient condition for a subgroup of a semigroup to be a left factor) Let S be an arbitrary semigroup. A subgroup Δ of S is a left factor if and only if the equation $s = xs$ has only a solution $x = e_\Delta$ in Δ, for every $s \in S$.*

Proof. Let $\Delta \leqslant S$ and $S = \Delta \cdot \Omega$. Then e_Δ is a left identity of S, clearly. Now if $s = \delta_0 s$ for a given $s \in S$ and some $\delta_0 \in \Delta$, then $\delta\omega = (\delta\delta_0)\omega$ where $s = \delta\omega$, $\delta \in \Delta$ and $\omega \in \Omega$. So $\delta = \delta\delta_0$ and so $\delta_0 = e_\Delta$.

Conversely if $\Delta \leqslant S$ and the condition holds, then $Uprd^\ell(\Delta) = \Delta \leqslant S$ and so all conditions of Theorem 2.5 hold except that the right cancelation property of S. Therefore $S = \Delta\Omega$ and $\delta_1\omega_1 = \delta_2\omega_2$ implies $\omega_1 = \omega_2 = \omega$, where Ω, δ_1, δ_2 and ω_1, ω_2 are as in proof of the theorem. Hence

$$\omega = e_\Delta\omega = (\delta_1^{-1}\delta_1)\omega = (\delta_1^{-1}\delta_2)\omega,$$

where δ_1^{-1} denotes the inverse of δ_1 in Δ. Thus the hypothesis implies $\delta_1^{-1}\delta_2 = e_\Delta$ and so $\delta_1 = \delta_2$. $\square$

Corollary 2.3. *If Δ is a left factor subgroup of S then e_Δ is a unique left identity of S. Indeed, as more generality, we have:*

If $S = \Delta\Omega$ (not necessary direct product) where Δ is a right Ω-cancelative sub-semigroup and contains a left identity (l), then S (and Δ) contains a unique left identity and the equation $s = xs$ has only the solution $x = l$ in Δ, for every $s \in S$.

The following corollary is a generalization of Lagrange theorem for semigroups.

Corollary 2.4. *Let S be a finite semigroup and Δ an its subgroup. If the equation $s = xs$ (resp. $s = sx$) has only one solution $x = e_\Delta$ in Δ, for every $s \in S$, then $|\Delta|$ divides $|S|$.*

Now we prove another generalization for the topic.

Theorem 2.5. *Let S be a right cancelative semigroup containing a left identity l. If Δ is a subset of S such that*

(i) $s \in \Delta s\ :\ \forall s \in S$ (e.g., if $l \in \Delta$)

(ii) Δ *is right complete* Δ*-periodic (i.e.* $Prd^r_\Delta(\Delta) = \Delta$*).*

(iii) For every $\delta \in \Delta$ *there exists* $\sigma \in Uprd^\ell(\Delta)$ *such that* $\sigma\delta = l$*,*

then Δ *is a left factor of* S*.*

Proof. Consider the following equivalence relation in S

$$s_1 \sim_\Delta s_2 \Leftrightarrow \Delta s_1 = \Delta s_2 \tag{1}$$

There exists a subset Ω of all representatives of the equivalence classes induced by $\sim_\Delta$, by the axiom of the choice. So (i) implies $S = \Delta\Omega$. Now if $\delta_1\omega_1 = \delta_2\omega_2$ where $\delta_1, \delta_2 \in \Delta$ and $\omega_1, \omega_2 \in \Omega$, then applying (iii) we have

$$\omega_1 = l\omega_1 = (\sigma_1\delta_2)\omega_2 \in \Delta\omega_2.$$

Thus $\omega_1 = \delta_0\omega_2$ for some $\delta_0 \in \Delta$, and so (ii) implies

$$\Delta\omega_1 = \Delta(\delta_0\omega_2) = (\Delta\delta_0)\omega_2 = \Delta\omega_2.$$

So $\omega_1 = \omega_2$ and so $\delta_1 = \delta_2$, because S is right cancelative. $\square$

Corollary 2.6. *Let* S *be a right cancelative semigroup with a left identity* l*. If*

$$(i)\ \ l \in \Delta \dot{\leqslant} S \qquad (ii)\ \ \forall \delta \in \Delta\ \exists \sigma \in S\ :\ \sigma\Delta \subseteq \Delta\ ,\ \sigma\delta = l$$

then Δ *is a left factor sub-semigroup of* S*.*

Note. If $S = G$ is a group then the conditions of Corollary 2.6 hold if and only if $\Delta \leqslant G$. Therefore it is a generalization of the mentioned property that says every subgroup of a group is a factor.

Example 2.7. Let C be a non-empty set and consider the monoid $M = O_C$ of all surjective functions from C to C (with the composition operation). This monoid is right cancelative and $\Delta = \{f \in M | f \text{ is bijective}\}$ is its subgroup (the group of all bijections with the identity element ι_C). Since Δ is a subgroup then the conditions of Corollary 2.6 (and Theorem 2.5) hold, and so Δ is a <u>left</u> factor subgroup of M. Also Δ is a <u>right</u> factor subgroup of the monoid I_c containing of all injective functions from C to C. But neither Δ nor O_C, I_C are left or right factors of

C^C (the semigroup of all functions from C to C with the composition operation). For if $C = \{1, 2, 3\}$ then $|\Delta| = |O_C| = |I_C| = 6$, $|C^C| = 27$ and $6 \nmid 27$.

Note that we can also obtain these results by using Theorem 2.2. For if $f = gf$ where f is surjective, then $g = \iota_C \in \Delta$.

In continuation, we give more properties regarding to factorization of a semigroup by its two subsets.

Theorem 2.8. **(A)** *Let X be a groupoid such that $X = \Delta \cdot \Omega$, then*

(a) If X is left Ω-cancelative and Δ is a normal subset of X, then $X = \Delta \cdot \Omega = \Omega \cdot \Delta$, so Δ, Ω are (two-sided) factors of X.

(b) If Δ contains a left identity of X, then $\Delta\Omega' \cap \Omega = \Omega'$, for every $\Omega' \subseteq \Omega$.

(c) The map $\Psi : 2^\Omega \to 2^X$ by $\Psi(\Omega') = \Delta\Omega'$ is injective and $\Psi(\Omega') = \Delta \cdot \Omega'$.

(B) *Let S be a semigroup such that $S = \Delta \cdot \Omega$, then*

(a) If Δ is a left cancelative sub-semigroup of S, then S is left Δ-cancelative.

(b) Suppose that Δ, Ω are left cancelative sub-semigroups of S . If Δ is left Ω-cancelative (i.e. $\omega\delta_1 = \omega\delta_2$ implies $\delta_1 = \delta_2$, for every $\omega \in \Omega$, $\delta_1, \delta_2 \in \Delta$) and $\omega\Delta \subseteq \Delta\omega$, for every $\omega \in \Omega$, then S is left cancelative.

(c) (Unique direct representation of left upper Δ-periodic subsets for a left symmetric factor Δ)

If S contains a left identity l, and Δ is l-left symmetric, i.e.

$$\forall \delta \in \Delta \; \exists \delta' \in \Delta \; : \; \delta'\delta = l,$$

then every left upper Δ-periodic subset A has the unique direct representation

$$A = \Delta \cdot \Omega' = \Delta \cdot (A \cap \Omega), \tag{2}$$

where $\Omega' \subseteq \Omega$. So $\Omega \cap A$ is a right factor of A.

Proof. (A-a): We have $X = \Delta\Omega = \Omega\Delta$ and if $\omega_1\delta_1 = \omega_2\delta_2$, where $\delta_1, \delta_2 \in \Delta$ and $\omega_1, \omega_2 \in \Omega$, then $\delta_1'\omega_1 = \delta_2'\omega_2$, for some $\delta_1', \delta_2' \in \Delta$. Thus $\omega_1 = \omega_2$ and so $\delta_1 =, \delta_2$ (because X is left Ω-cancelative).

Therefore $X = \Delta \cdot \Omega = \Omega \cdot \Delta$.

(A-b): Clearly $\Omega' \subseteq \Delta\Omega' \cap \Omega$. Now if $x \in \Delta\Omega' \cap \Omega$, then $x = \delta\sigma = \omega = l\omega$, where $\delta \in \Delta$, $\sigma \in \Omega'$, $\omega \in \Omega$ and l is the left identity of X that is in Δ. So $\delta = l$ and $x = \omega = \sigma \in \Omega'$.

(A-c): Clearly, $\Delta\Omega' = \Delta \cdot \Omega'$, for every $\Omega' \subseteq \Omega$. Let $\Delta\Omega_1 = \Delta\Omega_2$, where $\Omega_1, \Omega_2 \subseteq \Omega$. Since $\emptyset \neq X = \Delta \cdot \Omega$, then $\Delta \neq \emptyset$. Hence $\omega_1 \in \Omega_1$ implies $\delta\omega_1 \in \Delta\Omega_1 = \Delta\Omega_2$, for every $\delta \in \Delta$, and so $\omega_1 \in \Omega_2$ (similarly $\Omega_2 \subseteq \Omega_1$).

(B-a): If $\delta s_1 = \delta s_2$, where $\delta \in \Delta$ and $s_1, s_2 \in S$, then $(\delta\delta_1)\omega_1 = (\delta\delta_2)\omega_2$, where $s_1 = \delta_1\omega_1$ and $s_2 = \delta_1\omega_2$. So $\delta\delta_1 = \delta\delta_2$, $\omega_1 = \omega_2$ and so $\delta_1 = \delta_2$. Therefore $s_1 = \delta_1\omega_1 = \delta_2\omega_2 = s_2$.

(B-b): If $ts_1 = ts_2$, where $t, s_1, s_2 \in S$, then $\delta\omega\delta_1\omega_1 = \delta\omega\delta_2\omega_2$, where $t = \delta\omega$, $s_1 = \delta_1\omega_1$, $s_2 = \delta_2\omega_2$, $\delta_1\delta_2 \in \Delta$ and $\omega_1\omega_2 \in \Omega$. So $\delta\delta_1'\omega\omega_1 = \delta\delta_2'\omega\omega_2$, for some $\delta_1', \delta_2' \in \Delta$ such that $\omega\delta_1 = \delta_1'\omega_2$ and $\omega\delta_2 = \delta_2'\omega_2$. Thus $\delta\delta_1' = \delta\delta_2'$ and $\omega\omega_1 = \omega\omega_2$ and so $\delta_1' = \delta_2'$, $\omega_1 = \omega_2$. Hence $\omega\delta_1 = \omega\delta_2$ thus $\delta_1 = \delta_2$. So $s_1 = \delta_1\omega_1 = \delta_2\omega_2 = s_2$.

(B-c): Let $\Delta A \subseteq A$ and put $\Omega' = \Omega \cap A$. Then $\Delta\Omega' \subseteq \Delta A \subseteq A$ and if $a \in A$, then $a = \delta\omega$, for some $\delta \in \Delta$ and $\omega \in \Omega$. Thus there exists $\delta' \in \Delta$ such that $\omega = l\omega = (\delta'\delta)\omega = \delta'(\delta\omega) = \delta' a \in \Delta A \subseteq A$, and so $\omega \in \Omega \cap A = \Omega'$. Therefore $A = \Delta\Omega'$. But $\Delta\Omega = \Delta \cdot \Omega$ and $\Omega' \subseteq \Omega$ imply $A = \Delta \cdot \Omega' = \Delta \cdot (\Omega \cap A)$. This direct representation is unique by the part (A-c). $\square$

2.1 Relations to decomposer functions

Let $(G, .)$ be a group and f a function from G to G. Also, consider the function f^* [resp. f_*], namely *left $*$-conjugate of f* [resp. *right $*$-conjugate of f*] defined by $x = f^*(x)f(x) = f(x)f_*(x)$, for all x. Then we call f:
(a) *right [resp. left] decomposer* if

$$f(f^*(x)f(y)) = f(y) \quad [\text{resp. } f(f(x)f_*(y)) = f(x)] \quad : \ \forall x, y \in G.$$

(b) *right [resp. left] strong decomposer* if

$$f(f^*(x)y) = f(y) \quad [\text{resp. } f(xf_*(y)) = f(x)] \quad : \forall x, y \in G.$$

(c) *right canceler* [resp. *left canceler*] if

$$f(xf(y)) = f(xy) \; [\text{resp. } f(f(x)y) = f(xy)] \; : \quad \forall x, y \in G.$$

(d) *associative* if

$$f(xf(yz)) = f(f(xy)z) \; : \quad \forall x, y, z \in G.$$

(e) *strongly associative* if

$$f(xf(yz)) = f(f(xy)z) = f(xyz) \; : \quad \forall x, y, z \in G.$$

In [2] all of the above functions are characterized in arbitrary groups. For example, the general form of the right [resp. left] decomposer functions is all right [resp. left] projections (as explained bellow) exactly.

Projections. If $X = \Delta \cdot \Omega$, then for every $x \in X$ we can define the surjective functions $P_\Delta : X \longrightarrow \Delta$, $P_\Omega : X \longrightarrow \Omega$ by $P_\Delta(x) = \delta$, $P_\Omega(x) = \omega$, where $x = \delta\omega$. The functions P_Δ, P_Ω are called left and right projections of the decomposition. So $P_\Delta, P_\Omega : X \longrightarrow \Delta \cup \Omega$ and $P_\Delta(A) = \Delta$, $P_\Omega(A) = \Omega$. If $X = S$ is a cancelative semigroup, then $S = \Delta \cdot \Omega$ implies $P_\Omega^* = P_\Delta$ and $P_{\Delta_*} = P_\Omega$. It is interesting to know that the integer and fractional part functions are the two projections related to the factorization $\mathbb{R} = \mathbb{Z} \dot{+} [0, 1)$.

The next lemma is directly concluded from many results of [2].

Lemma 2.9. *Let f be a function from G to G.*

(a) Every sub-semigroup of a group is a left or right factor if and only if it is a subgroup. Therefore, if $\Delta \dot{\leqslant} G$ and $\Delta \not\leq G$, then Δ is not a left or right factor of G.

(b) If f is left [resp. right] decomposer, then $f(G)$ and $f^*(G)$ [resp. $f(G)$ and $f_*(G)$] are right and left [resp. left and right] factors of G, respectively.

(c) If f is (two-sided) strong decomposer (equivalently strong associative), then $f(G)$ is a permutational factor of G (i.e., $G = \Delta \cdot f(G) = f(G) \cdot \Delta$, for some $\Delta \subseteq G$).

(d) If f is associative, then $f^{-}(e)f(G)$ and $f(G)f^{-}(e)$ are commutative standard factors of G.

Proof. Part (a): is concluded from Remark 2.7 and Corollary 2.9 from [2].

(b): If f is left [resp. right] decomposer, then $G = f(G) \cdot f_{*}(G)$ [resp. $G = f^{*}(G) \cdot f(G)$], by Theorem 2.1 of [2].

(c): If f is strong decomposer, then $f^{*}(G) = f_{*}(G) \trianglelefteq G$ and $G = f(G) \cdot f^{*}(G) = f^{*}(G) \cdot f(G)$, by Theorem 3.5 of [2].

(d) If f is associative, then the functions $f^{-}(e) \cdot f$ and [resp. $f \cdot f^{-}(e)$] is standard strong decomposer, by Theorem 3.2 and Corollary 3.3 of [2].

This fact together (c) imply (d). $\square$

Example 2.10. All real sets $(M, +\infty)$ and $[M, +\infty)$, where $M \geqslant 0$, are not factors of the real numbers group (by Lemma 2.9 (a)). But every half open interval in $\mathbb{R}$ is a (two-sided) factor. Because the function $f(x) = c + x + (c-d)[\frac{x}{d-c}]$ (where [ ] denotes the integer part) is decomposer, for every distinct real numbers d, c, and $f(\mathbb{R}) = [c, d)$ if $d > c$ and $f(\mathbb{R}) = (d, c]$ if $d < c$.

References

[1] G. Hajs, *ber einfache und mehrfache Bedeckung des n-dimensionalen Raumes mit einem Wrfelgitter*, Math. Z., 47 (1941), 427-467.

[2] M. H. Hooshmand and H. Kamarul Haili, *Decomposer and Associative Functional Equations*, Indag. Mathem., N.S., 18 (4) (2007), 539-554.

[3] M. H. Hooshmand, *Upper and Lower Periodic Subsets of Semigroups*, Algebra Colloquium, 18 (3) (2011), 447-460.

[4] S. Szabo, A. D. Sands, *factoring groups into subsets*, CRC Press, 2009.

Mohammad Hadi Hooshmand
Associate Professor of Mathematics
Young Researchers and Elite Club
Shiraz Branch, Islamic Azad University
Shiraz, Iran
E-mail: hadi.hooshmand@gmail.com