碩士學位請求論文

A Note About a Right Group in the Semigroup

指導教授 玄 進 五

濟州大學校 教育大學院

數學教育專攻

李 鍾 宇

1985 年度

A Note About a Right Group in the Semigroup

이를 教育學碩士學位 論文으로 提出함.

濟州大學校 教育大學院 數學教育專攻

提出者 李 鍾 宇

指導教授 玄 進 五

1985 年 5月 日

李鍾宇의 碩士學位 論文을 認准함.

濟州大學校 教育大學院

主 審 ____________________

副 審 ____________________

副 審 ____________________

1985 年 5月 　 日

감 사 의 글

본 논문이 나오기까지 아낌없이 지도해 주신 현진오 교수님께 감사드리며, 아울러 그 동안 많은 도움을 주신 수학과 여러 교수님께 감사드립니다.

그리고 그 동안 저에게 격려를 하여 주신 주위의 많은 분들에게 감사를 드립니다.

1985 년 5월 일

이 종 우

Contents

1. Introduction

In [1], J.M.Howie has induced the definition of group by the property of a semigroup. In [2], T.K. Dutta has studied the relative ideals in a group.

In this paper we will review the definitions and properties of a semigroup and study properties of a group as a semigroup. Finally we will study the theorem with respect to a right group with the help of [1] and [2].

2. The basic properties and definitions

Definition 2-1) Let S be a non-empty set on which a binary operation μ is defined.

We shall say that (S,μ) is a *semigroup* if μ is associative, i.e. if $((x,y)\mu, z)\mu = (x,(y,z)\mu)\mu$ for any $x,y,z \in S$.

Remark 2-2) Following the usual practice in algebra we shall write $(x,y)\mu$ simply as xy.

Definition 2-3) If a semigroup $(S,\cdot)$ has the additional property that $xy = yx$ for any $x,y \in S$, then it is called a *commutative semigroup*.

Definiton 2-4) If a semigroup$(S,\cdot)$ has an element 1 such that $x1 = 1x = x$ for any $x \in S$, then 1 is called an *identity (element)* of S and S is called a *semigroup with identity*, or *monoid*.

Remark 2-5) If a semigroup S has no identity element it is very easy to adjoin an extra element 1 to the set S. Then if we define $1s = s1 = s$, and $11 = 1$, $S \cup \{1\}$ becomes a semigroup with identity element 1.

Definition 2-6)

$$\text{Let } S^1 = \begin{cases} S & \text{if } S \text{ has an identity element} \\ S \cup \{1\} & \text{otherwise.} \end{cases}$$

S^1 is called *the semigroup obtained from* S *by adjoinig an identity if necessary*.

Definition 2-7) If S is any non-empty set and $xy = x$ for any x, $y \in S$, then S is called a *left zero semigroup*. *Right zero semigroup* are defined analogously.

Remark 2-8) If A and B are subsets of a semigroup S, we write

$$AB = \{ab \mid a \in A,\ b \in B\}$$

$$\{a\}B = aB = \{ab \mid b \in B\} \quad \text{for } a \in S.$$

It is easy to see that

$$(AB)C = A(BC) \quad \text{for any } A, B, C \subseteq S.$$

Proposition 2-9) If S is a semigroup with a, then the following properties are satisfied.

(1) $S^1 a = Sa \cup \{a\}$

(2) $aS^1 = aS \cup \{a\}$

(3) $S^1aS^1 = SaS \cup Sa \cup aS \cup \{a\}$

Proof) (1). If $x \in S^1a$, then $x = sa$ for some $s \in S \cup \{1\}$. Here if $s \in S$, then $x \in Sa \subset Sa \cup \{a\}$ and if $s \in \{1\}$, i.e. $s = 1$, then $x = sa = a \in \{a\} \subset Sa \cup \{a\}$. Thus $S^1a \subset Sa \cup \{a\}$.

Conversely, if $y \in Sa \cup \{a\}$, then $y \in Sa$ or $y \in \{a\}$. Here if $y \in Sa$, then $y = sa$ for some $s \in S$, it follows that $y = sa \in Sa \subset S^1a$ and if $y \in \{a\}$, i.e. $y = a \in \{1\}a \subset S^1a$, then $Sa \cup \{a\} \subset S^1a$. Now we can easily prove (2) and (3) by similar method.

Definiton 2-10) If a semigroup S has the property $aS = Sa = S$ for any $a \in S$, then S is called a *group*.

Proposition 2-11) Definition 2-10) is equivalent to the usual definiton.

Proof) Suppose that $aS = S = Sa$ for some $a \in S$. Then there exist $e, e' \in S$ such that $ae = a$, $e'a = a$. Let $g \in S$. Then there exist $u, v \in S$ such that $au = g = va$.

Here $ge = (va)e = v(ae) = va = g$ and

$$e'g = e'(au) = (e'a)u = au = g.$$

Thus $e = e'e = e'$ and $ge = eg = g$ for any $g \in S$. Hence e is the unigue identity in S. Since $e \in S$ and $aS = Sa = S$, there exist $a_1, a_2 \in S$ such that $e = aa_1$, $e = a_2a$ for any $a \in S$. It follows that $a_2e = a_2aa_1 = ea_1$, i.e. $a_1 = a_2$. Hence $a_1 = a_2 = a^{-1}$ is the unique inverse of a. Thus S is a group.

Conversely, if S is a group, then $x = s = aa^{-1}s \in aS$ for any $x \in S$. Since $aS \subset S$, we have $aS = S = Sa$.

Proposition 2-12) Definition 2-10) is equivalent to the fact that there exist x, y in S such that $ax = b$ $yb = b$ for any $a, b \in S$.

Proof) Suppose that $aS = Sa = S$ for any $a \in S$. Then there exist x, y in S such that $ax = b$, $ya = b$ for any $a, b \in S$.

Conversely, assume that there exist x, y in S such that $ax = b$, $ya = b$. If a belongs to S, then there exists x in S such that $ax = a \in aS$. Thus S is a subset of Sa. Since aS and Sa are subsets of S. Hence $S = aS = Sa$.

Definition 2-13) If $(S, \cdot)$ is a semigroup, then a non-empty subset T of S is called a *subsemigroup* of S if it is closed under the multiplication, i.e. if $xy \in T$ for any $x, y \in T$.

Definition 2-14) If $\varnothing$ is a mapping from a semigroup $(S, \cdot)$ into a semigroup $(T, \cdot)$ we say that $\varnothing$ is a *homomorphism* if $(xy)\varnothing = (x\varnothing)(y\varnothing)$ for any $x, y \in S$.

If $\varnothing$ is one-one we shall call it a *monomorphism*, and if it is both one-one and onto we shall call it an *isomorphism*.

Definition 2-15) Let S and T be semigroups. Then the Cartesian product $S \times T$ becomes a semigroup if we define $(s,t)(s',t') = (ss',tt')$. We shall refer to this semigroup as the *direct product* of S and T.

Definition 2-16) A non-empty subset A of a semigroup S is called a *left ideal* if $SA \subseteq A$, a *righ ideal* if $AS \subseteq A$, and a (two-sided) *ideal* if it is both a left and a right ideal.

Proposition 2-17) If S is a semigroup with a, then $Sa \cup \{a\}$ is the smallest left ideal and also $Sa \cup \{a\}$ is called the *principal ideal generated by a*.

Proof) If x belongs to $S(Sa \cup \{a\})$, then $x = st$ for some $s \in S$, $t \in Sa \cup \{a\}$. Thus $t = \alpha a$ or $t = a$ for some $\alpha \in S$. If $t = \alpha a$, then $x = s\alpha a = (s\alpha)a \in Sa$.
If $t = a$, then $x = sa \in Sa$. Hence S is a subset of $Sa \cup \{a\}$.

Furthermore, if T is the left ideal containing a, then sa belongs to T for any $s \in S$. Therefore $Sa \cup \{a\}$ is a subset of T.

3. The properties of a group as a semigroup

Proposition 3-1) Let S be a semigroup. Then S is a group if and only if the complement of every ideal (both left and right) is also an ideal.

Proof) Suppose that A be an ideal of group S and $x \in S/A$. We shall show that $tx \in S/A$ and $xt \in S/A$ for any $t \in S$.

Now, if $tx \in A$, then $t^{-1}(tx) = x \in A$. This is a contradiction, implying that $tx \in S/A$. And $xt \in S/A$ by the same method.

Conversely, assume that A and S/A are ideals of S. Let $t \in S$ and $a \in A$. Then $ta \in A$ and $ta \in S/A$, since S/A is an idal of S. Thus S has no any proper ideal. Hence $S = Sa = aS$ for any $a \in S$, since Sa is a left ideal and aS is a right ideal. There exist e and e′ in S such that $ae = a$ and $e'a = a$ for any $a \in s$.

Thus $e = e'e = e'$ and $ae = ea = a$, i.e. e is the unique identity in S. Since e belongs to S and $aS = Sa = S$ for any $a \in S$, there exist a_1, a_2 in S such that $e = aa_1$ and $e = a_2a$ for any $a \in S$.

Thus $a_2e = a_2aa_1 = ea_1$. Hence $a_1 = a_2 = a^{-1}$ is the unique inverse of a.

Proposition 3-2) Let S be a semigroup. Then S is a group if and only if the difference A−B of two ideals is an ideal.

Proof) Suppose that S is a group and A, B are ideals. Let $s \in S$ and $\alpha \in A-B$. Then $s\alpha$ belongs to A, since if $s\alpha$ belongs to B, $s^{-1}s\alpha = \alpha$ belongs to B. This is contradiction. Hence $s\alpha \notin B$. By similar method, $\alpha s \in A-B$. Therefore A−B is an ideal in S.

Conversely, consider A which is any ideal of S. Then $S-A$ is an ideal. Let $s \in S-A$ and $a \in A$. Then $sa \in A$ and $sa \in S-A$. Hence S has no proper ideal. We can hold the proof by proposition 3-1).

Definition 3-3) $I_B(S)$ is the *set of all ideals* of semigroup S. $I_L(S)$ is the *set of all left ideals* of S. $I_R(S)$ is the *set of all right ideals* of S. $P_L(S)$ is the *set of all left ideals* such that $sa \in A$ imply $a \in A$ for any $s \in S$. $P_R(S)$ is the *set of all right ideals* such that $as \in A$ implies $a \in A$ for any $s \in S$. $P_B(S)$ is the *set of all both ideals* such that $sa \in A$ implies $a \in A$ and $as \in A$ imply $a \in A$ for any $s \in S$.

Proposition 2-4) Let S be a semigroup.

(1) If S is a group then $I_L(S) = P_L(S)$ and $I_R(S) = P_R(S)$.

(2) S is a group if and only if $I_B(S) = P_B(S)$.

Proof) (1) Evidently, $I_L(S) \supseteq P_L(S)$. Let A be a left ideal and $ta \in A$. Then $(t^{-1})ta = a \in A$. Thus $A \in P_L(S)$ imply $I_L(S) = P_L(S)$. By similar method, $I_R(S) = P_R(S)$. (2) Suppose that S is a group. Then $P(S) \subseteq I(S)$. Let $A \in I_B(S)$, $at \in A$ and $ta \in A$. Then $(at)t^{-1} = a \in A$ and $(t^{-1})ta = a \in A$. Hence $I_B(S) = P_B(S)$.

Conversely, assume that $I_B(S) = P_B(S)$. Let A be an ideal. We shall that G/A is also an ideal. Let $a \in G/A$ and $t \in S$. Then $at \in G/A$ and $ta \in G/A$, since if $ta \in A$ and $at \in A$ then $a \in A$. Hence G/A is also an ideal.

Proposition 3-5) Let S be a monid and let $M_I(S)$ be the set of all ideals of S which contain an identity. Then $M_I(S)$ is a monoid with a zero and $M_I(S) = \{S\}$.

Proof) Since $(AB)C = A(BC)$ for $A, B, C \in M_I(S)$, $S(AB) = (SA)B \subseteq AB$ and $(AB)S = A(BS) \subseteq AB$. Since $1 \in A$ and $1 \in B$, $1 \in AB$. Thus $AB \in M_I(S)$. Let $A \in M_I(S)$. Then $SA \subseteq A$ and $AS \subseteq A$. Since S has an identity, $A \subseteq SA$ and $A \subseteq AS$. Thus $SA = AS = A$, i.e. S is an identity in $M_I(S)$. Hence $M_I(S)$ is a monoid

Let $A \in M_1(S)$. Then A has an identity. Thus $AS = SA = S$, i.e. S is a zero element. Therefore $M_1(S) = \{S\}$.

4. Main Theorem

Definition 4-1) If S is a semigroup and $e \in S$ with $ee = e^2 = e$, then e is called an *idempotent*.

Definifion 4-2) An equivalence relation L (R) on a semigroup S is defined by the rule that $a L b$ (aRb) if and only if a and b generate the same principal left(right) ideal that is $S^1 a = S^1 b$ ($aS^1 = bS^1$).

Definition 4-3) A semigroup S is called *right simple* (*left simple*) if $R = S \times S$ ($L = S \times S$)

Definition 4-4) A semigroup is called *right cancellative* (*left cancellative*) if $ac = bc$ implies $a = b$ (if $ca = cb$ implies $a = b$) for all $a, b, c \in S$.

Definition 4-5) A semigroup that is right simple and left cancellative is called a *right group*.

Lemma 4-6) A semigroup S is right simple and left simple if and only if it is a group.

Proof) Suppose that a semigroup S is a group.

For any $a, b \in S$ we can consider $b = ba^{-1}a, a = ab^{-1}b$. Thus $S^1b = S^1ba^{-1}a \subseteq S^1a$ and $S^1a = S^1ab^{-1}b \subseteq S^1b$, i.e. $(a, b) \in L$.

Hence $S \times S = L$.

By similar method, $S \times S = R$.

Conversely, assume that a semigroup S is right simple and left simple. Then $aS^1 = bS^1$ and $S^1a = S^1b$ for any $a, b \in S$. If aS^1 is a singleton set then the proof is trivial.

Now, we can consider $\alpha \in aS^1$ with $\alpha \neq a$, i.e. $\alpha \in aS$. Since $bS^1 = aS^1 \subseteq aSS^1 \subseteq aS$ and $b \in bS \subseteq aS$, there exists x in S such that $b = ax$.

By similar method, there exists y in S such that $b = ya$.

Hence S is a group by proposition 2-12).

<u>Lemma 4-7)</u> The set E of idempotents of right group S is non-empty.

<u>Proof)</u> Suppose that E is the set of idempotents of right group S. Since S is right simple, there exists x in S such that $ax = a$ for any $a \in S$ by Lemma 4-6).

Here $ax = (ax)x = ax^2$, i.e. $x = x^2$. Thus $x \in E$. Hence E is non-empty.

<u>Lemma 4-8)</u> The set E of idempotents of right group S is a right zero subsemigroup of S.

Proof) Suppose that E is the set of idempotents of right group S. Since $e^2 f = ef$ for any $e, f \in E$, and S is left cancellative. Hence $ef = f$.

Lemma 4-9) If $e \in E$ then Se is a subgroup of S.

Proof) Since $(Se)(Se) \subset SSSe \subset Se$ and $a = xe$ for some $x \in S$ and $a \in Se$, $ae = xee = xe = a$.

Thus e is the identity of S and e is the right identity in Se. Since S is right simple and S has an identity e, $aS = bS$ for any $a, b \in S$. Thus $aS = eS = S$ and there exists x in S such that $ax = e$ for any $a \in S$. Hence $a(xe) = axe = ee = e$, i.e. xe is the right inverse of a.

Lemma 4-10) The direct product of two right simple semigroups is right simple.

Proof) Let S, T be right simple semigroups. Then there exist x in S and y in T such that $ax = c$, $by = d$ for every $a, c \in S$ and $b, d \in T$. Thus $(a,b)(x,y) = (ax, by) = (c,d)$, i.e. $(a,b)S \times T = S \times T$ for any $a \in S, b \in T$. Hence $S \times T$ is right simple.

Lemma 4-11) The direct product of two left cancellative semigroups is left cancellative.

Proof) Let S, T be left cancellative semigroups and let $(c_1,$

$c_2)(a_1, b_1) = (c_1, c_2)(a_2, b_2)$ for $(a_1, b_1), (a_2, b_2), (c_1, c_2) \in S \times T$.

Then $(c_1 a_1, c_2 b_1) = (c_1 a_2, c_2 b_2)$ and $c_1 a_1 = c_1 a_2$, $c_2 b_1 = c_2 b_2$. Thus $a_1 = a_2$, $b_1 = b_2$. Hence $(a_1, b_1) = (a_2, b_2)$.

Lemma 4-12) A right zero semigroup E is a right group.

Proof) Since $xy = y$ for any $x, y \in E$. Thus $xE = E$ for any $x \in E$, i.e. E is right simple, and if $ca = cb$ for $a, b, c \in E$ then $a = b$. Hence E is left cancellative.

Theorem 4-13) A semigroup S is a right group if and only if it is isomorphic to a direct product of a group G and a right zero semigroup E.

Proof) Let G be a group and let E be a right zero semigroup. Then $G \times E$ is a right group by Lemma 4 - 10, 4 - 11, 4 - 12).

Conversely, suppose that a semigroup S is a right group. Consider a fixed element f of E, $G = S_f$ and a function $\varnothing : G \times E \to S$ defined by $(a, e)\varnothing = ae$.

For any $a, b \in G$ and $e, g \in E$,

$\{(a, e)(b, g)\}\varnothing = (ab, eg)\varnothing = abeg = abg$ and

$(a, e)\varnothing(b, g)\varnothing = (ae)(bg) = a(eb)g = abg$. Thus

$(a, e)\varnothing(b, g)\varnothing = \{(a, e)(b, g)\}\varnothing$. Hence $\varnothing$ is a homormorphism.

And if $(a, e)\varnothing = (b, g)\varnothing$ then $ae = bg$. Since f is an identity of $G = S_f$, $a = af = aef = bgf = bf = b$, $ae = bg = ag$ and $e = g$. This implies that $\varnothing$ is injective. We last determine that $\varnothing$ is surjective. If $a \in S$, then there exists e in S such that $ae = a$. Thus $aee = ae$ implies $e^2 = e$, i.e. $e \in E$. Hence $af \in S_f = G$ and $(af, e)\varnothing = afe = ae = a$, and theorem 4-13) is established.

References

[1] Dutta, T.K. Relative ideals in groups. Kyungbook Math. J. 22, 1982.

[2] Howie, J.M. An introduction to semigroup theory. Academic press, 1976.

[3] Hungerford, T.W. Algebra. Holt Rinehart and winstone Inc., 1974.

[4] Suzuki. Group theory 1. Springer, 1982.

<國 文 抄 錄>

半群에서 右群에 관한 研究

李 鍾 宇

濟州大学校教育大学院 数学教育専攻
(指導教授 玄 進 五)

본 論文에서는 半群으로서의 群의 여러가지 성질을 다루었으며 최종적으로 右群과, 群과 右零半群의 直積은 서로 동형임을 보였다.