Multiplicative Ideal Theory of Semigroups

Ryuki MATSUDA*, Akira OKABE** and Iwao SATO**

ABSTRACT

The multiplicative ideal theory has been developped for commutative rings. The aim of this paper is to give a semigroup version of the multiplicative ideal theory of commutative rings. In this paper we shall prove some fundamental properties of ideals of G-semigroups. Here we call a torsion-free cancellative abelian additive semigroup with identity a G-semigroup, where G stands for Gilmer. It is expected that the ideal theory of G-semigroups is more simpler than that of commutative rings. But the multiplicative ideal theory of semigroups is itself interesting and important. For the multiplicative ideal theory of rings, we refer to [G1] and [LM].

1. Introduction.

An abelian (additive) semigroup $(S,+)$ with identity is called a monoid. The identity of a monoid S is denoted by 0. A monoid S is said to be cancellative, if $a+b=a+c$ where a,b,c are in S, then $b=c$, and S is said to be torsion-free if $ns=nt$, where $n\in N$ and s,t in S, then $s=t$. In [N], a cancellative monoid is called a grading monoid.

An abelian (additive) group G is called torsion-free if $na=0$ with $n\in N, a\in G$, then $a=0$. A subsemigroup $S\supset\{0\}$ of a torsion-free abelian group is a torsion-free grading monoid. In our paper we call a torsion-free grading monoid a G-semigroup, where G stands for Gilmer.

Let S be a G-semigroup. A subset $I\neq\phi$ of S is called an ideal of S if $S+I\subseteq I$. For each $x\in S$, set $(x)=x+S$. Then (x) is an ideal of S. An ideal I of S is called a principal ideal if $I=(x)$ for some $x\in S$. If each ideal of S is principal, then S is called a principal ideal semi-group(for short, PIS).

An element x of S is called a unit if $x+y=0$ for some $y\in S$. For $x\in S$, x is a unit if and only if $(x)=S$. If B is a nonempty subset of S, then $B+S=\{b+s \mid b\in B, s\in S\}$ is the ideal of S generated by B. An ideal A of S is called proper if $A\neq S$. An ideal A of S is called idempotent if $A=A+A$.

Let U be the set of units of S. Then $M=S\setminus U$ is an ideal of S that contains all other proper ideals of S and is called the maximal ideal of S. If I is an ideal of S, then the radical of I, denoted by $\sqrt{I}$, is defined to be $\sqrt{I}=\{s\in S \mid ns\in I \text{ for some } n\in N\}$. One easily see that $\sqrt{I}$ is an ideal of S.

Let $P\subset S$ be an ideal. Then P is called a prime ideal if $s_1+s_2\in P$ for $s_1,s_2\in S\Rightarrow s_1\in P$ or $s_2\in P$. An ideal Q of S is called a primary ideal if $s_1+s_2\in Q$ and $s_1\notin Q\Rightarrow ns_2\in Q$ for some $n\in N$. For a primary ideal Q of S, $\sqrt{Q}$ is a prime ideal. $\sqrt{Q}$ is called a prime ideal belonging to Q. Q is called a primary ideal belonging to $\sqrt{Q}$, or Q is $\sqrt{Q}$-primary.

If A is an ideal of S such that A can be expressed as a finite intersection of primary ideals $A=\bigcap_{i=1}^{n} Q_i$, then this representation of A is said to be a shortest representation of A if $\bigcap_{j\neq i} Q_j\neq A$ for each $1\leqq i\leqq n$, and $Q_1,\ldots, Q_n$ are mutually distinct.

* Department of Mathematics, Ibaraki University, Mito, Ibaraki 310, JAPAN

** Oyama National College of Technology, Oyama, Tochigi 323, JAPAN

<u>(1.1)Proposition</u>. Let $A=\cap_{i=1}^{n} Q_i$ be a shortest representation of A. Then the number n is uniquely determined, that is, if $A=\cap_{j=1}^{m} Q_j'$ be another shortest representation of A, then $n=m$.

Two elements a and b in S are said to be <u>associated</u> if there exists a unit u such that $b=a+u$(or equivalently, $a=b+v$ for some unit v). Let $s,s'\in S$. If $s+a=s'$ for some $a\in S$, then s is called a <u>divisor</u> of s'and s' is called a <u>multiple</u> of s. In this case, we denote $s \mid s'$. Note that divisors of 0 are units of S. If $s \mid s'$ and $s' \mid s$, then s and s' are associated. An element s of S is called an <u>irreducible element</u> if it satisfies the following conditions:
(1) s is not a unit.
(2) If $s=s_1+s_2$ $(s_i\in S)$, then either s_1 or s_2 is a unit.
A G-semigroup S is called a <u>unique factorization semigroup</u>(for short, a <u>UFS</u>) if it satisfies the following conditions:
(UF1) Every non-unit of S can be written as a finite sum of irreducible elements.
(UF2) If $a=p_1+p_2+\dots+p_n=q_1+q_2+\dots+q_m$, where p_i and q_j are irreducible, then $n=m$ and on re-numbering p_i and q_i are associated for each i.
In the case of $n=0$, we refer that a is a unit.

We shall consistently use Z to denote the ring of all integers, Z_0 to denote the set of nonnegative integers, and Q to denote the field of rational numbers. The symbol $\subseteq$ will denote containment; $\subset$ denotes proper containment. If A and B are sets, then $A\setminus B$ denotes the set of elements of A which are not in B. $|A|$ denotes the cardinal number of the set A. We use ϕ to denote the empty set.

2. Additive systems

Let T be a nonempty subset of a G-semigroup S. T is called an <u>additive system</u> in S, in case, if $t, t'\in T$, then $t+t'\in T$. For an additive system T, the <u>quotient semigroup</u> S_T is defined as follows:

$$S_T=\{s-t \mid s\in S, t\in T\}.$$

It is easy to see that S_T is a G-semigroup. Especially, if $T=S$,then the quotient semigroup $S_S=\{s_1-s_2 \mid s_1,s_2\in S\}$ is called the <u>quotient group</u> of S, and is denoted by q(S). Note that q(S) is an abelian (additive) group.

<u>(2.1)Remark</u>.
(1) Let S be a G-semigroup. Then S is torsion-free if and only if the quotient group is torsion-free.
(2) S is a canncellative subsemigroup of q(S) and the subsemigroup of $G=q(S)$ generated by S and $\{-s \mid s\in S\}$ is G. Each element of G is a unit of G.

<u>(2.2)Remark</u>. Let I be an ideal of a G-semigroup S. Then I is a prime ideal of S if and only if $S\setminus I$ is an additive system of S.

Let A be an ideal of S and T a subset of S. Then, set $A\text{-}T=\{x\in S \mid x=a-t,\ a\in A,\ t\in T\}$.

<u>Proof of (1.1)</u>. Set $\sqrt{Q_i}=P_i$, $\sqrt{Q_j}\,'=P_j'$. Let P be any one of $P_1,\dots,P_n$. Then it is enough to show that $P=P_j'$ for some j. Suitably changing the order, we assume that

$$P_1,\dots,P_{s-1}\subset P,\ P_s=P,\ P_s+1,\dots,P_n\not\subseteq P;\quad P_1',\dots,P_t'\subset P,\ P'_{t+1},\dots,P_m'\not\subseteq P.$$

Set $S\text{-}P=T$. Then we have

$$A\text{-}T=Q_1\cap\dots\cap Q_s=Q_1'\cap\dots\cap Q_t'.$$

If $P\neq P_j'$ $(1\leqq \forall j\leqq t)$, then there exists $a\in P$ such that

$$a \notin P'_1 \cup \ldots \cup P'_t \cup P_1 \cup \ldots \cup P_{s-1}.$$

Furthermore, there exists $k \in N$ such that

$$ka \in Q_s \text{ and } ka \notin Q'_1 \cup \ldots \cup Q'_t \cup Q_1 \cup \ldots \cup Q_{s-1}.$$

Thus we have

$$Q_i : ka = Q_i \ (1 \leqq i \leqq s\text{-}1),\ Q'_j : ka = Q'_j \ (1 \leqq j \leqq t),$$

where $A : U = \{x \in S \mid U + x \subset A\}$ for an ideal A and a subset U of S.
Therefore it follows that

$$(A\text{-}T) : ka = (\cap_{i=1}^{s-1} Q_i) : ka = Q_1 \cap \ldots \cap Q_{s-1}$$

and

$$(A\text{-}T) : ka = (\cap_{j=1}^{t} Q'_j) : ka = Q'_1 \cap \ldots \cap Q'_t = Q_1 \cap \ldots \cap Q_s.$$

But this is a contradiction.

(2.3)Lemma. Let T be an additive system of a G-semigroup S and let A be an ideal of S such that $A \cap T = \phi$. Then there is a prime ideal P of S such that $A \subseteq P$ and $P \cap T = \phi$.

Proof. By Zorn's Lemma, there is a maximal ideal P in the set $L = \{J \mid J$ is an ideal of S such that $A \subseteq J$ and $J \cap T = \phi\}$. If $x, y \in S \setminus P$, then $P \cup (x)$ and $P \cup (y)$ meet T so that $x + s_1,\ y + s_2 \in T$ forsome $s_1, s_2 \in S$. Then $x + y + s_1 + s_2 \in T$ and so $x + y \in S \setminus P$. Hence P is a prime ideal of S.

Let T be an additive system of S. Then the set $\{s \in S \mid s$ divides some element of $T\}$ is called the saturation of T. If the saturation of T coincides with T, then T is called a saturated additive system.

(2.4)Proposotion. Let T be an additive system in S, and let T' be the complement of T in S. The following conditions are equivalent:

(1) T is saturated.

(2) T' is the union of a set of prime ideals of S.

Proof. (1)⇒(2): We show that $T' = \cup \{P_\lambda \mid P_\lambda$ is a prime ideal of S not meeting $T\}$. $\supseteq$ is clear. Conversely, if $x \in T'$, then $(x) \cap T = \phi$, and so by (2.3), $(x) \subseteq P_\lambda$ for some prime ideal P_λ such that $P_\lambda \cap T = \phi$. Hence $\subseteq$ also holds.

(2)⇒(1): This is evident.

(2.5)Theorem. Let T be the quotient group of a G-semigroup R and let S_1 and S_2 be subsemigroups of T containing R such that $S_1 \subset S_2$.

(1) If S_2 is a quotient semigroup of R, then S_2 is a quotient semigroup of S_1.

(2) If S_1 is a quotient semigroup of R and if S_2 is a quotient semigroup of S_1,then S_2 is a quotient semigroup of R.

Proof. (1): Suppose that $S_2 = R_N$, where N is an additive system of R. Then it is easily seen that $S_2 = (S_1)_N$.

(2): Let $S_1 = R_{M_1}$ and $S_2 = (S_1)_{M_2}$. Then we shall show that $S_2 = R_M$, where $M = \{x \in R \mid x$ is a unit of $S_2\}$. Since $M_1 \subseteq M$, $S_1 = R_{M_1} \subseteq R_M$. Now let $u \in M_2 \subset S_1$. Then $u = r\text{-}v$ for some $r \in R$, $v \in M_1$, and then we have $r = u + v$, where u and v are units of S_2. Hence $r \in M$ and so $-u = v\text{-}r \in R_M$. Thus $-M_2 = \{-u \mid u \in M_2\} \subseteq R_M$, and then $S_2 = (S_1)_{M_2} \subseteq (R_M)_{M_2} = R_M$, i.e., $S_2 = R_M$.

If R is a G-semigroup and S is a semigroup such that $R \subset S \subset q(R)$, then S is said to be a oversemigroup of R. By (2.1), S is torsion-free, and so is a grading monoid.

(2.6)Corollary. If A is an ideal of a G-semigroup R and if $\{P_\lambda\}_{\lambda \in \Lambda}$ is the set of prime ideals of R containing A, then $\sqrt{A} = \cap P_\lambda$.

Proof. This follows from (2.3).

3. Fractional ideals

Let R be a G-semigroup and let T be the quotient group of R. A subset F of T is said to be a fractional ideal of R if $R+F \subseteq F$ and $r+F \subseteq R$ for some $r \in R$. Each ideal of R is called an integral ideal. For $t_1,\ldots,t_n \in T$, set $(t_1,\ldots,t_n) = \cup(t_i+R)$. This is a fractional ideal of R. The set $\{t_1,\ldots,t_n\}$ is called a generating set or a set of generators. A fractional ideal A of R is called finitely generated if there exist a finite set $\{t_1,\ldots,t_n\}$ of generators such that $A=(t_1,\ldots,t_n)$. If there exists $t \in T$ such that $A=(t)$, then A is said to be a principal fractional ideal.

Denote by F(R) the set of fractional ideals of a G-semigroup R, and by $F^*(R)$ the set of finitely generated fractional ideals of R. If $F_1,F_2 \in F(R)$, then F_1+F_2 is defined by $\{x+y \mid x \in F_1, y \in F_2\}$. And we define $[F_1:F_2]_T$ to be $\{x \in T \mid x+F_2 \subseteq F_1\}$. If F_1 and F_2 are integral ideals,then $F_1:F_2$ is defined by $\{x \in R \mid x+F_2 \subseteq F_1\}$.

(3.1)Theorem. Let R be a G-semigroup and let T be the quotient group of R.
(1) F(R) is closed under addition and finite intersection. If $F_1,F_2 \in F(R)$, then $[F_1:F_2]_T \in F(R)$.
(2) If $F_1,F_2 \in F(R)$ and if S_i is a set of generators for F_i,then $S_1 \cup S_2$ is a set of generators for $F_1 \cup F_2$ and $\{s+t \mid s \in S_1, t \in S_2\}$ is a set of generators for F_1+F_2. $F^*(R)$ is closed under union.
(3) If A is an integral ideal of R and if r is an element of R, then A-r is a fractional ideal of R.
(4) If $F \in F(R)$, then there is an integral ideal A of R and $r \in R$ such that $F=A-r$.

Proof. The proof is straightforward, and we omit it.

If each ideal of S is finitely generated, then S is said to be a Noetherian semigroup.

(3.2)Theorem. If each prime ideal of a G-semigroup R is finitely generated, then R is Noetherian.

Proof. Suppose that R is not Noetherian. Then there exists an ideal B of R maximal with respect to not being finitely generated. Moreover, it is easily shown that B is a prime ideal of R, contrary to our hypothesis. Therefore R is Noetherian.

4. Quotient semigroups

Let R and S be G-semigroups, and Ψ a homomorphism from R onto a subsemigroup of S. Let A be an ideal of R. Then the extension A^e of A is the ideal of S generated by $\Psi(A)$. Furthermore,let α be an ideal of S. Then the contraction α^c of α is defined by $\alpha^c = \Psi^{-1}(\alpha) = \Psi^{-1}(\alpha \cap \Psi(R))$.

(4.1)Theorem. Let R be a G-semigroup, N an additive system of R and $S=R_N$. Let Ψ be the canonical embedding of R into $S=R_N$. Then the following hlod.

(1) For an ideal B of R, $B^e=\{b\text{-}n \mid b\in B, n\in N\}$, $B^{ec}=\{x\in R \mid x+n\in B$ for some $n\in N\}$.
(2) For an ideal β of S, $\beta^{ce}=\beta$.
(3) For ideals A,B of R, $(A\cap B)^e=A^e\cap B^e$.
(4) If B is a finitely generated ideal of R, then $(A:B)^e=A^e:B^e$.
(5) For ideals α,β of S, $(\alpha:\beta)^c=\alpha^c:\beta^c$.
(6) For an ideal B of R, $(\sqrt{B})^e=\sqrt{B^e}$.

Proof. The proof, being routine, will be omitted.

(4.2)Theorem. Let R be a G-semigroup, and let N be an additive system in R. If $\{P_\alpha\}$ is the set of prime ideals of R which do not meet N, then $\{P_\alpha^e\}$ is the set of proper prime ideals of R_N. If $P\in\{P_\alpha\}$ and if $\{Q_\beta\}$is the set of P-primary ideals of R, then $\{Q_\beta^e\}$ is the set of P^e-primary ideals of R_N.

(4.3). Let $\{M_\lambda \mid \lambda\}$ be a nonempty set of prime ideals of a G-semigroup R satisfying the following conditions:
(1) There are no containment relations among distinct members of the set $\{M_\lambda \mid \lambda\}$.
(2) Each prime ideal of R contained in $\cup_\lambda\ M_\lambda$ is contained in some M_λ.
If these two conditions hold, then $\{M_\lambda^e \mid \lambda\}$ is the set of ideals of R maximal with respect to not meeting N, where $N=R\text{-}(\cup_{\lambda\in\Lambda} M_\lambda)$.

As a corollary of (4.3), we have the following.

(4.4)Corollary. If $\{P_\beta \mid \beta\}$ is the set of ideals of a G-semigroup R maximal with respect to not meeting the additive system N in R, then $\cup_\beta\ \{P_\beta^e \mid \beta\}$ is the maximal ideal of R_N.

Let S be a G-semigroup and R an extension G-semigroup of S. Then R is called an extension semigroup of S,and S is said to be a subsemigroup of R.

(4.5)Proposition. Let S be a subsemigroup of a G-semigroup R, and let $P_1,\dots,P_r$ be prime ideals of R such that $S\subset\cup P_i$. Then $S\subset P_i$ for some i.

Proof. Since $0\in S\subset\cup P_i$, $0\in P_k$ for some k. Then $S\subset R=P_k$.

(4.6)Remark. Let A be an ideal of a G-semigroup R, and let $P_1,\dots,P_r$ be ideals of R such that $A\subset\cup P_i$,and at most two of the ideals P_i are not prime. Then it is not necessarily true that $A\subset P_i$ for some i as the following example shows.

(4.7)Example. Let $R=\{0,2,3,4,5,\dots\}$, $A=\{2,3,4,5,\dots\}$, $P_1=(2)$ and $P_2=(3)$. Then $A\subset P_1\cup P_2$, but $A\not\subset P_1, A\not\subset P_2$.

For an ideal P of a G-semigroup R, set R_{R-P} by R_P. Then R_P is called the locarization at P. If A is an ideal of R and P is a prime ideal of R containing A, then P is called a minimal prime ideal of A if there is no prime ideal P_0 of R such that $A\subseteq P_0\subset P$. Each ideal B of R has minimal prime ideals.

Let P be a minimal prime ideal of an ideal A of R. We consider an extension from R to R_P. Then P^e is the unique minimal prime of A^e: that is, $P^e = \sqrt{A^e}$. $A^{ec} = \{x \in R \mid x+y \in A$ for some $y \in R-P\}$ is P-primary. This ideal A^{ec} is called the isolated P-primary component of A.

The set $\{x \in R \mid x+y \in kP$ for some $y \in R-P\}$, where $kP = \{a_1 + \ldots + a_k \mid a_i \in P, 1 \leqq i \leqq k\}$ is called the k th symbolic power of P and is denoted by $P^{(k)}$.

5. Some fundamental properties of quotient semigroups

(5.1)Proposition. Let S_N be a quotient semigroup of S with additive system N of S and M be the saturation of N. Then $M = \{x \in S \mid -x \in S_N\}$.

(5.2)Proposition. Let N be an additive system in a G-semigroup S and M be the saturation of N. Then $S_N = S_M$.

Proof. It is clear that $S_N \subseteq S_M$. Conversely, let $x = r-m \in S_M$, $r \in S$, $m \in M$. By hypothesis, we have $n = m+t \in N$ with $t \in S$. Since $r+t \in S$, $n \in N$, we have $x = (r+t)-n \in S_N$. Hence $S_M \subseteq S_N$.

(5.3)Lemma. If N is an additive system in a G-semigroup S,and P is a prime ideal of S not meeting N, then $S_P = (S_N)_{PS_N}$, where $PS_N = \{s-n \mid s \in P, n \in N\}$.

Proof. Let $x = r-s \in S_P$, $r \in S$, $s \in S-P$. Then, since $r-n \in S_N$, $s-n \in S_N - PS_N$ for $n \in N$, we have $x = r-s = (r-n)-(s-n) \in (S_N)_{PS_N}$. Hence we can define a mapping $\rho : S_P \rightarrow (S_N)_{PS_N}$.

Conversely, let $x = (r-n_1)-(s-n_2) \in (S_N)_{PS_N}$, $r \in S$, $s \in S-P$, $n_1, n_2 \in N$. Then we have $x = (r+n_2)-(s+n_1) \in S_P$. Hence we can define a mapping $\sigma : (S_N)_{PS_N} \rightarrow S_P$. Then we have $\rho \circ \sigma = \sigma \circ \rho = 1$(the identity map).

(5.4)Lemma. Let $\{P_\lambda\}_{\lambda \in \Lambda}$ be a set of prime ideals of S such that $\{P_\lambda\}$ satisfies the conditions of (4.3). If we set $N = S - \bigcup_{\lambda \in \Lambda} P_\lambda$, then $S_N = \bigcap_{\lambda \in \Lambda} S_{P_\lambda}$.

Proof. The proof is straightforward and will be omitted.

(5.5)Corollary. Each quotient semigroup of a G-semigroup S is an intersection of locarizations of S.

Proof. This immediately follows from (5.4).

6. Cancellation laws for ideals

An element s of a semigroup S is called cancellative if $s+a = s+b$ implies $a = b$ for $a, b \in S$. Let C be the set of cancellative elements of S. If $C \neq \phi$, then C is a subsemigroup of S. If $t \in S$ is invertible(see section 7), then t is cancellative.

(6.1)Theorem. Let $A = (a_1, \ldots, a_k)$ be a finitely generated ideal of S. If B,C are ideals of S such that $A+B \subset A+C$, then $kB \subset C$.

Proof. For $b_1, \ldots, b_k \in B$, we need only to show that $b_1 + \ldots + b_k \in C$. By hypothesis, $a_1 + b_1 = a_{i_1} + c_1$

with $c_1 \in C$. If $i_1=1$, then $b_1=c_1$ and $b_1+\ldots+b_k=c_1+b_2+\ldots+b_k \in C$. Suppose that $i_1 \neq 1$. Then $a_{i_1}+b_2=a_{i_2}+c_2$ with $c_2 \in C$. If $i_2=1$, then $a_1+a_{i_1}+b_1+b_2=a_{i_1}+a_1+c_1+c_2$ and so $b_1+b_2=c_1+c_2 \in C$. Hence $b_1+\ldots+b_k=c_1+c_2+b_3+\ldots+b_k \in C$. Iterating this procedure, we can find an integer $l \leqq k$ such that $b_1+\ldots+b_l=c_1+\ldots+c_l \in C$, and then $b_1+\ldots+b_k \in C$.

(6.2)Corollary. Let $A=(a_1,\ldots,a_k)$ be a finitely generated ideal of S. If B,C are ideals of S such that $A+B=A+C$, then $kB \subseteq C$ and $kC \subseteq B$, and hence $\sqrt{B}=\sqrt{C}$.

Proof. Let $A=(a_1,\ldots,a_k)$. Then, by (6.1), $kS \subseteq B$, since $A+S=A+B$. Hence $0 \in B$, i.e., $S=B$.

(6.3)Corollary. Let A be a finitely generated ideal of S such that $2A=A$. Then $A=S$.

Proof. Since $A=2A=A+A \subseteq A+S \subseteq A$, $A+A=A+S$. Then, by (6.2), $\sqrt{A}=\sqrt{S}=S$, and so $A=S$.

A fractional ideal F of S is called a cancellation ideal if $A+I \subset A+J \Rightarrow I \subset J$ for all $I,J \in F(S)$.

Let T be the quotient group of a G-semigroup S and let C be the set of all cancellation fractional ideals of S.

(6.4)Theorem.

(a) For $F \in F(S)$, the followings are equivalent:

(1) $F \in C$.

(2) If $F_1,F_2 \in F(S)$, $F+F_1 \subset F+F_2$, then $F_1 \subset F_2$.

(3) $[F_1+F:F]_T=F_1$ for each $F_1 \in F(S)$.

(b) If $\{F_i\}_{i=1}^n$ is a finite subset of F(S), then $F_1+\ldots+F_n \in C \Leftrightarrow F_i \in C$ for each i.

(c) If $F_1,\ldots,F_n \in F(S)$ such that $F=F_1+\ldots+F_n \in C$ and $k \in N$, then $kF=kF_1+\ldots+kF_n$. Especially, if $F=(a_1,\ldots,a_n)$, then $kF=(ka_1,\ldots,ka_n)$.

Proof. (a),(b): Straightforward.

(c): We need only consider the case where n and k are greater than 1. In this case, $(n(k-1)+1)F$ is the union of all ideals $e_1F_1+e_2F_2+\ldots+e_nF_n$, where $e_1+e_2+\ldots+e_n=n(k-1)+1$. In $e_1F_1+\ldots+e_nF_n$, at least one of the e_i must be greater than or equal to k. Hence $(n(k-1)+1)F \subset (kF_1 \cup \ldots \cup kF_n)+(n-1)(k-1)F$. Since $(n-1)(k-1)F$ is a cancellation ideal, $kF \subset kF_1+\ldots+kF_n$. The reverse containment is clear.

7. Invertible ideals

Let T be the quotient group of S. An element $A \in F(S)$ is said to be invertible if there exists $B \in F(S)$ such that $A+B=S$.

(7.1)Theorem. If S is a G-semigroup, then the following hold.

(1) If $F+B=S$, with $F,B \in F(S)$, then $B=F^{-1}=[S:F]_T=\{x \in T \mid x+F \subset S\}$ and F is principal.

(2) For $\mu \in S$, (μ) is invertible.

(3) If A is an integral ideal of S and if r is an element of T, then A-r is invertible if and only if A is invertible.

Proof. (1) There exist $f \in F, b \in B$ such that $f+b=0$. Let $x \in F^{-1}$. Then $x=(x+f)+b \in S+b \subset B$.

Hence $F^{-1} \subseteq B$, and so, $F^{-1}=B$, since $B \subseteq F^{-1}$ always holds.

Let $f+b=0$ and $f' \in F$. Then we have $f'=f'+b+f \in f+S \subset F$. Hence $(f)=F$.

(2) If $I=(\mu)$, then $I^{-1}=(-\mu)$ and $I+I^{-1}=S$.

(3) By (1) and (2), $F \in F(S)$ is invertible if and only if F is principal. Hence (3) is evident.

(7.2)Theorem. Let F_1, F_2 be fractional ideals of S such that F_2 is invertible and such that $F_1 \subseteq F_2$. Then there exists an integral ideal A of S such that $F_1=A+F_2$.

Proof. We have $F_1=F_1+F_2+F_2^{-1}$. If we set $A=F_1+F_2^{-1}$, then $F_1=A+F_2$ and A is an integral ideal of S.

An ideal A of S is called a general multiplication ideal if A is a factor of each ideal of S which it properly contains, that is, if B is an ideal of S such that $B \subset A$, then $B=A+C$ for some ideal C of S.

(7.3). An ideal A of S is a general multiplication ideal if and only if A is a principal ideal.

Proof. Assume that A is not principal. Let $a \in A$. Since $(a) \subset A$, there is an ideal C such that $(a)=A+C$. Then $S=(A\text{-}a)+C$, and so A-a is invertible. Thus, by Th. (7.1).(3), A itself is invertible, and so A is principle. This is a contradiction.

Conversely, suppose that $A=(a)$ is principal and $B \subset A$. Then $C=B\text{-}a$ is an ideal of S, and $B=A+C$.

(7.4)Theorem. Let P be an invertible proper prime ideal of a G-semigroup S.

(1) If $x \in kP\text{-}(k+1)P$ and $y \in tP\text{-}(t+1)P$, $x+y \in (k+t)P\text{-}(k+t+1)P$. Consequently, if $P_0=\bigcap_{k=1}^{\infty} kP$ is nonempty, then P_0 is a prime ideal.

(2) $\{kP\}_{k=1}^{\infty}$ is the set of P-primary ideals.

(3) If Q is a primary ideal of S such that $\sqrt{Q} \subset P$, then Q is contained in P_0.

(4) If A is an invertible ideal of S properly containing P, then $A=S$.

Proof. (1) By hypothesis, $(x)=A+kP$ and $(y)=B+tP$, where A,B are ideals of S, not contained in P. Then it follows that $(x)+(y)=A+B+(k+t)P$, where $A+B \not\subseteq P$. Hence $x+y \in (k+t)P \setminus (k+t+1)P$.

(2) For each $k \in N$, $\sqrt{kP}=P$. If $x+y \in kP$, where $x \in S \setminus P$, $y \in S$, then part (1) shows that $y \in kP$. Thus kP is P-primary.

We next assume that Q is P-primary. Since $Q \supset P_0$, $Q \not\subseteq nP$ for some $n>0$. we choose k such that $Q \subseteq kP$, $Q \not\subseteq (k+1)P$. Then $Q=A+kP$ for some ideal A of S and $A \not\subseteq P$. This implies that $kP \subseteq Q$, i.e.,$Q=kP$.

(3) Assume that $\sqrt{Q}=P' \subset P$. Since P is invertible, $Q=A+P$ for some ideal A of S. Then, since Q is primary and $P \subseteq P'$, we have $A \subseteq Q$ and so $Q=Q+P$. Therefore, $Q=Q+P=Q+2P=\ldots$, and so $Q \subseteq \cap kP=P_0$.

(4) We have $P=A+B$ for some ideal B of S. Since P is a prime ideal and $A \not\subseteq P$, we have $B \subseteq P$ so that $B=P$. Hence $P=S+P=A+P$, and so $A=S$.

References

[G1] R. Gilmer, Multiplicative Ideal Theory, Marcel Dekker, 1972.

[G2] R. Gilmer, Commutative semigroup rings, The Univ. Chicago Press, 1984.

[LM] M. D. Larsen and P. J. McCarthy, Multiplicative theory of ideals, Academic Press, New York and London, 1971.

[N] D. G. Northcott, Lessons on rings, modules and multiplicities, Cambridge Univ. Press, 1968.

(Received Sept. 25, 1996)