CHAPTER II

FREE SEMIGROUPS, FREE GROUPS, CYCLIC SEMIGROUPS AND CYCLIC GROUPS

The purpose of this chapter is to study whether each of following semigroups has a proper dense subsemigroup : free semigroups, free groups, cyclic semigroups, cyclic groups. We prove in this chapter that every free group and the infinite cyclic group have proper dense subsemigroups,but every free semigroup, every cyclic semigroup and every finite cyclic group does not have a proper dense subsemigroup. Moreover, dense subsemigroups of the infinite cyclic group are characterized.

Theorem 2.1. For any nonempty set X, the free semigroup on X has no proper dense subsemigroup.

Proof : Let X be a nonempty set and U a dense subsemigroup of $\mathcal{F}_X$, the free semigroup on X. If $X \subseteq U$, then $U = \mathcal{F}_X$. Suppose $U \neq \mathcal{F}_X$. Then there exists an element $x \in X$ such that $x \notin U$. By Theorem 1.1, $x = u_0 y_1$ for some $u_0 \in U$ and $y_1 \in \mathcal{F}_X$, contrary to the definition of $\mathcal{F}_X$. #

To prove that every free group has a proper dense subsemigroup, the following lemma which characterizes dense subsemigroups of groups is given first.

Lemma 2.2. Let G be a group and U a subsemigroup of G. Then U is dense in G if and only if $\langle U \cup U^{-1} \rangle = G$ where $U^{-1} = \{x^{-1} \mid x \in U\}$.

Proof : Assume that U is dense in G. Then Dom(U,G) = G. Since $U \subseteq \langle U \cup U^{-1} \rangle$, $Dom(U,G) \subseteq Dom(\langle U \cup U^{-1} \rangle, G)$. Then $G = Dom(\langle U \cup U^{-1} \rangle, G)$. Since $\langle U \cup U^{-1} \rangle$ is a subgroup of G, it follows from Theorem 1.2 that $Dom(\langle U \cup U^{-1} \rangle, G) = \langle U \cup U^{-1} \rangle$. Hence $G = \langle U \cup U^{-1} \rangle$.

For the converse, assume that $\langle U \cup U^{-1} \rangle = G$. We claim that $U^{-1} \subseteq Dom(U,G)$. To prove the claim, let $x \in U$. Then

$$x^{-1} = x(x^{-1})^2, \qquad x \in U, (x^{-1})^2 \in G,$$

$$= (x^{-1})^2 x^3 (x^{-1})^2, \qquad x^3 \in U, (x^{-1})^2 \in G, x = (x^{-1})^2 x^3,$$

$$= (x^{-1})^2 x, \qquad x \in U, x^3 (x^{-1})^2 = x .$$

By Theorem 1.1, $x^{-1} \in Dom(U,G)$. Therefore $U^{-1} \subseteq Dom(U,G)$ which implies that $\langle U \cup U^{-1} \rangle \subseteq Dom(U,G)$ since Dom(U,S) is a subsemigroup of G. It follows that Dom(U,G) = G. Hence U is dense in G. #

Theorem 2.3. For any nonempty set X, the free group on X has a proper dense subsemigroup.

Proof : Let X be a nonempty set. Let U be the set of all words over X. Then U is a proper subsemigroup of $\mathcal{G}_X$, the free group on X. It is clearly seen that $\langle U \cup U^{-1} \rangle = \mathcal{G}_X$. Hence, by Lemma 2.2, we have that U is dense in $\mathcal{G}_X$. #

Next, we shall prove that every cyclic semigroup has no proper dense subsemigroup. The following fact is recalled to use : If a

finite cyclic semigroup $S = \{a, a^2, \ldots, a^s\}$ is such that $a^{s+1} = a$ and $a^i \neq a^j$ if $i \neq j$, then S is the cyclic group of order s.

Theorem 2.4. Every cyclic semigroup has no proper dense subsemigroup.

Proof : Let S be a cyclic semigroup and $S = \langle a \rangle$. Let U be a proper subsemigroup of S. Then $a \notin U$, so U is a subsemigroup of the semigroup $\{a^i \mid i \in \mathbb{N}, i \geq 2\}$ which implies that $\mathrm{Dom}(U,S) \subseteq \mathrm{Dom}(\{a^i \mid i \in \mathbb{N}, i \geq 2\}, S)$.

Case 1 : $a^i \neq a$ for every $i \in \mathbb{N}$ with $i \geq 2$. Then $\{a^i \mid i \in \mathbb{N}, i \geq 2\}$ is an ideal of S, so we have that $\mathrm{Dom}(\{a^i \mid i \in \mathbb{N}, i \geq 2\}, S) = \{a^i \mid i \in \mathbb{N}, i \geq 2\} \neq S$. Hence $\mathrm{Dom}(U,S) \neq S$.

Case 2 : $a^i = a$ for some $i \in \mathbb{N}$ and $i \geq 2$. Let s be the smallest positive integer such that $a^{s+1} = a$. Then $S = \{a, a^2, \ldots, a^s\}$ and $a, a^2, \ldots, a^s$ are all distinct. It follows that S is the cyclic group of order s. Hence U is a subgroup of S. By Theorem 1.2, $\mathrm{Dom}(U,S) = U$, so $\mathrm{Dom}(U,S) \neq S$.

This proves that $\mathrm{Dom}(U,S) \neq S$ for every proper subsemigroup of S. Hence S has no proper dense subsemigroup. #

The following theorem follows easily from Theorem 1.2 and the fact that every subsemigroup of a finite group is a subgroup.

Theorem 2.5. Every finite group has no proper dense subsemigroup. In particular, every finite cyclic group has no proper dense subsemigroup.

Because the infinite cyclic group is the free group on a set of one element, by Theorem 2.3, we have that the infinite cyclic group has a proper dense subsemigroup.

In the last theorem of this chapter, we characterize proper dense subsemigroups of the infinite cyclic group. To prove the theorem, the following three lemmas are required.

Lemma 2.6. Let G be a group and U a subsemigroup of G. Then U is dense in G if and only if U^{-1} is dense in G.

Proof : First, we note that U^{-1} is a subsemigroup of G and $(U^{-1})^{-1} = U$. Then $\langle U \cup U^{-1}\rangle = \langle U^{-1} \cup (U^{-1})^{-1}\rangle$. Hence, it follows from Lemma 2.2 that U is dense in G if and only if U^{-1} is dense in G. #

Lemma 2.7. For every $n \in \mathbb{N}$, $\{n, n+1, n+2, \ldots\}$ and $\{-n, -n-1, -n-2, \ldots\}$ are dense subsemigroups of the group $(\mathbb{Z}, +)$, the group of integers under usual addition.

Proof : Let $n \in \mathbb{N}$,

$$A = \{n, n+1, n+2, \ldots\}$$

and

$$B = \{-n, -n-1, -n-2, \ldots\} .$$

Clearly, A and B are subsemigroups of the group $(\mathbb{Z}, +)$ and $B = -A$. To prove A is dense in the group $(\mathbb{Z}, +)$, let $m \in \mathbb{Z} \setminus A$.

Case 1 : $0 \leq m \leq n$. Then

$m = (n+m)+(-n)$, $\quad n+m \in A$, $\quad -n \in \mathbb{Z}$,

$= (-n)+(2n+m)+(-n)$, $\quad 2n+m \in A$, $\quad -n \in \mathbb{Z}$, $\quad n+m = (-n)+(2n+m)$,

$= (-n)+(n+m)$, $n+m \in A$, $(2n+m)+(-n) = n+m$.

By Theorem 1.1, $m \in \mathrm{Dom}(A, \mathbb{Z})$.

Case 2 : $m < 0$. Then

$m = (n-m)+(2m-n)$, $n-m \in A$, $2m-n \in \mathbb{Z}$,

$= (m-n)+2(n-m)+(2m-n)$, $2(n-m) \in A$, $m-n \in \mathbb{Z}$, $n-m = (m-n)+2(n-m)$,

$= (m-n)+n$, $n \in A$, $2(n-m)+(2m-n) = n$.

By Theorem 1.1, $m \in \mathrm{Dom}(A, \mathbb{Z})$.

Hence $\mathrm{Dom}(A, \mathbb{Z}) = \mathbb{Z}$. Therefore A is dense in the group $(\mathbb{Z}, +)$. By Lemma 2.6, B is also dense in the group $(\mathbb{Z}, +)$. #

Lemma 2.8. Let $m, n \in \mathbb{N}$ be such that $(m,n) = 1$. If $\ell \in \mathbb{N}$ is such that $\ell > mn$, then $\ell = mx+ny$ for some $x, y \in \mathbb{N}$.

Proof : Since $(m,n) = 1$, $ma+nb = 1$ for some $a, b \in \mathbb{Z}$. Then $\ell = m\ell a+n\ell b$ and for every $t \in \mathbb{Z}$,

$$\ell = m(\ell a+nt) + n(\ell b-mt) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(1).$$

Let $k \in \mathbb{Z}$ be such that

$$k \leqslant \frac{-\ell a}{n} < k + 1 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(2).$$

Since $\ell > mn > 0$ and $\ell = m\ell a+n\ell b$, we have that

$$1 < \frac{\ell}{mn} = \frac{\ell a}{n} + \frac{\ell b}{m} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(3).$$

Then from (2) and (3), we have that

$$-\frac{\ell a}{n} < 1+k < \frac{\ell a}{n} + \frac{\ell b}{m} + k \leqslant \frac{\ell a}{n} + \frac{\ell b}{m} - \frac{\ell a}{n} = \frac{\ell b}{m}$$

which implies that $n(k+1) > -\ell a$ and $m(k+1) < \ell b$. Let $x = \ell a + n(k+1)$ and $y = \ell b - m(k+1)$. Then $x, y \in \mathbb{N}$. Replace t in (1) with $k+1$,

we have that

$$\ell = m(\ell a+n(k+1)) + n(\ell b-m(k+1)) .$$

Hence $\ell = mx+ny$. #

Theorem 2.9. Let G be the infinite cyclic group with a group generator a and U a subsemigroup of G. Then U is dense in G if and only if there exists a positive integer n such that $\{a^n, a^{n+1}, a^{n+2},...\} \subseteq U$ or $\{a^{-n}, a^{-n-1}, a^{-n-2},...\} \subseteq U$.

Proof : Since G is isomorphic to the group $(\mathbb{Z}, +)$ by the isomorphism defined by $a^m \mapsto m$ $(m \in \mathbb{Z})$, it follows by Lemma 2.7 that for every $n \in \mathbb{N}$, $\{a^n, a^{n+1}, a^{n+2},...\}$ and $\{a^{-n}, a^{-n-1}, a^{-n-2},...\}$ are dense subsemigroups of G. Hence if $U \supseteq \{a^n, a^{n+1}, a^{n+2},...\}$ or $U \supseteq \{a^{-n}, a^{-n-1}, a^{-n-2},...\}$ for some $n \in \mathbb{N}$, then U is dense is G.

On the other hand, assume that U is dense in G. If $U = \{1\}$ where 1 is the identity of G, then $\mathrm{Dom}(U, G) = U \neq G$ (Theorem 1.2). Hence $U \cap \{a, a^2, a^3,...\} \neq \emptyset$ or $U \cap \{a^{-1}, a^{-2}, a^{-3},...\} \neq \emptyset$.

Case 1 : $U \cap \{a, a^2, a^3,...\} \neq \emptyset$ and $U \cap \{a^{-1}, a^{-2}, a^{-3},...\} = \emptyset$. Let k be the least positive integer such that $a^k \in U$. If $k = 1$, then $\{a, a^2, a^3,...\} \subseteq U$. Assume that $k > 1$. Then $k = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$ for some distinct primes $p_1, p_2,..., p_m$ and positive integers $r_1, r_2,... r_m$. Suppose that there exists $i \in \{1, 2,..., m\}$ such that $p_i \mid \ell$ for all $\ell \in \mathbb{N}$ with $a^\ell \in U$. Then $U \subseteq \langle a^{p_i}, a^{-p_i} \rangle$. But $\langle a^{p_i}, a^{-p_i} \rangle$ is a subgroup of G, so $\mathrm{Dom}(\langle a^{p_i}, a^{-p_i} \rangle, G) = \langle a^{p_i}, a^{-p_i} \rangle \neq G$ (Theorem 1.2). It is a contradiction since U is dense in G. Hence for every $i \in \{1, 2,..., m\}$, there exists $\ell_i \in \mathbb{N}$ such that $p_i \nmid \ell_i$ and

$a^{\ell_i} \in U$. For each $i \in \{1,2,\ldots, m\}$, let

$$q_i = \begin{cases} \ell_i \left(\prod_{\substack{j=1 \\ j\neq i}}^{m} p_j \right) & \text{if } m > 1, \\ \ell_i & \text{if } m = 1 . \end{cases}$$

Then for every $i \in \{1, 2,\ldots, m\}$, $a^{q_i} \in U$, $p_i \nmid q_i$ and $p_i \mid q_j$ for all $j \in \{1, 2,\ldots, m\}$, $i \neq j$. Claim that $(k, \sum_{i=1}^{m} q_i) = 1$. Suppose that $(k, \sum_{i=1}^{m} q_i) = d > 1$. Then $d \mid k$ which implies that there exists p_j ($j \in \{1, 2,\ldots, m\}$) such that $p_j \mid d$. Since $d \mid \sum_{i=1}^{m} q_i$, $p_j \mid \sum_{i=1}^{m} q_i$, contrary to the fact that $p_j \nmid q_j$ and $p_j \mid q_i$ for all $i \in \{1,2,\ldots,m\}$, $i \neq j$. Hence we have the claim. Let $n = k(\sum_{i=1}^{m} q_i) + 1$. Then $n \in \mathbb{N}$.

It follows from Lemma 2.8 that for every $\ell \in \mathbb{N}$, if $\ell \geq n$, then $\ell = kx + (\sum_{i=1}^{m} q_i)y$ for some $x, y \in \mathbb{N}$, and hence

$$\begin{aligned} a^{\ell} &= a^{kx + (\sum_{i=1}^{m} q_i)y} \\ &= (a^k)^x \, a^{(\sum_{i=1}^{m} q_i)y} \\ &= (a^k)^x (a^{q_1})^y (a^{q_2})^y \ldots (a^{q_m})^y \end{aligned}$$

which belongs to U since $a^k, a^{q_1}, a^{q_2},\ldots, a^{q_m} \in U$. This proves that $\{a^n, a^{n+1}, a^{n+2},\ldots\} \subseteq U$.

Case 2 : $U \cap \{a^{-1}, a^{-2}, a^{-3},\ldots\} \neq \emptyset$ and $U \cap \{a^1, a^2, a^3,\ldots\} = \emptyset$. Then $U^{-1} \cap \{a, a^2, a^3,\ldots\} \neq \emptyset$ and $U^{-1} \cap \{a^{-1}, a^{-2}, a^{-3},\ldots\} = \emptyset$.

Since U is dense is G, by Lemma 2.6, U^{-1} is dense in G. It follows from Case 1 that there exists $n \in \mathbb{N}$ such that $\{a^n, a^{n+1}, a^{n+2}, \ldots\} \subseteq U^{-1}$. Hence $\{a^{-n}, a^{-n-1}, a^{-n-2}, \ldots\} \subseteq U$.

Case 3 : $U \cap \{a, a^2, a^3, \ldots\} \neq \emptyset$ and $U \cap \{a^{-1}, a^{-2}, a^{-3}, \ldots\} \neq \emptyset$. Let k be the least positive integer such that $a^k \in U$ and let k' be the least positive integer such that $a^{-k'} \in U$. It is clearly seen that $k = k'$. If $k = 1$, then $\{a, a^2, a^3, \ldots\} \subseteq U$, so we are done. Assume that $k > 1$. Claim that for every $\ell \in \mathbb{N}$, $a^\ell \in U$ if and only if $a^{-\ell} \in U$. To prove this, let $\ell \in \mathbb{N}$ be such that $a^\ell \in U$. Then $(a^\ell)^{k-1} = a^{\ell k - \ell} \in U$. Since $(a^{-k})^\ell = a^{-\ell k} \in U$, it follows that $a^{-\ell} = a^{\ell k - \ell} a^{-\ell k} \in U$. Conversely, if $\ell \in \mathbb{N}$ such that $a^{-\ell} \in U$, then $(a^{-\ell})^{k-1} = a^{-\ell k + \ell} \in U$ which implies that $a^\ell = a^{-\ell k + \ell} a^{\ell k} \in U$ since $a^{\ell k} = (a^k)^\ell \in U$. Hence we have the claim.

Let $k = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$ where $p_1, p_2, \ldots, p_m$ are distinct primes and $r_1, r_2, \ldots, r_m$ are positive integers. Suppose that there exists $i \in \{1, 2, \ldots, m\}$ such that $p_i \mid \ell$ for all $\ell \in \mathbb{N}$ with $a^\ell \in U$. Then $U \cap \{a, a^2, a^3, \ldots\} \subseteq \langle a^{p_i}, a^{-p_i} \rangle$, so we have that $(U \cap \{a, a^2, a^3, \ldots\})^{-1} \subseteq \langle a^{p_i}, a^{-p_i} \rangle$ since $\langle a^{p_i}, a^{-p_i} \rangle$ is a subgroup of G. But we have from the claim that $(U \cap \{a, a^2, a^3, \ldots\})^{-1} = U \cap \{a^{-1}, a^{-2}, a^{-3}, \ldots\}$, it follows that $U = (U \cap \{a, a^2, a^3, \ldots\}) \cup (U \cap \{a^{-1}, a^{-2}, a^{-3}, \ldots\}) \cup \{1\} \subseteq \langle a^{p_i}, a^{-p_i} \rangle$. But $\langle a^{p_i}, a^{-p_i} \rangle$ is a subgroup of G, so $\mathrm{Dom}(\langle a^{p_i}, a^{-p_i} \rangle, G) = \langle a^{p_i}, a^{-p_i} \rangle \neq G$ (Theorem 1.2). It is a contradiction since U is dense in G. Hence for every $i \in \{1, 2, \ldots, m\}$, there exists $\ell_i \in \mathbb{N}$ such that $p_i \nmid \ell_i$ and $a^{\ell_i} \in U$.

The remaining of the proof for this case is the same as the proof in Case 1. #