PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 84, Number 3, March 1982

FREE E-m GROUPS AND FREE E-m SEMIGROUPS

TAKAYUKI TAMURA

ABSTRACT. A group [semigroup] is called E-m if it satisfies the identity $(xy)^m = x^m y^m$. In this paper the author studies a necessary and sufficient condition on m and n for the free E-m group [semigroup] to be homomorphic onto the free E-n group [semigroup].

1. Introduction. Let m be a positive integer greater than 1. Following Nordahl's definition [7], an E-m [semi]group is a [semi]group which satisfies the identity (called identity E-m)

$$(xy)^m = x^m y^m.$$

Alperin [1] called E-m groups m-abelian and studied the structure. For example, order-bounded groups are E-m groups for some m; commutative semigroups are E-m semigroups for all m. The structure of E-m semigroups was studied by Nordahl [7] and Cherubini and Varisco [2]. Let X be any set with cardinality $|X| > 1$, and let $F(X)$ be the free semigroup over X and ρ_m be the smallest E-m congruence on $F(X)$, namely, the congruence of $F(X)$ generated by the relation

$$\{((VW)^m, V^m W^m): V, W \in F(X)\}.$$

Let $F_m(X) = F(X)/\rho_m$. Then $F_m(X)$ is called the free E-m semigroup over X.

The free E-m group $G_m(X)$ over X is defined by $G_m(X) = G(X)/\rho_m$ where $G(X)$ is the free group over X, and ρ_m is the smallest E-m congruence on $G(X)$. It is obvious that $F_m(X)$ and $G_m(X)$ are unique up to isomorphism when m and X are fixed.

The purpose of this paper is to prove Theorems 1, 2, 3 below:

In Theorems 1, 2 and 3, assume $m > 2$ and $n > 2$ in case of groups, and $m > 1$ and $n > 1$ in case of semigoups. This does not lose generality since the other cases are obvious.

THEOREM 1. *The following are equivalent.*

(1.1) *$G_m(X)$ [$F_m(X)$] is isomorphic to $G_n(X)$ [$F_n(X)$].*

(1.2) *$G_n(X)$ [$F_n(X)$] is a homomorphic image of $G_m(X)$ [$F_m(X)$], and $G_m(X)$ [$F_m(X)$] is a homomorphic image of $G_n(X)$ [$F_n(X)$].*

(1.3) *$m = n$.*

THEOREM 2. *If $G_n(X)$ [$F_n(X)$] is a homomorphic image of $G_m(X)$ [$F_m(X)$] then $m \geqslant n$.*

Received by the editors April 1, 1980 and, in revised form, June 30, 1981.

AMS (MOS) subject classifications (1970). Primary 20M05; Secondary 20E05.

Key words and phrases. Free E-m groups, free E-m semigroups, exponent semigroups.

THEOREM 3.

(3.1) *$G_n(X)$ is a homomorphic image of $G_m(X)$ if and only if m is congruent to one of* 0, 1, n, $(n-1)^2$ mod $n(n-1)$.

(3.2) *$F_n(X)$ is a homomorphic image of $F_m(X)$ if and only if m is congruent to one of* 1 *and* n mod $n(n-1)$, *but* $m \neq n^2 - n + 1$.

Theorem 1 is straightforward from Theorem 2, and Theorem 2 is an immediate consequence of Theorem 3. However we will prove here Theorem 2 without using Theorem 3, but using the exponent semigroup of order-bound groups [**9**]. Theorem 3 is closely related to exponent semigroups and it will be proved by utilizing the recent results by Kobayashi [**6**] and Cherubini and Varisco [**3**]. It is interesting that Theorem 2 in case of semigroup will be able to be easily derived from the theorem in case of groups.

2. On Theorem 2. The exponent semigroup $E(S)$ of a semigroup S is the multiplicative semigroup of positive integers m for which the identity $(xy)^m = x^m y^m$ holds in S. Exponent semigroups were studied by the author [**9, 10**], Clarke, Pfiefer and Tamura [**4**], Kobayashi [**5, 6**] and Cherubini and Varisco [**3**].

The following lemmas are fundamental in this paper.

LEMMA 1 [**9**]. *If a semigroup T is a homomorphic image of S, then $E(S) \subseteq E(T)$.*

LEMMA 2. *The following are equivalent.*

(i) *$F_n(X)$ [$G_n(X)$] is a homomorphic image of $F_m(X)$ [$G_m(X)$].*

(ii) $m \in E(F_n(X))$. [$m \in E(G_n(X))$.]

(iii) $\rho_m \subseteq \rho_n$.

(i) *Identity E-n implies identity E-m in semigroups [in groups].*

PROOF. (i) $\rightarrow$ (ii) is obtained by Lemma 1. (ii) $\rightarrow$ (iii). The smallest E-m congruence on $F(X)$ equals the transitive closure of $\sigma_m \cup \sigma_m^{-1}$ where σ_m is defined as follows: $V \sigma_m W$ if and only if either $V = W$ or $V = Q(Z^m U^m)R$ and $W = Q(ZU)^m R$ for some Z, $U \in F$, and some Q, $R \in F^1$. The assumption $m \in E(F_n(X))$ implies $Z^m U^m \rho_n (ZU)^m$ for all Z, $U \in F(X)$; then $\sigma_m \subseteq \rho_n$ hence $\rho_m \subseteq \rho_n$. (iii) $\rightarrow$ (i) and (ii) $\rightarrow$ (iv) are obvious. (iv) $\rightarrow$ (i). Since $F_n(X)$ is E-m, (i) is derived.

PROOF OF THEOREM 2. Let Z_+ denote the set of positive integers and let $Z_+^0 = Z_+ \cup \{0\}$. For each positive integer $n > 2$ define a subset $M(n)$ of Z_+ by

$$M(n) = \{kn + n, kn + 1 \colon k \in Z_+^0\}.$$

$M(n)$ is a multiplicative semigroup. Let N_n be the subgroup of the free group $G(X)$ generated by

$$\{V^n \colon V \in G(X)\}.$$

N_n is necessarily a normal subgroup of $G(X)$. Let $H = G(X)/N_n$ and $K = G(X)/N_{n-1}$. Then H has exponent n and K has exponent $n-1$ where "exponent" is in the sense of the group theory, that is, n is the least one of l for which all elements x of H satisfy $x^l = 1$. Now X can be regarded as a subset of H and K since if $a, b \in X$ and $a \neq b$ then $ab^{-1} \notin N_n$ and $ab^{-1} \notin N_{n-1}$. Thus H and K are

E-n groups generated by X. Accordingly H and K are homomorphic images of $G_n(X)$, hence

$$E(G_n(X)) \subseteq E(H) \cap E(K)$$

by Lemma 1. (This is also obtained from **[1]** since it was essentially proved in **[1]** that $G_n(X)$ is isomorphic to a subdirect product of H, K and the free abelian group generated by X although the author of **[1]** did not state it explicitly.)

On the other hand, H is isomorphic to a subdirect product of subdirectly irreducible groups H_α of exponent n (see **[8]**), and the author proved in **[9]** that $E(H_\alpha) = M(n)$. The similar result holds for K. Therefore

$$E(H) \subseteqq M(n), \quad E(K) \subseteqq M(n-1).$$

We easily see that all elements of $M(n) \cap M(n-1)$ except 1 are greater than or equal to n. Now assume $G_n(X)$ is a homomorphic image of $G_m(X)$. Then $m \in E(G_n(X))$ by Lemma 2. By the above result, $m \geqslant n$, since $m > 2$.

If $F_n(X)$ is a homomorphic image of $F_m(X)$, then $m \in E(F_n(X))$. Again, consider the groups $H = G(X)/N_n$ and $K = G(X)/N_{n-1}$. Since H and K are periodic, H and K are E-n semigroups generated by X, hence H and K are homomorphic images of $F_n(X)$. By Lemma 1, we have

(1) $E(F_n(X)) \subseteq E(H) \cap E(K) \subseteqq M(n) \cap M(n-1)$.

As stated in case of groups, $m \in M(n) \cap M(n-1)$ implies $m \geqslant n$ since $m > 1$.

3. Proof of Theorem 3. First we define notations. Let r be a nonnegative integer with $0 \leqslant r < n(n-1)$. For each r, define

$$P(r) = \{x \in Z_+ : x \equiv r \bmod n(n-1)\}.$$

By Lemma 2, the statements (3.1), (3.2) of Theorem 3 are respectively restated as follows: For simplicity let $G_n = G_n(X)$ and $F_n = F_n(X)$.

$$(3.1') \qquad E(G_n) = P(0) \cup P(1) \cup P(n) \cup P\big((n-1)^2\big), \qquad n > 2.$$

$$(3.2') \qquad E(F_n) = (P(1) \cup P(n)) \setminus \{n^2 - n + 1\}, \qquad n > 1.$$

Proof of (3.1′). From the proof of Theorem 2,

$$(2) \qquad E(G_n) \subseteq M(n) \cap M(n-1).$$

By elementary number theory we have

$$(3) \qquad M(n) \cap M(n-1) = P(0) \cup P(1) \cup P(n) \cup P\big((n-1)^2\big).$$

Recently Kobayashi **[6]** has obtained

Theorem 4 **[6]**. *If S is a separative semigroup then $E(S)$ equals either $\{1\}$ or the intersection of a finite number of $M(m_i)$'s where $m_i \geqslant 2$.*

By a separative semigroup **[8]** we mean a semigroup satisfying (i) $x^2 = xy$ and $y^2 = yx$ imply $x = y$ and (ii) $x^2 = yx$ and $y^2 = xy$ imply $x = y$. Applying Theorem 4 to G_n,

$$(4) \qquad E(G_n) = \bigcap_{i=1}^{s} M(m_i)$$

where m_i is a positive integer $\geqslant 2$. Since $n \in E(G_n)$, $n \in M(m_i)$ for all $i = 1, \ldots, s$, but this is the case if and only if for each $i = 1, \ldots, s$, either $m_i | n$ or $m_i | n - 1$. Then

$$(5) \qquad P(0) \cup P(1) \cup P(n) \cup P((n-1)^2) \subseteq M(m_i) \quad \text{for } i = 1, \ldots, s.$$

By (2), (3), (4) and (5), we have (3.1′).

PROOF OF (3.2′). Let $V \in F(X)$, $V = x_1^{m_1} x_2^{m_2} \ldots x_k^{m_k}$ where $x_i \in X$ ($i = 1, \ldots, k$) and $x_i \neq x_{i+1}$ ($i = 1, \ldots, k-1$). The first letter x_1 in V is called the *head* of V denoted by $h(V)$; the last letter x_k is called the *tail* of V denoted by $t(V)$; $x_1^{m_1}$ is called the head part of V denoted by $H(V)$, $x_k^{m_k}$ is called the tail part of V denoted by $T(V)$; the positive integer m_1 is called the *head degree* of V denoted by $H_d(V)$; the m_k is called the *tail degree* of V denoted by $T_d(V)$. Let $L(V)$ denote the set of letters appearing in V. $L(V)$ is a finite subset of X.

The smallest E-n congruence ρ_n on $F(X)$ is described in the proof of Lemma 2. The following is obvious.

(6) *If* $V \rho_n W$ *then* $L(V) = L(W)$, $h(V) = h(W)$, *and* $t(V) = t(W)$.

LEMMA 3. *Let* $L(V) = \{a, b\}$, $a \neq b$. *If* $V \rho_n W$, $n > 1$, *then*

$$(\mathrm{H}) \qquad H_d(V) \equiv H_d(W) \mod (n-1).$$

$$(\mathrm{T}) \qquad T_d(V) \equiv T_d(W) \mod (n-1).$$

PROOF. We prove only (H) here since (T) is similarly obtained. It is sufficient to prove that if $V \sigma_n W$ then (H) holds. Let $V = a^{m_1} b^{n_1} \ldots$, that is, $h(V) = a$, $H_d(V) = m_1$. Assume $V \sigma_n W$ and $V \neq W$. Then either

(i) $V = QZ^n U^n R$ and $W = Q(ZU)^n R$, or

(ii) $V = Q(ZU)^n R$ and $W = QZ^n U^n R$,

for some $Z, U \in F(X)$, $Q, R \in F(X)^1$.

As subcases of (i) and (ii), the following four cases must be considered since $H(V) = H(W)$ in the other cases.

($\mathrm{i_a}$) $H(V) = QZ^n$.

($\mathrm{i_b}$) $H(V) = QZ^n U_1$ where $U = U_1 U_1'$, $U_1 \neq \varnothing$, $U_1' \neq \varnothing$.

($\mathrm{ii_a}$) $H(V) = QZ$.

($\mathrm{ii_b}$) $H(V) = QZU_1$ where $U = U_1 U_1'$, $U_1 \neq \varnothing$, $U_1' \neq \varnothing$.

Q could be void. Let $Z = a^i$ and $U_1 = a^j$. Then, in case ($\mathrm{i_a}$), $m_1 \geqslant in$; in case ($\mathrm{i_b}$), $m_1 \geqslant in + j$; hence $H_d(W) = m_1 - in + i$ in case (i). In case ($\mathrm{ii_a}$), $m_1 \geqslant i$; in case ($\mathrm{ii_b}$), $m_1 \geqslant i + j$; hence $H_d(W) = m_1 - i + in$ in case (ii). In all cases $H_d(V) \equiv H_d(W) \mod(n-1)$.

To prove (3.2′) we use the following two lemmas.

LEMMA 4 [KOBAYASHI 5, 6]. *Let* S *be a semigroup. If* $n \in E(S)$ *then* $\alpha n(n-1) + 1 \in E(S)$ *for all* $\alpha \geqslant 2$.

LEMMA 5 [CHERUBINI AND VARISCO 3]. *Let* S *be a semigroup. If* $n \in E(S)$ *then* $\alpha n(n-1) + n \in E(S)$ *for all* $\alpha > 0$.

Let $F = F(X)$, $|X| > 1$, and $F_n = F_n(X) = F/\rho_n$, $n > 1$. By Lemmas 4 and 5, we have

$$(P(1) \setminus \{n^2 - n + 1\}) \cup P(n) \subseteq E(F_n).$$

On the other hand (1) and (2) yield

$$E(F_n) \subseteq P(0) \cup P(1) \cup P(n) \cup P((n-1)^2).$$

We need prove

$$E(F_n) \cap P(0) = \varnothing, \quad E(F_n) \cap P((n-1)^2) = \varnothing, \quad n^2 - n + 1 \notin E(F_n).$$

Let $a,\ b \in X,\ a \neq b$, and let $\alpha \in Z_+$. Let $V = a^{\alpha n(n-1)} b^{\alpha n(n-1)}$ and $W = (ab)^{\alpha n(n-1)}$. Then $H_d(V) = \alpha n(n-1)$ and $H_d(W) = 1$, hence $H_d(V) \not\equiv H_d(W) \bmod (n-1)$. By Lemma 3 $(V, W) \notin \rho_n$, hence $\alpha n(n-1) \notin E(F_n)$ for any $\alpha \in Z_+$. Thus $E(F_n) \cap P(0) = \varnothing$. Likewise, since $\alpha n(n-1) + (n-1)^2 \not\equiv 1 \bmod (n-1)$, $E(F_n) \cap P((n-1)^2) = \varnothing$.

Next we want to show

$$\left(a^{n^2-n+1} b^{n^2-n+1}, (ab)^{n^2-n+1}\right) \notin \rho_n \quad \text{for } n > 1. \tag{7}$$

Let $A_1 = a^{n^2-n+1} b^{n^2-n+1}$, and suppose $A_1 \sigma_n \cup \sigma_n^{-1} A_2$ for some $A_2 \in F$, $A_1 \neq A_2$. We see that the only case $(\mathrm{i_a})$ described in the proof of Lemma 3 is possible for A_1.

For any $i, j \in Z_+$ satisfying $n^2 - n + 1 > in$ and $n^2 - n + 1 > jn$,

$$A_1 = a^{n(n-i-1)+1} a^{in} b^{jn} b^{n(n-j-1)+1}.$$

Hence

$$\begin{aligned} A_2 &= a^{n(n-i-1)+1} (a^i b^j)^n b^{n(n-j-1)+1} \\ &= a^{(n-1)(n-i)+1} (b^j a^i)^{n-1} b^{(n-1)(n-j)+1} \end{aligned}$$

for some $i, j \in Z_+$ satisfying $n^2 - n + 1 > in, jn$. Let

$$\begin{aligned} W_{a,i} &= a^{(n-1)(n-i)+1}, & W_{b,j} &= b^{(n-1)(n-j)+1}, \\ V_{a,i} &= a^{n(n-i-1)+1}, & V_{b,j} &= b^{n(n-j-1)+1}. \end{aligned}$$

Since $n^2 - n + 1 > in$ and $n^2 - n + 1 > jn$, $i \leq n - 1$ and $j \leq n - 1$. If $A_3 \in F$ and $A_2 \sigma_n \cup \sigma_n^{-1} A_3$ then what form does A_3 have?

Suppose $A_2 = Q(Z^n U^n)R$ or $Q(ZU)^n R$ for some $Z,\ U \in F$, $Q,\ R \in F^1$. As $i + j \leq 2(n-1)$, there are the only five possibilities for

$$A_2 = W_{a,i}(b^j a^i)^{n-1} W_{b,j} = V_{a,i}(a^i b^j)^n V_{b,j}.$$

(i) Either $W_{a,i} = W' Z^n U^n$ or $W_{a,i} = W'(ZU)^n$ for some $W' \in F^1$.
(ii) $(ZU)^n = (a^i b^j)^n$.
(iii) Either $W_{b,j} = Z^n U^n W'$ or $W_{b,j} = (ZU)^n W'$ for some $W' \in F^1$.
(iv) $V_{a,i} = V' Z^n$ and $U^n = (a^i b^j)^n$ for some $V' \in F^1$.
(v) $Z^n = (a^i b^j)^n$ and $V_{b,j} = U^n V'$ for some $V' \in F^1$.

Then $A_3 = A_2$ in cases (i) and (iii); $A_3 = A_1$ in case (ii).

In case (iv), let $Z = a^{i_1}$ where $n(n - i - 1) + 1 > i_1 n$, hence $i + i_1 < n - 1$. We have

$$A_3 = W_{a,i+i_1}(b^j a^{i+i_1})^{n-1} W_{b,j}.$$

In case (v), let $U = b^{j_1}$ where $n(n - j - 1) + 1 > j_1 n$, hence $j + j_1 < n - 1$. Then

$$A_3 = W_{a,i}(b^{j+j_1} a^i)^{n-1} W_{b,j+j_1}.$$

We can obtain A_k such that $A_3\sigma_n \cup \sigma_n^{-1}A_4\sigma_n \cup \sigma_n^{-1} \ldots \sigma_n \cup \sigma_n^{-1}A_k$, in the same way.

Let $\mathbb{S}$ be the subset of F defined by

$$\mathbb{S} = \{a^{n^2-n+1}b^{n^2-n+1}\} \cup \left\{ W_{a,\lambda}(b^\mu a^\lambda)^{n-1} W_{b,\mu} | \lambda, \mu \in Z_+, \lambda, \mu < n - 1 \right\}.$$

Partial mappings $\beta(i,j)$: $\mathbb{S} \to \mathbb{S}$ are defined as follows. If $0 < i < n - 1$ and $0 < j < n - 1$,

$$(a^{n^2-n+1}b^{n^2-n+1})\beta(i,j) = W_{a,i}(b^j a^i)^{n-1} W_{b,j}.$$

If $0 < \lambda + i < n - 1$ and $0 < \mu + j < n - 1$,

$$\left(W_{a,\lambda}(b^\mu a^\lambda)^{n-1} W_{b,\mu}\right)\beta(i,j) = W_{a,\lambda+i}(b^{\mu+j}a^{\lambda+i}) W_{b,u+j}.$$

If $A \in \mathbb{S}$ and if $A\beta(i,j)$ and $(A\beta(i,j))\beta(k, l)$ are defined, then $A\beta(k, l)$, $(A\beta(k, l))\beta(i,j)$ and $A\beta(i + k, j + l)$ are defined and

$$(A\beta(i,j))\beta(k, l) = (A\beta(k, l))\beta(i,j) = A\beta(i + k, j + l).$$

By the above results we have

$$A_1\rho_n A \text{ if and only if } A \in \mathbb{S}.$$

Finally we consider $H_d(A)$ and $T_d(A)$. If $A_1\rho_n A$, then, for some $i, j \in Z_+^0$

$$A = A_1\beta(i,j) = a^{(n-1)(n-i)+1}(b^j a^i)^{n-1} b^{(n-1)(n-j)+1}.$$

Since $i < n - 1$ and $j < n - 1$, $H_d(A) > 1$ and $T_d(A) > 1$ for all $A \in \mathbb{S}$, hence $(ab)^{n^2-n+1} \notin \mathbb{S}$. By Lemma 3 we have proved (7), completing the proof of (3.2′).

4. Remarks.

(4.1) Theorem 2 in case of semigroups can be easily proved by showing:

$$\text{If } m < n \text{ then } \rho_m \not\subseteq \rho_n.$$

If the length of a word in F is less than $2n$ then it composes a singleton ρ_n-class. Hence if $a, b \in X$,

$$(a^m b^m, (ab)^m) \notin \rho_n.$$

The proof of Theorem 2 in case of groups can be similarly considered.

(4.2) Kobayashi [6] defined $\overline{E}(S)$ for a semigroup S as follows:

$$\overline{E}(S) = \{\overline{m} \in Z_{n(n-1)}: \alpha n(n - 1) + m \in E(S) \text{ for some } \alpha \in Z_+^0\}$$

where $Z_{n(n-1)}$ is the ring of integers mod $n(n - 1)$.

COROLLARY 5. *Let S be a semigroup and assume $n \in E(S)$. Then $\bar{E}(S) = \{1, \bar{n}\}$ if and only if either*

$$E(S) = P(1) \cup P(n) \tag{5.1}$$

or

$$E(S) = (P(1) \cup P(n)) \setminus \{n^2 - n + 1\}. \tag{5.2}$$

PROOF. Necessity is due to Lemmas 4, 5. Sufficiency of (5.2) is obtained by (3.2′); case (5.1) was done by Cherubini and Varisco [3].

ACKNOWLEDGEMENT. The author expresses thanks to the referee for his useful suggestion.

REFERENCES

1. J. L. Alperin, *A classification of n-abelian groups*, Canad. J. Math. **21** (1969), 1238–1244.

2. A. Cherubini Spoletini and A. Varisco, *Some properties of E-m semigroups*, Semigroup Forum **17** (1979), 153–161.

3. ______, *On the exponent semigroup of an E-m semigroup* (to appear).

4. J. Clarke, R. Pfiefer and T. Tamura, *Identities E-2 and exponentially*, Proc. Japan Acad. Ser. A **55** (1979), 250–251.

5. Y. Kobayashi, *The exponent semigroup of a semigroup satisfying* $(xy)^3 = x^3y^3$, Semigroup Forum **19** (1980), 323–330.

6. ______, *On the structure of exponent semigroups*, J. Algebra (to appear).

7. T. Nordahl, *Semigroups satisfying* $(xy)^m = x^my^m$, Semigroup Forum **8** (1974), 332–346.

8. M. Petrich, *Introduction to semigroups*, Merrill, Columbus, Ohio, 1973.

9. T. Tamura, *Complementary semigroups and exponent semigroups of ordered bounded groups*, Math. Nachr. **49** (1974), 17–34.

10. ______, *On the exponents of inverse semigroups*, Proc. Symposium on Inverse Semigroups, Northern Illinois Univ., 1973, pp. 172–185.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, DAVIS, CALIFORNIA 95616