Hence the coefficients of $\sigma_{1,0}$ are obtained from 1 and the coefficients of $\sigma_2$ by means of $\sigma_1$ and $^{-1}$. Similarly, the coefficients of $\sigma_{0,0}$ are of the form $c, \sigma_{0,1}(1)/c$ where $c$ is obtained from 1 and the coefficients of $\sigma_2$ by means of addition and multiplication. We observe that the coefficients of $\sigma_2$ are independent of the concrete choice of the model $C_1$, the field $K$, and the ladder for $K$ — they are completely determined by the diagram of the exponential field $C$.

By the order of a term $t$ we mean the maximal number of iterations of the exponential function occurring in $t$. Thus we have proved

**Lemma 36.** Let $t(x, y, \ldots, y)$ be a term without parameters, let $C_1$ be a model of $T$ and $c_1, \ldots, c_n \in C_1$. Then, for every $h \in H_n$, there exists a term $u(y, \ldots, y)$ of the same order as $t$ such that $\sigma_{c_1, \ldots, c_n, h} = u(c_1, \ldots, c_n)$.

**Lemma 37.** Suppose $a \neq 0$ and $h = \maxsupp(a)$. Then there is a positive $e \in C$ such that $\sigma_e \neq \sigma_{h}(h) < e$.

**Proof.** The lemma is an easy consequence of the fact that $x^{-1}$ is the largest element of $H_n$, which is less than 1.

Since $\sigma: a \mapsto \sigma_a$ is an embedding of $C_0$ into $C^n$, Lemma 36 and Lemma 37 yield

**Theorem 38.** Let $t(x, y, \ldots, y)$ be a term without parameters, let $C_1$ be a model of $T$ and $c_1, \ldots, c_n \in C_1$ such that $t(x, c_1, \ldots, c_n)$ is not identically zero in $C_1$. Then $C_1 \vdash \text{"limit}(x, c_1, \ldots, c_n)$ exists" $\iff \maxsupp(\sigma_{c_1, \ldots, c_n}) \leq 1$.

If $c \in C_1$ is such that $C_1 \vdash \text{"limit}(x, c_1, \ldots, c_n) = e^c$, then there is a term $u(y, \ldots, y)$ of the same order as $t$ such that $c = u(c_1, \ldots, c_n)$.

**Corollary 39.** Let $C_1, C_2$ be models of $T$ containing an exponential field $C$ and let $t$ be a term with parameters from $C$. Then, for each $e \in C \cup \{\pm \infty\}$, $C_1 \vdash \text{"limit} = e^c$ $\iff C_2 \vdash \text{"limit} = e^c$.

**Proof.** Corollary 39 follows from Lemma 37 and Theorem 38 since the map $a \mapsto \sigma_a$ is the same for the models $C_1$ and $C_2$.

References


Received 24 December 1982

---

The automorphism group of some semigroups

Richard D. Byrd (Houston, Tex.), Justin T. Lloyd (Houston, Tex.), Franklin D. Pedersen (Carbondale, Ill.) and James W. Stepp (Houston, Tex.)

Abstract. Let $F(Z)$ denote the collection of all finite non-empty subsets of the integers $Z$. $F(Z)$ can be considered as a semigroup with addition defined by $A + B = \{a + b : a \in A, b \in B\}$. The main result in this paper is the determination of the automorphism group of $F(Z)$. In order to determine this automorphism group some algebraic results for $F(G)$ where $G$ is a group are obtained.

**Introduction.** Let $F(Z)$ denote the collection of all finite non-empty subsets of the integers $Z$. $F(Z)$ can be considered as a semigroup with addition defined by $A + B = \{a + b : a \in A, b \in B\}$. M. Deza and P. Erdős considered this set addition in [2] and G. A. Freiman also uses this notion of set addition in his book [3].

The same idea is used, but mainly for infinite sets, in the study of sequences, such as in H. Halberstam and K. Roth [4]. The main question that is considered in this paper is the determination of the automorphism group of this semigroup.

Since the answer to the main question can be obtained by considering the subsemigroup of $F(Z)$ composed of all subsets of the non-negative integers which contain 0, the first section is devoted to determining the automorphism group of this subsemigroup. It is necessary to introduce some algebraic results concerning retractions in order to answer the main question. Thus, the second section is devoted to providing the necessary facts about retractions in order to verify that the automorphism group of $F(Z)$ is a splitting extension of $Z$ by the Klein four group.

**Section I.**

**Definition 1.** For a group $G$ let $F(G) = \{A \in G \mid A \neq \emptyset \land |A| < \infty\}$. For the special case of $G = Z$ let $K = \{A \in F(Z) \mid 0 \in A, A \subseteq Z^+\}$.

The following lemma is due to Professor A. H. Clifford.

**Lemma 1.** If $\gamma \in \text{Aut} K$ and $n$ is a natural number, then $[0, n] \gamma = [0, n]$.

**Proof.** Let $P_0 = [0, n]$. Now $(n-1)[0, 1] + [0, n] = (2n-1)[0, 1]$ and thus $(n-1)P_0 + P_0 = (2n-1)P_0$. Let $Q = [0, 1]^+$. Then $Q + q[0, 1]$
Adding \(0, 2\) to each side of this equality and using the fact that \(0, 2\) is a cycle, we have that

\[
(0, 2, ..., n) \gamma = (0, 2, ..., n).
\]

Thus the lemma is true for \(k = 2\).

Before beginning the general case, we should note that

\[
(0, 3, 4, 5, 6, 7) \gamma \neq (0, 2, 3, 6, 7).
\]

To see this, we observe that \((0, 1)+ (0, 3) = (0, 1, 3, 4)\) is fixed by \(\gamma\) and

\[
(0, 3, 4, 5, 6, 7) + (0, 1, 3, 4) = (0, 1, 3, 4, 11)
\]

while

\[
(0, 2, 3, 6, 7) + (0, 1, 3, 4) = (0, 1, 3, 4, 11) + (0, 1, 3, 4, 11).
\]

Now suppose that \(k \geq 3, n \geq 2k - 2\), and the lemma holds for all \(l\) such that \(2 \leq l < k\). Let

\[
A = (0, k, \ldots, n)
\]

and let \(A B = (0, \ldots, n, 1)\). Now

\[
A^+ + 1 = (0, k - 1, \ldots, n + k - 1).
\]

Thus

\[
D = B + (0, k - 1) = A + (0, k - 1) \gamma = (A + (0, k - 1)) \gamma = (0, k - 1, \ldots, n + k - 1).
\]

Note that \(1, 2, \ldots, k - 2 \notin B\) while \(k \in B\). Now suppose that

\[
2k - 2 \leq n \leq 3k - 2
\]

and suppose (by way of contradiction) that \(k - 1 \in B\). Since \(A\) has a maximum gap of \(k - 1\), there exists \(x \in B\) with \(x + 1, x + 2, \ldots, x + k - 1 \notin B\) while \(x + k \in B\). Now

\[
x + 1, x + 2, \ldots, x + k - 1 \in D.
\]

Since \(x + 1 \notin B\), there exists \(y \in B\) such that \(y + k - 1 = x + 1\). Now \(x + k - 1 \leq n - 1 \leq 3k - 3\) and so \(x \leq 2k - 2\). Thus \(y + (k - 1) = x + 1 \leq 2k - 2\), and so \(y \leq k - 1\).

Case 1. \(y = k - 1\). Since \(x + 1 = y + k - 1 = (k - 1) + (k - 1)\), we have that

\[
x = 2k - 3\.
\]

Now \(x + k - 1 = 3k - 4 \notin B\). Also \(x + k \in B\) and \(x + k = 3k - 3\). Therefore,

\[
3k - 3 \leq n \leq 3k - 2,
\]

and so \(n = 3k - 2\) or \(n = 3k - 3\).

Subcase 1a. \(n = 3k - 2\). Now \(n + k - 1 = 4k - 4\) and so \(4k - 5 \in D\). If \(4k - 5 \in B\), then \(4k - 5 \leq n = 3k - 3\), and \(k \leq 2\), a contradiction. Thus \(4k - 5 \notin B\). Therefore, there exists \(z \in B\), \(z \neq 0\), such that \(z + k - 1 = 4k - 5\). But then \(x = 3k - 4 \in B\) and this contradicts the fact that \(3k - 4 \leq x + k - 1 \notin B\).

Subcase 1b. \(n = 3k - 3\). Then we have that \(n + k - 1 = 4k - 3\). Thus \(4k - 3 \in B\). If \(4k - 5 \in B\), then \(4k - 5 \leq 3k - 2\) and so \(k \leq 2\). If \(k = 2\), then \(n = 7\) and \(A = (0, 2, 3, 5, 6, 7)\) while \(B = (0, 2, 3, 6, 7)\) and this was taken care of in the
above. Thus $4k-5 \notin B$. Therefore, there exists $x \in B$, $x \not\equiv 0$, such that $z+k-1 = 4k-5$. Again we have that $z = 3k-4 = x+k-1 \notin B$.

It now follows that $y \neq k-1$.

Case 2. $y = k$. Then $x = 2k-2$. Now $x+k-1 = 2k-2+k-1 = 3k-3 \notin B$.

Also, $x+k \leq n$ and so $n \geq 3k-2$. By assumption $x \notin B$ and therefore $n = 3k-2$. Thus $n+k-1 = 4k-3$ and so $4k-4 \notin B$. Now $4k-4 \neq B$, and hence there exists $z \in B$, $z \not\equiv 0$, such that $z+k-1 = 4k-4$. But then $z = 3k-3 = x+k-1 \notin B$, a contradiction.

Thus we have shown that $k-1 \notin B$. We now prove that $B = \{0, k, \ldots, n\}$. Assume that there exists $x \in B$ with $k < x < n$. Then

$$2k-1 < x+k-1 < n-k-1$$

and so $x+k-1 \notin B$. Since $x \notin B$, it follows that $x+(k-1) \in B$ and so $x+k-1 < n \leq 3k-2$. Therefore, $x < 2k-1$. If $x < 2k-1$, then $x \notin B$, a contradiction. Thus, $x = 2k-1$ and it follows that $n = 3k-2$. Thus

$$A = \{0, k, \ldots, 3k-2\}$$

and $B = \{0, k, \ldots, 2k-2, 2k, \ldots, 3k-2\}$. Now $A+\{0, k\} = \{0, k, \ldots, 4k-2\}$ and $B+\{0, k\}$ has a gap at $2k-1$. By our argument we have that

$$\{0, k, \ldots, 3k-3\} = \{0, k, \ldots, 3k-3\}$$

Adding $\{0, k+1\}$ to each side of this equation we have that

$$\{0, k, \ldots, 4k-2\} = \{0, k, \ldots, 4k-2\}$$

and this is a contradiction.

We claim now that $\{0, k, \ldots, n\} \gamma = \{0, k, \ldots, n\}$ if $(l-1)k-2 \leq n \leq (l-1)k-2$, where $l \geq 3$. We have just completed the case for $l = 3$. The induction step is clear.

**Lemma 5.** If $\gamma \in AutK$ and $\{0, 2, 3\} = \{0, 2, 3\}$, then $\gamma$ is the identity automorphism of $K$.

**Proof.** Let $M = \{A \in K \mid A \neq A\}$ assume that $M \neq \emptyset$. For $A \in M$, define $G(A) = max{A+1 \mid A \not\subseteq A}$. Let $A_0 \in M$ be such that

$$G(A_0) + G(A_0) = t_0$$

is minimal. Note that $t_0 > 2$. Let $n = max A_0$ and $y$ be the largest integer such that $y \leq n-1$ and $\gamma \not\subseteq A_0$. Then $A_0 = \{0, \ldots, y+1, \ldots, n\}$.

Since we can add to $A_0$ and $A_0$ any set of the form $\{0, y+1, \ldots, m\}$, and preserve the structure of $A_0$, between 0 and $y+1$, we may assume that $n \geq 3y+1$. Next let

$$B_0 = A_0 + \{0, y, \ldots, y+n\} = \{0, y, \ldots, 3n+y\}.$$
such that \( A = C \). It is an easy matter to verify that if \( \sigma \) is a retraction of \( G \), then \( ker(\sigma) = \{ A \in F(G) \mid A \sigma = 1 \} \) is a \( G \)-complement. Conversely, if \( S \) is a \( G \)-complement and \( A \in F(G) \), then there exist unique \( C \in S \) and unique \( g \in G \) such that \( A = Cg \). Thus if one defines \( A \sigma = g \), then \( \sigma \) is a retraction of \( G \). It was shown in [1, Corollary 2.11] that there is a one-to-one correspondence between retraction of \( G \) and \( G \)-complements of \( F(G) \). If \( S \) and \( T \) are \( G \)-complements with \( T \leq S \), then \( T = S \) [1, Theorem 2.9].

The proof of the following theorem is straightforward and will be omitted.

**Theorem 2.** If \( \theta \in Aut(F(G)) \) and \( S \) is a \( G \)-complement of \( F(G) \), then \( \theta S \) is a \( G \)-complement of \( F(G) \).

If \( \sigma \) is a retraction of \( G \) and \( \alpha \) is either an automorphism or an anti-automorphism of \( G \), then \( \sigma a \alpha^{-1} \) can be considered as a map from \( F(G) \) into \( G \) and as such, is a retraction of \( G \) [1, Theorem 5.1]. In the case where \( \alpha \) is the anti-automorphism of \( G \) given by \( x\alpha = \alpha^{-1}x \) and \( \sigma \alpha = \alpha \sigma \), then \( \sigma \) is called the dual of \( \alpha \). If \( S' \) is the kernel of \( \alpha \) and \( S \) is the kernel of \( \sigma \), then \( S' = S \). \( \alpha^{-1} A \in S \) [1, Corollary 5.2]. In case \( \alpha = \sigma \), we say that \( \sigma \) is a self dual retraction of \( G \). If \( G \) is a 2-divisible torsion-free abelian group, then \( G \) admits a self dual retraction.

Let \( \leq \) be a total order on the abelian group \( G \), \( A \in F(G) \), and \( k \) be a fixed integer. If we define \( A \leq (k+1) \max A - k \min A + 1 \), then it is easily verified that \( \sigma \) is a retraction of \( G \). Moreover, \( \sigma \) is not self dual.

**Theorem 3.** Let \( \sigma \) be a retraction of the abelian group \( G \) and for each \( A \in E(G) \) define

\[
A \phi_\sigma = (A \sigma) A (A^{-1} \sigma) \epsilon.
\]

Then \( \phi_\sigma \) is a homomorphism of \( F(G) \) and if \( \sigma \) is not self dual, then \( \phi_\sigma \) is an element of finite order in \( Aut(F(G)) \).

Proof. It is easy to see that \( \phi_\sigma \) is a homomorphism from \( F(G) \) into \( F(G) \). The map \( \phi_\sigma^{-1} \) given by

\[
A \phi_\sigma^{-1} = (A \sigma)^{-1} A (A^{-1} \sigma)^{-1}
\]

is a two-sided inverse of \( \phi_\sigma \) and so \( \phi_\sigma \in Aut(F(G)) \). It is not difficult to verify that

\[
A \phi_\sigma^\epsilon = (A \sigma)^\epsilon A (A^{-1} \sigma)^\epsilon
\]

for each natural number \( n \). Suppose that \( \phi_\sigma^n = 1 \) for some natural number \( n \). Then if \( A \in ker(\sigma) = S \), we have that

\[
A = A \phi_\sigma^n = (A \sigma)^n A (A^{-1} \sigma)^n = A (A^{-1} \sigma)^n.
\]

Since \( S \) is a \( G \)-complement, it follows that \( (A^{-1} \sigma)^n = 1 \), and since \( G \) is torsion-free, we have that \( A^{-1} \sigma = 1 \). Hence \( A \sigma^{-1} S \) and so \( S = S^{-1} \). Consequently, \( \sigma \) is self dual.

We remark in passing that if \( \sigma \) is self dual, then \( \phi_\sigma = 1 \).

**Corollary 3.1.** If \( G \) is a torsion-free abelian group, then \( Aut(F(G)) \) is infinite.

Note that if \( \sigma \) is a retraction of \( G \), \( \sigma \neq \sigma' \), and \( \phi_\sigma \) is given in the statement of Theorem 3, then \( \phi_\sigma \) is the identity automorphism on the group of units of \( F(G) \) and so is not a standard automorphism of \( F(G) \).

Let \( \sigma \) be a retraction of the abelian group \( G \) and \( \alpha \in Aut(G) \). For each \( A \in F(G) \) define \( A \phi_\alpha \) as follows:

\[
A \phi_\alpha = C g \text{ for a unique } C \in ker(\sigma) \text{ and unique } g \in G.
\]

Then

\[
A \phi_\alpha = C g.
\]

It is a simple matter to verify that \( \phi_{\alpha \sigma} = \phi_\sigma\phi_\alpha \) and \( \phi_{\sigma^{-1}} = \phi_\sigma^{-1} \).

We state some properties of \( \phi_{\alpha \sigma} \) in the following two theorems.

**Theorem 4.** If \( \sigma \) is a retraction of the abelian group \( G \) and \( \alpha \in Aut(G) \), then \( \phi_{\alpha \sigma} \) is an automorphism of \( F(G) \) that leaves the elements of \( ker(\sigma) \) fixed. The map from \( Aut(G) \) into \( Aut(F(G)) \) that sends \( \alpha \) to \( \phi_{\alpha \sigma} \) is an isomorphism of \( Aut(G) \) into \( Aut(F(G)) \). Moreover, \( \phi_{\alpha \sigma} \cap \phi_{\sigma} = \{ 0 \} \) and if \( \alpha \neq 1 \), then \( \phi_{\alpha \sigma} \) is not a standard automorphism.

**Theorem 5.** Let \( \sigma \) be a retraction of the abelian group \( G \) and let \( \alpha \in Aut(G) \) with \( \alpha \neq 1 \). If \( \alpha \sigma = \max A \) with respect to some total order of \( G \), then \( \phi_{\alpha \sigma} \phi_{\alpha} \neq \phi_{\sigma \alpha} \).

An immediate consequence of Theorem 5 is

**Corollary 5.1.** If \( G \) is a torsion-free abelian group, then \( Aut(F(G)) \) is nonabelian.

The semigroup \( F(G) \) is a partially ordered semigroup with respect to the relation of set containment. In general, an automorphism of \( F(G) \) will not preserve this partial order. More specifically, we have

**Theorem 6.** The only order preserving automorphisms of \( F(G) \) are the standard automorphisms.

Proof. Suppose that \( \theta \) is an order preserving automorphism of \( F(G) \) and let \( \eta \) be the standard automorphism of \( F(G) \) induced by \( \theta \). We proceed by induction on the cardinality of the set \( A \in F(G) \). If \( |A| = 1 \), then \( \theta A = A \). Suppose that for all \( A \in F(G) \) with \( |A| < k \), \( \theta A = A \), and let \( |B| = k - 1 \). If \( D = B \), then let \( C \in F(G) \) be such that \( C \setminus D = D \). Since \( \theta \) is order preserving, if \( b \in B \), then \( b \theta \in B \). Thus \( b \theta \setminus B \). If \( x \in C \), then \( x \theta = x \theta \setminus D = D \) and \( \theta \). Hence \( x \theta \setminus B \) for some \( b \in B \). Therefore, \( C \setminus B \). Suppose that \( C \setminus B \). Then \( |C| < |B| = k - 1 \), and by induction \( C \theta = C \theta = D = B \). But then \( C \theta = C \). Thus \( \theta \) is the standard automorphism \( \eta \).

**Theorem 7.** Let \( G \) be a torsion-free abelian group and let \( \sigma, \tau \) be retraction of \( G \) with kernels \( S \) and \( T \) respectively. There there exists \( 0 \in Aut(F(G)) \) with \( S \theta = T \). Thus, any two \( G \)-complements of \( F(G) \) are isomorphic semigroups.

Proof. If \( A \in F(G) \), then \( A \theta = B \) for unique \( B \in S \), \( C \in T \), and \( g, h \in G \). Define \( A \theta = B \theta \). It is an easy matter to verify that \( 0 \in Aut(F(G)) \) and that \( S \theta = T \).

**Theorem 8.** Let \( G \) be a torsion-free abelian group and let \( \alpha, \beta \) be distinct retractions of \( G \) with kernels \( S \) and \( T \) respectively. Then there exists \( 0 \in Aut(F(G)) \) such that \( 0 S = T \) and \( 0 T = S \).
Proof. Let \(\sigma \in \text{Aut}G\) be given by \(\sigma x = x^{-1}\) for every \(x \in G\). Then by Theorem 4, \(\phi_{\sigma}S = S\). If \(A \in T, S\), then \(A = Cg\) with \(C \in S, g \in G\) and \(g \neq 1\). Thus \(A\phi_{\sigma} = C(\sigma g) = Cg^{-1} \neq Cg = A\).

All retractions of \(Z\) are given by the formula

\[
A_{\sigma} = (k+1)\max A - k\min A.
\]

where \(k\) is an integer \([1, 5.5.6]\). The retraction induced by the natural order of \(Z\) is \(\sigma_0\) and \(\sigma_{-1}\) is the retraction induced by the dual of this order. We shall use \(\phi_{\sigma}\) to denote the automorphism \(\phi_{\sigma}S\) of \(F(G)\). Note that \(K = \{A \in F(Z) | 0 \in A, A \in Z^*\}\) is the kernel of \(\sigma_{-1}\). The following lemmas are necessary for the determination of \(\text{Aut}F(Z)\).

**Lemma 6.** For each \(k \in Z\),

\[
(\varphi_{-1})^{(2k+1)} = \varphi_k.
\]

**Lemma 7.** For each \(k \in Z\),

\[
(\ker \sigma_{-1})\varphi_{-1} = \ker \sigma_{-1}.
\]

**Lemma 8.** Let \(G\) be a torsion-free abelian group, \(S\) and \(T\) be \(G\)-complements in \(F(G), \lambda = \text{an isomorphism of } S\) onto \(T\), and \(\sigma \in \text{Aut}G\). Then there is an automorphism \(\theta\) of \(F(G)\) such that \(\theta \lambda = \lambda\) and \(\theta G = G\).

**Proof.** If \(A \in F(G)\), then \(A = Cg\) for unique \(C \in S\) and \(g \in G\). Define \(\theta A = (C \lambda)(\sigma g)\). It is easy to verify that \(\theta\) has the stated properties. We will denote \(\theta\) by \(\theta_{\lambda}\).

**Lemma 9.** Let \(\sigma\) be the automorphism of \(Z\) given by \(\sigma x = -x\) and define \(\mu_1, \mu_2, \mu_3\), and \(\mu_4\) as follows:

\[
\mu_1 = \theta_{k+1}, \quad \mu_2 = \theta_{k-1}, \quad \mu_3 = \theta_{k+1}.
\]

Then \(\{1, \mu_1, \mu_2, \mu_3\}\) is a subgroup of \(\text{Aut}F(Z)\) which is isomorphic to the Klein four-group. Moreover, \(\mu_2 \varphi_{-1} \mu_2 = \varphi_{k}, \mu_2 \varphi_{-1} \mu_2 = \varphi_{-1}, \) and \(\mu_2 \varphi_{-1} \mu_3 = \varphi_{k}\).

**Theorem 9.** The automorphism group of \(F(Z)\) is a splitting extension of \(Z\) by the Klein four-group.

**Proof.** Let \(\theta \in \text{Aut}F(Z)\) and \(K\) be the kernel of \(\sigma_{-1}\). By Theorem 2, \(K\theta = \ker\sigma_j\) for \(j \in Z\). By Lemma 7, we have that

\[
(\ker \sigma_j)\varphi_{j}^{(2k+1)} = K.
\]

Thus \(K\theta = K\theta\varphi_{j}^{(2k+1)} = K\). Now

\[
\theta \varphi_{j}^{(2k+1)} 1 = 1 \lor \nu \quad \text{and} \quad \theta \varphi_{j}^{(2k+1)} 1 = 1 \lor \nu.
\]

It follows that \(\theta \varphi_{j}^{(2k+1)} \in \{1, \mu_1, \mu_2, \mu_3\}\) and hence \(\theta = \eta \varphi_{j}^{(2k+1)}\) for some \(\eta \in \{1, \mu_1, \mu_2, \mu_3\}\).