Proceedings of the Edinburgh Mathematical Society (1980), 23, 103–121 ©

ON THE ENDOMORPHISM NEAR-RING OF A FREE GROUP

by R. WARWICK ZEAMER
(Received 19th September 1978)

0. Introduction

Suppose F is an additively written free group of countably infinite rank with basis T and let $E = \mathrm{End}(F)$. If we add endomorphisms pointwise on T and multiply them by map composition, E becomes a near-ring. In her paper "On Varieties of Groups and their Associated Near Rings" Hanna Neumann studied the sub-near-ring of E consisting of the endomorphisms of F of finite support, that is, those endomorphisms taking almost all of the elements of T to zero. She called this near-ring Φ_ω. Now it happens that the ideals of Φ_ω are in one to one correspondence with varieties of groups. Moreover this correspondence is a monoid isomorphism where the ideals of Φ_ω are multiplied pointwise. The aim of Neumann's paper was to use this isomorphism to show that any variety can be written uniquely as a finite product of primes, and it was in this near-ring theoretic context that this problem was first raised. She succeeded in showing that the left cancellation law holds for varieties (namely, $U(V) = U'(V)$ implies $U = U'$) and that any variety can be written as a finite product of primes. The other cancellation law proved intractable. Later, unique prime factorization of varieties was proved by Neumann, Neumann and Neumann, in (7). A concise proof using these same wreath product techniques was also given in H. Neumann's book (6). These proofs, however, bear no relation to the original near-ring theoretic statement of the problem.

The present paper originated in an attempt to find a near-ring theoretic proof of unique prime factorization of varieties. In the course of this it was found that not only does the set $\underline{V}$, of varieties (or equivalently, fully invariant subgroups of F) possess a natural monoid structure, but this can be extended to an equally natural multiplication on $\underline{C}$, the set of characteristic subgroups of F. Moreover, all results that could be obtained near-ring theoretically about the arithmetic of $\underline{V}$ could also be obtained for $\underline{C}$. As a further indication that arithmetic in $\underline{C}$ is similar to arithmetic in $\underline{V}$, Lemma 23.21 of (6), which H. Neumann uses to prove unique prime factorization of varieties, can be restated verbatim for characteristic subgroups, and a proof of this would amount to a proof of unique prime factorization in $\underline{C}$.

The advantage of considering the full endomorphism near-ring E instead of Φ_ω for the study of subgroups of F, is that the ordered bases of infinite rank subgroups are elements of E. The set of ordered bases for elements of $\underline{C}$, denoted BC, turns out to be a multiplicative subset of E and contains a submonoid BV, consisting of the ordered bases of elements of $\underline{V}$. The problem of unique prime factorization in $\underline{C}$ amounts to the problem of unique prime factorization up to multiplication by units in

BC. As a possible indication that unique prime factorization holds in $\underline{C}$ we can show that both cancellation laws hold in *BC*.

Arithmetically, $\underline{V}$ is a very special submonoid of $\underline{C}$. In fact,

$$K, K' \in \underline{C},\ K(K') \in \underline{V} \text{ implies that } K, K' \in \underline{V}.$$

This means that unique prime factorization in $\underline{C}$ implies unique prime factorization in $\underline{V}$. The wreath product proof of unique prime factorization in $\underline{V}$ does not extend to a proof of that result for $\underline{C}$. We conjecture that unique prime factorization does hold in $\underline{C}$ but it is likely that much deeper methods than those developed in this paper will be necessary to prove this.

The rest of the paper is divided into two sections. In the first we give some purely near-ring theoretic results about E. We show, for instance, that the set of two sided ideals of E is a monoid under pointwise multiplication and that the closed ideals of E form a monoid isomorphic to $\underline{V}$. In the second section we investigate the arithmetic of $\underline{C}$.

1. The Near-Ring End(F)

For a set A, let $Z(A)$ denote the free group on A. Let $T = \{t_i\}_{i=1}^{\infty}$ be a countably infinite set and let $F = F_\infty = Z(T)$. Let E be the near-ring with underlying set End(F) and with addition and multiplication defined as follows:

For $f, g \in \text{End}(F)$, $(f+g)(t) = f(t) + g(t)$ for all $t \in T$ and $f \circ g = f \circ g$, where maps are composed on the left.

Let $S = \{s_i\}_{i=1}^{\infty}$ be a countably infinite set disjoint from T. For $t_i \in T$, let $\bar{t}_i = s_i$ and $\bar{s}_i = t_i$. The elements of E can be represented uniquely as infinite sums of the form: $\Sigma_{i=1}^{\infty} w_i s_i$, $w_i \in F$. Addition is given by $(\Sigma\, w_i s_i) + (\Sigma\, u_i s_i) = \Sigma\,(w_i + u_i) s_i$; multiplication by $(\Sigma\, w_i s_i) \circ (\Sigma\, u_i(t_{i_j}) s_i) = \Sigma\, u_i(w_{i_j}) s_i$. We will use this infinite sum notation throughout this paper, $\Sigma\, w_i s_i$ is understood to mean $\Sigma_{i=1}^{\infty} w_i s_i$.

If we let F have the discrete topology and then let $F^\omega = E$ have the induced product topology, P, (E, P) is a topological near-ring. Note that $x_i \to x$ in P if and only if for $N \geq 1$ there exists an $M \geq 1$ such that $i \geq M$ implies $(x_i)_j = (x)_j$ for $1 \leq j \leq N$. It is easy to see from this that $a_i \to a$, $b_i \to b$ in P implies that $a_i + b_i \to a + b$, $a_i \circ b_i \to a \circ b$ in P. Since P has a countable basis addition and multiplication are continuous in P. From now on, by a convergent sequence in E we mean a sequence convergent with respect to P.

Using the above topology we can define in E both infinite sums and infinite products though in both cases we must specify the direction in which the sum or product is taken.

For $f \in E$, let $(f)_i = f(t_i)$. Given $\{f_i\}_{i=1}^{\infty} \subseteq E$, $\Sigma_{i=1}^{\to\infty} f_i$ is the limit of $\{f_1 + \cdots + f_n\}_{n \geq 1}$; $\Sigma_{i=1}^{\leftarrow\infty} f_i$ is the limit of $\{f_n + \cdots + f_1\}_{n \geq 1}$. Whenever we write $\Sigma_{i=1}^{\infty} f_i$ we mean $\Sigma_{i=1}^{\to\infty} f_i$. Also define $\Pi_{i=1}^{\to\infty} f_i = \lim\{f_1 f_2 \ldots f_n\}_{n \geq 1}$ $\Pi_{i=1}^{\to\infty} f_i = \lim\{f_n \ldots f_2 f_1\}_{n \geq 1}$. Let $e = \text{id}_F$ be E's multiplicative identity.

Proposition 1. *Let* $\{f_i\}_{i=1}^{\infty} \subseteq E$.

(a) $\Sigma_{i=1}^{\to\infty} f_i$ *converges if and only if for* $N \geqslant 0$ *there is an* $M \geqslant 0$ *such that for* $i \leqslant M$, $(f_i)_N = 0$. *Moreover,* $\Sigma_{i=1}^{\to\infty} f_i$ *converges if and only if* $\Sigma_{i=1}^{\to\infty} - f_i$ *converges, if and only if* $\Sigma_{i=1}^{\leftarrow\infty} f_i$ *converges.*

(b) $\Pi_{i=1}^{\to\infty} f_i$ *converges if and only if for* $N \geqslant 1$ *there is an* $M \geqslant 1$ *such that* $(f_M \dots f_1)_N$ *is a fixed point of* f_i *for* $i > M$.

(c) $f_i \to e$ *implies* $\Pi_{i=1}^{\to\infty} f_i$ *converges.*

Proof. (a) $\Sigma_{i=1}^{\to\infty} f_i$ converges if and only if $\{\Sigma_{i=1}^{n} f_i\}_{n=1}$ converges, if and only if for all $N \geqslant 1$ there exists an $M \geqslant 1$ such that $j, i \geqslant M \Rightarrow \Sigma_{k=1}^{j} (f_k)_N = \Sigma_{k=1}^{i} (f_k)_N$. For all $N \geqslant 1$, there exists an $M \geqslant 1$ such that $i \leqslant M \Rightarrow (f_i)_N = 0$. Therefore $\Sigma_{i=1}^{\to\infty} f_i$ converges $\Leftrightarrow \Sigma_{i=1}^{\to\infty} - f_i$ converges $\Leftrightarrow \{\Sigma_{i=1}^{m} - f_i\}_{n \geqslant 1}$ converges $\Leftrightarrow \{\Sigma_{i=n}^{1} f_i\}_{n \geqslant 1}$ converges $\Leftrightarrow \Sigma_{i=1}^{\leftarrow\infty} f_i$ converges.

(b) $\Pi_{i=1}^{\leftarrow\infty} f_i$ converges $\Leftrightarrow \{f_n \dots f_1\}_{n \geqslant 1}$ converges $\Leftrightarrow$ for all $N \geqslant 1$ there exists an $M \geqslant 1$ such that $i, j \geqslant M$ implies $(f_i \dots f_1)_N = (f_j \dots f_1)_N \Leftrightarrow$ for all $N \geqslant 1$ there exists $M \geqslant 1$ such that $i \geqslant M \Rightarrow (f_i \dots f_1)_N = (f_M \dots f_1)_N$, i.e. $f_i(f_M \dots f_1)_N = (f_M \dots f_1)_N$ for all $i \geqslant M$.

(c) Let $f_i \to e$. Then for $N \geqslant 1$ there exists $M \geqslant 1$ such that $i \geqslant M$ implies $(f_i)_N = t_N$. Therefore $i \geqslant M$ implies $(f_1 \dots f_i)_N = (f_1 \dots f_M)_N$. Hence for $N \geqslant 1$ there exists an $M \geqslant 1$ such that $i, j \geqslant M \Rightarrow (f_1 \dots f_i)_N = (f_1 \dots f_j)_N$. Hence $\Pi_{i=1}^{\to\infty} f_i$ converges.

We now use infinite products to express any automorphism of $Z(T)$ in terms of elementary Nielsen transformations. We take all facts concerning Nielsen reduced subsets of F from Section 3.2 of (**4**). Following the definition given there we define an elementary Nielsen transformation in our notation as follows:

Definition 1. An *elementary Nielsen transformation* is an element of E of one of the following forms:

(1) $\Sigma_{k \neq i} t_k s_k + (t_i + t_j)s_i$ where $i \neq j$.
(2) $\Sigma_{k \neq i,j} t_k s_k + t_i s_j + t_j s_i$ where $i \neq j$.
(3) $\Sigma_{k \neq i} t_k s_k + -t_i s_i$.

Let Aut denote the group of automorphisms of F. Let $N = \{1, 2, 3, \dots\}$. For any $\tau \in \mathrm{Aut}$, $\tau = \Sigma_{i \in N-A} t_i s_i + \Sigma_{i \in A} \tau_i s_i$ where $\tau_i \neq t_i$ for all $i \in A$. We write τ as $\tau = \Sigma_{i \in A} \tau_i s_i$ with the understanding that for $i \notin A$ $(\tau)_i = t_i$. Now for $i \neq j$, $(t_i + \epsilon t_j)s_i = (\epsilon t_j s_j)((t_i + t_j)s_i)(\epsilon t_j s_j)$. Similarly $(\epsilon t_j + t_i)s_i$ can be written as a product of elementary Nielsen transformations. Thus any automorphism of F fixing all but finitely many elements of T can be written as a finite product of elementary Nielsen transformations. (See Section 3.2 of (**4**).)

Proposition 2. (a) *With the relative topology from E,* Aut *is a topological group.*
(b) $\Pi_{i=1}^{\to\infty} \tau_i = \tau$, $\Pi_{i=1}^{\leftarrow\infty} \sigma_i = \sigma$, *where* $\sigma_i, \tau_i, \sigma, \tau \in \mathrm{Aut}$, *implies*

$$\tau^{-1} = \prod_{i=1}^{\leftarrow\infty} \tau_i^{-1},$$

$$\sigma^{-1} = \prod_{i=1}^{\to\infty} \sigma_i^{-1}.$$

(c) *Every $\tau \in \mathrm{Aut}$ can be represented in the form,*

$$\tau = \prod_{i=1}^{\to\infty} \tau_i = \prod_{i=1}^{\leftarrow\infty} \tau'_i,$$

where τ_i, τ'_i are elementary Nielsen transformations.

Proof. (a) As E is a topological near-ring, we need only show that $\tau \mapsto \tau^{-1}$ is a continuous map $\mathrm{Aut} \to \mathrm{Aut}$. For this it suffices to show that $\tau_i \to \tau$ implies $\tau_i^{-1} \to \tau^{-1}$.

Now if $x_i \in \mathrm{Aut}$ and $x_i \to e$, then for all $N \geq 1$ there exists an $M \geq 1$ such that $i \geq M$ implies that for $1 \leq j \leq N(x_i)_j = t_j$ and so $(x_i^{-1})j = t_j$. Therefore $x_i \to e$ if and only if $x_i^{-1} \to e$. Since multiplication is continuous in E, $\tau_i \to \tau \Rightarrow \tau^{-1}\tau_i \to e \Rightarrow \tau_i^{-1}\tau \to e \Rightarrow \tau_i^{-1} \to \tau^{-1}$.

(b) Since $\Pi_{i=1}^{\to\infty} \tau_i = \tau$ where $\tau_i, \tau \in \mathrm{Aut}$, $\{\Pi_{i=1}^{n} \tau_i\}_{n\geq 1} \to \tau$ and so by part (a) $\{\Pi_{i=n}^{1} \tau_i^{-1}\}_{n\geq 1} \to \tau^{-1}$. Thus $\Pi_{i=1}^{\leftarrow\infty} \tau_i^{-1} = \tau^{-1}$. Similarly, $\Pi_{i=1}^{\leftarrow\infty} \sigma_i = \sigma$ implies that $\sigma^{-1} = \Pi_{i=1}^{\to\infty} \sigma_i^{-1}$.

(c) Given $\tau \in \mathrm{Aut}$, define $\sigma_n \in \mathrm{Aut}$ by induction as follows: Let $\sigma_1 = e$. Suppose σ_i has been defined for $i \leq n$, $n \geq 1$. Let $p_n = \tau\sigma_1 \ldots \sigma_n$ and let $\sigma_{n+1} \in \mathrm{Aut}$ be such that $\sigma_{n+1}(t_i) = t_i$ for all $i > n+1$ and $((p_n\sigma_{n+1})_1, \ldots, (p_n\sigma_{n+1})_{n+1})$ is the result of Nielsen reducing $((p_n)_1, \ldots, (p_n)_{n+1})$ and putting those t_i that occur in this result first, arranging them in the order of their indices. One can verify by induction on n that

$$\mathrm{gp}((p_n)_1, \ldots, (p_n)_n) = \mathrm{gp}((\tau)_1, \ldots, (\tau)_n).$$

Thus for $N \geq 1$ there exists an $M \geq 1$ such that $M' \geq M$ implies $t_1, \ldots, t_N \in \mathrm{gp}(\tau_i)_{i=1}^{M'}$ and so $((p_{M'})_1, \ldots, (p_{M'})_{M'}) = (t_1, \ldots, t_{N'}(p_{M'})_{N+1}, \ldots, (p_{M'})_{M'})$. This follows from the fact that if $t \in T$ is an element of a subgroup H of F and B is a Nielsen reduced basis for H, then $\pm t \in B$. Thus $\{p_n\}_{n\geq 1} \to e$, and so $\Pi_{i=1}^{\to\infty} \sigma_i = \tau^{-1}\tau = \Pi_{i=1}^{\leftarrow\infty} \sigma_i^{-1}$. Each σ_i^{-1} is a finite product of elementary Nielsen transformations we have half of our result. The other half is obtained by applying our representation for τ to τ^{-1} and then using part (b).

We now apply the theory of Nielsen transformations to characterise the idempotents of Hanna Neumann's near-ring $\Phi_\omega = \{f \in E \mid (f)_i = 0$ for almost all $i\}$. For $x \in E$ we write $(x)_t = x_t = x(t)$ and $x_i = (x)_i = (x)_i$ as long as this causes no confusion.

Proposition 3. *For $a \in \Phi_\omega$, $a^2 = a$ if and only if $a = \tau f \tau^{-1}$ where $\tau \in \mathrm{Aut}$ and $f \in \Phi_\omega$ is of the form $f = \Sigma_{t\in A} (t + K_t)\bar{t}$, A a finite subset of $T, K_t \in \mathrm{ngp}(T - A)$ for $t \in A$.*

Proof. $a = \Sigma_{t\in B}\, a_t\bar{t}$ where $B = \{t \in T \mid a_t \neq 0\}$ is finite. Now there exists an $x \in \mathrm{Aut}$ such that $x_t = t$ for $t \notin B$ and $\{(ax)_t \neq 0 \mid t \in B\}$ is Nielsen reduced. Let $A = \{t \in T \mid (ax)_t \neq 0\} \subseteq B$. Then $f = x^{-1}ax = \Sigma_{t\in A}\, x^{-1}((ax)_t)\bar{t}$ is idempotent with kernel $\mathrm{ngp}(T - A)$ and $\{f_t\}_{t\in A} = \}(x^{-1}ax)_t\}_{t\in A}$ is free.

$f^2 = f \Rightarrow f(f - e) = 0$. For $t \in A$, $f_t - t$ is in $\mathrm{ngp}(T - A)$ so $f_t = t + K_t$ where $K_t \in \mathrm{ngp}(T - A)$. Therefore $f = \Sigma_{t\in A}\, (t + K_t)\bar{t}$ and $a = xfx^{-1}$, completing the proof.

Problem. The above characterisation of the idempotents of Φ_ω can be extended to the whole of E if the following is true:

$f \in E \Rightarrow$ there exists an $x \in \text{Aut}$ such that $\{(fx)_t \neq 0 \mid t \in T\}$ is free. This is equivalent to saying that if $f \in \text{End}(F)$, $\text{Ker}(f) = \text{ngp}(B')$ for some $B' \subseteq B$, B is a basis for F. As yet we have been unable to prove or disprove this.

Though E is not d.g., it *is* topologically d.g., as noted by Tharmaratnam in (8). Thus every $f \in E$ can be written as an infinite convergent sum of distributive elements.

Consider $\{t_i s_j\}_{i,j \geq 1}$. These are clearly distributive elements. For $f \in E$, $f = \Sigma_{i=1}^{\infty} w_i(t_{i_j}) s_i = w_1(t_{1_j} s_1) + w_2(t_{2_j} s_2) + \cdots + w_i(t_{i_j} s_i) + \cdots$ which is clearly a convergent sum of distributive elements. This infinite sum representation gives multiplication in E the same convenient structure it has in a d.g. near ring.

Proposition 4. *The monoid of distributive elements of E is $D = \{\Sigma_{i=1}^{\infty} d_i s_i \mid d_i \in T^0\}$, where $T^0 = T \cup \{0\}$.*

Proof. Let D denote E's monoid of distributive elements. Clearly $x \in T^0$ implies $xs_i \in D$. Thus if $d = \Sigma_{i=1}^{\infty} d_i s_i$, $d_i \in T^0$ then if $a, b \in E$,

$$(a+b)d = \Sigma_{i=1}^{\infty} (a+b)(d_i s_i) = \Sigma_{i=1}^{\infty} (a(d_i s_i) + b(d_i s_i)) = ad + bd,$$

since multiplication in E is continuous.

Now suppose $d \in D$. Since $t_i s_i \in D$ we have $d_i s_i \in D$. Let $d_i = w(t_{i1}, \ldots, t_{in})$ in F and let $x = \Sigma_{j=1}^{n} t_{ij} s_{ij}$. For $k \geq 1$, $(kx)(d_i s_i) = k(x(d_i s_i))$ and so $w(kt_{i1}, \ldots, kt_{in}) = kw$. Thus $w = Mt$ for some $M \in Z$ and $t \in T$. $Mts_i \in D$ implies that $(t_i \bar{t} + t_2 \bar{t})Mts_i = (Mt_1 + Mt_2)s_i = M(t_1 + t_2)s_i$. Hence M is 1 or 0 and $d_i \in T^0$, completing the proof.

We will now consider the ideal theory of E. First we need some notation. If $x \in E$, denote $\{x_i \mid i \geq 1\}$ by $\text{cmp}(x)$. Let $\underline{\text{gp}}(x) = \text{gp}(\text{cmp}(x))$ and $\underline{\text{ngp}}(x) = \text{ngp}(\text{cmp}(x))$. If $A \subseteq E$, let $\underline{\text{gp}}(A) = \text{gp}(\cup_{a \in A} \text{cmp}(a))$ and $\underline{\text{ngp}}(A) = \text{ngp}(\cup_{a \in A} \text{cmp}(a))$.

Note that the underlying group of the near-ring E is F^{ω} so we will often refer to subsets of E of the form $H^{(\omega)}$ where H is a subset of F and $H^{(\omega)} = H^{\omega} \cap \Phi_{\omega}$.

Definition 2. For $A \subseteq E$, A is *left closed* if $E \cdot A \subseteq A$. A is *right closed* if $A \cdot E \subseteq A$. A is two-sided if A is right and left closed.

Remark 1. For $x \in E$, $x \cdot E = \underline{\text{gp}}(x)^{\omega}$.

Remark 2. For a subgroup H of F, $H^{\omega} \subseteq E$ is a right closed subgroup of E.

Proposition 5. *The following are equivalent*:

(1) *$A \subseteq E$ is an ideal*;

(2) *$A \subseteq E$ is a two-sided normal subgroup of E*;

(3) *$A \subseteq E$ is a two-sided subgroup and $\underline{\text{ngp}}(a)^{\omega} \subseteq A$ for $a \in A$.*

Proof. (1) $\Rightarrow$ (2): If $A \subseteq E$ an ideal then $A < E$, $EA = A$ and for $x, y \in E$, $a \in A$, $(x+a)y - xy \in A$. Letting $x = 0$, we have that A is right closed.

(2) $\Rightarrow$ (3): Since $|S| = \omega$ we may write S as a disjoint union, $S = \cup_{f \in F} \{s_{i_f}\}_{i=1}^{\infty}$. Let $x = \Sigma_{f \in F} \Sigma_{i=1}^{\infty} f s_{i_f} \in E$, $y = \Sigma_{f \in F} \Sigma_{i=1}^{\infty} t_i s_{i_f} \in E$. Take $a \in A$. $z = x + ay - x \in A$ so for

$f \in F$, $i \geqslant 1$ $z_{i_f} = x_{i_f} + (ay)_{i_f} - x_{i_f} = f + a_i - f$. By Remark 1, $zE = \underline{\mathrm{gp}}(z)^\omega = \underline{\mathrm{ngp}}(a)^\omega \subseteq A$.

(3) $\Rightarrow$ (1): We need only show that $x, y \in E$, $a \in A$ implies that $(x + a)y - xy \in A$. But $(x + a)y - xy = d + xy - xy$ where $d \in \underline{\mathrm{ngp}}(a)^\omega \subseteq A$. This completes the proof.

We now give explicit formulas for the two-sided subgroup, ideal, and right closed subgroup generated by a subset of E.

Proposition 6. *For any $A \subseteq E$,*

(1) *The two-sided subgroup generated by A is*

$$RL(A) = \cup\{\underline{\mathrm{gp}}(B)^\omega \mid B \text{ a finite subset of } EA\}.$$

(2) *The ideal generated by A is*

$$\mathrm{Ideal}(A) = \cup\{\underline{\mathrm{ngp}}(B)^\omega \mid B \text{ a finite subset of } EA\}.$$

(3) *The right closed subgroup generated by A is*

$$R(A) = \cup\{\underline{\mathrm{gp}}(B)^\omega \mid B \text{ a finite subset of } A\}.$$

Proof. (1): $x, y \in RL(A) \Rightarrow x \in \underline{\mathrm{gp}}(B)^\omega$, $y \in \underline{\mathrm{gp}}(C)^\omega, B, C \subseteq EA$ finite $x + y \in \underline{\mathrm{gp}}(B \cup C)^\omega$ and so $x + y \in RL(A)$. Thus $RL(A)$ is a subgroup and similarly $\mathrm{Ideal}(A)$ and $R(A)$ is a subgroup. All three sets are right closed by Remark 2. Therefore $R(A)$ is a right closed subgroup.

For $x \in E$ and a finite $B \subseteq EA$, $x\underline{\mathrm{ngp}}(B)^\omega \subseteq \underline{\mathrm{ngp}}(xB)^\omega$ and $x + \mathrm{ngp}(B)^\omega - x$ is contained in $\underline{\mathrm{ngp}}(B)^\omega$. Hence $\mathrm{Ideal}(A)$ is an ideal of E. Similarly one can show that $RL(A)$ is a two-sided subgroup of E.

Now suppose $K \supseteq A$, where K is a two-sided subgroup of E. Then $K \supseteq EA$. Suppose that $\{b_1, \ldots, b_n\} = B \subseteq EA$, finite. Write $S = \cup_{i=1}^{m} \{s_{ij}\}_{j=1}^{\infty}$, a disjoint union of countably infinite sets. Let $f_i = \Sigma_{j=1}^{\infty} t_j s_{ij}$ for $1 \leqslant i \leqslant n$. Then $b = \Sigma_{i=1}^{n} b_i f_i$ is in K. Thus $bE = \underline{\mathrm{gp}}(b)^\omega = \underline{\mathrm{gp}}(B)^\omega \subseteq K$. This proves (1) and a similar argument proves (3).

To prove (2) suppose $K \supseteq A$ is an ideal. Take a finite $B \subseteq EA$. As in the proof of (1) we have $b \in K$ such that $\underline{\mathrm{gp}}(b) = \underline{\mathrm{gp}}(B)$. Hence $\underline{\mathrm{ngp}}(b) = \underline{\mathrm{ngp}}(B)$ and by Proposition 5, $\underline{\mathrm{ngp}}(B)^\omega = \underline{\mathrm{ngp}}(b)^\omega \subseteq K$. Therefore $K \supseteq \mathrm{Ideal}(A)$, completing the proof.

We now turn to the multiplicative structure of the set of two-sided subgroups of E which we denote by RL.

Definition 3. For $A, B \in RL$, define $A \cdot B = AB = \{\Sigma_{i=1}^{n} a_i b_i \mid a_i \in A,\ b_i \in B\}$.

AB is certainly a left closed subgroup of E but we do not know *a priori* whether it is right closed since E is not d.g.. The following theorem shows that it is. The proof is an adaption to E of H. Neumann's proof that ideal multiplication is associative in Φ_ω.

Notation. For $w \in Z(X)$, let

$$X(w) = \{x \in X \mid x \text{ occurs in the reduced } X\text{-form of } w.\}$$

For $f \in E$ let

$$\mathrm{supp}(f) = \{t \in T \mid f_t \neq 0\}.$$

https://doi.org/10.1017/S0013091500003655 Published online by Cambridge University Press

Theorem 1. *$A, B \in RL$ implies $AB = \{\Sigma_{i=1}^{m} a_i b_i \mid a_i \in A, b_i \in B\} = \{ab \mid a \in A, b \in B\}$. Thus RL forms a monoid under pointwise multiplication.*

Proof. Take $A, B \in RL$. It suffices to show that for $a_1, a_2 \in A$, $b_1, b_2 \in B$,

$$a_1 b_1 + a_2 b_2 = ab \text{ for some } a \in A,\ b \in B.$$

Since $F = Z(T)$ and T is infinite we may take right distributive elements (Proposition 4) f, f', g, g' in E such that $ff' = gg' = e$ and $T(f'(F)) \cap \text{supp}(g) = t(g'(F)) \cap \text{supp}(f) = \emptyset$, and so $gf' = g'f = 0$. Let $a = a_1 f + a_2 g$, $b = f'b_1 + g'b_2$. Then $a \in A$, $b \in B$, and

$$\begin{aligned} ab &= (a_1 f + a_2 g) f' b_1 + (a_1 f + a_2 g) g' b_2 \\ &= (a_1 ff' + a_2 gf') b_1 + (a_1 fg' + a_2 gg') b_2 \\ &= (a_1 e + a_2 0) b_1 + (a_1 0 + a_2 e) b_2 = a_1 b_1 + a_2 b_2. \end{aligned}$$

This monoid RL is also a lattice with respect to containment and can be written as a disjoint union of sublattices in the following way: Let $\underline{V}$ denote the set of fully invariant subgroups of F. Then

$$RL = \cup_{V \in \underline{V}} RL_V, \text{ where } RL_V = \{A \in RL \mid V^{(\omega)} \subseteq A \subseteq V^{\omega}\}.$$

To see this suppose A is right closed, $A \subseteq E$. For $i \geq 1$ define $p_i : E \to F$, an additive homomorphism by $p_i(f) = f_i$ for $f \in E$. $A \cdot (t_i s_j) = p_i(A) s_j \subseteq A$ since A is right closed. Hence $p_j(p_i(A) s_j) \subseteq p_j(A)$, and so $p_i(A) \subseteq p_j(A)$. Thus for all $i, j, p_i(A) = p_j(A) = H$, a subgroup of F. Clearly $A \subseteq H^{\omega}$ and since $A \supseteq Hs_i$ for all i, $A \supseteq H^{(\omega)}$. If A is left closed $H \in \underline{V}$.

Theorem 2. (1) $RL_V \cdot RL_U \subseteq RL_{U(V)}$.

(2) *The minimal and maximal ideals of RL_V are I_V and V^{ω} respectively, where $I_V = \cup\{\text{ngp}(A)^{\omega} \mid A$ a finite subset of $V\}$.*

(3) *The minimal and maximal elements of RL_V are $MV = \cup\{\text{gp}(A)^{\omega} \| A$ a finite subset of $V\}$ and V^{ω} respectively.*

(4) *For $U, V \in \underline{V}$, $M_V \cdot M_U = M_{U(V)}$ and $V^{\omega} \cdot U^{\omega} = U(V)^{\omega}$. Thus $\{M_V\}_{V \in \underline{V}}$ and $\{V^{\omega}\}_{V \in \underline{V}}$ are submonoids of RL anti-isomorphic to $\underline{V}$.*

Proof. Take $A \in RL_V$, $B \in RL_U$. Then $V^{(\omega)} \cdot U^{(\omega)} \subseteq AB \subseteq V^{\omega} \cdot U^{\omega} \subseteq (U(V))^{\omega}$. H. Neumann proved in (5) that $V^{(\omega)} \cdot U^{(\omega)} = U(V)^{(\omega)}$. This proves (1).

(2): V is clearly a two-sided normal subgroup of E and hence the maximal ideal and the maximal element of RL_V. Following the proof of Proposition 6, I_V is easily checked to be an ideal of E. Suppose $K \in RL_V$ is an ideal. For $A = \{a_1, \ldots, a_n\} \subseteq V$, $f = a_1 s_1 + \cdots + a_n s_n \in V^{(\omega)} \subseteq K$ so by Proposition 5, $\text{ngp}(A)^{\omega} = \underline{\text{ngp}(f)}^{\omega} \subseteq K$. Hence $I_V \subseteq K$. This proves (2).

(3): M_V is easily checked to be in RL_V. Now if $K \supseteq V^{(\omega)}$ and $K \in RL_V$ then for $A = \{a_1, \ldots, a_n\} \subseteq V$, $f = a_1 s_1 + \cdots + a_n s_n \in V^{(\omega)} \subseteq K$. Hence $\text{gp}(A)^{\omega} = \underline{\text{gp}}(f)^{\omega} \subseteq K$ and so $K \supseteq M_V$. This proves (3).

(4): By (1), $M_V \cdot M_U \supseteq M_{U(V)}$. Take $v \in M_V$, $u \in M_U$. Then $v \in \text{gp}(A)^{\omega}$, $u \in \text{gp}(B)^{\omega}$ where A, B are finite, $A \subseteq V$, $B \subseteq U$. But $vu \in \underline{\text{gp}}(vu)^{\omega} \subseteq \text{gp}(vB)^{\omega}$. Therefore since $vB \subseteq U(V)$ is finite, $vu \in M_{U(V)}$. Hence $M_V \cdot M_U \subseteq M_{U(V)}$.

It remains to show $U(V)^{\omega} = V^{\omega} \cdot U^{\omega}$ where $U, V \subseteq F$ are verbal. Now consider $f = \Sigma_{i=1}^{\infty} u_i(\underline{v_{ij}})_{j=1}^{n_i} s_i \in U(V)^{\omega}$. $T = \cup_{i=1}^{\infty} T_i$, a disjoint union where each $T_i\{t_{ij}\}_{j=1}^{n_i}$. $f = (\Sigma_{i=1}^{\infty} \Sigma_{j=1}^{n_i} v_{ij}\bar{t}_{ij})(\Sigma_{i=1}^{\infty} u_i(t_{ij})s_i) \in V^{\omega} \cdot U^{\omega}$. Thus $U(V)^{\omega} \subseteq V^{\omega} \cdot U^{\omega}$. On the other hand if $v = \Sigma_{i=1}^{\infty} v_i s_i$ and $u = \Sigma_{i=1}^{\infty} u_i(t_{ij})_{j=1}^{n_i} s_i$, then $v \cdot u = \Sigma_{i=1}^{\infty} u_i(v_{ij})_{j=1}^{n_i} s_i \in U(V)^{\omega}$. Hence $U(V)^{\omega} = V^{\omega} \cdot U^{\omega}$, proving (4).

Corollary 1. *The closed ideals of E form a monoid anti-isomorphic to the monoid of varieties. The anti-isomorphism is:* $\underline{V} \ni V \mapsto V^{\omega}$.

Proof. In light of Theorem 2, we need only show that A is a closed ideal of E if and only if A has form V^{ω} for some $V \in \underline{V}$. First V^{ω} is an ideal and it is clearly closed. If A is a closed ideal then $A \in RL_V$ for some $V \in \underline{V}$ and so $V^{(\omega)} \subseteq A$. Now if $v \in V^{\omega}$, then for all $n \geqslant 1, \Sigma_{i=1}^{n} v_i s_i = p_n \in A$. Since $p_n \to v$ and A is closed, $v \in A$. Therefore $A = V^{\omega}$.

2. The Monoid of Characteristic Subgroups of F

In this section we use E to study the multiplicative structure of the set of subgroups of F.

Definition 1. For $M \subseteq E$ a semigroup, call $x \in E$ an *M-element* if $\overline{\mathrm{gp}}(x)$ is M invariant, that is, $M \cdot \overline{\mathrm{gp}}(x)$. In particular, if x is an E-element we say x is *verbal.* If x is an Aut-element, we say x is *characteristic.*

Definition 2. Suppose $K \subseteq F$ is infinite rank. We say $x \in E$ is *basic for* K if $\mathrm{cmp}(x)$ is a basis for K. By convention, $0 \in E$ is basic for $\{0\}$. We call $x \in E$ *free* if $\mathrm{cmp}(x)$ is free.

Remark 1. If $M \subseteq E$ is a multiplicative semigroup then x is an M-element if and only if $m \in M \Rightarrow mx = xm'$ for some $m' \in E$.

Remark 2. $\{x \mid x$ is basic for some $K \subseteq F, \mathrm{rank}(K) = \omega\} = \mathrm{Mon}(F, F) = \{x \in E \mid x$ is free$\}$.

Remark 3. The free elements of E form a multiplicative monoid.

Now suppose that $K, U \subseteq F$ are subgroups where K is of infinite rank and $U \neq 0$ is characteristic. Then we may take $k, u \in E$ such that k is basic for K, u is basic for U. Define the product of subgroups $K \cdot U = U(K) = \overline{\mathrm{gp}}(ku)$. To show this product is well defined we must show it is independent of our choice of k and u. So take k' and u' basic for K and U respectively. Then there are $x, y \in \mathrm{Aut}$ such that $k' = kx$ and $u' = uy$. $k'u' = kxuy = kux'y$ and so $\overline{\mathrm{gp}}(k'u') \subseteq \overline{\mathrm{gp}}(ku)$. By symmetry we have equality and hence the product of subgroups, $U(K)$, is well defined. Note that k basic for K, u basic for U implies that ku is basic for $U(K)$. Note also that according to our definitions, $0(K) = U(0) = 0$.

It happens that the above definition of $U(K)$ for U characteristic extends the usual definition of $U(K)$ for U verbal. To see this suppose U is verbal and take u basic for U, k basic for K. $\underline{\text{gp}}(ku) = kU \subseteq \{u(a_1, \ldots, a_n) \mid u \in U, a_i \in K\}$. But if $x = u(a_1, \ldots, a_n)$ where $u \in U$ and $a_i = a_i(k_{ij})_{j=1}^{n_i}$, $k_{ij} \in \text{cmp}(k)$, then U verbal implies $x \in \underline{\text{gp}}(ku)$. Therefore $\underline{\text{gp}}(ku) = \{u(a_1, \ldots, a_n) \mid u \in U, a_i \in K\}$, which is the usual definition of $U(K)$.

Proposition 1. *The set $\underline{C}$ of characteristic subgroups of F has a natural monoid structure extending the monoid structure on $\underline{V}$.*

Proof. $\underline{C}$ will be multiplicatively closed if for k basic for $K \in \underline{C}$. $x \in \text{Aut}$ implies that x' in $xk = kx'$ is an element of Aut. But this must be so since k and xk are basic for K. Thus $\underline{C}$ is multiplicatively closed. Clearly it has identity F. It remains to show that the multiplication we have defined is associative: Take $K, H, L \in \underline{C}$ with k, h, l basic for K, H, L respectively. $(KH)L = \underline{\text{gp}}((kh)l) = \underline{\text{gp}}(k(hl)) = K(HL)$ since hl is basic for HL.

We now introduce two multiplicative submonoids of $(E, \cdot)$ which will play a central role throughout the rest of this paper.

Let $BC = \{x \in E \mid x \text{ is basic for some } K \in \underline{C}\}$, and let $BV = \{x \in E \mid x \text{ is basic for some } V \in \underline{V}\}$.

Proposition 2. *$BV \subseteq BC$ are multiplicative submonoids of E such that*

(1) *$BV = \{x \in E \mid \text{For } y \in E,\ yx = xy' \text{ for some unique } y' \in E\}$.*

(2) *$BC = \{x \in E \mid \text{For } y \in \text{Aut},\ yx = xy' \text{ for some } y' \text{ unique in } E\}$.*

(3) *$\underline{\text{gp}} : BC \to \underline{C}$ and $\underline{\text{gp}} : BV \to \underline{V}$ are monoid epimorphisms. For $a, b \in BC$ $\underline{\text{gp}}(a) = \underline{\text{gp}}(b)$ if and only if $a = bx$ for some $x \in$ Aut.*

Proof. $a, b \in BV$, $f \in E$ implies $fab = af'b = abf''$ for some f', f'' in E since a, b are both E-elements. Hence $ab \in BV$ since a, b are free. Now suppose $a, b \in BC$. $x \in \text{Aut} \Rightarrow xab = ax'b = abx''$ for some $x', x'' \in$ Aut by the proof of Proposition 1. ab is therefore characteristic. It is free since a and b are free. Thus $ab \in BC$.

Since for x free $xz = xy$ implies $z = y$ and any x basic for $K \in \underline{C}$ is an Aut-element, $\subseteq$ holds in (2). Now take x in the right hand side of (2). $\underline{\text{gp}}(x)$ is characteristic and it remains to show that x is free. If not, there exists a $k, \overline{0} \neq k \in E$, such that $xk = 0$. But then $e \cdot x = x \cdot e = x \cdot (e + k)$, a contradiction of the uniqueness of the e' such that $e \cdot x = x \cdot e'$. Thus x is free and hence in BC. (1) is proved similarly.

(3): Since $\underline{\text{gp}} : BC \to \underline{C}$ is a monoid homomorphism by the definition of multiplication in $\underline{C}$ and is onto since every $0 \neq K \in \underline{C}$ has a countably infinite basis and 0 is basic for $0 \in \underline{C}$, the first statement of (3) is proved.

Suppose $a, b \in BC$. $\underline{\text{gp}}(a) = \underline{\text{gp}}(b) \Rightarrow \text{cmp}(a), \text{cmp}(b)$ are bases for the same subgroup of $F \Rightarrow$ there exists $x \in$ Aut such that $a = bx$.

Proposition 2 *allows us to define the following multiplicative homomorphisms.*

Definition 3. For $a \in BV$ define $Y_a : E \to E$ such that for $x \in E$, $xa = a(x)Y_a$. For

$a \in BC$ define $C_a : \mathrm{Aut} \to \mathrm{Aut}$ such that $x \in \mathrm{Aut}$ implies that $xa = a(x)C_a$. Both maps are well defined by Proposition 2.

Proposition 3. (1) *For* $a \in BV$, $Y_a | \mathrm{Aut} = C_a$.

(2) *For* $a, b \in BV$, $Y_{ab} = Y_a \circ Y_b$; *for* $a, b \in BC$, $C_{ab} = C_a \circ C_b$.

(3) *For* $a \in \mathrm{Aut}$, $(x)Y_a = a^{-1}xa$ *for all* $x \in E$.

(4) *For* $a \in BV$, $Y_a : E \to E$ *is a multiplicative homomorphism. For* $a \in BC$, $C_a : \mathrm{Aut} \to \mathrm{Aut}$ *is a group homomorphism.*

Proof. $BV \subseteq BC$ implies (1) is obvious from Definition 3.

(2): For $a, b \in BV$, $x \in E$, $ab(x)Y_{ab} = xab = a(x)Y_a b = ab((x)Y_a)Y_b$. ab free gives $Y_{ab} = Y_a \circ Y_b$. Similarly $C_{ab} = C_a \circ C_b$.

(3): $a \in \mathrm{Aut} \Rightarrow$ For $x \in E$, $xa = aa^{-1}xa = a(x)Y_a$ and so $a^{-1}xa = (x)Y_a$.

(4): $a \in BV$ implies that for $x, y \in E$, $xya = a(xy)Y_a$. Also $xya = xa(y)Y_a = a(x)Y_a(y)Y_a$. Similarly C_a is a group homomorphism for all $\alpha \in BC$.

We have laid the basis for our discussion of $\underline{C}$.

2.1. Cancellation in $\underline{C}$

In this section we show that one cancellation law in $\underline{C}$ is trivial and that the real problem in the arithmetic of $\underline{C}$, as in the arithmetic of $\underline{V}$, is the proof of the other one. We are able to prove a weak form of this other cancellation law.

Proposition 4. *Left cancellation holds in* $\underline{C}$, *that is,* $K, H', H \in BC, KH = KH'$ *implies* $H = H'$.

Proof. If k, h, h' basic for K, H, H' respectively, $KH = \underline{\mathrm{gp}}(kh) = \underline{\mathrm{gp}}(kh') = KH'$ implies that $kh = kh'x$ for some $x \in \mathrm{Aut}$. But k free implies $\overline{h = h'x}$ and so $H = H'$.

We aim to prove the following weak form of the right cancellation law in $\underline{C}$: If $U \neq 0$ is in $\underline{C}$ and K, K' are subgroups of F of infinite rank then

$$KU = K'U, K' \subseteq K \Rightarrow K = K'.$$

We prove this by combinatorial methods.

Notation 1. For $w \in F$ let $|w|$ be the length of its T-reduced form.

2. For $u, v \in F$, $u + v$ is a reduced sum if $|u + v| = |u| + |v|$.

3. Recall from Section 3.2 of (4) that if $A \subseteq F$, A is Nielsen reduced if and only if for $a, b, c \in \pm A$, $b \neq -a, -c$, $|a + b| \geq |a|, |b|$ and $|a + b + c| > |a| + |c| - |b|$. Note that this last condition implies that if $0 \in A$, $A = \{0\}$.

4. Suppose A is Nielsen reduced, $A \subseteq F$. Then any $a \in A$ has the unique representation, $a = a_0 + c(a) + a_1$, a reduced sum where $c(a)$, the core of a, is the section of a none of whose symbols is cancelled in any reduced A-sum, $\epsilon a' + a + \delta a''$, $a', a'' \in A$, $\epsilon, \delta = \pm$. Note $c(a) \neq 0$ since A is Nielsen reduced and $c(a)$ is the section of a not cancelled in any reduced word, $w(a, a_1, \ldots, a_n)$, $a_i \in A$. (See Chapter I of (3).)

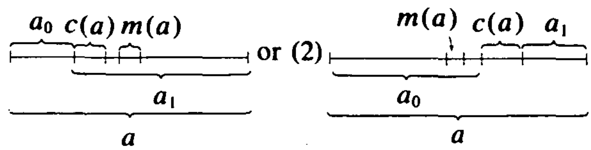
5. Suppose $0 \neq x \in F$. Let $m(x)$, the middle of x, be the non-zero section of x of

minimal length such that $x = x_0 + m(x) + x_1$, is a reduced sum where $|x_0| = |x_1|$. Note $|m(x)|$ is one if $|x|$ is odd and two if $|x|$ is even.

6. For $A \subseteq F$ define $|A| = \min\{|a| \mid a \in A\}$.

Lemma 1. *If $A \subseteq F$, a Nielsen reduced set, then $a \in A$ implies $m(a)$ and $c(a)$ must overlap.*

Proof. If $c(a)$ and $m(a)$ do not overlap we have:

(1)


If (1) holds there exists $\epsilon a' \in \pm A$ such that $\epsilon a' \neq -a$ and in the sum, $a + \epsilon a'$, a_1 is cancelled. But then $|a + \epsilon a'| < |a'|$, a contradiction of A's being Nielsen reduced. Case (2) is treated similarly.

The following lemma is the heart of our proof of the weak right cancellation law.

Lemma 2. *If $U \neq 0$ in $\underline{C}$ and $a \in E$ is free then $a \cdot U \supseteq U$ implies $a \in$* Aut.

Proof. $\underline{\text{gp}}(a)$ is a free group of infinite rank and so has a Nielsen reduced basis B. Let $B = \{b_i\}_{i=1}^{\infty}$ and put $b = \Sigma_{i=1}^{\infty} b_i s_i$. Then there exists $x \in \text{Aut}$ such that $ax = b$. Thus $bU = axU = aU \supseteq U$. For any ϵt in $\pm T$ there exists a $u \in U$ of minimal length in U such that $u = \epsilon t + u'$, a reduced T-sum for some $u' \in F$. Now there exists a $v(t_{ij})_{j=1}^{n} \in U$ such that $bv = v(b_{ij})_{j=1}^{n} = u$. B Nielsen reduced $\Rightarrow |v| = |u|$ and each element of B involved in bv contributes exactly its core (which must have length one) to the reduced T-form of u. $v = \delta t_{ij} + v'$ is a reduced T-sum where $v' \in F$. Hence $u = \delta b_{ij} + bv'$ is a B-reduced sum. Thus $c(b_{ij}) = \epsilon t$ and by Lemma 1 $\delta b_{ij} = \underline{\epsilon t} + \eta t'$, $\eta t' \in \pm T^0$, where we have underlined the core of b_{ij} in δb_{ij}. If $\eta t' \neq 0$ then by repeating the same argument with $-\eta t'$ in place of ϵt we get a $\gamma b_k \in \pm B$ such that $\gamma b_k = \underline{-\eta t'} + \xi t''$. Since $-\eta t'$ is the core of γb_k it can only cancel in an unreduced B-sum. Thus we have $\delta b_{ij} = -\gamma b_k = -\xi t'' + \underline{\eta t'} = \underline{\epsilon t} + \eta t'$. But this puts the core of b_{ij} in two mutually exclusive places. Thus $\eta t' = 0$ and for any ϵt in $\pm T$ there is a $\delta b_{ij} \in \pm B$ such that $\delta b_{ij} = \epsilon t$. Thus $\underline{\text{gp}}(a) = \underline{\text{gp}}(b) = F$ and so $a \in \text{Aut}$.

Theorem 3. *If $U \neq 0$ is characteristic and $K, K' \subseteq F$ are subgroups of infinite rank then $K' \subseteq K$, $K'U \supseteq KU$ implies $K = K'$.*

Proof. Let u, k, k' be basic for U, K, K' respectively. ku and $k'u$ are basic for KU and $K'U$ respectively. Thus since $K'U \supseteq KU$, there exists an $x \in E$ such that $ku = k'ux$. Since $K' \subseteq K$ there exists $y \in E$ such that $ky = k'$. k' free implies y is free. Hence $ku = k'ux = kyux \Rightarrow u = yux \Rightarrow U \subseteq yU$ so by Lemma 2 $y \in \text{Aut}$. So $K = K'$, completing the proof.

2.2. On Y_a and C_a

In this section we will use the techniques of Section 2.1 to show that for $a \in BC$, $C_a : \mathrm{Aut} \to \mathrm{Aut}$ is a group monomorphism which is epi if and only if $a \in \mathrm{Aut}$.

Lemma 3. *Suppose K is a subgroup of F. $K_0 = \{k \in K \mid 0 \neq |k| \text{ minimal}\}$. Then K_0 consists of primitive elements of K and if B is a Nielsen reduced basis for K, $k \in K_0$ is either in $\pm B$ or of the form $k = \epsilon b_i + \delta b_2$, where $b_1 \neq b_2$ are in $B \subseteq K_0$.*

Proof. This is simply Corollary 3.4 of (4).

Lemma 4. *If $0 \neq H \subseteq K \subseteq F$, where H is characteristic in K, then $|H| > |K|$.*

Proof. $|H| = |K|$ implies there exists $k \in K_0 \cap H$. By Lemma 3 k is primitive in K and so since H is characteristic in K, $H = K$. Thus $|H| > |K|$.

Lemma 5. *A monomorphism $F \to F$ which fixes the elements of minimal length of a non-zero characteristic subgroup must be the identity.*

Proof. Take $f \in E$ free such that $fa = a$ for all $a \in K_0$, where $0 \neq K$ is in $\underline{C}$. Note $PK_0 = K_0$ where $P = \{\Sigma\, \epsilon_i t_{f(i)} s_i \mid f \text{ a bijection of } N\}$. Fix $k \in K_0$ and let $A = T(k) = \{t_{ij}\}_{j=1}^{n}$. There exists $x \in \mathrm{Aut}$ such that $x_r = t_r$ for r such that $t_r \notin T(k)$, $T(x_{ij}) \subset A$ for $1 \leq j \leq n$, and $fx = y$ where $(y_{i1}, \ldots, y_{in})$ is the Nielsen reduction of $(f_{i1}, \ldots, f_{in})$. For all $p \in P$ such that $pk \in Z(A)$ we have $yx^{-1}pk = pk$. Note also that $T(x^{-1}pk) \subseteq A$. Since $x^{-1}pk \in K$ and $(y_{ij})_{j=1}^{n}$ is Nielsen reduced $|x^{-1}pk| = |pk| = |k|$. Moreover $yx^{-1}pk = pk$, and so each y_{ij} contributes exactly its core (which must have length one) to the reduced T-form of pk. For any $\epsilon t_{ij} \in \pm A$ we may pick $pk = \epsilon t_{ij} + h \in Z(A)$ a reduced T-sum. Thus there is a permutation σ of $\{1, 2, \ldots, n\}$ such that $c(y_{i\sigma(j)}) = \pm t_{ij}$. Since $\pm y_{i\sigma(j)}$ must begin with its core, it consists only of its core, that is, $y_{i\sigma(j)} = \pm t_{ij}$. Hence $\mathrm{gp}(\{f_{ij}\}_{j=1}^{n}) = \mathrm{gp}(\{y_{i\sigma(j)}\}_{j=1}^{n}) = Z(A)$. Now since $PK_0 = K_0$, we have that for any $t \in T$ there exist $p, p' \in P$ such that $\{t\} = T(pk) \cap T(p'k)$.

$$f_t \in \mathrm{gp}(fT(pk)) \cap \mathrm{gp}(fT(p'k)) = Z(T(pk)) \cap Z(T(p'k)) = Zt.$$

Hence $f_t = mt$ for some $m \in Z$. $m \neq 0$ since f is free. But then it is easy to see that $fk = k$ for all $k \in K_0$ implies $m = 1$, $f_t = t$. Therefore $f = e$.

Lemma 6. *Let K be a proper, non-zero characteristic subgroup of F with basis B. Then $\{|b| \mid b \in B\}$ is unbounded.*

Proof. We may assume B is Nielsen reduced. Let Q be the minimal Schreier system of coset representatives corresponding to B. Suppose $|b| < N$ for all $b \in B$. Suppose $q \in Q$ is such that $|q| > N$. K characteristic implies there exists $0 \neq k \in K$ such that $T(q) \cap T(k) = \emptyset$ and so $q + k$ is a reduced sum not in Q. Since $q + k \equiv q \bmod K$ we can write $k = a + \epsilon t + c$, a reduced sum where $q + a \in Q$ and $q + a + \epsilon t \notin Q$. But then for some $q' \in Q$, $b = q + a + \epsilon t - q'$ is a T-reduced sum, $b \in \pm B$ with $|b| > N$, a contradiction. Therefore $|q| \leq N$ for all $q \in Q$. It is easy to see that

$\{\Sigma_{i=1}^n t_i\}_{n=1}^\infty$ is a basis for F. For $n > N$. $z = \Sigma_{i=1}^n t_i - q \in K$ for some $q \in Q$. $z \neq 0$ since $|q| \leq N$. z must contain exactly one occurrence of some t_i and hence is primitive in F. But then $K = F$. This contradiction completes the proof.

Theorem 4. *For $a \in BC$, $C_a : \mathrm{Aut} \to \mathrm{Aut}$ is a group monomorphism. C_a is epi if and only if $a \in \mathrm{Aut}$.*

Proof. If $x \in \mathrm{Ker}(C_a)$, $C_a(x) = e \Rightarrow xa = ae = a \Rightarrow x$ is the identity on $K = \underline{\mathrm{gp}}(a)$ and hence on K_0. Thus $x = e$ by Lemma 5. Hence C_a is a monomorphism.

Now suppose $a \in BC$ and C_a is onto. $K = \underline{\mathrm{gp}}(a)$ is characteristic and non-zero. Assume $K \neq F$ and let B be a Nielsen reduced basis for K. By Lemma 3, K_0 is contained in $\mathrm{gp}(K_0 \cap B)$. Lemma 6 implies $B - (K_0 \cap B)$ is infinite so there exists $x \in \mathrm{Aut}(K)$ such that x non trivially permutes the elements of $B - (K_0 \cap B)$. But if x were in the image of C_a, x would be the restriction to K of an element of $\mathrm{Aut}(F)$, say y. y would then fix the elements of K_0 and so be the identity by Lemma 5. Thus x is not in the image of C_a so C_a is not onto. Hence C_a onto $\Rightarrow K = F \Rightarrow a \in \mathrm{Aut}$.

For the converse, take $a \in \mathrm{Aut}$ and note that $x \in \mathrm{Aut} \Rightarrow ax = (axa^{-1})a$ so $C_a(axa^{-1}) = x$.

Corollary 2. *For $a \in BV$, Y_a is onto if and only if $a \in \mathrm{Aut}$.*

Proof. if $a \in \mathrm{Aut}$ then $x \in E \Rightarrow ax = (axa^{-1})a \Rightarrow x = Y_a(axa^{-1})$. Hence $a \in \mathrm{Aut}$ implies Y_a is onto.

Suppose Y_a is onto. By Proposition 3 (1) of Section 2, $Y_a | \mathrm{Aut} = C_a$ so by Theorem 4 it suffices to show that for $x \in E$, $Y_a(x) \in \mathrm{Aut} \Rightarrow x \in \mathrm{Aut}$. Suppose $Y_a(x) \in \mathrm{Aut}$. Let $V = \underline{\mathrm{gp}}(a)$. $Y_a(x)$ free $\Rightarrow x|_V$ is one to one $\Rightarrow \mathrm{Ker}(x) = 0$, since if not $\mathrm{Ker}(x) \cap V \supseteq V(\mathrm{Ker}(x)) \neq 0$ since $\mathrm{Ker}(x) \neq 0 \Rightarrow \mathrm{rank}(\mathrm{Ker}(x)) = \omega$. $x|_V : V \to V$ onto implies by Lemma 2, of Section 2 that $x \in \mathrm{Aut}$.

2.3. Prime Factorization in $\underline{C}$

In this section we define primes in $\underline{C}$ and BC and prove those results we have on unique prime factorization in $\underline{C}$.

Note that Aut is the group of units of the near ring E.

Definition 4. Suppose $\mathrm{Aut} \subseteq M \subseteq E$ where M is a multiplicative submonoid of E. We say that $p \in M$ is *M-prime* if $p \notin \mathrm{Aut}$ and $p = ab$, $a, b \in M \Rightarrow a$ or b is in Aut. K is *prime* in $\underline{C}$ if $K = HH' \Rightarrow H$ or H' is F.

Since $BC, BV \supseteq \mathrm{Aut}$, the above definition defines the primes of BC and BV. Since $\underline{\mathrm{gp}} : BC \to \underline{C}$ and $\underline{\mathrm{gp}} : BV \to \underline{V}$ are monoid epimorphisms, the primes of $BC(BV)$ are exactly those elements of E basic for some prime in $\underline{C}(\underline{V})$. Thus $x \in BC(BV)$ is prime if and only if $\underline{\mathrm{gp}}(x)$ is prime in $\underline{C}(\underline{V})$.

Theorem 5. (a) *Every $k \in BC$ can be written as a finite product of BC primes.*

(b) *Every $K \in \underline{C}$ can be written as a finite product of primes and any such* *factorization takes the form*: $K = \Pi_{i=1}^{n} P_i$ *where* $n < |K|$, P_i *prime in* $\underline{C}$.

Proof. First we show that if a, b are non-units of BC, $\underline{gp}(ab)$ is a proper characteristic subgroup of $\underline{gp}(a)$. Clearly $\underline{gp}(ab)$ is a subgroup of $\underline{gp}(a)$. If $\underline{gp}(ab) = \underline{gp}(a)$ then there exists $x \in \text{Aut}$ such that $abx = a \Rightarrow bx = e$ and so $b \in \text{Aut}$. Thus $\underline{gp}(ab) \subseteq \underline{gp}(a)$.

If $x \in \text{Aut}(\underline{gp}(a))$ there exists a $y \in \text{Aut}$ such that for all $i \geq 1$ $x(a_i) = (ay)_i$. Therefore $x(\underline{gp}(ab)) = \underline{gp}((\Sigma\, x(a_i)s_i)b) = \underline{gp}(ayb) = \underline{gp}(abC_b(y)) = \underline{gp}(ab)$. Thus $\underline{gp}(ab)$ is a proper characteristic subgroup of $\underline{gp}(a)$ and so by Lemma 4, $|\underline{gp}(ab)| > |\underline{gp}(a)|$.

From this we have that if $\{K_1, \ldots, K_n\}$ are proper characteristic subgroups then $|\Pi_{i=1}^{n} K_i| > n$. Thus if $K \in \underline{C}$ cannot be written as a finite product of primes it can be represented as an arbitrarily long product of proper characteristic subgroups, and so it has arbitrarily large length. This contradiction implies any $0 \neq K \neq F$ can be written as a finite product of primes of the form: $K = \Pi_{i=1}^{n} P_i$ where $n < |K|$, and P_i prime in $\underline{C}$. This proves (b).

Now if $a \in BC$ cannot be written as a finite product of primes, $\underline{gp}(a)$ can be written as an arbitrarily long product of proper characteristic subgroups. This contradiction proves (a).

Proposition 5. *Unique prime factorization holds in* $\underline{C}$ *if and only if it holds up to multiplication by units in BC.*

Proof. $p_i \ldots p_n = q_1 \ldots q_m$, p_i, q_j prime in $BC \Rightarrow \Pi_{i=1}^{n} \underline{gp}(p_i) = \Pi_{i=1}^{m} \underline{gp}(q_i) \Rightarrow n = m$, $\underline{gp}(p_i) = \underline{gp}(q_i)$ for $1 \leq i \leq n \Rightarrow n = m$, and for all i, $p_i = q_i x_i$ for some $x_i \in \text{Aut}$.

If $\Pi_{i=1}^{n} P_i = \Pi_{i=1}^{m} Q_i$ for P_i, Q_i prime in $\underline{C}$, take p_i basic for P_i, q_j basic for Q_j for all i, j. Then there exists $x \in \text{Aut}$ such that

$$p_1 \ldots p_n = q_1 \ldots q_m x.$$

By hypothesis $n = m$ and $p_i = q_i x_i$ $1 \leq i < n$, $p_n = q_n x x_n$ where $x_i \in \text{Aut}$. Hence $n = m$ and $P_i = Q_i$ for all $1 \leq i \leq n$.

We now show that a proof of unique prime factorization in $\underline{C}$ would also give a proof of unique prime factorization in $\underline{V}$. To do this we need a lemma.

Lemma 7. *If K is non-zero in* $\underline{C}$ *then for any* $m \geq 1$ *there is a basis B of K such that* $B \supseteq \{b_1, \ldots, b_m\}$ *and the* $T(b_i)$ *are pairwise disjoint.*

Proof. Let B be a Nielsen reduced basis for K. Take $k_1, \ldots, k_n \in K_0$ such that the $T(k_i)$ are pairwise disjoint. By Lemma 3, if $k_i \in \pm B$ then $k_i = \epsilon_i b_{i1} + \delta_i b_{i2}$ for $\epsilon_i, \delta_i = \pm$, and $b_{ij} \in B$. If $b_{ij} = b_{rs}$ for $r \neq i$ then $c(b_{ij})$ occurs in the reduced T-form of both k_i and k_r, a contradiction. Therefore $(B - \{b_{i1} \mid k_i \not\in \pm B\}) \cup \{k_i \mid k_i \not\in \pm B\} = B'$ is a basis of K such that $B' \cup -B' \supseteq \{\pm k_i\}_{i=1}^{m}$. This proves the lemma.

For A, a subset of F, define $P_A \in E$ by $P_A(t) = \begin{cases} 0 & \text{if } t \in A \\ t & \text{if } t \not\in A \end{cases}$.

We say a subgroup $K \subseteq F$ is *projection closed* if $P_A(K) \subseteq K$ for all $A \subseteq T$.

Proposition 6. *$K \in \underline{C}$ is projection closed if and only if $K \in \underline{V}$.*

Proof. Given $K \in \underline{C}$ is projection closed, $w(t_{ij})_{j=1}^{n} \in K$ and $\{w_j\}_{j=1}^{n} \subseteq F$. Take $R = \{r_j\}_{j=1}^{n} \subseteq T$ such that $\{r_j\}_{j=1}^{n} \cap (\cup_{j=1}^{n} T(w_j)) = \emptyset$. $\{r_j + w_j\}_{j=1}^{n}$ is primitive so since $K \in \underline{C}$, $w(r_j + w_j)_{j=1}^{n} \in K$. Since K is projection closed $P_R(w(r_j + w_j)_{j=1}^{n}) = w(w_j)_{j=1}^{n} \in K$. Therefore $K \in \underline{V}$.

Note that $K \in \underline{C}$ is projection closed if and only if $P_R(K) \subseteq K$ for some finite $R \subseteq T$. If $t \in T$, let $P_{\{t\}} = P_t$.

Theorem 6. *$K, H \in \underline{C}$, $KH \in \underline{V}$ implies $K, H \in \underline{V}$. Thus if unique prime factorization holds in $\underline{C}$ it also holds in $\underline{V}$.*

Proof. To show $H \in \underline{V}$ take $w(t_{ij})_{j=1}^{n} \in H$ and show $P_{t_{i1}}(w) \in H$. By Lemma 7, we may take b basic for K such that $T(b_{ij}) \cap T(b_{is}) = \emptyset$ for $r \neq s$. $bH = KH$ implies $bw = w(b_{ij}) \in KH$. Since $KH \in \underline{V}$, $P_{T(b_{i1})}(w(b_{ij})) = bP_{t_{i1}}(w)$, which is in KH. Therefore $bP_{t_{i1}}(w) = bh$ for some $h \in H$. b free implies $P_{t_{i1}}(w) = h \in H$. Thus $H \in \underline{V}$.

Now EK is the verbal subgroup generated by K. To show this we need only show EK is a group. Clearly $-(EK) \subseteq EK$. If $f, g \in E$ and $x, y \in K$, then $K \in \underline{C}$ implies there exists an $f' \in E, x' \in K$ such that $fx = f'x'$ and $T(x') \cap T(y) = \emptyset$. Then clearly there exists a $q \in E$ such that $q(x' + y) = qx' + qy = f'x' + gy = fx + gy$. Thus $EK \in \underline{V}$.

Let $EK = \bar{K} \in \underline{V}$ and let $\bar{k}$, k, h be basic for $\bar{K}$, K, H respectively.

$$E \cdot k \cdot E = E \cdot (K^{\omega}) = \bar{K}^{\omega} = \bar{k} \cdot E$$

The middle equality comes from the fact that $EK = \bar{K}$ and for any $x \in \bar{K}^{\omega}$, $x = f(\Sigma\, k_i s_i)$ where $k_i \in K$ and the $T(k_i)$ are pairwise disjoint. Hence

$$\bar{K}H = \underline{\mathrm{gp}}(\bar{k}hE) = \underline{\mathrm{gp}}(\bar{k}EhE) = \underline{\mathrm{gp}}(EkEhE) = \underline{\mathrm{gp}}(EkhE) = \underline{\mathrm{gp}}(khE) = KH.$$

Therefore $\bar{K}H = KH$ and $\bar{K} \supseteq K$. By Theorem 3, $\bar{K} = K$ so $K \in \underline{V}$. This proves our first statement.

Now from the above it is easy to see that P prime in $\underline{V}$ implies P prime in $\underline{C}$. Thus if unique prime factorization holds in $\underline{C}$ it also holds in $\underline{V}$.

In the remainder of this section we introduce a notion due to Frohlich (see (1)). This, it happens, is important in proving unique prime factorization in $\underline{V}$ and might well prove important in constructing a proof of unique prime factorization in $\underline{C}$.

Definition 5. For $K, K' \in \underline{C}$, define $K\backslash K' = \sup\{H \in \underline{C} \mid KH \subseteq K'\}$.

Clearly $K\backslash K' \in \underline{C}$. Let k be basic for K. For $H \in \underline{C}$, $KH = kH$. If $x \in K\backslash K'$, $x = \Sigma_{i=1}^{n} h_i$ where $h_i \in H_i$, and $KH_i \subseteq K'$. Thus $kx = \Sigma_{i=1}^{n} kh_i \in K'$, and so

$$K(K\backslash K') \subseteq K'.$$

$K\backslash K'$ is therefore the unique maximal characteristic subgroup H such that $KH \subseteq K'$.

If we replace $\underline{C}$ by $\underline{V}$ in the above definition we get a slicing operation on $\underline{V}$. (This is actually the restriction to $\underline{V}$ of the slicing operation on $\underline{V}$ though there is not space here to prove this. For a proof, see (9), Chapter V, Section 3.) The essential step in proving unique prime factorization in $\underline{V}$ is Lemma 23.21 of *Varieties of Groups*, which in our notation becomes:

$$V, V' \in \underline{V} \text{ and } U \not\subseteq V \Rightarrow U\backslash(VV') = (U\backslash V)V'.$$

It happens that the same lemma extended to $\underline{C}$ will yield unique prime factorization in $\underline{C}$.

Theorem 6. *Suppose that if $H, K, K' \in \underline{C}$ and $H \not\subseteq K$ then $H\backslash(KK') = (H\backslash K)K'$. Then unique prime factorization holds in $\underline{C}$.*

Proof. First we show that under our hypotheses, $K, K', H \in \underline{C}$ implies that $KH = K'H \Rightarrow K = K'$. Assume $KH = K'H$ and $K \not\subseteq K'$. Since $H \subseteq K\backslash(K'H)$, $K(K\backslash(K'H)) = KH = K'H$. By hypothesis, since $K \not\subseteq K'$, $K(K\backslash(K'H)) = K(K\backslash K')H = KH$. By the easy cancellation law, $(K\backslash K')H = H = FH$. Hence by Theorem 3, $K\backslash K' = F$. But $K(K\backslash K') \subseteq K'$ implies $K \subseteq K'$, a contradiction. Thus if $KH = K'H$, we must assume $K \subseteq K'$ or $K' \subseteq K$. By Theorem 3 again, $K = K'$, and we have our right cancellation law.

Now suppose $PH = QK$, where $P, Q, H, K \in \underline{C}$, P, Q primes. Suppose $P \not\subseteq Q$. Then $P\backslash(QK) = (P\backslash Q)K$. $H \subseteq P\backslash(QK) \Rightarrow P(P\backslash(QK)) = P(P\backslash Q)K = QK$ so by the right cancellation law, $P(P\backslash Q) = Q$. P, Q are prime implies $P\backslash Q = F$ so $P \subseteq Q$, a contradiction. Hence $P \subseteq Q$, and by symmetry, $P \supseteq Q$. Hence $P = Q$, proving the theorem.

2.4. Cancellation in *BC*

Although we do not have a proof that both cancellation laws hold in $\underline{C}$, as an indication that this is true we can prove that both cancellation laws hold in BC. This result reduces the problem of proving the right cancellation law in $\underline{C}$ to the problem of showing that if $a, a', b \in BC$ and $ab = a'bx$ for some $x \in \text{Aut}$, then $x = C_b(y)$ for some $y \in \text{Aut}$.

Definition 6. $x \in F$ is *indecomposable* if and only if $x = ny$, $n \geqslant 1 \Rightarrow n = 1$.

The following results are well known:

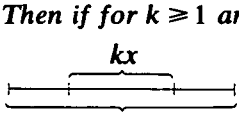
1. For any $z \in F$, there exists a unique indecomposable $x \in F$ such that $z = nx$ for some $n \geqslant 1$. We denote this x by $I(z)$.

2. Any indecomposable $x = g + y - g$, where this is a reduced sum for some $g \in F$ and some cyclically reduced indecomposable, y.

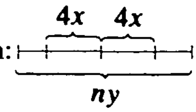
3. If y is a cyclically reduced indecomposable then all y's cyclic permutations are distinct.

4. If x, y are indecomposable and $x \neq \pm y$, then $\{x, y\}$ is free. *Proof*: For clearly $\text{gp}(\{x, y\})$ is non-cyclic. Since free groups of finite rank are Hopfian, $\{x, y\}$ is a basis for $\text{gp}(\{x, y\})$.

Lemma 8. *Suppose $x, y \in F$ are cyclically reduced indecomposables and $|x| \geqslant |y|$. Then if for $k \geqslant 1$ arbitrarily large we have a diagram of the form:*

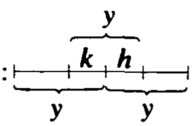


, where x is a cyclic permutation of y, $n \geqslant 1$.

Proof. Take a $k \geqslant 8$. We have a diagram of form: 

where $n \geqslant 1$.

Therefore $4x = a + k_1y + b = c + k_2y + d$ where both sums are reduced; $k_1, k_2 \geqslant 2$; b, d are proper initial segments of y; a, c are proper terminal segments of y, and $y = b + c$, a reduced sum.

If $a \neq c$ then it is easy to see we have a diagram: 

, where $k, h \neq 0$.

Therefore $y = k + h = h + k$, so y is a proper cyclic permutation of itself and hence not indecomposable, a contradiction. Thus $a = c$ so $b = d$, $k_1 = k_2$ and $4x = (k_1 + 1)(a + b)$. $a + b$ is a cyclic permutation of y and hence indecomposable. Thus $4 = k_1 + 1$, $a + b = x$.

Lemma 9. *Suppose u, w are non-zero in F and $I(u) \neq \pm I(w)$. Let $w = g + w' - g$, a reduced sum where w' is cyclically reduced. Then for any $\epsilon, \delta = \pm$ there is an $N \geqslant 1$ such that for $k, k' \geqslant N$ the reduced T-form of $k(\epsilon w) + u + k'(\delta w)$ has $g + \epsilon w'$ for an initial segment and $\delta w' - g$ for a terminal segment.*

Proof. For $N \geqslant 1$ let $x_N = N\epsilon w + u + N\delta w$. By Remark 4, $\{w, u\}$ is free so (1) $\{|x_N| \mid N \geqslant 1\}$ is unbounded. Suppose x_N never has both $g + \epsilon w'$ for an initial segment and $\delta w' - g$ for a terminal segment. Then we always have $|x_N| \leqslant 4|g| + |u| + 2N|w'| - 2(N-1)|w'| = 4|g| + |u| + 2|w'|$, contradicting (1). This proves the lemma.

Along the same lines as Lemma 9 we have:

Remark 5. Let u, w, ϵ, δ be as in Lemma 9. Then there exists an $N \geqslant 1$ such that for $M \geqslant N$, $M\epsilon w + u$ has initial segment $g + \epsilon w'$ and $u + M\delta w$ has terminal segment $\delta w' - g$.

Theorem 7. *Suppose $a, a' \in E$ are free and $b \in BC$. Then if $ab = a'b$, we have $a = a'$.*

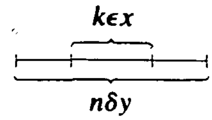
Proof. $ab = a'b$ implies $aw = aw'$ for all $w \in \underline{\text{gp}}(b) = B \in \underline{C}$. Pick $w \in B$ such that $t_i \notin T(w)$ and $w = t_j + w'$, a T-reduced sum for some $t_j \in T$. For $k \geqslant 1$, define $x_k \in \text{Aut}$ such that $x_k(t) = \begin{cases} t \text{ if } t \neq t_j \\ kt_i + t_j \text{ if } t = t_j \end{cases}$.

Let $w_k = x_k w$. Then for $k \geqslant 1$ $w_k = \Sigma_{r=1}^{H} (k(\epsilon_r t_i) + v_r)$ is a T-reduced sum where $\epsilon_1 = +$, $0 \neq v_r \in \text{gp}(T(w))$ for $1 \leqslant r < H$, and H is the number of occurrences of $\pm t_j$ in w. $v_H \in \text{gp}(T(w))$ may be 0.

We claim that: $u \in \text{gp}(aT(w))$ implies $I(u) \neq \pm I(a_i)$ and $u \in \text{gp}(a'T(w))$ implies $I(u) \neq \pm I(a_i')$.

To prove the first implication assume $I(u) = \pm I(a_i)$. Then $na_i \in \text{gp}(aT(w))$ for some $n \geqslant 1$, contradicting the freeness of $\{a_i\} \cup aT(w)$. The second statement of our claim is proved similarly.

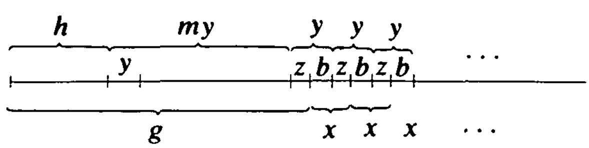
Now $a_i = g + Mx - g$ and $a'_i = h + M'y - h$, where these are both reduced sums, $M, M' \geqslant 1$, and x, y are cyclically reduced indecomposables. By our claim, for all $1 \leqslant r \leqslant H$, $I(av_r) \neq \pm I(a_i)$ and $I(a'v_r) \neq \pm I(a_i)$.

By repeatedly using Lemma 9 and Remark 5 on both sides of the equation $aw_k = a'w_k$ we have if $|x| \geqslant |y|$, a diagram of form 

exists for arbitrarily large k. If $|x| \leqslant |y|$ we get the same situation with x and y interchanged. Therefore Lemma 8 applies showing that x is a cyclic permutation of $\pm y$. Hence $|x| = |y|$.

For k sufficiently large, $kM|x| + c = |aw_k| = |a'w_k| = kM'|y| + d$, where c and d are constants not depending on k. Using the fact that $|x| = |y|$, and letting k go to infinity, we get $M = M'$.

Now suppose $|g| \neq |h|$. Then $|g| < |h|$ or $|g| > |h|$. Suppose $|g| > |h|$. Since w_k begins with kt_i, for k sufficiently large, we get from the equation, $aw_k = a'w_k$, a diagram of the form



where $m \geqslant 0$ and z may be zero.

If $z \neq 0$, $y = z + b$, $x = b + z$, reduced sums and $g + x - g$ is a reduced sum. Thus $(h + my + z) + (b + z) + (-z - my - h)$ is a reduced sum, which it isn't. Hence $z = 0$ and $x = y$. But this means that since $g + x - g$ is a reduced sum we must have $m = 0$ and $h = g$. Therefore

$$a_i = g + Mx - g = h + M'y - h = a'_i.$$

Since t_i was arbitrary, $a = a'$.

Corollary 3. *Both cancellation laws hold in BC.*

REFERENCES

(1) A. FROHLICH, Distributively generated near rings (I): Ideal Theory, *Proc. London Math. Soc.* (3) **8** (1958), 74–94.

(2) A. FROHLICH, Distributively generated near rings (II): Representation Theory, *Proc. London Math. Soc.* (3) **8** (1958), 95–108.

(3) R. C. LYNDON and P. E. SCHUPP, *Combinatorial Group Theory* (Springer-Verlag, 1977).

(4) W. MAGNUS, A. KARRASS and D. SOLITAR, *Combinatorial Group Theory* (Interscience tracts in Pure and Applied Mathematics, Vol. XIII, Interscience Publishers, N.Y., 1966).

(5) H. NEUMANN, On varieties of groups and their associated near rings, *Math. Z.* **65** (1956), 36–69.

(6) H. NEUMANN, *Varieties of Groups* (Springer-Verlag, 1967).

(7) B. H. NEUMANN, H. NEUMANN and P. M. NEUMANN, Wreath products and varieties of groups, *Math. Z.* **80** (1962), 44–62.

(8) V. THARMARATNAM, Endomorphism near rings of relatively free groups, *Math. Z.* **113**.

(9) R. W. ZEAMER, *On Near Rings Associated with Free Groups*, (Ph.D. thesis, McGill University, Montreal, Canada, 1977).

QUEEN MARY COLLEGE