2
Test Elements

This chapter is about *test elements* of various groups. The idea here is to distinguish, for example, automorphisms among arbitrary endomorphisms by means of their action on a single element, a test element. More precisely:

Definition 2.0.1 ([352]). An element $g \in G$ is called a test element (for recognizing automorphisms) of a group G if, whenever $\varphi(g) = g$ for an endomorphism φ of G, it follows that φ is an automorphism.

The condition "$\varphi(g) = g$" in this definition can be obviously replaced by "$\varphi(g) = \alpha(g)$ for some $\alpha \in \mathrm{Aut}(G)$". Thus, the definition can be informally rephrased as "if an endomorphism φ acts like an automorphism on one particular element g, then φ is itself an automorphism".

In this chapter, we are going to describe test elements in various groups, but the focus is on free groups. The first result of this particular type was that of Nielsen [293], who proved that if an endomorphism of the free group of rank 2 fixes the commutator of a pair of generators, then it is an automorphism. Similar results for other particular elements of a free group were later obtained by Zieschang [417, 418], Rosenberger [318], Dold [100], Rips [314], Durnev [115], and others. Shpilrain [352, 355] generalized most of these results and put them in perspective. Turner [383] characterized test elements of a free group as elements that do not belong to any proper retract. Based on this characterization, Comerford [82] suggested an algorithm for recognizing test elements of a free group.

The idea behind the definition of a test element has numerous ramifications; for example, one can consider properties (other than being an automorphism) of an endomorphism that can be recovered from its action

on a single element. Also, one can consider *test sets* rather than just test elements.

The situation in arbitrary groups is more complex. Turner and his students have several results on test elements in hyperbolic groups [289], direct products of groups [290], and free products of finite cyclic groups [396]. We concentrate here, in Section 2.1, on two-generator groups, where there were numerous attempts to expand Nielsen's "commutator test" to one-relator groups by Hill and Pride [151], to free metabelian groups by Durnev [115], and to free solvable and other groups by Gupta and Shpilrain [147].

There is also a nice application of test elements to solving equations in free groups pointed out by Durnev in [116].

In Section 2.3 of this chapter, we describe another result related to the idea of test elements. D. Lee [204], based on ideas of S. Ivanov [153], confirmed the following conjecture of Shpilrain [42, Problem (F7)]: every endomorphism of a free group of finite rank is completely determined by its values on just two (explicitly given) elements unless the image of this endomorphism is cyclic. We therefore have a test set of two elements that allows one to distinguish any two endomorphisms of a free group that have noncyclic images.

2.1 Nielsen's Commutator Test

Nielsen [293] gave the following commutator test for an endomorphism of the free group $F = F_2 = \langle x, y\rangle$ to be an automorphism: an endomorphism $\varphi\colon F \to F$ is an automorphism if and only if the commutator $[\varphi(x), \varphi(y)]$ is conjugate in F to $[x, y]^{\pm 1}$. He obtained this test as a corollary to his well-known result that every IA-automorphism of F (i.e., one that fixes F modulo its commutator subgroup) is an inner automorphism. Bachmuth et al. [29] have proved that IA-automorphisms of most two-generator groups of the type F/R' are inner, and it becomes natural to ask if Nielsen's commutator test remains valid for those groups as well. Durnev [115] considered this question for the free metabelian group F/F'' and confirmed the validity of the commutator test in this case. Here we will show that Nielsen's test does *not* hold for a large class of F/R' groups and, as a corollary, deduce that it does not hold for any nonmetabelian solvable group of the form F/R''. On the other hand, we give a sufficient condition under which Nielsen's commutator test is valid for a given pair of generating elements of F modulo $[R', F]$.

The negative result for F/R' groups yields the following natural question (see [43, Problem (S9)]): Does the free solvable group of rank 2 and derived length $d > 2$ have any test elements? Roman'kov [317] has constructed test elements in the free solvable group of rank 2 and derived length 3. It is plausible that the same method can be used for constructing test elements

in the free solvable group of any bigger rank as well, but technically it is getting more complicated.

We also mention a related result of Timoshenko [382], who proved that a free metabelian group of rank > 2 does *not* have any test elements.

Now we get to the main results of this section.

Theorem 2.1.1 ([147]). *Let $R \leq F'$ be a nontrivial normal subgroup of F such that*

(i) *the center of $F/[R,F]$ is $R/[R,F]$ and*

(ii) *the group ring $\mathbb{Z}(F/R)$ is an Ore domain (i.e., $\mathbb{Z}(F/R)$ has no zero divisors and any two nonzero elements have a common nonzero multiple).*

Then there exist $u, v \in F$ such that $[u,v] \equiv [x,y] \pmod{R'}$, while the endomorphism $x \to u,\ y \to v$ of F does not induce an automorphism of F/R'.

We need one preliminary lemma.

Lemma 2.1.2. *The mapping $\tau\colon x \to xr,\ y \to ys$ with $r, s \in F'$ defines an automorphism of F if and only if $r = [x,f]$ and $s = [y,f]$ for some $f \in F$. Similarly, the mapping $\tau'\colon x \to rx,\ y \to sy$ with $r, s \in F'$ defines an automorphism of F if and only if $r = [f, x^{-1}]$ and $s = [f, y^{-1}]$ for some $f \in F$.*

Proof. Consider an automorphism τ of F of the form

$$\tau\colon x \to xr,\ y \to ys \quad \text{where} \quad r, s \in F'.$$

Then τ is an IA-automorphism and hence, by Nielsen's characterization, τ must be an inner automorphism $x \to x^f,\ y \to y^f$, induced by some $f \in F$. Comparing the two formulations of τ yields the result. ■

Proof of Theorem 2.1.1. Choose some $r \in R$, $r \notin R'$. Let $u \equiv r^a x \pmod{R'}$ and $v \equiv r^b y \pmod{R'}$ for some $a, b \in \mathbb{Z}F$ (to be specified later). Then, modulo R', we have

$$\begin{aligned}[r^a x, r^b, y] &\equiv [r^a x, y][r^a x, r^b]^y \equiv [r^a, y]^x [x,y][x, r^b]^y \\ &\equiv [x,y][r^a, y]^{x[x,y]}[x, r^b]^y \equiv [x,y][r^a, y]^{y^{-1}xy}[x, r^b]^y \\ &\equiv [x,y][y^{-1}, r^a]^{xy}[r^b, x^{-1}]^{xy} \equiv [x,y] r^{(a(1-y^{-1})+b(x^{-1}-1))xy}.\end{aligned}$$

Thus, the congruence $[r^a x, r^b y] \equiv [x,y] \pmod{R'}$ is equivalent to the congruence

$$r^{(a(1-y^{-1})+b(x^{-1}-1))} \equiv 1 \pmod{R'}.$$

Since $\mathbb{Z}(F/R)$ has no zero divisors, it follows by Lemma 1.4.4 that

$$a(y^{-1}-1) \equiv b(x^{-1}-1) \ \text{ modulo } \ \Delta_R, \tag{2.1}$$

where $a, b \in \Delta_F$ (since $R \leq F'$ implies that Δ_R lies in Δ_F^2). By condition (ii) of our theorem, there exist $a, b \notin \Delta_R$ satisfying the congruence (2.1). We choose one such pair of elements a and b satisfying (2.1) and consider elements u and v of F such that

$$u \equiv r^a x \quad \text{and} \quad v \equiv r^b y \pmod{R'}.$$

For this choice of u and v, it is easy to see that the congruence $[u, v] \equiv [x, y] \pmod{R'}$ holds. Suppose that the mapping $x \to u$, $y \to v$ induces an automorphism of the group F/R'. Then, this being an IA-automorphism of F/R', it must be inner by a result of Bachmuth et al. [29]. In that case, as in Lemma 2.1.2, we would have, for some $f \in F$,

$$r^a \equiv [f, x^{-1}] \pmod{R'} \quad \text{and} \quad r^b \equiv [f, y^{-1}] \pmod{R'}. \tag{2.2}$$

Since r^a, r^b are in $[R, F]$ ($a, b \in \Delta_F$), it follows that $f[R, F]$ is in the center of $F/[R, F]$, which by hypothesis is $R/[R, F]$. Thus $f \in R \setminus R'$. Now, (2.2) yields, by commuting appropriately with y^{-1} and x^{-1}, the congruences

$$r^{a(y^{-1}-1)} \equiv [f, x^{-1}, y^{-1}] \quad \text{and} \quad r^{b(x^{-1}-1)} \equiv [f, y^{-1}, x^{-1}] \pmod{R'},$$

which upon using (2.1) yield the congruence

$$[f, x^{-1}, y^{-1}] \equiv [f, y^{-1}, x^{-1}] \pmod{R'},$$

or, equivalently, $[f, x^{-1}y^{-1}] \equiv [f, y^{-1}x^{-1}] \pmod{R'}$, since $f \in R$. Now, an application of this last congruence in the expansion of the equation $[f, x^{-1}y^{-1}] = [f, [x, y]y^{-1}x^{-1}]$ modulo R' gives $[f, [x, y]] \in R'$, which implies (using Lemma 1.4.4) that $[y, x] \in R$, implying that F/R is abelian, contrary to the choice of R. This completes the proof of the theorem. ■

The following corollary to Theorem 2.1.1 contrasts sharply with the cited result of Durnev [115].

Corollary 2.1.3. *Let N be a proper normal subgroup of F such that F/N is solvable. Then there are elements u, v in F such that $[u, v] \equiv [x, y] \pmod{N''}$ but the endomorphism $x \to u$, $y \to v$ of F does not induce an automorphism of F/N''.*

Proof. Since F/N' is a torsion-free solvable group (see [146, p. 23], it follows by a theorem of Kropholler et al. [187] that the group ring $\mathbb{Z}(F/N')$ has no zero divisors. Thus, with $R = N'$, F/R is solvable and $\mathbb{Z}(F/R)$ has no zero divisors. It follows by a result of Lewin [214] that $\mathbb{Z}(F/R)$ is an Ore domain. Since the center of $F/[R, F]$ ($= F/[N', F]$) is always $R/[R, F]$ (see [146, p. 117]), the hypothesis of Theorem 2.1.1 is satisfied by R and the corollary follows. ■

Corollary 2.1.4.

(a) *For each $k \geq 3$, there exists an endomorphism $\varphi_k \colon F \to F$ that does not induce an automorphism of the free solvable group $F/F^{(k)}$*

of derived length k, whereas (by Corollary 2.1.3) $[\varphi_k(x), \varphi_k(y)] \equiv [x, y] \bmod F^{(k)}$;

(b) *For each $c \geq 3$, there exists an endomorphism $\psi_c \colon F \to F$ that does not induce an automorphism of $F/[\gamma_c(F), \gamma_c(F)]$, whereas $[\psi_c(x), \psi_c(y)] \equiv [x, y] \bmod [\gamma_c(F), \gamma_c(F)]$ (by Theorem 2.1.1).*

While Nielsen's commutator test does not hold for most F/R' groups of rank 2, the groups of the form $F/[R', F]$ behave altogether differently. Here we prove the following result.

Theorem 2.1.5 ([147]). *Let R be a nontrivial normal subgroup of the free group $F = \langle x, y; \varnothing \rangle$. If $[u, v] \equiv [x, y]^{\pm g} \bmod [R', F]$ for some $g \in F$, then u and v generate F modulo $[R', F]$.*

Proof. We may clearly assume that $[u, v] \equiv [x, y] \bmod [R', F]$. Since $[R', F] - 1 \leq \Delta_F \Delta_R \Delta_F$ (see, for instance, [146, p. 113]), we have

$$[u, v] \equiv [x, y] \pmod{\Delta_F \Delta_R \Delta_F}. \tag{2.3}$$

Taking right Fox derivatives of both sides of (2.3) yields

$$\begin{aligned} \partial' u/\partial' x(v - [u, v]) + \partial' v/\partial' x(1 - v^{-1}uv) &\equiv (y - [x, y]) \bmod \Delta_R \Delta_F, \\ \partial' u/\partial' y(v - [u, v]) + \partial' v/\partial' y(1 - v^{-1}uv) &\equiv (1 - y^{-1}xy) \bmod \Delta_R \Delta_F. \end{aligned} \tag{2.4}$$

Now, taking the left Fox derivatives of both sides of the congruences in (2.4) yields four congruences modulo Δ_R given by the following matrix equation:

$$\begin{pmatrix} \partial' u/\partial' x & \partial' v/\partial' x \\ \partial' u/\partial' y & \partial' v/\partial' y \end{pmatrix} \begin{pmatrix} \partial(v - [u, v])/\partial x & \partial(v - [u, v])/\partial y \\ \partial(1 - v^{-1}uv)/\partial x & \partial(1 - v^{-1}uv)/\partial y \end{pmatrix} = \begin{pmatrix} x^{-1}y^{-1}(y - 1) & 1 - x^{-1}y^{-1}(x - 1) \\ -y^{-1} & y^{-1} - y^{-1}x \end{pmatrix}.$$

It is easily verified that the matrix on the right-hand side above is invertible over $\mathbb{Z}F$ and hence also over $\mathbb{Z}F \pmod{\Delta_R}$. Hence the Jacobian matrix on the left-hand side is also invertible over $\mathbb{Z}F \pmod{\Delta_R}$, which, by a result of Krasnikov [186] (see [146, p. 29]), implies that u and v generate F modulo R'. It follows that u and v also generate F modulo any normal subgroup V of R such that R/V is nilpotent. Thus u and v generate F modulo $[R', F]$, as was to be proved. ■

Although the elements u and v generate the group $F/[R', F]$ under the conditions of Theorem 2.1.5, we cannot, in general, conclude that the mapping induced by $x \to u$, $y \to v$ defines an automorphism of the group $F/[R', F]$ since, for instance, $F/[R', F]$ may be non-Hopfian. Since $[R', F]$ might not be fully invariant in F, this mapping may not even define an endomorphism of $F/[R', F]$. As a (partial) converse of Theorem 2.1.5, we can prove the following result.

Proposition 2.1.6. *Let R be a normal subgroup of the free group F such that $R \leq F'$ and the group ring $\mathbb{Z}(F/R)$ has no zero divisors. If the mapping $\tau\colon x \to u,\ y \to v$ induces an automorphism of the group $F/[R', F]$, then $[u, v] \equiv [x, y]^{\pm g} \bmod [R', F]$ for some $g \in F$.*

Proof. Let τ induce some automorphism ψ of the group F/R'. Then ψ is tame (Bachmuth et al. [29]) and hence a composition of inner automorphisms of F/R' together with the automorphisms of F/R' induced by the maps $x \to y,\ y \to x$ and $x \to xy,\ y \to y$. It suffices, therefore, to verify that the congruence $[\tau(x), \tau(y)] \equiv [x, y]^{\pm g} \bmod [R', F]$ holds for some g in F when τ is assumed to be an inner automorphism of $F/[R', F]$ or else defined by the maps $x \to y,\ y \to x$ and $x \to xy,\ y \to y$. These verifications are straightforward, and we omit the details. ■

2.2 Recognizing Test Elements

In this section, we give a remarkable characterization, due to Turner [383], of test elements in a free group of finite rank along with some other interesting auxiliary results. Then, based on Turner's characterization, we describe an algorithm, due to Comerford [82], for recognizing test elements.

We denote by $F_r = F(x_1, \ldots, x_r)$ the free group of rank $r \geq 2$ with basis $\{x_1, \ldots, x_r\}$ and by F a free group of unspecified rank.

Definition 2.2.1 ([352]). The *rank* of $w \in F$ is the smallest rank of a free factor of F containing w.

It is clear that if w is a test word, then w has maximal rank. The following example shows that the converse is not true in general.

Example 2.2.2. Let $\varphi\colon F_2 \to F_2$ be defined by

$$\varphi(x_1) = x_1^2 x_2 x_1^{-1} x_2^{-1}, \quad \varphi(x_2) = 1.$$

Then φ fixes $x_1^2 x_2 x_1^{-1} x_2^{-1}$, but $x_1^2 x_2 x_1^{-1} x_2^{-1}$ lies in no proper free factor (see, for example, [71, p. 139]).

What distinguishes $x_1^2 x_2 x_1^{-1} x_2^{-1}$ from, say, $x_1 x_2 x_1^{-1} x_2^{-1}$ is that the former lies in a proper retract (namely, the image of φ) while the latter does not. We recall the definition of a retract:

Definition 2.2.3. A *retract* R of a group G is a subgroup with the property that the identity map $i\colon R \to R$ extends to a homomorphism $\rho\colon G \to R$. Equivalently, a *retraction* $\rho\colon G \to G$ is a homomorphism such that $\rho^2 = \rho$ and a retract is the image of a retraction.

Free factors are retracts, but not all retracts of free groups are free factors. The next definition is important for what follows.

Definition 2.2.4 ([152]). If $\varphi\colon F \to F$ is an endomorphism of the free group F, then the *stable image* of φ is

$$\varphi^\infty(F) = \bigcap_{i=0}^{\infty} \varphi^i(F), \quad \text{and} \quad \varphi_\infty = \varphi \mid \varphi^\infty(F).$$

It is shown in [152] that φ_∞ is an automorphism and clearly $\varphi^\infty(F)$ contains $\mathrm{Fix}(\varphi)$, the set of words fixed by φ.

Theorem 2.2.5 ([383]). *If $\varphi\colon F \to F$ is an endomorphism of the finitely generated free group F, then $\varphi^\infty(F)$ is a retract of F; $\varphi^\infty(F)$ is a proper retract precisely when φ fails to be an automorphism. If φ is a monomorphism, then $\varphi^\infty(F)$ is a free factor.*

Proof. It follows from [231, Problem 33, p. 118] (see also [152]) that $\varphi^\infty(F)$ is a free factor of $\varphi^n(F)$ for almost all n. Choose a particular such n, let $\hat{F}$ be a complementary free factor, and consider

$$\varphi^n\colon F \to \varphi^n(F) = \varphi^\infty(F) * \hat{F}.$$

If φ is a monomorphism, then $\varphi^n\colon F \to \varphi^n(F)$ is an isomorphism, so letting $F' = (\varphi^n)^{-1}(\hat{F})$,

$$F = (\varphi^n)^{-1}(\varphi^\infty(F)) * (\varphi^n)^{-1}(\hat{F}) = \varphi^\infty(F) * F'.$$

More generally, let $\pi\colon \varphi^n(F) \to \varphi^\infty(F)$ be a projection on the first factor of the decomposition above. If ρ is the composition $\rho = (\varphi_\infty^{-1})^n \circ \pi \circ \varphi^n$,

$$F \xrightarrow{\varphi^n} \varphi^n(F) \xrightarrow{\pi} \varphi^\infty(F) \xrightarrow{(\varphi_\infty^{-1})^n} \varphi^\infty(F),$$

then ρ is a retraction. ■

Corollary 2.2.6. *The test words in F are the words not contained in proper retracts. The test words for monomorphisms in F_r are the words of rank r.*

Proof. We show that w is not a test word if and only if w is contained in a proper retract. It is clear that if w lies in a proper retract, then it is not a test word since it is fixed by the retraction that is not an automorphism. Conversely, suppose that $w \in F$ is not a test word and that φ is an endomorphism fixing w that is not an automorphism. Then, by Theorem 2.2.5, $\varphi^\infty(F)$ is a proper retract containing w.

If w is not a test word for monomorphisms and is fixed by the monomorphism μ that is not an automorphism, then $w \in \mu^\infty(F)$, which is a proper free factor; thus w has nonmaximal rank. ■

Example 2.2.7. The following are test elements in a free group F_n: $x_1^k \cdot \dots \cdot x_n^k$, $k \geq 2$, $[x_1, \dots, x_n]$, $[x_1, x_2] \dots [x_{2m-1}, x_{2m}]$ if $n = 2m$.

In a special case $n = 2$, test elements can be described more explicitly. Let $\sigma_{x_i}(u)$ be the sum of the exponents to which x_i occurs in the word u.

Corollary 2.2.8. *A word $u \in F_2$, which is not a proper power, is a test word if and only if* $\mathrm{g.c.d.}(\sigma_{x_1}(u), \sigma_{x_2}(u)) > 1$. *In particular, every* $u \in [F_2, F_2]$ *is a test word.*

Proof. Suppose first that $\mathrm{g.c.d.}(\sigma_{x_1}(u), \sigma_{x_2}(u)) = 1$. Then, upon taking x_1 and x_2 to appropriate powers of x_1, we can take u to x_1 by an endomorphism. Then apply another endomorphism, taking x_1 to u and x_2 to 1. The composition of these two endomorphisms is a retraction that takes F_2 onto the subgroup generated by u. Thus, u belongs to a proper retract of F_2 and therefore is not a test word by Corollary 2.2.6.

If $\mathrm{g.c.d.}(\sigma_{x_1}(u), \sigma_{x_2}(u)) > 1$, then any automorphic image of u has the same property. Suppose, by way of contradiction, that u belongs to a proper retract of F_2. Since every proper retract of F_2 is cyclic and u is not a proper power, u must be a generator of a proper retract. Then, by [231, p. 140], upon applying an automorphism to u, we can take it to an element of the form $x_1 \cdot c$, where c belongs to the normal closure of x_2. In an element v of this form, one has $\sigma_{x_1}(v) = 1$, hence $\mathrm{g.c.d.}(\sigma_{x_1}(v), \sigma_{x_2}(v)) = 1$, a contradiction. Thus, u does not belong to any proper retract of F_2 and therefore is a test word by Corollary 2.2.6. ■

For free groups of higher rank, the situation is more complex, and an algorithm for recognizing test elements is more sophisticated. Before we describe this algorithm (due to Comerford [82]), we give an example (due to D. Voce) showing that Turner's characterization of test elements may not hold in nonfree groups. More precisely, test elements can never lie in proper retracts, but there might be elements that do not lie in any proper retract and yet are not test elements.

Example 2.2.9. In the group K presented by $\langle a, b \mid aba^{-1} = b^{-1} \rangle$, b lies in no proper retract, but the endomorphism φ defined by

$$\varphi(a) = a^3 b, \quad \varphi(b) = b$$

is not surjective. Furthermore, $\varphi^\infty(K) = \langle b \rangle$, showing that Theorem 2.2.5 does not generalize to K.

Now we get to Comerford's algorithm for recognizing test elements in a free group. Here we shall use the following terminology and notation. We let G and H be free groups freely generated by sets A and B, respectively; when we speak of lengths of elements of H and G, it will be with respect to these generating sets. If $\alpha\colon H \to G$ is a homomorphism, we say that $w \in G$ is a *Nielsen-reduced image* of $u \in H$ under α if $\alpha(u) = w$, $u = s_1 \dots s_k$ with $s_1, \dots, s_k \in B \cup B^{-1}$, $s_{i+1} \neq s_i^{-1}$ for $1 \leq i \leq k-1$ and, as reduced words on $A \cup A^{-1}$, $\alpha(s_1), \dots, \alpha(s_k)$ satisfy

$$\begin{aligned}
&\alpha(s_i) \neq 1 && \text{for } 1 \leq i \leq k, \\
&|\alpha(s_i s_{i+1})| \geq |\alpha(s_i)|, |\alpha(s_{i+1})| && \text{for } 1 \leq i \leq k-1, \quad \text{and} \\
&|\alpha(s_i s_{i+1} s_{i+2})| > |\alpha(s_i)| - |\alpha(s_{i+1})| + |\alpha(s_{i+2})| && \text{for } 1 \leq i \leq k-2.
\end{aligned}$$

In other words, no letter of u has an empty image under α, not more than half the image of a letter of u cancels with the image of an adjacent letter of u, and no interior letter of u has its image cancelled entirely by the images of the two adjacent letters.

Given a homomorphism $\alpha\colon H \to G$ with $\alpha(u) = w$, we want to produce an endomorphism τ of H and a homomorphism $\beta\colon H \to G$ such that w is a Nielsen-reduced image of $\tau(u)$ under β. We use a Nielsen reduction technique similar to that employed by Lyndon in [225]. Following Lyndon, we call an automorphism of H defined by $s \mapsto st^{-1}$ with $s, t \in B \cup B^{-1}$ and $t \neq s^{\pm 1}$ and $f\colon b \mapsto b$ for $b \in B$, $b \neq s^{\pm 1}$, an *elementary regular transformation*. This transformation is *attached* to a reduced $u \in H$ if st or $t^{-1}s^{-1}$ is a subword of u. We also include the identity map on H as an elementary regular transformation attached to every element of H. An endomorphism of H defined by $c \mapsto 1$ for some $c \in B$ and $b \mapsto b$ for $b \in B - \{c\}$ is called an *elementary singular transformation* and is *attached* to a reduced $u \in H$ if c or c^{-1} occurs in u. A *Nielsen transformation* is an endomorphism τ of H of the form $\tau = \tau_1 \dots \tau_k$, where each τ is an elementary regular or singular transformation; we call τ *regular* or *singular* if each factor τ_i is regular or each τ_i is singular. We say that τ is *attached* to $u \in H$ if τ_i is attached to $\tau_1 \dots \tau_{i-1}(u)$ for $1 \leq i \leq k$.

We also need the notion of the *star graph* (or *co-initial graph* or *Whitehead graph*) $\Sigma(u)$ of a reduced $u \in H$. The set of vertices of $\Sigma(u)$ is $B \cup B^{-1}$. For each subword st of u with $s, t \in B \cup B^{-1}$, $\Sigma(u)$ has a directed edge from s to t^{-1}; if p and q are the terminal and initial letters of u, $\Sigma(u)$ also has an edge from p to q^{-1} called the *external edge*. For a subset S of $B \cup B^{-1}$, the *subgraph of* $\Sigma(u)$ *spanned by* S is a graph with set S of vertices and with edges being those edges of $\Sigma(u)$ both of whose endpoints lie in S. We say that $u \in H$ is *connected* if the subgraph of $\Sigma(u)$ spanned by $\mathrm{gen}(u) \cup (\mathrm{gen}(u))^{-1}$ is connected, where $\mathrm{gen}(u) = \{b \in B\colon\ b \text{ or } b^{-1} \text{ occurs in } u\}$.

We shall also make use of Whitehead automorphisms of H. They are of two types. The first, called *level Whitehead automorphisms*, simply permute $B \cup B^{-1}$. The second type of Whitehead automorphism is denoted (S, s), where $S \subseteq B \cup B^{-1}$ with $s \in S$ and $s^{-1} \notin S$. The map (S, s) is defined by $t \mapsto ts$ if $t \in S$, $t^{-1} \notin S$, and $t \neq s$, by $t \mapsto s^{-1}ts$ if $t, t^{-1} \in S$, and by $b \mapsto b$ if $b \in B$, $b, b^{-1} \notin S$, or $b = s$ or s^{-1}. A Whitehead automorphism (S, s) is *attached* to a reduced word $u \in H$ if the subgraph of $\Sigma(u)$ spanned by S is connected. We observe the following:

Lemma 2.2.10. *Every Whitehead automorphism (S, s) attached to a reduced word $u \in H$ is a regular Nielsen transformation attached to u.*

Proof. We use induction on $|S|$, the number of elements of S. If $|S| = 1$, $S = \{s\}$ and (S, s) is the identity map. If $|S| \geq 2$, choose $t \in S$ such that $t \neq s$ but t and s are joined by an edge in $\Sigma(u)$. It is easy to see that $(S, s) = (\{t, s\}, s)(S - \{t\}, s)$ and that $(\{t, s\}, s)$ is an elementary regular

transformation attached to u. It remains to show that $(S-\{t\}, s)$ is attached to $\varrho(u)$, where $\varrho = (\{t, s\}, s)$.

If $S - \{t\} = \{s\}$, we are finished, so suppose that $p \in S - \{t\}$, $p \neq s$. Since (S, s) is attached to u, there is an edge-path $e_1 \dots e_k$ in $\Sigma(u)$ with e_i an edge from p_{i-1} to p_i, $p_i \in S$ for $0 \leq i \leq k$, $p_0 = p$, and $p_k = s$; among all such edge-paths, pick one with k minimal. If $p_i \neq t$ for $0 \leq i \leq k$, then $e_1 \dots e_k$ is an edge-path in $\Sigma(\varrho(u))$ witnessing that p and s are in the same component of the subgraph of $\Sigma(\varrho(u))$ spanned by $S - \{t\}$. If $p_i = t$ for some i, $0 \leq i \leq k$, our choice of edge-path shows that $p_{k-1} = t$ and $p_i \neq t$ for $0 \leq k - 1$. In $\Sigma(\varrho(u))$ there is an edge e'_{k-1} from p_{k-2} to s, and so $e_1 \dots e_{k-2} e'_{k-1}$ is an edge-path from p to s in the subgraph of $\Sigma(\varrho(u))$ spanned by $S - \{t\}$. It follows that the subgraph of $\Sigma(\varrho(u))$ spanned by $S - \{t\}$ is connected, and so $(S - \{t\}, s)$ is attached to $\varrho(u)$. ■

We are now ready to prove the following generalization of [225, Proposition 6].

Proposition 2.2.11. *If G and H are free groups freely generated by sets A and B, respectively, and if $u \in H$, $w \in G$, and $\alpha\colon H \to G$ is a homomorphism with $\alpha(u) = w$, then there is a Nielsen transformation τ of H attached to u and a homomorphism $\beta\colon H \to G$ such that $\tau(u)$ is connected, w is a Nielsen-reduced image of $\tau(u)$ under β, and $\beta(H) = \alpha(H)$.*

Proof. The proof here is, for the most part, a standard Nielsen reduction argument. We make use of a function K introduced in [225]; K is a map from G to the positive integers with the properties that $|u| \leq |v|$ implies $K(u) \leq K(v)$ and that $K(u) = K(v)$ if and only if $u = v$ or $u = v^{-1}$. We use induction, first on $|\operatorname{gen}(u)|$, the number of generators of H occurring in u, and second on $\sum_{b \in \operatorname{gen}(u)} K(\alpha(b))$. If u is not connected, there is some $s \in \operatorname{gen}(u)$ such that s and s^{-1} are in different components of $\Sigma(u)$. At least one of these components, say that of s, fails to contain the external edge. We let S be the set of vertices in the component of s in $\Sigma(u)$ and note that (S, s) is attached to u, that $|\operatorname{gen}((u)(S, s))| \leq |\operatorname{gen}(u)|$, and that $\alpha((H)(S, s)^{-1}) = \alpha(H)$. We replace u by $(u)(S, s)$ and α by $(S, s)^{-1}\alpha$ and appeal to the induction hypothesis.

Suppose now that u is connected and that $\alpha(c) = 1$ for some $c \in \operatorname{gen}(u)$. In this case, we use the Nielsen transformation τ defined by $\tau(c) = 1$ and $\tau(b) = b$ for $b \in B - \{c\}$. Now τ is attached to u and $|\operatorname{gen}(\tau(u))| \leq |\operatorname{gen}(u)|$, so we may replace u by $\tau(u)$ and again invoke the induction hypothesis.

Finally, suppose that u is connected and $\alpha(b) \neq 1$ for $b \in \operatorname{gen}(u)$ but that w is not a Nielsen-reduced image of u under α. Then either u has a subword st with $s, t \in B \cup B^{-1}$ and more than half of either $\alpha(s)$ or $\alpha(t)$ cancels in the product $\alpha(s)\alpha(t)$, or u has a subword rst with $r, s, t \in B \cup B^{-1}$ and $\alpha(s)$ cancels entirely in the product $\alpha(r)\alpha(s)\alpha(t)$. As in the proof of [225, Lemma 3], there is an elementary regular Nielsen transformation τ attached to u such that $|\operatorname{gen}(\tau(u))| \leq |\operatorname{gen}(u)|$ and

$\sum_{b\in\mathrm{gen}(\tau(u))} K((\tau^{-1}\alpha(b))) \leq \sum_{b\in\mathrm{gen}(u)} K(\alpha(b))$. Here we replace u by $\tau(u)$, α by $\tau^{-1}\alpha$ (notice that $\tau^{-1}\alpha(H) = \alpha(H)$), and use the induction hypothesis. ■

Theorem 2.2.12. *There is an algorithm to tell which elements of a free group G are test elements; that is, to decide for $w \in G$ whether or not every endomorphism α of G with $\alpha(w) = w$ is an automorphism of G.*

Proof. Let us fix a free generating set A for G. We may assume that A is finite, for otherwise no element of G is a test element. If $w \in G$ and α is an endomorphism of G with $\alpha(w) = w$, then by Proposition 2.2.11 there are endomorphisms τ and β of G such that w is a Nielsen-reduced image of $\tau(w)$ under β. We can effectively enumerate the pairs $(v_1, \beta_1), \ldots, (v_2, \beta_k)$ such that w is a Nielsen-reduced image of $v_i \in G$ under the endomorphism β_i of G, but β_i is not surjective. (If $|A| \geq 2$, there will be such pairs. For example, if $A = \{a_1, a_2, \ldots, a_n\}$, we have the pair (a_1, β) with $\beta(a_1) = w$ and $\beta(a_i) = 1$ for $2 \leq i \leq n$.) We next check to see if any of $v_1, \ldots, v_k$ are endomorphic images of w in G; this is decidable by Makanin's algorithm [232] to tell if equations have solutions in a free group. If one of $v_1, \ldots, v_k$ is an endomorphic image of w in G, then w is not a test element for G; otherwise, w is a test element for G. ■

2.3 Test Sets

One can consider test sets rather than just single test elements. This allows one to detect more subtle distinctions between different automorphisms of a free group. In particular, the following natural problem has attracted a lot of attention:

Problem 2.3.1 ([43]). Denote by $\mathrm{Epi}(n, k)$ the set of all homomorphisms from a free group F_n onto a free group F_k; $n, k \geq 2$. Are there two elements $g_1, g_2 \in F_n$ with the following property: whenever $\varphi(g_i) = \psi(g_i)$, $i = 1, 2$, for some homomorphisms $\varphi, \psi \in \mathrm{Epi}(n, k)$, then $\varphi = \psi$? (In other words, every homomorphism from $\mathrm{Epi}(n, k)$ is completely determined by its values on just two elements.)

Addressing this problem, S. Ivanov [153] proved that every *injective* homomorphism from $\mathrm{Epi}(n, k)$ is completely determined by its values on just two elements.

More recently, D. Lee [204], based on the ideas of [153], settled the problem completely. Below we sketch some ideas from Ivanov's paper [153] and refer the reader to [153] and [204] for full proofs.

Definition 2.3.2. A nontrivial element $w \in F_m$ is an M-test word for F_m if for every endomorphism φ and monomorphism ψ of F_m the equation $\varphi(w) = \psi(w)$ implies that φ is also a monomorphism.

Definition 2.3.3. A nontrivial word $w(x_1, \dots, x_n)$ is a C-test word in n letters for F_m if for any two n-tuples $(A_1, \dots, A_n)$, $(B_1, \dots, B_n)$ of elements of F_m the equality $w(A_1, \dots, A_n) = w(B_1, \dots, B_n) \neq 1$ implies the existence of an element $S \in F_m$ such that $B_i = SA_iS^{-1}$ for all $i = 1, 2, \dots, n$.

We can make several observations related to Definitions 2.3.2–2.3.3. First, any C-test word in n letters is both a test and M-test element for F_n. In this sense, Definition 2.3.3 is the most restrictive one. The commutator $[x_1, x_2]$ is an M-test word (for F_2) but not a C-test word in two letters. If a C-test word w in n letters is not a proper power, then the stabilizer of w in $\operatorname{Aut} F_n$ is $\langle \tau_w \rangle$.

The word $w = [x_1, x_2][x_3, x_4] \dots [x_{2m-1}, x_{2m}]$ with $m > 1$ is neither a C- nor M-test one. To see the latter, consider an even m and put $A_1 = x_1, \dots$, $A_m = x_m$, $A_{m+1} = x_{2m}x_m x_{2m}^{-1}$, $A_{m+2} = x_{2m}x_{m-1}x_{2m}^{-1}, \dots$, $A_{2m-1} = x_{2m}x_2x_{2m}^{-1}$, $A_{2m} = x_{2m}x_1x_{2m}^{-1}$. Then $\operatorname{rank}\langle A_1, \dots, A_{2m} \rangle = 2m$ but

$$[A_1, A_2][A_3, A_4] \dots [A_{2m-1}, A_{2m}] = [[x_1, x_2] \dots [x_{m-1}, x_m], x_{2m}].$$

Therefore, setting $\varphi(x_1) = [x_1, x_2] \dots [x_{m-1}, x_m]$, $\varphi(x_2) = x_{2m}$, $\varphi(x_3) = \dots = \varphi(x_{2m}) = 1$, we see that w fails to be an M-test word. Clearly, a similar argument can be used to consider the case of odd $m > 1$.

It is not clear whether or not there are M-test words in F_m, $m \geq 3$, among the words of the form $x_1^{k_1} \dots x_m^{k_m}$, and this might be a rather interesting and difficult problem. If $m = 2$, then any word $x_1^{k_1}x_2^{k_2}$, where k_1, k_2 are multiples of $k > 1$, is an M-test word. This follows from a result of Lyndon and Schützenberger [228] that elements of a solution of the equation $x^{l_1}y^{l_2}z^{l_3} = 1$ with $l_i > 1$ in F_m lie in a cyclic subgroup.

On the other hand, it is easy to see from considering values of a C-test word $w(x_1, \dots, x_n)$ on a cyclic subgroup of F_m that if $n > 1$ then $w \in F_n'$, where F_n' is the commutator subgroup of the free group F_n with basis $\{x_1, \dots, x_n\}$. This implies that there are no C-test words among the words $x_1^{k_1} \dots x_m^{k_m}$.

The words $[x_1, \dots, x_m]$ with $m > 2$ are neither M- nor C-test ones. To see this, put $A_1 = x_3x_1x_3^{-1}$, $A_2 = x_3x_2x_3^{-1}$, $A_3 = [x_1, x_2]$. Then $\operatorname{rank}\langle A_1, A_2, A_3 \rangle = 3$ and

$$[[A_1, A_2], A_3] = [x_3[x_1, x_3]x_3^{-1}, [x_1, x_2]] = [[x_3, [x_1, x_2]], [x_1, x_2]].$$

Hence, upon setting $\varphi(x_1) = x_3$, $\varphi(x_2) = \varphi(x_3) = [x_1, x_2]$, we see that $[[x_1, x_2], x_3]$ is not an M-test word, and now the claim becomes obvious.

Thus, Definitions 2.3.2–2.3.3 are rather restrictive, and the very existence of M-test words for F_m, $m > 2$, and, especially, C-test words in n letters for F_m with $m, n > 1$ is unclear. However, it turns out that C-test words do exist.

Theorem 2.3.4 ([153]). *For arbitrary $n \geq 2$, there exists a word $w_n(x_1, \ldots, x_n)$ that is a C-test word in n letters for any free group F_m of rank $m \geq 2$. In addition, $w_n(x_1, \ldots, x_n)$ is not a proper power.*

Corollary 2.3.5. *There is an element $u \in F_m$ such that if φ is an endomorphism, ψ is a monomorphism of F_m, and $\varphi(u) = \psi(u)$, then φ is also a monomorphism and, more specifically, $\varphi = \tau_u^k \psi$, where τ_u is the inner automorphism of F_m defined by means of u and k is an integer.*

Corollary 2.3.6. *There are two elements $u_1, u_2 \in F_m$ such that any monomorphism ψ of F_m is uniquely determined by $\psi(u_1), \psi(u_2)$.*

Corollaries 2.3.5 and 2.3.6 follow immediately from Theorem 2.3.4: It suffices to put $u = w_m(x_1, \ldots, x_m)$ in Corollary 2.3.5 and $u_1 = w_m(x_1, \ldots, x_m)$, $u_2 \notin \langle w_m(x_1, \ldots, x_m) \rangle$ in Corollary 2.3.6.

The construction of the C-test word $w_n(x_1, \ldots, x_n)$ is as follows: If $n = 2$, then

$$w_2(x_1, x_2) = [x_1^8, x_2^8]^{100} x_1 [x_1^8, x_2^8]^{200} x_1 [x_1^8, x_2^8]^{300} x_1^{-1} [x_1^8, x_2^8]^{400} \times x_1^{-1} [x_1^8, x_2^8]^{500} x_2 [x_1^8, x_2^8]^{600} x_2 [x_1^8, x_2^8]^{700} x_2^{-1} [x_1^8, x_2^8]^{800} x_2^{-1}.$$

For $n \geq 3$,

$$w_n(x_1, \ldots, x_n) = w_2(w_{n-1}(x_1, \ldots, x_{n-1}), w_{n-1}(x_2, \ldots, x_n)).$$

To conclude this section, we give a definition of the *test rank* of a finitely generated group G:

Definition 2.3.7. Let G be an n-generator group. Call a set of elements $\{g_1, \ldots, g_k\}$, $k \leq n$, a test set for the group G if, whenever $\varphi(g_i) = g_i$, $i = 1, \ldots, k$, for some endomorphism f of the group G, this φ is actually an automorphism of G. The test rank of G is the minimal cardinality of a test set.

A natural question now is (see [43, Problem (FP23)]): can the test rank of G be equal to 2 if $n > 2$? If G has a test element, the test rank of G is obviously 1. For example, any free group of finite rank has test rank 1. On the other hand, there are groups (for example, free abelian groups of finite rank) whose test rank equals their rank. (Obviously, it cannot be bigger than that.)

Timoshenko [382] proved that a free metabelian group of rank ≥ 3 has test rank 2. Rocca and Turner [316] have shown recently that for any pair of integers (k, n) with $1 \leq k \leq n$, there are finitely generated abelian groups of rank n and test rank k.

2.4 The "Double Jacobian" Matrix

In this section, we establish a direct connection between the "test element" approach to recognizing automorphisms and the "inverse function theorem" due to Birman [54] (see our Section 1.4).

We define for any element $u \in F_n$ the "double Jacobian" matrix $D_u = (d'_i(d_j(u)))_{1\le i,j\le n}$, where d_j is the "usual", or left, Fox derivation and d'_i is the right Fox derivation (see Section 1.4). Then:

Theorem 2.4.1. *Let φ be an endomorphism of the group F. It is an automorphism*

(i) *if and only if the matrix $D_{\varphi(u)}$ is invertible over $\mathbb{Z}F$ with $u = [x_1, x_2]\dots[x_{n-1}, x_n]$, n even;*

(ii) *if and only if the natural image over $\mathbb{Z}_2F$ of the matrix $D_{\varphi(u)}$ is invertible over $\mathbb{Z}_2F$ with $u = x_1^2x_2^2\dots x_n^2$.*

Proof. (i) Let $\varphi(x_i) = y_i$, $1 \le i \le n$, $n = 2m$, and let $v = \varphi(u)$. Apply a left Fox derivation d_j to both sides of this equality; by Lemma 1.4.5, this gives

$$d_j(u) = \sum_{1\le k\le n} \varphi(d_k(u))d_j(y_k). \tag{2.5}$$

Note that every $\varphi(d_k(u))$ has augmentation 0 since u belongs to the commutator subgroup F' so that $d_k(u) \in \Delta$, $1 \le k \le n$. Applying now a right Fox derivation d'_i to both sides of (2.5), we get by Lemma 1.4.5

$$d'_i(d_j(v)) = \sum_{1\le k\le n}\sum_{1\le m\le n} d'_i(y_m)\varphi(d'_m(d_k(u)))d_j(y_k). \tag{2.6}$$

When i and j run through $\{1,\dots,n\}$, (2.6) becomes a system of n^2 equalities that can be written in the matrix form as

$$D_{\varphi(u)} = J'_\varphi \varphi(D_u) J_\varphi, \tag{2.7}$$

where $J_\varphi = (d_j(y_i))_{1\le i,j\le n}$ is the left Jacobian matrix of φ; $J'_\varphi = (d'_i(y_j))_{1\le i,j\le n}$ is the right Jacobian matrix of φ.

Suppose the matrix $D_{\varphi(u)}$ is invertible. Then every matrix on the right-hand side of (2.7) must be invertible, too, which implies φ is an automorphism by Birman's result.

Conversely, suppose φ is an automorphism. Then, again by Birman's theorem, the matrices J'_φ and J_φ are invertible (actually, the result of Birman applies to the matrix J_φ, but applying Lemma 1.4.7 immediately gives the same result for J'_φ as well). Now we have to consider the matrix D_u; it is a block-matrix having m 2×2 matrices B_k along the diagonal and zeros below; here

$$B_k = \begin{pmatrix} x_{2k-1}^{-1}x_{2k}^{-1}(x_{2k}-1) & 1 - x_{2k-1}^{-1}x_{2k}^{-1}(x_{2k-1}-1) \\ -x_{2k}^{-1} & x_{2k}^{-1} - x_{2k}^{-1}x_{2k-1} \end{pmatrix},$$

$1 \leq k \leq m$. It can be easily verified that every matrix B_k has the inverse

$$B_k^{-1} = \begin{pmatrix} x_{2k-1} - x_{2k-1}^2 & (1 - x_{2k-1})(x_{2k} - 1) - x_{2k} \\ x_{2k-1} & x_{2k-1} \end{pmatrix}.$$

Hence the matrix D_u is invertible, and so is the matrix $D_{\varphi(u)}$ on the left-hand side of (2.7). This completes the proof of part (i) of the theorem.

(ii) The proof goes along the same lines as that of part (i) upon replacing the group ring $\mathbb{Z}F$ with $\mathbb{Z}_2F$. On the right-hand side of (2.5), the elements $\varphi(d_k(u))$ will have augmentation 0 because, in the ring $\mathbb{Z}_2F$, one has $d_k(u) \in \Delta_F$ whenever $u \in F^2$. Then, Birman's theorem remains valid on replacing $\mathbb{Z}F$ with $\mathbb{Z}_2F$ (see Remark 1.4.9). Finally, for $u = x_1^2 x_2^2 \dots x_n^2$, the matrix D_u is an upper triangular matrix with the units on the diagonal; in particular, it is invertible over any ring, and this completes the proof. ■

It is easy to produce many examples of elements u of the group ring $\mathbb{Z}F$ with D_u invertible. However, in the group F itself, the only elements we know with this property are $[x_1, x_2] \dots [x_{n-1}, x_n]$, $x_1^2 x_2^2 \dots x_n^2$ and their automorphic images. We have to admit that we do not know what makes the double Jacobian matrix of an element $u \in F$ invertible. It is clear that if an element $u \in F$ has the matrix D_u invertible, then it is a test element for recognizing automorphisms; the converse, however, is not true. For example, elements of the form $x_1^p x_2^p \dots x_n^p$, $p \geq 3$, are test elements, but they have the double Jacobian matrix noninvertible.

Remark 2.4.2. If we switch left and right Fox derivatives in the definition of the double Jacobian matrix (i.e., put $D'_u = (d_i(d'_j(u)))_{1 \leq i,j \leq n}$), then D'_u turns out to be the transpose of D_u. In particular, Theorem 2.4.1 holds also on replacing $D_{\varphi(u)}$ with $D'_{\varphi(u)}$.

http://www.springer.com/978-0-387-40562-9

Combinatorial Methods
Free Groups, Polynomials, and Free Algebras
Shpilrain, V.; Mikhalev, A.; Yu, J.-t.
2004, XII, 315 p., Hardcover
ISBN: 978-0-387-40562-9