# A commutative version of the group ring

W.H. MANNAN[*]

July 19, 2012

### Abstract

We construct a commutative version of the group ring and show that it allows one to translate questions about the normal generation of groups into questions about the generation of ideals in commutative rings. We demonstrate this with an alternative proof of a result about the normal generation of the free product of two cyclic groups.

## 1  Introduction

A number of outstanding problems arising in low dimensional topology and combinatorial group theory share a common core difficulty; it is in general hard to show that a normal subgroup $H$ of a group $G$ cannot be normally generated by a set of elements, $X \subset H$, with some specified property. The most obvious obstruction is that if $H$ is normally generated by $X$, then the image of $X$ would generate the image of $H$ in the abelianisation, $G/[G,G]$. However a new obstruction is required to address problems where abelianisation is too blunt.

Fix a field $\kappa$. The normal subgroup structure of a group $G$ is reflected in the ideal structure of its group ring $\kappa[G]$, in a fairly simple way: if $h_1, \cdots, h_n$ normally generate a normal subgroup $H \lhd G$, then the elements $1 - h_1, \cdots, 1 - h_n$ generate the kernel of the induced map $\kappa[G] \to \kappa[G/H]$ as a two-sided ideal. However even for a finitely presented group $G$, the group ring $\kappa[G]$ need not be either Noetherian or commutative, making its ideals harder to work with.

The approach of this paper is to instead work with a commutative version of the group ring (taken over a field $\kappa$ of characteristic 0). This provides a functor from the category of groups to the category of commutative rings. Questions about the normal generation of subgroups are thus turned into questions about the generation of ideals. We demonstrate how non-trivial group theoretic results may thus be obtained from elementary commutative algebra.

We note that our construction has similarities to various existing algebraic structures. For example the identities in Lemma 3.5 and Corollary 3.6 suggest a relationship with Clifford algebras, whilst Lemma 2.7 suggests a relationship with the trace polynomials of Horowitz [8]. One can think of our construction as 'less free' than these. Another commutative analogue of group rings is given in [19].

We first outline some problems which require a new such obstruction. Given a finite set of generators for a finitely presented group $G$, let $F$ be the free group on the

---

[*]School of Mathematics, University of Southampton, Southampton, SO17 1BJ.
e-mail : `wajid@mannan.info`

generators and let $G \cong F/R$ where $R \lhd F$. **The Relation Gap problem** [5] asks: Must the minimal number of elements needed to normally generate $R$ in $F$ equal the minimal number of elements needed to normally generate a subgroup of $R$ in $F$, which surjects onto the abelianisation $R/[R, R]$.

**Wall's D2 problem** is a major unanswered question in low dimensional topology. It asks if cohomological dimension and geometric dimension agree for homotopy types of finite cell complexes. C.T.C. Wall proved that they do agree, except possibly for cell complexes of geometric dimension 3 and cohomological dimension 2 [17, Theorem E]. However this remaining case has resisted attack for the last forty five years. It has long been known that a counterexample resolving the Relation Gap problem would under certain hypotheses also solve Wall's D2 problem [7]. More recently these hypotheses have been reduced [13]. In [14] Wall's D2 problem is expressed in terms of normal generation.

**The Kervaire conjecture** posits that the free product of the integers with a non-trivial group cannot be normally generated by a single element.

**The Wiegold problem** [16, Question 5.52] asks if a finitely generated perfect group must be normally generated by one element. For a finite perfect group it is elementary to show that it is the normal closure of a single element. It is easy to find finitely generated perfect groups where this is apparently not the case, yet there do not currently exist obstructions which would allow us to prove this.

A conjecture due to H. Short [9, Conjecture 2] posits: The number of elements needed to normally generate a free product of $n$ (non-trivial) cyclic groups is at least $n/2$. For $n = 3$ this was known for forty years as the Scott-Wiegold conjecture [15, Problem 5.53], and was eventually proven [9] by Jim Howie. This problem is too subtle to approach by abelianisation as the free product of 3 cyclic groups may abelianise to a cyclic group (which is generated by a single element). In this case it was resolved using topological methods.

The $n = 4$ case of the above conjecture is trivially implied by the $n = 3$ case. If it could be proven for $n = 5$ then the Wiegold problem would be solved:

**Potential counterexample 1.1.** Let $G = C_p * C_q * C_r * C_s * C_t / \langle \pi \rangle$, where $\pi$ is the product of the generators of the cyclic factors, and $p, q, r, s, t$ are pairwise coprime. $G$ is perfect (by the Chinese remainder Theorem) but if it were the normal closure of a single element $x$, then the free product of 5 cyclic groups would be normally generated by just 2 elements: $\pi, x$. Note that $G$ here is generated by 4 generators, as the triviality of $\pi$ in $G$ implies that we may express one generator in terms of the other 4.

There are also many potential counterexamples which could solve Wall's D2 problem and / or the Relation Gap problem [2, 5, 10]. We mention a candidate due to recently published work by Gruenberg and Linnell [6]:

**Potential counterexample 1.2.** Fix coprime integers $p, q$ and let $G = (C_p \times \mathbb{Z}) * (C_q \times \mathbb{Z})$. Let $F$ be the free group on the natural 4 generators of $G$ and let $G \cong F/R$, where $R \lhd F$. From [6, Proposition 1.2] we know that 3 elements of $R$ may be chosen so that their normal closure in $F$ surjects onto the quotient $R/[R, R]$. However it appears that $R$ cannot be normally generated by fewer than 4 elements.

If this could be proven then the Relation Gap problem would be solved. Further, if it was shown that every finite presentation of $G$ required at least as many relators as generators, then Wall's D2 problem would also be solved. Without loss of generality,

the generators in such a presentation would be the natural 4 generators, together with a finite set of trivial generators (representing $e \in G$).

In the context of our methods, the Relation Gap and Wiegold problems could be approached by computing the commutative rings for the groups from the examples above, and showing that the relevant ideal cannot be generated in an undesirable way.

Although we do not attempt to attack these problems in this paper, we are able to demonstrate the method by proving a similar result (originally due to Boyer [4]); the free product of two cyclic groups cannot be normally generated by a proper power. As in the examples above, this problem cannot be approached by abelianising the group, as the abelianisation would be cyclic if the orders of the cyclic factors are coprime.

In §2 we define the commutative version of a group ring. In §3, §4 we discuss its properties, culminating in a complete description. In §5 we compute this for the free product of two cyclic groups. We show that in the light of our methods, Boyer's result reduces to an absolutely elementary statement in commutative algebra. Finally we show that the Scott-Wiegold conjecture may also be reduced to a statement about a commutative ring. This time however the statement is not immediately obvious.

Having applied our commutative version of group rings to problems concerning 2-generated and 3-generated groups, it is our hope that these methods may be applied to the 4-generated groups in Potential counterexamples 1.1 and 1.2. In this way we hope that our methods will eventually be able to resolve the major questions which we have mentioned here.

# 2   Construction of the commutative group ring

Fix a field $\kappa$ of characteristic 0. All ring homomorphisms of $\kappa$– algebras will be understood to fix $\kappa$. The inverse operation on a group $G$ extends $\kappa$–linearly to an involution $* \colon \kappa[G] \to \kappa[G]$. The invariants of $*$, $\kappa[G]^*$, are then a subset of $\kappa[G]$. The set of commutators $[\kappa[G], \kappa[G]^*]$ generate a 2-sided ideal:

$$\langle [\kappa[G], \kappa[G]^*] \rangle \lhd \kappa[G].$$

**Definition 2.1.** *Let $A_G = \kappa[G]/\langle [\kappa[G], \kappa[G]^*] \rangle$.*

Thus $A_G$ is the group ring of $G$ with the added relations that the invariants of $*$ are central. Given $x \in \kappa[G]$ we denote the corresponding element in $A_G$ by $[x]$.

**Lemma 2.2.** *The action of $*$ is well defined on $A_G$.*

*Proof.* For $z \in [\kappa[G], \kappa[G]^*]$, we have $z = ab - ba$ for some $b$ satisfying $b^* = b$. Thus

$$z^* = (ab - ba)^* = b^* a^* - a^* b^* = ba^* - a^* b \in \langle [\kappa[G], \kappa[G]^*] \rangle.$$

If $[x] = [y]$ then $x - y \in \langle [\kappa[G], \kappa[G]^*] \rangle$, so $(x-y)^* \in \langle [\kappa[G], \kappa[G]^*] \rangle$ and $[x^*] = [y^*]$. ☐

Let $\kappa[G]^{\#} = A_G{}^*$, the invariants of this action. Let $\Lambda_G$ be the anti-invariants of the action: $\Lambda_G = \{[x] \in A_G |\ [x]^* = -[x]\}$. For $x \in \kappa[G]$ let:

$$\bar{x} = \frac{x + x^*}{2} \in \kappa[G]^*, \qquad \vec{x} = \frac{x - x^*}{2} \in \kappa[G],$$

so $[\bar{x}] \in \kappa[G]^{\#}$, $[\vec{x}] \in \Lambda_G$.

**Lemma 2.3.** *We have a decomposition of $\kappa$–linear vector spaces:*

$$A_G = \kappa[G]^\# \oplus \Lambda_G.$$

*Proof.* If $[x] \in \kappa[G]^\# \cap \Lambda_G$ then $[x] = [x]^* = -[x]$ so $[x] = 0$. Given any $[y] \in A_G$ we have $[y] = [\bar{y}] + [\vec{y}]$. □

**Lemma 2.4.** *If $[x] \in \kappa[G]^\#$ then $[x] = [\bar{x}]$ and if $[x] \in \Lambda_G$ then $[x] = [\vec{x}]$.*

*Proof.* If $[x] \in \kappa[G]^\#$ then

$$[x] = [\bar{x} + \vec{x}] = [\bar{x}] + \frac{[x - x^*]}{2} = [\bar{x}] + \frac{[x] - [x]^*}{2} = [\bar{x}].$$

If $[x] \in \Lambda_G$ then

$$[x] = [\bar{x} + \vec{x}] = \frac{[x + x^*]}{2} + [\vec{x}] = \frac{[x] + [x]^*}{2} + [\vec{x}] = [\vec{x}].$$

□

As $\bar{x} \in \kappa[G]^*$, we have $[\bar{x}]$ central in $A_G$. Thus $\kappa[G]^\#$ is central in $A_G$.

**Lemma 2.5.** *$\kappa[G]^\#$ is a subring of $A_G$ and $\Lambda_G$ is a (right) module over $\kappa[G]^\#$.*

*Proof.* Clearly $1 = [e] \in \kappa[G]^\#$ and $\kappa[G]^\#$ is closed under addition and subtraction. If $[x], [y] \in \kappa[G]^\#$ then $[x][y] \in \kappa[G]^\#$ as

$$([x][y])^* = [(xy)^*] = [y^*x^*] = [y]^*[x]^* = [y][x] = [x][y].$$

Thus $\kappa[G]^\#$ is also closed under multiplication, and therefore a subring of $A_G$.

To see that $\Lambda_G$ is a module over $\kappa[G]^\#$, we check that $\Lambda_G$ is closed under multiplication by elements of $\kappa[G]^\#$. To that end let $[x] \in \kappa[G]^\#, [y] \in \Lambda_G$. Then:

$$([y][x])^* = [(yx)^*] = [x^*y^*] = [x]^*[y]^* = -[x][y] = -[y][x].$$

so $[y][x] \in \Lambda_G$. □

As $\kappa[G]^\#$ is central in $A_G$, we know that $\kappa[G]^\#$ is a commutative ring.

**Definition 2.6.** *We define the commutative version of the group ring for the group $G$, over a field $\kappa$, to be $\kappa[G]^\#$.*

We note the following identities in $\kappa[G]^\#$:

**Lemma 2.7.** *Let $[x], [y], [z] \in A_G$. Then:*
*i)* $[\overline{xy}] = [\overline{yx}]$.
*ii)* $2[\bar{y}][\overline{xz}] = [\overline{xyz}] + [\overline{xy^*z}]$, so in particular $[\bar{x}][\bar{y}] = \frac{1}{2}([\overline{xy}] + [\overline{xy^*}])$.
*iii)* $[\overline{x^*}] = [\bar{x}]$.

*Proof.* i) We have:
$$\overline{xy} - \overline{yx} = (\bar{x}y - y\bar{x}) + (\bar{y}x^* - x^*\bar{y}).$$

As $[\bar{x}], [\bar{y}] \in \kappa[G]^{\#}$ we conclude $[\overline{xy}] - [\overline{yx}] = [0]$.

ii) We have
$$\overline{xyz} + \overline{xy^*z} = x\bar{y}z + z^*\bar{y}x^*.$$

As $[\bar{y}] \in \kappa[G]^{\#}$ we conclude $[\overline{xyz}] + [\overline{xy^*z}] = 2[\bar{y}]\,[\overline{xz}]$.

iii) Trivial. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

Let $f\colon G \to H$ be a group homomorphism. Then $f$ extends $\kappa$–linearly to a ring homomorphism $f\colon \kappa[G] \to \kappa[H]$. We will now show that this induces a ring homomorphism:
$$f^{\#}\colon \kappa[G]^{\#} \to \kappa[H]^{\#}.$$

**Lemma 2.8.** *$f$ induces a well defined ring homomorphism $\hat{f}\colon A_G \to A_H$.*

*Proof.* From the definition of group homomorphism we know that $(f(x))^* = f(x^*)$ for all $x \in G$ and hence for all $x \in \kappa[G]$. Thus if $x \in \kappa[G]^*$, then

$$(f(x))^* = f(x^*) = f(x).$$

Thus $f(x) \in \kappa[H]^*$ and if $z = yx - xy$ for some $y \in \kappa[G]$, then

$$f(z) = f(y)f(x) - f(x)f(y) \in [\kappa[H], \kappa[H]^*].$$

Hence if $[x] = [y]$, then $[f(x)] = [f(y)]$ and we may define $\hat{f}([x]) = [f(x)]$. $\quad\square$

Clearly $\hat{f}([x]^*) = (\hat{f}([x]))^*$, so if $[x] \in \kappa[G]^{\#}$ then

$$(\hat{f}([x]))^* = \hat{f}([x]^*) = \hat{f}([x])$$

and $\hat{f}([x]) \in \kappa[H]^{\#}$. Thus we may define:

**Definition 2.9.** *For a group homomorphism $f\colon G \to H$, we define the map of commutative rings $f^{\#}\colon \kappa[G]^{\#} \to \kappa[H]^{\#}$ to be the restriction of $\hat{f}$ to $\kappa[G]^{\#}$.*

By construction $(fl)^{\#} = f^{\#}l^{\#}$, where $l$ is a group homomorphism $H \to M$, so we have a functor **Group** $\to$ **Commutative Ring**, sending a group $G$ to the commutative ring $\kappa[G]^{\#}$, and the group homomorphism, $f\colon G \to H$ to the ring homomorphism $f^{\#}\colon \kappa[G]^{\#} \to \kappa[H]^{\#}$. This functor has the following 'half-exactness' property:

**Lemma 2.10.** *If $f\colon G \to H$ is a surjective group homomorphism, then the ring homomorphism $f^{\#}\colon \kappa[G]^{\#} \to \kappa[H]^{\#}$ is also surjective.*

We note in passing that the dual statement is not true. For example let $D_8$ denote the group of symmetries of a square and let $V$ be the subgroup generated by reflections through lines parallel to the edges. Then the inclusion $\iota\colon V \hookrightarrow D_8$ is an injective group homomorphism, but $\iota^{\#}$ is not injective.

Proof of Lemma 2.10:   The ring homomorphism $f \colon \kappa[G] \to \kappa[H]$ is surjective so the induced map $\hat{f} \colon A_G \to A_H$ is also surjective. Hence given $[x] \in \kappa[H]^{\#}$ we have $y \in \kappa[G]$ with $\hat{f}([y]) = [x]$. Then

$$f^{\#}([\bar{y}]) = [f(\bar{y})] = \frac{1}{2}([f(y)] + [f(y^*)]) = \frac{1}{2}(\hat{f}([y]) + (\hat{f}([y]))^*) = \frac{1}{2}([x] + [x]^*) = [x]$$

as required.                                                                           □

For the remainder of this section $f \colon G \to H$ is a surjective group homomorphism, with kernel $K \lhd G$. We wish to find generators for the ideal $\ker(f^{\#}) \lhd \kappa[G]^{\#}$.

**Lemma 2.11.** *As vector spaces over $\kappa$:*
*i)* $\ker(f \colon \kappa[G] \to \kappa[H])$ *is generated by the set* $S = \{gk - g \mid g \in G, k \in K\}$.
*ii)* $\ker(\hat{f} \colon A_G \to A_H)$ *is generated by the set* $S' = \{[gk] - [g] \mid g \in G, k \in K\}$.
*iii)* $\ker(f^{\#} \colon \kappa[G]^{\#} \to \kappa[H]^{\#})$ *is generated by the set* $S'' = \{[\overline{gk}] - [\bar{g}] \mid g \in G, k \in K\}$.

*Proof.* i) In $\kappa[G]/\langle S \rangle \kappa$ there is precisely one way of representing each element of $\kappa[H]$.

ii) We know that $S'\kappa$ is a 2-sided ideal in the ring $A_G$ as

$$([gk] - [g])[h] = [gh(h^{-1}kh)] - [gh], \qquad [h]([gk] - [g]) = [hgk] - [hg]$$

for $g, h \in G$, $k \in K$. Thus $A_G/\langle S' \rangle \kappa$ is a ring. From (i) we know that $A_G/\langle S' \rangle \kappa$ may be identified with a quotient ring of $\kappa[H]$.

To see that this quotient ring is $A_H$, we check that the additional relation in $A_H$:

$$f(x) = (f(x))^* \implies [f(x)] \text{ central},$$

is satisfied in $A_G/\langle S' \rangle \kappa$. That is we need:

$$f(x) = (f(x))^* \implies [x] \in A_G/\langle S' \rangle \kappa \text{ is central.}$$

Note that given $x \in \kappa[G]$ with $f(x) = (f(x))^*$, we have $f(\bar{x}) = f(x)$. Thus from (i) we have $[x] \sim [\bar{x}]$ in $A_G/\langle S' \rangle \kappa$ and $[\bar{x}]$ is already central in $A_G$.

iii) We have $[gk] - [g] = [\overline{gk}] - [\bar{g}] + \overrightarrow{[gk]} - \vec{[g]}$, so by (ii), $\ker(\hat{f})$ is generated over $\kappa$ by:

$$S'' \cup \{\overrightarrow{[gk]} - \vec{[g]} \mid g \in G,\ k \in K\}.$$

Thus if $[x] \in \ker(f^{\#})$, then $[x] = [y] + [z]$, where $[y] \in \langle S'' \rangle \kappa$ and $z \in \Lambda_G$. We have $[z] = [x] - [y] \in \kappa[G]^{\#}$, so by Lemma 2.3 we know $[z] = 0$.                                              □

For $x \in A_G$, $[\bar{x}] = \frac{1}{2}([x] + [x]^*)$, which depends only on $[x]$, so we have a well defined $\kappa$–linear map $m_G \colon A_G \to \kappa[G]^{\#}$ given by $[x] \mapsto [\bar{x}]$.

**Lemma 2.12.** *The following maps are linear over $\kappa[G]^{\#}$:*
*i) The map $A_G \to A_G$ given by $[x] \mapsto [xg]$, for some fixed $g \in G$.*
*ii) The map $m_G \colon A_G \to \kappa[G]^{\#}$.*

*Proof.* i) Multiplication by a ring element is always linear over a central subring.

ii) Let $[x] \in A_G$ and $[y] \in \kappa[G]^{\#}$. We must check that $m_G([x][y]) = m_G([x])[y]$:

$$m_G([x][y]) = \frac{1}{2}([x][y] + ([x][y])^*) = \frac{1}{2}([x] + [x]^*)[y] = m_G([x])[y].$$

$\square$

Let $B \subset A_G$ be a generating set for $A_G$ as a module over $\kappa[G]^{\#}$.

**Lemma 2.13.** *Given $l \in G$, the ideal in $\kappa[G]^{\#}$ generated by $\{[\overline{bl}] - [\bar{b}]|\, [b] \in B\}$ contains $[\overline{xl}] - [\bar{x}]$ for any $x \in A_G$.*

*Proof.* By Lemma 2.12 we have a linear map $t_l \colon A_G \to \kappa[G]^{\#}$ given by:

$$[y] \mapsto [\overline{yl}] - [\bar{y}].$$

We may express $[x]$ as a sum $[x] = [b_1][y_1] + \cdots + [b_r][y_r]$ with the $[b_i] \in B, [y_i] \in \kappa[G]^{\#}$. Then applying $t_l$ to both sides gives

$$[\overline{xl}] - [\bar{x}] = ([\overline{b_1 l}] - [\bar{b_1}])[y_1] + \cdots + ([\overline{b_r l}] - [\bar{b_r}])[y_r].$$

$\square$

**Definition 2.14.** *Given a set $L \subset G$, we define $L^{\#} \lhd \kappa[G]^{\#}$ to be the ideal generated by $\{[\overline{bl}] - [\bar{b}]|\, [b] \in B, l \in L\}$.*

By Lemma 2.13, $L^{\#}$ is independent of the choice of generating set $B$. In fact we could take a different generating set of $A_G$, $B_l$ for each $l \in L$ and would still have:

**Lemma 2.15.** *The ideal $L^{\#} \lhd \kappa[G]^{\#}$ is generated by $\{[\overline{bl}] - [\bar{b}]|\, l \in L, [b] \in B_l\}$.*

**Theorem 2.16.** *If the set $L \subset K$ normally generates $K$, then $\ker(f^{\#}) = L^{\#}$.*

*Proof.* As $L \subset K$ it is clear that $L^{\#} \subset \ker(f^{\#})$. Let $K'$ denote the set of $k \in K$ such that for all $g \in G$, $[\overline{gk}] - [\bar{g}] \in L^{\#}$. By Lemma 2.13 we have that $L \subset K'$. Clearly $[\bar{g}] - [\bar{g}] = 0 \in L^{\#}$ for all $g \in G$, so $e \in K'$.

Suppose $k_1, k_2 \in K'$. Then for all $g \in G$ we have

$$[\overline{gk_1 k_2}] - [\bar{g}] = ([\overline{(gk_1)k_2}] - [\overline{gk_1}]) + ([\overline{gk_1}] - [\bar{g}]) \in L^{\#}.$$

Thus $k_1 k_2 \in K'$.

Also if $k \in K'$, then for all $g \in G$ we have

$$[\overline{gk^{-1}}] - [\bar{g}] = -([\overline{(gk^{-1})k}] - [\overline{gk^{-1}}]) \in L^{\#}.$$

Thus $k^{-1} \in K'$.

Let $h \in G$ and suppose $k \in K'$. Then for all $g \in G$, using Lemma 2.7i we have

$$[\overline{g(hkh^{-1})}] - [\bar{g}] = [\overline{(h^{-1}gh)k}] - [\overline{h^{-1}gh}] \in L^{\#}.$$

Thus $hkh^{-1} \in K'$.

So $K'$ contains $L$ and the identity, and is closed under multiplication, inverse and conjugation. As $L$ normally generates $K$, we have $K' = K$. So $L^{\#}$ contains $[\overline{gk}] - [\bar{g}]$ for all $g \in G$ and $k \in K$. Thus by Lemma 2.11iii we obtain $L^{\#} = \ker(f^{\#})$. $\square$

Theorem 2.16 fails if we drop the condition that $f$ is a surjective group homomorphism. For example, if we let $f\colon V \to D_8$ be the inclusion mentioned before, then we may take $L = \phi$ the empty set, to normally generate $\ker(f)$ (as $f$ is injective). However $\ker(f^{\#})$ is non-zero in this case.

Theorem 2.16 is at the heart of our approach. If $K$ is normally generated by $N \subset K$ and we wish to show that some other set $L \subset K$ does not normally generate $K$, then by Theorem 2.16, $N^{\#} = \ker(f^{\#})$ and it is enough to show that $L^{\#} \neq N^{\#}$.

For this purpose, it will sometimes be more convenient to use a refinement of $L^{\#}$. Let $B$ now be a generating set for the module $\Lambda_G$ over $\kappa[G]^{\#}$. Note that by Lemma 2.3, the set $B \sqcup \{1\}$ generates the module $A_G$ over $\kappa[G]^{\#}$.

**Definition 2.17.** *Given a set $L \subset G$ we define $L^{\#\#} \lhd \kappa[G]^{\#}$ to be the ideal generated by $\{[\overline{bl}] - [\overline{bl^{-1}}] \mid [b] \in B,\, l \in L\}$.*

**Lemma 2.18.** *Given $l \in G$, the ideal in $\kappa[G]^{\#}$ generated by $\{[\overline{bl}] - [\overline{bl^{-1}}] \mid [b] \in B\}$ contains $[\overline{xl}] - [\overline{x^{-1}}]$ for any $[x] \in A_G$.*

*Proof.* We proceed as in Lemma 2.13 by expressing $[x]$ as a linear combination of the elements of $B \sqcup \{[1]\}$ and hence express $[\overline{xl}] - [\overline{xl^{-1}}]$ as a linear combination of the $\{[\overline{bl}] - [\overline{bl^{-1}}] \mid [b] \in B\}$ and $[\overline{1l}] - [\overline{1l^{-1}}]$ which equals 0 by Lemma 2.7iii. $\qquad\square$

Thus $L^{\#\#}$ is independent of the choice of $B$, a generating set for $\Lambda_G$. Indeed, as before one may chose a different generating set $B_l$ for each $l \in L$ and still have $L^{\#\#}$ generated by $\{[\overline{bl}] - [\overline{bl^{-1}}] \mid l \in L, [b] \in B_l\}$

**Theorem 2.19.** *If $L$ normally generates a normal subgroup $K \lhd G$, then $L^{\#\#} = K^{\#\#}$.*

*Proof.* This proof follows the structure of the proof of Theorem 2.16. Let $K'$ denote the set of $k \in K$ such that for all $g \in G$, $[\overline{gk}] - [\overline{gk^{-1}}] \in L^{\#\#}$. By Lemma 2.18 we have that $L \subset K'$. As before it is clear that $e \in K'$ and that $K'$ is closed under taking inverses. In order to show that $K' = K$ and hence prove the theorem, it remains to show that $K'$ is closed under group multiplication and conjugation.

Given $g, h \in G$ and $k \in k'$ from Lemma 2.7i we again have:

$$[\overline{g(hkh^{-1})}] - [\overline{g(hk^{-1}h^{-1})}] = [\overline{(h^{-1}gh)k}] - [\overline{(h^{-1}gh)k^{-1}}] \in L^{\#\#}.$$

Thus $K'$ is closed under conjugation.

Given $g \in G$ and $j, k \in K'$, we may expand $[\overline{k}]\,([\overline{gj}] - [\overline{gj^{-1}}])$ using Lemma 2.7ii:

$$[\overline{k}]\,([\overline{gj}] - [\overline{gj^{-1}}]) = \frac{[\overline{gjk}] + [\overline{gjk^{-1}}]}{2} - \frac{[\overline{gkj^{-1}}] + [\overline{gk^{-1}j^{-1}}]}{2}.$$

Set $z = \frac{gj + j^{-1}g}{2}$. Then using Lemma 2.7i we obtain:

$$[\overline{g(jk)}] - [\overline{g(jk)^{-1}}] = [\overline{k}]\,([\overline{gj}] - [\overline{gj^{-1}}]) + [\overline{zk}] - [\overline{zk^{-1}}] \in L^{\#\#}.$$

Thus $K'$ is closed under multiplication.

$\qquad\square$

Thus given a normal subgroup $K \lhd G$, normally genrated by a set of elements $N \subset K$, we may use Theorem 2.19 to show that $K$ is not normally generated by a set $L \subset K$. All one need do is show that $L^{\#\#} \neq N^{\#\#}$. In Section 5 we apply this

method to provide an alternative proof of a result due to Boyer [9]. In Section 6 we apply this method to the Scott-Wiegold conjecture [4]. Before that, we must be able to compute the commutative ring $\kappa[G]^\#$ and the relevant ideals $L^{\#\#}$. We build up the theory to do that in Section 3 and Section 4.

Finally in this section, we will comment on the relationship between $L^\#$ and $L^{\#\#}$. Given a set $L \subset G$, one might naively generalize from the case of the usual group ring, and consider $L^\bullet \lhd \kappa[G]^\#$ to be the relevant ideal in relation to the normal closure of $L$ (rather than $L^\#$ or $L^{\#\#}$), where $L^\bullet$ is the ideal generated by $\{1 - [\bar{l}] \mid l \in L\}$. These three ideals are related as follows:

**Lemma 2.20.** *We have $L^\# = L^{\#\#} \dot{+} L^\bullet$.*

*Proof.* Let $g \in G$ and $l \in L$. Applying Lemma 2.7ii we get:

$$[\overline{gl}] - [\bar{g}] = \frac{[\overline{gl}] - [\overline{gl^{-1}}]}{2} + [\bar{g}]([\bar{l}] - 1) \in L^{\#\#} \dot{+} L^\bullet.$$

$\square$

# 3   Identities in $A_G$

In order to implement our approach, we need to have a description of the commutative ring $\kappa[G]^\#$ and we need a generating set $B$ for $A_G$ as a module over $\kappa[G]^\#$. Then given $K \lhd G$, a set $N \subset K$, which normally generates $K$, and another set $L \subset K$, we would have generators for the ideals $N^\#, L^\#$ (resp. $N^{\#\#}, L^{\#\#}$). Working out whether or not $L^\# = N^\#$ (resp. $N^{\#\#} = L^{\#\#}$)is then purely a problem in commutative ring theory. If then $L^\# \neq N^\#$ (or $N^{\#\#} \neq L^{\#\#}$), we may conclude that $L$ does not normally generate $K$.

In §4 we will show in general how to compute $\kappa[G]^\#$ and $B$, from a presentation of $G$. However to do this we first need to build up a collection of identities which hold in $A_G$. We will now drop the square parentheses which we have used to distinguish elements of $\kappa[G]$ and elements of $A_G$. Thus from now on, given $x \in \kappa[G]$ it will be understood that $x$ may also denote $[x] \in A_G$ depending on context.

By Lemma 2.4, we know that if $x \in \kappa[G]^\#$ then $x = \bar{x}$, and if $y \in \Lambda_G$ then $y = \vec{y}$ (noting dropped parentheses). Conversely for all $x \in A_G$ we have $\bar{x} \in \kappa[G]^\#$, $\vec{x} \in \Lambda_G$. So we may denote a general element of $\kappa[G]^\#$ by $\bar{x}$ and a general element of $\Lambda_G$ by $\vec{x}$.

**Lemma 3.1.** *Given $\vec{x}, \vec{y} \in \Lambda_G$ we have, $\vec{x}\vec{y} + \vec{y}\vec{x} \in \kappa[G]^\#$, $\vec{x}\vec{y} - \vec{y}\vec{x} \in \Lambda_G$.*

*Proof.* We need only note that $(\vec{x}\vec{y})^* = \vec{y}^*\vec{x}^* = \vec{y}\vec{x}$ and similarly $(\vec{y}\vec{x})^* = \vec{x}\vec{y}$. $\square$

**Definition 3.2.** *We define a dot product $\Lambda_G \times \Lambda_G \to \kappa[G]^\#$ and bracket $\Lambda_G \times \Lambda_G \to \Lambda_G$:*

$$\vec{x} \cdot \vec{y} = -\frac{1}{2}(\vec{x}\vec{y} + \vec{y}\vec{x}), \qquad [\vec{x}, \vec{y}] = \frac{1}{2}(\vec{x}\vec{y} - \vec{y}\vec{x}).$$

**Lemma 3.3.** *For $\vec{x}, \vec{y}, \vec{z} \in \Lambda_G$ we have:*
*i)*   $\vec{x} \cdot \vec{y} = -\frac{1}{2}(\overline{xy} - \overline{xy^*}) = \bar{x}\bar{y} - \overline{xy}$,
*ii)*   $[\vec{x}, \vec{y}] = \frac{1}{2}(xy - yx)$ (so in particular $xy - yx \in \Lambda_G$),
*iii)*   $[\vec{x}, \vec{y}] \cdot \vec{z} = -\frac{1}{2}(\overline{xyz} - \overline{zyx})$.

*Proof.* i) We have

$$\vec{x} \cdot \vec{y} = -\frac{1}{8}\left((x - x^*)(y - y^*) + (y - y^*)(x - x^*)\right)$$

$$= -\frac{1}{4}(\overline{xy} + \overline{yx} - \overline{xy^*} - \overline{y^*x}) = -\frac{1}{2}(\overline{xy} - \overline{xy^*}).$$

using Lemma 2.7i. Then Lemma 2.7ii gives:

$$-\frac{1}{2}(\overline{xy} - \overline{xy^*}) = -\frac{1}{2}(2\overline{xy} - 2\overline{x}\overline{y}) = \overline{x}\overline{y} - \overline{xy}.$$

ii) As $\bar{x}$, $\bar{y}$ are central in $A_G$, we have:

$$\vec{x}\vec{y} - \vec{y}\vec{x} = (x - \bar{x})(y - \bar{y}) - (y - \bar{y})(x - \bar{x}) = xy - yx.$$

iii) From (i) and (ii) we know that:

$$[\vec{x}, \vec{y}] \cdot \vec{z} = -\frac{1}{4}\overline{((xy - yx)z)} - \overline{(xy - yx)z^*}).$$

Also from (ii) we know that $(xy - yx)^* = yx - xy$, so by Lemma 2.7iii:

$$[\vec{x}, \vec{y}] \cdot \vec{z} = -\frac{1}{4}(\overline{((xy - yx)z)} - \overline{z(yx - xy)}) = -\frac{1}{2}(\overline{xyz} - \overline{zyx}).$$

<div style="text-align: right;">□</div>

Recall Defintion 2.17. Let $B$ be a generating set for the module $\Lambda_G$ over the ring $\kappa[G]^{\#}$. From Lemma 3.3i it immediately follows that:

**Corollary 3.4.** *Given a set $L \subset G$, we have the ideal $L^{\#\#} \lhd \kappa[G]^{\#}$ generated by* $\{\vec{b} \cdot \vec{l} \mid \vec{b} \in B,\ l \in L\}.$

Recall from Lemma 2.5 that $\Lambda_G$ is a module over $\kappa[G]^{\#}$.

**Lemma 3.5.** *i) The dot product and the bracket are bilinear maps over $\kappa[G]^{\#}$.*
*ii) The dot product is symmetric and the bracket is skew-symmetric.*
*iii) The bracket obeys the Jacobi identity:* $[[\vec{x}, \vec{y}], \vec{z}] + [[\vec{y}, \vec{z}], \vec{x}] + [[\vec{z}, \vec{x}], \vec{y}] = 0.$
*iv) The scalar triple product $(\vec{x}, \vec{y}, \vec{z}) \mapsto [\vec{x}, \vec{y}] \cdot \vec{z}$, is an alternating trilinear map.*
*v) The triple bracket may be expanded as follows:*

$$[[\vec{x}, \vec{y}], \vec{z}] = (\vec{x} \cdot \vec{z})\vec{y} - (\vec{y} \cdot \vec{z})\vec{x}.$$

*Proof.* i) This follows from the centrality of $\kappa[G]^{\#}$ in $A_G$.
ii) This is immediate from the definitions.
iii) This follows from the form of the definition and may be verified by calculation.
iv) Consider the form of the scalar triple product given by Lemma 3.3iii. If any pair of $\vec{x}, \vec{y}, \vec{z}$ are equal then applying Lemma 2.7i if necessary, we get $[\vec{x}, \vec{y}] \cdot \vec{z} = 0$.

v) We have

$$[[\vec{x}, \vec{y}], \vec{z}] = \frac{1}{4}\left(\vec{x}\vec{y}\vec{z} - \vec{y}\vec{x}\vec{z} - \vec{z}\vec{x}\vec{y} + \vec{z}\vec{y}\vec{x}\right).$$

On the other hand:

$$(\vec{x} \cdot \vec{z})\vec{y} - (\vec{y} \cdot \vec{z})\vec{x} = -\frac{1}{2}((\vec{x}\vec{z} + \vec{z}\vec{x})\vec{y} - \vec{x}(\vec{y}\vec{z} + \vec{z}\vec{y})) = \frac{1}{2}(\vec{x}\vec{y}\vec{z} - \vec{z}\vec{x}\vec{y}).$$

Thus taking the difference gives:

$$[[\vec{x}, \vec{y}], \vec{z}] - ((\vec{x} \cdot \vec{z})\vec{y} - (\vec{y} \cdot \vec{z})\vec{x}) = \frac{1}{4}\left(-(\vec{x}\vec{y} + \vec{y}\vec{x})\vec{z} + \vec{z}(\vec{x}\vec{y} + \vec{y}\vec{x})\right) = 0,$$

as by Lemma 3.1 we have $\vec{x}\vec{y} + \vec{y}\vec{x} \in \kappa[G]^{\#}$ central.

$\square$

**Corollary 3.6.** *We may deduce that given $\vec{x}, \vec{y}, \vec{z}, \vec{w} \in \Lambda_G$ we have*:
*i)*  $[\vec{x}, \vec{y}] \cdot \vec{z} = [\vec{y}, \vec{z}] \cdot \vec{x} = [\vec{z}, \vec{x}] \cdot \vec{y}.$
*ii)*  $[\vec{x}, \vec{y}] \cdot [\vec{z}, \vec{w}] = (\vec{x} \cdot \vec{z})(\vec{y} \cdot \vec{w}) - (\vec{x} \cdot \vec{w})(\vec{y} \cdot \vec{z}).$
*iii)* $[[\vec{x}, \vec{y}], [\vec{z}, \vec{w}]] = ([\vec{x}, \vec{z}] \cdot \vec{w})\vec{y} - ([\vec{y}, \vec{z}] \cdot \vec{w})\vec{x}$
   $\qquad\qquad\qquad = -([\vec{x}, \vec{y}] \cdot \vec{z})\vec{w} + ([\vec{x}, \vec{y}] \cdot \vec{w})\vec{z}\ .$
*iv)* $([\vec{x}, \vec{y}] \cdot \vec{z})\vec{w} = (\vec{x} \cdot \vec{w})[\vec{y}, \vec{z}] - (\vec{y} \cdot \vec{w})[\vec{x}, \vec{z}] + (\vec{z} \cdot \vec{w})[\vec{x}, \vec{y}].$
*v)*  $[[\vec{x}, \vec{y}], [\vec{z}, \vec{w}]] = (\vec{x} \cdot \vec{z})[\vec{y}, \vec{w}] + (\vec{y} \cdot \vec{w})[\vec{x}, \vec{z}] - (\vec{x} \cdot \vec{w})[\vec{y}, \vec{z}] - (\vec{y} \cdot \vec{z})[\vec{x}, \vec{w}].$

*Proof.* i) As 3-cycles are even permutations, this follows from Lemma 3.5iv.

ii) From (i) we have $[\vec{x}, \vec{y}] \cdot [\vec{z}, \vec{w}] = [[\vec{z}, \vec{w}], \vec{x}] \cdot \vec{y}$. Then Lemma 3.5v gives

$$[[\vec{z}, \vec{w}], \vec{x}] \cdot \vec{y} = ((\vec{z} \cdot \vec{x})\vec{w} - (\vec{w} \cdot \vec{x})\vec{z}) \cdot \vec{y} = (\vec{x} \cdot \vec{z})(\vec{y} \cdot \vec{w}) - (\vec{x} \cdot \vec{w})(\vec{y} \cdot \vec{z}).$$

iii) We expand using Lemma 3.5v, taking $[\vec{z}, \vec{w}]$ as an input to get the first identity, and $[\vec{x}, \vec{y}]$ as an input to get the second.

iv) We use Lemma 3.5v to expand the quadruple product $[[[\vec{x}, \vec{y}], \vec{w}], \vec{z}]$ in two ways:

$$[[[\vec{x}, \vec{y}], \vec{w}], \vec{z}] = ([\vec{x}, \vec{y}] \cdot \vec{z})\vec{w} - (\vec{z} \cdot \vec{w})[\vec{x}, \vec{y}],$$
$$[[[\vec{x}, \vec{y}], \vec{w}], \vec{z}] = (\vec{x} \cdot \vec{w})[\vec{y}, \vec{z}] - (\vec{y} \cdot \vec{w})[\vec{x}, \vec{z}].$$

Equating the two yields the result.

v) From (iii) we have $[[\vec{x}, \vec{y}], [\vec{z}, \vec{w}]] = -([\vec{x}, \vec{y}] \cdot \vec{z})\vec{w} + ([\vec{x}, \vec{y}] \cdot \vec{w})\vec{z}\ .$ We may then use (iv) to substitute in for the expressions $([\vec{x}, \vec{y}] \cdot \vec{z})\vec{w}$ and $([\vec{x}, \vec{y}] \cdot \vec{w})\vec{z}.$      $\square$

We can recover multiplication in $A_G$ from the module structure of $\Lambda_G$ over the ring $\kappa[G]^{\#}$, together with the dot product and bracket:

**Lemma 3.7.** *Given $x, y \in A_G$ we may express their product in the following terms*:

$$xy = \bar{x}\bar{y} - \vec{x} \cdot \vec{y} + \bar{x}\vec{y} + \bar{y}\vec{x} + [\vec{x}, \vec{y}]$$

*Thus in particular $\overline{xy} = \bar{x}\bar{y} - \vec{x} \cdot \vec{y}$ and $\overrightarrow{xy} = \bar{x}\vec{y} + \bar{y}\vec{x} + [\vec{x}, \vec{y}]$.*

*Proof.* We have

$$xy \;=\; (\bar{x} + \vec{x})(\bar{y} + \vec{y}) \;=\; \bar{x}\bar{y} + \vec{x}\vec{y} + \bar{x}\vec{y} + \bar{y}\vec{x} \;=\; \bar{x}\bar{y} - \vec{x} \cdot \vec{y} + \bar{x}\vec{y} + \bar{y}\vec{x} + [\vec{x}, \vec{y}].$$

To get the expressions for $\overline{xy}$ and $\overrightarrow{xy}$, note that $xy = \overline{xy} + \overrightarrow{xy}$, and by Lemma 2.3 this is the unique decomposition as a sum of an element of $\kappa[G]^{\#}$ and an element of $\Lambda_G$.

$\square$

**Lemma 3.8.** *For $\vec{x}, \vec{y}, \vec{z}, \vec{w} \in \Lambda_G$ we may expand the following products in $A_G$:*
*i)*  $\vec{x}\vec{y} = -\vec{x} \cdot \vec{y} + [\vec{x}, \vec{y}],$
*ii)* $[\vec{x}, \vec{y}]\vec{z} = -[\vec{x}, \vec{y}] \cdot \vec{z} + (\vec{x} \cdot \vec{z})\vec{y} - (\vec{y} \cdot \vec{z})\vec{x},$
$\quad\; \vec{z}[\vec{x}, \vec{y}] = -[\vec{x}, \vec{y}] \cdot \vec{z} - (\vec{x} \cdot \vec{z})\vec{y} + (\vec{y} \cdot \vec{z})\vec{x},$

*iii)* $[\vec{x}, \vec{y}][\vec{z}, \vec{w}] = -(\vec{x} \cdot \vec{z})(\vec{y} \cdot \vec{w}) + (\vec{x} \cdot \vec{w})(\vec{y} \cdot \vec{z}) + ([\vec{x}, \vec{z}] \cdot \vec{w})\vec{y} - ([\vec{y}, \vec{z}] \cdot \vec{w})\vec{x}$
$\qquad\qquad\qquad = -(\vec{x} \cdot \vec{z})(\vec{y} \cdot \vec{w}) + (\vec{x} \cdot \vec{w})(\vec{y} \cdot \vec{z}) - ([\vec{x}, \vec{y}] \cdot \vec{z})\vec{w} + ([\vec{x}, \vec{y}] \cdot \vec{w})\vec{z}.$

*Proof.* i) This follows immediately from Definition 3.2.
ii) By Lemma 3.7 the products may be written:

$$[\vec{x}, \vec{y}]\vec{z} = -[\vec{x}, \vec{y}] \cdot \vec{z} + [[\vec{x}, \vec{y}], \vec{z}], \qquad \vec{z}[\vec{x}, \vec{y}] = -[\vec{x}, \vec{y}] \cdot \vec{z} - [[\vec{x}, \vec{y}], \vec{z}].$$

The triple bracket may then be expanded by Lemma 3.5v to give the result.

iii) From Lemma 3.7 we have

$$[\vec{x}, \vec{y}][\vec{z}, \vec{w}] = -[\vec{x}, \vec{y}] \cdot [\vec{z}, \vec{w}] + [[\vec{x}, \vec{y}], [\vec{z}, \vec{w}]].$$

We then expand $[\vec{x}, \vec{y}] \cdot [\vec{z}, \vec{w}]$ by Corollary 3.6ii and $[[\vec{x}, \vec{y}], [\vec{z}, \vec{w}]]$ by Corollary 3.6iii.
$\hfill\square$

Expanding products in $A_G$ can yield identities in $\kappa[G]^{\#}$:

**Lemma 3.9.** *For $x, y, z \in A_G$ we have $\frac{1}{2}(\overline{xyz} + \overline{zyx}) = \overline{xy}\,\bar{z} + \overline{xz}\,\bar{y} + \overline{yz}\,\bar{x} - 2\bar{x}\,\bar{y}\,\bar{z}.$*

*Proof.* By Lemma 3.7 we have

$$\overline{xyz} + \overrightarrow{xyz} = xyz = (\bar{x}\bar{y} - \vec{x} \cdot \vec{y} + \bar{x}\vec{y} + \bar{y}\vec{x} + [\vec{x}, \vec{y}])(\bar{z} + \vec{z}).$$

Equating components in $\kappa[G]^{\#}$, we get

$$\overline{xyz} = \bar{x}\,\bar{y}\,\bar{z} - (\vec{x} \cdot \vec{y})\bar{z} - (\vec{y} \cdot \vec{z})\bar{x} - (\vec{x} \cdot \vec{z})\bar{y} - [\vec{x}, \vec{y}]) \cdot \vec{z}.$$

Only the last term changes sign when $x$ and $z$ are swapped, so

$$\frac{1}{2}(\overline{xyz} + \overline{zyx}) = \bar{x}\,\bar{y}\,\bar{z} - (\vec{x} \cdot \vec{y})\bar{z} - (\vec{y} \cdot \vec{z})\bar{x} - (\vec{x} \cdot \vec{z})\bar{y}.$$

Finally, we may use Lemma 3.3i to substitute in expressions for the dot products.
$\hfill\square$

**Lemma 3.10.** *Given $\vec{x}, \vec{y}, \vec{z}, \vec{u}, \vec{v}, \vec{w} \in \Lambda_G$, we have the following identities in $\kappa[G]^{\#}$:*
*i)*

$$([\vec{y}, \vec{z}] \cdot \vec{w})(\vec{x} \cdot \vec{u}) - ([\vec{x}, \vec{z}] \cdot \vec{w})(\vec{y} \cdot \vec{u}) + ([\vec{x}, \vec{y}] \cdot \vec{w})(\vec{z} \cdot \vec{u}) - ([\vec{x}, \vec{y}] \cdot \vec{z})(\vec{w} \cdot \vec{u}) = 0.$$

*ii)*

$$([\vec{x}, \vec{y}] \cdot \vec{z})([\vec{u}, \vec{v}] \cdot \vec{w}) = \begin{vmatrix} \vec{x} \cdot \vec{u} & \vec{x} \cdot \vec{v} & \vec{x} \cdot \vec{w} \\ \vec{y} \cdot \vec{u} & \vec{y} \cdot \vec{v} & \vec{y} \cdot \vec{w} \\ \vec{z} \cdot \vec{u} & \vec{z} \cdot \vec{v} & \vec{z} \cdot \vec{w} \end{vmatrix}.$$

*Proof.* i) From Corollary 3.6iii we know

$$([\vec{y}, \vec{z}] \cdot \vec{w})\vec{x} - ([\vec{x}, \vec{z}] \cdot \vec{w})\vec{y} + ([\vec{x}, \vec{y}] \cdot \vec{w})\vec{z} - ([\vec{x}, \vec{y}] \cdot \vec{z})\vec{w} = 0.$$

We then take the dot product of both sides with $\vec{u}$ to obtain the result.

ii) By Corollary 3.6ii we have

$$[[\vec{x}, \vec{y}], \vec{w}] \cdot [[\vec{u}, \vec{v}], \vec{z}] \;=\; ([\vec{x}, \vec{y}] \cdot [\vec{u}, \vec{v}])(\vec{z} \cdot \vec{w}) - ([\vec{x}, \vec{y}] \cdot \vec{z})([\vec{u}, \vec{v}] \cdot \vec{w}). \tag{1}$$

From Lemma 3.5v we have

$$[[\vec{x}, \vec{y}], \vec{w}] \;=\; (\vec{x} \cdot \vec{w})\vec{y} - (\vec{y} \cdot \vec{w})\vec{x} \qquad \text{and} \qquad [[\vec{u}, \vec{v}], \vec{z}] \;=\; (\vec{u} \cdot \vec{z})\vec{v} - (\vec{v} \cdot \vec{z})\vec{u}.$$

Also by Corollary 3.6ii we have

$$([\vec{x}, \vec{y}] \cdot [\vec{u}, \vec{v}]) \;=\; (\vec{x} \cdot \vec{u})(\vec{y} \cdot \vec{v}) - (\vec{x} \cdot \vec{v})(\vec{y} \cdot \vec{u}).$$

Substituting these three expressions into (1) and rearranging gives:

$$([\vec{x}, \vec{y}] \cdot \vec{z})([\vec{u}, \vec{v}] \cdot \vec{w}) \;=\; \left( (\vec{x} \cdot \vec{u})(\vec{y} \cdot \vec{v}) - (\vec{x} \cdot \vec{v})(\vec{y} \cdot \vec{u}) \right)(\vec{z} \cdot \vec{w})$$
$$- \left( (\vec{x} \cdot \vec{w})\vec{y} - (\vec{y} \cdot \vec{w})\vec{x} \right) \cdot \left( (\vec{u} \cdot \vec{z})\vec{v} - (\vec{v} \cdot \vec{z})\vec{u} \right)$$

Multiplying out the dot product then gives the result. $\qquad\square$

This lemma will be sufficient for describing the ring structure of $\kappa[G]^{\#}$ in §4. We note one further identity, this time between dot products only:

**Corollary 3.11.** *Let $\vec{x}, \vec{y}, \vec{z}, \vec{w}, \vec{u}, \vec{v}, \vec{s}, \vec{t} \in \Lambda_G$. We have:*

$$\begin{vmatrix} \vec{x} \cdot \vec{u} & \vec{x} \cdot \vec{v} & \vec{x} \cdot \vec{s} & \vec{x} \cdot \vec{t} \\ \vec{y} \cdot \vec{u} & \vec{y} \cdot \vec{v} & \vec{y} \cdot \vec{s} & \vec{y} \cdot \vec{t} \\ \vec{z} \cdot \vec{u} & \vec{z} \cdot \vec{v} & \vec{z} \cdot \vec{s} & \vec{z} \cdot \vec{t} \\ \vec{w} \cdot \vec{u} & \vec{w} \cdot \vec{v} & \vec{w} \cdot \vec{s} & \vec{w} \cdot \vec{t} \end{vmatrix} = 0.$$

*Proof.* We expand the determinant along the top row, using Lemma 3.10ii to express the minors:

$$\left( [\vec{y}, \vec{z}] \cdot \vec{w} \right)\left( ([\vec{v}, \vec{s}] \cdot \vec{t})(\vec{u} \cdot \vec{x}) - ([\vec{u}, \vec{s}] \cdot \vec{t})(\vec{v} \cdot \vec{x}) + ([\vec{u}, \vec{v}] \cdot \vec{t})(\vec{s} \cdot \vec{x}) - ([\vec{u}, \vec{v}] \cdot \vec{s})(\vec{t} \cdot \vec{x}) \right)$$

Lemma 3.10i then implies that the second factor here is 0. $\qquad\square$

We finish this section with some identities relating to powers and commutators of group elements.

**Definition 3.12.** *For $n \in \mathbb{Z}$ let $P_n$ be the polynomial over $\kappa$ determined by:*

$$P_0 = 0, \qquad P_1 = 1, \qquad 2x P_n(x) = P_{n-1}(x) + P_{n+1}(x).$$

We may break down powers of group elements using Lemma 2.7ii:

**Lemma 3.13.** *Given $g, h, k \in G$ we have $\overline{gh^n k} = \overline{ghk} P_n(\bar{h}) - \overline{gk} P_{n-1}(\bar{h})$.*

*Proof.* The cases $n = 0, 1$ follow from $P_{-1} = -1, P_0 = 0, P_1 = 1$. For $r \in \mathbb{Z}$ we have

$$
\begin{array}{rcl}
\overline{gh^{r-1}k} & = & 2\bar{h}\overline{gh^r k} - \overline{gh^{r+1}k}, \\
\overline{gh^{r+2}k} & = & 2\bar{h}\overline{gh^{r+1}k} - \overline{gh^r k},
\end{array}
$$

by Lemma 2.7ii. Thus if the statement of the lemma holds for $n = r, r+1$, then it also holds for $n = r-1, r+2$ and we are done by induction. $\qquad\square$

**Lemma 3.14.** *Given $g, h \in G$ we have $\overline{gh^n} - \overline{gh^{-n}} = (\overline{gh} - \overline{gh^{-1}}) P_n(\bar{h})$.*

*Proof.* Apply Lemma 3.13 with $k = e$ to get: $\overline{gh^n} - \overline{gh^{-n}} =$

$$
(\overline{gh} P_n(\bar{h}) - \bar{g} P_{n-1}(\bar{h})) - (\overline{gh^{-1}} P_n(\bar{h}) - \bar{g} P_{n-1}(\bar{h})) = (\overline{gh} - \overline{gh^{-1}}) P_n(\bar{h}).
$$

$\qquad\square$

**Corollary 3.15.** *Given $h \in G$ the ideal $\{h^n\}^{\#\#} \lhd \kappa[G]^{\#}$ is contained in the ideal generated by $P_n(\bar{h})$.*

This will be important when we consider free products of cyclic groups in Sections 5 and 6, as they may be expressed as free groups, quotiented out by the normal subgroup generated by a power of each generator.

Let $a, b \in G$ and let $I \lhd \kappa[G]^{\#}$ be the ideal generated by scalar triple products $\{[\vec{a}, \vec{b}] \cdot \vec{c} \mid \vec{c} \in \Lambda_G\}$. The following lemma shows that if $x, y \in G$ map to the same group element when the relation that $a$ commutes with $b$ is added, then $\bar{x} - \bar{y} \in I$.

**Lemma 3.16.** *We have an equality of ideals: $\{a^{-1}b^{-1}ab\}^{\#} = I$.*

*Proof.* Given $\vec{c} \in \Lambda_G$, Lemma 3.3iii gives:

$$
[\vec{a}, \vec{b}] \cdot \vec{c} = -\frac{1}{2}(\overline{cab} - \overline{cba}) = -\frac{1}{2}\left(\overline{cba(a^{-1}b^{-1}ab)} - \overline{cba}\right) \in \{a^{-1}b^{-1}ab\}^{\#}.
$$

Thus $I \subset \{a^{-1}b^{-1}ab\}^{\#}$. Conversely, given $c \in A_G$, Lemma 3.3iii gives:

$$
-\frac{1}{2}\left(\overline{c(a^{-1}b^{-1}ab)} - \bar{c}\right) = -\frac{1}{2}\left(\overline{(ca^{-1}b^{-1})ab} - \overline{(ca^{-1}b^{-1})ba}\right) = [\vec{a}, \vec{b}] \cdot \overrightarrow{(ca^{-1}b^{-1})} \in I.
$$

Thus $\{a^{-1}b^{-1}ab\}^{\#} \subset I$. $\qquad\square$

**Lemma 3.17.** *i) We have: $[\vec{a}, \vec{b}] \cdot [\vec{a}, \vec{b}] = (\vec{a} \cdot \vec{a})(\vec{b} \cdot \vec{b}) - (\vec{a} \cdot \vec{b})^2$.*
*ii) Commutators in $\kappa[G]^{\#}$ break down as follows:*

$$
\overline{aba^{-1}b^{-1}} = 2\overline{ab}^2 - 4\bar{a}\overline{ab}\bar{b} + 2\bar{a}^2 + 2\bar{b}^2 - 1.
$$

*Proof.* i) This follows immediately from Corollary 3.6ii.

ii) Lemma 3.7 yields an expression for $\overrightarrow{ba}$. Noting that $[\vec{a}, \vec{b}] \cdot \vec{a} = [\vec{a}, \vec{b}] \cdot \vec{b} = 0$ by Lemma 3.5iv, this gives: $[\vec{a}, \vec{b}] \cdot [\vec{a}, \vec{b}] = -[\vec{a}, \vec{b}] \cdot \overrightarrow{ba} = [\vec{a}, \vec{b}] \cdot \overrightarrow{(a^{-1}b^{-1})}$.

Thus Lemma 3.3iii gives

$$[\vec{a}, \vec{b}] \cdot [\vec{a}, \vec{b}] = [\vec{a}, \vec{b}] \cdot \overrightarrow{(a^{-1}b^{-1})} = -\frac{1}{2}(\overline{aba^{-1}b^{-1}} - 1).$$

Thus from (i):

$$\overline{aba^{-1}b^{-1}} = 1 - 2([\vec{a}, \vec{b}] \cdot [\vec{a}, \vec{b}]) = 1 - 2((\vec{a} \cdot \vec{a})(\vec{b} \cdot \vec{b}) - (\vec{a} \cdot \vec{b})^2).$$

We complete the proof by substituting in the identities:

$$\vec{a} \cdot \vec{a} = -(\vec{a} \cdot \overrightarrow{a^{-1}}) = 1 - \bar{a}^2, \qquad \vec{b} \cdot \vec{b} = 1 - \bar{b}^2, \qquad \vec{a} \cdot \vec{b} = \bar{a}\bar{b} - \overline{ab},$$

which all follow from Lemma 3.3i.                                    □

# 4   A complete description of $\kappa[G]^{\#}$

By a complete description of $\kappa[G]^{\#}$ we mean a set of elements which generate $\kappa[G]^{\#}$ as a ring over $\kappa$, together with a defining set of relations which those generators satisfy.

Suppose that $K$ is a normal subgroup of $G$ with $G/K \cong H$, and suppose that $L \subset K$ normally generates $K$ in $G$. By Theorem 2.16 we know that if we have a complete description of $\kappa[G]^{\#}$ and a generating set for $A_G$ over $\kappa[G]^{\#}$, then we also have a complete description of $\kappa[H]^{\#} = \kappa[G]^{\#}/L^{\#}$. We merely need to add the generating set for $L^{\#}$ (from Definition 2.14) to the set of relations describing $\kappa[G]^{\#}$.

Given an indexing set $I$, for each $i \in I$, let $g_i \in F_I$ denote the corresponding letter in the free group on $I$. Let $L = \{r_j \in F_I | j \in J\}$, for some indexing set $J$ and elements $r_J \in J$. As before let $K \lhd G$ be the normal closure of $L$.

**Definition 4.1.** *A presentation of $G$ is a pair of lists: $\langle g_i, i \in I | r_j, j \in J \rangle$, together with a group isomorphism $F_I/K \cong G$ (with $L, K$ defined as above).*

We now fix a presentation $\langle g_i, i \in I | r_j, j \in J \rangle$ of a group $G$ with $K, L$ as before. Elements of $F_I$ may be regarded as elements of $G$, via the isomorphism $F_I/K \cong G$. We will make clear which of these we mean from context.

The purpose of this section is to produce a complete description of $\kappa[G]^{\#}$ from this data. From the discussion above we only need a complete description of $\kappa[F_I]^{\#}$ and a generating set for $A_{F_I}$ as a module over $\kappa[F_I]^{\#}$. Then, using $\kappa[G]^{\#} \cong \kappa[F_I]^{\#}/L^{\#}$, we have a complete description of $\kappa[G]^{\#}$.

If the indexing set $I$ is finite, then we will show that we only require a finite number of generators for $\kappa[G]^{\#}$ as a ring over $\kappa$. Further, if $J$ is also finite, then our description of $\kappa[G]^{\#}$ will only have a finite number of relations.

We begin by defining an abstract ring $R_I$ which we will later identify with $\kappa[F_I]^{\#}$. Let $R_I$ denote the quotient of the polynomial ring $\kappa[\lambda_i, m_{ij}, w_{ijk} | i, j, k \in I]$ by the following relations for $i, j, k, l, s, t \in I$:

R1:     $m_{ij} = m_{ji}, \quad w_{ijk} = w_{kij}, \quad w_{ijk} = -w_{kji}$
R2:     $m_{ii} = 1 - \lambda_i^2$
R3:     $w_{jkl}m_{is} - w_{ikl}m_{js} + w_{ijl}m_{ks} - w_{ijk}m_{ls} = 0$

R4:     $w_{ijk}w_{lst} = \begin{vmatrix} m_{il} & m_{is} & m_{it} \\ m_{jl} & m_{js} & m_{jt} \\ m_{kl} & m_{ks} & m_{kt} \end{vmatrix}$

We define a ring homomorphism $\phi\colon R_I \to \kappa[G]^{\#}$ by:

$$\phi\colon \quad \begin{aligned} \lambda_i &\mapsto & \bar{g}_i, & \qquad i \in I, \\ m_{ij} &\mapsto & \vec{g}_i \cdot \vec{g}_j, & \qquad i, j \in I, \\ w_{ijk} &\mapsto & [\vec{g}_i, \vec{g}_j] \cdot \vec{g}_k, & \qquad i, j, k \in I. \end{aligned}$$

**Lemma 4.2.** *The ring homomorphism $\phi$ is well defined.*

*Proof.* We must check that the relations R1, R2, R3, R4 are respected by $\phi$. This is the case for R1 by Lemma 3.5ii, Lemma 3.5iv and Corollary 3.6i.

It is also the case for R2 as by Lemma 3.3i we have

$$\phi(m_{ii}) = \vec{g}_i \cdot \vec{g}_i = -\vec{g}_i \cdot \vec{g}_i^{\,-1} = 1 - \bar{g}_i^{\,2} = \phi(1 - \lambda_i^2).$$

Lemma 3.10i implies $\phi$ respects R3 and Lemma 3.10ii implies $\phi$ respects R4.  □

Let $B$ denote the set: $\{1\} \cup \{\vec{g}_i \,|\, i \in I\} \cup \{[\vec{g}_i, \vec{g}_j] \,|\, i, j \in I\} \subset A_G$.

**Lemma 4.3.** *$\phi$ is surjective and $B$ is a generating set for $A_G$ as a module over $\kappa[G]^{\#}$.*

*Proof.* We will show that any element of $A_G$ is a linear combination of elements of $B$ over $\phi(R_I)$. Then given $x \in \kappa[G]^{\#}$ we will have $x = 1\phi(\alpha) + y$, for some $\alpha \in R_I, y \in \Lambda_G$. By Lemma 2.3 $y = 0$ and $x = \phi(\alpha)$ so we conclude $\phi$ is surjective.

Let $\langle B \rangle \phi(R_I)$ denote the set of linear combinations of $B$ over $\phi(R_I)$. Clearly $\langle B \rangle \phi(R_I)$ is a vector space over $\kappa$. For $i \in I$ we have $g_i, g_i^{-1} \in \langle B \rangle \phi(R_I)$ as

$$g_i = 1\phi(\lambda_i) + \vec{g}_i, \qquad g_i^{-1} = 1\phi(\lambda_i) - \vec{g}_i.$$

Further, by Lemma 3.8 we know $\langle B \rangle \phi(R_I)$ is closed under multiplication.  □

Thus we have an explicit generating set $B$ for $A_G$ as a module over $\kappa[G]^{\#}$. Note that if $I$ is finite, then $B$ is also a finite set. Further, given any finite set $S \subset G$, the ideal $S^{\#}$ is then generated by a finite set (given in Definition 2.14).

Also, if $I$ is finite then $R_I$ is a finitely generated commutative ring over $\kappa$ and hence Noetherian. By Lemma 4.3 $\kappa[G]^{\#}$ is a quotient of $R_I$, so we also have that $\kappa[G]^{\#}$ is a Noetherian ring, finitely generated over $\kappa$. This is a stark contrast with the usual group ring, which need not be Noetherian for a finitely generated group.

Let $C \subset \{g_i g_j \,|\, i, j \in I\}$ satisfy that for all $i, j \in I$, either $g_i g_j \in C$ or $g_j g_i \in C$. Let $B' = \{1\} \cup \{g_i \,|\, i \in I\} \cup C \subset A_G$. This can be a convenient alternative to $B$:

**Lemma 4.4.** *$B'$ is also a generating set for $A_G$ as a module over $\kappa[G]^{\#}$.*

*Proof.* For $i, j \in I$ we have $\vec{g}_i = -1\bar{g}_i + g_i$. By Lemma 3.7,

$$\begin{aligned} [\vec{g}_i, \vec{g}_j] &= & 1(\vec{g}_i \cdot \vec{g}_j - \bar{g}_i \bar{g}_j) + g_i g_j - \vec{g}_i \bar{g}_j - \vec{g}_j \bar{g}_i \\ &= & -1(\vec{g}_i \cdot \vec{g}_j - \bar{g}_i \bar{g}_j) - g_j g_i + \vec{g}_i \bar{g}_j + \vec{g}_j \bar{g}_i. \end{aligned}$$

Hence the span of $B'$ contains $B$, which (by Lemma 4.3) generates $A_G$.  □

We have sets:

$$\begin{aligned} \widehat{B} &= & \{1\} \cup \{\vec{g}_i \,|\, i \in I\} \cup \{[\vec{g}_i, \vec{g}_j] \,|\, i, j \in I\} \subset A_{F_I}, \\ \widehat{B'} &= & \{1\} \cup \{g_i \,|\, i \in I\} \cup \widehat{C} \subset A_{F_I}, \end{aligned}$$

where $\widehat{C} \subset \{g_i g_j \,|\, i, j \in I\} \subset A_{F_I}$ satisfies that for all $i, j \in I$, either $g_i g_j \in \widehat{C}$ or $g_j g_i \in \widehat{C}$. (Note that here we are no longer identifying the $g_i$ with their images in $G$).

Taking Lemma 4.2 with $J = \phi$ gives a ring homomorphism $\hat{\phi} \colon R_I \to \kappa[F_I]^{\#}$:

$$
\hat{\phi} \colon \quad
\begin{aligned}
\lambda_i &\mapsto \bar{g}_i, & i \in I, \\
m_{ij} &\mapsto \vec{g}_i \cdot \vec{g}_j, & i, j \in I, \\
w_{ijk} &\mapsto [\vec{g}_i, \vec{g}_j] \cdot \vec{g}_k, & i, j, k \in I.
\end{aligned}
$$

Taking the $J = \emptyset$ case of Lemma 4.3 and Lemma 4.4 we get:

**Lemma 4.5.** $\hat{\phi}$ *is surjective and* $\widehat{B}, \widehat{B'}$ *generate* $A_{F_I}$ *as a module over* $\kappa[F_I]^{\#}$.

The remainder of this section will be devoted to showing that $\hat{\phi}$ is injective and hence a ring isomorphism. As $R_I$ was defined in terms of generators and relations, we will have a complete description for $\kappa[F_I]^{\#}$. Lemma 4.5 gives generating sets $\widehat{B}, \widehat{B'}$ for $A_{F_I}$ as a $\kappa[F_I]^{\#}$–module. Definition 2.14 provides generating sets for the ideal $L^{\#} \lhd \kappa[F_I]^{\#}$. Thus we will then have a complete description for $\kappa[G]^{\#} \cong \kappa[F_I]^{\#}/L^{\#}$.

In particular if $I$ is a finite set then $R_I$ is finitely generated and our presentation for it has a finite set of generators and relations. Thus once we have proved the injectivity of $\hat{\phi}$, we will have a finite description of $\kappa[F_I]^{\#}$. Further if $I$ is finite then so are $\widehat{B}, \widehat{B'}$. Hence if $J$ is also finite, we will have a finite generating set for the ideal $L^{\#} \lhd \kappa[F_I]^{\#}$ and thus a finite description of $\kappa[G]^{\#}$.

Our strategy in proving that $\hat{\phi} \colon R_I \to \kappa[F_I]^{\#}$ is injective will be to construct another ring homomorphism $\psi \colon \kappa[F_I]^{\#} \to S_I$, where $S_I$ is an algebraic extension of a ring of invariants of $SO_3(\kappa)$. As descriptions of such rings are provided by the fundamental theorems of classical invariant theory, we may then verify that the composition $\psi\hat{\phi} \colon R_I \to S_I$ is injective. Thus we will have shown that $\hat{\phi}$ is injective.

Let $T_I$ be the polynomial ring $\kappa[\mu_i, x_i, y_i, z_i \,|\, i \in I]$, quotiented by the relations:

$$
\mu_i^2 + x_i^2 + y_i^2 + z_i^2 = 1, \qquad \forall i \in I.
$$

Let $H_I = T_I[e_1, e_2, e_3]$, where $e_1, e_2, e_3$ are non-commuting variables satisfying:

$$
e_1{}^2 = e_2{}^2 = e_3{}^2 = e_1 e_2 e_3 = -1.
$$

Note in particular that $e_1 e_2 = -e_2 e_1 = e_3$. Also $H_I$ has a basis $\{1, e_1, e_2, e_3\}$ over $T_I$.

We define a ring homomorphism $\hat{\psi} \colon \kappa[F_I] \to H_I$ by:

$$
\hat{\psi} \colon \quad
\begin{aligned}
g_i &\mapsto \mu_i + x_i e_1 + y_i e_2 + z_i e_3, & i \in I, \\
g_i^{-1} &\mapsto \mu_i - x_i e_1 - y_i e_2 - z_i e_3, & i \in I.
\end{aligned}
$$

**Lemma 4.6.** $\hat{\psi} \colon \kappa[F_I] \to H_I$ *is a well defined ring homomorphism.*

*Proof.* Note that:

$$
\begin{aligned}
\hat{\psi}(g_i)\hat{\psi}(g_i^{-1}) &= (\mu_i + x_i e_1 + y_i e_2 + z_i e_3)(\mu_i - x_i e_1 - y_i e_2 - z_i e_3) = 1, \\
\hat{\psi}(g_i^{-1})\hat{\psi}(g_i) &= (\mu_i - x_i e_1 - y_i e_2 - z_i e_3)(\mu_i + x_i e_1 + y_i e_2 + z_i e_3) = 1.
\end{aligned}
$$

$\square$

**Definition 4.7.** *For any* $q = u + ae_1 + be_2 + ce_3 \in H_I$, *with* $u, a, b, c \in T_I$, *we define its* conjugate *to be* $q^* = u - ae_1 - be_2 - ce_3$.

One may directly verify that for $q_1$, $q_2 \in H_I$, one has $(q_1 q_2)^* = q_2^* q_1^*$.

**Lemma 4.8.** *For $\alpha \in \kappa[F_I]$ we have $\widehat{\psi}(\alpha^*) = (\widehat{\psi}(\alpha))^*$.*

*Proof.* This is true when $\alpha = g_i$ or $\alpha = g_i^{-1}$ for any $i \in I$. Clearly if it is true for $\alpha, \beta \in \kappa[F_I]$ then it is true for any $\kappa$–linear combination of $\alpha$ and $\beta$. It remains to show that it is true for $\alpha\beta$:

$$
\begin{aligned}
(\widehat{\psi}(\alpha\beta))^* &= (\widehat{\psi}(\alpha)\widehat{\psi}(\beta))^* = (\widehat{\psi}(\beta))^*(\widehat{\psi}(\alpha))^* \\
&= \widehat{\psi}(\beta^*)\widehat{\psi}(\alpha^*) = \widehat{\psi}(\beta^*\alpha^*) = \widehat{\psi}((\alpha\beta)^*).
\end{aligned}
$$

$\square$

If $\alpha \in \kappa[F_I]^*$, then

$$
\widehat{\psi}(\alpha) = \widehat{\psi}(\alpha^*) = (\widehat{\psi}(\alpha))^*,
$$

so $\widehat{\psi}(\alpha) \in T_I$ and is central in $H_I$. Thus $\widehat{\psi}$ induces a well defined ring homomorphism:

$$
\widetilde{\psi} \colon A_{F_I} \to H_I.
$$

Let $S_I \subset T_I$ denote the image of $\kappa[F_I]^{\#} \subset A_{F_I}$ under this induced map. Then let

$$
\psi \colon \kappa[F_I]^{\#} \to S_I
$$

denote the restriction of $\widetilde{\psi}$ to $\kappa[F_I]^{\#}$.

For $\alpha, \alpha' \in A_{F_I}$, we may pick $u, u', a, a', b, b', c, c' \in T_I$ such that

$$
\begin{aligned}
\widetilde{\psi}(\alpha) &= u + ae_1 + be_2 + ce_3, \\
\widetilde{\psi}(\alpha') &= u' + a'e_1 + b'e_2 + c'e_3.
\end{aligned}
$$

Then

$$
\begin{aligned}
\psi(\bar{\alpha}) &= \frac{1}{2}\left(\widetilde{\psi}(\alpha) + \widetilde{\psi}(\alpha^*)\right) = \frac{1}{2}\left(\widetilde{\psi}(\alpha) + (\widetilde{\psi}(\alpha))^*\right) = u, \\
\widetilde{\psi}(\vec{\alpha}) &= \frac{1}{2}\left(\widetilde{\psi}(\alpha) - \widetilde{\psi}(\alpha^*)\right) = \frac{1}{2}\left(\widetilde{\psi}(\alpha) - (\widetilde{\psi}(\alpha))^*\right) = ae_1 + be_2 + ce_3.
\end{aligned}
$$

Similarly, $\psi(\bar{\alpha}') = u'$ and $\widetilde{\psi}(\vec{\alpha}') = a'e_1 + b'e_2 + c'e_3$.

**Lemma 4.9.** *Continuing with this notation we have:*
*i)* $\psi(\vec{\alpha} \cdot \vec{\alpha}') = aa' + bb' + cc'$.
*ii)* $\widetilde{\psi}([\vec{\alpha}, \vec{\alpha}']) = (bc' - cb')e_1 - (ac' - ca')e_2 + (ab' - ba')e_3$.

*Proof.* From Definition 3.2 we have:

$$
\begin{aligned}
\psi(\vec{\alpha} \cdot \vec{\alpha}') &= -\tfrac{1}{2}\left(\widetilde{\psi}(\vec{\alpha})\widetilde{\psi}(\vec{\alpha}') + \widetilde{\psi}(\vec{\alpha}')\widetilde{\psi}(\vec{\alpha}')\right) &&= aa' + bb' + cc', \\
\widetilde{\psi}([\vec{\alpha}, \vec{\alpha}']) &= \tfrac{1}{2}\left(\widetilde{\psi}(\vec{\alpha})\widetilde{\psi}(\vec{\alpha}') - \widetilde{\psi}(\vec{\alpha}')\widetilde{\psi}(\vec{\alpha}')\right) &&= \\
&\quad (bc' - cb')e_1 \quad - \quad (ac' - ca')e_2 \quad + \quad (ab' - ba')e_3.
\end{aligned}
$$

$\square$

We now need to show that the composition $\psi\widehat{\phi}\colon R_I \to S_I$ is injective. We know that $\widehat{\phi}$ is surjective. By construction $\psi$ is also surjective. Therefore $S_I$ is generated by the $\psi\widehat{\phi}(\lambda_i)$, $\psi\widehat{\phi}(m_{ij})$, $\psi\widehat{\phi}(w_{ijk})$ over all $i,j,k \in I$. By Lemma 4.9 we have:

$$
\begin{array}{rclccrcl}
\psi\widehat{\phi}(\lambda_i) & = & \psi(\bar{g}_i) & = & \mu_i, & i & \in & I, \\
\psi\widehat{\phi}(m_{ij}) & = & \psi(\vec{g}_i \cdot \vec{g}_j) & = & (x_i x_j + y_i y_j + z_i z_j), & i,j & \in & I, \\
\psi\widehat{\phi}(w_{ijk}) & = & \psi([\vec{g}_i,\vec{g}_j]\cdot\vec{g}_k) & = & \begin{vmatrix} x_i & y_i & z_i \\ x_j & y_j & z_j \\ x_k & y_k & z_k \end{vmatrix}, & i,j,k & \in & I.
\end{array}
$$

Let $V_I \subset S_I$ be the subring generated over $\kappa$ by the $\psi\widehat{\phi}(m_{ij})$ and $\psi\widehat{\phi}(w_{ijk})$. The second fundamental theorem of the invariant theory of $\mathrm{SO}_3(\kappa)$ [18, Chap. II §17] states that the relations between these elements are precisely those implied by R1, R3, R4. Note that the proof in [18, Chap. II §17] is for the case $\kappa = \mathbb{R}$. However the result is clearly independent of the field of characteristic zero, $\kappa$.

From the construction of $T_I$, we have that $S_I$ is a multiple quadratic extension of $V_I$ by the elements $\{\mu_i \,|\, i \in I\}$, where each $\mu_i$ satisfies the relation implied by R2: $\mu_i^2 + \psi\widehat{\phi}(m_{ii}) = 1$.

**Lemma 4.10.** *The relations* R1, R2, R3, R4 *imply all relations between the elements*

$$
\psi\widehat{\phi}(\lambda_i), \qquad \psi\widehat{\phi}(m_{ij}), \qquad \psi\widehat{\phi}(w_{ijk}).
$$

*Proof.* Suppose some polynomial expression in the $\psi\widehat{\phi}(\lambda_i)$, $\psi\widehat{\phi}(m_{ij})$, $\psi\widehat{\phi}(w_{ijk})$ is zero in $S_I$. Under the relation implied by R2, this expression may be written as a $V_I$–linear combination of products of distinct $\psi\widehat{\phi}(\lambda_i)$. As these are linearly independent over $V_I$, each coefficient must be zero as an element of $V_I$ and hence trivial under the relations implied by R1, R3, R4. $\qquad\square$

**Lemma 4.11.** *The composition* $\psi\widehat{\phi}\colon R_I \to S_I$ *is an isomorphism.*

*Proof.* The ring $S_I$ is generated by the $\psi\widehat{\phi}(\lambda_i)$, $\psi\widehat{\phi}(m_{ij})$, $\psi\widehat{\phi}(w_{ijk}), i,j,k \in I$, subject to precisely the relations implied by R1, R2, R3, R4. $\qquad\square$

**Theorem 4.12.** *We have an isomorphism of rings* $\phi\colon \kappa[F_I]^{\#} \to R_I$.

*Proof.* We know $\widehat{\phi}$ is surjective by Lemma 4.5 and injective by Lemma 4.11. $\qquad\square$

From now on we regard the isomorphism $\widehat{\phi}\colon R_I \to \kappa[F_I]^{\#}$ as simply the identity. That is we regard the $\lambda_i, m_{ij}, w_{ijk}$ as elements of $\kappa[F_I]^{\#}$, or indeed their images in $\kappa[G]^{\#}$ depending on context. Also we write $R_I$ and $\kappa[F_I]^{\#}$ interchangeably. We summarize the results from this section in the following theorems:

**Theorem 4.13.** *Suppose we have a presentation* $\langle g_i, i \in I \,|\, r_j, j \in J \rangle$ *for a group $G$. Let* $L, B, B', \widehat{B}, \widehat{B'}, R_I$ *be as defined in this section.*
*i) We may describe* $\kappa[F_I]^{\#}$ *by identifying it with $R_I$.*
*ii) Both $\widehat{B}$ and $\widehat{B'}$ are generating sets for $A_{F_I}$ as a module over $\kappa[F_I]^{\#}$.*
*iii) We may then describe* $\kappa[G]^{\#}$ *by identifying it with $\kappa[F_I]^{\#}/L^{\#}$.*
*iv) We may take either $B$ or $B'$ as generating sets for $A_G$ as a module over $\kappa[G]^{\#}$.*

**Theorem 4.14.** *In particular, if $I$ and $J$ are finite:*
*i) We have a finite description of $\kappa[F_I]^{\#}$.*
*ii) The sets $\widehat{B}, \widehat{B'}$ are finite and we have a finite generating set for the ideal $L^{\#}$.*
*iii) Thus we have a finite description of $\kappa[G]^{\#}$. In particular $\kappa[G]^{\#}$ is Noetherian, and finitely generated as an algebra over $\kappa$.*
*iv) Also $B, B'$ are finite sets.*

Now given a finitely presented group $G$ and two finite subsets $N, M \subset G$ we are in a position to apply Theorem 2.16 (or Theorem 2.19) to attempt to show that they do not generate the same normal subgroup. From the theorems above we may compute the ring $\kappa[G]^{\#}$ and find finite sets of generators for the ideals $N^{\#}, M^{\#}$ (or $N^{\#\#}, M^{\#\#}$). We are then left with the task of determining if these ideals are identical. In the next section we demonstrate this method by giving a proof of a result to do with the normal generation of free products of pairs of cyclic groups.

# 5   Free product of two cyclic groups

We may now compute $\kappa[G]^{\#}$ from a presentation of $G$. As an example we consider:

$$G = C_s \star C_t = \langle g_1, g_2 | \, g_1^s, g_2^t \rangle,$$

where $s, t > 1$. Here the indexing set for the generators is just $I = \{1, 2\}$.

**Lemma 5.1.** *$R_I$ is the polynomial ring in three variables: $R_I = \kappa[\lambda_1, \lambda_2, m_{12}]$.*

*Proof.* From R1 we have $m_{12} = m_{21}$. Also by R1 we have that $w_{ijk} = -w_{ijk} = 0$ for all $i, j, k \in \{1, 2\}$, as $i, j, k$ cannot be distinct. R3 then becomes vacuous as does R4 (noting that a matrix with repeated rows must have zero determinant). Finally R2 allows us to express $m_{11}, m_{22}$ in terms of $\lambda_1, \lambda_2$.                    $\square$

If we let $L = \{g_1^s, g_2^t\} \subset F_I$, then we have that $\kappa[G]^{\#} \cong R_I/L^{\#}$ (by Theorems 2.16 and 4.12). To compute $L^{\#}$ we first need generating sets for $A_{F_I}$ over $R_I$. By Lemma 4.5 we may take $B_{g_1^s} = \{1, g_1, g_2, g_2g_1\}$ and $B_{g_2^t} = \{1, g_2, g_1, g_1g_2\}$. Hence by Lemma 2.15 the following elements generate the ideal $L^{\#}$:

$$
\begin{array}{llll}
\overline{g_1^s} - 1, & \overline{g_1^{s+1}} - \overline{g_1}, & \overline{g_2 g_1^s} - \overline{g_2}, & \overline{g_2 g_1^{s+1}} - \overline{g_2 g_1}, \\
\overline{g_2^t} - 1, & \overline{g_2^{t+1}} - \overline{g_2}, & \overline{g_1 g_2^t} - \overline{g_1}, & \overline{g_1 g_2^{t+1}} - \overline{g_1 g_2}.
\end{array}
\qquad (2)
$$

Recall Lemma 3.13, taking $k = e$: Given $g, h \in F_I$ we have:

$$\overline{gh^n} = \overline{gh}P_n(\overline{h}) - \overline{g}P_{n-1}(\overline{h}).$$

Thus we may express our generating set (2) as polynomial expressions in $\overline{g_1}, \overline{g_2}, \overline{g_1 g_2}, \overline{g_2 g_1}$. Further, by Lemma 2.7i and Lemma 3.3i, we may express these in terms of $\lambda_1, \lambda_2, m_{12}$:

$$\overline{g_1} = \lambda_1, \qquad \overline{g_2} = \lambda_2, \qquad \overline{g_1 g_2} = \overline{g_2 g_1} = \lambda_1 \lambda_2 - m_{12}$$

**Lemma 5.2.** *We conclude that $\kappa[G]^{\#}$ is the ring $\kappa[\lambda_1, \lambda_2, m_{12}]$ quotiented by the set of elements (2), expressed as polynomial expressions in the $\lambda_1, \lambda_2, m_{12}$.*

We now consider a result due to Boyer [4]. This states that for any $w \in C_s \star C_t$, the normal closure of a proper power $w^r$, where $r > 1$, is not the whole group. This result is an instance of a more general phenomena in combinatorial group theory, where proper powers are seen to have smaller normal closures than general elements. In a certain sense, an element of the form $g^r$ is counted as merely $\frac{1}{r}$ of an element as far as normal generation is concerned (see for example [1]). This idea is central to the Potential Counterexamples 1.1 and 1.2.

We will prove Boyer's result, demonstrating that a group theoretic result proved in 1988 may be reduced to elementary algebra when one considers the commutative version of the group ring.

Let $G = C_s \star C_t$ for $s, t > 1$ and take any $w \in G$ and integer $r > 1$. Let

$$f \colon G \to C_s \times C_t$$

be the abelianisation homomorphism. If $w^r$ did normally generate $G$ then $f(w)$ would generate $C_s \times C_t$, so we may write $f(w) = (g_1, g_2)$ where $g_1$ is a generator for $C_s$ and $g_2$ is a generator for $C_t$. We then have:

$$G = \langle g_1, g_2 \,|\, g_1^s, g_2^t \rangle.$$

Pick a word in the letters $g_1, g_2$ to represent $w$, so that the total index of the letter $g_1$ is 1, and the total index of the letter $g_2$ is also 1 (as $f(w) = (g_1, g_2) \in C_s \times C_t$ this can be achieved by adding the correct powers of $g_1^s$ and $g_2^t$ to any word representing $w$). We abuse notation by also denoting this word $w$.

If $w^r$ did normally generate $G$, then we would have that the normal closure of $g_1^s, g_2^t, w^r \in F_I$ was the whole group (where, as before, $I = \{1, 2\}$). That is, to show that $w^r$ does not normally generate $G$, it is sufficient by Theorem 2.19 to show that the ideals $\{g_1^s, g_2^t, w^r\}^{\#\#}, \{g_1, g_2\}^{\#\#} \lhd \kappa[F_I]^{\#}$ are not equal.

From Corollary 3.15 we know that $\{g_1^s, g_2^t, w^r\}^{\#\#}$ is contained in the ideal generated by $P_s(\overline{g_1}), P_t(\overline{g_2}), P_r(\overline{w})$. It is therefore sufficient to show that this ideal does not contain the elements $\overline{g_1}^2 - 1, \overline{g_2}^2 - 1 \in \{g_1, g_2\}^{\#\#}$.

**Lemma 5.3.** *There exists a (possibly trivial) field extension $\mathbb{F}$ of $\kappa$ which contains roots $\mu_1, \mu_2$ of the polynomials $P_s, P_t$ respectively, as well as elements $s_1, s_2$ satisfying $s_1^2 + \mu_1^2 = 1$ and $s_2^2 + \mu_2^2 = 1$.*

*Further, in any such field $\mathbb{F}$, we have $s_1, s_2$ invertible.*

*Proof.* The degrees of $P_s, P_t$ are $s - 1, t - 1 > 0$ respectively (see Definition 3.12), so we may obtain $\mathbb{F}$ by (if necessary) adjoining to $\kappa$ the roots $\mu_1, \mu_2$, as well as the roots $s_1, s_2$ of the quadratics $s_1^2 + \mu_1^2 = 1$ and $s_2^2 + \mu_2^2 = 1$.

The only way $s_1$ or $s_2$ could be 0 is if $\mu_1 = \pm 1$ or $\mu_2 = \pm 1$. In that case we would have $P_s(1) = 0$ or $P_s(-1) = 0$ or $P_t(1) = 0$ or $P_t(-1) = 0$.

However $P_n(1) = n$ and $P_n(-1) = -1^{n+1} n$ (see Defintion 3.12). $\qquad\square$

Recall that $\kappa[F_I]^{\#}$ is identified with $R_I$ by Theorem 4.12, and $R_I$ is merely $\kappa[\lambda_1, \lambda_2, m_{12}]$ by Lemma 5.1. We have a ring homomorphism $\theta \colon \kappa[F_I]^{\#} \to \mathbb{F}[x]$:

$$\theta \colon \begin{array}{ccc} \lambda_1 & \mapsto & \mu_1 \\ \lambda_2 & \mapsto & \mu_2 \\ m_{12} & \mapsto & s_1 s_2 x \end{array}$$

where $\theta$ restricts to the identity on $\kappa$. (Here $\mathbb{F}[x]$ denotes the polynomial ring).

**Lemma 5.4.** *If $G$ is normally generated by a proper power $w^r$, then $P_r(\theta(\overline{w}))$ is a unit.*

*Proof.* By construction $\theta(P_s(\overline{g_1})) = 0$ and $\theta(P_t(\overline{g_2})) = 0$. By Lemma 2.7ii:

$$\theta(\overline{g_1}^2 - 1) = 2\theta(\overline{g_1}^2 - 1) = -2s_1{}^2 \qquad \text{and} \qquad \theta(\overline{g_2}^2 - 1) = 2\theta(\overline{g_2}^2 - 1) = -2s_2{}^2.$$

Here we know $-2s_1{}^2, -2s_2{}^2$ are invertible by Lemma 5.3. Thus the only way that the ideal generated by $P_s(\overline{g_1}), P_t(\overline{g_2}), P_r(\overline{w})$ could contain the elements $\overline{g_1}^2 - 1, \overline{g_2}^2 - 1$ is if $\theta(P_r(\overline{w})) = P_r(\theta(\overline{w}))$ is a unit in $\mathbb{F}[x]$. $\qquad\square$

As $P_r$ has strictly positive degree $r - 1$, in order to show that $P_r(\theta(\overline{w}))$ is not a degree 0 polynomial in $\mathbb{F}[x]$, it suffices to show that $\theta(\overline{w})$ is not a degree 0 polynomial in $\mathbb{F}[x]$. We therefore examine $\overline{w}$ more closely.

Recall that our choice of generators $g_1, g_2$ and choice of word to represent $w$ implies that in $F_I$ we have $w = g_1 g_2 C$, for some $C$ in the commutator subgroup $[F_I, F_I] \lhd F_I$. Thus $\overline{w} - \overline{g_1 g_2} \in \ker(h^\#)$, where $h \colon F_I \to \mathbb{Z} \times \mathbb{Z}$ is the abelianisation homomorphism.

**Lemma 5.5.** *The ideal $\ker(h^\#)$ is generated by $[\vec{g_1}, \vec{g_2}] \cdot [\vec{g_1}, \vec{g_2}]$.*

*Proof.* The kernel of $h$ is normally generated by $g_1^{-1} g_2^{-1} g_1 g_2 \in F_I$. Thus by Theorem 2.16, we have $\ker(h^\#) = \{g_1^{-1} g_2^{-1} g_1 g_2\}^\#$.

By Lemma 4.3 we have the following generating set for $\Lambda_{F_I}$ over $\kappa[F_I]^\#$: $\{\vec{g_1}, \vec{g_2}, [\vec{g_1}, \vec{g_2}]\}$. Thus by Lemma 3.16 we have $\{g_1^{-1} g_2^{-1} g_1 g_2\}^\#$ generated by:

$$[\vec{g_1}, \vec{g_2}] \cdot \vec{g_1} = 0, \qquad [\vec{g_1}, \vec{g_2}] \cdot \vec{g_2} = 0, \qquad [\vec{g_1}, \vec{g_2}] \cdot [\vec{g_1}, \vec{g_2}]$$

$\qquad\square$

**Lemma 5.6.** *For some polynomial $q(x) \in \mathbb{F}[x]$ we have:*

$$\theta(\overline{w}) = -s_1 s_2 x + \mu_1 \mu_2 + (1 - x^2) q(x).$$

*Proof.* By Lemma 5.5 for some $Q \in \kappa[F_I]^\#$ we have: $\overline{w} = \overline{g_1 g_2} + [\vec{g_1}, \vec{g_2}] \cdot [\vec{g_1}, \vec{g_2}] Q$. Applying Lemma 3.3i and Lemma 3.17i to this we get:

$$\overline{w} = -(\vec{g_1} \cdot \vec{g_2}) + \overline{g_1}\,\overline{g_2} + ((1 - \overline{g_1}^2)(1 - \overline{g_2}^2) - (\vec{g_1} \cdot \vec{g_2})^2) Q.$$

Applying $\theta$ to both sides we obtain the desired identity. $\qquad\square$

Combining Lemma 5.4 and Lemma 5.6 we have:

**Theorem 5.7.** *Let $G = C_s \star C_t$ and let $w^r$ be a proper power of some element $w \in G$, for $r, s, t > 1$. For a field $\kappa$ let $\mathbb{F}$ and $\mu_1, \mu_2, s_1, s_2 \in \mathbb{F}$ and $q(x) \in \mathbb{F}[x]$ be as previously defined. We have an implication $\mathbf{B2} \implies \mathbf{B1}$ where $\mathbf{B1}, \mathbf{B2}$ are the statements:*

$\mathbf{B1}$: *The proper power $w^r$ does not normally generate $G$.*
$\mathbf{B2}$: *The polynomial $P_r(-s_1 s_2 x + \mu_1 \mu_2 + (1 - x^2) q(x)) \in \mathbb{F}[x]$ is not a unit.*

However statement $\mathbf{B2}$ is an immediate consequence of the elementary result:

**Lemma 5.8.** *Let $\mathbb{F}$ be any field and let $\mu_1, \mu_2, s_1, s_2 \in \mathbb{F}$ with $s_1, s_2 \neq 0$ and let $q(x) \in \mathbb{F}[x]$. For $r > 1$ we have that the polynomial*

$$P_r(-s_1 s_2 x + \mu_1 \mu_2 + (1 - x^2) q(x)) \in \mathbb{F}[x] \tag{3}$$

*has degree at least $r - 1$. Thus in particular it is not a unit in $\mathbb{F}[x]$.*

*Proof.* The polynomial $P_r$ has degree $r - 1$ (see Definition 3.12). Thus if $q(x) = 0$ then (3) has degree $r - 1$ and if $q(x) \neq 0$ then (3) has degree at least $2(r - 1)$.   $\square$

Thus we have an alternative proof of the following theorem:

**Theorem 5.9** (Boyer). *The free product $C_s \star C_t$ cannot be normally generated by a proper power $w^r$, where $r, s, t > 1$.*

Intuitively speaking, we wished to show that repeating a word $r$ times would lead to an element in $G$ which was too 'big' to normally generate the whole group. However, because of the mysterious way in which words can unexpectedly appear in the normal closure of other words, this intuition was hard to pin down. Applying the functor $\#$ reduced the difficult to prove statement **B1** to the elementary statement **B2**, that a polynomial of positive degree is too 'big' to be a unit.

As the number of generators needed to generate the groups we consider goes up, so too does the complexity of the commutative algebra we are left with after applying the functor $\#$. In the next section we consider a result involving the free product of 3 cyclic groups. The statement in commutative algebra which this reduces too is concise and it is possible that it may be provable by elementary commutative algebra. However, unlike **B2**, it is not immediately obvious that this is the case.

# 6   The Scott-Wiegold conjecture

The Scott-Wiegold conjecture [15, Problem 5.53] was an open problem for forty years, before it was proven [9] by Jim Howie. Thus it illustrates how even very difficult problems in group theory can be translated into (hopefully simpler) problems in commutative algebra, by considering the commutative version of the group ring.

We take the statement of the Scott-Wiegold conjecture (**SW1**) and reduce it to a statement purely about commutative rings (**SW2**) analogously to Theorem 5.7. However this time it is not immediately obvious if it is just a case of a general result in commutative algebra, analogous to Lemma 5.8.

We will leave a more general result as a conjecture (Conjecture 6.18), though we expect that it is true at least in the case when we choose our field to be $\mathbb{R}$. As in Theorem 5.7, the statement **SW2** need only be true over one field to imply **SW1**.

Fix $r, s, t > 1$ and let $G = C_r \star C_s \star C_t$. The Scott-Wiegold Conjecture states that for any $w \in G$, the group $G$ is not normally generated by $w$.

Suppose that it was and (as in §5) consider the abelianisation homomorphism:

$$f \colon G \to C_r \times C_s \times C_t.$$

If $w \in G$ did normally generate $G$ then $f(w)$ would generate $C_r \times C_s \times C_t$, so we may write $f(w) = (g_1, g_2, g_3)$ where $g_1$ is a generator for $C_r$, $g_2$ is a generator for $C_s$ and $g_3$ is a generator for $C_t$. We then have:

$$G = \langle g_1, g_2, g_3 \,|\, g_1^r, g_2^s, g_3^t \rangle.$$

Let $I = \{1, 2.3\}$ so that $F_I$ denotes the group of words in the letters $g_1, g_2, g_3$ (and their inverses). Pick a word in $F_I$ to represent $w$, so that the total index of the letters $g_1, g_2, g_3$ is 1 in each case (we know $f(w) = (g_1, g_2, g_3) \in C_r \times C_s \times C_t$, so this can be achieved by adding the correct powers of $g_1^r, g_2^s, g_3^t$ to any word representing $w$). We abuse notation by also denoting this word $w \in F_I$.

If $w \in G$ did normally generate $G$, then we would have that the normal closure of $g_1^r, g_2^s, g_3^t, w \in F_I$ was the whole group. That is, to show that $w$ does not normally generate $G$, it is sufficient by Theorem 2.19 to show that:

$$\{g_1^r, g_2^s, g_3^t, w\}^{\#\#} \neq \{g_1, g_2, g_3\}^{\#\#} \tag{4}$$

as ideals in $\kappa[F_I]^{\#} = R_I$.

**Lemma 6.1.** *$R_I$ is the polynomial ring in 7 variables, subject to a single relation:*

$$R_I = \kappa[\lambda_1, \lambda_2, \lambda_3, m_{12}, m_{23}, m_{31}, w_{123}]/\text{Relation}$$

*where* Relation *is given by:*

$$w_{123}^2 = \begin{vmatrix} 1 - \lambda_1^2 & m_{12} & m_{31} \\ m_{12} & 1 - \lambda_2^2 & m_{23} \\ m_{31} & m_{23} & 1 - \lambda_3^2 \end{vmatrix}$$

*Proof.* Recall from §4 the relations R1, R2, R3, R4 which $R_I$ is subject to. By R1 we know that $w_{123}$ is up to sign the only non-zero $w_{ijk}$ and that for $i \neq j$, $m_{ij}$ must be $m_{12}, m_{23}$ or $m_{31}$. By R2 we may express the $m_{ii}$ in terms of the $\lambda_i$.

Then R4 implies Relation, taking $i, j, k$ and $l, s, t$ to be $1, 2, 3$ respectively. Noting that the determinant of a matrix is alternating in the column vectors of the matrix (resp. the row vectors of a matrix), we see that assigning different values to the indices, we get no new relations from R4.

Finally note that two of the indices $i, j, k, l$ must be identical in R3. One may check that R1 implies that the left hand side of R3 is alternating in $i, j, k, l$. Thus whichever values are assigned to the indices $i, j, k, l$, R3 merely gives $0 = 0$.  □

For $i = 1, 2, 3$, we have that the image of $\lambda_i$ in $\kappa[G]^{\#}$ is algebraic over $\kappa$ (apply Lemma 3.13 to $\overline{g_i^n}$ to see that $\lambda_i P_n(\lambda_i) - P_{n-1}(\lambda_i) - 1 \mapsto 0 \in \kappa[G]^{\#}$, for $n = r, s,$ or $t$). As in §5, we 'absorb' these 'pre-algebraic' elements by extending the field $\kappa$.

**Lemma 6.2.** *There exists a (possibly trivial) field extension $\mathbb{F}$ of $\kappa$ which contains roots $\mu_1, \mu_2, \mu_3$ of the polynomials $P_r, P_s, P_t$ respectively, as well as elements $s_1, s_2, s_3$ satisfying $s_i^2 + \mu_i^2 = 1$, $i = 1, 2, 3$. Further, in any such field the $s_i$ are invertible.*

*Proof.* Same as for Lemma 5.3: We note that for $i = 1, 2, 3$ we have $\mu_i \neq \pm 1$, as -1,1 are not roots of $P_r, P_s$ or $P_t$.  □

Let $A = \mathbb{F}[x, y, u, v]/\langle(1 - x^2)(1 - y^2) - (u^2 + v^2)\rangle$. We define a map $\theta \colon \kappa[F_I]^{\#} \to A$:

$$\theta \colon \begin{array}{rcl} \lambda_1 & \mapsto & \mu_1 \\ \lambda_2 & \mapsto & \mu_2 \\ \lambda_3 & \mapsto & \mu_3 \\ m_{12} & \mapsto & s_1 s_2 x \\ m_{31} & \mapsto & s_3 s_1 y \\ m_{23} & \mapsto & s_2 s_3 (u + xy) \\ w_{123} & \mapsto & s_1 s_2 s_3 v \end{array}$$

where $\theta$ is a ring homomorphism which restricts to the identity on $\kappa$.

**Lemma 6.3.** *The map $\theta$ is well defined.*

*Proof.* It is sufficient to verify that $\theta$ applied to both sides of Relation results in a true identity in $A$. That is, we must check that:

$$v^2 = \begin{vmatrix} 1 & x & y \\ x & 1 & u+xy \\ y & u+xy & 1 \end{vmatrix}$$

Note we have cleared the factors of $s_1^2, s_2^2, s_3^2$ on both sides here, which on the right hand side come from pulling out a factor of $s_1$, $s_2$ and $s_3$ from the 1$^{\text{st}}$, 2$^{\text{nd}}$ and 3$^{\text{rd}}$ rows and columns of the matrix respectively. Expanding the determinant we get: $(1-x^2)(1-y^2)-u^2$, which does indeed equal $v^2$, by the defining relation in $A$. □

**Lemma 6.4.** *The ideal in $A$ generated by $\theta(\{g_1, g_2, g_3\}^{\#\#})$ is the entire ring.*

*Proof.* Corollary 3.4 gives $\vec{g_i} \cdot \vec{g_i} \in \{g_1, g_2, g_3\}^{\#\#}$ for $i = 1, 2, 3$. But $\theta(\vec{g_i} \cdot \vec{g_i}) = \theta(1 - \overline{g_i}^2) = 1 - \mu_i^2 = s_i^2$, which is invertible in $A$ by Lemma 6.2. □

**Lemma 6.5.** *The ideal generated by $\theta(\{g_1^r, g_2^s, g_3^t, w\}^{\#\#})$ is generated by $\theta(\{w\}^{\#\#})$.*

*Proof.* By Corollary 3.15 we have that the ideal $\{g_1^r, g_2^s, g_3^t\}^{\#\#}$ is contained in the ideal generated by $P_r(\overline{g_1}), P_s(\overline{g_2}), P_t(\overline{g_3})$. Applying $\theta$ to these three elements gives: $P_r(\mu_1), P_s(\mu_2), P_t(\mu_3) \in A$, which by construction equal 0. □

Thus combining Lemma 6.4 and Lemma 6.5 we deduce:

**Lemma 6.6.** *If $\theta(\{w\}^{\#\#})$ generates a proper ideal in $A$ then (4) holds and hence $w$ does not normally generate $G$.*

Let $w_1, w_2, w_2', w_3, w_3'$ demote the following elements of $A$:

$$w_1 = \theta(\vec{g_1} \cdot \vec{w}), \quad w_2 = s_2^{-1}\theta([\vec{g_1}, \vec{g_2}] \cdot \vec{w}), \quad w_2' = s_1^{-1}s_2^{-1}\theta([\vec{g_1}, \vec{g_2}] \cdot [\vec{g_1}, \vec{w}]),$$
$$w_3 = s_3^{-1}\theta([\vec{g_1}, \vec{g_3}] \cdot \vec{w}), \quad w_3' = s_1^{-1}s_3^{-1}\theta([\vec{g_1}, \vec{g_3}] \cdot [\vec{g_1}, \vec{w}]).$$

**Lemma 6.7.** *The ideal generated by $\theta(\{w\}^{\#\#})$ has generating set: $\{w_1, w_2, w_2', w_3, w_3'\}$.*

*Proof.* From Lemma 4.3 we obtain a generating set for $\Lambda_{F_I}$. Then applying Corollary 3.4 we obtain a generating set for $\{w\}^{\#\#}$. Applying $\theta$ yields a generating set for the ideal generated by $\theta(\{w\}^{\#\#})$:

$$v_1 = \theta(\vec{g_1} \cdot \vec{w}), \qquad v_2 = \theta(\vec{g_2} \cdot \vec{w}), \qquad v_3 = \theta(\vec{g_3} \cdot \vec{w}),$$
$$v_{12} = \theta([\vec{g_1}, \vec{g_2}] \cdot \vec{w}), \quad v_{23} = \theta([\vec{g_2}, \vec{g_3}] \cdot \vec{w}), \quad v_{31} = \theta([\vec{g_3}, \vec{g_1}] \cdot \vec{w})).$$

We must first verify that the $w_i, w_i'$ all lie in the ideal generated by these elements. Clearly, $w_1 = v_1, w_2 = s_2^{-1}v_{12}, w_3 = -s_3^{-1}v_{31}$. By Corollary 3.6ii:

$$[\vec{g_1}, \vec{g_2}] \cdot [\vec{g_1}, \vec{w}] = (\vec{g_1} \cdot \vec{g_1})(\vec{g_2} \cdot \vec{w}) - (\vec{g_1} \cdot \vec{w})(\vec{g_2} \cdot \vec{g_1}),$$
$$[\vec{g_1}, \vec{g_3}] \cdot [\vec{g_1}, \vec{w}] = (\vec{g_1} \cdot \vec{g_1})(\vec{g_3} \cdot \vec{w}) - (\vec{g_1} \cdot \vec{w})(\vec{g_3} \cdot \vec{g_1}).$$

Applying $\theta$ and dividing through by $s_1 s_2$, $s_1 s_3$ respectively we get:

$$w_2' = s_1 s_2^{-1} v_2 - x v_1, \qquad w_3' = s_1 s_3^{-1} v_3 - y v_1. \tag{5}$$

Now we must show that the $w_i, w_i'$ generate the $v_i, v_{ij}$. Again we have, $v_1 = w_1, v_{12} = s_2 w_2, v_{31} = -s_3 w_3$. Rearranging (5) we get:

$$v_2 = s_1^{-1} s_2 w_2' + s_1^{-1} s_2 x w_1, \qquad v_3 = s_1^{-1} s_3 w_3' + s_1^{-1} s_3 y w_1.$$

It remains to show that $v_{23}$ lies in the span of the $w_i, w_i'$. By Corollary 3.6iv:

$$([\vec{g_1}, \vec{g_2}] \cdot \vec{g_3})\,\vec{g_1} = (\vec{g_1} \cdot \vec{g_1})[\vec{g_2}, \vec{g_3}] - (\vec{g_2} \cdot \vec{g_1})[\vec{g_1}, \vec{g_3}] + (\vec{g_3} \cdot \vec{g_1})[\vec{g_1}, \vec{g_2}].$$

Taking the $\cdot$ product with $\vec{w}$ and applying $\theta$ we get:

$$s_1 s_2 s_3 v w_1 = s_1^2 v_{23} - s_1 s_2 s_3 x w_3 + s_1 s_2 s_3 y w_2.$$

Rearranging gives $v_{23} = s_1^{-1} s_2 s_3 v w_1 + s_1^{-1} s_2 s_3 x w_3 - s_1^{-1} s_2 s_3 y w_2$, as required. $\qquad\square$

Thus by Lemma 6.6, in order to show that $w$ does not normally generate $G$, it suffices to show that $1 \in A$ cannot be expressed as a linear combination of the $w_i, w_i'$.

**Lemma 6.8.** *We have the following relation between* $w_2, w_2', w_3, w_3'$:

$$
\begin{pmatrix}
-u & v & 1-x^2 & 0 \\
-v & -u & 0 & 1-x^2 \\
1-y^2 & 0 & -u & -v \\
0 & 1-y^2 & v & -u
\end{pmatrix}
\begin{pmatrix}
w_2 \\
w_2' \\
w_3 \\
w_3'
\end{pmatrix}
=
\begin{pmatrix}
0 \\
0 \\
0 \\
0
\end{pmatrix}. \tag{6}
$$

*Proof.* Consider the expression:

$$[[\vec{g_1}, \vec{g_2}], \vec{g_3}] \cdot [[\vec{g_1}, \vec{g_2}], [\vec{g_1}, \vec{w}]].$$

Expanding this as a $\cdot$ product of two brackets using Corollary 3.6ii we get:

$$
\begin{aligned}
&[[\vec{g_1}, \vec{g_2}], \vec{g_3}] \cdot [[\vec{g_1}, \vec{g_2}], [\vec{g_1}, \vec{w}]] \\
=\ & ([\vec{g_1}, \vec{g_2}] \cdot [\vec{g_1}, \vec{g_2}])(\vec{g_3} \cdot [\vec{g_1}, \vec{w}]) - ([\vec{g_1}, \vec{g_2}] \cdot [\vec{g_1}, \vec{w}])(\vec{g_3} \cdot [\vec{g_1}, \vec{g_2}]) \\
=\ & -((\vec{g_1} \cdot \vec{g_1})(\vec{g_2} \cdot \vec{g_2}) - (\vec{g_1} \cdot \vec{g_2})^2)([\vec{g_1}, \vec{g_3}] \cdot \vec{w}) - ([\vec{g_1}, \vec{g_2}] \cdot \vec{g_3})([\vec{g_1}, \vec{g_2}] \cdot [\vec{g_1}, \vec{w}]).
\end{aligned}
$$

On the other hand we may replace $[[\vec{g_1}, \vec{g_2}], [\vec{g_1}, \vec{w}]]$ with $([\vec{g_1}, \vec{g_2}] \cdot \vec{w})\,\vec{g_1}$ by Corollary 3.6iii. Thus:

$$
\begin{aligned}
&[[\vec{g_1}, \vec{g_2}], \vec{g_3}] \cdot [[\vec{g_1}, \vec{g_2}], [\vec{g_1}, \vec{w}]] \\
=\ & ([[\vec{g_1}, \vec{g_2}], \vec{g_3}] \cdot \vec{g_1})([\vec{g_1}, \vec{g_2}] \cdot \vec{w}) \\
=\ & ([\vec{g_3}, \vec{g_1}] \cdot [\vec{g_1}, \vec{g_2}])([\vec{g_1}, \vec{g_2}] \cdot \vec{w}) \qquad \text{(cycling 1}^\text{st}\text{ scalar triple product)} \\
=\ & ((\vec{g_1} \cdot \vec{g_3})(\vec{g_1} \cdot \vec{g_2}) - (\vec{g_1} \cdot \vec{g_1})(\vec{g_2} \cdot \vec{g_3}))([\vec{g_1}, \vec{g_2}] \cdot \vec{w}).
\end{aligned}
$$

Equating these two expansions of $[[\vec{g_1}, \vec{g_2}], \vec{g_3}] \cdot [[\vec{g_1}, \vec{g_2}], [\vec{g_1}, \vec{w}]]$, applying $\theta$ to both sides, and dividing through by $s_1^2 s_2^2 s_3$, yields the top row of (6).

If instead we equate the two expansions of $[[\vec{g_1}, \vec{g_2}], \vec{g_3}] \cdot [[\vec{g_1}, \vec{g_2}], [\vec{g_1}, \vec{w}]]$, but interchange all $\vec{g_2}$'s and $\vec{g_3}$'s, before applying $\theta$ to both sides, and dividing through by $s_1^2 s_2 s_3^2$, we obtain the third row of (6).

Now consider the expression:

$$[[\vec{g_1}, \vec{g_2}], [\vec{g_1}, \vec{g_3}]] \cdot [[\vec{g_1}, \vec{g_2}], [\vec{g_1}, \vec{w}]].$$

By Corollary 3.6iii we substitute $([\vec{g_1}, \vec{g_2}] \cdot \vec{g_3})\,\vec{g_1}$ for $[[\vec{g_1}, \vec{g_2}], [\vec{g_1}, \vec{g_3}]]$ and $([\vec{g_1}, \vec{g_2}] \cdot \vec{w})\,\vec{g_1}$ for $[[\vec{g_1}, \vec{g_2}], [\vec{g_1}, \vec{w}]]$:

$$
\begin{aligned}
&[[\vec{g_1}, \vec{g_2}], [\vec{g_1}, \vec{g_3}]] \cdot [[\vec{g_1}, \vec{g_2}], [\vec{g_1}, \vec{w}]] \\
=\ & (\vec{g_1} \cdot \vec{g_1})([\vec{g_1}, \vec{g_2}] \cdot \vec{g_3})([\vec{g_1}, \vec{g_2}] \cdot \vec{w}).
\end{aligned}
$$

On the other hand we could apply Corollary 3.6ii to expand the expression as a $\cdot$ product of two brackets:

$$
\begin{aligned}
&[[\vec{g_1}, \vec{g_2}], [\vec{g_1}, \vec{g_3}]] \cdot [[\vec{g_1}, \vec{g_2}], [\vec{g_1}, \vec{w}]] \\
=\ & ([\vec{g_1}, \vec{g_2}] \cdot [\vec{g_1}, \vec{g_2}])([\vec{g_1}, \vec{g_3}] \cdot [\vec{g_1}, \vec{w}]) - ([\vec{g_1}, \vec{g_2}] \cdot [\vec{g_1}, \vec{g_3}])([\vec{g_1}, \vec{g_2}] \cdot [\vec{g_1}, \vec{w}]) \\
=\ & ((\vec{g_1} \cdot \vec{g_1})(\vec{g_2} \cdot \vec{g_2}) - (\vec{g_1} \cdot \vec{g_2})^2)([\vec{g_1}, \vec{g_3}] \cdot [\vec{g_1}, \vec{w}]) \\
& -((\vec{g_1} \cdot \vec{g_1})(\vec{g_2} \cdot \vec{g_3}) - (\vec{g_1} \cdot \vec{g_3})(\vec{g_1} \cdot \vec{g_2}))([\vec{g_1}, \vec{g_2}] \cdot [\vec{g_1}, \vec{w}]).
\end{aligned}
$$

Equating these two expansions of $[[\vec{g_1}, \vec{g_2}], [\vec{g_1}, \vec{g_3}]] \cdot [[\vec{g_1}, \vec{g_2}], [\vec{g_1}, \vec{w}]]$, applying $\theta$ to both sides, and dividing through by $s_1^3 s_2^2 s_3$, yields the second row of (6).

If instead we equate the two expansions of $[[\vec{g_1}, \vec{g_2}], [\vec{g_1}, \vec{g_3}]] \cdot [[\vec{g_1}, \vec{g_2}], [\vec{g_1}, \vec{w}]]$, but interchange all $\vec{g_2}$'s and $\vec{g_3}$'s, before applying $\theta$ to both sides, and dividing through by $s_1^3 s_2 s_3^2$, we obtain the fourth row of (6).  $\square$

We will give a generating set for the kernel of the matrix in Lemma 6.8. First we need to better understand the ring $A$.

**Lemma 6.9.** *We may regard $A$ as a quadratic extension of the polynomial ring $\mathbb{F}[x, y, u]$; so every element of $A$ may written uniquely in the form $a + a'v$ with $a, a' \in \mathbb{F}[x, y, u]$.*

*Proof.* Given any element of $A$ we may regard it as a polynomial in $v$, with coefficients in $\mathbb{F}[x, y, u]$. If an element of $A$ has degree greater than 1 as a polynomial in $v$, then the defining relation in $A$: $(1 - x^2)(1 - y^2) = u^2 + v^2$, allows us to represent the element as a polynomial in $v$ of lesser degree. Any element of $A$ may be represented as a polynomial in $v$ of minimal degree, which will then have the required form.

To see that this is unique, suppose we have two degree at most 1 polynomials in $v$ representing the same element of $A$. Then the difference must be at most degree 1 as a polynomial in $v$. However it must also be divisible by the degree 2 polynomial $(1 - x^2)(1 - y^2) - u^2 - v^2$. Thus the difference is 0.  $\square$

Let $M$ denote the matrix:

$$
M = \begin{pmatrix}
u & v & 1 - x^2 & 0 \\
-v & u & 0 & 1 - x^2 \\
1 - y^2 & 0 & u & -v \\
0 & 1 - y^2 & v & u
\end{pmatrix} \tag{7}
$$

**Lemma 6.10.** *The columns of the matrix $M$ generate the kernel of the matrix in* (6).

*Proof.* Direct calculation shows that the columns of $M$ lie in the kernel.

Now suppose that:

$$
\begin{pmatrix}
-u & v & 1 - x^2 & 0 \\
-v & -u & 0 & 1 - x^2 \\
1 - y^2 & 0 & -u & -v \\
0 & 1 - y^2 & v & -u
\end{pmatrix}
\begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \end{pmatrix}
=
\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \tag{8}
$$

Reducing the third row of (8) modulo the ideal $I = \langle u, v, 1 - x^2 \rangle$ we get $(1 - y^2)z_1 = 0$. However $1 - y^2$ is not a zero divisor in the ring $A/I = \mathbb{F}[x, y]/\langle 1 - x^2 \rangle$. Thus

$z_1 \in I$, and subtracting some $A$-linear combination of the first three columns of $M$ from $(z_1, z_2, z_3, z_4)^T$, we may assume that $z_1 = 0$.

Then the second row of (8) gives $uz_2 = (1 - x^2)z_4$. Representing $z_2, z_4$ as in Lemma 6.9 and noting that the polynomial ring $\mathbb{F}[x, y, u]$ is a unique factorisation domain, we have that $1 - x^2$ divides $z_2$. Thus subtracting some multiple of the fourth column of $M$ from $(z_1, z_2, z_3, z_4)^T$, we may assume that $z_1 = z_2 = 0$.

Then the first and second row of (8) give $(1 - x^2)z_3 = 0$ and $(1 - x^2)z_4 = 0$. Representing $z_3, z_4$ as in Lemma 6.9 and noting that $1 - x^2$ is not a zero divisor in the polynomial ring $\mathbb{F}[x, y, u]$, we conclude that $z_3 = z_4 = 0$.

Thus starting with an arbitrary $(z_1, z_2, z_3, z_4)^T$ satisfying (8) and subtracting a linear combination of the columns of $M$, we are left with $(0, 0, 0, 0)^T$. $\qquad\square$

**Definition 6.11.** *We say that an element of $A$ is* represented *by $M$ if it lies in the image of the bilinear map represented by $M$. That is $a \in A$ is represented by $M$ precisely when there exist $\mathbf{q_1}, \mathbf{q_2} \in A^4$ such that $a = \mathbf{q_1}^T M \mathbf{q_2}$.*

**Lemma 6.12.** *Any linear combination of $w_2, w_2', w_3, w_3'$ is represented by $M$.*

*Proof.* By Lemma 6.8 we have that $(w_2, w_2', w_3, w_3')^T$ satisfies (8). Thus by Lemma 6.10 we have $(w_2, w_2', w_3, w_3')^T = M\mathbf{q_2}$ for some $\mathbf{q_2} \in A^4$. So if $a \in A$ is a linear combination of $w_2, w_2', w_3, w_3'$, then $a = \mathbf{q_1}^T M \mathbf{q_2}$ for some $\mathbf{q_1} \in A^4$. $\qquad\square$

Having thus constrained linear combinations of $w_2, w_2', w_3, w_3'$, we turn our attention to the element $w_1 = \theta(\vec{g_1} \cdot \vec{w}) \in A$. Our approach is similar to that in §5, in that we first consider the abelianisation homomorphism:

$$h \colon F_I \to \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}.$$

**Lemma 6.13.** *We have $(\vec{g_1} \cdot \vec{w}) - (\vec{g_1} \cdot g_1\vec{g_2}g_3) \in \ker(h^{\#})$.*

*Proof.* By Lemma 3.3i we have:

$$(\vec{g_1} \cdot \vec{w}) - (\vec{g_1} \cdot g_1\vec{g_2}g_3) = -\frac{1}{2}((\overline{g_1w} - \overline{g_1^2g_2g_3}) - (\overline{g_1^{-1}w} - \overline{g_2g_3})). \tag{9}$$

Recall that the word $w \in F_I$ was constructed so that $h(w) = h(g_1g_2g_3)$. Thus $h(g_1w) = h(g_1^2g_2g_3)$ and $h(g_1^{-1}w) = h(g_2g_3)$. We conclude:

$$h^{\#}(\overline{g_1w} - \overline{g_1^2g_2g_3}) = 0, \qquad h^{\#}(\overline{g_1^{-1}w} - \overline{g_2g_3}) = 0,$$

so by (9) we get $h^{\#}((\vec{g_1} \cdot \vec{w}) - (\vec{g_1} \cdot g_1\vec{g_2}g_3)) = 0$. $\qquad\square$

Hence we know that $w_1$ has the form $\theta(\vec{g_1} \cdot g_1\vec{g_2}g_3) + \alpha$ for some $\alpha$ in the ideal $J$ generated by $\theta(\ker(h^{\#}))$. We will proceed to give a generating set for the ideal $J$, but first we expand $\theta(\vec{g_1} \cdot g_1\vec{g_2}g_3)$.

Fix $W \in A$ to be the following:

$$W = -s_1^2 s_2 s_3 xy + \mu_1\mu_3 s_1 s_2 x + \mu_1\mu_2 s_1 s_3 y + s_1^2\mu_2\mu_3. \tag{10}$$

**Lemma 6.14.** *We have $\theta(\vec{g_1} \cdot g_1\vec{g_2}g_3) = W - s_1^2 s_2 s_3 u + \mu_1 s_1 s_2 s_3 v$.*

*Proof.* By Lemma 3.7 we have $g_2g_3 = \overline{g_2}\,\overline{g_3} - (\vec{g_2} \cdot \vec{g_3}) + \overline{g_3}\,\vec{g_2} + \overline{g_2}\,\vec{g_3} + [\vec{g_2}, \vec{g_3}]$. Again applying Lemma 3.7 we have:

$$g_1\vec{g_2}g_3 = (\overline{g_2}\,\overline{g_3} - \vec{g_2} \cdot \vec{g_3})\,\vec{g_1} + \overline{g_1}(\overline{g_3}\,\vec{g_2} + \overline{g_2}\,\vec{g_3} + [\vec{g_2}, \vec{g_3}]) + [\vec{g_1}, \overline{g_3}\,\vec{g_2} + \overline{g_2}\,\vec{g_3} + [\vec{g_2}, \vec{g_3}]].$$

Taking the $\cdot$ product with $\vec{g_1}$, the last term vanishes. Then applying $\theta$ to both sides yields the result. $\square$

**Lemma 6.15.** *The ideal $J$ generated by $\theta(\ker(h^\#))$ is generated by: $u, v, 1 - x^2, 1 - y^2$.*

*Proof.* As $F_I$ has three generators $g_1, g_2, g_3$, the kernel of $h$ is normally generated by the commutators $g_1^{-1}g_2^{-1}g_1g_2$, $g_1^{-1}g_3^{-1}g_1g_3$, $g_2^{-1}g_3^{-1}g_2g_3$. Thus by Theorem 2.16:

$$\ker(h^\#) = \{g_1^{-1}g_2^{-1}g_1g_2,\ g_1^{-1}g_3^{-1}g_1g_3,\ g_2^{-1}g_3^{-1}g_2g_3\}^\#.$$

Taking the generating set for $\Lambda_{F_I}$ from Lemma 4.3 and applying Lemma 3.16 we obtain a generating set for $\ker(h^\#)$ given by taking the $\cdot$ products of

$$[\vec{g_1}, \vec{g_2}], [\vec{g_1}, \vec{g_3}], [\vec{g_2}, \vec{g_3}] \qquad \text{with} \qquad \vec{g_1}, \vec{g_2}, \vec{g_3}, [\vec{g_1}, \vec{g_2}], [\vec{g_1}, \vec{g_3}], [\vec{g_2}, \vec{g_3}].$$

Avoiding zero's and repeats this leaves a generating set of seven elements for $\ker(h^\#)$. After applying $\theta$ to these seven elements (using Corollary 3.6ii to simplify) and rescaling by units in $\mathbb{F}$, we are left with a generating set for $J$:

$$u, v, 1 - x^2, 1 - y^2, \qquad 1 - (u + xy)^2, \qquad x(u + xy) - y, \qquad x - y(u + xy).$$

To complete the proof we need only note that:

$$
\begin{aligned}
1 - (u + xy)^2 &= (1 - x^2) + x^2(1 - y^2) - (u + 2xy)u, \\
x(u + xy) - y &= xu - y(1 - x^2), \\
x - y(u + xy) &= x(1 - y^2) - yu.
\end{aligned}
$$

$\square$

**Lemma 6.16.** *We have $w_1 = W + \alpha$, for some $\alpha \in J$.*

*Proof.* By Lemma 6.13 we have $w_1 - \theta(\vec{g_1} \cdot g_1\vec{g_2}g_3) \in J$. Thus by Lemma 6.14:

$$w_1 - W + s_1^2 s_2 s_3 u - \mu_1 s_1 s_2 s_3 v \in J.$$

Noting that $s_1^2 s_2 s_3 u - \mu_1 s_1 s_2 s_3 v \in J$ we have $w_1 - W \in J$. $\square$

**Theorem 6.17.** *For $r, s, t > 1$ let $G = C_r \star C_s \star C_t$, let the field $\mathbb{F}$ and elements $\mu_1, \mu_2, \mu_3, s_1, s_2, s_3 \in \mathbb{F}$ be as in Lemma 6.2 and let $A = \mathbb{F}[x, y, u, v]/\langle(1 - x^2)(1 - y^2) - (u^2 + v^2)\rangle$. Further let $J \lhd A$ be the ideal generated by $\{u, v, 1 - x^2, 1 - y^2\}$, let $W \in A$ be as given by (10) and let the matrix $M$ be as given by (7).*

*We have an implication of statements* **SW2** $\implies$ **SW1** *where* **SW1**, **SW2** *are:*

**SW1**: *No $w \in G$ normally generates $G$.*
**SW2**: *Given $a \in A$ represented by $M$ and $\alpha \in J$, the elements $\{a, W + \alpha\}$ generate a proper ideal in $A$.*

*Proof.* Assume that SW2 is true. Suppose $w \in G$ normally generates $G$. Let $a$ be any linear combination of $w_2, w_2', w_3, w_3'$. Lemma 6.12 tells us $a$ is represented by $M$. Lemma 6.16 tells us $w_1 = W + \alpha$ for some $\alpha \in J$. Then **SW2** implies that we cannot write $1 = \lambda w_1 + a$ with $\lambda \in A$. Thus $w_1, w_2, w_2', w_3, w_3'$ generate a proper ideal in $A$.

From Lemma 6.7 we know that this proper ideal is precisely the ideal generated by $\theta(\{w\}^{\#\#})$. From Lemma 6.6 we conclude that $w$ does not normally generate $G$. $\square$

Thus applying the functor $\#$ to the groups involved in the Scott-Wiegold conjecture reduces the problem to proving **SW2**, a statement in commutative algebra. Unlike **B2** this statement is not immediately obvious, so we cannot claim this time, that the theory associated to $\#$ immediately proves the result.

Note however that Theorem 6.17 holds for any field $\mathbb{F}$ satisfying the properties demanded by Lemma 6.2. That is **SW2** only needs to hold for one such field in order to deduce the Scott-Wiegold conjecture. We expect that modifying Howie's original proof [9], one may take $\mathbb{F} = \mathbb{R}$ and have $|s_1^2 s_2 s_3| > |s_1 s_2 \mu_1 \mu_3| + |s_1 s_3 \mu_1 \mu_2| + |s_1^2 \mu_2 \mu_3|$, and prove **SW2** in this case, thus proving the Scott-Wiegold conjecture.

This may seem a long-winded approach given the concise nature of the proof in [9]. One benefit of doing it this way is that the topological arguments in [9], when applied to statements about ideal generation such as **SW2**, can be understood algebraically in terms of Euler classes / Euler class groups [3, 12], and weak Mennicke symbols [11].

However what would really be illuminating is a proof of a more general algebraic statement which implies **SW2**, analogous to how Lemma 5.8 implies **B2**. Ideally:

**Conjecture 6.18.** *Let $\mathbb{F}$ be any field, let*

$$A = \mathbb{F}[x, y, u, v]/\langle(1 - x^2)(1 - y^2) - (u^2 + v^2)\rangle,$$

*and let $J \lhd A$ be the ideal generated by $\{u, v, 1 - x^2, 1 - y^2\}$. Let $M$ be as defined in (7) and let $W' = c_3 xy + c_2 y + c_1 x + c_0$, with $c_0, c_1, c_2, c_3 \in \mathbb{F}$ and $c_3 \neq 0$.*

*Given $a \in A$ represented by $M$ and $\alpha \in J$, the elements $\{a, W' + \alpha\}$ generate a proper ideal in $A$.*

If a result such as this could be proved then we would understand, at the level of commutative group rings, the obstruction to normally generating $C_r \star C_s \star C_t$ by a single element. Then having attained results using $\#$ about 3-generated groups as well as 2-generated groups (Theorem 5.9), we could hope to approach the 4-generated groups from Potential counterexamples 1.1 and 1.2 by these means. As discussed in §1, if successful this could result in the resolution of several conjectures; in the first place the Wiegold conjecture and the Relation Gap problem.

# References

[1] **Daniel Allcock** ; *Spotting infinite groups* ; Math. Proc. Camb. Phil. Soc. 125 (1999) pp. 39–42

[2] **F R Beyl, N Waller** ; *Examples of exotic free 2–complexes and stably free nonfree modules for quaternion groups* : Algebr. Geom. Topol. 8 (2008) pp. 1–17

[3] **S. M. Bhatwadekar and Raja Sridharan** ; *The Euler Class Group of a Noetherian Ring* : Compositio Mathematica 122: (2000) pp. 183–222

[4] **S. Boyer** ; *On proper powers in free products and Dehn surgery* : J. Pure and Appl. Alg. 51 (1988) pp. 217–229

[5] **Martin R. Bridson and Michael Tweedale** ; *Deficiency and abelianized deficiency of some virtually free groups* : Math. Proc. Camb. Phil. Soc. 143 (2007) pp. 257–264

[6] **K. Gruenberg and P. Linnell** ; *Generation gaps and abelianized defects of free products* : J. Group Theory 11, Issue 5 (2008) pp. 587–608

[7] **J. Harlander** ; *Some aspects of efficiency* : Groups–Korea '98 (Pusan), de Gruyter, (2000) pp. 165–180

[8] **R.D. Horowitz** ; *Characters of free groups represented in the two-dimensional special linear group* : Comm. Pure Appl. Math. 25 (1972) pp. 635–649

[9] **James Howie** ; *A proof of the Scott-Wiegold conjecture on free products of cyclic groups* : J. Pure and Appl. Alg. 173 (2002) pp. 167–176

[10] **F.E.A. Johnson** ; *Minimal 2-complexes and the D(2)-problem* : Proceedings of the American Mathematical Society 132.3 (2003) pp. 579–586

[11] **W. van der Kallen** ; *Module structure on certain orbit sets of unimodular rows* : J. of Pure and Aplied Algebra 57 (1989) pp. 281–316

[12] **Maynard Kong** ; *Euler Classes of Inner Product Modules* : Journal of Algebra 49 (1977) pp. 276–303

[13] **W.H. Mannan** ; *Realizing algebraic 2-complexes by cell complexes* : Mathematical Proceedings of the Cambridge Philosophical Society 14 (2009) pp. 671–673

[14] **W.H. Mannan** ; *Quillen's plus construction and the D(2) problem* : Algebraic and Geometric Topology 9 (2009) pp. 1399–1411

[15] **V.D. Mazurov, E.I. Khukhro (Eds.)** ; *Unsolved Problems in Group Theory*: *The Kourovka Notebook* 12$^{th}$ Ed., Russian Academy of Sciences, Novosibirsk (1992)

[16] **V.D. Mazurov, E.I. Khukhro (Eds.)** ; *Unsolved Problems in Group Theory*: *The Kourovka Notebook* 14$^{th}$ Ed., Instit. of Math. SO RAN, Novosibirsk (1999)

[17] **C.T.C. Wall** ; *Finiteness conditions for CW complexes* : Annals of Maths 81 (1965) pp. 56–69

[18] **H. Weyl** ; *The Classical Groups: Their Invariants and Representations* : Princeton University Press, Princeton (1939)

[19] **C.F. Woodcock** ; *A commutative analogue of the group ring* : Journal of Pure and Applied Algebra 210.1 (2007) pp. 193–199