Algorithms for polycyclic groups

Eamonn O'Brien

University of Auckland

September 2021

Let F be free group on a non-empty set X.

Group presentation: X and a set $\mathcal{R}$ of words in X, written $\{X \mid \mathcal{R}\}$.

If R is the normal closure of $\mathcal{R}$ in F, the group G defined by the presentation is F/R and is written $\langle\, X \mid \mathcal{R}\,\rangle$.

Example

$$G = \langle a, b | a^4, b^2, a^b = a^{-1} \rangle$$

$$H = \langle a, b | a^4, b^2 = a^2, a^b = a^{-1} \rangle$$

What can we discover about the structure of G or H?

One area of substantial progress at algorithmic and computational level is in the study of particular quotients of G.

Examples include abelian, p-quotient, soluble quotients.

May discover that G infinite, by examining the invariants of its largest abelian quotient.

Can compute "useful" presentations for quotient Q of the group: those which have prime-power order, are nilpotent, or are soluble.

Central feature of these presentations is that they provide a solution to the *word problem* for Q:

Decide if two words in generators of Q represent the same element of Q.

Outline of lecture series

- Abelian quotients.
- Polycyclic generating sequences: basic properties.
- Polycyclic presentations: consistency and collection.
- Constructing polycyclic presentations.
- Generating descriptions of p-groups.
- An application: SmallGroups.

Abelian quotients

Lemma

G/N abelian if and only if $N \geq G'$.

Largest abelian quotient of G is G/G'.

Structure of this abelian group can be determined fairly readily.

Definition

B is in Smith Normal Form if for some $k \geq 0$ the entries $d_i = B_{i,i}$ for $1 \leq i \leq k$ are positive, B has no other non-zero entries, and $d_i | d_{i+1}$ for $1 \leq i \leq k$.

Smith normal form

Example

$$B := \begin{pmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 12 & 0 & 0 \end{pmatrix}$$

is in Smith normal form.

Determine the structure of G/G'

1. Abelianise the presentation of G by adding relations to make G abelian.
2. $G/G' \cong \mathbb{Z}^n/B$ where B is a subgroup of $\mathbb{Z}^n$.
3. Describe B by a matrix $S(B)$.
4. To obtain the structure of $\mathbb{Z}^n/B$, we apply row-and-column operations to $S(B)$ to convert it to *Smith normal form* S.
5. We read off abelian invariants of $\mathbb{Z}^n/B$ from S.

Lemma

Suppose

$$B := \begin{pmatrix} d_1 & & & & & & & & \\ & d_2 & & & & & & & \\ & & \ddots & & & & & & \\ & & & d_k & & & & & \\ & & & & 0 & & & & \\ & & & & & \ddots & & & \\ & & & & & & 0 & 0 & \cdots 0 \end{pmatrix}$$

is an $m \times n$ matrix in Smith normal form with $m \leq n$. Then

$$\mathbb{Z}^n/S(B) \simeq Z_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_k} \oplus \mathbb{Z}^s,$$

where $s = n - k$.

Example

$G = \langle x, y, z \mid (xyz^{-1})^2, (x^{-1}y^2z)^2, (xy^{-2}z^{-1})^2 \rangle$

Abelianise to obtain

$$\begin{aligned} G/G' &= \langle x, y, z \mid (xyz^{-1})^2, (x^{-1}y^2z)^2, (xy^{-2}z^{-1})^2, \\ & \qquad xy = yx, xz = zx, yz = zy \rangle \end{aligned}$$

Describe B by $S(B) = \begin{pmatrix} 2 & 2 & -2 \\ -2 & 4 & 2 \\ 2 & -4 & -2 \end{pmatrix}$

Smith Normal form of $S(B)$ is $\begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 0 \end{pmatrix}$

Hence $G/G' \cong \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}$ and so it is infinite.

Polycyclic Groups

Definition

G is *polycyclic* if it has a descending chain of subgroups

$$G = G_1 \geq G_2 \geq \cdots \geq G_{n+1} = 1$$

in which $G_{i+1} \lhd G_i$, and G_i/G_{i+1} is cyclic. Such a chain of subgroups is called a *polycyclic series*.

Polycyclic groups: solvable groups in which every subgroup is finitely generated.

Example

$G = \mathrm{Alt}(4) = \langle (1,3)(2,4), (1,2)(3,4), (1,2,3) \rangle$ where
$V = \langle (1,3)(2,4), (1,2)(3,4) \rangle \lhd G$ and $\mathbb{Z}_2 = \langle (1,3)(2,4) \rangle \lhd V$.

So $\mathrm{Alt}(4) \rhd V \rhd \mathbb{Z}_2$.

Let G be polycyclic with polycyclic series

$$G = G_1 \geq G_2 \geq \cdots \geq G_{n+1} = 1.$$

Since G_i/G_{i+1} is cyclic, there exist $x_i \in G$ with $\langle x_i G_{i+1} \rangle = G_i/G_{i+1}$ for every $i \in \{1, \ldots, n\}$.

Definition

$X = [x_1, \ldots, x_n]$ such that $\langle x_i G_{i+1} \rangle = G_i/G_{i+1}$ for $1 \leq i \leq n$ is a *polycyclic generating sequence* (PCGS) for G.

Definition

Let X be a PCGS sequence for G. $R(X) := (r_1, \ldots, r_n)$ defined by $r_i := |G_i : G_{i+1}| \in \mathbb{N} \cup \{\infty\}$ is the sequence of *relative orders* for X. Let $I(X) := \{i \in \{1 \ldots n\} \mid r_i \text{ finite}\}$.

Example

$X := [(1,2,3),(1,2)(3,4),(1,3)(2,4)]$ is PCGS for $\mathrm{Alt}(4)$ where $R(X) = (3,2,2)$ and $I(X) = \{1,2,3\}$.

Relative orders exhibit information about G.

G is finite iff every entry in $R(X)$ is finite or, equivalently iff $I(X) = \{1 \ldots n\}$.

If G is finite, then $|G| = r_1 \cdots r_n$, the product of the entries in $R(X)$.

Example

Let $G := \langle (1,2,3,4), (1,3) \rangle \cong D_8$.

a) Let $G_2 := \langle (1,2,3,4) \rangle \cong C_4$.
Then $G = G_1 \geq G_2 \geq G_3 = 1$ is polycyclic series for G.

$X := [(1,3), (1,2,3,4)]$ and
$Y := [(2,4), (1,4,3,2)]$ are PCGS defining this series.
$R(X) = R(Y) = (2,4)$ and $I(X) = I(Y) = \{1,2\}$.

b) Let $G_2 := \langle (1,2)(3,4), (1,3)(2,4) \rangle \cong V$ and
$G_3 := \langle (1,3)(2,4) \rangle \cong C_2$.

So $G = G_1 \geq G_2 \geq G_3 \geq G_4 = 1$.

$X := [(2,4), (1,2)(3,4), (1,3)(2,4)]$ and
$Y := [(1,2,3,4), (1,2)(3,4), (1,3)(2,4)]$ are polycyclic sequences defining this series.
$R(X) = R(Y) = (2,2,2)$ and $I(X) = I(Y) = \{1,2,3\}$.

Example

Let $G := \langle a, b \rangle$ with

$$a := \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } b := \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}.$$

$G \cong D_\infty$, the infinite dihedral group.

A polycyclic sequence for G is $X := [a, ab]$ with relative orders $R(X) = (2, \infty)$ and $I(X) = \{1\}$.

Lemma

Let $X = [x_1, \ldots, x_n]$ be a polycyclic sequence for G with the relative orders $R(X) = (r_1, \ldots, r_n)$. For every $g \in G$ there exists a sequence $(e_1, \ldots, e_n)$, with $e_i \in \mathbb{Z}$ for $1 \leq i \leq n$ and $0 \leq e_i < r_i$ if $i \in I(X)$, such that $g = x_1^{e_1} \cdots x_n^{e_n}$.

Proof.

Since $G_1/G_2 = \langle x_1 G_2 \rangle$, we find that $gG_2 = x_1^{e_1} G_2$ for some $e_1 \in \mathbb{Z}$.

If $1 \in I(X)$, then $r_1 < \infty$ and we can choose $e_i \in \{0 \ldots r_1 - 1\}$.

Let $h = x_1^{-e_1} g \in G_2$.

By induction on the length of a polycyclic sequence, we can assume that we know expression of the desired form for h; that is, $h = x_2^{e_2} \cdots x_n^{e_n}$.

Hence $g = x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$ as desired. □

Example

$G = \mathrm{Alt}(4)$

$X := [x_1 = (1,2,3), x_2 = (1,2)(3,4), x_3 = (1,3)(2,4)]$
is PCGS for G where $R(X) = (3,2,2)$ and $I(X) = \{1,2,3\}$.

$V = \langle x_2, x_3 \rangle$ and $H = \langle x_3 \rangle$.

$g = (1,2,4)$.

$gV = x_1^2 V$ so $x_1^{-2} g = (1,4)(2,3) \in V$.

Now $v := (1,4)(2,3)$ satisfies $vH = x_2 H$, so
$x_2^{-1} v = (1,3)(2,4) \in H$. Hence $x_2^{-1} v = x_3$ so $v = x_2 x_3$.

Hence $g = x_1^2 x_2 x_3$.

Normal form

Definition

The expression $g = x_1^{e_1} \cdots x_n^{e_n}$ is the *normal form* of $g \in G$ with respect to X.

The sequence $\exp_X(g) := (e_1, \ldots, e_n)$ is the *exponent vector* of g with respect to X.

Can define an injective map $G \to \mathbb{Z}^n : g \mapsto \exp_X(g)$ from G into the additive group of $\mathbb{Z}^n$. This is *not* a group homomorphism!

Polycyclic group to presentation?

Exponent vectors of elements of G can be used to describe relations for G in terms of X.

Lemma

Let $X = [x_1, \ldots, x_n]$ be a polycyclic sequence for G with relative orders $R(X) = (r_1, \ldots, r_n)$.

a) *Let $i \in I(X)$. The normal form of a power $x_i^{r_i}$ is* $x_i^{r_i} = x_{i+1}^{a_{i,i+1}} \cdots x_n^{a_{i,n}}$.

b) *Let $1 \leq j < i \leq n$. The normal form of a conjugate $x_j^{-1} x_i x_j$ is* $x_j^{-1} x_i x_j = x_{j+1}^{b_{i,j,j+1}} \cdots x_n^{b_{i,j,n}}$.

c) *Let $1 \leq j < i \leq n$. The normal form of a conjugate $x_j x_i x_j^{-1}$ is* $x_j x_i x_j^{-1} = x_{j+1}^{c_{i,j,j+1}} \cdots x_n^{c_{i,j,n}}$.

Polycyclic presentation

Definition

A presentation $\{ x_1, \ldots, x_n \mid R \}$ is a *polycyclic presentation* if there is a sequence $S = (s_1, \ldots, s_n)$ with $s_i \in \mathbb{N} \cup \{\infty\}$ and integers $a_{i,k}, b_{i,j,k}, c_{i,j,k}$ such that R consists of the following relations:

$$
\begin{aligned}
x_i^{s_i} &= x_{i+1}^{a_{i,i+1}} \cdots x_n^{a_{i,n}} \text{ for } 1 \leq i \leq n \text{ with } s_i < \infty, \\
x_j^{-1} x_i x_j &= x_{j+1}^{b_{i,j,j+1}} \cdots x_n^{b_{i,j,n}} \text{ for } 1 \leq j < i \leq n, \\
x_j x_i x_j^{-1} &= x_{j+1}^{c_{i,j,j+1}} \cdots x_n^{c_{i,j,n}} \text{ for } 1 \leq j < i \leq n.
\end{aligned}
$$

We describe the presentation by $\mathrm{Pc}\langle x_1, \ldots, x_n \mid R \rangle$. If G is defined by such a polycyclic presentation then G is a *PC-group*.

Group to presentation?

Every polycyclic group G has a polycyclic sequence X.

X induces a complete set of polycyclic relations.

The *power exponents* S of the presentation equal the relative orders $R(X)$ in this case.

Theorem

Every polycyclic sequence determines a (unique) polycyclic presentation. Thus every polycyclic group can be defined by a polycyclic presentation.

Example

Let $D_8 := \langle (1,3), (1,2,3,4) \rangle$ with polycyclic sequence $X := [(1,3), (1,2,3,4)]$ and relative orders $R(X) = (2,4)$.

Polycyclic presentation defined by X has generators x_1, x_2, power exponents $s_1 = 2$ and $s_2 = 4$. Relations are $x_1^2 = 1$, $x_2^4 = 1$, $x_1 x_2 x_1^{-1} = x_2^3$ and $x_1^{-1} x_2 x_1 = x_2^3$.

Example

S_4 has PCGS

$$X = [(3,4), (2,4,3), (1,3)(2,4), (1,2)(3,4)]$$

where $R(X) = (2,3,2,2)$.

$$\begin{aligned} \mathrm{Pc}\langle x_1, x_2, x_3, x_4 \quad | \quad & x_1^2 = x_2^3 = x_3^2 = x_4^2 = 1, x_2^{x_1} = x_2^2, \\ & x_3^{x_1} = x_3 x_4, x_3^{x_2} = x_4, x_4^{x_2} = x_3 x_4 \rangle \end{aligned}$$

Presentation to group?

Every polycyclic presentation defines a polycyclic group.

Theorem

Let G be group defined by $\mathrm{Pc}\langle x_1, \ldots, x_n \mid R \rangle$ with power-exponents S. Then G is polycyclic and $X = [x_1, \ldots, x_n]$ is a polycyclic sequence for G. Its relative orders $(r_1, \ldots, r_n)$ satisfy $r_i \leq s_i$ for $1 \leq i \leq n$.

Proof.

Define $G_i := \langle x_i, \ldots, x_n \rangle \leq G$. The conjugate relations in R enforce that G_{i+1} is normal in G_i for $1 \leq i \leq n$. By construction, G_i/G_{i+1} is cyclic and hence G is polycyclic. Since $G_i = \langle x_i G_{i+1} \rangle$ by definition, X is a polycyclic sequence for G. Finally, the power relations enforce that $r_i = |G_i : G_{i+1}| \leq s_i$ for $1 \leq i \leq n$. □

Example

Let G be defined by the following polycyclic presentation with power exponents $S = (3, 2, \infty)$.

$$G := \mathrm{Pc}\langle\, x_1, x_2, x_3 \quad | \quad x_1^3 = x_3,\ x_2^2 = x_3,$$
$$x_1^{-1} x_2 x_1 = x_2 x_3,\ x_1 x_2 x_1^{-1} = x_2 x_3 \,\rangle.$$

Hence $X = [x_1, x_2, x_3]$ is a polycyclic sequence for G with relative orders $R(X) \leq (3, 2, \infty)$.

But coset enumeration shows that the precise relative orders are $R(X) = (3, 2, 1)$.

Hence the power exponents in a polycyclic presentation give an **upper bound** for the relative orders only. Cannot read off from the power exponents whether G is finite or infinite.

Inconsistent presentations

Equivalently: polycyclic presentations in which two **different** normal words represent the **same** element of the group.

Example

$$\mathrm{Pc}\langle x_1, x_2, x_3 \mid x_1^2 = x_2, x_2^2 = x_3, x_3^2 = 1, [x_2, x_1] = x_3, [x_3, x_1] = 1, [x_3, x_2] = 1 \rangle$$

$$x_1x_2 = x_1x_1^2 = x_1^2x_1 = x_2x_1 = x_1x_2x_3.$$

Hence, not every element of the presented group has a unique normal form.

Consistent presentations

A polycyclic presentation in which every element is represented by exactly *one* normal word is *consistent*.

Equivalently: a polycyclic presentation $\mathrm{Pc}\langle X \mid R \rangle$ with power exponents S is *consistent* if $R(X) = S$.

Effective algorithm to convert an inconsistent presentation to a consistent one.

Example

$G := \mathrm{Pc}\langle x_1, x_2 \mid x_1^3 = 1,\ x_2^2 = 1, x_2^{x_1} = x_2 \rangle$ defines $\mathbb{Z}_6$.

Collection

A method to determine the *normal form* for an element in a group given by a polycyclic presentation.

Lemma

Let $G = \text{Pc}\langle X \mid R \rangle$ *be a polycyclic presentation with power exponents* S*. For every* $g \in G$ *there exists a word representing* g *of the form* $x_1^{e_1} \cdots x_n^{e_n}$ *with* $e_i \in \mathbb{Z}$ *and* $0 \le e_i < s_i$ *if* $s_i < \infty$*.*

Definition

Let $G = \mathrm{Pc}\langle X \mid R \rangle$. Write word w in X as a string $w = x_{i_1}^{a_1} \cdots x_{i_r}^{a_r}$ with $a_j \in \mathbb{Z}$. Assume that $i_j \neq i_{j+1}$ for $1 \leq j \leq r-1$ and $a_j \neq 0$ for $1 \leq j \leq r$.

a) A word w is *collected* if $w = x_{i_1}^{a_1} \cdots x_{i_r}^{a_r}$ with $i_1 < i_2 < \cdots < i_r$ and $a_j \in \{1, \ldots, s_j - 1\}$ if $s_j < \infty$. Otherwise w is *uncollected*.

b) A word u in X is a *minimal non-normal subword* of the word w if u is a subword of w and it has one of the following forms:
   i) $u = x_{i_j}^{a_j} \cdot x_{i_{j+1}}$ for $i_j > i_{j+1}$,
   ii) $u = x_{i_j}^{a_j} \cdot x_{i_{j+1}}^{-1}$ for $i_j > i_{j+1}$,
   iii) $u = x_{i_j}^{a_j}$ for $r_{i_j} \neq \infty$ and $a_j \notin \{1 \ldots s_{i_j} - 1\}$.

Word is collected if and only if it does not contain a minimal non-normal subword.

Example

$G = S_4$ has PCGS

$$X = [(3,4),(2,4,3),(1,3)(2,4),(1,2)(3,4)]$$

where $R(X) = (2,3,2,2)$ and

$$G = \mathrm{Pc}\langle x_1, x_2, x_3, x_4 \mid x_1^2 = x_2^3 = x_3^2 = x_4^2 = 1, x_2^{x_1} = x_2^2, x_3^{x_1} = x_3x_4, x_3^{x_2} = x_4, x_4^{x_2} = x_3x_4\rangle$$

$$\begin{aligned} x_2x_1 &\mapsto x_1x_2^2 \\ x_1x_2^{-1} &\mapsto x_1x_2^2 \\ x_2^{-1}x_4x_1 &\mapsto x_1x_2x_4 \\ x_4x_3x_2x_1 &\mapsto x_1x_2^2x_4 \end{aligned}$$

Usually write *power-commutator* presentation.

$$\begin{aligned}\mathrm{Pc}\langle x_1,\ldots,x_n \mid x_i^p &= \prod_{k=i+1}^{n} x_k^{\alpha(i,k)},\ 0\le \alpha(i,k) < p\,,\ 1\le i\le n\,,\\ [x_j,x_i] &= \prod_{k=j+1}^{n} x_k^{\beta(i,j,k)},\ 0\le \beta(i,j,k) < p, 1\le i<j\le n\rangle.\end{aligned}$$

An example

Let G be D_{16}

$$\begin{aligned} \text{Pc}\langle x_1, x_2, x_3, x_4 \quad | \quad & x_1^2 = 1, x_2^2 = x_3 x_4, \\ & x_3^2 = x_4, x_4^2 = 1, \\ & [x_2, x_1] = x_3, [x_3, x_1] = x_4, \\ & [x_3, x_2] = 1, [x_4, x_1] = 1, \\ & [x_4, x_2] = 1, [x_4, x_3] = 1\rangle \end{aligned}$$

Normal form for elements of G is

$$x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3} x_4^{\alpha_4}$$

where $0 \leq \alpha_i \leq 1$.

Every element of a p-group presented by a power-commutator presentation on $X := \{x_1, \ldots, x_n\}$ can be written as normal word

$$x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$$

where $0 \leq \alpha_i < p$.

Collection: introduced by P. Hall (1934), in the context of nilpotent groups.

Consider collection in context of all semigroup words on X. Inverses of words may be ignored since they can be eliminated using the power relations.

The input to the process is a word, w.

- If w is normal the process terminates.
- If w is not normal, it has a *minimal non-normal subword* u, where

$$u = x_i^p \qquad \text{or} \qquad u = x_j x_i$$

and $1 \leq i < j \leq n$.

Now replace u by

$$\prod_{k=i+1}^{n} x_k^{\alpha(i,k)} \qquad \text{or} \qquad x_i x_j \prod_{k=j+1}^{n} x_k^{\beta(i,j,k)},$$

where $0 \leq \alpha(\ldots), \beta(\ldots) < p$, respectively.

- Resulting word, w, is now input to the process.

Replacement of minimal non-normal subwords by their normal equivalents results in the construction of a normal word from an arbitrary word.

Theorem

Collection terminates.

Proof uses induction on $|X|$: $w \mapsto x_1 v$.

If w contains more than one minimal non-normal subword, a rule is used to determine which of the subwords is replaced by its normal equivalent, thereby ensuring that the process is well defined.

Collection strategies

- *Collection to the left* – all occurrences of x_1 are moved left to the beginning of the word. Next, all occurrences of x_2 are moved left until they are adjacent to the x_1's. *etc.*
  P. Hall (1934).
- *Collection from the right* – the minimal non-normal subword occurring nearest the end of a word is selected for replacement.
  Havas & Nicholson (1976).
- *Collection from the left* – the minimal non-normal subword nearest the beginning of a word is chosen for collection.

  Leedham-Green & Soicher (1990); Vaughan-Lee (1990).

Efficiency of the collection process is affected by the rule.

Collection from the left: most efficient.

Example

Consider D_{16}.

$$\begin{aligned} \text{Pc}\langle x_1, x_2, x_3, x_4 \quad | \quad & x_1^2 = 1, x_2^2 = x_3x_4, \\ & x_3^2 = x_4, x_4^2 = 1, \\ & [x_2, x_1] = x_3, [x_3, x_1] = x_4, \\ & [x_3, x_2] = 1, [x_4, x_1] = 1, \\ & [x_4, x_2] = 1, [x_4, x_3] = 1\rangle \end{aligned}$$

Suppose we collect $x_3x_2x_1$.

“To the left"

$$\mathrm{Pc}\langle x_1, x_2, x_3, x_4 \mid \begin{array}{l} x_1^2 = 1, x_2^2 = x_3x_4, \\ x_3^2 = x_4, x_4^2 = 1, \\ [x_2, x_1] = x_3, [x_3, x_1] = x_4, \\ [x_3, x_2] = 1, [x_4, x_1] = 1, \\ [x_4, x_2] = 1, [x_4, x_3] = 1\rangle \end{array}$$

$$\begin{aligned} 3\underline{21} &= \underline{31}23 \\ &= 13\underline{42}3 \\ &= 1\underline{32}43 \\ &= 123\underline{43} \\ &= 12\underline{33}4 \\ &= 12\underline{44} \\ &= 12 \end{aligned}$$

"From the right"

$$\mathrm{Pc}\langle x_1, x_2, x_3, x_4 \mid x_1^2 = 1, x_2^2 = x_3x_4, \\ x_3^2 = x_4, x_4^2 = 1, \\ [x_2, x_1] = x_3, [x_3, x_1] = x_4, \\ [x_3, x_2] = 1, [x_4, x_1] = 1, \\ [x_4, x_2] = 1, [x_4, x_3] = 1\rangle$$

$$\begin{aligned} 3\underline{21} &= \underline{31}23 \\ &= 13\underline{42}3 \\ &= 132\underline{43} \\ &= 1\underline{32}34 \\ &= 12\underline{33}4 \\ &= 12\underline{44} \\ &= 12 \end{aligned}$$

“From the left"

$$\begin{aligned}\mathrm{Pc}\langle x_1, x_2, x_3, x_4 \quad | \quad & x_1^2 = 1, x_2^2 = x_3 x_4, \\ & x_3^2 = x_4, x_4^2 = 1, \\ & [x_2, x_1] = x_3, [x_3, x_1] = x_4, \\ & [x_3, x_2] = 1, [x_4, x_1] = 1, \\ & [x_4, x_2] = 1, [x_4, x_3] = 1\rangle\end{aligned}$$

$$\begin{aligned}\underline{32}1 &= 2\underline{31} \\ &= \underline{21}34 \\ &= 12\underline{33}4 \\ &= 12\underline{44} \\ &= 12\end{aligned}$$

An exercise

$G = S_4$

$$\mathrm{Pc}\langle x_1, x_2, x_3, x_4 \quad | \quad x_1^2 = x_2^3 = x_3^2 = x_4^2, x_2^{x_1} = x_2^2, \\ x_3^{x_1} = x_3x_4, x_3^{x_2} = x_4, x_4^{x_2} = x_3x_4\rangle$$

$x_3x_2x_1 \mapsto x_1x_2^2x_3$

- 11 steps using "To the left".
- 5 steps using "From the left".

Number of normal forms

Given a consistent power-commutator presentation, the set of elements of G can be regarded as the set of normal words and the group multiplication is defined by collection:

the product of two normal words is the word which results from collecting their concatenation.

Order of G is the number of normal words.