Cambridge University Press & Assessment
978-1-316-60652-0 — Groups, Languages and Automata
Derek F. Holt , Sarah Rees , Claas E. Röver
Excerpt
More Information

PART ONE

INTRODUCTION

Cambridge University Press & Assessment
978-1-316-60652-0 — Groups, Languages and Automata
Derek F. Holt , Sarah Rees , Claas E. Röver
Excerpt
More Information

1
Group theory

1.1 Introduction and basic notation

In this book we are assuming that the reader has studied group theory at undergraduate level, and is familiar with its fundamental results, including the basic theory of free groups and group presentations. However, in many of the interactions between group theory and formal language theory, it is convenient to consider group presentations as special cases of semigroup and monoid presentations, so we describe them from that aspect here.

We refer the reader to one of the standard textbooks on group theory, such as [223] or [221] for the definitions and basic properties of nilpotent, soluble (solvable) and polycyclic groups,

We also include some specific topics, mainly from combinatorial group theory, that will be required later. The normal form theorems for free products with amalgamation and HNN-extensions are used in the proofs of the insolubility of the word problem in groups, and we summarise their proofs. We introduce Cayley graphs and their metrical properties, and the idea of *quasi-isometry* between groups, which plays a central role in the area and throughout geometric group theory, and we define the small cancellation properties of presentations and describe related results.

The final section of the chapter is devoted to a brief introduction to some of the specific families of groups, such as Coxeter groups and braid groups, that arise frequently as examples throughout the book. The informed reader may prefer not to read this chapter in detail, but to refer back to it as necessary.

1.1.1 Some basic notation For g, h in a group, we define the conjugate of g by h, often written as g^h, to be hgh^{-1} and the commutator $[g, h]$ to be $ghg^{-1}h^{-1}$. But we note that some authors use the notations g^h and $[g, h]$ to mean $h^{-1}gh$ and $g^{-1}h^{-1}gh$, respectively.

We recall that a *semigroup* is a set with an associative binary operation, usually written as multiplication, a *monoid* is a semigroup with an identity element, and a *group* is a monoid G in which every element is invertible.

We extend the multiplication of elements of a semigroup S to its subsets, defining $TU = \{tu : t \in T, u \in U\}$ and we frequently shorten $\{t\}U$ to tU, as we do for cosets of subgroups of groups.

1.1.2 Strings and words Strings over a finite set are important for us, since they are used to represent elements of a finitely generated group.

Let A be a finite set: we often refer to A as an *alphabet*. We call the elements of A its *letters*, and we call a finite sequence $a_1a_2\cdots a_k$ of elements from A a *string* or *word* of length k over A. We use these two terms interchangeably. We denote by ε the string of length 0, and call this the *null string* or *empty word*. For a word w, we write $|w|$ for the length of w.

We denote by A^k the set of all strings of length k over A, by A^* the set (or monoid) of all strings over A, and by A^+ the set (or semigroup) of all nonempty strings over A; that is

$$A^* = \bigcup_{k=0}^{\infty} A^k, \quad A^+ = \bigcup_{k=1}^{\infty} A^k = A^* \setminus \{\varepsilon\}.$$

For $w = a_1a_2\cdots a_k$ and $i \in \mathbb{N}_0$, we write $w(i)$ for the prefix $a_1a_2\cdots a_i$ of w when $0 < i \leq k$, $w(0) = \varepsilon$ and $w(i) = w$ for $i > k$.

In this book, A often denotes the set $X \cup X^{-1}$ of generators and their inverses for a group G; we abbreviate $X \cup X^{-1}$ as $X^{\pm}$. In this situation, we often refer to words in A^* as *words over* X even though they are really words over the alphabet A.

For $g \in G$, a word w over X of minimal length that represents g is called a *geodesic word* over X, and we denote the set of all such geodesic words by $\mathcal{G}(G, X)$. If w is an arbitrary word representing $g \in G$, then we write $|g|$ or $|w|_G$ (or $|g|_X$ or $|w|_{G,X}$ if X needs to be specified) for the length of a geodesic word over X that represents g. Similarly, we use $v = w$ to mean that the words v and w are identical as strings of symbols, and $v =_G w$ to mean that v and w represent the same element of the group.

We call a set of strings (i.e. a subset of A^*) a *language*; the study of languages is the topic of Chapter 2. It is convenient at this stage to introduce briefly the notation of a language for a group.

1.1.3 Languages for groups For a group G generated by X, we call a subset of $(X^{\pm})^*$ that contains at least one representative of each element in G a *language for* G; if the set contains precisely one representative of each element we call it a *normal form* for G. We shall be interested in finding *good* languages for a group G; clearly we shall need to decide what constitutes a good language. Typically we find good examples as the minimal representative words under a word order, such as word length or *shortlex*, $<_{\mathrm{slex}}$, defined below in 1.1.4. The *shortlex normal form* for a group selects the least representative of each group element under the shortlex ordering as its normal form word. The set $\mathcal{G}(G, X)$ of all geodesic words provides a natural language that is not in general a normal form.

1.1.4 Shortlex orderings *Shortlex* orderings (also known as *lenlex* orderings) of A^* arise frequently in this book. They are defined as follows. We start with any total ordering $<_A$ of A. Then, for $u, v \in A^*$, we define $u <_{\mathrm{slex}} v$ if either (i) $|u| < |v|$ or (ii) $|u| = |v|$ and u is less than v in the lexicographic (dictionary) ordering of strings induced by the chosen ordering $<_A$ of A.

More precisely, if $u = a_1 \cdots a_m$, $v = b_1 \cdots b_n$, then $u <_{\mathrm{slex}} v$ if either (i) $m < n$ or (ii) $m = n$ and, for some k with $1 \leq k \leq m$, we have $a_i = b_i$ for $i < k$ and $a_k <_A b_k$.

Note that $<_{\mathrm{slex}}$ is a well-ordering whenever $<_A$ is, which of course is the case when A is finite.

1.2 Generators, congruences and presentations

1.2.1 Generators If X is a subset of a semigroup S, monoid M or group G, then we define $\mathrm{Sgp}\langle X\rangle$, $\mathrm{Mon}\langle X\rangle$ or $\langle X\rangle$ to be the smallest subsemigroup, submonoid or subgroup of S, M or G that contains X. Then X is called a semigroup, monoid or group *generating set* if that substructure is equal to S, M or G respectively, and the elements of X are called *generators*.

We say that a semigroup, monoid or group is *finitely generated* if it possesses a finite generating set X.

1.2.2 Congruences If S is a semigroup and $\sim$ is an equivalence relation on S, then we say that $\sim$ is a *congruence* if

$$s_1 \sim s_2,\ t_1 \sim t_2 \implies s_1 t_1 \sim s_2 t_2.$$

We then define the semigroup $S/{\sim}$ to be the semigroup with elements the equivalence classes $[s] = \{t \in S : t \sim s\}$ of $\sim$, where $[s_1][s_2] = [s_1 s_2]$.

1.2.3 Presentations for semigroups, monoids and groups For a semigroup S generated by a set X, let $\mathcal{R} = \{(\alpha_i, \beta_i) : i \in I\}$ be a set of pairs of words from X^+ with $\alpha_i =_S \beta_i$ for each i. The elements of $\mathcal{R}$ are called *relations* of S. If $\sim$ is the smallest congruence on X^+ containing $\mathcal{R}$, and S is isomorphic to $X^+/\sim$, then we say that $\mathcal{R}$ is a *set of defining relations* for S, and that $\mathrm{Sgp}\langle X \mid \mathcal{R}\rangle$ is a *presentation* for S. In practice, we usually write $\alpha_i = \beta_i$ instead of (α_i, β_i). (This is an abuse of notation but the context should make it clear that we do not mean identity of words here.) Similarly the monoid presentation $\mathrm{Mon}\langle X \mid \mathcal{R}\rangle$ defines the monoid $X^*/\simeq$, for which $\simeq$ is the smallest congruence on X^* containing $\mathcal{R}$.

For groups the situation is marginally more complicated. If G is a group generated by a set X and $A = X^{\pm}$, then G is isomorphic to $A^*/\sim$, where $\sim$ is some congruence on A^* containing $\{(aa^{-1}, \varepsilon), (a^{-1}a, \varepsilon) : a \in X\}$. We define a *relator* of G to be a word $\alpha \in A^*$ with $\alpha =_G \varepsilon$. Let $R = \{\alpha_i : i \in I\}$ be a set of relators of G. If $\sim$ is the smallest congruence on A^* containing

$$\{(\alpha, \varepsilon) : \alpha \in R\} \cup \{(aa^{-1}, \varepsilon) : a \in X\} \cup \{(a^{-1}a, \varepsilon) : a \in X\},$$

and if G is isomorphic to $A^*/\sim$, then we say that R is a *set of defining relators* for G and that $\langle X \mid R\rangle$ is a *presentation* for G. Rather than specifying a relator α, so that α represents the identity, we can specify a *relation* $\beta = \gamma$ (as in the case of monoids or semigroups), which is equivalent to $\beta\gamma^{-1}$ being a relator.

We say that a semigroup, monoid or group is *finitely presented* (or, more accurately, *finitely presentable*) if it has a presentation in which the sets of generators and defining relations or relators are both finite.

1.2.4 Exercise Let $G = \langle X \mid R\rangle$ and let $A = X^{\pm}$. Show that

$$G \cong \mathrm{Mon}\langle A \mid \mathcal{I}_X \cup \mathcal{R}\rangle,$$

where $\mathcal{I}_X = \{(xx^{-1}, \varepsilon) : x \in X\} \cup \{(x^{-1}x, \varepsilon) : x \in X\}$ and $\mathcal{R} = \{(w, \varepsilon) : w \in R\}$.

1.2.5 Free semigroups, monoids and groups If S is a semigroup with presentation $\mathrm{Sgp}\langle X \mid \emptyset\rangle$ (which we usually write as $\mathrm{Sgp}\langle X \mid\rangle$), then we say that S is the *free semigroup* on X; we see that S is isomorphic to X^+ in this case. Similarly, if M is a monoid with presentation $\mathrm{Mon}\langle X \mid\rangle$, then we say that M is the *free monoid* on X, and we see that M is then isomorphic to X^*. If $S = X^+$ and $L \subseteq S$, then $\mathrm{Sgp}\langle L\rangle = L^+$; similarly, if $M = X^*$ and $L \subseteq M$, then $\mathrm{Mon}\langle L\rangle = L^*$.

If F is a group with a presentation $\langle X \mid\rangle$, then we say that F is the *free group* on X; if $|X| = k$, then we say that F is the free group of *rank* k (any two free groups of the same rank being isomorphic). We write $F(X)$ for the free group on X and F_k to denote a free group of rank k.

1.2.6 Exercise Let $G = \langle X \mid R\rangle$ be a presentation of a group G. Show that the above definition of G, which is essentially as a monoid presentation, agrees with the more familiar definition $\langle X \mid R\rangle = F(X)/\langle R^{F(X)}\rangle$, where $\langle R^{F(X)}\rangle$ denotes the normal closure of R in $F(X)$.

1.2.7 Reduced and cyclically reduced words In $F(X)$, the free group on X, every element has a unique representation of the form $w = x_1^{\epsilon_1} x_2^{\epsilon_2} \ldots x_n^{\epsilon_n}$, where $n \geq 0$, $x_i \in X$ and $\epsilon_i \in \{1, -1\}$ for all i, and where we do not have both $x_i = x_{i+1}$ and $\epsilon_i = -\epsilon_{i+1}$ for any i; in this case, we say that the word w is *reduced*. Each word $v \in A^*$ is equal in $F(X)$ to a unique reduced word w.

If w is a reduced word and w is not of the form $x^{-1}vx$ or xvx^{-1} for some $x \in X$ and $v \in A^*$, then we say that w is *cyclically reduced*. Since replacing a defining relator by a conjugate in $F(X)$ does not change the group defined, we may (and often do) assume that all defining relators are cyclically reduced words.

1.3 Decision problems

In his two well-known papers in 1911 and 1912 [75, 76], Dehn defined and considered three decision problems in finitely generated groups, the word, conjugacy and isomorphism problems. While the word problem in groups is one of the main topics studied in this book, the other two will only be fleetingly considered. A good general reference on these and other decision problems in groups is the survey article by Miller [192].

1.3.1 The word problem A semigroup S is said to have *soluble word problem* if there exists an algorithm that, for any given words $\alpha, \beta \in X^+$, decides whether $\alpha =_S \beta$. The solubility of the word problem for a monoid or group generated by X is defined identically except that we consider words α, β in X^* or $(X^{\pm})^*$. For groups, the problem is equivalent to deciding whether an input word is equal to the identity element. The word problem for groups is discussed further in Chapter 3 and in Part Three of this book. Examples of finitely presented semigroups and groups with insoluble word problem are described in Theorems 2.9.7 and 10.1.1.

1.3.2 The conjugacy and isomorphism problems The conjugacy problem in a semigroup S is to decide, given two elements $x, y \in S$, whether there exists $z \in S$ with $zx = yz$. Note that this relation is not necessarily symmetric in x and

Cambridge University Press & Assessment
978-1-316-60652-0 — Groups, Languages and Automata
Derek F. Holt , Sarah Rees , Claas E. Röver
Excerpt
More Information

y, but in a group G it is equivalent to deciding whether x and y are conjugate in G.

Since the word problem in a group is equivalent to deciding whether an element is conjugate to the identity, the conjugacy problem is at least as hard as the word problem, and there are examples of groups with soluble word problem but insoluble conjugacy problem. A number of such examples are described in the survey article by Miller [192], including Theorem 4.8 (an extension of one finitely generated free group by another), Theorem 4.11 (examples showing that having soluble conjugacy problem is not inherited by subgroups or overgroups of index 2), Theorem 5.4 (residually finite examples), Theorem 6.3 (a simple group), Theorem 7.7 (asynchronously automatic groups), and Theorem 7.8 (groups with finite complete rewriting systems) of that article.

The isomorphism problem is to decide whether two given groups, monoids or semigroups are isomorphic. Typically the input is defined by presentations, but could also be given in other ways, for example as groups of matrices. There are relatively few classes for which the isomorphism problem is known to be soluble. These classes include polycyclic and hyperbolic groups [232, 234, 72].

1.3.3 The generalised word problem Given a subgroup H of a group G, the generalised word problem is to decide, given $g \in G$, whether $g \in H$. So the word problem is the special case in which H is trivial. We shall encounter some situations in which this problem is soluble in Chapter 8. As for the conjugacy problem, the survey article [192] is an excellent source of examples (in particular in Theorems 5.4 and 7.8 of that article), in this case of groups with soluble word problem that have finitely generated subgroups with insoluble generalised word problem.

1.4 Subgroups and Schreier generators

Let H be a subgroup of a group $G = \langle X \rangle$, and let U be a right transversal of H in G. For $g \in G$, denote the unique element of $Hg \cap U$ by $\overline{g}$. Define

$$Z := \left\{ux\overline{ux}^{-1} : u \in U, x \in X\right\}.$$

Then $Z \subseteq H$.

1.4.1 Theorem *With the above notation, we have $H = \langle Z \rangle$.*

Our proof needs the following result.

1.4.2 Lemma *Let $S = \{ux^{-1}\overline{ux^{-1}}^{-1} : u \in U, x \in X\}$. Then $Z^{-1} = S$.*

Proof Let $g \in Z^{-1}$, so $g = (ux\overline{ux}^{-1})^{-1} = \overline{ux}x^{-1}u^{-1}$. Let $v := \overline{ux} \in U$. Then, since the elements vx^{-1} and u are in the same coset of H, we have $\overline{vx^{-1}} = u$, and $g = vx^{-1}\overline{vx^{-1}}^{-1} \in S$.

Conversely, let $g = ux^{-1}\overline{ux^{-1}}^{-1} \in S$, so $g^{-1} = \overline{ux^{-1}}xu^{-1}$. Let $v := \overline{ux^{-1}}$. Then $\overline{vx} = u$, so $g^{-1} = vx\overline{vx}^{-1} \in Z$ and $g \in Z^{-1}$. □

Proof of Theorem 1.4.1 Let $U \cap H = \{u_0\}$. (We usually choose $u_0 = 1$, but this is not essential.) Let $h \in H$. Then we can write $u_0^{-1}hu_0 = a_1 \cdots a_l$ for some $a_i \in A := X^{\pm}$. For $1 \le i \le l$, let $u_i := \overline{a_1 \cdots a_l}$. Since $u_0^{-1}hu_0 \in H$, we have $u_l = u_0$. Then

$$h =_G (u_0a_1u_1^{-1})(u_1a_2u_2^{-1})\cdots(u_{l-1}a_lu_l^{-1}).$$

Note that $u_{i+1} = \overline{a_1 \cdots a_{l+1}}$ is in the same coset of H as u_ia_{i+1}, so $\overline{u_ia_{i+1}} = u_{i+1}$, and

$$h =_G (u_0a_1\overline{u_0a_1}^{-1})(u_1a_2\overline{u_1a_2}^{-1})\cdots(u_{l-1}a_l\overline{u_{l-1}a_l}^{-1}). \qquad (\dagger)$$

Each bracketed term is in Z if $a_i \in X$, and in Z^{-1} if $a_i \in X^{-1}$ by Lemma 1.4.2. So $H = \langle Z\rangle$. □

1.4.3 Corollary *A subgroup of finite index in a finitely generated group is finitely generated.*

1.4.4 Rewriting The process described in the above proof of calculating a word v over Z from a word w over X that represents an element of H is called *Reidemeister–Schreier rewriting*. We may clearly omit the identity element from the rewritten word, which results in a word over $Y = Z \setminus \{1\}$, which we denote by $\rho_{X,Y}(w)$. From the proof, we see immediately that:

1.4.5 Remark If $1 \in U$, then $|\rho_{X,Y}(w)| \le |w|$.

1.4.6 Schreier generators and transversals The above set Y of non-identity elements of Z is called the set of *Schreier generators* of H in G. Of course, this set depends on X and on U.

The set U is called a *Schreier transversal* if there is a set of words over X representing the elements of U that is closed under taking prefixes. Note that such a set must contain the empty word, and hence $1 \in U$. By choosing the least word in each coset under some *reduction ordering* of A^* (where $A = X^{\pm}$), it can be shown that Schreier transversals always exist. Reduction orderings are defined in 4.1.5. They include the shortlex orderings defined in 1.1.4.

It was proved by Schreier [228] that, if G is a free group and U is a Schreier transversal, then the Schreier generators freely generate H.

The following result, known as the *Reidemeister–Schreier Theorem*, which we shall not prove here, provides a method of computing a presentation of the subgroup H from a presentation of the group G. Note that it immediately implies the celebrated *Nielsen–Schreier Theorem*, that any subgroup of a free group is free. As with many of the results stated in this chapter, we refer the reader to the standard textbook on combinatorial group theory by Lyndon and Schupp [183] for the proof.

1.4.7 Theorem (Reidemeister–Schreier Theorem [183, Proposition II.4.1]) *Let $G = \langle X \mid R \rangle = F/N$ be a group presentation, where $F = F(X)$ is the free group on X, and let $H = E/N \le G$. Let U be a Schreier transversal of E in F and let Y be the associated set of Schreier generators. Then $\langle Y \mid S \rangle$ with $S = \left\{\rho_{X,Y}(uru^{-1}) : u \in U, r \in R\right\}$ is a presentation of H.*

1.4.8 Corollary *A subgroup of finite index in a finitely presented group is finitely presented.*

1.5 Combining groups

In this section we introduce various constructions that combine groups. We leave the details of many of the proofs of stated results to the reader, who is referred to [183, Chapter IV] for details.

1.5.1 Free products Informally, the *free product* $G * H$ of the groups G, H is the largest group that contains G and H as subgroups and is generated by G and H. Formally, it can be defined by its universal property:

(i) there are homomorphisms $\iota_G \colon G \to G * H$ and $\iota_H \colon H \to G * H$;
(ii) if K is any group and $\tau_G \colon G \to K$, $\tau_H \colon H \to K$ are homomorphisms, then there is a unique homomorphism $\alpha \colon G * H \to K$ with $\alpha\iota_G = \tau_G$ and $\alpha\iota_H = \tau_H$.

As is often the case with such definitions, it is straightforward to prove uniqueness, in the sense that any two free products of G and H are isomorphic, and it is not hard to show that $G * H$ is generated by $\iota_G(G)$ and $\iota_H(H)$. But the existence of the free product is not immediately clear.

To prove existence, let $G = \langle X \mid R \rangle$ and $H = \langle Y \mid S \rangle$ be presentations of G and H. Then we can take

$$G * H = \langle X \cup Y \mid R \cup S \rangle,$$

where ι_G and ι_H are the homomorphisms induced by the embeddings $X \to X \cup Y$ and $Y \to X \cup Y$; we tacitly assumed that X and Y are disjoint.

It is not completely obvious that ι_G and ι_H are monomorphisms. This follows from another equivalent description of $G * H$ as the set of alternating products of arbitrary length (including length 0) of non-trivial elements of G and H, with multiplication defined by concatenation and multiplications within G and H. With this description, ι_G and ι_H are the obvious embeddings, and G and H are visibly subgroups of $G * H$, known as the *free factors* of $G * H$. The equivalence of the two descriptions follows immediately in a more general context from Proposition 1.5.12.

The definition extends easily to the free product of any family of groups. The following result, which we shall not prove here, is used in the proof of the special case of the Muller–Schupp Theorem (Theorem 11.1.1) that torsion-free groups with context-free word problem are virtually free.

1.5.2 Theorem (Grushko's Theorem [183, IV.1.9]) *For a group G, let $d(G)$ denote the minimal number of generators of G. Then $d(G * H) = d(G) + d(H)$.*

1.5.3 Direct products The *direct product* $G \times H$ of two groups G, H is usually defined as the set $G \times H$ with component-wise multiplication. We generally identify G and H with the component subgroups, which commute with each other, and are called the *direct factors* of $G \times H$. Then each element has a unique representation as a product of elements of G and H. It can also be defined by a universal property:

(i) there are homomorphisms $\pi_G\colon G \times H \to G$ and $\pi_H\colon G \times H \to H$;
(ii) if K is any group and $\tau_G\colon K \to G$ and $\tau_H\colon K \to H$ are homomorphisms, then there is a unique homomorphism $\varphi\colon K \to G \times H$ with $\tau_G = \pi_G \circ \varphi$ and $\tau_H = \pi_H \circ \varphi$.

If $G = \langle X \mid R \rangle$ and $H = \langle Y \mid S \rangle$ are presentations, then $G \times H$ has the presentation

$$G \times H = \langle X \cup Y \mid R \cup S \cup \{[x, y] : x \in X, y \in Y\} \rangle.$$

We can extend this definition to direct products of families of groups as follows. Let $\{G_\omega : \omega \in \Omega\}$ be a family of groups. Then the *(full) direct product*, also known sometimes as the *Cartesian product*, $\prod_{\omega \in \Omega} G_\omega$ of the family consists of the set of functions $\beta\colon \Omega \to \cup_{\omega \in \Omega} G_\omega$ for which $\beta(\omega) \in G_\omega$ for all $\omega \in \Omega$, where the group operation is component-wise multiplication in each G_ω; that is, $\beta_1\beta_2(\omega) = \beta_1(\omega)\beta_2(\omega)$ for all $\omega \in \Omega$.