

Section VII.40. Group Presentations

Note. The idea of group presentation is to give the generators of a group along with a collection of equations which relates the generators to each other. In this way, a very large group can be “presented” in a compact form, as opposed to giving the table for the group (which could be very large). In this section, we define group presentation, give examples, and illustrate its use in determining the existence or nonexistence of groups of certain orders.

Example. In the exercises of this section (primarily Exercise 11, but it also involves other exercises in this section) it is shown that a group with generating set $\{a, b\}$ where elements a and b satisfy the three equations $a^3 = 1$, $b^2 = 1$, and $ba = a^2b$ must be isomorphic to $S_3 \cong A_3$. That is, a *group presentation* of $S_3 \cong A_3$ is $(a, b : a^3 = 1, b^2 = 1, ba = a^2b)$.

Note. The *ATLAS of Finite Groups* by Conway, Curtis, Norton, Parker, and Wilson (Oxford: Clarendon Press, 1985) mentioned in my “Small Groups” supplement to the note of Section 11 gives the presentation of certain very large (but finite) groups. In particular (as an elementary example), a presentation of A_5 is given on page *xviii* of the *ATLAS* as $(a, b : a^2 = b^3 = (ab)^5 = 1)$. So the group A_5 is described using just four pieces of information: (1) there are two generators a and b , (2) $a^2 = 1$, (3) $b^3 = 1$, and (4) $(ab)^5 = 1$. A group table of the nonabelian A_5 , on the other hand, involves $|A_5|^2 = (60)^2 = 3600$ entries.

Note. An online relative of the ATLAS is “ATLAS of Finite Groups—Version 3” and is available online at <http://brauer.maths.qmul.ac.uk/Atlas/vs/> (accessed 3/8/2014). This gives a presentation of the group M_{11} (a “Mathieu group”—see my “Finite Simple Groups” supplement to Section 15). The group is of order $|M_{11}| = 7920$ and a table for the group would consist of $(7920)^2 = 62,726,400$ entries. The online ATLAS gives a presentation of M_{11} as $(a, b : a^2 = 1, b^4 = 1, (ab)^{11} = 1, (abababbababbabb)^4 = 1)$.

Note. In my supplement “Small Groups” I mentioned the “dicyclic group of order 12.” This group has presentation $(a, b : a^6 = 1, a^3 = b^2, b^{-1}ab = a^{-1})$ (from Gallian, page 453). So this gives us some idea of the structure of a group we have not explored before.

Note. As suggested in the past, dihedral groups are generated by two elements. In fact (see Exercise 26.9 of Gallian) a group presentation of D_n is $(a, b : a^n = 1, b^2 = 1, (ab)^2 = 1)$. In fact, the dihedral group can be classified in terms of the properties of the generators:

Theorem. Characterization of Dihedral Groups. (Gallian’s Theorem 26.5.)

Any group generated by a pair of elements of order 2 is dihedral.

The two generators here are considered to be b and ab (as opposed to a and b). Geometrically, b represents a “flip” of the n -gon and a represents a rotation through $2\pi/n$ radians (say). For this theorem to be true, we must introduce the infinite dihedral group D_∞ with presentation $(a, b : a^2 = b^2 = 1)$.

Example 40.1. Suppose group G has generators x and y and that we impose the relation $xy = yx$ (or equivalently $xyx^{-1}y^{-1} = 1$). Then G is a free abelian group with basis $\{x, y\}$. So by the comments in the last note of Section 39, $G \cong F[\{x, y\}]/C$ where C is the commutator subgroup of $F[\{x, y\}]$.

Note. Any equation in $F[A]$ can be written in a form where the right-hand side is 1. For example, the equation $ba = a^2b$ in the above presentation of $S_3 \cong A_3$ can be replaced with $a^{-1}bab^{-1} = 1$. So a collection of equations in $F[A]$ can be written as $r_i = 1$ for $i \in I$ where $r_i \in F[A]$ (so r_i is a product of powers of the elements of A). With each $r_i = 1$, then $x(r_i^n)x^{-1} = 1$ for any $x \in F[A]$ and $n \in \mathbb{Z}$. Also any product of elements equal to 1 is again equal to 1. So any finite product of the form $\prod_j x_j(r_{i_j}^{n_j})x_j^{-1}$ must equal 1 (where the r_{i_j} need not be distinct). Let R be the set of all products. Then R is a subgroup of $F[A]$ since $1 \in R$ and for any product of elements of A which equal 1 has an inverse whose elements multiply to give 1 (for example, if $a^2b^3 = 1$ then $b^{-3}a^{-2} = 1$). In fact, R is a normal subgroup of $F[A]$ since for all $f \in F[A]$ we have $fR = Rf$ (since $r \in R$ implies $r = 1$ and so $fr = f \cdot 1 = 1 \cdot f = rf$). Then the group $F[A]/R$ is a group (in Fraleigh's words) "as much like $F[A]$ as it can be, subject to certain equations that we want satisfied" (the equations are the $r_i \in R$).

Note. Now that we have an intuitive idea of what a group presentation is, we give the formal definition. However, we will not really use the formal definition in our applications; the informal idea will suffice for our applications.

Definition 40.2. Let A be a set and let $\{r_i\} \subseteq F[A]$. Let R be the least normal subgroup of $F[A]$ containing the r_i . An isomorphism ϕ of $F[A]/R$ onto a group G is a *presentation* of G . The sets A and $\{r_i\}$ give a *group presentation*. The set A is the *set of generators for the presentation* and each r_i is a *relator*. Each $r \in R$ is a *consequence* of $\{r_i\}$. An equation $r_i = 1$ is a *relation*. A *finite presentation* is one in which both A and $\{r_i\}$ are finite sets.

Example 40.3. Consider the group presentation $(a : a^6 = 1)$. Of course, this group is isomorphic to \mathbb{Z}_6 (technically, the group is $F[\{a\}]/\{a^6\}$). Now consider the group with two generators a and b where $a^2 = 1$, $b^3 = 1$, and $ab = ba$. The presentation is $(a, b : a^2 = 1, b^3 = 1, aba^{-1}b^{-1} = 1)$. Since $a^2 = 1$ then $a^{-1} = a$. Since $b^3 = 1$ then $b^{-1} = b^2$. Since $ab = ba$, the group is abelian and every element is then of the form $a^m b^n$ (where m is 0 or 1 and $n = 0, 1, 2$). The elements are then $1 = a^0 b^0$, $a = a^{-1}$, b , $b^2 = b^{-1}$, ab , ab^2 . Since we are dealing with a group of order 6 which is abelian, this must be another presentation of a group isomorphic to \mathbb{Z}_6 .

Definition. When two presentations describe the same group (up to isomorphism), we have isomorphic presentations.

Note. Fraleigh comments on page 348 that there is no “*routine* and well-defined way” of determining, in general, when two group presentations are isomorphic.

Example 40.5. There is a unique nonabelian group of order 10.

Suppose that G is a nonabelian group of order 10. By the First Sylow Theorem (Theorem 36.8) G has a subgroup H of order 5. The only group of order 5 up to isomorphism is \mathbb{Z}_5 so H is cyclic. Let $H = \langle a \rangle$. Notice that by the Third Sylow Theorem (Theorem 36.11) H is a normal subgroup of G . So G/H exists and is of order 2; hence G/H is isomorphic to \mathbb{Z}_2 . If $b \in G$ and $b \notin H$ then $b^2 \in H$ (since G/H consists of two cosets, say bH and $b^2H = H$. H consists of four elements of order 5 and the identity a . If $b^2 \in H$ is of order 5, then b is of order 10 and $G = \langle b \rangle$, contradicting the fact that G is nonabelian. So it must be that $b^2 = 1$. Since H is a normal subgroup of G , then $bab^{-1} \in H$ (Theorem 14.13) and, in particular, $bab^{-1} \in H$. Since conjugation by b is an automorphism of H (the inner automorphism of G , i_b —see Definition 14.15) and $bab^{-1} \neq 1$ (because $bab^{-1} = 1$ implies $ba = b$ or $a = b^{-1}b = 1$, a contradiction), then bab^{-1} must be an element of H of order 5. So bab^{-1} must be either a , a^2 , a^3 , or a^4 . But $bab^{-1} = a$ implies $ba = ab$ and this implies, since a and b are generators of G , that G is abelian, a contradiction. So this leaves three possible presentations for G :

1. $(a, b : a^5 = 1, b^2 = 1, ba = a^2b)$,
2. $(a, b : a^5 = 1, b^2 = 1, ba = a^3b)$,
3. $(a, b : a^5 = 1, b^2 = 1, ba = a^4b)$.

The relation $ba = a^i b$ allows us to move all a 's to the left and all b 's to the right in any product (for example, $b^2 ab^3 = b(ba)b^3 = babb^3 = (ab)b^4 = ab^5$). So every element of G is of the form $a^s b^t$. Since $a^5 = 1$ and $b^2 = 1$, then the 10 possible

elements of G are:

$$\begin{aligned} & \{a^0b^0, a^1b^0, a^2b^0, a^3b^0, a^4b^0, a^0b^1, a^1b^1, a^2b^1, a^3b^1, a^4b^1\} \\ & = \{1, a, a^2, a^3, a^4, b, ab, a^2b, a^3b, a^4b\}. \end{aligned}$$

We now analyze the three presentations.

Consider $(a, b : a^5 = 1, b^2 = 1, ba = a^2b)$. This implies

$$\begin{aligned} a &= 1 \cdot a = b^2a = b(ba) = b(a^2b) = (ba)(ab) = (a^2b)(ab) \\ &= a^2(ba)b = a^2(a^2b)b = a^4b^2 = a^4 \cdot 1 = a^4. \end{aligned}$$

But $a = a^4$ implies that $a^3 = 1$, contradicting the fact that a is of order 5. In fact, $a^3 = 1$ and $a^5 = 1$ combine to imply that $a = 1$. In this case, the elements of G are b and $b^2 = 1$. So this presentation implies a group isomorphic to \mathbb{Z}_2 .

Consider $(a, b : a^5 = 1, b^2 = 1, ba = a^3b)$. Again,

$$\begin{aligned} a &= 1 \cdot a = b^2a = (b(ba)) = ba^3b = (ba)(a^2b) = (a^3b)(a^2b) = a^3(ba)ab \\ &= a^3(a^3b)ab = a^6(ba)b = a^6(a^3b)b = a^9b^2 = a^4a^5b^2 = a^4 \cdot 1 \cdot 1 = a^4. \end{aligned}$$

So this and the previous presentation are isomorphic presentations and again we have a presentation of \mathbb{Z}_2 .

Consider $(a, b : a^5 = 1, b^2 = 1, ba = a^4b)$. As in the equations above, we use the relation $ba = a^4b$ to express a product $(a^s b^t)(a^u b^v)$ in the form $a^x b^y$. This leads to x being the remainder when $s + u(4^t)$ is divided by 5 and y being the remainder when $t + v$ is divided by 2. We have $a^0 b^0$ as the identity, and that by defining first $t \equiv -v \pmod{2}$ and second $s \equiv -u(4^t) \pmod{5}$, element $a^s b^t$ is a left inverse of $a^u b^v$. So we have a group structure on the 10 elements if associativity holds. Since

$4^2 \equiv 1 \pmod{5}$, by Exercise 40.13, associativity holds. So we have a presentation of a nonabelian group of order 10 and any other nonabelian group of order 10 must be isomorphic to this group. Since D_5 is an example of such a group, then this presentation must be a group presentation for D_5 and D_5 is the unique (up to isomorphism) nonabelian group of order 10.

Example 40.6. There are 5 groups of order 8.

By the Fundamental Theorem of Finitely Generated Abelian Groups (Theorem 11.12), there are three abelian groups of order 8: $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, and \mathbb{Z}_8 . We now use group presentations to classify the nonabelian groups of order 8.

Let G be a nonabelian group of order 8. Since G is nonabelian, it has no elements of order 8. So each element of G (other than 1) is of order 2 or 4. If every such element is of order 2, then for $a, g \in G$ we would have $(ab)^2 = 1$ or $abab = 1$. But then, since $a^2 = b^2 = 1$, we would have $ba = a^2bab^2 = a(ab)^2b = a \cdot 1 \cdot b = ab$ and G would be abelian. Thus G must have an element of order 4.

Let $\langle a \rangle$ be a subgroup of G of order 4. So there are only two cosets of $\langle a \rangle$ in G ; one coset is $\langle a \rangle = g\langle a \rangle = \langle a \rangle g$ for $g \in \langle a \rangle$ and the other coset is $g\langle a \rangle = \langle a \rangle g$ for $g \notin \langle a \rangle$. So $\langle a \rangle$ is a normal subgroup of G . So $G/\langle a \rangle$ exists and is of order 2, so $G/\langle a \rangle \cong \mathbb{Z}_2$. As in the previous example, since $b \notin \langle a \rangle$, then $b^2 \in \langle a \rangle$ (and the cosets of $\langle a \rangle$ are $b\langle a \rangle$ and $b^2\langle a \rangle = \langle a \rangle$). If $b^2 = a$ or $b^3 = a$ then b would be of order 8. Hence $b^2 = 1$ or $b^2 = a^2$. Since $\langle a \rangle$ is normal, we have $bab^{-1} \in \langle a \rangle$ by Theorem 14.13, and $b\langle a \rangle b^{-1}$ is a subgroup of G conjugate to $\langle a \rangle$ and hence isomorphic to $\langle a \rangle$ (under the inner automorphism i_b —see Definition 14.15), so bab^{-1} must be an element of order 4. So $bab^{-1} = a$ or $bab^{-1} = a^3$. If $bab^{-1} = a$, then $ba = ab$ and G

is abelian since a and b are generators of G , a contradiction. So it must be that $bab^{-1} = a^3$ and $ba = a^3b$. So we have two possible presentations for G :

$$G_1 = (a, b : a^4 = 1, b^2 = 1, ba = a^3b),$$

$$G_2 = (a, b : a^4 = 1, b^2 = a^2, ba = a^3b).$$

Notice that in both G_1 and G_2 we have $a^{-1} = a^3$. In G_1 , $b^{-1} = b$. In G_2 , $b^{-1} = b^3$. As in the other examples of this section, $ba = a^3b$ allows us to write every element in the form $a^m b^n$. Since $a^4 = 1$ and $b^2 = 1$, we get the 8 elements: $a, a, a^2, a^3, b, ab, a^2b, a^3b$. Since in G_1 with $m = 4$, $n = 2$, $r = 3$, Exercise 401.3 gives $r^n = 3^2 \equiv 1 \pmod{4} = 1 \pmod{m}$, so G_1 determines a group of order $mn = 8$. Fraleigh states that “An argument similar to that used in Exercise 13 shows that G_2 has order 8 also.”

Since $ba = a^3b \neq ab$ (since $a^2 \neq 1$), then both G_1 and G_2 are nonabelian. We can show that G_1 and G_2 are not isomorphic by considering elements of certain orders. Based on the 8 elements listed above, we can confirm that G_1 has two elements of order 4 (a and a^3). In G_2 all elements are of order 4 except 1 and a^2 . The group tables are asked for in Exercise 40.3. In fact, $G_1 \cong D_4$ and is sometimes called the *octic group*. G_2 is isomorphic to the *quaternion group* which was introduced in Section 24.

Note. Arthur Cayley in his 1859 paper “On the Theory of Groups as Depending on the Symbolic Equation $\theta^n = 1$. Third Part,” gives a presentation of the octic group and shows that $(a, b : a^m = 1, b^n = 1, ba = a^r b)$ is the presentation of a group of order mn if and only if $r^n \equiv 1 \pmod{m}$ (this is Exercise 40.13). In the early

1890s, Otto Hölder, using the techniques of Sections 36, 37, and 40 (Sylow theory and group presentations—recall that the Sylow Theorems were proved for abstract groups by Frobenius in 1887) to classify all simple groups up to order 200, and all groups of orders p^3 , pq^2 , pqr , and p^4 where p, q, r are distinct primes.

Revised: 3/9/2014