Describing a Group

Suppose you have a group --How can you communicate it to someone? The most direct way is to give the multiplication table: you list (i.e. name) all the elements of the group and tell how they multiply. For example, you could communicate the cyclic group of order 3 by saying the group G has three elements, which you choose to call \(a, b, c\), and they multiply by the rules...

\[
\begin{array}{ccc}
  & a & b & c \\
 a & a & b & c \\
b & b & c & a \\
c & c & a & b \\
\end{array}
\]

If someone else wrote the group

\[
\begin{array}{ccc}
  & x & y & z \\
x & x & y & z \\
y & y & z & x \\
z & z & x & y \\
\end{array}
\]

you could see that the two groups are isomorphic because the function \(a \rightarrow x, b \rightarrow y, c \rightarrow z\) is a bijection of the sets that respects the multiplication.

Giving a group via a table like this lets a person verify that the structure is indeed a group: “a” is an identity, multiplication is associative, etc. **But if you know that the structure is a group,** then you don't really need to give the whole table. Let's see how much of the first table is not really necessary.

We know that in a group, if \(a\) is a left identity, then \(a\) also is a right identity: . So some items in the table are redundant (provided we know that the table is describing a group, rather than wanting to use the information in the table to check that the structure really is a group).
\[
\begin{array}{ccc}
|   & a & b & c \\
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>a &amp; b &amp; c</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b</td>
<td>b &amp; c &amp; a</td>
<td></td>
<td></td>
</tr>
<tr>
<td>c</td>
<td>e &amp; a &amp; b</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
\end{array}
\]

In fact, once we know that \(aa=a\), we know \(a\) is the identity element, so the rest of row 1 is redundant. Let's also replace the symbol \(a\) with the symbol \(1\) to remind us that this is the identity element.

\[
\begin{array}{ccc}
|   & 1 & b & c \\
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1 &amp; b &amp; e</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b</td>
<td>b &amp; c &amp; 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>c</td>
<td>e &amp; 1 &amp; b</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
\end{array}
\]

The (remaining) equations in row 2 imply the (remaining) equations in row 3 as follows: \(bb = c\) and \(bc = 1 \Rightarrow b^3 = 1\). Then we can deduce the third row: \(cb = (bb)b = b^3 = 1\), and \(cc = (bb)(bb) = (bbb)(b) = (1)b = b\). So our economical table now is

\[
\begin{array}{ccc}
|   & 1 & b & c \\
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1 &amp; b &amp; e</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b</td>
<td>b &amp; c &amp; 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>c</td>
<td>e &amp; 1 &amp; b</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
\end{array}
\]

Now let's try to shorten the list of elements. We already replaced the element \(a\) by \(1\); each group has such an element, so we really don't need to list it (and row 1) separately. In row 2, we have \(bb = c\). This tells us that \(c\) is just a symbol denoting \(b^2\). Any group with an element \(b\), of course also has the element \(b^2\) (either as a new element or the identity - in this case a new element). So we don't need to list \(c\) as a group element since we already have \(b, b^2, b^3, \text{ etc.}\) Just as we replaced \(a\) by \(1\), let's replace \(c\) by \(b^2\).

\[
\begin{array}{ccc}
|   & 1 & b & b^2 \\
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1 &amp; b &amp; e</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b</td>
<td>b &amp; b^2 &amp; 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b^2</td>
<td>e &amp; 1 &amp; b</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
\end{array}
\]

© 2003 J. Simon  All rights reserved.
We don't need someone to tell us that $bb = b^2$, so the middle entry in row 2 also is unnecessary. We end up with the following very efficient description of our group, from which (following the various steps above) we could deduce the whole original multiplication table:

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>b</th>
<th>$b^2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>+</td>
<td>b</td>
<td>$b^2$</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>$b^2$</td>
<td>e</td>
<td>b</td>
<td></td>
</tr>
</tbody>
</table>

So if someone says to you, "I have a group with an element $b$ such that every other element is just some power of $b$, and $b^3 = 1$", then you know that group is isomorphic to the one we started with. This is the idea of group presentations: descriptions of groups in terms of some list of generators and some list of equations or relations that are satisfied by those generators, from which all other elements of the group can be deduced (as expressions in the generators) and all other relations among elements can be deduced (from the given ones).

**Example (and HOMEWORK):** Let $G$ be a group with generators $a$ and $b$ in which $a^2 = 1$, $b^3 = 1$, and $ab = ba$. Write a multiplication table for this group.

Hints: Here is one possible outline of how to proceed.
1. Since $a$ and $b$ are given as generators, we know that each other element $g \in G$ can be expressed in terms of $a, b$, i.e.

   \[ g = a^{p_1} b^{q_1} a^{p_2} b^{q_2} \ldots a^{p_n} b^{q_n} \]

2. Since $ab = ba$, we can collect terms in the above, to get

   \[ g = a^{(p_1 + \ldots + p_n)} b^{(q_1 + \ldots + q_n)} \]

so in fact each element of the group can be written in the form $g = a^p b^q$. Furthermore, (again because $ab = ba$), multiplication is component-wise.

3. Now list what are all the elements of $G$.

4. Write out the multiplication table.

In the above example, the group $G$ is finite. When the group is infinite, there may be little advantage to actually writing out the multiplication table - we are content to list a set of generators and a set of equations from which all others can be deduced.
The group $G$ in the above homework could be described in the following form, which is called a presentation of $G$. Let's invent notation "::" to mean "$G$ is described by"

$$G :: < a, b \mid a^2 = 1, b^3 = 1, ab = ba > .$$

If we eliminate some of the equations, we get (in general) larger groups. For example, suppose

$$H :: < A, B \mid B^3 = 1, AB = BA > .$$

Then $H$ is an infinite abelian group. Furthermore, $G$ is a homomorphic image of $H$. We can (try to) define a function $\varphi: H \to G$ by saying $\varphi(A) = a$, $\varphi(B) = b$. Since $A, B$ generate $H$, there is no choice about where any other element of $H$ is sent. (This is very much like the theorem about vector spaces that in order to define a linear map from one vector space to another, you just have to specify where the elements of a basis are sent.) For example, $\varphi$ will have to send the element $ABABB^2$ to $abab^2$. Without looking at the defining relations for $G$ or $H$, the function $\varphi$ is just a set-function from the abstract set of expressions in $A$ and $B$ into $G$. Since the image of $\varphi$ includes a set of generators for $G$, the set-function is surjective. But we know nothing (yet) about whether it is 1-1 or whether it is a homomorphism. In fact we do not yet know if $\varphi$ is well defined; certainly an element of $H$ can be written in two different ways (e.g. $BBBBB$ and $BABBA^{-1}B^{-1}$), and we need some way of knowing that both of these expressions are sent to the same place in $G$.

**Theorem** (the most basic and important theorem in the theory of group-presentations): If the set-function $\varphi$ respects the relations in $H$ then the function $\varphi$ is a well-defined homomorphism of $H \to G$.

In our case, it is easy to check that the relations are preserved. In $H$ we have $B^3 = 1$. Under $\varphi$, we have $B \to b$; and in $G$, $\varphi(B)^3 = b^3 = 1$ also. Similarly, in $H$, we have $AB = BA$; applying $\varphi$ we have

$$\varphi(AB) = [\text{def of } \varphi] \cdot \varphi(A)\varphi(B) = ab = (\text{in } G) \cdot ba = [\text{def of } \varphi] \cdot \varphi(B)\varphi(A) = [\text{def of } \varphi] \cdot \varphi(BA).$$

Here is another interesting example:

$$K :: < a, b \mid a^2 = 1, b^3 = 1 > .$$

This group is infinite, non-abelian, and famous (maybe all groups with short simple looking presentations are famous). You can show it is nonabelian by finding a nonabelian homomorphic image. **Homework** Just find some permutation group in which there is an element of order 2, another element of order 3, and they don't commute. The 'big theorem' above then tells us that $K$ has a nonabelian homomorphic image, namely the group generated by the two non-commuting permutations.

**Unassigned homework:** Can you find a homomorphic image of $K$ that you know is infinite?