The University of Sydney

MATH2008 Introduction to Modern Algebra

(http://www.maths.usyd.edu.au/u/UG/IM/MATH2008/)

Semester 2, 2003 Lecturer: R. Howlett

Tutorial 12

1. Let G be the group of all matrices of the form $\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}$, where $x \in \mathbb{R}$, with the operation of matrix multiplication. Let H be the group of all real numbers under addition. Define $f\colon G \to H$ by

$$f\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} = x.$$

Show that f is an isomorphism from G to H.

Solution.

We must prove that f is one-to-one and onto, and that it is a homomorphism.

Let $A, B \in G$ be such that $f(A) = f(B)$. By the definition of G we have $A = \left(\begin{smallmatrix} 1 & 0 \\ x & 1 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} 1 & 0 \\ y & 1 \end{smallmatrix}\right)$ for some $x, y \in \mathbb{R}$, and the definition of f gives $f(A) = x$ and $f(B) = y$. But $f(A) = f(B)$; so $x = y$, and so

$$A = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix} = B.$$

So $f(A)$ can only equal $f(B)$ if $A = B$; that is, f is one-to-one.

Let t be any element of $\mathbb{R}$. The matrix A defined by $A = \left(\begin{smallmatrix} 1 & 0 \\ t & 1 \end{smallmatrix}\right)$ is in G and $f(A) = t$. So every element of $\mathbb{R}$ is in the image of f, and so f is onto.

Recall that f a homomorphism is a function that preserves the group structure. Here, since the group operation in G written as multiplication and the group operation on H is written as addition, to say that f is a homomorphism is to say that $f(AB) = f(A) + f(B)$ for all $A, B \in G$. So, let A, B be arbitrary elements of G. Then $A = \left(\begin{smallmatrix} 1 & 0 \\ x & 1 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} 1 & 0 \\ y & 1 \end{smallmatrix}\right)$ for some $x, y \in \mathbb{R}$, and matrix multiplication gives $AB = \left(\begin{smallmatrix} 1 & 0 \\ x+y & 1 \end{smallmatrix}\right)$. So $f(AB) = x+y = f(A)+f(B)$, as required.

2. (i) Let C_n be a cyclic group of order n. Suppose that k is a number that is a divisor of n. Show that C_n contains an element of order k.

(ii) Find an example of a group G of order n and a divisor k of n for which G does not contain any element of order k.

Solution.

(i) Let a be a generator of C_n. Then a has order n; that is, $a^n = e$ and $a^j \neq e$ for $0 < j < n$. If k divides n, then $n = mk$ for some positive integer m. and so $(a^m)^k = e$. Furthermore, if $0 < j < k$ then $0 < mj < mk = n$, and so $(a^m)^j = a^{mj} \neq e$. Hence the least positive integer j such that $(a^m)^j = e$ is $j = k$, and thus a^m has order k.

(ii) The group $G = \mathrm{Sym}(3)$ has order $n = 6$. The number $k = 6$ is a divisor of n, and G does not have any element of order 6. (Indeed, G has three elements of order 2 (the transpositions), two of order 3 (the 3-cycles) and one of order 1 (the identity), and these are all the elements of G since its order is 6.)

3. If G is a group, H a subgroup of G and g an element of G, then we define $g^{-1}Hg$ to be the set of all elements of G of the form $g^{-1}hg$, where h is in H.

(i) Let $G = \mathrm{Sym}(4)$ and $H = \{\mathrm{id}, (1,2,4), (1,4,2)\}$, and let $g = (2,3,4)$. Calculate all of the elements of $g^{-1}Hg$.

(ii) Let $G = \mathrm{Sym}(4)$ and $L = \{\, \sigma \in G \mid 3^\sigma = 3 \,\}$. Write out all 6 elements of L. Is L a subgroup of G?

(iii) Let L be as in Part (ii) and let $g = (2,3,4)$. Show that

$$g^{-1}Hg = \{\, \tau \in G \mid 4^\tau = 4 \,\}.$$

Solution.

(i) Obviously, $(2,4,3)\mathrm{id}(2,3,4) = \mathrm{id}$. Calculating $(2,4,3)(1,2,4)(2,3,4)$ involves finding the result of applying $(2,4,3)$, followed by $(1,2,4)$, followed by $(2,3,4)$, to each of the numbers 1, 2, 3, 4. We have

$$\begin{gathered}
1 \xrightarrow{(2,4,3)} 1 \xrightarrow{(1,2,4)} 2 \xrightarrow{(2,3,4)} 3 \\
2 \xrightarrow{(2,4,3)} 4 \xrightarrow{(1,2,4)} 1 \xrightarrow{(2,3,4)} 1 \\
3 \xrightarrow{(2,4,3)} 2 \xrightarrow{(1,2,4)} 4 \xrightarrow{(2,3,4)} 2 \\
4 \xrightarrow{(2,4,3)} 3 \xrightarrow{(1,2,4)} 3 \xrightarrow{(2,3,4)} 4.
\end{gathered}$$

Thus $(2,4,3)(1,2,4)(2,3,4) = (1,3,2)$. Products of the form $g^{-1}xg$ can also be calculated using the method described in Question 2 of Computer Tutorial 6 and Question 1 of Assignment 2: $g^{-1}xg$ can be found by writing x as a product of cycles and replacing each number i that appears there by i^g (the number that i "goes to" under g). Thus $g^{-1}(1,4,2)g = (1^g, 4^g, 2^g)$ (for any g), and when $g = (2,3,4)$ this is $(1,2,3)$. So $g^{-1}Hg = \{\mathrm{id}, (1,3,2), (1,2,3)\}$.

(*ii*) We must list all the permutations of $\{1,2,3,4\}$ that take 3 to 3, and thus take 1, 2 and 4 to 1, 2 and 4 in some order. Answer: id, $(1,2)$, $(1,4)$, $(2,4)$, $(1,2,4)$ and $(1,4,2)$.

(*iii*) You could just calculate all six products $(2,4,3)h(2,3,4)$, where h runs through the six permutations listed in the answer to Part (*ii*). Three have already been calculated in Part (*i*); the others are $(2,4,3)(1,2)(2,3,4) = (1,4)$, $(2,4,3)(1,4)(2,3,4) = (1,3)$ and $(2,4,3)(2,4)(2,3,4) = (4,3)$. So you do indeed get the six permutations of $\{1,2,3,4\}$ that take 4 to 4. One can also apply the principle that is the basis of the CompTut6/Assgt2 method for the calculation of $g^{-1}hg$, namely, if h takes i to j then $g^{-1}hg$ takes i^g to j^g. So if h takes 3 to 3 then $(2,3,4)^{-1}x(2,3,4)$ takes $3^{(2,3,4)}$ to $3^{(2,3,4)}$. Since $3^{(2,3,4)} = 4$, this shows that if h is in the stabilizer of 3 then $(2,3,4)^{-1}h(2,3,4)$ is in the stabilizer of 4.

More directly, given that h takes 3 to 3, applying $(2,3,4)^{-1}$ followed by h followed by $(2,3,4)$ we find that

$$4 \xrightarrow{(2,4,3)} 3 \xrightarrow{h} 3 \xrightarrow{(2,3,4)} 4,$$

and so $(2,3,4)^{-1}h(2,3,4)$ takes 4 to 4, as required.

4. Let G be any group, H any subgroup of G and g any element of G.

Show that $g^{-1}Hg$ is a subgroup of G. (Hint: you must use the fact that H satisfies (SG1), (SG2) and (SG3) to show that $g^{-1}Hg$ also does.)

Solution.

Sice H is a subgroup of G we know that H satisfies (SG1): for all h and k, if h, $k \in H$ then hk in H. We use this to show that $g^{-1}Hg$ satisfies (SG1): for all x and y, if x, $y \in g^{-1}Hg$ then xy in $g^{-1}Hg$.

Let x, $y \in g^{-1}Hg$. Then $x = g^{-1}hg$ for some $h \in H$ and $y = g^{-1}kg$ for some $k \in H$. So

$$xy = (g^{-1}hg)(g^{-1}kg) = g^{-1}h(gg^{-1})kg = g^{-1}(hek)g = g^{-1}(hk)g$$

(where e is the identity element of G). But h, $k \in H$; so by (SG1) for H it follows that $hk \in H$. Hence $g^{-1}(hk)g \in g^{-1}Hg$; that is, $xy \in g^{-1}Hg$. But x, y were arbitrary elements of $g^{-1}Hg$. So we have shown that $xy \in g^{-1}Hg$ for all x, $y \in g^{-1}Hg$, as required.

Since H is a subgroup it satisfies (SG2); that is, $e \in H$. So $g^{-1}eg \in g^{-1}Hg$. But $g^{-1}eg = g^{-1}g = e$; so $e \in g^{-1}Hg$. Thus $g^{-1}Hg$ satisfies (SG2).

Since H is a subgroup it satisfies (SG3): for all h, if $h \in H$ then $h^{-1} \in H$. Now suppose that x is an arbitrary element of $g^{-1}Hg$. Then $x = g^{-1}hg$ for some $h \in H$. Since taking inverses reverses the order of factors in a product—that is, $(ab)^{-1} = b^{-1}a^{-1}$—it follows that $x^{-1} = g^{-1}h^{-1}(g^{-1})^{-1} = g^{-1}h^{-1}g$. But since $h \in H$ it follows from (SG3) for H that $h^{-1} \in H$, and hence $g^{-1}h^{-1}g \in g^{-1}Hg$. So we have shown that for all x, if $x \in g^{-1}Hg$ then $x^{-1} \in g^{-1}Hg$. That is, $g^{-1}Hg$ satisfies (SG3).

Since $g^{-1}Hg$ satisfies (SG1), (SG2) and (SG3) it is a subgroup of G.

5. Let H be a subgroup of G, and let g be an element of G. Prove that the map $f\colon H \to g^{-1}Hg$ defined by $f(h) = g^{-1}hg$ is a homomorphism. Prove also that f is one-to-one and onto.

Solution.

Let h_1, h_2 be arbitrary elements of H. Then

$$f(h_1)f(h_2) = (g^{-1}h_1g)(g^{-1}h_2g) = g^{-1}h_1h_2g = f(h_1h_2),$$

and so f is a homomorphism.

By definition, $g^{-1}Hg$ is the set of all elements of the form $g^{-1}hg$ for some $h \in H$. Since $g^{-1}hg = f(h)$ this says that every element of $g^{-1}Hg$ has the form$f(h)$ for some $h \in H$. So f is onto.

Suppose that h_1, $h_2 \in H$ satisfy $f(h_1) = f(h_2)$. Then $g^{-1}h_1g = g^{-1}h_2g$, and it follows that

$$h_1 = g(g^{-1}h_1g)g^{-1} = g(g^{-1}h_2g)g^{-1} = h_2.$$

Thus f is one-to-one.