

### Tutorial 1

1. Let  $A, B, C$  and  $D$  be sets, and let  $f: A \rightarrow B$ ,  $g: B \rightarrow C$  and  $h: C \rightarrow D$  be functions. Show that the composites  $(hg)f$  and  $h(gf)$  are equal.

*Solution.*

We must show that the functions  $(hg)f$  and  $h(gf)$  have the same domain and codomain; then we must show that  $((hg)f)x = (h(gf))x$  for all  $x$  in their common domain. Implicitly, the first part of this involves showing that  $(hg)f$  and  $h(gf)$  both exist.

Since the codomain of  $f$  is the domain of  $g$ , it follows that  $gf$  is defined, with domain equal to the domain of  $f$  and codomain equal to the codomain of  $g$ . That is,  $gf$  is a function from  $A$  to  $C$ . Now since  $h$  is a function from  $C$  to  $D$ , it follows that  $h(gf)$  exists and is a function from  $A$  to  $D$ .

Since the codomain of  $g$  is the domain of  $h$ , it follows that  $hg$  is defined, with domain equal to the domain of  $g$  and codomain equal to the codomain of  $h$ . That is,  $hg$  is a function from  $B$  to  $D$ . And since  $f$  is a function from  $A$  to  $B$ , it follows that  $(hg)f$  exists and is a function from  $A$  to  $D$ . So we have shown that  $(hg)f$  and  $h(gf)$  have the same domain and codomain.

Let  $x \in A$  be arbitrary. By the definition of the composite of the functions  $hg$  and  $f$  we have that  $((hg)f)x = (hg)(fx)$ . Similarly, the definition of  $hg$  tells us that  $(hg)y = h(gy)$ , for all  $y \in B$ . So, in particular,  $(hg)(fx) = h(g(fx))$ . Similarly, the definition of the composite of  $h$  and  $gf$  gives  $(h(gf))x = h((gf)x)$ , and the definition of  $gf$  gives  $(gf)x = g(fx)$ . So  $(h(gf))x = h(g(fx))$ . Thus we have shown that  $(h(gf))x = ((hg)f)x$  for all  $x \in A$ ; whence  $(hg)f = h(gf)$ .

2. Let  $G$  be a group and  $g \in G$ , and consider the sequence  $g, g^2, g^3, g^4, \dots$  of positive powers of  $g$ . Show that either

- (a) all the terms of this sequence are different from one another, or  
 (b) the identity element 1 appears somewhere in the sequence.

In case (b), show also that if  $n$  is the least positive integer such that  $g^n = 1$  then the sequence is periodic of period  $n$ , and the first  $n$  terms are different from one another.

*Solution.*

If there is a repetition then there exist integers  $i$  and  $k$  such that  $1 \leq i < k$  and  $g^i = g^k$ . Amongst all such repetitions, choose the first: the one for which  $k$  is least. Observe that  $g^i = g^k$  implies that

$$g^{i-1} = g^{-1}g^i = g^{-1}g^k = g^{k-1},$$

and if it were true that  $i \leq i-1 < k-1$  this would contradict the fact that we originally chose the first repetition. But  $1 \leq i < k$  certainly implies that  $i-1 < k-1$ , and if  $1 < i$  we would also have  $1 \leq i-1$ . So we must have  $i = 1$ . Thus  $i < k$  and  $g^i = g^k$  becomes  $1 < k$  and  $g = g^k$ . And  $g^{i-1} = g^{k-1}$  becomes  $1 = g^{k-1}$ . Since  $k-1 \geq 1$ , this shows that 1 occurs in the sequence. So if (a) does not hold then (b) does, as required.

The argument we have given also proves the last part. We showed that the identity element 1 occurs in the sequence immediately before the first  $g^k$  that equals an earlier term of the sequence. So there is no repetition in the part of the sequence up to and including this occurrence of the identity element (which, perforce, must be the first occurrence of the identity). Finally,  $g^n = 1$  implies that  $g^{i+n} = g^i g^n = g^i 1 = g^i$ , showing that the sequence is periodic. Choosing  $n$  as small as possible (subject to  $g^n = 1$ ) ensures that the period is  $n$  (rather than some proper divisor of  $n$ ).

3. The set of all permutations of  $\{1, 2, \dots, n\}$  is a group under permutation multiplication. This group is called the *symmetric group* of degree  $n$ , and we denote it by  $\text{Sym}(n)$ .

- (i) Let  $\begin{pmatrix} 1 & 2 & 3 & 4 \\ i & j & k & l \end{pmatrix}$  be an arbitrary permutation of  $\{1, 2, 3, 4\}$ . Show that

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ i & j & k & l \end{pmatrix} (1, 2) \begin{pmatrix} 1 & 2 & 3 & 4 \\ i & j & k & l \end{pmatrix}^{-1} = (i, j),$$

and deduce that if a normal subgroup of  $\text{Sym}(4)$  contains one transposition  $(i, j)$  then it contains them all.

- (ii) Prove results similar to Part (i), with  $(1, 2)$  replaced by  $(1, 2, 3)$ ,  $(1, 2, 3, 4)$ , and  $(1, 2)(3, 4)$ .  
 (iii) How many permutations of each ‘‘cycle type’’ are there in  $\text{Sym}(4)$ ? (That is, how many transpositions, how many 3-cycles, etc..)  
 (iv) Find all the normal subgroups of  $\text{Sym}(4)$ .

*Solution.*

For Parts (i) and (ii), we prove a more general statement: we show that for all permutations  $\sigma, \tau \in \text{Sym}(n)$ , if  $\tau$  written in cycle notation is

$$(i_1^{(1)}, i_2^{(1)}, \dots, i_{k_1}^{(1)})(i_1^{(2)}, i_2^{(2)}, \dots, i_{k_2}^{(2)}) \dots (i_1^{(l)}, i_2^{(l)}, \dots, i_{k_l}^{(l)})$$

then  $\sigma\tau\sigma^{-1}$  in cycle notation is

$$(\sigma i_1^{(1)}, \sigma i_2^{(1)}, \dots, \sigma i_{k_1}^{(1)})(\sigma i_1^{(2)}, \sigma i_2^{(2)}, \dots, \sigma i_{k_2}^{(2)}) \dots (\sigma i_1^{(l)}, \sigma i_2^{(l)}, \dots, \sigma i_{k_l}^{(l)}).$$

More simply, the claim is that if  $(i_1, i_2, \dots, i_k)$  is one of the cycles in the permutation  $\tau$ , then  $(\sigma i_1, \sigma i_2, \dots, \sigma i_k)$  is one of the cycles in the permutation  $\sigma\tau\sigma^{-1}$ .

In fact, all this really says is that if  $j$  follows  $i$  in one of  $\tau$ 's cycles, then  $\sigma j$  follows  $\sigma i$  in one of  $\sigma\tau\sigma^{-1}$ 's cycles. In turn, all this says is that if  $\tau i = j$  then  $(\sigma\tau\sigma^{-1})(\sigma i) = \sigma j$ . And this is just about obvious:

$$(\sigma\tau\sigma^{-1})(\sigma i) = (\sigma\tau\sigma^{-1}\sigma)i = (\sigma\tau)i = \sigma(\tau i) = \sigma j,$$

where the first and third equalities follow from the definition of permutation multiplication as composition of functions, and the second from the fact that  $\sigma^{-1}\sigma$  is the identity.

In particular (answering Part (ii) explicitly), if  $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ i & j & k & l \end{pmatrix}$  then

$$\begin{aligned} \sigma((1, 2)(3)(4))\sigma^{-1} &= (i, j)(k)(l), \\ \sigma((1, 2, 3)(4))\sigma^{-1} &= (i, j, k)(l), \\ \sigma((1, 2, 3, 4))\sigma^{-1} &= (i, j, k, l), \\ \sigma((1, 2)(3, 4))\sigma^{-1} &= (i, j)(k, l). \end{aligned}$$

4. Let  $G$  be a group of permutations of  $\{1, 2, 3, 4, 5\}$ . Suppose that

- (a) for each  $i \in \{1, 2, 3, 4, 5\}$  there exists an  $\alpha_i \in G$  such that  $\alpha_i 5 = i$ ,
- (b)  $(4, 5) \in G$ .

Show that  $G = \text{Sym}(5)$ .

(Hint: By considering  $\alpha_i(4, 5)\alpha_i^{-1}$  show that  $G$  contains transpositions  $(a, 3)$ ,  $(b, 2)$  and  $(c, 1)$  for some  $a, b, c$ . Then show that there exist  $i, j, k$  such that  $G$  contains all 6 permutations of  $\{i, j, k\}$ . Eventually, show that  $G$  contains all ten transpositions.)

*Solution.*

By Question 3 and the fact that  $\alpha_i 5 = i$  we know that  $\alpha_i(4, 5)\alpha_i^{-1} = (\alpha_i 4, i)$ . By closure of  $G$  under multiplication and inversion this shows that  $G$  contains  $(a, 3)$ ,  $(b, 2)$  and  $(c, 1)$ , where  $a, b$  and  $c$  are (respectively)  $\alpha_3 4$ ,  $\alpha_2 4$  and  $\alpha_1 4$ . Note that  $a \neq 3$  (since  $\alpha_3 4 \neq \alpha_3 5$ , and similarly  $b \neq 2$  and  $c \neq 1$ ).

If  $a = 4$  then  $G$  contains  $(4, 3)$  as well as  $(4, 5)$ , and so it contains all six permutations that permute  $\{3, 4, 5\}$  while fixing 1 and 2, since these six permutations are

$$I, (4, 5), (4, 3), (4, 5)(4, 3), (4, 3)(4, 5), (4, 3)(4, 5)(4, 3),$$

all of which are in  $G$  by closure. The same holds if  $a = 5$ , since this would tell us that  $G$  contains all of

$$I, (4, 5), (5, 3), (4, 5)(5, 3), (5, 3)(4, 5), (5, 3)(4, 5)(5, 3).$$

The general fact we are using is that if  $i, j, k$  are distinct and  $G$  contains  $(i, j)$  and  $(i, k)$  then it contains all six permutations of  $\{i, j, k\}$ , because these permutations can all be expressed as products involving only  $(i, j)$  and  $(i, k)$ . (We say that  $(i, j)$  and  $(i, k)$  generate the group  $\text{Sym}(\{i, j, k\})$ .)

Thus  $G$  contains  $\text{Sym}(\{3, 4, 5\})$  if  $a$  is 4 or 5. Similarly  $G$  contains  $\text{Sym}(\{2, 4, 5\})$  if  $b$  is 4 or 5, and  $G$  contains  $\text{Sym}(\{1, 4, 5\})$  if  $c$  is 4 or 5. If none of these situations occur, then we must have  $a = 1$  or  $a = 2$ , we must have  $b = 1$  or  $b = 3$ , and we must have  $c = 2$  or  $c = 3$ . If  $a = 1$  then  $G$  contains  $(1, 3)$  and either  $(1, 2)$  (if  $b = 1$ ) or  $(3, 2)$  (if  $b = 3$ ), and in either case it follows that  $G$  contains  $\text{Sym}(\{1, 2, 3\})$ . Similarly, if  $a = 2$  then  $G$  contains  $(2, 3)$  and either  $(2, 1)$  (if  $c = 2$ ) or  $(3, 1)$  (if  $c = 3$ ), and again in either case it follows that  $G$  contains  $\text{Sym}(\{1, 2, 3\})$ . So we have shown that there are three numbers  $i, j, k$  such that  $G$  contains  $\text{Sym}(\{i, j, k\})$ .

Choose three numbers  $i, j, k$  such that  $G$  contains  $\text{Sym}(\{i, j, k\})$ , and let  $l, m$  be the other two numbers, so that  $\{i, j, k, l, m\} = \{1, 2, 3, 4, 5\}$ . Observe that the permutation  $\beta = \alpha_l \alpha_i^{-1}$  is in  $G$  and satisfies  $\beta i = l$ ; hence  $\beta(i, j)\beta^{-1} = (l, \beta j)$  and  $\beta(i, k)\beta^{-1} = (l, \beta k)$  are both in  $G$ . Now  $\beta j$  and  $\beta k$  cannot both lie in the set  $\{l, m\}$ , since they are different from each other and neither of them is equal to  $l$ . So at least one of them lies in  $\{i, j, k\}$ . So  $G$  contains one of  $(l, i)$ ,  $(l, j)$  or  $(l, k)$ . But if  $G$  contains  $(l, i)$  then it also contains  $(i, j)(l, i)(i, j) = (l, j)$  and  $(i, k)(l, i)(i, k) = (l, k)$ . Similarly, if  $G$  contains  $(l, j)$  then it also contains  $(i, j)(l, j)(i, j) = (l, i)$  and  $(j, k)(l, j)(j, k) = (l, k)$ , and if  $G$  contains  $(l, k)$  then it also contains  $(i, k)(l, k)(i, k) = (l, i)$  and  $(j, k)(l, k)(j, k) = (l, j)$ . So in all cases  $G$  contains all of  $(l, i)$ ,  $(l, j)$  and  $(l, k)$ .

The permutation  $\gamma = \alpha_m \alpha_i^{-1}$  is in  $G$  and satisfies  $\gamma i = m$ ; so  $G$  contains all of  $\gamma(i, j)\gamma^{-1} = (m, \gamma j)$ ,  $\gamma(i, k)\gamma^{-1} = (m, \gamma k)$  and  $\gamma(i, l)\gamma^{-1} = (m, \gamma l)$ . This tells us that  $G$  contains at least three of the four transpositions  $(m, i)$ ,  $(m, j)$ ,  $(m, k)$  and  $(m, l)$ . So  $G$  contains at least 9 of the 10 transpositions in  $\text{Sym}(5)$ : all except  $(m, t)$  for some  $t \in \{i, j, k, l\}$ . But if  $s$  is any number different from  $m$  and  $t$  then  $G$  has to contain both  $(s, t)$  and  $(m, s)$ , and hence also contains  $(s, t)(m, s)(s, t) = (m, t)$ . Thus  $G$  contains all 10 transpositions in  $\text{Sym}(5)$ .

Finally, to show that  $G = \text{Sym}(5)$ , it remains to show that every permutation can be expressed as a product of transpositions. Since we already know that every permutation is a product of cycles, it is sufficient to show that every cycle is a product of transpositions. And this is trivial to check: a straightforward calculation gives

$$(i_1, i_2, i_3, i_4, \dots, i_n) = (i_1, i_2)(i_2, i_3)(i_3, i_4) \cdots (i_{n-1}, i_n).$$