R. P. BURN

GROUPS

A PATH TO GEOMETRY

CAMBRIDGE
UNIVERSITY PRESS

PUBLISHED BY THE PRESS SYNDICATE OF THE UNIVERSITY OF CAMBRIDGE
The Pitt Building, Trumpington Street, Cambridge CB2 1RP, United Kingdom

CAMBRIDGE UNIVERSITY PRESS
The Edinburgh Building, Cambridge CB2 2RU, United Kingdom
40 West 20th Street, New York, NY 10011–4211, USA
10 Stamford Road, Oakleigh, Melbourne 3166, Australia

First published 1985
First paperback edition with corrections 1987
Reprinted 1988, 1991, 1994, 1996

A catalogue record for this book is available from the British Library

Library of Congress Cataloguing in Publication data available

ISBN 0 521 34793 9 paperback

Transferred to digital printing 2001

APL

Contents

1

Functions

Throughout the nineteenth century, group theory was a study of permutations and substitutions. Group elements were generally referred to as 'operations', being what we would now call transformations (bijections) of a set to itself. This view of groups suits geometers very well, and it is the view that we adopt for most of this book.

In this first chapter we establish those properties of transformations which make sets of transformations form groups under composition and we do this with a set-theoretic rigour unknown in the nineteenth century. This chapter is the most abstract chapter in the book, and the student who finds this uncomfortable may start at chapter 2 provided that he accepts the results of the last question of chapter 1.

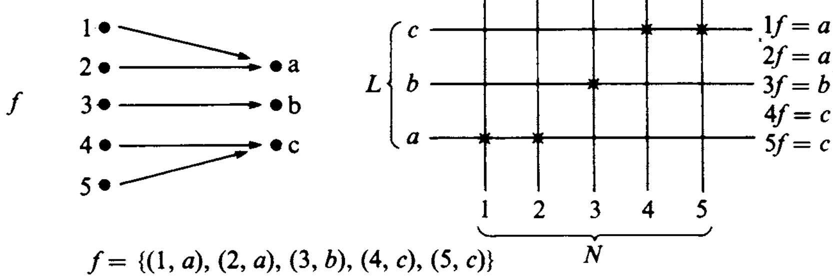
Because we will be establishing a formal definition of a function in this chapter we will also be providing a background for the terms isomorphism, homomorphism and one–one correspondence, all of which describe special kinds of functions which are of use in group theory, which are not usually thought of as group elements themselves.

Concurrent reading: Green, chapter 3.

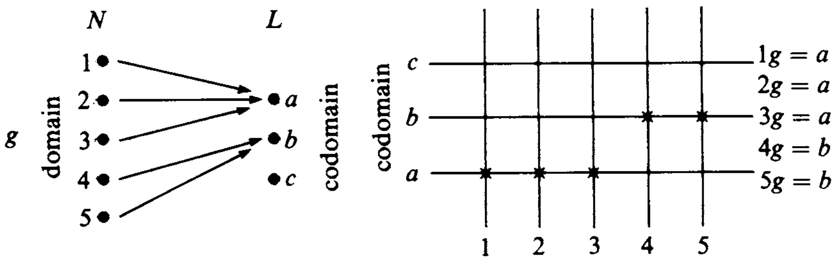
FUNCTIONS $N \to L$

Arrow diagram *Graph*

N = *numbers* L = *letters*



$f = \{(1, a), (2, a), (3, b), (4, c), (5, c)\}$



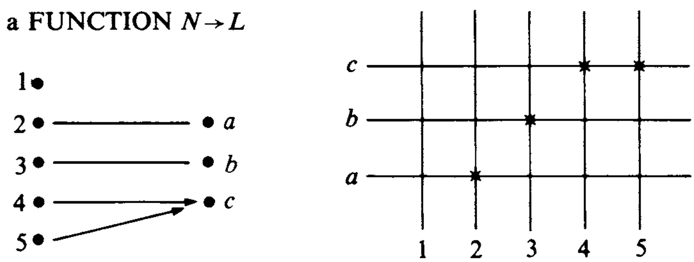
$g = \{(1, a), (2, a), (3, a), (4, b), (5, b)\}$ domain

Domain $N = \{1, 2, 3, 4, 5\}$, Codomain $L = \{a, b, c\}$.

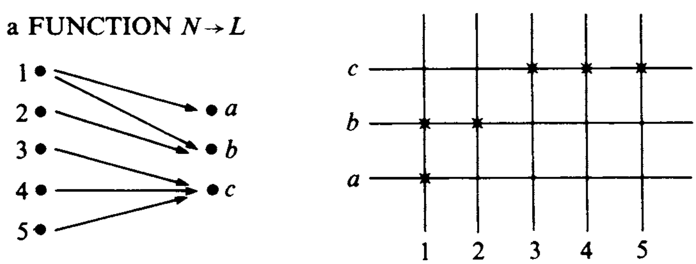
Both f and g are examples of functions from N to L,

$f: N \to L$ and $g: N \to L$

NOT a FUNCTION $N \to L$



NOT a FUNCTION $N \to L$



1 Use the diagrams on page 2, with their implied rules to complete the following sentence.
A function $f: N \to L$ is defined when for each element n of the set N there is. . . . .

2 Use the diagrams on page 2, with their implied rules to complete the last sentence.
The rectangular array used for the graphs of the functions on page 2 represents the so-called *cartesian product* $N \times L$. Each element of $N \times L$ is an ordered pair (n, x) with n from N and x from L. The graph of a function $N \to L$ consists of a subset of $N \times L$ with exactly one element (n, x) for each . . . .

3 Which of these define functions of the real numbers $\mathbb{R} \to \mathbb{R}$?

(i) $x \mapsto x^2$,

(ii) $x^2 \mapsto x$,

(iii) $x \mapsto 1/x$,

(iv) $x \mapsto \sin x$,

(v) $x \mapsto \tan x$.

4 If $A = \{0, 1\}$, how many different functions, $A \to A$, are there?

Injections (one–one)

5 Draw sketch graphs of the functions $\mathbb{R} \to \mathbb{R}$ given by
(i) $x \mapsto x^3$ and by (ii) $x \mapsto x^2$.
If $x^3 = y^3$, does it follow that $x = y$?
If $x^2 = y^2$, does it follow that $x = y$?
The distinction here leads us to call $\alpha: \mathbb{R} \to \mathbb{R}$ defined by $\alpha: x \mapsto x^3$, a *one–one* function or *injection*. We say that $\beta: x \mapsto x^2$ is *not* one–one on $\mathbb{R}$.

6 Let $A = \{1, 2, 3, 4\}$.

(i) Exhibit the graph of a one–one function $A \to A$.

(ii) Exhibit the graph of a function $A \to A$ which is not one–one.

(iii) How many functions $A \to A$ exist?

7 Let $\mathbb{N}$ denote the set of natural numbers $\{1, 2, 3, \ldots\}$. Draw part of the graph of the function $\mathbb{N} \to \mathbb{N}$ defined by $n \mapsto n^2$. Is this a one–one function?

8 What can be said about the rows of the graph of a function if that function is known to be one–one?

Surjections (onto)

9 Draw sketch graphs of the functions $\mathbb{R} \to \mathbb{R}$ given by

(i) $\alpha : x \mapsto e^x$ and (ii) $\beta : x \mapsto x + 1$.

Can you always find a real number x, such that $\alpha : x \mapsto y$ for any choice of the real number y?
Can you always find a real number x, such that $\beta : x \mapsto y$ for any choice of the real number y?

The distinction here leads us to call β an *onto* function or *surjection* and to say that α is *not* onto.

10 Let $A = \{1, 2, 3, 4\}$. Exhibit the graph of a function $A \to A$
(i) which is onto,
(ii) which is not onto.

11 Illustrate part of the graph of the function $\mathbb{N} \to \mathbb{N}$ defined by

the even number $2n \mapsto n$,
the odd number $2n - 1 \mapsto n$.

Is this a one–one function?
Is this an onto function?

12 What can be said about the rows of the graph of an onto function?

13 Let $A = \{1, 2, 3, 4\}$.
Can you construct a function $A \to A$ which is one–one but not onto?
Can you construct a function $A \to A$ which is onto but not one–one?

14 Can you construct a function $\mathbb{N} \to \mathbb{N}$ which is one–one but not onto?
Can you construct a function $\mathbb{N} \to \mathbb{N}$ which is onto but not one–one?

15 Conjecture a condition on an arbitrary set A such that every one–one function $A \to A$ must be onto, and every onto function $A \to A$ must be one–one. Justify your conjecture with the help of qn 8 and qn 12.

An injection which is also a surjection is called a *bijection*. In the context of functions with the same finite set as domain and codomain, injections, surjections and bijections are in fact indistinguishable.

16 Give examples of functions $\mathbb{R} \to \mathbb{R}$ which are
(i) one–one and onto (bijections),
(ii) one–one but not onto (injections),
(iii) onto but not one–one (surjections),
(iv) neither one–one nor onto.

17 If there exists a one–one function $A \to A$ which is not onto, what can be said about the set A?

Composition of functions

18 If α and β are functions $\mathbb{R} \to \mathbb{R}$ defined by

$\alpha : x \mapsto 2x$ and $\beta : x \mapsto x + 1$,

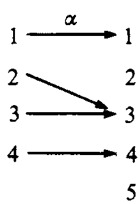
then we *define* $\alpha\beta : x \mapsto 2x + 1$.

$$x \overset{\alpha}{\mapsto} 2x \overset{\beta}{\mapsto} 2x + 1.$$

We write this $(x)\alpha\beta = (2x)\beta = 2x + 1$.
Determine $(x)\beta\alpha$ under a similar definition.

19 If $\alpha : A \to B$ and $\beta : B \to C$ are functions, give a formal definition of $\alpha\beta : A \to C$ by determining $(x)\alpha\beta$ (the image of x under the function $\alpha\beta$: first α, then β).

The function $\alpha\beta$ is called the *composite* of the function α and β.

20 If 

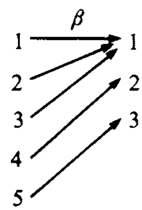
and 

exhibit $\alpha\beta$.

21 What formal condition makes $\alpha : A \to B$ a one–one function or injection?

22 If $\alpha : A \to B$ and $\beta : B \to C$ are injections, what can be said about $\alpha\beta : A \to C$?

23 Let $A = \{1, 2, 3\}$ and $B = \{1, 2, 3, 4\}$ and let $\alpha : A \to B$ be an injection.
Can you construct a function $\beta : B \to A$ such that
(i) $\beta\alpha$ is the identity function $B \to B$,
(ii) $\alpha\beta$ is the identity function $A \to A$?
(Under the *identity function* on the set, each point is its own image.)

Inverse functions

24 Let A and B be arbitrary sets, with $\alpha : A \to B$ an injection.
Show how to define $\beta : B \to A$ such that $\alpha\beta$ is the identity function on A.

The function β is then called a *right inverse* for α. So injections have right inverses.

25 What formal condition makes $\alpha: A \to B$ an onto function or surjection?

26 If $\alpha: A \to B$ and $\beta: B \to C$ are surjections, what can be said about the composite function $\alpha\beta: A \to C$?

27 Let $A = \{1, 2, 3, 4\}$ and $B = \{1, 2, 3\}$ and let $\alpha: A \to B$ be a surjection.
 (i) Can you construct a function $\beta: B \to A$ such that $\alpha\beta$ is the identity function on A?
 (ii) Can you construct a function $\beta: B \to A$ such that $\beta\alpha: B \to B$ is the identity function on B?

28 Let A and B be arbitrary sets, with $\alpha: A \to B$ a surjection.
Show how to define a function $\beta: B \to A$ such that $\beta\alpha$ is the identity function on B.

The function β is then called a *left inverse* for α. So surjections have left inverses.

29 Let $A = \{1, 2, 3\}$. Make a list of the bijections $A \to A$, or in other words of the permutations of A.
Find a left inverse for each bijection.
Find a right inverse for each bijection.

30 For any bijection $\alpha: A \to B$, define a bijection $\beta: B \to A$ such that $\alpha\beta$ is the identity function $I: A \to A$ and $\beta\alpha$ is the identity function $B \to B$.
Prove that *either* $\alpha\beta = I: A \to A$ *or* $\beta\alpha = I: B \to B$, determines β uniquely.
So bijections have two-sided inverses.

Closure

31 If α and β are both bijections $A \to A$, what can be said about $\alpha\beta: A \to A$?

Associativity

32 Let $\alpha: A \to B$, $\beta: B \to C$ and $\gamma: C \to D$ be functions. Use your definition of qn 19 to show that for each point x of A,

$$(x)[(\alpha\beta)\gamma] = (x)[\alpha(\beta\gamma)],$$

so that the two functions $A \to D$, $(\alpha\beta)\gamma$ and $\alpha(\beta\gamma)$ are indistinguishable.

The theorem $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ is called the *associative law* for functions under composition.

33 Use the associative law to prove for four functions $\alpha : A \to B$, $\beta : B \to C$, $\gamma : C \to D$, $\delta : D \to E$ that $\alpha[\beta(\gamma\delta)] = [(\alpha\beta)\gamma]\delta$.

The symmetric group

34 Let S be the set of all bijections $A \to A$.
Justify each of the following claims.
(i) If α and β are in S, then $\alpha\beta$ is in S (*closure*).
(ii) If α, β and γ are in S, then $\alpha(\beta\gamma) = (\alpha\beta)\gamma$ (*associativity*).
(iii) $I : A \to A$, defined by $I : x \mapsto x$ for all x in A, is in S (*identity*). $I\alpha = \alpha I = \alpha$ for all α in S.
(iv) For each α in S there is a β in S such that $\alpha\beta = \beta\alpha = I$. (*inverses*)

These four theorems are summarised in the statement that the bijections of a set to itself form a *group* under composition. The group in this case is called the symmetric group on A and is denoted by S_A.

Summary

Definition qn 1 — A *function* $\alpha : A \to B$, with domain A and codomain B is defined when, for each $a \in A$, there is a unique $b \in B$ such that $a\alpha = \alpha(a) = b$.

Definition qn 8 — A function $\alpha : A \to B$ is an *injection* when, for any $a_1, a_2 \in A$, $a_1\alpha = a_2\alpha \Rightarrow a_1 = a_2$.

Definition qn 12 — A function $\alpha : A \to B$ is a *surjection* when, for each $b \in B$, there exists an $a \in A$ such that $a\alpha = b$.

Definition qn 19 — The *composite* (or *product*) $\alpha\beta$ of two functions $\alpha : A \to B$ and $\beta : B \to C$ is defined by $(a)\alpha\beta = (a\alpha)\beta$.

Theorem qn 22 — The product of two composable injections is an injection.

Theorem qn 24 — An injection has a right inverse.

Theorem qn 26 — The product of two composable surjections is a surjection.

Theorem qn 28 — A surjection has a left inverse.

Theorem qn 30 — A bijection (an injection which is also a surjection) has a unique two-sided inverse.

Theorem qn 32 — The composition of functions is associative.

Theorem qn 34 — The set of bijections of a set to itself forms a group under composition. If the set is A, the group is called the *symmetric group* on A and is denoted by S_A.

Historical note

The modern notion of a function, with domain, and codomain, is essentially that of P. G. L. Dirichlet (1837). The language and style in which functions are discussed today owes much to the corporate twentieth-century French mathematician N. Bourbaki.

Answers to chapter 1

1 A function $f: N \to L$ is defined when for each element $n \in N$ there is a unique $l \in L$ with $nf = l$. Many authors write $f(n) = l$.

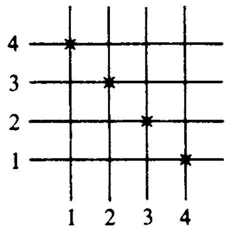
2 Exactly one element (n, x) for each $n \in N$.

3 (i) yes, (ii) 1 has no unique image, (iii) 0 has no image,
(iv) yes, (v) $\frac{1}{2}\pi$ has no image.

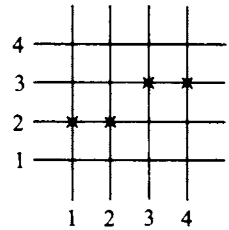
4 Four.

5 $x^3 = y^3 \Rightarrow x = y$. $x^2 = y^2 \Rightarrow x = \pm y$.

6 (i)



(ii)



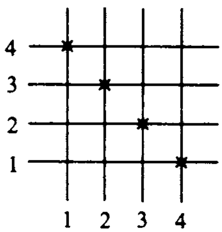
(iii) 4^4.

7 Yes.

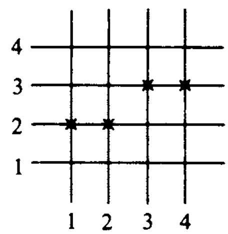
8 Each row contains at most one entry.

9 (i) If $e^x = y$, y must be positive. (ii) If $x + 1 = y$, every y is possible.

10 (i)



(ii)



11 Onto, but not one–one.

12 Each row contains at least one entry.

13 No, no.

14 Yes, in qn 7.
Yes, in qn 11.

15 A must be finite. In this case the number of entries in the graph is equal to the number of rows. The condition that each row contains at least one entry is then equivalent to the condition that each row contains at most one entry.

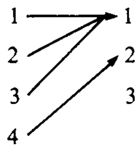
16 (i) $x \mapsto x + 1$, (ii) $x \mapsto e^x$, (iii) $x \mapsto x^3 - x$, (iv) $x \mapsto \sin x$.

17 A is infinite.

18 $(x)\beta\alpha = 2x + 2$. The left to right convention which we adopt is preferred by many algebraists. It has geometrical advantages in matrix algebra.

19 We define $\alpha\beta : A \to C$ by $(x)\alpha\beta = (x\alpha)\beta$.

20



21 $x\alpha = y\alpha \Rightarrow x = y$.

22 $x\alpha\beta = y\alpha\beta \Rightarrow x\alpha = y\alpha$ since β is an injection, $\Rightarrow x = y$ since α is an injection. Thus $\alpha\beta$ is an injection.

23 (i) No, because there is one point of B which is not an image under α. (ii) Yes. 1α, 2α and 3α are well defined and distinct. Let b be the fourth element of B. Define $(a\alpha)\beta = a$ for $a = 1, 2, 3$ and define $b\beta = 1$.

24 For $a \in A$ define $(a\alpha)\beta = a$. For $b \in B, b \neq a\alpha$ for any a, define $b\beta = a_1 \in A$.

25 Given $b \in B$, there exists $a \in A$ such that $a\alpha = b$.

26 Given $c \in C$, there exists $b \in B$ such that $b\beta = c$ and there exists $a \in A$ such that $a\alpha = b$ so $a\alpha\beta = c$ and $\alpha\beta$ is a surjection.

27 (i) No, because one point of A is not an image under β.
(ii) For each $b \in B$ there is at least one $a \in A$ such that $a\alpha = b$. For each $b \in B$, define $b\beta$ to be one element $a \in A$ such that $a\alpha = b$.

28 As in the second part of qn 27.

29 Images of (1, 2, 3) are (1, 2, 3), (2, 3, 1), (3, 1, 2), (1, 3, 2), (3, 2, 1), (2, 1, 3). First, fourth, fifth and sixth bijections are self-inverse. Second and third bijections are inverses of each other.

30 For each $b \in B$ there is a unique $a \in A$ such that $a\alpha = b$. Define $b\beta = a$. If $\alpha\beta = I$, then $a\alpha\beta = a$ so $(a\alpha)\beta = a$. If $\beta\alpha = I$, then $b\beta\alpha = b = a\alpha$ for a unique a. Now α is an injection so $b\beta = a$, and, as before, $a\alpha\beta = a$.

31 From qn 22 and qn 26, $\alpha\beta$ is a bijection.

32 $x[(\alpha\beta)\gamma] = [x(\alpha\beta)]\gamma = [(x\alpha)\beta]\gamma = (x\alpha)(\beta\gamma) = x[\alpha(\beta\gamma)]$.

33 $\alpha[\beta(\gamma\delta)] = (\alpha\beta)(\gamma\delta) = [(\alpha\beta)\gamma]\delta$. This kind of argument can be extended to any finite product, to show that its value is independent of the position of the brackets.

34 (i) from qn 31, (ii) from qn 32, (iii) obvious, (iv) from qn 30.