Mich. 2024 **GROUPS – INTRODUCTORY SHEET** G. Taylor

Please attempt questions 1–9.

Since you might not have studied groups yet, this sheet doesn't rely on much theory. If you haven't encountered groups at all then it will require some research on your part – find out the definition of a group, and look up any unfamiliar words below (e.g., 'abelian', 'proper', 'binary operation', ...).

You are welcome to mail me for help (glt1000@cam.ac.uk), but you should tell me what you've tried.

1. Write down the group axioms clearly, and also what it means for a group to be abelian.

2. For each of the examples below, determine (giving reasons) which of the group axioms hold and which do not, and whether the operation is commutative. For those examples that are groups, write down two distinct, proper, non-trivial subgroups.

   (i) the integers $\mathbb{Z}$ under subtraction
   (ii) the rationals $\mathbb{Q}$ under addition
   (iii) the real numbers $\mathbb{R}$ under multiplication
   (iv) the complex numbers $\mathbb{C}$ under the operation $a * b = a + b + i$, where $i = \sqrt{-1}$
   (v) the set of non-zero vectors in $\mathbb{R}^3$ under the vector ('cross') product
   (vi) the set of 2×2 real matrices with non-zero determinant under matrix multiplication
   (vii) the set $\{0, 1, 2, 3, 4, 5\}$ under the operation $a * b = |a - b|$
   (viii) the set $\{1, 2, 3, 4, 5\}$ under multiplication modulo 6
   (ix) the set $\{1, 2, 3, 4, 5, 6\}$ under multiplication modulo 7

3. Let G be a group with operation $*$. The associativity axiom says that for all a, b, c in G, we have $(a * b) * c = a * (b * c)$. This allows us to write $a * b * c$ without ambiguity, as both ways of bracketing the terms give equal expressions.

   Show that there are five different ways of bracketing terms in $a * b * c * d$. Using the rule of associativity for three terms, show carefully that all five ways give equal expressions.

   How many different ways of bracketing $a * b * c * d * e$ are there?

4. (a) Let $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$. Show explicitly that $AB \neq BA$ and $(AB)^2 \neq A^2B^2$.

   (b) Let G be a group, and let $a, b \in G$. Prove that if a, b commute then $(ab)^n = a^n b^n$ for all $n \in \mathbb{N}$. Also prove the converse: if $(ab)^n = a^n b^n$ for all $n \in \mathbb{N}$, then a, b commute.

   (c) Find 2×2 matrices C, D which do not commute but with $(CD)^n = C^n D^n$ for all $n \in \mathbb{N}$. Why does this not contradict (b)?

5. Show that the set $\left\{ \begin{pmatrix} t & 0 \\ 0 & 0 \end{pmatrix} : t \in \mathbb{R},\ t \neq 0 \right\}$ forms a group under matrix multiplication.

   More generally, show that if a set of matrices forms a group under multiplication, then either all matrices in the set have non-zero determinant, or all have zero determinant.

6. Show that, for each integer $n \geqslant 0$, the set $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$ under addition. Does $\mathbb{Z}$ have any other subgroups? For $m, n \geqslant 0$, show that the intersection $m\mathbb{Z} \cap n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. When is the union $m\mathbb{Z} \cup n\mathbb{Z}$ a subgroup of $\mathbb{Z}$?

7. (a) For a matrix A, we write A_{ij} for the entry in the i^{th} row and j^{th} column. Convince (or remind) yourself that for an $m \times n$ matrix A and an $n \times p$ matrix B, the standard rule for multiplying matrices gives $(AB)_{ij} = \sum_{k=1}^{n} A_{ik}B_{kj}$, for all $1 \leqslant i \leqslant m$ and $1 \leqslant j \leqslant p$.

   Use this to prove that matrix multiplication is always associative: if A, B, C are matrices of compatible sizes, then $(AB)C = A(BC)$.

   (b) Let S be a set. For functions $f, g : S \to S$, we define the composition $f \circ g : S \to S$ by setting $(f \circ g)(x) = f(g(x))$ for all $x \in S$.

   Prove that composition of functions is associative: if $f, g, h : S \to S$ are functions, then the functions $(f \circ g) \circ h$ and $f \circ (g \circ h)$ are the same.

   Give an example to show that composition of functions need not be commutative.

8. A *Latin square* is an array of symbols such that each row and column contains the same set of symbols, and no row or column contains a duplicated entry. For example, a correctly completed Sudoku puzzle forms a Latin square.

   (a) Explain why the multiplication table (officially, 'Cayley table') of a finite group forms a Latin square. Explain how the table can be used to find what the identity is and what the inverse of each element is, and to tell whether the group is abelian.

   (b) Is the following Latin square the Cayley table of a group?

$*$	e	a	b	c	d
e	e	a	b	c	d
a	a	e	c	d	b
b	b	d	e	a	c
c	c	b	d	e	a
d	d	c	a	b	e

   (c) Let S be a non-empty finite set, and let $*$ be an associative (and closed) binary operation on S whose multiplication table forms a Latin square. Prove that $(S, *)$ is a group.

9. Let S be a set, and let $\circ$ and $*$ be two binary operations on S, each with its own identity element, and suppose that for all $a, b, c, d \in S$, we have $(a \circ b) * (c \circ d) = (a * c) \circ (b * d)$.

   Show that $\circ$ and $*$ are in fact the same operation with the same identity element, and that this operation is associative and commutative.

Additional questions

These are optional. Attempt them if they interest you, but not at the expense of other work.

10. Construct an operation that makes $\mathbb{N} = \{1, 2, 3, \ldots\}$ into a group.

11. Let G be the set of integers $\{0, 1, 2, \ldots, 2^n - 1\}$ with operation

$$x * y = 4xy + x(-1)^y + y(-1)^x \pmod{2^n}.$$

    Show that G is a group. What is the order of 1?

12. Let S be a non-empty set with an associative (and closed) binary operation, such that for every $x \in S$ there is a unique x' such that $xx'x = x$. Prove that S is a group.