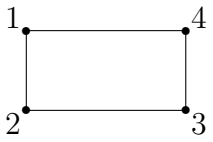
University of Birmingham
School of Mathematics

1AC Algebra and Combinatorics

Problem Sheet 5: Algebra part

You should carefully write out your solutions to all the questions below.
Ensure you have read and understood the Canvas assignment for the problem sheet for instructions about submitting solutions to SUM questions.

AQ1. Let G be the symmetry group of the rectangle below.



(a) Write down all elements of G expressed as permutations of the vertices.

(b) Calculate the multiplication table of G.
The multiplication table has rows and columns labelled by the elements of G and the entries are given by the products in G.

AQ2. (SUM) Let $p, q \in \mathbb{N}$ be primes with $p \neq q$ and let $G = \{[a]_{pq} \in \mathbb{Z}_{pq} : p \nmid a \text{ and } q \nmid a\}$. Prove that G is a group under multiplication.

AQ3. (SUM) Determine which of the following subsets of S_8 are subgroups of S_8.

(a) $H = \{g \in S_8 : g^2 = e\}$.

(b) $H = \{g \in S_8 : g(4) = 4 \text{ and } g(5) = 5\}$

(c) $H = \{g \in S_8 : g(i) \in \{1, 2, 3, 4\} \text{ for all } i \in \{1, 2, 3, 4\}\}$.

You should justify your answers.

AQ4. Prove Lemma 5.15.

Lemma. *Let G be a group and let $g \in G$. Then*

(a) $\langle g \rangle = \{g^m : m \in \mathbb{Z}\}$ *is a subgroup of* G.

(b) *If g has finite order, then $\langle g \rangle$ is finite and $|\langle g \rangle| = o(g)$.*

AQ5. (a) Let G be a group. Suppose that $g^2 = e$ for all $g \in G$. Prove that G is abelian.

(b) Prove Corollary 5.20.

Corollary. *Let $p \in \mathbb{N}$ be a prime and let G be a finite group of order p. Then G is cyclic.*

AQ6. Let $p = 37$ and $q = 43$, $N = pq = 1591$, and we let $e = 5$. Consider the RSA cryptosystem with public key (N, e).

(a) Calculate the private key d for the cryptosystem.

(b) You are sent the ciphertext $\mathbf{c} = (154, 798, 362)$. Decipher it.

It will help to use a modular arithmetic calculator for this question, and you should be able to find such a calculator online.