
MA2004 SETS AND ALGEBRAIC STRUCTURES
EXAMPLES 8

- Write out from memory the definitions of the following terms, and then check your notes to see if you got them right:
 - Function, injective function, surjective function, bijective function.
 - Relation, equivalence relation, equivalence class.
 - Binary operation, group, abelian group, subgroup, left coset, right coset.
- Let a and b be elements of a group G . If $aba = bab$ and $a^2 = e$ (where e is the identity element), show that $b^2 = e$. [Hint: first show that b is conjugate to a]
- Find all the subgroups of the group of question 10 of example sheet 5, namely the group consisting of the eight symmetries of the square.

You may want to use Lagrange's theorem to help you. Start by listing some subgroups, and then see if you can either find more subgroups or see why there are no more. It may also help you to know that the answer should be a list of ten different subgroups.
- Let $S = \{a, b, c, d\}$, and let R be the relation $\{(a, b), (c, b)\} \subseteq S \times S$. Let \sim be the smallest equivalence relation containing R . Write down \sim as a subset of $S \times S$, and find the equivalence classes for \sim .
- Let G be the group A_4 of even permutations on the set $\{1, 2, 3, 4\}$ and let H be the subgroup generated by the permutation $(1\ 2\ 3)$. Write down the elements of the group G and the subgroup H . What is $|G : H|$? Write down the left cosets of H in G . Write down the right cosets. Are they the same?
- Using Fermat's Little Theorem,
 - Find the remainder when 3^{16} is divided by 17.
 - Find the remainder when 3^{67} is divided by 17.
- If a and n are positive integers with $n > 1$ and $\gcd(a, n) = 1$, prove that $a^{\phi(n)} \equiv 1 \pmod{n}$, where $\phi(n)$ is Euler's phi function of n .

[Hint: Look at the proof of Fermat's Little Theorem, and see if you can mimic it]
- Use the previous question to find the remainder when 2^{17} is divided by 15.
- Let p be a prime number.
 - Show that if x^2 is congruent to 1 modulo p then x is congruent to either 1 or -1 modulo p .

Hint: factorise $x^2 - 1$ and use the fact that p is a prime number.
 - According to part (a), among the numbers $1, 2, \dots, p - 1$, the only ones which are their own multiplicative inverses (mod p) are 1 and $p - 1$. Use this to prove that $(p - 1)!$ is congruent to -1 modulo p .