Reading notes on Chapter 6: Cosets and Lagrange's Theorem

In chapter 4 on cyclic groups you proved in theorem 4.10 that every subgroup of a cyclic group is cyclic (i.e. generated by a single element) and moreover, in theorem 4.13, that the order of any element of a cyclic group divides the order of the group.

This latter result generalises to the famous Lagrange's Theorem, which says that in any finite group G, the order of any subgroup of G is always a divisor of the order of G.

This chapter uses the concept of *cosets* (a type of 'translate' of a subgroup) to prove the theorem.

It is important to be aware of the status of what is commonly known as the converse of Lagrange's theorem, i.e. is there a subgroup of G or order d is d is a divisor of the order of G? It is not necessary that there is. Proposition 6.15 shows a counter-example to this using the group A_4.

Section 6.3 then looks at some applciations of Lagrange's theorem to the multiplicative group of integers modulo n. These results will be familiar to you from your study of Number Theory last year.

Submission problems

Questions 6, 11 and 19 from section 6.4.

We may show some of the parts of question 11 in the lectures. Question 6 requires some thought and investigation but question 19 should be relatively straightforward compared to the other two.