Imperial College London

UNIVERSITY OF LONDON

BSc and MSci EXAMINATIONS (MATHEMATICS)

May-June 2006

This paper is also taken for the relevant examination for the Associateship.

M2P2

Groups, Rings and Numbers

Date: Thursday, 18th May 2006 Time: 10 am – 12 noon

Credit will be given for all questions attempted but extra credit will be given for complete or nearly complete answers.

Calculators may not be used.

1. Define the symmetric group S_n of degree n and the alternating group A_n of degree n, and state the order of each of these groups.

Let G be a group and let $g_1, \ldots, g_r$ be elements of G. Define $\langle g_1, \ldots, g_r \rangle$, the subgroup of G generated by $g_1, \ldots, g_r$.

Now let $G = S_4$. Stating carefully any general results to which you appeal, prove that

(a) $\langle (123), (234) \rangle = A_4$,

(b) $\langle (12), (23), (34) \rangle = S_4$.

2. State what it means to say that a group is *cyclic*.

(a) Prove that every subgroup of a cyclic group is cyclic.

(b) Stating carefully any results you require, prove that every group of prime order is cyclic.

Now let p and q be distinct prime numbers.

(c) Prove that $C_p \times C_q$ is cyclic.

(d) Prove that $(p\mathbb{Z}, +) \times (q\mathbb{Z}, +)$ is *not* cyclic.

3. Suppose that X is a set and G is a group of permutations of X. What does it mean to say that the elements s and t of X are in the same orbit? If $g \in G$, what is meant by $fix(g)$?

State, without proof, Burnside's Lemma concerning the number of orbits.

(a) Let X be the set of possible labellings of the faces of a cube with the numbers 1, 2, ..., 6, with different faces having different labels (thus X has size 6!), and let G be the group of rotations of the cube. You may assume that $|G|$ =24. Prove that if g is a non-identity element of G then $\mathit{fix}(g) = 0$. Deduce the number of essentially different dice.

(b) Let X be a finite set of size greater than 1, and G be a group of permutations of X. Prove that if the number of orbits is 1 then there exists $g \in G$ with $\mathit{fix}(g) = 0$.

4. (a) Prove that $6^{(6^{11}-1)} - 1$ is divisible by 5.

(b) Prove that $5^{(5^{11}-1)} - 1$ is divisible by 13.

(c) Prove that if $2^{(2^n-1)} - 1$ is prime then n is prime.

(d) Prove that $2^{(2^{11}-1)} - 1$ is *not* prime.

5. Suppose that G and H are groups, and that ϕ is a homomorphism from G to H. Prove that

$$G/\ker\,\phi \cong \operatorname{Im}\phi.$$

Now let $G = (\mathbb{Z}, +)$ and $H = (4\mathbb{Z}, +)$ and let ϕ be a homomorphism from G to H. Prove that $\operatorname{Im}\phi = (4m\mathbb{Z}, +)$ for some integer m. What is $\ker\phi$?