MATH 100A FALL 2015 MIDTERM 2 SOLUTIONS

1 Let $\phi : G_1 \to G_2$ be a homomorphism between two groups.

(a) (3 pts). Prove that $\phi(e) = e$. (This is a result in the text, so you must reprove it).

(b) (3 pts). Prove that if $a \in G_1$ has finite order, then $o(\phi(a))$ divides $o(a)$. (This is a result in the text, so you must reprove it).

(c) (4 pts). Suppose that $|G_1| = m$ and $|G_2| = n$, with $\gcd(m, n) = 1$. Prove that $\phi(a) = e$ for all $a \in G_1$.

Solution. (a). Since $e^2 = e$, we have $\phi(e) = \phi(e^2) = \phi(e)\phi(e)$. Multiplying on the right by $\phi(e)^{-1}$, we get $e = \phi(e)$.

(b). Suppose that $o(a) = n$. Then in particular $a^n = e$. Applying ϕ to this equation and using the defining property of a homomorphism gives $(\phi(a))^n = \phi(a^n) = \phi(e) = e$ (using part (a) for the final equality). Since if $b = \phi(a)$ then $b^n = e$, this implies by the properties of order that $o(b)$ divides n.

(c). If $a \in G_1$, then by the Corollary to Lagrange's theorem we have $o(a)|m$. By part (b), $o(\phi(a))|o(a)$, so $o(\phi(a))|m$. Since $\phi(a) \in G_2$, we also have $o(\phi(a))|n$ by the corollary to Lagrange's theorem. Since $\gcd(m, n) = 1$, we conclude that $o(\phi(a)) = 1$. This forces $\phi(a) = e$, since the identity element e is the only element of order 1 in G_2.

2. Consider $\alpha = (14532)(251)(53) \in S_5$.

(a) (3 pts). Write α as a product of transpositions. Is $\alpha \in A_5$?

(b) (3 pts). Find $o(\alpha)$.

(c) (2 pts). Write α^{-1} in disjoint cycle form.

(d) (2 pts). Is there $\sigma \in S_5$ such that $\sigma^2 = \alpha$? Justify your answer.

Solution. (a). Since in general $(a_1 a_2 \dots a_m) = (a_1 a_2)(a_2 a_3) \dots (a_{m-1} a_m)$, we get

$$\alpha = (14)(45)(53)(32)(25)(51)(53).$$

Date: November 13, 2015.

Since this is a product of 7 transpositions, α is an odd permutation, so $\alpha \notin A_5$.

(b). We calculate that $\alpha = (1)(2345)$ in disjoint cycle form. Since a k-cycle has order k, we get $o(\alpha) = 4$.

(c). We have $\alpha^{-1} = (2345)^{-1} = (5432)$ since in general $(a_1 a_2 \dots a_m)^{-1} = (a_m \dots a_2 a_1)$ by a direct calculation.

(d). Since a product of two even permutations is even and a product of two odd permutations is even, regardless of whether σ is even or odd we have σ^2 is even. Thus we cannot have $\sigma^2 = \alpha$, since α is odd.

3 (a) (3 pts). Suppose that a is an element of a group G with $o(a) = n$ for some $n \geq 1$. If d is a positive divisor of n, find $o(a^d)$. Justify your answer.

(b) (7 pts). Let G be a group with p^k elements, where p is a prime number and $k \geq 1$. Prove that G has a subgroup H with $|H| = p$.

Solution. (a). Let $n = dq$. We claim $o(a^d) = q$. First note that $(a^d)^q = a^{dq} = a^n = e$. On the other hand, if $1 \leq i < q$ then $(a^d)^i = a^{id}$ and $1 \leq id < qd = n$ and so $a^{id} \neq e$ since n is the smallest positive exponent of a for which $a^n = e$. Thus q is the smallest positive exponent of a^d which gives e and hence $o(a^d) = q$ as claimed.

(b). Since $k \geq 1$, G has some non-identity element a. Consider the cyclic subgroup $\langle a \rangle$. By the Corollary to Lagrange's theorem, $o(a)$ divides p^k and so must be equal to some power of p as well, say $o(a) = p^d$. We have $d > 0$ since $a \neq e$ and so $o(a) \neq 1$. Now by part (a), if $b = a^{p^{d-1}}$, then $o(b) = p^d/p^{d-1} = p$. So we have found an element of order p in the group. Then $H = \langle b \rangle$ is a cyclic subgroup with $|H| = p$, as required.

4 (10 pts). Let G be a *finite* group with $|G| > 1$, such that G has no subgroup H with $\{e\} \subsetneq H \subsetneq G$. Prove that $G \cong \mathbb{Z}_p$ for some prime number p.

Solution. Since $|G| > 1$, G has an element other than the identity element, say a. Consider $H = \langle a \rangle$. Since $a \neq e$, $o(a) > 1$ and so $|H| \neq \{e\}$. By hypothesis we must have $H = G$. Thus $G = \langle a \rangle$ is cyclic. By assumption G is finite and so $o(a) = n$ is finite.

Suppose that n is not prime, but rather $n = mq$ with $1 < m < n$, $1 < q < n$. Then $K = \langle a^m \rangle$ is a subgroup, and clearly $o(a^m) = q$, by problem 3(a). Since $o(a^m) = q$, $|K| = q$

and so $\{e\} \subsetneq K \subseteq G$. This contradicts the hypothesis. Thus n is prime, say $n = p$. Finally, a theorem from class and the text shows that a cyclic group of prime order p is isomorphic to $\mathbb{Z}_p$ under addition.