Midterm 1 Solutions

1.a. We know for any homomorphism $B \xrightarrow{g} C$ of finite groups $\#B = \#(\ker g) \cdot \#(\operatorname{im} g)$. As g is surjective $\operatorname{im} g = C$ so $\#\operatorname{im} g = \# C$. Similarly $A \xrightarrow{f} B$ is injective so $\# A = \# \operatorname{im} f = \# \ker g$ (as $\operatorname{im} f = \ker g$ by hypothesis). So $\# B = \# A \cdot \# C$.

A stronger statement, which follows from the 1st Isomorphism theorem is that $B/\ker g \simeq C$. As $\ker g = \operatorname{im} f$ we have $B/\operatorname{im} f \simeq C$ where again $A \simeq \operatorname{im} f$. We know that $\#(B/H) \cdot \# H = \# B$ so $\# H = \# \operatorname{im} f = \# A \Rightarrow \# B = \# A \cdot \# C$.

b. B is <u>not</u> always isomorphic to $A \times C$. Here are two counter-examples:

$$\mathbb{Z}/2\mathbb{Z} \xrightarrow{\text{mult by } 2} \mathbb{Z}/4\mathbb{Z} \xrightarrow[\text{mod } 2]{\text{reduce}} \mathbb{Z}/2\mathbb{Z}$$

$$A_3 \xrightarrow{\text{inclusion}} S_3 \xrightarrow{\text{sign}} \langle \pm 1 \rangle$$

It is easy to check that in each case the image of the first homomorphism is the image of the second. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is the Klein 4 group which is not cyclic like $\mathbb{Z}/4\mathbb{Z}$. $A_3 \times \langle \pm 1 \rangle$ is abelian because both A_3 and $\langle \pm 1 \rangle$ are, while S_3 is not.

2\. a. $Z = \{ z \in G \mid zg = gz \ \forall g \in G \}$

Let $\varphi : G \to \mathrm{Aut}(G)$ be the conjugation map discussed in class. Namely $g \longmapsto [h \mapsto ghg^{-1}]$. We've seen that this is a group homomorphism. Note that $\ker \varphi = \{ g \in G \mid h \mapsto ghg^{-1}$ is the identity map$\}$ $= \{ g \in G \mid ghg^{-1} = h \ \forall h \in G \} = \{ g \in G \mid gh = hg \ \forall h \in G \} = Z$. As any kernel of a group homomorphism is a normal subgroup, so is Z.

b. If G/Z is cyclic, then there is some coset aZ that is a generator. As $Z \trianglelefteq G$, $(aZ)^n$ is a coset of Z that contains $(a \cdot 1)^n = a^n$. In particular each coset of G has the form $a^n Z$ for some $n \in \mathbb{Z}$.

Let $g, h \in G$. Then $g = a^n z_1$ and $h = a^m z_2$ for some $m, n \in \mathbb{Z}$, $z_1, z_2 \in Z$. Then $gh = (a^n z_1)(a^m z_2) = a^n a^m z_1 z_2 = a^m a^n z_1 z_2 = a^m a^n z_2 z_1$ $= a^m z_2 a^n z_1 = hg$ as the z_1, z_2 commute with everything and a^m commutes with a^n. So G is abelian.

78 exams. Answers

HARVARD COLLEGE

BENEDICT H. GROSS
LEVERETT PROFESSOR OF MATHEMATICS
DEAN OF HARVARD COLLEGE

UNIVERSITY HALL, FIRST FLOOR
CAMBRIDGE, MASSACHUSETTS 02138
(617) 495-1560

3 a) If a is in HgH, then $a = hgh'$

so $g = h^{-1} a (h')^{-1}$ is in HaH

so $HgH = HaH$

Hence if HgH and $Hg'H$ have the element a in common, they are both equal to HaH.

b) If H is normal, $gH = Hg$ for all g

Hence $HgH = (Hg) \cdot H = (gH) \cdot H = gH$

c) If H is not normal, $gH \neq Hg$ for some g

If HgH is a single left coset, it must be gH,

as it contains gH.

But it also contains Hg, so cannot be equal to gH.

d) There are n single cosets gH, determined by $g(n)$.

There are 2 double cosets : $HeH = H$ of elements fixing n

$HgH = G - H$ of elements not fixing n

The first has $(n-1)!$ elements

The second has $n! - (n-1)!$ elements

HARVARD COLLEGE

BENEDICT H. GROSS
LEVERETT PROFESSOR OF MATHEMATICS
DEAN OF HARVARD COLLEGE

UNIVERSITY HALL, FIRST FLOOR
CAMBRIDGE, MASSACHUSETTS 02138
(617) 495-1560

4 a) The order of S_n is $n!$
If $p > n$ then p does not divide $n!$
Since the order of any element divides the order of a group, S_n does not contain an element of order p.

b) If $p \leq n$ the element
$$g = (1\,2\,3 \ldots p)$$
in S_n has order p.

c) If p is odd, then the element g in part b) lies in the subgroup $A_n = \ker(\text{sign}: S_n \to \pm 1)$.
Indeed, $\text{sign}(g)^p = \text{sign}(g^p) = \text{sign}(e) = +1$, so $\text{sign}(g) = +1$. So for p odd, we need $n \geq p$.
If $p = 2$, we need $n \geq 4$. The element $(12)(34)$ then lies in A_n. The groups A_2 and A_3 do not contain any elements of order 2.