M2PM2 Algebra II, Progress Test 2, solutions, 25/11/2014.

Q1.

i) The only ways of breaking up 12 into factors: $12 = 12 = 2 \times 6 = 3 \times 4 = 2 \times 2 \times 3$. So by the fundamental theorem, all abelian groups of order 12 are isomorphic to C_{12}, $C_2 \times C_6$, $C_3 \times C_4$ or $C_2 \times C_2 \times C_3$. However some of these groups might be isomorphic, and indeed some of them are: $C_3 \times C_4 \cong C_{12}$ by the result in lectures saying that if a and b are coprime then $C_a \times C_b \cong C_{ab}$. Similarly $C_2 \times C_3 \cong C_6$ so $C_2 \times C_2 \times C_3 \cong C_2 \times C_6$ (if $G \cong H$ then $K \times G \cong K \times H$ and the proof is not hard; I'm happy for the students to assume this).

So far we have deduced that every abelian group of order 12 is isomorphic to either C_{12} or $C_2 \times C_6$. However these last two groups are not isomorphic – indeed C_{12} has an element of order 12, but for any $(x, y) \in C_2 \times C_6$ we see $(x, y)^6$ is the identity, so there are no elements of order 12 in $C_2 \times C_6$. Two marks only for this question – not because I'm mean, but because a harder version of this question was on an example sheet.

ii) Say $C_6 = \langle x \rangle$, so x has order 6. Say $\phi : C_6 \to C_6$ is an isomorphism. Then $\phi(x)$ will also have order 6; this is a basic fact about isomorphisms, proved in lectures. But $C_6 = \{1, x, x^2, x^3, x^4, x^5\}$ and one checks easily that x^2, x^4 have order 3 and x^3 has order 2, and 1 of course has order 1, so the only elements of order 6 in C_6 are x and x^5. Next note that if $\phi : C_6 \to C_6$ is an isomorphism and if we know $\phi(x) = y$ then we know ϕ completely, because $\phi(x^n) = y^n$ for all n.

So now we know what to do – we need to see if there is an isomorphism sending x to x, and see if there is an isomorphism sending x to x^{-1}. Let's consider an isomorphism sending x to x. Is ther one? Yes – the identity is one, and by the above remark it's the only one. So there's one isomorphism. What about an isomorphism sending x to $x^5 = x^{-1}$? Again there can be at most one, and indeed there is exactly one; it's the map sending x^n to x^{-n} for all n; I would be happy if people said that this was "obviously" an isomorphism, but a formal proof would be to note that x^a goes to x^{-a}, and x^b goes to x^{-b}, and x^{a+b} goes to $x^{-(a+b)}$ which is indeed $x^{-a}x^{-b}$. So there are two isomorphisms from C_6 to C_6. Three marks.

iii) How about $C_2 \times C_2 \times C_2 \times \cdots \times C_2$, where there are 7 (or more) terms in the product; this group has order 2^7 (or more) which is bigger than 100, but clearly the square of any element in this group is the identity, so all but one element has order 2 and the other one has order 1. Two marks.

iv) ϕ is a bijection because if ψ is the map sending y to gyg^{-1} then I claim ϕ and ψ are inverses. Indeed $\phi(\psi(y)) = \phi(gyg^{-1}) = g^{-1}gyg^{-1}g = y$, and similarly $\psi(\phi(x)) = gg^{-1}xgg^{-1} = x$. Alternatively just prove injectivity and surjectivity by hand.

Next ϕ is an isomorphism because $\phi(xy) = g^{-1}xyg$ and $\phi(x)\phi(y) = g^{-1}xgg^{-1}yg = g^{-1}xyg = \phi(xy)$. Three marks because this is a bit abstract.

Q2.

i) Let G be C_4, generated by g of order 4 (if we consider C_4 to be the 4th roots of unity, as we did in the course, then g can be i) and let H be C_2, generated by h of order 2 (so $h = -1$). Consider the map $G \to H$ sending z to z^2. This is easily checked to be a group homomorphism ($(zw)^2 = z^2w^2$) and it sends G to H because if $z^4 = 1$ then $(z^2)^2 = 1$. Finally it sends g to h, so we're done. Two marks.

ii) There does not, because a result from the course says that the order of $\phi(g)$ divides the order of g, and 3 does not divide 4. Two marks.

iii) Set $H = M \cap N$. If $g \in G$ then, by a result in the course, we need to check that $gHg^{-1} \subseteq H$, so we need to check $gHg^{-1} \subseteq M$ and $gHg^{-1} \subseteq N$. But this is clear because $gHg^{-1} \subseteq gMg^{-1} = M$ (as M is normal) and $gHg^{-1} \subseteq gNg^{-1} = N$ (as N is normal), so we're done. Two marks.

iv) This is a bit of a curveball because I hadn't mentioned this result at all in the course. I'll give four marks for it, so there's plenty of scope for partial credit.

To check X is a subgroup we need to check that it contains the identity, and if $x, y \in X$ then so are xy and x^{-1}. The identity is fine: M and N are normal subgroups, and $e \in M$, $e \in N$, so $e = e^2 \in X$.

The other arguments are a bit harder. Let's prove the lemma first. Say $m \in M$ and $n \in N$. Because M is normal we have $g^{-1}Mg = M$ for all g, so (multiplying on the left by g) we have $Mg = gM$. Now set $g = n$ and we deduce that $nm \in nM = Mn$, which means that $nm = m'n$ for some $m' \in M$. In particular $nm \in X$.

Now let's prove that X is a subgroup. Say $x = mn \in X$, with $m \in M$ and $n \in N$. Then $x^{-1} = n^{-1}m^{-1}$ and $n^{-1} \in N$, $m^{-1} \in M$, so by the lemma $n^{-1}m^{-1} \in X$. So X is closed under inverses.

Finally let's check X is closed under multiplication. Say $x = m_1n_1 \in X$ and $y = m_2n_2 \in X$. Then $xy = m_1n_1m_2n_2$. Applying the lemma to n_1m_2 we deduce that $n_1m_2 = m_3n_3$ for some $m_3 \in M$ and $n_3 \in N$. Hence $xy = m_1m_3n_3n_2 = (m_1m_3)(n_3n_2) \in X$ and we are home. Well done to any student who got that out.