HONORS ALGEBRA: SOLUTIONS TO HOMEWORK 4

2.5, Q12. Whenever $z \in Z(G)$ and $g \in G$, one has $zg = gz$, and hence $g^{-1}zg = (g^{-1}g)z = z$, whence $g^{-1}Z(G)g \subseteq Z(G)$ for each $g \in G$. Thus $Z(G) \lhd G$, as required.

2.5, Q15. Suppose that $N \lhd G$ and $\varphi : G \to G'$ is a surjective homomorphism. Since N is itself a group, we know (Lemma 2.5.3) that $\varphi(N)$ is a subgroup of G'. By the surjectivity of φ, whenever $g \in G'$ and $n \in \varphi(N)$, there exists $a \in G$ and $b \in N$ with the property that $\varphi(a) = g$ and $\varphi(b) = n$. Thus, we have $g^{-1}ng = \varphi(a)^{-1}\varphi(b)\varphi(a) = \varphi(a^{-1})\varphi(b)\varphi(a) = \varphi(a^{-1}ba)$. But since $N \lhd G$, we have $a^{-1}ba \in N$, and thus $g^{-1}\varphi(N)g \subseteq \varphi(N)$. Hence $\varphi(N) \lhd G'$, as required.

2.5, Q20. Since $M \lhd G$, for each $m \in M$ and each $n \in N \subseteq G$, one has $n^{-1}mn \in M$, whence $m^{-1}n^{-1}mn \in M$. Also, since $N \lhd G$, for each $n \in N$ and each $m \in M \subseteq G$, one has $m^{-1}n^{-1}m \in N$, whence $m^{-1}n^{-1}mn \in N$. Thus, one has $m^{-1}n^{-1}mn \in M \cap N = \{e\}$. Hence we conclude that $m^{-1}n^{-1}mn = e$, whence $mn = nm$ for all $m \in M$ and $n \in N$.

2.5, Q26. Define $\psi : G \to A(G)$ by $\psi(a) = \sigma_a$ for $a \in G$, where $\sigma_a(g) = aga^{-1}$ for all $g \in G$.
(a) For all $a, b \in G$, one has $\psi(ab) = \sigma_{ab}$, where $\sigma_{ab}(g) = abg(ab)^{-1} = a(bgb^{-1})a^{-1} = \sigma_a(\sigma_b(g))$, for all $g \in G$. Thus $\sigma_{ab} = \sigma_a \circ \sigma_b = \psi(a) \circ \psi(b)$, and hence $\psi(ab) = \psi(a)\psi(b)$ for all $a, b \in G$. So ψ is indeed a homomorphism from G into $A(G)$, as required.
(b) One has $\ker(\psi) = \{a \in G : \psi(a) = \mathrm{id}\} = \{a \in G : \sigma_a(g) = g \text{ for all } g \in G\} = \{a \in G : aga^{-1} = g \text{ for all } g \in G\} = \{a \in G : ag = ga \text{ for all } g \in G\} = Z(G)$.

2.5, Q34. The group $A(G)$ of bijective self-maps of G discussed in Q26 has a subgroup $\mathcal{A}(G)$ consisting of all the automorphisms of G (that is, bijective self-maps that are also homomorphisms). Let $I(G) = \{\sigma_a : a \in G\}$, where $\sigma_a(g) = aga^{-1}$ for all $g \in G$. If $\varphi \in \mathcal{A}(G)$ and $\sigma_a \in I(G)$, then the map $\varphi^{-1}\sigma_a\varphi$ is the automorphism satisfying the property that for all $g \in G$, one has $(\varphi^{-1}\sigma_a\varphi)(g) = \varphi^{-1}(\sigma_a(\varphi(g))) = \varphi^{-1}(a\varphi(g)a^{-1})$. Since φ, and hence also φ^{-1}, is a homomorphism, however, the latter is equal to $\varphi^{-1}(a)\varphi^{-1}(\varphi(g))\varphi^{-1}(a)^{-1} = hgh^{-1}$, in which we write $h = \varphi^{-1}(a)$. But then, for all $g \in G$, we have $(\varphi^{-1}\sigma_a\varphi)(g) = hgh^{-1} = \sigma_h(g)$, whence $\varphi^{-1}\sigma_a\varphi = \sigma_h \in I(G)$. Since this relation holds for all $\sigma_a \in I(G)$, we see that for all $\varphi \in \mathcal{A}(G)$ we have $\varphi^{-1}I(G)\varphi \subseteq I(G)$, so that $I(G) \lhd \mathcal{A}(G)$.

2.5, Q40. Suppose that G is a finite group of order n, and $H \le G$ satisfies $n \nmid i_G(H)!$. Let $A(S)$ denote the group of bijective self-mappings of the set $S = \{Ha : a \in G\}$. Since $|S| = |G|/|H| = i_G(H)$, and $A(S)$ is a group of permutations of S, it follows that $|A(S)| = i_G(H)!$. We define a map $\varphi : G \to A(S)$ by $g \mapsto T_g$, where $T_g(Ha) = Hag^{-1}$ for each right coset Ha. We claim that this mapping is a homomorphism of groups. The mapping is plainly well-defined, and when $g, h \in G$ one has $(gh)^{-1} = h^{-1}g^{-1}$, so $\varphi(gh) = T_{gh} = T_g \circ T_h = \varphi(g) \circ \varphi(h)$. Hence φ possesses the homomorphism property. Moreover, one has that $\ker(\varphi)$ is a normal subgroup of G (Theorem 2.5.5). Suppose for the moment that $\ker(\varphi)$ is trivial and is equal to $\{\mathrm{id}\}$ in $A(S)$. Then the mapping φ is injective, and hence the group $\varphi(G)$ has order $|G| = n$. But $\varphi(G)$ is a subgroup of $A(S)$, and hence Lagrange's theorem shows that $|\varphi(G)| = n$ divides $|A(S)| = i_G(H)!$. This conclusion contradicts our initial hypothesis, so $\ker(\varphi)$ cannot be trivial. Hence $\ker(\varphi)$ is a normal subgroup of G which is not equal to the trivial group $\{e\}$. In fact, one has $\ker(\varphi) = \{g \in G : T_g = \mathrm{id}\} = \{g \in G : Hag^{-1} = Ha \text{ for all } a \in G\}$. Thus, if we take

$a = e$ in the last relation, we see that $\ker(\varphi) \subseteq \{g \in G : g^{-1} \in H\} = H$. We therefore conclude that $\ker(\varphi)$ is a normal subgroup of G not equal to $\{e\}$ and contained in H.

2.5, Q44. Suppose that G is a group of order p^2, with p a prime number. By Lagrange's theorem, any subgroup of G has order dividing $|G| = p^2$, and thus if $a \in G$ is not the identity element, then the order of a is either p or p^2. In the latter case, the element a^p has order p^2. Thus, in either case, the group G contains an element b of order p, and hence a subgroup $H = \langle b \rangle$ of order p. One then has $i_G(H) = |G|/|H| = p^2/p = p$. Observe that $p^2 \nmid p!$, and hence $|G|$ does not divide $i_G(H)!$. We thus deduce from the conclusion of Q40 that there is a normal subgroup $N \neq \{e\}$ of G contained in H. But H has order p a prime, so has no proper subgroups, and thus $N = H$. Hence $H \lhd G$, and G has a normal subgroup H of order p.

2.6, Q7. Suppose that G is a cyclic group, say $G = \langle a \rangle$, and N is a subgroup of G. Since G is cyclic, and hence abelian, we have $N \lhd G$. But then we can examine the group G/N and observe that $\langle Na \rangle = \{Na^j : j \in \mathbb{Z}\} = \{Nb : b \in G\} = G/N$. Thus $G/N = \langle Na \rangle$ is cyclic, as required.

2.6, Q11. Suppose that G is a group satisfying the property that $G/Z(G)$ is cyclic, say $G/Z(G) = \langle Z(G)a \rangle = \{Z(G)a^j : j \in \mathbb{Z}\}$. Consider two elements $g, h \in G$. For some integers j and k, one has $g \in Z(G)a^j$ and $h \in Z(G)a^k$. Hence, there exist $z_1, z_2 \in Z(G)$ for which $g = z_1 a^j$ and $h = z_2 a^k$. Notice that from the definition of $Z(G)$, the elements z_1 and z_2 commute with all elements of G. In particular, one sees that $gh = (z_1 a^j)(z_2 a^k) = (z_1 z_2) a^{j+k} = (z_2 z_1) a^{k+j} = (z_2 a^k)(z_1 a^j) = hg$. Since this relation holds for all $g, h \in G$, we are forced to conclude that G is abelian.

2.6, Q13. Suppose that G is a group, and $N \lhd G$ satisfies the property that for all $a, b \in G$, one has $aba^{-1}b^{-1} \in N$. Consider two elements $Ng, Nh \in G/N$. One has

$$(Ng)(Nh)(Ng)^{-1}(Nh)^{-1} = (Ng)(Nh)(Ng^{-1})(Nh^{-1}) = N(ghg^{-1}h^{-1}) \in N.$$

Thus $(Ng)(Nh)(Ng)^{-1}(Nh)^{-1} = Ne$, so that $(Ng)(Nh) = (Nh)(Ng)$. Since this relation holds for all $Ng, Nh \in G/N$, we conclude that G/N is abelian.

2.6, Q14. Suppose that G is an abelian group of order $n = p_1 p_2 \cdots p_k$, where the p_i are distinct primes. It follows from Cauchy's theorem that for each i, since p_i divides $|G|$, then the group G has an element a_i of order p_i. Consider the element $b = a_1 a_2 \cdots a_k$. Suppose that r is the least positive integer for which $b^r = e$. If we write n_i for the integer n/p_i for each i, and observe that n_i is divisible by p_j for all $j \neq i$, we see that $(a_j^{p_j})^{rn_i/p_j} = e$ for each integer $j \neq i$. Thus $e = (b^r)^{n_i} = a_i^{rn_i}$ for each i, whence $p_i | rn_i$ for each i. But $p_i \nmid n_i$, so $p_i | r$ for each i. Consequently, we find that r must be divisible by $p_1 p_2 \cdots p_k = n$. But then the subgroup $\langle b \rangle$ has order at least $n = |G|$, whence $G = \langle b \rangle$ must be cyclic.

2.6, Q15. Suppose that G is an abelian group having one element a of order m, and another element b of order n, with $(m, n) = 1$. Suppose that r is a positive integer for which $(ab)^r = e$. Then $e = ((ab)^r)^m = (a^m)^r b^{rm} = e^r b^{rm} = b^{rm}$. But since the order of b is n and $b^{rm} = e$, we must have $n | (rm)$, and since $(m, n) = 1$, this implies that $n | r$. Similarly, and symmetrically, we deduce from the relation $e = ((ab)^r)^n$ that $m | r$. Thus, since $(m, n) = 1$ and both m and n divide r, we must have $(mn) | r$. Then since $(ab)^{mn} = (a^m)^n (b^n)^m = e$, it follows that r is the smallest positive integer with the property that $(ab)^r = e$, and thus the order of ab is mn, as claimed.