HONORS ALGEBRA: SOLUTIONS TO HOMEWORK 7

2.8, Q2. Let G be a group of order 35. Then since $35 = 5 \times 7$ as a product of primes, and $7 > 5$ with $5 \nmid (7-1)$, we find from Theorem 2.8.5 that G is cyclic.

2.8, Q4. We can formally construct a non-abelian group G of order 21 using two generators, namely a of order 3 and b of order 7. Thus $a^3 = b^7 = e$. Every element of G can be written in the shape $a^i b^j$ with $0 \le i < 3$ and $0 \le j < 7$, with the canonical group law, provided that we write ba in such a form. Notice that all 21 of these elements are distinct. We can apply the corollary to Lemma 2.8.3 with $p = 7$ and $q = 3$ to see that $a^{-1}ba = b^i$ for some integer i with $0 \le i < 7$. But, since $a^3 = e$, we can argue as in the proof of Theorem 2.8.5 that $b = a^{-3}ba^3 = b^{i^3}$. Thus, since b has order 7, we find that this is consistent only when $i^3 \equiv 1 \pmod 7$, so that $i = 1$, 2 or 4. The case $i = 1$ corresponds to the abelian relation $ba = ab$, and we may ignore this since we seek a non-abelian group of order 21. Thus we may take either $ba = ab^2$ or $ba = ab^4$, and both relations yield a non-abelian group of order 21. Notice that $b^m a = ab^{im}$ for each m, and thus any product $(a^l b^j)(a^{l'} b^{j'})$ can be rewritten in the form $a^{l''} b^{j''}$ for suitable l'' and j''.

2.8, Q5. Let G be a group of order $p^n m$ with p prime, $p \nmid m$, and suppose that $P \lhd G$ satisfies $|P| = p^n$. We claim that P is the only normal subgroup of G having order p^n. Suppose, by way of deriving a contradiction, that there is a second such subgroup, say Q. Then $P \cap Q \lhd P$ and $|P \cap Q| < |P|$. By the Second Homomorphism Theorem, we then have $P/(P \cap Q) \cong (PQ)/Q$, whence $|PQ| = |P| \cdot |Q|/|P \cap Q| > |Q| = p^n$. But by Lagrange's theorem, the order of $P \cap Q$ is a power of p, and thus PQ is a subgroup of G having order p^k with $k > n$. This yields a contradiction, since $p^k \nmid |G|$, and so we conclude that P is indeed the only normal subgroup of G of order p^n. Suppose next that θ is an automorphism of G. Then given $g \in G$, there exists $h \in G$ with $\theta(h) = g$, and thus $g^{-1}\theta(P)g = \theta(h)^{-1}\theta(P)\theta(h) = \theta(h^{-1}Ph) = \theta(P)$, by the normality of P in G. Since $\theta(P) \le G$, it follows that $\theta(P) \lhd G$. But $|\theta(P)| = |P| = p^n$, and P is the only normal subgroup of G having order p^n. We are therefore forced to conclude that $\theta(P) = P$ for all automorphisms θ of G.

2.8, Q8. Let G be a group of order 99. It follows from Cauchy's theorem that G contains an element a of order 11, and hence a subgroup $A = \langle a \rangle$ of order 11. We claim that A is the only subgroup of G of order 11. For if B is a subgroup of order 11 and $B \ne A$, then just as in the proof of Lemma 2.8.3 we find that AB is a subset of G having $11^2 > |G|$ elements, which yields a contradiction. Then A is indeed the only subgroup of G having 11 elements, whence $g^{-1}Ag = A$ for all $g \in G$. Hence $A \lhd G$ and G has a nontrivial normal subgroup.

2.8, Q9. By Cauchy's theorem, a group G of order 42 has elements of order 2, 3 and 7. Suppose that a is an element of order 7, and put $A = \langle a \rangle$. We claim that A is the only subgroup of G of order 7. For if B is a subgroup of order 7 and $B \ne A$, then just as in the proof of Lemma 2.8.3 we find that AB is a subset of G having $7^2 > |G|$ elements, which yields a contradiction. Then A is indeed the only subgroup of G having 7 elements, whence $g^{-1}Ag = A$ for all $g \in G$. Hence $A \lhd G$ and G has a nontrivial normal subgroup.

2.8, Q10. Let G be a group of order 42. Then we know that G has a normal subgroup N of order 7. Write $G' = G/N$. Then Theorem 2.6.2 shows that there is a surjective homomorphism

$\psi : G \to G'$ with $\ker(\psi) = N$. Since $|G'| = |G|/|N| = 42/7 = 6$, it follows from Cauchy's theorem that G' has an element b of order 3. Put $H' = \langle b \rangle$. Then from Lemma 2.8.3 we see that $H' \lhd G'$. Putting $H = \{g \in G : \psi(g) \in H'\}$, we find from the Correspondence Theorem that $H \lhd G$ and $H/N \cong H'$. But then $3 = |H'| = |H|/|N| = |H|/7$, whence $|H| = 21$. So there is indeed a normal subgroup H of G having order 21.

2.8, Q12. Let G be a non-abelian group of order 21. Then by Cauchy's theorem, we find that G has an element a of order 3, and an element b of order 7, and these elements are necessarily distinct. Moreover, the corollary to Lemma 2.8.3 shows that one necessarily has $a^{-1}ba = b^i$ for some integer i with $0 \leq i < 7$. As we saw in question 4, one must then have $i = 2$ or 4 if G is to be non-abelian. Thus, the group G is isomorphic to one of the two groups corresponding to these values of i defined in question 4. For $i = 2$ and 4, consider the group G_i corresponding to i with generators a_i and b_i satisfying $a_i^3 = b_i^7 = e_i$ and $b_i a_i = ab_i^i$. We consider the map $\varphi : G_2 \to G_4$ defined by taking $\varphi(a_2^m b_2^n) = a_4^{2m} b_4^{4n}$. Thus $\varphi(a_2) = a_4^2$ and $\varphi(b_2) = b_4^4$. It is apparent that this defines a bijection by considering the inverse map $\psi : G_4 \to G_2$ defined by taking $\psi(a_4^m b_2^n) = a_2^{2m} b_2^{2n}$. The homomorphism property of φ is confirmed by observing that

$$\varphi(a_2^m b_2^n a_2^{m'} b_2^{n'}) = \varphi(a_2^{m+m'} b_2^{n2^{m'}+n'}) = a_4^{2m+2m'} b_4^{4n2^{m'}+4n'} = a_4^{2m+2m'} (b_4^4)^{n4^{2m'}+n'}$$
$$= a_4^{2m} (b_4^4)^n a_4^{2m'} (b_4^4)^{n'} = \varphi(a_2^m b_2^n) \varphi(a_2^{m'} b_2^{n'}).$$

Then $G_2 \cong G_4$, and we see that any two non-abelian groups of order 21 are isomorphic.

2.9, Q1. Define the map $\varphi : G_1 \times G_2 \to G_2 \times G_1$ by taking $\varphi(g_1, g_2) = (g_2, g_1)$. By considering the inverse map $\psi : G_2 \times G_1 \to G_1 \times G_2$ defined by putting $\psi(g_2, g_1) = (g_1, g_2)$, we see that φ is a bijection. Moreover, when (g_1, g_2) and (h_1, h_2) both lie in $G_1 \times G_2$, one finds that $\varphi((g_1, g_2)(h_1, h_2)) = \varphi(g_1 h_1, g_2 h_2) = (g_2 h_2, g_1 h_1) = (g_2, g_1)(h_2, h_1) = \varphi(g_1, g_2)\varphi(h_1, h_2)$, so that φ satisfies the homomorphism property. Thus φ is an isomorphism, and one has $G_1 \times G_2 \cong G_2 \times G_1$.

2.9, Q2. Suppose that G_1 and G_2 are cyclic groups of respective orders m and n. We have that $G_1 \times G_2$ is cyclic with generator (a, b) if and only if (a, b) has order $mn = |G_1 \times G_2|$. But the order of a divides m and the order of b divides n. Suppose that $(m, n) = d$. Then $(a, b)^{mn/d} = ((a^m)^{n/d}, (b^n)^{m/d}) = (e, e)$, so that (a, b) has order dividing mn/d. In particular, if $d = (m, n) > 1$, then (a, b) has order smaller than mn and $G_1 \times G_2$ cannot be cyclic. When $(m, n) = 1$, meanwhile, we may assume that $G_1 = \langle a \rangle$ and $G_2 = \langle b \rangle$ with a of order m and b of order n. If $(e, e) = (a, b)^r = (a^r, b^r)$, then $m|r$ and $n|r$, whence $mn|r$, and so (a, b) has order mn and $G_1 \times G_2 = \langle (a, b) \rangle$, so that $G_1 \times G_2$ is cyclic. Thus $G_1 \times G_2$ is cyclic if and only if $(m, n) = 1$.

2.9, Q3. (a) Define the map $\varphi : G \to T$ by taking $g \mapsto (g, g)$. Then φ is plainly well-defined and surjective. Moreover, one has $\varphi(g) = \varphi(h)$ if and only if $(g, g) = (h, h)$, which holds if and only if $g = h$, and so φ is also injective. Finally, whenever $g, h \in G$, one has $\varphi(gh) = (gh, gh) = (g, g)(h, h) = \varphi(g)\varphi(h)$, so φ is a homomorphism. Thus, the map φ is an isomorphism, and so $T \cong G$.

(b) If G is abelian, then given any element $(a, a) \in T$, whenever $(g, h) \in A$ one has $(g, h)^{-1}(a, a)(g, h) = (g^{-1}ag, h^{-1}ah) = (g^{-1}ga, h^{-1}ha) = (a, a)$. Hence, for all $\gamma \in A$ one has $\gamma^{-1}T\gamma = T$, whence $T \lhd A$. If, on the other hand, one has $T \lhd A$, then for all $a, b \in G$ one has $(e, b)^{-1}(a, a)(e, b) \in A$, whence for some element $c \in G$ one has $(a, b^{-1}ab) = (c, c)$. Thus $c = a$ and $b^{-1}ab = c = a$. We therefore conclude that for all $a, b \in G$ one has $ab = ba$, which is to say that G is abelian. Thus $T \lhd A$ if and only if G is abelian.

2.9, Q5. Suppose that $G = N_1N_2 \cdots N_k$ and some element $g \in G$ has more than one representation in the form $g = g_1g_2 \cdots g_k$, with $g_i \in N_i$ for each i. Then one must have $|G| < |N_1||N_2| \cdots |N_k|$, yielding a contradiction. Thus each element $g \in G$ must have a unique representation in the form $g = g_1g_2 \cdots g_k$, with $g_i \in N_i$ for each i, so that G is the internal direct product of $N_1, N_2, \ldots, N_k$.

2.9, Q6. For each i, write $M_i = N_1N_2 \cdots N_{i-1}N_{i+1} \cdots N_k$. Observe that whenever $j \neq i$ and $g_j \in N_j$, one has $g_j = ee \cdots eg_je \cdots e \in M_i$. Thus, if $N_i \cap M_i = \{e\}$ for each i, then we have $N_i \cap N_j = \{e\}$ whenever $i \neq j$. The Corollary to Lemma 2.9.3 therefore shows that whenever $g_i \in N_i$, then g_i commutes with every element of N_j $(j \neq i)$, and hence with every element of M_i. But then, if $g_i, h_i \in N_i$ $(1 \leq i \leq k)$, one has that $g_1 \cdots g_k = h_1 \cdots h_k$ if and only if $e = g_k^{-1} \cdots g_2^{-1}(g_1^{-1}h_1)h_2 \cdots h_k = (g_1^{-1}h_1)(g_2^{-1}h_2) \cdots (g_k^{-1}h_k)$. The latter holds if and only if $h_1^{-1}g_1 = (g_2^{-1}h_2) \cdots (g_k^{-1}h_k) \in M_1$. Since $h_1^{-1}g_1 \in N_1$ and $N_1 \cap M_1 = \{e\}$, it follows that $h_1^{-1}g_1 = e$ and thus $g_1 = h_1$. We can repeat this argument now with the index 2 in place of 1, and proceeding inductively, we deduce that $g_i = h_i$ for each i. Thus, each element of $N_1N_2 \cdots N_k$ has a unique representation $g_1g_2 \cdots g_k$ with $g_i \in N_i$ for each i, whence $|G| = |N_1||N_2| \cdots |N_k|$. We therefore conclude from Q5 that G is the internal direct product of $N_1, N_2, \ldots, N_k$.