HONORS ALGEBRA: SOLUTIONS TO HOMEWORK 5

2.6, Q16. Let G be an abelian group of order $p^n m$, where p is a prime with $p \nmid m$, and put $P = \{a \in G : a^{p^k} = e \text{ for some } k \text{ depending on } a\}$.
(a) The set P is non-empty, and if $a, b \in P$, then for some integers k and h one has $a^{p^k} = b^{p^h} = e$, whence $(ab^{-1})^{p^{k+h}} = (a^{p^k})^{p^h}(b^{p^h})^{-p^k} = e^{p^h}e^{-p^k} = e$. The latter implies that $ab^{-1} \in P$. Hence $P \leq G$, as a consequence of the subgroup criterion.
(b) Since G is abelian, the subgroup P of G is normal. Suppose that $Px \in G/P$ has order p. Then we have $P = (Px)^p = Px^p$, so that $x^p \in P$. But then the definition of p implies that for some k depending on x, one has $e = (x^p)^{p^k} = x^{p^{k+1}}$, whence $x \in P$. We are therefore forced to conclude that $Px = P$, and the latter coset has order 1 in G/P, yielding a contradiction. There is therefore no element in G/P having order p.
(c) Suppose that $|P| = t$. By Lagrange's theorem, the order of P divides that of G, and so $t|(p^n m)$. Thus, if $p^n \nmid t$, one has that p divides $(p^n m)/t = |G|/|P| = |G/P|$. However, Cauchy's theorem shows that when p divides $|G/P|$, then G/P has an element of order p, and we have shown in part (b) that this is not the case. We must therefore conclude that $p^n|t$. Suppose, if possible, that $t \neq p^n$, so that t is divisible by a prime q different from p. In such circumstances, Cauchy's theorem shows that P has an element a of order q. But the definition of P ensures that the order of a divides p^k for some $k \in \mathbb{N}$, and this is impossible since $q \nmid p^k$. Thus we deduce that $t = p^n$, and hence $|P| = p^n$.

2.6, Q18. (a) In order to confirm that the set $T = \{a \in G : a^m = e \text{ for some } m > 1 \text{ depending on } a\}$ is a subgroup of G, observe first that $e \in T$, so that T is non-empty. Next, when $a, b \in T$, there exist integers $n > 1$ and $m > 1$ with $a^n = b^m = e$, and thus (since G is abelian) one has $(ab^{-1})^{nm} = (a^n)^m(b^m)^{-n} = e^m e^{-n} = e$. Hence $ab^{-1} \in T$, and so $T \leq G$ by the subgroup criterion.
(b) Since G is abelian, the subgroup T of G must be normal. Suppose that G/T has an element Tx of finite order, say $e = (Tx)^k = Tx^k$ for some $k \in \mathbb{N}$. Then $x^k \in T$, so that for some $n \in \mathbb{N}$ one has $e = (x^k)^n = x^{kn}$. But the latter implies that $x \in T$, whence $Tx = T$. Then G/T has no element, other than the identity element T, of finite order.

2.7, Q4. (a) Define $\psi : G \to G_2$ by putting $\psi((a, b)) = b$. This map is well-defined, and for all (a_1, b_1) and (a_2, b_2) in G, one has $\psi((a_1, b_1)(a_2, b_2)) = \psi((a_1a_2, b_1b_2)) = b_1b_2 = \psi((a_1, b_1))\psi((a_2, b_2))$, so ψ is a homomorphism. Moreover, we have $\ker(\psi) = \{(a, b) \in G : \psi((a, b)) = e_2\} = \{(a, e_2) : a \in G_1\} = N$. Since $\ker(\psi) \lhd G$, we have $N \lhd G$.
(b) We construct an isomorphism $\varphi : N \to G_1$ by defining $\varphi((a, e_2)) = a$. This map is well-defined, and for all (a, e_2) and (b, e_2) in N, one has $\varphi((a, e_2)(b, e_2)) = \varphi(ab, e_2) = ab = \varphi((a, e_2))\varphi((b, e_2))$, so that φ is a homomorphism. If $\varphi((a, e_2)) = \varphi((b, e_2))$, then $a = b$, whence $(a, e_2) = (b, e_2)$, and so φ is injective. Moreover, whenever $a \in G_1$, one has $\varphi((a, e_2)) = a$, and $(a, e_2) \in N$, so that φ is surjective. Then φ is an injective and surjective homomorphism from N to G_1, and hence an isomorphism, whence $N \cong G_1$.
(c) The map ψ from part (a) is plainly surjective, and so it follows from the First Homomorphism Theorem that $G/N = G/\ker(\psi) \cong G_2$.

2.7, Q6. Define $\varphi : G \to G/N$ to be the canonical homomorphism, and suppose $a \in G$ has finite order $n = o(a)$. Then since $(Na)^n = \varphi(a)^n = \varphi(a^n) = \varphi(e) = N$, it follows that the order of Na in G/N has order m dividing n, which is to say that $m|o(a)$.

2.7, Q7. Suppose that $\varphi : G \to G'$ is a surjective homomorphism. If $N \lhd G$, then we know that $\varphi(N) \le G'$ (Lemma 2.5.3). Moreover, since φ is surjective, whenever $g' \in G'$ there exists $g \in G$ with $\varphi(g) = g'$, and hence $(g')^{-1}\varphi(N)g' = \varphi(g)^{-1}\varphi(N)\varphi(g) = \varphi(g^{-1}Ng)$. But $g^{-1}Ng \subseteq N$ by the normality of N in G, and hence, for all $g' \in G'$ one has $(g')^{-1}\varphi(N)g' \subseteq \varphi(N)$. Thus $\varphi(N) \lhd G'$, as required.

3.2, Q3. (a) Since $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 4 & 2 & 7 & 6 & 9 & 8 & 5 \end{pmatrix} = (1,3,4,2)\,(5,7,9)$, the permutation in question is a product of a disjoint 4-cycle and 3-cycle, and hence has order $\mathrm{lcm}(3,4) = 12$.
(b) Since $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix} = (1,7)\,(2,6)\,(3,5)$, the permutation in question is a product of 3 disjoint 2-cycles, and hence has order $\mathrm{lcm}(2,2,2) = 2$.
(c) Since $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 5 & 3 & 4 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 5 & 6 & 7 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 5 & 7 & 4 & 2 & 1 & 3 \end{pmatrix} = (1,6)\,(2,5)\,(3,7)$, the permutation in question is a product of 3 disjoint 2-cycles, and hence has order $\mathrm{lcm}(2,2,2) = 2$.

3.2, Q9. We obtain σ by applying a transposition that switches 2 and 3, thereby obtaining $(1,3)$ from $(1,2)$. Thus $(2,3)\,(1,2)\,(2,3)^{-1} = (2,3)\,(1,2)\,(2,3) = (1,3)$, and we take $\sigma = (2,3)$.

3.2, Q11. We need to switch 1 with 4, 2 with 5, and 3 with 6, so try $\sigma = (1,4)\,(2,5)\,(3,6)$. We have $\sigma(1,2,3)\sigma^{-1} = (1,4)\,(2,5)\,(3,6)\,(1,2,3)\,(1,4)\,(2,5)\,(3,6) = (4,5,6)$.

3.2, Q14. Let τ be a transposition, say $\tau = (a,b)$ with $a \neq b$. If σ is another permutation and n is an element with $\sigma^{-1}(n)$ different from a and b, then $\sigma\tau\sigma^{-1}(n) = \sigma\sigma^{-1}(n) = n$. On the other hand, if $\sigma^{-1}(n) = a$, we have $\tau\sigma^{-1}(n) = \tau(a) = b$, whence $\sigma\tau\sigma^{-1}(n) = \sigma(b)$, and similarly when $\sigma^{-1}(n) = b$ we obtain $\sigma\tau\sigma^{-1}(n) = \sigma(a)$. Thus $\sigma\tau\sigma^{-1} = (\sigma(a), \sigma(b))$, which is again a transposition.

3.2, Q17. We begin by showing that all transpositions $(1,a)$ with $1 \le a \le n$ are contained in any subgroup H containing $(1,2)$ and $\sigma = (1,2,\ldots,n)$. For by Q14, whenever $(1,a) \in H$ with $2 \le a < n$, the closure of H implies that we have $\sigma^{-1}(1,a)\sigma = (\sigma(1), \sigma(a)) = (2, a+1) \in H$, and hence $(2,a+1)^{-1}(1,2)(2,a+1) = (1,a+1) \in H$. Thus $(1,a) \in H$ for all $2 \le a \le n$, whence $(1,b)^{-1}(1,a)(1,b) = (a,b) \in H$ for all $a \neq b$. Then H contains all transpositions. Since every element of S_n is a product of transpositions, and H contains all transpositions, we conclude by the closure of H that $H = S_n$, as required.

3.2, Q20. Suppose that τ_1 and τ_2 are distinct transpositions. By relabelling elements, we may suppose that $\tau_1 = (1,2)$ and τ_2 is either $(1,3)$ or $(3,4)$. In the former case $\tau_1\tau_2 = (1,2)(1,3) = (1,3,2)$ has order 3, and in the latter case $\tau_1\tau_2 = (1,2)(3,4)$ has order 2.

3.2, Q23. If $\nu = (a_1, a_2, \ldots, a_k)$ is a k-cycle and $\rho \in S_n$, then in a similar manner as in the discussion of Q14, one has $\rho\nu\rho^{-1} = (\rho(a_1), \rho(a_2), \ldots, \rho(a_k))$. Let the m_j-cycles in σ and τ be respectively $(a_1, \ldots, a_m)$ and $(b_1, \ldots, b_m)$, where $m = m_j$. Then any permutation with $\rho(a_h) = b_h$ for $1 \le h \le m$ has the property that $\rho(a_1, \ldots, a_m)\rho^{-1} = (b_1, \ldots, b_m)$. This determines the action of the permutation ρ on the elements in the m_j-cycle. But the elements in each cycle comprising σ are disjoint, and so ρ is completely determined by its action on all of these cycles (including the trivial 1-cycles). Notice that since the cycles comprising τ are likewise disjoint, the action of ρ determined in this way does indeed define a permutation, since the action is injective. Let the cycles of length $m_1, \ldots m_k$ in σ and τ be respectively $\sigma_1, \ldots, \sigma_k$ and $\tau_1, \ldots, \tau_k$. Then we have $\rho\sigma_j\rho^{-1} = \tau_j$ for $1 \le j \le k$, and hence

$$\rho\sigma\rho^{-1} = \rho\sigma_1\sigma_2\ldots\sigma_k\rho^{-1} = (\rho\sigma_1\rho^{-1})(\rho\sigma_2\rho^{-1})\ldots(\rho\sigma_k\rho^{-1}) = \tau_1\tau_2\ldots\tau_k = \tau.$$