HONORS ALGEBRA: SOLUTIONS TO HOMEWORK 3

2.4, Q8. If every right coset of H in G is a left coset of H in G, then for each $a \in G$ there is an $b \in G$ such that $Ha = bH$. Since $e \in H$, one therefore sees that for some $h \in H$ one has $b = ha$. Thus $H = b^{-1}Ha = (ha)^{-1}Ha = a^{-1}h^{-1}Ha = a^{-1}Ha$, whence $aHa^{-1} = H$. Since this relation holds for all $a \in G$, we have established the required relation.

2.4, Q13. The elements of U_{18} are integers a with $1 \le a < 18$ for which a is coprime to both 2 and 3. Thus $U_{18} = \{1, 5, 7, 11, 13, 17\}$. Of course, the element 1 has order 1. One can check that

$$\langle 5 \rangle = \langle 11 \rangle = \{1, 5, 7, 11, 13, 17\}, \quad \langle 7 \rangle = \langle 13 \rangle = \{1, 7, 13\}, \quad \langle 17 \rangle = \{1, 17\},$$

and so

$$o(1) = 1, \quad o(17) = 2, \quad o(7) = o(13) = 3, \quad o(5) = o(11) = 6.$$

In particular, we see that U_{18} is cyclic, because $U_{18} = \langle 5 \rangle$.

2.4, Q16. If $G = \{a_1, \ldots, a_n\}$ is an abelian group, we can pair each element a with its inverse a^{-1}. Since $(a^{-1})^{-1} = a$, then we can partition G into subsets $\{a, a^{-1}\}$. Possibly, one or more of these disjoint sets might have the property that $a = a^{-1}$. By relabeling the elements of G, we may suppose that $a_{2i-1} = a_{2i}^{-1}$ for $1 \le i \le r$, and that $a_j = a_j^{-1}$ for $2r + 1 \le j \le n$. Thus, if we write $x = a_1 \cdots a_n$, then we have

$$x^2 = \left(\prod_{i=1}^{r} a_{2i-1} a_{2i} \right)^2 \prod_{j=2r+1}^{n} a_j^2.$$

But $a_{2i-1}a_{2i} = e$ for $1 \le i \le r$, and $a_j^2 = e$ for $2r + 1 \le j \le n$, so all terms in both products are equal to e. Hence $x^2 = e$, as required.

2.4, Q18. We apply the method of problem 16 in the case $G = U_p$. The problem itself shows that $((p-1)!)^2 \equiv 1 \pmod{p}$. However, if $x^2 \equiv 1 \pmod{p}$, we have $(x-1)(x+1) \equiv 0 \pmod{p}$, and thus $x - 1 \equiv 0 \pmod{p}$ or $x + 1 \equiv 0 \pmod{p}$. Thus $x \equiv \pm 1 \pmod{p}$. Hence $(p-1)! \equiv \pm 1 \pmod{p}$. To distinguish the choice of sign, observe that 1 and $p - 1$ are the only self-inverse elements of U_p. Thus, when p is odd, the elements $2, 3, \ldots, p-2$ can be partitioned into pairs a, b, where $ab \equiv 1 \pmod{p}$ and $a \ne b$. Thus $(p-1)! = (p-1) \cdot ((p-2) \cdot (p-3) \cdots 2) \equiv p - 1 \equiv -1 \pmod{p}$.

2.4, Q27. We may assume that whenever $aH = bH$, one has $Ha = Hb$, in G. Given $a \in G$ and $h \in H$, observe that $aH = ahH$, whence the hypothesis shows that $Ha = Hah$. From the latter, there exists $h' \in H$ so that $ah = h'a$ and hence $aha^{-1} = h' \in H$. Since this relation holds for all $h \in H$, it follows that $aHa^{-1} \subseteq H$. Again, this holds for all $a \in G$, so replacing a by a^{-1} we obtain $a^{-1}Ha \subseteq H$, and thus $H \subseteq aHa^{-1}$. We therefore conclude that $aHa^{-1} = H$ for all $a \in G$, as required.

2.4, Q31. Use the division algorithm to write $s = qm + r$, where $q \in \mathbb{Z}$ and $0 \le r < m$. Then we have $e = a^s = a^{qm+r} = (a^m)^q a^r$. But $o(a) = m$, so $a^m = e$, whence $e = a^r$. But $0 \le r < m$, so the hypothesis that $o(a) = m$ implies that $r = 0$, and hence $s = qm$. Thus $m | s$.

2.4, Q37. Suppose that G is a finite cyclic group of order n, so that $G = \langle a \rangle$ for some element $a \in G$ having order n. The elements of G are the elements $e, a, a^2, \ldots, a^{n-1}$. Suppose that a^r has order m. Since $e = (a^r)^m = a^{rm}$, we must have $n | rm$, so that r is a multiple of n/m, say $r = ln/m$ for some integer l with $0 \leq l < m$. But $a^{ln/m}$ has order m if and only if the smallest positive integer k for which $(a^{ln/m})^k = e$ is m. However, this holds if and only if the smallest positive integer k for which lk/m is an integer is m. Thus a^r has order m if and only if $(l, m) = 1$. Thus the number of elements of G having order m is given by the number of integers l with $0 \leq l < m$ and $(l, m) = 1$, namely $\varphi(m)$.

2.5, Q2. (a) The identity mapping $\mathrm{id} : G_1 \to G_1$ with $g \mapsto g$ gives a trivial isomorphism from G_1 to G_1, whence $G_1 \cong G_1$.

(b) If $G_1 \cong G_2$, then there is a bijective homomorphism $\varphi : G_1 \to G_2$. Since φ is bijective, it has an inverse mapping $\varphi^{-1} : G_2 \to G_1$ which is also bijective. Moreover, since φ is surjective, whenever $g_2, h_2 \in G_2$, there exist $g_1, h_1 \in G_1$ with $\varphi(g_1) = g_2$ and $\varphi(h_1) = h_2$. Hence, using the homomorphism property of φ, we obtain

$$\begin{aligned}\varphi^{-1}(g_2)\varphi^{-1}(h_2) &= (\varphi^{-1} \circ \varphi(g_1))(\varphi^{-1} \circ \varphi(h_1)) = g_1 h_1 \\ &= \varphi^{-1} \circ \varphi(g_1 h_1) = \varphi^{-1}(\varphi(g_1)\varphi(h_1)) = \varphi^{-1}(g_2 h_2).\end{aligned}$$

Since this relation holds for all $g_2, h_2 \in G_2$, we see that φ^{-1} is a homomorphism as well as being bijective, and hence $\varphi^{-1} : G_2 \to G_1$ is an isomorphism. Thus $G_2 \cong G_1$.

(c) If $G_1 \cong G_2$ and $G_2 \cong G_3$, then there exist bijective homomorphisms $\varphi : G_1 \to G_2$ and $\psi : G_2 \to G_3$. Consider the map $\psi \circ \varphi : G_1 \to G_3$. Since φ and ψ are each bijective, we have that $\psi \circ \varphi$ is also bijective. Moreover, for each $g, h \in G_1$, if we use the homomorphism properties of φ and ψ, we obtain

$$\psi \circ \varphi(gh) = \psi(\varphi(g)\varphi(h)) = \psi(\varphi(g))\psi(\varphi(h)) = (\psi \circ \varphi(g))(\psi \circ \varphi(h)).$$

Since this relation holds for all $g, h \in G_1$, we see that $\psi \circ \varphi$ is a homomorphism as well as being bijective, and hence $\psi \circ \varphi : G_1 \to G_3$ is an isomorphism. Thus $G_1 \cong G_3$.

2.5, Q6. We show that when $\varphi : G \to G'$ is a homomorphism of groups, then $\varphi(G) \leq G'$. To confirm this, observe first that $\varphi(e) = e'$, where e and e' are the respective identities of G and G'. For we have $\varphi(x) = \varphi(xe) = \varphi(x)\varphi(e)$, whence $\varphi(e) = e'$ by cancellation. Hence, also, for every $a \in G$ one has $e' = \varphi(e) = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1})$, whence $\varphi(a^{-1}) = \varphi(a)^{-1}$. Finally, whenever $a, b \in G$, we have

$$\varphi(a)\varphi(b)^{-1} = \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1}) \in \varphi(G).$$

Thus, for all $g, h \in \varphi(G)$, we have $gh^{-1} \in \varphi(G)$, so $\varphi(G) \leq G'$ by the subgroup criterion.

2.5, Q7. We show that $\varphi : G \to G'$ is a monomorphism of groups if and only if $\ker(\varphi) = \{e\}$. First, plainly, if $\ker(\varphi) \neq \{e\}$, then there exists $g \in \ker(\varphi) \setminus \{e\}$, and so φ cannot be a monomorphism. To see this note that $\varphi(g) = e' = \varphi(e)$ whilst $g \neq e$. So $\ker(\varphi)$ must be trivial if φ is to be a monomorphism. On the other hand, if $\ker(\varphi)$ is trivial, then whenever $\varphi(g_1) = \varphi(g_2)$, one has $g_1 = g_2$. If this were not the case, and for some $g_1 \neq g_2$ one has $\varphi(g_1) = \varphi(g_2)$, then $\varphi(g_1 g_2^{-1}) = \varphi(g_1)\varphi(g_2)^{-1} = \varphi(g_1)\varphi(g_1)^{-1} = e'$, so $g_1 g_2^{-1} = e$ whilst $g_1 \neq g_2$, yielding a contradiction. When $\ker(\varphi)$ is trivial, therefore, we see that φ is injective, and hence a monomorphism.