HONORS ALGEBRA: SOLUTIONS TO HOMEWORK 2

2.1, Q8. When $n = 1$ the claimed conclusion is immediate. We prove the general result by induction, supposing that $n > 1$ and that it has already been established that when $1 \le m < n$, one has $(a * b)^m = a^m * b^m$. Let $n > 1$. Then $(a * b)^n = (a * b) * (a * b)^{n-1}$. By the inductive hypothesis, one has $(a * b)^{n-1} = a^{n-1} * b^{n-1}$, and hence

$$\begin{aligned}(a * b)^n &= (a * b) * (a^{n-1} * b^{n-1}) = a * (b * a^{n-1}) * b^{n-1} \\ &= a * (a^{n-1} * b) * b^{n-1} = (a * a^{n-1}) * (b * b^{n-1}) = a^n * b^n.\end{aligned}$$

This confirms the inductive hypothesis for $m = n$, and so the desired conclusion follows for positive integers n by induction. When $n = 0$ one has $(a * b)^0 = e = a^0 * b^0$. Also, when n is negative, say $n = -N$ with $N > 0$, one may use the first part already proved to show that one has $(a * b)^n = ((a * b)^{-1})^N = (b^{-1} * a^{-1})^N = (b^{-1})^N * (a^{-1})^N = b^{-N} * a^{-N} = a^{-N} * b^{-N} = a^n * b^n$.

2.1, Q9. If $a^2 = e$ for all $a \in G$, then $a^{-1} = a$ for all $a \in G$. Thus, since $(ab)^2 = e$ for all $a, b \in G$, we see that $abab = e$, whence $a^{-1}(abab)b^{-1} = ab$, and thus $ba = ab$. Hence G is abelian.

2.1, Q18. When $a \in G$, one has $a * a^{-1} = e = a^{-1} * a$, by the definition of an inverse. Hence $a^{-1} * a = e = a * a^{-1}$, so that a acts as an inverse of a^{-1}, so $(a^{-1})^{-1} = a$. We can therefore pair elements $a \in G$ with their corresponding inverse elements $a^{-1} \in G$. Since $(a^{-1})^{-1} = a$, these pairs are disjoint from one another. So one can partition the elements of a finite group into subsets $\{a, b\}$ where $b = a^{-1}$. It is possible that $a^{-1} = a$, in which case $b = a$. Let r denote the number of these sets $\{a, b\}$ where $b = a$, and let s denote the corresponding number with $b \ne a$. Then $|G| = r + 2s$. Notice that $r \ge 1$, in view of the special subset with $a = b = e$. If $|G|$ is even, we must have r even, and hence $r \ge 2$. Thus, there is at least one subset $\{a, b\}$ in this partition with $a = b$ aside from the trivial case with $a = b = e$. Hence there is indeed an element $a \in G$ with $a = a^{-1}$.

2.1, Q26. Since G is finite, the powers a^m cannot all be distinct for $m \in \mathbb{Z}_{\ge 0}$, and so there must be integers n and k with $0 \le k < n + k$ satisfying $a^k = a^{n+k}$. Thus, by the cancellation property, one has $a^n = e$. Notice that this integer n may depend on a.

2.1, Q27. By problem 26, for each $a \in G$ there exists an integer $n = n(a)$ satisfying the property that $a^n = e$. Take m to be the least common multiple of all the integers $n(a)$, for $a \in G$. This integer exists because G is finite, and moreover $n(a)|m$ for each $a \in G$. Putting $l(a) = m/n(a)$, we see that for each $a \in G$, one has

$$a^m = a^{l(a)n(a)} = (a^{n(a)})^{l(a)} = e^{l(a)} = e,$$

and thus $a^m = e$ uniformly for every $a \in G$.

2.1, Q28. Suppose that $x \in G$. Then there exists $y \in G$ so that $y * x = e$, and there exists $z \in G$ so that $z * y = e$. Thus $z * ((y * x) * y) = z * (e * y) = z * y = e$, and yet $(z * y) * (x * y) = e * (x * y) = x * y$. Hence, by associativity, we have $x * y = e$. This shows that left inverses are always right inverses. Consequently, we find that $x * e = x * (y * x) = (x * y) * x = e * x = x$. Hence $x * e = x$ for all $x \in G$, which shows that left identities are always right identities. This completes the proof that G is a group.

2.2, Q1. We must show that G contains an identity, and also that each element of G has an inverse. But for each $a \in G$, property (1) shows that there is an $x \in G$ such that $ax = a$, and property (2) shows that there is a $u \in G$ such that $ua = a$. Of course, these elements x and u might depend on a. But if b is any element of G, then there exists $z \in G$ so that $az = b$, and then $ub = uaz = az = b$, and there exists $w \in G$ so that $wa = b$, and then $bx = wax = wa = b$. Thus we see that u and x are left and right inverses for all elements of G. In particular, one has $u = ux = x$, so that there is an element $e = u = x$ which acts as an identity for all elements of G. Observe next that properties (1) and (2) show that for each $a \in G$, there exist $g, h \in G$ for which $ag = e$ and $ha = e$. But then $h = he = hag = eg = g$. Thus all elements $a \in G$ possess an inverse element ($a^{-1} = g = h$) that acts as an inverse on both left and right.

2.2, Q3. Suppose that $(ab)^i = a^i b^i$ for $i = n$, $n+1$ and $n+2$. Then one has $(ab)^n = a^n b^n$ and $(ab)^{n+1} = a^{n+1}b^{n+1}$, whence $a^{n+1}b^{n+1} = ab(ab)^n = aba^n b^n$. By the cancellation property (multiply by a^{-1} on the left and b^{-n} on the right), this shows that $a^n b = ba^n$. Similarly, one has $a^{n+1}b = ba^{n+1}$. But then $ba^{n+1} = a(a^n b) = aba^n$, so that the cancellation property (multiply by a^{-n} on the right) yields $ba = ab$. Since this relation is presumed to hold for all a and b, we find that G is abelian.

2.2, Q5. Consider arbitrary elements a and b of G, and apply the cancellation property. We have $a(ba)^2 b = a^3 b^3$, whence $(ba)^2 = a^2 b^2$. Likewise, we have $a(ba)^4 b = a^5 b^5$, so that $(ba)^4 = a^4 b^4$. Hence $a^4 b^4 = (a^2 b^2)(a^2 b^2)$, and this shows that $a^2 b^2 = b^2 a^2$. Since these relations hold for all $a, b \in G$, we can reverse the roles of a and b to obtain $b^2 a^2 = (ab)^2$, whence $a^2 b^2 = b^2 a^2 = abab$, which in turn shows that $ab = ba$. Since this relation holds for all $a, b \in G$, we have shown that G is abelian.

2.3, Q3. We can write the elements of S_3 in cycle notation, so that

$$S_3 = \{e,\ (1,2),\ (1,3),\ (2,3),\ (1,2,3),\ (1,3,2)\}.$$

By Lagrange's theorem, any subgroup of S_3 must have order dividing $|S_3| = 6$, so the possible orders for subgroups are 1, 2, 3, 6. The only subgroup of order 1 is $\{e\}$, and the only subgroup of order 6 is S_3 itself. Any subgroup of order 2 must be cyclic, because 2 is prime, and thus we have 3 subgroups of order 2, namely

$$H_1 = \langle (1,2) \rangle, \quad H_2 = \langle (1,3) \rangle, \quad H_3 = \langle (2,3) \rangle.$$

Any subgroup containing more than one distinct transposition has order larger than 2, while the 3-cycles generate a subgroup of order 3, namely

$$H_4 = \langle (1,2,3) \rangle = \langle (1,3,2) \rangle = \{e,\ (1,2,3),\ (1,3,2)\}.$$

The only subgroups of order 3 are again cyclic, since 3 is prime, and so cannot contain any transposition (an element of order 2). Thus H_4 is the only subgroup of order 3. We have therefore shown that the only subgroups of S_3 are the trivial subgroups $\{e\}$ and S_3, three subgroups H_1, H_2 and H_3 of order 2, and one subgroup H_4 of order 3. [Of course, one can achieve the same answer without using Lagrange's theorem, by observing that whenever a subgroup contains any two distinct transpositions, then it contains the whole of S_3, and likewise if it contains a transposition and a 3-cycle.]

2.3, Q12. Consider the cyclic group $G = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}$. If one considers any two elements of G, say a^n and a^m for some integers $m, n \in \mathbb{Z}$, then one finds that $a^n a^m = a^{n+m} = a^{m+n} = a^m a^n$. Thus any two elements of G commute, and we see that all cyclic groups are abelian. (Notice that the abelian property of $(\mathbb{Z}, +)$ is inherited by $\langle a \rangle$ by virtue of the fact that its elements are defined by the exponent of a).

2.3, Q14. Suppose that G has no proper subgroups, and (by way of deriving a contradiction) assume that G is not cyclic. Since G is not cyclic, it cannot be the trivial group, and so contains an element $a \neq e$. Since G is not cyclic, it is not equal to the cyclic group $\langle a \rangle$, and thus there is an element b of G with $b \notin \langle a \rangle$. But then $\langle a \rangle$ is a subgroup of G which is not equal to either $\{e\}$ or G, and hence is a proper subgroup. So we derive a contradiction, and are forced to conclude that whenever G has no proper subgroups, it is cyclic.

2.3, Q24. We apply the subgroup criterion. If $a, b \in N$, then $a, b \in x^{-1}Hx$ for all $x \in G$, whence xax^{-1} and xbx^{-1} both lie in H for all $x \in G$. But then $(xax^{-1})(xbx^{-1})^{-1} = (xax^{-1})(xb^{-1}x^{-1}) = xab^{-1}x^{-1} \in H$ for all $x \in G$, whence $ab^{-1} \in x^{-1}Hx$ for all $x \in G$. Thus $ab^{-1} \in N$, and by the subgroup criterion, it follows that N is a subgroup of G.

Similarly, if $n \in N$, then $xnx^{-1} \in H$ for all $x \in G$, whence for any given $y \in G$ we have $x(y^{-1}ny)x^{-1} = (xy^{-1})n(xy^{-1})^{-1} \in H$ for all $x \in G$. Thus $y^{-1}ny \in N$ for all $y \in G$, whence $y^{-1}Ny \subseteq N$ for all $y \in G$. A similar argument shows that $yNy^{-1} \subseteq N$ for all $y \in G$, whence $N \subseteq y^{-1}Ny$ for all $y \in G$. Thus indeed $N = y^{-1}Ny$ for each $y \in G$.

2.3, Q26. If $Ha \cap Hb \neq \emptyset$, then there exists some element $g \in G$ with $g \in Ha$ and $g \in Hb$, say $h_1a = g = h_2b$ for some $h_1, h_2 \in H$. But then $b = h_3a$, with $h_3 = h_2^{-1}h_1 \in H$. This shows that whenever $h \in H$, one has $hb = hh_3a \in Ha$, whence $Hb \subseteq Ha$. Similarly, and by symmetry, one has $Ha \subseteq Hb$, and thus $Ha = Hb$. So for all $a, b \in G$, one has either $Ha \cap Hb = \emptyset$, or $Ha = Hb$, as required.

2.3, Q29. We have $x^{-1}Mx \subseteq M$ for all $x \in G$. Then for all $m \in M$ and all $y \in G$, one has $y^{-1}my \in M$, say $y^{-1}my = m_0$, for some $m_0 \in M$ depending on y. Given any $x \in G$, by considering the situation with $y = x^{-1}$, we see that $m = ym_0y^{-1} = x^{-1}m_0x \in x^{-1}Mx$. Then for all $x \in G$, we see that $x^{-1}Mx$ contains all elements m of M, that is $M \subseteq x^{-1}Mx$. Since we started by assuming that $x^{-1}Mx \subseteq M$ for all $x \in G$, we see that in fact $x^{-1}Mx = M$ for all $x \in G$.