HONORS ALGEBRA: SOLUTIONS TO HOMEWORK 9

2.11, Q15. Suppose that $b \in B(N)$ and $g \in G$. Given any $n \in N$, we put $a = gng^{-1}$. Then $n = g^{-1}ag$ and, since $N \lhd G$, we have $a \in N$ and hence $a^{-1}ba = b$. Moreover, we see that $n^{-1}(g^{-1}bg)n = (g^{-1}a^{-1}g)(g^{-1}bg)(g^{-1}ag) = g^{-1}(a^{-1}ba)g = g^{-1}bg$. Since this relation holds for all $n \in N$, we must conclude that $g^{-1}bg \in B(N)$. This relation holds for all $b \in B(N)$ and all $g \in G$, and thus $B(N) \lhd G$.

2.11, Q16. By the first Sylow theorem, any group G of order 36 contains a Sylow 3-subgroup H of order 9, and then $i_G(H) = |G|/|H| = 36/9 = 4$. But $4! = 24$ and $36 \nmid 24$, whence $|G|$ does not divide $i_G(H)!$. Thus, by the conclusion of Q40 of section 2.5, the group G contains a normal subgroup $N \neq \{e\}$ contained in H Since $|H| = 9$, it follows from Lagrange's theorem that N has order 3 or 9.

2.11, Q18. Suppose that $|G| = p^n m$ with p prime and $p \nmid m$, and P is a Sylow p-subgroup of G. We have $P \leq N(P) \leq N(N(P)) \leq G$, so the largest power of p dividing $|N(P)|$ is p^n, and likewise the largest power of p dividing $|N(N(P))|$ is p^n. Since $P \leq N(P)$, when $x \in N(N(P))$ we have $x^{-1}Px \leq x^{-1}N(P)x = N(P)$. But $|x^{-1}Px| = |P| = p^n$, so $x^{-1}Px$ is a Sylow p-subgroup of $N(P)$. But Sylow's second theorem shows that all Sylow p-subgroups of a given group are conjugate, and thus (since P is also a Sylow p-subgroup of $N(P)$) there exists $y \in N(P)$ with $y^{-1}Py = x^{-1}Px$. But then the definition of $N(P)$ shows that $y^{-1}Py = P$, so that $x^{-1}Px = P$. We have therefore shown that, for all $x \in N(N(P))$, we have $x \in N(P)$, whence $N(N(P)) \leq N(P)$. But $N(P) \leq N(N(P))$, and thus $N(N(P)) = N(P)$, as required.

2.11, Q20. Suppose that $|G| = p^n k$ with p prime and $p \nmid k$. Then G has a Sylow p-subgroup of order p^n. Suppose that $1 \leq l \leq n$ and G has a subgroup H of order p^l. We have noted already that this property holds when $l = n$. It follows from Theorem 2.11.6 that H has a normal subgroup N of order p^{l-1}, and hence G also has the subgroup N of order p^{l-1}. By induction, therefore, the group G possesses a subgroup of order p^m, for any integer m with $0 \leq m \leq n$. But then, whenever p^m divides $|G|$, the group G possesses a subgroup of order p^m.

2.11, Q23. (a) For all $a, b, c \in G$, we have $a = e^{-1}ae$ with $e \in H$, so $a \sim a$ (reflexivity); $b = h^{-1}ah$ for some $h \in H$ if and only if $a = g^{-1}bg$ for some g (equal to h^{-1}) in H, so $a \sim b$ if and only if $b \sim a$ (symmetry); and $b = h^{-1}ah$ and $c = g^{-1}bg$ for some $h, g \in H$ implies $c = (hg)^{-1}a(hg)$ with $hg \in H$, so $a \sim b$ and $b \sim c$ implies $a \sim c$ (transitivity). Thus, the relation $\sim$ is indeed an equivalence relation.
(b) Suppose that $b = h^{-1}ah$ and $b = g^{-1}ag$ with $g, h \in H$. Then $g^{-1}ag = h^{-1}ah$, whence $(gh^{-1})^{-1}a(gh^{-1}) = a$, so that $gh^{-1} \in C(a) \cap H$ and hence $g \in (C(a) \cap H)h$. Thus (since this line of reasoning can be reversed), we see that for each fixed h the number of choices for g with $g^{-1}ag = h^{-1}ah$ is equal to $|C(a) \cap H|$. The number of elements in the equivalence class of a is therefore $|G|/|C(a) \cap H| = i_H(H \cap C(a))$.

2.11, Q24. (a) For all $A, B, C \leq G$, we have $A = e^{-1}Ae$ with $e \in H$, so $A \sim A$ (reflexivity); $B = h^{-1}Ah$ for some $h \in H$ if and only if $A = g^{-1}Bg$ for some g (equal to h^{-1}) in H, so $A \sim B$ if and only if $B \sim A$ (symmetry); and $B = h^{-1}Ah$ and $C = g^{-1}Bg$ for some $h, g \in H$ implies $C = (hg)^{-1}A(hg)$ with $hg \in H$, so $A \sim B$ and $B \sim C$ implies

$A \sim C$ (transitivity). Thus, the relation $\sim$ is indeed an equivalence relation on the set of subgroups of G.

(b) Suppose that $B = h^{-1}Ah$ and $B = g^{-1}Ag$ with $g, h \in H$. Then $g^{-1}Ag = h^{-1}Ah$, whence $(gh^{-1})^{-1}A(gh^{-1}) = A$, so that $gh^{-1} \in N(A) \cap H$ and hence $g \in (N(A) \cap H)h$. Thus (since this line of reasoning can be reversed), we see that for each fixed h the number of choices for g with $g^{-1}Ag = h^{-1}Ah$ is equal to $|N(A) \cap H|$. The number of elements in the equivalence class of A is therefore $|G|/|N(A) \cap H| = i_H(N(A) \cap H)$.

SG, QA. (a) By Theorem 2.11.6, if $n \geq 2$ and G is a group of order p^n, then G has a normal subgroup of order $p^{n-1} > 1$, and hence cannot be simple.

(b) We apply Sylow's third theorem. We suppose that $p \neq 2$ and $|G| = 2p^n$ with $n \geq 1$. Then G has $pk + 1$ Sylow p-subgroups for some integer k with $(pk + 1)|2p^n$. If $k \geq 1$, then $(pk + 1) \nmid 2$, and thus we must have $k = 0$. Then G has precisely one Sylow p-subgroup, and so this must be fixed under conjugation and hence must be normal in G. But then G cannot be simple. The same argument applies when $|G| = 3p^n$ (the case with $p = 3$ having been proved in part (a)), since $(pk + 1) \nmid 3$ when $k \geq 1$. Likewise, when $|G| = 5p^n$, we have $(pk+1) \nmid 5$ when $k \geq 1$, and the same argument applies. Thus no group of order $2p^n$, or $3p^n$, or $5p^n$ can be simple when $n \geq 1$ and p is prime.

(c) We proceed in a similar manner to part (b). When $k \geq 1$ and $p \neq 3$, one has $(pk + 1) \nmid 4$, and thus $(pk + 1) \nmid |G|$ when $|G| = 4p^n$ and $n \geq 1$. Then Sylow's third theorem shows that G has a unique, and hence normal, Sylow p-subgroup, whence G is not simple.

SG, QB. (a) Let G be a group of order $56 = 7 \cdot 2^3$. By the third Sylow theorem, the number of Sylow 7-subgroups is of the shape $1 + 7k$ for some $k \in \mathbb{Z}$, and divides 56. Since $(7k + 1) \nmid 56$ for $k \geq 2$, we find that there are 1 or 8 Sylow 7-subgroups of G. Similarly, the number of Sylow 2- subgroups is of the shape $1 + 2k$ for some integer k, and divides 56. Since $(2k + 1) \nmid 56$ when $k \neq 0, 3$, we find G has 1 or 7 Sylow 2-subgroups.

(b) Suppose that G has two distinct Sylow 7-subgroups. Each has order 7, so is cyclic, and we may assume that these subgroups are $\langle a \rangle$ and $\langle b \rangle$, with $a \neq b$. Suppose that these subgroups have non-trivial intersection. Then for some integers r and s with $1 \leq r, s \leq 6$ we have $a^r = b^s$. But both a and b have order 7, so on choosing t with $rt \equiv 1 \pmod 7$, we find that $a = a^{rt} = b^{st}$, so that $a \in \langle b \rangle$ and hence $\langle a \rangle \leq \langle b \rangle$. But $\langle a \rangle$ and $\langle b \rangle$ have the same number of elements, so in fact these subgroups are equal, leading to a contradiction. Thus any two Sylow 7-subgroups have trivial intersection. If G has just 1 Sylow 7-subgroup, then this is fixed under conjugation and hence is normal, and this shows that G is not simple. Suppose instead that G has 8 Sylow 7-subgroups. These subgroups pairwise have trivial intersection. Each element of such a subgroup different from e has order 7, so we see that G has at least $8 \cdot (7 - 1) = 48$ elements of order 7. The number of elements of order a power of 2 is therefore at most $56 - 48 = 8$, and this is the size of a Sylow 2-subgroup. So there is precisely one Sylow 2-subgroup of order 8, which must be fixed under conjugation and is hence normal. Thus, again we find that G cannot be simple.

SG, QC. Let G be a group of order $30 = 2 \cdot 3 \cdot 5$. By applying the third Sylow theorem, we see that G has 1 or 10 Sylow 3-subgroups, and 1 or 6 Sylow 5-subgroups. If G has just 1 Sylow 3-subgroup, then this is fixed under conjugation and is hence normal, so that G is not simple. Likewise, if G has just 1 Sylow 5-subgroup, then this is fixed under conjugation, so is normal, and hence G is not simple. We may therefore assume that G has 10 Sylow 3-subgroups and 6 Sylow 5-subgroups. Any two Sylow 5-subgroups have trivial intersection, so G contains at least $6 \cdot (5 - 1) = 24$ elements of order 5. Similarly, we find that G contains at least $10\cdot(3-1)=20$ elements of order 3. Then G contains at least $24+20=44$ elements, yielding a contradiction since $|G|=30$. We must therefore conclude that G is not simple.

SG, QD. (a) Groups of order 36 are already handled in Q16 of section 2.11 above. We may proceed similarly in the remaining cases. Thus, if $|G|=12$, we use the Sylow 2-subgroup H of G of order 4 to see that $|G|\nmid i_G(H)!$, noting that $12\nmid 3!=(12/4)!$. When instead $|G|=24$, we use the Sylow 2-subgroup H of G of order 8 to see that $|G|\nmid i_G(H)!$, noting that $24\nmid 3!=(24/8)!$. Finally, when $|G|=48$, we use the Sylow 2-subgroup H of G of order 16 to see that $|G|\nmid i_G(H)!$, noting that $48\nmid 3!=(48/16)!$. In each case G contains a normal subgroup $N\neq\{e\}$ contained in H, and cannot be simple.

(b) Let G be a simple group of order n with $2\le n\le 59$. It follows from question A(a) that $n\notin\{4,8,9,16,25,27,32,49\}$, question A(b) that

$$n\notin\{6,10,14,15,18,22,26,33,34,35,38,39,45,46,50,51,54,55,57,58\},$$

and question A(c) that $n\notin\{20,28,44,52\}$. Questions B, C and D show that $n\notin\{12,24,30,36,48,56\}$. All remaining integers with $2\le n\le 59$ are the primes

$$\{2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59\},$$

except for 40 and 42. When G is a group of order 40, Sylow's third theorem shows that it has a unique Sylow 5-subgroup, which must be normal, so that G is not simple. Also, when G is a group of order 42, Sylow's third theorem shows that it has a unique Sylow 7-subgroup, which must be normal, so that G is not simple. Thus we conclude that the only simple groups of order smaller than 60 are the cyclic groups of prime order.