HONORS ALGEBRA: SOLUTIONS TO HOMEWORK 8

2.10, Q1. Suppose that for some $a \neq e$, one has $a \in A \cap \langle b \rangle$ with b of order p. Then, for some integer r with $1 \leq r < p$, one has $a = b^r$. Since $(r,p) = 1$, there is an integer s with $rs \equiv 1 \pmod{p}$, and we have $b = b^{rs} = a^s \in A$. But this contradicts our assumption that $b \notin A$, and thus $A \cap \langle b \rangle = \{e\}$.

2.10, Q3. (a) Suppose that the order of a in G is d. Then $(aN)^d = a^d N = eN = N$. If the order of aN in G/N is r, meanwhile, then since $(d,r) = ud + vr$ for some integers u and v, we have $(aN)^{(d,r)} = ((aN)^d)^u ((aN)^r)^v = N$, so that $r \leq (d,r)$. Hence $r = (d,r)$, which shows that $r|d$, which is to say that $o(aN)$ divides $o(a)$.
(b) If the order of aN is r and $r < d = o(a)$, then $a^r N = (aN)^r = N$, whence $a^r \in N$, yet $a^r \neq e$. Thus $\langle a \rangle \cap N$ contains $a^r \neq e$, contradicting the assumption that $\langle a \rangle \cap N = \{e\}$. It follows that when $\langle a \rangle \cap N = \{e\}$, then $o(aN) = o(a)$.

2.10, QA. Observe that $240 = 2^4 \cdot 3 \cdot 5$. Then, by the classification theorem for finite abelian groups, representatives of the isomorphism classes of abelian groups of order 240 are given by

$$\begin{gathered}
\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{30} \\
\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{60} \\
\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_4 \times \mathbb{Z}_{60} \\
\mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_2 \times \mathbb{Z}_{120} \\
\mathbb{Z}_{16} \times \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{240}.
\end{gathered}$$

2.10, QB. Observe that $540 = 2^2 \cdot 3^3 \cdot 5$. Then, by the classification theorem for finite abelian groups, representatives of the isomorphism classes of abelian groups of order 540 are given by

$$\begin{gathered}
\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_3 \times \mathbb{Z}_6 \times \mathbb{Z}_{30} \\
\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \cong \mathbb{Z}_6 \times \mathbb{Z}_{90} \\
\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{27} \times \mathbb{Z}_5 \cong \mathbb{Z}_2 \times \mathbb{Z}_{270} \\
\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{60} \\
\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \cong \mathbb{Z}_3 \times \mathbb{Z}_{180} \\
\mathbb{Z}_4 \times \mathbb{Z}_{27} \times \mathbb{Z}_5 \cong \mathbb{Z}_{540}.
\end{gathered}$$

2.11, Q1. Using cycle notation, we can write $S_3 = \{e, (1,2), (2,3), (1,3), (1,2,3), (1,3,2)\}$. One can then check that $(2,3)^{-1}(1,2)(2,3) = (1,3)$ and $(1,3)^{-1}(1,2)(1,3) = (2,3)$, and so on, so that

$$\mathrm{cl}(e) = \{e\}, \quad \mathrm{cl}((1,2)) = \{(1,2), (1,3), (2,3)\}, \quad \mathrm{cl}((1,2,3)) = \{(1,2,3), (1,3,2)\}.$$

Also,

$$\begin{gathered}
C((1,2)) = \{e, (1,2)\}, \quad C((1,3)) = \{e, (1,3)\}, \quad C((2,3)) = \{e, (2,3)\}, \\
C(e) = S_3, \quad C((1,2,3)) = C((1,3,2)) = \{e, (1,2,3), (1,3,2)\}.
\end{gathered}$$

Thus, the indices of the distinct conjugacy classes are

$$i_{S_3}(e) = |S_3| = 6, \quad i_{S_3}(C((1,2))) = 6/2, \quad i_{S_3}(C((1,2,3))) = 6/3.$$

Hence, the class equation yields

$$|S_3| = 6 = \frac{6}{6} + \frac{6}{2} + \frac{6}{3} = \sum_a \frac{|S_3|}{|C(a)|}.$$

2.11, Q3. One has

$$\begin{aligned} C(x^{-1}ax) &= \{y \in G : y^{-1}(x^{-1}ax)y = x^{-1}ax\} = \{y \in G : (xyx^{-1})^{-1}a(xyx^{-1}) = a\} \\ &= \{x^{-1}zx \in G : z \in C(a)\} = x^{-1}C(a)x. \end{aligned}$$

2.11, Q4. If φ is an automorphism of G, then $C(\varphi(a)) = \{x \in G : x^{-1}\varphi(a)x = \varphi(a)\}$. But since φ is an automorphism, for each $x \in G$ there exists $y \in G$ with $\varphi(y) = x$, whence (using the homomorphism property of φ), we obtain $\varphi(a) = x^{-1}\varphi(a)x = \varphi(y)^{-1}\varphi(a)\varphi(y) = \varphi(y^{-1}ay)$. Since φ is an automorphism, it possesses an inverse, and hence $a = y^{-1}ay$. So $C(\varphi(a)) = \{x \in G : y \in C(a)\} = \{x \in G : \varphi^{-1}(x) \in C(a)\} = \{x \in G : x \in \varphi(C(a))\}$, whence $C(\varphi(a)) = \varphi(C(a))$.

2.11, Q5. Suppose that $|G| = p^3$ and $Z(G) \geq p^2$. By Lagrange's theorem, since $Z(G) \lhd G$, one has that $|Z(G)|$ divides $|G|$, so that $|Z(G)|$ is either p^2 or p^3. In the latter case $Z(G) = G$ and so G is abelian. In the former case we have $|G/Z(G)| = p$, so that the quotient group $G/Z(G)$ is cyclic. But then homework 2.6.11 shows that G is abelian.

2.11, Q9. Plainly $e \in N(H)$, so $N(H)$ is non-empty. Next, whenever $g, h \in N(H)$, one has $g^{-1}Hg = H$ and $h^{-1}Hh = H$, whence also $hHh^{-1} = H$. Thus $(gh^{-1})^{-1}H(gh^{-1}) = h(g^{-1}Hg)h^{-1} = hHh^{-1} = H$, so that $gh^{-1} \in N(H)$. Then by the subgroup criterion, we see that $N(H) \leq G$. Also, trivially, whenever $h \in H$ one has $h^{-1}Hh \subseteq H$, so that $h \in N(H)$. This shows that $H \subseteq N(H)$. Moreover, whenever $x \in N(H)$, one has $x^{-1}Hx = H$, so that $H \lhd N(H)$.

2.11, Q13. Suppose that G is a finite group and $H \leq G$. Let us define a relation on G by defining $x \sim y$ when $x^{-1}Hx = y^{-1}Hy$. This relation is easily seen to be reflexive, symmetric and transitive, and hence defines an equivalence relation on G. We find that $x \sim y$ if and only if $H = (xy^{-1})^{-1}Hxy^{-1}$, so that $xy^{-1} \in N(H)$. In this way we find that $x \sim y$ if and only if $x \in N(H)y$. Then the distinct subgroups $x^{-1}Hx$ are in bijective correspondence with the right cosets of $G/N(H)$. But then the number of distinct subgroups $x^{-1}Hx$ is equal to $|G/N(H)| = |G|/|N(H)| = i_G(N(H))$.