Partial HW7 Solutions

2.86 Recall that the group of quaternions $\mathbf{Q}$ (defined in Example 2.98) consists of the 8 matrices in $\mathrm{GL}(2, \mathbb{C})$,

$$\mathbf{Q} = \{I, A, A^2, A^3, B, BA, BA^2, BA^3\},$$

where $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$.

(i) Prove that $\mathbf{Q}$ is a nonabelian group with operation matrix multiplication.

Solution. We merely organize the needed calculations. First, show that $\mathbf{Q}$ is closed under multiplication in the same way as D_{2n} was shown to be closed in the previous exercise. Define $X = \{A^i : 0 \le i < 4\}$ and $Y = \{BA^i : 0 \le i < 4\}$, and show that $XX \subseteq \mathbf{Q}$, $XY \subseteq \mathbf{Q}$, etc. Second, the inverse of each matrix $M \in \mathbf{Q}$ also lies in $\mathbf{Q}$.

(ii) Prove that $-I$ is the only element in $\mathbf{Q}$ of order 2, and that all other elements $M \neq I$ satisfy $M^2 = -I$.

Solution. Straightforward multiplication.

(iii) Show that $\mathbf{Q}$ has a unique subgroup of order 2, and it is the center of $\mathbf{Q}$.

Solution. A group of order 2 must be a cyclic group generated by an element of order 2. It is shown, in part (i), that $-I$ is the only element of order 2. It is clear that $\langle -I \rangle \le Z(\mathbf{Q})$, for scalar matrices commute with every matrix. On the other hand, for every element $M \neq \pm I$, there is $N \in \mathbf{Q}$ with $MN \neq NM$.

(iv) Prove that $\langle -I \rangle$ is the center $Z(\mathbf{Q})$.

Solution. For each $M \in \mathbf{Q}$ but not in $\langle -I \rangle$, there is a matrix $M' \in \mathbf{Q}$ with $MM' \neq M'M$.

2.99 Let G be a finite group, let p be a prime, and let H be a normal subgroup of G. Prove that if both $|H|$ and $|G/H|$ are powers of p, then $|G|$ is a power of p.

Solution. If $|H| = p^h$ and $|G/H| = p^m$, then $|G| = |G/H||H| = p^{h+m}$.

2.104 (i) Prove that $\mathbf{Q}/Z(\mathbf{Q}) \cong \mathbf{V}$, where $\mathbf{Q}$ is the group of quaternions and $\mathbf{V}$ is the four-group. Conclude that the quotient of a nonabelian group by its center can be abelian.

Solution. In Exercise 2.86, we saw that $Z(\mathbf{Q}) = \{\pm E\}$, so that $\mathbf{Q}/Z(\mathbf{Q})$ has order 4. It is also shown in that exercise that if $M \neq \pm I$, then $M^2 = -I$. It follows that every nonidentity element in $\mathbf{Q}/Z(\mathbf{Q})$ has order 2, and hence, $\mathbf{Q}/Z(\mathbf{Q}) \cong \mathbf{V}$ (any bijection $\varphi\colon \mathbf{Q}/Z(\mathbf{Q}) \to \mathbf{V}$ with $\varphi(1) = 1$ must be an isomorphism).

(ii) Prove that $\mathbf{Q}$ has no subgroup isomorphic to $\mathbf{V}$. Conclude that the quotient $\mathbf{Q}/Z(\mathbf{Q})$ is not isomorphic to a subgroup of $\mathbf{Q}$.

Solution. Exercise 2.86 shows that $\mathbf{Q}$ has a unique element of order 2, whereas $\mathbf{V}$ has 3 elements of order 2.

2.106 Let H and K be subgroups of a group G.

(i) Prove that HK is a subgroup of G if and only if $HK = KH$. In particular, the condition holds if $hk = kh$ for all $h \in H$ and $k \in K$.

Solution. If HK is a subgroup, then it is closed under multiplication. But, if $h \in H$ and $k \in K$, then $h, k \in HK$ and so $kh \in HK$. Therefore, $KH \subseteq HK$. For the reverse inclusion, if $hk \in HK$, then $h^{-1}, k^{-1}, (hk)^{-1} \in HK$. But $hk = (h^{-1}k^{-1})^{-1} = (k^{-1})^{-1}(h^{-1})^{-1} \in KH$, and so $HK \subseteq KH$.

Conversely, assume that $HK = KH$. We use Proposition 2.68 to prove that HK is a subgroup: $HK \neq \varnothing$, for it contains 1, and so it suffices to show that if $x, y \in HK$, then $xy^{-1} \in HK$. Now $x = h'k'$ and $y = hk$, where $h', h \in H$ and $k', k \in K$. Hence,

$xy^{-1} = h'k'(hk)^{-1} = h'k'k^{-1}h^{-1}$. But $k'k^{-1} = k'' \in K$ and $k'k^{-1}h^{-1} = k''h^{-1} = h_1k_1$ for $h_1 \in H$ and $k_1 \in K$ because $KH = HK$. Therefore, $xy^{-1} = (h'h_1)k_1 \in HK$, as desired.

2.109 Generalize Theorem 2.128 as follows. Let G be a finite (additive) abelian group of order mn, where $(m, n) = 1$. Define

$$G_m = \{g \in G : \text{order}(g) \mid m\} \quad \text{and} \quad G_n = \{h \in G : \text{order}(h) \mid n\}.$$

(i) Prove that G_m and G_n are subgroups with $G_m \cap G_{n'} = \{0\}$.

Solution. If $x \in G_m \cap G_n$, then the order of x is a common divisor of m and n. As the gcd$(m, n) = 1$, the element x has order 1 and so $x = 1$.

(ii) Prove that $G = G_m + G_n = \{g + h : g \in G_m \text{ and } h \in G_n\}$.

Solution. Since G is abelian, every subgroup is normal, and so the second isomorphism theorem applies. As $G_m \cap G_n) = \{0\}$, we have $G_m \cong (G_m + G_n)/G_n$, so that $|G_m + G_n| = |G_M||G_N| = mn = |G|$. Therefore, $G_m + G_n = G$.

(iii) Prove that $G \cong G_m \times G_n$.

Solution. The result now follows from Proposition 2.127.

Notes on (ii) It is not obvious that $|G_i| = i$

Another way to prove $G_m + G_n \supseteq G$ is to write $1 = sm + tn$ and then $g \in G$ satisfies:

$g = (g^{sm})(g^{tn})$ and $g^{sm} \in G_n$, $g^{tn} \in G_m$

so $g \in G_m + G_n$.