Solutions to Math 3E03 Homework 5

2.96. We shall show the first isomorphism $U(\mathbb{I}_9) \cong \mathbb{I}_6$. Note that the group $U(\mathbb{I}_9) = \{[1],[2],[4],[5],[7],[8]\}$ has order 6. Also one sees that $[2]^2 = [4]$, $[2]^3 = [8]$ and $[2]^6 = [1]$. Thus $[2]$ has order 6 and since $U(\mathbb{I}_9)$ also has order 6, it follows that $[2]$ is a generator of $U(\mathbb{I}_9)$. Hence $U(\mathbb{I}_9)$ is a cyclic group of order 6 and so is isomorphic to $\mathbb{I}_6$.

To show that $U(\mathbb{I}_{15}) \cong \mathbb{I}_4 \times \mathbb{I}_2$, we give two approaches.

Approach 1: $U(\mathbb{I}_{15}) = \{[1],[2],[4],[7],[8],[11],[13],[14]\}$. Since $[2]^2 = [4], [2]^3 = [8]$ and $[2]^4 = [1]$, we have $\langle [2] \rangle = \{[1],[2],[4],[8]\}$. Also $[14]^2 = [1]$ and so we have $\langle [14] \rangle = \{[1],[14]\}$. Clearly, $\langle [2] \rangle \cap \langle [14] \rangle = \{[1]\}$. Also by the product formula, we have $|\langle [2] \rangle \langle [14] \rangle| = 8$. Since $\langle [2] \rangle \langle [14] \rangle$ is contained in $U(\mathbb{I}_{15})$ and has the same order as $U(\mathbb{I}_{15})$, it follows they are equal. By Proposition 2.127, $U(\mathbb{I}_{15}) \cong \langle [2] \rangle \times \langle [14] \rangle \cong \mathbb{I}_4 \times \mathbb{I}_2$.

Approach 2: We recall the isomorphism $U(\mathbb{I}_{15}) \cong U(\mathbb{I}_5) \times U(\mathbb{I}_3)$. One can check easily that $U(\mathbb{I}_5)$ is a cyclic group of order 4 generated by $[2]$. Similarly, one can check that $U(\mathbb{I}_3)$ is a cyclic group of order 2. Hence we have the required isomorphism.

2.98. Since $G/Z(G)$ is cyclic, we have $G/Z(G) = \langle gZ(G) \rangle$ for some $g \in G$. For any $a, b \in G$, we have $aZ(G) = g^i Z(G)$ for some integer i. This implies that $a = g^i x$ for some $x \in Z(G)$. Similarly one has $b = g^j y$ for some $y \in Z(G)$. Then one has $ab = g^i x g^j y = g^i g^j y x = g^j g^i y x = g^j y g^i x = ba$.

2.99. Suppose $|H| = p^n$ and $|G/H| = p^m$ for some integers n and m, then we have $|G| = |H||G:H| = |H||G/H| = p^{n+m}$.

2.102. Let $b \in \ker \gamma$. Since α is surjective, we have $b = \alpha(a)$ for some $a \in A$. Then $\beta(a) = \gamma\alpha(a) = \gamma(b) = 1$. Thus $a \in \ker \beta$ and $b \in \alpha(\ker \beta)$.

Conversely suppose $b \in \alpha(\ker \beta)$, then $b = \alpha(a)$ for some $a \in \ker \beta$. Therefore $\gamma(b) = \gamma\alpha(a) = \beta(a) = 1$ and so $b \in \ker \gamma$.

2.104. (i) Recall that the eight elements of $\mathbf{Q}$ are I, $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $A^2 = -I$, $A^3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$, $BA = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$, $BA^2 = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$ and $BA^3 =$

$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ and $Z(\mathbf{Q}) = \{I, -I\}$. Therefore $\mathbf{Q}/Z(\mathbf{Q})$ is a group of order 4. Now since $BA^{-1} = BA^3$ does not lie in $Z(\mathbf{Q})$, therefore $AZ(\mathbf{Q})$ and $BZ(\mathbf{Q})$ are two distinct elements in $\mathbf{Q}/Z(\mathbf{Q})$. Thus one has $\mathbf{Q}/Z(\mathbf{Q}) = \{Z(\mathbf{Q}), AZ(\mathbf{Q}), BZ(\mathbf{Q}), BAZ(\mathbf{Q})\}$. Since each non-identity element $\mathbf{Q}/Z(\mathbf{Q})$ is represented by $MZ(\mathbf{Q})$ where $M \neq I, -I$, it is of order 2 by part (ii) of question **2.86**. In particular, $\langle AZ(\mathbf{Q})\rangle \cap \langle BZ(\mathbf{Q})\rangle = \{Z(\mathbf{Q})\}$. Thus by the product formula, $\langle AZ(\mathbf{Q})\rangle\langle BZ(\mathbf{Q})\rangle$ is subset of $\mathbf{Q}/Z(\mathbf{Q})$ of order 4 and so must be equal to $\mathbf{Q}/Z(\mathbf{Q})$. Hence we have $\mathbf{Q}/Z(\mathbf{Q}) \cong \langle AZ(\mathbf{Q})\rangle \times \langle BZ(\mathbf{Q})\rangle \cong \mathbb{I}_2 \times \mathbb{I}_2 \cong \mathbf{V}$.

(ii) Since $\mathbf{V}$ has three elements of order 2 and $\mathbf{Q}$ only has one element of order 2, $\mathbf{Q}$ cannot have a subgroup isomorphic to $\mathbf{V}$.

2.106. Suppose HK is a subgroup of G, then for each $x \in HK$, we have $x^{-1} \in HK$. Therefore, we have $x^{-1} = hk$ for some $h \in H, k \in K$. Then $x = k^{-1}h^{-1} \in KH$. On the other hand, for each $x \in KH$, we have $x = kh$ for some $k \in K$ and $h \in H$. In particular, $k = 1k \in HK$ and $h = h1 \in HK$. But since HK is a subgroup, it follows that $x = kh \in HK$.

Conversely suppose $HK = KH$, we want to show that HK is a subgroup of G. Clearly $1 \in HK$. Now let $x, y \in HK$, then $x = h_1k_1$ and $y = h_2k_2$ for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Then one has $xy^{-1} = h_1k_1k_2^{-1}h_2^{-1}$. Since $HK = KH$, we have $k_1k_2^{-1}h_2^{-1} = hk$ for some $h \in H, k \in K$. Hence $xy^{-1} = h_1hk \in HK$ and so we have shown that HK is a subgroup.

2.113. (i) For $g, x, y \in G$, $g(xyx^{-1}y^{-1})g^{-1} = (gxg^{-1})(gyg^{-1})(gx^{-1}g^{-1})(gy^{-1}g^{-1}) = (gxg^{-1})(gyg^{-1})(gxg^{-1})^{-1}(gyg^{-1})^{-1}$. Thus we have shown that a conjugate of a commutator is still a commutator. Now suppose $z \in G'$, then $z = c_1 \cdots c_n$ where each c_i is some commutator. Then for each $g \in G$, $gzg^{-1} = gc_1 \cdots c_ng^{-1} = gc_1g^{-1} \cdots gc_ng^{-1}$. By the above argument, this is still a product of commutators. Hence $gzg^{-1} \in G'$ and so G' is normal in G.

(ii) By the definition of G', for any $x, y \in G$, $xyx^{-1}y^{-1}G' = G'$. Rearranging this, one obtains $xG'yG' = yG'xG'$.

(iii) For $x, y \in G$, one has $\varphi(xyx^{-1}y^{-1}) = \varphi(x)\varphi(y)\varphi(x)^{-1}\varphi(y)^{-1} = 1$ since A is abelian. Then for an element $z \in G'$, we have $z = c_1 \cdots c_n$ (where each c_i is some commutator) and $\varphi(z) = \varphi(c_1) \cdots \varphi(c_n)$. Since the image of a commutator is 1 by the preceding argument, one obtains $\varphi(z) = 1$. Thus $G' \subseteq \ker \varphi$.

Conversely if $G' \subseteq \ker \varphi$, then for $x, y \in G$, we have $\varphi(xyx^{-1}y^{-1}) = 1$. Rearranging this, one obtains $\varphi(x)\varphi(y) = \varphi(y)\varphi(x)$.

(iv) For $h \in H, g \in G$, we have $ghg^{-1}h^{-1} \in G' \subseteq H$. This implies $ghg^{-1} \in Hh = H$. Hence H is normal in G.