Solutions to Math 3E03 Homework 4

2.18. (Reflexivity) Let $x \in X$. Since one clearly has $f(x) = f(x)$, $x \equiv x$.

(Symmetry) Let $x_1, x_2 \in X$ and $x \equiv y$. Then $f(x) = f(y)$ which is the same as saying $f(y) = f(x)$. Hence $y \equiv x$.

(Transitivity) Let $x_1, x_2, x_3 \in X$ with $x \equiv y$ and $y \equiv z$. Then we have $f(x) = f(y)$ and $f(y) = f(z)$ which combines to give $f(x) = f(z)$. Thus, $x \equiv z$.

2.68. G is abelian $\iff ab = ba$ for all $a, b \in G \iff (ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$ $\iff f(ab) = f(a)f(b)$ for all $a, b \in G \iff f$ is a homomorphism.

2.73. Let $\sigma, \tau \in S_n$ and let $e_1, ..., e_n$ be the standard basis for $\mathbb{R}^n$. Then for each i, $P_{\sigma\tau}(e_i) = e_{\sigma\tau(i)} = e_{\sigma(\tau(i))} = P_\sigma(e_{\tau(i)}) = P_\sigma(P_\tau(e_i))$. Therefore $P_{\sigma\tau} = P_\sigma P_\tau$ and thus, f is a group homomorphism.

Clearly $P_\sigma = I_n$ if and only if $\sigma = 1$. Thus $\ker f = \{1\}$ and so f is injective by Proposition 2.93(ii). Hence f is an isomorphism from S_n to im f, which is a subgroup of $\mathrm{GL}(n, \mathbb{R})$.

2.75. Since $ab = a(ba)a^{-1}$, ab and ba are conjugate to each other and so have the same order by Proposition 2.94(ii).

2.80. Let $H_i, i \in I$ be a family of normal subgroups of G. From Proposition 2.76, we have that $\bigcap_{i \in I} H_i$ is a subgroup of G. To show that this is normal, let $g \in G, x \in \bigcap_{i \in I} H_i$. Then $x \in H_i$ for all i. Since each H_i is normal in G, $gxg^{-1} \in H_i$. Since this is true for all i, we have $gxg^{-1} \in \bigcap_{i \in I} H_i$.

2.84. Supposing we have a matrix of the form $aI, a \neq 0$ where I is the 2×2 identity matrix, then for any $A \in \mathrm{GL}(2, \mathbb{R})$, $(aI)A = aA = Aa = A(aI)$. Therefore such a matrix lies in the center of $\mathrm{GL}(2, \mathbb{R})$.

Conversely suppose $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is in the center of $\mathrm{GL}(2, \mathbb{R})$, then considering

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

we obtain

$$\begin{pmatrix} a & -b \\ c & -d \end{pmatrix} = \begin{pmatrix} a & b \\ -c & -d \end{pmatrix}.$$

This yields $-b = b$ and $c = -c$ which imply $b = c = 0$. Now considering

$$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix},$$

we obtain

$$\begin{pmatrix} 0 & a \\ d & 0 \end{pmatrix} = \begin{pmatrix} 0 & d \\ a & 0 \end{pmatrix}.$$

This implies that $a = d$ and since the matrix is invertible, $a \neq 0$. Hence the center of $\mathrm{GL}(2, \mathbb{R})$ consists precisely of matrices of the form $aI, a \neq 0$.

2.86. We first compute explicitly the elements of $\mathbf{Q}$. They 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 $BA^3 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$.

(i) One checks that $AB = BA^3 \neq BA$. Thus $\mathbf{Q}$ is not an abelian group.

(ii) One checks this directly.

(iii) and (iv): Let H be a subgroup of $\mathbf{Q}$ with order 2. Then the nonidentity element in H must have order 2 (it has order either 1 or 2 by Lagrange's Theorem but since it is not the identity. it's order must be 2). But $\mathbf{Q}$ has only one element of order 2 which is $-I$. Hence $H = \langle -I \rangle$. Thus $\mathbf{Q}$ only has one subgroup of order 2.

Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be in $Z(\mathbf{Q})$. Then considering

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

we obtain

$$\begin{pmatrix} -b & a \\ -d & c \end{pmatrix} = \begin{pmatrix} c & d \\ -a & -b \end{pmatrix}.$$

Thus we obtain $a = d$ and $b = -c$. Now considering

$$\begin{pmatrix} a & -c \\ c & a \end{pmatrix} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \begin{pmatrix} a & -c \\ c & a \end{pmatrix},$$

we obtain

$$\begin{pmatrix} -ci & ai \\ ai & ci \end{pmatrix} = \begin{pmatrix} ci & ai \\ ai & -ci \end{pmatrix}.$$

From the above, we obtain $ci = -ci$ implying $c = 0$. Thus an element in $Z(\mathbf{Q})$ is of the form of a scalar matrix. Now the only scalar matrices in $\mathbf{Q}$ are I and $A^2 = -I$, and clearly these two matrices lie in the center. Hence $\langle -I \rangle = Z(\mathbf{Q})$.

2.87. From 2.86, $\mathbf{Q}$ has only one element of order 2 whereas D_8 has at least two elements of order 2 (for instances reflection and rotations by 180^0). Hence $\mathbf{Q}$ and D_8 are nonisomorphic to each other by Problem 2.69.

2.92. (i) Clearly the identity map is an automorphism. Therefore $\mathrm{Aut}(G)$ is nonempty. Let $f, g \in \mathrm{Aut}(G)$. Since f and g are bijective, so is $f \circ g$. To see that $f \circ g \in \mathrm{Aut}(G)$, it remains to show that $f \circ g$ is a group homomorphism. Let $x, y \in G$. Then $(f \circ g)(xy) = f(g(xy)) = f(g(x)g(y)) = f(g(x))f(g(y)) = (f \circ g)(x)(f \circ g)(y)$. Hence we have show that composition is a binary operation. Associativity follows from the basic properties of functions and the identity map is clearly the identity element in $\mathrm{Aut}(G)$.

We are left with the verification of inverse. Let $f \in \mathrm{Aut}(G)$. Since f is bijective, it has an inverse (as a function!) g. We now show that g is also a group homomorphism. Let $x, y \in G$. Then there exists $a, b \in G$ such that $f(a) = x$ and $f(b) = y$. Therefore we have $g(x) = a$ and $g(y) = b$. Hence $g(xy) = g(f(a)f(b)) = g(f(ab)) = ab = g(x)g(y)$.

(ii) Let $g, h \in G$. Then for every $x \in G$, $\gamma_{gh}(x) = (gh)x(gh)^{-1} = g(hxh^{-1})g^{-1} = \gamma_g(hxh^{-1}) = \gamma_g(\gamma_h(x)) = (\gamma_g \circ \gamma_h)(x)$. Thus $\gamma_{gh} = \gamma_g \circ \gamma_h$.

(iii) $\gamma_g = 1 \Longleftrightarrow \gamma_g(x) = x$ for all $x \in G \Longleftrightarrow gxg^{-1} = x$ for all $x \in G \Longleftrightarrow g \in Z(G)$.

(iv) Let $\delta \in \mathrm{Aut}(G), g \in G$. Then for every $x \in G$, we have $(\delta \circ \gamma_g \circ \delta^{-1})(x) = \delta(\gamma_g(\delta^{-1}(x))) = \delta(g\delta^{-1}(x)g^{-1}) = \delta(g)x\delta(g^{-1}) = \delta(g)x\delta(g)^{-1} = \gamma_{\delta(g)}(x)$. Hence $\delta \circ \gamma_g \circ \delta^{-1} = \gamma_{\delta(g)} \in \mathrm{im}\gamma$. Therefore $\mathrm{im}\gamma$ is a normal subgroup of $\mathrm{Aut}(G)$.

2.94. Let x be a generator of C and $f \in \mathrm{Aut}(C)$. Then $f(x) = x^i$ for some $0 \leq i < n$. Since f is an automorphism, x^i must generate the group C. But this is only possible if $\gcd(i, n) = 1$.

Conversely let i be an integer such that $0 \leq i < n$ and $\gcd(i, n) = 1$. Define a function $f : C \to C$ by $f(x^j) = x^{ij}$. This is a group homomorphism as $f(x^{j+r}) = x^{i(j+r)} = x^{ij+ir} = x^{ij}x^{ir} = f(x^j)f(x^r)$. Since x^i is in the image of f and is a generator of C, it follows that f is surjective. Since C is a finite group, f is an automorphism. Thus we have shown that the $\mathrm{Aut}(C)$ consists precisely of maps sending x to x^i where $0 \leq i < n$ and $\gcd(i, n) = 1$. Therefore, $|\mathrm{Aut}(C)| = \phi(n)$.