HW 4 - MATH403

Danesh Sivakumar

June 14, 2022

Problem 1 (Chapter 6, Exercise 6)

Prove that isomorphism is an equivalence relation. That is, for any groups G, H, and K
$G \cong G$;
$G \cong H$ implies $H \cong G$
$G \cong H$ and $H \cong K$ implies $G \cong K$.

Proof. First, we prove that isomorphism is reflexive; that is, $G \cong G$. To this end, consider the identity isomorphism $\phi_{id} \colon G \to G$, $\phi_{id}(x) = x$. This is an isomorphism because it is a bijection and a homomorphism; it is a bijection because it is one-to-one and onto. To prove it is one-to-one, suppose $\phi_{id}(x) = \phi_{id}(y)$. By definition this implies $x = y$, so that it is one-to-one. To prove it is onto, note that given $y = \phi_{id}(x)$, it follows that $x = y$ by definition. Finally, ϕ_{id} is a homomorphism because $\phi_{id}(xx) = xx = \phi_{id}(x)\phi_{id}(x)$
Second, we prove that isomorphism is symmetric; that is, $G \cong H$ implies $H \cong G$. To this end, note that because the isomorphism $\phi \colon G \to H$ is a bijection, $\phi^{-1} \colon H \to G$ is also a bijection. To prove that ϕ^{-1} is a homomorphism, suppose that there exist $h_1, h_2 \in H$ with $\phi^{-1}(h_1) = g_1$ and $\phi^{-1}(h_2) = g_2$, with $g_1, g_2 \in G$ (which exist because ϕ^{-1} is onto in particular). Then, it follows that $\phi^{-1}(h_1h_2) = \phi^{-1}(\phi(g_1)\phi(g_2)) = \phi^{-1}(\phi(g_1g_2)) = g_1g_2 = \phi^{-1}(h_1)\phi^{-1}(h_2)$.
Third, we prove that isomorphism is transitive; that is, $G \cong H$ and $H \cong K$ implies $G \cong K$. Consider the isomorphisms $\phi_1 \colon G \to H$ and $\phi_2 \colon H \to K$; we want to show that $\phi_3 \colon G \to K$, $\phi_3 = \phi_2 \circ \phi_1$ is an isomorphism. It follows that ϕ_3 is a bijection, since ϕ_1 and ϕ_2 are bijections and the composition of two bijections is a bijection. To show that ϕ_3 is a homomorphism, note that $\phi_3(g_1g_2) = \phi_2(\phi_1(g_1g_2)) = \phi_2(\phi_1(g_1)\phi_1(g_2)) = \phi_2(\phi_1(g_1))\phi_2(\phi_1(g_2)) = \phi_3(g_1)\phi_3(g_2)$; thus ϕ_3 is an isomorphism.
Thus isomorphism is an equivalence relation.

□

Problem 2 (Chapter 6, Exercise 14)

Find two groups G and H such that $G \ncong H$ but $\mathrm{Aut}(G) \cong \mathrm{Aut}(H)$.

Proof. Consider $G = \{e\}$ and $H = \mathbb{Z}_2 = \{0, 1\}$. These groups are not isomorphic (as their orders are different and thus a bijection cannot be made between them). However, notice that $\mathbb{Z}_2$ only has one generator (namely 1, because it is the only integer relatively prime to 2), so that the only automorphism of H is the identity map $f_1(x) = x$. Trivially, the only automorphism of G is the identity map $f_1(x) = x$; because both $\text{Aut}(G)$ and $\text{Aut}(H)$ each only contain the identity map, they are isomorphic to $U(1)$ and thus each other. □

Problem 3 (Chapter 6, Exercise 17)

If G is a group, prove that $\text{Aut}(G)$ and $\text{Inn}(G)$ are groups.

Proof. $\text{Aut}(G)$ and $\text{Inn}(G)$ are each isomorphic to subsets of S_n, where n is the order of G; because each of them contain the identity and are thus nonempty, it suffices to use the subgroup test. First, we will prove $\text{Aut}(G)$ is a group. Suppose that $\alpha, \beta \in \text{Aut}(G)$. Then it follows that $\alpha\beta$ and α^{-1} are bijections by properties of bijections, so we will show the operation preserving property on each of them. For any $x, y \in G$, it follows that $\alpha\beta(xy) = \alpha(\beta(xy)) = \alpha(\beta(x)\beta(y)) = \alpha(\beta(x))\alpha(\beta(y) = \alpha\beta(x)\alpha\beta(y)$, so that $\alpha\beta \in \text{Aut}(G)$. Suppose that $a, b \in G$ such that $c = \alpha(a)$ and $d = \alpha(b)$. Then we have that $\alpha^{-1}(cd) = \alpha^{-1}(\alpha(a)\alpha(b)) = \alpha^{-1}(\alpha(ab)) = ab = \alpha^{-1}(c)\alpha^{-1}(d)$, so that $\alpha^{-1} \in \text{Aut}(G)$. Thus, $\text{Aut}(G)$ is a group.
Next, we will prove $\text{Inn}(G)$ is a group. Suppose that $\phi_a, \phi_b \in \text{Inn}(G)$, induced by a and b respectively. Then $\phi_a\phi_b(x) = \phi_a(\phi_b(x)) = \phi_a(bxb^{-1}) = abxb^{-1}a^{-1} = (ab)x(ab)^{-1} = \phi_{ab}(x)$, so that $\phi_{ab}(x) \in \text{Inn}(G)$. Next, we show that $\phi_a^{-1} \in \text{Inn}(G)$. To this end, consider $\phi_{a^{-1}} \in \text{Inn}(G)$; we have that $\phi_{a^{-1}}\phi_a(x) = \phi_{a^{-1}}(\phi_a(x)) = \phi_{a^{-1}}(axa^{-1}) = a^{-1}axa^{-1}a = x$ and $\phi_a\phi_{a^{-1}}(x) = \phi_a(\phi_{a^{-1}}(x)) = \phi_a(a^{-1}xa) = aa^{-1}xaa^{-1} = x$, so that $\phi_a^{-1} = \phi_{a^{-1}} \in \text{Inn}(G)$. Thus, $\text{Inn}(G)$ is a group. □

Problem 4 (Chapter 6, Exercise 20)

Let H be the subgroup of all rotations in D_n and let ϕ be an automorphism of D_n. Prove that $\phi(H) = H$.

Proof. Suppose that $a \in H$ is a rotation that generates H ($H = \langle a \rangle$), which exists because the subgroup of all rotations is cyclic and finite of order n; then a has order n. Because isomorphisms preserve order, it follows that $\phi(a) \in D_n$ also has order n and is thus also a rotation (because a rotation and reflection cannot have the same order); thus it follows that $\phi(a) \in H$, so that $\phi(H) \subseteq H$. Because ϕ is an automorphism of D_n, it follows that ϕ^{-1} is also an automorphism of D_n. Using ϕ^{-1} in place of ϕ above, it follows that $\phi^{-1}(H) \subseteq H$, so that $H \subseteq \phi(H)$. Thus $\phi(H) = H$. □

Problem 5 (Chapter 6, Exercise 21)

Let $H = \{\beta \in S_5 \mid \beta(1) = 1\}$ and $K = \{\beta \in S_5 \mid \beta(2) = 2\}$. Prove that H is isomorphic to K. Is the same true if S_5 is replaced by S_n, where $n \geq 3$?

Proof. Note that H is a subgroup of S_5 that fixes 1, and is thus isomorphic to a subgroup of S_4. Similarly, K is a subgroup of S_5 that fixes 2, and is thus isomorphic to a subgroup of S_4. By the transitivity of isomorphism, it follows that H is isomorphic to K. Also, note that $\beta_k = (12)\beta_h(12)$ and $\beta_h = (12)\beta_k(12)$, because each of H and K only fix 1 and 2 respectively; thus $\phi \colon H \to K$ where ϕ is right and left multiplying by (12) is an isomorphism, as $\phi(\beta_h)\phi(\beta_k) = (12)\beta_h(12)(12)\beta_k(12) = (12)\beta_h\beta_k(12) = \phi(\beta_h\beta_k)$. The map is injective because of cancellation, and the map is surjective because it is injective and between sets of the same cardinality. The same result will hold for S_n with $n \geq 3$ by noticing that each of H and K are isomorphic to S_{n-1}

□

Problem 6 (Chapter 6, Exercise 26)

Suppose that $\phi \colon \mathbb{Z}_{20} \to \mathbb{Z}_{20}$ is an automorphism and $\phi(5) = 5$. What are the possibilities for $\phi(x)$?

Proof. Automorphisms map generators to generators, so it suffices to find the possibilities for $\phi(1)$, and the candidates are 1, 3, 7, 9, 11, 13, 17, 19. We know that $\phi(5) \equiv 5 \pmod{20}$. We also know that $\phi(5) = 5\phi(1)$, so that $5\phi(1) \equiv 5 \pmod{20}$. Notice that $5 \cdot 3 = 15 \not\equiv 5 \pmod{20}$, $5 \cdot 7 = 35 \not\equiv 5 \pmod{20}$, $5 \cdot 11 = 55 \not\equiv 5 \pmod{20}$, and $5 \cdot 19 = 95 \not\equiv 5 \pmod{20}$. Thus $\phi(1)$ can only be 1, 9, 13, 17, so that $\phi(x) = x$, $9x$, $13x$, or $17x$.

□

Problem 7 (Chapter 6, Exercise 34)

Prove property 4 of Theorem 6.3:
Suppose that ϕ is an isomorphism from a group G onto a group $\overline{G}$. Then:
If K is a subgroup of G, then $\phi(K) = \{\phi(k) \mid k \in K\}$ is a subgroup of $\overline{G}$.

Proof. Since K is a subgroup of G, it follows that $a, b \in K \implies ab \in K$ and $a \in K \implies a^{-1} \in K$. Let $\phi a, \phi(b) \in \phi(K)$. Then by the isomorphism property, $\phi(a)\phi(b) = \phi(ab)$; because $ab \in K$, it follows that $\phi(ab) \in \phi(K)$. // Now suppose $\phi(a) \in \phi(K)$. We want to show $\phi(a)^{-1} \in \phi(K)$. To this end, notice that $\phi(a)^{-1} = \phi(c)$ for some $c \in K$, we have that $\phi(a)\phi(c) = e \implies \phi(ac) = e$, so that $ac = e$, and $c = a^{-1}$. By assumption, $a^{-1} \in K$, so that $\phi(a)^{-1} = \phi(a^{-1}) = \phi(c) \in \phi(K)$. Thus $\phi(K)$ is a subgroup of $\overline{G}$.

□

Problem 8 (Chapter 6, Exercise 38)

Let

$$G = \{a + b\sqrt{2} \mid a, b \text{ are rational}\}$$

and

$$H = \left\{ \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \;\middle|\; a, b \text{ are rational} \right\}.$$

Show that G and H are isomorphic under addition. Prove that G and H are closed under multiplication. Does your isomorphism preserve multiplication as well as addition?

Proof. Define $\phi\colon G \to H$, $\phi(a+b\sqrt{2}) = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$. To show ϕ is injective, suppose $\phi(a + b\sqrt{2} = \phi(c + d\sqrt{2}$. Then $\begin{bmatrix} a & 2b \\ b & a \end{bmatrix} = \begin{bmatrix} c & 2d \\ d & c \end{bmatrix}$, so that $a = c$ and $b = d$. To show ϕ is surjective, note that for any value in the image $\begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$, there is always a value $a + b\sqrt{2} \in G$ by definition of the mapping. Thus ϕ is a bijection.
To show that ϕ is an isomorphism under addition, note that $\phi((a + b\sqrt{2}) + (c + d\sqrt{2})) = \phi(a + c + (b + d)\sqrt{2}) = \begin{bmatrix} a + c & 2(b + d) \\ b + d & a + c \end{bmatrix} = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix} + \begin{bmatrix} c & 2d \\ d & d \end{bmatrix} = \phi(a + b\sqrt{2}) + \phi(c + d\sqrt{2})$.
G is closed under multiplication because $(a + b\sqrt{2})(c + d\sqrt{2}) = ac + 2bd + (ad + bc)\sqrt{2}$.
H is closed under multiplication because $\begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \cdot \begin{bmatrix} c & 2d \\ d & c \end{bmatrix} = \begin{bmatrix} ac + 2bd & 2(ad + bc) \\ (ad + bc) & ac + 2bd \end{bmatrix}$
To show ϕ preserves multiplication, note that $\phi((a + \sqrt{2})(c + d\sqrt{2}) = \phi(ac + 2bd + (ad + bc)\sqrt{2}) = \begin{bmatrix} ac + 2bd & 2(ad + bc) \\ (ad + bc) & ac + 2bd \end{bmatrix} = \phi(a + b\sqrt{2})\phi(c + d\sqrt{2})$.

□

Problem 9 (Chapter 6, Exercise 40)

Explain why S_8 contains subgroups isomorphic to Z_{15}, $U(16)$, and D_8.

Proof. Note that $(12345)(678) \in S_8$ has order 15, so that $\langle(12345)(678)\rangle \subseteq S_8$ is a cyclic subgroup of order 15 and thus isomorphic to $\mathbb{Z}_{15}$.
Note that $U(16) = \{1, 3, 5, 7, 9, 11, 13, 15\}$, and multiplying every element by any particular element of this group will permute the set, so that the group of all of these actions can be interpreted as a group of permutations of eight elements, which is isomorphic to a subgroup of S_8.
Note that D_8 describes the symmetries of a regular octagon, so take each vertex of the octagon to be an element in $\{1, \cdots, 8\}$; then every element of D_8 can be interpreted as a permutation of each of those eight elements, or an element of S_8; this is indeed a subgroup.

□

Problem 10 (Chapter 6, Exercise 44)

Suppose that G is a finite Abelian group and G has no element of order 2. Show that the mapping $g \to g^2$ is an automorphism of G. Show, by example, that there is an infinite Abelian group for which the mapping $g \to g^2$ is one-to-one and operation-preserving but not an automorphism.

Proof. Let $\phi\colon g \to g^2$ be the mapping. Then because G is Abelian we have that for any $g, h \in G$, $\phi(gh) = g^2h^2 = ghgh = \phi(g)\phi(h)$, so that ϕ is a homomorphism. If $\phi(g) = e$, then because G has no element of order 2 it follows that $g = e$; this implies that ϕ is an injective map (this follows from the fact that $\phi(h) = h\phi(e)$. Because G is finite, the map is also surjective; thus ϕ is an automorphism.

Consider $(\mathbb{Z}, +)$, the integers under addition, which is clearly a group. The map now becomes $\phi(x) = 2x$, which is a scaling map and thus operation preserving. This map is clearly injective by cancellation, but it is not surjective because for any odd integer there is no integer mapping to it, because the image is only even integers; thus ϕ cannot be an automorphism.

□

Problem 11 (Chapter 6, Exercise 64)

Prove that $\mathbb{Q}$, the group of rational numbers under addition, is not isomorphic to a proper subgroup of itself.

Proof. Suppose that $\phi\colon \mathbb{Q} \to H$ is an isomorphism between $\mathbb{Q}$ and $H \subseteq \mathbb{Q}$. Note that for $a, b \in \mathbb{Z}$, it follows that $\phi(\frac{a}{b}) = a\phi(\frac{1}{b})$ by the isomorphism property. Also, because $\phi(\frac{1}{b}) = b\frac{1}{b}\phi(\frac{1}{b}) = \frac{1}{b}\phi(b\frac{1}{b}) = \frac{1}{b}\phi(1)$, it follows that $\phi(\frac{a}{b}) = \frac{a}{b}\phi(1)$, so that ϕ is simply multiplication by $\phi(1)$. Because ϕ is an isomorphism, it must be injective and surjective; thus for any $q \in \mathbb{Q}$, it follows that $\phi(\frac{q}{\phi(1)}) = q$. This implies that the image of ϕ is the entirety of $\mathbb{Q}$.

□