# Math 103 HW 9 Solutions to Selected Problems

4. **Show that $U(8)$ is not isomorphic to $U(10)$.**

   **Solution:** Unfortunately, the two groups have the same order: the elements are $U(n)$ are just the coprime elements of $Z_n$, so $U(8) = \{1, 3, 5, 7\}$ while $U(10) = \{1.3.7.9\}$. Thus, we must examine the elements further. We claim that $U(10)$ is cyclic. This is easy to calculate:

$$\begin{aligned} 3^2 &\equiv 9 \\ 3^3 &= 27 \\ &\equiv 7 \\ 3^4 &\equiv 3 \cdot 7 \\ &\equiv 1 \pmod{10} \end{aligned}$$

   which means 3 generates $U(10)$.

   Now if $U(10)$ and $U(8)$ were isomorphic, we have seen that this would mean $U(8)$ was cyclic as well. In particular, it would have a generator of order 4. However, we can see that

$$\begin{aligned} 3^2 &= 9 \\ &\equiv 1 \\ 5^2 &= 25 \\ &\equiv 1 \\ 7^2 &= 49 \\ &\equiv 1 \pmod{8} \end{aligned}$$

   so every element of $U(8)$ has order dividing 2. Therefore, $U(8)$ is not cyclic, hence is not isomorphic to $U(10)$.

12. **Let $G$ be a group. Prove that the mapping $\alpha(g) = g^{-1}$ for all $g$ in $G$ is an automorphism if and only if $G$ is Abelian.**

**Solution:** $\alpha$ is clearly its own inverse, so it is always a bijective map. The only question is whether it is a morphism of groups, so it is enough to show this is true if and only if $G$ is Abelian. If $G$ is Abelian, then certainly

$$\begin{aligned}\alpha(gh) &= (gh)^{-1}\\ &= h^{-1}g^{-1}\\ &= g^{-1}h^{-1}\\ &= \alpha(g)\alpha(h)\end{aligned}$$

since we can commute elements, so $\alpha$ is a morphism. On the other hand, by definition $\alpha$ being a morphism is equivalent to $(gh)^{-1} = g^{-1}h^{-1}$ for every $g, h \in G$. By problem 25 from Homework 4, this implies that $G$ is Abelian. Putting the two together, we have our result.

17. **If $G$ is a group, prove that $Aut(G)$ and $Inn(G)$ are groups.**

**Solution:** We first show that each has an identity. The operation is function composition, so the identity here is just the identity function $id_G$ on $G$. This is certainly bijective, and it is a morphism simply because $G$ is a group. This shows $id_G \in Aut(G)$. Function composition is also associative (see Theorem 0.8.1), we know that the composition of bijective functions is bijective, and it easy to check that the composition of morphisms is again a morphism [1]. Thus, $Aut(G)$ is closed under multiplication. It remains to show it is closed under inversion. We know at least that the *function* $\alpha^{-1}$ exists for $\alpha \in Aut(G)$ (since bijective is equivalent to invertible). If we let $g, h$ be in $G$, then

$$\begin{aligned}\alpha^{-1}(gh) &= \alpha^{-1}(\alpha(\alpha^{-1}(g))\alpha(\alpha^{-1}(h))\\ &= \alpha^{-1}(\alpha(\alpha^{-1}(g)\alpha^{-1}(h))) \text{ (since } \alpha \text{ is a morphism)}\\ &= \alpha^{-1}(g)\alpha^{-1}(h)\end{aligned}$$

meaning $\alpha^{-1}$ is actually in $Aut(G)$. This shows that $Aut(G)$ is a group.

$Inn(G)$ is defined as a subset of $Aut(G)$, so we need not show associativity again. For any $g \in G$, $ege = g$, so $id_G = \phi_e$, which is certainly an element of $Inn(G)$. Furthermore,

$$\begin{aligned}\phi_g\phi_h(x) &= \phi_g(hxh^{-1})\\ &= ghxh^{-1}g^{-1}\\ &= \phi_{gh}(x)\end{aligned}$$

for each $x \in G$, so $\phi_g\phi_h = \phi_{gh}$ is in $Inn(G)$. In particular, this show thats $\phi_g\phi_{g^{-1}} = \phi_{g^{-1}}\phi_g = \phi_e$, the identity, so $(\phi_g)^{-1} = \phi_{g^{-1}}$. Thus $Inn(G)$ is closed under multiplication and taking inverses, and contains the identity, so it is indeed a subgroup of $Aut(G)$.

[1] that is, if $\alpha$ and $\beta$ are two morphisms from $G$ to $G$, $\alpha(\beta(gh)) = \alpha(\beta(gh)) = \alpha(\beta(g)\beta(h)) = \alpha(\beta(g))\alpha(\beta(h))$

24. **Let $\phi$ be an automorphism of a group $G$. Prove that $H = \{x \in G | \phi(x) = x\}$ is a subgroup of $G$.**

    **Solution:** For any morphism $G \to G$, $\phi(e) = e$, meaning $e \in H$. Since $\phi$ is a morphism, if $x, y \in H$, $\phi(xy) = \phi(x)\phi(y) = xy$, so $xy \in H$ as well. We also know that $\phi(g)^{-1} = \phi(g^{-1})$ for all $g \in G$, so $x \in H$ implies $\phi(x^{-1}) = \phi(x)^{-1} = x^{-1}$; ie, $x^{-1} \in H$. Thus, $H$ is a subgroup.

26. **Suppose that $\phi : Z_{20} \to Z_{20}$ is an automorphism and $\phi(5) = 5$. What are the possiblities for $\phi(x)$?**

    **Solution:** Note that since $Z_{20}$ is cyclic, generated by 1, $\phi$ is completely determined by $\phi(1)$: $\phi(x) = \phi(x \cdot 1) = x \cdot \phi(1)$ since $\phi$ is a morphism. This shows that the morphisms from $Z_{20}$ to itself are precisely given by $\phi_m(x) = mx$ for $m \in Z_{20}$ (this is a morphism because $\phi(x + y) = m(x + y) = mx + my$). To be an automorphism, it is enough for $\phi_m(1) = m$ to generate $Z_{20}$, since for finite sets, surjective implies bijective. This means that $m$ must be coprime to 20. Let our $\phi$ be one of these $\phi_m$. The only other constraint we have is that $\phi(5) = 5$ in $Z_{20}$; that is, $5m \equiv 5 \pmod{20}$. But we know this is true if and only if 20 divides $5m - 5 = 5(m - 1)$, or in other words 4 divides $m - 1$. Checking all the members of $Z_{20}^{\times}$, we see that the only $m$ satisfying this condition are $m = 1, 9, 13$ and 17, so these are the only possibilities for $\phi(x) = mx$.

30. **The group $\left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \middle| a \in \mathbb{Z} \right\}$ is isomorphic to what familiar group? What if $\mathbb{Z}$ is replaced by $\mathbb{R}$?**

    **Solution:** Let $G$ be this group (implicit here is that the operation is matrix multiplication). We claim that $G$ is isomorphic to $\mathbb{Z}$. To this end, we try to use the easiest map $\phi : G \to \mathbb{Z}$ possible, given by $\phi(\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}) = a$. This is a morphism because

$$\begin{aligned} \phi(\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}) \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}) &= \phi(\begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}) \\ &= a + b \\ &= \phi(\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}) + \phi(\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}) \end{aligned}$$

    On the other hand, we can see that $\phi$ is invertible: if we let $\psi : \mathbb{Z} \to G$, $a \mapsto \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$, then certainly $\psi \circ \phi(\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ and $\phi \circ \psi(a) = a$ for all $a \in \mathbb{Z}$, so $\psi = \phi^{-1}$. Thus, $\phi$ is an isomorphism. Nothing about our proof relied on any properties of $\mathbb{Z}$, besides that it had an additive structure, so, , replacing $\mathbb{Z}$ with $\mathbb{R}$ everywhere, it would work for $\mathbb{R}$ as well.

38. **Let**

$$G = \{a + b\sqrt{2} |\ a, b \textbf{ are rational}\}$$

**and**

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

**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?**

**Solution:** Define $\phi : H \to G$ by $\phi(\begin{pmatrix} a & 2b \\ b & a \end{pmatrix}) = a + b\sqrt{2}$ (which is in $G$ since $a, b \in \mathbb{Q}$). This is definitely surjective, so we must show it is an injective morphism. Given $a, b, c, d \in \mathbb{Q}$,

$$\begin{aligned}
\phi(\begin{pmatrix} a & 2b \\ b & a \end{pmatrix} + \begin{pmatrix} c & 2d \\ d & c \end{pmatrix}) &= \phi(\begin{pmatrix} a+c & 2(b+d) \\ b+d & a+c \end{pmatrix} \\
&= (a+c) + (b+d)\sqrt{2} \\
&= a + b\sqrt{2} + c + d\sqrt{2} \\
&= \phi(\begin{pmatrix} a & 2b \\ b & a \end{pmatrix}) + \phi(\begin{pmatrix} c & 2d \\ d & c \end{pmatrix})
\end{aligned}$$

as desired, hence $\phi$ is a morphism. As we proved in section [2], $\phi$ being injective is equivalent to saying that $\phi(h) = 0$ implies $h = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ (the identity in $H$) for any $h \in H$. In other words, we must show that (letting $h = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix}$) if $a, b \in \mathbb{Q}$, $a + b\sqrt{2} = 0$ implies $a = b = 0$. Suppose not; then $a = -b\sqrt{2}$, so $b$ must not be 0 or else $a = 0\sqrt{2} = 0$. But then $-\frac{a}{b} = \sqrt{2}$, meaning we can write $\sqrt{2}$ as the quotient of two rational numbers. This forces $\sqrt{2}$ itself to be rational, as $\mathbb{Q}$ is a field (so closed under division by nonzero elements). However, it is well known (for example, often proved in Math 109) that $\sqrt{2}$ is irrational, so we must have $a = b = 0$ after all.

$G$ is closed under multiplication, as

$$(a + b\sqrt{2})(c + d\sqrt{2}) = ac + 2bd + (ad + bc)\sqrt{2}$$

which is in $G$ since the rationals are closed under multiplication and addition. What's more,

$$\begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \begin{pmatrix} c & 2d \\ d & c \end{pmatrix} = \begin{pmatrix} ac + 2bd & 2(bc + ad) \\ (bc + ad) & ac + 2bd \end{pmatrix}$$

which is in $H$ for the same reasons. This shows that $H$ is closed under multiplication, and also that $\phi$ preserves multiplication.

[2]and is useful to prove yourself if you didn't go to section

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

**Solution:** Call this map $\alpha$. Since $G$ is Abelian, $\alpha(gh) = ghgh = g^2h^2\ \forall g, h \in G$, hence $\alpha$ is a morphism. Suppose $\alpha(g) = e$. Then either $g = e$ or $g$ has order 2, so by assumption we must have $g = e$. By the fact mentioned in the previous problem, this is enough to show $\alpha$ is injective. As $G$ is finite, injective implies bijective, so $\alpha$ is an automorphism.

Now consider the infinite Abelian group $\mathbb{Z}$. In additive notation, $\alpha : \mathbb{Z} \to \mathbb{Z}$ is defined by $\alpha(x) = 2x$. We know that every element of $\mathbb{Z}$ has infinite order except the identity, so the proof above still works to show that $\alpha$ is an injective morphism (or we can just divide the equation $2x = 2y$ by 2). However, injective does not imply bijective in this case: the image of $\alpha$ is the even integers, which definitely isn't all of $\mathbb{Z}$. Therefore, $\alpha$ is not surjective, and hence cannot be an automorphism.

55. **Let $\phi$ be an automorphism of $\mathbb{C}^*$, the group of nonzero complex numbers under multiplication. Determine $\phi(-1)$. Determine the possibilities for $\phi(i)$.**

**Solution:** We have seen that isomorphisms preserve orders, and so $(-1)^2 = 1$ implies that $\phi(-1)$ has order 2. What are the elements of order 2 in $\mathbb{C}^*$? Such an element—call it $x$—must be a solution to $x^2 - 1 = 0$, which factorizes as $(x-1)(x+1) = 0$. We cannot have $x = 1$ since 1 has order 1, so we can divide by (the nonzero) $x - 1$ to get $x + 1 = 0$; ie, $x = -1$. Thus, the only option is $\phi(-1) = -1$.

Similarly, $i^2 = -1, i^3 = -i$, and $i^4 = 1$, so $\phi(i)$ must have the same order, 4, as $i$. The elements of order 4 are solutions in $\mathbb{C}^*$ to $x^4 - 1 = 0$, which we can factorize as

$$\begin{aligned} 0 &= x^4 - 1 \\ &= (x^2 - 1)(x^2 + 1) \\ &= (x - 1)(x + 1)(x - i)(x + i) \end{aligned}$$

By the same reasoning as above, this means that the elements of order 4 must be $\pm 1$ or $\pm i$. The former do not have order 4, and $-i$ has order 4 too (for example, because it's $i^{-1}$), so $\phi(i)$ must be $\pm i$.

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

**Solution:** Let $\phi : \mathbb{Q} \to H$ be an isomorphism with a subgroup $H$ of $\mathbb{Q}$. We want to show that $H = \mathbb{Q}$. However, if $x, y$ are $\in \mathbb{Z}$, $\phi(x) = x \cdot \phi(1)$, while $\phi(\frac{x}{y})$ (if $y \neq 0$) is equal to $x\phi(\frac{1}{y})$, which—since $\phi(1) = \phi(y \cdot \frac{1}{y}) = y\phi(\frac{1}{y})$—must be $\frac{x}{y}\phi(1)$. This shows that $\phi$ is completely determined by $\phi(1)$, and in fact that $\phi$ is just multiplication by $\phi(1)$.

$\phi$ is an isomorphism, so in particular it must be injective, with $\phi(1) \neq 0$. But then for any $g \in \mathbb{Q}$, $\phi(\frac{g}{\phi(1)}) = g$, so the image of $\phi$ is $\mathbb{Q}$. Since $im(\phi)$ is contained in $H$ almost by definition, this forces $H = \mathbb{Q}$, so $H$ cannot be a proper subgroup.