Homework #8 Solutions

p 132, #10 ($\Rightarrow$) Suppose that α is an automorphism of G. Let $a, b \in G$. Then

$$b^{-1}a^{-1} = (ab)^{-1} = \alpha(ab) = \alpha(a)\alpha(b) = a^{-1}b^{-1}$$

which implies that $ab = ba$. Since $a, b \in G$ were arbitrary we conclude that G is abelian.

($\Leftarrow$) Suppose that G is abelian. Let $a, b \in G$. If $\alpha(a) = \alpha(b)$ then we have

$$a^{-1} = b^{-1}$$

which implies that $a = b$, proving that α is one-to-one. Given any $a \in G$, we know that $a^{-1} \in G$ and

$$\alpha(a^{-1}) = (a^{-1})^{-1} = a$$

which proves that α is onto. Finally, if $a, b \in G$ then, since G is abelian,

$$\alpha(ab) = (ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = \alpha(a)\alpha(b)$$

so that α is operation preserving. Therefore, α is an automorphism of G.

p 132, #12 Let $H = \mathbb{Z}_7$ and $G = \mathbb{Z}_9$. Since $|G| \neq |H|$, we know that $H \ncong G$. However

$$\mathrm{Aut}(\mathbb{Z}_7) \cong U(7) \cong \mathbb{Z}_6$$

and

$$\mathrm{Aut}(\mathbb{Z}_9) \cong U(9) \cong \mathbb{Z}_6$$

so that $\mathrm{Aut}(H) \cong \mathrm{Aut}(G)$.

p 134, #30 Let the mapping in question be denoted by s. That is, $s : G \to G$ is given by $s(g) = g^2$. Let $g, h \in G$. Since G is abelian we have

$$s(gh) = (gh)^2 = g^2h^2 = s(g)s(h)$$

which shows that s preserves operations. In order to show that s is an automorphism of G it remains to show that s is one-to-one and onto. Since G is finite, it suffices to show that s is one-to-one. So suppose that $g, h \in G$ and $s(g) = s(h)$. Then, by the definition of s, we have $g^2 = h^2$ or $g^2h^{-2} = e$. Again using the fact that G is abelian we have $(gh^{-1})^2 = e$. Since G has no element of order it must be that $gh^{-1} = e$. This implies that $g = h$, proving that s is one-to-one, completing the proof that s is an automorphism of G.

If we let $G = \mathbb{Z}$ then for any $n \in \mathbb{Z}$ we have $s(n) = 2n$, so that the image of s consists only of even integers. It follows that s is not onto and hence is not an automorphism of $\mathbb{Z}$.

Automorphism Exercise 1.

(b) Let $\phi \in \mathrm{Aut}_c(\mathbb{R})$. The proof given in Homework #7 (word for word) shows that $\phi(r) = r\phi(1)$ for all $r \in \mathbb{Q}$. Let $x \in \mathbb{R}$. Then there is a sequence $r_1, r_2, r_3, \dots$ of rational numbers so that $r_n \to x$ as $n \to \infty$. By the continuity of ϕ and what we've shown so far

$$\phi(x) = \lim_{n\to\infty} \phi(r_n) = \lim_{n\to\infty} r_n\phi(1) = \left(\lim_{n\to\infty} r_n\right)\phi(1) = x\phi(1)$$

which is what we needed to show.

(a) We use part (b) and the two step subgroup test. First of all, $\mathrm{Aut}_c(\mathbb{R}) \neq \emptyset$ since the identity function $1_{\mathbb{R}}(x) = x$ is a continuous automorphism of $\mathbb{R}$. Let $\phi, \psi \in \mathrm{Aut}_c(\mathbb{R})$. Since ϕ and ψ are both automorphisms of $\mathbb{R}$, we know that $\phi \circ \psi$ is also an automorphism of $\mathbb{R}$. Since the composition of continuous functions is continuous, we also know that $\phi \circ \psi$ is continuous. It follows that $\phi \circ \psi \in \mathrm{Aut}_c(\mathbb{R})$. We know that ϕ^{-1} is an automorphism of $\mathbb{R}$, but it remains to show that ϕ^{-1} is also continuous. By part (b), $\phi(x) = x\phi(1)$ and since ϕ is one-to-one, $\phi(1) \neq 0$. Therefore, ϕ^{-1} is given by

$$\phi^{-1}(x) = (\phi(1))^{-1}\, x$$

which we know is a continuous function on $\mathbb{R}$. It follows that $\phi^{-1} \in \mathrm{Aut}_c(\mathbb{R})$. Therefore, by the two-step subgroup test, $\mathrm{Aut}_c(\mathbb{R})$ is a subgroup of $\mathrm{Aut}(\mathbb{R})$.

(c) Given $\phi \in \mathrm{Aut}_c(\mathbb{R})$, we know that $\phi(1) \in \mathbb{R}^\times$ since ϕ is one-to-one and $\phi(0) = 0$. It follows that the function

$$F : \mathrm{Aut}_c(\mathbb{R}) \to \mathbb{R}^\times$$

defined by $F(\phi) = \phi(1)$ is well-defined. We claim that F is, in fact, an isomorphism.

If $\phi, \psi \in \mathrm{Aut}_c(\mathbb{R})$ and $F(\phi) = F(\psi)$ then $\phi(1) = \psi(1)$, by the definition of F. But, by part (b), this implies that for any $x \in \mathbb{R}$ we have

$$\phi(x) = x\phi(1) = x\psi(1) = \psi(x)$$

and so $\phi = \psi$. Hence, F is one-to-one.

Given $c \in \mathbb{R}^\times$, define $\phi(x) = cx$. Since $c \neq 0$, ϕ is easily seen to be one-to-one, onto and continuous. We also see that $\phi(x + y) = c(x + y) = cx + cy = \phi(x) + \phi(y)$ for any $x, y \in \mathbb{R}$. This shows that $\phi \in \mathrm{Aut}_c(\mathbb{R})$ and we see that

$$F(\phi) = \phi(1) = c \cdot 1 = c$$

which proves that F is onto.

Finally, if $\phi, \psi \in \mathrm{Aut}_c(\mathbb{R})$ then, by part (b) again,

$$F(\phi \circ \psi) = (\phi \circ \psi)(1) = \phi(\psi(1)) = \psi(1)\phi(1) = \phi(1)\psi(1) = F(\phi)F(\psi)$$

proving that F is operation preserving.

We conclude that F is an isomorphism and hence that $\mathrm{Aut}_c(\mathbb{R}) \cong \mathbb{R}^\times$.

Automorphism Exercise 2. We first show that $\hat{\phi}$ is well-defined, i.e. that given $f \in \text{Aut}(G)$ we have $\hat{\phi}(f) \in \text{Aut}(H)$. This is not difficult, but merits a quick argument. It is clear that $\phi \circ f \circ \phi^{-1}$ is a function from H to H and since ϕ, f and ϕ^{-1} are all one-to-one and onto, so is their composition. Finally, if $a, b \in H$ then, since ϕ, f and ϕ^{-1} preserve operations:

$$\begin{aligned}(\phi \circ f \circ \phi^{-1})(ab) &= \phi(f(\phi^{-1}(ab))) \\ &= \phi(f(\phi^{-1}(a)\phi^{-1}(b))) \\ &= \phi(f(\phi^{-1}(a))f(\phi^{-1}(b))) \\ &= \phi(f(\phi^{-1}(a)))\phi(f(\phi^{-1}(b))) \\ &= (\phi \circ f \circ \phi^{-1})(a)(\phi \circ f \circ \phi^{-1})(b).\end{aligned}$$

That is, $\phi \circ f\phi^{-1}$ preserves operations. Therefore $\hat{\phi}(f) = \phi \circ f \circ \phi^{-1} \in \text{Aut}(\mathbb{R})$, so that $\hat{\phi}$ is well-defined.

Now that we know that $\hat{\phi}$ is a well-defined function we proceed to show it is an isomorphism. Let $f, g \in \text{Aut}(G)$. If $\hat{\phi}(f) = \hat{\phi}(g)$ then $\phi \circ f \circ \phi^{-1} = \phi \circ g \circ \phi^{-1}$. Composing on the left by ϕ^{-1} and on the right by ϕ we find that $f = g$, so that $\hat{\phi}$ is one-to-one. Let $h \in \text{Aut}(H)$. Then, the argument used above shows that $f = \phi^{-1} \circ h \circ \phi \in \text{Aut}(G)$ (since $\phi^{-1} : H \to G$ is an isomorphism) and we see that

$$\hat{\phi}(f) = \phi \circ f \circ \phi^{-1} = \phi \circ \phi^{-1} \circ h \circ \phi \circ \phi^{-1} = h$$

so that $\hat{\phi}$ is also onto. Finally

$$\hat{\phi}(f \circ g) = \phi \circ f \circ g \circ \phi^{-1} = \phi \circ f \circ \phi^{-1} \circ \phi g \circ \phi^{-1} = \hat{\phi}(f) \circ \hat{\phi}(g)$$

proving that $\hat{\phi}$ is operation preserving.

Since $\hat{\phi} : \text{Aut}(G) \to \text{Aut}(H)$ is one-to-one, onto and preserves operations it is an isomorphism, i.e.

$$\text{Aut}(G) \cong \text{Aut}(H).$$

p 148, #2 Since $|H| = 4$ and $|S_4| = 4! = 24$, Lagrange's Theorem tells us that the number of left cosets of H in S_4 is

$$[S_4 : H] = \frac{|S_4|}{|H|} = \frac{24}{4} = 6.$$

p 148, #6 Let $a, b \in \mathbb{Z}$. Then $a + H = b + H$ if and only if $b - a \in H$ which is true if and only if $b - a$ is a multiple of n. That is, $a + H = b + H$ if and only if $a \bmod n = b \bmod n$. Since the remainders $\{0, 1, 2, 3, \ldots, n-1\}$ are all distinct mod$n$ and every integer mod$n$ is equal to exactly one of these, we see that there are n distinct (left) cosets of H in $\mathbb{Z}$ and they are

$$H, 1 + H, 2 + H, 3 + H, \ldots, (n-1) + H.$$

p 148, #8 If $|a| = 15$ then

$$|a^5| = \frac{15}{(15,5)} = \frac{15}{5} = 3.$$

Hence

$$[\langle a \rangle : \langle a^5 \rangle] = \frac{|\langle a \rangle|}{|\langle a^5 \rangle|} = \frac{15}{3} = 5.$$

Therefore $\langle a^5 \rangle$ has 5 cosets in $\langle a \rangle$ and it is easy to check that they are

$$\langle a^5 \rangle, a\langle a^5 \rangle, a^2\langle a^5 \rangle, a^3\langle a^5 \rangle, a^4\langle a^5 \rangle.$$

p 148, #10 Let H be any subgroup of G containing a and b. Since $|a|, |b| \neq 1$ are distinct and divide $|G| = 155$, Lagrange's Theorem implies, without loss of generality, that we must be in one of the following situations.

Case 1. $|a| = 155$. In this case $G = \langle a \rangle \leq H \leq G$ so that $H = G$ as desired.

Case 2. $|a| = 31$ and $|b| = 5$. Since the order of any element must divide the order of the group, it must be that 31 and 5 both divide $|H|$. Therefore 155, the least common multiple of 31 and 5, must divide $|H|$. Since $H \leq G$, we have

$$155 \leq |H| \leq |G| = 155$$

so that $|H| = 155$. It follows that $H = G$.

p 148, #14 Since $K < H$, Lagrange's Theorem implies that $42 = |K|$ divides (but does not equal) $|H|$. Since $H < G$, Lagrange's Theorem implies that $|H|$ divides (but does not equal) $420 = |G|$. Since $420 = 2 \cdot 5 \cdot 42$, the only possibilities for $|H|$ are

$$|H| = 84 \text{ or } 210.$$

p 148, #16 Let $n \geq 2$ be an integer and let $a \in \mathbb{Z}$. If $(a, n) = 1$ then we know that $(a \bmod n, n) = 1$ so that $a \bmod n \in U(n)$. Since $|U(n)| = \phi(n)$, the fourth corollary to Lagrange's Theorem implies that

$$a^{\phi(n)} \bmod n = (a \bmod n)^{\phi(n)} \bmod n = 1 \bmod n = 1.$$