Homework 9

MATH 301/601

Solutions to Graded Problems

Exercise 2. Let G be a finite abelian group of order n. Suppose $m \in \mathbb{N}$ is relatively prime to n. Prove that $\varphi\colon G \to G$ given by $\varphi(g) = g^m$ is an automorphism of G. (This says that every element of G has an m^{th}-root.)

Solution. We need to show that φ is bijective and that $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in G$. Let us consider the latter condition first. If $a, b \in G$, then

$$\begin{aligned} \varphi(ab) &= (ab)^m \\ &= (a^m)(b^m) \\ &= \varphi(a)\varphi(b), \end{aligned}$$

where the second equality is using the fact that G is abelian.

Now, since G is finite and both the domain and codomain of φ are G, we know that if φ is injective or surjective, then it is bijective. So, it is enough to show either injectivity or surjectivity; however, I will give an argument for each of three as reference.

First, let us consider injectivity. Let $a, b \in G$. If $\varphi(a) = \varphi(b)$, then $a^m = b^m$, implying that $a^m b^{-m} = e$. Using the standard exponent laws and the fact that G is abelian, we can rewrite this equation as $(ab^{-1})^m = e$. This equality, together with Lagrange's Theorem, tells us that $|ab^{-1}|$ divides m. Lagrange's Theorem also tells us that $|ab^{-1}|$ divides n. Now, as n and m are relatively prime, we can conclude that $|ab^{-1}| = e$, and hence $ab^{-1} = e$. Therefore, $a = b$, and φ is injective.

Next, let us consider surjectivity. Let $g \in G$. We must show that g is in the range of φ. As m and n are relatively prime, there exists $s, t \in \mathbb{Z}$ such that $1 = ms + nt$. Observe:

$$\begin{aligned} g &= g^1 \\ &= g^{ms+nt} \\ &= (g^s)^m (g^n)^t \\ &= (g^s)^m \\ &= \varphi(g^s), \end{aligned}$$

where the fourth equality uses the fact that $g^n = e$, as $n = |G|$. Hence, φ is surjective. $\square$

****Exercise 6.** Let $\mathbb{Q}$ denote the group $(\mathbb{Q}, +)$, and let $\mathbb{Q}^\times$ denote the group $(\mathbb{Q} \setminus \{0\}, \cdot)$.

(a) Let $\varphi\colon \mathbb{Q} \to \mathbb{Q}$ be an isomorphism. Prove that $\varphi(x) = x \cdot \varphi(1)$ for all $x \in \mathbb{Q}$. (This is saying that every automorphism of $\mathbb{Q}$ is $\mathbb{Q}$-linear.)

(b) Use part (a) to prove that if $\varphi\colon \mathbb{Q} \to \mathbb{Q}$ is an isomorphism, then there exists $q \in \mathbb{Q} \setminus \{0\}$ such that $\varphi(x) = qx$ for all $x \in \mathbb{Q}$.

(c) Use part (b) to prove that $\mathrm{Aut}(\mathbb{Q}) \cong \mathbb{Q}^\times$.

Solution.

(a) Let $\frac{a}{b} \in \mathbb{Q}$. Recall that $\mathbb{Q}$ is a group under addition. This means that $\varphi(nq) = n\varphi(q)$ for any $n \in \mathbb{Z}$. We can therefore write $\varphi(a/b) = a\varphi(1/b)$. And also,

$$b\varphi(1/b) = b\varphi(1/b) = \varphi(b \cdot 1/b) = \varphi(1),$$

and hence $\varphi(1/b) = \frac{1}{b}\varphi(1)$. Substituting back into the equation above yields $\varphi(a/b) = \frac{a}{b}\varphi(1)$, as desired.

(b) Let $q = \varphi(1)$. Part (1) immediately implies that $\varphi(x) = qx$. Moreover, as φ is an automorphism, we must have that $q \neq 0$.

(c) Given $q \in \mathbb{Q}^\times$, let $\varphi_q \in \mathrm{Aut}(\mathbb{Q})$ be defined by $\varphi_q(x) = qx$. Define $\Phi\colon \mathbb{Q}^\times \to \mathrm{Aut}(\mathbb{Q})$ by $\Phi(q) = \varphi_q$. We claim that Φ is an isomorphism. First, we see it is injective: if $\Phi(q) = \Phi(q')$, then $q = \varphi_q(1) = \varphi_{q'}(1) = q'$. Now, surjectivity follows from part (b): if $\varphi \in \mathrm{Aut}(\mathbb{Q})$, then there exists $q \in \mathbb{Q}^\times$ such that $\varphi = \varphi_q$, and hence $\varphi = \Phi(q)$. Finally, we need to check that $\Phi(qq') = \Phi(q) \circ \Phi(q')$ for all $q, q' \in \mathbb{Q}^\times$. Let $q, q \in \mathbb{Q}^\times$, and let $x \in \mathbb{Q}$. We compute:

$$\begin{aligned}
\Phi(qq')(x) &= \varphi_{qq'}(x) \\
&= (qq')x = q(q'x) \\
&= q\varphi_{q'}(x) \\
&= \varphi_q(\varphi_{q'}(x)) \\
&= (\varphi_q \circ \varphi_{q'})(x) \\
&= (\Phi(q) \circ \Phi(q'))(x),
\end{aligned}$$

and hence $\Phi(qq') = \Phi(q) \circ \Phi(q')$.

□