Math 453

Selected Solutions to Assignment 5

Problem 3: Prove of disprove the following:
(a) $\mathrm{Aut}\,(\mathbb{Z}_8)$ is abelian.
(b) $\mathrm{Aut}\,(\mathbb{Z}_8)$ is cyclic.

Solution: (A) This is true. Let G be a finite cyclic group; let g be a generator of G; let $\phi \in \mathrm{Aut}(G)$; and let $h \in G$. Since g is a generator of G, $h = g^{n_h}$ for some $n_h \in \mathbb{Z}$. Similarly, we have $\phi(g) = g^{n_\phi}$ for some $n_\phi \in \mathbb{Z}$. Since ϕ is a homomorphism, we have

$$\phi(h) = \phi(g^{n_h}) = (\phi(g))^{n_h} = (g^{n_\phi})^{n_h} = (g^{n_h})^{n_\phi} = h^{n_\phi}.$$

By the generality of ϕ and h, for each $\phi \in \mathrm{Aut}(G)$, there exists some $n_\phi \in \mathbb{Z}$ such that for all $h \in H$, $\phi(h) = h^{n_\phi}$.

Now, let $\phi, \psi \in \mathrm{Aut}(G)$, and let $h \in G$. Then

$$(\phi \circ \psi)(h) = \phi(h^{n_\psi}) = (h^{n_\psi})^{n_\phi} = (h^{n_\phi})^{n_\psi} = \psi(h^{n_\phi}) = (\psi \circ \phi)(h).$$

Hence, $\mathrm{Aut}(G)$ is abelian. Since $\mathbb{Z}_n$ is a finite cyclic group, $\mathrm{Aut}\,(\mathbb{Z}_8)$ is abelian.

(B) This is false. By Problem 4 below, the four elements of $\mathrm{Aut}\,(\mathbb{Z}_8)$ are defined by $\phi_1(1) = 1$, $\phi_3(1) = 3$, $\phi_5(1) = 5$, and $\phi_7(1) = 7$. Note that by problem 2, ϕ_1 is the identity, so $|\phi_1| = 1$. Also, note that $(\phi_3 \circ \phi_3)(1) = 1$, so $|\phi_3| = 2$; $(\phi_5 \circ \phi_5)(1) = 1$, so $|\phi_5| = 2$; and $(\phi_7 \circ \phi_7)(1) = 1$, so $|\phi_7| = 2$. Since $|\mathrm{Aut}\,(\mathbb{Z}_8)\,| = 4$, no element of $\mathrm{Aut}\,(\mathbb{Z}_8)$ generates $\mathrm{Aut}\,(\mathbb{Z}_8)$, so $\mathrm{Aut}\,(\mathbb{Z}_8)$ is not cyclic.

Problem 4: Compute the order of $\mathrm{Aut}\,(\mathbb{Z}_n)$.

Solution: Let G be a finite cyclic group; let $g \in G$ be a generator of G; and let $\phi \in \mathrm{Aut}(G)$. We claim that $\phi(g)$ is a generator of G. Let $h \in G$; since ϕ is surjective, there exists $c \in G$ such that $\phi(c) = h$; since g generates G, we have $g^{n_h} = c$ for some $n_h \in \mathbb{Z}$; and since ϕ is a homomorphism, we have

$$(\phi(g))^{n_h} = \phi(g^{n_h}) = \phi(c) = h.$$

Hence, $\phi(g)$ generates G. By the generality of g, we therefore have that an automorphism of G sends every generator to another generator.

Now, let $\phi, \psi \in \mathrm{Aut}(G)$. If $\phi = \psi$, then clearly $\phi(g) = \psi(g)$. On the other hand, suppose $\phi(g) = \psi(g)$, and let $k \in G$. Since g generates G, $k = g^{n_k}$ for some $n_k \in \mathbb{Z}$, so

$$\phi(k) = \phi(g^{n_k}) = (\phi(g))^{n_k} = (\psi(g))^{n_k} = \psi(g^{n_k}) = \psi(k).$$

By the generality of g, an automorphism of G is uniquely determined by its action on a generator.

By the above two paragraphs, we therefore have that the distinct automorphisms of a finite cyclic group $\mathbb{Z}_n$ for $n \in \mathbb{N}$ are precisely the number of unique generators of $\mathbb{Z}_n$. By a result from class, there are $\phi(n)$ unique generators of $\mathbb{Z}_n$. Hence, $|\mathrm{Aut}\,(\mathbb{Z}_n)\,| = \phi(n)$.

Problem 7 Let $f : G \to G'$ be an isomorphism. Prove that the orders of $g \in G$ and $f(g) \in G'$ are the same.

Solution: Let G, G' be groups, $g \in G$, and $f : G \to G'$ be an isomorphism. Suppose $n = |g| \in \mathbb{N}$. Then $g^n = e_G$; since f is a homomorphism, we have $e_{G'} = f(e_G) = f(g^n) = (f(g))^n$, so $|f(g)| \in \mathbb{N}$ and divides $n = |g|$.

On the other hand, suppose $n = |f(g)| \in \mathbb{N}$. Then again since f is a homomorphism, $f(g^n) = (f(g))^n = e_{G'}$; since f is injective, this implies $g^n = e_G$. Hence, $|g| \in \mathbb{N}$ and divides $n = |f(g)|$. Therefore, the orders of $g \in G$ and $f(g) \in G'$ are the same.