Tutorial 5

Problem 1. Let G, H be groups where $G = \langle g_1, \ldots, g_k \rangle$.

a) Let $\varphi, \psi : G \to H$ be isomorphisms. Show that $\varphi = \psi$ if $\varphi(g_i) = \psi(g_i)$ for all i. That is to say, an isomorphism is uniquely determined by what it maps the generators of a group to.

b) Suppose $\varphi : G \to H$ is a bijective map such that $o(g_i) = o(\varphi(g_i))$ for all i. [We know any isomorphism must have this property from Exercise 59.] Is φ necessarily an isomorphism? Prove it or give a counterexample.

Solution

a) Any element of G must be a product of exponents of $g_1, \ldots, g_k$, which φ and ψ send to the same product of exponents of $\varphi(g_1), \ldots, \varphi(g_k)$.

b) No: Consider the map $\varphi : G \to G, x \mapsto x^{-1}$. Then $o(x) = o(x^{-1}) = o(\varphi(x))$ for all $x \in G$, but we showed in PS2Q1 that this is not always an isomorphism.

Problem 2. Show that $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong U(n)$.

Solution

For any automorphism φ on $\mathbb{Z}/n\mathbb{Z}$, if $\varphi([1]) = [t]$, then Q1a) tells us that we must have

$$\varphi([a]) = \varphi([1]^a) = [t]^a = [at].$$

In particular, note that $o(\varphi([1])) = o([1]) = n$ means $[t]$ must be a generator of $\mathbb{Z}/n\mathbb{Z}$. That is, $[t]$ must be in $U(n)$.

On the other hand, suppose $[t] \in U(n)$. Then we may define $\varphi_{[t]}([k]) = [kt]$. This is a well-defined function [why?]. Since $[t]$ is a generator, the image of this map is $\langle t \rangle = \mathbb{Z}/n\mathbb{Z}$. Since the sets are finite and of same size, the map is automatically injective. We may check that

$$\varphi_{[t]}([a] + [b]) = \varphi_{[t]}([a+b]) = [t(a+b)] = [ta + tb] = [ta] + [tb] = \varphi_{[t]}([a]) + \varphi_{[t]}([b]).$$

Thus the set of automorphism is exactly $\varphi_{[t]}$ where $[t] \in U(n)$. A natural candidate for showing that this set is isomorphic to $U(n)$ is the map

$$f : U(n) \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}), [t] \mapsto \varphi_{[t]}.$$

We check that for any $r \in \mathbb{Z}/n\mathbb{Z}$,

$$\varphi_{[s]} \circ \varphi_{[t]}([r]) = \varphi_{[s]}(\varphi_{[t]}([r])) = \varphi_{[s]}([tr]) = [str] = \varphi_{[st]}(r)$$

So this map preserves the group structure. For bijectivity, note that both groups have order $\varphi(n)$ and the map is injective because $\varphi_{[s]}([1]) = [s] \neq \varphi_{[t]}([1]) = [t]$ for any $[s] \neq [t]$.

Problem 3. For this problem, we fix $n > 2$ and consider the group D_n. Let ψ be an automorphism on D_n.

a) Show that $\psi(r) = r^a$ for some a such that $\gcd(a, n) = 1$.

b) Show that $\psi(f) = fr^b$ for some b. That is, ψ cannot send f to a rotation.

c) Show that $o(\mathrm{Aut}(D_n)) = n\varphi(n)$.

Solution

a) We know $o(\psi(r)) = o(r) = n$, so ψ must send r to another element of order n. When $n > 2$, all elements or the form fr^i have order 2 and hence cannot be the image of r under ψ. Then r must be mapped to some rotation in $\langle r \rangle$, which is isomorphic to $\mathbb{Z}/n\mathbb{Z}$. From Q2, we know it must be mapped to some element of the form r^a with $\gcd(a, n) = 1$.

b) Note that $\psi(r)$ generates all of $\langle r \rangle$. So if f is also sent to a rotation, then $\psi(f) = \psi(r^k)$ for some k. Thus the map will not be injective and hence not an automorphism. As such, we must send f to another flip, meaning $\psi(f) = fr^b$ for some b.

c) From a) and b), we have that any automorphism ψ on D_n satisfies

$$\psi(r) = r^a \quad \text{and} \quad \psi(f) = fr^b,$$

for $\gcd(n, a) = 1$ and $0 \leq b \leq n - 1$. There are exactly $n\varphi(n)$ choices for k and i, so it remains to show that these choices all yield automorphisms.

From 1a), we know if ψ is an automorphism, then the values $\psi(r)$ and $\psi(f)$ uniquely determine that of ψ. then we know the value of ψ on any element of D_n by

$$\psi(f^i r^j) = (fr^b)^i (r^a)^j.$$

We claim that such a function is an isomorphism whenever $\gcd(k, n) = 1$. Clearly this map is surjective (the image contains a rotation r^k of order n and a flip fr^i, so they together generate D_n) between finite sets of same size and hence is bijective.

We will liberally use the relations $r^m f = fr^{-m}$ and $(fr^m)^2 = e$.

Case 1. Checking isomorphism law for two rotations.

$$\psi(r^i \cdot r^j) = \psi(r^{i+j}) = r^{a(i+j)} = r^{ai} r^{aj} = \psi(r^i)\psi(r^j).$$

Case 2. Checking isomorphism law for rotation followed by a flip.

$$\begin{aligned}\psi(r^i \cdot fr^j) &= \psi(fr^{j-i}) = (fr^b)r^{a(j-i)} = fr^{b-ai}r^{aj} = fr^{-ai}r^b r^{aj} \\ &= r^{ai}fr^b(r^{aj}) = (r^{ai})(fr^b r^{aj}) = \psi(r^i)\psi(fr^j).\end{aligned}$$

Case 3. Checking isomorphism law for flip followed by a rotation.

$$\psi(fr^i \cdot r^j) = \psi(fr^{i+j}) = (fr^b)r^{a(j+i)} = (fr^b r^{ai})(r^{aj}) = \psi(fr^i)\psi(r^j).$$

Case 4. Checking isomorphism law for two flips.

$$\begin{aligned}\psi(fr^i \cdot fr^j) &= \psi(f^2 r^{j-i}) = \psi(r^{j-i}) = r^{a(j-i)} = r^{-ai}r^{aj} \\ &= r^{-ai}(fr^b)^2 r^{aj} = (r^{-ai}fr^b)((fr^b)r^{aj}) = (fr^{ai}r^b)((fr^b)r^{aj}) \\ &= (fr^{ai+b})((fr^b)r^{aj}) = ((fr^b)r^{ai})((fr^b)r^{aj}) \\ &= \psi(fr^i)\psi(fr^j).\end{aligned}$$