PMATH 336: INTRODUCTION TO GROUP THEORY WITH APPLICATIONS
NOTES FOR WEEK 5

INSTRUCTOR: ARUNDHATHI KRISHNAN

6. Isomorphisms

6.1. Definition and examples of isomorphisms.

Definition 6.1.1. A homomorphism φ from a group G equipped with a product $\cdot$ to another group $\overline{G}$ with product $\star$ is a mapping that preserves the group operation. i.e.,

$$\varphi(a \cdot b) = \varphi(a) \star \varphi(b), \ \forall a, b \in G.$$

While we have explicitly written the symbols for the products in G and $\overline{G}$ above, we often will simply write $\varphi(ab) = \varphi(a)\varphi(b)$, where it is understood that the product of a and b on the left hand side is in G and the product of $\varphi(a)$ and $\varphi(b)$ on the right is in $\overline{G}$.

We will have more to say about homomorphisms later, but at the moment we will discuss a special kind of homomorphism called an isomorphism.

Definition 6.1.2. An isomorphism from a group G to a group $\overline{G}$ is a homomorphism which is one-to-one and onto. In this case, we say that the groups G and $\overline{G}$ are *isomorphic* and write $G \cong \overline{G}$.

We note that it is implicit in the existence of a bijection (which is also multiplicative) between G and $\overline{G}$ that G and $\overline{G}$ have the same order. Let us reiterate that to prove that two groups are isomorphic, we must show the existence of a well-defined function between the two sets, which is bijective and preserves the group structure.

We will consider some examples, and show what we promised when looking at cyclic groups, namely that cyclic groups can be completely characterized up to isomorphism.

Example 6.1.3.

(i) Let G be the group of real numbers with addition and $\overline{G}$ be the set of positive real numbers with multiplication. Then G and $\overline{G}$ are isomorphic under the mapping $\varphi(x) = 2^x$. Let us check that φ is indeed an isomorphism. First $\varphi(x+y) = 2^{x+y} = 2^x 2^y = \varphi(x)\varphi(y)$ so it is indeed a group homomorphism. Suppose $2^x = 2^y$, then $\log_2 2^x = \log_2 2^y$ so that $x = y$. Hence φ is injective. Finally, that it is surjective follows by noting that for every positive real number y, $x = \log_2(y)$ is the pre-image of y under φ.

(ii) A cyclic group of infinite order is isomorphic to $\mathbb{Z}$. Let $G = \langle a \rangle$. Define $\varphi : G \to \mathbb{Z}$ by $\phi(a^k) = k$. Then φ is well-defined (check this!) and an isomorphism as the following hold:
   (a) $\varphi(a^k a^l) = \varphi(a^{k+l}) = k + l = \varphi(a^k) + \varphi(a^l)$, so φ is a homomorphism (recall that the group operation in $\mathbb{Z}$ is addition!);
   (b) $\varphi(a^k) = \varphi(a^l) \implies k = l \implies a^k = a^l$, so φ is injective;
   (c) For each $k \in \mathbb{Z}$, the element $a^k \in G$ is mapped to k under φ, so φ is surjective.

(iii) A finite cyclic group $\langle a \rangle$ of order n is isomorphic to $\mathbb{Z}_n$ under the mapping $\varphi(a^k) = k \mod n$. The mapping φ is well-defined because $a^k = a^l$ in a cyclic group of order n implies that n divides $k - l$. It is an isomorphism as the following hold:
  (a) $\varphi(a^k a^l) = \varphi(a^{k+l}) = k + l \mod n = k \mod n + l \mod n = \varphi(a^k) + \varphi(a^l)$, so φ is a homomorphism (recall that the group operation in $\mathbb{Z}_n$ is addition mod n);
  (b) $\varphi(a^k) = \varphi(a^l) \implies k \mod n = l \mod n \implies n|(k - l)$, so by Theorem 4.1.3, $a^k = a^l$. Hence φ is injective;
  (c) For each $k \in \mathbb{Z}_n$, the element $a^k \in G$ is mapped to k under φ, so φ is surjective.

(iv) $U(10)$ and $U(5)$ are both isomorphic to $\mathbb{Z}_4$. Recall that $U(10) = \{1, 3, 7, 9\} = \langle 3 \rangle$ and $U(5) = \{1, 2, 3, 4\} = \langle 3 \rangle$, so both groups are cyclic of order 4 and hence isomorphic to $\mathbb{Z}_4$ by (iii).

(v) Let $G = SL(2, \mathbb{R})$, the simple linear group of 2×2 real matrices with determinant equal to 1. Let $M \in SL(2, \mathbb{R})$ and define φ_M from G to itself by $\varphi_M(A) = MAM^{-1}$ for $A \in G$. As the determinant is multiplicative, MAM^{-1} does indeed belong to G for each $A \in G$. We will show that φ_M is indeed an isomorphism of G into itself.
  (a) $\varphi_M(AB) = MABM^{-1} = MAM^{-1}MBM^{-1} = \varphi_M(A)\varphi_M(B)$, so φ_M is a group homomorphism.
  (b) Suppose $\varphi_M(A) = \varphi_M(B)$. Then $MAM^{-1} = MBM^{-1}$, so $A = B$ follows by left and right cancellation. So φ_M is one-to-one.
  (c) Let $B \in G$. Then $A = M^{-1}BM \in G$ and $\varphi_M(A) = MM^{-1}BMM^{-1} = B$, so φ is onto.

  The mapping φ_M is called *conjugation* by M.

Let us now consider some non-examples.

Example 6.1.4.

(i) The mapping from $\mathbb{R}$ with addition to itself given by $\varphi(x) = x^3$ is not an isomorphism. φ is one-to-one and onto but not a group homomorphism as it is not true that $(x + y)^3 = x^3 + y^3$ for all $x, y \in \mathbb{R}$.

(ii) Two groups of the same order need not be isomorphic. For example, consider $U(10) = \{1, 3, 7, 9\}$ and $U(12) = \{1, 5, 7, 11\}$ both of which are of order 4. Note that $U(10)$ is cyclic with generators 3 and 7, but $U(12)$ is not cyclic. In fact, for each $x \in U(12)$, $x^2 = 1$. Suppose that φ is a group homomorphism from $U(10)$ onto $U(12)$. Then

$$\varphi(9) = \varphi(3 \cdot 3) = \varphi(3)\varphi(3) = 1,$$

and

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

as the square of *every* element in $U(12)$ is 1. But this means φ cannot be injective. So $U(10) \ncong U(12)$. Indeed, we will show in Theorem 6.3.2 that if two groups are isomorphic and one is cyclic, then the other must also be cyclic. This condition is of course not satisfied in this example.

(iii) There is no isomorphism from $\mathbb{Q}$, the group of rational numbers with addition, to $\mathbb{Q}^*$, the group of non-zero rational numbers under multiplication. If φ were a group isomorphism from $\mathbb{Q}$ onto $\mathbb{Q}^*$, there would exists some rational number a such that $\varphi(a) = -1$. Then

$$-1 = \varphi(a) = \varphi(\frac{a}{2} + \frac{a}{2}) = \varphi(\frac{a}{2})\varphi(\frac{a}{2}) = \left(\varphi(\frac{a}{2})\right)^2.$$

However, the square of a rational number cannot be equal to -1.

6.2. **Cayley's Theorem.** The main goal of this week is to show that any group is isomorphic to a permutation group. This is known as Cayley's theorem. It gives a concrete realization of *any* group as a group of permutations.

Theorem 6.2.1 (Cayley's Theorem)**.** *Every group is isomorphic to a group of permutations.*

Proof. Let G be a group. For $g \in G$, define $L_g : G \to G$ by

$$L_g(x) = gx, \ \forall x \in G.$$

That is, for each $g \in G$, L_g is the function of left multiplication by g on G. Then L_g is a permutation on G, that is, it is a one-to-one, onto mapping from G to itself. Verify that each L_g is actually bijective!

Let $\overline{G} = \{L_g \mid g \in G\}$. We will define an operation on $\overline{G}$ that makes it a group. As $\overline{G}$ is a set consisting of functions, the obvious operation to define on it is function composition. We will show that $\overline{G}$ is indeed a group with this operation.

- For $g, h \in G$, $L_g L_h(x) = L_g(hx) = g(hx) = (gh)x = L_{gh}x$. Hence function composition is a binary operation on $\overline{G}$, that is, $\overline{G}$ is closed under the operation of function composition.
- Let $g, h, k \in G$. Then $L_g(L_h L_k) = (L_g L_h)L_k$ follows by associativity of function composition.
- L_e is the identity element of $\overline{G}$, where e is the identity of G.
- For each $g \in G$, $L_{g^{-1}}$ is the inverse of L_g.

Hence we have shown that $\overline{G}$ is a group. We will now show that there exists an isomorphism φ from G onto $\overline{G}$. Define $\varphi : G \to \overline{G}$ in the obvious way as

$$\varphi(g) = L_g, \ g \in G.$$

We will complete our proof by showing that φ is indeed an isomorphism. We have already shown that $L_{gh} = L_g L_h$, so that $\varphi(gh) = \varphi(g)\varphi(h)$. Suppose $L_g = L_h$. Then in particular, $L_g(e) = L_h(e)$, so that $ge = he$, that is, $g = h$. Hence φ is one-to-one. By the definition of $\overline{G}$, it is clear that φ is onto. Hence we have shown that G is isomorphic to the group $\overline{G}$ of permutations of left multipliers on G. $\overline{G}$ is called the left regular representation of G. □

6.3. **Properties of Isomorphisms.**

Theorem 6.3.1. *Suppose that φ is an isomorphism from a group G onto a group $\overline{G}$ with identity elements denoted by e_G and $e_{\overline{G}}$ respectively. Then the following properties hold.*

(i) φ carries the identity of G to $\overline{G}$, that is, $\varphi(e_G) = e_{\overline{G}}$.
(ii) For each $n \in \mathbb{Z}$ and $a \in G$, $\varphi(a^n) = (\varphi(a))^n$. In particular, $\varphi(a^{-1}) = \varphi(a)^{-1}$.
(iii) For $a, b \in G$, $ab = ba$ if and only if $\varphi(a)\varphi(b) = \varphi(b)\varphi(a)$.
(iv) $G = \langle a \rangle$ if and only if $\overline{G} = \langle \varphi(a) \rangle$.
(v) $|\, a \,| = |\, \varphi(a) \,|$ for all $a \in G$.
(vi) For $k \in \mathbb{Z}$ and $b \in G$, the equation $x^k = b$ has the same number of solutions in G as does the equation $y^k = \varphi(b)$ in $\overline{G}$.
(vii) If $|\, G \,|$ is finite, then G and $\overline{G}$ have exactly the same number of elements of every order.

Proof. (i) $e_{\overline{G}}\varphi(e_G) = \varphi(e_G) = \varphi(e_G \cdot e_G) = \varphi(e_G)\varphi(e_G)$. By cancellation, $\varphi(e_G) = e_{\overline{G}}$.

(ii) For positive integers $n \in \mathbb{N}$, we prove $\varphi(a^n) = \varphi(a)^n$ by induction. Of course, the result is true for $n = 1, 2$. Suppose it is true for $k \in \mathbb{N}$, that is, $\varphi(a^k) = \varphi(a)^k$. Then $\varphi(a^{k+1}) = \varphi(a^k a) = \varphi(a^k)\varphi(a) = \varphi(a)^k\varphi(a) = \varphi(a)^{k+1}$. For $n = 0$, we already

have the equality $\varphi(e_G) = e_{\overline{G}}$. For $n < 0$, note that $e_{\overline{G}} = \varphi(e_G) = \varphi(a^n a^{-n}) = \varphi(a^n)\varphi(a^{-n}) = \varphi(a^n)\varphi(a)^{-n}$ by the observation for the positive integer case. Hence $\varphi(a^n) = \varphi(a)^n$ in this case also.

(iii) $ab = ba \iff \varphi(ab) = \varphi(ba) \iff \varphi(a)\varphi(b) = \varphi(b)\varphi(a)$ by the injectivity and multiplicativity of φ.

(iv) Suppose $G = \langle a \rangle$, then certainly $\langle \varphi(a) \rangle \leq \overline{G}$. On the other hand, for any $\overline{g} \in \overline{G}$, there exists $g \in G = \langle a \rangle$ such that $\varphi(g) = \overline{g}$. The element g must be of the form a^k for some $k \in \mathbb{Z}$, hence $\overline{g} = \varphi(a^k) = \varphi(a)^k \in \langle \varphi(a) \rangle$.

The converse implication- that if $\overline{G}$ is cyclic, then so is G- is left as an exercise.

(v) If $\varphi(a)^m = e_{\overline{G}}$ for $m \in \mathbb{N}$ and m is the smallest such positive integer, then $\varphi(a^m) = e_{\overline{G}} = \varphi(e_G)$ so that $a^m = e_G$ by injectivity of φ. Suppose $a^k = e_G$ for some smaller positive integer than m, then $\varphi(a)^k = e_{\overline{G}}$, a contradiction. Hence $| a | = | \varphi(a) |$.

(vi) Suppose $g^k = b$ for some $g \in G$, then $\varphi(g)^k = \varphi(g^k) = \varphi(b)$, so that $\varphi(g)$ is a solution of the equation $y^k = \varphi(b)$ in $\overline{G}$. Conversely, if $\overline{g}^k = \varphi(b)$ and let $g \in G$ be the unique pre-image of $\overline{g}$ under φ. Then $\varphi(g^k) = \varphi(g)^k = \overline{g}^k = \varphi(b)$, so that $g^k = b$ by injectivity.

(vii) This follows by (v).

□

The failure of one of the above properties can be used to show that certain groups are not isomorphic. For example, $\mathbb{C}^*$ and $\mathbb{R}^*$, non-zero complex and real numbers respectively with multiplication, can be seen to be non-isomorphic as the equation $x^4 = 1$ has four solutions in $\mathbb{C}^*$ but only two in $\mathbb{R}^*$.

Theorem 6.3.2. *Suppose that φ is an isomorphism from a group G onto a group $\overline{G}$. Then*

(i) φ^{-1} is an isomorphism from $\overline{G}$ onto G.
(ii) G is Abelian if and only if $\overline{G}$ is Abelian.
(iii) G is cyclic if and only if $\overline{G}$ is cyclic.
(iv) If K is a subgroup of G, then $\varphi(K) = \{\varphi(k) \mid k \in K\}$ is a subgroup of $\overline{G}$.
(v) If $\overline{K}$ is a subgroup of $\overline{G}$, then $\varphi^{-1}(\overline{K}) = \{g \in G \mid \varphi(g) \in \overline{K}\}$ is a subgroup of G.
(vi) $\varphi(Z(G)) = Z(\overline{G})$.

Proof. (i) We show that φ^{-1} is a group homomorphism. Let $x, y \in \overline{G}$. Then there exist $a, b \in G$ such that $x = \varphi(a), y = \varphi(b)$. Hence $\varphi^{-1}(xy) = \varphi^{-1}(\varphi(a)\varphi(b)) = \varphi^{-1}(\varphi(ab)) = ab = \varphi^{-1}(x)\varphi^{-1}(y)$. It is left as an exercise to show that φ^{-1} is a bijection.

(ii) This follows from (iii) of Theorem 6.3.1.

(iii) This follows from (iv) of Theorem 6.3.1.

(iv) Clearly $e_{\overline{G}} = \varphi(e_G) \in \varphi(K)$ so $\varphi(K)$ is non-empty. Suppose $\varphi(k_1), \varphi(k_2) \in \varphi(K)$, then $\varphi(k_1)\varphi(k_2)^{-1} = \varphi(k_1 k_2^{-1}) \in \varphi(K)$ as $k_1 k_2^{-1} \in K$. Hence $\varphi(K)$ is a subgroup.

(v) This follows from (i) and (iv).

(vi) This follows from (iii) of Theorem 6.3.1.

□

6.4. **Automorphisms.**

Definition 6.4.1. An isomorphism from a group G onto itself is called an automorphism.

Example 6.4.2. Define $\varphi : \mathbb{C} \to \mathbb{C}$ by $\varphi(a + bi) = a - bi$, where $\mathbb{C}$ is the set of complex numbers with addition. Then φ is an automorphism.

Definition 6.4.3. Let G be a group and $a \in G$. The function φ_a defined on G by $\varphi_a(g) = aga^{-1}$ for all $g \in G$ is called the inner automorphism of G induced by a.

Actually, we have already seen an example of an inner automorphism via the conjugation mapping in (v) of Example 6.1.3.

Exercise 6.4.4. Prove that an inner automorphism of a group is actually an automorphism.

Example 6.4.5. Let us consider the example of an inner automorphism induced by r_1 (rotation counterclockwise by $\frac{\pi}{2}$) in D_4, the dihedral group of order 8. Recall that $r_1^{-1} = r_3$. We get the following:

x	$\overset{\varphi_{r_1}}{\mapsto}$	$r_1 x r_1^{-1}$
r_0	$\overset{\varphi_{r_1}}{\mapsto}$	$r_1 r_0 r_1^{-1} = r_1 r_0 r_3 = r_0$
r_1	$\overset{\varphi_{r_1}}{\mapsto}$	$r_1 r_1 r_1^{-1} = r_1$
r_2	$\overset{\varphi_{r_1}}{\mapsto}$	$r_1 r_2 r_1^{-1} = r_1 r_2 r_3 = r_2$
r_3	$\overset{\varphi_{r_1}}{\mapsto}$	$r_1 r_3 r_1^{-1} = r_1 r_3 r_3 = r_3$
s_0	$\overset{\varphi_{r_1}}{\mapsto}$	$r_1 s_0 r_1^{-1} = r_1 s_0 r_3 = s_2$
s_1	$\overset{\varphi_{r_1}}{\mapsto}$	$r_1 s_1 r_1^{-1} = r_1 s_1 r_3 = s_3$
s_2	$\overset{\varphi_{r_1}}{\mapsto}$	$r_1 s_2 r_1^{-1} = r_1 s_2 r_3 = s_0$
s_3	$\overset{\varphi_{r_1}}{\mapsto}$	$r_1 s_3 r_1^{-1} = r_1 s_3 r_3 = s_1$

Notation 6.4.6. The set of automorphisms of a group G is denoted by $\mathrm{Aut}(G)$ and the set of inner automorphisms by $\mathrm{Inn}(G)$.

Theorem 6.4.7. *For a group G, $\mathrm{Aut}(G)$ and $\mathrm{Inn}(G)$ are groups under the operation of function composition.*

Proof. We prove the theorem for inner automorphisms. The automorphism case is left as an exercise. Suppose φ_a, φ_b are inner automorphisms induced by $a, b \in G$. Then $\varphi_a\varphi_b(x) = \varphi_a(bxb^{-1}) = a(bxb^{-1})a^{-1} = (ab)x(ab)^{-1} = \varphi_{ab}(x)$, that is, the inner automorphism induced by ab. Hence we have closure of the set under the given operation. Associativity follows by the associativity of composition of functions. Clearly, φ_e is the identity, and the inverse of φ_a is $\varphi_{a^{-1}}$. □

Example 6.4.8.

(i) We compute $\mathrm{Inn}(D_4)$. On first glance, $\mathrm{Inn}(D_4) = \{\varphi_{r_0}, \varphi_{r_1}, \varphi_{r_2}, \varphi_{r_3}, \varphi_{s_0}, \varphi_{s_1}, \varphi_{s_2}, \varphi_{s_3}\}$, but we will go through the list to ensure that there are no repetitions.

Let us write the multiplication table for D_4 to make this a little easier.

	r_0	r_1	r_2	r_3	s_0	s_1	s_2	s_3
r_0	r_0	r_1	r_2	r_3	s_0	s_1	s_2	s_3
r_1	r_1	r_2	r_3	r_0	s_1	s_2	s_3	s_0
r_2	r_2	r_3	r_0	r_1	s_2	s_3	s_0	s_1
r_3	r_3	r_0	r_1	r_2	s_3	s_0	s_1	s_2
s_0	s_0	s_3	s_2	s_1	r_0	r_3	r_2	r_1
s_1	s_1	s_0	s_3	s_2	r_1	r_0	r_3	r_2
s_2	s_2	s_1	s_0	s_3	r_2	r_1	r_0	r_3
s_3	s_3	s_2	s_1	s_0	r_3	r_2	r_1	r_0

Our first observation is that for any $y \in Z(G)$, $\varphi_y = \varphi_{r_0}$ which is the identity automorphism. Note from the table that $r_0, r_2 \in Z(D_4)$. Hence $\varphi_{r_2} = \varphi_{r_0}$. Also, $\varphi_{r_3}(x) = r_3 x r_3^{-1} = r_1 r_2 x r_2^{-1} r_1^{-1} = r_1 x r_1^{-1} = \varphi_{r_1}(x)$. Similarly, as $s_0 = r_2 s_2$ and $s_1 = r_2 s_3$, we have $\varphi_{s_0} = \varphi_{s_2}$ and $\varphi_{s_1} = \varphi_{s_3}$, so we are now left with only $\varphi_{r_0}, \varphi_{r_1}, \varphi_{s_0}, \varphi_{s_1}$. We claim that these are distinct maps. As an exercise, for each pair of inner automorphisms from $\{\varphi_{r_0}, \varphi_{r_1}, \varphi_{s_0}, \varphi_{s_1}\}$, find $y \in D_4$ such that the two automorphisms differ on y. For example, for φ_{r_1} and φ_{s_1} choose $y = r_1$ as $s_1 r_1 s_1^{-1} = s_1 r_1 s_1 = s_1 s_2 = r_3$, whereas $r_1 r_1 r_1^{-1} = r_1$, so that $\varphi_{r_1}(r_1) \neq \varphi_{s_1}(r_1)$.

(ii) We now show how to compute $\mathrm{Aut}(\mathbb{Z}_{10})$. Let $\alpha \in \mathrm{Aut}(\mathbb{Z}_{10})$. Then by the group homomorphism property, α is completely determined by its value at 1, as $\alpha(l) = \alpha(l(1)) = l\alpha(1)$. As 1 is an element of order 10, by (v) of Theorem 6.3.1, for α to be an isomorphism, $\alpha(1)$ must also be an element of order 10. By Corollary 4.1.10 applied to $\mathbb{Z}_{10}$, we have $|\, k \,| = |\, 1 \,| = 10$ if and only if $\gcd(10, k) = 1$, hence $k = 1, 3, 7$ or 9. Hence we can choose $\alpha(1)$ to be one of these four possible values. Depending on our choice, let us denote the corresponding mappings by $\alpha_1, \alpha_3, \alpha_7$ or α_9. we will now show that each of these mappings α_k is indeed an automorphism.

As $\alpha_1(k) = k\alpha_1(1) = k$, α_1 is the identity automorphism. What about the remaining α_k? For each k, $x \mod 10 \equiv y \mod 10 \implies kx \mod 10 \equiv ky \mod 10$ as $\gcd(k, 10) = 1$. Hence each α_k is well-defined. It is clearly a group homomorphism as $\alpha_k(a+b) = k(a+b) \mod 10 = ka + kb \mod 10 = \alpha_k(a) + \alpha_k(b) \mod 10$. As k is a generator of $\mathbb{Z}_{10}$ for each k with $\gcd(k, 10) = 1$ (again, by Corollary 4.1.10), each α_k is onto. Why is it one-to-one? Suppose $\alpha_k(a) = \alpha_k(b)$, then $ka \equiv kb \mod 10$ which implies 10 divides $k(b-a)$. But $\gcd(k, 10) = 1 \implies 10|(b-a)$ so $a \equiv b \mod 10$.

Now that we have determined the set $\mathrm{Aut}(\mathbb{Z}_{10})$, let us write its multiplication table:

	α_1	α_3	α_7	α_9
α_1	α_1	α_3	α_7	α_9
α_3	α_3	α_9	α_1	α_7
α_7	α_7	α_1	α_9	α_3
α_9	α_9	α_7	α_3	α_1

This table probably looks familiar. Indeed we have $\alpha_{k_1}\alpha_{k_2} = \alpha_{k_1 k_2 \mod 10}$ for each k_1, k_2. It is in fact exactly in parallel to the multiplication table of $U(10)$. This is not a coincidence, and we tackle this in the next theorem.

Theorem 6.4.9. *For each $n \in \mathbb{N}$, $\mathrm{Aut}(\mathbb{Z}_n)$ is isomorphic to $U(n)$.*

Proof. Any automorphism α is determined by the value of $\alpha(1)$. As $\alpha(1)$ must have order equal to the order of 1 which is n, it can take values in $U(n)$ by Corollary 4.1.10. Define the map $T : \mathrm{Aut}(\mathbb{Z}_n) \to U(n)$ by $T(\alpha) = \alpha(1)$. As α is uniquely determined by $\alpha(1)$, T is a one-to-one mapping.

To prove that T is onto, let $k \in U(n)$. Let $\alpha_k \in \mathrm{Aut}(\mathbb{Z}_n)$ be the map such that $\alpha_k(1) = k$ (it is an automorphism for the reason outlined in Example 6.4.8 (ii)). Then of course $T(\alpha_k) = k$.

Finally, we show that T is a group homomorphism. Let $\alpha, \beta \in \mathrm{Aut}(\mathbb{Z}_n)$. Then

$$\begin{aligned} T(\alpha\beta) &= \alpha\beta(1) = \alpha\underbrace{(1+1+\cdots+1)}_{\beta(1) \text{ times}} \\ &= \underbrace{\alpha(1)+\alpha(1)+\cdots+\alpha(1)}_{\beta(1) \text{ times}} = \alpha(1)\beta(1) \\ &= T(\alpha)T(\beta). \end{aligned}$$

□

References

[1] Chapter 6. Gallian, Joseph. Contemporary abstract algebra. Nelson Education, 2012.