# DERIVATION OF THE CYCLE INDEX FORMULA OF THE AFFINE $(p)$ GROUP AS A SEMIDIRECT PRODUCT OF THE CYCLIC GROUPS $C_p$ AND $C_{p-1}$

**Geoffrey Ngovi Muthoka**
Department of Pure and Applied Sciences
Kirinyaga University P.O. Box 143-10300 Kerugoya-Kenya Corresponding author
+254723 387 621

**Ireri Kamuti**
Department of Mathematics and Actuarial Sciences
Kenyatta University P.O. Box 43844-00100, Nairobi-Kenya

**Mutie Kavila**
Department of Mathematics and Actuarial Sciences
Kenyatta University P.O. Box 43844-00100, Nairobi-Kenya

**Abstract**

*In this paper, we derive the cycle index formula of an affine*$(p)$ *group acting on the* $p$ *elements of the field* $\mathbb{Z}_p$*.The resulting cycle index is given as;*$Z_{(G,X)} = \frac{1}{|G|}\left(t_1^p + (p-1)t_p + p\sum_{\substack{d|(p-1)\\ d\neq 1}} \emptyset(d)t_1 t_d^{\frac{p-1}{d}}\right)$*.We further express the resulting cycle in terms of the cycle index formula of*$C_p = \{x + b \text{ where } b \in \mathbb{Z}_p\}$ *and the cycle index formula of* $C_{p-1} = \{ax \text{ where } 0 \neq a \in \mathbb{Z}_p\}$ *which the affine(p) group is a semi-direct product of. We also use the resulting cycle index formulas to solve some examples.*

**Keywords:** Affine$(p)$ group, Cycle Index and Semi-direct product group.

## 1. Introduction

A geometrical substructure of the Euclidean space which generalizes some of the properties of the Euclidean space such that it's independent of the concepts of distance and measure of angles but maintains the properties related to parallelism and ratio of lengths for parallel line segments is referred to as an affine space.An affine transformation is a function from an affine space to another affine space which preserves points, straight lines and planes.

The set of all invertible affine transformations from an affine space onto itself form a group $G$ over an affine space called the affine group. The set $C_p = \{x + b \text{ where } b \in \mathbb{Z}_p\}$ (translations) form a normal cyclic subgroup of the affine group under addition of order $p$, the set $C_{p-1} = \{ax \text{ where } 0 \neq a \in \mathbb{Z}_p\}$ form a cyclic group under multiplication and the affine group is a semi direct of the two.

In this case the Affine (p) group can be written as $Aff(p) = C_p \rtimes C_{p-1}$ since the Affine(p) group is a semi direct product of the two subgroups.

## 2. preliminary results

**Definition 2.1**

If a finite group $G$ acts on a set $X$, $|X| = n$, and $g \in G$ has cycle type $(\alpha_1, \alpha_2, \dots, \alpha_n)$, we define the monomial of $g$ to be $mon(g) = t_1^{\alpha_1} t_2^{\alpha_2} \dots t_n^{\alpha_n}$,where $t_1, t_2, \dots, t_n$ are distinct

**Definition 2.2**

The cycle index of the action of $G$ on $X$ is the polynomial (say over the rational field Q) in $t_1, t_2, \dots, t_n$ given by; $Z(G) = Z_{G,X}(t_1, t_2, \dots t_n) = \frac{1}{|G|}\sum_{g \in G}\{mon(g)\}$.

Note that if G has conjugacy classes $K_1, K_2, \dots, K_m$ with $g_i \in K_i$ then $Z(G) = \frac{1}{|G|}\sum_{i=1}^{m}|K_i| mon(g_i)$

.**Definition 2.3**

A group $G$ is said to be a semi-direct product group of $N$ by $H$ if;

i) $N \lhd G$ and $H < G$

ii) $N \cap H = \{e\}$

iii) $NH = G$

and we symbolically express this as $G = N \rtimes H$.

**Theorem 2.1**

The Möbius function of any $n \in N$ is given by,

$$\mu(n) = \begin{cases} -1 & \text{if n is a square free with an odd number of prime factors} \\ 0 & \text{if n has a squared prime factor} \\ 1 & \text{if n is a square free with an even number of prime factors} \end{cases}$$

**Theorem 2.2**

Let $x$ be a permutation with cycle type $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n$ then:

(i) The number $\pi(x^l)$ of cycles of length one in $x^l$ is $\sum_{i|l} i\,\alpha_i$

(ii) $\alpha_l = \frac{i}{l}\sum_{i|l}\pi\left(x^{\frac{i}{i}}\right)\mu(i)$ where $\mu$ is the Möbius function.

(iii)

## 3. Main Results

**Theorem 3.1**

Let $p$ be a prime, the cycle index formula of the affine$(p)$ group acting on the $p$ elements of $Z_p$ is given by;

$$Z_{(G,X)} = \frac{1}{|G|}\left(t_1^p + (p-1)t_p + p\sum_{\substack{d|(p-1)\\ d\neq 1}} \emptyset(d) t_1 t_d^{\frac{p-1}{d}}\right)$$

Where$|G| = p(p-1)$, $\emptyset(d)$ is the Euler's phi function and $X$ the $p$ elements of the $Z_p$group.

**Proof**

The elements of the $Aff(p)$ group are partitioned into $I, \tau_1$ (the set of elements that fix one element on the field$Z_p$) and $\tau_0$ (the set of elements that do not fix any element of $Z_p$). To derive the cycle index formula we need to find the number of $\tau_0$ and $\tau_1$ elements and the respective cycle types.

Let $g \in \tau_1$, then $C_G(g) = C_{p-1}$

$\Rightarrow |C^g| = \frac{p(p-1)}{(p-1)} = p$ ………………...…………… 3.1.1

Where $C^g$ is the conjugacy class in $G$ containing $g$.

Let $g \in \tau_0$, then $C_G(g) = C_p$

$\Rightarrow |C^g| = \frac{p(p-1)}{p} = p-1$ ………………...…………… 3.1.2

$N_G(C_{p-1}) = C_{p-1}$ Implying there are $\frac{p(p-1)}{(p-1)} = p$ conjugate cyclic groups $C_{p-1}$ in $G$.

These cyclic groups intersect only at the identity thus;

$|\tau_1| = (p-2)p$ ………………...…………… 3.1.3

We find the number of $\tau_0$ elements by subtracting the number of $\tau_1$ elements and the identity from the order of $G$.

$|\tau_0| = [p(p-1) - (p-2)p - 1] = p - 1$=$|C^g|$ by 3.1.2 implying all elements in $\tau_0$are conjugate in $G$ and are of order p.

Therefore;

$Z_{(G,X)} =$

$\frac{1}{|G|}(t_1^p + (p-1).monomial\ of\ an\ element\ in\ \tau_0 +$

$p(sumation\ of\ all\ monomials\ of\ the\ nontrivial\ elements\ in\ cyclic\ subgroups\ Cp{-}1)$

i.e $Z_{(G,X)} = \frac{1}{|G|}\left(t_1^p + (p-1).mon(x) + p\sum_{g\in C_{p-1}\setminus\{I\}} mon(g)\right)$ ……. 3.1.4

Where $x \in \tau_0$

The number $\alpha_l$ of cycles of length $l$ is given by, $\alpha_l = \frac{1}{l}\sum_{i|l}\pi\left(g^{\frac{l}{i}}\right)\mu(i)$ (Kamuti 1992)

Let $x \in \tau_0$, then $\pi(x) = 0$

It follows that $\pi(x^p) = p$ and if $l < p, \pi(x^l) = 0$
Now if $0 < l < p$ then,

$$\alpha_l = \frac{1}{l}\sum_{i|l}\pi\left(x^{\frac{l}{i}}\right)\mu(i) = \frac{1}{l}\sum_{i|l} 0\,\mu(i) = 0$$

$$\alpha_p = \frac{1}{p}\sum_{i|p}\pi\left(x^{\frac{l}{i}}\right)\mu(i) = \frac{1}{p}[\pi(x^p) - \pi(x)] = \frac{1}{p}[p-0] = \frac{p}{p} = 1$$

The resulting monomial is $t_p$ ................................ 3.1.5
If $g \in \tau_1$, then $\pi(g) = 1, \pi(g^d) = \frac{p}{d}$ and $\pi(g^l) = 1$ when $l < d$
$\alpha_l = \frac{1}{l}\sum_{i|l}\pi\left(g^{\frac{l}{i}}\right)\mu(i) = \frac{1}{l}\sum_{i|l}(1)\,\mu(i) = \frac{1}{l}\sum_{i|l}\mu(i) = 0$ (From the definition of the Mobius function)

$$\alpha_d = \frac{1}{d}\sum_{i|d}\pi\left(g^{\frac{d}{i}}\right)\mu(i) = \frac{1}{d}\left[\pi(g^d) + \sum_{i|d}\pi\left(g^{\frac{d}{i}}\right)\mu(i) - \pi(g)\right] = \frac{1}{d}[\pi(g^d) - \pi(g)] = \frac{1}{d}[p-1]$$

$$= \frac{p-1}{d}$$

Thus the resulting monomial is $t_1 t_d^{\frac{p-1}{d}}$ .................... 3.1.6
Substituting for $mon(x)$ (equation 3.1.5) and $mon(g)$ (equation 3.1.6) in equation 3.1.4 we get;

$$Z_{(G,X)} = \frac{1}{|G|}\left(t_1^p + (p-1)t_p + p\sum_{1\neq d|(p-1)} \emptyset(d) t_1 t_d^{\frac{p-1}{d}}\right)$$

**Example 3.1.1**
Let $p = 17$, $|G| = 272$
Possible values of $d$ are; 2, 4, 8 and 16
$\emptyset(2) = 1$, $\emptyset(4) = 2$, $\emptyset(8) = 4$, and $\emptyset(16) = 8$
Substituting in theorem 3.1.1 we have;

$$Z_{(Aff(17),X)} = \frac{1}{272}(t_1^{17} + 16t_{17} + 17t_1t_2^8 + 34t_1t_4^4 + 68t_1t_8^2 + 136t_1t_{16})$$

**Expressing the cycle index of the Affine(p) group in terms of the cycle index of the cyclic groups $C_p$ and $C_{p-1}$**

The equation in theorem 3.1.1 can be simplified as;

$$Z_{(G,X)} = \frac{1}{p(p-1)}\left(t_1^p + (p-1)t_p\right) + \frac{1}{p(p-1)}\left(pt_1^p + p\sum_{1\neq d|(p-1)} \emptyset(d)t_1 t_d^{\frac{p-1}{d}}\right) - \frac{1}{(p-1)}t_1^p$$

$$= \frac{1}{(p-1)}Z_{(C_p,X)} + \frac{1}{(p-1)}\left(t_1^p + \sum_{1\neq d|(p-1)} \emptyset(d)t_1 t_d^{\frac{p-1}{d}}\right) - \frac{1}{(p-1)}t_1^p$$

$$= \frac{1}{(p-1)}Z_{(C_p,X)} + Z_{(C_{p-1},X)} - \frac{1}{(p-1)}t_1^p$$

$$= \frac{1}{|C_{p-1}|}Z_{(C_p,X)} + Z_{(C_{p-1},X)} - \frac{1}{|C_{p-1}|}Z_{(1,X)} \qquad \text{……..……… 3.1.7}$$

**Example 3.1.2**

Let $p = 11$ then $G\ is\ Aff(11)$ and $X = \{0,1,2,3,4,5,6,7,8,9,10\}$ and

$$Z_{(G,X)} = \frac{1}{110}\left(t_1^{11} + 10t_{11} + 11\sum_{1\neq d|10} \emptyset(d)t_1 t_d^{\frac{10}{d}}\right) \text{ from 3.1.1}$$

Which can be simplified as

$$Z_{(G,X)} = \frac{1}{11(10)}(t_1^{11} + 10t_{11}) + \frac{1}{11(10)}\left(11t_1^{11} + 11\sum_{1\neq d|10} \emptyset(d)t_1 t_d^{\frac{10}{d}}\right) - \frac{1}{10}t_1^{11}$$

$$= \frac{1}{10}Z_{(C_{11},X)} + Z_{(C_{10},X)} - \frac{1}{10}t_1^{11}$$

$$= \frac{1}{10}Z_{(C_{11},X)} + Z_{(C_{10},X)} - \frac{1}{10}Z_{(1,X)} \qquad \text{from 3.1.7.}$$

## 4. References

[1] Cameron, P. J. (2007). *Permutation Groups,* London Math. Soc. Student Texts 45, Cambridge University Press, Cambridge.

[2] Harald F. 1997.Cycle Indices of Linear, A□ne and Projective Groups.*Linear Algebra and Its Applications,* 263:133 – 156.

[3] Harary, F. & Palmer E. (1966). Power group enumeration theorem. *Journal of Combinarial Theory* 1:157-173.

[4] Harary, F. (1967). *Applications of Pólya's theorem to permutation groups,* Ed. 4. Academic Press, New York.

[5] Kamuti, I. N. (1992). *Combinatorial formulas, invariants and structures associated with primitive permutation representations of PGL(2,q) and PSL(2,q).*Ph.d, Mathematical studies. xiv, 20, 26, 31, 33, 66, 147

[6] Krishnamurthy, V. (1985). *Combinatorics: Theory and application.* Affiliated East-West Press Private Limited, New Delhi.

[7] Peter. J. and Jason. S. (2017). The cycle polynomial of permutation group. *The electronic journal of combinatorics* *25*:1-16