Journal of the Nigerian Association of Mathematical Physics
***Volume* 13 (November, 2008), 31 - 34**

On the isomorphism of aut($\mathbb{Z}_n$), *U*-group *U*(*n*) and permutation group *U*(*n*)*

H. Praise Adeyemo
Department of Mathematics
University of Ibadan, Nigeria.

Abstract

***In this paper, we compute Aut($\mathbb{Z}_n$) and U-group, U(n) and establish that these groups are isomorphic and give the systematic construction of the permutation group, U(n)* which is isomorphic to to U(n). Hence we establish the isomorphism of Aut($\mathbb{Z}_n$), U-group U(n) and Permutation group U(n)*. We consider only when n* = 20**.

1.0 Introduction.

Given a positive integer n, it is not a mere routine matter to find how many isomorphism types of groups of order n are there. Every group of prime order is cyclic. Since Langrage's theorem implies the cyclic group generated by any of its non-identity elements is the whole group.

***Theorem* A [5]**

Suppose φ is an isomorphism from a group X to a group Y then

(i) φ *preserves the identity elements*

(ii) *Commutativity is invariant under* φ

(iii) $|x| = |\varphi(x)|\ \forall\, x \in X$ *i.e* φ *preserves order*

(iv) X *is cyclic if and only if Y is cyclic*

(v) *If T is a subgroup of X, then* $\varphi(T) = \{ \varphi(t) : t \in T\}$ *is a subgroup of Y.*

***Definition* 1.1**

An isomorphism from a group (X, •) to itself is called an automorphism of this group.

***Definition* 1.2**

The set of all automorphism in X is given by Aut(X).

***Lemma* B**

A function from a finite set to itself is injective if and only if it is surjective.

2.0 The main results

In this section, we give the result when $n = 20$. We suppose β is an element of Aut(Z_{20}) and try to discover enough information about β to determine how β must be defined.

***Theorem* C**

There are only eight distinct automorphisms in Aut(Z_{20}).

Proof

Let $\beta \in$ Aut(Z_{20}), we consider $\beta(1)$ and give the choices which turn it to be an automorphism in Z_{20}. Theorem A(iii), gives

$$\beta(1)=1,\ \beta(1)= 3,\ \beta(1)=7,\ \beta(1)=9,\ \beta(1)=11,\ \beta(1) =13,\ \beta(1)=17,\ \beta(1) = 19$$

These eight automorphisms are defined as follows:

$\beta_1: Z_{20}\to Z_{20}$

$\beta_1(x) = x,\ \forall x \in Z_{20}$

e-mail: adepraise5000@yahoo.com.au, Mobile Phone: +2348068288896.

The author would like to thank International Center For Theoretical Physics (ICTP) and Crawford University, Ogun State for providing a conducive atmosphere for me while carrying out this research. I would also like to thank Mr Seun Fagbamila for his support.

$\beta_3 : Z_{20} \rightarrow Z_{20}$

$\beta_3(x) = 3x, \forall x \in Z_{20}$

$\beta_7 : Z_{20} \rightarrow Z_{20}$

$\beta_7(x) = 7x, \forall x \in Z_{20}$

$\beta_9 : Z_{20} \rightarrow Z_{20}$

$\beta_9(x) = 9x, \forall x \in Z_{20}$

$\beta_{11} : Z_{20} \rightarrow Z_{20}$

$\beta_{11}(x) = 11x, \forall x \in Z_{20}$

$\beta_{13} : Z_{20} \rightarrow Z_{20}$

$\beta_{13}(x) = 13x, \forall x \in Z_{20}$

$\beta_{17} : Z_{20} \rightarrow Z_{20}$

$\beta_{17}(x) = 17x, \forall x \in Z_{20}$

$\beta_{19} : Z_{20} \rightarrow Z_{20}$

$\beta_{19}(x) = 19x \ \forall x \in Z_{20}$

We claim that these are the only distinct automorphisms of Z_{20} and any other one will be equal to one of these eight.

Next, we give the Cayley table to show the structure of Aut(Z_{20}) is a group under the composition of functions.

Figure 2.1

o	β_1	β_3	β_7	β_7	β_{11}	β_{13}	β_{17}	β_{19}
β_1	β_1	β_3	β_7	β_9	β_{11}	β_{13}	β_{17}	β_{19}
β_3	β_3	β_9	β_1	β_7	β_{13}	β_{19}	β_{11}	β_{17}
β_7	β_7	β_1	β_9	β_3	β_{17}	β_{11}	β_{19}	β_{13}
β_9	β_9	β_7	β_3	β_1	β_{19}	β_{17}	β_{13}	β_{11}
β_{11}	β_{11}	β_{13}	β_{17}	β_{19}	β_1	β_3	β_7	β_9
β_{13}	β_{13}	β_{19}	β_{11}	β_{17}	β_3	β	β_1	β_7
β_{14}	β_{17}	β_{11}	β_{19}	β_{13}	β_7	β_1	β_9	β_3
β_{19}	β_{19}	β_{17}	β_{13}	β_{11}	β_9	β_7	β_3	β_1

3.0 Construction of group of units modulo *n*, (U-group, U(*n*)), *n* = 20

***Definition* 3.1**

U(*n*) *is the set of all positive integers less than n and relatively prime to n.*

***Remark* 3.2**

U(*n*) *is a group under multiplication,* (•) *modulo n called the group of units modulo n* (*U-group*).

***Theorem* 3.1**

Let U(*n*) *consist of a reduced system of residue modulo n such that* $|U(n)| = |\varphi(n)|$, *the Euler's phi-function*. *Then* (*U*(*n*),*) *is an Abelian group*.

For *n* = 20, we have: *U*(*n*) = {1, 3, 7, 9, 11, 13, 17, 19}.

The Cayley table gives:

•	1	3	7	9	11	13	17	19
1	1	3	7	9	11	13	17	19
3	3	9	1	7	13	19	11	17
7	7	1	9	3	17	11	19	13

9	9	7	3	1	19	17	13	11
11	11	13	17	19	1	3	7	9
13	13	19	11	17	3	9	1	7
17	17	11	19	13	7	1	9	3
19	19	17	13	11	9	7	3	1

Figure 3.1

4.0 Construction of permutation group *U*(20)* which is isomorphic to *U*-group U(20)

In this section, we give a result of how to construct the permutation group U(20) that is isomorphic to the *U*-group U(20).

***Definition* 4.1**

A permutation of a set G is a function from G to itself which is one-to-one and onto.

Next, we give the result in the section.

4.2 Lemma 4.2

There is one-to–one correspondence between the U-group, U(20) *and the permutation group U*(20)*

Proof

For any r Є U(20), define a mapping: α_r:U(20) → U(20) by

$$\alpha_r(y) = yr \ \forall y \in U(20) \qquad (4.1)$$

It is obvious that each α_r bijective. Therefore, it is a permutation. Define

$$U(20)^* = \{ \alpha_r : r \in U(20) \ \forall r \in U(20)\} \qquad (4.2)$$

U(20)* is a group under the composition of functions. In fact, U(20)* is a group on the set U(20). Next, define a map Γ:U(20) → U(20)* by

$$\Gamma(r) = \alpha_r \ \forall r \in U(20) \qquad (4.3)$$

Γ gives the following permutations

$$\Gamma(1) = \alpha_1 = \begin{pmatrix} 1 & 3 & 7 & 9 & 11 & 13 & 17 & 19 \\ 1 & 3 & 7 & 9 & 11 & 13 & 17 & 19 \end{pmatrix}$$

$$\Gamma(3) = \alpha_3 = \begin{pmatrix} 1 & 3 & 7 & 9 & 11 & 13 & 17 & 19 \\ 3 & 9 & 1 & 7 & 13 & 19 & 11 & 17 \end{pmatrix}$$

$$\Gamma(7) = \alpha_7 = \begin{pmatrix} 1 & 3 & 7 & 9 & 11 & 13 & 17 & 19 \\ 7 & 1 & 9 & 3 & 17 & 11 & 19 & 13 \end{pmatrix}$$

$$\Gamma(9) = \alpha_9 = \begin{pmatrix} 1 & 3 & 7 & 9 & 11 & 13 & 17 & 19 \\ 9 & 7 & 3 & 1 & 19 & 17 & 13 & 11 \end{pmatrix}$$

$$\Gamma(11) = \alpha_{11} = \begin{pmatrix} 1 & 3 & 7 & 9 & 11 & 13 & 17 & 19 \\ 11 & 13 & 17 & 19 & 1 & 3 & 7 & 9 \end{pmatrix}$$

$$\Gamma(13) = \alpha_{13} = \begin{pmatrix} 1 & 3 & 7 & 9 & 11 & 13 & 17 & 19 \\ 13 & 19 & 11 & 17 & 3 & 9 & 1 & 7 \end{pmatrix}$$

$$\Gamma(17) = \alpha_{17} = \begin{pmatrix} 1 & 3 & 7 & 9 & 11 & 13 & 17 & 19 \\ 17 & 11 & 19 & 13 & 7 & 1 & 9 & 3 \end{pmatrix}$$

$$\Gamma(19) = \alpha_{19} = \begin{pmatrix} 1 & 3 & 7 & 9 & 11 & 13 & 17 & 19 \\ 19 & 17 & 13 & 11 & 9 & 7 & 3 & 1 \end{pmatrix}$$

Therefore, U(20)*= { $\alpha_1, \alpha_3, \alpha_7, \alpha_{11}, \alpha_{13}, \alpha_{17}, \alpha_{19}$ } .It is a group under the composition of functions. The Cayley table is given by :

•	α_1	α_3	α_7	α_9	α_{11}	α_{13}	α_{17}	α_{19}
α_1	α_1	α_3	α_7	α_9	α_{11}	α_{13}	α_{17}	α_{19}
α_3	α_3	α_9	α_1	α_7	α_{13}	α_{19}	α_{11}	α_{17}
α_7	α_7	α_1	α_9	α_3	α_{17}	α_{11}	α_{19}	α_{13}
α_9	α_9	α_7	α_3	α_1	α_{19}	α_{17}	α_{13}	α_{11}

α_{11}	α_{11}	α_{13}	α_{17}	α_{19}	α_1	α_3	α_7	α_9
α_{13}	α_{13}	α_{19}	α_{11}	α_{17}	α_3	α_9	α_1	α_7
α_{17}	α_{17}	α_{11}	α_{19}	α_{13}	α_7	α_1	α_9	α_3
α_{19}	α_{19}	α_{17}	α_{13}	α_{11}	α_9	α_7	α_3	α_1

Figure 4.1

From Theorem A, Γ is an isomorphism and hence U(20) is isomorphic to U(20)*. The same arguments go for Aut(Z_{20}) and U(20), hence , these groups are isomorphic.

5.0 Conclusion

In this paper, we compute a very special case of a well-motivated problem. Further work is in progress to generalize these results using recent developments in group theory.

References

[1] P. Hall. A Contribution to the Theory of Groups of Prime Orders, Proc. Lond. Math. Soc.(2), 36 (1933), pp 77-141.

[2] W.Burnside . On Criteria for the finiteness of the Order of a Group of Linear Substitutions, Proc. Lond. Math. Soc(2), 3 (1905), pp435-440.

[3] R. Baer. Finiteness Properties of Groups, Duke Math. J. 15 (1948) pp 1021-1032.

[4] O. Ore, Contribution to the Theory of Groups of Finite Order, Duke Math. J., 5 (1939) pp431-460.

[5] J.A Gallian, Contemporary Abstract Algebra, D.C Heath and Company Toronto 1986.