Finite Groupoids Using $Z_n$

Saleh M.A. Mustafa and Shaban A. Tranina

Department of Mathematics, Faculty of Science, University of Garyounis

Abstract: In this paper we obtain conditions on $n$ and on the pair $t$ and $u$ for the groupoid $Z_n(t,u)$ to be normal, semi-normal, conjugate and ideal groupoid. We were able to find all sub-groupoids and their order. These groupoids show interesting properties. Some of their properties are studied and some interesting results are obtained and provided, throughout this paper.

Key words: Groupoid - Sub-groupoid - Ideal - Normal - Conjugate

INTRODUCTION

In this paper, we introduce groupoids using $Z_n$ let $Z_n = \{0, 1, 2,...,n-1\}$ for the groupoid $Z_n(t,u)$ where $t, u$ are two distinct integers in $Z_n$, $’+$' is the usual addition of two integers and $ta$ means the product of the two integers $t$ and $a$.

We denote this groupoid by $\{Z_n(t,u),’+$\} or in short by $Z_n(t,u)$.

These groupoids show interesting properties. Some of their properties are studied and some interesting results are obtained and provided, throughout this paper.

Remarks:

- For varying $t, u \in Z_n\{0\}$ we get a collection of groupoids for a fixed integer $n$.
- This collection of groupoids is denoted by $Z(n)$.
- The number of groupoids in $Z(n)$ is even, since, if $Z_n(t,u)$ is a groupoid in $Z(n)$, then $Z_n(t,u)$ is also a groupoid.

Example: Let $Z_3 = \{0, 1, 2\}$, $Z_3(1,2) \in Z(3)$, is a groupoid given by the following table:

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
</tbody>
</table>

This groupoid is also non commutative and non associative. Hence, in $Z_3$ we have only two groupoid of order 3 using $Z_n$.

Finite Groupoid Using $Z_n$: In this section, we introduce some special properties of $Z_n$ and obtain some interesting results.

Remark: $Z_n(t,u)$ be a groupoid given by the following Table:

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>$n-1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>$t$</td>
<td>$2u$</td>
<td>$3u$</td>
<td>$(n-1)u$</td>
</tr>
<tr>
<td>1</td>
<td>$t$</td>
<td>$t+u$</td>
<td>$t+2u$</td>
<td>$t+3u$</td>
<td>$(t+(n-1)u)$</td>
</tr>
<tr>
<td>2</td>
<td>$2t$</td>
<td>$2t+u$</td>
<td>$2t+2u$</td>
<td>$2t+3u$</td>
<td>$2t+(n-1)u$</td>
</tr>
<tr>
<td>3</td>
<td>$3t$</td>
<td>$3t+u$</td>
<td>$3t+2u$</td>
<td>$3t+3u$</td>
<td>$3t+(n-1)u$</td>
</tr>
<tr>
<td>$n-1$</td>
<td>$(n-1)t$</td>
<td>$(n-1)t+u$</td>
<td>$(n-1)t+2u$</td>
<td>$(n-1)t+3u$</td>
<td>$(n-1)(t+1)$</td>
</tr>
</tbody>
</table>

- If $x \in Z_n(t,u)$, then $x = a_i * b_j$, $i, j = 0, 1, 2,...,n-1$.
- $a_i = I$ and $b_j = j$.
- $a_i * b_{j+1} = (a_i * b_j) + u$.

Proof: Let $H. S = a_i * b_{j+1} = ta_i + ub_{j+1} = ta_i + ub_j + u = (a_i * b_j) + u = R. H. S$.

Theorems and Corollary

Theorem 2.1: In the groupoid $Z_n(t,u)$, if $a_i * b_j = a_i * b_{j+1}$, then $a_i * b_{j+1} = a_i * b_{j+k}$.

Proof: Since, $a_i * b_j = a_i * b_{j+k}$, then $ta_i + ub_{j+k} = (mod n) = ta_i + ub_{j+k} (mod n)$.

So, $ta_i + ta_j - ub_j + ub_{j+k} (mod n)$.

Now, $a_i * b_{j+1} = ta_i + ub_{j+k} (mod n)$.

Let $a_i * b_{j+1} - ta_i + ub_{j+k} (mod n) = ta_i + ub_{j+k} = a_i * b_{j+k+1}$

Theorem 2.2: In the groupoid $Z_n(t,u)$, all rows (columns) have the same number of distinct elements.

Corresponding Author: Saleh M.A. Mustafa, Department of Mathematics, Faculty of Science, University of Garyounis.

Tel. +21891 774 3026.
Proof: Suppose that the number of distinct elements in two rows are not equivalent, then \( a_u \ast b_j = a_u \ast b_{j+1} \), such that, \( \alpha \beta \ast b_j \neq a \beta \ast b_{j+1} \), where \( \alpha, \beta, k \in \mathbb{Z}_n \).

Now,
\[
a_u \ast b_j = ta_u + ub_j \mod n = a_u \ast b_{j+1} = ta_u + ub_{j+1} \mod n.
\]

Then,
\[
ta_u + ub_j \mod n = ta_u + ub_{j+1} \mod n
\]
\[
ub_j \mod n = ub_{j+1} \mod n
\]
(1)
\[
a_u \ast b_j = ta_u + ub_j \mod n \quad \text{and} \quad a \beta \ast b_{j+1} = ta \beta + ub_{j+1} \mod n
\]
But,
\[
a \beta + ub_j \mod n \neq ta \beta + ub_{j+1} \mod n
\]
Hence,
\[
b_{j+1} \mod n \neq ub_j \mod n, \text{ from (1) this is a contradiction.}
\]

We will get a similar result for the columns.

Theorem 2.3: In the groupoid \( Z_s(t, u) \),

- If \( (n, u) = d \), then the number of distinct elements in each row is equal \( (n/d) \).
- If \( (n, u) = d \), then the number of distinct elements in each column is equal \( (n/d) \).

Proof: (1) Let \( (n, u) = d \), take \( a = 0 \), then,
\[
a \ast b_j = ta + ub \mod n = ub \mod n
\]
Since, \( d \mid n \), then there exist \( b_j \in \mathbb{Z}_n \) such that, \( b_j = n/d \).
Thus,
\[
a \ast b_j = ub \mod n = (u)(n/d) \mod n = 0, \text{ since, } (n, u) = d/j.
\]
Now, let \( D = \{ x \in \mathbb{Z}_n : 0 < x < \frac{n}{d} \} \) and suppose that \( xu = 0 \mod n \) for some \( x \in D \).
Thus, \( xu = kn \) where, \( k \) is a positive integer, but \( x < (n/d) \), then,
\[
\frac{kn}{u} \leq \frac{n}{d} \Rightarrow \frac{k}{u} \leq \frac{1}{d} \Rightarrow \frac{u}{k} > d.
\]
Since, \( x < n \) and \( u < n \), then, \( xu = 0 \mod n \) only if \( x/n \) or \( u/n \).

Now, if \( x \mid n \) then, \( k \mid u \), implies that, \( \frac{u}{k} = \frac{n}{d} \), which is a contradiction.

Also, if \( k \mid n \), then \( (n, u) = u \), which is a contradiction, then \( ux \neq 0 \mod n \) for all \( x \in D \).

Therefore, \( b_i \) is the smallest integer, such that, \( b_i = 0 \mod n \).

Nevertheless, the number of distinct elements between \( b_i \) and \( b_{i+k} \) is \( b \) by theorem (2.1) and the number of distinct elements between \( b_i \) and \( b_i \) is equal to the number of distinct elements between \( 2b_i \) and \( 3b_i \) which means the first row has only \( b_i \) elements. By theorem (2.2), the number of distinct elements in each row is equal to \( b_i = n/d \).

- Similar result will be obtained for the columns.

Corollary 2.4: In the groupoid \( Z_s(t, u) \),

- If \( (u, n) = 1 \), then the elements in each row are distinct.
- If \( (u, n) = 1 \), then the number of distinct elements in each column is equal \( n \).

Proof: Suppose that the number of distinct elements in each row are not equal, then, there exist \( i, j \), such that, \( a_i \ast b_j = a_i \ast b_{j+1} \), where \( k = 1, 2, \ldots, n - 1 \). Now, take \( i = 0 \) then, \( ub_j = ub_{j+1} \) implies that, \( b_j = b_{j+1} \) if and only if, \( k = 0 \) or \( k = n \); which is a contradiction. Hence, the order of the rows is equal.

Theorem 2.5: In the groupoid \( Z_s(t, u) \), if \( n \) is even, then

- If \( t \) is even and \( u \) is odd, then we have four sub-groupoids as follows,
  \[
  H_1 = \{ x \in \mathbb{Z}_n : x \text{ is even} \} \quad |H_1| = \frac{n}{2}
  \]
  \[
  H_2 = \{ x \in \mathbb{Z}_n : x \text{ is odd} \} \quad |H_2| = \frac{n}{2}
  \]
  \[
  H_3 = \left\{ 0, \frac{n}{2} \right\}, \quad H_4 = \left\{ \frac{n}{2} \right\}
  \]
- If \( t \) and \( u \) are both even or odd, then we have two sub-groupoids
  \[
  H_1 = \{ x \in \mathbb{Z}_n : x \text{ is even} \} \quad |H_1| = \frac{n}{2}, \quad H_2 = \left\{ 0, \frac{n}{2} \right\}
  \]

Proof: (1) If \( t \) is even and \( u \) is odd, Let \( a, b_j \in H_1 \), \( i, j = 0, 1, 2, \ldots, n - 1 \). Since, \( a_i \ast b_j = ta_i + ub_j \mod n \), then \( a_i \ast b_j \) is even and \( a_i \ast b_j \in H_1 \) thus, \( H_1 \) is a sub-groupoid and its order is \( \frac{n}{2} \).
Also, let \( a_2, b_2 \in H_2 \), then \( a_2 \ast b_2 = ta_1 + ub \text{mod} n \). So, 
\( ta_1 \) is even and \( ub \) is odd, which means that \( a_2 \ast b_2 \in H_2 \).
Hence \( H_2 \) is a sub-groupoid and its order is \( \frac{n}{2} \).

\[
\left\{ \left( \frac{0}{2}, \frac{n}{2} \right) \right\}
\]
is a sub-groupoid since,
\[
0 \ast \frac{0}{2} = \frac{n}{2} \text{mod} n = \frac{n}{2} \text{mod} n,
\]
since \( u \) is odd,

Now, \( \frac{1}{2} \ast 0 = i \frac{n}{2} \text{mod} n = 0 \), since \( t \) is even.

\[
\left\{ \frac{n}{2} \right\}
\]
is a sub-groupoid since,
\[
\frac{n}{2} \ast \frac{n}{2} = \frac{n}{2} \text{mod} n = \frac{n}{2} \text{mod} n,
\]
since \( u \) is odd.

- If \( t \) and \( u \) are odd, let \( a_2, b_2 \in H_2 \), then \( a_2 \ast b_2 = ta_1 + ub \text{mod} n \) is even. Hence, \( a_2 \ast b_2 \in H_2 \), so \( H_2 \) is a sub-groupoid and its order \( \frac{n}{2} \).

\[
\left\{ \left( \frac{0}{2}, \frac{n}{2} \right) \right\}
\]
is a sub-groupoid.

Since, \( \frac{n}{2} \ast \frac{n}{2} = i \frac{n}{2} + \frac{n}{2} \text{mod} n = (t + u) \frac{n}{2} \text{mod} n = 0 \text{mod} n \), where \( t, u \) is odd and,
\[
\frac{n}{2} \ast 0 = i \frac{n}{2} \text{mod} n = \frac{n}{2} \text{mod} n = \frac{n}{2} \text{mod} n,
\]
since \( t \) and \( u \) are odd.

In a similar way, it can be proved all cases if \( t \) and \( u \) are even.

**Theorem 2.6[3]:** \( P \) is a left ideal of \( Z_4(t,u) \), if and only if, \( P \) is a right ideal of \( Z_4(t,u) \).

**Theorem 2.7:** In the groupoid \( Z_4(t,u) \), if \( (n,t) = d_1 \) and \( (n,u) = d_2 \), then the first column and the first row are sub-groupoids of order \( (n/d_1), (n/d_2) \) respectively.

**Proof:** \( \{x \} = \{ y \in Z_4(t,u) : y = x \text{mod} n \} \).
We can write the first row and the first column as follows:

\[
R_0 = \{(u_i) : i = 0, 1, 2, ..., n-1 \}, \quad C_0 = \{(t_i) : j = 0, 1, 2, ..., n-1 \}. \]

Let \( \{ux\}, \{uy\} \in R_0 \), \( x, y = 0, 1, 2, ..., n-1 \), \( ux \ast uy = tx + u(y \text{mod} n) = tx + uy \text{mod} n \) take \( tx + uy = m \), \( ux \ast uy = mu \text{mod} n \) \( \in R_0 \) and by theorem \( 2.5.3 \), \( R_0 = (n/d) \).

Similarly we can proof the first column and a sub-groupoid of order \( (n/d). \)

**Corollary 2.8:** In theorem 2.7, if \( (n,u) = d_1 \) and \( (n,t) = d_2 \) then,

- \( R_0 \) is a right ideal.
- \( C_0 \) is a left ideal.

- \( R_0 \) is not conjugate with \( C_0 \).

- \( R_0 \) and \( C_0 \) are normal sub-groupoids, Where \( R_0 \) the first is row and \( C_0 \) is the first column.

**Proof:** (1) \( R_0 = \{(u_i) : i = 0, 1, 2, ..., n-1 \}, \) let \( x \in Z_4(t,u) \) and let \( uy \in R_0 \), \( 0 \leq y < n \) \( uy \ast x = uy + ux \text{mod} n = u(tx + y) \text{mod} n \). Since, \( x, y, t \in Z_4 \), \( 0 \leq y + x < n \), then \( uy \ast x \in R_0 \), thus, \( R_0 \) is a right ideal.

- Similar to the proof of (1).

- Since, \( 0 \in R_0 \), then \( R_0 \) is not conjugate with \( C_0 \).

- For all \( x \in R_0 \), \( xR_0 = R_0x = R_0 \) and all \( y \in C_0 \), \( yC_0 = C_0 \), then \( R_0 \) and \( C_0 \) are normal sub-groupoids.

**Theorem 2.9:** In the groupoid \( Z_4(t,u) \), if \( (n,u) = d \), then every row is a sub-groupoid of order \( \frac{n}{d} \).

**Proof:** We can write any row as, \( R_i = \{(i + u_j) : i, j = 0, 1, 2, ..., n-1 \} \).
Now, let \( x + uy_1, x + uy_2 \in R_i \) such that, \( x, y_1, y_2 = 0, 1, 2, ..., n-1 \) then

\[
(x + uy_1) \ast (x + uy_2) = x + uy_1 + u(x + uy_2) \text{mod} n = x + u(x + y_1 + uy_2) \text{mod} n.
\]

Take \( m = x + y_1 + uy_2 \), then \( (x + uy_1) \ast (x + uy_2) = x + um \in R_i \).
Therefore, \( R_i \) is a sub-groupoid and by theorem \( 2.5.4 \), \( |R_i| = \frac{n}{d} \).

**Corollary 2.10:** In the above theorem if \( (n,t) = d \), then every column in \( Z_4(t,1) \) is a sub-groupoid as \( C_i = \{(ti + j) : i, j = 0, 1, 2, ..., n-1 \}, \) \( |C_i| = \frac{n}{d} \).

**Corollary 2.11:**

1. In \( Z_4(1,u) \), if \( (n,u) = d \), then

- \( R_i \) is a right ideal for all \( i \).
- Any two distinct rows are conjugate with each other.
- \( R_0 \) is a normal sub-groupoid for each \( i \).

2. In \( Z_4(t,1) \) if \( (n,t) = d \), then

- \( C_0 \) is a left ideal for all \( i \).
- Any two distinct columns are conjugate with each other.
- \( C_0 \) is a normal sub-groupoid for all \( i \).
Theorem 2.12: In the groupoid \( Z(t,u) \), if \( t + u \equiv 1 (mod \ n) \), then

- If \( (n, t) = d \), then each column is a sub-groupoid of order \( (n/d) \).
- If \( (n, u) = d \), then each row is a sub-groupoid of order \( (n/d) \).

Proof: (1) We can write any column as follows,

\[
C_a = \{ [it + au] : i = 0, 1, 2, \ldots, n-1 \}.
\]

Now, let \( x + iu, y + au \in C_a \),

\[
(x + au + y + au) = x + y + au = (y + au) (mod \ n).
\]

Let \( t + u \equiv m (mod \ n) \), since, \( t + u \equiv m (mod \ n) \),

\[
(x + iu)(y + au) = x + au (mod \ n).
\]

(2) Similar result applied for the row.

Corollary 2.13: In theorem 2.12, if \( (n, u) = d \), then each column is a left ideal, a normal sub-groupoid and every two distinct columns are conjugate with each other.

Moreover, if \( (n, u) = d \), then each row is a right ideal, a normal sub-groupoid and every two distinct rows are conjugate sub-groupoids with each other.

Note: In the groupoid \( Z(t,u) \) if \( n \) and \( t + u \equiv 1 (mod \ n) \), then each row and column has the same distinct elements. Therefore, each row (column) is an ideal and normal sub-groupoid, but not conjugate.

Corollary 2.14: In the last theorem if \( (n, t) = d \), then each column is a left ideal, a normal sub-groupoid and every two distinct columns are conjugate with each other.

In addition, if \( (n, t) = d \), then each column is a right ideal, a normal sub-groupoid and every two distinct rows are conjugate sub-groupoids with each other.

Theorem 2.15: In \( Z_n(1,1) \) if \( n = p_1^{k_1}p_2^{k_2} \ldots p_r^{k_r} \), then \( Z_n(1,1) \) has \( r \) sub-groupoids defined by

\[
H_i = \{ [xp_i] : x = 0, 1, 2, \ldots, n-1 \} \quad (1 \leq i \leq r).
\]

Proof: Let \( x p_i y p_i \in H_i \), where \( x, y = 0, 1, 2, \ldots, n-1 \). Define * by,

\[
x p_i * y p_i = (px + y)(mod \ n) \in H_i,
\]

then, \( H_i \) is a sub-groupoid and since \( n = p_1^{k_1}p_2^{k_2} \ldots p_r^{k_r} \), thus \( Z_n(1,1) \) has \( r \) sub-groupoids.

Corollary 2.16: In theorem 2.15, each sub-groupoid \( H_i \) is neither left (nor right) ideal, nor normal sub-groupoid. In fact, \( Z_n(1,1) \) is simple.

Theorem 2.17[3]: Let \( Z_n = \{0,1,2,\ldots,n-1\} \). A groupoid in \( Z(n) \) is a semi-group if and only if \( t^2 \equiv t (mod \ n) \) and \( u^2 \equiv u (mod \ n) \) for \( t, u \in Z_n \) and \( (t, u) = 1 \).

Proof: Suppose that \( t^2 \equiv t (mod \ n) \), then we can say that \( u + t = n + 1 \) and \( u = n - t + 1 \). So, \( (n - t + 1)^2 \equiv (n - t + 1)^2 (mod \ n) \) implies that \( t^2 + t^2 - 2nt - t + n \equiv 0 (mod \ n) \).

Clearly, \( n^2 - 2nt - n \equiv 0 (mod \ n) \), thus, \( u^2 \equiv u (mod \ n) \).

Theorem 2.18: Let \( Z_n(t,u) \) be collection of groupoids and \( t \in Z_n \) \{0, 1\}, such that, \( t^2 \equiv t (mod \ n) \) and \( u \in Z_n \) \{0, 1, t\},

such that, \( u + t = n + 1 \), then \( u^2 \equiv u (mod \ n) \).

Proof: Suppose that \( t^2 \equiv t (mod \ n) \), then \( x \equiv x (mod \ n) \) and \( x \notin \{0, 1\} \), then \( x \equiv 1 (mod \ n) \) or \( x \equiv 1 (mod \ n) \). This is a contradiction. As a result, \( Z(p^k) \) contains no semi-group.

Theorem 2.19: If \( n = p^k \), where \( p \) is a prime and \( k \) is a positive integer, then \( Z(p^k) \) contains no semi-group.

Proof: Suppose that \( x^2 \equiv x (mod \ n) \) and \( x \notin \{0, 1\} \), then \( x \equiv 1 (mod \ n) \) or \( x \equiv 1 (mod \ n) \). This is a contradiction. As a result, \( Z(p^k) \) contains no semi-group.

Theorem 2.20: If \( n \) is odd, then \( Z_n(n,n + 1) \) is a semi-group.

Proof: (1) \( n^2 \equiv n (mod \ 2n) \), since \( (n, 2) = 1 \) and \( n = 1 (mod \ 2) \) so, \( n^2 = n (mod \ 2n) \).

And since, \( n^2 = n (mod \ n) \), then \( n^2 = n (mod \ n) \).

(2) \( (n + 1)^2 \equiv (n + 1) (mod \ 2n) \), since \( n = 1 (mod \ n) \) so, \( n^2 \equiv n (mod \ 2) \), or \( (n + 1)^2 \equiv (n + 1) (mod \ 2) \). Also, \( (n + 1)^2 \equiv (n + 1) (mod \ n) \), then \( n + 1 = 1 (mod \ n) \).

Theorem 2.21: If \( Z_n(t,u) \) is a semi-group with \( t \neq 1 \), then either \( n, t = d \) or \( (n, u) = d \).

Proof: Suppose that \( (n, t) = 1 \) \( (n, u) \) and \( Z_n(t,u) \) is a semi-group, then \( t^2 = t (mod \ n) \) and \( u^2 = u (mod \ n) \).

Now, if \( n, t = 1 \) \( (n, u) \), then \( t = 1 (mod \ n) \) and \( u = 1 (mod \ n) \), which is impossible, since \( n \) and \( u < n \). Then either \( (n, t) = d \) or \( (n, u) = d \).

Theorem 2.22: Let \( Z_d(t, u) \) be a semi-group with \( t + u = 1 \) \( (mod \ n) \), then

(1) There are \( d_1 = (n, t) \) sub-groupoids of order \( d_2 = (n, u) \).
(2) There are \( d_1 = (n, u) \) sub-groupoids of order \( d_1 = (n, t) \).

Proof: (1) Since \( t + u = 1 (mod \ n) \), which means that both of \( t \) and \( u \) does not equal to 1, then \( (n, t) = d \) or \( (n, u) = d \). So, by theorem (2.5) each column is a sub-groupoid of order \( n/d_1 \) or each row is a sub-groupoid of order \( n/d_1 \).
Finally, we can see that \( \frac{n}{d_1} = d_2 \) and \( \frac{n}{d_2} = d_1 \).

(3) Same as (1).

**Corollary 2.23:** From theorem 2.22 we have the following.

- Each \( R_i \) is a right ideal.
- Each \( C_i \) is a left ideal.
- Any two distinct rows are conjugate to each other.
- Any two distinct columns are conjugate to each other.
- \( R_i, C_i \) are normal sub-groupoids.
- \( R_i, C_i \) are not conjugate.

**Theorem 2.24:** Let \( Z(n) \) be a collection of groupoids and \( n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r} \), then the number of semi-groups in the collection is \( 2^{2^r} - 1 \).

**Proof:** this is trivial, since the number of idempotent elements is \( 2^r \).

**CONCLUSION**

In this paper we started by providing a general description of \( Z_t(u) \) by representing a table of the finite to prove that any row or column is sub-groupoid and then determining the order of the groupoid. On top of that, we have discussed and checked which of these are, ideal, normal or sub-groupoids. Also, which of the two distinct columns (or rows) are conjugate and finally, which of the groupoids is a semi-group.

**REFERENCES**