

## MENENTUKAN GRUP SIKLIK HINGGA DENGAN PASCAL

Elfi fauziah<sup>1</sup>, Riswal Hanafi Siregar<sup>2</sup>  
<sup>1,2</sup>Teknik Informatika, Fakultas Teknik, Universitas Pamulang  
 email: dosen00475@unpam.ac.id

### ABSTRAK

Tulisan ini bertujuan untuk menentukan suatu grup siklik dengan membuat suatu program dengan bahasa pemrograman pascal. Grup (G) disebut siklik, bila ada elemen  $a \in G$  sedemikian hingga  $G = \{a^n \mid n \in \mathbb{Z}\}$ . Elemen  $a$  disebut pembangun dari grup siklik tersebut. Setiap grup siklik hingga dengan unsur yang dikandungnya. sebanyak in adalah isomorfik dengan grup bilangan bulat modulo in dengan operasi penjumlahan  $Z$ . Sehingga untuk menentukan suatu grup siklik hingga, hanya diperlukan komputasi numerik biasa. Dengan bahasa pemrograman, seperti Pascal.

Kata Kunci: Grup Siklik Hingga, Pemrograman, Pascal

### 1. PENDAHULUAN

Grup Siklis merupakan suatu sistem matematika yang merupakan suatu himpunan tak hampa yang dipenuhi oleh suatu operasi dan memenuhi sifat asosiatif, memiliki unsure kesatuan dan memiliki balikan.

Yaitu ;

Asosiatif :

Sifat ini memenuhi  $x(yz) = (xy)z$ , dimana untuk setiap unsure  $x, y, z$  merupakan anggota dari  $G$ .

Terdapat unsure kesatuan( $e$ ) :

Untuk setiap unsure yang merupakan anggota dari  $G$  dioperasikan dengan  $e$  anggota dari  $G$  menghasilkan unsure itu sendiri, yang memenuhi  $ex = xe = x$

Terdapat unsure balikan :

untuk setiap unsure  $x$  di  $G$  dan  $x^{-1}$  di  $G$  memenuhi  $xx^{-1} = x^{-1}x = e$  dimana unsure  $x^{-1}$  disebut balikan unsure  $x$

Definisi 3.1.1

- Sifat Asosiatif

Untuk setiap unsure  $x, y, z$  anggota  $G$  memenuhi  $x(yz) = (xy)z$

- Unsure kesatuan

Unsure kesatuan tersebut kita tandai dengan  $e$ ,

Di mana  $e$  anggota di  $G$ .

Apabila anggota di  $G$  dioperasikan dengan  $e$  akan menghasilkan dirinya sendiri.

$ex = xe = x$

- Balikan

untuk setiap unsure  $x^{-1}$  di  $G$  terdapat unsure  $x$  di  $G$  yang memenuhi  $xx^{-1} = x^{-1}x = e$ .

Path sisi lain dinyatakan bahwa setiap grup siklik hingga dengan unsur yang dikandungnya. sebanyak in adalah isomorfik dengan grup bilangan bulat modulo in dengan operasi penjumlahan  $Z$ . Sehingga untuk menentukan suatu grup siklik hingga, hanya diperlukan komputasi numerik biasa. B hasapemrograman, seperti Pascal dapat dipergunakan sebagai alternatif untuk menentukan subgrup—subgrup dari suatu grup siklik hingga.

### 2. METODOLOGI PENELITIAN

Untuk membuat suatu program dalam masalah ini diperlukan beberapa *teori* pendukung pendukung yang menyangkut sifat-sifat dan grup sildik dan subgrup-subgrupnya.

Sehingga tulisan mi disusun berdasarkan kerangka pemikiran dengan langkah langkah sebagai berikut:

Langkah 2 : Pengenalan konsep-konsep dasar dalam teori grup.

Langkah 3 : Pembahasan aspek-aspek numerik dan grup.

Langkah 4 : Pembahasan sifat-sifat dan grup siklik.

Langkah 5 : Pembuatan algoritma dan diagram alir

Langkah 6 : Pembuatan program

### 3. PEMBAHASAN

Grup  $(G, \cdot)$  disebut siklik, bila ada elemen  $a \in G$  sedemikian hingga  $G = \{a^n \mid n \in \mathbb{Z}\}$

$Z$ }. Elemen  $a$  disebut pembangun dari grup siklik tersebut.

Grup  $(G,+)$  disebut siklik, bila ada elemen  $a \in G$  sedemikian hingga  $G = \{na \mid n \in Z\}$ .

Sehingga secara umum dapat ditulis

Misalkan  $(G,*)$  adalah suatu Grup dan  $a \in G$ , maka generator  $a$  yang membangun suatu subgrup  $[a]$  dinamakan Subgrup Siklik dari  $(G,*)$ .

#### A. Teorema

Diketahui  $(G,*)$  merupakan grup dan  $a \in G$ . Himpunan  $H = \{a^n \mid n \in Z\}$  merupakan subgrup atas  $G$  sekaligus subgrup terkecil yang memuat  $a$ .

Bukti.

1. Akan ditunjukkan bahwa  $H$  merupakan subgrup atas  $G$ . Ambil sebarang  $a^r, a^s \in H$  untuk suatu  $r, s \in Z$ .

$$\begin{aligned} a^r * a^s &= (a * a * a * \dots * a) (a * a * a * \dots * a) \\ &\text{r kali} \quad \quad \quad \text{s kali} \\ &= (a * a * a * \dots * a) \\ &\text{r+s kali} \\ &= a^{r+s} \end{aligned}$$

dan  $r+s \in Z$  akibatnya  $a^{r+s} \in H$ . Jelas bahwa  $H$  bukan merupakan himpunan kosong, karena  $a^1 = a \in H$ . Diperhatikan juga bahwa  $a^0 = e \in H$  dan untuk setiap  $a^r \in H$  berlaku  $a^{-r} \in H$ . Jadi, terbukti bahwa  $H$  merupakan subgrup atas  $G$ .

2. Akan ditunjukkan bahwa  $H$  merupakan subgrup terkecil yang memuat  $a$ . Andaikan ada subgrup  $K$  atas  $G$  yang memuat  $a$ . Karena  $a^1 = a \in H$ , dan karena  $a^n \in H$  untuk setiap  $n \in Z$   $a \in H \subseteq K$  untuk setiap subgrup  $K$  atas  $G$  yang memuat  $a$ . Jadi,  $H$  merupakan subgrup terkecil yang memuat  $a$ .

Hal ini dapat dilihat dari beberapa kasus:

a. Kasus 1

Misalkan  $G = \{-1, 1\}$  adalah suatu Grup terhadap operasi perkalian  $(G, \cdot)$ . Tentukan Grup Siklik dari Grup tersebut.

Generator dari  $G = \{-1, 1\}$  adalah  $-1$  dan  $1$

$$\begin{aligned} [-1] &= \{(-1)^n \mid n \in Z\} \\ &= \{(-1)^0, (-1)^1, (-1)^2, \dots\} \\ &= \{-1, 1\} \\ [1] &= \{(1)^n \mid n \in Z\} \\ &= \{(1)^0, (1)^1, (1)^2, \dots\} \\ &= \{1\} \end{aligned}$$

generator  $-1$  adalah membangun suatu Grup Siklik, sehingga :

$$[-1] = \{-1, 1\}$$

generator  $1$  adalah membangun Subgrup Siklik, sehingga :

$$[1] = \{1\}.$$

b. Kasus 2

Misalkan  $G = \{0, 1, 2, 3\}$  adalah suatu Grup terhadap penjumlahan  $(G,+)$ . Tentukan Grup Siklik dari Grup tersebut.

Generator dari  $G = \{0, 1, 2, 3\}$  adalah  $0, 1, 2$  dan  $3$

$$\begin{aligned} [0] &= \{n(0) \mid n \in Z\} \\ &= \{0\} \\ [1] &= \{n(1) \mid n \in Z\} \\ &= \{0.1, 1.1, 2.1, 3.1, \dots\} \\ &= \{0, 1, 2, 3\} \\ [2] &= \{n(2) \mid n \in Z\} \\ &= \{0.2, 1.2, 2.2, 3.2, \dots\} \\ &= \{0, 2\} \\ [3] &= \{n(3) \mid n \in Z\} \\ &= \{0.3, 1.3, 2.3, 3.3, \dots\} \\ &= \{0, 3, 2, 1\} \end{aligned}$$

generator  $1$  dan  $3$  adalah membangun suatu Grup Siklik, sehingga :

$$[1] = [3] = \{0, 1, 2, 3\}$$

generator  $0$  dan  $2$  adalah membangun Subgrup Siklik, sehingga :

$$\begin{aligned} [0] &= \{0\} \\ [2] &= \{0, 2\} \end{aligned}$$

#### B. Teorema

Setiap grup siklik merupakan grup komutatif.

Bukti.

Misalkan  $G$  adalah grup siklik dan  $a \in G$  merupakan pembangun  $G$ . Ambil sebarang elemen  $g_1, g_2 \in G$ . Karena  $G$  merupakan grup siklik, maka terdapat bilangan  $r, s \in Z$  sehingga  $g_1 = a^r$  dan  $g_2 = a^s$ . Diperhatikan bahwa:

$$\begin{aligned} g_1 * g_2 &= a^r * a^s \\ &= a * a * \dots * a \\ &\text{r+s kali} \\ &= a^{r+s} \\ &= a^{s+r} \\ &= a^s * a^r \\ &= g_2 * g_1 \end{aligned}$$

#### C. Teorema

Subgrup pada suatu grup siklik merupakan grup siklik.

Bukti.

Misalkan  $G$  merupakan grup siklik yang dibangun oleh  $a$  dan  $H$  subgrup dari  $G$ .

Akan ditunjukkan bahwa  $H$  merupakan grup siklik. Jika  $H = \{e\}$ , jelas bahwa  $e = H$  sehingga  $H$  merupakan grup siklik. Jika  $H \neq \{e\}$ , maka terdapat elemen  $x \in H$  dengan  $x \neq e$ .

Karena  $H$  merupakan subgrup dari  $G$ , maka  $x \in G$  dan berakibat  $x = a^n \in H$  untuk suatu  $n \in \mathbb{Z}^+$ . Pilih bilangan  $m \in \mathbb{Z}^+$  sebagai bilangan yang terkecil sehingga  $a^m \in H$ .

Akan ditunjukkan bahwa  $a^m = H$ . Diambil sebarang  $y \in H$  dan karena  $H$  merupakan subgrup dari  $G$ , maka  $x \in G$  dan berakibat  $y = a^k \in H$  untuk suatu  $k \in \mathbb{Z}^+$ . Diperhatikan bahwa  $m \leq z$  dan dari algoritma pembagian pada  $\mathbb{Z}$  diperoleh  $k = mq + r$  untuk suatu  $q, r \in \mathbb{Z}$  dan  $0 \leq r < m$ . Dengan demikian diperoleh:

$$a^k = a^{mq+r} = a^{mq} a^r$$

dan

$$a^r = (a^m)^{-q} a^k$$

Karena  $a^m, a^k \in H$  dan  $H$  merupakan grup, akibatnya  $(a^m)^{-q} \in H$  dan  $(a^m)^{-q} a^k \in H$ . Dengan demikian diperoleh  $(a^r) = (a^m)^{-q} a^k \in H$ . Karena  $m$  merupakan bilangan yang terkecil sehingga  $a^m \in H$  dan karena  $0 \leq r < m$ , dengan kata lain  $r = 0$  sehingga

$$a^r = a^0 = e \text{ dan diperoleh:}$$

$$a^z = a^{mq+r} = a^{mq}$$

Jadi, karena untuk sebarang  $y \in H$  berlaku  $(y) = a^{mq}$ , maka  $\langle a^m \rangle = H$  dan dengan kata lain  $H$  merupakan grup siklik.

1. Dan uraian sebelumnya dapat dilihat bahwa beberapa unsur yang berbeda membangun subgrup yang sama. Subgrup-subgrup dan  $Z_6$  adalah  $\langle 0 \rangle, \langle 1 \rangle = \{5\}$ ,  $\langle 2 \rangle = \{4\}$ , dan  $\langle 3 \rangle$ . Sehingga dan uraian di atas diperoleh fakta bahwa:

1. Bila  $r \mid n$ , maka subgrup yang dapat dibangun berorde  $n/r$ .
2. Bila  $r \nmid n$ , maka terdapat dua kasus yaitu:
  - a) Bila  $\text{ppb}(r, n) = 1$ , maka  $(r) = \langle 1 \rangle$ . Pada uraian di atas diberikan oleh  $\langle 1 \rangle = \{5\}$ ,
  - b) Bila  $\text{ppb}(r, n) = d$  maka  $(r) = \langle d \rangle$ . Pada uraian di atas diberikan oleh  $\langle 2 \rangle = \{4\}$  Sehingga banyaknya subgrup dari 4 sama dengan banyaknya pembagi positif atau factor dari 6

Secara umum untuk menentukan subgrup-subgrup dan suatu grup siklik dilakukan dengan cara sebagai berikut. Andaikan  $G$  adalah grup siklik hingga berorde

$n$  dengan unsur pembangun  $a \in G$ . Untuk setiap  $d \in G$ , subgrup  $\langle d \rangle$  yang dapat dibangun oleh  $d$  diklasifikasikan berdasarkan pembagi persekutuan terbesar dan  $r$  dan  $n$ , yaitu:

- a)  $\text{ppb}(r, n) = r$ ,
- b)  $\text{ppb}(r, n) = 1$
- c)  $\text{ppb}(r, n) = d$ , dengan  $d \neq 1$ ,

Rangkaian teorema berikut : secara umum membahas ketiga kasus dalam menentukan subgrup-subgroup dari grup siklik hingga tersebut.

Kasus pertama, yaitu bila  $\text{ppb}(r, n) = r$ . Teorema 4.1. [Saracino, hal.50] Jika  $G$  adalah suatu grup siklik hingga berorde  $n$  dan terdapat bilangan  $b$  positif  $m$ , maka  $G$  mempunyai subgrup berorde  $m$  jika dan hanya jika  $m$  membagi  $n$ .

Bukti. Andaikan  $a \in G$  sehingga  $G = \langle a \rangle$  dan  $\text{orde}(a) = n$ . Jika  $m$  membagi  $n$  dan  $H = \langle a^{n/m} \rangle$ , maka teorema 2.4.4 menjamin bahwa  $H$  adalah subgrup dari  $G$ . karena  $n/m$  membagi  $n$ , maka  $\text{ppb}(n/m, n) = n/m$ . berdasarkan teorema 2.5.5 akan diperoleh  $\text{orde} \langle a^{n/m} \rangle = n / \text{ppb}(n/m, n) = n / (n/m) = m$ .

Andaikan  $\langle a^{m/n} \rangle$ , adalah subgrup dari  $G$  dengan orde  $\langle a^{m/n} \rangle = m$  dan  $H = \langle a^k \rangle$  dengan  $|H| = m$ . dengan Teorema 2.5.5 diperoleh orde  $(a^k) = n / \text{ppb}(k, n) = m$  sehingga  $n = m \cdot \text{ppb}(k, n)$ , artinya  $m$  membagi  $n$ .

Pada kenyataannya  $Z_6$  mempunyai subgrup tunggal untuk setiap orde yang ditentukan. Secara umum suatu grup siklik hingga berorde  $n$  mempunyai subgrup tunggal berorde  $m$  jika  $m$  membagi  $n$ . Pernyataan ini akan dibuktikan pada teorema berikut :

Teorema 4.2. [Saracino, hal. 50]. Jika  $G$  adalah grup siklik hingga berorde  $n$  dengan pembangun  $a \in G$ , maka untuk setiap pembagi positif  $d$  dari  $n$ ,  $G$  mempunyai subgrup tunggal berorde  $d$ .

Bukti, Jika  $d \mid n$ , maka terdapat bilangan bulat positif  $n$  sehingga  $n = du$ . Karena  $u \mid n$ , maka  $\text{ppb}(u, n) = u$ . berdasarkan Teorema 2.5.5 diperoleh  $a^u$  membangun subgrup berorde  $n / \text{ppb}(n, u) = n / u = d$ .

Akan diperlihatkan bahwa  $G$  mempunyai subgrup tunggal berorde  $d$ . Asumsikan bahwa  $H$  dan  $H$  adalah subgrup dari  $G$ , dengan  $|H| = |H| = d$  dan  $d \mid n$ . Karena  $d \mid n$ , maka terdapat bilangan bulat positif  $k$  dan  $k$  sehingga  $dk$  dan  $dk \mid n$ . Teorema 2.6.4.

menjamin bahwa  $H$  dan  $H'$  adalah grup siklik karena  $G$  adalah grup siklik. Misalkan  $H = \langle a^k \rangle$

Berdasarkan Teorema 2.5.5.  $\langle a^k \rangle = \text{ppb}(k, n)$  dan  $I(a^k) = I_n / \text{ppb}(k, n)$ . Karena  $k \perp n$ , maka  $\text{ppb}(k, n) = k$  dan karena  $k \perp n$ , maka  $\text{ppb}(k', n) = k'$ . Sehingga diperoleh  $nk = nk'$  atau  $Ic = Ic'$ . Karena  $k = k'$ , maka  $|\langle a^k \rangle| = |\langle a^{k'} \rangle|$  atau  $H = H'$

Kasus kedua, yaitu bila  $\text{ppb}(r, n) = 1$ .

Teorema 4.3. [Gallian, hal.69] *Jilijj G adalah grup siklik hingga berorde  $n$  dengan unsur pembangun dari  $a \in G$ , maka  $a^r \in G$  adalah unsur pembangun dari grup  $G$  jika dan hanya  $r$  dan  $n$  adalah bilangan yang prima relative atau  $\text{ppb}(r, n) = 1$*

Bukti Andaikan  $r$  dan  $a$  adalah bilangan yang prima relatif akan diperlihatkan bahwa  $G = \langle a^r \rangle = \{a^i : 0 \leq i < n, Ic \in Z\}$ . Cukup diperlihatkan bahwa  $a \in \langle a^r \rangle$  sehingga semua perpangkatan  $a$  berada di  $\langle a^r \rangle$ . Jika  $r$  dan  $n$  adalah bilangan yang prima relatif atau  $\text{ppb}(r, n) = 1$ , maka Teorema 2.1.6. menjamin untuk bilangan bulat positif  $r$  dan  $n$  terdapat bilangan bulat  $s$  dan  $t$  sehingga  $rs + nt = 1$ , Diperoleh  $a = a^{rs + nt} = (a^{rs})^s = (a^{ns})^t = a^{er} = a^e$

Karena  $a$  dapat dinyatakan sebagai perpangkatan dari  $a^r$ , maka  $a \in \langle a^r \rangle$  sehingga  $G = \langle a^r \rangle$  dan  $d = \text{ppb}(rn) = d$  dan  $d$

Sebaliknya, andaikan  $G = \langle a^d \rangle$  akan diperlihatkan bahwa  $r$  dan  $n$  adalah bilangan yang prima relative. Akan dibuktikan dengan kontraposisifnya, yaitu bila  $r$  dan  $n$  adalah bilangan yang prima relative, maka  $d$  bukan unsur pembangun dari  $G$ . misalkan  $\text{ppb}(r, n) = d$  dan  $d \neq 1$  dengan demikian terdapat bilangan bulat positif  $s$  dan  $t$  sehingga  $rs + nt = d$  dan  $dn$ . Akibatnya  $(a^{dn})^s = (a^{ds})^t =$  karena orde  $(a) = n$ ,

Maka  $a^{rt} = e$ . karena  $t < n$ , maka orde  $(d) < n$  berarti  $d$  bukanlah unsur pembangun dari  $G$ .

Kasus ketiga, yaitu bila  $\text{ppb}(r, n) = d$  dengan  $d \neq 1$

Untuk kasus yang ketiga sebagai perluasan dari Teorema 4.3 akan dibuktikan akibat berikut,

Akibat 4,4 andaikan  $G$  adalah suatu grup siklik hingga berorde  $n$  dengan unsur pembangun  $a \in G$ . jika  $d \in G$  dengan  $\text{ppb}(r, n) = d$ , maka  $\langle d \rangle = \langle a^d \rangle$

Bukti, Pernyataan diatas akan diperlihatkan dengan dua cara

### Cara pertama

Asumsikan  $\text{ppb}(r, n) = d$  artinya  $d \mid r$  dan  $d \mid n$ . berdasarkan teorema 2.5.5 diperoleh  $|\langle d \rangle| = n/d$ . karena  $d \mid n$ , maka  $\text{ppb}(d, n) = d$  sehingga  $|\langle d \rangle| = n/d$ . teorema 2.4.4 dan teorema 2.6.4 menjamin bahwa  $\langle d \rangle$  dan  $\langle a^d \rangle$  adalah subgroup dari  $G$ . karena orde dari  $\langle a \rangle$  dan  $\langle a^d \rangle$  sama yaitu  $|\langle d \rangle| = |\langle a^d \rangle| = n/d$  maka teorema 4.2 menjamin bahwa  $G$  mempunyai subgroup tunggal untuk setiap orde yang ditentukan. Sehingga  $\langle d \rangle = \langle a^d \rangle$ .

### Cara kedua

Jika  $\text{ppb}(r, n) = d$ , maka Teorema 2.1.8 menjamin bahwa  $\text{ppb}(r/d, n/d) = 1$  karena  $d \mid n$ , maka  $\text{ppb}(d, n) = d$  sehingga berdasarkan Teorema 2.5.5  $a^d$  akan membangun subgroup berorde  $n/d$ . misalkan  $y = a^d$ , sehingga diperoleh  $\langle y \rangle = \{y^1 y^2 \dots y^{n/d}\}$  karena  $\text{ppb}(r/d, n/d) = 1$ , maka menurut Teorema 4.3 diperoleh bahwa  $\langle y \rangle = \langle y^{r/d} \rangle$  sehingga  $\langle (a^d)^{r/d} \rangle = \langle a^d \rangle = \langle a^d \rangle$  atau  $\langle d \rangle = \langle a^d \rangle$ .

Dari teorema 4.1., Teorema 4.2., Teorema 4.3., dan akibat 4.4 dapat dilihat bahwa subgroup – subgroup yang dapat dibangun dari grup siklik hingga berorde  $n$  sangat bergantung pada pembagi persekutuan terbesar dari  $r$  dan  $n$  dengan  $0 < r < n$ . untuk semua  $0 < r < n$  banyaknya  $\text{ppb}(r, n)$  sama dengan banyaknya pembagi positif dari  $n$ . dari uraian diatas dapat diperoleh suatu akibat yaitu :

Akibat 4.5 Jika  $G$  adalah suatu grup siklik hingga berorde  $n$ , maka banyaknya subgroup dari  $G$  sampai dengan banyaknya pembagi positif dari  $n$ .

Dengan mengasumsikan grup siklik hingga tersebut adalah  $Z_n$ , maka diperoleh akibat berikut:

1. unsur  $u \in Z_n$  adalah unsur pembangun dari  $Z_n$ , jika dan hanya jika  $U$  dan  $n$  adalah bilangan prima yang prima relative atau  $\text{ppb}(u, n) = 1$
2. bila  $s \in Z_n$ , dengan  $\text{ppb}(u, n) = s$ , maka  $\langle u \rangle = \langle s \rangle$
3. banyaknya subgroup dari  $Z_n$  sama dengan banyaknya pembagi positif dari  $n$

Sebelum menyusun suatu program untuk menyelesaikan suatu permasalahan yang paling utama dilakukan adalah mempelajari dan memahami prosedur kerja dan langkah-langkah penyelesaian masalah tersebut.

Prosedur kerja dan langkah-langkah penyelesaian tersebut dapat digambarkan dalam diagram air (flowchart) dan dituliskan dalam suatu algoritma yang memberikan langkah-langkah urutan pengerjaan suatu program dari awal sampai akhir.

*Algoritma menentukan subgrup-subgrup dari grup siklik hingga*

Algoritma ini digunakan untuk menentukan subgrup-subgrup dari grup siklik hingga berorde  $n$ . sebagai masukan input adalah orde dari suatu group siklik hingga yaitu  $n$ , sebagai keluaran output adalah subgrup-subgrup yang dibangun oleh unsur-unsur dari grup tersebut dan banyaknya subgrup. Algoritma selengkapnya adalah sebagai berikut :

Algoritma untuk menentukan subgrup dari grup siklik hingga (procedure subgrup)

Input : Orde dari grup,  $n$   
 Output : Daftar dari subgrup  
 Langkah 1 : For  $i$ : 1 to  $n$  do langkah 2-3  
 Langkah 2 : Set  $k$  :  $n \bmod i$   
 Langkah 3 : If  $K=0$ , then

Write ('< $i$ >' = ' $\cdot$ ')  
 Set  $j$  : = 0  
 While ( $j \leq n - i$ ) do  
 Write ( $j$ )  
 $j$  : =  $j + i$

Algoritma untuk menentukan Subgrup yang dibangun oleh unsur tertentu (Procedure Bangun)

Input : Orde dari grup,  $n$ , Unsur pembangun subgrup,  $m$   
 Output : Daftar unsur dari subrup yang dibangun oleh  $m$

Langkah 1 : set  $i = \text{ppb}(m,n)$   
 Langkah 2 : Write ('< $m$ >' = ' $\cdot$ ')  
 Langkah 3 : set  $j$  : 0  
 Langkah 4 : while ( $j \leq n-1$ ) do  
 Write ( $j$ )  
 $j$  : =  $j + i$

Algoritma untuk menentukan Pembagi persekutuan terbesar (Function ppb ( $m,n$ ))

Input : dua bilangan bulat positif  $m,n$   
 Output : ppb ( $m,n$ )  
 Langkah 1 : Set  $a = m$   
 $b = n$   
 $d = a*b$

langkah 2 : While ( $d \neq 0$ ), do langkah 3

langkah 3 : if ( $b \leq a$ ), then langkah 4 :  
 $\text{ppb} := b$   
 $a := a-b$   
 else  
 $b := b-a$

#### 4. KESIMPULAN

Untuk menentukan subgrup- subgrup dari grup siklik hingga  $n$  dapat dilakukan melalui grup bilangan bulat modulo  $n$  dengan operasi penjumlahan  $Z_n$ . hal ini disebabkan bahwa setiap grup siklik hingga berorde  $n$ , isomorfik dengan  $Z_n$ .

Untuk grup dengan orde yng semakin tinggi dibutuhkan perhitungan yang lama, sehingga cara manual tidaklah efisien. Dengan menggunakan komputer perhitungan yang dilakukan akan lebih efisien.

Karena sifat numeric dari  $Z_n$ . maka dapat dibuat suatu program yang hanya memerlukan komputasi numerik biasa. Bahasa pemograman pascal dapat digunakan sebagai penyelesaian untuk menentukan subgrup-subgrup dari suatu grup siklik hingga

#### DAFTAR PUSTAKA

- Durbin J.R, Modern Algebra and Introduction, John Wiley and Sons Incorporation, New York, 1985.  
 Fraleigh, SB, *A First Course in Abstract Algebra*, Addison Wesley Publishing Company, Massachusetts,1993.  
 Gallian, J.A, *Contemporary Abstract Algebra*, D.C.Heath and Company, Canada, 1990  
 Rosen, K.H, *Elementary Number Theory and Its Applications*, Addison Wesley Publishing Company, Massachusetts, 1983.  
 Santosa, P.1, *Peniograman Pascal Tingkat Lanjut*, Andi Offset, Yogyakarta, 1989.  
 Saracino, Dan, *Abstract Algebra A First Course*, Addison Wesley Publishing Company, Massachusetts, 1980.