ISSN 2541-1004

MENENTUKAN GRUP SIKLIK HINGGA DENGAN PASCAL

Elfi fauziah[1], Riswal Hanafi Siregar[2]
[1,2]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 pemograman pascal. Grup (G) disebut siklik, bila ada elemen a $\in$ G sedemikian hingga G = $\{a^n \mid n \in Z\}$. 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 pemograman, 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 mrupakan 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 = xx = 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 sikilk hingga, hanya dipenlukan komputasi numenik biasa. B hasapemograman, seperti Pascal dapat dipergunaakan sebagal alternatifuntuk menentukan subgrup—subgrup dani 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 numenik 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, .) disebut siklik, bila ada elemen a $\in$ G sedemikian hingga G =$\{a^n \mid n \in$

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

Grup (G,+) disebut siklik, bila ada elemen a ∈ G sedemikian hingga G ={na | n ∈ Z}.

Sehingga secara umum dapat ditulis

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

A.Teorema

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

Bukti.

1. Akan ditunjukkan bahwa H merupakan subgrup atas G. Ambil sebarang ar,as ∈ H untuk suatu r,s ∈ Z .

$a^r * a^s$ = (a*a*a*…*a) (a*a*a*…*a)

r kali s kali

= (a*a*a*…*a)

r+s kali

= a^{r+s}

dan $r+s \in Z$ akibatnya $a^r * a^s \in H$. 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 a1 = a∈H, dan karena an ∈H untuk setiap n ∈ Z a ∈ H⊆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, .). Tentukan Grup Siklik dari Grup tersebut.

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

[-1] = {$(-1)^n$ | n ∈ Z}

= {$(-1)^0$, $(-1)^1$, $(-1)^2$, …}

= {-1, 1}

[1] = {$(1)^n$ | n ∈ Z}

= {$(1)^0$, $(1)^1$, $(1)^2$, …}

= {1}

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

[0] = {n(0) | n ∈ Z}

= {0}

[1] = {n(1) | n ∈ Z}

= {0.1, 1.1, 2.1, 3.1, …}

= {0, 1, 2, 3}

[2] = {n(2) | n ∈ Z}

= {0.2, 1.2, 2.2, 3.2, …}

= {0, 2}

[3] = {n(3) | n ∈ Z}

= {0.3, 1.3, 2.3, 3.3, …}

= {0, 3, 2, 1}

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 :

[0] = {0}

[2] = {0, 2}

B. Teorema

Setiap grup siklik merupakan grup komutatif.

Bukti.

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

$g_1 * g_2 = a^r * a^s$

= a*a*…*a

r+s kali

= a^{r+s}

= a^{s+r}

= $a^s * a^r$

= $g_2 * g_1$

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 ≠ {e}, maka terdapat elemen x ∈ H dengan x ≠ e .
Karena H merupakan subgrup dari G, maka x ∈ G dan berakibat x=a^n ∈ H untuk suatu n∈ Z^+ . Pilih bilangan m ∈ Z^+ sebagai bilangan yang terkecil sehingga a^m ∈ H.

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

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

dan

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

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

$a^r = a^0$ = e dan diperoleh:

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

Jadi, karena untuk sebarang y ∈H berlaku (y) = $a^{m\ \ q}$, maka <am> =H dan dengan kata lain H merupakan grup siklik.

1. Dan uraian sebelunmya dapat dilihat bahwa beberapa unsur yang berbeda membangun subgnup yang sama. Subgrup-subgrup dan Z_6 adalah 0 >0, <1> = (5), (2> = (4), dan (3), Sehingga dan uraian di atas diperoleh fakta bahwa:
   1. Bila *r*|*in,* maka subgrup yang dapat dibangun berorde *nir.*
   2. Bila *r*|*in,* maka terdapat dua kasus yaitu:
   a) Bila ppb*(r,n)* =1, maka (r) *(1)*. Pada uraian di atas diberikan oleh (1) = *(5),*
   b) Bila ppb*(r,n)*= *d* maka *(r) (ci)*. Pada uraian di atas diberikan etch <2> *<4>* Sehingga banyaknya subgrup daii 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 € G.* Untuk setiap d € G, subgrup <*d*> yang dapat dibangun oleh *d* diklasilikasikan berdasarkan pembagi persekutuan terbesar dan *r* dan n, yaitu:

a) ppb (r,n) = r,
b) ppb (r,n) = 1
c) ppb (r,n) = d, dengan d ≠ 1,

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

Kasus pertama, yaitu bila ppb(r,n) = r. Teorema 41. [Saracino, hal.50] Jika G adalah suatu grup sikilk hingga berorde n dan terdapat bilangan b positif m, maka G rnempulyat srthgrup berorde mjika dan hanya jika m membagi n.

Bukti. Andaikan a € G sehingga G <a> dan orde(a) = n. Jika *m* membagi *n* dan *H* = <$a^{m/m}$>, maka terorema 2.4.4 menjamin bahwa *H* adalah subgroup dari *G*. karena *n/m* membagi *n,* maka ppb (n/m,n) = n/m. berdasarkan terorema 2.5.5 akan diperoleh orde <$a^{m/m}$>, = n/pbb(n/mn) = n/(n/m) = m.

Andaikan <$a^{m/m}$>, adalah subgroup dari G dengan orde <$a^{m/m}$>, = *m* dan *H* = (a^k) dengan |*H*| = *m.* dengan Teorema 2.5.5 peroleh orde (a^k) = *n/*ppb (k,n) = m sehingga *n*= *m*. pbb(k,n), artinya *m* membagi *n.*

Pada kenyataannya Z_6 mempunyai subgroup tunggal untuk setiap orde yang ditentukan. Secara umum suatu group siklik hingga berorde *n* mempunyai subgroup tunggal berorde *m* jika *m* membagi *n.* Pernyataan ini akan dibuktikan pada terorema berikut :

Terorema 4.2**.** [Saracino, hal. 50]. *Jika G* adalah grup siklik hingga berorde *n* dengan pembangun a *€ G,* maka untuk setiap pembagi positif *d* dari *n, G* mempunyai subgroup tunggal berorde *d.*

Bukti, Jika d|n, maka terdapat bilangan bulat positif *n* sehingga *n = du*. Karena *U*|*n*, maka ppb *(u,n) = u.* berdasarkan Terorema 2.5.5 diperoleh a^u membangun subgrup berorde *n/*ppb (n,u) = n/n = d.

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

menjamin bahwa *H* dan *H'* adalah grup siklik karena G adalah grup siklik. Misalkan *H* = (d^k)

Berdasarkan Terorema 2.5.5. (d^k)= nppb(k,n) dan I *(at')* I n/ppb(k n). Karena *k* I a, maka ppb(k,n) *k* dan karena k ' I a, maka ppb(k',n) *Ic'*. Sehingga diperoieh *nk* = *nk'* atau *Ic* = Ic'. Karena k = k ', maka $|<a^k>|$ = $|<a^k>|$ atau H = H

Kasus kedua, yaitu bila. ppb(r,n) I.

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

Bukti Andaikan *r* dan *a* adalah bilangan yang prima relatif akan diperlihatkan bahwa G *(a7)* = *{(a:* ii E G, *Ic* E *Z}*. Cukup diperlihatkan 1,ahwa a E (d) sehiugga semua perpangkatan a berada di *at.* Jika *r* dan a adaiah bilangan yang prima relatif atau ppb(r,n) = 1, maka Teorema 2.1.6. menjamin untuk bilangan bulat positif *r* dan a terdapatbilanganbulatkdan 'a sehinggakr *rnn* 1, Diperoleh *a a1 =(af* "n - *aa = a"= a(er= ae*

Karena a dapat dinyatakan sebagai peqangkatan dan *at,* maka a c *cat)* sehingga G = *d. ppb(rn) = d* dan *d*

Sebaliknya, andaikan *G* = *d* akan diperlihatkan bahwa *r* dan *n* adalah bilangan yang prima relative. Akan dibuktikan dengan kontrapositifnya, yaitu bila *r* dan *n* adalah bilangan yang prima relative, maka *d* bukan unsur pembangun dari G. misalkan ppb (r,n) = *d* dan *d* ≠ 1 dengan demikian terdapat bilangan bulat positif *s* dan *t* sehingga *r ds* dan *dn.* Akibatnya $(a^{dt})^s = (a^{ds})^t$ = 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 ppb (r,n) = d dengan d≠ 1

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

Akibat 4,4 andaikan G adalah suatu group siklik hingga berorde n dengan unsur pembangun a € G. jika d € G dengan ppb (r,n) = d, maka $<d> = <a^d>$

Bukti, Pernyataan diatas akan diperlihatkan dengan dua cara

Cara pertama

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

Cara kedua

Jika ppb (r,n) = d, maka Terorema 2.1.8 menjamin bahwa ppb (r/d,n/d) = karena d|n, maka ppb (d,n) = d sehingga berdasarkan Terorema 2.5.5 a^d akan membangun subgroup berorde n/d. misalkan y = ad, sehingga diperoleh $<y>$ ={y1y2……yn/d} karena ppb (r/d,n/d) =1, maka menurut Terorema 4.3 diperoleh bahwa $<y> = <yr/d>$ sehingga $<(ad)r/d> = (ad> = <ad>$ atau $<d> = <ad>$.

Dari terorema 4.1., Terorema 4.2., Terorema 4.3., dan akibat 4.4 dapat dilihat bahwa subgroup – subgroup yang dapat dibangun dari group siklik hingga berorde n sangat bergantung pada pembagi persekutuan terbesar dari r dan n dengan 0 <r<n. untuk semua 0 < r < n banyaknya 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 group siklik hingga berorde n, maka banyaknya subgrup dari G sampai dengan banyaknya pembagi positif dari n.

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

1. unsur u € Z_n adalah unsur pembangun dari $Z_{n,}$ jika dan hanya jika U dan n adalah bilangan prima yang prima relative atau ppb (u,n) = 1
2. bila s € Z_n, dengan ppb (u,n) = s, maka $<u> = <s>$
3. banyaknya subgrup 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-subrup 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 mod, i
Langkah 3 : If K= 0, then

Write (‘<i>’ = ‘)
Set*j : = 0*
While *(j ≤ 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* = ppb (m,n)
Langkah 2 : Write (‘<m>’=’)
Langkah 3 : set *j* : 0
Langkah 4 : while *(j ≤ 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≠0), do langkah 3
langkah 3 : if (b ≤ a), then langkah 4 :
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, l990

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.