GRUP FUNGSI BILINEAR ATAS HIMPUNAN BILANGAN BULAT MODULO-P

SKRIPSI

Diajukan untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Pendidikan
Program Studi Pendidikan Matematika

Oleh :

GREGORIUS ASIH ATIN AGUNG SAPUTRA

NIM : 991414027

PROGRAM STUDI PENDIDIKAN MATEMATIKA
JURUSAN PENDIDIKAN DAN ILMU PENGETAHUAN ALAM
FAKULTAS KEGURUAN DAN ILMU PENDIDIKAN
UNIVERSITAS SANATA DHARMA
YOGYAKARTA
2004

SKRIPSI

GRUP FUNGSI BILINEAR ATAS HIMPUNAN BILANGAN BULAT MODULO-P

Yang disusun oleh :

GREGORIUS ASIH ATIN AGUNG SAPUTRA

NIM : 991414027

Telah disetujui oleh :

Pembimbing

Wanty Widjaja, S. Pd., M. Ed.

Tanggal : 2 April 2004

Pengesahan Skripsi Berjudul

GRUP FUNGSI BILINEAR ATAS HIMPUNAN BILANGAN BULAT MODULO-P

Yang dipersiapkan dan ditulis oleh :

GREGORIUS ASIH ATIN AGUNG SAPUTRA

NIM : 991414027

Dipertahankan di hadapan Panitia Penguji Skripsi
Fakultas Keguruan dan Ilmu Pendidikan
Universitas Sanata Dharma
Pada tanggal : 24 Maret 2004

Susunan Panitia Penguji

	Nama lengkap	Tanda Tangan
Ketua	: Drs. A. Atmadi, M. Si.	
Sekretaris	: Drs. Th. Sugiarto, MT.	
Anggota	: Wanty Widjaja, S. Pd., M. Ed.	
Anggota	: Drs. A. Mardjono	
Anggota	: M. Andy Rudhito, S. Pd., M. Si.	

Yogyakarta, 24 Maret 2004
Fakultas Keguruan dan Ilmu Pendidikan
Universitas Sanata Dharma
Dekan,

Dr. A. M. Slamet Soewandi, M. Pd.

HALAMAN PERSEMBAHAN

"Jika seseorang ingin menjadi yang terdahulu, hendaklah

ia menjadi yang terakhir dari semuanya dan pelayan dari semuanya"

(Markus 9 : 35)

Dengan segenap ketulusan hatiku, kupersembahkan skripsi ini buat :

Simbah Kakung – Putri, sebagai tanda terima kasihku

Bapak – Ibu Al. Samiutama, sebagai tanda bakti dan terima kasihku

Mas Widodo, Mbak Yayuk, sebagai tanda kasih dan sayangku

Sisca, sebagai cintaku

My friends Angkatan'99

PERNYATAAN KEASLIAN KARYA

Saya menyatakan dengan sesungguhnya bahwa skripsi yang saya tulis ini tidak memuat karya atau bagian karya orang lain, kecuali yang telah disebutkan dalam kutipan dan daftar pustaka, sebagaimana layaknya karya ilmiah.

Yogyakarta, 24 Maret 2004

Penulis

Gregorius Asih Atin Agung Saputra

KATA PENGANTAR

Puji dan syukur kehadirat Tuhan Yang Maha Kuasa, karena atas kasih dan karunia-Nya, penulis dapat menyelesaikan skripsi yang berjudul ***GRUP FUNGSI BILINEAR ATAS HIMPUNAN BILANGAN BULAT MODULO-P*** ini. Skripsi ini merupakan salah satu syarat untuk mencapai jenjang kesarjanaan S1 pada Fakultas Keguruan dan Ilmu Pendidikan Universitas Sanata Dharma Yogyakarta sekaligus sebagai upaya memperdalam dan memperkaya wawasan berpikir pada umumnya.

Dalam penulisan skripsi ini penulis memperoleh banyak bantuan dari berbagai pihak. Oleh karena itu penulis mengucapkan banyak terima kasih kepada :

1. Ibu Wanty Widjaja, S. Pd., M. Ed., selaku Dosen Pembimbing yang telah memberikan saran dan masukan demi terselesaikannya skripsi ini.
2. Bapak Drs Th. Sugiarto, MT. selaku Kaprodi yang telah memberikan saran dan masukan selama kuliah.
3. Bapak Dr. St. Suwarsono selaku Dosen Pembimbing Akademik yang telah memberikan bimbingan selama studi.
4. Segenap Dosen PMIPA / MIPA Universitas Sanata Dharma yang telah membantu penulis selama masa kuliah.
5. Staf Perpustakaan Universitas Sanata Dharma atas pelayanan dan fasilitas yang telah diberikan.
6. Bapak dan Ibu, Simbah, Adik, Mas Widodo, Mbak Yayuk yang telah memberikan bantuan, dukungan dan doa.

7. Adikku *Sisca* terkasih dan tersayang atas waktu, doa dan dukungan yang telah diberikan selama ini.
8. My best friends : Wury, Agus, Taoge, Yati atas keceriaan dan kesusahan yang telah kita alami bersama.
9. Teman-teman Angkatan'99 : Krecek, Yuli, Asih, Anna, Krupuk, Cicil, Anas, Heni, Heti, dkk atas kebersamaan selama kuliah.
10. Segenap pihak yang tidak dapat penulis sebutkan satu persatu yang telah membantu penulis dalam menyusun skripsi ini.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna, oleh karena itu segala kritik dan saran dari pembaca yang sifatnya membangun sangat penulis harapkan guna penyempurnaan skripsi ini. Akhirnya semoga skripsi ini bermanfaat bagi pembaca khususnya mahasiswa Program Studi Pendidikan Matematika.

Yogyakarta, Maret 2004

Penulis

(Gregorius Asih Atin Agung Saputra)

DAFTAR ISI

ABSTRAK

Fungsi bilinear atas himpunan bilangan bulat modulo-p mempunyai bentuk umum $f(x) = \dfrac{ax+b}{cx+d}$ dengan a, b, c, d $\in Z_p$ dan $ad - bc \neq 0$. Himpunan semua fungsi bilinear atas himpunan bilangan bulat modulo-p dengan operasi komposisi fungsi membentuk suatu Grup yang disebut Grup Fungsi Bilinear atas Himpunan Bilangan Bulat Modulo-p dan dinotasikan $GFBZ_p$.

Pusat dari Grup $GFBZ_p$ adalah fungsi f dengan $f(x) = x$. Order dari $GFBZ_p$ atau $|GFBZ_p|$ adalah $p^3 - p$. Setiap fungsi bilinear dalam $GFBZ_p$ mempunyai paling banyak 2 titik tetep (sikel yang panjangnya 1). Grup $GFBZ_p$ beraksi pada himpunan P_p ($Z_p + \{\infty\}$), sehingga P_p merupakan himpunan-$GFBZ_p$.

ABSTRACT

Bilinear function over the set of integers modulo-p has form of $f(x) = \dfrac{ax+b}{cx+d}$ with a, b, c, d $\in Z_p$ and $ad - bc \neq 0$. The set of bilinear function over the set of integers modulo-p with respect to composition function forms a Group called Group of Bilinear Function over Modulo-p and denoted by $GFBZ_p$.

The center of $GFBZ_p$ is an identity function f defined by f (x) = x. Order of $GFBZ_p = |GFBZ_p|$ is $p^3 - p$. Every bilinear function of $GFBZ_P$ has at most 2 fixed points (cycle with length 1). Group $GFBZ_p$ acts on a set P_p ($Z_p + \{\infty\}$), so P_p is $GFBZ_p$-set.

BAB I

PENDAHULUAN

A. Latar Belakang

Fungsi merupakan salah satu topik penting dalam matematika. Ada berbagai macam bentuk fungsi misalnya fungsi konstan, fungsi linear, fungsi trigonometri dan fungsi kuadrat. Istilah fungsi-fungsi di atas sudah sering kita dengar pada waktu kita duduk di sekolah menegah.

Ada suatu bentuk fungsi yang mungkin belum kita tahu sebelumnya yakni fungsi bilinear. Istilah fungsi bilinear mungkin masih baru bagi kita dan belum pernah kita pelajari sebelumnya, karena di sekolah menengah topik tersebut tidak dibahas. Pada penulisan ini, penulis ingin mempelajari mengenai fungsi bilinear atas himpunan bilangan bulat modulo-p (Z_p).

Bentuk umum dari fungsi bilinear atas himpunan bilangan bulat modulo-p (Z_p) yakni $f(x) = \dfrac{ax+b}{cx+d}$, dengan a, b, c, d $\in Z_p$ dan $ad - bc \neq 0$. Himpunan fungsi bilinear atas himpunan Z_p memiliki struktur dan sifat-sifat khusus. Pada penulisan ini akan dibahas struktur dan sifat-sifat khusus dari himpunan semua fungsi bilinear atas himpunan Z_p.

B. Perumusan Masalah

Pokok perumusan masalah yang akan dibahas dalam penulisan ini dapat dirumuskan sebagai berikut :

1. Bagaimana struktur himpunan semua fungsi bilinear atas himpunan Z_p ?
2. Bagaimana hubungan antara struktur dari himpunan semua fungsi bilinear atas himpunan Z_p dengan struktur grup khususnya mengenai pusat dari grup dan aksi grup pada himpunan ?

C. Tujuan Penulisan

Tujuan dari penulisan ini adalah mempelajari struktur himpunan semua fungsi bilinear atas himpunan Z_p, termasuk menemukan rumus umum untuk mencari order dari himpunan semua fungsi bilinear atas himpunan Z_P, dan mencari hubungan antara struktur dari himpunan semua fungsi bilinear atas himpunan Z_p dengan struktur grup khususnya mengenai pusat dari grup dan aksi grup pada himpunan.

D. Manfaat Penulisan

Manfaat dari mempelajari grup fungsi bilinear atas himpunan Z_p adalah dapat mengetahui struktur dari himpunan semua fungsi bilinear atas himpunan Z_P.

E. Sistematika Penulisan

Adapun sistematika dalam penulisan ini adalah sebagai berikut : Bab pertama membahas tentang gambaran umum dari tulisan ini.

Bab dua membahas tentang materi prasyarat sebagai landasan teori dari tulisan ini yaitu tentang grup, sikel dan aksi grup pada himpunan.

Bab tiga membahas tentang pengertian dan sifat-sifat fungsi dan bilangan bulat modulo-p (Z_P) kemudian dilanjutkan pembahasan mengenai fungsi bilinear atas Z_p.

Bab empat membahas struktur dari himpunan fungsi bilinear atas Z_p.

Bab lima berisi kesimpulan dan saran.

F. Metode Penulisan

Metode yang digunakan dalam penulisan ini adalah metode studi pustaka, yakni dengan mempelajari buku-buku yang berkaitan dengan grup fungsi bilinear atas Z_p.

BAB II

GRUP

Dalam bab ini akan dibahas mengenai grup beserta sifat-sifat yang mendukung untuk memahami bab-bab selanjutnya. Definisi-definisi, teorema-teorema dan beberapa contoh diberikan pula dalam bab ini. Sebelum kita mulai dengan pembahasan tentang grup, terlebih dahulu harus diketahui tentang pengertian dari operasi biner. Oleh karena itu, akan dijelaskan tentang pengertian operasi biner di bawah ini.

A. Operasi Biner

Pembahasan tentang operasi biner diawali dengan pengertian dari operasi biner dan dilanjutkan pembahasan mengenai sifat-sifat yang berlaku pada operasi biner.

Definisi 2.A.1 :

Operasi biner "$*$" pada suatu himpunan S adalah suatu aturan yang memasangkan setiap pasangan terurut $(a, b) \in S \times S$ dengan suatu elemen tunggal $c \in S$.

Jadi $\forall (a, b) \in S \times S\ (\exists! c \in S)\ (a * b = c)$.

Contoh 1 :

Penjumlahan (+) merupakan operasi biner pada himpunan semua bilangan Real

(R), sebab untuk $(\forall x, y \in R)$ $(\exists z \in R)$ $(z = x + y)$.

Pembagian bukan operasi biner pada himpunan semua bilangan Bulat, sebab $(\exists 1, 0 \in Z)$ $\left(\frac{1}{0} \notin Z\right)$.

Definisi 2.A.2 :

Suatu operasi biner "$*$" pada himpunan S dikatakan bersifat asosiatif bila dan hanya bila dipenuhi $(\forall a, b, c \in S)$ $a * (b * c) = (a * b) * c$.

Definisi 2.A.3 :

Suatu elemen e dalam himpunan S disebut elemen identitas terhadap suatu operasi "$*$" pada himpunan S bila dan hanya bila $(\forall a \in S)$ $e * a = a * e = a$.

Contoh 2 :

- Fungsi f (x) = x adalah elemen identitas terhadap operasi komposisi fungsi pada himpunan fungsi linear.

Definisi 2.A.4 :

Diketahui "$*$" adalah operasi biner pada suatu himpunan S dengan elemen identitas e dan sembarang $a \in S$. Suatu elemen $b \in S$ disebut invers dari a terhadap "$*$" bila dan hanya bila dipenuhi $a * b = b * a = e$.

Contoh 3 :

- Pada himpunan semua fungsi linear f (x) = ax + b, a $\neq$ 0, yang mempunyai elemen identitas f (x) = x, maka invers dari fungsi g (x) = ax + b adalah fungsi h (x) = $\dfrac{x - b}{a}$.

Definisi 2.A.5 :

Suatu operasi "$*$" pada himpunan S disebut komutatif jika dan hanya jika dipenuhi $(\forall a, b \in S)\ a * b = b * a$.

Contoh 4 :

- Operasi komposisi fungsi pada himpunan semua fungsi linear tidak komutatif, sebab ada f (x) = 2x dan g (x) = x + 1 sehingga (f o g) (x) = 2x + 2 dan (g o f) (x) = 2x +1. Jadi (f o g) $\neq$ (g o f).

B. Grup

Pada subbab ini akan dibahas tentang grup. Pembahasan mengenai grup diawali dengan pengertian grup dan dilanjutkan dengan sifat-sifat yang berlaku pada grup.

Definisi 2.B.1 :

Suatu himpunan tidak kosong G dengan operasi biner "$*$" pada G disebut grup bila dan hanya bila memenuhi aksioma-aksioma berikut ini :

1. Operasi $*$ bersifat asosiatif, yaitu

   $(\forall a, b, c \in G)\ (a * b) * c = a * (b * c)$.

2. Mempunyai elemen identitas

   $(\exists e \in G)\ (\forall a \in G)\ a * e = e * a = a$.

3. Setiap elemen dalam G mempunyai invers

   $(\forall a \in G)\ (\exists b \in G)\ a * b = b * a = e$.

Contoh 5 :

- Z merupakan himpunan bilangan bulat. Z dengan operasi penjumlahan ditulis (Z, +) merupakan suatu grup.
- $M = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| \ a, b, c, d \in R \wedge ad - bc \neq 0 \right\}$. (M, .) merupakan grup terhadap operasi perkalian matriks.

Definisi 2.B.2 :

Suatu grup $(G, *)$ disebut grup Abelian jika dan hanya jika operasi "$*$" dalam G bersifat komutatif yakni $(\forall a, b \in G)\ a * b = b * a$.

Contoh 7 :

- (Z, +) merupakan grup Abelian sebab

  $(\forall a, b \in Z)\ (a + b = b + a)$.

- $M = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| \ a, b, c, d \in R \wedge ad - bc \neq 0 \right\}$, (M, .) bukan grup Abelian

  sebab jika diambil matriks $A = \begin{bmatrix} 2 & 2 \\ 1 & 2 \end{bmatrix}$ dan $B = \begin{bmatrix} 3 & 4 \\ 4 & 1 \end{bmatrix}$ maka

  $AB = \begin{bmatrix} 2 & 2 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 3 & 4 \\ 4 & 1 \end{bmatrix} = \begin{bmatrix} 14 & 10 \\ 11 & 6 \end{bmatrix}$ dan

  $BA = \begin{bmatrix} 3 & 4 \\ 4 & 1 \end{bmatrix} \begin{bmatrix} 2 & 2 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 10 & 14 \\ 9 & 10 \end{bmatrix}$

  Sehingga $AB \neq BA$.

Selanjutnya akan dibuktikan bahwa dalam grup (G, $*$) ada tepat satu elemen identitas dan setiap elemen mempunyai invers yang tunggal.

Teorema 2.B.1 :

Andaikan (G, $*$) grup, maka :

a) Elemen identitas dari (G, $*$) adalah tunggal.

b) Setiap elemen dalam (G, $*$) mempunyai invers yang tunggal.

Bukti :

a) Misalkan e dan f adalah elemen identitas dari G, maka

   $e * f = f * e = f$ (e elemen identitas)

$e * f = f * e = e$ (f elemen identitas)

Karena hasil operasi adalah tunggal maka $e = f$.

Terbukti bahwa elemen identitas dari G adalah tunggal. ■

b) Misalkan x, y adalah invers dari $a \in G$.

Karena $x = x * e$ maka

$$
\begin{aligned}
x &= x * (a * y) \\
&= (x * a) * y \quad \text{(asosiatif)} \\
&= e * y \\
&= y \\
x &= y
\end{aligned}
$$

Terbukti bahwa invers dari setiap elemen dalam G adalah tunggal. ■

Definisi 2.B.3 :

Banyaknya elemen dari suatu grup G disebut order grup G dan dinotasikan dengan $|G|$. Jika banyaknya elemen dalam G tak hingga, maka G disebut grup tak hingga (*infinite grup*), sedangkan jika banyaknya elemen dalam G berhingga, maka G disebut grup berhingga (*finite grup*).

Dalam suatu grup G kita mengenal pusat dari grup G yakni himpunan anggota G yang komutatif dengan setiap elemen G. Berikut didefinisikan pengertian pusat dari grup G.

Definisi 2.B.4:

Diketahui $(G,*)$ grup, pusat dari grup G yakni $Z(G) = \{x \in G \mid (\forall y \in G)(x * y = y * x)\}$.

C. Subgrup

Suatu himpunan bagian yang tidak kosong dari suatu grup G yang memenuhi aksioma-aksioma grup disebut subgrup. Berikut ini akan dibahas subgrup dan sifat-sifat yang terkait dengan subgrup yang tertuang dalam beberapa teorema di bawah ini.

Definisi 2.C.1 :

Jika $(G, *)$ grup dan $H \subseteq G$ maka H disebut subgrup dari G bila H merupakan grup dengan operasi "$*$".

Teorema 2.C.1 :

Jika $(G, *)$ grup dan $H \subseteq G$ maka H adalah subgrup dari G bila dan hanya bila

(a) $H \neq \phi$.

(b) $\forall a, b \in H$ maka $a * b \in H$.

(c) $\forall a \in H$ maka $a^{-1} \in H$.

Bukti :

($\Rightarrow$)

- $H \neq \phi$, karena H sekurang-kurangnya memuat elemen identitas.
- Kondisi b dan c pasti dipenuhi karena diketahui $(H, *)$ grup.

($\Leftarrow$)

(1) Sifat tertutup pada H terpenuhi karena kondisi b terpenuhi.

(2) Sifat asosiatif pada H terpenuhi karena $H \subseteq G$ dan G grup.

(3) Ambil sembarang $a \in H$ $(H \neq \phi)$, maka menurut syarat (c) ada $a^{-1} \in H$ dan dari syarat (b), $a * a^{-1} = e \in H$, sehingga terdapat $e \in H$.

(4) Menurut syarat (c) setiap elemen dalam H mempunyai invers dalam H.

Dari (1), (2), (3) dan (4) disimpulkan bahwa $(H, *)$ merupakan subgrup dari $(G, *)$. ■

D. Koset

Dalam subbab ini akan dibahas pengertian koset dan beberapa sifat yang terkait. Pembahasan tentang koset diawali dengan definisi tentang relasi ekuivalensi.

Definisi 2.D.1 :

Suatu relasi "~" di dalam himpunan tidak kosong disebut relasi ekuivalensi jika relasi tersebut memenuhi :

a. Sifat refleksif yakni $(\forall a \in S)\ a \sim a$.

b. Sifat simetris yakni $(\forall a, b \in S)$ jika $a \sim b$ maka $b \sim a$.

c. Sifat transitif yakni $(\forall a, b, c \in S)$ jika $a \sim b$ dan $b \sim c$ maka $a \sim c$.

Teorema 2.D.1 :

H subgrup dari grup $(G, *)$ dan didefinisikan relasi "$\sim$" pada G sebagai berikut $a \sim b$ bila dan hanya bila $a * b^{-1} \in H$ adalah relasi ekuivalensi pada G.

Bukti :

Akan ditunjukkan bahwa "$\sim$" relasi ekuivalensi pada G.

a. Jika sembarang $a \in G$, maka $a \sim a$ karena $a * a^{-1} = e \in H$, $\forall a \in G$.

   Sifat refleksif dipenuhi.

b. Ambil sembarang $a, b \in G$.

   Jika $a \sim b$ maka $a * b^{-1} \in H$. Karena H subgrup dari G maka $(a * b^{-1})^{-1} = b * a^{-1} \in H$. Sehingga $b \sim a$.

   Sifat simetris dipenuhi.

c. Ambil sembarang $a, b, c \in G$.

   Jika $a \sim b$ dan $b \sim c$ maka $a * b^{-1} \in H$ dan $b * c^{-1} \in H$, sehingga

   $(a * b^{-1}) * (b * c^{-1}) \in H$

   $a * (b^{-1} * b) * c^{-1} \in H$

   $a * c^{-1} \in H$

   Karena $a * c^{-1} \in H$ maka $a \sim c$.

Jadi sifat transitif dipenuhi.

Dari a, b, dan c terbukti bahwa "~" merupakan relasi ekuivalensi pada G. ■

Jika pada G diberikan relasi ekuivalensi "~" maka G akan terpartisi menjadi kelas-kelas ekuivalensi yang saling asing. Berikut akan didefinisikan pengertian kelas ekuivalensi.

Definisi 2.D.2 :

Jika "~" adalah relasi ekuivalensi pada G maka $[a] = \{b \in G \mid b \sim a\}$ disebut kelas ekuivalensi yang memuat a.

Definisi 2.D.3 :

Diketahui $(G, *)$ grup, $a \in G$ dan H subgrup dari G himpunan $Ha = \{h * a \mid h \in H\}$ disebut koset kanan dari H dalam G sedangkan himpunan $aH = \{a * h \mid h \in H\}$ disebut koset kiri dari H dalam G.

Teorema 2.D.2 :

Jika H subgrup dari $(G, *)$ dan $a, b \in G$ maka empat pernyataan berikut adalah ekuivalen.

(a) $a * b^{-1} \in H$

(b) $a = h * b$, untuk suatu $h \in H$

(c) $a \in Hb$

(d) $Hb = Ha$

Bukti :

Untuk membuktikan empat pernyataan tersebut ekuivalen cukup dibuktikan (a) $\Rightarrow$ (b) $\Rightarrow$ (c) $\Rightarrow$ (d) $\Rightarrow$ (a)

(i) $a \Rightarrow b$

Diketahui $a * b^{-1} \in H$. Karena $a * b^{-1} \in H$, maka $a * b^{-1} = h$, untuk suatu $h \in H$, sehingga $a = h * b$.

(ii) $b \Rightarrow c$

Perhatikan bahwa $Hb = \{h * b \mid h \in H\}$. Karena $a = h * b$, untuk suatu $h \in H$, maka $a \in Hb$.

(iii) $c \Rightarrow d$

Akan ditunjukkan (•) $Ha \subseteq Hb$ dan (••) $Hb \subseteq Ha$.

(•) Ambil sembarang $x \in Ha$, maka $x = h * a$, untuk suatu $h \in H$.

Diketahui $a \in Hb$, maka $a = h_1 * b$, untuk suatu $h_1 \in H$ sehingga $x = h * (h_1 * b) = (h * h_1) * b = h_2 * b$, dengan $h_2 = h * h_1 \in H$.

Jadi $x = h_2 * b$, untuk suatu $h_2 \in H$ sehingga $x \in Hb$.

(••) Ambil sembarang $x \in Hb$, maka $x = h_3 * b$, untuk suatu $h_3 \in H$.

Diketahui $a \in Hb$, maka $a = h_4 * b$, untuk suatu $h_4 \in H$ sehingga $h_4^{-1} * a = b$.

$x = h_3 * (h_4^{-1} * a)$

$= (h_3 * h_4^{-1}) * a$

$= h_5 * a$, dengan $h_5 = h_3 * h_4^{-1} \in H$

Jadi $x = h_5 * a$, untuk suatu $h_5 \in H$ sehingga $x \in Ha$.

Dari (•) dan (••) maka Ha = Hb.

(iv) $d \Rightarrow a$

Diketahui Ha = Hb, akan ditunjukkan bahwa $a * b^{-1} \in H$.

Karena $a \in Ha$ dan $Ha = Hb$ maka $a \in Hb$, dengan demikian $a = h * b$, untuk suatu $h \in H$. Oleh karena $b \in G$ dan G grup, maka $b^{-1} \in G$, sehingga $h = a * b^{-1} \in H$.

Jadi $a * b^{-1} \in H$. ■

Selanjutnya akan dibuktikan bahwa banyaknya anggota-anggota dalam koset-koset yang dibangun oleh suatu subgrupnya adalah sama. Dengan kata lain jika H subgrup dari grup (G, ∗) dan a sembarang elemen G maka $|H| = |Ha|$. Tetapi sebelumnya kita definisikan dahulu pengertian fungsi, fungsi surjektif, fungsi injektif dan fungsi bijektif.

Definisi 2.D.4 :

Suatu fungsi f dari himpunan A ke himpunan B ialah suatu aturan yang mengawankan secara tunggal setiap elemen x di himpunan A dengan tepat satu elemen y di himpunan B.

Suatu fungsi f dari A ke B disajikan dengan simbol $f : A \rightarrow B$. Elemen $y \in B$ yang terkawankan dengan $x \in A$ dinyatakan dengan $y = f(x)$, sehingga fungsi ini sering ditulis $y = f(x)$, $x \in A$. Himpunan A disebut daerah asal atau domain dan himpunan B disebut daerah kawan atau kodomain. Himpunan semua nilai fungsi $f = \{y \in B \mid y = f(x) \in B\}$ dinamakan daerah hasil fungsi f.

Contoh 8 :

Misalkan $A = \{1,2,3,4\}$ dan $B = \{a,b,c,d\}$.

1. Jika $f(1) = d$, $f(2) = d$, $f(3) = b$, $f(4) = a$, maka f suatu fungsi, karena setiap elemen di A terkawankan secara tunggal dengan elemen di B.
2. Jika $f(1) = d$, $f(1) = c$, $f(3) = b$, $f(4) = a$, maka f bukan suatu fungsi, karena ada elemen di A yaitu 1 yang mempunyai 2 kawan di B yaitu c dan d.

Definisi 2.D.5 :

Suatu fungsi f dari A ke B disebut fungsi surjektif (*onto*) bila dan hanya bila setiap elemen di B merupakan bayangan dari paling sedikit satu elemen di A.

Definisi di atas dapat dinyatakan dengan simbol logika sebagai berikut :

$f : A \rightarrow B$ adalah fungsi surjektif bila dan hanya bila $(\forall y \in B)\ (\exists x \in A)\ f(x) = y$.

Contoh 9 :

Fungsi $f : R - \{0\} \rightarrow R^+$, R^+ = himpunan semua bilangan real positif dengan aturan $f(x) = x^2$ merupakan fungsi surjektif, sebab untuk semua $y \in R^+$ selalu ada $x \in R - \{0\}$ sehingga $y = f(x) = x^2$.

Definisi 2.D.6 :

Suatu fungsi dari A ke B disebut fungsi injektif bila dan hanya bila setiap elemen yang berbeda di A mempunyai kawan yang berbeda di B.

Hal ini dinyatakan dengan simbol logika sebagai berikut :

$f : A \rightarrow B$ injektif bila dan hanya bila $(\forall x_1, x_2 \in A)\ f(x_1) = f(x_2) \Rightarrow x_1 = x_2$ atau

$f : A \rightarrow B$ injektif bila dan hanya bila $(\forall x_1, x_2 \in A)\ x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$.

Contoh 10 :

Fungsi $f : R^+ \rightarrow R$ dengan aturan $f(x) = 2x$ merupakan fungsi injektif sebab untuk x_1 dan $x_2 \in R^+$ dengan $x_1 \neq x_2$ maka $2x_1 \neq 2x_2$ $(f(x_1) \neq f(x_2))$.

Definisi 2.D.7 :

Fungsi $f : A \rightarrow B$ disebut fungsi bijektif bila dan hanya bila fungsi itu merupakan fungsi surjektif dan fungsi injektif.

Contoh 11 :

Fungsi $f : R \rightarrow R$ dengan aturan $f(x) = 3x + 2$ merupakan fungsi bijektif sebab :

- Fungsi f merupakan fungsi surjektif yakni untuk semua $y \in R$ selalu ada $x = \dfrac{y-2}{3} \in R$ sehingga $y = f(x) = 3x + 2$.
- Fungsi f merupakan fungsi injektif yakni untuk x_1 dan $x_2 \in R$ dengan $x_1 \neq x_2$ maka $3x_1 + 2 \neq 3x_2 + 2$ ($f(x_1) \neq f(x_2)$).

Lemma 2.D.1 :

Jika H subgrup berhingga dari grup $(G, *)$ dan a sembarang elemen G, maka $|H| = |Ha|$.

Bukti :

Akan diperlihatkan bahwa terdapat korespondensi 1-1 antara H dan Ha, untuk itu didefinisikan suatu fungsi $\alpha : H \rightarrow Ha$, dengan aturan sebagai berikut

$f(h) = h * a, \forall h \in H$

- \- Terlebih dahulu ditunjukkan fungsi f terdefinisi dengan baik

  Ambil sembarang $h_1, h_2 \in H$ dengan $h_1 = h_2$ maka $h_1 * a = h_2 * a$, didapat $f(h_1) = f(h_2)$.

- Ambil sembarang $h_1 \in H$ maka $\exists\ h_1 * a \in Ha$ sehingga $f(h_1) = h_1 * a$.

- Ditunjukkan f injektif

  Ambil $h_1, h_2 \in H$ dengan $f(h_1) = f(h_2)$, maka $h_1 * a = h_2 * a$, dengan hukum kanselasi didapat $h_1 = h_2$. Jadi f fungsi injektif.

- Ditunjukkan f surjektif

  Ambil sembarang $x \in Ha$, maka $x = h_1 * a$, untuk suatu $h_1 \in H$, sehingga dapat ditemukan $h_1 \in H$ yang memenuhi $f(h_1) = h_1 * a = x$.

  Jadi f surjektif.

Karena terdapat korespondensi 1-1 antara H dengan Ha dan diketahui H himpunan berhingga maka $|H| = |Ha|$. ■

Teorema 2.D.3 (Teorema Lagrange) :

Jika G adalah grup berhingga dan H subgrup dari G maka order dari H membagi order dari G.

Bukti :

Perhatikan bahwa $\forall a \in G$ maka $\exists Ha$ sedemikian hingga $a \in Ha$.

Koset-koset kanan dari H merupakan kelas-kelas ekuivalensi yang membentuk partisi dari G, dan karena diketahui G berhingga, maka G dapat ditulis

$G = Ha_1 \cup Ha_2 \cup Ha_3 \cup \ldots \cup Ha_k$, dengan $a_1, a_2, a_3, \ldots, a_k \in G$.

Sehingga didapat

$|G| = |Ha_1 \cup Ha_2 \cup Ha_3 \cup \ldots \cup Ha_k|$

$= |Ha_1| + |Ha_2| + |Ha_3| + \ldots + |Ha_k|$

$= \underbrace{|H| + |H| + |H| + \ldots + |H|}_{k}$

$= k\,|H|$

Jadi order dari H membagi habis order dari G. ∎

E. Orbit dan Sikel

Pada bagian depan sudah dijelaskan tentang pemetaan atau fungsi. Untuk subbab mengenai permutasi, kita akan menggunakan dasar atau landasan dari pembahasan mengenai pemetaan atau fungsi. Definisi fungsi injektif, fungsi surjektif, dan fungsi bijektif akan digunakan dalam pendefinisian permutasi.

1. Permutasi

Definisi 2.E.1 :

Suatu permutasi pada himpunan S adalah suatu fungsi bijektif dari S ke S.

Permutasi dinotasikan dengan $\alpha : S \rightarrow S$, dengan α adalah fungsi bijektif. Jika diberikan suatu himpunan $S = \{a_1, a_2, a_3, \ldots, a_n\}$ dan α adalah fungsi bijektif yang memetakan himpunan S ke himpunan S sendiri, maka permutasi α ditulis $\begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_n \\ \downarrow & \downarrow & \downarrow & \ldots & \downarrow \\ \alpha(a_1) & \alpha(a_2) & \alpha(a_3) & \ldots & \alpha(a_n) \end{pmatrix}$. Sebagai contoh diberikan permutasi pada $S = \{1, 2, 3\}$ dengan α adalah fungsi bijektif berikut ini $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$. Ini berarti bahwa $\alpha(1) = 3$, $\alpha(2) = 2$, $\alpha(3) = 1$.

Untuk suatu himpunan $S_3 = \{1, 2, 3\}$ ada 6 permutasi yang dapat dibentuk, yaitu : $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$. Himpunan semua permutasi pada himpunan S dinotasikan dengan A (S).

Teorema 2.E.1 :

Jika S mempunyai elemen sebanyak n, maka A (S) mempunyai elemen sebanyak n!.

Bukti :

Andaikan S = {1 2 3 4 5 … n} yang mempunyai n elemen.

Misalkan $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \ldots & n \\ a & b & c & d & e & \ldots & j \end{pmatrix}$ menunjukkan sembarang permutasi dari S, maka a dapat dipilih dari sembarang elemen S yang jumlahnya n. Setelah a ditentukan, maka b dapat dipilih dari sembarang elemen S yang belum dipilihkan pada a, yang jumlahnya n – 1. Setelah a dan b dipilih, maka c dapat dipilih dari sembarang elemen S yang belum dipilihkan pada a dan b, yang jumlahnya n – 2. Proses ini berlanjut sampai j, sehingga j hanya dapat dipilih dari elemen S yang belum diisikan pada a, b, c, d, e, …, j – 1 yang jumlahnya 1.

Sehingga banyaknya permutasi yang mungkin dari S yang anggotanya n adalah n . (n – 1) . (n – 2) . (n – 3) … 2 . 1 = n!. ■

2. Komposisi Permutasi

Jika diberikan suatu permutasi $X = \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$, maka berarti $X(1) = a_1$, $X(2) = a_2$, $X(3) = a_3$, dan seterusnya. Berarti bahwa 1 oleh X dipetakan ke a_1, 2 dipetakan oleh X ke a_2, dan seterusnya. Apabila diberikan dua permutasi yang masing-masing mempunyai elemen sebanyak n, maka perkalian kedua permutasi tersebut dikerjakan pada permutasi kedua kemudian dilanjutkan permutasi yang pertama. Komposisi permutasi-permutasi akan menghasilkan permutasi, karena komposisi fungsi-fungsi bijektif menghasilkan fungsi bijektif.

Andaikan diberikan permutasi-permutasi berikut ini :

$X = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}$ dan $Y = \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$, maka komposisi kedua permutasi tersebut adalah :

$$XY = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix} \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \dots & n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}.$$

Berarti $XY(1) = b_1$, $XY(2) = b_2$, $XY(3) = b_3$, dan seterusnya.

Contoh 12 :

Diberikan permutasi-permutasi $X = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ dan $Y = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$.

Akan dicari hasil komposisi kedua permutasi tersebut.

$$XY = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Berarti bahwa XY (1) = 2, XY (2) = 3, XY (3) = 1.

Jika S = {1, 2, 3, ..., n}, maka permutasi $i \in A(S)$ yang memetakan setiap elemen ke dirinya sendiri disebut permutasi identitas, sehingga :

$$i = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2 & 3 & \dots & n \end{pmatrix}.$$

Sebelum membahas tentang sikel, terlebih dahulu akan diuraikan mengenai orbit yang menjadi dasar dalam pembentukan suatu sikel.

3. Orbit

Jika $S \neq \phi$ dan pada himpunan S diberikan relasi "~" yang didefinisikan berikut $(\forall a, b \in S)$ $(a \sim b)$ bila dan hanya bila $b = \sigma^n(a)$, $n \in Z$, maka relasi "~" merupakan relasi ekuivalensi.

Akan ditunjukkan relasi tersebut merupakan relasi ekuivalensi.

1) $(\forall a \in S)$ $a \sim a$, karena $a = 1a = \sigma^0(a)$, $0 \in Z$.

   Sifat refleksif dipenuhi.

2) Akan ditunjukkan $(\forall a, b \in S)$ $a \sim b \Rightarrow b \sim a$.

Jika $a \sim b$, maka $b = \sigma^n(a)$, $n \in Z$ dan pasti ada $-n \in Z$ sehingga $a = \sigma^{-n}(b)$, berarti $b \sim a$.

Sifat simetris dipenuhi.

3) Akan ditunjukkan $(\forall a, b, c \in S)$ $a \sim b$ dan $b \sim c \Rightarrow a \sim c$.

Jika $a \sim b$ dan $b \sim c$, maka $b = \sigma^n(a)$, $n \in Z$ dan $c = \sigma^m(b)$, $m \in Z$.

Berarti $c = \sigma^m(\sigma^n(a)) = \sigma^{m+n}(a)$, $m + n \in Z$, sehingga $a \sim c$.

Sifat transitif dipenuhi.

Jadi, relasi "$\sim$" pada S yang didefinisikan $(\forall a, b \in S)$ $a \sim b$ bila dan hanya bila $b = \sigma^n(a)$, $n \in Z$ merupakan relasi ekuivalensi yang saling asing.

Karena relasi "$\sim$" yang didefinisikan $\forall a, b \in S$, $a \sim b$ bila dan hanya bila $b = \sigma^n(a)$, $n \in Z$ merupakan relasi ekuivalensi maka "$\sim$" akan mempartisi S menjadi kelas-kelas ekuivalensi.

Jika $a \in S$ maka kelas ekuivalensi dari $a = [a] = \{b \in S \mid b \sim a\}$

$$= \{b \in S \mid b = \sigma^n(a), n \in Z\}.$$

Definisi 2.E.2 :

Kelas-kelas ekuivalensi pada himpunan S yang tertentu oleh relasi ekuivalensi : $(\forall a, b \in S)$ $a \sim b$ bila dan hanya bila $b = \sigma^n(a)$, $n \in Z$, dengan σ adalah permutasi pada himpunan S disebut suatu orbit dari σ.

Kelas ekuivalensi $[a] = \{b \in S \mid b = \sigma^n(a)\}$ disebut orbit yang memuat a.

Contoh 13 :

Diberikan S = {1, 2, 3, 4, 5, 6, 7, 8}. Tentukan orbit-orbit dari permutasi σ yang didefinisikan berikut ini.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix}, \text{ dengan } \sigma \in A(S).$$

Jawab :

Pertama, kita pilih sembarang elemen dalam S, misal 1, sehingga

$$1 \xrightarrow{\sigma} 3 \xrightarrow{\sigma} 6 \xrightarrow{\sigma} 1 \xrightarrow{\sigma} 3 \xrightarrow{\sigma} \ldots$$

Berarti orbit yang memuat 1 adalah {1, 3, 6}.

Kedua, kita pilih sembarang elemen dalam S selain anggota {1, 3, 6}.

Misalkan 2, sehingga

$$2 \xrightarrow{\sigma} 8 \xrightarrow{\sigma} 2 \xrightarrow{\sigma} 8 \xrightarrow{\sigma} \ldots$$

Orbit yang memuat 2 adalah {2, 8}.

Ketiga, kita pilih elemen lain dalam S, selain anggota {1, 3, 6} dan {2, 8}.

Misalkan kita pilih 4, sehingga

$$4 \xrightarrow{\sigma} 7 \xrightarrow{\sigma} 5 \xrightarrow{\sigma} 4 \xrightarrow{\sigma} \ldots$$

Orbit yang memuat 4 adalah {4, 7, 5}.

Semua elemen dalam S sudah termuat dalam orbit-orbit tersebut. Jadi, orbit-orbit dari permutasi σ adalah {2, 8}, {1, 3, 6}, {4, 7, 5}.

Untuk elemen yang tetap / dipetakan ke dirinya sendiri, artinya $\sigma(a) = a$, $a \in S$, maka orbit yang memuat a adalah {a}.

4. Sikel

Definisi 2.E.3 :

Suatu permutasi $\sigma \in$ A (S) disebut sikel, jika permutasi tersebut mempunyai paling banyak satu orbit yang memuat lebih dari satu elemen.

Pada himpunan S = {1, 2, 3, 4, 5, 6, 7, 8} dan σ adalah permutasi dalam A (S) yang didefinisikan pada contoh di atas, menghasilkan orbit-orbit {1, 3, 6}, {2, 8}, {4, 7, 5}.

Suatu orbit yang elemen-elemennya terurut akan membentuk sikel. Kita lihat orbit {1, 3, 6}, orbit tersebut menghasilkan sikel (1 3 6) atau (3 6 1) atau (6 1 3). Begitu juga orbit {2, 8} akan menghasilkan sikel (2 8) atau (8 2). Sedangkan orbit {4, 7, 5} menghasilkan sikel (4 7 5) atau (7 5 4) atau (5 4 7).

Contoh 14 :

Diberikan S = {1, 2, 3, 4, 5, 6, 7} dan permutasi θ yang didefinisikan :

$$\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 5 & 1 & 7 & 4 & 3 & 2 \end{pmatrix}.$$

Akan ditentukan sikel-sikel saling asing dari permutasi θ.

Jawab :

Terlebih dahulu akan ditentukan orbit-orbitnya.

Kita pilih sembarang elemen dalam S, misal 1, sehingga :

$\theta^1(1) = 6, \theta^2(1) = 3, \theta^3(1) = 1, \theta^4(1) = 6, \ldots$

Orbit yang memuat 1 adalah {1, 6, 3} sehingga membentuk sikel (1 6 3) atau (6 3 1) atau (3 1 6) dengan urutannya tetap.

Selanjutnya dipilih elemen dalam S yang bukan merupakan anggota {1, 6, 3} misal kita pilih 2, maka :

$\theta^1(2) = 5, \theta^2(2) = 4, \theta^3(2) = 7, \theta^4(2) = 2, \theta^5(2) = 5, \ldots$

Jadi orbit yang memuat 2 adalah {2, 5, 4, 7} dan membentuk sikel (2 5 4 7) atau (5 4 7 2) atau (4 7 2 5) atau (7 2 5 4). Semua elemen dalam S sudah termuat dalam orbit-orbit yang saling asing tersebut, maka sikel-sikel yang terbentuk juga saling asing.

Panjang dari sikel adalah banyak elemen dalam orbit yang paling besar.

Contoh 15 :

1) $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = (1\ 3\ 4\ 2)$ panjang sikelnya 4.

2) $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 5 & 6 & 4 & 2 \end{pmatrix} = (2\ 3\ 4\ 5\ 6)$ panjang sikelnya 5.

Selanjutnya suatu permutasi dapat dinyatakan dalam pergandaan sikel-sikel. Hal ini akan dijelaskan pada teorema berikut.

Teorema 2.E.2 :

Setiap permutasi $\alpha \in A$ (S) dan S adalah himpunan berhingga, merupakan pergandaan dari sikel-sikel yang saling asing.

Bukti :

Jika diberikan sembarang permutasi α dengan $\alpha \neq (1)$ atau permutasi α bukan merupakan permutasi identitas, maka untuk suatu elemen $a_i \in S$, $\alpha(a_i) \neq a_i$. Andaikan $\alpha(a_1) = a_2$, $\alpha(a_2) = a_3$ dan seterusnya hingga $\alpha(a_r)$ merupakan salah satu dari $a_1, a_2, a_3, \ldots, a_{r-1}$. Pasti dapat dipilih a_1 sehingga $\alpha(a_r) = a_1$, sebab apabila dipilih elemen diantara $a_2, a_3, \ldots, a_{r-1}$, akan bertentangan dengan pengertian permutasi, yaitu α merupakan fungsi yang bijektif, sehingga terbentuk sikel dari α, yaitu $(a_1, a_2, a_3, \ldots, a_r)$. Ada kemungkinan bahwa masih terdapat elemen-elemen lain selain $a_1, a_2, a_3, \ldots, a_r$ yang dipetakan ke dirinya sendiri, sehingga $\alpha = (a_1, a_2, a_3, \ldots, a_r)$. Tetapi jika ada elemen S selain a_i, $1 \leq i \leq r$, misal b_1 dan $\alpha(b_1) \neq b_1$, maka proses di atas akan diulang lagi, hingga membentuk sikel $(b_1, b_2, \ldots, b_s)$, sehingga $(a_1, a_2, a_3, \ldots, a_r)$ dan $(b_1, b_2, \ldots, b_s)$ saling asing. Apabila semua elemen dalam S yang oleh α tidak dipetakan ke dirinya sendiri sudah termuat dalam sikel-sikel tersebut, maka

$$\alpha = (a_1, a_2, a_3, \ldots, a_r)(b_1, b_2, \ldots, b_s).$$

Jika terdapat elemen selain a_i, $1 \leq i \leq r$ dan b_j, $1 \leq j \leq s$, misal $c_1 \in S$, sehingga $\alpha(c_1) \neq c_1$, maka dengan cara yang sama akan diperoleh sikel lain dari α yang saling asing. Proses tersebut dapat dilanjutkan sampai semua elemen S yang oleh α tidak dipetakan ke dirinya sendiri termuat dalam sikel-sikel tersebut. ■

Perkalian permutasi secara umum tidak komutatif, tetapi perkalian sikel saling asing komutatif. Dengan demikian $\theta = (1\ \ 6\ \ 3)\ (2\ \ 5\ \ 4\ \ 7)$ dapat ditulis $\theta = (2\ \ 5\ \ 4\ \ 7)\ (1\ \ 6\ \ 3)$. Penulisan hasil kali sikel saling asing sering mengabaikan sikel yang panjangnya 1. Sehingga jika $\alpha = (1\ \ 6\ \ 3)\ (2\ \ 5\ \ 7)\ (4)$ sering ditulis $\alpha = (1\ \ 6\ \ 3)\ (2\ \ 5\ \ 7)$.

F. Aksi Grup pada Himpunan

Aksi grup pada suatu himpunan adalah suatu pemetaan yang memenuhi persyaratan tertentu. Berikut akan didefinisikan pengertian aksi grup pada himpunan.

Definisi 2.F.1 :

Aksi dari Grup $(G, *)$ pada himpunan X adalah pemetaan $\psi : G \times X \to X$ sedemikian hingga memenuhi :

1. $\psi(e, x) = x$, $\forall x \in X$ dan e elemen identitas di G.
2. $\psi(g_1 * g_2, x) = \psi(g_1, \psi(g_2, x))$, $\forall g_1, g_2 \in G$ dan $\forall x \in X$.

Jika dapat ditemukan aksi dari Grup G pada himpunan X maka X disebut himpunan-G (G-set).

Selanjutnya untuk menyederhanakan penulisan ψ (g, x) ditulis dengan gx dan Grup (G, $*$) ditulis Grup G, sedangkan a $*$ b akan ditulis ab.

Contoh 16 :

Jika G grup dan H subgrup G, maka $\lambda : H \times G \to G$ dengan aturan :

$\lambda(h, g) = hgh^{-1}$, $\forall h \in H$ dan $\forall g \in G$ merupakan aksi dari H pada G.

1) λ terdefinisi dengan baik sebab :

   Jika diambil sembarang $(h, g) \in H \times G$ maka $h \in H$ dan $g \in G$.

   Dengan demikian $hgh^{-1} \in G$ dan $\lambda(h, g) = hgh^{-1}$.

   Ambil sembarang $(h_1, g_1), (h_2, g_2) \in H \times G$ sehingga $(h_1, g_1) = (h_2, g_2)$ maka $h_1 = h_2$ dan $g_1 = g_2$ sehingga $h_1g_1h_1^{-1} = h_2g_2h_2^{-1}$.

   Jadi $\lambda(h_1, g_1) = \lambda(h_2, g_2)$.

2) Misal e adalah elemen identitas dalam H, maka untuk sembarang $g \in G$, $\lambda(e, g) = ege^{-1} = g$.

3) Ambil sembarang $h_1, h_2 \in H$ dan sembarang $g \in G$ maka didapat

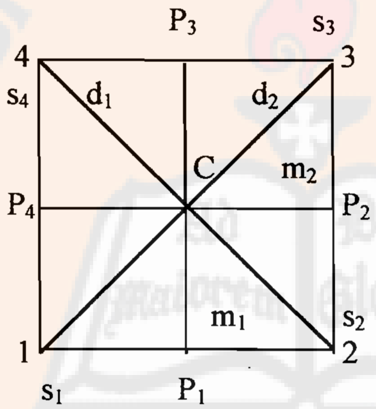
$$\begin{aligned}\lambda(h_1h_2, g) &= h_1h_2g(h_1h_2)^{-1}\\ &= h_1h_2gh_2^{-1}h_1^{-1}\\ &= h_1\,\lambda(h_2, g)\,h_1^{-1}\\ &= \lambda(h_1, \lambda(h_2, g)).\end{aligned}$$

Jadi λ adalah aksi dari H pada G.

Definisi 2.F.2 :

Andaikan H subgrup dari grup G dan H aksi pada G. Pemetaan yang mengawankan $H \times G$ ke G dengan aturan $(h, g) \to hgh^{-1}$ disebut Konjugasi. Sedangkan elemen hgh^{-1} disebut konjugat dari g terhadap aksi dari H pada G.

Contoh 17 :



ρ_1 menyatakan rotasi yang berpusat pada C sebesar $\pi i/2$ radian berlawanan dengan arah jarum jam.

μ_1 menyatakan refleksi terhadap garis m_i.

δ_1 menyatakan refleksi terhadap d_i.

$G = \{\rho_0, \rho_1, \rho_2, \rho_3, \mu_1, \mu_2, \delta_1, \delta_2\}$.

Bahwa G merupakan Grup terhadap operasi komposisi permutasi dapat dilihat dari tabel di bawah ini :

	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_0	ρ_0	ρ_1	ρ_2	ρ_3	μ_1	μ_2	δ_1	δ_2
ρ_1	ρ_1	ρ_2	ρ_3	ρ_0	δ_1	δ_2	μ_2	μ_1
ρ_2	ρ_2	ρ_3	ρ_0	ρ_1	μ_2	μ_1	δ_2	δ_1
ρ_3	ρ_3	ρ_0	ρ_1	ρ_2	δ_2	δ_1	μ_1	μ_2
μ_1	μ_1	δ_2	μ_2	δ_1	ρ_0	ρ_2	ρ_3	ρ_1
μ_2	μ_2	δ_1	μ_1	δ_2	ρ_2	ρ_0	ρ_1	ρ_3
δ_1	δ_1	μ_1	δ_2	μ_2	ρ_1	ρ_3	ρ_0	ρ_2
δ_2	δ_2	μ_2	δ_1	μ_1	ρ_3	ρ_1	ρ_2	ρ_0

Tabel A

Misalkan X = {1, 2, 3, 4, s_1, s_2, s_3, s_4, m_1, m_2, d_1, d_2, C, P_1, P_2, P_3, P_4}.

X adalah Himpunan-G (G-set) terhadap operasi komposisi permutasi.

Hasil permutasi elemen-elemen X disajikan dalam tabel di bawah ini :

	1	2	3	4	s_1	s_2	s_3	s_4	m_1	m_2	d_1	d_2	C	P_1	P_2	P_3	P_4
ρ_0	1	2	3	4	s_1	s_2	s_3	s_4	m_1	m_2	d_1	d_2	C	P_1	P_2	P_3	P_4
ρ_1	2	3	4	1	s_2	s_3	s_4	s_1	m_2	m_1	d_2	d_1	C	P_2	P_3	P_4	P_1
ρ_2	3	4	1	2	s_3	s_4	s_1	s_2	m_1	m_2	d_1	d_2	C	P_3	P_4	P_1	P_2
ρ_3	4	1	2	3	s_4	s_1	s_2	s_3	m_2	m_1	d_2	d_1	C	P_4	P_1	P_2	P_3
μ_1	2	1	4	3	s_1	s_4	s_3	s_2	m_1	m_2	d_2	d_1	C	P_1	P_4	P_3	P_2
μ_2	4	3	2	1	s_3	s_2	s_1	s_4	m_1	m_2	d_2	d_1	C	P_3	P_2	P_1	P_4
δ_1	3	2	1	4	s_2	s_1	s_4	s_3	m_2	m_1	d_1	d_2	C	P_2	P_1	P_4	P_3
δ_2	1	4	3	2	s_4	s_3	s_2	s_1	m_2	m_1	d_1	d_2	C	P_4	P_3	P_2	P_1

Tabel B

Perhatikan bahwa elemen identitas dari G = ρ_0, berlaku bahwa $\rho_0(x) = x$, $\forall x \in X$

dan dipenuhi juga $(\forall g_1, g_2 \in G)\ (\forall x \in X)\ (g_1g_2)(x) = g_1(g_2(x))$.

Teorema 2.F.1 :

Diketahui X himpunan-G dan $x \in X$, maka $G_x = \{g \in G \mid gx = x\}$, $x \in X$, merupakan subgrup dari grup G.

Bukti :

$G_x = \{g \in G \mid gx = x\}$.

- $G_x \neq \phi$ sebab $e \in G$ dan $ex = x$, untuk $x \in X$ sehingga $e \in G_x$.
- Ambil sembarang $g_1, g_2 \in G_x$ berarti $g_1, g_2 \in G$ dan $g_1x = x$, $g_2x = x$.

  Karena $g_1, g_2 \in G$ maka $g_1g_2 \in G$ dan $(g_1g_2)\,x = g_1\,(g_2x) = g_1x = x$.

  Jadi $g_1g_2 \in G_x$.
- Ambil sembarang $g \in G_x$ berarti $g \in G$ dan $gx = x$.

  Karena $g \in G$ maka $g^{-1} \in G$ dan $g^{-1}\,(gx) = g^{-1}x$.

  Padahal $g^{-1}\,(gx) = (g^{-1}g)\,x = ex = x$. Didapat $x = g^{-1}x$.

  Jadi $g^{-1} \in G_x$.

Terbukti G_x subgrup dari G. ■

Definisi 2.F.3 :

Jika X himpunan-G dan $x \in X$, maka subgrup G_x disebut subgrup isotropi dari x atau subgrup stabilisator dari x.

Contoh 18 :

$G = \{\rho_0, \rho_1, \rho_2, \rho_3, \mu_1, \mu_2, \delta_1, \delta_2\}$.

$X = \{1, 2, 3, 4, s_1, s_2, s_3, s_4, m_1, m_2, d_1, d_2, C, P_1, P_2, P_3, P_4\}$.

$G_x = \{g \in G \mid gx = x\}$.

$G_1 = \{\rho_0, \delta_2\}$.

$G_{s3} = \{\rho_0, \mu_1\}$.

Pada pembahasan tentang sikel, sudah didefinisikan pengertian orbit. Sekarang akan diberikan contoh orbit pada Himpunan-G.

Contoh 19 :

1. $X = \{1, 2, 3, 4\}$, $H = \{\rho_0, \rho_2\}$ subgrup dari Grup G (Contoh 8).

   X adalah Himpunan-H (H-set).

   Orbit dari 1 = H1 = $\{x \in X \mid (\exists\rho_i \in H)\ \rho_i x = 1\} = \{1, 3\}$.

   Orbit dari 2 = H2 = $\{x \in X \mid (\exists\rho_i \in H)\ \rho_i x = 2\} = \{2, 4\}$.

   Orbit dari 3 = H3 = $\{x \in X \mid (\exists\rho_i \in H)\ \rho_i x = 3\} = \{1, 3\}$.

   Orbit dari 4 = H4 = $\{x \in X \mid (\exists\rho_i \in H)\ \rho_i x = 4\} = \{2, 4\}$.

   Jadi orbit-orbit dalam X oleh Grup H adalah $\{1, 3\}$ dan $\{2, 4\}$.

BAB III

FUNGSI BILINEAR ATAS Z_p

Pada bagian ini akan dibahas tentang fungsi bilinear atas himpunan bilangan bulat modulo-p (Z_p). Tetapi sebelumnya akan dibahas dahulu pengertian dan sifat-sifat fungsi serta himpunan bilangan bulat modulo-p (Z_p).

A. Fungsi

Pada bagian depan sudah didefinisikan pengertian fungsi dari himpunan A ke himpunan B yakni suatu aturan yang mengawankan secara tunggal setiap elemen x di himpunan A dengan tepat satu elemen y di himpunan B. Suatu fungsi f dari A ke B disajikan dengan simbol $f : A \to B$. Elemen $y \in B$ yang terkawankan dengan $x \in A$ dinyatakan dengan $y = f(x)$, $x \in A$. Pada bagian depan sudah dibahas mengenai fungsi surjektif, fungsi injektif dan fungsi bijektif. Selanjutnya akan dibahas tentang komposisi fungsi dan fungsi invers.

i. Komposisi Fungsi

Jika $f : A \to B$, $g : B \to C$, maka komposisi dari f dan g ialah suatu fungsi $g \circ f : A \to C$ yang didefinisikan dengan aturan $(g \circ f)(x) = g(f(x))$ untuk setiap $x \in A$.Pengerjaan fungsi $g \circ f$ dimulai dari pengerjaan fungsi f dan diikuti pengerjaan fungsi g. Fungsi g o f tersebut dinamakan fungsi komposisi dari fungsi f dan fungsi g.

Contoh 1 :

Fungsi $f : R \to R$ dan $g : R \to R$ didefinisikan sebagai berikut

Jika $f(x) = x^2$ dan $g(x) = x + 3$, maka

$$\begin{aligned}(f \circ g)(x) &= f(g(x)) \\ &= f(x+3) \\ &= x^2 + 6x + 9\end{aligned}$$

dan

$$\begin{aligned}(g \circ f)(x) &= g(f(x)) \\ &= g(x^2) \\ &= x^2 + 3\end{aligned}$$

Teorema 3.A.1 :

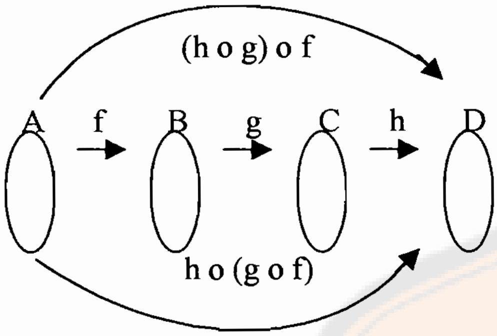
Jika $f : A \to B$, $g : B \to C$, dan $h : C \to D$, maka berlakulah $(h \circ g) \circ f = h \circ (g \circ f)$.

Bukti :

Untuk membuktikan teorema ini harus diperlihatkan :

1. $(h \circ g) \circ f$ dan $h \circ (g \circ f)$ mempunyai domain dan kodomain yang sama.
2. $(\forall x \in A)\ ((h \circ g) \circ f)(x) = (h \circ (g \circ f))(x)$.

Kita lihat sketsa di bawah ini



1. Dengan sketsa di atas, maka

   fungsi h o g : B $\rightarrow$ D sehingga (g o h) o f : A $\rightarrow$ D

   fungsi g o f : A $\rightarrow$ C sehingga h o (g o f) : A $\rightarrow$ D

   Jadi (h o g) o f dan h o (g o f) mempunyai domain yang sama, yaitu A dan kodomain yang sama yaitu D.

2. Jika x $\in$ A maka

   $$\begin{aligned} ((h \circ g) \circ f)(x) &= (h \circ g)\, f(x) \\ &= h(g(f(x))) \\ &= h((g \circ f)(x)) \\ &= (h \circ (g \circ f))(x) \end{aligned}$$

   Jadi (h o g) o f = h o (g o f). ■

Berikut ini akan didefinisikan pengertian fungsi identitas.

Definisi 3.A.1 :

Fungsi identitas adalah fungsi bijektif dari A ke A yang memetakan setiap elemen $x \in A$ ke dirinya sendiri. Jadi i adalah fungsi identitas dari A ke A bila dan hanya bila $i(x) = x, \forall x \in A$. Fungsi identitas dari A ke A sering dinyatakan dengan i_A dan $i_A(x) = x, \forall x \in A$.

ii. Fungsi Invers

Misalkan fungsi $f : A \rightarrow B$ adalah fungsi bijektif, yaitu fungsi yang injektif dan surjektif, maka setiap elemen B dapat dinyatakan sebagai $f(x)$ untuk setiap x elemen A. Dengan fungsi $f : A \rightarrow B$ itu, kita juga dapat mendefinisikan fungsi dari B ke A, sehingga x merupakan kawan dari $f(x)$, untuk setiap $x \in A$. Fungsi dari B ke A sering dinotasikan f^{-1} atau fungsi invers dari f. Fungsi $f^{-1} : B \rightarrow A$ didefinisikan dengan $f^{-1}(f(x)) = x$, $x \in A$.

Teorema 3.A.2 :

Jika $f : A \rightarrow B$ merupakan fungsi bijektif maka invers fungsi f atau f^{-1} adalah tunggal.

Bukti :

Diandaikan bahwa invers dari fungsi f tidak tunggal. Andaikan g dan h merupakan invers dari fungsi f. Akan diperlihatkan g = h.

Karena g dan h merupakan invers dari fungsi f, maka $g : B \to A$ dan $h : B \to A$.

$(g \circ f) \circ h = g \circ (f \circ h)$ Teorema 3.B.1

$i_A \circ h = g \circ i_B$ fungsi g dan h merupakan fungsi invers dari f

$h = g$

Terbukti bahwa fungsi invers dari fungsi $f : A \to B$ adalah tunggal. ■

Karena kita akan membahas fungsi bilinear atas himpunan bilangan bulat modulo-p (Z_p), maka kita akan membahas dahulu tentang bilangan bulat modulo-p (Z_p).

B. Bilangan Bulat Modulo-p

Pembahasan mengenai bilangan bulat modulo-p, kita awali dengan pembahasan mengenai relasi kongruen modulo-p.

Definisi 3.B.1 :

Jika n bilangan bulat positif, maka a dan b dikatakan kongruen modulo-p jika $(a - b)$ habis dibagi p, ditulis $a \equiv b \pmod{p}$.

Contoh 2 :

$17 \equiv 3 \pmod{7}$ karena 7 pembagi $17 - 3 = 14$

$18 \not\equiv 4 \pmod 5$ karena 5 bukan pembagi $18 - 4 = 14$

Lemma 3.B.1 :

Kongruensi modulo-p adalah relasi ekuivalensi dalam himpunan bilangan bulat, untuk sembarang bilangan bulat positif p.

Bukti :

a. Sifat refleksif terpenuhi, sebab jika $a \in Z$, maka $p \mid (a - a)$, sehingga $a \equiv a \pmod p$.

b. Sifat transitif terpenuhi, sebab jika $a \equiv b \pmod p$ maka ada bilangan bulat r yang memenuhi

   $(a - b) = pr$

   $-(a - b) = -pr$

   $b - a = -pr$

   $p \mid b - a$

c. Sifat transitif terpenuhi, sebab jika $a \equiv b \pmod p$ dan $b \equiv c \pmod p$ maka ada bilangan bulat r sehingga $a - b = pr$ dan ada bilangan bulat q sehingga $b - c = pq$ sehingga $(a - b) + (b - c) = pr + pq$

   $$(a - b) + (b - c) = p(r + q).$$

   Didapat $p \mid (a - b) + (b - c)$ atau $p \mid (a - c)$. ■

Karena relasi kongruensi modulo-p pada himpunan bilangan bulat merupakan relasi ekuivalensi, maka himpunan bilangan bulat terpartisi menjadi himpunan bagian – himpunan bagian yang asing. Kelas ekuivalensi untuk relasi ekuivalensi ini disebut kelas kongruensi modulo-p. Himpunan kelas- kelas kongruensi modulo-p disebut himpunan bilangan bulat modulo-p (Z_P). Sehingga $Z_P = \{[0], [1], [2], \ldots, [p-1]\}$. Sebagai contoh $Z_7 = \{[0], [1], [2], [3], [4], [5], [6]\}$.

Definisi 3.B.2 :

Jika $[a] \in Z_p$ dan $[b] \in Z_p$, maka $[a] \oplus [b] = [a+b]$ dan $[a] \Theta [b] = [ab]$.

Selanjutnya akan ditunjukkan bahwa Z_p dengan operasi $\oplus$ merupakan suatu grup dan $Z_P - \{[0]\}$ dengan operasi Θ juga merupakan grup.

Teorema 3.B.1 :

Himpunan semua bilangan bulat modulo-p dengan operasi $\oplus$ atau $(Z_p, \oplus)$ adalah grup Abelian.

Bukti :

1. $(\forall [a], [b] \in Z_p)$ $(\exists [c] \in Z_p)$ sehingga $[a] \oplus [b] = [c]$.

   Sifat tertutup terpenuhi.

2. Ambil sembarang $[a], [b], [c] \in Z_p$ maka

   $[a] \oplus ([b] \oplus [c]) = [a] \oplus [b+c]$

$= [a + (b + c)]$

$= [(a + b) + c]$

$= [a + b] \oplus [c]$

$= ([a] \oplus [b]) \oplus [c]$

Jadi operasi $\oplus$ bersifat asosiatif.

3. Eleman identitas dari Z_p adalah [0], sebab untuk sembarang $[a] \in Z_p$ $[0] + [a] = [0 + a] = [a]$ dan $[a] + [0] = [a + 0] = [a]$.

4. Ambil sembarang $[a] \in Z_p$ dan dimisalkan [b] merupakan invers dari [a] maka akan diperlihatkan $[b] \in Z_p$.

   $[a] \oplus [b] = [0]$

   $[a + b] \quad = [0]$

   $a + b \quad = 0$

   $b \quad = -a$

   Karena $[a] \in Z_p$ maka $[b] = [-a] \in Z_p$.

   Jadi $[b] \in Z_p$.

   Jadi setiap elemen dari Z_p mempunyai invers.

5. Ambil sembarang $[a], [b] \in Z_p$ maka

   $[a] \oplus [b] = [a + b] = [b + a] = [b] \oplus [a]$.

   Jadi operasi $\oplus$ bersifat komutatif. ■

Selanjutnya akan ditunjukkan bahwa $(Z_p - \{[0]\}, \odot)$ merupakan suatu grup.

Lemma 3.B.2 :

Jika Z_p dengan p bilangan prima maka untuk setiap $[r] \in Z_p$ dengan $[r] \neq [0]$ ada $[a] \in Z_p$ sedemikian hingga $[r] \odot [a] = [1]$.

Bukti :

Karena p bilangan prima maka p dan r adalah prima relatif sehingga ada bilangan bulat a dan b sedemikian hingga ra + pb = 1.

Sehingga $ra \equiv 1 \quad$ (modulo-p)

$[ra] = [1]$

$[r] \odot [a] = [1]$.

Karena a bilangan bulat maka a kongruen modulo-p dengan tepat satu bilangan bulat 1, 2, 3, …, p - 1, sehingga $[a] \in Z_p$.

Jika $(\forall [r] \in Z_p)\ (\exists [a] \in Z_p)\ [r] \odot [a] = [1]$. ■

Teorema 3.B.2 :

$Z_p - \{[0]\}$ dengan operasi $\odot$ merupakan grup Abelian.

Bukti :

1. $\forall [a], [b] \in Z_p - \{[0]\}, \exists [c] \in Z_p - \{[0]\}$ sehingga $[a] \odot [b] = [c]$.

   Jadi operasi $\odot$ bersifat tertutup.

2. Ambil $[a], [b], [c] \in Z_p - \{[0]\}$ maka

   $[a] \odot ([b] \odot [c]) = [a] \odot [bc]$

   $= [a\,(bc)]$

$= [(ab)\ c]$

$= [ab] \odot [c]$

$= ([a] \odot [b]) \odot [c]$

Jadi operasi $\odot$ bersifat asosiatif.

3. Elemen identitas pada $Z_p - \{[0]\}$ adalah [1], sebab untuk sembarang $[a] \in Z_p - \{[0]\}$, $[a] \odot [1] = [a1] = [a]$ dan $[1] \odot [a] = [1a] = [a]$.
4. Menurut lemma 2.B.2 setiap elemen $Z_p - \{[0]\}$ mempunyai invers.
5. Ambil $[a], [b] \in Z_p - \{[0]\}$ maka $[a] \odot [b] = [ab] = [ba] = [b] \odot [a]$.

   Jadi operasi $\odot$ bersifat komutatif. ■

Pada pembahasan selanjutnya operasi "$\odot$" pada Z_p tidak ditulis, sehingga $[r] \odot [a] = [1]$ ditulis $[r][a] = [1]$ dan operasi "$\oplus$" pada Z_p ditulis "+", sehingga $[r] \oplus [a] = [1]$ ditulis $[r] + [a] = [1]$.

Selanjutnya kita akan membahas mengenai persamaan kongruensi dalam Z_p, tetapi sebelumnya kita bahas lema berikut.

Lemma 3.B.3 :

Andaikan $a, b, c \in Z$, a relatif prima dengan b dan $a \mid bc$ maka $a \mid c$.

Bukti :

Karena a dan b relatif prima, ada bilangan bulat s dan t sedemikian hingga $sa + tb = 1$. Jika kita kalikan dengan c maka $sac + tbc = c$. Karena diketahui $a \mid bc$ maka $a \mid tbc$, sehingga $a \mid sac + tbc$ atau $a \mid c$. ■

Lemma 3.B.4 :

Andaikan $a, b, c, p \in Z$, c relatif prima dengan p dan $ca \equiv cb \pmod{p}$ maka $a \equiv b \pmod{p}$.

Bukti :

$ca \equiv cb \pmod{p}$ maka $p \mid c(b - a)$. Karena p dan c relatif prima maka menurut lemma 3.B.3 $p \mid (b - a)$ sehingga $b \equiv a \pmod{p}$. ■

Teorema 3.B.3 :

Andaikan $b, c, p \in Z$, c relatif prima dengan p maka $cx \equiv b \pmod{p}$ mempunyai penyelesaian dalam x. Jika x_1 dan x_2 merupakan penyelesaian maka $x_1 \equiv x_2 \pmod{p}$.

Bukti :

Karena c dan p relatif prima maka ada bilangan bulat s dan t sedemikian hingga $sc + tp = 1$. Jika kita kalikan dengan b maka $scb + tpb = b$. Sehingga kita dapatkan $b \equiv (bs)\,c \pmod{p}$. Kita dapatkan penyelesaian untuk x yakni $x = bs$.

Andaikan ada 2 penyelesaian yakni x_1 dan x_2, yang berarti $cx_1 \equiv b \pmod{p}$ dan $cx_2 \equiv b \pmod{p}$. Karena relasi kongruensi bersifat simetris dan transitif maka $cx_1 \equiv cx_2 \pmod{p}$. Karena c dan p relatif prima, maka menurut lemma 3.B.4, $x_1 \equiv x_2 \pmod{p}$. ■

Berikut ini akan ditunjukkan bahwa dalam Z_p tidak memuat pembagi nol.

Teorema 3.B.4 :

Dalam Z_p, jika $[s], [t] \in Z_p$ dan $[s].[t] = [0]$ maka $[s] = [0] \vee [t] = [0]$.

Bukti :

Akan dibuktikan dengan kontraposisi.

Andaikan $[s], [t] \in Z_p$ dan $[s] \neq [0] \wedge [t] \neq [0]$. Karena p prima maka faktor dari p hanya 1 dan p. Jadi perkalian yang menyebabkan bernilai [p] hanya [1].[p]. Padahal dalam Z_p, $[p] = [0]$. Karena $[s], [t] \neq [0]$ maka tidak mungkin $[s].[t] = [0]$.

Jadi jika $[s], [t] \in Z_p$, $[s].[t] = [0]$ maka $[s] = [0] \vee [t] = [0]$. ■

Suatu persamaan dengan $f(x) \equiv 0 \pmod{n}$ disebut persamaan kongruensi modulo-n.

Sebagai contoh :

$f(x) = [a_m]x^m + [a_{m-1}]x^{m-1} + [a_{m-2}]x^{m-2} + \ldots + [a_0] = [0]$, dengan $[a] \neq [0]$, $[a_m], [a_{m-1}], \ldots, [a_0] \in Z_p$ merupakan persamaan kongruensi modulo-n berderajad m. Jika [b] $\in Z_p$ memenuhi persamaan di atas maka [b] dikatakan akar dari persamaan kongruensi tersebut.

Suatu persamaan kongruensi modulo-p berderajad m mempunyai akar-akar yang jumlahnya tidak melebihi m. Hal itu akan disajikan dalam teorema berikut.

Teorema 3.B.5 :

Persamaan kongruensi modulo-p (prima) berderajad m mempunyai paling banyak m akar.

Bukti :

Pada pembuktian disini [a] ditulis a.

Andaikan persamaan kongruensi modulo-p tersebut adalah

$$f(x) = a_m x^m + a_{m-1} x^{m-1} + a_{m-2} x^{m-2} + \ldots + a_0 = 0 \qquad \ldots (1)$$

Dengan x_1 merupakan salah satu akar persamaan tersebut, maka

$$a_m x_1^m + a_{m-1} x_1^{m-1} + a_{m-2} x_1^{m-2} + \ldots + a_0 = 0 \qquad \ldots (2)$$

Sehingga kita dapatkan

$$a_m (x^m - x_1^m) + a_{m-1} (x^{m-1} - x_1^{m-1}) + a_{m-2} (x^{m-2} - x_1^{m-2}) + \ldots + a_0 (x - x_1) = 0 \qquad \ldots (3)$$

Padahal $(x^m - x_1^m) = (x^{m-1} + x_1 x^{m-2} + x_1^2 x^{m-3} + \ldots + x_1^{m-1})(x - x_1)$ $\quad \ldots (4)$

Dari persamaan (3) dan (4) kita dapatkan

$(x - x_1)\ (a_m x^{m-1} + b_{m-2} x^{m-2} + b_{m-3} x^{m-3} + \ldots + b_0) = 0$, untuk suatu $b_{m-2}, b_{m-3}, \ldots, b_0 \in Z_p$.

Jika $x - x_1 \neq 0$ maka $a_m x^{m-1} + b_{m-2}x^{m-2} + b_{m-3}x^{m-3} + \ldots + b_0 = 0$ karena Z_p (p prima) tidak memuat pembagi nol.

Sehingga setiap akar dari f (x) selain x_1 merupakan akar dari persamaan $a_m x^{m-1} + b_{m-2}x^{m-2} + b_{m-3}x^{m-3} + \ldots + b_0 = 0$.

Selanjutnya untuk membuktikan teorema itu kita gunakan induksi matematika.

- Menurut teorema 3.B.3 persamaan kongruensi berderajad 1 yakni $ax - b = 0$ mempunyai 1 penyelesaian. Jadi untuk persamaan kongruensi modulo-p berderajad 1 mempunyai akar 1.
- Diandaikan keadaan itu benar untuk persamaan kongruensi modulo-p berderajad $m - 1$.

  Sehingga dari pembahasan di atas

  $$g(x) = a_m x^{m-1} + b_{m-2}x^{m-2} + b_{m-3}x^{m-3} + \ldots + b_0 = 0$$

  mempunyai paling banyak $m - 1$ akar.

  Sekarang ambil fungsi $f(x) = a_m x^m + a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \ldots + a_0 = 0$ yang berderajat m. Akan ditunjukkan f (x) mempunyai paling banyak m akar.

  Andaikan x_1 merupakan akar dari f (x) maka

  $$(x - x_1)(a_m x^{m-1} + b_{m-2}x^{m-2} + b_{m-3}x^{m-3} + \ldots + b_0) = 0$$

  Karena Z_p tidak memuat pembagi nol maka

  $$x - x_1 = 0 \vee a_m x^{m-1} + b_{m-2}x^{m-2} + b_{m-3}x^{m-3} + \ldots + b_0 = 0$$

Karena $a_m x^{m-1} + b_{m-2}x^{m-2} + b_{m-3}x^{m-3} + \ldots + b_0$ mempunyai paling banyak $m - 1$ akar maka fungsi f (x) mempunyai paling banyak m akar. ■

Sesudah kita membahas fungsi dan bilangan bulat modulo-p (Z_p), selanjutnya akan dibahas fungsi bilinear atas (Z_p).

C. Fungsi Bilinear atas Z_p

Setelah membahas mengenai fungsi termasuk teorema-teorema yang berkaitan dengan fungsi dan tentang bilangan bulat modulo-p, selanjutnya akan dibahas mengenai salah satu bentuk fungsi yakni fungsi bilinear atas bilangan bulat modulo-p (Z_p).

Bentuk umum dari fungsi bilinear atas Z_p yaitu

$$f(x) = y = \frac{[a]x + [b]}{[c]x + [d]}$$

dengan [a], [b], [c] dan [d] $\in Z_p$ dan [ad] + [-bc] $\neq$ [0]. Sebagai catatan, jika [a], [b] $\in Z_p$ maka $\frac{[a]}{[b]}$ = [ab^{-1}], ([b^{-1}] yakni invers dari [b] terhadap operasi "Θ" dengan elemen identitas [1]) dan [a] – [b] = [a] + [-b], ([-b] yakni invers dari [b] terhadap operasi "⊕" dengan elemen identitas [0]).

Jika [c] $\neq$ [0], untuk setiap x = $\frac{[-d]}{[c]}$ maka [c]x + [d] = [0]. Karena pembagian dengan bilangan 0 tidak didefinisikan, maka untuk hasil pembagian dengan bilangan 0 kita menuliskan symbol baru yakni "∞". Sehingga untuk x = $\frac{[-d]}{[c]}$ maka y = ∞. Hubungan antara notasi "∞" dan [a] $\in Z_p$ yakni :

1. $\infty \pm [a] = \infty, \forall [a] \neq \infty$

2. $\infty \cdot [a] = \infty, \forall [a] \neq \infty$

3. $\frac{[a]}{\infty} = [0]\ dan\ \frac{\infty}{[a]} = \infty, \forall [a] \neq \infty$

4. $\frac{[a]}{[0]} = \infty, \forall [a] \neq [0]$

Selanjutnya akan diselidiki fungsi bilinear atas Z_p dengan daerah asal dan daerah hasil fungsi $Z_p + \{\infty\}$ atau P_p. Jika $[c] \neq [0]$, maka untuk setiap $x = \frac{[-d]}{[c]}$ dikawankan dengan $y = \infty$. Jika $[c] = [0]$, maka haruslah $[a] \neq [0]$ dan $[d] \neq [0]$ sehingga syarat fungsi bilinear terpenuhi, maka $y = \infty$ diambil sebagai kawan dari $x = \infty$.

Dari fungsi $y = \frac{[a]x + [b]}{[c]x + [d]}$ maka $x = \frac{[-d]y + [b]}{[c]y + [-a]}$. Jika $[c] \neq [0]$ maka $y = \frac{[a]}{[c]}$ merupakan kawan dari $x = \infty$.

Selanjutnya akan dibahas tentang titik tetap dan kesamaan 2 fungsi bilinear atas Z_p.

Definisi 3.C.1 :

Jika f : $P_p \rightarrow P_p$: f (x) = y = $\dfrac{[a]x+[b]}{[c]x+[d]}$, [ad] + [-bc] ≠ [0], maka p disebut titik tetap fungsi bilinear tersebut jika p = f (p).

Contoh 3 :

Suatu fungsi f : $P_7 \rightarrow P_7$ dengan aturan f (x) = $\dfrac{[5]x+[-2]}{x+[2]}$, f merupakan fungsi bilinear pada Z_7, maka [1] dan [2] merupakan titik tetap fungsi tersebut karena

untuk x = [1] maka $\dfrac{[5]([1])+[-2]}{[1]+[2]} = \dfrac{[5]+[-2]}{[3]} = \dfrac{[3]}{[3]} = [1]$ dan

untuk x = [2] maka $\dfrac{[5]([2])+[-2]}{[2]+[2]} = \dfrac{[8]}{[4]} = [2]$.

Definisi 3.C.2 :

Jika FBZ_p merupakan himpunan fungsi bilinear pada Z_p dan f (x) = $\dfrac{[a]x+[b]}{[c]x+[d]}$,

g (x) = $\dfrac{[e]x+[f]}{[g]x+[h]}$ ∈ FBZ_p dengan [a], [b], [c], [d], [e], [f], [g], [h] ∈ Z_p, [ad] + [-bc] ≠ [0], [eh] + [-gf] ≠ [0], maka fungsi f (x) sama dengan fungsi g (x) jika dan hanya jika f (x) = g (x), ∀x ∈ P_p.

Contoh 4 :

Jika $f(x) = \dfrac{x + [2]}{x}$ dan $g(x) = \dfrac{[2]x + [1]}{[2]x} \in FBZ_3$, apakah f (x) = g (x) ?

Jawab :

Akan diselidiki apakah untuk semua $x \in P_p$, f (x) = g (x).

- untuk x = [0]

  $f([0]) = \dfrac{[0] + [2]}{[0]} = \infty$, $g([0]) = \dfrac{[2][0] + [1]}{[2][0]} = \infty$

  f ([0]) = g ([0])

- untuk x = [1]

  $f([1]) = \dfrac{[1] + [2]}{[1]} = [0]$, $g([1]) = \dfrac{[2][1] + [1]}{[2][1]} = [0]$

  f ([1]) = g ([1])

- untuk x = [2]

  $f([2]) = \dfrac{[2] + [2]}{[2]} = [2]$, $g([2]) = \dfrac{[2][2] + [1]}{[2][2]} = [2]$

  f ([2]) = g ([2])

- untuk x = ∞

  $f(\infty) = \dfrac{[1]}{[1]} = [1]$, $g(\infty) = \dfrac{[2]}{[2]} = [1]$

  f (∞) = g (∞)

Jadi $(\forall x \in P_3)$ f (x) = g (x), sehingga fungsi f (x) = g (x).

Selanjutnya akan dibahas mengenai komposisi dan invers fungsi bilinear atas Z_p.

i. Komposisi Fungsi Bilinear atas P_p

Jika u dan v fungsi bilinear atas P_p yang didefinisikan sebagai berikut

$$u : P_p \to P_p : u(x) = \frac{[a]x + [b]}{[c]x + [d]},\ [a], [b], [c]\ [d] \in Z_p \text{ dan } [ad] + [-bc] \neq [0]$$

$$v : P_p \to P_p : v(x) = \frac{[e]x + [f]}{[g]x + [h]},\ [e], [f], [g], [h] \in Z_p \text{ dan } [eh] + [-fg] \neq [0]$$

maka komposisi fungsi u dan v adalah

$$(u \circ v)(x) = u(v(x))$$

$$= u\left(\frac{[e]x + [f]}{[g]x + [h]}\right)$$

$$= \frac{[a]\left(\frac{[e]x + [f]}{[g]x + [h]}\right) + [b]}{[c]\left(\frac{[e]x + [f]}{[g]x + [h]}\right) + [d]}$$

$$= \frac{\dfrac{([ae] + [bg])x + [af] + [bh]}{[g]x + [h]}}{\dfrac{([ce] + [dg])x + [cf] + [dh]}{[g]x + [h]}}$$

$$= \frac{([ae] + [bg])x + [af] + [bh]}{([ce] + [dg])x + [cf] + [dh]}$$

dengan $([ae] + [bg])([cf] + [dh]) + \{-([ce] + [dg])([af] + [bh])\}$

$= [aecf] + [aedh] + [bgcf] + [bgdh] + \{-[ceaf]-[cebh]-[dgaf]-[dgbh]\}$

$= ([ad] + [-bc])\,([eh] + [-fg]) \neq [0]$, karena $([ad] + [-bc]) \neq [0]$ dan $([eh] + [-fg]) \neq [0]$.

Selanjutnya kita akan menunjukkan bahwa jika u, v dan w fungsi bilinear atas P_p maka berlaku (u o v) o w = u o (v o w).

$u : P_p \to P_p : u(x) = \dfrac{[a]x + [b]}{[c]x + [d]}$, [a], [b], [c], [d] $\in Z_p$ dan $[ad] + [-bc] \neq [0]$

$v : P_p \to P_p : v(x) = \dfrac{[e]x + [f]}{[g]x + [h]}$, [e], [f], [g], [h] $\in Z_p$ dan $[eh] + [-fg] \neq [0]$

$w : P_p \to P_p : w(x) = \dfrac{[i]x + [j]}{[k]x + [l]}$, [i], [j], [k], [l] $\in Z_p$ dan $[il] + [-jk] \neq [0]$

Fungsi (u o v) : $P_p \to P_p$ sehingga (u o v) o w : $P_p \to P_p$

Fungsi (v o w) : $P_p \to P_p$ sehingga u o (v o w) : $P_p \to P_p$

Akan ditunjukkan bahwa ((u o v) o w) (x) = (u o (v o w)) (x)

a) (u o v) (x) = u (v (x))

$$= u\left(\frac{[e]x + [f]}{[g]x + [h]}\right)$$

$$= \frac{[a]\left(\dfrac{[e]x + [f]}{[g]x + [h]}\right) + [b]}{[c]\left(\dfrac{[e]x + [f]}{[g]x + [h]}\right) + [d]}$$

$$= \frac{([ae] + [bg])x + ([af] + [bh])}{([ce] + [dg])x + ([cf] + [dh])}$$

dengan ([ae] + [bg]) ([cf] + [dh]) + {-([ce] + [dg]) ([af] + [bh])}

= ([ad] + [-bc]) ([eh] + [-fg]) $\neq$ [0], karena ([ad] + [-bc]) $\neq$ [0]

dan ([eh] + [-fg]) $\neq$ [0].

((u o v) o w) (x) = (u o v) w (x)

$$= (u \circ v)\left(\frac{[i]x+[j]}{[k]x+[l]}\right)$$

$$= \frac{[ae]+[bg]\left(\frac{[i]x+[j]}{[k]x+[l]}\right)+[af]+[bh]}{[ce]+[dg]\left(\frac{[i]x+[j]}{[k]x+[l]}\right)+[cf]+[dh]}$$

$$= \frac{([aei]+[bgi]+[afk]+[bhk])x+[aej]+[bgj]+[afl]+[bhl]}{([cei]+[dgi]+[cfk]+[dhk])x+[cej]+[dgj]+[cfl]+[dhl]}$$

dengan ([aei] + [bgi] + [afk] + [bhk]) ([cej] + [dgj] + [cfl] + [dhl]) + {-([cei] + [dgi] + [cfk] + [dhk]) ([aej] + [bgj] + [afl] + [bhl])}

= ([ad] + [-bc]) ([eh] + [-fg]) ([il] + [-kj]) $\neq$ [0], karena ([ad] + [-bc]) $\neq$ [0], ([eh] + [-fg]) $\neq$ [0] dan ([il] + [-kj]) $\neq$ [0]

b) (v o w) (x) = v (w (x))

$$= v\left(\frac{[i]x+[j]}{[k]x+[l]}\right)$$

$$= \frac{[e]\left(\frac{[i]x+[j]}{[k]x+[l]}\right)+[f]}{[g]\left(\frac{[i]x+[j]}{[k]x+[l]}\right)+[h]}$$

$$= \frac{([ei] + [fk])x + ([ej] + [fl])}{([gi] + [hk])x + ([gj] + [hl])}$$

dengan ([ei] + [fk]) ([gj] + [hl]) + {-([gi] + [hk]) ([ej] + [fl])}

= ([eh] + [-fg]) ([il] + [-kj]) ≠ [0], karena ([eh] + [-fg]) ≠ [0] dan ([il] + [-kj]) ≠ [0].

(u o (v o w)) (x) = u ((v o w) (x))

$$= u\left(\frac{([ei] + [fk])x + ([ej] + [fl])}{([gi] + [hk])x + ([gj] + [hl])}\right)$$

$$= \frac{[a]\left(\frac{([ei] + [fk])x + ([ej] + [fl])}{([gi] + [hk])x + ([gj] + [hl])}\right) + [b]}{[c]\left(\frac{([ei] + [fk])x + ([ej] + [fl])}{([gi] + [hk])x + ([gj] + [hl])}\right) + [d]}$$

$$= \frac{([aei] + [fak] + [bgi] + [bhk])x + ([aej] + [afl] + [bgj] + [bhl])}{([cei] + [fkc] + [dgi] + [dhk])x + ([cej] + [cfl] + [dgj] + [dhl])}$$

dengan ([aei] + [fak] + [bgi] + [bhk]) ([cej] + [cfl] + [dgj] + [dhl]) + {-([cei] + [fkc] + [dgi] + [dhk]) ([aej] + [afl] + [bgj] + [bhl])}

= ([ad] + [-bc]) ([eh] + [-fg]) ([il] + [-kj]) ≠ [0], karena ([ad] + [-bc]) ≠ [0], ([eh] + [-fg]) ≠ [0] dan ([il] + [-kj]) ≠ [0]

Terbukti komposisi fungsi bilinear atas Z_p bersifat asosiatif.

ii. Invers Fungsi Bilinear atas Z_p

Suatu fungsi mempunyai fungsi invers bila dan hanya bila fungsi itu merupakan fungsi bijektif.

Akan diperlihatkan bahwa fungsi bilinear atas Z_p dari P_p ke P_p merupakan fungsi bijektif.

$f : P_p \rightarrow P_p : f(x) = y = \dfrac{[a]x + [b]}{[c]x + [d]}$; [a], [b], [c], [d] $\in Z_p$, [ad] + [-bc] $\neq$ [0]

a. Akan ditunjukkan bahwa f merupakan fungsi injektif.

Diambil $x_1, x_2 \in P_p$ dengan $f(x_1) = f(x_2)$

maka $\dfrac{[a]x_1 + [b]}{[c]x_1 + [d]} = \dfrac{[a]x_2 + [b]}{[c]x_2 + [d]}$

$$\begin{aligned}
([a]x_1 + [b])([c]x_2 + [d]) &= ([a]x_2 + [b])([c]x_1 + [d]) \\
[ac]x_1x_2 + [bc]x_2 + [ad]x_1 + [bd] &= [ac]x_1x_2 + [bc]x_1 + [ad]x_2 + [bd] \\
[ad]x_1 + [bc]x_2 &= [bc]x_1 + [ad]x_2 \\
([ad] + [-bc])\, x_1 &= ([ad] + [-bc])\, x_2 \\
x_1 &= x_2.
\end{aligned}$$

Jadi f merupakan fungsi injektif.

b. Akan ditunjukkan bahwa f merupakan fungsi surjektif.

Kita ambil $y \in P_p$ maka ada $x = \dfrac{[-d]y + [b]}{[c]y + [-a]}$ sehingga $f(x) = y = \dfrac{[a]x + [b]}{[c]x + [d]}$.

Jadi f merupakan fungsi surjektif.

Karena f merupakan fungsi injektif dan surjektif, maka f merupakan fungsi bijektif, sehingga fungsi bilinear atas Z_p dari P_p ke P_p mempunyai invers.

Jika f (x) = y = $\frac{[a]x+[b]}{[c]x+[d]}$, [ad] + [-bc] $\neq$ [0], maka ([c]x + [d]) y = [a]x + [b],

sehingga $x = \frac{[-d]y+[b]}{[c]y+[-a]}$, [ad] + [-bc] $\neq$ [0].

Invers fungsi bilinear atas Z_p dari P_p ke P_p merupakan fungsi bilinear atas Z_p juga.

BAB IV

GRUP FUNGSI BILINEAR ATAS Z_P

Setelah kita mempelajari mengenai grup dan fungsi bilinear atas Z_p, kita akan membahas mengenai grup fungsi bilinear atas Z_p yang dilengkapi dengan operasi komposisi fungsi. Sebelum kita buktikan bahwa himpunan fungsi bilinear atas Z_p yang dilengkapi dengan operasi komposisi fungsi merupakan suatu grup, kita lihat dulu beberapa contoh himpunan fungsi bilinear atas Z_p.

Dalam penulisan di sini [a] ditulis dengan a.

Contoh 1 :

Himpunan fungsi bilinear atas $Z_2 = \{0, 1\}$ yakni

$$\left\{x, \frac{1}{x}, x+1, \frac{1}{x+1}, \frac{x}{x+1}, \frac{x+1}{x}\right\}$$

Contoh 2 :

Himpunan fungsi bilinear atas $Z_3 = \{0, 1, 2\}$ yakni

$$\left\{x, \frac{1}{x}, \frac{1}{x+1}, \frac{1}{x+2}, \frac{1}{2x}, \frac{1}{2x+1}, \frac{1}{2x+2}, \frac{x}{2}, \frac{x}{x+1}, \frac{x}{x+2}, \frac{x}{2x+1}, \frac{x}{2x+2}, x+1, \frac{x+1}{2}\right.$$

$$\left.\frac{x+1}{x}, \frac{x+1}{x+2}, \frac{x+1}{2x}, \frac{x+1}{2x+1}, x+2, \frac{x+2}{2}, \frac{x+2}{x}, \frac{x+2}{2x}, \frac{x+2}{x+1}, \frac{x+2}{2x+2}\right\}$$

Contoh 3 :

Himpunan fungsi bilinear atas $Z_5 = \{0, 1, 2, 3, 4\}$ yakni

$$\{x,\ x+1,\ x+2,\ x+3,\ x+4,\ 2x,\ 2x+1,\ 2x+2,\ 2x+3,\ 2x+4,\ 3x,\ 3x+1,\ 3x+2,\ 3x+3,$$

$$3x+4,\ 4x,\ 4x+1,\ 4x+2,\ 4x+3,\ 4x+4,\ \frac{1}{x},\frac{2}{x},\frac{3}{x},\frac{4}{x},\frac{x+1}{x},\frac{x+2}{x},\frac{x+3}{x},\frac{x+4}{x},$$

$$\frac{2x+1}{x},\frac{2x+2}{x},\frac{2x+3}{x},\frac{2x+4}{x},\frac{3x+1}{x},\frac{3x+2}{x},\frac{3x+3}{x},\frac{3x+4}{x},\frac{4x+1}{x},\frac{4x+2}{x},$$

$$\frac{4x+3}{x},\frac{4x+4}{x},\frac{1}{x+1},\frac{2}{x+1},\frac{3}{x+1},\frac{4}{x+1},\frac{x}{x+1},\frac{x+2}{x+1},\frac{x+3}{x+1},\frac{x+4}{x+1},\frac{2x}{x+1},\frac{2x+1}{x+1},$$

$$\frac{2x+3}{x+1},\frac{2x+4}{x+1},\frac{3x}{x+1},\frac{3x+1}{x+1},\frac{3x+2}{x+1},\frac{3x+4}{x+1},\frac{4x}{x+1},\frac{4x+1}{x+1},\frac{4x+2}{x+1},\frac{4x+3}{x+1},\frac{1}{x+2},$$

$$\frac{2}{x+2},\frac{3}{x+2},\frac{4}{x+2},\frac{x}{x+2},\frac{x+1}{x+2},\frac{x+3}{x+2},\frac{x+4}{x+2},\frac{2x}{x+2},\frac{2x+1}{x+2},\frac{2x+2}{x+2},\frac{2x+3}{x+2},\frac{3x}{x+2},$$

$$\frac{3x+2}{x+2},\frac{3x+3}{x+2},\frac{3x+4}{x+2},\frac{4x}{x+2},\frac{4x+1}{x+2},\frac{4x+2}{x+2},\frac{4x+4}{x+2},\frac{1}{x+3},\frac{2}{x+3},\frac{3}{x+3},\frac{4}{x+3},$$

$$\frac{x}{x+3},\frac{x+1}{x+3},\frac{x+2}{x+3},\frac{x+4}{x+3},\frac{2x}{x+3},\frac{2x+2}{x+3},\frac{2x+3}{x+3},\frac{2x+4}{x+3},\frac{3x}{x+3},\frac{3x+1}{x+3},\frac{3x+2}{x+3},$$

$$\frac{3x+3}{x+3},\frac{4x}{x+3},\frac{4x+1}{x+3},\frac{4x+3}{x+3},\frac{4x+4}{x+3},\frac{1}{x+4},\frac{2}{x+4},\frac{3}{x+4},\frac{4}{x+4},\frac{x}{x+4},\frac{x+1}{x+4},$$

$$\frac{x+2}{x+4},\frac{x+3}{x+4},\frac{2x}{x+4},\frac{2x+1}{x+4},\frac{2x+2}{x+4},\frac{2x+4}{x+4},\frac{3x}{x+4},\frac{3x+1}{x+4},\frac{3x+3}{x+4},\frac{3x+4}{x+4},\frac{4x}{x+4},$$

$$\frac{4x+2}{x+4},\frac{4x+3}{x+4},\frac{4x+4}{x+4}\}$$

A. Grup Fungsi Bilinear atas Z_p

Himpunan fungsi bilinear atas Z_p yang dilengkapi operasi "o" yakni operasi komposisi fungsi membentuk suatu grup, disebut Grup Fungsi Bilinear atas Z_p dan dinotasikan $GFBZ_p$.

Teorema berikut akan membuktikan bahwa himpunan fungsi bilinear atas Z_p yang dilengkapi operasi komposisi fungsi merupakan grup.

Teorema 4.A.1 :

Jika FBZ_p adalah himpunan fungsi bilinear atas Z_p yang dilengkapi operasi komposisi fungsi maka (FBZ_p, o) merupakan grup yang dinotasikan $GFBZ_p$.

Bukti :

a. Ambil sembarang $k, l \in FBZ_p$ dengan $k(x) = \dfrac{ax+b}{cx+d}$, $ad - bc \neq 0$, $a, b, c, d \in Z_p$ dan $l(x) = \dfrac{ex+f}{gx+h}$, $eh - fg \neq 0$, $e, f, g, h \in Z_p$.

Akan ditunjukkan $k \circ l \in FBZ_p$.

$$(k \circ l)(x) = k(l(x)) = k\left(\frac{ex+f}{gx+h}\right)$$

$$= \frac{(ae+bg)x + (af+bh)}{(ce+dg)x + (cf+dh)}$$

dengan $ae + bg, af + bh, ce + dg, cf + dh \in Z_p$ dan

$$(ae + bg)(cf + dh) - (ce + dg)(af + bh)$$

= (ad – bc) (eh – fg) ≠ 0, karena ad – bc ≠ 0 dan eh – fg ≠ 0.

b. Ambil sembarang k, l, m ∈ FBZ_p, dengan k (x) = $\frac{ax+b}{cx+d}$, ad – bc ≠ 0, a, b, c, d ∈ Z_p, l (x) = $\frac{ex+f}{gx+h}$, eh – fg ≠ 0, e, f, g, h ∈ Z_p dan m (x) = $\frac{ix+j}{nx+p}$, ip – nj ≠ 0, i, j, n, p ∈ Z_p, maka menurut sub bab 3.C.ii, komposisi fungsi bilinear atas Z_p bersifat asosiatif, sehingga (k o l) o m = k o (l o m).

c. Terdapat fungsi identitas yakni k ∈ FBZ_p dengan k (x) = x, sedemikian hingga

(∀l ∈ FBZ_p) (k o l) (x) = (l o k) (x) = l (x).

d. Ambil sembarang k ∈ FBZ_p dengan k (x) = $\frac{ax+b}{cx+d}$, ad – bc ≠ 0, a, b, c, d ∈ Z_p, maka menurut sub bab 3.C.i, dapat ditemukan k^{-1} ∈ FBZ_p dengan k^{-1} (x) = $\frac{dx-b}{-cx+a}$, ad – bc ≠ 0, d, -b, -c, a ∈ Z_p.

Dari a, b, c, dan d terbukti bahwa (FBZ_p, o) merupakan grup. ■

Contoh 4 :

Himpunan fungsi bilinear atas Z_2 (FBZ_2) yang dilengkapi operasi komposisi fungsi merupakan suatu grup.

$$FBZ_2 = \left\{x, \frac{1}{x}, x+1, \frac{1}{x+1}, \frac{x+1}{x}, \frac{x}{x+1}\right\} = \{f_0, f_1, f_2, f_3, f_4, f_5\}$$

Perhatikan tabel hasil operasi komposisi dari fungsi-fungsi anggota FBZ_2 di bawah ini

o	f_0	f_1	f_2	f_3	f_4	f_5
f_0	f_0	f_1	f_2	f_3	f_4	f_5
f_1	f_1	f_0	f_3	f_2	f_5	f_4
f_2	f_2	f_4	f_0	f_5	f_1	f_3
f_3	f_3	f_5	f_1	f_4	f_0	f_2
f_4	f_4	f_2	f_5	f_0	f_3	f_1
f_5	f_5	f_3	f_4	f_1	f_2	f_0

Tabel A

- Jika diambil sembarang $f, g \in FBZ_2$ maka $f \circ g \in FBZ_2$.

  Sehingga sifat tertutup terpenuhi.
- Ambil sembarang $f, g, h \in FBZ_2$ maka $f \circ (g \circ h) = (f \circ g) \circ h$.

  Sehingga sifat asosiatif terpenuhi.
- Untuk semua $f \in FBZ_p$ maka terdapat $f_0 = x \in FBZ_p$ sedemikian sehingga untuk $(\forall f \in FBZ_p)\ (f \circ f_0) = f = (f_0 \circ f)$.
- Ambil sembarang $f \in FBZ_2$ maka terdapat $f^{-1} \in FBZ_2$ sedemikian sehingga $(f \circ f^{-1}) = (f^{-1} \circ f) = f_0 = x$.

Jadi terbukti bahwa (FBZ_2, o) merupakan grup.

1. Pusat dari $GFBZ_p$

Dalam grup G kita mengenal pusat dari G yang dinotasikan dengan Z (G) yaitu himpunan semua elemen dari G yang komutatif dengan sembarang elemen dari G. Di dalam $GFBZ_p$ juga terdapat pusat, untuk itu perhatikanlah teorema berikut.

Teorema 4.A.2 :

$H = \{f \mid f(x) = x\}$ merupakan pusat dari $GFBZ_p$, sehingga $H = Z(GFBZ_p)$.

Bukti :

a. Akan dibuktikan $H \subseteq Z(GFBZ_p)$.

Ambil $f \in H$ dengan $f(x) = x$ dan ambil sembarang fungsi $g \in GFBZ_p$ dengan $g(x) = \dfrac{ax+b}{cx+d}$, a, b, c, d $\in Z_p$, $ad - bc \neq 0$.

Akan ditunjukkan $f \in Z(GFBZ_p)$ yakni $f \circ g = g \circ f$.

Karena fungsi f dengan $f(x) = x$ merupakan fungsi identitas pada $GFBZ_p$, maka untuk semua fungsi $g \in GFBZ_p$ dengan $g(x) = \dfrac{ax+b}{cx+d}$, a, b, c, d $\in Z_p$, $ad - bc \neq 0$ berlaku $f \circ g = g \circ f = g$.

Sehingga $f \circ g = g \circ f$.

Jadi terbukti $H \subseteq Z(GFBZ_p)$.

b. Akan dibuktikan $Z(GFBZ_p) \subseteq H$.

Ambil sembarang $f \in Z(GFBZ_p)$ dengan $f(x) = \dfrac{ax+b}{cx+d}$, a, b, c, d $\in Z_p$, $ad - bc \neq 0$.

Akan ditunjukkan $f \in H$ yakni $f(x) = x$. Karena $f \in Z(GFBZ_p)$ maka untuk semua $g \in GFBZ_p$ dengan $g(x) = \dfrac{ex+f}{gx+h}$, $e, f, g, h \in Z_p$, $eh - fg \neq 0$, maka $f \circ g = g \circ f$. Misalkan diambil fungsi $h \in GFBZ_p$ dengan $h(x) = x + 1$. Sebagai catatan, untuk bilangan prima p manapun fungsi h selalu di dalam $GFBZ_p$.

Perhatikan bahwa

$$(f \circ h)(x) = (h \circ f)(x)$$

$$f(x+1) = h\left(\frac{ax+b}{cx+d}\right)$$

$$\frac{ax+(a+b)}{cx+(c+d)} = \frac{(a+c)x+(b+d)}{cx+d}$$

sehingga didapat persamaan

$$acx^2+adx+(a+b)cx+(a+b)d = (a+c)cx^2+(b+d)cx+(c+d)(a+c)x+(c+d)(b+d).$$

Dari persamaan di atas didapat

i) $acx^2 = (a + c)cx^2$, maka $a = a + c$ sehingga $c = 0$.

ii) $(a + b)d = (c + d)(b + d)$, maka $ad + bd = db + dd$ sehingga $a = d$.

Dengan demikian didapat fungsi f dengan $f(x) = \dfrac{ax+b}{a}$ anggota dari $Z(GFBZ_p)$.

Jika diambil fungsi $l \in GFBZ_p$ dengan $l(x) = \dfrac{x}{x+1}$. Untuk bilangan prima p berapapun fungsi l selalu merupakan elemen dari $GFBZ_p$.

Karena $f \in Z(GFBZ_p)$ dan $l \in GFBZ_p$, maka

$$(f \circ l)(x) = (l \circ f)(x)$$

$$f\left(\frac{x}{x+1}\right) = l\left(\frac{ax+b}{a}\right)$$

$$\frac{(a+b)x+b}{ax+a} = \frac{ax+b}{ax+(a+b)}$$

sehingga didapat persamaan berikut

$(a + b)ax^2 + (a + b)(a + b)x + abx + (a + b)b = aax^2 + (ab + aa)x + ab$

Dari persamaan tersebut didapat a + b = a sehingga b = 0.

Maka didapat fungsi f dengan $f(x) = \dfrac{ax}{a} = x$ elemen dari H.

Sehingga $Z(GFBZ_p) \subseteq H$.

Dari a dan b terbukti bahwa $H = Z(GFBZ_p)$. ■

2. Order $GFBZ_p$

Banyaknya elemen pada suatu grup, misalnya grup G disebut order dari grup G dan dinotasikan $|G|$. Apabila $|G|$ berhingga maka G disebut grup berhingga dan apabila $|G|$ tak hingga maka G disebut grup tak hingga. Anggota dari $GFBZ_p$ yakni $\{f \mid f(x) = \dfrac{ax+b}{cx+d}$, $a, b, c, d \in Z_p$, $ad - bc \neq 0\}$. Karena Z_p berhingga maka $|GFBZ_p|$ juga berhingga. Selanjutnya akan dicari rumus umum untuk menentukan $|GFBZ_p|$. Dalam pembahasan nanti, pembahasan diawali dari contoh-contoh $GFBZ_p$ dengan p yang sederhana dahulu, sehingga kita dapat langsung menghitung ordernya. Setelah itu, kita baru mencari rumus umum untuk $|GFBZ_p|$.

Anggota dari $GFBZ_p$ yakni fungsi f dengan $f(x) = \dfrac{ax+b}{cx+d}$, $a, b, c, d \in Z_p$ dan $ad - bc \neq 0$.

Pada penulisan di depan sudah diberikan contoh himpunan dari $GFBZ_2$ yakni $\left\{x, \dfrac{1}{x}, x+1, \dfrac{1}{x+1}, \dfrac{x}{x+1}, \dfrac{x+1}{x}\right\}$. Sehingga order dari $GFBZ_2$ atau $|GFBZ_2|$ yakni 6.

Untuk mencari fungsi bilinear atas Z_2 dapat dicari dengan bantuan tabel berikut

c,d \ a,b	0,0	0,1	1,0	1,1
0,0	x	x	x	x
0,1	x	x	v	v
1,0	x	v	x	v
1,1	x	v	v	x

(x) menunjukkan nilai $ad - bc = 0$

(v) menunjukkan nilai $ad - bc \neq 0$

Tabel B

- Baris paling atas menunjukkan semua pasangan terurut (a, b) dengan $a, b \in Z_p$.
- Kolom paling kiri menunjukkan semua pasangan terurut (c, d) dengan $c, d \in Z_p$.

Sehingga anggota fungsi bilinear atas Z_2 yakni fungsi-fungsi

$$\frac{1}{x}, \frac{1}{x+1}, x, \frac{x}{x+1}, x+1, \frac{x+1}{x}.$$

Demikian juga jika kita mencari fungsi bilinear atas Z_3 dapat dicari dengan cara yang sama dengan cara di atas.

c,d \ a,b	0,0	0,1	0,2	1,0	1,1	1,2	2,0	2,1	2,2
0,0	x	x	x	x	x	x	x	x	x
0,1	x	x	x	v	v	v	v	v	v
0,2	x	x	x	v	v	v	v	v	v
1,0	x	v	v	x	v	v	x	v	v
1,1	x	v	v	v	x	v	v	v	x
1,2	x	v	v	v	v	x	v	x	v
2,0	x	v	v	x	v	v	x	v	v
2,1	x	v	v	v	v	x	v	x	v
2,2	x	v	v	v	x	v	v	v	x

Tabel C

Sehingga fungsi yang memenuhi syarat sebagai fungsi bilinear yakni himpunan

$$\left\{\frac{1}{x}, \frac{1}{x+1}, \frac{1}{x+2}, \frac{1}{2x}, \frac{1}{2x+1}, \frac{1}{2x+2}, \frac{2}{x}, \frac{2}{x+1}, \frac{2}{x+2}, \frac{2}{2x}, \frac{2}{2x+1}, \frac{2}{2x+2}, x,\right.$$

$$\frac{x}{2}, \frac{x}{x+1}, \frac{x}{x+2}, \frac{x}{2x+1}, \frac{x}{2x+2}, x+1, \frac{x+1}{2}, \frac{x+1}{x}, \frac{x+1}{x+2}, \frac{x+1}{2x}, \frac{x+1}{2x+1}, x+2,$$

$$\frac{x+2}{2}, \frac{x+2}{x}, \frac{x+2}{x+1}, \frac{x+2}{2x}, \frac{x+2}{2x+2}, 2x, \frac{2x}{2}, \frac{2x}{x+1}, \frac{2x}{x+2}, \frac{2x}{2x+1}, \frac{2x}{2x+2},$$

$2x+1, \frac{2x+1}{2}, \frac{2x+1}{x}, \frac{2x+1}{x+1}, \frac{2x+1}{2x}, \frac{2x+1}{2x+2}, 2x+2, \frac{2x+2}{2}, \frac{2x+2}{x}, \frac{2x+2}{x+2},$

$\left.\frac{2x+2}{2x}, \frac{2x+2}{2x+1}\right\}.$

Tetapi karena fungsi $\frac{ax+b}{cx+d} = \frac{n}{n}\left(\frac{ax+b}{cx+d}\right)$ dengan n $\in Z_3 - \{0\}$, yakni n = 1 dan n = 2, maka setiap fungsi dalam himpunan di atas pastilah terdapat satu fungsi lain yang sama, misalnya fungsi $\frac{1}{x}$ sama dengan fungsi $\frac{2}{2x}$ karena $\frac{2}{2x} = \frac{2}{2}\left(\frac{1}{x}\right) = \frac{1}{x}$, fungsi $\frac{2x+1}{2}$ sama dengan fungsi x + 2 karena $\frac{2x+1}{2} = \frac{2}{2}\left(\frac{x+2}{1}\right) = x + 2$.

Jadi fungsi bilinear atas Z_3 yakni

$\left\{x, \frac{1}{x}, \frac{1}{x+1}, \frac{1}{x+2}, \frac{1}{2x}, \frac{1}{2x+1}, \frac{1}{2x+2}, \frac{x}{2}, \frac{x}{x+1}, \frac{x}{x+2}, \frac{x}{2x+1}, \frac{x}{2x+2}, x+1,\right.$

$\left.\frac{x+1}{2}, \frac{x+1}{x}, \frac{x+1}{x+2}, \frac{x+1}{2x}, \frac{x+1}{2x+1}, x+2, \frac{x+2}{2}, \frac{x+2}{x}, \frac{x+2}{2x}, \frac{x+2}{x+1}, \frac{x+2}{2x+2}\right\}$

Sehingga $|\,GFBZ_3\,| = \frac{48}{n}$, dengan n banyaknya elemen dalam $Z_3 - \{0\}$

$= \frac{48}{2}$

$= 24.$

Berikut ini akan dicari rumus umum untuk menentukan banyaknya anggota dalam $GFBZ_p$ atau order dari $GFBZ_p$.

Diandaikan a, b, c, d $\in Z_p$, akan dicari fungsi bilinear atas Z_p.

Perhatikan tabel berikut ini

Semua pasangan terurut (a, b)	Nilai c dan d yang menyebabkan nilai ad – bc = 0		Banyaknya pasangan terurut (c, d) yang menyebabkan ad – bc = 0
(0, 0)	$c : 0 \rightarrow p - 1$	$d : 0 \rightarrow p - 1$	p^2
(0, 1)	$c = 0$	$d : 0 \rightarrow p - 1$	p
(0, 2)	$c = 0$	$d : 0 \rightarrow p - 1$	p
(0, 3)	$c = 0$	$d : 0 \rightarrow p - 1$	p
$\vdots$	$\vdots$	$\vdots$	$\vdots$
(0, p – 1)	$c = 0$	$d : 0 \rightarrow p - 1$	p
(1, 0)	$c : 0 \rightarrow n - 1$	$d = 0$	p
(1, 1)	$c = d$	$d : 0 \rightarrow p - 1$	p
(1, 2)	$2c = d$	$d : 0 \rightarrow p - 1$	p
(1, 3)	$3c = d$	$d : 0 \rightarrow p - 1$	p
$\vdots$	$\vdots$	$\vdots$	$\vdots$
(1, p – 1)	$(p - 1)c = d$	$d : 0 \rightarrow p - 1$	p
(2, 0)	$c : 0 \rightarrow n - 1$	$d = 0$	p
(2, 1)	$c = 2d$	$d : 0 \rightarrow p - 1$	p
(2, 2)	$c = d$	$d : 0 \rightarrow p - 1$	p
(2, 3)	$3c = 2d$	$d : 0 \rightarrow p - 1$	p
(2, 4)	$4c = 2d$	$d : 0 \rightarrow p - 1$	p
$\vdots$	$\vdots$	$\vdots$	$\vdots$
(2, p – 1)	$(p - 1)c = 2d$	$d : 0 \rightarrow p - 1$	p
(3, 0)	$c : 0 \rightarrow p - 1$	$d = 0$	p
(3, 1)	$c = 3d$	$d : 0 \rightarrow p - 1$	p
(3, 2)	$2c = 3d$	$d : 0 \rightarrow p - 1$	p
(3, 3)	$c = d$	$d : 0 \rightarrow p - 1$	p
(3, 4)	$4c = 3d$	$d : 0 \rightarrow p - 1$	p

(3, 5) ⋮ (3, p – 1)	$5c = 3d$ ⋮ $(p-1)c = 3d$	$d : 0 \to p-1$ ⋮ $d : 0 \to p-1$	p ⋮ p
⋮	⋮	⋮	⋮
(p – 1, 0) (p – 1, 1) (p – 1, 2) (p – 1, 3) (p – 1, 4) (p – 1, 5) ⋮ (p – 1, p – 1)	$c : 0 \to p-1$ $c = (p-1)d$ $2c = (p-1)d$ $3c = (p-1)d$ $4c = (p-1)d$ $5c = (p-1)d$ ⋮ $c = d$	$d = 0$ $d : 0 \to p-1$ $d : 0 \to p-1$ $d : 0 \to p-1$ $d : 0 \to p-1$ $d : 0 \to p-1$ ⋮ $d : 0 \to p-1$	p p p p p p ⋮ p

Tabel D

- Banyaknya pasangan terurut (a, b) yakni p^2.
- Banyaknya pasangan terurut (c, d) yakni p^2.
- Untuk pasangan terurut (a, b) = (0, 0), terdapat p^2 buah pasangan terurut (c, d) yang menyebabkan ad – bc = 0.
- Untuk setiap pasangan terurut (a, b) ≠ (0, 0), terdapat p buah pasangan terurut (c, d) yang menyebabkan ad – bc = 0. Sehingga banyaknya pasangan terurut (a, b) yang menyebabkan ad – bc = 0 di sini ada $p^2 - 1$.

Untuk setiap fungsi $\dfrac{ax+b}{cx+d} \in FBZ_p$ maka $\dfrac{ax+b}{cx+d} = \dfrac{n}{n}\left(\dfrac{ax+b}{cx+d}\right)$ dengan

$n \in Z_p - \{0\}$ (banyaknya n = p – 1), sehingga

$$|GFBZ_p| = \frac{p^2.p^2 - (p^2 + (p\,(p^2 - 1)))}{p-1}$$

$$= \frac{p^4 - p^3 - p^2 + p}{p - 1}$$

$$= \frac{(p^3 - p)(p - 1)}{p - 1}$$

$$= p^3 - p$$

Jadi banyaknya $|GFBZ_p|$ adalah $p^3 - p$.

3. Sikel

Fungsi $f \in GFBZ_p$ merupakan fungsi bijektif dari P_p ke P_p, sehingga f merupakan permutasi dari P_p ke P_p.

Sebagai contoh :

- Jika $f \in GFBZ_7$ dengan $f(x) = \dfrac{2x+1}{x+1}$, maka

$f(0) = 1$	$f(4) = 6$
$f(1) = 5$	$f(5) = 3$
$f(2) = 4$	$f(6) = \infty$
$f(3) = 0$	$f(\infty) = 2$

Maka orbit yang memuat 0 yakni (0, 1, 5, 3) yang membentuk sikel (0 1 5 3), orbit yang memuat 2 yakni (2, 4, 6, ∞) yang membentuk sikel (2 4 6 ∞) dan tidak terdapat titik tetap (sikel yang panjangnya 1).

Jadi terdapat 2 sikel yang panjangnya 4 dan tidak ada titik tetap.

Akan diselidiki sikel yang terbentuk oleh fungsi yang sama, tetapi dengan P_p yang lain. Misal fungsi yang diambil fungsi f dengan $f(x) = \frac{2x+1}{x+1}$.

1) Jika $f : P_3 \to P_3$ maka dengan cara yang sama seperti cara di atas akan diperoleh 2 sikel yakni (0 1) dan (2 ∞) yang panjangnya 2 dan tidak ada titik tetap.
2) Jika $f : P_5 \to P_5$ maka terdapat 1 sikel yakni (0 1 4 ∞ 2) yang panjangnya 5 dan ada 1 titik tetap yakni untuk $x = 3$.
3) Jika $f : P_{11} \to P_{11}$ maka terdapat 2 sikel yakni (0 1 7 6 5) dan (2 9 3 10 ∞) yang panjangnya 5 dan ada 2 titik tetap yakni untuk $x = 4$ dan $x = 8$.
4) Jika $f : P_{13} \to P_{13}$ maka terdapat 2 sikel yakni (0 1 8 12 ∞ 2 6) dan (3 5 4 7 10 9 11) yang panjangnya 7 dan tidak ada titik tetap.

Dari contoh di atas tampak bahwa jumlah titik tetap (sikel yang panjangnya 1) jumlahnya tidak lebih dari 2 elemen. Berikut ini akan dibuktikan teorema yang menunjukkan bahwa jumlah titik tetap fungsi $f \in GFBZ_p$ (f bukan fungsi identitas) tidak lebih dari 2. Tetapi sebelumnya kita buktikan dahulu teorema berikut.

Teorema 4.A.3 :

Jika $a \in Z_p$, $p > 2$, maka persamaan $x^2 = a$ akan mempunyai 2 penyelesaian yaitu r dan $p - r$ atau tidak mempunyai penyelesaian. Terkecuali untuk $x^2 = 0$, maka persamaan itu akan mempunyai 1 penyelesaian yakni 0.

Bukti :

Berdasarkan teorema 2.H.6 maka persamaan $x^2 = a$ tidak mungkin mempunyai lebih dari 2 penyelesaian. Sehingga persamaan $x^2 = a$, paling banyak mempunyai 2 penyelesaian.

Andaikan ada $r \in Z_p$ sedemikian hingga $x^2 = r^2$ maka kita dapatkan $(x + r)(x - r) = 0$. Dalam Z_p tidak memuat pembagi nol sehingga penyelesaiannya $x = r$ atau $x = -r$. Sedangkan $-r = p - r$. Jadi kita dapatkan 2 penyelesaian $x = r$ atau $x = p - r$.

Jika tidak ada $r \in Z_p$ sedemikian hingga $x^2 = r^2$ maka persamaan itu tidak mempunyai penyelesaian.

Jika $p = 2$ maka kita hanya mendapatkan 1 penyelesaian yakni $x = r$, karena $\forall a \in Z_2$ maka $a = p - a$. ■

Selanjutnya kita akan membuktikan jumlah titik tetap dalam fungsi $f \in GFBZ_p$ (f bukan fungsi identitas) paling banyak 2 elemen.

Teorema 4.A.4 :

Jika $GFBZ_p$ merupakan grup fungsi bilinear pada Z_p, maka setiap anggota dari $GFBZ_p$ yang bukan fungsi identitas mempunyai paling banyak 2 titik tetap.

Bukti :

Andaikan $f \in GFBZ_p$ dengan $f(x) = \dfrac{ax + b}{cx + d}$, $ad - bc \neq 0$, $a, b, c, d \in Z_p$ dan z merupakan titik tetap dalam f. Karena z titik tetap dalam f maka $f(z) = \dfrac{az + b}{cz + d} = z$, dan kita peroleh $cz^2 + (d - a)z - b = 0$ yang merupakan persamaan kuadratik dalam z.

Penyelesaian persamaan itu yakni $z_1 = \dfrac{(a-d) + \sqrt{(d-a)^2 + 4bc}}{2c}$ dan $z_2 = \dfrac{(a-d) - \sqrt{(d-a)^2 + 4bc}}{2c}$.

Andaikan $y^2 = \dfrac{(d-a)^2 + 4bc}{2c}$, maka menurut teorema 4.A.3 persamaan itu akan mempunyai 2 penyelesaian untuk y yakni e dan p – e atau tidak mempunyai penyelesaian.

- Jika mempunyai 2 penyelesaian e dan p – e maka

  $z_{1.1} = \dfrac{(a-d)+e}{2c}$, $z_{1.2} = \dfrac{(a-d)+(p-e)}{2c} = \dfrac{(a-d)-e}{2c}$

  dan

$z_{2.1} = \dfrac{(a-d)-e}{2c}$, $z_{2.2} = \dfrac{(a-d)-(p-e)}{2c} = \dfrac{(a-d)+e}{2c}$

Karena $z_{1.1} = z_{2.2}$ dan $z_{2.1} = z_{1.2}$, maka kita mendapatkan 2 titik tetap yakni

$z_1 = \dfrac{(a-d)+e}{2c}$ dan $z_2 = \dfrac{(a-d)-e}{2c}$.

- Jika persamaan $y^2 = \dfrac{(d-a)^2 + 4bc}{2c}$ tidak mempunyai penyelesaian untuk y maka fungsi itu tidak mempunyai titik tetap.
- Jika $y^2 = \dfrac{(d-a)^2 + 4bc}{2c} = 0$ yang berarti bahwa ada 1 penyelesaian untuk y yakni 0 maka fungsi itu akan mempunyai 1 titik tetap yakni $z = \dfrac{a-d}{2c}$.

Jadi terbukti bahwa jumlah titik tetap dalam fungsi f $\in GFBZ_p$ tidak lebih dari 2 elemen. ■

Selanjutnya dari fungsi-fungsi dalam $GFBZ_p$ dengan $p > 2$ akan dicari kemungkinan untuk titik tetapnya.

Andaikan f $\in GFBZ_p$ dengan $f(x) = \dfrac{ax+b}{cx+d}$, $ad - bc \neq 0$, a, b, c, d $\in Z_p$.

1) Jika $c \neq 0$, $(d-a)^2 + 4bc \neq 0$, dan ada $e \in Z_p$ sedemikian hingga $e^2 = (d-a)^2 + 4bc$, maka fungsi itu mempunyai 2 titik tetap yakni $z_1 = \dfrac{(a-d)+e}{2c}$ dan $z_2 = \dfrac{(a-d)-e}{2c}$.

2) Jika $c \neq 0$, $(d-a)^2 + 4bc = 0$, maka fungsi itu mempunyai 1 titik tetap yakni $z_1 = \frac{a-d}{2c}$.

3) Jika $c \neq 0$, $(d-a)^2 + 4bc \neq 0$ dan tidak ada $e \in Z_p$ sedemikian hingga $e^2 = (d-a)^2 + 4bc$, maka fungsi itu tidak mempunyai titik tetap.

4) Jika $c = 0$, $d - a \neq 0$ maka fungsi $f(x) = \frac{ax+b}{d}$.

   Jika z merupakan titik tetap maka $f(z) = \frac{az+b}{d} = z$, sehingga kita dapatkan $z = \frac{b}{d-a}$, sebagai titik tetap fungsi f.

   Tetapi untuk $c = 0$, $f(\infty) = \infty$. Jadi kita mendapatkan 2 titik tetap yakni $z = \infty$ dan $z = \frac{b}{d-a}$.

5) Jika $c = 0$, $d - a = 0$ maka dalam f hanya ada satu titik tetap yakni untuk $z = \infty$.

Contoh 5 :

Fungsi $g \in GFBZ_7$ dengan $g(x) = \frac{2x+2}{3x+1}$.

$a = 2$, $b = 2$, $c = 3 \neq 0$, $d = 1$.

Nilai $= (d-a)^2 + 4bc$

$\quad = (1-2)^2 + 4\,(2.3)$

$= 25$

$= 4$

Ada $e_1 = 2$ dan $e_2 = 5$ sedemikian hingga $e^2 = 4$, sehingga fungsi g mempunyai 2 titik tetap yakni

$$z_1 = \frac{1+2}{4} = 6$$

$$z_2 = \frac{1-2}{4} = 5$$

Jadi titik tetap dalam fungsi g tersebut yakni untuk z = 5 dan z = 6.

Contoh 6 :

Fungsi g $\in$ $GFBZ_7$ dengan g (x) = $\dfrac{5x+4}{2}$.

a = 5, b = 4, c = 0, d = 2, d – a = -3.

Titik tetap untuk fungsi g yakni z = $\dfrac{b}{d-a} = \dfrac{4}{-3} = 1$.

Karena c = 0 dan (d – a) $\neq$ 0 maka g (∞) = ∞.

Jadi terdapat 2 titik tetap yakni z = 1 dan z = ∞.

4. Aksi $GFBZ_p$ pada P_p

Seperti dibahas pada bab 2.F, aksi dari grup G pada himpunan X adalah pemetaan $\psi : G \times X \rightarrow X$ sedemikian hingga memenuhi :

i. ψ (e, x) = x, $\forall x \in X$ dan e elemen identitas pada G.

ii. $\psi(g_1 * g_2, x) = \psi(g_1, \psi(g_2, x)), \forall g_1, g_2 \in G$ dan $\forall x \in X$.

Akan ditunjukkan bahwa $GFBZ_p$ beraksi pada himpunan P_p.

Teorema 4.A.5 :

Jika $G = GFBZ_p$ dan $P_p = Z_p + \{\infty\}$ maka pemetaan $\lambda : G \times P_p \to P_p$ dengan aturan : $\lambda(f, a) = f(a), \forall f \in G$ dan $\forall a \in P_p$ merupakan aksi dari G pada P_p.

Bukti :

1) λ terdefinisi dengan baik, sebab

   Jika diambil sembarang $(f, a) \in G \times P_p$ maka $f(a) \in P_p$ dan $f(a) = \lambda(f, a)$.

   Ambil sembarang $(f_1, a_1), (f_2, a_2) \in G \times P_p$ sedemikian sehingga $(f_1, a_1) = (f_2, a_2)$, maka $f_1 = f_2$ dan $a_1 = a_2$, sehingga $f_1(a_1) = f_2(a_2)$.

   Jadi $\lambda(f_1, a_1) = \lambda(f_2, a_2)$.

2) Jika $g \in G$ dengan $g(x) = x, \forall x \in P_p$ merupakan elemen identitas dari G maka $\lambda(g, x) = g(x) = x$.

3) Ambil sembarang $f, g \in G$ dan sembarang $a \in P_p$, maka

$$\begin{aligned}\lambda(f \circ g, x) &= (f \circ g)(x)\\ &= f(g(x))\\ &= f(\lambda(g, x))\\ &= \lambda(f, \lambda(g, x))\end{aligned}$$

Jadi λ merupakan aksi grup $GFBZ_p$ pada himpunan P_p. ■

Pada contoh 17 bab II sudah ditunjukkan bahwa jika G grup dan H subgrup G, maka $\lambda : H \times G \rightarrow G$ dengan aturan $\lambda (h, g) = hgh^{-1}$, $\forall h \in H$ dan $\forall g \in G$ merupakan aksi dari H pada G dan disebut konjugat. Sedangkan elemen hgh^{-1} disebut konjugat dari g terhadap aksi dari H pada G.

Karena $GFBZ_p$ merupakan subgrup dari $GFBZ_p$ maka $\lambda : GFBZ_p \times GFBZ_p \rightarrow GFBZ_p$ dengan aturan $\lambda (h, g) = hgh^{-1}$, $\forall h \in GFBZ_p$ dan $\forall g \in GFBZ_p$ merupakan aksi dari $GFBZ_p$ pada $GFBZ_p$, sedangkan elemen hgh^{-1} disebut konjugat dari g terhadap aksi dari $GFBZ_p$ pada $GFBZ_p$.

Definisi 4.A.1 :

Jika f, g $\in GFBZ_p$ maka f dikatakan konjugat dari g (diberi simbol $f \sim g$), jika $\exists h \in GFBZ_p$ sedemikian sehingga $g = hfh^{-1}$.

Teorema 4.A.6 :

Jika $GFBZ_p$ grup maka konjugasi merupakan relasi ekuivalensi pada $GFBZ_p$.

Bukti :

Telah didefinisikan relasi konjugasi $f \sim g$ bila dan hanya bila $g = hfh$, untuk suatu $h \in GFBZ_p$.

- Relasi "$\sim$" bersifat refleksif sebab $g = ege^{-1}$, untuk suatu $e \in GFBZ_p$. Hal ini berarti $g \sim g$.

- Jika $f \sim g$ maka $g = hfh^{-1}$, untuk suatu $h \in GFBZ_p$. Sehingga $f = h^{-1}gh = h^{-1}g\,(h^{-1})^{-1}$, dengan $h^{-1} \in GFBZ_p$. Hal ini berarti $g \sim f$. Jadi sifat simetris terpenuhi.
- Jika $f \sim g$ maka $g = hfh^{-1}$ untuk suatu $h \in GFBZ_p$.

  Jika $g \sim k$ maka $k = lgl^{-1}$ untuk suatu $l \in GFBZ_p$.

  Maka $k = l\,(hfh^{-1})\,l^{-1}$

  $= (lh)\,f\,(h^{-1}l^{-1})$

  $= (lh)\,f\,(lh)^{-1}$, untuk suatu $lh \in GFBZ_p$.

  Jadi sifat transitif terpenuhi.

Dengan demikian relasi "~" merupakan relasi ekuivalensi. ■

Perhatikan bahwa jika diberikan $GFBZ_p$ grup dan $g \in GFBZ_p$ maka kelas konjugasi dari g pada $GFBZ_p$ adalah $\{f \in GFBZ_p \mid g = hfh^{-1}, h \in GFBZ_p\}$.

Contoh 7 :

Dalam $GFBZ_3$ fungsi f dengan $f(x) = x + 1$ merupakan konjugat dari fungsi g dengan $g(x) = \dfrac{1}{2x+2}$, karena terdapat fungsi h dengan $h(x) = \dfrac{x}{x+1}$, $h^{-1} = \dfrac{x}{2x+1}$ sedemikian hingga $g(x) = h(f(h^{-1}(x)))$

$$= h\left(f\left(\frac{x}{2x+1}\right)\right)$$

$$= h\left(\frac{1}{2x+1}\right)$$

$$= \frac{1}{2x+2}.$$

Contoh 8 :

Dalam $GFBZ_5$ fungsi f dengan f (x) = $\frac{3x+1}{2}$ merupakan konjugat dari fungsi g dengan g (x) = $\frac{x}{x+4}$, karena terdapat fungsi h = $\frac{2x+2}{x}$ dengan $h^{-1} = \frac{3}{4x+2}$, sedemikian hingga g (x) = h (f (h^{-1} (x)))

$$= h\left(f\left(\frac{3}{4x+2}\right)\right)$$

$$= h\left(\frac{4x+1}{3x+4}\right)$$

$$= \frac{4x}{4x+1}$$

$$= \frac{4}{4}\left(\frac{x}{x+4}\right)$$

$$= \frac{x}{x+4}.$$

Selanjutnya akan dicari subgrup isotropi dan orbit dalam himpunan P_p oleh $GFBZ_p$. Dalam pembahasan di sini penulis hanya membahas subgrup isotropi dari orbit dalam himpunan P_p oleh $GFBZ_2$ dan $GFBZ_3$, karena untuk $GFBZ_2$ dan $GFBZ_3$ jumlah anggotanya belum terlalu banyak.

Sebelumnya, kita lihat dahulu tabel nilai fungsi dari fungsi-fungsi dalam $GFBZ_2$ dan $GFBZ_3$.

- $GFBZ_2$

f(x) \ x	0	1	∞
x	0	1	∞
$\frac{1}{x}$	∞	1	0
$x+1$	1	0	∞
$\frac{1}{x+1}$	1	∞	0
$\frac{x}{x+1}$	0	∞	1
$\frac{x+1}{x}$	∞	0	1

Tabel E

- $GFBZ_3$

f(x) \ x	0	1	2	∞
x	0	1	2	∞
$\frac{1}{x}$	∞	1	2	0

f(x) \ x	0	1	2	∞
$x+1$	1	2	0	∞
$\frac{x+1}{2}$	2	1	0	∞

$\frac{1}{x+1}$	1	2	∞	0	$\frac{x+1}{x}$	∞	2	0	1
$\frac{1}{x+2}$	2	∞	1	0	$\frac{x+1}{x+2}$	2	∞	0	1
$\frac{1}{2x}$	∞	2	1	0	$\frac{x+1}{2x}$	∞	1	0	2
$\frac{1}{2x+1}$	1	∞	2	0	$\frac{x+1}{2x+1}$	1	∞	0	2
$\frac{1}{2x+2}$	2	1	∞	0	$x+2$	2	0	1	∞
$\frac{x}{2}$	0	2	1	∞	$\frac{x+2}{2}$	1	0	2	∞
$\frac{x}{x+1}$	0	2	∞	1	$\frac{x+2}{x}$	∞	0	2	1
$\frac{x}{x+2}$	0	∞	2	1	$\frac{x+2}{2x}$	∞	0	1	2
$\frac{x}{2x+1}$	0	∞	1	2	$\frac{x+2}{x+1}$	2	0	∞	1
$\frac{x}{2x+2}$	0	1	∞	2	$\frac{x+2}{2x+2}$	1	0	∞	2

Tabel F

Subgrup isotropi dalam $GFBZ_2$:

- Subgrup isotropi dari 0 : $G_0 = \left\{x, \frac{x}{x+1}\right\}$.

- Subgrup isotropi dari 1 : $G_1 = \left\{x, \frac{1}{x}\right\}$.

- Subgrup isotropi dari ∞ : $G_\infty = \{x, x+1\}$.

Subgrup isotropi dalam $GFBZ_3$:

- Subgrup isotropi dari 0 : $G_0 = \left\{x, \frac{x}{2}, \frac{x}{x+1}, \frac{x}{x+2}, \frac{x}{2x+1}, \frac{x}{2x+2}\right\}$.

- Subgrup isotropi dari 1 : $G_1 = \left\{x, \frac{1}{x}, \frac{1}{2x+2}, \frac{x}{2x+2}, \frac{x+1}{2}, \frac{x+1}{2x}\right\}$.

- Subgrup isotropi dari 2 : $G_2 = \left\{x, \frac{1}{x}, \frac{1}{2x+1}, \frac{x}{x+2}, \frac{x+2}{2}, \frac{x+2}{x}\right\}$.

- Subgrup isotropi dari ∞ : $G\infty = \left\{x, \frac{x}{2}, x+1, \frac{x+1}{2}, x+2, \frac{x+2}{2}\right\}$.

Akan dicari orbit-orbit dalam P_2 oleh $GFBZ_2$.

$P_2 = \{0, 1, \infty\}$

- Orbit dari 0 = G0 = $\{x \in P_2 \mid (\exists f \in GFBZ_2)\, f(x) = 0\} = \{0, 1, \infty\}$.
- Orbit dari 1 = G1 = $\{x \in P_2 \mid (\exists f \in GFBZ_2)\, f(x) = 1\} = \{0, 1, \infty\}$.
- Orbit dari ∞ = G∞ = $\{x \in P_2 \mid (\exists f \in GFBZ_2)\, f(x) = \infty\} = \{0, 1, \infty\}$.

Jadi orbit dalam P_2 oleh $GFBZ_2$ adalah $\{0, 1, \infty\}$.

Akan dicari orbit-orbit dalam P_3 oleh $GFBZ_3$.

$P_3 = \{0, 1, 2, \infty\}$

- Orbit dari 0 = G0 = $\{x \in P_3 \mid (\exists f \in GFBZ_3)\, f(x) = 0\} = \{0, 1, 2, \infty\}$.
- Orbit dari 1 = G1 = $\{x \in P_3 \mid (\exists f \in GFBZ_3)\, f(x) = 1\} = \{0, 1, 2, \infty\}$.
- Orbit dari 2 = G0 = $\{x \in P_3 \mid (\exists f \in GFBZ_3)\, f(x) = 2\} = \{0, 1, 2, \infty\}$.

- Orbit dari ∞ = $G\infty = \{x \in P_3 \mid (\exists f \in GFBZ_3)\ f(x) = \infty\} = \{0, 1, 2, \infty\}$.

Jadi orbit dalam P_3 oleh $GFBZ_3$ adalah $\{0, 1, 2, \infty\}$.

Contoh 9 :

Jika $P_3 = \{0, 1, 2, \infty\}$, $H = \left\{x, \frac{x}{2}, \frac{x}{x+1}, \frac{x}{x+2}, \frac{x}{2x+1}, \frac{x}{2x+2}\right\}$ subgrup dari $GFBZ_3$, tentukan orbit-orbit dalam P_3 oleh grup H.

P_3 adalah Himpunan-H.

- Orbit dari 0 = $H0 = \{x \in P_3 \mid (\exists f \in H)\ f(x) = 0\} = \{0\}$.
- Orbit dari 1 = $H1 = \{x \in P_3 \mid (\exists f \in H)\ f(x) = 1\} = \{1, 2, \infty\}$.
- Orbit dari 2 = $H2 = \{x \in P_3 \mid (\exists f \in H)\ f(x) = 2\} = \{1, 2, \infty\}$.
- Orbit dari ∞ = $H\infty = \{x \in P_3 \mid (\exists f \in H)\ f(x) = \infty\} = \{1, 2, \infty\}$.

Jadi orbit-orbit dalam P_3 oleh grup H adalah $\{0\}$ dan $\{1, 2, \infty\}$.

BAB V

PENUTUP

A. Kesimpulan

Berdasarkan uraian dari bab-bab sebelumnya, maka dapat disimpulkan hal-hal sebagai berikut :

1. Fungsi bilinear atas bilangan bulat modulo-p (Z_p) mempunyai bentuk umum $f(x) = \dfrac{ax+b}{cx+d}$ dengan a, b, c, d $\in Z_p$ dan $ad - bc \neq 0$.

   Himpunan fungsi bilinear atas Z_p dinotasikan dengan FBZ_p.

   Fungsi $f \in FBZ_p : P_p (Z_p + \{\infty\}) \rightarrow P_p$ merupakan fungsi bijektif.
2. Himpunan fungsi bilinear atas Z_p (FBZ_p) memenuhi struktur Grup terhadap operasi komposisi fungsi. Grup ini disebut fungsi bilinear atas himpunan bilangan bulat modulo-p dan dinotasikan $GFBZ_p$.
3. Pusat dari grup $GFBZ_p$ yakni fungsi $f \in GFBZ_p$ dengan $f(x) = x$, yang sekaligus merupakan elemen identitas dalam $GFBZ_p$.
4. Order dari $GFBZ_p$ atau $|\ GFBZ_p\ | = p^3 - p$.
5. Semua fungsi bilinear $f \in GFBZ_p$ mempunyai paling banyak 2 titik tetap (sikel yang panjangnya 1).
6. Ada aksi dari $GFBZ_p$ pada himpunan P_p ($Z_p + \{\infty\}$), sehingga P_p merupakan himpunan-$GFBZ_p$.

B. Saran

Pada fungsi bilinear anggota $GFBZ_p$ yang mempunyai 2 atau lebih sikel selain titik tetap, maka panjang sikel-sikel itu selalu sama. Karena keterbatasan penulis, penulis belum dapat membahas dan membuktikan bahwa panjang sikel dalam suatu fungsi bilinear anggota $GFBZ_p$ yang mempunyai 2 atau lebih sikel yang bukan titik tetap selalu sama. Hal tersebut dapat digunakan sebagai bahan penelitian lebih lanjut.

DAFTAR PUSTAKA

Durbin, R. John. 1985. *Modern Algebra*. New York : John Wiley and Sons, Inc.

Fraleigh, B. John. 1989. *A First Course in Abstract Algebra*. New York : Addison-Wesley Publishing Company.

Hall, F. M. 1972. *An Introduction to Abstract Algebra*. New York : Cambridge University Press.

Herstein, N. I. 1990. *Abstract Algebra*. New Jersey : Prentice-Hall International. Inc.

Herstein, N. I. 1976. *Topics in Algebra*. New York : John Wiley and Sons, Inc.

Narayan, Shanti. 1979. *A Text Book of Modern Abstract Algebra*. New Delhi : S. Chand and Company Ltd.

Narayan, Shanti. 1979. *Theory of Functions of Complex Variable*. New Delhi : S. Chand and Company Ltd.