MONOID DAN PENERAPANNYA PADA OTOMATA

SKRIPSI

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

Oleh :

Cornellius Heri S.
NIM : 981414032

PROGRAM STUDI PENDIDIKAN MATEMATIKA
JURUSAN PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM
FAKULTAS KEGURUAN DAN ILMU PENDIDIKAN
UNIVERSITAS SANATA DHARMA
YOGYAKARTA
2002

SKRIPSI

MONOID DAN PENERAPANNYA PADA OTOMATA

Yang disusun oleh :

Cornellius Heri S.

NIM : 981414032

Telah disetujui oleh :

Pembimbing,

M.V. Any Herawati, S.Si., M.Si.

Tanggal 25 - 9 - 2002

Pengesahan Skripsi
Berjudul

MONOID DAN PENERAPANNYA PADA OTOMATA

Yang disusun dan dipersiapkan oleh :

Cornellius Heri S.
NIM : 981414032

Telah dipertahankan di hadapan Panitia Penguji Skripsi
Fakultas Keguruan dan Ilmu Pendidikan
Universitas Sanata Dharma
Pada tanggal 7 September 2002

Susunan Panitia Penguji

	Nama lengkap	Tanda tangan
Ketua	: Drs. A. Atmadi, M.Si.	....
Sekretaris	: Drs. Th. Sugiarto, M.T.	....
Anggota	: M.V. Any Herawati, S.Si., M.Si.	....
Anggota	: Dra. Maria Agustiani, M.Si.	....
Anggota	: Dr. Y. Marpaung	....

Yogyakarta, 7 September 2002
Fakultas Keguruan dan Ilmu Pendidikan
Universitas Sanata Dharma
Dekan,

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

Tak seorangpun di dunia ini yang akan dikalahkan oleh nasib,

kecuali kalau orang itu menerima nasibnya sebagai suatu kekalahan.

Napoleon Hill

"Berbahagialah atas apa yang telah kau berikan,

bukan dari apa yang telah kau terima."

Sebagai wujud tanggung jawabku atas kepercayaan yang telah diberikan:

Keluarga besar A. Gunandi, Semarang;

Yang tersayang, Priskila Nike Artina;

Malaikatku, Angela.

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 daftar pustaka sebagaimana layaknya karya ilmiah.

Yogyakarta, 7 September 2002

Penulis,

Cornellius Heri S.

DAFTAR ISI

Halaman

KATA PENGANTAR

Puji dan syukur kehadirat Tuhan Yang Maha Esa atas rahmat dan karuniaNya sehingga penulis dapat menyelesaikan skripsi yang berjudul "Monoid dan Penerapannya pada Otomata". Laporan penelitian ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Pendidikan Program Studi Pendidikan Matematika.

Dalam menyusun dan menyelesaikan laporan penelitian ini, banyak pihak yang telah ikut berperan baik secara langsung maupun tidak langsung. Oleh karena itu, dengan segala kerendahan hati penulis mengucapkan terima kasih kepada :

1. Bapak dan Ibuku, atas kesempatan belajar dan dorongan yang diberikan baik secara material maupun spiritual.
2. Ibu Any Herawati, S.Si., M.Si., atas segala kesabaran dan masukan berharga yang diberikan selama penyusunan skripsi ini.
3. Segenap dosen JPMIPA, khususnya program studi Pendidikan Matematika Universitas Sanata Dharma atas pengetahuan yang penulis dapatkan.
4. Bapak Sunarjo dan Bapak Sugeng (Sekretariat JP MIPA) atas keramahannya dalam melayani kepentingan mahasiswa.
5. Priskila Nike Artina, atas dukungan dan kasihnya.
6. Sylvia dan Mini, terima kasih atas dorongannya.
7. Rekan-rekan mahasiswa Pendidikan Matematika angkatan '98 atas kebersamaannya selama kuliah.

8. Teman-teman sepakbola JP. MIPA.
9. Dan pihak-pihak lain yang belum disebutkan.

Penulis juga menyadari bahwa laporan penelitian ini masih belum sempurna. Seperti peribahasa kita, tiada gading yang tak retak, oleh karenanya segala tegur sapa demi perbaikan laporan penelitian ini akan diterima dengan senang hati.

Akhir kata, semoga laporan penelitian ini bermanfaat bagi para pembaca sekalian.

Penulis

ABSTRAK

Monoid adalah himpunan M yang tidak kosong bersama operasi ~~biner~~ yang bersifat tertutup dan asosiatif di M, dan memuat elemen identitas. Setiap grup adalah monoid, selain itu ada berbagai jenis monoid yang lain, yakni submonoid, monoid komutatif, monoid transformasi-transformasi, monoid siklis, monoid bebas, dan monoid faktor.

Otomata status berhingga (S,I,m) terdiri atas himpunan status $S = \{s_1, s_2, \ldots, s_t\}$, himpunan input $I = \{i_1, i_2, \ldots, i_r\}$, dan fungsi transisi m: $I \times S \to S$ yang menyatakan bagaimana input mengubah status. Setiap input menetapkan fungsi dari himpunan status ke dirinya sendiri. Bayangan dari himpunan status membentuk himpunan bagian dari himpunan status, yang dihasilkan dari input yang diberikan. Sehingga diperoleh fungsi m': $I \to S^S$ di mana $S^S = \{f: S \to S\}$, dan $m'(i)$: $S \to S$ didefinisikan oleh $(m'(i))(s) = m(i,s)$, dengan $i \in I$ dan $s \in S$. Untuk setiap $i \in I$, fungsi $m'(i)$ menyatakan efek yang diakibatkan oleh input i terhadap himpunan status dari otomata. Jika input yang diberikan berupa rangkaian input maka efek dari rangkaian input dinyatakan oleh homomorfisma monoid h: $FM(I) \to S^S$, yakni $h(i_1 i_2 \ldots i_r) = m'(i_1) \circ m'(i_2) \circ \ldots \circ m'(i_r)$, $i_1 i_2 \ldots i_r \in FM(I)$. Dengan membentuk suatu relasi kongruensi: $\alpha R \beta$ jika $h(\alpha) = h(\beta)$, $\forall \alpha, \beta \in FM(I)$, maka diperoleh monoid faktor $FM(I)/R$, yang disebut monoid dari otomata. Monoid ini menyatakan kemampuan otomata dalam menanggapi rangkaian input yang diberikan, berkaitan dengan banyaknya efek yang dimilikinya.

ABSTRACT

A monoid $(M,\#)$ is a nonempty set M together with an operation "#" that closed and associatived in M, and there exists an identity element. Every grup is a monoid, beside that there are many kinds of monoid, i.e. a submonoid, a commutative monoid, a monoid of transformations, a cyclic monoid, a free monoid, and a quotient monoid.

A finite-state automata (S,I,m) consists of a set of states $S = \{s_1, s_2, \ldots, s_t\}$, a set of inputs $I = \{i_1, i_2, \ldots, i_r\}$, and a transition function m: $I \times S \to S$ which describes how each input changes the states. Each input defines a function from the set of states to itself. The image from the set of state construct a subset of the set of states which is produced by the given input. Hence we have a function m': $I \to S^S$ where $S^S = \{f: S \to S\}$, and $m'(i)$: $S \to S$ is defined by $(m'(i))(s) = m(i,s)$, with $i \in I$ and $s \in S$. For every $i \in I$, a function $m'(i)$ implies the effect that result by the input i to the set of states in automata. If the given input is an input sequence then the effect of an input sequence is defined by a monoid homomorphism h: $FM(I) \to S^S$, that is $h(i_1 i_2 \ldots i_r) = m'(i_1) \circ m'(i_2) \circ \ldots \circ m'(i_r)$, $i_1 i_2 \ldots i_r \in FM(I)$. By defines a congruence relation: $\alpha R \beta$ if $h(\alpha) = h(\beta)$, $\forall \alpha, \beta \in FM(I)$, we get the quotient monoid $FM(I)/R$, which is called the monoid of the automata. This monoid reflects the capability of the automata to respond to the given input sequence, which related to the number of its effects.

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Dalam perkuliahan, kita sudah mengenal suatu struktur aljabar dengan satu operasi, yang dinamakan grup. Grup itu sendiri merupakan suatu himpunan yang tidak kosong bersama sebuah operasi pada himpunan tersebut yang memenuhi beberapa aksioma tertentu. Selain itu ada struktur aljabar dengan satu operasi, di mana aksioma-aksioma yang disyaratkan lebih sedikit daripada aksioma-aksioma yang disyaratkan pada grup, yakni tidak disyaratkan keberadaan elemen invers seperti halnya yang disyaratkan pada grup. Dan struktur aljabar tersebut dinamakan monoid. Dengan demikian monoid merupakan suatu struktur aljabar yang lebih umum daripada grup.

Kita mengenal *automata*/otomata atau mesin dalam kehidupan sehari-hari dalam berbagai bentuk, seperti lift, mesin hitung, komputer, dan lain-lain. Ternyata, monoid memiliki penerapan dalam bidang otomata tersebut.

Hal-hal tersebut di atas mendasari keinginan penulis untuk meneliti mengenai monoid dan penerapannya pada otomata.

B. Perumusan Masalah

Sesuai dengan apa yang telah dikemukakan dalam latar belakang permasalahan, maka masalah-masalah yang akan diteliti adalah:

1. Apa yang dimaksud dengan monoid, dan gagasan apa saja yang ada di dalamnya?

2. Hubungan apa saja yang ada antara monoid dengan grup?
3. Penerapan yang bagaimana yang disumbangkan monoid pada otomata?

C. Tujuan Penelitian

Tujuan dari penelitian ini adalah:

1. Memperkenalkan suatu struktur aljabar yang lebih umum daripada grup, yakni monoid dan gagasan-gagasan yang ada di dalamnya, serta menunjukkan hubungan yang ada di antara keduanya.
2. Memperlihatkan penerapan monoid pada otomata.

D. Metode Penelitian

Penelitian yang dilakukan menggunakan metode studi pustaka, dengan mempelajari buku-buku yang memuat materi-materi yang dibahas dalam laporan penelitian ini, seperti yang telah disebutkan dalam daftar pustaka.

E. Ruang Lingkup Pembahasan

Laporan penelitian ini membahas mengenai relasi, fungsi, semigrup, grup, monoid, otomata, dan penerapan monoid pada otomata tersebut. Sedangkan otomata yang akan diteliti dibatasi untuk jenis otomata dengan status berhingga. Untuk dapat memahami topik-topik yang dibahas dalam laporan penelitian ini, diharapkan pembaca telah menguasai beberapa topik pendukung yang tidak dibahas di sini. Topik pendukung tersebut antara lain himpunan dan operasi.

F. Sistematika Pembahasan

Bab II membahas mengenai relasi, fungsi, dan semigrup serta gagasan-gagasan lain yang ada di dalamnya. Pada bab III dibahas mengenai monoid, beberapa macam monoid, dan gagasan-gagasan yang ada pada monoid. Kemudian dibahas juga grup, beberapa macam grup, dan gagasan-gagasan yang ada pada grup. Selain itu, juga dibahas mengenai hubungan yang ada antara monoid dan grup.

Bab IV membahas mengenai otomata status berhingga dan penerapan monoid pada otomata status berhingga tersebut, kemudian pada bab terakhir, yakni bab V, disajikan kesimpulan mengenai keseluruhan hasil pembahasan.

BAB II

LANDASAN TEORI

Pada bagian ini akan dibahas beberapa konsep pendukung yaitu relasi, fungsi, semigrup dan subsemigrup, serta gagasan-gagasan yang ada di dalamnya yang akan digunakan untuk membahas materi pada bab-bab selanjutnya.

A. Relasi dan Fungsi

1. Relasi

Definisi 2.1 Suatu *relasi* R dari himpunan A ke himpunan B adalah himpunan bagian dari A x B. Suatu elemen a disebut *berelasi* dengan elemen b, bila pasangan (a,b) merupakan anggota dari R, dan ditulis sebagai $(a,b)\in R$ atau aRb.

Definisi 2.2 Bila $A = B$ maka relasi R dari himpunan A ke himpunan B disebut *relasi pada* A. Dengan kata lain relasi pada A adalah relasi dari A ke dirinya sendiri.

Definisi 2.3 Suatu relasi R pada himpunan A disebut *relasi ekuivalensi*, bila memenuhi sifat-sifat berikut:

(i) Sifat *refleksif*, yakni aRa, $\forall a\in A$.

(ii) Sifat *simetris*, yakni bila aRb maka bRa, $\forall a,b\in A$.

(iii) Sifat *transitif*, yakni bila aRb dan bRc, maka aRc, $\forall a,b,c\in A$.

Bila R suatu relasi ekuivalensi pada A dan $a \in A$, maka $[a] = \{x \in A: xRa\}$ disebut *kelas ekuivalensi* dari a.

Contoh 2.1 Andaikan n adalah bilangan bulat positif, dan $a,b \in \mathbf{Z}$. Maka aRb menyatakan *a kongruen dengan b modulo n*, bila n membagi habis $a - b$, yang dinyatakan oleh $a \equiv b \bmod n$. Tunjukkan bahwa relasi kongruen modulo n adalah suatu relasi ekuivalensi pada Z!

Penyelesaian.

Andaikan "$n \mid m$" berarti "n membagi habis m", yang artinya ada suatu bilangan bulat k sedemikian hingga $m = nk$. Jadi $a \equiv b \bmod n$ bila dan hanya bila $n \mid (a - b)$.

(i) Ambil sebarang $a \in \mathrm{Z}$, maka $(a - a) = n.0$. Sehingga $n \mid (a - a)$, yang berarti $a \equiv a \bmod n$. Jadi relasi tersebut refleksif.

(ii) Ambil sebarang $a,b \in \mathrm{Z}$. Andaikan $a \equiv b \bmod n$, maka $(a - b) = nk$, dengan $k \in \mathrm{Z}$. Karena $-k \in \mathrm{Z}$, maka $-(a - b) = n(-k)$ yang artinya $n \mid (b - a)$ atau $b \equiv a \bmod n$. Jadi relasi tersebut simetris.

(iii) Ambil sebarang $a,b,c \in \mathrm{Z}$. Andaikan $a \equiv b \bmod n$ dan $b \equiv c \bmod n$, maka $(a - b) = nk$ dan $(b - c) = nl$, dengan $k,l \in \mathrm{Z}$. Sehingga $(a - b) + (b - c) = nk + nl \Leftrightarrow (a - c) = n(k + l)$, dengan $(k + l) \in \mathrm{Z}$. Dengan demikian $a \equiv c \bmod n$. Jadi relasi tersebut transitif.

Jadi kongruen modulo n adalah suatu relasi ekuivalensi pada $\mathbf{Z}$.

Contoh 2.2 Di dalam relasi kongruen modulo 3, kita mempunyai kelas-kelas ekuivalensi berikut:

$[0] = \{ \ldots, -3, 0, 3, 6, 9, \ldots \}$ $\qquad$ $[2] = \{ \ldots, -1, 2, 5, 8, 11, \ldots \}$

$[1] = \{ \ldots, -2, 1, 4, 7, 10, \ldots \}$ $\qquad$ $[3] = \{ \ldots, 0, 3, 6, 9, 12, \ldots \} = [0]$.

Suatu kelas ekuivalensi pada bilangan bulat modulo 3 haruslah satu di antara [0], [1], atau [2].

Teorema 2.1 Bila R relasi ekuivalensi pada himpunan A dan $a \in A$, maka $a \in [a]$.

Bukti:

Andaikan R relasi ekuivalensi pada A, maka R refleksif, simetris dan transitif. Karena R refleksif maka aRa, sehingga $a \in [a]$. ∎

Teorema di atas mengimplikasikan bahwa untuk setiap $a \in A$, kelas ekuivalensi $[a]$ tidak pernah kosong.

Teorema 2.2 Bila R relasi ekuivalensi pada himpunan A dan $b \in [a]$, maka $[b] = [a]$.

Bukti:

Andaikan R relasi ekuivalensi pada himpunan A dan $b \in [a]$, maka bRa. Karena R relasi ekuivalensi maka R simetris, sehingga aRb. Akan dibuktikan bahwa $[b] \subseteq [a]$ dan $[a] \subseteq [b]$.

(i) Ambil sebarang $x \in [b]$, maka xRb. Karena R transitif dan bRa, maka xRa. Ini berarti $x \in [a]$. Jadi $[b] \subseteq [a]$.

(ii) Ambil sebarang $y \in [a]$, maka yRa. Karena R transitif dan aRb, maka yRb. Ini berarti $y \in [b]$. Jadi $[a] \subseteq [b]$.

Kesimpulan dari (i) dan (ii) adalah $[b] = [a]$. ∎

2. Fungsi atau Pemetaan

Fungsi atau pemetaan merupakan suatu relasi yang khusus, artinya bahwa fungsi adalah suatu relasi, akan tetapi suatu relasi belum tentu merupakan suatu fungsi.

Definisi 2.4 Andaikan A dan B dua himpunan yang tidak kosong. Relasi f dari himpunan A ke himpunan B, dinotasikan dengan $f: A \to B$, disebut *fungsi* bila dipenuhi:

(i) Setiap elemen himpunan A memiliki kawan di B.

$(\forall x \in A)(\exists y \in B)\ (x,y) \in f$.

(ii) Kawannya setiap anggota A di B itu tunggal.

$(\forall x \in A)\ (x,y_1) \in f \wedge (x,y_2) \in f \Rightarrow y_1 = y_2$.

Untuk selanjutnya $(x,y) \in f$ dapat ditulis dengan $y = f(x)$. Himpunan A disebut *daerah asal* atau *domain*, dan himpunan B disebut *daerah kawan* atau *kodomain*. Elemen $f(x)$ disebut *bayangan* x oleh pemetaan f. Dengan demikian, kedua syarat fungsi di atas dapat ditulis:

(i) $(\forall x \in A)(\exists y \in B)\ y = f(x)$.

(ii) $(\forall x_1, x_2 \in A)\ x_1 = x_2 \Rightarrow f(x_1) = f(x_2)$.

Definisi 2.5 Andaikan f suatu fungsi dari himpunan A ke himpunan B. Yang dimaksud dengan *daerah hasil* (*range*) dari fungsi f adalah himpunan semua elemen y di B yang merupakan bayangan elemen-elemen di A oleh pemetaan f, dan dinotasikan oleh $f(A) = \{f(x): x \in A\}$.

Definisi 2.6 Andaikan $f: A \to B$ suatu fungsi dari himpunan A ke himpunan B, maka:

(i) Fungsi f disebut *fungsi surjektif* bila setiap elemen di B memiliki kawan di A atau ($f: A \to B$ surjektif $:\Leftrightarrow (\forall y \in B)(\exists x \in A)\ y = f(x)$).

(ii) Fungsi f disebut *fungsi injektif* bila setiap elemen di B yang memiliki kawan di A, kawannya itu tunggal atau ($f: A \to B$ injektif: $\Leftrightarrow (\forall x_1, x_2 \in A)$ $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$).

(iii) Fungsi f disebut *fungsi bijektif* bila f sekaligus merupakan fungsi surjektif dan injektif.

Definisi 2.7 Dua fungsi f dan g dari himpunan A ke himpunan B dikatakan *sama* bila dan hanya bila $f(x) = g(x)$, $\forall x \in A$.

Definisi 2.8 Fungsi $f: A \to A$ disebut *fungsi identitas*, bila untuk setiap $x \in A$ berlaku $f(x) = x$. Fungsi ini dinotasikan dengan $i^A: A \to A$.

Definisi 2.9 Jika f: $A \rightarrow B$ dan g: $B \rightarrow C$, maka untuk setiap $x \in A$ didefinisikan f o g: $A \rightarrow C$ yang disebut *komposisi fungsi f* dan *g*, dan $(f \circ g)(x) = f(g(x))$ dan $f(g(x)) \in C$. Definisi ini mengimplikasikan bahwa syarat yang harus dipenuhi agar fungsi-fungsi f dan g dapat dikomposisikan adalah daerah hasil fungsi f harus sama dengan domain fungsi g atau daerah hasil fungsi g harus sama dengan domain fungsi f.

Contoh 2.3 Andaikan f dan g fungsi-fungsi dari R ke R, masing-masing didefinisikan oleh $f(x) = 2x$ dan $g(x) = x^2$, $\forall x \in \mathrm{R}$. Maka $(f \circ g)(5) = f(g(5)) = f(25) = 50$, dan $(g \circ f)(5) = g(f(5)) = g(10) = 100$. Secara umum $(f \circ g)(x) = f(g(x)) = f(x^2) = 2x^2$, dan $(g \circ f)(x) = g(f(x)) = g(2x) = (2x)^2 = 4x^2, \forall x \in \mathrm{R}$.

Teorema 2.3 Bila f: $A \rightarrow B$, g: $B \rightarrow C$, dan h: $C \rightarrow D$ maka berlaku:

$((h \circ g) \circ f)(x) = (h \circ (g \circ f))(x)$, $\forall x \in A$.

Bukti:

(i) $h \circ g$: $B \rightarrow D$ sehingga $(h \circ g) \circ f$: $A \rightarrow D$.

Dan $g \circ f$: $A \rightarrow C$ sehingga $h \circ (g \circ f)$: $A \rightarrow D$.

Jadi $(h \circ g) \circ f$ dan $h \circ (g \circ f)$ memiliki domain yang sama, yakni A dan kodomain yang sama, yakni D.

(ii) Ambil sebarang $x \in A$, maka: $((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x)))$ dan $(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x)))$.

Jadi terbukti bahwa $((h \circ g) \circ f)(x) = (h \circ (g \circ f))(x)$, $\forall x \in A$. ∎

Teorema 2.4 Bila $f: A \to A$ maka $i^A \circ f = f \circ i^A = f$.

Bukti:

(i) Jelaslah bahwa fungsi-fungsi $i^A \circ f$, $f \circ i^A$, dan f memiliki daerah asal yang sama, yakni A dan daerah kawan yang sama, yakni A.

(ii) Ambil sebarang $x \in A$, maka $(i^A \circ f)(x) = i^A(f(x)) = f(x)$, kemudian: $(f \circ i^A)(x) = f(i^A(x)) = f(x)$.

Jadi terbukti bahwa bila $f: A \to A$ maka $i^A \circ f = f \circ i^A = f$. ∎

Definisi 2.10 Andaikan $f: A \to B$ suatu fungsi. Yang dimaksud dengan *invers* suatu fungsi f adalah relasi $f^{-1}: B \to A$ sedemikian hingga $(y,x) \in f^{-1}$ bila dan hanya bila $(x,y) \in f$. Jadi $f^{-1} = \{(y,x): (x,y) \in f\}$.

Andaikan fungsi $f: \mathrm{R} \to \mathrm{R}$ yang didefinisikan oleh $f(x) = x^2$, $\forall x \in \mathrm{R}$. Perhatikan bahwa $f(1) = f(-1) = 1$, sehingga $f^{-1}(1) = 1$ dan $f^{-1}(1) = -1$. Ini menunjukkan bahwa $f^{-1}(1) \neq f^{-1}(1)$. Dengan demikian invers dari suatu fungsi belum tentu merupakan fungsi. Dari sini timbul pertanyaan, fungsi yang bagaimanakah yang inversnya juga merupakan fungsi?

Teorema 2.5 Bila $f: A \to B$ maka f^{-1} fungsi dari B ke A bila dan hanya bila fungsi f bijektif.

Bukti:

($\Leftarrow$) Andaikan f fungsi bijektif dari A ke B. Maka f surjektif, yakni $(\forall y \in B)(\exists x \in A)\ y = f(x)$. Berarti $(\forall y \in B)(\exists x \in A)\ (x,y) \in f$. Dan ini berarti pula

$(\forall y \in B)(\exists x \in A)\ (y,x) \in f^{-1}$. Karena f juga injektif maka $(\forall x_1, x_2 \in A)\ f(x_1) = f(x_2) \Rightarrow x_1 = x_2$. Berarti $(\forall x_1, x_2 \in A)\ (x_1, y_1) \in f \wedge (x_2, y_2) \in f \wedge y_1 = y_2 \Rightarrow x_1 = x_2$. Ini sama artinya dengan $(\forall y_1, y_2 \in B)\ (y_1, x_1) \in f^{-1} \wedge (y_2, x_2) \in f^{-1} \Rightarrow x_1 = x_2$. Jadi f^{-1}: $B \rightarrow A$ merupakan fungsi.

($\Rightarrow$) Andaikan f fungsi dari A ke B dan f^{-1} fungsi. Maka $(\forall y \in B)(\exists x \in A)$ $(y,x) \in f^{-1}$. Berarti $(\forall y \in B)(\exists x \in A)\ (x,y) \in f$ atau $y = f(x)$. Jadi f furjektif. Kemudian $(\forall y_1, y_2 \in B)\ (y_1, x_1) \in f^{-1} \wedge (y_2, x_2) \in f^{-1} \wedge y_1 = y_2 \Rightarrow x_1 = x_2$. Karena f surjektif maka berarti pula $(\forall x_1, x_2 \in A)\ (x_1, y_1) \in f \wedge (x_2, y_2) \in f \wedge y_1 = y_2 \Rightarrow x_1 = x_2$ atau $(\forall x_1, x_2 \in A)\ f(x_1) = f(x_2) \Rightarrow x_1 = x_2$. Jadi f injektif. Dengan demikian f bijektif. ∎

Dari teorema di atas diperoleh kesimpulan bahwa setiap fungsi yang bijektif, inversnya juga merupakan fungsi.

B. Semigrup dan Subsemigrup

Definisi 2.11 *Semigrup* $(S,\#)$ adalah suatu himpunan S yang tidak kosong bersama dengan operasi "#", yang memenuhi:

(i) Operasi "#" di S bersifat tertutup.

$(\forall a,b \in S)\ a \# b \in S$.

(ii) Operasi "#" di S bersifat asosiatif.

$(\forall a,b,c \in S)\ a \# (b \# c) = (a \# b) \# c$.

Untuk selanjutnya semigrup $(S,\#)$ dapat ditulis sebagai semigrup S saja, dengan S sebagai himpunan dasarnya. Meskipun demikian tetap harus diingat bahwa semigrup merupakan suatu pasangan antara suatu himpunan dengan operasi yang didefinisikan pada himpunan itu. Selain itu agar efisien, penulisan hasil operasi antar elemen di semigrup, misalnya "$a \# b$" yang menyatakan hasil operasi "#" antara elemen a dan b, cukup ditulis dengan "ab" saja.

Definisi 2.12 Semigrup $(S,\#)$ disebut *semigrup komutatif* bila dan hanya bila operasi "#" di S bersifat komutatif, yakni $a \# b = b \# a$, $\forall a,b \in S$.

Definisi 2.13 *Orde suatu semigrup* S ialah banyaknya elemen dari himpunan S, dan dinotasikan dengan $|S|$. Suatu semigrup S disebut *semigrup berhingga* bila ordenya berhingga, dan disebut *semigrup tak hingga* bila ordenya tak berhingga.

Contoh 2.4

1. $(\mathbf{Z},+)$ adalah suatu semigrup, karena **Z** jelas merupakan himpunan yang tidak kosong, operasi penjumlahan pada himpunan bilangan bulat bersifat tertutup dan asosiatif. Selain itu operasi penjumlahan pada himpunan bilangan bulat juga bersifat komutatif, maka $(\mathbf{Z},+)$ disebut juga semigrup komutatif.
2. $(\mathbf{Z},-)$ bukanlah semigrup karena operasi pengurangan pada himpunan bilangan bulat tidak bersifat asosiatif. Misalnya $(2 - 5) - 4 = -3 - 4 = -7$, tetapi $2 - (5 - 4) = 2 - 1 = 3$.

3. Andaikan $M_{nxn}(\mathrm{R})$ adalah himpunan semua matriks berordo n x n dengan elemen bilangan real. Karena $M_{nxn}(\mathrm{R})$ jelas tidak kosong, kemudian operasi perkalian pada matriks tersebut bersifat tertutup dan asosiatif, maka $(M_{nxn}(\mathrm{R}),.)$ adalah semigrup. Tetapi semigrup ini bukanlah semigrup komutatif, karena operasi perkalian pada matriks tidak bersifat komutatif.

Definisi 2.14 Jika $(S, .)$ adalah semigrup dan $x \in S$, maka *pangkat dari elemen* dalam S didefinisikan sebagai:

(i) $x^1 = x$.

(ii) $x^{n+1} = x^n x$, di mana $n = 1, 2, 3, 4, \ldots$.

Teorema 2.6 Andaikan $(S,.)$ semigrup, maka $\forall m,n \in \mathrm{N}$ dan $\forall x \in S$ berlaku:

(i) $x^m x^n = x^{m+n}$.

(ii) $(x^m)^n = x^{mn}$.

Bukti:

Teorema ini akan dibuktikan dengan menggunakan induksi matematika.

(i) Ambil sebarang $m \in \mathrm{N}$.

- Akan dibuktikan $x^m x^n = x^{m+n}$ benar untuk $n = 1$.

$$\begin{aligned} x^m x^n &= x^m x^1 \\ &= x^{m+1} \\ &= x^{m+n}. \end{aligned}$$

Jadi pernyataan $x^m x^n = x^{m+n}$ benar untuk $n = 1$.

- Andaikan pernyataan $x^m\ x^n = x^{m+n}$ benar untuk $n = k$, maka $x^m\ x^k = x^{m+k}$.

  Akan dibuktikan bahwa $x^m\ x^n = x^{m+n}$ juga benar untuk $n = k + 1$.

  $$\begin{aligned} x^m\ x^n &= x^m\ x^{k+1} \\ &= x^m\ (x^k\ x^1) \\ &= (x^m\ x^k)x^1 \\ &= (x^{m+k})x^1 \\ &= x^{(m+k)+1} \\ &= x^{m+(k+1)} \\ &= x^{m+n}. \end{aligned}$$

  Jadi pernyataan $x^m\ x^n = x^{m+n}$ benar untuk $n = k + 1$.

Dengan demikian terbukti bahwa $x^m\ x^n = x^{m+n}$ benar untuk setiap $n \in \mathrm{N}$. Secara analog dapat dibuktikan pula bahwa $x^m\ x^n = x^{m+n}$ benar untuk setiap m$\in$N.

(ii) Ambil sebarang $m \in \mathrm{N}$.

- Akan dibuktikan $(x^m)^n = x^{mn}$ benar untuk $n = 1$.

  $$\begin{aligned} (x^m)^n &= (x^m)^1 \\ &= x^m \\ &= x^{m.1} \\ &= x^{mn}. \end{aligned}$$

  Jadi pernyataan $(x^m)^n = x^{mn}$ benar untuk $n = 1$.

- Andaikan pernyataan $(x^m)^n = x^{mn}$ benar untuk $n = k$, maka $(x^m)^k = x^{mk}$. Akan dibuktikan bahwa $x^m\ x^n = x^{m+n}$ juga benar untuk $n = k + 1$.

  $$\begin{aligned} (x^m)^n &= (x^m)^{k+1} \\ &= (x^m)^k\ x^m \end{aligned}$$

$= x^{mk}\,x^{m}$

$= x^{mk+m}$

$= x^{m(k+1)}$

$= x^{mn}$.

Jadi pernyataan $(x^m)^n = x^{mn}$ benar untuk $n = k + 1$.

Dengan demikian terbukti bahwa $(x^m)^n = x^{mn}$ benar untuk setiap $n \in \mathbf{N}$. Secara analog dapat dibuktikan pula bahwa $(x^m)^n = x^{mn}$ benar untuk setiap $m \in \mathbf{N}$. ∎

Perhatikan bahwa definisi 2.14 berlaku untuk semigrup dengan operasi perkalian. Untuk semigrup S dengan operasi penjumlahan, definisi yang berpadanan dengan "x^n" adalah "nx" (n dikalikan dengan x), sedemikian rupa sehingga $1x = x$, dan $(n + 1)x = nx + x$, $\forall n \in \mathbf{N}$ dan $x \in S$. Oleh karena itu yang berlaku pada semigrup $(S,+)$ adalah $mx + nx = (m + n)x$ dan $n(mx) = (mn)x$, $\forall m,n \in \mathbf{N}$ dan $x \in S$.

Definisi 2.15 Dalam semigrup $(S,\#)$, suatu elemen e dalam S disebut elemen *identitas* bila dan hanya bila $(\forall x \in S)\ e \# x = x \# e = x$.

Definisi tersebut mengimplikasikan bahwa suatu semigrup mungkin memiliki elemen identitas, mungkin tidak. Misalnya pada semigrup (Z,.), elemen 1 adalah elemen identitas, karena $1 \,.\, x = x \,.\, 1 = x$, $\forall x \in S$. Akan tetapi semigrup (E,.) dengan E adalah himpunan bilangan bulat yang genap, tidak memiliki elemen identitas. Teorema berikut ini akan menjelaskan keunikan dari elemen identitas .

Teorema 2.7 Jika semigrup $(S,\#)$ memiliki elemen identitas, maka elemen identitas tersebut pasti tunggal.

Bukti:

Andaikan e dan f, keduanya merupakan elemen identitas di S. Maka akan diperoleh: $e = e \# f$ (karena f adalah elemen identitas)

$= f$ (karena e adalah elemen identitas). ∎

Definisi 2.16 Andaikan $(S,\#)$ semigrup dengan elemen identitas e, dan andaikan pula $x \in S$. Suatu elemen $y \in S$ disebut *invers* dari x (dan sebaliknya) bila dan hanya bila $x \# y = y \# x = e$.

Jika semigrup $(S,\#)$ memiliki elemen identitas e, berdasarkan definisi di atas, e adalah invers dari dirinya sendiri, karena $e \# e = e$. Akan tetapi harus diingat bahwa tidak semua elemen di S memiliki invers. Sebagai contoh, misalnya pada semigrup (Z,.), yang memiliki elemen identitas yakni 1. Elemen 1 dan –1 dari Z, masing-masing memiliki invers yakni dirinya sendiri, akan tetapi elemen lain di Z tidak memiliki invers.

Seperti halnya elemen identitas, elemen invers juga memiliki keunikan, yang akan dijelaskan pada teorema berikut ini.

Teorema 2.8 Andaikan $(S,\#)$ adalah semigrup dengan elemen identitas e, dan andaikan pula $x \in S$. Jika x memiliki invers, maka pastilah inversnya tersebut adalah tunggal.

Bukti:

Andaikan y dan z, masing-masing adalah invers dari x. Maka akan diperoleh:

$$
\begin{aligned}
y &= y \# e && \text{(karena e adalah elemen identitas)}\\
&= y \# (x \# z) && \text{(karena z adalah invers dari x)}\\
&= (y \# x) \# z && \text{(sifat asosiatif)}\\
&= e \# z && \text{(karena y adalah invers dari x)}\\
&= z. \ \blacksquare
\end{aligned}
$$

Dalam suatu semigrup dengan operasi perkalian, di mana elemen identitasnya adalah 1, notasi untuk elemen invers dari x (jika ada) adalah x^{-1}, yang memenuhi: $xx^{-1} = x^{-1}x = 1$.

Sedangkan dalam semigrup dengan operasi penjumlahan, di mana elemen identitasnya adalah 0, notasi untuk elemen invers dari x (jika ada) adalah $-x$, yang memenuhi: $x + (-x) = (-x) + x = 0$.

Definisi 2.17 Andaikan T himpunan bagian yang tidak kosong dari S, dan $(S,\#)$ adalah semigrup. Maka T adalah subsemigrup dari S bila dan hanya bila operasi "#" pada T bersifat tertutup.

Dari definisi tersebut diatas dapat diturunkan pernyataan, bahwa untuk setiap semigrup S, S adalah subsemigrup dari dirinya sendiri.

Contoh 2.5 Dalam semigrup (**Z**,.), **N** adalah subsemigrup dari **Z**, karena **N** adalah himpunan bagian yang tidak kosong dari **Z** dan operasi perkalian di **N** bersifat tertutup. Selain itu **Z** adalah subsemigrup dari **Z** itu sendiri.

Teorema berikut akan memberikan suatu alternatif lain untuk menentukan apakah suatu himpunan bagian yang tidak kosong, yang telah diketahui, dari himpunan dasar suatu semigrup adalah subsemigrup.

Teorema 2.9 Andaikan (S,#) adalah semigrup dan T adalah himpunan bagian dari S ($T \subseteq S$). Maka T adalah subsemigrup dari S bila dan hanya bila (T,#) adalah semigrup.

Bukti:

($\Rightarrow$) Diketahui T adalah subsemigrup dari S, maka operasi "#" di T bersifat tertutup. (S,#) semigrup maka operasi "#" di S bersifat asosiatif. Karena T adalah himpunan bagian dari S, maka setiap elemen di T adalah elemen di S. Sehingga operasi "#" di T juga bersifat asosiatif. Jadi (T,#) semigrup.

($\Leftarrow$) Diketahui (T,#) semigrup. Maka operasi "#" di T bersifat tertutup dan $T \neq \emptyset$. Karena T adalah himpunan bagian dari S, maka dari definisi subsemigrup disimpulkan bahwa (T,#) adalah subsemigrup dari (S,#). ∎

Contoh 2.6 Diketahui (M_{2x2}(R),.) adalah semigrup. Andaikan diketahui T = $\left\{\begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix} : x \in \mathrm{R}\right\}$, buktikan bahwa T adalah subsemigrup dari M_{2x2}(R) tersebut!

Penyelesaian.

T adalah himpunan bagian dari M_{2x2}(R), karena T adalah himpunan matriks berordo 2 x 2, dan $x,0 \in \mathrm{R}$. Kemudian $T \neq \varnothing$ jelas.

Ambil sebarang $A = \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix}$, $B = \begin{bmatrix} y & 0 \\ 0 & 0 \end{bmatrix}$ dalam T, maka $x,y \in \mathrm{R}$. Kemudian $A.B = \begin{bmatrix} xy & 0 \\ 0 & 0 \end{bmatrix}$ juga dalam T, karena $xy \in \mathrm{R}$. Oleh karena itu operasi perkalian bersifat tertutup di T. Dengan demikian terbukti bahwa T adalah subsemigrup dari M_{2x2}(R).

Perhatikan contoh 2.6. Semigrup M_{2x2}(R) memiliki elemen identitas yakni $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Meskipun $I \notin T$, subsemigrup T memiliki elemen identitas, yakni matriks $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$. Hal ini jelas karena:

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix}, \ \forall x \in \mathrm{R}.$$

Sehingga dalam suatu semigrup S yang memiliki elemen identitas, elemen identitas (jika ada) dari suatu subsemigrupnya tidak selalu sama dengan yang ada pada S.

BAB III

MONOID DAN HUBUNGANNYA DENGAN GRUP

Bab ini membahas mengenai monoid dan berbagai macam monoid, seperti monoid komutatif, monoid transformasi, monoid siklis, monoid bebas, dan monoid faktor, serta homomorfisma dalam monoid. Kemudian juga dibahas grup dan beberapa macam grup, seperti grup siklis, subgrup normal dan grup faktor, grup bebas, serta homomorfisma dalam grup. Selain juga dibahas mengenai hubungan yang ada antara monoid dan grup.

A. Monoid

1. Monoid dan Submonoid

Berikut ini akan dibahas suatu struktur aljabar yang lebih khusus daripada semigrup. Struktur aljabar ini lebih khusus karena dua dari tiga aksioma yang disyaratkan pasti dipenuhi oleh semigrup. Untuk lebih jelasnya kita mulai dengan definisi berikut.

Definisi 3.1 *Monoid* $(M,\#)$ adalah suatu himpunan M yang tidak kosong bersama dengan operasi "#", yang memenuhi aksioma-aksioma berikut ini:

(i) Operasi "#" di M bersifat tertutup.

$(\forall a,b \in M)\ a \# b \in M.$

(ii) Operasi "#" di M bersifat asosiatif.

$(\forall a,b,c \in M)\ a \# (b \# c) = (a \# b) \# c.$

(iii) M memuat elemen identitas e.

$$(\exists e \in M)(\forall a \in M)\ e \# a = a \# e = a.$$

Dengan demikian dapat juga dikatakan bahwa monoid adalah suatu semigrup yang memiliki elemen identitas, sehingga setiap monoid adalah semigrup. Oleh karena itu apa yang berlaku pada semigrup juga berlaku pada monoid.

Karena monoid memuat elemen identitas, maka berdasarkan teorema 2.7 disimpulkan bahwa elemen identitas di monoid tersebut juga tunggal.

Definisi 3.2 Andaikan $(M,\#)$ monoid dengan $x \in M$. Elemen x disebut *idempoten* dalam M bila $x \# x = x$.

Contoh 3.1

1. $(\mathbf{N}_0,+)$ adalah monoid karena operasi penjumlahan pada himpunan bilangan bulat bersifat tertutup dan asosiatif, dan elemen identitasnya adalah 0 sebab $0 + m = m + 0 = m$, $\forall m \in \mathbf{N}_0$. Hanya elemen 0 yang memiliki invers, karena $0 + 0 = 0$. Untuk selanjutnya $\mathbf{N}_0$ menyatakan himpunan bilangan cacah.
2. $(\mathbf{Z},+)$ adalah monoid karena berdasarkan contoh 2.4 telah dijelaskan bahwa $(\mathbf{Z},+)$ adalah semigrup, dan elemen identitasnya adalah 0 karena $0 + x = x + 0 = x$, $\forall x \in \mathbf{Z}$.

3. (Z,.) adalah monoid dengan elemen identitas 1. Elemen dalam Z yang memiliki invers adalah 1 dan -1, kemudian idempotennya adalah 0 dan 1.
4. (Q,.) juga monoid dengan 1 sebagai elemen identitasnya dan setiap elemen di Q memiliki invers kecuali 0. Idempotennya adalah 0 dan 1.

Definisi 3.3 Jika $(M,\#)$ monoid maka $G_M = \{x \in M\text{: } x \text{ memiliki invers}\}$ disebut *grup kernel* dari $(M,\#)$.

Definisi 3.4 Monoid $(M,\#)$ disebut *monoid komutatif*, jika operasi "#" dalam M bersifat komutatif, yaitu: $a \# b = b \# a$, $\forall a,b \in M$. Oleh karena itu, jika M monoid komutatif maka M juga semigrup komutatif.

Contoh 3.2 Buktikan bahwa (Z,♥) adalah suatu monoid komutatif, dimana $x \heartsuit y = 6 - 2x - 2y + xy$, $\forall x,y \in \mathrm{Z}$!

Penyelesaian.

(i) Z tertutup terhadap operasi "♥", karena operasi-operasi penjumlahan, pengurangan, dan perkalian bersifat tertutup di Z.

(ii) Ambil sebarang $x,y \in \mathrm{Z}$, maka $x \heartsuit y = 6 - 2x - 2y + xy = 6 - 2y - 2x + yx = y \heartsuit x$, sehingga ♥ adalah operasi biner yang komutatif pada Z.

(iii) Ambil sebarang $x,y,z \in \mathrm{Z}$ maka:

$$\begin{aligned} x \heartsuit (y \heartsuit z) &= x \heartsuit (6 - 2y - 2z + yz) \\ &= 6 - 2x + (-2 + x)(6 - 2y - 2z + yz) \end{aligned}$$

$$= -6 + 4(x + y + z) - 2(xy + xz + yz) + xyz.$$

$$\begin{aligned}(x\heartsuit y)\heartsuit z &= (6 - 2x - 2y + xy)\heartsuit z \\ &= 6 + (-2 + z)(6 - 2x - 2y + xy) - 2z \\ &= -6 + 4(x + y + z) - 2(xy + xz + yz) + xyz \\ &= x\heartsuit(y\heartsuit z).\end{aligned}$$

Jadi operasi "♥" juga asosiatif dalam **Z**.

(iv) Andaikan elemen identitas itu adalah e maka $e\heartsuit x = x$, $\forall x \in \mathbf{Z}$. Sehingga:

$$\begin{aligned}6 - 2e - 2x + ex = x \Leftrightarrow 6 - 2e - 3x + ex &= 0 \\ (x - 2)(e - 3) &= 0.\end{aligned}$$

Jadi $e\heartsuit x = x$, $\forall x \in \mathbf{Z}$ bila dan hanya bila $e = 3$.

Oleh karena itu terbukti bahwa $(\mathbf{Z},\heartsuit)$ adalah suatu monoid komutatif dengan 3 sebagai elemen identitasnya.

Definisi 3.5 Andaikan $(M,\#)$ monoid dengan elemen identitas e dan T adalah himpunan bagian yang tidak kosong dari M. Maka T disebut *submonoid* dari M, bila T tertutup terhadap operasi "#" dan $e \in T$.

Teorema 3.1 Andaikan $(M,\#)$ monoid dan $N \subseteq M$. Maka N adalah submonoid dari $(M,\#)$ bila dan hanya bila $(N,\#)$ adalah monoid.

Bukti:

($\Leftarrow$) Diketahui $(N,\#)$ monoid. Maka $N \neq \emptyset$, operasi "#" bersifat tertutup di N, dan N memuat elemen identitas. Jadi N adalah submonoid.

($\Rightarrow$) Diketahui N submonoid dari M. Maka N tertutup terhadap operasi "#" dan $e \in N$. Karena N himpunan bagian dari M dan M monoid, maka operasi "#" bersifat asosiatif di N. Jadi N monoid. ∎

Sehingga jika $(M,\#)$ adalah monoid, maka $(M,\#)$ adalah submonoid dari dirinya sendiri. Dan jika $N = \{e\}$ maka $(N,\#)$ juga submonoid dari $(M,\#)$.

Teorema 3.2 Andaikan X adalah suatu himpunan yang tak kosong dan $X^X = \{f: X \rightarrow X\}$ adalah himpunan semua fungsi dari X ke X sendiri. Maka (X^X, o) adalah suatu monoid.

Bukti:

Jelaslah bahwa suatu fungsi identitas $i^X: X \rightarrow X$ dalam X^X. Ini menunjukkan bahwa X^X tidak kosong.

Ambil sebarang $f,g \in X^X \Rightarrow (f \text{ o } g) \in X^X$, $\forall f,g \in X^X$. Komposisi dari fungsi-fungsi selalu asosiatif, karena $\forall f,g,h \in X^X$ berlaku $f \text{ o } (g \text{ o } h)(\text{x}) = f(g(h(x)))$ kemudian $(f \text{ o } g) \text{ o } h(x) = f(g(h(x)))$. Fungsi identitas $i^X: X \rightarrow X$ yang didefinisikan oleh $i^X(x) = x$ adalah identitas untuk komposisi fungsi. Jadi terbukti bahwa (X^X, o) adalah monoid. ∎

Definisi 3.6 Monoid (X^X, o) disebut *monoid dari transformasi-transformasi* dalam X.

Contoh 3.3 Andaikan $X = \{0,1\}$. Buatlah tabel komposisi fungsi untuk monoid transformasi (X^X, o)!

Penyelesaian.

X^X mempunyai empat elemen e, f, g, dan h yang didefinisikan sebagai berikut:

$e(0) = 0,\qquad f(0) = 0,\qquad g(0) = 1,\qquad h(0) = 1$

$e(1) = 1,\qquad f(1) = 0,\qquad g(1) = 0,\qquad h(1) = 1$

Dengan demikian elemen identitasnya adalah fungsi e.

Kemudian $e \circ e(0) = e(e(0)) = e(0) = 0$ dan $e \circ e(1) = e(e(1)) = e(1) = 1$, sehingga $e \circ e = e$. Kemudian $g \circ f(0) = g(f(0)) = g(0) = 1$ dan $g \circ f(1) = g(f(1)) = g(0) = 1$, sehingga $g \circ f = h$. Komposisi-komposisi fungsi lainnya dapat dihitung dengan cara serupa sehingga didapatkan tabel hasil operasi komposisi fungsi dari elemen-elemen monoid transformasi dalam {0,1}, seperti pada tabel 3.1 berikut.

o	e	f	g	h
e	e	f	g	h
f	f	f	f	f
g	g	h	e	f
h	h	h	h	h

Tabel 3.1 Hasil komposisi fungsi-fungsi dalam monoid transformasi dalam {0,1}.

Jelaslah bahwa grup kernel dari monoid (X^X,o) adalah fungsi-fungsi dalam X^X yang memiliki invers. Dengan demikian grup kernel dari monoid (X^X,o) adalah fungsi-fungsi yang bijektif dalam X^X.

Teorema 3.3 Bila himpunan X memuat n elemen, maka banyaknya elemen dari X^X adalah n^n.

Bukti:

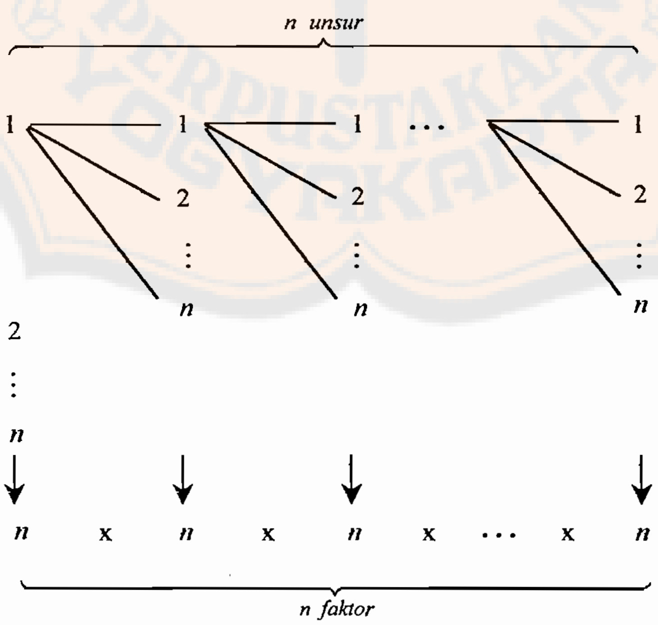
Banyaknya elemen dari X^X adalah banyaknya fungsi yang dapat dibentuk dari $\{1,2,3,\ldots,n\}$ ke dirinya sendiri.

Pandang beberapa fungsi yang dapat dibentuk, yang ditulis berdasarkan pemetaan tiap elemen di domain, misalnya:

$$
\begin{array}{cccc}
1 \to 1 & 1 \to 2 & 1 \to 1 & 1 \to 1 \\
2 \to 1 & 2 \to 1 & 2 \to 2 & 2 \to 1 \\
\vdots & \vdots & \vdots & \vdots \\
n \to 1 & n \to 1 & n \to 1 & n \to 2
\end{array}
$$

Jika kita lihat range dari fungsi-fungsi tersebut dan menyusunnya dalam suatu urutan, misalnya $\{1,1,\ldots,1\}$ yang berarti setiap elemen dari $\{1,2,\ldots,n\}$ dipetakan ke 1, $\{2,1,\ldots,1\}$ yang artinya 1 dipetakan ke 2 sedangkan elemen lainnya dipetakan ke 1, maka banyaknya elemen dari X^X adalah banyaknya susunan n unsur dalam suatu urutan, yang dapat dibentuk dari n unsur berbeda dan tiap unsur boleh ditulis berulang.

Dengan menggunakan diagram pohon kita dapatkan hasil berikut ini.



Jadi banyaknya elemen dari X^X adalah n^n. ∎

2. Monoid Siklis

Karena setiap monoid adalah semigrup, maka gagasan-gagasan yang ada pada semigrup juga berlaku untuk monoid. Sehingga suatu monoid disebut berhingga bila ordenya berhingga, bila ordenya tak berhingga disebut monoid tak hingga.

Seperti halnya pada semigrup, pada monoid juga didefinisikan perpangkatan elemen-elemen dalam monoid.

Definisi 3.7 Dalam suatu monoid $(M,.)$ dengan elemen identitas e, perpangkatan suatu elemen $x \in M$ didefinisikan sebagai:

(i) $x^0 = e$.

(ii) $x^{n+1} = x^n\, x$, dengan $n = 0, 1, 2, 3, \ldots$.

Teorema 3.4 Andaikan $(M,.)$ monoid, maka $\forall x \in M$ dan $\forall m,n \in \mathbf{N}_0$, berlaku:

(i) $x^m\, x^n = x^{m+n}$.

(ii) $(x^m)^n = x^{mn}$.

Bukti:

Karena monoid adalah semigrup, maka teorema 2.6 juga berlaku untuk monoid, dengan demikian cukup dibuktikan bahwa $x^m x^n = x^{m+n}$ dan $(x^m)^n = x^{mn}$ benar untuk setiap $m \in \mathbf{N}_0$, $n = 0$ dan untuk setiap $n \in \mathbf{N}_0$, $m = 0$.

(i) Ambil sebarang $m \in \mathbf{N}_0$.

Akan dibuktikan bahwa $x^m x^n = x^{m+n}$ benar untuk $n = 0$.

$$\begin{aligned} x^m\, x^n &= x^m\, x^0 \\ &= x^m\, e \\ &= x^m \\ &= x^{m+0} \\ &= x^{m+n}. \end{aligned}$$

Jadi $x^m x^n = x^{m+n}$ benar untuk $n = 0$ dan $\forall m \in \mathbf{N}_0$.

Secara analog dapat dibuktikan pula bahwa $x^m x^n = x^{m+n}$ benar untuk setiap $n \in \mathbf{N}_0$, dengan $m = 0$.

(ii) Ambil sebarang $m \in \mathbf{N}_0$.

Akan dibuktikan bahwa $(x^m)^n = x^{mn}$ benar untuk $n = 0$.

$$\begin{aligned} (x^m)^n &= (x^m)^0 \\ &= e \\ &= x^0 \\ &= x^{m.0} \\ &= x^{mn}. \end{aligned}$$

Jadi terbukti bahwa $(x^m)^n = x^{mn}$ benar untuk $n = 0$ dan $\forall m \in \mathbf{N}_0$.

Secara analog dapat dibuktikan bahwa $(x^m)^n = x^{mn}$ benar untuk setiap $n \in \mathbf{N}_0$, dengan $m = 0$. ∎

Definisi 3.8 Suatu monoid $(M,\#)$ disebut *dibangun oleh* A di mana $A \subseteq M$ dan $A \neq \varnothing$, bila setiap elemen dari M dapat dinyatakan sebagai kombinasi terhingga dari perpangkatan elemen-elemen dalam A, yaitu $\forall m \in M$ dapat ditulis sebagai:

$m = a_1^{n_1} \# a_2^{n_2} \# a_3^{n_3} \# \ldots \# a_n^{n_n}$, dengan $a_1, a_2, \ldots, a_n \in A$ dan $n_1, n_2, \ldots, n_n \in \mathbf{N}_0$.

Contoh 3.4

1. Monoid $(\mathbf{Z}^+, .)$ dibangun oleh {P}dengan P adalah himpunan semua bilangan prima, karena setiap bilangan bulat positif dapat dinyatakan sebagai perkalian terhingga dari perpangkatan bilangan prima.
2. Monoid $(\mathbf{N}_0, +)$ dibangun oleh {1} karena setiap bilangan cacah dapat ditulis sebagai jumlahan dari 1 sebanyak c, dengan $c \in \mathbf{N}_0$.

Definisi 3.9 Suatu monoid M yang disebut *monoid siklis*, bila ada A yang membangun M dan A hanya memuat satu elemen.

Dengan demikian monoid $(\mathbf{Z}^+, .)$ bukan monoid siklis karena ada lebih dari satu bilangan prima sebagai pembangunnya. Sedangkan monoid $(\mathbf{N}_0, +)$ adalah monoid siklis.

3. Monoid Bebas

Andaikan A suatu himpunan. Andaikan pula A^n, $n \in \mathbf{N}_0$ adalah himpunan dari n-tupel elemen-elemen dalam A. Dalam hal ini *n-tupel* adalah rangkaian berhingga n elemen-elemen dalam A tanpa simbol apapun di antara elemen-elemen tersebut.

Definisi 3.10 Elemen-elemen dari A^n disebut *pesan* dengan *panjang* n dalam A, di mana $n \in \mathbf{N}_0$.

Definisi 3.11 Pesan dengan panjang 0 adalah *pesan kosong*, dan dilambangkan dengan Δ.

Contoh 3.5 Bila $A = \{a, b\}$ maka $baabbaba \in A^8$, $A^0 = \{\Delta\}$ dan, $A^3 = \{aaa, aab, aba, abb, baa, bab, bba, bbb\}$.

Definisi 3.12 Andaikan A suatu himpunan dan andaikan pula $FM(A) = A^0 \cup A \cup A^2 \cup \ldots = \bigcup_{n=0}^{\infty} A^n$. Didefinisikan *operasi rangkaian* "$\star$" dalam $FM(A)$ yaitu: $\alpha \star \beta = \alpha\beta$, untuk setiap $\alpha, \beta \in FM(A)$. Sedangkan $\alpha\beta$ adalah suatu pesan yang diperoleh dengan meletakkan pesan β di sebelah kanan pesan α, tanpa simbol apapun di antara keduanya.

Dengan demikian $FM(A)$ adalah himpunan dari semua rangkaian berhingga dari elemen-elemen dalam A, atau $FM(A)$ beranggotakan semua pesan yang dapat dibentuk dari elemen-elemen dalam A. Perhatikan bahwa jika $A = \varnothing$, maka $FM(A) = \{\Delta\}$.

Andaikan $\alpha, \beta \in FM(A)$ di mana $\alpha = a_1 a_2 \ldots a_n$ dan $\beta = a_1' a_2' \ldots a_m'$ maka didefinisikan bahwa $\alpha = \beta$ bila dan hanya bila $n = m$ dan $a_i = a_i'$, untuk setiap $i \in \{1, 2, \ldots, n\}$. Khususnya, bila $\alpha = \Delta$ maka $\alpha = \beta$ bila dan hanya bila $\beta = \Delta$.

Definisi 3.13 Jika A suatu himpunan dan $a_i \in A$, maka untuk elemen $a_i \in FM(A)$, $i \in \mathbf{N}$, berlaku:

(i) $a_i^0 = \Delta$.

(ii) $a_i^m a_i^n = a_i^{m+n}$, $\forall m,n \in \mathbf{N}_0$.

Contoh 3.6 Jika α = *aaabbaac* dan β = *abbbccaba*, maka $\alpha \star \beta$ = *aaabbaacabbbccaba*.

Teorema 3.5 Jika $\alpha,\beta \in FM(A)$ di mana α adalah pesan dengan panjang m dan β adalah pesan dengan panjang n, maka $\alpha \star \beta$ adalah pesan dengan panjang $m + n$, $\forall m,n \in \mathbf{N}_0$.

Bukti:

Teorema ini akan dibuktikan dengan memperhatikan empat kemungkinan, yakni:

(i) Jika $m = 0$ dan $n = 0$, maka $\alpha = \beta = \Delta$ sehingga $\alpha \star \beta = \Delta \star \Delta = \Delta$. Ingat bahwa Δ merupakan pesan dengan panjang 0 dan $m + n = 0$.

Jadi terbukti bahwa $\alpha \star \beta$ merupakan pesan yang panjangnya $m + n$, untuk $m = n = 0$.

(ii) Jika $m = 0$ dan $n = k$, dengan $k \in \mathbf{N}$, maka $\alpha \star \beta = \Delta \star \beta = \beta$.

Jadi terbukti bahwa $\alpha \star \beta$ merupakan pesan dengan panjang $m + n = k$.

(iii) Jika $m = j$ dan $n = 0$, di mana $j \in \mathbf{N}$, maka $\alpha \star \beta = \alpha \star \Delta = \alpha$.

Jadi terbukti bahwa $\alpha \star \beta$ merupakan pesan dengan panjang $m + n = j$.

(iv) Jika $m = j$ dan $n = k$, di mana $j,k \in \mathrm{N}$. Andaikan $\alpha = a_1a_2 \ldots a_j$ dan $\beta = a_1a_2 \ldots a_k$, dengan $a_i \in \mathrm{N}$. Maka $\alpha \star \beta = a_1a_2 \ldots a_ja_1a_2 \ldots a_k$ merupakan pesan dengan panjang $j + k$.

Jadi terbukti jika α adalah pesan dengan panjang m dan β adalah pesan dengan panjang n, maka $\alpha \star \beta$ adalah pesan dengan panjang $m + n$, $\forall m,n \in \mathrm{N}_0$. ∎

Teorema 3.6 $(FM(A),\star)$ di mana $\star$ adalah operasi rangkaian, adalah suatu monoid.

Bukti:

(i) Akan dibuktikan bahwa operasi rangkaian "$\star$" terdefinisi dengan baik. Ambil sebarang $\alpha,\beta,\alpha',\beta' \in FM(A)$ dimana $\alpha = \alpha'$ dan $\beta = \beta'$. Maka $\alpha \star \beta = \alpha\beta = \alpha'\beta' = \alpha' \star \beta'$.

Jadi operasi "$\star$" terdefinisi dengan baik di $FM(A)$.

(ii) Ambil sebarang $\alpha,\beta \in FM(A)$ di mana α adalah pesan dengan panjang m dan β adalah pesan dengan panjang n, maka $\alpha \star \beta$ adalah pesan dengan panjang $m + n$, $\forall m,n \in \mathrm{N}_0$. Karena $(m + n) \in \mathrm{N}_0$ maka $\alpha \star \beta \in FM(A)$.

Jadi operasi "$\star$" bersifat tertutup di $FM(A)$.

(iii) Ambil sebarang $\alpha,\beta,\gamma \in FM(A)$ maka $\alpha \star (\beta \star \gamma) = \alpha \star \beta\gamma = \alpha\beta\gamma = \alpha\beta \star \gamma = (\alpha \star \beta) \star \gamma$.

Jadi operasi "$\star$" bersifat asosiatif di $FM(A)$.

(iv) Elemen identitas di $FM(A)$ adalah Δ, karena $\Delta \star \alpha = \alpha \star \Delta = \alpha$, $\forall \alpha \in FM(A)$.

Jadi terbukti bahwa $FM(A)$ adalah monoid. ∎

Definisi 3.14 Monoid $(FM(A),\star)$ yang diperoleh dari teorema 3.6 disebut *monoid bebas* yang dibangun oleh A, dengan A sebagai *basis* dari $FM(A)$.

Jika kita bentuk $FS(A) = FM(A) - \{\Delta\}$, maka akan kita peroleh semigrup $(FS(A),\star)$ yang disebut *semigrup bebas* yang dibangun oleh A.

Contoh 3.7 Andaikan $A = \{a\}$ maka $(FM(A),\star)$ adalah monoid dengan $FM(A) = \{\Delta, a, aa, aaa, \ldots\} = \{\Delta, a, a^2, a^3, \ldots\}$. Jelaslah bahwa monoid bebas ini adalah monoid siklis yang komutatif.

Jika elemen dari A lebih dari 1, maka $FM(A)$ tidak komutatif, karena untuk $a,b\in A$, di mana $a \neq b$, kita dapatkan $a\star b = ab \neq ba = b\star a$. Kemudian $FM(A)$ adalah monoid tak berhingga untuk setiap himpunan A yang tidak kosong.

4. Homomorfisma dalam Monoid

Definisi 3.15 Bila $(M,\#)$ dan (N,o) adalah monoid-monoid dengan elemen identitas masing-masing adalah e_M dan e_N, maka pemetaan ϕ: $M\rightarrow N$ disebut *homomorfisma monoid* dari $(M,\#)$ ke (N,o), bila memenuhi:

(i) $\phi(x \# y) = \phi(x) \text{ o } \phi(y)$, $\forall x,y\in M$.

(ii) $\phi(e_M) = e_N$.

Telah diketahui bahwa ada beberapa macam jenis fungsi, misalnya fungsi injektif, fungsi surjektif, dan fungsi bijektif. Oleh karena homomorfisma monoid berkaitan dengan fungsi, maka didefinisikan beberapa macam homomorfisma monoid berkaitan dengan jenis fungsinya.

Definisi 3.16 Andaikan $(M,\#)$ dan (N,o) adalah monoid-monoid dengan ϕ: $M \to N$ homomorfisma monoid.

(i) Jika ϕ merupakan fungsi surjektif, maka ϕ disebut *epimorfisma monoid.*

(ii) Jika ϕ merupakan fungsi injektif, maka ϕ disebut *monomorfisma monoid.*

(iii) Jika ϕ merupakan fungsi bijektif, maka ϕ disebut *isomorfisma monoid.* Bila ada isomorfisma monoid dari M ke N maka dikatakan M isomorfis dengan N, yang dinyatakan oleh $(M,\#) \approx (N,o)$.

Contoh 3.8 Andaikan φ: $(\mathbf{N}_0,+) \to (\mathbf{N},.)$ yang didefinisikan oleh $\varphi(n) = 2^n$, $\forall n \in \mathbf{N}_0$. Maka φ adalah homomorfisma monoid karena:

(i) $\varphi(n + m) = 2^{n+m} = 2^n \,.\, 2^m = \varphi(n).\varphi(m)$, $\forall n,m \in \mathbf{N}_0$.

(ii) $\varphi(0) = 2^0 = 1$, di mana 0 adalah elemen identitas di $\mathbf{N}_0$ dan 1 adalah elemen identitas di $\mathbf{N}$.

Sebaliknya, σ: $(\mathbf{N}_0,+) \to (\mathbf{N}_0,+)$ yang didefinisikan oleh $\sigma(x) = x^2$, $\forall x \in \mathbf{N}_0$, bukan homomorfisma monoid. Karena $\sigma(x + y) = (x + y)^2 \neq \sigma(x) + \sigma(y) = x^2 + y^2$, misalnya $\sigma(1 + 1) = 4$, sedangkan $\sigma(1) + \sigma(1) = 2$.

Teorema 3.7 Andaikan fungsi f: $(M,\#) \to (N,o)$ suatu homomorfisma monoid, maka *range* dari f yaitu $f(M) = \{f(x) : x \in M\}$ adalah submonoid dari N.

Bukti:

Jelaslah bahwa $f(M)\subseteq N$.

(i) Ambil sebarang $f(x_1),f(x_2)\in f(M)$, maka $x_1,x_2\in M$. Kemudian $f(x_1) \circ f(x_2) = f(x_1 \# x_2)$. Karena M monoid maka $x_1 \# x_2\in M$, sehingga $f(x_1 \# x_2)\in f(M)$. Jadi operasi "o" bersifat tertutup di $f(M)$.

(ii) Karena f homomorfisma monoid maka $f(e_M) = e_N$, sehingga $e_N\in f(M)$.

Tebukti bahwa $f(M)$ sumonoid dari N. ∎

Teorema 3.8 Suatu monoid bebas dengan basis $\{a\}$ isomorfis dengan monoid $(N_0,+)$.

Bukti:

Andaikan κ: $FM(\{a\})\rightarrow N_0$ suatu fungsi yang memetakan setiap pesan di $FM(\{a\})$ ke suatu bilangan yang menyatakan panjang pesan tersebut.

(i) Akan dibuktikan bahwa κ terdefinisi dengan baik. Ambil sebarang $a^m,a^n\in FM(\{a\})$ sedemikian hingga $a^m = a^n$. Sehingga $m,n\in N_0$ dan $m = n$. Oleh karena itu $\kappa(a^m) = \kappa(a^n)$.

Jadi κ terdefinisi dengan baik.

(ii) Akan dibuktikan bahwa κ adalah suatu homomorfisma monoid. Ambil sebarang $\alpha,\beta\in FM(\{a\})$ di mana α mempunyai panjang m dan β mempunyai panjang n, dengan $m,n\in N_0$. Maka berdasarkan teorema 3.5 $\kappa(\alpha\star\beta) = \kappa(\alpha\beta) = m + n = \kappa(\alpha) + \kappa(\beta)$. Jelaslah bahwa $\kappa(\Delta) = 0$, dan 0 adalah elemen identitas di N_0.

Jadi terbukti bahwa κ adalah suatu homomorfisma monoid.

(iii) Ambil sebarang $n \in \mathbf{N}_0$, maka pastilah ada $\alpha \in FM(\{a\})$ dengan panjang n, yaitu $\alpha = a^n$, sehingga $n = \kappa(\alpha)$.

Jadi κ adalah fungsi surjektif.

(iv) Ambil sebarang $\alpha, \beta \in FM(\{a\})$ di mana α mempunyai panjang m dan β mempunyai panjang n, dimana $m,n \in \mathbf{N}_0$, sedemikian hingga $\kappa(\alpha) = \kappa(\beta)$. Maka $m = n$. Karena $A = \{a\}$ maka A^n hanya memiliki elemen yang tunggal, padahal $\alpha, \beta \in A^n$. Maka haruslah $\alpha = \beta$.

Jadi κ adalah fungsi injektif.

Dengan demikian terbukti bahwa suatu monoid bebas $(FM(\{a\}), \star)$ isomorfis dengan monoid $(\mathrm{N}_0, +)$. ∎

Teorema 3.9 Andaikan $(FM(A), \star)$ suatu monoid bebas yang dibangun oleh A dan andaikan i: $A \to FM(A)$ adalah fungsi yang memetakan tiap elemen dari A ke pesan dengan panjang 1, sehingga $i(a) = a$, $\forall a \in A$. Bila g: $A \to M$ suatu fungsi dari A ke dalam himpunan dasar dari monoid $(M, \#)$, maka ada homomorfisma monoid yang tunggal h: $(FM(A), \star) \to (M, \#)$ sedemikian hingga $h \circ i = g$.

Bukti:

Bila h memenuhi $h \circ i = g$, maka h haruslah terdefinisi pada pesan dengan panjang 1 oleh $h(a) = g(a)$, $\forall a \in A$. Andaikan α suatu pesan dengan panjang $n \geq 2$ dalam $FM(A)$. Jika α diganti dengan $\beta \star \gamma$ dimana β pesan yang panjangnya n-1 dan γ pesan yang panjangnya 1, maka $h(\alpha) = h(\beta \star \gamma) = h(\beta)$ #

$h(\gamma) = h(\beta) \# g(\gamma)$. Dengan cara yang sama, kita lakukan pula pada pesan β dan seterusnya sampai pesan tersebut panjangnya adalah 1. Sehingga h dapat ditentukan dengan cara induksi pada panjang pesan, yakni bila $\alpha = a_1a_2\ldots a_n$, dengan $a_i \in A$ dan $1 \leq i \leq n$, maka $h(\alpha) = g(a_1) \# g(a_2) \# \ldots \# g(a_n)$, dan $h(\Delta)$ adalah identitas dari M.

Andaikan f homomorfisma monoid dari $FM(A)$ ke M, dan memenuhi $f \circ i = g$. Oleh karenanya f harus terdefinisikan pada pesan dengan panjang 1, yakni $f(a) = g(a) = h(a)$, $\forall a \in A$. Dan $f(\Delta) = h(\Delta)$, sehingga $f = h$. Jadi hanya ada satu homomorfisma dari $FM(A)$ ke M yang memenuhi $h \circ i = g$. ∎

5. Monoid Faktor

Definisi 3.17 Relasi ekuivalensi R pada himpunan M disebut *relasi kongruensi* pada monoid $(M,\bullet)$ jika aRb menyatakan $(a\bullet c)R(b\bullet c)$ dan $(c\bullet a)R(c\bullet b)$, $\forall c \in M$. *Kelas kongruensi* dari $a \in M$ adalah $[a] = \{x \in M: xRa\}$.

Definisi di atas mengimplikasikan bahwa setiap relasi ekuivalensi pada M belum tentu merupakan relasi kongruensi pada monoid $(M,\bullet)$. Artinya ada relasi ekuivalensi pada M yang bukan merupakan relasi kongruensi pada monoid $(M,\bullet)$. Untuk lebih jelasnya perhatikan dua contoh berikut ini.

Contoh 3.9 Jika relasi R didefinisikan sebagai aRb bila $10|a-b$, $\forall a,b \in N_0$, tunjukkan bahwa R adalah relasi kongruensi pada monoid $(N_0,+)$!

Penyelesaian.

Pada contoh 2.1 telah ditunjukkan bahwa relasi R ini adalah suatu relasi ekuivalensi. Dengan demikian cukup ditunjukkan bahwa aRb menyatakan $(a+c)R(b+c)$ dan $(c+a)R(c+b)$, $\forall c \in N_0$.

Ambil sebarang $a,b \in N_0$. Jika $a - b = 10p$, $p \in Z$, maka $(a + c) - (b + c) = 10p$ dan $(c + a) - (c + b) = 10p$, $\forall c \in N_0$. Jadi aRb menyatakan $(a+c)R(b+c)$ dan $(c+a)R(c+b)$, $\forall c \in N_0$. Jadi R relasi kongruensi pada monoid $(N_0,+)$.

Contoh 3.10 Andaikan R adalah suatu relasi pada N_0 yang didefinisikan sebagai: aRb bila dan hanya bila $a = 2^r b$, untuk suatu $r \in Z$. Apakah R merupakan relasi kongruensi pada monoid $(N_0,+)$?

Penyelesaian.

Akan ditunjukkan dahulu bahwa R adalah relasi ekuivalensi pada N_0.

(i) Ambil sebarang $a \in N_0$. Maka $a = 2^0.a$ dan $0 \in Z$, sehingga aRa. Jadi R refleksif.

(ii) Ambil sebarang $a,b \in N_0$. Andaikan aRb maka $a = 2^r b$, $r \in Z$. Sehingga $b = 2^{-r} a$ dan $-r \in Z$. Dengan demikian bRa. Jadi R simetris.

(iii) Ambil sebarang $a,b,c \in N_0$. Andaikan aRb dan bRc. Maka $a = 2^r b$, $r \in Z$ dan $b = 2^p c$, $p \in Z$. Sehingga $a = 2^r 2^p c = 2^{r+p} c$ dan $r+p \in Z$. Dengan demikian aRc. Jadi R transitif.

(iv) Karena $12 = 2^2.3$, maka $(12,3) \in R$. Tetapi $12 + 2 = 14$ dan $2^2(3+2) = 20$, sehingga $(12+2,3+2) \notin R$. Ini menunjukkan bahwa ada $a,b \in N_0$, di mana

$(a,b)\in R$ dan $(a+c,b+c)\notin R$, untuk suatu $c\in \mathbf{N}_0$. Jadi R bukan relasi kongruensi pada monoid $(\mathbf{N}_0,+)$.

Contoh ini menunjukkan suatu relasi ekuivalensi pada $\mathbf{N}_0$ yang bukan merupakan relasi kongruensi pada monoid $(\mathbf{N}_0,+)$.

Teorema 3.10 Jika R adalah relasi kongruensi pada monoid $(M,\bullet)$, himpunan faktor $M/R = \{[a]: a\in M\}$ adalah monoid dengan operasi yang didefinisikan sebagai $[a]\text{o}[b] = [a\bullet b]$, $\forall a,b\in M$.

Bukti:

(i) Akan dibuktikan bahwa operasi tersebut terdefinisi dengan baik pada kelas-kelas kongruensi. Ambil sebarang $[a],[b],[a'],[b']\in M/R$ sedemikian hingga $[a] = [a']$ dan $[b] = [b']$. Andaikan $x\in[a]$ maka xRa, sehingga aRx karena R simetris. Tetapi xRa' karena $[a] = [a']$, maka aRa' karena R transitif. Dengan cara yang sama diperoleh bRb'. Sehingga $(a\bullet b)R(a\bullet b')$ dan $(a\bullet b')R(a'\bullet b')$. Karena R transitif, $(a\bullet b)R(a'\bullet b')$ dan $[a\bullet b] = [a'\bullet b']$. Ini menunjukkan bahwa operasi pada M/R terdefinisi dengan baik.

(ii) Sifat asosiatif dalam M/R diturunkan dari sifat asosiatif dalam M. Ambil sebarang $[a],[b],[c]\in M/R$, maka:

$[a]\text{o}([b]\text{o}[c]) = [a]\text{o}([b\bullet c]) = [a\bullet b\bullet c] = ([a\bullet b])\text{o}[c] = ([a]\text{o}[b])\text{o}[c]$.

Jadi operasi pada M/R bersifat asosiatif.

(iii) Jika e elemen identitas di M, maka $[e]$ adalah elemen identitas di M/R, karena $[a]\text{o}[e] = [a\bullet e] = [a]$ dan $[e]\text{o}[a] = [e\bullet a] = [a]$, $\forall[a]\in M/R$.

Jadi terbukti bahwa M/R adalah monoid. ∎

Definisi 3.18 Monoid yang diperoleh dari teorema 3.10 disebut *monoid faktor* dari M oleh R, dinotasikan M/R.

Contoh 3.11 Jika kita perhatikan contoh 3.9 sebelumnya, monoid faktor (N_0/R,o) beranggotakan kelas-kelas kongruensi [1], [2], [3], ..., dan [10]. Karena [10] o [1] = [10 + 1] = [11] dan [11] = {1, 11, 21, ... } = [1], maka [10] o [1] = [1]. Hasil operasi untuk kelas-kelas kongruensi dalam monoid faktor (N_0/R,o) lainnya dapat dicari dengan cara serupa, yang hasilnya disajikan pada tabel 3.2 berikut ini.

o	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]
[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[1]
[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[1]	[2]
[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[1]	[2]	[3]
[4]	[5]	[6]	[7]	[8]	[9]	[10]	[1]	[2]	[3]	[4]
[5]	[6]	[7]	[8]	[9]	[10]	[1]	[2]	[3]	[4]	[5]
[6]	[7]	[8]	[9]	[10]	[1]	[2]	[3]	[4]	[5]	[6]
[7]	[8]	[9]	[10]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[8]	[9]	[10]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
[9]	[10]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]
[10]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]

Tabel 3.2 Hasil operasi antar elemen-elemen dalam monoid faktor (N_0/R,o).

Teorema 3.11 Andaikan ϕ: $(M,\bullet) \rightarrow (N,\#)$ epimorfisma monoid dan R adalah relasi kongruensi pada $(M,\bullet)$ yang didefinisikan sebagai aRb jika dan hanya jika $\phi(a) = \phi(b)$, $\forall a,b \in M$, maka monoid faktor $(M/R, \text{o})$ isomorfis dengan $(N,\#)$.

Bukti:

Andaikan φ: $(M/R,\text{o}) \rightarrow (N,\#)$ suatu fungsi yang didefinisikan sebagai $\varphi([a]) = \phi(a)$, $\forall [a] \in M/R$.

(i) Akan ditunjukkan bahwa φ terdefinisi dengan baik. Ambil sebarang $[a],[b] \in M/R$ sedemikian hingga $[a] = [b]$, maka aRb. Sehingga $\phi(a) = \phi(b)$, dan akibatnya $\varphi([a]) = \varphi([b])$.

Jadi φ terdefinisi dengan baik.

(ii) Ambil sebarang $[a],[b] \in M/R$. Maka:

$$\begin{aligned}
\varphi([a]\text{o}[b]) &= \varphi([a \bullet b]) \\
&= \phi(a \bullet b) \\
&= \phi(a) \# \phi(b) \\
&= \varphi([a]) \# \varphi([b]).
\end{aligned}$$

Kemudian, andaikan e elemen identitas di M, maka $[e]$ adalah elemen identitas di M/R. Dan $\varphi([e]) = \phi(e)$, di mana $\phi(e)$ elemen identitas di N.

Jadi φ suatu homomorfisma monoid.

(iii) Ambil sebarang $y \in N$. Karena ϕ epimorfisma monoid dari M ke N, maka ada $x \in M$ sedemikian sehingga $y = \phi(x)$. Karena $x \in M$ maka $[x] \in M/R$, oleh karenanya $y = \phi(x) = \varphi([x])$.

Jadi terbukti bahwa φ surjektif.

(iv) Ambil sebarang $[a],[b]\in M/R$. Andaikan $\varphi([a]) = \varphi([b])$, maka $\phi(a) = \phi(b)$. Sehingga aRb. Karena R relasi ekuvalensi maka $a\in[b]$. Berdasarkan teorema 2.2 disimpulkan $[a] = [b]$.

Jadi terbukti bahwa φ injektif.

Dengan demikian terbukti bahwa $(M/R,\text{o})$ isomorfis dengan $(N,\#)$. ∎

Pada teorema 3.11 tersebut jika ϕ tidak surjektif, yakni ϕ hanyalah merupakan homomorfisma monoid dari M ke N saja, maka akan diperoleh isomorfisma yang lain, yang disajikan dalam teorema berikut ini.

Teorema 3.12 Andaikan f: $(M,\bullet)\to(N,\#)$ homomorfisma monoid dan R adalah relasi kongruensi pada $(M,\bullet)$ yang didefinisikan sebagai aRb jika dan hanya jika $f(a) = f(b)$, $\forall a,b\in M$, maka monoid faktor $(M/R,\text{o})$ isomorfis dengan submonoid dari $(N,\#)$, yakni $f(M)$, dan isomorfisma monoid yang dimaksud adalah φ: $M/R\to f(M)$ yang didefinisikan oleh $\varphi([x]) = f(x)$, $\forall[x]\in M/R$.

Bukti:

Pada teorema 3.11 telah dibuktikan bahwa φ terdefinisi dengan baik dan φ merupakan homomorfisma monoid sekaligus injektif, sehingga cukup dibuktikan bahwa φ surjektif.

Ambil sebarang $y\in f(M)$. Karena $f(M)$ merupakan range dari f maka ada $x\in M$ sedemikian hingga $y = f(x)$. Karena $x\in M$ maka $[x]\in M/R$, sehingga $y = f(x) = \varphi([x])$. Jadi terbukti bahwa φ surjektif. Terbukti bahwa $M/R \approx f(M)$. ∎

B. Grup

1. Grup dan Subgrup

Sekarang akan dibahas struktur aljabar yang lebih khusus daripada monoid. Struktur aljabar ini lebih khusus karena tiga dari empat aksioma yang disyaratkan pasti dipenuhi oleh monoid.

Definisi 3.19 Suatu *grup* $(G,\#)$ adalah suatu himpunan G yang tidak kosong bersama operasi "#", yang memenuhi aksioma-aksioma berikut:

(i) Operasi "#" di G bersifat tertutup.

$(\forall a,b \in G)\ a \# b \in G.$

(ii) Operasi "#" di G bersifat asosiatif.

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

(iii) G memuat elemen identitas e.

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

(iv) Setiap elemen di G memiliki elemen invers.

$(\forall a \in G)(\exists a^{-1} \in G)\ a \# a^{-1} = a^{-1} \# a = e.$

Dengan kata lain grup adalah monoid yang setiap elemennya memiliki invers, sehingga setiap grup adalah monoid. Karena setiap monoid adalah semigrup maka setiap grup juga merupakan semigrup. Dengan demikian hal-hal yang berlaku pada semigrup maupun monoid, juga berlaku pada grup.

Berdasarkan teorema 2.7 dan teorema 2.8, diperoleh kesimpulan bahwa setiap grup hanya memiliki satu elemen identitas, dan setiap elemen dalam grup memiliki invers yang tunggal.

Teorema 3.13 Andaikan $(G,\#)$ grup, maka:

(i) Jika $a \in G$ dan $a \# a = a$ maka $a = e$.

(ii) $(\forall a,b,c \in G)\ a \# b = a \# c \Rightarrow b = c$ (hukum kanselasi kiri), dan

$(\forall a,b,c \in G)\ b \# a = c \# a \Rightarrow b = c$ (hukum kanselasi kanan).

(iii) $(\forall a \in G)\ (a^{-1})^{-1} = a$.

(iv) $(\forall a,b \in G)\ (a \# b)^{-1} = b^{-1} \# a^{-1}$.

(v) $(\forall a,b \in G)\ ax = b$ dan $ya = b$, masing-masing memiliki penyelesaian tunggal di G, yakni $x = a^{-1} \# b$ dan $y = b \# a^{-1}$.

Bukti:

(i) $$\begin{aligned} a \# a = a \Rightarrow\ a^{-1} \# (a \# a) &= a^{-1} \# a \\ (a^{-1} \# a) \# a &= a^{-1} \# a \\ e \# a &= e \\ a &= e. \end{aligned}$$

(ii) Ambil sebarang $a,b,c \in G$.

$$\begin{aligned} \text{Diketahui } a \# b = a \# c \Rightarrow a^{-1} \# (a \# b) &= a^{-1} \# (a \# c) \\ (a^{-1} \# a) \# b &= (a^{-1} \# a) \# c \\ e \# b &= e \# c \\ b &= c. \end{aligned}$$

Bukti bagian yang kedua analog.

(iii) Invers dari elemen a^{-1} adalah elemen unik x sedemikian hingga $a^{-1} \# x = e$. Tetapi $a^{-1} \# a = e$, sehingga invers dari a^{-1} haruslah a.

Dengan demikian $(a^{-1})^{-1} = a$.

(iv) Invers dari $(a \# b)$ adalah elemen unik x sedemikian hingga $(a \# b) \# x = e$. Dan $(a \# b) \# (b^{-1} \# a^{-1}) = a \# (b \# b^{-1}) \# a^{-1} = a \# e \# a^{-1} = a \# a^{-1} = e$. Kemudian $(b^{-1} \# a^{-1}) \# (a \# b) = b^{-1} \# (a^{-1} \# a) \# b = b^{-1} \# e \# b = b^{-1} \# b = e$. Sehingga invers dari $(a \# b)$ haruslah $(b^{-1} \# a^{-1})$.

Jadi $(a \# b)^{-1} = b^{-1} \# a^{-1}$.

(v) Ambil sebarang $a,b \in G$. Diketahui $a \# x = b$, maka $a^{-1} \# (a \# x) = a^{-1} \# b$. Kemudian $(a^{-1} \# a) \# x = a^{-1} \# b$, maka $e \# x = a^{-1} \# b$ sehingga $x = a^{-1} \# b$. Jadi penyelesaian persamaan $a \# x = b$ adalah $x = a^{-1} \# b$.

Andaikan $x = x_1$ dan $x = x_2$ masing-masing adalah penyelesaian dari $a \# x = b$, maka $a \# x_1 = b$ dan $a \# x_2 = b$, sehingga $a \# x_1 = a \# x_2$. Menurut hukum kanselasi kiri diperoleh $x_1 = x_2$. Jadi penyelesaian persamaan $a \# x = b$ adalah tunggal.

Untuk masalah yang kedua, pembuktiannya analog. ∎

Definisi 3.20 Andaikan $(G,\#)$ grup. Jika operasi "#" di G bersifat komutatif maka $(G,\#)$ disebut *grup Abel*.

Dengan demikian jelaslah bahwa setiap grup Abel adalah monoid komutatif. Namun setiap monoid komutatif belum tentu merupakan grup Abel, atau secara umum tidak benar bahwa setiap monoid adalah grup.

Contoh 3.12

1. Himpunan dari semua bilangan bulat membentuk grup Abel $(\mathbf{Z},+)$ terhadap operasi penjumlahan. Hal ini dikarenakan $(\mathbf{Z},+)$ monoid dengan elemen

identitas 0, dan invers dari setiap elemennya adalah negatif dari elemen tersebut.

2. (R-{0},.) adalah grup, karena jelas semigrup, kemudian elemen identitasnya adalah 1. Dan untuk setiap $x \in$ R-{0}, elemen inversnya adalah $1/x$. Karena operasi perkalian pada R-{0}juga bersifat komutatif, maka (R-{0},.) adalah grup Abel juga.

3. Tunjukkan bahwa himpunan bilangan bulat yang genap adalah grup terhadap operasi penjumlahan.

Penyelesaian.

Diketahui E = {$2n$: $n \in$ Z}. Akan ditunjukkan (E,+) adalah grup.

(i) Ambil sebarang $x,y \in$ E maka $x = 2n$ dan $y = 2\ m$, dimana n,m$\in$Z.

$x + y = 2n + 2m = 2\ (n + m) = 2s$, dimana $s = n + m \in$ Z.

Jadi operasi penjumlahan pada E bersifat tertutup.

(ii) Ambil sebarang $x,y,z \in$ E maka $x = 2n$, $y = 2m$, $z = 2k$, dimana $n,m,k \in$ Z.

$(x\ + y) + z = (2n + 2m) + 2k = 2n + (2m + 2k) = x + (y + z)$.

Jadi operasi penjumlahan pada E bersifat asosiatif.

(iii) Ambil sebarang $x \in$ E maka $x = 2n$, dimana $n \in$ Z.

$0 + 2n = 2n + 0 = 2n$, dan $0 \in$ E karena $0 = 2.0$, $0 \in$ Z.

Jadi elemen identitasnya adalah 0.

(iv) Ambil sebarang $x \in$ E maka $x = 2n$, dimana $n \in$ Z. Andaikan y adalah invers dari x, maka $x + y = y + x = 0$. Sehingga

$2n + y = y + 2n = 0 \Leftrightarrow y = -2n = 2(-n)$, $-n \in$ Z.

Jadi $(\forall x = 2n \in \mathrm{E})\ (\exists y = 2(-n) \in \mathrm{E})\ x + y = y + x = 0$.

Dengan demikian telah ditunjukkan bahwa (E,+) adalah grup.

Definisi 3.21 Andaikan $(G,\#)$ grup dan H adalah himpunan bagian yang tidak kosong dari G, maka $(H,\#)$ disebut *subgrup* dari G bila:

(i) $(\forall a,b \in H)\ a \# b \in H$ (operasi "#" di H bersifat tertutup).

(ii) $(\forall a \in H)\ a^{-1} \in H$ (H memuat invers dari setiap elemennya).

Teorema 3.14 Andaikan $(G,\#)$ grup dan $H \subseteq G$. Maka H subgrup dari $(G,\#)$ bila dan hanya bila $(H,\#)$ adalah grup.

Bukti:

($\Rightarrow$) Andaikan H subgrup dari $(G,\#)$. Maka operasi "#" bersifat tertutup di H. Bila $a,b,c \in H$ maka $(a \# b) \# c = a \# (b \# c)$ dalam G adalah juga dalam H, karena H himpunan bagian dari G. Karena $H \neq \varnothing$, maka H memuat paling sedikit satu elemen, misalnya h. Dari definisi, $h^{-1} \in \mathrm{H}$ sehingga $h \# h^{-1}$ adalah elemen identitas di H. Dan dari definisi subgrup sendiri dapat disimpulkan bahwa $(H,\#)$ memuat elemen invers dari setiap elemennya. Dengan demikian $(H,\#)$ adalah grup.

($\Leftarrow$) Andaikan $(H,\#)$ adalah grup. Maka $H \neq \varnothing$, operasi "#" di H bersifat tertutup, dan H memuat invers dari setiap elemennya. Karena $\mathrm{H} \subseteq G$ maka $(H,\#)$ adalah subgrup dari $(G,\#)$. ∎

Contoh 3.13 Diketahui (G = {1, -1, i, -i},.) adalah grup. Buktikan bahwa T = {1,-1} membentuk subgrup terhadap perkalian!

Penyelesaian.

$T \subseteq G$ dan $T \neq \varnothing$ jelas. T tertutup terhadap perkalian dapat dilihat pada tabel berikut:

.	1	-1
1	1	-1
-1	-1	1

Tabel 3.3

Elemen identitasnya adalah 1, dan invers dari setiap elemennya adalah dirinya sendiri. Dengan demikian terbukti bahwa T subgrup dari G.

Definisi 3.22 Bila (G,.) grup, $a \in G$ dan $n \in \mathbb{Z}^+$, maka *pangkat dari elemen dalam grup* didefinisikan sebagai: $a^{-n} = (a^{-1})^n$.

Ingat bahwa hal-hal yang berlaku pada monoid juga berlaku pada grup, sehingga untuk grup (G,.) dan $\forall a \in G$ berlaku: $a^0 = e$ dan $a^{n+1} = a^n a$, $n \in \mathbb{N}_0$.

Teorema 3.15 Jika (G,.) grup dan $a \in G$, maka untuk setiap $m,n \in \mathbb{Z}$ berlaku:

(i) $a^m a^n = a^{m+n}$.

(ii) $(a^m)^n = a^{mn}$.

Bukti:

Karena setiap grup adalah monoid, maka teorema 3.4 juga berlaku untuk setiap elemen dalam grup. Dengan demikian cukup dibuktikan bahwa $a^m a^n = a^{m+n}$ dan $(a^m)^n = a^{mn}$ benar $\forall m \in \mathbb{Z}, \forall n \in \mathbb{Z}^-$ dan $\forall n \in \mathbb{Z}, \forall m \in \mathbb{Z}^-$.

(i) Ambil sebarang $m \in \mathbb{Z}$.

Akan dibuktikan bahwa $a^m a^n = a^{m+n}$ benar untuk setiap $n \in \mathbb{Z}^-$. Andaikan $n \in \mathbb{Z}^-$, maka ada bilangan positif $p \in \mathbb{Z}^+$ sedemikian hingga $n = -p$. Andaikan pula $a^m a^n = a^{m+n}$ benar untuk $p = k$, maka $a^m a^{-k} = a^{m-k}$. Akan ditunjukkan bahwa $a^m a^n = a^{m+n}$ benar untuk $p = k + 1$.

$$\begin{aligned}
a^m a^n = a^m a^{-p} &= a^m a^{-(k+1)} \\
&= a^m((a^{-1})^{k+1}) \\
&= a^m((a^{-1})^k(a^{-1})) \\
&= a^m(a^{-k}a^{-1}) \\
&= (a^m a^{-k})a^{-1} \\
&= a^{(m-k)}a^{-1} \\
&= a^{(m-k)-1} \\
&= a^{m+(-k-1)} \\
&= a^{m-(k+1)} \\
&= a^{m+n}.
\end{aligned}$$

Jadi $a^m a^n = a^{m+n}$ benar untuk setiap $n \in \mathbb{Z}^-$ dan untuk setiap $m \in \mathbb{Z}$.

Secara analog dapat pula dibuktikan bahwa $a^m a^n = a^{m+n}$ benar, $\forall n \in \mathbb{Z}$ dan $\forall m \in \mathbb{Z}^-$.

(ii) Ambil sebarang $m \in \mathbb{Z}$.

Akan dibuktikan bahwa $(a^m)^n = a^{mn}$ benar untuk setiap $n \in Z^-$. Andaikan $n \in Z^-$, maka ada bilangan positif $p \in Z^+$ sedemikian hingga $n = -p$.

$$
\begin{aligned}
(a^m)^n &= (a^m)^{-p} \\
&= ((a^m)^{-1})^p \\
&= (a^{-m})^p \\
&= ((a^{-1})^m)^p \\
&= (a^{-1})^{mp} \\
&= a^{-mp} \\
&= a^{m(-p)} \\
&= a^{mn}.
\end{aligned}
$$

Jadi $(a^m)^n = a^{mn}$ benar untuk $n \in Z^-$ dan untuk setiap $m \in Z$.

Secara analog dapat pula dibuktikan bahwa $(a^m)^n = a^{mn}$ benar, $\forall n \in Z$ dan $\forall m \in Z^-$. ∎

Definisi 3.23 Jika G adalah grup dan $a \in G$, maka bilangan bulat positif terkecil n sedemikian hingga $a^n = e$ disebut *orde dari a*, ditulis $|a|$. Jika tidak ada bilangan seperti n tersebut maka $|a|$ tak berhingga.

2. Grup Siklis

Ada suatu grup yang setiap elemennya dapat ditulis sebagai perpangkatan (positif atau negatif) dari suatu elemen tetap dari grup tersebut. Grup macam ini akan diperoleh setelah pembuktian teorema berikut.

Teorema 3.16 Jika G grup dan $a \in G$ maka $<a> = \{x \in G: x = a^n, n \in \mathbf{Z}\}$ merupakan subgrup dari G.

Bukti:

(i) $<a> \neq \varnothing$, karena $a = a^1 \in <a>$.

(ii) Ambil sebarang $x,y \in <a>$ maka $x = a^m$, $m \in \mathbf{Z}$ dan $y = a^n$, $n \in \mathbf{Z}$. Sehingga $xy = a^m a^n = a^{m+n}$. Karena $m,n \in \mathbf{Z}$ maka $m+n \in \mathbf{Z}$. Dengan demikian $xy \in <a>$.

(iii) Ambil sebarang $x \in <a>$ maka $x = a^n$, $n \in \mathbf{Z}$. Kemudian $x^{-1} = (a^n)^{-1} = a^{-n}$. Karena $n \in \mathbf{Z}$ maka $-n \in \mathbf{Z}$. Sehingga disimpulkan $x^{-1} \in <a>$.

Jadi terbukti bahwa $<a>$ merupakan subgrup dari G. ∎

Definisi 3.24 Jika G grup dan $a \in G$, maka $<a> = \{x \in G: x = a^n, n \in \mathbf{Z}\}$ disebut *subgrup siklis* yang dibangun oleh a.

Definisi 3.25 Suatu elemen a dalam grup G dikatakan *membangun* G, bila $<a> = G$. Suatu grup G disebut *grup siklis* jika ada $a \in G$ yang membangun G.

Teorema 3.17 Setiap grup siklis pasti abelian.

Bukti:

Andaikan G adalah grup siklis, maka $G = <a>$, untuk suatu $a \in G$. Ambil sebarang $x,y \in G$. Karena $G = <a>$, maka $x = a^m$ dan $y = a^n$, dengan $m,n \in \mathbf{Z}$. Sehingga $xy = a^m a^n = a^{m+n} = a^{n+m} = a^n a^m = yx$. Dengan demikian terbukti bahwa untuk setiap $x,y \in G$ berlaku $xy = yx$, dengan kata lain G adalah grup abelian. ∎

Teorema 3.18 Setiap subgrup dari grup siklis adalah siklis.

Bukti:

Andaikan G grup siklis yang dibangun oleh a dan H subgrup dari $G = \langle a \rangle$.

(i) Jika $H = \{e\}$ maka H adalah grup siklis yang dibangun oleh e.

(ii) $H \neq \{e\}$. Andaikan m adalah bilangan bulat positif terkecil sedemikian hingga $a^m \in H$. Akan ditunjukkan $H = \langle a^m \rangle$.

Ambil sebarang $x \in H$ maka $x \in G$, sehingga ada $p \in \mathbf{Z}$ sedemikian hingga $x = a^p$. Menurut algoritma pembagian pada $\mathbf{Z}$, ada $q,r \in \mathbf{Z}$ sedemikian hingga $p = mq + r$, dimana $0 \leq r < m$.

Kemudian didapat: $x = a^p = a^{mq+r} = a^{mq}a^r = (a^m)^q a^r$. Sehingga $a^r = (a^m)^{-q}a^p$. Ingat bahwa m adalah bilangan bulat positif terkecil sedemikian hingga $a^m \in H$, padahal $r < m$ dan $a^r \in H$, maka haruslah $r = 0$, sehingga $a^p = (a^m)^q$.

Karena untuk sebarang $x \in H$ ada $q \in \mathbf{Z}$ sedemikian hingga $x = (a^m)^q$, maka terbukti bahwa subgrup H dari G adalah siklis. ∎

Teorema 3.19 Andaikan $(G,.)$ grup siklis yang dibangun oleh a.

(i) Jika orde dari a berhingga dengan $|a| = k$, $(k \in \mathbf{N})$, maka:

a. Jika bilangan bulat n dibagi k mempunyai sisa r, maka $a^n = a^r$.

b. $(\forall n \in \mathbf{Z})\ a^n = e \Leftrightarrow k \mid n$.

c. $e, a, a^2, a^3, \ldots, a^{k-1}$ adalah elemen-elemen yang berbeda dalam $\langle a \rangle$.

d. $|\langle a \rangle| = k$ (orde dari grup siklis yang dibangun oleh a sama dengan orde dari elemen a).

(ii) Jika orde dari a tak berhingga berlaku: $(\forall m,n \in Z)\ m \neq n \Rightarrow a^m \neq a^n$.

Bukti:

(i) Diketahui orde dari a berhingga dengan $|a| = k$, $(k \in N)$.

a. Andaikan $n \in Z$ dan n dibagi k memiliki sisa r, maka $n = qk + r$, untuk suatu $q \in Z$. Sehingga $a^n = a^{qk+r} = a^{kq+r} = (a^k)^q a^r = e^q a^r = ea^r = a^r$. Jadi $a^n = a^r$.

b. Andaikan $n \in Z$.

($\Rightarrow$) Andaikan $a^n = e$. Andaikan pula r adalah sisa dari pembagian n oleh k. Dari teorema 3.19 (a) diperoleh $a^r = a^n = e$. Akan tetapi $0 \leq r \leq k$-1, dan k adalah orde dari a, sehingga $a^s \neq e$ jikalau $1 \leq s \leq k$-1. Dengan demikian haruslah $r = 0$, yang mengakibatkan $k \mid n$. Jadi $a^n = e \Rightarrow k \mid n$.

($\Leftarrow$) $k \mid n$ maka $n = jk$, untuk suatu $j \in Z$. Sehingga $a^n = a^{jk} = a^{kj} = (a^k)^j = e^j = e$. Jadi $k \mid n \Rightarrow a^n = e$.

c. Berdasarkan teorema 3.19 (a) dan (b), maka disimpulkan bahwa setiap pangkat dari a sama dengan salah satu dari $e, a, a^2, a^3, \ldots, a^{k-1}$. Karena jika $n \in Z$ adalah sebarang pangkat dari a, maka $a^n = a^r$, dimana r adalah sisa dari pembagian n oleh k. Jadi jika sisanya 0 maka $a^n = e$, jika sisanya 1 maka $a^n = a$, dan seterusnya. Sehingga e, $a, a^2, a^3, \ldots, a^{k-1}$ adalah elemen-elemen berbeda dari $<a>$.

d. Dari teorema 3.19 (c), dapat langsung disimpulkan $|<a>| = k$, karena $<a>$ memuat k elemen yang berbeda.

(ii) Andaikan orde dari a tak berhingga dan $(\exists m,n \in \mathbf{Z})\ m \neq n$ dan $a^m = a^n$. Andaikan $m > n$, maka $a^m a^{-n} = a^{n-n} = a^0 = e$. Sehingga $a^{m-n} = e$. Ini berarti ada $p \in \mathbf{N}$ sedemikian hingga $a^p = e$. Oleh karena itu orde dari a berhingga. Terjadi kontradiksi. Dengan demikian bila $|a|$ tak berhingga maka $(\forall m,n \in \mathbf{Z})\ m \neq n \Rightarrow a^m \neq a^n$. ∎

Sehingga dari teorema 3.19 diperoleh dua hal yang berbeda, yakni:

1. Jika $G = <a>$ tak berhingga, maka elemen-elemen dari G adalah $e = a^0, a^{\pm 1}, a^{\pm 2}, a^{\pm 3}, \ldots, a^{\pm n}, \ldots$.
2. Jika $G = <a>$ berhingga, misalnya dengan orde m, maka elemen-elemen yang berbeda di G adalah $e = a^0, a, a^2, a^3, \ldots, a^{m-1}$. Grup siklis berorde m dinotasikan dengan C_m.

Teorema 3.20 Jika G adalah grup siklis dengan pembangun a, maka a^{-1} juga merupakan pembangun dari G.

Bukti:

Ambil sebarang $x \in G$, maka ada suatu $p \in \mathbf{Z}$ sedemikian hingga $x = a^p$. Kemudian $x = (x^{-1})^{-1} = ((a^p)^{-1})^{-1} = (a^{-p})^{-1} = a^{-p(-1)} = a^{-(-p)} = (a^{-1})^{-p}$. Karena $p \in \mathbf{Z}$ maka $-p$ juga dalam $\mathbf{Z}$. Jadi setiap elemen di G dapat dinyatakan sebagai perpangkatan bilangan bulat dari a^{-1}. Dengan demikian a^{-1} juga merupakan pembangun dari G. ■

Dengan demikian setiap grup siklis memiliki paling sedikit sebuah elemen sebagai pembangunnya, bisa juga memiliki lebih dari sebuah elemen pembangun. Akan tetapi tidak harus semua elemen di G yang dapat menjadi pembangun G.

Contoh 3.14

1. Grup ({1, -1, i, $-i$},.) adalah grup siklis berorde 4 dengan pembangun i, karena:

$$\begin{cases} 1 = i^{4n} \\ i = i^{4n+1} \\ -1 = i^{4n+2} \\ -i = i^{4n+3} \end{cases} \quad \text{dengan } n = 0,\ 1,\ 2,\ 3,\ \ldots.$$

Sehingga $|1| = 1$, $|i| = 4$, $|-1| = 2$, dan $|-i| = 4$. Oleh karena itu, grup tersebut dapat ditulis sebagai ({1, i^1, i^2, i^3},.), dengan 4 sebagai orde grupnya.

2. Untuk grup dengan operasi penjumlahan, grup $(G,+)$ adalah siklis bila $G = \{ng : n \in \mathbf{Z}\}$, untuk suatu $g \in G$. Sehingga grup $(\mathbf{Z},+)$ adalah grup siklis berorde tak hingga. Pembangun grup ini adalah 1 dan -1, karena:

$$\begin{aligned} \mathbf{Z} &= \{\ldots, (-3)1, (-2)1, (-1)1, 0.1, 1.1, 2.1, 3.1, \ldots\} \\ &= \{\ldots, 3(-1), 2(-1), 1(-1), 0(-1), (-1)(-1), (-2)(-1), (-3)(-1), \ldots\}. \end{aligned}$$

Elemen identitas 0 memiliki orde 1, sedangkan elemen-elemen lainnya berorde tak hingga, karena $(\forall a \in \mathbf{Z}, a \neq 0)(\forall n \in \mathbf{N})\ na \neq 0$.

3. Subgrup Normal dan Grup Faktor

Relasi kongruen modulo n dalam himpunan bilangan bulat **Z** pada contoh 2.1, dapat didefinisikan oleh $a \equiv b \bmod n$ bila dan hanya bila $(a - b) \in n\mathbf{Z}$, di mana $n\mathbf{Z}$ adalah subgrup dari **Z** yang memuat semua bilangan bulat yang merupakan kelipatan dari n. Sekarang konsep tersebut akan digeneralisasikan, dengan kekongruensian didefinisikan di dalam suatu grup dengan modulonya adalah salah satu dari subgrupnya.

Definisi 3.26 Andaikan $(G,.)$ grup dan H suatu subgrup dari G. Untuk setiap $a,b \in G$, dikatakan bahwa a *kongruen* dengan b *modulo* H, dan ditulis $a \equiv b \bmod H$, bila dan hanya bila $ab^{-1} \in H$.

Teorema 3.21 Relasi $a \equiv b \bmod H$ dari definisi 3.26 adalah suatu relasi ekuivalensi pada G.

Bukti:

(i) Untuk setiap $a \in G$, $aa^{-1} = e \in H$, jadi relasi tersebut refleksif.

(ii) Untuk setiap $a,b \in G$, bila $a \equiv b \bmod H$ maka $ab^{-1} \in H$. Kemudian $(ab^{-1})^{-1} = ba^{-1} \in H$, yang berarti $b \equiv a \bmod H$. Jadi relasi tersebut simetris.

(iii) Untuk setiap $a,b,c \in G$, bila $a \equiv b$ mod H dan $b \equiv c$ mod H maka $ab^{-1} \in H$ dan $bc^{-1} \in H$, sehingga $(ab^{-1})(bc^{-1}) = ac^{-1} \in H$, yaitu $a \equiv c$ mod H. Jadi relasi tersebut transitif.

Terbukti bahwa relasi $a \equiv b$ mod H adalah relasi ekuivalensi. ∎

Definisi 3.27 Andaikan $(G,.)$ grup dan H suatu subgrup dari G, dan $a \equiv b$ mod H bila $ab^{-1} \in H$, $\forall a,b \in G$. Kelas ekuivalensi dari $a \in G$ disebut *koset kanan* dari H dalam G, ditulis dengan Ha dan didefinisikan sebagai:

$$\begin{aligned} \{x \in G: x \equiv a \text{ mod } H\} &= \{x \in G: xa^{-1} = h \in H\} \\ &= \{x \in G: x = ha, h \in H\} \\ &= \{ha: h \in H\}. \end{aligned}$$

Contoh 3.15 Carilah koset-koset kanan dari $H = \{e, g^4, g^8\}$ dalam grup siklis $(C_{12},.)$ yang dibangun oleh elemen $g \in C_{12}$!

Penyelesaian.

H sendiri adalah suatu koset. Koset lainnya adalah $Hg = \{g, g^5, g^9\}$. Kedua koset tersebut tidak memuat semua elemen dari C_{12}, misalnya g^2 tidak termasuk dalam H atau Hg. Sedangkan koset yang ketiga adalah $Hg^2 = \{g^2, g^5, g^{10}\}$ dan koset keempat adalah $Hg^3 = \{g^3, g^7, g^{11}\}$.

Teorema 3.22 Jika H subgrup dari grup $(G,.)$ dan $a,b \in G$, maka pernyataan-pernyataan berikut ini ekuivalen.

(i) $ab^{-1} \in H$.

(ii) $a = hb$, untuk suatu $h \in H$.

(iii) $a \in Hb$.

(iv) $Ha = Hb$.

Bukti:

a. (i) $\Rightarrow$ (ii).

Karena $ab^{-1} \in H$ maka $ab^{-1} = h$, untuk suatu $h \in H$.

Kemudian:
$$\begin{aligned} ab^{-1} &= h \\ (ab^{-1})b &= hb \\ a(b^{-1}b) &= hb \\ ae &= hb \\ a &= hb. \end{aligned}$$

Jadi: $ab^{-1} \in H \Rightarrow a = hb$, untuk suatu $h \in H$.

b. (ii) $\Rightarrow$ (iii).

Diketahui $a = hb$. Karena $Hb = \{hb: h \in H\}$ maka $a \in Hb$.

Jadi: $a = hb \Rightarrow a \in Hb$.

c. (iii) $\Rightarrow$ (iv).

Diketahui $a \in Hb$, akan ditunjukkan $Ha = Hb$, yaitu $Ha \subseteq Hb$ dan $Hb \subseteq Ha$.

Ambil sebarang $x \in Ha$, maka $x = h_1a$, untuk suatu $h_1 \in H$. Karena $a \in Hb$ maka $a = h_2b$, untuk suatu $h_2 \in H$. Sehingga $x = h_1(h_2b) = (h_1h_2)b = h_3b$, dimana $h_3 = h_1h_2 \in H$. Jadi $x \in Hb$, sehingga $Ha \subseteq Hb$.

Ambil sebarang $y \in Hb$, maka $y = h_4b$, untuk suatu $h_4 \in H$. Karena $a \in Hb$ maka $a = h_5b$, untuk suatu $h_5 \in H$. Sehingga $b = h_5^{-1}a$, dimana $h_5^{-1} \in H$.

Dengan demikian $y = h_4(h_5^{-1}a) = (h_4h_5^{-1})a = h_6a$, dimana $h_6 = h_4h_5^{-1} \in H$. Jadi $y \in Ha$, sehingga $Hb \subseteq Ha$.

Oleh karena itu: $a \in Hb \Rightarrow Ha = Hb$.

d. (iv) $\Rightarrow$ (i).

Diketahui $Ha = Hb$. Karena $a = ea$, untuk suatu $e \in H$ maka $a \in Ha$, sehingga $a \in Hb$. Dengan demikian $a = hb$, untuk suatu $h \in H$. Kemudian: $ab^{-1} = (hb)b^{-1} = h(bb^{-1}) = he = h$. Oleh karena itu $ab^{-1} \in H$.

Jadi: $Ha = Hb \Rightarrow ab^{-1} \in H$. ∎

Definisi 3.28 Andaikan G grup dan H subgrup dari G, maka kita juga dapat mendefinisikan relasi L dalam G, yaitu aLb bila dan hanya bila $b^{-1}a \in H$, $\forall a,b \in G$. Dengan cara yang sama dapat dibuktikan bahwa relasi L adalah suatu relasi ekuivalensi, dan kelas ekuivalensi dari a disebut *koset kiri*, yakni $aH = \{ah: h \in H\}$.

Definisi 3.29 Andaikan $(G,\#)$ grup dan N subgrup dari G. Maka N disebut *subgrup normal* dari G, ditulis $N \lhd G$, bila $g \# n \# g^{-1} \in N$, $\forall n \in N$ dan $\forall g \in G$.

Definisi tersebut bukanlah satu-satunya cara untuk menentukan subgrup normal. Cara lain untuk menentukan subgrup normal dibahas dalam teorema berikut ini.

Teorema 3.23 Jika N subgrup dari $(G,.)$ maka $N \triangleleft G$, bila dan hanya bila $Ng = gN$, $\forall g \in G$.

Bukti:

($\Rightarrow$) Diketahui $N \triangleleft G$. Akan dibuktikan $Ng \subseteq gN$ dan $gN \subseteq Ng$.

Ambil sebarang $x \in Ng$ maka $x = ng$, untuk suatu $n \in N$. Kemudian:

$x = eng = (gg^{-1})ng = g(g^{-1}ng) = gn_1$, untuk suatu $n_1 = g^{-1}ng \in N$. Sehingga $gn_1 \in gN$. Jadi $Ng \subseteq gN$.

Ambil sebarang $y \in gN$ maka $y = gn_2$, untuk suatu $n_2 \in N$. Kemudian:

$y = (gn_2)e = (gn_2)g^{-1}g = (gn_2g^{-1})g = n_3g$, untuk suatu $n_3 = gn_2g^{-1} \in N$. Sehingga $n_3g \in Ng$. Jadi $gN \subseteq Ng$.

($\Leftarrow$) Diketahui $Ng = gN$. Maka untuk suatu elemen $n \in N$, $ng \in Ng = gN$.

Oleh karena itu $ng = gn_1$, untuk suatu $n_1 \in N$. Kemudian: $g^{-1}(ng) = g^{-1}(gn_1)$

$$\begin{aligned} g^{-1}ng &= (g^{-1}g)n_1 \\ &= en_1 \\ &= n_1 \in N. \end{aligned}$$

Jadi N adalah subgrup normal dari G. ∎

Teorema 3.24 Jika $(G,\#)$ grup Abel dan N subgrup dari G, maka $N \triangleleft G$.

Bukti:

Ambil sebarang $n \in N$ dan $g \in G$, maka:

$$\begin{aligned} g \# n \# g^{-1} &= g \# (n \# g^{-1}) \\ &= g \# (g^{-1} \# n) \\ &= (g \# g^{-1}) \# n \end{aligned}$$

$= e \# n = n.$

Karena $n \in N$ maka $g \# n \# g^{-1} \in N$. Jadi terbukti $N \triangleleft G$. ∎

Jika diberikan grup G dan $N \triangleleft G$, maka dapat dibentuk suatu grup yang disebut grup faktor, dimana elemen-elemennya berupa koset-koset. Ingat bahwa dalam subgrup normal berlaku koset kiri sama dengan koset kanan, sehingga dalam hal ini hanya akan digunakan koset kanan.

Teorema 3.25 Andaikan $(G,.)$ grup. Jika $N \triangleleft G$ dan G/N menyatakan himpunan semua koset kanan N dari G, maka G/N merupakan grup terhadap operasi $(Na)(Nb) = N(ab)$, $\forall Na, Nb \in G/N$.

Bukti:

(i) Akan dibuktikan bahwa operasi pada G/N terdefinisi dengan baik, yakni jika $Na_1 = Na_2$ dan $Nb_1 = Nb_2$, maka akan diperoleh $N(a_1b_1) = N(a_2b_2)$.

Jika $Na_1 = Na_2$ maka $a_1 = n_1a_2$, untuk suatu $n_1 \in N$, dan jika $Nb_1 = Nb_2$ maka $b_1 = n_2b_2$, untuk suatu $n_2 \in N$. Dengan demikian:

$$\begin{aligned} a_1b_1 &= (n_1a_2)(n_2b_2) \\ &= n_1(a_2n_2)b_2 \\ &= n_1(a_2n_2e)b_2 \\ &= n_1(a_2n_2a_2^{-1}a_2)b_2 \\ &= n_1(n_3a_2)b_2, \text{ dengan } n_3 = a_2n_2a_2^{-1} \in N; \\ &= (n_1n_3)(a_2b_2) \end{aligned}$$

$= n_4(a_2b_2)$, dengan $n_4 = n_1n_3 \in N$.

Jadi terbukti $N(a_1b_1) = N(a_2b_2)$.

(ii) Operasi pada G/N adalah tertutup, karena $\forall Na, Nb \in G/N$, dengan $a,b \in G$ berlaku: $(Na)(Nb) = N(ab) = Nc$, dengan $c = ab \in G$.

(iii) Operasi pada G/N bersifat asosiatif, karena $\forall Na, Nb, Nc \in G/N$ dengan $a,b,c \in G$ berlaku: $((Na)(Nb))(Nc) = (N(ab))(Nc)$

$$= N((ab)c)$$
$$= N(a(bc))$$
$$= (Na)(N(bc))$$
$$= (Na)((Nb)(Nc)).$$

(iv) Elemen identitas dalam G/N adalah $Ne = N$, karena $\forall Na \in G/N$ dengan $a \in G$, berlaku: $(Na)(Ne) = N(ae) = Na$ dan $(Ne)(Na) = N(ea) = Na$.

(v) Untuk setiap $Na \in G/N$, inversnya adalah $Na^{-1} \in G/N$, karena:
$(Na)(Na^{-1}) = N(aa^{-1}) = Ne = N$ dan $(Na^{-1})(Na) = N(a^{-1}a) = Ne = N$.

Jadi terbukti bahwa G/N adalah grup. ∎

Definisi 3.30 Grup seperti yang disebutkan pada teorema 3.25 disebut *grup faktor* dari G oleh N, dinotasikan G/N.

4. Homomorfisma dalam Grup

Definisi 3.31 Jika $(G,\#)$ dan (H,o) grup, maka pemetaan $\theta: G \to H$ disebut *homomorfisma grup* bila memenuhi: $\theta(a \# b) = \theta(a) \text{ o } \theta(b)$, $\forall a,b \in G$.

Seperti halnya pada homomorfisma monoid, pada homomorfisma grup juga didefinisikan beberapa macam homomorfisma grup berkaitan dengan jenis fungsinya.

Definisi 3.32 Andaikan $(G,\#)$ dan (H,o) grup dengan homomorfisma grup $\theta: G \to H$.

(i) Jika θ merupakan fungsi surjektif, maka θ disebut *epimorfisma grup*.

(ii) Jika θ merupakan fungsi injektif, maka θ disebut *monomorfisma grup*.

(iii) Jika θ merupakan fungsi bijektif, maka θ disebut *isomorfisma grup*. Jika ada isomorfisma dari G ke H maka dikatakan G *isomorfis* dengan H, dan dinotasikan oleh $(G,\#) \approx (H,\mathrm{o})$.

Contoh 3.16 Pemetaan θ dari himpunan bilangan bulat ke himpunan bilangan bulat yang genap yang didefinisikan oleh $\theta(n) = 2n$, $\forall n \in \mathbf{Z}$, adalah homomorfisma grup. Karena himpunan bilangan bulat dan himpunan bilangan bulat yang genap, masing-masing adalah grup dengan operasi penjumlahan, dan $\theta(n + m) = 2(n + m) = 2n + 2m = \theta(n) + \theta(m)$, $\forall n,m \in \mathbf{Z}$.

Teorema 3.26 Jika $\theta: (G,\#) \to (H,\mathrm{o})$ homomorfisma grup dengan e_G dan e_H secara berturut-turut adalah elemen indentitas di G dan di H, maka berlakulah:

(i) $\theta(e_G) = e_H$.

(ii) $\theta(a^{-1}) = (\theta(a))^{-1}$, $\forall a \in G$.

(iii) $\theta(a^k) = (\theta(a))^k$, $\forall a \in G$ dan $\forall k \in \mathbf{Z}$.

(iv) $\theta(G)$ subgrup dari H.

(v) Jika θ injektif maka $G \approx \theta(G)$.

Bukti:

(i) Karena $(G,\#)$ grup dan e_G elemen identitas di G, maka $e_G \# e_G = e_G$. Dengan demikian $\theta(e_G \# e_G) = \theta(e_G)$. Kemudian θ: $(G,\#) \to (H,\text{o})$ homomorfisma grup maka diperoleh $\theta(e_G \# e_G) = \theta(e_G) \text{ o } \theta(e_G) = \theta(e_G)$. Oleh karena $\theta(e_G)$ dan e_H di H maka $\theta(e_G) \text{ o } e_H = \theta(e_G)$. Sehingga $\theta(e_G) \text{ o } \theta(e_G) = \theta(e_G) \text{ o } e_H$. Berdasarkan hukum kanselasi kiri disimpulkan $\theta(e_G) = e_H$.

(ii) Ambil sebarang $a \in G$. Karena G grup maka $a^{-1} \in G$ dan $a \# a^{-1} = a^{-1} \# a = e_G$. Karena θ homomorfisma grup maka $e_H = \theta(e_G) = \theta(a \# a^{-1}) = \theta(a) \text{ o } \theta(a^{-1})$. H grup, sehingga untuk $\theta(a) \in H$ ada $(\theta(a))^{-1} \in H$ sedemikian hingga $\theta(a) \text{ o } (\theta(a))^{-1} = e_H$. Maka $\theta(a) \text{ o } (\theta(a))^{-1} = \theta(a) \text{ o } \theta(a^{-1})$. Menurut hukum kanselasi kiri disimpulkan $\theta(a^{-1}) = (\theta(a))^{-1}$.

(iii) Ambil sebarang $a \in G$. Akan dibuktikan $\theta(a^k) = (\theta(a))^k$ benar untuk setiap $k \in \mathbf{Z}$.

- Untuk $k = 0$.

$$\begin{aligned} \theta(a^k) &= \theta(a^0) \\ &= \theta(e_G) \\ &= e_H \\ &= (\theta(a))^0 \end{aligned}$$

$= (\theta(a))^k.$

Jadi $\theta(a^k) = (\theta(a))^k$ benar untuk $k = 0$.

- Untuk $k > 0$.

Untuk $k = 1$ maka $\theta(a^k) = \theta(a^1) = \theta(a) = (\theta(a))^1 = (\theta(a))^k$. Jadi $\theta(a^k) = (\theta(a))^k$ benar untuk $k = 1$.

Andaikan $\theta(a^k) = (\theta(a))^k$ benar untuk $k = n$ maka $\theta(a^n) = (\theta(a))^n$. Akan ditunjukkan bahwa $\theta(a^k) = (\theta(a))^k$ benar untuk $k = n + 1$.

$$\begin{aligned}
\theta(a^k) &= \theta(a^{n+1}) \\
&= \theta(a^n \# a) \\
&= \theta(a^n) \circ \theta(a) \\
&= (\theta(a))^n \circ (\theta(a))^1 \\
&= (\theta(a))^{n+1} \\
&= (\theta(a))^k.
\end{aligned}$$

Jadi $\theta(a^k) = (\theta(a))^k$ benar untuk $k > 0$.

- Untuk $k < 0$.

Andaikan $k \in \mathbb{Z}$, maka ada $m \in \mathbb{Z}^+$ sedemikian hingga $k = -m$. Andaikan $\theta(a^k) = (\theta(a))^k$ benar untuk $m = n$, maka $\theta(a^{-n}) = (\theta(a))^{-n}$. Akan ditunjukkan bahwa $\theta(a^k) = (\theta(a))^k$ benar untuk $m = n + 1$.

$$\begin{aligned}
\theta(a^k) &= \theta(a^{-(n+1)}) \\
&= \theta(a^{-n+(-1)}) \\
&= \theta(a^{-n} \# a^{-1}) \\
&= \theta(a^{-n}) \circ \theta(a^{-1}) \\
&= (\theta(a))^{-n} \circ (\theta(a))^{-1}
\end{aligned}$$

$= (\theta(a))^{-n+(-1)}$

$= (\theta(a))^{-(n+1)}$

$= (\theta(a))^{k}$.

Jadi $\theta(a^k) = (\theta(a))^k$ benar untuk $k < 0$.

Dengan demikian terbukti bahwa $\theta(a^k) = (\theta(a))^k$ benar, $\forall a \in G$ dan $\forall k \in \mathbf{Z}$.

(iv) $\theta(G) = \{y \in H: (\exists x \in G)\ y = \theta(x)\}$.

- $\theta(G) \neq \varnothing$, karena ada e_H di H dimana $e_H = \theta(e_G)$, dengan $e_G \in G$. Dengan demikian $e_H \in \theta(G)$.
- Ambil sebarang $y_1, y_2 \in \theta(G)$ maka $y_1, y_2 \in H$, dan ada $x_1, x_2 \in G$ sedemikian hingga $y_1 = \theta(x_1)$ dan $y_2 = \theta(x_2)$.

  $y_1 \text{ o } y_2 = \theta(x_1) \text{ o } \theta(x_2)$

  $= \theta(x_1 \# x_2)$.

  Karena $x_1, x_2 \in G$, $y_1, y_2 \in H$, dan G maupun H grup maka $x_1 \# x_2 \in G$ dan $y_1 \text{ o } y_2 \in H$. Dilain pihak $\theta(x_1 \# x_2) = y_1 \text{ o } y_2$, maka $y_1 \text{ o } y_2 \in \theta(G)$.

  Jadi $\theta(G)$ tertutup terhadap operasi "o".
- Ambil sebarang $y \in \theta(G)$ maka $y \in H$, dan ada $x \in G$ sedemikian hingga $y = \theta(x)$. Kemudian:

  $y = \theta(x) \Rightarrow y^{-1} = (\theta(x))^{-1}$

  $= \theta(x^{-1})$.

  Karena G dan H grup maka $x^{-1} \in G$ dan $y^{-1} \in H$. Sehingga ada $x^{-1} \in G$ sedemikian hingga $y^{-1} = \theta(x^{-1})$. Oleh karena itu $y^{-1} \in \theta(G)$.

Jadi $(\forall y \in \theta(G))\ y^{-1} \in \theta(G)$.

Dan karena jelas $\theta(G) \subseteq H$, maka terbukti bahwa $\theta(G)$ subgrup dari H.

(v) Diketahui θ: $G \rightarrow H$ injektif.

Ambil sebarang $y \in \theta(G)$ maka ada $x \in G$ sedemikian hingga $y = \theta(x)$. Jadi θ: $G \rightarrow \theta(G)$ surjektif. Karena θ: $G \rightarrow H$ homomorfisma grup dan injektif, maka demikian juga θ: $G \rightarrow \theta(G)$, sehingga $G \approx \theta(G)$. ∎

Definisi 3.33 Jika θ: $(G,\#) \rightarrow (H,\text{o})$ homomorfisma grup maka *kernel* dari θ, atau *Ker* θ adalah himpunan semua elemen di G yang kawannya adalah elemen identitas di H. Dengan demikian *Ker* $\theta = \{x \in G: \theta(x) = e_H\}$.

Teorema 3.27 Jika θ: $(G,\#) \rightarrow (H,\text{o})$ homomorfisma grup, maka:

(i) *Ker* θ subgrup dari G.

(ii) *Ker* $\theta = \{e_G\}$ bila dan hanya bila θ injektif.

(iii) *Ker* $\theta \lhd G$.

Bukti:

(i) *Ker* $\theta \subseteq G$ jelas.

- *Ker* $\theta \neq \varnothing$ karena ada $e_G \in G$ dimana $\theta(e_G) = e_H$. Sehingga $e_G \in$ *Ker* θ.
- Ambil sebarang $x,y \in$ *Ker* θ, maka $\theta(x) = \theta(y) = e_H$.

  $\theta(x \# y) = \theta(x) \text{ o } \theta(y) = e_H \text{ o } e_H = e_H$.

  Jadi $x \# y \in$ *Ker* θ, sehingga $(\forall x,y \in \textit{Ker } \theta)\ x \# y \in$ *Ker* θ.
- Ambil sebarang $x \in$ *Ker* θ, maka $\theta(x) = e_H$.

$\theta(x^{-1}) = (\theta(x))^{-1} = e_H^{-1} = e_H$.

Jadi $x^{-1} \in Ker\ \theta$, sehingga $(\forall x \in Ker\ \theta)\ x^{-1} \in Ker\ \theta$.

Dengan demikian terbukti bahwa $Ker\ \theta$ subgrup dari G.

(ii) ($\Rightarrow$) Ambil sebarang $x,y \in G$ sedemikian hingga $\theta(x) = \theta(y)$. Karena G grup maka $y^{-1} \in G$ dan $x \# y^{-1} \in G$. Kemudian:

$$\begin{aligned}
\theta(x) = \theta(y) \Leftrightarrow \theta(x) \circ \theta(y^{-1}) &= \theta(y) \circ \theta(y^{-1}) \\
\theta(x) \circ \theta(y^{-1}) &= \theta(y) \circ (\theta(y))^{-1} \\
\theta(x \# y^{-1}) &= e_H.
\end{aligned}$$

Jadi $x \# y^{-1} \in Ker\ \theta$. Diketahui $Ker\ \theta = \{e_G\}$, maka $x \# y^{-1} \in \{e_G\}$.

Sehingga: $x \# y^{-1} = e_G$

$$\begin{aligned}
(x \# y^{-1}) \# y &= e_G \# y \\
x \# (y^{-1} \# y) &= y \\
x \# e_G &= y \\
x &= y.
\end{aligned}$$

Jadi $(\forall x,y \in G)\ \theta(x) = \theta(y) \Rightarrow x = y$, atau θ injektif.

($\Leftarrow$) Diketahui θ injektif.
$$\begin{aligned}
Ker\ \theta &= \{x \in G: \theta(x) = e_H\} \\
&= \{x \in G: \theta(x) = \theta(e_G)\} \\
&= \{x \in G: x = e_G\} \\
&= \{e_G\}.
\end{aligned}$$

Jadi terbukti bahwa: θ injektif $\Rightarrow Ker\ \theta = \{e_G\}$.

(iii) Ambil sebarang $x \in G$ dan $y \in Ker\ \theta$, maka $\theta(y) = e_H$.

$$\begin{aligned}
\theta(x \# y \# x^{-1}) &= \theta(x) \circ \theta(y) \circ \theta(x^{-1}) \\
&= \theta(x) \circ e_H \circ \theta(x^{-1})
\end{aligned}$$

$$= \theta(x) \circ \theta(x^{-1})$$

$$= \theta(x \# x^{-1})$$

$$= \theta(e_G)$$

$$= e_H.$$

Jadi $x \# y \# x^{-1} \in Ker\ \theta$, sehingga $Ker\ \theta \lhd G$. ∎

Teorema 3.28 Andaikan θ: $(G,\#) \to (H,\circ)$ epimorfisma grup dengan $Ker\ \theta = K$. Jika μ: $G/K \to H$ yang didefinisikan sebagai $\mu(Kx) = \theta(x)$, $\forall Kx \in G/K$, maka μ merupakan isomorfisma grup dari G/K ke H. Sehingga $G/K \approx H$.

Bukti:

(i) Akan ditunjukkan bahwa μ terdefinisi dengan baik.

Ambil sebarang $Ka, Kb \in G/K$ sedemikian hingga $Ka = Kb$. Menurut teorema 3.22 diperoleh $a = k \# b$, untuk suatu $k \in K$. Sehingga:

$$\theta(a) = \theta(k \# b) \Leftrightarrow \theta(a) = \theta(k) \circ \theta(b)$$

$$\theta(a) = e_H \circ \theta(b)$$

$$\theta(a) = \theta(b)$$

$$\mu(Ka) = \mu(Kb).$$

Jadi μ terdefinisi dengan baik.

(ii) Ambil sebarang $Ka, Kb \in G/K$.

$$\mu((Ka)(Kb)) = \mu(K(a \# b))$$

$$= \theta(a \# b)$$

$$= \theta(a) \circ \theta(b)$$

$$= \mu(Ka) \circ \mu(Kb).$$

Jadi μ homomorfisma grup.

(iii) Ambil sebarang $y \in H$. Karena $\theta: G \to H$ homomorfisma grup dan surjektif maka ada $x \in G$ sedemikian hingga $y = \theta(x)$. Karena $x \in G$ maka $Kx \in G/K$, sehingga $y = \theta(x) = \mu(Kx)$.

Jadi terbukti bahwa μ surjektif.

(iv) Ambil sebarang $Ka, Kb \in G/K$. Andaikan $\mu(Ka) = \mu(Kb)$ maka $\theta(a) = \theta(b)$.

$$\theta(a) = \theta(b) \Leftrightarrow \theta(a) \circ (\theta(b))^{-1} = \theta(b) \circ (\theta(b))^{-1}$$

$$\theta(a) \circ \theta(b^{-1}) = \theta(b) \circ (\theta(b))^{-1}$$

$$\theta(a \# b^{-1}) = e_H.$$

Dengan demikian $a \# b^{-1} \in K$, sehingga menurut teorema 3.22 $Ka = Kb$.

Jadi terbukti bahwa μ injektif.

Jadi terbukti bahwa $\mu: G/K \to H$ homomorfisma grup dan μ bijektif. Oleh karenanya $G/K \approx H$. ∎

5. Grup Bebas

Andaikan A adalah suatu himpunan dan $a_i \in A$, $i \in \mathbf{N}$. Kadang-kadang A disebut *himpunan abjad* dengan a_i sebagai *huruf* dalam himpunan abjad tersebut.

Definisi 3.34 Andaikan A adalah suatu himpunan. Suatu simbol berbentuk a_i^n, dengan $a_i \in A$, $n \in \mathbf{Z}$, $i \in \mathbf{N}$, disebut *suku kata* dalam A, kemudian rangkaian berhingga dari suku kata yang ditulis tanpa simbol apapun diantaranya disebut *kata* dalam A.

Definisi 3.35 Suatu *kata kosong* adalah kata tanpa suku kata apapun, dinotasikan dengan Δ.

Contoh 3.17 Andaikan $A = \{a_1, a_2, a_3\}$ maka $a_1a_3^{-4}a_2^2a_3$, $a_2^3a_2^{-1}a_3a_1^2a_1^{-7}$, dan a_3^2 adalah kata-kata dalam A.

Ada dua macam perubahan dari suatu kata yang diketahui, yang disebut *singkatan mendasar* dan disajikan dalam definisi berikut ini.

Definisi 3.36 Jika A suatu himpunan dan a_i^n, $i \in \mathrm{N}$ dan $n \in \mathrm{Z}$, adalah suku kata dalam A, maka berlaku:

(i) $a_i^0 = \Delta$.

(ii) $a_i^m a_i^n = a_i^{m+n}$, $\forall m,n \in \mathrm{Z}$.

Dengan demikian setiap kata dapat diubah menjadi kata dalam bentuk *tereduksi*, dengan memanipulasi perpangkatan dalam bilangan bulat, sebagaimana telah disebutkan dalam definisi di atas.

Contoh 3.18 Bentuk tereduksi dari kata $a_2^3a_2^{-1}a_3a_1^2a_1^{-7}$ pada contoh 2.6.1 adalah $a_2^2a_3a_1^{-5}$, sedangkan bentuk tereduksi dari kata $a_1a_3^{-4}a_2^2a_3$ adalah dirinya sendiri.

Definisi 3.37 Dua buah kata w_1 dan w_2 dikatakan *sama* bila dan hanya bila bentuk tereduksi w_1 sama dengan bentuk tereduksi w_2.

Definisi 3.38 Andaikan A adalah suatu himpunan dan $F(A)$ adalah himpunan semua kata yang tereduksi dalam A. Didefinisikan *operasi rangkaian* "$\star$" dimana $(\forall w_1,w_2 \in F(A))$ $w_1 \star w_2$ menyatakan bentuk tereduksi dari w_1w_2, dimana w_1w_2 adalah kata yang diperoleh dengan meletakkan w_2 disebelah kanan w_1. Jika $A = \varnothing$, maka $F(A) = \{\Delta\}$.

Contoh 3.19 Jika $w_1 = a_2^3a_1^{-5}a_3^2$ dan $w_2 = a_3^{-2}a_1^2a_3a_2^{-2}$, maka $w_1 \star w_2$ menyatakan bentuk tereduksi dari $a_2^3a_1^{-5}a_3^2a_3^{-2}a_1^2a_3a_2^{-2}$, yaitu $a_2^3a_1^{-3}a_3a_2^{-2}$.

Teorema 3.29 $F(A)$ adalah grup terhadap operasi rangkaian "$\star$".

Bukti:

(i) Akan dibuktikan bahwa operasi rangkaian "$\star$" tersebut terdefinisi dengan baik. Ambil sebarang $w_1,w_2,w_1',w_2' \in F(A)$ dimana $w_1 = w_1'$ dan $w_2 = w_2'$. Maka $w_1w_2 = w_1'w_2'$, sehingga $w_1 \star w_2$ adalah bentuk tereduksi dari w_1w_2, yang berarti pula bentuk tereduksi dari $w_1'w_2'$, yaitu $w_1' \star w_2'$. Jadi operasi "$\star$" terdefinisi dengan baik di $F(A)$.

(ii) Ambil sebarang $w_1,w_2 \in F(A)$ maka $w_1 \star w_2 \in F(A)$, karena $w_1 \star w_2$ merupakan bentuk tereduksi dari kata w_1w_2 dan $F(A)$ himpunan semua kata tereduksi dalam A. Jadi operasi "$\star$" bersifat tertutup.

(iii) Jelaslah bahwa sifat asosiatif di $F(A)$ diturunkan dari sifat asosiatif pada penjumlahan bilangan bulat, karena kata tereduksi diperoleh dengan memanipulasi perpangkatan dalam bilangan bulat.

(iv) Elemen identitas di $F(A)$ adalah Δ karena $w \star \Delta = \Delta \star w = w, \forall w \in F(A)$.

(v) Ambil sebarang $w \in F(A)$. Elemen invers dari w diperoleh dengan membentuk kata yang berisikan suku kata-suku kata dari w dalam urutan terbalik dan mengganti setiap suku kata a_i^n dengan a_i^{-n}. Sehingga diperoleh kata w^{-1} yang juga merupakan kata tereduksi, dan $w \star w^{-1} = w^{-1} \star w = \Delta$. Jadi setiap kata tereduksi di $F(A)$ memiliki invers.

Dengan demikian terbukti bahwa $(F(A), \star)$ merupakan grup. ∎

Definisi 3.39 Grup $F(A)$ yang diperoleh dari teorema 3.29 disebut *grup bebas* yang dibangun oleh A. Dalam hal ini A disebut *basis* dari F.

Contoh 3.20 Jika $A = \{a\}$ maka jelaslah bahwa $F(A) = \{\ldots, a^{-3}, a^{-2}, a^{-1}, \Delta, a, a^2, a^3, \ldots\}$.

Teorema 3.30 Suatu grup bebas dengan basis $\{a\}$ isomorfis dengan grup $(\mathbf{Z},+)$.

Bukti:

Andaikan μ: $F(\{a\}) \rightarrow \mathbf{Z}$ suatu fungsi yang memetakan setiap kata di $F(\{a\})$ ke suatu bilangan yang menyatakan pangkat dari kata tersebut.

(i) Akan dibuktikan bahwa μ terdefinisi dengan baik. Ambil sebarang $a^m, a^n \in F(\{a\})$ sedemikian hingga $a^m = a^n$. Maka $m, n \in \mathbf{Z}$ dan $m = n$. Sehingga $\mu(a^m) = \mu(a^n)$. Jadi μ terdefinisi dengan baik.

(ii) Akan dibuktikan bahwa μ adalah suatu homomorfisma grup. Ambil sebarang $w_1, w_2 \in F(\{a\})$ dimana $w_1 = a^m$ dan $w_2 = a^n$, dimana $m,n \in Z$. Maka $\mu(w_1 \star w_2) = \mu(a^{m+n}) = m + n = \mu(w_1) + \mu(w_2)$.

Jadi terbukti bahwa μ adalah suatu homomorfisma grup.

(iii) Ambil sebarang $n \in Z$, maka pasti ada $w \in F(\{a\})$ dimana $w = a^n$, sehingga $\mu(w) = n$.

Jadi μ adalah fungsi surjektif.

(iv) Ambil sebarang $w_1, w_2 \in F(\{a\})$ dimana $w_1 = a^m$ dan $w_2 = a^n$, dimana $m,n \in Z$, sedemikian hingga $\mu(w_1) = \mu(w_2)$. Maka $m = n$, sehingga $a^m = a^n$. Oleh karenanya $w_1 = w_2$.

Jadi μ adalah fungsi injektif.

Dengan demikian terbukti bahwa suatu grup bebas $(F(\{a\}),\star)$ isomorfis dengan grup $(Z,+)$. ∎

C. Hubungan antara Monoid dengan Grup

Dari pembahasan mengenai monoid dan grup, diperoleh hubungan antara monoid dengan grup yang akan disajikan secara langsung maupun melalui teorema-teorema berikut.

Pertama, setiap grup adalah monoid. Kesimpulan ini berdasarkan definisi monoid dan definisi grup. Akibatnya, setiap grup Abel adalah juga monoid komutatif. Karena setiap subgrup adalah grup dan setiap submonoid adalah monoid, bila $(H,\#)$ subgrup dari grup $(G,\#)$ maka $(H,\#)$ sekaligus submonoid dari monoid $(G,\#)$.

Teorema 3.31 Andaikan $(M,\#)$ adalah monoid dan $G_M = \{x \in M: x$ memiliki invers$\}$, maka $(G_M,\#)$ membentuk grup.

Bukti:

(i) Karena $e \in M$ dan e memiliki invers yakni dirinya sendiri, maka $e \in G_M$. Jadi G_M tidak kosong dan memuat elemen identitas.

(ii) Ambil sebarang $x,y \in G_M$ maka x dan y memiliki invers, yakni x^{-1} dan y^{-1}. Jelaslah bahwa x^{-1} dan y^{-1} juga dalam G_M. Kemudian $x \# y$ memiliki invers yakni $y^{-1} \# x^{-1}$. Jadi $x \# y \in G_M$.

(iii) Sifat asosiatif di G_M diturunkan dari sifat asosiatif di M, karena M monoid dan $G_M \subseteq M$.

(iv) Jika $x \in G_M$ maka $x \# x^{-1} = x^{-1} \# x = e$, sehingga $(x^{-1})^{-1} = x$. Jadi $x^{-1} \in G_M$. Dengan demikian setiap elemen di G_M memiliki invers di G_M.

Jadi terbukti bahwa $(G_M,\#)$ adalah grup. ∎

Contoh 3.21 Monoid (N,.) memiliki grup kernel {1}, sedangkan monoid (Z,.) memiliki grup kernel {-1, 1}. Untuk monoid (Q,.), grup kernelnya Q* = Q – {0}. Bila G grup maka grup kernelnya adalah G.

Teorema 3.32 Jika $(M,\#)$ grup maka $(M,\#)$ adalah monoid yang idempotennya hanya e.

Bukti:

Andaikan e dan sebarang $x \in M$ adalah idempoten dari M, maka:

$x \# x^{-1} = e \Leftrightarrow x \# (x \# x^{-1}) = x \# e$

$$(x \# x) \# x^{-1} = x$$

$$x \# x^{-1} = x$$

$$e = x.$$

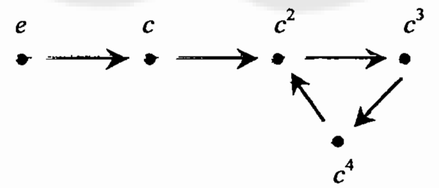
Jadi terbukti bahwa hanya e yang merupakan idempotennya. ∎

Teorema 3.33 Jika G grup siklis berhingga maka G monoid siklis.

Bukti:

Andaikan G = $<a>$ grup siklis berhingga, maka berdasarkan teorema 3.19 $<a> = a^0, a^1, a^2, a^3, \ldots, a^{k-1}$ dimana k adalah orde dari G. Dengan kata lain setiap elemen di G dapat dinyatakan sebagai perpangkatan dari a, dengan a sebagai pembangun dari G. Karena G juga monoid dan pembangunnya satu elemen yakni a, maka G sekaligus monoid siklis. Jadi setiap grup siklis berhingga pasti monoid siklis. ∎

Perhatikan bahwa kasus di atas tidak berlaku untuk grup siklis tak hingga. Sebagai contoh grup siklis tak hingga (Z,+) bukan suatu monoid siklis, karena pembangun dari **Z** adalah –1 dan 1. Selain itu, tidak semua monoid siklis terhingga adalah grup. Misalnya monoid siklis $(\{e,c,c^2,c^3,c^4\},.)$ dimana perkalian dengan elemen c dinyatakan dengan anak panah, yang tampak pada gambar 3.1.



Gambar 3.1 Monoid siklis $(\{e,c,c^2,c^3,c^4\},.)$.

Hal tersebut akan tampak jelas bila kita bentuk tabel hasil perkalian antara elemen-elemennya, seperti pada tabel 3.4, yang menunjukkan bahwa elemen-elemen c, c^2, c^3, dan c^4 tidak memiliki elemen invers. Dengan demikian monoid siklis terhingga ($\{e,c,c^2,c^3,c^4\}$, .) bukanlah grup.

.	e	C	c^2	C^3	c^4
e	e	C	c^2	C^3	c^4
c	c	c^2	c^3	C^4	c^2
c^2	c^2	c^3	c^4	C^2	c^3
c^3	c^3	c^4	c^2	C^3	c^4
c^4	c^4	c^2	c^3	C^4	c^2

Tabel 3.4 Perkalian elemen-elemen monoid siklis ($\{e,c,c^2,c^3,c^4\}$,.).

Berikut ini akan kita dapatkan suatu grup yang himpunan dasarnya terdiri atas isomorfisma-isomorfisma monoid dari suatu monoid ke dirinya sendiri.

Teorema 3.34 Himpunan semua isomorfisma monoid dari $(M,\#)$ ke dirinya sendiri membentuk suatu grup terhadap komposisi fungsi.

Bukti:

Andaikan G adalah himpunan semua isomorfisma monoid dari M ke M.

(i) Ambil suatu fungsi identitas i^M: $M \to M$. Maka $i^M(x \# y) = x \# y = i^M(x) \# i^M(y)$, $\forall x,y \in M$, dan $i^M(e_M) = e_M$. Jelaslah bahwa i^M bijektif. Ini menunjukkan bahwa $i^M \in G$.

Jadi G tidak kosong.

(ii) Ambil sebarang $u, v \in G$. Maka $\forall x, y \in M$ berlaku:

$$\begin{aligned} u \circ v(x \# y) &= u(v(x \# y)) \\ &= u(v(x) \# v(y)) \qquad \text{(karena } v \text{ isomorfisma monoid)} \\ &= u(v(x)) \# u(v(y)) \qquad \text{(karena } u \text{ isomorfisma monoid).} \end{aligned}$$

Dan $u \circ v(e_M) = u(v(e_M)) = u(e_M) = e_M$. Sehingga $u \circ v \in G$.

Jadi operasi komposisi fungsi di G bersifat tertutup.

(iii) Ambil sebarang $u, v, w \in G$. Maka $\forall x \in M$ berlaku:

$u \circ (v \circ w)(x) = u(v(w(x)))$ dan $(u \circ v) \circ w(x) = u(v(w(x)))$.

Jadi operasi komposisi fungsi di G bersifat asosiatif.

(iv) Elemen identitas di G adalah fungsi identitas i^M, karena $\forall u \in G$ dan $\forall x \in M$ berlaku: $i_M \circ u(x) = i_M(u(x)) = u(x)$ dan $u \circ i_M(x) = u(i_M(x)) = u(x)$.

(v) G adalah himpunan semua isomorfisma monoid maka setiap elemen di G adalah fungsi bijektif. Sehingga setiap elemen di G memiliki invers. Akan dibuktikan bahwa elemen inversnya tersebut juga di G.

Ambil sebarang $u \in G$ maka $u(x \# y) = u(x) \# u(y)$, $\forall x, y \in M$. Andaikan v adalah invers dari u, maka $v(u(x)) = x$ dan $v(u(y)) = y$. Kemudian:

$v(u(x) \# u(y)) = v(u(x \# y)) = x \# y = v(u(x)) \# v(u(y))$.

Perhatikan bahwa $v(u(e_M)) = v(e_M)$ dan $v(u(e_M)) = e_M$, maka $v(e_M) = e_M$.

Dengan demikian v yang merupakan fungsi invers dari fungsi u, adalah isomorfisma monoid juga.

Jadi setiap elemen di G memiliki invers di G.

Dengan demikian terbukti bahwa himpunan semua isomorfisma monoid dari M ke M membentuk suatu grup terhadap komposisi fungsi. ∎

BAB IV

PENERAPAN

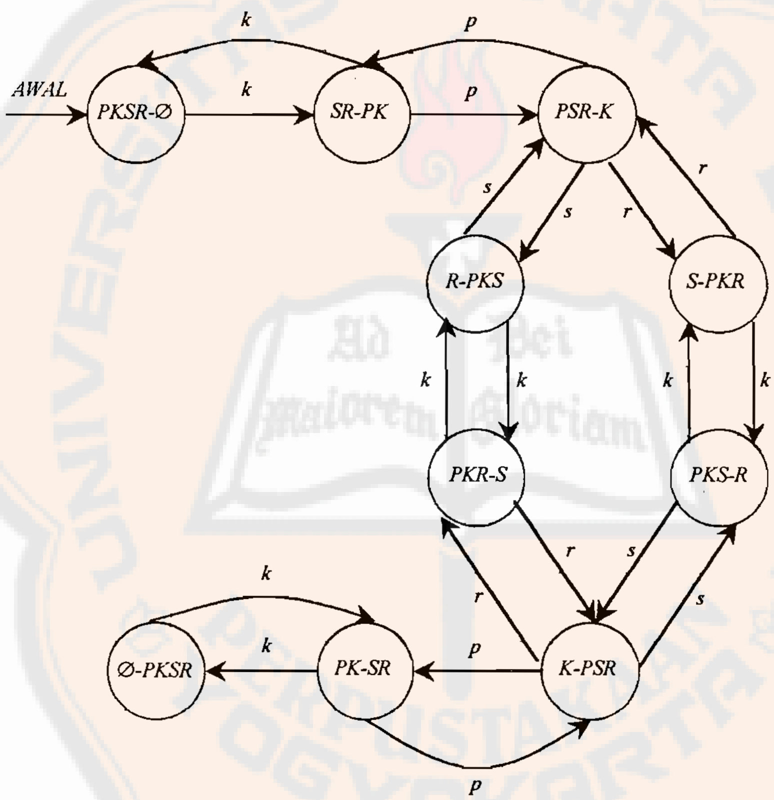
Pada bagian ini akan dibahas mengenai penerapan monoid pada *automata* atau otomata. Untuk itu, sebelumnya akan dibahas dahulu mengenai konsep otomata itu sendiri. Dalam hal ini otomata yang akan dibahas dibatasi untuk jenis *otomata status berhingga.*

A. Otomata Status Berhingga

Kita menjumpai otomata dalam berbagai bentuk, misalnya lift, mesin hitung, dan komputer. Semuanya itu memiliki salah satu aspek yakni status atau keadaan, pada saat tertentu. Status tersebut dapat berubah ke status yang lain karena pengaruh dari luar (disebut *input*), sehingga otomata bereaksi menghasilkan gerakan, perhitungan, atau sebagaimana fungsinya. Otomata yang dimaksud di sini bukanlah mesin secara fisik, melainkan model matematika dari suatu sistem yang menerima input sedemikian rupa sehingga statusnya berubah.

Suatu otomata status berhingga memiliki status yang banyaknya berhingga, dan dapat berpindah-pindah dari suatu status ke status yang lain. Perubahan status ini dinyatakan oleh *fungsi transisi*. Sebelum melangkah ke definisi dari otomata status berhingga, perhatikan dahulu kasus menarik berikut.

Seorang petani dengan seekor kambing, seekor serigala, dan seikat rumput berada pada suatu sisi sungai (kita sebut saja sisi kiri). Terdapat sebuah perahu kecil yang hanya bisa memuat petani itu dan salah satu dari kambing, serigala, atau rumput. Petani itu akan menyeberangkan ketiganya ke sisi kanan sungai. Tetapi jika petani meninggalkan serigala dan kambing pada suatu sisi sungai, maka kambing akan dimakan serigala. Begitu pula jika kambing ditinggalkan bersama rumput, maka kambing akan memakan rumput. Mungkinkah untuk menemukan cara melintasi sungai tanpa menyebabkan kambing atau rumput dimakan?



Gambar 4.1 Diagram transisi untuk permasalahan petani, kambing, serigala, dan rumput.

Masalah tersebut di atas bisa dimodelkan dengan memperhatikan mereka yang menempati setiap sisi sungai. Andaikan P, K, S, dan R secara berturut-turut menyatakan petani, kambing, serigala, dan rumput. Tinjau keadaan awal atau status awal yakni *PKSR*-∅ (semua berada di sisi kiri sungai), dan status akhir yakni ∅-*PKSR* (semua berada di sisi kanan sungai).

Pada gambar 4.1, ada 10 status dari 16 status yang mungkin. Karena terdapat status yang tidak boleh dimasuki, misalnya *KR-PS* (kambing dan rumput di sisi kiri sungai-petani dan serigala di sisi kanan sungai), karena rumput akan dimakan kambing. Input dari sistem ini adalah tindakan yang dilakukan oleh petani. Petani bisa menyeberang sendirian (*input p*), dengan kambing (*input k*), dengan serigala (*input s*), atau dengan rumput (*input r*). Sehingga diperoleh dua solusi singkat dengan menelusuri lintasan dari status awal ke status akhir.

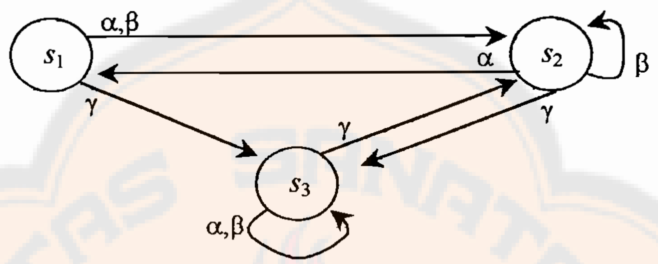
Definisi 4.1 *Otomata status berhingga* (S,I,m) terdiri dari himpunan *status* $S = \{s_1,s_2,\dots,s_n\}$, himpunan *input* $I = \{i_1,i_2,\dots,i_t\}$, $n,t \in \mathrm{N}$, dan *fungsi transisi* m: $I \mathrm{x} S \to S$ yang menyatakan bagaimana setiap input yang diberikan mengubah status. Perhatikan bahwa jika otomata berada pada status s_n dan input i_t diberikan pada otomata tersebut, maka otomata akan mengubahnya ke status $m(i_t,s_n)$.

Untuk selanjutnya kata otomata dipakai untuk menyatakan otomata status berhingga. Dengan demikian, model dari pemecahan pada masalah petani, kambing, serigala, dan rumput memiliki himpunan status S dan himpunan input I, di mana:

$$S = \{PKSR\text{-}\varnothing,\ SR\text{-}PK,\ PSR\text{-}K,\ R\text{-}PSK,\ S\text{-}PKR,\ PKR\text{-}S,\ PSK\text{-}R,\ K\text{-}PSR,\ PK\text{-}SR,\ \varnothing\text{-}PKSR\}$$

$$I = \{p, k, s, r\}.$$

Contoh 4.1 Otomata yang ditunjukkan oleh diagram transisi pada gambar 4.2 memiliki tiga status, yakni s_1, s_2, dan s_3, dengan tiga input α, β, dan γ. Sedangkan fungsi transisi dari otomata ini ditunjukkan pada tabel 4.1 berikut.



Gambar 4.2 Diagram transisi.

Status awal	Status selanjutnya		
	Input		
	α	β	γ
S_1	s_2	s_2	s_3
S_2	s_1	s_2	s_3
S_3	s_3	s_3	s_2

Tabel 4.1 Fungsi transisi.

Dengan demikian, jika kita perhatikan gambar 4.1 dan 4.2, maka akan tampak bahwa suatu otomata dapat diilustrasikan dalam bentuk diagram transisi, di mana:

- Kurva tertutup menyatakan status/kedudukan.
- Label pada kuva tertutup adalah nama dari status tersebut.
- Busur menyatakan transisi, yakni perpindahan status.

- Label pada busur adalah simbol input.

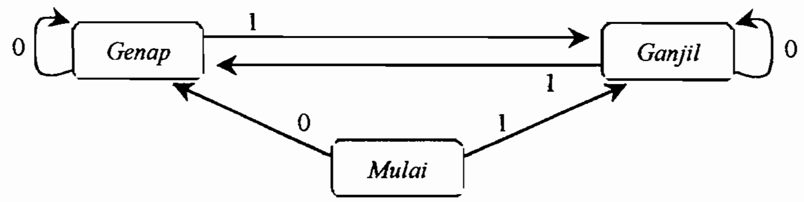
Jadi jika input i menyebabkan perubahan status s_1 ke s_2, kita lukis busur dengan label i dari s_1 ke s_2 pada diagramnya.

Contoh 4.2 Otomata yang menyatakan banyaknya bilangan 1 pada input sebagai bilangan ganjil atau genap, memiliki himpunan status $S = \{Mulai, Genap, Ganjil\}$ dan himpunan input $I = \{0, 1\}$. Fungsi transisi m: Ix$S \rightarrow S$ dinyatakan pada tabel 4.2, dan diagram transisinya diilustrasikan pada gambar 4.3.

Status awal	Status selanjutnya	
	Input	
	0	1
Mulai	*Genap*	*Ganjil*
Genap	*Genap*	*Ganjil*
Ganjil	*Ganjil*	*Genap*

Tabel 4.2 Fungsi transisi.

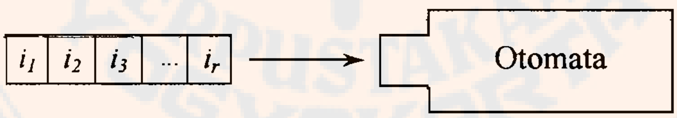
Pada status *Mulai*, jika input 0 diberikan kepada otomata ini maka statusnya akan berubah ke status *Genap*, dan jika input 1 diberikan kepada otomata ini maka statusnya akan berubah ke status *Ganjil*.



Gambar 4.3 Diagram transisi.

Andaikan I himpunan input dari suatu otomata dengan himpunan status S dan fungsi transisi m: Ix$S \rightarrow S$. Setiap input menetapkan fungsi dari himpunan status ke dirinya sendiri, bayangan dari himpunan status membentuk himpunan bagian dari himpunan status, yang dihasilkan dari input yang diberikan. Sehingga diperoleh fungsi m': $I \rightarrow S^S$ dimana $S^S = \{f: S \rightarrow S\}$, dan $m'(i)$: $S \rightarrow S$ didefinisikan oleh $(m'(i))(s) = m(i,s)$, di mana $i \in I$ dan $s \in S$. Untuk setiap $i \in I$, fungsi $m'(i)$ menyatakan *efek* yang dimiliki input i terhadap himpunan status dari otomata.

Suatu input dapat diberikan ke otomata berupa rangkaian input. Himpunan dari semua rangkaian input adalah himpunan dasar dari monoid bebas $(FM(I), \star)$, sebagai himpunan input. Berdasarkan teorema 3.9, fungsi m': $I \rightarrow S^S$ dapat diperluas menjadi homomorfisma monoid h: $(FM(I), \star) \rightarrow (S^S, \circ)$ dimana $h(i_1 i_2 ... i_r) = m'(i_1) \circ m'(i_2) \circ ... \circ m'(i_r)$, dengan $i_1 i_2 ... i_r \in FM(I)$. Dengan catatan, bahwa input i_r yang pertama diberikan pada otomata tersebut. Ilustrasi dari pemberian rangkaian input pada suatu otomata dapat dilihat pada gambar 4.4 berikut ini.



Gambar 4.4 Suatu rangkaian input yang akan diberikan pada otomata.

Sebagai contoh, pada otomata yang menyatakan banyaknya bilangan 1 pada input sebagai bilangan ganjil atau genap (contoh 4.2). Himpunan statusnya adalah $S = \{Mulai, Genap, Ganjil\}$ dengan fungsi-fungsi m': $\{0,1\} \rightarrow S^S$ dan h: $FM(I) \rightarrow S^S$, di mana $(m'(i))(s) = m(i,s)$, untuk $i \in \{0,1\}$ dan $s \in S$, fungsi transisi m dinyatakan pada tabel 4.2. Dengan demikian kita dapatkan fungsi m' seperti pada tabel 4.3 berikut ini.

Status awal	Status selanjutnya	
	$M'(0)$	$m'(1)$
Mulai	*Genap*	*Ganjil*
Genap	*Genap*	*Ganjil*
Ganjil	*Ganjil*	*Genap*

Tabel 4.3 Fungsi m': $\{0,1\} \rightarrow S^S$.

Kemudian $h(0) = m'(0)$ dan $h(1) = m'(1)$. Sedangkan $(h(00))(Mulai) = (m'(0) \circ m'(0))(Mulai) = (m'(0))((m'(0))(Mulai)) = (m'(0))(Genap) = Genap$; kemudian $(h(00))(Genap) = (m'(0) \circ m'(0))(Genap) = (m'(0))((m'(0))(Genap)) = (m'(0))(Genap) = Genap$; dan $(h(00))(Ganjil) = (m'(0) \circ m'(0))(Ganjil) = (m'(0))((m'(0))(Ganjil)) = (m'(0))(Ganjil) = Ganjil$. Untuk rangkaian input dengan panjang 2 lainnya dapat dihitung dengan cara serupa, sehingga diperoleh tabel 4.4 berikut ini.

Status awal	Status selanjutnya						
	$h(\Delta)$	$h(0)$	$h(1)$	$h(00)$	$h(01)$	$h(10)$	$h(11)$
Mulai	*Mulai*	*Genap*	*Ganjil*	*Genap*	*Ganjil*	*Ganjil*	*Genap*
Genap	*Genap*	*Genap*	*Ganjil*	*Genap*	*Ganjil*	*Ganjil*	*Genap*
Ganjil	*Ganjil*	*Ganjil*	*Genap*	*Ganjil*	*Genap*	*Genap*	*Ganjil*

Tabel 4.4 Efek dari rangkaian input dengan panjang ≤ 2.

Dan jika kita lanjutkan perhitungan untuk efek dari rangkaian input dengan panjang ≥ 3, maka akan kita dapatkan hasil bahwa homomorfisma monoid h dinyatakan oleh:

$$h(\text{rangkaian input}) = \begin{cases} m'(0), & \text{jika banyaknya bilangan 1 pada rangkaian} \\ & \text{input adalah genap atau nol,} \\ m'(1), & \text{jika banyaknya bilangan 1 pada rangkaian} \\ & \text{input adalah ganjil,} \\ \text{fungsi identitas di } S^S, & \text{jika rangkaian inputnya kosong.} \end{cases}$$

B. Monoid dari Otomata Status Berhingga

Telah dikatakan sebelumnya bahwa dalam otomata (S,I,m), efek dari suatu input $i \in I$ dinyatakan oleh fungsi $m'(i)$: $S \to S$, di mana $(m'(i))(s) = m(i,s)$, $\forall s \in S$. Kemudian, jika input yang diberikan berupa rangkaian input, maka efek dari rangkaian input tersebut dinyatakan oleh $h(i_1 i_2 \ldots i_r) = m'(i_1) \circ m'(i_2) \circ \ldots \circ m'(i_r)$, $\forall i_1 i_2 \ldots i_r \in FM(I)$.

Dalam suatu otomata dengan n status (S), rangkaian inputnya paling banyak memberi n^n efek yang berbeda (diperoleh dari orde S^S). Karena banyaknya rangkaian input dalam $FM(I)$ tak berhingga, maka ada kemungkinan bahwa suatu rangkaian input memiliki efek yang sama dengan rangkaian input lainnya, yang tidak dapat dibedakan oleh otomata. Dengan mengelompokkan efek-efek yang sama tersebut, maka kita dapat mengetahui kemampuan otomata tersebut dalam menanggapi rangkaian input yang diberikan, berkaitan dengan banyaknya efek yang dimilikinya. Hal ini dilakukan dengan menetapkan suatu relasi kongruensi pada monoid bebas *FM(I)*, dan hasilnya disajikan pada teorema 4.1 berikut ini.

Teorema 4.1 Andaikan (S,I,m) adalah otomata status berhingga dan efek dari rangkaian inputnya dinyatakan oleh homomorfisma monoid h: $FM(I) \to S^S$. Jika didefinisikan relasi R pada $FM(I)$ yaitu $\alpha R\beta$ jika $h(\alpha) = h(\beta)$, $\forall \alpha,\beta \in FM(I)$, maka diperoleh monoid faktor $FM(I)/R$.

Bukti:

Untuk membuktikan teorema ini, cukup dibuktikan bahwa relasi R tersebut adalah relasi kongruensi pada $FM(I)$, sehingga harus dibuktikan pula bahwa R relasi ekuivalensi.

Ambil sebarang $\alpha,\beta,\gamma \in FM(I)$. Maka $h(\alpha) = h(\alpha)$, sehingga $\alpha R\alpha$, yang berarti R refleksif. Andaikan $\alpha R\beta$ maka: $h(\alpha) = h(\beta) \Leftrightarrow h(\beta) = h(\alpha)$. Dengan demikian $\beta R\alpha$. Jadi R simetris. Selanjutnya, andaikan $\alpha R\beta$ dan $\beta R\gamma$. Maka $h(\alpha) = h(\beta)$ dan $h(\beta) = h(\gamma)$, sehingga $h(\alpha) = h(\gamma)$, yang berarti $\alpha R\gamma$. Jadi R transitif, oleh karenanya R adalah relasi ekuivalensi.

Andaikan $\alpha R\beta$, maka $h(\alpha) = h(\beta)$, dan $h(\alpha \star \gamma) = h(\alpha) \circ h(\gamma) = h(\beta) \circ h(\gamma) = h(\beta \star \gamma)$. Dengan demikian $(\alpha \star \gamma) R (\beta \star \gamma)$, dan dengan cara yang sama dapat dibuktikan bahwa $(\gamma \star \alpha) R (\gamma \star \beta)$. Jadi R adalah relasi kongruensi pada monoid bebas $(FM(I), \star)$. ∎

Definisi 4.2 Monoid faktor $FM(I)/R$ yang diperoleh dari teorema 4.1 di atas, disebut *monoid dari otomata status berhingga (S,I,m)*.

Monoid dari otomata ini menyatakan kemampuan otomata dalam menanggapi rangkaian input yang diberikan. Karena banyaknya rangkaian input dalam $FM(I)$ tak berhingga, sedangkan banyaknya elemen dalam monoid faktor $FM(I)/R$ kurang dari atau sama dengan n^n, sehingga berdasarkan teorema 4.1, dua rangkaian input yang berbeda berada dalam kelas kongruensi yang sama bila dan hanya bila keduanya memiliki efek yang sama.

Dengan menerapkan teorema 3.12 pada homomorfisma monoid h: $FM(I) \rightarrow S^S$, maka didapat bahwa monoid faktor $FM(I)/R$ isomorfis dengan Imh. Isomorfisma monoid ini menentukan transisi yang unik di antara status, untuk setiap kelas kongruensi dalam $FM(I)/R$.

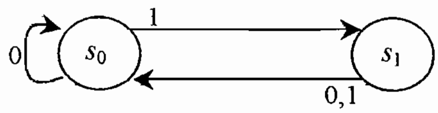
Contoh 4.3 Lukis diagram transisi dan temukan monoid dari otomata (S,I,m) berikut. Otomata memiliki dua status, s_0 dan s_1, dan $I = \{0, 1\}$. Efek dari input diberikan oleh fungsi $m'(0), m'(1)$: $S \rightarrow S$, yang dinyatakan oleh tabel 4.5.

Status awal	Status selanjutnya	
	$m'(0)$	$m'(1)$
s_0	s_0	s_1
s_1	s_0	s_0

Tabel 4.5 Efek dari input.

Penyelesaian.

Dari tabel 4.5, kita peroleh diagram transisi untuk otomata tersebut, yang disajikan pada gambar 4.5 berikut.



Gambar 4.5 Diagram transisi.

Akan dihitung efek dari rangkaian input dengan panjang 2, dengan mengingat bahwa $h(ij) = m'(i) \circ m'(j)$, $i,j \in I$, di mana j yang pertama diberikan ke otomata. Sehingga $h(00)(s_0) = (m'(0) \circ m'(0))(s_0) = (m'(0))((m'(0))(s_0)) = (m'(0))(s_0) = s_0$; dan $h(00)(s_1) = (m'(0) \circ m'(0))(s_1) = (m'(0))((m'(0))(s_1)) = (m'(0))(s_0) = s_0$. Dengan cara yang sama dapat dihitung efek untuk rangkaian input 01, 10, dan 11 lainnya, sehingga diperoleh tabel 4.6. Dari tabel 4.5 dan 4.6, tampak bahwa $h(00) = h(01) = h(0)$, sehingga $[00] = [01] = [0]$ dalam monoid dari otomata ini. Hanya ada empat fungsi dari $\{s_0,s_1\}$ ke $\{s_0,s_1\}$, yaitu $h(0)$, $h(1)$, $h(10)$, dan $h(11)$. Dengan demikian monoid dari otomata ini berisikan empat kelas kongruensi yakni [0], [1], [10], dan [11].

Status awal	Status selanjutnya			
	$h(00)$	$h(01)$	$h(10)$	$h(11)$
s_0	s_0	s_0	s_1	s_0
s_1	s_0	s_0	s_1	s_1

Tabel 4.6 Efek dari rangkaian input dengan panjang dua.

Sebagai contoh, $[1]\circ[10] = [1\star 10] = [110]$. Karena $(h(110))(s_0) = (m'(1) \circ m'(1) \circ m'(0))(s_0) = (m'(1) \circ m'(1))((m'(0))(s_0)) = (m'(1) \circ m'(1))(s_0) = (m'(1))((m'(1))(s_0)) = (m'(1))(s_1) = s_0$, dan $(h(110))(s_1) = (m'(1) \circ m'(1) \circ$

$m'(0))(s_1) = (m'(1) \circ m'(1))((m'(0))(s_1)) = (m'(1) \circ m'(1))(s_0) = (m'(1))((m'(1))(s_0)) = (m'(1))(s_1) = s_0$, maka $h(110) = h(0)$ sehingga [110] = [0]. Untuk elemen-elemen lainnya dapat dicari dengan cara serupa, sehingga diperoleh tabel operasi antar elemen-elemen dalam monoid dari otomata ini, yang ditunjukkan pada tabel 4.7 berikut. Perhatikan bahwa [11] adalah elemen identitas, sehingga dalam monoid dari otomata ini [Δ] = [11].

o	[0]	[1]	[10]	[11]
[0]	[0]	[0]	[0]	[0]
[1]	[10]	[11]	[0]	[1]
[10]	[10]	[10]	[10]	[10]
[11]	[0]	[1]	[10]	[11]

Tabel 4.7 Hasil operasi antar elemen-elemen dalam monoid dari otomata.

Contoh 4.4 Carilah monoid dari otomata ({*Mulai*,*Genap*,*Ganjil*},{0,1}, m) yang menyatakan banyaknya bilangan 1 pada input sebagai bilangan genap atau ganjil!

Penyelesaian.

Pada halaman 86 telah ditunjukkan bahwa setiap rangkaian input yang memuat bilangan 1 dalam jumlah yang genap atau nol memiliki efek yang sama dengan input 0, dan setiap rangkaian input yang memuat bilangan 1 dalam jumlah yang ganjil memiliki efek yang sama dengan input 1, kemudian jika inputnya kosong maka efeknya berupa fungsi identitas dari {*Mulai*,*Genap*,*Ganjil*} ke dirinya sendiri. Sehingga rangkaian input dari otomata ini hanya memberikan tiga efek, yang diwakili oleh $h(\Delta)$, $h(0)$, dan $h(1)$, seperti yang ditunjukkan pada tabel 4.8 berikut ini.

Status awal	Status selanjutnya		
	$h(\Delta)$	$h(0)$	$h(1)$
Mulai	*Mulai*	*Genap*	*Ganjil*
Genap	*Genap*	*Genap*	*Ganjil*
Ganjil	*Ganjil*	*Ganjil*	*Genap*

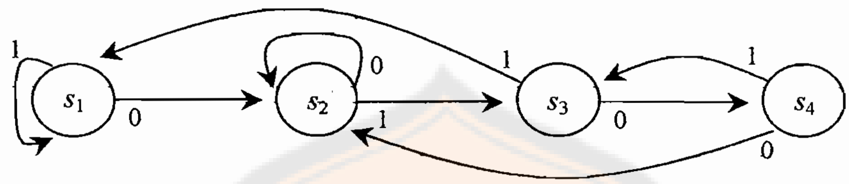
Tabel 4.8 Efek dari rangkaian input.

Dengan demikian monoid dari otomata beranggotakan tiga elemen $[\Delta]$, $[0]$, dan $[1]$. Karena $[1]\mathrm{o}[1] = [1\star 1] = [11]$, dan $(h(11))(Mulai) = (m'(1) \text{ o } m'(1))(Mulai) = (m'(1))((m'(1))(Mulai)) = (m'(1))(Ganjil) = Genap$; $(h(11))(Genap) = (m'(1) \text{ o } m'(1))(Genap) = (m'(1))((m'(1))(Genap)) = (m'(1))(Ganjil) = Genap$; dan $(h(11))(Ganjil) = (m'(1) \text{ o } m'(1))(Ganjil) = (m'(1))((m'(1))(Ganjil)) = (m'(1))(Genap) = Ganjil$, maka $h(11) = h(0)$ sehingga $[11] = [0]$. Secara analog, hasil operasi antara elemen-elemen lainnya dapat dicari dengan cara serupa, sehingga didapat tabel untuk monoid ini, yang ditunjukkan pada tabel 4.9 berikut.

o	$[\Delta]$	$[0]$	$[1]$
$[\Delta]$	$[\Delta]$	$[0]$	$[1]$
$[0]$	$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[1]$	$[0]$

Tabel 4.9 Hasil operasi antar elemen-elemen dalam monoid dari otomata.

Contoh 4.5 Tentukan monoid dari otomata yang ditunjukkan oleh diagram transisi pada gambar 4.6 berikut!



Gambar 4.6 Diagram transisi.

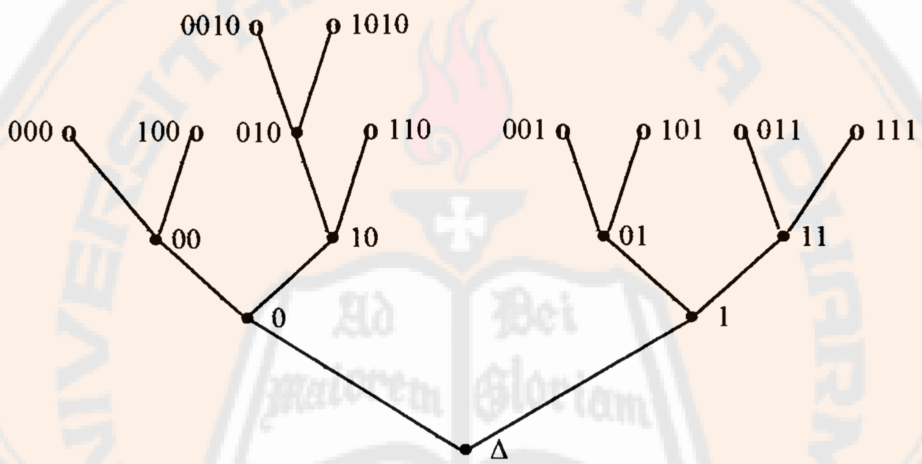
Penyelesaian.

Otomata ini memiliki empat status sehingga total fungsi dari himpunan status ke dirinya sendiri ada $4^4 = 256$ kemungkinan. Dengan cara yang sama seperti pada dua contoh sebelumnya, kita dapat menghitung efek-efek dari rangkaian input dengan panjang 0, 1, dan 2, yang hasilnya disajikan pada tabel 4.10. Pada tabel tersebut ditunjukkan bahwa rangkaian input dengan panjang masing-masing 0, 1, dan 2, semuanya memiliki efek yang berbeda satu sama lain. Akan tetapi, tujuh dari delapan rangkaian input dengan panjang 3 memiliki efek yang sama dengan rangkaian input dengan panjang 2. Satu-satunya rangkaian input dengan efek yang berbeda adalah 010. Untuk itu, rangkaian input dengan panjang 4 yang kita periksa hanyalah yang input awalnya 010, yakni 0010 dan 1010.

Status awal	Status akhir dari berbagai rangkaian input									
	$h(\Delta)$	$h(0)$	$h(1)$	$h(00)$	$h(01)$	$h(10)$	$h(11)$	$h(000)$	$h(001)$	$h(010)$
s_1	s_1	s_2	s_1	s_2	s_2	s_3	s_1	s_2	s_2	s_4
s_2	s_2	s_2	s_3	s_2	s_4	s_3	s_1	s_2	s_2	s_4
s_3	s_3	s_4	s_1	s_2	s_2	s_3	s_1	s_2	s_2	s_4
s_4	s_4	s_2	s_3	s_2	s_4	s_3	s_1	s_2	s_2	s_4

Status awal	Status akhir						
	$h(011)$	$h(100)$	$h(101)$	$h(110)$	$h(111)$	$h(0010)$	$h(1010)$
s_1	s_2	s_3	s_3	s_1	s_1	s_2	s_3
s_2	s_2	s_3	s_3	s_1	s_1	s_2	s_3
s_3	s_2	s_3	s_3	s_1	s_1	s_2	s_3
s_4	s_2	s_3	s_3	s_1	s_1	s_2	s_3

Tabel 4.10 Efek dari berbagai rangkaian input pada status dari otomata.



Gambar 4.7 Diagram pohon dari rangkaian input.

Kita dapat menggunakan diagram pohon, seperti pada gambar 4.7, untuk memeriksa apakah kita telah mencakup semua kemungkinan fungsi transisi, yang diperoleh dari setiap rangkaian input yang ada. Noktah pada pohon melambangkan rangkaian input. Pada setiap noktah α, akan ada ranting naik yang diakhiri oleh noktah $0\star\alpha$ dan $1\star\alpha$. Pohon kita pangkas pada noktah α, jika α memberikan efek yang sama dengan yang diberikan noktah β lainnya pada pohon. Pada akhirnya, pohon akan terhenti pertumbuhannya karena fungsi transisi yang terhingga banyaknya. Dan setiap rangkaian input tadi pasti memiliki efek yang sama dengan salah satu dari rangkaian input yang dinyatakan oleh noktah hitam pada gambar 4.7. Noktah-noktah hitam inilah yang melambangkan semua rangkaian input yang memberikan efek berbeda satu sama lain.

Dengan demikian, monoid dari otomata ini hanya memiliki delapan elemen, yakni [Δ], [0], [1], [11], [01], [10], [11], dan [010], dari 256 fungsi transisi yang mungkin. Tabel hasil operasi antar elemen-elemen dalam monoid ini diberikan pada tabel 4.11.

o	[Δ]	[0]	[1]	[00]	[01]	[10]	[11]	[010]
[Δ]	[Δ]	[0]	[1]	[00]	[01]	[10]	[11]	[010]
[0]	[0]	[00]	[01]	[00]	[00]	[010]	[00]	[00]
[1]	[1]	[10]	[11]	[10]	[10]	[11]	[11]	[10]
[00]	[00]	[00]	[00]	[00]	[00]	[00]	[00]	[00]
[01]	[01]	[010]	[00]	[010]	[010]	[00]	[00]	[010]
[10]	[10]	[10]	[10]	[10]	[10]	[10]	[10]	[10]
[11]	[11]	[11]	[11]	[11]	[11]	[11]	[11]	[11]
[010]	[010]	[010]	[010]	[010]	[010]	[010]	[010]	[010]

Tabel 4.11 Hasil operasi antar elemen-elemen dalam monoid dari otomata.

Contoh 4.6 Tentukan monoid dari otomata pada contoh 4.1!

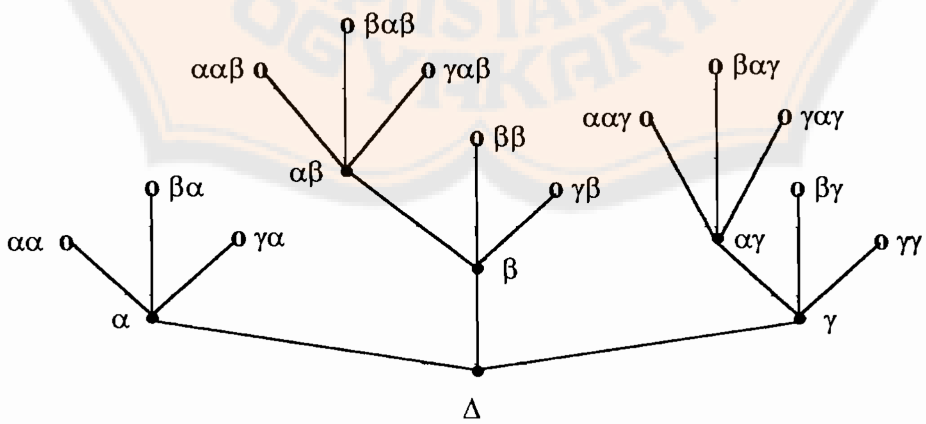
Penyelesaian.

Dengan cara yang sama seperti pada contoh sebelumnya, akan dihitung efek dari rangkaian input dengan panjang 0, 1, dan 2. Ternyata, dari sembilan rangkaian input dengan panjang 2, hanya ada dua rangkaian input yang memiliki efek yang berbeda dengan rangkaian input dengan panjang 0 ataupun 1. Rangkaian input tersebut adalah $\alpha\beta$ dan $\alpha\gamma$. Sehingga rangkaian input dengan panjang 3 yang kita periksa hanyalah $\alpha\alpha\beta$, $\beta\alpha\beta$, $\gamma\alpha\beta$, $\alpha\alpha\gamma$, $\beta\alpha\gamma$, dan $\gamma\alpha\gamma$, dari 27 rangkaian input yang mungkin. Hasil perhitungan efek dari berbagai rangkaian input ini diberikan pada tabel 4.12 berikut. Sedangkan pemeriksaan dengan menggunakan diagram pohon disajikan pada gambar 4.8.

Status awal	Status akhir dari berbagai rangkaian input									
	$h(\Delta)$	$h(\alpha)$	$h(\beta)$	$h(\gamma)$	$h(\alpha\alpha)$	$h(\alpha\beta)$	$h(\alpha\gamma)$	$h(\beta\beta)$	$h(\beta\alpha)$	$h(\beta\gamma)$
s_1	s_1	s_2	s_2	s_3	s_1	s_1	s_3	s_2	s_2	s_3
s_2	s_2	s_1	s_2	s_3	s_2	s_1	s_3	s_2	s_2	s_3
s_3	s_3	s_3	s_3	s_2	s_3	s_3	s_1	s_3	s_3	s_2

Status awal	Status akhir								
	$h(\gamma\gamma)$	$h(\gamma\alpha)$	$h(\gamma\beta)$	$h(\alpha\alpha\beta)$	$h(\beta\alpha\beta)$	$h(\gamma\alpha\beta)$	$h(\alpha\alpha\gamma)$	$h(\beta\alpha\gamma)$	$h(\gamma\alpha\gamma)$
s_1	s_2	s_3	s_3	s_2	s_2	s_3	s_3	s_3	s_2
s_2	s_2	s_3	s_3	s_2	s_2	s_3	s_3	s_3	s_2
s_3	s_3	s_2	s_2	s_3	s_3	s_2	s_2	s_2	s_3

Tabel 4.12 Efek dari berbagai rangkaian input.



Gambar 4.8 Diagram pohon dari rangkaian input.

Jadi, monoid dari otomata pada contoh 4.1 memiliki enam elemen, yakni $[\Delta]$, $[\alpha]$, $[\beta]$, $[\gamma]$, $[\alpha\beta]$, dan $[\alpha\gamma]$. Tabel hasil operasi antar elemen-elemen dalam monoid ini diberikan pada tabel 4.13 di bawah ini.

o	$[\Delta]$	$[\alpha]$	$[\beta]$	$[\gamma]$	$[\alpha\beta]$	$[\alpha\gamma]$
$[\Delta]$	$[\Delta]$	$[\alpha]$	$[\beta]$	$[\gamma]$	$[\alpha\beta]$	$[\alpha\gamma]$
$[\alpha]$	$[\alpha]$	$[\Delta]$	$[\alpha\beta]$	$[\alpha\gamma]$	$[\beta]$	$[\gamma]$
$[\beta]$	$[\beta]$	$[\beta]$	$[\beta]$	$[\gamma]$	$[\beta]$	$[\gamma]$
$[\gamma]$	$[\gamma]$	$[\gamma]$	$[\gamma]$	$[\beta]$	$[\gamma]$	$[\beta]$
$[\alpha\beta]$	$[\alpha\beta]$	$[\alpha\beta]$	$[\alpha\beta]$	$[\alpha\gamma]$	$[\alpha\beta]$	$[\alpha\gamma]$
$[\alpha\gamma]$	$[\alpha\gamma]$	$[\alpha\gamma]$	$[\alpha\gamma]$	$[\alpha\beta]$	$[\alpha\gamma]$	$[\alpha\beta]$

Tabel 4.13 Hasil operasi antar elemen-elemen dalam monoid dari otomata.

BAB V

KESIMPULAN

Monoid (M,#) adalah suatu himpunan M yang tidak kosong bersama operasi "#", yang memuat elemen identitas, di mana operasi pada himpunan M tersebut bersifat tertutup dan asosiatif. Dengan demikian setiap grup adalah monoid. Gagasan-gagasan yang ada pada monoid antara lain submonoid, monoid komutatif, monoid siklis, homomorfisma monoid, monoid bebas, dan monoid faktor. Grup abelian adalah monoid komutatif. Setiap submonoid adalah monoid, selain itu jika (H,#) subgrup dari grup (G,#) maka (H,#) juga submonoid dari monoid (G,#). Dan setiap grup siklis berhingga adalah monoid siklis.

Otomata status berhingga memuat himpunan status yang berhingga, himpunan input, dan fungsi transisi yang menyatakan bagaimana input mengubah status. Suatu otomata dengan n status, rangkaian inputnya paling banyak memberikan n^n efek yang berbeda. Karena banyaknya rangkaian input tak berhingga, maka ada kemungkinan suatu rangkaian input memiliki efek yang sama dengan rangkaian input lainnya, yang tidak dapat dibedakan oleh otomata. Dengan mendefinisikan suatu relasi kongruensi pada monoid bebas yang merupakan himpunan rangkaian input pada otomata tersebut, maka akan diperoleh monoid faktor yang menyatakan kemampuan otomata dalam menanggapi rangkaian input yang diberikan, berkaitan dengan banyaknya efek yang dimilikinya.

DAFTAR PUSTAKA

Crouch, Ralph; Beckman, David, 1966, *Fundamental Mathematical Structures: Algebraic System*, Illinois: Scoot, Foresman and Company.

Durbin, John R., 1985, *Modern Algebra, An Introduction*, 2nd ed, New York: John Wiley & Sons, Inc..

Fraleigh, John B., 1989, *A First Course in Abstract Algebra*, 4th ed, Massachusetts: Addison-Wesley Publishing Company.

Gilbert, William J., 1976, *Modern Algebra with Applications*, New York: John Wiley & Sons, Inc..

Hungerford, Thomas W., 1974, *Graduate Texts in Mathematics: Algebra*, New York: Springer-Verlag.

Kolman, B.; Busby, R.C., 1987, *Discrete Mathematical Structures for Computer Science*, 2nd ed, New Jersey: Prentice-Hall.

Lidl, Rudolf; Pilz, Gunter, 1998, *Applied Abstract Algebra*, 2nd ed, New York: Springer-Verlag.

Marpaung, Y., 1990, *Struktur Aljabar I*, Edisi Revisi, Yogyakarta: IKIP Sanata Dharma.

Moore, John T., 1962, *Elements of Abstract Algebra*, 2nd ed, New York: The Macmillan Company.

Narayan, Shanti, 1979, *A Text Book of Modern Abstract Algebra*, 6th revised ed, New Delhi: S. Chand & Company Ltd.

Utdirartatmo, Firrar, 2001, *Teori Bahasa dan Otomata*, Yogyakarta: J & J Learning.

White Law, T.A., 1995, *Introduction to Abstract Algebra*, 3rd ed, Glasgow: Blackie Academic & Professional.