UNIVERSITAS INDONESIA

KARAKTER MATRIKS DARI ENDOMORFISMA SEBAGAI AUTOMORFISMA PADA GRUP HINGGA KOMUTATIF

SKRIPSI

CITRA NATALIA
0806325466

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
PROGRAM STUDI SARJANA MATEMATIKA
DEPOK
JUNI 2012

UNIVERSITAS INDONESIA

KARAKTER MATRIKS DARI ENDOMORFISMA SEBAGAI AUTOMORFISMA PADA GRUP HINGGA KOMUTATIF

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar sarjana sains

CITRA NATALIA
0806325466

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
PROGRAM STUDI SARJANA MATEMATIKA

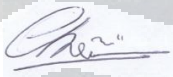
DEPOK
JUNI 2012

HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri,

dan semua sumber baik yang dikutip maupun dirujuk

telah saya nyatakan dengan benar.

Nama	: Citra Natalia
NPM	: 0806325466
Tanda Tangan	: 
Tanggal	: 14 Juni 2012

HALAMAN PENGESAHAN

Skripsi ini diajukan oleh

Nama	:	Citra Natalia
NPM	:	0806325466
Program Studi	:	Sarjana Matematika
Judul Skripsi	:	Karakter Matriks dari Endomorfisma sebagai Automorfisma pada Grup Hingga Komutatif

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Sains pada Program Studi S1 Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Indonesia

DEWAN PENGUJI

Pembimbing I	: Dra. Nora Hariadi, M.Si	(	)
Penguji I	: Dr. Hengki Tasman	(	)
Penguji II	: Arie Wibowo, M.Si	(	)
Penguji III	: Rahmi Rusin S.Si.,M.Sc.Tech	(	)

Ditetapkan di : Depok
Tanggal : 14 Juni 2012

KATA PENGANTAR

Puji syukur kepada Tuhan Yesus Kristus, atas segala hikmat dan kasih penyertaan yang telah diberikan sehingga penulis dapat menyelesaikan tugas akhir ini. Penulis sadar bahwa penyelesaian tugas akhir ini tidak terlepas dari bantuan dan dukungan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis ingin mengucapkan terima kasih kepada pihak-pihak yang telah berjasa dalam penulisan tugas akhir ini maupun selama penulis kuliah. Ucapan terima kasih penulis haturkan kepada:

1. Ibu Dra. Nora Hariadi, M.Si., selaku dosen pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan penulis dalam penyusunan skripsi ini.
2. Segenap dosen yang telah memberikan ilmunya selama 4 tahun ini, terutama Ibu Dr. Sri Mardiyati selaku Pembimbing Akademis saya.
3. Bapak Dr.Yudi Satria,M.T selaku Ketua Departemen, Ibu Rahmi Rusin, S.Si, M.Sc.Tech selaku Sekretaris Departemen, dan Ibu Dr. Dian Lestari selaku Koordinator Pendidikan yang telah banyak membantu proses penyelesaian tugas akhir ini.
4. Seluruh karyawan (Mbak Santi, Pak Saliman, Pak Salman, Pak Wawan, Mbak Via) di Departemen Matematika UI atas bantuan yang telah diberikan selama penulis kuliah sampai penulis menyelesaikan tugas akhir.
5. Keluarga penulis, Ayahanda Eddy Manullang, Ibunda Liana Setiadharma, Abang Miko, Kak Sondang, Kak Tita, dan segenap keluarga besar, Uda Hasahatan, yang telah banyak membantu selama kuliah baik secara finansial maupun doa.
6. Kak Ajat Adriansyah, S.Si., yang sangat membantu dalam membimbing penulis dari awal pengerjaan skripsi hingga akhir.
7. Sahabat penulis, Nita Astuti, Gayatri Bagawanti, Agnes yang telah menemani melewati masa suka dan duka selama kuliah.
8. Teman satu bimbingan, Yulial dan Hendri yang banyak membantu melewati masa-masa sulit dalam pengerjaan skripsi.

9. Seluruh teman-teman angkatan 2008 : Siwi, Uci D, Resti, Olin, Fani, Emi, Eka, May, Nisah, Ifah, Maul,Wulan, Ade,Sita, Risya, Dila, Kiki, Tuti, Numa, Cindy, Adi, Arif, Hindun, Andi, Dheni, Asri, Dewe, Dian, Janu, Nora, Uci L, Vika, Dea, Lutfah, Nadia, Bowo, Umbu, Arman, AW, Arkis, Maimun, Puput, Dhanis terimakasih atas segala kebersamaannya selama masa kuliah sampai saat ini.
10. Semua teman-teman di Matematika UI: Ka Tika, Ka Oza, Martin, Ka Nora, Ka Ayat, Eja, Luthfir, Putri, Sofi, Revi, Anna serta senior dan junior lainnya angkatan 2005, 2006, 2007, 2009, 2010 dan 2011, terima kasih atas semangat dan dukungannya.

Penulis juga ingin mengucapkan terima kasih kepada seluruh pihak yang tidak dapat disebutkan satu per satu, yang telah membantu dalam penyusunan skripsi ini. Akhir kata, penulis mohon maaf jika terdapat kesalahan atau kekurangan dalam skripsi ini. Penulis berharap semoga skripsi ini bermanfaat bagi pembaca.

Penulis

2012

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Indonesia, saya yang bertanda tangan di bawah ini:

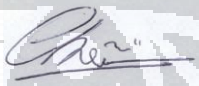
Nama	: Citra Natalia
NPM	: 0806325466
Program Studi	: Sarjana Matematika
Departemen	: Matematika
Fakultas	: Matematika dan Ilmu Pengetahuan Alam
Jenis karya	: Skripsi

demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul :
Karakter Matriks dari Endomorfisma sebagai Automorfisma pada Grup Hingga Komutatif.

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Indonesia berhak menyimpan, mengalihmedia/format-kan, mengelola dalam bentuk pangkalan data (database), merawat, dan memublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Depok
Pada tanggal : 14 Juni 2012
Yang menyatakan



(Citra Natalia)

ABSTRAK

Nama : Citra Natalia
Program Studi : Matematika
Judul : Karakter Matriks dari Endomorfisma sebagai Automorfisma pada Grup Hingga Komutatif

Misalkan H_p menyatakan grup hingga komutatif dengan order p bilangan prima. Karena himpunan automorfisma grup adalah himpunan bagian dari himpunan endomorfisma grup, maka mempelajari automorfisma grup H_p dapat melalui endomorfisma grup H_p. Dengan adanya pemetaan homomorfisma surjektif dari gelanggang matriks ke gelanggang endomorfisma H_p, maka setiap endomorfisma H_p akan memiliki padanan suatu matriks. Dalam skripsi ini dibahas tentang karakter matriks dari endomorfisma H_p yang dapat memberikan automorfisma H_p.

Kata kunci : Grup hingga komutatif, automorfisma grup, endomorfisma grup.
x+33 halaman : -
Daftar Pustaka : 8 (1907-2007)

ABSTRACT

Name : Citra Natalia
Major : Mathematics
Title : Character of Matrix Endomorphism as an Automorphism of Finite Abelian Group.

Let H_p denotes a finite commutative group of order p where p is a prime number. Since automorphism group is a subset of endomorphism group, then it is possible to study the group automorphism of H_p by analyzing the group endomorphism of H_p. With the existence of a surjective homomorphism mapping from the ring of matrices to the endomorphism ring of H_p, then each element in the endomorphism ring of H_p will have a matrix associated to it. This mini thesis will discuss the characteristic of the matrix of the endomorphism H_p that gives the automorphism of H_p.

Keywords : Finite abelian group, group automorphism, group endomorphism.
x+33 pages : -
Bibliography : 8 (1907-2007)

DAFTAR ISI

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Dalam Teorema Fundamental dari Grup Hingga Komutatif, dikatakan bahwa setiap grup hingga yang komutatif dapat dinyatakan sebagai hasil kali langsung dari grup-grup siklik (Herstein, 1996). Misalkan G adalah grup hingga yang komutatif, maka menurut Teorema Fundamental, G dapat ditulis sebagai $G = H_{p_1} \times ... \times H_{p_k}$ dimana $H_{p_j} = T_{p_j}^1 \times T_{p_j}^2 \times \cdots T_{p_j}^n$ dengan $T_{p_j}^l$ adalah grup siklik dengan order $p_j^{e_l}$, p_j bilangan prima (Hillar & Rhea, 2007). H_{p_j} adalah grup-grup hingga komutatif dengan order yang saling relatif prima. Dengan kata lain, Teorema Fundamental menyatakan bahwa grup hingga komutatif G dapat dinyatakan sebagai hasil kali langsung dari grup berorder pangkat dari bilangan prima p_j yaitu H_{p_j}.

Automorfisma dari suatu grup merupakan isomorfisma yang memetakan sebuah grup ke dirinya sendiri. Untuk suatu grup hingga, automorfisma dari grup tersebut memiliki order yang terbatas (Horosevskii, 1974). Ranum pada penelitiannya telah mencoba untuk memberikan karakter pada automorfisma dari grup hingga komutatif G (Ranum, 1907). Karena G dapat dinyatakan sebagai hasil kali langsung dari H_{p_j}, maka automorfisma dari G dapat dinyatakan sebagai automorfisma dari hasil kali langsung H_{p_j}, yaitu $Aut(G) = Aut\left(H_{p_1} \times ... \times H_{p_k}\right)$. Lebih lanjut, karena automorfisma dari hasil kali langsung dua buah grup yang ordernya saling relatif prima isomorfik dengan hasil kali langsung dari masing-masing automorfisma grup tersebut (Hillar & Rhea, 2007), maka automorfisma G akan isomorfik dengan hasil kali langsung dari automorfisma H_{p_j}, $Aut(G) \cong Aut\left(H_{p_1}\right) \times \cdots \times Aut\left(H_{p_k}\right)$. Dengan demikian untuk mempelajari automorfisma G dapat melalui automorfisma H_{p_j}.

Karena himpunan automorfisma suatu grup merupakan himpunan bagian dari himpunan endomorfisma, maka untuk melihat karakter dari himpunan

automorfisma H_{p_j} dapat melalui gelanggang endomorfisma H_{p_j} yang dinotasikan dengan $End(H_{p_j})$. Melalui sebuah pemetaan homomorfisma yang memetakan suatu himpunan matriks ke $End(H_{p_j})$, dapat ditunjukkan setiap elemen di $End(H_{p_j})$ memiliki padanan matriks. Padanan matriks yang berkoresponden dengan elemen-elemen $End(H_{p_j})$ dan memenuhi sifat tertentu akan memberikan automorfisma pada H_{p_j}.

1.2 Rumusan Masalah dan Ruang Lingkup

Berdasarkan latar belakang diatas permasalahan tugas akhir ini adalah menentukan karakter dari matriks endomorfisma H_{p_j} yang memberikan automorfisma H_{p_j}. Ruang lingkup dari permasalahan ini adalah grup yang ditelaah adalah grup hingga komutatif H_p dimana $H_p = \mathbb{Z}/p^{e_1}\mathbb{Z} \times ... \times \mathbb{Z}/p^{e_n}\mathbb{Z}$ untuk p adalah bilangan prima, berlaku $1 \leq e_1 \leq \cdots \leq e_n$, dan e_i adalah bilangan bulat positif yang bernilai unik untuk suatu dekomposisi.

1.3 Metode Penelitian

Penelitian dilakukan dengan studi literatur.

1.4 Tujuan Penulisan

Tujuan penulisan tugas akhir ini adalah mempelajari karakter dari matriks suatu $End(H_p)$ yang memberikan automorfisma H_p.

BAB 2
LANDASAN TEORI

Pada bab ini dibahas beberapa teori dasar yang diperlukan untuk mempelajari karakter matriks bagi gelanggang endomorfisma dari grup hingga komutatif. Materi yang dibahas adalah mengenai teori bilangan, pemetaan, grup, dan gelanggang.

2.1 Teori Bilangan

Sebuah bilangan bulat b dikatakan **habis dibagi** oleh bilangan bulat $a \neq 0$, dinotasikan dengan simbol $a|b$, jika terdapat sebuah bilangan bulat c sedemikan sehingga $b = ac$. Dua buah bilangan bulat a dan b, dimana salah satunya tidak sama dengan nol, memiliki **faktor persekutuan terbesar** d, yang dinotasikan dengan $FPB(a, b) = d$ jika memenuhi dua kondisi. Kondisi pertama adalah d habis membagi a dan d habis membagi b. Kondisi kedua adalah jika terdapat c dimana c habis membagi a dan c habis membagi b maka $c \leq d$ (Burton, 2002).

Misalkan a dan b adalah bilangan bulat yang tidak sama dengan nol, maka a dan b dikatakan saling relatif prima jika $FPB(a, b) = 1$ (Burton, 2002). Berikut lemma yang menunjukkan sifat dari dua bilangan bulat yang saling relatif prima.

Lemma 2.1.1 Misalkan a dan b adalah dua buah bilangan bulat yang tidak sama dengan nol. a dan b dikatakan saling relatif prima jika dan hanya jika terdapat bilangan bulat x dan y sedemikian sehingga $1 = ax + by$.
(Burton, 2002)

Definisi 2.1.2 Misalkan n adalah bilangan bulat positif. Dua bilangan bulat a dan b dikatakan kongruen modulo n, yang disimbolkan sebagai $a \equiv b (\mathrm{mod}\ n)$, jika n habis membagi $a - b$ atau $a - b = kn$ untuk suatu bilangan bulat k.
(Burton, 2002)

Himpunan bilangan bulat a yang memenuhi $a \equiv b(\mathrm{mod}\, n)$, dinotasikan $\bar{a}$, untuk suatu bilangan bulat b dan bilangan bulat positif n adalah $\bar{a} = \{a \in \mathbb{Z} : a \equiv b \pmod{n}\}$.

Contoh 2.1.3 Misalkan untuk $n = 5$, maka

$$3 \equiv 23(\mathrm{mod}\ 5) \qquad -4 \equiv 21(\mathrm{mod}\ 5) \qquad -17 \equiv -12(\mathrm{mod}\ 5)$$

Sifat 2.1.4 Misalkan untuk $n > 1$ dan a, b, c, d adalah bilangan bulat sembarang, maka bilangan bulat ini memenuhi sifat-sifat

(a) $a \equiv a(\mathrm{mod}\, n)$.

(b) Jika $a \equiv b(\mathrm{mod}\, n)$, maka $b \equiv a(\mathrm{mod}\, n)$.

(c) Jika $a \equiv b(\mathrm{mod}\, n)$ dan $b \equiv c(\mathrm{mod}\, n)$, maka $a \equiv c(\mathrm{mod}\, n)$.

(d) Jika $a \equiv b(\mathrm{mod}\, n)$ dan $c \equiv d(\mathrm{mod}\, n)$, maka $a + c \equiv b + d \pmod{n}$ dan $ac \equiv bd \pmod{n}$.

(e) Jika $a \equiv b(\mathrm{mod}\, n)$, maka $a + c \equiv b + c \pmod{n}$ dan $ac \equiv bc \pmod{n}$.

(f) Jika $a \equiv b(\mathrm{mod}\, n)$, maka $a^k \equiv b^k(\mathrm{mod}\, n)$ untuk suatu bilangan bulat positif k.

(Burton, 2002)

2.2 Pemetaan

Misalkan terdapat dua himpunan S dan T. Pemetaan f dari S ke T adalah sebuah aturan yang memasangkan tiap elemen di S dengan tepat satu elemen di T. Pemetaan f dikatakan **surjektif** atau pada, jika untuk setiap t di T terdapat s di S sedemikian sehingga $t = f(s)$. Pemetaan f dikatakan **injektif** atau satu-satu jika untuk s_1, s_2 di S dimana berlaku $f(s_1) = f(s_2)$, maka $s_1 = s_2$. Pemetaan yang memenuhi sifat surjektif dan injektif disebut sebagai pemetaan **bijektif** .
Pemetaan dari suatu himpunan T ke T disebut sebagai **pemetaan identitas**, i_T, jika memenuhi $i_T(x) = x$ untuk setiap x di T.

Misalkan f adalah pemetaan dari S ke T. **Invers** dari f, yang dinotasikan dengan f^{-1}, adalah pemetaan dari T ke S sedemikian sehingga memenuhi $f \circ f^{-1} = i_T$ dan $f^{-1} \circ f = i_S$ dimana i_T dan i_S adalah pemetaan identitas di T dan di S. Berikut lemma yang menunjukkan keterkaitan antara pemetaan bijektif dengan invers dari pemetaan tersebut.

Lemma 2.2.1 Pemetaan $f: S \to T$ adalah pemetaan bijektif jika dan hanya jika terdapat $f^{-1}: T \to S$ yang memenuhi $f \circ f^{-1} = i_T$ dan $f^{-1} \circ f = i_S$ dimana i_T dan i_S masing-masing adalah pemetaan identitas dari T dan S.
(Herstein, 1996)

Bukti. Misalkan untuk suatu pemetaan $f: S \to T$ terdapat $f^{-1}: T \to S$ yang memenuhi $f \circ f^{-1} = i_T$ dan $f^{-1} \circ f = i_S$ dimana i_T dan i_S adalah pemetaan identitas dari T dan S, maka akan dibuktikan f pemetaan bijektif. Pertama akan ditunjukkan f adalah pemetaan injektif. Misalkan $f(a) = f(b)$ untuk $a, b \in S$, maka,

$$\begin{aligned} a &= i_S(a) \\ &= (f^{-1} \circ f)(a) \\ &= f^{-1}\big(f(a)\big) \\ &= f^{-1}\big(f(b)\big) \\ &= i_S(b) = b. \end{aligned}$$

Dengan demikian, untuk $f(a) = f(b)$ maka $a = b$. Jadi terbukti f adalah pemetaan injektif.

Kemudian akan dibuktikan f adalah pemetaan surjektif. Misalkan t adalah sembarang elemen di T. Karena terdapat pemetaan $f^{-1}: T \to S$, dimana $f^{-1}(t) = s \in S$ maka,

$$\begin{aligned} t &= i_T(t) \\ &= f \circ f^{-1}(t) \\ &= f\big(f^{-1}(t)\big) \\ &= f(s). \end{aligned}$$

Dengan demikian terbukti f adalah pemetaan surjektif. Jadi terbukti f adalah pemetaan bijektif.

Sebaliknya akan dibuktikan jika $f: S \to T$ merupakan pemetaan bijektif maka terdapat pemetaan $f^{-1}: T \to S$ yang memenuhi $f \circ f^{-1} = i_T$ dan $f^{-1} \circ f = i_S$ dimana i_T dan i_S adalah pemetaan identitas dari T dan S. Karena f surjektif, untuk sembarang $t \in T$ terdapat $s_t \in S$ sedemikian sehingga $f(s_t) = t$. Definisikan pemetaan $g: T \to S$ yang memenuhi untuk setiap $t \in T$ maka $g(t) = s_t$. Akan dibuktikan bahwa pemetaan g adalah invers dari dari f. Pertama akan ditunjukkan g terdefinisi dengan baik. Misalkan $t_1, t_2 \in T$ dimana $t_1 = t_2$, serta $g(t_1) = s_{t_1}$ dan $g(t_2) = s_{t_2}$. Karena f injektif dan $f(s_{t_1}) = t_1 = t_2 = f(s_{t_2})$, maka $s_{t_1} = s_{t_2}$ atau didapat $g(t_1) = g(t_2)$. Jadi terbukti g terdefinisi dengan baik.

Selanjutnya akan ditunjukkan bahwa pemetaan g adalah invers dari f yaitu memenuhi sifat $f \circ g = i_T$ dan $g \circ f = i_S$. Ambil $t \in T$. Berdasarkan definisi s_t, yaitu $f(s_t) = t$ dan $g(t) = s_t$ diperoleh $f(g(t)) = f(s_t) = t$, sedemikian sehingga $f \circ g = i_T$. Ambil $s \in S$. Karena $f(s_t) = t = f(s)$ dan f injektif maka $s = s_t$. Karena $g(t) = s_t$ dan $s = s_t$, akibatnya $g(f(s)) = g(t) = s_t = s$ atau $g \circ f = i_S$. Karena $g: T \to S$ terdefinisi dengan baik dan memenuhi $g \circ f = i_S$ dan $f \circ g = i_T$ maka g adalah invers dari f dan ditulis sebagai $g = f^{-1}$.■

2.3 Grup

Grup adalah suatu himpunan yang tidak kosong, dimana didalamnya didefinisikan suatu operasi biner yang memenuhi beberapa sifat tertentu. Berikut definisi dan contoh dari grup.

Definisi 2.3.1 Misalkan G adalah himpunan tak kosong. G disebut **grup** jika di G didefinisikan suatu operasi biner $*$, sedemikian sehingga memenuhi keempat aksioma berikut:

(a) Jika $a, b \in G$ maka $a * b \in G$.

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

(c) Terdapat $e \in G$ sedemikian sehingga $a * e = e * a = a$ untuk setiap $a \in G$.

(d) Untuk setiap $a \in G$ terdapat $a^{-1} \in G$ sedemikian sehingga $a * a^{-1} = a^{-1} * a = e$.

(Herstein, 1996)

Contoh 2.3.2 Misalkan $A = \left\{\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}, \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}\right\}$ dan * merupakan operasi perkalian matriks. A merupakan suatu grup dengan $e = \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}; \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}^{-1} = \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$.

Apabila sebuah himpunan hanya memenuhi sifat tertutup dan asosiatif, maka himpunan tersebut disebut sebagai **semigrup**. Grup G dikatakan **grup komutatif** jika $a * b = b * a$ untuk setiap $a, b \in G$. Apabila banyak elemen di grup G hingga maka G disebut **grup hingga**. Banyaknya elemen dalam G disebut sebagai **order** dari G dan dinotasikan dengan $|G|$ (Herstein, 1996).

Definisi 2.3.3 Sebuah grup G dikatakan grup siklik jika terdapat $a \in G$ sedemikian sehingga untuk setiap $x \in G$ dapat dinyatakan sebagai $x = a^j$ untuk suatu bilangan bulat j. Elemen a disebut sebagai pembangkit untuk G.
(Herstein, 1996)

Misalkan terdapat subhimpunan tak kosong A dari grup G, dimana subhimpunan tersebut juga memenuhi keempat aksioma grup terhadap operasi yang sama yang didefinisikan di dalam G, maka subhimpunan A dikatakan sebagai **subgrup** dari G.

Definisi 2.3.4 Misalkan A adalah subgrup dari G dan $g \in G$. Himpunan $Ag = \{ag\ ;\ a \in A\}$ disebut sebagai koset kanan dari A di G dan himpunan $gA = \{ga\ ; a \in A\}$ disebut sebagai koset kiri dari A di G.
(Herstein, 1996)

Contoh 2.3.5 Misalkan $G = \mathbb{Z}$ suatu grup dengan operasi penjumlahan dan $A = 4\mathbb{Z}$ adalah subgrup dari G. Maka didapat himpunan koset kanan dan koset kiri sebagai berikut

$$Ag = 4\mathbb{Z} + g = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$$
$$gA = g + 4\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}.$$

Subgrup N dari grup G yang memenuhi $g^{-1}Ng \subseteq N$ untuk setiap $g \in G$, disebut sebagai **subgrup normal** di G. Peranan subgrup normal sangat penting dalam aljabar. Berikut salah satu peranan dari subgrup normal.

Definisi 2.3.6 Misalkan N adalah subgrup normal dari G. Grup faktor G oleh N, yang dinotasikan dengan G/N, adalah

$$G/N = \{[a] | \, a \in G\} = \{Na | \, a \in G\}$$

dengan operasi $[a][b] = [ab]$.
(Herstein, 1996)

Contoh 2.3.7 Misalkan $N = 3\mathbb{Z}$ adalah subgrup normal dari grup $G = \mathbb{Z}$, maka $\mathbb{Z}/3\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}\}$ adalah grup faktor $\mathbb{Z}$ oleh $3\mathbb{Z}$.

Berikutnya dibahas mengenai pemetaan homomorfisma pada grup.

Definisi 2.3.8 Misalkan G dan G' adalah grup. Pemetaan $\phi: G \to G'$ adalah homomorfisma jika memenuhi $\phi(ab) = \phi(a)\phi(b)$ untuk setiap $a, b \in G$.
(Herstein, 1996)

Contoh 2.3.9 Misalkan G adalah grup komutatif. Misalkan pula pemetaan $\phi: G \to G$ didefinisikan sebagai $\phi(a) = a^2$ untuk setiap $a \in G$. Untuk $a, b \in G$ berlaku $\phi(ab) = (ab)^2 = a^2b^2 = \phi(a)\phi(b)$. Maka ϕ adalah pemetaan homomorfisma dari G ke dirinya sendiri.

Homomorfisma ϕ dikatakan **isomorfisma** jika ϕ adalah homomorfisma yang bijektif. Homomorfisma yang memetakan G ke dirinya sendiri disebut

endomorfisma. Sedangkan sebuah isomorfisma yang memetakan G ke dirinya sendiri adalah **automorfisma** (Herstein, 1996). Pada suatu homomorfisma dikenal himpunan yang dinamakan kernel. Berikut adalah definisi dari kernel suatu homomorfisma.

Definisi 2.3.10 Jika ϕ adalah suatu homomorfisma dari grup G ke grup G', maka kernel dari ϕ adalah

$$\ker \phi = \{a \in G \mid \phi(a) = e'\}$$

dimana e' adalah elemen identitas di G'.
(Herstein, 1996)

2.4 Gelanggang

Gelanggang adalah himpunan yang tidak kosong dimana pada himpunan ini didefinisikan dua buah operasi, yaitu penjumlahan dan perkalian sedemikian sehingga memenuhi beberapa aksioma. Berikut adalah definisi serta contoh dari gelanggang.

Definisi 2.4.1 Misalkan R adalah himpunan tidak kosong. R disebut gelanggang jika didalam R terdapat dua operasi $+$ dan $\cdot$ sedemikian sehingga membentuk grup komutatif terhadap operasi penjumlahan, semigrup terhadap operasi perkalian dan memenuhi sifat distributif terhadap operasi penjumlahan dan perkalian.
(Lang, 2002)

Contoh 2.4.2 Misalkan $R = \{(a_{ij}) \in \mathbb{Z}^{2\times 2}\}$ adalah himpunan matriks dengan entri di $\mathbb{Z}$. Himpunan R akan membentuk gelanggang terhadap operasi penjumlahan dan perkalian matriks.

Gelanggang yang memiliki elemen identitas terhadap operasi perkalian dikatakan sebagai **gelanggang dengan unit**. Sedangkan gelanggang yang memenuhi sifat komutatif terhadap operasi perkalian disebut sebagai **gelanggang**

komutatif. Apabila setiap elemen $a \neq 0$ dalam gelanggang memiliki invers terhadap operasi perkalian, maka gelanggang tersebut disebut **gelanggang hasil bagi** (Herstein, 1996).

Sama halnya dengan grup, pada bagian ini juga akan dibahas homomorfisma gelanggang. Berikut adalah definisi dari homomorfisma gelanggang serta kernel dari homomorfisma gelanggang.

Definisi 2.4.3 Misalkan R dan R' adalah gelanggang. Pemetaan $\varphi: R \to R'$ adalah homomorfisma jika $\varphi(a+b) = \varphi(a) + \varphi(b)$ dan $\varphi(ab) = \varphi(a)\varphi(b)$ untuk setiap $a, b \in R$.
(Herstein, 1996)

Definisi 2.4.4 Misalkan φ adalah sebuah homomorfisma gelanggang dari R pada R' maka kernel dari φ adalah

$$\ker \varphi = \{x \in R \mid \varphi(x) = 0\}$$

dimana 0 adalah elemen identitas di R'.
(Herstein, 1996)

Misalkan G adalah grup komutatif terhadap operasi penjumlahan. Definisikan $End(G)$ adalah himpunan endomorfisma dari G ke G dengan operasi penjumlahan dan perkalian sebagai berikut

$$(f+g)(x) = f(x) + g(x) \text{ dan } (fg)(x) = f\big(g(x)\big)$$

untuk setiap $f, g \in End(G)$ dan $x \in G$. Himpunan $End(G)$ dengan dua operasi biner ini membentuk gelanggang.
(Bhattacharya, Jain, & Nagpul, 1994)

Contoh 2.4.5 Misalkan $G = \mathbb{Z}/6\mathbb{Z}$ adalah grup komutatif terhadap operasi penjumlahan modulo 6. Himpunan pemetaan endomorfisma dari G ke G akan membentuk gelanggang terhadap operasi penjumlahan dan komposisi fungsi.

Gelanggang yang elemen-elemennya membentuk grup komutatif terhadap operasi perkalian disebut sebagai lapangan. Berikut definisi lengkap dari lapangan.

Definisi 2.4.6 Misalkan F adalah himpunan tidak kosong. F disebut lapangan jika didalam F terdapat dua operasi $+$ dan $\cdot$ sedemikian sehingga membentuk gelanggang hasil bagi yang komutatif.
(Herstein, 1996)

Sebuah lapangan F dikatakan memiliki karakteristik $p \neq 0$ jika untuk sebuah bilangan bulat p, $px = 0$ untuk setiap $x \in F$, dan tidak ada bilangan bulat positif yang lebih kecil dari p yang memenuhi sifat ini (Herstein, 1996).

Contoh 2.4.7 Misalkan $F = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ adalah lapangan terhadap operasi penjumlahan dan perkalian modulo. Karena berlaku $5\bar{x} = \bar{0}$ untuk setiap $\bar{x} \in F$, maka lapangan F memiliki karakteristik $p = 5$.

Berikut didefinisikan himpunan matriks invertibel dimana entri-entrinya merupakan elemen dari suatu lapangan.

Definisi 2.4.8 Himpunan matriks berukuran $n \times n$ yang invertibel dengan entri di suatu lapangan F yang memiliki order p, membentuk grup dengan operasi perkalian matriks, dan dilambangkan dengan $GL_n(F_p)$.
(Lang, 2002)

Contoh 2.4.9 Misalkan terdapat lapangan F, dimana $F = \{\bar{0}, \bar{1}\}$. Dibentuk himpunan G yang anggotanya adalah matriks-matriks invertibel yang entri-entrinya adalah elemen dari F

$$G = \left\{ \begin{bmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{bmatrix}, \begin{bmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{0} \end{bmatrix}, \begin{bmatrix} \bar{1} & \bar{1} \\ \bar{1} & \bar{0} \end{bmatrix}, \begin{bmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{1} \end{bmatrix}, \begin{bmatrix} \bar{1} & \bar{0} \\ \bar{1} & \bar{1} \end{bmatrix}, \begin{bmatrix} \bar{1} & \bar{1} \\ \bar{0} & \bar{1} \end{bmatrix} \right\}$$

maka G akan membentuk grup terhadap perkalian matriks.

BAB 3
KARAKTER MATRIKS ENDOMORFISMA GRUP HINGGA KOMUTATIF SEBAGAI AUTOMORFISMA

Seperti yang sudah disebutkan pada Bab 1, H_p adalah grup hingga komutatif. Menurut Teorema Fundametal, H_p dapat dinyatakan sebagai hasil kali langsung dari grup-grup siklik yaitu

$$H_p = \mathbb{Z}/p^{e_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{e_n}\mathbb{Z}$$

untuk p adalah bilangan prima dan $1 \leq e_1 \leq \cdots \leq e_n$ dengan e_i adalah bilangan bulat positif yang bernilai unik untuk suatu dekomposisi. Pada bab ini dibahas tentang gelanggang endomorfisma dari H_p, serta sifat matriks endomorfisma dari H_p yang memenuhi automorfisma H_p.

3.1 Gelanggang Endomorfisma dari H_p

Definisi 3.1.1 Himpunan matriks R_p, adalah
$R_p = \{(a_{ij}) \in \mathbb{Z}^{n\times n}; p^{e_i - e_j} | a_{ij}$ untuk setiap i dan j yang memenuhi $1 \leq j \leq i \leq n\}$.
(Hillar & Rhea, 2007)

Berikut diberikan contoh anggota-anggota di R_p untuk $p = 2$.

Contoh 3.1.2 Misalkan $p = 2, n = 3, e_1 = 1, e_2 = 2, e_3 = 4$. Karena memenuhi $p^{e_i - e_j} | a_{ij}$ untuk $1 \leq j \leq i \leq n$ maka didapat

$$p^{e_1 - e_1} | a_{11} = 2^0 | a_{11} \leftrightarrow a_{11} = b_{11}$$
$$p^{e_2 - e_1} | a_{21} = 2^1 | a_{21} \leftrightarrow a_{21} = 2b_{21}$$
$$p^{e_2 - e_2} | a_{22} = 2^0 | a_{22} \leftrightarrow a_{22} = b_{22}$$
$$p^{e_3 - e_1} | a_{31} = 2^3 | a_{31} \leftrightarrow a_{31} = 8b_{31}$$
$$p^{e_3 - e_2} | a_{32} = 2^2 | a_{32} \leftrightarrow a_{32} = 4b_{32}$$
$$p^{e_3 - e_3} | a_{33} = 2^0 | a_{33} \leftrightarrow a_{33} = b_{33}$$

dimana $b_{ij} \in \mathbb{Z}$. Dengan demikian didapat himpunan

$$R_2: \left\{ \begin{bmatrix} b_{11} & b_{12} & b_{13} \\ 2b_{21} & b_{22} & b_{23} \\ 8b_{31} & 4b_{32} & b_{33} \end{bmatrix}; b_{ij} \in \mathbb{Z} \right\}.$$

Pada lemma berikut ditunjukkan bahwa setiap matriks yang merupakan elemen dari R_p dapat didekomposisi.

Lemma 3.1.3 $A \in R_p$ jika dan hanya jika A dapat dinyatakan sebagai dekomposisi $A = PA'P^{-1}$ untuk matriks diagonal P, dimana P =diagonal$(p^{e_1}, \dots, p^{e_n})$ dan $A' \in \mathbb{Z}^{n \times n}$.

Bukti. Pertama, misalkan $A \in R_p$, akan dibuktikan terdapat matriks $A' \in \mathbb{Z}^{n \times n}$ sedemikian sehingga $A = PA'P^{-1}$ dimana $P =$ diagonal$(p^{e_1}, \dots, p^{e_n})$. Karena $A \in R_p$ dengan $A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}$ maka berlaku $p^{e_i - e_j} | a_{ij}$ untuk $i \geq j$.

Akibatnya terdapat $b_{ij} \in \mathbb{Z}$ sedemikian sehingga $a_{ij} = b_{ij} p^{e_i - e_j}$ untuk $i \geq j$. Bentuk matriks $A' = (b_{ij}) \in \mathbb{Z}^{n \times n}$ dan P =diagonal$(p^{e_1}, \dots, p^{e_n})$, maka dapat ditunjukkan bahwa $A = PA'P^{-1}$ atau $AP = PA'$.

$$AP = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21}p^{e_2 - e_1} & b_{22} & & b_{2n} \\ b_{31}p^{e_3 - e_1} & b_{32}p^{e_3 - e_2} & \ddots & b_{3n} \\ \vdots & \vdots & & \vdots \\ b_{n1}p^{e_n - e_1} & b_{n2}p^{e_n - e_2} & \cdots & b_{nn} \end{pmatrix} \begin{pmatrix} p^{e_1} & 0 & & 0 \\ 0 & p^{e_2} & & 0 \\ 0 & 0 & \ddots & \vdots \\ \vdots & \vdots & & 0 \\ 0 & \cdots & 0 & p^{e_n} \end{pmatrix}$$

$$= \begin{pmatrix} b_{11}p^{e_1} & b_{12}p^{e_1} & \cdots & b_{1n}p^{e_1} \\ b_{21}p^{e_2} & b_{22}p^{e_2} & \cdots & b_{2n}p^{e_2} \\ \vdots & \vdots & & \vdots \\ b_{n1}p^{e_n} & b_{n2}p^{e_n} & \cdots & b_{nn}p^{e_n} \end{pmatrix}$$

$$= \begin{pmatrix} p^{e_1} & 0 & & 0 \\ 0 & p^{e_2} & & 0 \\ 0 & 0 & \ddots & \vdots \\ \vdots & \vdots & & 0 \\ 0 & \cdots & 0 & p^{e_n} \end{pmatrix} \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ & & \\ \vdots & & \vdots \\ & & \\ b_{n1} & \cdots & b_{nn} \end{pmatrix}$$

$$= PA'.$$

Jadi terbukti bahwa untuk setiap $A \in R_p$ dapat didekomposisi menjadi $A = PA'P^{-1}$ dengan $A' \in \mathbb{Z}^{n \times n}$ dan P =diagonal$(p^{e_1}, \dots, p^{e_n})$.

Sebaliknya akan dibuktikan, bahwa apabila terdapat matriks $A' \in \mathbb{Z}^{n\times n}$ dan matriks P =diagonal$(p^{e_1}, \dots, p^{e_n})$ sedemikian sehingga $PA'P^{-1} = A$ maka $A \in R_p$. Misalkan $A' = (b_{ij}) \in \mathbb{Z}^{n\times n}$, maka

$$PA'P^{-1}$$

$$= \begin{pmatrix} p^{e_1} & 0 & \dots & 0 \\ 0 & p^{e_2} & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \dots & 0 & p^{e_n} \end{pmatrix} \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \vdots & & \vdots \\ b_{n1} & \dots & b_{nn} \end{pmatrix} \begin{pmatrix} 1/p^{e_1} & 0 & \dots & 0 \\ 0 & 1/p^{e_2} & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \dots & 0 & 1/p^{e_n} \end{pmatrix}$$

$$= \begin{pmatrix} b_{11}p^{e_1} & \dots & b_{1n}p^{e_1} \\ \vdots & & \vdots \\ b_{n1}p^{e_n} & \dots & b_{nn}p^{e_n} \end{pmatrix} \begin{pmatrix} 1/p^{e_1} & 0 & \dots & 0 \\ 0 & 1/p^{e_2} & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \dots & 0 & 1/p^{e_n} \end{pmatrix}$$

$$= \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21}p^{e_2-e_1} & b_{22} & & b_{2n} \\ b_{31}p^{e_3-e_1} & b_{32}p^{e_3-e_2} & \ddots & b_{3n} \\ \vdots & \vdots & & \vdots \\ b_{n1}p^{e_n-e_1} & b_{n2}p^{e_n-e_2} & \dots & b_{nn} \end{pmatrix}.$$

Jadi

$$\begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21}p^{e_2-e_1} & b_{22} & & b_{2n} \\ b_{31}p^{e_3-e_1} & b_{32}p^{e_3-e_2} & \ddots & b_{3n} \\ \vdots & \vdots & & \vdots \\ b_{n1}p^{e_n-e_1} & b_{n2}p^{e_n-e_2} & \dots & b_{nn} \end{pmatrix} = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}.$$

Akibatnya $a_{ij} = b_{ij}p^{e_i-e_j}$ untuk $i \geq j$ dan $a_{ij} = b_{ij}$ untuk $i < j$. Dengan demikian berlaku $p^{e_i-e_j} | a_{ij}$ untuk $i \geq j$. Hal ini mengakibatkan $A = (a_{ij}) \in R_p$. ■

Dengan menggunakan Lemma 3.1.3, dapat ditunjukkan bahwa himpunan matriks R_p dengan operasi penjumlahan dan perkalian matriks membentuk gelanggang dengan unit.

Lemma 3.1.4 R_p membentuk gelanggang terhadap operasi penjumlahan dan perkalian matriks dan R_p yang memuat unit.

Bukti. Pertama akan dibuktikan R_p membentuk grup komutatif terhadap operasi penjumlahan matriks. Misalkan $A = (a_{ij}) \in R_p$ dan $C = (c_{ij}) \in R_p$, akan ditunjukkan R_p tertutup terhadap operasi penjumlahan matriks. Karena $A, C \in R_p$ maka

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} = \begin{pmatrix} b_{11} & \dots & b_{1n} \\ b_{21}p^{e_2-e_1} & \ddots & b_{2n} \\ \vdots & & \vdots \\ b_{n1}p^{e_n-e_1} & \dots & b_{nn} \end{pmatrix} \text{ dan}$$

$$C = \begin{pmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & & \vdots \\ c_{n1} & \cdots & c_{nn} \end{pmatrix} = \begin{pmatrix} d_{11} & \dots & d_{1n} \\ d_{21}p^{e_2-e_1} & \ddots & d_{2n} \\ \vdots & & \vdots \\ d_{n1}p^{e_n-e_1} & \dots & d_{nn} \end{pmatrix}$$

dengan $b_{ij}, d_{ij} \in \mathbb{Z}$.

$$A + C = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} + \begin{pmatrix} c_{11} & \cdots & c_{1n} \\ \vdots & & \vdots \\ c_{n1} & \cdots & c_{nn} \end{pmatrix}$$

$$= \begin{pmatrix} b_{11} & \dots & b_{1n} \\ b_{21}p^{e_2-e_1} & \ddots & b_{2n} \\ \vdots & & \vdots \\ b_{n1}p^{e_n-e_1} & \dots & b_{nn} \end{pmatrix} + \begin{pmatrix} d_{11} & \dots & d_{1n} \\ d_{21}p^{e_2-e_1} & \ddots & d_{2n} \\ \vdots & & \vdots \\ d_{n1}p^{e_n-e_1} & \dots & d_{nn} \end{pmatrix}$$

$$= \begin{pmatrix} b_{11} + d_{11} & \dots & b_{1n} + d_{1n} \\ (b_{21} + d_{21})p^{e_2-e_1} & \ddots & b_{2n} + d_{2n} \\ \vdots & & \vdots \\ (b_{n1} + d_{n1})p^{e_n-e_1} & \dots & b_{nn} + d_{nn} \end{pmatrix}.$$

Karena $A + C = \begin{pmatrix} a_{11} + c_{11} & \cdots & a_{1n} + c_{1n} \\ \vdots & & \vdots \\ a_{n1} + c_{n1} & \cdots & a_{nn} + c_{nn} \end{pmatrix}$ dengan demikian didapat

$$\begin{pmatrix} a_{11} + c_{11} & \cdots & a_{1n} + c_{1n} \\ \vdots & & \vdots \\ a_{n1} + c_{n1} & \cdots & a_{nn} + c_{nn} \end{pmatrix} = \begin{pmatrix} b_{11} + d_{11} & \dots & b_{1n} + d_{1n} \\ (b_{21} + d_{21})p^{e_2-e_1} & \ddots & b_{2n} + d_{2n} \\ \vdots & & \vdots \\ (b_{n1} + d_{n1})p^{e_n-e_1} & \dots & b_{nn} + d_{nn} \end{pmatrix}.$$

Karena $b_{ij} + d_{ij} \in \mathbb{Z}$ dan berlaku $p^{e_i-e_j} \big| (a_{ij} + c_{ij})$ maka $A + C \in R_p$. Jadi R_p tertutup terhadap operasi penjumlahan matriks.

Karena $p^{e_i-e_j} | 0$ untuk setiap i, j yang memenuhi $1 \leq j \leq i \leq n$ maka matriks 0 juga merupakan anggota R_p. Lebih lanjut karena berlaku $0 + A = A + 0 = A$ untuk setiap $A \in R_p$, maka matriks 0 merupakan identitas terhadap operasi

penjumlahan matriks di R_p. Berdasarkan sifat penjumlahan pada matriks maka sifat asosiatif dan komutatif berlaku juga di R_p, yaitu $(A+B)+C = A+(B+C)$ dan $A+B = B+A$ untuk $A, B, C \in R_p$. Dengan demikian, terbukti R_p merupakan grup komutatif terhadap operasi penjumlahan matriks.

Selanjutnya akan dibuktikan R_p tertutup terhadap operasi perkalian matriks. Misalkan $A, B \in R_p$. Berdasarkan Lemma 3.1.3, A dan B dapat dinyatakan sebagai $A = PA'P^{-1}$ dan $B = PB'P^{-1}$ untuk suatu $A', B' \in \mathbb{Z}^{n\times n}$ dan P =diagonal$(p^{e_1}, \dots, p^{e_n})$. Maka

$$\begin{aligned} AB &= (PA'P^{-1})(PB'P^{-1}) \\ &= PA'IB'P^{-1} \\ &= P(A'B')P^{-1}. \end{aligned}$$

Karena $A', B' \in \mathbb{Z}^{n\times n}$ dan AB dapat dinyatakan sebagai dekomposisi $P(A'B')P^{-1}$ maka menurut Lemma 3.1.3 $AB \in R_p$. Jadi terbukti R_p tertutup terhadap operasi perkalian matriks.

Berdasarkan sifat perkalian pada matriks berlaku sifat asosiatif pada R_p, yaitu $(A\cdot B)\cdot C = A\cdot(B\cdot C)$ untuk $A, B, C \in R_p$. Lebih lanjut, sifat distributif terhadap penjumlahan dan perkalian juga berlaku di R_p, yaitu $A\cdot(B+C) = A\cdot B + A\cdot C$ dan $(B+C)\cdot A = B\cdot A + C\cdot A$ untuk $A, B, C \in R_p$. Jadi terbukti R_p adalah gelanggang.

Selanjutnya akan ditunjukkan bahwa gelanggang R_p memuat unit dan unitnya adalah matriks identitas. Karena berlaku $p^{e_i-e_j}|1$ untuk $i = j$ dan $p^{e_i-e_j}|0$ untuk setiap i, j yang memenuhi $1 \le j < i \le n$, maka matriks identitas I adalah elemen R_p dan berlaku $IA = AI = A$ untuk setiap $A \in R_p$. Dengan demikian terbukti himpunan R_p membentuk gelanggang terhadap operasi penjumlahan dan perkalian matriks dan memuat unit yang berupa matriks identitas I.■

Sebelum pembahasan dilanjutkan, diberikan beberapa notasi yang nantinya digunakan. Misalkan $C_{p^{e_i}} = \mathbb{Z}/p^{e_i}\mathbb{Z}$ adalah grup siklik terhadap operasi penjumlahan modulo p^{e_i} dimana g_i adalah generator untuk $C_{p^{e_i}}$. Secara spesifik g_i dapat dilihat sebagai kelas $\overline{1} = \{x \in \mathbb{Z}; x \equiv 1 \pmod{p^{e_i}}\}$. Misalkan pula

$\overline{h_i} \in \mathbb{Z}/p^{e_i}\mathbb{Z}$ untuk $h_i \in \mathbb{Z}$, maka H_p dapat dinyatakan sebagai vektor kolom $\left(\overline{h_1}, \dots, \overline{h_n}\right)^T$.

Selanjutnya definisikan pemetaan π dari $\mathbb{Z}^n$ ke H_p dengan

$$\pi(h_1, \dots, h_n)^T = \left(\pi_1(h_1), \dots, \pi_n(h_n)\right)^T = \left(\overline{h_1}, \dots, \overline{h_n}\right)^T \quad \textbf{(3.1)}$$

dimana $\pi_i: \mathbb{Z} \to \mathbb{Z}/p^{e_i}\mathbb{Z}$. Pada Lemma 3.1.5 ditunjukkan bahwa pemetaan π ini adalah suatu homomorfisma grup.

Lemma 3.1.5 Pemetaan π: $\mathbb{Z}^n \to H_p$ dengan

$$\pi(h_1, \dots, h_n)^T = \left(\overline{h_1}, \dots, \overline{h_n}\right)^T$$

adalah suatu homomorfisma grup.

Bukti. Misalkan $(h_1, \dots, h_n)^T, (k_1, \dots, k_n)^T \in \mathbb{Z}^n$, maka

$$\begin{aligned}
\pi((h_1, \dots, h_n)^T + (k_1, \dots, k_n)^T) &= \pi(h_1 + k_1, \dots, h_n + k_n)^T \\
&= \left(\pi_1(h_1 + k_1), \dots, \pi_n(h_n + k_n)\right)^T \\
&= \left(\overline{h_1 + k_1}, \dots, \overline{h_1 + k_1}\right)^T \\
&= \left(\overline{h_1} + \overline{k_1}, \dots, \overline{h_n} + \overline{k_n}\right)^T \\
&= \left(\overline{h_1}, \dots, \overline{h_n}\right)^T + \left(\overline{k_1}, \dots, \overline{k_n}\right)^T \\
&= \pi(h_1, \dots, h_n)^T + \pi(k_1, \dots, k_n)^T.
\end{aligned}$$

Karena $\pi((h_1, \dots, h_n)^T + (k_1, \dots, k_n)^T) = \pi(h_1, \dots, h_n)^T + \pi(k_1, \dots, k_n)^T$ maka π adalah homomorfisma grup.

Selanjutnya ditunjukkan bahwa setiap elemen di $End(H_p)$ memiliki padanan matriks di R_p melalui pemetaan ψ yang memetakan R_p ke $End(H_p)$.

Definisi 3.1.6 Misalkan $A \in R_p$, $(h_1, \dots, h_n)^T \in \mathbb{Z}^n$ dan $\left(\overline{h_1}, \dots, \overline{h_n}\right)^T) \in H_p$. Pemetaan $\psi: R_p \to End(H_p)$ adalah

$$\psi(A)\left(\overline{h_1}, \dots, \overline{h_n}\right)^T = \pi(A(h_1, \dots, h_n)^T) \quad \textbf{(3.2)}$$

dengan π seperti didefinisikan pada Persamaan (3.1).
(Hillar & Rhea, 2007)

Sebelum masuk pada pemetaan ψ, akan ditunjukkan terlebih dahulu $\psi(A)\colon H_p \to H_p$ pada Persamaan (3.2) adalah pemetaan yang terdefinisi dengan baik dan merupakan elemen di $End(H_p)$.

Lemma 3.1.7 Pemetaan $\psi(A)\colon H_p \to H_p$ dengan $A \in R_p$ dan

$$\psi(A)(\overline{h_1}, \dots, \overline{h_n})^T = \pi(A(h_1, \dots, h_n)^T)$$

adalah elemen dari $End(H_p)$.

Bukti. Pertama akan dibuktikan $\psi(A)$ merupakan pemetaan yang terdefinisi dengan baik. Misalkan $A = (a_{ij}) \in R_p$. Misalkan pula $(\overline{r_1}, \dots, \overline{r_n})^T = (\overline{s_1}, \dots, \overline{s_n})^T$ untuk $(\overline{r_1}, \dots, \overline{r_n})^T, (\overline{s_1}, \dots, \overline{s_n})^T \in H_p$ dan $r_t, s_t \in \mathbb{Z}$ dengan $p^{e_t} | r_t - s_t$ untuk setiap $t = 1, \dots, n$. Akan dibuktikan $\psi(A)(\overline{r_1}, \dots, \overline{r_n})^T = \psi(A)(\overline{s_1}, \dots, \overline{s_n})^T$ dengan cara menunjukkan $\pi(A(r_1, \dots, r_n)^T) - \pi(A(s_1, \dots, s_n)^T) = \overline{0}$. Perhatikan bahwa selisih $\pi(A(r_1, \dots, r_n)^T) - \pi(A(s_1, \dots, s_n)^T)$ adalah

$$\pi\left(\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}\begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix}\right) - \pi\left(\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}\begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix}\right)$$

$$= \pi\begin{pmatrix} a_{11}r_1 + \cdots + a_{1n}r_n \\ \vdots \\ a_{n1}r_1 + \cdots + a_{nn}r_n \end{pmatrix} - \pi\begin{pmatrix} a_{11}s_1 + \cdots + a_{1n}s_n \\ \vdots \\ a_{n1}s_1 + \cdots + a_{nn}s_n \end{pmatrix}$$

atau dapat dinyatakan dalam selisih vektor baris ke-k sebagai berikut

$$\pi_k\left(\sum_{t=1}^{n} a_{kt}r_t\right) - \pi_k\left(\sum_{t=1}^{n} a_{kt}s_t\right)$$

untuk $k = 1, \dots, n$. Karena π_k adalah homomorfisma maka

$$\pi_k\left(\sum_{t=1}^{n} a_{kt}r_t\right) - \pi_k\left(\sum_{t=1}^{n} a_{kt}s_t\right) = \pi_k\left(\sum_{t=1}^{n} a_{kt}r_t - \sum_{t=1}^{n} a_{kt}s_t\right)$$

$$= \pi_k\left(\sum_{t=1}^{n} a_{kt}r_t - a_{kt}s_t\right)$$

$$= \sum_{t=1}^{n} \pi_k(a_{kt}(r_t - s_t)).$$

Jika $a_{kt}(r_t - s_t)$ dikalikan dengan $\frac{p^{e_k - e_t}}{p^{e_k - e_t}}$ maka didapat

$$\pi_k\left(\sum_{t=1}^{n} a_{kt} r_t\right) - \pi_k\left(\sum_{t=1}^{n} a_{kt} s_t\right) = \sum_{t=1}^{n} \pi_k\left(\frac{a_{kt}}{p^{e_k - e_t}}(r_t - s_t)p^{e_k - e_t}\right).$$

Karena $(a_{ij}) \in R_p$ maka $p^{e_k - e_t} | a_{kt}$ atau dengan kata lain $\frac{a_{kt}}{p^{e_k - e_t}} \in \mathbb{Z}$. Lebih lanjut karena $p^{e_t} | (r_t - s_t)$ maka $(r_t - s_t) = v p^{e_t}$ untuk suatu $v \in \mathbb{Z}$. Jika kedua ruas dari $(r_t - s_t) = v p^{e_t}$ dikalikan dengan p^{e_k} maka diperoleh

$$p^{e_k}(r_t - s_t) = v p^{e_t} p^{e_k}$$
$$p^{e_k - e_t}(r_t - s_t) = v p^{e_k}.$$

Jadi, untuk $k \geq t$ didapat $p^{e_k} | p^{e_k - e_t}(r_t - s_t)$. Sedangkan untuk $k < t$ diperoleh $p^{e_k} | p^{e_t}$. Karena $p^{e_t} | (r_t - s_t)$ dan $p^{e_k} | p^{e_t}$ maka $p^{e_k} | (r_t - s_t)$. Dengan demikian untuk $k = 1, \dots, n$ didapat

$$\pi_k\left(\sum_{t=1}^{n} a_{kt} r_t\right) - \pi_k\left(\sum_{t=1}^{n} a_{kt} s_t\right) = \sum_{t=1}^{n} \pi_k\left(\frac{a_{kt}}{p^{e_k - e_t}}(r_t - s_t)p^{e_k - e_t}\right) = \bar{0}$$

$$\pi_k\left(\sum_{t=1}^{n} a_{kt} r_t\right) = \pi_k\left(\sum_{t=1}^{n} a_{kt} s_t\right)$$

atau $\psi(A)(\overline{r_1}, \dots, \overline{r_n})^T = \psi(A)(\overline{s_1}, \dots, \overline{s_n})^T$. Jadi terbukti $\psi(A)$ merupakan pemetaan yang terdefinisi dengan baik.

Kemudian akan dibuktikan $\psi(A)$ adalah homomorfisma grup. Karena π homomorfisma grup dan operasi pada R_p memenuhi sifat distributif, maka untuk $\left(\overline{h_1}, \dots, \overline{h_n}\right)^T \in H_p$ dan $\left(\overline{k_1}, \dots, \overline{k_n}\right)^T \in H_p$ berlaku

$$\begin{aligned}
\psi(A)\left(\left(\overline{h_1}, \dots, \overline{h_n}\right)^T + \left(\overline{k_1}, \dots, \overline{k_n}\right)^T\right) &= \psi(A)\left(\left(\overline{h_1} + \overline{k_1}, \dots, \overline{k_n} + \overline{h_n}\right)^T\right) \\
&= \psi(A)\left(\overline{h_1 + k_1}, \dots, \overline{h_n + k_n}\right)^T \\
&= \pi(A(h_1 + k_1, \dots, h_n + k_1)^T) \\
&= \pi(A(h_1, \dots, h_n)^T + A(k_1, \dots, k_n)^T) \\
&= \pi(A(h_1, \dots, h_n)^T) + \pi(A(k_1, \dots, k_n)^T) \\
&= \psi(A)\left(\overline{h_1}, \dots, \overline{h_n}\right)^T + \psi(A)\left(\overline{k_1}, \dots, \overline{k_n}\right)^T.
\end{aligned}$$

Jadi terbukti $\psi(A)$ merupakan homomorfisma grup.

Karena $\psi(A)$ merupakan pemetaan yang terdefinisi dengan baik dan juga homomorfisma grup dari H_p ke H_p, maka terbukti $\psi(A) \in End(H_p)$. ■

Setelah ditunjukkan $\psi(A)$ pemetaan yang terdefinisi dengan baik dan $\psi(A) \in End(H_p)$, akan ditunjukkan pemetaan ψ seperti pada Definisi 3.1.6 merupakan homomorfisma gelanggang yang surjektif.

Teorema 3.1.8 Pemetaan $\psi: R_p \to End(H_p)$ yang didefinisikan sebagai

$$\psi(A)\left(\overline{h_1}, \dots, \overline{h_n}\right)^T = \pi(A(h_1, \dots, h_n)^T)$$

adalah suatu homomorfisma gelanggang yang surjektif.
(Hillar & Rhea, 2007)

Bukti. Pertama akan ditunjukkan ψ merupakan pemetaan yang terdefinisi dengan baik. Misalkan $A, B \in R_p$ dimana $A = B$ dan $\left(\overline{h_1}, \dots, \overline{h_n}\right)^T \in H_p$. Akan ditunjukkan $\psi(A)\left(\overline{h_1}, \dots, \overline{h_n}\right)^T = \psi(B)\left(\overline{h_1}, \dots, \overline{h_n}\right)^T$. Berdasarkan Lemma 3.1.7, $\psi(A)$ terdefinisi dengan baik dan $\psi(A) \in End(H_p)$, maka

$$\begin{aligned}\psi(A)\left(\overline{h_1}, \dots, \overline{h_n}\right)^T &= \pi(A(h_1, \dots, h_n)^T) \\ &= \pi(B(h_1, \dots, h_n)^T) \\ &= \psi(B)\left(\overline{h_1}, \dots, \overline{h_n}\right)^T.\end{aligned}$$

Jadi terbukti ψ terdefinisi dengan baik.

Selanjutnya akan dibuktikan pemetaan ψ adalah pemetaan surjektif. Misalkan $w_i = (\bar{0}, \dots, g_i, \dots, \bar{0})^T \in H_p$ dengan g_i adalah elemen ke-i dan merupakan generator dari $\mathbb{Z}/p^{e_i}\mathbb{Z}$. Misalkan pula $M \in End(H_p)$ memetakan setiap w_j. Namun tidak ada kebebasan penuh dalam mendefinisikan pemetaan ini, secara khusus misalkan

$$M(w_j) = \left(\overline{h_{1j}}, \dots, \overline{h_{nj}}\right)^T = \pi\left(h_{1j}, \dots, h_{nj}\right)^T \qquad \textbf{(3.3)}$$

untuk $h_{ij} \in \mathbb{Z}$, $i = 1, \dots, n$. Karena g_j adalah generator dari grup $\mathbb{Z}/p^{e_j}\mathbb{Z}$ dengan order p^{e_j}, maka $g_j p^{e_j} = \bar{0}$. Akibatnya,

$$\begin{aligned}(\bar{0}, \dots, \bar{0})^T &= M(\bar{0}, \dots, \bar{0})^T \\ &= M\left(\bar{0}, \dots, g_j p^{e_j}, \dots, \bar{0}\right)^T \\ &= M(p^{e_j} w_j)\end{aligned}$$

dengan $w_j = (\bar{0}, \dots, g_j, \dots, \bar{0})^T$. Karena $M \in End(H_p)$, maka berlaku $M(p^{e_j} w_j) = \underbrace{M(w_j) + \cdots + M(w_j)}_{p^{e_j}}$. Berdasarkan Persamaan 3.3 didapat

$$M(p^{e_j} w_j) = \underbrace{M(w_j) + \cdots + M(w_j)}_{p^{e_j}} = \underbrace{(\overline{h_{1j}}, \dots, \overline{h_{nj}})^T + \cdots + (\overline{h_{1j}}, \dots, \overline{h_{nj}})^T}_{p^{e_j}}$$
$$= (\overline{p^{e_j} h_{1j}}, \dots, \overline{p^{e_j} h_{nj}})^T.$$

Maka diperoleh $(\overline{p^{e_j} h_{1j}}, \dots, \overline{p^{e_j} h_{nj}})^T = (\bar{0}, \dots, \bar{0})^T$ atau $\overline{p^{e_j} h_{ij}} = \bar{0}$, untuk $i = 1, \dots, n$. Dengan kata lain $p^{e_i} | p^{e_j} h_{ij}$ untuk setiap i, j. Akibatnya $p^{e_i - e_j} | h_{ij}$ untuk $i \geq j$. Karena $p^{e_i - e_j} | h_{ij}$ untuk $i \geq j$, maka dapat dibentuk matriks $H = (h_{ij}) \in R_p$ dimana

$$\psi(H)(\overline{k_1}, \dots, \overline{k_n})^T = \pi(H(k_1, \dots, k_n)^T)$$
$$= \pi\left(\begin{pmatrix} h_{11} & \cdots & h_{1n} \\ \vdots & \ddots & \vdots \\ h_{n1} & \cdots & h_{nn} \end{pmatrix}\begin{pmatrix} k_1 \\ \vdots \\ k_n \end{pmatrix}\right)$$
$$= \pi\begin{pmatrix} h_{11}k_1 + \cdots + h_{1n}k_n \\ \vdots \\ h_{n1}k_1 + \cdots + h_{nn}k_n \end{pmatrix}$$
$$= \pi\left(k_1\begin{pmatrix} h_{11} \\ \vdots \\ h_{n1} \end{pmatrix} + \cdots + k_n\begin{pmatrix} h_{1n} \\ \vdots \\ h_{nn} \end{pmatrix}\right)$$
$$= k_1\pi\begin{pmatrix} h_{11} \\ \vdots \\ h_{n1} \end{pmatrix} + \cdots + k_n\pi\begin{pmatrix} h_{1n} \\ \vdots \\ h_{nn} \end{pmatrix}.$$

Berdasarkan Persamaan (3.3)

$$k_1\pi\begin{pmatrix} h_{11} \\ \vdots \\ h_{n1} \end{pmatrix} + \cdots + k_n\pi\begin{pmatrix} h_{1n} \\ \vdots \\ h_{nn} \end{pmatrix} = k_1 M(w_1) + \cdots + k_n M(w_n).$$

Dengan demikian didapat

$$\psi(H)(\overline{k_1}, \dots, \overline{k_n})^T = k_1 M(w_1) + \cdots + k_n M(w_n)$$
$$= M(k_1 w_1) + \cdots + M(k_n w_n)$$
$$= M\left(k_1\begin{pmatrix} g_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \cdots + k_n\begin{pmatrix} 0 \\ \vdots \\ 0 \\ g_n \end{pmatrix}\right)$$

$$= M\begin{pmatrix} k_1 g_1 \\ \vdots \\ k_n g_n \end{pmatrix}.$$

Karena g_i adalah generator dari $\mathbb{Z}/p^{e_i}\mathbb{Z}$, maka g_i dapat dipandang sebagai $\bar{1} = \{x \in \mathbb{Z}; x \equiv 1 \pmod{p^{e_i}}\}$. Dengan demikian $k_i g_i = \overline{k_i}$ dan akibatnya

$$\psi(H)\left(\overline{k_1}, \dots, \overline{k_n}\right)^T = M\left(\overline{k_1}, \dots, \overline{k_n}\right)^T$$

atau untuk setiap $M \in End(H_p)$ terdapat $H \in R_p$ sedemikian sehingga $\psi(H) = M$. Jadi terbukti bahwa ψ pemetaan surjektif.

Berikutnya, akan dibuktikan ψ adalah homomorfisma gelanggang.

Misalkan $A, B \in R_p$ dan $\left(\overline{h_1}, \dots, \overline{h_n}\right)^T \in H_p$

$$\psi(A+B)\left(\overline{h_1}, \dots, \overline{h_n}\right)^T = \pi\left((A+B)(h_1, \dots, h_n)^T\right).$$

Karena sifat asosiatif pada operasi matriks dan π adalah homomorfisma, maka

$$\begin{aligned}
\psi(A+B)\left(\overline{h_1}, \dots, \overline{h_n}\right)^T &= \pi(A(h_1, \dots, h_n)^T + B(h_1, \dots, h_n)^T) \\
&= \pi(A(h_1, \dots, h_n)^T) + \pi(B(h_1, \dots, h_n)^T) \\
&= \psi(A)\left(\overline{h_1}, \dots, \overline{h_n}\right)^T + \psi(B)\left(\overline{h_1}, \dots, \overline{h_n}\right)^T \\
&= (\psi(A) + \psi(B))\left(\overline{h_1}, \dots, \overline{h_n}\right)^T.
\end{aligned}$$

Lebih lanjut,

$$\begin{aligned}
\psi(AB)\left(\overline{h_1}, \dots, \overline{h_n}\right)^T &= \pi(AB(h_1, \dots, h_n)^T) \\
&= \pi(A(b_{11}h_1 + \cdots + b_{1n}h_n, \dots, b_{n1}h_1 + \cdots + b_{nn}h_n)^T) \\
&= \psi(A)\left(\overline{b_{11}h_1 + \cdots + b_{1n}h_n}, \dots, \overline{b_{n1}h_1 + \cdots + b_{nn}h_n}\right)^T \\
&= \psi(A)(\pi(b_{11}h_1 + \cdots + b_{1n}h_n, \dots, b_{n1}h_1 + \cdots + b_{nn}h_n))^T \\
&= \psi(A)\left(\pi(B(h_1, \dots, h_n)^T)\right) \\
&= \psi(A)\left(\psi(B)\left(\overline{h_1}, \dots, \overline{h_n}\right)^T\right) \\
&= \psi(A) \circ \psi(B)\left(\overline{h_1}, \dots, \overline{h_n}\right)^T.
\end{aligned}$$

Terbukti ψ adalah homomorfisma gelanggang.

Terakhir akan dibuktikan pemetaan ψ memetakan matriks identitas I di R_p ke identitas di $End(H_p)$ yaitu id_{E_p}.

$$\begin{aligned}
\psi(I)\left(\overline{h_1}, \dots, \overline{h_n}\right)^T &= \pi(I(h_1, \dots, h_n)^T) \\
&= \pi(h_1, \dots, h_n)^T
\end{aligned}$$

$$= \left(\overline{h_1}, \dots, \overline{h_n}\right)^T$$
$$= \mathrm{id}_{E_p}\left(\overline{h_1}, \dots, \overline{h_n}\right)^T.$$

Jadi terbukti $\psi(I) = \mathrm{id}_{E_p}$. Dengan demikian terbukti ψ adalah homomorfisma gelanggang yang surjektif.■

Teorema diatas memiliki makna bahwa setiap elemen di $End(H_p)$ memiliki padanan matriks di R_p. Lemma berikut akan menunjukkan matriks seperti apa yang merupakan anggota dari kernel ψ.

Lemma 3.1.9 Misalkan $A = (a_{ij}) \in R_p$. Misalkan pula ψ adalah pemetaan seperti pada Definisi 3.1.6. yaitu,

$$\psi(A)\left(\overline{h_1}, \dots, \overline{h_n}\right)^T = \pi(A(h_1, \dots, h_n)^T).$$

Maka $A \in \ker \psi$ jika dan hanya jika memenuhi $p^{e_i} | a_{ij}$ untuk setiap i, j. (Hillar & Rhea, 2007)

Bukti. Pertama-tama misalkan $A = (a_{ij}) \in R_p$ adalah matriks yang memenuhi $p^{e_i} | a_{ij}$ untuk setiap i, j. Maka akan dibuktikan $A \in \ker \psi$. Misalkan pula $w_j = \left(\bar{0}, \dots, g_j, \dots, \bar{0}\right)^T \in H_p$, dengan $g_j$adalah generator dari $\mathbb{Z}/p^{e_j}\mathbb{Z}$ yang dapat dipandang sebagai $\bar{1} = \{x \in \mathbb{Z}; x \equiv 1 \pmod{p^{e_j}}\}$. Berdasarkan Persamaan 3.3 untuk $A = (a_{ij}) \in R_p$, maka

$$\psi(A)w_j = \psi(A)\left(\bar{0}, \dots, g_j, \dots, \bar{0}\right)^T$$
$$= \psi(A)(\bar{0}, \dots, \bar{1}, \dots, \bar{0})^T$$
$$= \pi(A(0, \dots, 1, \dots, 0)^T)$$
$$= \pi\left(\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}\begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}\right)$$
$$= \pi\begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{pmatrix}$$

$$= \left(\pi_1(a_{1j}), \dots, \pi_n(a_{nj})\right)^T.$$

Karena berlaku $p^{e_i}|a_{ij}$ dan berdasarkan definisi $\pi_i: \mathbb{Z} \to \mathbb{Z}/p^{e_i}\mathbb{Z}$ maka didapat $\pi_i(a_{ij}) = \bar{0}$ atau $\psi(A)w_j = (\bar{0}, \dots, \bar{0})^T = 0$. Karena $h \in H_p$ adalah kombinasi linier dari w_j, maka $\psi(A)h = 0$ untuk setiap $h \in H_p$. Berdasarkan definisi dari kernel homomorfisma gelanggang maka $A \in \ker\psi$.

Untuk pembuktian sebaliknya, misalkan $A = (a_{ij}) \in R_p$ adalah elemen dari $\ker\psi$, maka matriks $A = (a_{ij})$ memenuhi $p^{e_i}|a_{ij}$. Berdasarkan definisi kernel homomorfisma gelanggang, untuk $A \in \ker\psi$ berlaku $\psi(A)w_j = 0$ untuk setiap $w_j \in H_p$. Dengan menggunakan perhitungan sebelumnya

$$\psi(A)w_j = \left(\pi_1(a_{1j}), \dots, \pi_n(a_{nj})\right)^T = 0.$$

Berdasarkan definisi π_i, karena $\pi_i(a_{ij}) = \bar{0}$ maka $p^{e_i}|a_{ij}$. Jadi terbukti untuk $A = (a_{ij}) \in \ker\psi$ memenuhi $p^{e_i}|a_{ij}$. Dengan demikian terbukti $A = (a_{ij}) \in R_p$ adalah elemen dari kenel ψ jika dan hanya jika memenuhi $p^{e_i}|a_{ij}$ untuk setiap i, j.■

3.2 Karakter Matriks Endomorfisma H_p sebagai Automorfisma H_p

Pada Lemma 3.1.7 telah ditunjukkan bahwa $\psi(A)$ dimana $A \in R_p$ merupakan elemen dari $End(H_p)$. Dengan demikian, dalam menunjukkan elemen-elemen $End(H_p)$ yang merupakan automorfisma, matriks yang akan dipelajari adalah matriks didalam himpunan R_p. Namun sebelum itu terlebih dahulu dipelajari beberapa penggunaan teori matriks pada himpunan matriks R_p.

Lemma 3.2.1 Misalkan $A \in \mathbb{Z}^{n\times n}$ dengan $\det(A) \neq 0$. Maka terdapat matriks yang unik $B \in \mathbb{Z}^{n\times n}$, yang disebut sebagai *adjugate* dari A sedemikian sehingga $AB = BA = \det(A)I$.
(Hillar & Rhea, 2007)

Bukti. Misalkan $A = (a_{ij}) \in \mathbb{Z}^{n\times n}$ dengan $\det(A) \neq 0$, akan ditunjukkan terdapat $B \in \mathbb{Z}^{n\times n}$ yang unik sedemikian sehingga $AB = BA = \det(A)I$. Misalkan M_{ij} dengan $i,j \in \{1,2,\dots,n\}$ adalah determinan matriks $(n-1)\times(n-1)$ dengan menghilangkan baris ke-i dan kolom ke-j dari matriks A. Karena $a_{ij} \in \mathbb{Z}$ maka $M_{ij} \in \mathbb{Z}$. Selanjutnya misalkan pula C_{ij} kofaktor dari A, yaitu $C_{ij} = (-1)^{i+j}(M_{ij})$. Karena $M_{ij} \in \mathbb{Z}$, maka $C_{ij} \in \mathbb{Z}$ untuk setiap $i,j \in \{1,2,\dots,n\}$.

Definisikan matriks $C = (C_{ij})$ dan $B = C^T$ dimana $B, C \in \mathbb{Z}^{n\times n}$. Maka

$$AB = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}\begin{pmatrix} C_{11} & \cdots & C_{n1} \\ \vdots & \ddots & \vdots \\ C_{1n} & \cdots & C_{nn} \end{pmatrix} = \begin{pmatrix} z_{11} & \cdots & z_{1n} \\ \vdots & \ddots & \vdots \\ z_{n1} & \cdots & z_{nn} \end{pmatrix}$$

dengan $z_{ij} = \sum_{k=1}^{n} a_{ik}C_{jk}$. Untuk $i = j$ berlaku $z_{ii} = \sum_{k=1}^{n} a_{ik}C_{ik} = \det(A)$. Untuk $i \neq j$, dimisalkan $A_{st}^{*} = \left(a_{ij}^{*}\right) \in \mathbb{Z}^{n\times n}$ adalah matriks yang diperoleh dari matriks A dengan mengganti elemen-elemen baris ke-t dengan baris ke-s sedemikian sehingga dua baris tersebut identik, dimana $s,t \in \{1,2,\dots,n\}$ dan $s \neq t$. Karena matriks A_{st}^{*} memiliki dua baris yang identik maka $\det(A_{st}^{*}) = 0$. Misalkan M_{ij}^{*} dengan $i,j \in \{1,2,\dots,n\}$ adalah determinan matriks $(n-1)\times(n-1)$ dengan menghilangkan baris ke-i dan kolom ke-j dari matriks A_{st}^{*}. Karena $a_{ij}^{*} \in \mathbb{Z}$ maka $M_{ij}^{*} \in \mathbb{Z}$. Misalkan pula C_{ij}^{*} kofaktor dari A_{st}^{*} yaitu $C_{ij}^{*} = (-1)^{i+j}(M_{ij}^{*})$. Karena $M_{ij}^{*} \in \mathbb{Z}$, maka $C_{ij}^{*} \in \mathbb{Z}$ untuk setiap $i,j \in \{1,2,\dots,n\}$.

Karena pada A_{st}^{*} baris ke-t sama dengan baris ke-s, dan baris ke-s pada A_{st}^{*} sama dengan baris ke-s pada A maka diperoleh $a_{tj}^{*} = a_{sj}^{*} = a_{sj}$ dan $C_{tj} = C_{tj}^{*}$, dengan demikian didapat

$$0 = \det(A_{st}^{*}) = \sum_{k=1}^{n} a_{tk}^{*}C_{tk}^{*} = \sum_{k=1}^{n} a_{sk}C_{tk} = z_{st}$$

untuk $s \neq t$. Jadi dapat disimpulkan

$$z_{ij} = \begin{cases} \det(A) & i = j \\ 0 & i \neq j \end{cases}$$

$$AB = \begin{pmatrix} \det(A) & 0 & \dots & 0 \\ 0 & \det(A) & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \dots & 0 & \det(A) \end{pmatrix} = \det(A)\, I.$$

Karena $A \in \mathbb{Z}^{n\times n}$ dan $\det(A) \neq 0$ maka terdapat A^{-1}. Jika kedua ruas dari $AB = \det(A)\, I$ dikalikan dengan matriks A^{-1} dan A, maka $A^{-1}ABA =$

$A^{-1}\det(A)\,IA$. Dengan demikian diperoleh $BA = \det(A)\,A^{-1}A$ atau $BA = \det(A)\,I$. Jadi telah ditunjukkan terdapat $B \in \mathbb{Z}^{n\times n}$ dimana $AB = \det(A)\,I = BA$.

Selanjutnya akan ditunjukkan B yang merupakan *adjugate* dari A adalah matriks yang unik. Misalkan terdapat matriks $B_1 \neq B$ dan memenuhi $AB_1 = B_1A = \det(A)\,I$. Karena matriks B juga memenuhi $AB = BA = \det(A)\,I$ maka $AB = AB_1$. Jika kedua ruas dari $AB = AB_1$ dikalikan dengan A^{-1} didapat

$$A^{-1}AB = A^{-1}AB_1$$

$$B = B_1.$$

Jadi terbukti B matriks *adjugate* dari A yang memenuhi $AB = BA = \det(A)\,I$ adalah matriks yang unik.■

Selanjutnya akan ditunjukkan untuk setiap A di R_p dengan $\det A \neq 0$ maka A memiliki matriks *adjugate* B yang juga terdapat di R_p.

Lemma 3.2.2 Jika $A \in R_p$ dengan $\det(A) \neq 0$, maka terdapat matriks $B \in R_p$ sedemikian sehingga $AB = BA = \det(A)\,I$.

Bukti. Misalkan $A \in R_p$ dengan $\det(A) \neq 0$. Misalkan pula $B \in \mathbb{Z}^{n\times n}$ adalah matriks *adjugate* dari A yang memenuhi $AB = BA = \det(A)\,I$. Akan ditunjukkan $B \in R_p$.

Berdasarkan Lemma 3.1.3 untuk setiap $A \in R_p$, terdapat P =diagonal$(p^{e_1}, \dots, p^{e_n})$ sedemikian sehingga $A = PA'P^{-1}$ untuk suatu $A' \in \mathbb{Z}^{n\times n}$. Karena A similar dengan A' maka $\det(A) = \det(A')$. Karena $\det(A) \neq 0$ maka $\det(A') \neq 0$. Dengan demikian berdasarkan Lemma 3.2.1 untuk suatu $A' \in \mathbb{Z}^{n\times n}$ dimana $\det(A') \neq 0$ terdapat $B' \in \mathbb{Z}^{n\times n}$ sedemikian sehingga memenuhi $A'B' = B'A' = \det(A')\,I = \det(A)\,I$. Pilih $C \in R_p$ yang memenuhi $C = PB'P^{-1}$ maka

$$\begin{aligned} AC &= PA'P^{-1}PB'P^{-1} \\ &= PA'IB'P^{-1} \\ &= PA'B'P^{-1} \\ &= P\det(A)IP^{-1} \\ &= \det(A)\,PP^{-1} \\ &= \det(A)\,I \end{aligned}$$

$$\begin{aligned} CA &= PB'P^{-1}PA'P^{-1} \\ &= PB'IA'P^{-1} \end{aligned}$$

$= PB'A'P^{-1}$ $= \det(A)\, PP^{-1}$

$= P\, \det(A) IP^{-1}$ $= \det(A)\, I.$

Dengan demikian didapat $AC = CA = \det(A)\, I$. Berdasarkan Lemma 3.2.1, B matriks *adjugate* dari A, adalah matriks yang unik, maka $B = C = PB'P^{-1} \in R_p$. Jadi terbukti $B \in R_p$. ■

Lemma 3.2.3 Jika $A, B \in \mathbb{Z}^{n\times n}$ dimana $A = pB + I$ untuk suatu bilangan prima p maka $\det(A) \equiv 1 \pmod p$.

Bukti. Misalkan $A = (a_{ij}), B = (b_{ij}) \in \mathbb{Z}^{n\times n}$ dengan $A = pB + I$ dapat dinyatakan sebagai

$$A = \begin{pmatrix} b_{11}p+1 & b_{12}p & \cdots & b_{1n}p \\ b_{21}p & b_{22}p+1 & \cdots & b_{2n}p \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1}p & b_{n2}p & \cdots & b_{nn}p+1 \end{pmatrix}.$$

Akan ditunjukkan $\det(A) \equiv 1 \pmod p$ dengan mengunakan induksi.

Akan ditunjukkan benar bahwa $\det(A) \equiv 1 \pmod p$ untuk $n = 2$.

$$A = \begin{pmatrix} b_{11}p+1 & b_{12}p \\ b_{21}p & b_{22}p+1 \end{pmatrix}$$

$$\begin{aligned} \det(A) &= (b_{11}p+1)(b_{22}p+1) - (b_{21}p)(b_{12}p) \\ &= 1 + p(b_{11}b_{22}p + b_{11} + b_{22} + b_{21}b_{12}p). \end{aligned}$$

Misalkan $b_{11}b_{22}p + b_{11} + b_{22} + b_{21}b_{12}p = t$, maka $\det(A) = 1 + pt$. Dengan demikian berlaku $\det(A) \equiv 1 \pmod p$ untuk $n = 2$.

Asumsikan benar bahwa $\det(A) \equiv 1 \pmod p$ untuk $n = k$. Akan ditunjukkan benar bahwa $\det(A) \equiv 1 \pmod p$ untuk $n = k + 1$

$$A = \begin{pmatrix} b_{11}p+1 & b_{12}p & \cdots & b_{1\,k}p & b_{1\,k+1}p \\ b_{21}p & b_{22}p+1 & \cdots & b_{2\,k}p & b_{2\,k+1}p \\ \vdots & \vdots & & \vdots & \vdots \\ b_{k\,1}p & b_{k\,2}p & \cdots & b_{k\,k}p+1 & b_{k\,k+1}p \\ b_{k+1\,1}p & b_{k+1\,2}p & \cdots & b_{k+1\,k}p & b_{k+1\,k+1}p+1 \end{pmatrix}.$$

Dengan ekspansi baris pertama diperoleh

$$\det(A) = (b_{11}p+1)\begin{vmatrix} b_{22}p+1 & \cdots & b_{2\,k+1}p \\ \vdots & \ddots & \vdots \\ b_{k+1\,2}p & \cdots & b_{k+1\,k+1}p+1 \end{vmatrix} + b_{12}p\begin{vmatrix} b_{21}p & \cdots & b_{2\,k+1}p \\ \vdots & \ddots & \vdots \\ b_{k+1\,1}p & \cdots & b_{k+1\,k+1}p+1 \end{vmatrix} + \cdots + b_{1\,k+1}p\begin{vmatrix} b_{21}p & \cdots & b_{2\,k}p \\ \vdots & \ddots & \vdots \\ b_{k+1\,1}p & \cdots & b_{k+1\,k}p \end{vmatrix}.$$

Berdasarkan asumsi, nilai dari $\begin{vmatrix} b_{22}p+1 & \cdots & b_{2\,k+1}p \\ \vdots & \ddots & \vdots \\ b_{k+1\,2}p & \cdots & b_{k+1\,k+1}p+1 \end{vmatrix}$ adalah $1 \pmod p$ atau $1+up$ untuk suatu $u \in \mathbb{Z}$. Misalkan

$\begin{vmatrix} b_{21}p & \cdots & b_{2\,k+1}p \\ \vdots & \ddots & \vdots \\ b_{k+1\,1}p & \cdots & b_{k+1\,k+1}p+1 \end{vmatrix} = v_1, \ldots, \begin{vmatrix} b_{21}p & \cdots & b_{2\,k}p \\ \vdots & \ddots & \vdots \\ b_{k+1\,1}p & \cdots & b_{k+1\,k}p \end{vmatrix} = v_n$, dimana $v_i \in \mathbb{Z}$ untuk $i = 1, \ldots, n$. Maka diperoleh

$$\begin{aligned}\det(A) &= (b_{11}p+1)(1+up) + b_{12}pv_1 + \cdots + b_{1\,k+1}pv_n \\ &= 1 + p(b_{11} + u + b_{11}up + b_{12}v_1 + \cdots + b_{1\,k+1}v_n).\end{aligned}$$

Misalkan pula $b_{11} + u + b_{11}up + b_{12}v_1 + \cdots + b_{1\,k+1}v_n = w$, maka $\det(A) = 1 + pw$ untuk $w \in \mathbb{Z}$. Jadi terbukti $\det(A) \equiv 1 \pmod p$ untuk $A, B \in \mathbb{Z}^{n\times n}$ dimana $A = pB + I$. ■

Lemma 3.2.4 Untuk setiap $A \in R_p$, $p \nmid \det(A)$ jika dan hanya jika $A \pmod p \in GL_n(F_p)$.

Bukti. Pertama misalkan $A \in R_p$ dengan $p \nmid \det(A)$ maka akan ditunjukkan $A \pmod p \in GL_n(F_p)$. Untuk $A = (a_{ij}) \in R_p$, definisikan $\bar{A} = (h_{ij})$ dimana $h_{ij} \equiv a_{ij} \pmod p$. Berdasarkan definisi determinan

$$\det(A) = \sum_{\sigma} sign(\sigma)\, a_{1\sigma(1)} \ldots a_{n\sigma(n)}$$

maka

$$\det(A) \pmod p \equiv \left[\sum_{\sigma} sign(\sigma)\, a_{1\sigma(1)} \ldots a_{n\sigma(n)}\right] \pmod p$$

$$\equiv \sum_{\sigma} sign(\sigma)\, h_{1\sigma(1)} \dots h_{n\sigma(n)}$$

$$\equiv \det(\bar{A}) \pmod{p}.$$

Karena $p \nmid \det(A)$ maka $\det(A) \neq pk$ untuk setiap $k \in \mathbb{Z}$ atau $\det(A) \pmod{p} \not\equiv 0$. Dengan demikian $\det(\bar{A}) \pmod{p} \not\equiv 0 \in F_p$. Sehingga $\bar{A}$ invertibel menurut operasi di F_p. Jadi terbukti $A \pmod{p} \in GL_n(F_p)$.

Sebaliknya, misalkan $A \pmod{p} \in GL_n(F_p)$, akan ditunjukkan $p \nmid \det(A)$. Karena $\bar{A} \in GL_n(F_p)$ maka $\det(\bar{A}) \pmod{p} \not\equiv 0 \in F_p$. Karena $\det(A) \pmod{p} \equiv \det(\bar{A}) \pmod{p}$ maka $\det(A) \pmod{p} \not\equiv 0$ atau $\det(A) \neq pk$ untuk setiap $k \in \mathbb{Z}$. Dengan demikian terbukti $p \nmid \det(A)$. ■

Dengan informasi tersebut maka untuk memeriksa elemen-elemen $End(H_p)$ yang dapat menjadi automorfisma dapat melalui matriks didalam himpunan R_p yang berkoresponden dengan endomorfisma H_p.

Teorema 3.2.5 Endomorfisma $M = \psi(A)$, dengan $\psi: R_p \to End(H_p)$, adalah suatu automorfisma jika dan hanya jika $A \pmod{p} \in GL_n(F_p)$.
(Hillar & Rhea, 2007)

Bukti. Pertama, misalkan $A \pmod{p} \in GL_n(F_p)$ dimana $A \in R_p$. Akan dibuktikan $M = \psi(A)$ adalah automorfisma. Karena $\psi(A)$ adalah endomorfisma dari H_p ke H_p, maka cukup ditunjukkan $\psi(A)$ pemetaan bijektif. Dengan menggunakan Lemma 2.2.1 akan ditunjukkan $\psi(A)$ memiliki invers yang memenuhi $\psi(A)(\psi(A))^{-1} = (\psi(A))^{-1}\psi(A) = \mathrm{id}_{E_p}$.

Misalkan $A \pmod{p} \in GL_n(F_p)$ dengan $A \in R_p$ maka menurut Lemma 3.2.4 $p \nmid \det(A)$ dan $\det(A) \neq 0$. Karena $p \nmid \det(A)$ maka $FPB(\det(A), p^{e_n}) = 1$. Berdasarkan Lemma 2.1.1 diperoleh $s \cdot \det(A) + t \cdot p^{e_n} = 1$ untuk $s, t \in \mathbb{Z}$, yang mengakibatkan $s \cdot \det(A) \equiv 1 \bmod p^{e_n}$. Dengan demikian $s \in \mathbb{Z}$ merupakan invers dari $\det(A) \bmod p^{e_n}$. Karena $s \cdot \det(A) \equiv 1 \bmod p^{e_n}$ maka berlaku pula $s \cdot \det(A) \equiv 1 \bmod p^{e_j}$ untuk $1 \leq j \leq n$.

Berdasarkan Lemma 3.2.2, untuk suatu $A \in R_p$ dan $\det(A) \neq 0$, maka terdapat $B \in R_p$ sedemikan sehingga $AB = BA = \det(A)\, I$. Misalkan $A^{(-1)} \in R_p$ dimana $A^{(-1)} \coloneqq s\, B$, maka

$$A^{(-1)}A = s\, BA = s \det(A)\, I = \ s\, AB = A\, s\, B = AA^{(-1)}.$$

Karena $\psi(s \det(A)\, I) = \mathrm{id}_{\mathrm{Ep}}$ dan ψ adalah homomorfisma dengan demikian

$$\psi\left(AA^{(-1)}\right) = \psi(A)\psi\left(A^{(-1)}\right) = \mathrm{id}_{E_p},$$

$$\psi\left(A^{(-1)}A\right) = \psi\left(A^{(-1)}\right)\psi(A) = \mathrm{id}_{E_p},$$

atau terdapat $\psi\left(A^{(-1)}\right) = \left(\psi(A)\right)^{-1} \in End(H_p)$ yang memenuhi

$$\psi(A)\left(\psi(A)\right)^{-1} = \left(\psi(A)\right)^{-1}\psi(A) = \mathrm{id}_{E_p}.$$

Jadi terbukti $\psi(A)$ pemetaan bijektif serta $\psi(A)$ merupakan automorfisma pada H_p.

Sebaliknya, dimisalkan $\psi(A)$ adalah automorfisma untuk $A \in R_p$ maka akan dibuktikan $A(\mathrm{mod}\ p) \in GL_n(F_p)$. Berdasarkan Teorema 3.1.8, untuk setiap $M \in End(H_p)$ terdapat $A \in R_p$ sedemikian sehingga $\psi(A) = M$. Karena $\psi(A) = M$ adalah automorfisma, maka terdapat $M^{-1} \in End(H_p)$ sedemikian sehingga $MM^{-1} = M^{-1}M = \mathrm{id}_{E_p}$. Karena $M^{-1} \in End(H_p)$ maka terdapat $C \in R_p$ sedemikian sehingga $\psi(C) = M^{-1}$. ψ homomorfisma gelanggang, dengan demikian diperoleh

$$\begin{aligned}\psi(AC - I) &= \psi(AC) - \psi(I)\\ &= \psi(A)\psi(C) - \mathrm{id}_{E_p}\\ &= MM^{-1} - \mathrm{id}_{E_p}\\ &= \mathrm{id}_{E_p} - \mathrm{id}_{E_p}\\ &= 0.\end{aligned}$$

Jadi $AC - I \in \ker\psi$. Misalkan $AC = (b_{ij})$ maka

$$AC - I = \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ b_{21} & \ddots & b_{2n} \\ \vdots & & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix} - I = \begin{pmatrix} b_{11} - 1 & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} - 1 & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} - 1 \end{pmatrix}.$$

Berdasarkan Lemma 3.1.9, jika $AC - I \in \ker\psi$ maka p habis membagi elemen-elemen matriks $AC - I$, akibatnya

$$b_{ij} = \begin{cases} k_{ij}p + 1 & i = j \\ k_{ij}p & i \neq j \end{cases}$$

untuk $k_{ij} \in \mathbb{Z}$.

$$AC = \begin{pmatrix} k_{11}p + 1 & k_{12}p & \cdots & k_{1n}p \\ k_{21}p & k_{22}p + 1 & \cdots & k_{2n}p \\ \vdots & \vdots & \ddots & \vdots \\ k_{n1}p & k_{n2}p & \cdots & k_{nn}p + 1 \end{pmatrix} = \begin{pmatrix} k_{11}p & \cdots & k_{1n}p \\ k_{21}p & \ddots & k_{2n}p \\ \vdots & \cdots & \vdots \\ k_{n1}p & \cdots & k_{nn}p \end{pmatrix} + I.$$

Pilih $K = (k_{ij}) \in \mathbb{Z}^{n\times n}$, maka $AC = pK + I$. Dengan menggunakan Lemma 3.2.3 didapat $\det(AC) = \det(A)\det(C) \equiv 1 \pmod p$. Dengan demikian $p \nmid \det(A)$. Berdasarkan Lemma 3.2.4, karena $p \nmid \det(A)$, terbukti $A \pmod p \in GL_n(F_p)$. Jadi terbukti endomorfisma $\psi(A)$ adalah suatu automorfisma jika dan hanya jika $A \pmod p \in GL_n(F_p)$.■

Dengan demikian telah ditunjukkan, melalui Teorema 3.2.5, karakter yang harus dipenuhi matriks di R_p yang dapat memberikan automorfisma H_p.

BAB 4
KESIMPULAN

Pada skripsi ini telah ditunjukkan bahwa setiap pemetaan endomorfisma H_p memiliki matriks padanan di himpunan gelanggang matriks R_p (Teorema 3.1.8). Teorema 3.2.5 menyatakan bahwa, jika matriks endomorfisma H_p, yang masing-masing entrinya dimodulo dengan p, merupakan anggota $GL_n(F_p)$, maka matriks tersebut berpadanan dengan automorfisma H_p. Berlaku pula sebaliknya, jika endomorfisma H_p merupakan automorfisma, maka matriks endomorfisma H_p, yang masing-masing entrinya dimodulo dengan p merupakan anggota $GL_n(F_p)$.

DAFTAR PUSTAKA

Anton, H. (2000). *Elementary Linear Algebra 8th ed.* New York: Willey.

Bhattacharya, P., Jain, S., & Nagpul, S. (1994). *Basic Abstract Algebra 2nd ed.* New York: Cambridge University Press.

Burton, D. M. (2002). *Elementary Number Theory 5th ed.* New York: McGraw-Hill Companies, Inc.

Herstein, I. N. (1996). *Abstract Algebra 3rd ed.* New Jersey: Prentice-Hall.

Hillar, C., & Rhea, D. L. (2007). Automorphisms of Finite Abelian Groups. *The American Mathematical Monthly*, 917-923.

Jacob, B. (1990). *Linear Algebra.* New York: W. H. Freeman and Company.

Lang, S. (2002). *Algebra 3rd ed.* New York: Springer-Verlag.

Ranum, A. (1907). The Group of Classes of Congruent Matrices with Application to the Group of Isomorphism of any Abelian Group. *Trans. Amer. Math. Soc*, 71-91.