SKRIPSI

ALGORITMA ENKRIPSI CITRA DENGAN MENGGUNAKAN LAPANGAN GALOIS DAN SISTEM *CHAOS HYBRID*

Disusun dan diajukan oleh

SYAIFULLAH HI NURDIN

H011171019

PROGRAM STUDI MATEMATIKA

DEPARTEMEN MATEMATIKA

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS HASANUDDIN

MAKASSAR

2023

ALGORITMA ENKRIPSI CITRA DENGAN MENGGUNAKAN LAPANGAN GALOIS DAN SISTEM CHAOS HYBRID

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Sains pada Program Studi Matematika Departemen Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Hasanuddin

SYAIFULLAH HI NURDIN

H011171019

PROGRAM STUDI MATEMATIKA
DEPARTEMEN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS HASANUDDIN
MAKASSAR
2023

PERNYATAAN KEASLIAN

Saya yang bertanda tangan di bawah ini:

Nama : Syaifullah Hi Nurdin

NIM : H011171019

Program Studi : Matematika

Jenjang : S1

menyatakan dengan ini bahwa karya tulis saya dengan judul :

Algoritma Enkripsi Citra dengan Menggunakan Lapangan Galois dan Sistem *Chaos Hybrid*

adalah benar hasil karya sendiri, bukan hasil plagiat dan belum pernah dipublikasikan dalam bentuk apapun.

Apabila dikemudian hari terbukti atau dapat dibuktikan bahwa sebagian atau keseluruhan skripsi ini hasil karya orang lain, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Makassar, 27 April 2023

Syaifullah Hi Nurdin
H011171019

ALGORITMA ENKRIPSI CITRA DENGAN MENGGUNAKAN LAPANGAN GALOIS DAN SISTEM *CHAOS HYBRID*

Disusun dan diajukan oleh:

Syaifullah Hi Nurdin
H011171019

Telah diperhatikan di hadapan Panitian Ujian yang dibentuk dalam rangka Penyelesaian Studi Program Sarjana Program Studi Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam pada 27 April 2023 dan dinyatakan telah memenuhi syarat kelulusan

Menyetujui,

Pembimbing Utama,	**Pembimbing Pertama,**
Dr. Khaeruddin, M.Sc.	**Dr. Andi Muhammad Anwar, S.Si., M.Si.**
NIP. 196509141991031003	**NIP. 199012282018031001**

Ketua Departemen,

Prof. Dr. Nurdin, S.Si., M.Si,
NIP. 19700807200003100 2

HALAMAN PENGESAHAN

Skripsi ini diajukan oleh:

Nama : Syaifullah Hi Nurdin
NIM : H011171019
Program Studi : Matematika
Judul Skripsi : Algoritma Enkripsi Citra dengan Menggunakan Lapangan Galois dan Sistem *Chaos Hybrid*

Telah berhasil mempertahankan di hadapan dewan penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Sains pada Program Studi Sistem Informasi Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Hasanuddin.

DEWAN PENGUJI

		Tanda Tangan
1. Ketua	: Dr. Khaeruddin, M.Sc.	(.....)
2. Sekretaris	: Dr. Andi Muhammad Anwar, S.Si., M.Si.	(.....)
3. Anggota	: Prof. Dr. Eng. Mawardi Bahri, S.Si., M.Si.	(.....)
4. Anggota	: Prof. Dr. Budi Nurwahyu, MS.	(.....)

Ditetapkan di : Makassar
Tanggal : 27 April 2023

KATA PENGANTAR

Alhamdulillahirabbil'alamin. Puji syukur penulis panjatkan ke hadirat Allah SWT, yang telah melimpahkan rahmat, hidayah, serta karunia-Nya kepada penulis, sehingga penulis dapat menyelesaikan penelitian dan menyusun skripsi ini yang berjudul "Algoritma Enkripsi Citra dengan Menggunakan Lapangan Galois dan Sistem Chaos Hybrid". Penelitian ini dilakukan sebagai upaya untuk mengembangkan teknologi keamanan informasi yang semakin penting dalam era digital saat ini.

Penulis menyadari bahwa skripsi ini tidak lepas dari kekurangan. Oleh karena, dengan kerendahan hati, penulis menerima kritik dan saran agar supaya bisa menjadi lebih baik lagi.

Penulis juga ingin mengucapkan terima kasih yang sebesar-besarnya kepada beberapa pihak yang telah memberikan dukungan dan bantuan selama penelitian ini berlangsung, antara lain:

1. Bapak **Prof. Dr. Nurdin, S.Si., M.Si.** selaku Ketua Departemen Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam serta selaku Ketua Program Studi Matematika Universitas Hasanuddin.
2. Bapak **Dr. Khaeruddin, M.Sc.** sebagai pembimbing utama yang telah memberikan ide dan motivasi dalam proses penyusunan skripsi ini serta telah banyak memberikan bantuan dalam perkuliahan dan hal-hal lain.
3. Bapak **Dr. Andi Muhammad Anwar, S.Si., M.Si.** sebagai pembimbing pendamping yang senantiasa memberikan dukungan dan masukan pada penulis serta telah banyak membantu dalam situasi yang sulit.
4. Bapak **Prof. Dr. Eng. Mawardi Bahri, S.Si., M.Si.** dan Bapak **Prof. Dr. Budi Nurwahyu, MS.** Yang telah memberikan masukan dan saran pada penulis dalam menyelesaikan penelitian ini.
5. Orantua tercinta, Ayahanda **Hi Nurdin Abdul Malik** dan Ibunda **Hj Hasniati Hamid** beserta seluruh keluarga yang senantiasa memberikan doa, kasih sayang, dan materi agar supaya bisa menuntut ilmu hingga bisa kuliah di Universitas Hasanuddin.

6. Seluruh dosen di Departemen Matematika FMIPA Universitas Hasanuddin yang telah memberikan pendidikan, pengajaran, bimbingan, dan berbagi ilmu pengetahuan kepada penulis.
7. Teman-teman seperjuangan **Matematika 2017** yang telah saling mendukung, menemani, dan membantu dalam proses perjuangan dalam menuntut ilmu.
8. Kakak-kakak senior dan adik-adik junior Program Studi Matematika.
9. Teman-teman **Tamalanrea 9 UNHAS** yang telah berjuang bersama dalam kegiatan KKN di tengah-tengah pandemi COVID 19.
10. Berbagai pihak yang tidak bisa disebutkan satu per satu telah memberikan bantuan pada penulis dalam menyelesaikan skripsi ini.

Semoga skripsi ini dapat memberikan manfaat dan sumbangan yang positif bagi perkembangan ilmu pengetahuan dan teknologi, khususnya dalam bidang keamanan informasi. Aamiin.

Makassar, 17 Maret 2023

Syaifullah Hi Nurdin

ABSTRAK

Kriptografi adalah ilmu tentang penyembunyian informasi berupa teks, gambar, atau bentuk lain ke bentuk serupa atau lain dengan tujuan informasi aslinya hanya diketahui oleh pihak tertentu. Kombinasi beberapa bidang matematika dapat digunakan dalam kriptografi seperti aljabar abstrak dan teori *chaos*. Aljabar abstrak berguna dalam pengembangan algoritma enkripsi yang rumit dipecahkan dengan memanfaatkan sifat bilangan. Sedangkan, teori *chaos* berguna untuk mengembangkan suatu sistem yang bersifat sulit diprediksi sebagai alat penambah keacakan pada algoritma enkripsi sehingga semakin sulit ditebak. Pada penelitian ini, penulis mengembangkan algoritma enkripsi/dekripsi dari penelitian yang dilakukan oleh Liu sebelumnya dengan menggunakan lapangan Galois berorde 256, serta kombinasi sistem *Chaos Hybrid* Cao dan sistem Vaidyanathan. Dalam penelitian ini diperoleh algoritma enkripsi/dekripsi yang menghasilkan citra enkripsi beberapa citra dengan distribusi pikselnya mendekati seragam serta sangat terpengaruh oleh nilai awal sistem yang dikembangkan.

Kata Kunci : Enkripsi, Dekripsi, Citra, Sistem *Chaos*, Lapangan Galois

ABSTRACT

Cryptography is the science of concealing information in the form of text, images, or other forms into similar or different forms with the aim that the original information is only known by certain parties. Several fields of mathematics can be used in cryptography such as abstract algebra and chaos theory. Abstract algebra is useful in developing complex encryption algorithms that can be solved by utilizing number properties. Meanwhile, chaos theory is useful in developing a system that is difficult to predict as a tool for adding randomness to encryption algorithms, making them even more difficult to decipher. In this research, the author developed an encryption/decryption algorithm based on previous research conducted by Liu using a Galois field of order 256, as well as a combination of Chaos Hybrid Cao system and Vaidyanathan system. The result of this research is an encryption/decryption algorithm that produces encrypted images with pixel distributions that are close to uniform and highly influenced by the initial values of the developed system.

Keywords : Encryption, Decryption, Image, *Chaos* System, Galois Field

DAFTAR ISI

PERNYATAAN KEASLIAN ii
KATA PENGANTAR v
ABSTRAK vii
ABSTRACT viii
DAFTAR ISI ix
DAFTAR TABEL xi
DAFTAR GAMBAR xii
BAB 1 PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 4
1.3 Batasan Masalah 4
1.4 Tujuan Penelitian 4
1.5 Manfaat Penelitian 4
BAB 2 TINJAUAN PUSTAKA 6
2.1 Citra Digital 6
2.2 Proses Enkripsi 10
2.3 Teori *Chaos* 11
2.4 Metode Runge-Kutta 17
2.5 Struktur Aljabar Lapangan Hingga 20
BAB 3 METODOLOGI PENELITIAN 33
3.1 Tahap Pendahuluan 33
3.2 Tahap Pemodifikasian 33
3.3 Tahap Pengaplikasian 34
3.4 Tahap Penyimpulan 34

3.5 Alur Kerja 35
BAB 4 PEMBAHASAN 36
4.1 Sistem Peta *Chaotic Hybrid* Cao 36
4.2 Penggunaan Metode Runge Kutta untuk Membentuk Peta dari Sistem Persamaan Diferensial 36
4.3 Masalah Komputasi Peta Vaidyanathan 37
4.4 Masalah Titik Tetap Peta *Chaotic Hybrid* Cao 38
4.5 Sistem Chaos Hybrid Baru Kombinasi Peta Hybrid Cao dan Vaidyanathan 40
4.6 Aritmetika dalam Proses Enkripsi/Dekripsi dengan Sistem Hybrid Baru 41
4.7 Algoritma Enkripsi Citra dengan Sistem Baru (4.4) 43
4.8 Algoritma Dekripsi Citra dengan Sistem Baru (4.4) 49
4.9 Bagan Alir Algoritma Enkripsi/Dekripsi dengan Sistem *Chaos* Baru 51
4.10 Pengaplikasian Algoritma pada Citra 54
BAB 5 KESIMPULAN DAN SARAN 81
5.1 Kesimpulan 81
5.2 Saran 82
DAFTAR PUSTAKA 83
LAMPIRAN 85

DAFTAR TABEL

Tabel 2.1 Tabel Operasi Grup Klein V 21

Tabel 2.2 Tabel Operasi di Lapangan $\mathbb{Z}_2[X]/[x^2+x+1]$.....28

Tabel 4.1 Tabel Kunci 1, 2, dan 3.....71

DAFTAR GAMBAR

Gambar 2.1 Contoh tampilan citra biner.....7

Gambar 2.2 Contoh tampilan citra *grayscale* 8

Gambar 2.3 Gambar representasi K_1,K_2,K_3 9

Gambar 2.4 Gambar representasi hasil komposisi K_1, K_2, K_3 9

Gambar 2.5 Grafik peta logistik dengan dua nilai awal yang hampir sama 13

Gambar 2.6 Grafik nilai x_n dan x'_n untuk $n \leq 50$ 14

Gambar 2.7 Grafik nilai y_n dan y'_n untuk $n \leq 50$ 14

Gambar 2.8 Grafik nilai x_n dan x'_n untuk $n \leq 100$.....15

Gambar 2.9 Grafik nilai y_n dan y'_n untuk $n \leq 100$ 15

Gambar 2.10 Grafik nilai x_n dan x'_n untuk $n \leq 70$ 16

Gambar 2.11 Grafik nilai y_n dan y'_n untuk $n \leq 70$ 16

Gambar 3.1 Bagan Alir Penelitian 35

Gambar 4.1 Bagan alir enkripsi bagian pertama.....51

Gambar 4.2 Bagan alir enkripsi bagian kedua 52

Gambar 4.3 Bagan alir dekrispi bagian pertama.....53

Gambar 4.4 Bagan alir dekripsi bagian kedua 54

Gambar 4.5 Tampilan citra *plaintext P* (kiri) dan *ciphertext* (kanan) 69

Gambar 4.6 Citra-citra *plaintext* 70

Gambar 4.7 Citra-citra *ciphertext* enkripsi P_1 dengan masing-masing kunci.....72

Gambar 4.8 Citra-citra *ciphertext* enkripsi P_2 dengan masing-masing kunci.....73

Gambar 4.9 Citra-citra *ciphertext* enkripsi P_3 dengan masing-masing kunci.....73

Gambar 4.10 Hasil dekripsi $C_{1,1}$ dengan masing-masing kunci 74

Gambar 4.11 Hasil dekripsi $C_{1,2}$ dengan masing-masing kunci 75

Gambar 4.12 Hasil dekripsi $C_{1,3}$ dengan masing-masing kunci 75

Gambar 4.13 Hasil dekripsi $C_{2,1}$ dengan masing-masing kunci 76

Gambar 4.14 Hasil dekripsi $C_{2,2}$ dengan masing-masing kunci 76

Gambar 4.15 Hasil dekripsi $C_{2,3}$ dengan masing-masing kunci 76

Gambar 4.16 Hasil dekripsi $C_{3,1}$ dengan masing-masing kunci 77

Gambar 4.17 Hasil dekripsi $C_{3,2}$ dengan masing-masing kunci 77

Gambar 4.18 Hasil dekripsi $C_{3,3}$ dengan masing-masing kunci 77

Gambar 4.19 Perbandingan pola yang muncul dari hasil dekripsi dan *plaintext*...78

Gambar 4.20 Hasil dekripsi $C_{3,3}$ dengan kunci 1 saat diberikan efek *fragment blur* 78

Gambar 4.21 Diagram distribusi frekuensi nilai piksel hasil enkripsi citra berukuruan kecil P_1 dan P_2 79

Gambar 4.22 Diagram distributsi frekuensi nilai piksel hasil enkripsi citra berukuran besar P_3 80

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi yang sudah sangat maju membuat kehidupan manusia semakin mudah. Beberapa teknologi yang tampak jelas perkembangannya antara lain adalah sistem komputer yang memungkinkan pengolahan citra digital berwarna dan sistem jaringan internet yang memungkinkan penyebaran data digital dengan cepat. Keberadaan teknologi ini tentu saja sangat membantu pekerjaan manusia misalnya dalam bidang jurnalistik, pencantuman gambar *thumbnail* pada berita daring sudah menjadi hal yang dianggap wajib sebagai ilustrasi atau berguna untuk menarik pembaca. Selain itu, di bidang kesehatan pengolahan dan pengiriman citra digital juga sering digunakan contohnya pada hasil rontgen (Mardhiyah, 2011), kamera mikroskop, dll. Sedangkan, dalam kehidupan sehari-hari teknologi ini biasa digunakan dalam media sosial yang memiliki fitur berbagi gambar.

Seperti data digital yang menyimpan informasi teks, terdapat pula citra digital yang bersifat rahasia karena menyangkut privasi dari pemilik gambar atau foto yang tersimpan pada citra digital tersebut. Misalnya foto hasil pemeriksaan seorang pasien di rumah sakit tidak boleh disebarluaskan tanpa izin dari pasien yang bersangkutan. Contoh lainnya adalah foto pribadi seseorang yang dikirim melalui aplikasi pengiriman pesan yang hanya boleh dilihat oleh orang yang diinginkan. Oleh sebab itu, diperlukan suatu metode agar bisa mengamankan citra digital sehingga isi dari citra digital tersebut tidak dapat dilihat oleh orang-orang yang tidak diinginkan. Metode-metode yang digunakan untuk mengamankan data digital merupakan topik dalam bidang ilmu kriptografi.

Citra digital merupakan data digital yang berupa larik (array) dua dimensi yang setiap nilai di setiap baris dan kolomnya menunjukkan warna pada posisi tersebut. Setiap posisi baris dan kolom pada citra digital disebut piksel. Mengingat citra digital pada umumnya merepresentasikan gambar atau foto yang bermakna bagi manusia, maka terdapat pola data pada citra tersebut sehingga setiap piksel akan mempunyai hubungan dengan piksel yang ada di dekatnya misalnya pada

foto apel merah, warna piksel di sekitar piksel berwarna merah kemungkinan besar juga ikut berwarna merah meskipun terdapat sedikit perbedaan seperti sedikit lebih terang, lebih gelap, atau sedikit mendekati warna kuning. Piksel berwarna biru sangat jarang ada di sekitar piksel yang berwarna merah kecuali di bagian pinggiran gambar apel jika seandainya latar belakangnya berwarna biru. Oleh karena itu, pada citra digital tidak hanya diberlakukan proses enkripsi dan dekripsi saja melainkan diperlukan adanya proses yang dapat menghilangkan sifat keterhubungan antara suatu piksel dengan piksel di dekatnya. Sifat keterhubungan pada citra ini disebut autokorelasi. Sifat ini perlu diperhatikan sebab jika suatu citra mempunyai pola, ada kemungkinan hasil enkripsinya juga memiliki pola sehingga memudahkan penyerang untuk menebak kunci yang digunakan dalam proses pengenkripsian.

Untuk mengatasi autokorelasi pada citra digital, diperlukan suatu algoritma yang dapat membuat citra digital yang awalnya berpola menjadi acak serta mengembalikannya seperti semula. Mengingat pemrosesan data digital pada komputer bersifat deterministik, maka algoritma tersebut juga harus bersifat deterministik dengan bergantung pada beberapa parameter yang disebut nilai-nilai awal. Selain itu, algoritma tersebut juga harus mempunyai sifat tak dapat diprediksi agar bisa menghasilkan keacakan meskipun nilai-nilai awalnya diubah sedikit. Kedua sifat ini yakni deterministik dan tak dapat diprediksi merupakan sifat yang dimiliki oleh sistem *chaos*. Dengan kedua sifat ini, sistem *chaos* sangat cocok digunakan sebagai RNG (*Random Number Generator*) untuk membangkitkan kunci secara acak.

Pengenkripsian data dengan menggunakan sistem *chaos* sudah banyak diterapkan pada berbagai kriptosistem. Salah satu contohnya adalah sistem *chaos* dapat digunakan sebagai pembangkit kunci pada AES (Arab dkk, 2019). Selain itu, kriptosistem berbasis sistem *chaos* sudah banyak diusulkan dengan dikombinasikan dengan teori-teori lain matematika khususnya pada bidang aljabar abstrak. Beberapa sistem *chaos* yang pernah digunakan pada kriptosistem berbasis *chaos* antara lain peta logistik (*logistic map*), peta Hénon (Hénon *map*), peta Ikeda (Ikeda *map*) (Cao, 2013), sistem *cubic jerk* (Vaidyanathan, 2017), sistem *chaos* Hussein (Hussein dkk, 2019), peta Bernoulli (Revanna, Keshavamurthy, 2020),

dan bahkan ada usulan desain kriptosistem yang menggunakan sistem *hyper chaotic* seperti sistem Chen (Liu dkk, 2019). Sistem-sistem *chaos* tersebut diimplementasikan dan dikombinasikan dengan teori lain pada matematika dan skema-skema kriptosistem yang sudah ada sebelumnya misalnya Liu dkk (2019) mengombinasikan sistem *chaos* dengan teori lapangan Galois.

Liu dkk (2019) mengembangkan skema enkripsi dengan cara merepresentasikan nilai-nilai intensitas warna piksel pada citra digital yang nilainya berupa bilangan bulat dalam rentang 0 sampai 255 sebagai polinomial yang ada di lapangan Galois dengan banyak elemen 256, $GF(256)$. Dalam algoritma enkripsi/dekripsinya, nilai-nilai pada piksel ini kemudian dioperasikan bersama barisan bilangan bulat acak antara 0 sampai 255 yang juga direpresentasikan sebagai polinomial di $GF(256)$ dengan menggunakan operasi aritmetika (penjumlahan dan perkalian) di lapangan $GF(256)$. Barisan acak ini dihasilkan dari suatu algoritma dengan memanfaatkan sifat sistem *chaos* yang sulit terprediksi.

Menurut Liu dkk (2019) di "*Color pathological image encryption algorithm using arithmetic over Galois field and coupled hyper chaotic system*", skema-skema berbasis perkalian polinomial di lapangan Galois belum ada yang terlaporkan sehingga skema-skema berbasis *chaos* dan perkalian di lapangan Galois dapat dikatakan masih jarang diusulkan. Oleh karena itu, penelitian ini akan membahas skema baru menggunakan operasi pada lapangan Galois dengan cara memodifikasi skema usulan Liu dkk dan menggunakan sistem *chaos* yang berbeda. Dalam hal ini, sistem *chaos* yang digunakan adalah sistem *chaos hybrid* 6 dimensi atau lebih hasil komposisi dari beberapa sistem *chaos*. Sistem-sistem *chaos* yang dikomposisikan pada penelitian ini adalah peta logistik, Hénon, peta Ikeda. Sistem-sistem ini pernah digunakan oleh Cao dalam konstruksi sistem *chaos* 5 dimensi. Selain ketiga sistem *chaos* tersebut, sistem yang lebih mutakhir yakni sistem *cubic jerk* Vaidyanathan juga akan digunakan untuk melengkapi sistem sehingga menjadi 6 dimensi. Dengan demikian, masalah yang akan diselesaikan adalah penentuan sistem *chaos hybrid* dan pengembangan skema enkripsi menggunakan skema enkripsi tersebut. Berdasarkan uraian masalah tersebut, maka hasil dari penelitian ini dituangkan dalam skripsi berjudul

"*Algoritma Enkripsi Citra dengan Menggunakan Lapangan Galois dan Sistem Chaos Hybrid*".

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, maka rumusan masalah yang akan dibahas, yaitu:

a. Bagaimana konstruksi sistem *chaos hybrid* hasil komposisi peta logistik, Hénon, dan Ikeda serta sistem *cubic jerk*?
b. Bagaimana algoritma enkripsi dan dekripsi citra menggunakan sistem *chaos hybrid* yang telah dikonstruksi dan perkalian polinomial pada lapangan Galois?

1.3 Batasan Masalah

Pembahasan masalah hanya terbatas pada konstruksi sistem *chaos hybrid* serta pengimplementasiannya dalam pengembangan algoritma enkripsi dan dekripsi citra. Pada penelitian ini analisis kekacauan, distribusi frekuensi piksel pada hasil enkripsi, serta analisis keamanan dan efisiensi belum dilakukan sehingga menjadi masalah terbuka untuk penelitian-penelitian berikutnya. Selain itu, citra yang akan digunakan dalam proses enkripsi/dekripsi adalah citra dengan format *TrueColor*, yakni citra yang setiap pikselnya menyimpan 24 bit informasi warna yang terbagi menjadi 3 komponen warna.

1.4 Tujuan Penelitian

Tujuan penelitian yakni untuk:

a. Menentukan konstruksi sistem *chaos hybrid* dengan komposisi peta logistik, Hénon, dan Ikeda serta sistem *cubic jerk*.
b. Mengembangkan algoritma enkripsi dan dekripsi citra menggunakan sistem *chaos hybrid* yang telah dikonstruksi dan perkalian polinomial pada lapangan Galois.

1.5 Manfaat Penelitian

Penelitian ini bermanfaat untuk menambah wawasan serta pengetahuan tentang sistem *chaos*, lapangan Galois, dan pengaplikasiannya dalam kriptografi. Selain itu, penelitian ini juga dapat menghasilkan pengeluaran berupa program

yang bisa digunakan untuk melakukan enkripsi/dekripsi citra dan dapat dimodifikasi sesuai kebutuhan.

BAB 2
TINJAUAN PUSTAKA

2.1 Citra Digital

Definisi 2.1 ***(Citra)*** *Misalkan* $A \subseteq \mathbb{R}^2$. *Suatu citra adalah fungsi* $f: A \to B$ *dengan* B *adalah suatu himpunan yang dapat berupa himpunan bilangan rill atau kompleks. Nilai* f *pada suatu titik* (x, y) *disebut intensintas atau tingkat keabuan pada titik tersebut.*

Definisi 2.2 ***(Citra Digital)*** *Citra digital adalah fungsi* $f: A \to B$ *dengan* $A = \{1,2, \dots, M\} \times \{1,2,3, \dots, N\}$ *untuk suatu bilangan-bilangan asli* M, N *dan* B *adalah suatu himpunan berhingga.*

Pemrosesan citra digital dilakukan dengan menggunakan komputer digital. Sebagai data dalam komputer, citra digital dapat direpesentasikan sebagai fungsi $f: \{1,2, \dots, M\} \times \{1,2,3, \dots, N\} \to \mathbb{N}$ atau sebagai matriks bilangan asli berukuran $M \times N$ dengan $M, N \in \mathbb{N}$. (Jain, 1989; Gonzalez dan Woods, 2008)

2.1.1 Macam-Macam Citra Digital

Terdapat banyak jenis format citra digital yang masing-masing mempunyai kelebihan dan kekurangan dari segi efisiensi dalam penyimpanan ataupun dari segi banyaknya warna yang dapat ditampilkan. Beberapa jenis model citra digital antara lain citra biner, citra skala abu-abu (*grayscale*), dan citra RGB.

2.1.1.1 Model Citra Digital Biner (Citra Hitam-Putih)

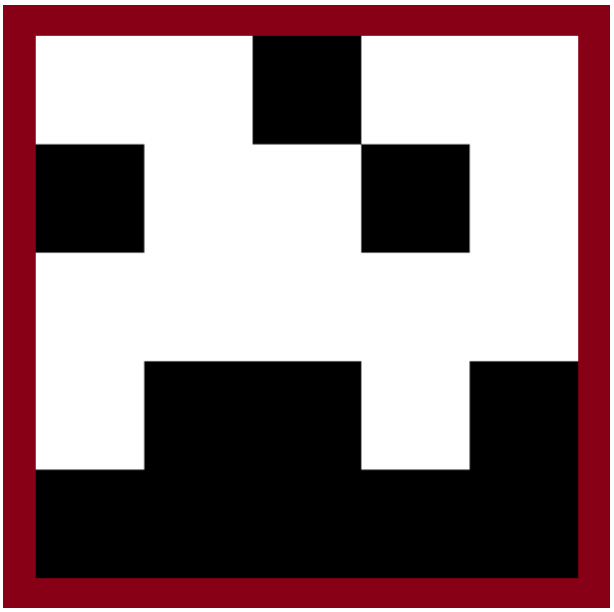
Citra digital biner atau citra biner adalah citra yang setiap pikselnya hanya mempunyai nilai 0 atau 1. Dengan kata lain, kodomain dari citra biner adalah himpunan $\{0,1\}$. Saat citra biner ditampilkan, nilai 0 ditunjukkan dengan warna hitam dan nilai 1 ditunjukkan dengan warna putih. (Jung dan Yoo, 2009).

Contoh 2.1

Misalkan suatu citra biner berukuran 5×5 direpresentasikan dalam bentuk matriks berikut.

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Apabila citra ini ditampilkan maka akan menghasilkan gambar yang dapat dilihat pada Gambar 2.1 (bingkai merah hanya pembatas dan bukan bagian dari citra).



Gambar 2.1 Contoh tampilan citra biner

2.1.1.2 Model Citra Digital *Grayscale* (Skala abu-abu)

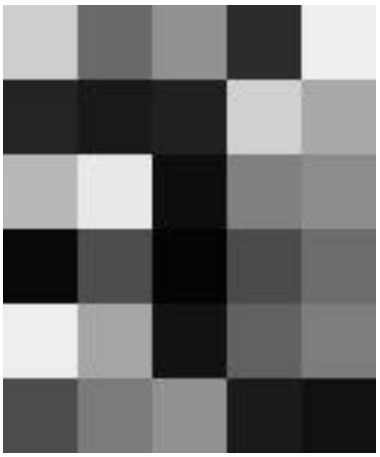
Citra digital *grayscale* atau citra *grayscale* adalah citra yang mempunyai kodomain yang lebih besar daripada citra biner. Nilai-nilai di tiap piksel pada citra *grayscale* sudah dapat menunjukkan intensitas atau tingkat kecerahan cahaya tapi tidak menunjukkan informasi warna. Sesuai dengan namanya, citra *grayscale* dapat ditampilkan sebagai gambar yang hanya mempunyai warna dalam skala abu-abu. (Kumar dan Verma, 2010)

Contoh 2.2

Misalkan G adalah suatu citra *grayscale* berukuran 6×5 serta nilai pada tiap pikselnya berupa bilangan bulat di $[0,255]$ dengan 0 menunjukkan intensitas cahaya paling gelap dan 255 menunjukkan intensitas cahaya paling terang. Misalkan pula nilai-nilai pada tiap piksel di G ditunjukkan oleh matriks

$$\begin{pmatrix} 206 & 105 & 146 & 44 & 239 \\ 36 & 25 & 33 & 209 & 169 \\ 184 & 233 & 14 & 129 & 140 \\ 8 & 77 & 4 & 75 & 108 \\ 238 & 166 & 18 & 98 & 125 \\ 76 & 123 & 145 & 27 & 17 \end{pmatrix}.$$

Gambar dari citra G dapat dilihat pada Gambar 2.2.



Gambar 2.2 Contoh tampilan citra *grayscale*

2.1.1.3 Model Citra Digital Berwarna Model RGB

Citra digital berwarna model RGB adalah citra digital yang terdiri atas 3 komponen citra digital *grayscale* berukuran seragam yang masing-masing secara berurutan mewakili komponen warna merah, hijau, dan biru. Nilai pada setiap piksel pada tiap komponen menunjukkan intensitas warna yang bersesuaian pada piksel tersebut. Saat citra digital berwarna ditampilkan, ketiga warna pada tiap piksel berkomposisi dan menghasilkan warna baru saat dilihat misalnya warna merah dan hijau berkomposisi menghasilkan warna kuning. Citra digital berwarna dapat dipandang sebagai suatu fungsi $f: \{1,2, \dots, M\} \times \{1,2,3, \dots, N\} \times \{1,2,3\} \to \mathbb{R}$, fungsi $f: \{1,2, \dots, M\} \times \{1,2,3, \dots, N\} \to \mathbb{R}^3$ atau $array$ (larik) berukuruan $M \times N \times 3$ dengan entri-entri bilangan riil. (Jain, 1989)

Contoh 2.3

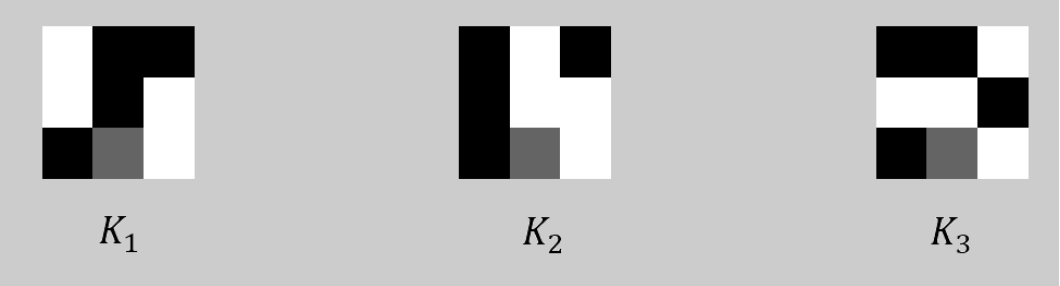
Misalkan suatu citra digital berwarna berukuran 3×3 dengan nilai 0 menunjukkan intensitas cahaya paling gelap dan 255 menunjukkan intensitas paling terang serta komponen-komponenya adalah K_1, K_2, K_3 sebagai berikut.

$$K_1 = \begin{pmatrix} 255 & 0 & 0 \\ 255 & 0 & 255 \\ 0 & 100 & 255 \end{pmatrix},$$

$$K_2 = \begin{pmatrix} 0 & 255 & 0 \\ 0 & 255 & 255 \\ 0 & 100 & 255 \end{pmatrix},$$

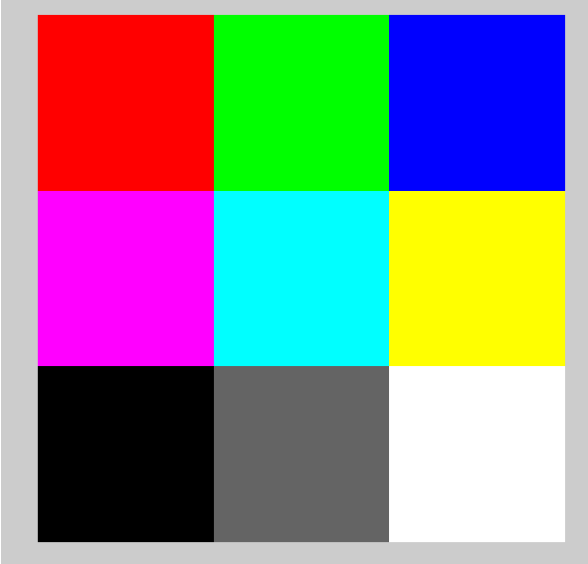
$$K_3 = \begin{pmatrix} 0 & 0 & 255 \\ 255 & 255 & 0 \\ 0 & 100 & 255 \end{pmatrix}.$$

Sebagai citra *grayscale*, gambar yang direpresentasikan oleh K_1, K_2, K_3 dapat dilihat pada Gambar 2.3.



Gambar 2.3 Gambar representasi K_1, K_2, K_3

Selanjutnya, gambar berwarna yang direpresentasi oleh ketiga komponen tersebut dapat dilihat pada Gambar 2.4.



Gambar 2.4 Gambar representasi hasil komposisi K_1, K_2, K_3

2.2 Proses Enkripsi

Definisi 2.3 (*Skema Enkripsi*) *Suatu skema enkripsi atau kriptosistem adalah suatu tuple* (P, C, K, E, D) *dengan sifat-sifat sebagai berikut:*

1. P *adalah suatu himpunan.* P *disebut ruang plaintext serta elemen-elemennya disebut plaintext.*
2. C *adalah suatu himpunan.* C *disebut ruang ciphertext serta elemen-elemennya disebut ciphertext.*
3. K *adalah suatu himpunan.* K *disebut ruang kunci serta elemen-elemennya disebut kunci.*
4. $E = \{e_k : k \in K\}$ *adalah keluarga fungsi* $e_k : P \to C$. *Elemen-elemennya disebut fungsi enkripsi.*
5. $D = \{d_k : k \in K\}$ *adalah keluarga fungsi* $d_k : C \to P$. *Elemen-elemennya disebut fungsi dekripsi.*
6. *Untuk setiap* $m \in K$ *terdapat* $s \in K$ *sedemikian sehingga* $d_s(e_m(p)) = p$ *untuk setiap* $p \in P$. (Buchmann, 2001)

Contoh 2.4 (*Sandi Caesar*)

Skema enkripsi sandi Caesar adalah *tuple* (P, C, K, E, D) dengan P, C, K adalah himpunan huruf latin {A,B,C, …,Z}. Misalkan setiap huruf A,B,C, ..., dan Z secara berturut-turut diwakili oleh bilangan $0, 1, 2$, ..., dan 25. Dengan demikian, $\text{A} = 0$, $\text{B} = 1$, dst. Untuk setiap $m \in K$ aturan pemetaan fungsi enkripsi $e_m \in E$, dengan $e_m : P \to C$ adalah $e_m(p) = p + m \pmod{26}$ untuk setiap $p \in P$. Sedangkan, aturan pemetaan fungsi dekripsi $d_s \in D$ dengan $d_s : C \to P$ untuk setiap $s \in K$ adalah $d_s(c) = c - s \pmod{26}$.

Dalam kasus skema ini, kunci dekripsi dan enkripsi sama yakni $m = s$. Sebab, untuk setiap $p, m \in \{\text{A,B,C, …,Z}\} = \{0,1,2,3 \ldots,25\}$ berlaku $d_m(e_m(p)) = p + m - m \pmod{26} = p$.

Sebagai contoh, jika pesan “ABRAXAS GROSSULARIATA” dienkripsi dengan menggunakan kunci enkripsi $m = 1 \in K$ maka diperoleh hasil enkripsinya adalah “BCSBYBT HSPTTVMBSJBUB” karena dengan enkripsi tiap huruf diperoleh $e_1(\text{A}) = e_1(0) = 0 + 1 \pmod{26} = 1 = \text{B}$, $e_1(\text{B}) = \text{C}$, dst.

2.3 Teori *Chaos*

Definisi 2.4 ***(Peta dan Orbit)*** *Suatu peta adalah fungsi* $f: \mathbb{R}^n \to \mathbb{R}^n$. *Dengan peta* f *yang diberikan, didefinisikan orbit dari suatu titik* $x \in \mathbb{R}^n$ *adalah barisan*

$$(x, f(x), f\big(f(x)\big), \dots, f^n(x), \dots)$$

dengan $f^n(x) = f(f^{n-1}(x))$ *yang disebut sebagai iterasi ke-n dari* f.

Untuk selanjutnya orbit tersebut dapat dinyatakan sebagai relasi rekurensi

$$x_{n+1} = f(x_n)$$

dengan $x_1 = x$. (Glendinning, 1994; Nagashima, 1999)

Contoh 2.5

Peta $f: \mathbb{R}^2 \to \mathbb{R}^2$ dengan $f(x) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} x$ untuk setiap $x \in \mathbb{R}^2$ adalah peta rotasi yang merotasi setiap vektor di $\mathbb{R}^2$ terhadap titik $(0,0)$ sebesar 90° berlawanan arah jarum jam. Orbit dari $(1,0)^t \in \mathbb{R}^2$ dengan peta tersebut adalah

$$\left((1,0)^t, (0,1)^t, (-1,0)^t, (0,-1)^t, \dots, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^n (1,0)^t, \dots\right)$$

Definisi 2.5 ***(Periode)*** *Suatu peta* f *dikatakan berperiode k jika terdapat c elemen dari domain* f *sehingga* $c, f(c), f^2(c), \dots, f^{k-1}$ *berbeda dan* $f^k(c) = c$. (Glendinning, 1994)

Contoh 2.6

Peta f pada Contoh 2.5 mempunyai periode 4 sebab untuk setiap $x \in \mathbb{R}^2$ dengan x taknol $x, f(x), f^2(x), f^3(x)$ berbeda dan $f^4(x) = x$. Peta f juga mempunyai periode 1 sebab $f(\mathbf{0}) = \mathbf{0}$.

2.3.1 Sistem *Chaos*

Kata *chaos* berasal dari bahasa Yunani *χάος* (kháos) yang berarti jurang. Kemudian, dalam kehidupan sehari-hari kata *chaos* biasanya diartikan sebagai "keadaan yang takberaturan" atau "kekacauan". Dalam teori *chaos*, *chaos* merujuk pada sistem dinamik atau sistem persamaan yang berperilaku tidak beraturan, tak dapat diprediksi walaupun bersifat deterministik, serta sensitif

terhadap kondisi awal. Biasanya sistem-sistem nonlinier adalah sistem yang seperti ini. (Glendinning, 1994; Nagashima, 1999)

2.3.2 Tolok Ukur Kekacauan (*Chaotic*)

Suatu sistem yang *chaos* dapat dinilai secara kualitatif melalui pengamatan atau secara kuantitatif dengan membuat batasan definisi sistem *chaos*. Salah satu definisi dari peta yang *chaotic* menggunakan konsep tapal kuda (*horseshoe*).

Definisi 2.6 ***(Tapal Kuda)*** *Misalkan f adalah peta kontinu pada suatu interval I. Peta f mempunyai tapal kuda jika dan hanya jika terdapat $J \subseteq I$ serta subinterval saling lepas $K_1, K_2 \subseteq J$ sehingga $f(K_1) = f(K_2) = J$.* (Glendinning, 1994)

Definisi 2.7 ***(Fungsi Chaotic)*** *Suatu peta kontinu f dikatakan chaotic jika dan hanya jika f^n mempunyai tapal kuda untuk suatu $n \geq 1$.* (Glendinning, 1994)

Teorema 2.1 ***(Teorema Li Yorke)*** *Jika suatu peta kontinu $f: [a, b] \to \mathbb{R}$ mempunyai orbit berperiode 3 atau lebih maka f chaotic.* (Glendinning, 1994)

2.3.3 Contoh-Contoh Sistem *Chaos*

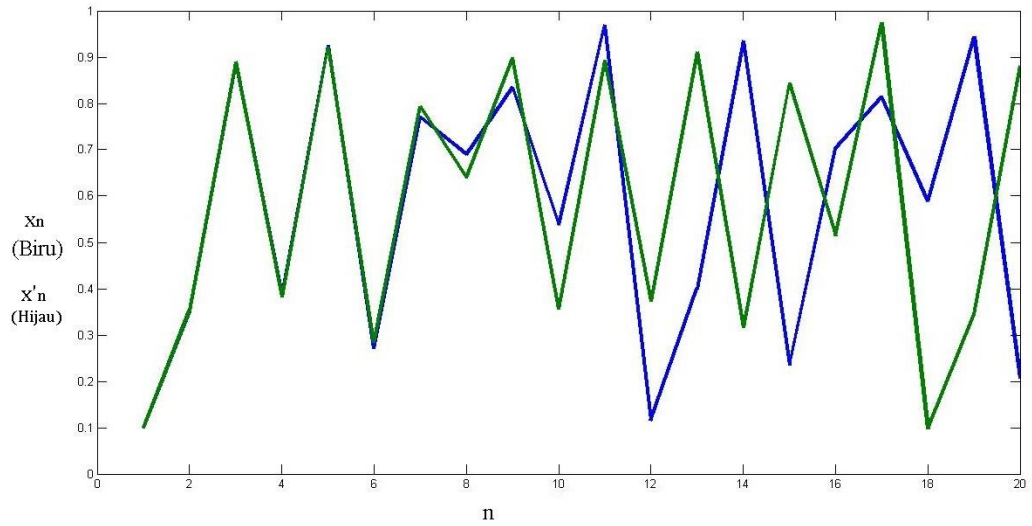
Contoh 2.7 ***(Peta Logistik)*** (May, 1974)

Suatu peta logistik adalah pemetaan polinomial berderajat dua sebagai berikut.

$$x_{n+1} = cx_n(1 - x_n) \tag{2.1}$$

dengan $x_n \in (0,1)$ dan $c \in (3.57, 4]$.

Dengan menggunakan nilai parameter $c = 3.9$, serta dengan dua nilai awal berbeda tapi lumayan dekat $x_1 = 0.1$ dan $x_1' = 0.1004$, diperoleh grafik barisan (x_n) dan (x_n') untuk $n = 1,2, \ldots, 20$ pada Gambar 2.5.



Gambar 2.5 Grafik peta logistik dengan dua nilai awal yang hampir sama

Dapat diamati bahwa di saat-saat awal atau saat $n < 12$, nilai x_n hampir sama dengan nilai x_n' serta mengalami kenaikan dan penurunan di saat yang sama (selaras). Namun, karena sifat *chaotic* dari peta ini, dalam jangka panjang nilai x_n dan x_n' akan berbeda jauh yang sudah dapat dilihat saat $n \geq 12$. Bahkan, kenaikan serta penurunan nilai x_n dan x_n' sudah tidak selaras lagi meskipun menggunakan nilai awal yang hampir sama.

Contoh 2.8 ***(Peta Ikeda)*** (Ikeda, 1979)

Peta Ikeda adalah sistem *chaos* dua dimensi diskrit sebagai berikut.

$$x_{n+1} = 1 + u\left(x_n \cos\left(c - \frac{6}{1 + x_n^2 + y_n^2}\right) - y_n \sin\left(c - \frac{6}{1 + x_n^2 + y_n^2}\right)\right)$$

$$y_{n+1} = u\left(x_n \sin\left(c - \frac{6}{1 + x_n^2 + y_n^2}\right) - y_n \cos\left(c - \frac{6}{1 + x_n^2 + y_n^2}\right)\right) \qquad (2.2)$$

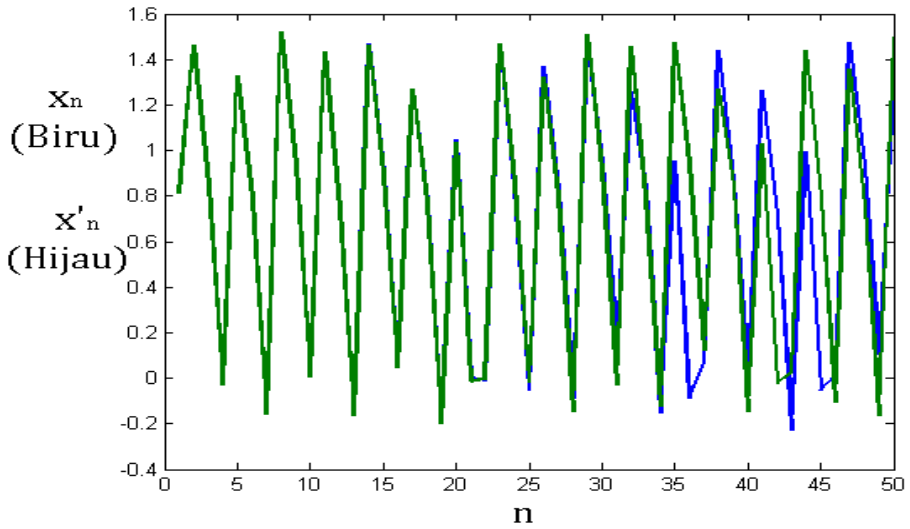
dengan u dan c adalah parameter.

Selanjutnya, dengan memisalkan $t_n = c - \frac{6}{1+x_n^2+y_n^2}$, Sistem (2.2) berubah menjadi Sistem (2.3).

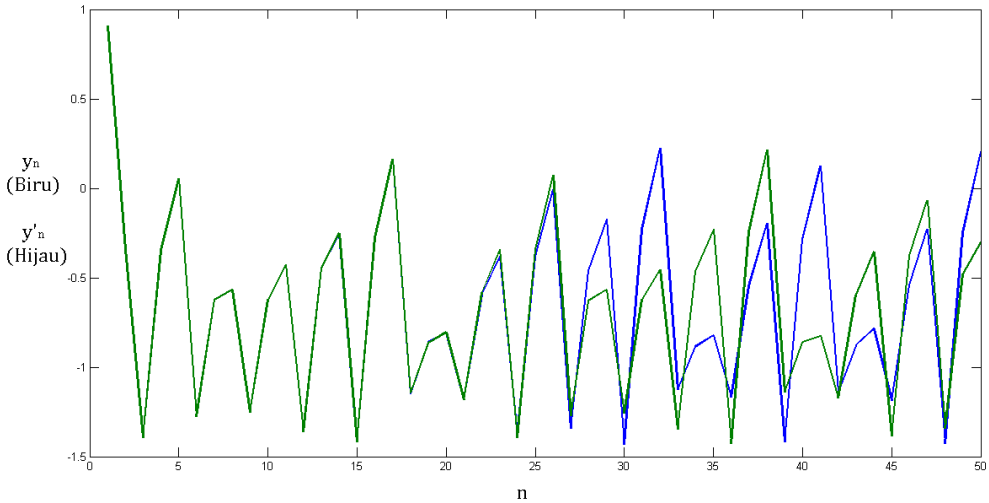
$$x_{n+1} = 1 + u(x_n \cos t_n - y_n \sin t_n)$$

$$y_{n+1} = u(x_n \sin t_n - y_n \cos t_n) \qquad (2.3)$$

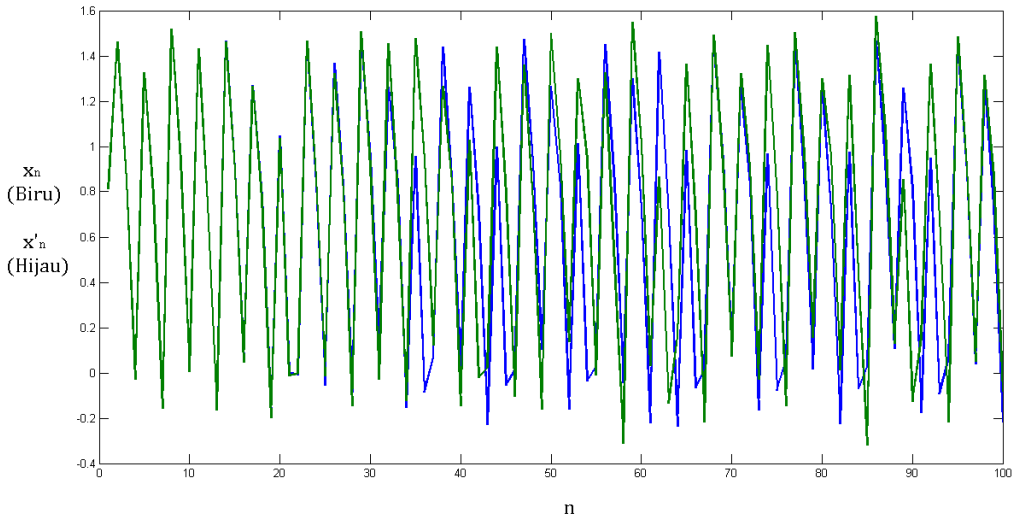
Misalkan $c = 0.4$, $u = 0.99$, serta dua pasang nilai awal yang lumayan dekat $(x_1, y_1) = (0.81479, 0.9058)$, dan $(x_1', y_1') = (0.8148, 0.905798)$. Grafik dari peta Ikeda dengan nilai-nilai awal tersebut dapat dilihat pada Gambar 2.6, Gambar 2.7, Gambar 2.8, dan Gambar 2.9.



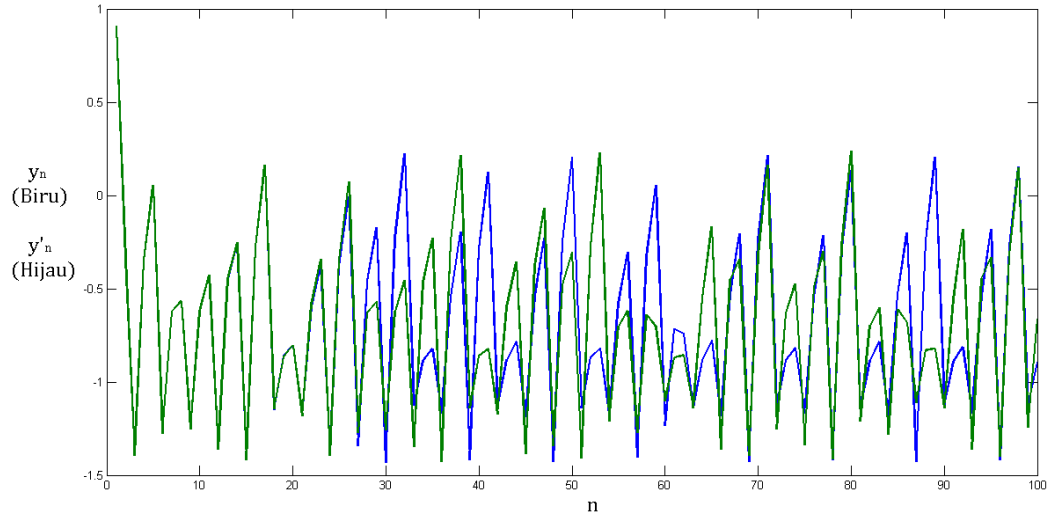
Gambar 2.6 Grafik nilai x_n dan x_n' untuk $n \leq 50$



Gambar 2.7 Grafik nilai y_n dan y_n' untuk $n \leq 50$



Gambar 2.8 Grafik nilai x_n dan x'_n untuk $n \leq 100$



Gambar 2.9 Grafik nilai y_n dan y'_n untuk $n \leq 100$

Dapat diamati bahwa pada saat-saat awal (n relatif kecil), nilai (x_n, y_n) dan (x'_n, y'_n) masih lumayan dekat sehingga kedua kurva pada grafiknya tampak saling berimpit untuk n yang kecil. Namun, untuk n yang lumayan besar atau untuk jangka panjang, nilai (x_n, y_n) akan sangat berbeda dengan nilai (x'_n, y'_n).

Contoh 2.9 ***(Peta Hénon)*** (Hénon, 1976)

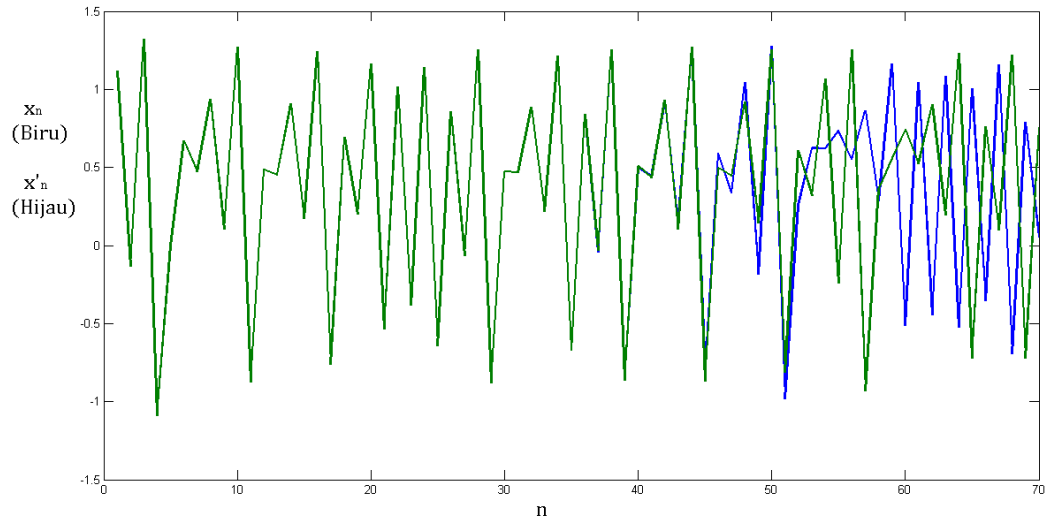
Peta Hénon adalah peta *chaotic* nonlinier yang bersifat reversibel. Peta Hénon didefinisikan sebagai berikut.

$$x_{n+1} = 1 - ax_n^2 + y_n$$

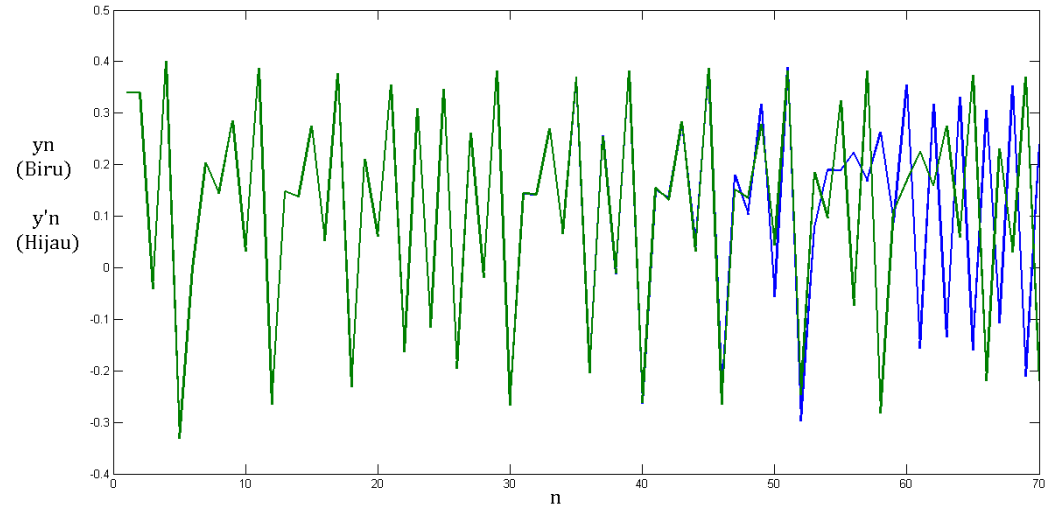
$$y_{n+1} = bx_n \tag{2.4}$$

dengan $a \in (0, 1.4]$ dan $b \in (0.2, 0.314]$ adalah parameter kontrol. Peta ini dikatakan bersifat reversibel karena jika (x_{n+1}, y_{n+1}) diketahui untuk suatu bilangan asli n maka pasangan (x_n, y_n) dapat diperoleh secara tunggal.

Dengan pemilihan parameter $a = 1.1778$, $b = 0.3041$, serta dua pasang nilai awal $(x_1, y_1) = (1.1178, 0.3399)$ dan $(x_1', y_1') = (1.1178, 0.339902)$, grafik peta Hénon dapat dilihat pada Gambar 2.10 dan Gambar 2.11.



Gambar 2.10 Grafik nilai x_n dan x_n' untuk $n \leq 70$



Gambar 2.11 Grafik nilai y_n dan y_n' untuk $n \leq 70$

Contoh 2.10 ***(Sistem Jerk Baru)*** (Vaidyanathan, 2017)

Sistem *jerk* yang dikembangkan oleh Vaidyanathan adalah sistem *jerk* baru hasil pengembangan sistem *jerk* sebelumnya. Sistem ini merupakan sistem persamaan diferensial yang bersifat *chaotic*. Bentuk sistem persamaan ini adalah sebagai berikut.

$$\begin{aligned} \dot{x_1} &= x_2 \\ \dot{x_2} &= x_3 \\ \dot{x_3} &= -ax_1 + bx_1x_2 - cx_3 + px_1x_2^2 - qx_1^3 \end{aligned} \tag{2.5}$$

dengan $a, b, c, p,$ dan q adalah parameter-parameter bilangan riil.

2.4 Metode Runge-Kutta

Metode Runge-Kutta adalah metode yang dapat digunakan untuk menyelesaikan persamaan diferensial. Metode ini merupakan hasil modifikasi dari metode Taylor dengan mempertahankan batas orde kesalahan serta menghilangkan keharusan untuk menghitung turunan parsial dari fungsi yang terdapat pada persamaan. (Faires, 2002)

Metode Runge-Kutta dapat digunakan untuk menyelesaikan masalah nilai awal yang berupa persamaan diferensial berbentuk $y' = f(x, y)$ dan mempunyai banyak variasi dengan tingkat ketelitian dan kompleksitas yang berbeda-beda.

2.4.1 Metode Runge-Kutta Orde 2

Metode Runge-Kutta yang sederhana adalah metode Runge-Kutta berorde 2 yang terkenal dengan nama metode *midpoint* (metode titik tengah).

Misalkan terdapat masalah nilai awal sebagai berikut.

$$\begin{aligned} &\frac{dy}{dx} = f(x, y) \\ &y(x_0) = y_0 \end{aligned} \tag{2.6}$$

dengan y adalah fungsi terhadap variabel x pada interval $[x_0, x_t]$, serta nilai awal x_0, y_0, dan fungsi dua variabel f diberikan. Masalah nilai awal ini bisa diselesaikan secara numerik. Pertama-tama, diskritisasi dilakukan dengan mempartisi interval domain y menjadi beberapa subinterval yang rentangnya sama. Misalkan banyaknya subinterval adalah n sehingga subinterval-subinterval

hasil partisinya adalah $[x_0, x_1]$, $[x_1, x_2]$, $[x_2, x_3]$, …, $[x_{n-1}, x_n]$ dengan $x_n = x_t$, $x_i < x_j$ jika dan hanya jika $i < j$, dan $x_i - x_{i-1} = x_j - x_{j-1}$ untuk setiap $i, j = 1,2,3, \dots, n$. Diperoleh rentang dari setiap subinterval adalah $h = x_1 - x_0 = \frac{1}{n}$. Selanjutnya, misalkan nilai pendekatan dari $y(x_0 + ih) = y(x_i)$ adalah y_i untuk $1 \leq i \leq n$ yang diperoleh dengan menggunakan algoritma berikut.

$$y_{i+1} = y_i + hf\left(x_i + \frac{h}{2}, y_i + \frac{h}{2} f(x_i, y_i)\right)$$

untuk $0 \leq i \leq n - 1$. Dengan demikian nilai fungsi y pada batas-batas subinterval telah didekati oleh nilai-nilai $y_0, y_1, \dots, y_n$. Selanjutnya, dengan mengasumsikan y kontinu, nilai-nilai fungsi y pada titik selain titik batas subinterval dapat didekati dengan berbagai macam metode interpolasi.

2.4.2 Metode Runge-Kutta Orde 4

Metode Runge-Kutta Orde 4 (RK4) merupakan metode yang lebih rumit dibandingkan dengan metode *midpoint.* Namun, metode ini mempunyai orde kesalahan yang lebih tinggi sehingga dapat dijadikan sebagai pengganti metode *midpoint* apabila perhitungan pendekatan solusi dari suatu masalah nilai awal diinginkan lebih akurat. Penyelesaian Masalah Nilai Awal (2.6) dapat diselesaikan dengan cara serupa dengan metode *midpoint* yakni dengan dilakukan diskritisasi interval menjadi subinterval-subinterval dengan rentang h kemudian nilai pendekatan $y_1, y_2, \dots, y_n$ dapat diperoleh dengan algoritma berikut.

Untuk setiap $i = 0, 1, 2, \dots, n - 1$, diperoleh

$$y_{i+1} = y_i + \frac{1}{6}(k_1 + 2k_2 + 2k_3 + k_4)$$

dengan

$$k_1 = hf(x_i, y_i),$$
$$k_2 = hf\left(x_i + \frac{h}{2}, y_i + \frac{1}{2}k_1\right),$$
$$k_3 = hf\left(x_i + \frac{h}{2}, y_i + \frac{1}{2}k_2\right), \text{ dan}$$
$$k_4 = hf(x_{i+1}, y_i + k_3). \text{ (Faires, 2002)}$$

2.4.2.1 Metode Runge-Kutta Orde 4 untuk Sistem Persamaan Diferensial

Skema metode Runge-Kutta Orde 4 dapat diperumum sehingga tidak hanya dapat menyelesaikan masalah nilai awal yang berupa persamaan diferensial dengan orde 1 tapi juga dapat digunakan untuk menyelesaikan persamaan diferensial berorde tinggi atau sistem persamaan diferensial. Dalam hal ini, persamaan diferensial berorde tinggi dikonversi ke dalam bentuk sistem persamaan diferensial terlebih dahulu dengan memisalkan variabel-variabel baru sebagai turunan pertama, kedua, dst dari variabel terikat lalu kemudian diselesaikan dengan metode Runge-Kutta.

Misalkan terdapat masalah nilai awal sebagai berikut.

$$y^{(n)} = f(x, y, y', y'', \dots, y^{(n-1)})$$

$$y^{(i)}(x_0) = \alpha_i, i = 0,1,2, \dots, n-1 \tag{2.7}$$

dengan y adalah fungsi terhadap variabel x pada interval $[x_0, x_t]$, serta nilai awal x_0, α_0, α_1, α_2, ..., α_{n-1}, fungsi dua variabel f diberikan, dan disepakati $y^{(0)} = y$. Masalah nilai awal ini dapat dijadikan sistem persamaan diferensial dengan memisalkan variabel-variabel $z_i = y^{(i)}$ untuk setiap $i = 0,1,2, \dots, n-1$. Dengan demikian, sistem persamaan yang terbentuk dari Masalah Nilai Awal (2.7) adalah sebagai berikut.

$$z_i' = z_{i+1}, i = 0,1,2,3, \dots, n-2$$

$$z_{n-1}' = f(x, z_0, z_1, z_2, \dots, z_{n-1})$$
$$z_i(x_0) = \alpha_i, i = 0,1,2, \dots, n-1. \tag{2.8}$$

Masalah Nilai Awal (2.8) yang berupa sistem persamaan diferensial dapat diselesaikan dengan menggunakan metode RK4. Bahkan, bentuk Masalah Nilai Awal yang lebih umum seperti Masalah Nilai Awal (2.9) dapat diselesaikan dengan RK4.

$$z_i' = f_i(x, z_0, z_1, z_2, \dots, z_{n-1}), i = 0,1,2,3, \dots, n-1$$

$$z_i(x_0) = \alpha_i, i = 0,1,2, \dots, n-1 \tag{2.9}$$

dengan $z_0, z_1, \dots, z_{n-1}$ adalah fungsi-fungsi terhadap variabel x pada interval $[x_0, x_t]$, serta nilai awal x_0, α_0, α_1, α_2, ..., α_{n-1}, dan fungsi-fungsi $n+1$ variabel $f_0, f_1, \dots, f_{n-1}$ diberikan.

Selanjutnya, Masalah Nilai Awal (2.9) dapat diselesaikan dengan cara yang serupa dengan pennyelesaian Masalah Nilai Awal (2.6) yakni dilakukan diskritisasi dengan mempartisi domain menjadi beberapa subinterval yang mempunyai rentang h sehingga diperoleh N+1 titik batas. Misalkan $w_{i,j}$ adalah nilai pendekatan dari $z_i(x_0 + jh) = z_i(x_j)$ untuk setiap $i = 0,1,2, \dots, n-1$ dan $j = 0,1,2, \dots, N$. Kemudian, misalkan untuk suatu $j = 0,1,2, \dots, N-1$, nilai dari $w_{i,j}$ telah dihitung untuk setiap $i = 0,1,2, \dots, n-1$, maka nilai dari $w_{i,j+1}$ dapat diperoleh untuk setiap $i = 0,1,2, \dots, n-1$ sebagai berikut.

Langkah pertama, untuk setiap $i = 0,1,2, \dots, n-1$, hitung

$k_{1,i} = hf_i(x_j, w_{0,j}, w_{1,j}, \dots, w_{n-1,j})$.

Kemudian, untuk setiap $i = 0,1,2, \dots, n-1$, hitung

$k_{2,i} = hf_i\left(x_j + \frac{h}{2}, w_{0,j} + \frac{1}{2}k_{1,0}, w_{1,j} + \frac{1}{2}k_{1,1}, \dots, w_{n-1,j} + \frac{1}{2}k_{1,n-1}\right)$.

Selanjutnya, untuk setiap $i = 0,1,2, \dots, n-1$, hitung

$k_{3,i} = hf_i\left(x_j + \frac{h}{2}, w_{0,j} + \frac{1}{2}k_{2,0}, w_{1,j} + \frac{1}{2}k_{2,1}, \dots, w_{n-1,j} + \frac{1}{2}k_{2,n-1}\right)$.

Terakhir, untuk untuk setiap $i = 0,1,2, \dots, n-1$, hitung pula

$k_{4,i} = hf_i(x_j + h, w_{0,j} + k_{3,0}, w_{1,j} + k_{3,1}, \dots, w_{n-1,j} + k_{3,n-1})$.

Dengan menggunakan nilai-nilai tersebut, maka untuk setiap $i = 0,1,2, \dots, n-1$ diperoleh $w_{i,j+1} = w_{i,j} + \frac{1}{6}(k_{1,i} + 2k_{2,i} + 2k_{3,i} + k_{4,i})$. (Faires, 2002)

2.5 Struktur Aljabar Lapangan Hingga

2.5.1 Teori Grup

Definisi 2.8 ***(Grup)*** *Suatu grup adalah struktur aljabar yang terdiri atas himpunan takkosong G dengan dilengkapi operasi biner $*: G \times G \to G$ (dinotasikan $g * h = *(g, h)$ untuk setiap $g, h \in G$) sehingga*

1. $\forall g, h \in G, g * h \in G$ *(sifat tertutup atas operasi* $*$*)*
2. $\forall g, h, k \in G, (g * h) * k = g * (h * k)$ *(sifat asosiatif),*
3. $\exists e \in G$ *sehingga* $\forall g \in G, g * e = e * g = g$ *(unsur identitas),*
4. $\forall g \in G, \exists g^{-1} \in G$ *sehingga* $g * g^{-1} = g^{-1} * g = e$ *(sifat invers).*

Lebih lanjut, jika berlaku $\forall g, h \in G\ g * h = h * g$ *(sifat komutatif) maka grup G disebut grup komutatif atau grup abel. Untuk selanjutnya, "*$g * h$*" hanya ditulis "*gh*" jika tidak ada ambiguitas (hanya terdapat satu operasi).* (Jacobson, 1985)

Contoh 2.11

Pasangan $(\mathbb{Z}, +)$ dengan $\mathbb{Z}$ adalah himpunan bilangan bulat dan $+$ adalah operasi penjumlahan biasa merupakan grup dengan elemen identitas 0. Jelas bahwa operasi $+$ bersifat asosiatif di himpunan $\mathbb{Z}$ dan setiap elemen $x \in \mathbb{Z}$ mempunyai invers penjumlahan $-x$. Grup ini juga merupakan grup abel karena sifatnya komutatif.

Contoh 2.12

Pasangan $(V, *)$ dengan $V = \{e, a, b, c\}$ dan $*$ adalah operasi yang ditunjukkan oleh Tabel 2.1 (hasil operasi $x * y$ disepakati ada di baris x yang ditandai warna biru dan kolom y yang ditandai warna kuning untuk setiap x, y di V) merupakan grup dengan elemen identitas e. Tabel yang menunjukkan operasi dari tiap elemen pada sebarang himpunan yang dilengkapi oleh operasi seperti Tabel 2.1 disebut dengan tabel Cayley.

Tabel 2.1 Tabel Operasi Grup Klein V

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Berdasarkan Tabel 2.1, dapat diperoleh semua hasil operasi dari elemen-elemen di grup V misalnya $a * b = c$. Grup ini bernama grup Klein. Grup ini juga adalah grup abel sebab operasinya bersifat komutatif yang dapat diamati dengan jelas dari kesimetrisan tabel Cayley terhadap sumbu diagonal.

Contoh 2.13

Misalkan $S_3 = \{\sigma \mid \sigma: \{1,2,3\} \to \{1,2,3\}, \sigma \text{ bijektif}\}$ adalah himpunan permutasi 3 bilangan dan $\circ$ adalah operasi komposisi fungsi. Notasikan untuk setiap elemen σ di S_3, $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ \sigma(1) & \sigma(2) & \sigma(3) \end{pmatrix}$. Pasangan $(S_3, \circ)$ membentuk grup dengan elemen identitas $\iota = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$. Grup ini bukan merupakan grup abel sebab grup ini tidak komutatif, misalnya $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ tidak sama dengan $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$.

Contoh 2.14

Himpunan $\mathbb{Z}_n = \{0,1,2,3, \dots, n-1\}$ dengan operasi penjumlahan $(+)$ modulo n merupakan gelanggang dengan unsur identitas penjumlahannya adalah 0.

Definisi 2.9 ***(Orde)*** *Misalkan $(G,*)$ adalah sebuah grup dan misalkan a adalah suatu elemen di G. Definisikan $a^n = a * (a^{n-1})$ untuk $n \geq 2$, dan $a^1 = a$. Jika terdapat bilangan asli n sehingga $a^n = e$ dengan e adalah unsur identitas di grup G maka orde dari a yang dinotasikan dengan $|a|$ adalah bilangan asli terkecil sehingga $a^{|a|} = e$. Sebaliknya, jika tidak ada bilangan asli n yang memenuhi $a^n = e$ maka order dari a disepakati $|a| = 0$ atau tak hingga. Selain itu, didefinisikan orde dari grup G adalah kardinalitas dari G.* (Jacobson, 1985)

Contoh 2.15

$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ adalah salah satu permutasi di grup S_3 (Contoh 2.13) yang berorde 2 sebab $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}^2 = \iota$ tapi $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \neq \iota$.

2.5.1.1 Subgrup

Definisi 2.10 ***(Subgrup)*** *Misalkan* $(G,*)$ *adalah grup. Suatu subhimpunan* H *dari* G *disebut subgrup dari grup* G *apabila* $(H,*)$ *membentuk grup. Jika* H *subgrup dari* G *maka dinotasikan* $H \leq G$. (Jacobson, 1985)

Contoh 2.16

Himpunan bilangan genap $2\mathbb{Z}$ adalah subgrup dari $\mathbb{Z}$ dengan operasi penjumlahan biasa atau $2\mathbb{Z} \leq \mathbb{Z}$.

Definisi 2.11 ***(Subgrup yang Direntang Subhimpunan)*** *Misalkan* $(G,*)$ *adalah grup dan* $H \subseteq G$. *Definisikan* $\langle H \rangle$ *adalah subgrup terkecil dari* G *sehingga berlaku* $H \subseteq \langle H \rangle$. *Dengan kata lain, jika terdapat subgrup* K *sehingga berlaku* $H \subseteq K \leq G$, *maka* $H \subseteq \langle H \rangle \leq K \leq G$. *Lebih lanjut, jika* $H = \{a\}$ *yang berupa singleton maka dapat ditulis* $\langle a \rangle = \langle \{a\} \rangle = \langle H \rangle$ *dan* $\langle a \rangle$ *disebut subgrup siklik dari* G. (Jacobson, 1985)

Contoh 2.17

Himpunan bilangan genap $2\mathbb{Z}$ adalah subgrup dari $\mathbb{Z}$ dengan operasi penjumlahan biasa atau $2\mathbb{Z} \leq \mathbb{Z}$.

Teorema 2.2 *Misalkan* $(G,*)$ *adalah grup dan* a *adalah salah satu elemen di* G. *Notasikan* $a^{-n} = (a^n)^{-1}$ *adalah invers dari* a^n *untuk setiap bilangan asli n serta definisikan* $a^0 = e$ *adalah unsur identitas di* G, *maka setiap elemen di* $\langle a \rangle$ *dapat dinyatakan sebagai* a^n *untuk suatu bilangan bulat* n. *Dengan kata lain* $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$. (Jacobson, 1985)

Contoh 2.18

Subgrup siklik yang direntang oleh $2 \in \mathbb{Z}$ adalah himpunan bilangan genap $2\mathbb{Z}$. Lebih umum, subgrup siklik yang direntang oleh $n \in \mathbb{Z}$ adalah himpunan bilangan kelipatan n $n\mathbb{Z}$.

2.5.1.2 Grup Siklik

Definisi 2.12 ***(Grup Siklik)*** *Misalkan* $(G,*)$ *adalah grup. Jika terdapat* $a \in G$ *sehingga* $\langle a \rangle = G$ *maka* G *disebut grup siklik dan* a *adalah generator siklik dari* G. (Jacobson, 1985)

Contoh 2.19

Untuk setiap bilangan asli $n \geq 2$, grup $\mathbb{Z}_n$ adalah grup siklik berorde n yang direntang oleh 1 atau $\mathbb{Z}_n = \langle 1 \rangle$. Lebih khusus, $\mathbb{Z}_1 = \langle 0 \rangle$.

Contoh 2.20

Himpunan bilangan bulat $\mathbb{Z}$ dengan operasi penjumlahan biasa adalah grup siklik yang direntang oleh 1 atau $\mathbb{Z} = \langle 1 \rangle$. $\mathbb{Z}$ juga direntang oleh -1 sehingga berlaku $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.

2.5.1.3 Koset

Definisi 2.13 ***(Koset)*** *Misalkan $(G, +)$ adalah grup dan H adalah suatu subgrup dari G. Untuk setiap $a \in G$, definisikan $a + H = \{a + h : h \in H\}$. $a + H$ disebut koset kiri dari subgrup H. Adapun $H + a = \{h + a : H \in H\}$ disebut koset kanan dari subgrup H. Jika $a + H = H + a$ maka $a + H$ cukup disebut koset dari H.* (Jacobson, 1985)

Teorema 2.3 *Misalkan $(G, +)$ adalah grup dan $H \leq G$, maka berlaku:*

1. $a + H = b + H \Leftrightarrow b \in a + H \Leftrightarrow (-b) + a \in H$, *dan*
2. *jika G abel maka $a + H = H + a$.* (Jacobson, 1985)

2.5.2 Teori Gelanggang (*Ring*)

Definisi 2.14 ***(Gelanggang)*** *Suatu gelanggang (ring) adalah struktur yang terdiri atas himpunan takkosong R yang dilengkapi dengan dua buah operasi biner, $+$ (yang disebut penjumlahanan) dan $\cdot$ (yang disebut perkalian) pada R (ditulis $(R, +, \cdot)$ $adalah\ gelanggang$) serta dua elemen berbeda $0,1 \in R$ sehingga*

1. $(R, +)$ *adalah grup abel dengan identitas* 0,
2. $\forall a, b \in R, a \cdot b \in R$ *(sifat tertutup atas perkalian)*
3. $\forall a, b \in R, (a \cdot b) \cdot c = a \cdot (b \cdot c)$ *(sifat asosiatif),*
4. $\forall a \in R, a \cdot 1 = 1 \cdot a = a$ *(unsur identitas),*
5. $\forall a, b, c \in R, a \cdot (b + c) = a \cdot b + a \cdot c$ *(sifat distributif kiri), dan*
6. $\forall a, b, c \in R, (b + c) \cdot a = b \cdot a + c \cdot a$ *(sifat distributif kanan).*

Apabila berlaku $a \cdot b = b \cdot a$ untuk setiap $a, b \in R$ (sifat komutatif) maka gelanggang R disebut gelanggang komutatif. Untuk selanjutnya notasi "$a \cdot b$"

hanya ditulis "ab". Adapun operasi penjumlahannya $(+)$ tetap ditulis. Selain itu, invers penjumlahan dari elemen a dinotasikan dengan "$-a$" dan jika ada invers perkaliannya maka dinotasikan dengan "a^{-1}". (Jacobson, 1985)

Contoh 2.21

Himpunan bilangan riil $\mathbb{R}$ membentuk suatu gelanggang dengan operasi penjumlahan $(+)$ dan perkalian $(\cdot)$ biasa serta unsur identitas penjumlahannya adalah 0 dan identitas perkaliannya adalah 1.

Contoh 2.22

Himpunan bilangan kompleks $\mathbb{C}$ membentuk suatu gelanggang dengan operasi penjumlahan $(+)$ dan perkalian $(\cdot)$ bilangan kompleks biasa serta unsur identitas penjumlahannya adalah 0 dan identitas perkaliannya adalah 1. Dapat diamati bahwa himpunan bilangan riil $\mathbb{R}$ termuat dalam $\mathbb{C}$ atau dengan kata lain $\mathbb{R} \subset \mathbb{C}$. Dengan demikian $\mathbb{R}$ merupakan subgrup dari $\mathbb{C}$ atau bahkan dapat disebut subgelanggang dari $\mathbb{C}$ yang akan dibahas di subbab berikutnya.

Contoh 2.23

Himpunan matriks riil berukuran 2×2 $M_2(\mathbb{R})$ membentuk suatu gelanggang dengan operasi penjumlahan $(+)$ dan perkalian $(\cdot)$ matriks dengan unsur identitas penjumlahannya adalah matriks nol $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ dan identitas perkaliannya adalah $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Contoh 2.24

Himpunan $\mathbb{Z}_n = \{0,1,2,3, \dots, n-1\}$ dengan operasi penjumlahan $(+)$ dan perkalian $(\cdot)$ modulo n merupakan gelanggang dengan unsur identitas penjumlahannya adalah 0 dan unsur identitas perkaliannya adalah 1.

Contoh 2.25 (Gelanggang Polinomial atas $\mathbb{Z}_n$)

Himpunan polinomial $\mathbb{Z}_n[X] = \{\sum_{i=0}^{m} a_i x^i : m \in \mathbb{Z}_{\geq 0}, \forall i = 0,1, \dots, m, a_i \in \mathbb{Z}_n\}$ dengan koefisien-koefisennya merupakan anggota di $\mathbb{Z}_n$ untuk suatu bilangan asli n serta operasi penjumlahan $(+)$ dan perkalian $(\cdot)$ polinomial modulo n

merupakan gelanggang dengan unsur identitas penjumlahannya adalah polinomial 0 dan unsur identitas perkaliannya adalah polinomial 1. (Jacobson, 1985)

Definisi 2.15 ***(Subgelanggang)*** *Misalkan* $(R,+,\cdot)$ *adalah suatu gelanggang. Suatu himpunan* S *dikatakan subgelanggang dari gelanggang* R *jika dan hanya jika* $S \subseteq R$ *dan* S *membentuk gelanggang dengan operasi yang sama. Lebih lanjut,* S *disebut subgelanggang sejati dari* R. (Jacobson, 1985)

Contoh 2.26

Gelanggang bilangan rasional $\mathbb{Q}$ adalah subgelanggang dari gelanggang bilangan riil $\mathbb{R}$. Lebih jauh, gelanggang $\mathbb{Q}$ dan $\mathbb{R}$ adalah subgelanggang dari gelanggang bilangan kompleks $\mathbb{C}$.

Definisi 2.16 ***(Isomorfisma gelanggang)*** *Misalkan* $(R,+_R,\cdot_R)$ *dan* $(S,+_S,\cdot_S)$ *adalah gelanggang. Suatu fungsi bijektif* $f: R \to S$ *disebut isomorfisma gelanggang apabila berlaku* $\forall a,b \in R$, $f(a+_R b) = f(a)+_s f(b)$ *dan* $f(a \cdot_R b) = f(a) \cdot_s f(b)$. *Apabila terdapat suatu isomorfisma* f *yang memetakan gelanggang* R *ke gelanggang* S *maka dikatakan* R *isomorfik dengan* S *yang dinotasikan dengan* $R \cong S$. (Jacobson, 1985)

Teorema 2.4 *Misalkan* R, S, *dan* T *gelanggang, maka berlaku:*

1. $R \cong R$,
2. $R \cong S \Longrightarrow S \cong R$, *dan*
3. $(R \cong S \wedge S \cong T) \Longrightarrow R \cong T$. (Jacobson, 1985)

2.5.2.1 Ideal dan Gelanggang Faktor

Definisi 2.17 ***(Ideal)*** *Misalkan* R *adalah gelanggang. Suatu subgrup* I *dari* R *dengan operasi penjumlahannya disebut ideal dari* R *jika dan hanya jika untuk setiap* $s \in I$ *dan* $r \in R$ *berlaku* $rs, sr \in I$. (Jacobson, 1985)

Contoh 2.27

Himpunan bilangan bulat $2\mathbb{Z}$ adalah ideal dari $\mathbb{Z}$ sebab $2\mathbb{Z} \leq \mathbb{Z}$ dan perkalian bilangan bulat dengan bilangan genap selalu menghasilkan bilangan genap.

Contoh 2.28

Himpunan polinomial di $\mathbb{Z}_n[X]$ tanpa unsur konstanta (unsur konstantanya 0) membentuk subgrup dari $\mathbb{Z}_n[X]$ dan juga merupakan ideal dari $\mathbb{Z}_n[X]$ atau dengan kata lain $I = \{\sum_{i=1}^{m} a_i x^i : m \in \mathbb{N}, \forall i = 1, \dots, m, a_i \in \mathbb{Z}_n\}$ adalah ideal dari $\mathbb{Z}_n[X]$.

Definisi 2.18 ***(Gelanggang Faktor)*** *Misalkan* $(R, +, \cdot)$ *adalah gelanggang dan I adalah salah satu ideal dari R. Definisikan* $R/I = \{a + I : a \in R\}$ *adalah himpunan setiap koset dari ideal I.* R/I *dengan operasi penjumlahan* $(+)$ *dan perkalian* $(\cdot)$ *sehingga* $\forall a + I, b + I \in R/I$*:*

1. $(a + I) + (b + I) = (a + b) + I$, *serta*
2. $(a + I) \cdot (b + I) = (a \cdot b) + I$

membentuk gelanggang. Gelanggang R/I *disebut gelanggang faktor dari R.* (Jacobson, 1985)

Contoh 2.29

Salah satu gelanggang faktor dari $\mathbb{Z}$ adalah $\mathbb{Z}/2\mathbb{Z}$ yang isomorfik dengan $\mathbb{Z}_2$. Lebih umum, gelanggang faktor $\mathbb{Z}/n\mathbb{Z}$ isomorfik dengan $\mathbb{Z}_n$ untuk setiap bilangan asli n.

Definisi 2.19 ***(Ideal yang Direntang Subhimpunan)*** *Misalkan* $(R, +, \cdot)$ *adalah gelanggang dan* $S \subseteq R$*. Definisikan* $[S]$ *adalah ideal terkecil dari G sehingga berlaku* $S \subseteq [S]$*. Dengan kata lain, jika terdapat ideal I dari G sehingga berlaku* $S \subseteq I$*, maka* $S \subseteq [S] \subseteq I$*. Lebih lanjut, jika* $S = \{a\}$ *yang berupa singleton maka dapat ditulis* $[a] = [\{a\}] = [S]$. (Jacobson, 1985)

Teorema 2.5 *Misalkan* $(R, +, \cdot)$ *adalah gelanggang komutatif dan* $a \in R$*. Semua elemen di* $[a]$ *dapat dinyatakan sebagai* ar *untuk suatu* $r \in R$. (Jacobson, 1985)

2.5.3 Teori Lapangan Hingga

Definisi 2.20 ***(Lapangan)*** *Suatu gelanggang R dengan operasi perkalian* $\cdot$ *dan identitas perkalian* 1 *adalah lapangan apabila berlaku sifat komutatif terhadap operasi* $\cdot$ *dan setiap elemen taknol* $a \in R$ *mempunyai invers* $b \in R$ *sedemikian sehingga* $a \cdot b = b \cdot a = 1$*, ditulis* $b = a^{-1}$*. Suatu lapangan R yang banyak*

elemennya berhingga disebut lapangan hingga atau lapangan Galois. Selain itu, $(R-\{0\},\cdot)$ *dengan* 0 *adalah identias penjumlahan di* R *membentuk grup dan disebut grup kali dari lapangan* R*. Grup kali dari suatu lapangan* $\mathbb{F}$ *dinotasikan dengan* $\mathbb{F}^{\times}$*.* (Jacobson, 1985)

Contoh 2.30

Gelanggang-gelanggang $\mathbb{Q}$, $\mathbb{R}$, dan $\mathbb{C}$ adalah lapangan.

Contoh 2.31

Gelanggang $\mathbb{Z}_p$ dengan p adalah bilangan prima membentuk lapangan hingga.

Contoh 2.32

Gelanggang faktor $\mathbb{F} = {\mathbb{Z}_2[X]}\big/{[x^2+x+1]}$ membentuk lapangan dengan operasi penjumlahan dan perkaliannya dapat dilihat pada Tabel 2.2 ($p(x)+[x^2+x+1]$ disepakati cukup ditulis $p(x)$ dengan $p(x)$ adalah polinomial di $\mathbb{Z}_2[X]$).

Tabel 2.2 Tabel Operasi di Lapangan ${\mathbb{Z}_2[X]}\big/{[x^2+x+1]}$

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Definisi 2.33 ***(Pengaitan Bilangan Bulat)*** *Misalkan* $\mathbb{F}$ *adalah suatu lapangan. Definisikan operasi pengaitan elemen di lapangan* $\mathbb{F}$ *dengan bilangan bulat adalah* $\cdot_B\colon \mathbb{Z}\times\mathbb{F}\to\mathbb{F}$ *sedemikian sehingga untuk setiap* $a\in\mathbb{F}$*:* (Jacobson, 1985)

1. $1\cdot_B a = a$*, dan*
2. $n\cdot_B a = a+(n-1)\cdot_B a$ *untuk setiap* $n\in\mathbb{Z}$

Selanjutnya disepakati "$n \cdot_B a$" cukup ditulis "$n \cdot a$" atau "na" selama tidak ada ambiguitas. (Jacobson, 1985)

Teorema 2.6 *Misalkan* $\mathbb{F}$ *adalah suatu lapangan dan* $a, b \in \mathbb{F}$*, maka berlaku:*

1. $-(n \cdot a) = (-n) \cdot a$ *untuk setiap* $n \in \mathbb{Z}$,
2. $0 \cdot a = 0_{\mathbb{F}}$ *dengan* $0_{\mathbb{F}}$ *adalah unsur identitas penjumlahan di* $\mathbb{F}$,
3. $(n + m) \cdot a = n \cdot a + m \cdot a$
4. $(mn) \cdot a = m \cdot (n \cdot a)$,
5. $(na) \cdot b = n \cdot (ab) = a(n \cdot b)$, *dan*
6. $n \cdot (a + b) = (n \cdot a) + (n \cdot b)$. (Jacobson, 1985)

Definisi 2.22 ***(Karakteristik Lapangan)*** *Misalkan* $\mathbb{F}$ *adalah suatu lapangan dan* $1_{\mathbb{F}}$ *adalah unsur identitas perkalian di lapangan* $\mathbb{F}$*. Jika terdapat bilangan asli* n *sehingga* $n \cdot 1_{\mathbb{F}} = 0_{\mathbb{F}}$ *dengan* $0_{\mathbb{F}}$ *adalah identitas penjumlahan di* $\mathbb{F}$ $maka$ *bilangan asli* m *terkecil sehingga* $m \cdot 1_{\mathbb{F}} = 0_{\mathbb{F}}$ *adalah karakteristik dari lapangan* $\mathbb{F}$ *yang dinotasikan dengan* $\mathrm{char}(\mathbb{F})$*. Sebaliknya, jika tidak ada bilangan asli* n *yang memenuhi maka didefinisikan* $\mathrm{char}(\mathbb{F}) = 0$*. Dengan demikian, setiap lapangan mempunyai nilai karakteristik.* (Jacobson, 1985)

Teorema 2.7 *Misalkan* $\mathbb{F}$ *adalah lapangan. Jika* $\mathrm{char}(\mathbb{F}) \neq 0$ *maka* $\mathrm{char}(\mathbb{F})$ *adalah bilangan prima.* (Jacobson, 1985)

Teorema 2.8 *Misalkan* $\mathbb{F}$ *adalah lapangan hingga. Banyaknya elemen dari lapangan* $\mathbb{F}$ *adalah* p^n *dengan* p *bilangan prima dan* $n \in \mathbb{N}$*. Lebih jauh, jika terdapat lapangan* $\mathbb{G}$ *yang banyak elemennya juga adalah* p^n *maka* $\mathbb{F} \cong \mathbb{G}$*. Karena semua lapangan hingga yang banyak elemennya sama saling isomorfik maka lapangan hingga berorde (yang mempunyai banyak elemen)* p^n *dinotasikan dengan* $GF(p^n)$ *atau* $\mathbb{F}_{p^n}$. (Jacobson, 1985)

2.5.3.1 Konstruksi Lapangan Hingga

Definisi 2.23 ***(Polinomial Tak Tereduksi)*** *Misalkan* $\mathbb{F}$ *adalah lapangan dan* $\mathbb{F}[X]$ *adalah gelanggang polinomial dengan koefiesien-koefiesiannya di* $\mathbb{F}$*. Suatu polinomial* $p(x) \in \mathbb{F}[X]$ *dikatakan tak tereduksi jika dan hanya jika* $p(x)$ *adalah polinomial tak konstan (berderajat* $r \geq 1$*) dan tidak dapat dinyatakan sebagai perkalian dua polinomial tak konstan di* $\mathbb{F}[X]$*. Dengan kata lain,* $p(x)$ *tidak bisa*

dinyatakan sebagai $f(x)g(x)$ *dengan derajat* $f(x)$ *dan* $g(x)$ *lebih dari* 0. (Gallian, 2021)

Contoh 2.33

$x^6 + x^5 + x^3 + x^2 + 1$ adalah salah satu polinomial di $\mathbb{Z}_2[X]$ yang tak tereduksi. (Ruskey, 1970)

Teorema 2.9 *Misalkan* $\mathbb{F}$ *adalah lapangan dan* $p(x)$ *adalah suatu polinomial di* $\mathbb{F}[X]$. *Gelanggang faktor* $\mathbb{F}[X]/[p(x)]$ *membentuk lapangan jika dan hanya jika* $p(x)$ *adalah polinomial tak tereduksi di* $\mathbb{F}[X]$. (Gallian, 2021)

Contoh 2.34

Polinomial $x^6 + x^5 + x^3 + x^2 + 1$ dari Contoh 2.31 dapat digunakan untuk mengonstruksi lapangan Galois $\mathbb{Z}_2[X]/[\,x^6 + x^5 + x^3 + x^2 + 1]$ karena polinomial $x^6 + x^5 + x^3 + x^2 + 1$ adalah polinomial tak tereduksi. Lebih lanjut, di lapangan $\mathbb{Z}_2[X]/[\,x^6 + x^5 + x^3 + x^2 + 1]$ (dengan menggunakan kesepakatan $p(x) + [\,x^6 + x^5 + x^3 + x^2 + 1]$ cukup ditulis $p(x)$) diperoleh

$x^6 = x^5 + x^3 + x^2 + 1, x^7 = x^6 + x^4 + x^3 + x = x^5 + x^4 + x^2 + x + 1,$

$x^8 = x^6 + x^5 + x^3 + x^2 + x = x + 1, \quad x^9 = x^2 + x, \quad x^{10} = x^3 + x^2,$

$x^{11} = x^4 + x^3, \quad x^{12} = x^5 + x^4, \quad x^{13} = x^6 + x^5 = x^3 + x^2 + 1,$

$x^{14} = x^4 + x^3 + x, \quad x^{15} = x^5 + x^4 + x^2, \quad x^{16} = x^6 + x^5 + x^3 = x^2 + 1,$

$x^{17} = x^3 + x, \quad x^{18} = x^4 + x^2, \quad x^{19} = x^5 + x^3,$

$x^{20} = x^6 + x^4 = x^5 + x^4 + x^3 + x^2 + 1,$

$x^{21} = x^6 + x^5 + x^4 + x^3 + x = x^4 + x^2 + x + 1, \quad x^{22} = x^5 + x^3 + x^2 + x,$

$x^{23} = x^6 + x^4 + x^3 + x^2 = x^5 + x^4 + 1,$

$x^{24} = x^6 + x^5 + x = x^3 + x^2 + x + 1, \quad x^{25} = x^4 + x^3 + x^2 + x,$

$x^{26} = x^5 + x^4 + x^3 + x^2, \quad x^{27} = x^6 + x^5 + x^4 + x^3 = x^4 + x^2 + 1,$

$x^{28} = x^5 + x^3 + x, \quad x^{29} = x^6 + x^4 + x^2 = x^5 + x^4 + x^3 + 1,$

$x^{30} = x^6 + x^5 + x^4 + x = x^4 + x^3 + x^2 + x + 1,$

$x^{31} = x^5 + x^4 + x^3 + x^2 + x, \quad x^{32} = x^6 + x^5 + x^4 + x^3 + x^2 = x^4 + 1,$

$x^{33} = x^5 + x, \quad x^{34} = x^6 + x^2 = x^5 + x^3 + 1,$

$x^{35} = x^6 + x^4 + x = x^5 + x^4 + x^3 + x^2 + x + 1,$

$x^{36} = x^6 + x^5 + x^4 + x^3 + x^2 + x = x^4 + x + 1,$ $x^{37} = x^5 + x^2 + x,$

$x^{38} = x^6 + x^3 + x^2 = x^5 + 1,$

$x^{39} = x^6 + x = x^5 + x^3 + x^2 + x + 1,$

$x^{40} = x^6 + x^4 + x^3 + x^2 + x = x^5 + x^4 + x + 1,$

$x^{41} = x^6 + x^5 + x^2 + x = x^3 + x + 1,$

$x^{42} = x^4 + x^2 + x,$ $x^{43} = x^5 + x^3 + x^2,$

$x^{44} = x^6 + x^4 + x^3 = x^5 + x^4 + x^2 + 1,$

$x^{45} = x^6 + x^5 + x^3 + x = x^2 + x + 1,$ $x^{46} = x^3 + x^2 + x,$

$x^{47} = x^4 + x^3 + x^2,$ $x^{48} = x^5 + x^4 + x^3,$

$x^{49} = x^6 + x^5 + x^4 = x^4 + x^3 + x^2 + 1,$ $x^{50} = x^5 + x^4 + x^3 + x,$

$x^{51} = x^6 + x^5 + x^4 + x^2 = x^4 + x^3 + 1,$ $x^{52} = x^5 + x^4 + x,$

$x^{53} = x^6 + x^5 + x^2 = x^3 + 1,$ $x^{54} = x^4 + x,$ $x^{55} = x^5 + x^2,$

$x^{56} = x^6 + x^3 = x^5 + x^2 + 1,$ $x^{57} = x^6 + x^3 + x = x^5 + x^2 + x + 1,$

$x^{58} = x^6 + x^3 + x^2 + x = x^5 + x + 1,$ $x^{59} = x^6 + x^2 + x = x^5 + x^3 + x + 1,$

$x^{60} = x^6 + x^4 + x^2 + x = x^5 + x^4 + x^3 + x + 1,$

$x^{61} = x^6 + x^5 + x^4 + x^2 + x = x^4 + x^3 + x + 1,$

$x^{62} = x^5 + x^4 + x^2 + x,$ $x^{63} = x^6 + x^5 + x^3 + x^2,$

serta x, x^2, x^3, x^4, x^5, dan 0 merupakan semua koset yang mungkin dari $[x^6 + x^5 + x^3 + x^2 + 1]$ yang masing-masing berkorespondensi dengan polinomial berderajat 5 ke bawah. Selain itu, grup kali $\left(\mathbb{Z}_2[X]/[x^6 + x^5 + x^3 + x^2 + 1]^{\times}, \cdot\right)$ adalah grup siklik berorde 63 dengan x sebagai generator siklik sehingga $\mathbb{Z}_2[X]/[x^6 + x^5 + x^3 + x^2 + 1]^{\times} \cong \mathbb{Z}_{63}$. Jadi, setiap elemen taknol di $\mathbb{Z}_2[X]/[x^6 + x^5 + x^3 + x^2 + 1]$ yang dinyatakan dalam bentuk polinomial dapat ditulis sebagai perpangkatan dari x.

Contoh 2.36

Polinomial $x^3 + x^2 + 1$ adalah polinomial tak tereduksi di $\mathbb{Z}_2[X]$ sebab seandainya tereduksi maka polinomial yang berderajat 3 ini haruslah dapat dinyatakan sebagai perkalian polinomial berderajat 1 dan polinomial berderajat 2.

Keberadaaan faktor linier (polinomial berderajat 1) mengimplikasikan keberadaan akar. Sementara itu, $x^3 + x^2 + 1$ tidak mempunyai akar di $\mathbb{Z}_2$ karena apabila disubstitusi $x = 0$ dan $x = 1$, diperoleh $0^3 + 0^2 + 1 = 1 \neq 0$ dan juga diperoleh $1^3 + 1^2 + 1 = 1 \neq 0$. Ini adalah kontradiksi, sehingga haruslah $x^3 + x^2 + 1$ adalah polinomial tak tereduksi.

Karena $x^3 + x^2 + 1$ adalah polinomial tak tereduksi di $\mathbb{Z}_2[X]$ maka $\mathbb{Z}_2[X]/[\,x^3 + x^2 + 1\,]$ membentuk lapangan. Di lapangan ini, diperoleh

$x^3 = x^2 + 1$,

$x^4 = x^3 + x = x^2 + x + 1$,

$x^5 = x^3 + x^2 + 1 = x + 1$,

$x^6 = x^2 + x$, dan

$x^7 = x^3 + x^2 = 1$.

Contoh 2.37

Pemilihan polinomial tak tereduksi yang berbeda dapat memengaruhi hasil operasi perkalian pada lapangan yang dikonstruksi. Sebagai contoh, $x^3 + x + 1$ juga merupakan polinomial tak tereduksi di $\mathbb{Z}_2[X]$ sehingga dapat digunakan untuk mengonstruksi lapangan $\mathbb{Z}_2[X]/[\,x^3 + x + 1\,]$. Pada lapangan $\mathbb{Z}_2[X]/[\,x^3 + x + 1\,]$, diperoleh hasil kali

$(x^2 + x)(x + 1) = x^3 + x^2 + x^2 + x = x^3 + x = x + 1 + x = 1.$

Sedangkan, di lapangan $\mathbb{Z}_2[X]/[\,x^3 + x^2 + 1\,]$, diperoleh hasil kali $(x^2 + x)(x + 1) = x^3 + x^2 + x^2 + x = x^3 + x = x^2 + 1 + x.$

Dengan demikian, polinomial tak tereduksi yang digunakan dapat dijadikan sebagai kunci dalam proses enkripsi sebab pemilihan polinomial berbeda mengakibatkan hasil perhitungan aritmetika yang berbeda pula.