PENGANTAR GALOIS FIELD

KONSTRUKSI SUATU LAPANGAN BERHINGGA

BERORDE PRIME POWER

Skripsi
untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S-1

Program Studi Matematika

diajukan oleh
Mahmudi
06610006

Kepada

PROGRAM STUDI MATEMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UIN SUNAN KALIJAGA

YOGYAKARTA

2010

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal :

Lam :

Kepada

Yth. Dekan Fakultas Sains dan Teknologi

UIN Sunan Kalijaga Yogyakarta

Di Yogyakarta

Assalamu'alaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka kami selaku pembimbing berpendapat bahwa skripsi saudara:

Nama	**: Mahmudi**
NIM	**: 06610006**
Judul Skripsi	**: Pengantar *Galois Field*, Konstruksi suatu Lapangan Berhingga Berorde *Prime Power***

sudah dapat diajukan kembali kepada Fakultas Sains dan Teknologi Program Studi Matematika UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana strata Satu dalam Sains (Matematika)

Dengan ini kami mengharap agar skripsi/tugas akhir Saudara tersebut di atas dapat segera dimunaqosyahkan. Atas perhatianya kami ucapkan terima kasih.

Yogyakarta, 22 Februari 2010
Pembimbing I

Dra. Hj. Khurul Wardati, M.Si
NIP. 19660731 200003 2 001

Universitas Islam Negeri Sunan Kalijaga FM-UINSK-BM-05-07/R0

PENGESAHAN SKRIPSI/TUGAS AKHIR

Nomor : UIN.02/D.ST/PP.01.1/686/2010

Skripsi/Tugas Akhir dengan judul	:	Pengantar *Galois Field*, Konstruksi suatu Lapangan Berhingga Berorde *Prime Power*
Yang dipersiapkan dan disusun oleh	:	
Nama	:	Mahmudi
NIM	:	06610006
Telah dimunaqasyahkan pada	:	1 Maret 2010
Nilai Munaqasyah	:	A

Dan dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga

TIM MUNAQASYAH :

Ketua Sidang

Dra. Hj. Khurul Wardati, M.Si.
NIP. 19660731 200003 2 001

Penguji I

Suroto, M.Sc

Penguji II

Muhammad Wakhid Musthofa, M.Si
NIP. 19800402 200501 1 003

Yogyakarta, 11 Maret 2010
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
Dekan

Dra. Maizer Said Nahdi, M.Si
NIP. 19550427 198403 2 001

PERNYATAAN KEASLIAN

Dengan ini saya menyatakan bahwa skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 22 Februari 2010

METERAI TEMPEL
9F1A6AAF002313309
ENAM RIBU RUPIAH
6000 DJP

Mahmudi
NIM. 06610006

KATA PENGANTAR

Allāhumma lakal-hamdu kulluhu, wa lakasy-syukru kulluhu, wa ilaika yurja`ul-amru kulluhu, ’alā niyyatuhu wa sirruhu, inna rabbi lasamī’ud-du’ā`i. Puji dan syukur hanya pantas terucapkan kepada Dzat Maha Penyayang di antara para penyayang, yang kepadaNya kembali segala urusan, yang atas segala karunia, hidayah, perkenan dan kehendakNya penulis dapat menyelesaikan penulisan skripsi ini. Shalawat dan salam semoga senantiasa tercurahkan kepada Nabi Muhammad SAW beserta keluarga, para sahabat dan para pengikutnya, yang dengan kehadiran Beliau telah menjadi rahmat buat sekalian alam.

Penyusunan skripsi ini dimaksudkan untuk memenuhi sebagian persyaratan guna memperoleh gelar Sarjana Program Studi Matematika. Skripsi ini berisi mengenai pembahasan konsep lapangan berhingga berorde *prime power*.

Terselesaikannya skripsi ini juga tak dapat lepas dari berbagai pihak, oleh karena itu pada kesempatan ini penulis ingin mengucapkan terima kasih kepada pihak-pihak yang tersebutkan dibawah ini, semoga Allah jua-lah yang akan memberikan balasan. Amien.

1. Ibu Dra. Maizer Said Nahdi, M.Si., selaku Dekan Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta.
2. Ibu Sri Utami Zuliana, S.Si., M.Sc., selaku Ketua Program Studi Matematika dan juga selaku Dosen Penasehat Akademik yang telah memberikan pengarahan, motivasi, dan bimbingan selama penulis belajar di Program Studi Matematika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta

3. Ibu Dra. Khurul Wardati, M.Si., selaku Dosen Pembimbing Skripsi yang telah bersedia meluangkan banyak waktu untuk memberi motivasi, bimbingan, petunjuk, saran, dan kritik selama penyusunan skripsi.
4. Bapak/Ibu Dosen dan seluruh staf karyawan Fakultas Sains dan Teknologi atas ilmu yang telah diberikan serta bantuan selama perkuliahan.
5. Ayah, Mak, dan Adek dirumah, atas segala kasih sayang, dukungan, motivasi dan kesabaran dalam penantian. Segala apa yang telah kalian curahkan untuk penulis, tiadalah cukup kata-kata untuk dapat penulis wakili.
6. Buat Nun, atas waktu dan perhatian yang telah terabaikan.
7. Buat sahabat-sahabatku di Prodi Matematika dan Prodi Pend. Matematika atas segala dukungan, waktu yang terluangkan untuk diskusi. Khususnya untuk teman-teman Matematika 2006.

Penulis menyadari bahwa dalam penyusunan skripsi ini masih jauh dari sempurna, oleh karena itu dengan kerendahan hati penulis mengharapkan kritik dan saran kepada para pembaca skripsi. Semoga skripsi ini dapat bermanfaat bagi semua pihak.

Yogyakarta, Februari 2010

Penulis

Mahmudi

PERSEMBAHAN

Skripsi ini penulis persembahkan untuk :

- Ayah, Mak, dan Adek Meutia yang kucintai dan selalu kusayangi
- Teman-teman Matematika UIN SUNAN KALIJAGA Angkatan 2006
- Almamater Fakultas Sainteks UIN SUKA Yogyakarta

MOTTO

مَّا يَفْتَحِ ٱللَّهُ لِلنَّاسِ مِن رَّحْمَةٍ فَلَا مُمْسِكَ لَهَا ۖ وَمَا يُمْسِكْ فَلَا مُرْسِلَ لَهُۥ مِنۢ بَعْدِهِۦ ۚ وَهُوَ
ٱلْعَزِيزُ ٱلْحَكِيمُ ﴿٢﴾ يَٰٓأَيُّهَا ٱلنَّاسُ ٱذْكُرُوا۟ نِعْمَتَ ٱللَّهِ عَلَيْكُمْ ۚ هَلْ مِنْ خَٰلِقٍ غَيْرُ ٱللَّهِ يَرْزُقُكُم مِّنَ
ٱلسَّمَآءِ وَٱلْأَرْضِ ۚ لَآ إِلَٰهَ إِلَّا هُوَ ۖ فَأَنَّىٰ تُؤْفَكُونَ ﴿٣﴾

(2.) Apa saja yang Allah anugerahkan kepada manusia berupa rahmat, maka tidak ada seorangpun yang dapat menahannya; dan apa saja yang ditahan oleh Allah maka tidak seorangpun yang sanggup melepaskannya sesudah itu. Dan Dialah yang Maha Perkasa lagi Maha Bijaksana.

(3.) Hai manusia, ingatlah akan nikmat Allah kepadamu. Adakah Pencipta selain Allah yang dapat memberikan rezki kepada kamu dari langit dan bumi ? tidak ada Tuhan selain Dia; maka mengapakah kamu berpaling (dari ketauhidan)?

(Surah 35, Fathir; ayat 2-3)

إِنَّمَآ أَمْرُهُۥٓ إِذَآ أَرَادَ شَيْـًٔا أَن يَقُولَ لَهُۥ كُن فَيَكُونُ ﴿٨٢﴾

82. Sesungguhnya keadaan-Nya apabila Dia menghendaki sesuatu hanyalah berkata kepadanya: "Jadilah!" Maka terjadilah ia.

(Surah 36, Yasin; ayat 82)

DAFTAR ISI

$\Longrightarrow$	”Berakibat,” 20 atau Bukti implikasi ke arah kanan, 22
$\Longleftarrow$	Bukti implikasi ke arah kiri, 22
$[0], [1], \dots, [n-1]$	Kelas ekuivalen *modulo* n, 23
$d \not\equiv c \pmod{n}$	d tidak kongruen c *modulo* n, 23
a^{-1}	Invers dari a, 30
$\mathbb{Q}$	Himpunan semua bilangan rasional, 31
$\mathbb{R}$	Himpunan semua bilangan real, 31
$\varphi : R \to R'$	φ suatu pemetaan dari *ring* R ke *ring* R', 39
$\varphi(a)$	Bayangan dari elemen a oleh φ, 39
$R[x]$	Polinomial dalam x atas R, 41
$\forall$	Kuantor universal, 41
$\sum_{i=0}^{n} a_i x^i$	Notasi sigma, 43
Maks $\{m, n, k\}$	Nilai terbesar dari m, n, dan k, 47
$\exists$	Kuantor eksistensial, 52
$R \cong R'$	R isomorfis dengan R', 52
der $f(x)$	Derajat polinomial $f(x)$, 53
$F[x]$	Polinomial *ring* atas lapangan F, 56
$f(x) \mid g(x), f(x) \nmid g(x)$	$f(x)$ membagi $g(x)$, $f(x)$ tidak membagi $g(x)$, 56
$f(x) \equiv g(x) \pmod{p(x)}$	$f(x)$ kongruen *modulo* $p(x)$ dengan $g(x)$, 80
$[f(x)]$	Kelas ekuivalen dari $f(x)$ *modulo* $p(x)$, 82
$\mathbb{Z}_p[x]/p(x)$	Himpunan polinomial dari semua kelas ekuivalen modulo $p(x)$, 86

ARTI LAMBANG DAN SINGKATAN

$\mathbb{Z}$	Himpunan semua bilangan bulat, 1
$\mathbb{Z}_n$	Himpunan semua kelas ekuivalen modulo n, 1
$GF(q)$	*Galois Field* berorde q, 2
$\mathbb{Z}_p[x]$	Polinomial ring atas $\mathbb{Z}_p$, 2
(x, y)	Pasangan berurutan dari x, y, 6
$x \in A$	x elemen himpunan A, 6
$y \notin B$	y bukan elemen himpunan B, 6
$A \times B$	Perkalian kartesius dari A dan B, 6
xRy, $(x, y) \in R$	x berelasi R dengan y, 7
$[x]$	Kelas ekuivalen yang memuat x, 8
$[x] \subset A$	$[x]$ himpunan bagian dari himpunan A, 9
$a \sim c$	a berelasi ekuivalen dengan c, 9
$\emptyset$	Himpunan kosong, 9
$[a] \cap [b]$	Himpunan $[a]$ beririsan dengan himpunan $[b]$, 9
$[a] = [b]$	Himpunan $[a]$ dan $[b]$ adalah himpunan yang sama, 9
$\blacksquare$	Teorema atau Akibat telah selesai dibuktikan, 9
$b \mid a$	b pembagi bilangan a, 11
$b \nmid a$	b bukan pembagi a, 11
$\Leftrightarrow$	Biimplikasi, 13
S^+	Himpunan semua bilangan bulat positif di S, 14
(a, b), FPB(a, b)	Faktor persekutuan terbesar dari a dan b, 16
$x \equiv y \pmod{n}$	x kongruen y *modulo* n, 19

Pengantar *Galois Field*, Konstruksi suatu Lapangan Berhingga

Berorde *Prime Power*

Oleh : Mahmudi (06610006)

ABSTRAKSI

Kongruensi modulo n pada daerah integral $\mathbb{Z}$ adalah suatu relasi ekuivalen, sehingga terbentuk suatu partisi dalam $\mathbb{Z}$, yang tiap himpunan bagiannya disebut dengan kelas ekuivalen. Himpunan semua kelas ekuivalen tersebut dinotasikan $\mathbb{Z}_n$ dan merupakan *ring*. Lebih lanjut untuk suatu $n = p$, dengan p prima, maka $\mathbb{Z}_p$ adalah lapangan berhingga berorde prima.

Analogi dengan kongruensi modulo n pada daerah integral $\mathbb{Z}$ adalah kongruensi modulo $p(x)$ pada daerah integral $F[x]$, polinomial *ring* atas lapangan F. Jika terdapat suatu lapangan $\mathbb{Z}_p$ dan polinomial $p(x)$ berderajat n maka akan dapat dibentuk suatu himpunan semua kelas ekuivalen modulo $p(x)$, ditulis $\mathbb{Z}_p[x]/p(x)$, yang memiliki elemen sebanyak p^n.

Khususnya untuk $p(x)$ suatu polinomial tak tereduksi atas $\mathbb{Z}_p$, maka $\mathbb{Z}_p[x]/p(x)$ merupakan suatu lapangan berhingga berorde *prime power*. Lapangan berhingga tersebut dinotasikan $GF(p^n)$. Lapangan berhingga $GF(p^n)$ akan memuat lapangan $\mathbb{Z}_p$ dan akar polinomial $p(x)$.

Kata kunci : *kongruensi modulo $p(x)$, polinomial tak tereduksi, prime power.*

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Materi aljabar abstrak yang telah penulis dapatkan adalah mengenai konsep *ring*, daerah integral, dan lapangan. Salah satu contoh *ring* yang menarik untuk dipelajari adalah *ring* bilangan bulat, yaitu himpunan semua bilangan bulat, dinotasikan $\mathbb{Z}$, yang dilengkapi dengan operasi penjumlahan $(+)$ dan pergandaan $(\cdot)$; ditulis $(\mathbb{Z}, +, \cdot)$. Lebih lanjut, karena $\mathbb{Z}$ tidak memuat pembagi nol maka $(\mathbb{Z}, +, \cdot)$ merupakan daerah integral.

Salah satu sifat dari daerah integral $\mathbb{Z}$ adalah berlakunya Algoritma Pembagian sedemikian sehingga terdapat suatu relasi kongruensi pada $\mathbb{Z}$, disebut relasi kongruensi *modulo* n. Relasi kongruensi merupakan suatu relasi ekuivalen, sehingga terbentuk suatu partisi dalam $\mathbb{Z}$. Himpunan bagian dari partisi yang terbentuk disebut kelas ekuivalen *modulo* n. Himpunan dari semua kelas ekuivalen *modulo* n dinotasikan dengan $\mathbb{Z}_n$.

Selanjutnya $\mathbb{Z}_n$ yang dilengkapi dengan operasi penjumlahan dan pergandaan *modulo* n akan membentuk *ring*. Khususnya, untuk n suatu bilangan prima maka $\mathbb{Z}_n$ adalah lapangan, yang dinotasikan $\mathbb{Z}_p$. Lapangan berhingga $\mathbb{Z}_p$ merupakan suatu struktur lapangan berhingga yang sudah umum diketahui, yaitu lapangan berhingga berorde prima. Lapangan berhingga berorde prima adalah lapangan yang memiliki elemen sebanyak suatu bilangan prima tertentu.

Suatu kasus yang dihadapi penulis adalah pertanyaan mengenai struktur lapangan yang terbentuk dari polinomial ring atas lapangan berhingga $\mathbb{Z}_p$. Kasus tersebut didapat oleh penulis dari soal ”Olimpiade Matematika untuk Mahasiswa 2006” dalam bidang Struktur Aljabar. Pertanyaannya adalah sebagai berikut :

> ”Perhatikan ring polinom $\mathbb{Z}_3[x]$ dan jika $f \in \mathbb{Z}_3[x]$, notasi $\langle f \rangle$ menyatakan ideal yang dibangun oleh f. Bilangan $c \in \mathbb{Z}_3$ sehingga $\mathbb{Z}_3[x]/\langle x^3 + cx^2 + 1 \rangle$ membentuk *field* adalah ...”

Dalam penelitian mandiri yang telah dilakukan oleh penulis, jawaban yang didapatkan adalah suatu lapangan yang tidak berorde prima, akan tetapi lapangan berhingga berorde 27. Bilangan 27 bukanlah suatu bilangan prima tetapi *prime power*, yaitu pangkat suatu bilangan prima dan dalam kasus ini $27 = 3^3$. Dengan demikian terdapat suatu lapangan berhingga berorde *prime power*. Lapangan berhingga seperti ini disebut *Galois Field*, dinotasikan $GF(q)$ dengan $q = p^n$, p bilangan prima dan n bilangan bulat positif.

Berdasarkan hasil tersebut, penulis tertarik untuk menjadikan tema *Galois Field* sebagai bahan penelitian tugas akhir penulis. Penelitian ini merupakan penelitian pengembangan dari materi-materi aljabar abstrak yang telah didapatkan oleh penulis, yaitu konsep lapangan berhingga $\mathbb{Z}_p$ dan konsep polinomial ring atas *ring* R, dinotasikan $R[x]$.

Perpaduan kedua konsep tersebut menghasilkan suatu konsep daerah integral $\mathbb{Z}_p[x]$, sehingga dapat dilakukan perbandingan pada sifat-sifat yang dimiliki oleh daerah integral $\mathbb{Z}$, terutama yang berkaitan dengan terbentuknya lapangan berhingga $\mathbb{Z}_p$, dengan sifat-sifat yang dimiliki daerah integral $\mathbb{Z}_p[x]$.

Dengan demikian berdasarkan analogi kedua konsep tersebut, diharapkan pada akhir penelitian ini penulis dapat mengkontruksikan beberapa lapangan berhingga berorde *prime power* dan dapat mengetahui sifat-sifatnya.

1.2 Batasan Masalah

Pembatasan masalah diperlukan dalam suatu penelitian ilmiah karena dapat membantu penulis untuk fokus pada suatu objek penelitian.

Demikian juga dengan penelitian yang penulis lakukan. Dikarenakan bilangan yang merupakan hasil pangkat suatu bilangan prima tak berhingga banyaknya, maka diperlukan batasan orde dari lapangan berhingga yang akan dikonstruksi.

Penelitian ini akan difokuskan pada konstruksi lapangan berhingga berorde *prime power*, $GF(q)$ dengan $q = p^n \leq 10$, serta dikaji juga beberapa sifat yang terdapat dalam struktur lapangan berhingga tersebut.

1.3 Rumusan Masalah

Berdasarkan latar belakang dan batasan masalah yang telah diuraikan, maka dirumuskan permasalahan sebagai berikut:

1. Bagaimanakah konsep lapangan berhingga berorde *prime power* ?
2. Bagaimanakah terbentuknya suatu lapangan berhingga berorde *prime power* ?
3. Bagaimanakah sifat-sifat yang dimiliki oleh lapangan berhingga berorde *prime power* ?

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah :

1. Mengkaji tentang konsep lapangan berhingga berorde *prime power*
2. Mengkaji cara terbentuknya lapangan berhingga berorde *prime power*
3. Mengkaji sifat-sifat lapangan berhingga berorde *prime power*

1.5 Manfaat Penelitian

Hasil penelitian ini diharapkan dapat memberikan beberapa manfaat, di antaranya sebagai berikut :

1. Memberikan pengetahuan tentang struktur lapangan berhingga berorde *prime power*.
2. Memberikan pengetahuan cara mencari dan membentuk suatu struktur lapangan berhingga berorde *prime power*.
3. Memberikan motivasi kepada peneliti-peneliti selanjutnya untuk mengembangkan penelitian mengenai *Galois Field*.

1.6 Tinjauan Pustaka

Sumber pokok dalam penulisan skripsi ini adalah buku yang ditulis oleh Thomas W Hungerford, yang berjudul *Abstract Algebra : An Introduction*. Penulis mengacu pada *Chapter* 4: *Arithmetic in* $F[x]$ dan *Chapter* 5: *Congruence in* $F[x]$ *and Congruence-Class Arithmetic*.

Selain itu, dalam penulisan tugas akhir ini penulis juga menggunakan suatu tinjauan pustaka sebuah tesis berjudul ”Galois Field”, yang ditulis oleh mahasiswa pasca sarjana UGM, Bambang Irawanto. Dalam tesis tersebut, Bambang Irawanto membahas mengenai syarat perlu dan cukup suatu lapangan berhingga dengan p^n elemen, p prima dan bilangan bulat $n \geq 1$. Tesis tersebut juga berisikan pembahasan mengenai hubungan antara lapangan pemisah dengan *Galois Field* serta penggunaan elemen-elemen *Galois Field* untuk mengkonstruksi sistem geometri dan pembentukan bujur sangkar latin yang saling orthogonal.

Pembahasan tesis tersebut memberikan suatu gambaran terdapatnya suatu lapangan berhingga berorde *prime power*. Hal ini penulis jadikan sebagai landasan untuk mengkaji suatu metode yang berbeda dalam pembentukan struktur lapangan berhingga berorde *prime power*. Metode yang penulis pilih adalah dengan menggunakan konsep kongruensi pada struktur daerah integral $F[x]$. Sedangkan dalam tesis tersebut, Bambang Irawanto menggunakan konsep ideal maksimal pada daerah integral $F[x]$.

BAB V

PENUTUP

5.1 Simpulan

Berdasarkan hasil studi literatur yang telah penulis lakukakan mengenai konsep lapangan berhingga berorde *prime power*, maka dapat diambil simpulan sebagai berikut:

1. Terdapat suatu *ring* berhingga berorde p^n, yaitu himpunan dari semua kelas ekuivalen modulo $p(x)$ atas suatu lapangan $\mathbb{Z}_p$, dinotasikan $\mathbb{Z}_p[x]/p(x)$, yang berbentuk

   $$\mathbb{Z}_p[x]/p(x) = \{a_0 + a_1x + \cdots + a_{n-1}x^{n-1} | a_i \in \mathbb{Z}_p\},$$

   dengan operasi penjumlahan dan pergandaan modulo $p(x)$.
2. Jika $p(x)$ polinomial tak tereduksi di $\mathbb{Z}_p[x]$, maka himpunan $\mathbb{Z}_p[x]/p(x)$ merupakan lapangan, yaitu lapangan berhingga berorde *prime power*, dinotasikan $GF(p^n)$, dengan p bilangan prima dan $n \geq 1$.
3. Lapangan berhingga $GF(p^n)$ merupakan suatu lapangan perluasan yang memuat lapangan $\mathbb{Z}_p$ dan akar polinomial tak tereduksi $p(x)$.

5.2 Saran-saran

Berdasarkan pada proses penelitian yang telah penulis lakukan, maka dapat disampaikan beberapa saran berikut:

1. Penelitian ini hanya dibatasi pada salah satu cara untuk mengkontruksi lapangan berhingga berorde *prime power*, yaitu dengan menggunakan sifat kongruensi pada daerah integral $F[x]$, diharapkan ada penelitian lebih

lanjut mengenai metode-metode yang lain yang memungkinkan untuk membentuk struktur lapangan berhingga berorde *prime power*.

2. Penelitian ini juga hanya mencakup pembahasan mengenai polinomial tak tereduksi berorde 2 dan 3, sehingga dimungkinkan dilakukan penelitian pengembangan mengenai struktur lapangan berhingga dengan polinomial tak tereduksi berorde lebih besar dari tiga.

Demikian saran-saran yang dapat disampaikan oleh penulis. Semoga skripsi ini dapat menjadi inspirasi bagi pembaca untuk mengembangkan lebih lanjut tentang konsep lapangan berhingga berorde *prime power* khususnya, dan konsep aljabar abstrak pada umumnya.

DAFTAR PUSTAKA

Arifin, Ahmad. 2000. *Aljabar*. Bandung : Penerbit ITB.

Bhattacharya, P. B., S.K. Jain, dan S.R. Nagpaul. 1994. *Basic Abstract Algebra*. Second Edition. Cambridge : Cambridge University Press.

Cherowitzo, William E. ”Introduction to Finite Fields.” [html document]. Di Akses dari Catatan Kuliah Online : http://www-math.cudenver.edu/ ~wcherowi /courses/finflds.html.

Fraleigh, John B. 2002. *A First Course in Abstract Algebra*. Seventh Edition. Addison Wesley.

Gilbert, Jimmie dan Linda Gilbert. 2000. *The Elements Of Abstract Algebra*. Fifth Edition. USA : Brook/Cole.

Gallian, Joseph A. 1990. *Contemporary Abstract Algebra*. Second Edition. Toronto : D. C. Heath Company.

Herstein, I.N. 1996. *Abstract Algebra*. Third Edition. USA : Prentice – Hall, Inc.

Hungerford, Thomas W. 1990. *Abstract algebra: an introduction*. First Edition. Philadelphia : Saunders College.

Irawanto, Bambang. 2001. “Galois Field.” Tesis Pasca Sarjana, Universitas Gadjah Mada.