PEMBENTUKAN *EXTENSION FIELD*

ACHMAD FAHRUROZI

0305010017

UNIVERSITAS INDONESIA

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

DEPARTEMEN MATEMATIKA

DEPOK

2009

PEMBENTUKAN *EXTENSION FIELD*

Skripsi diajukan sebagai salah satu syarat
untuk memperoleh gelar Sarjana Sains

Oleh:
ACHMAD FAHRUROZI
0305010017

DEPOK
2009

SKRIPSI : PEMBENTUKAN *EXTENSION FIELD*

NAMA : ACHMAD FAHRUROZI

NPM : 0305010017

SKRIPSI INI TELAH DIPERIKSA DAN DISETUJUI

DEPOK, JULI 2009

DR. SRI MARDIYATI, M.KOM	HELEN BURHAN, M.SI
PEMBIMBING I	PEMBIMBING II

Tanggal Lulus Ujian Sidang Sarjana: Juli 2009

Penguji I : Dr. Sri Mardiyati, M.Kom.

Penguji II : Dra. Nora Hariadi, M.Si.

Penguji III : Dra. Suarsih Utama

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT, karena atas berkat dan rahmatnya penulisan tugas akhir dapat selasai tepat pada waktunya.

Penulis menyadari, tugas akhir ini tidak akan dapat diselesaikan tanpa bantuan, dukungan dan do'a dari orang-orang disekitar penulis. Untuk itu penulis mengucapkan banyak terima kasih kepada pihak-pihak yang telah membantu dalam penulisan tugas akhir ini, khususnya penulis sampaikan kepada:

1. Bu Sri Mardiyati, selaku pembimbing I, terima kasih atas bimbingan, arahan, dan masukannya, serta kesabaran dalam membimbing penulis.
2. Bu Helen Burhan, selaku pembimbing II, terima kasih atas bimbingan, arahan, serta kritik dan saran yang membangun kepada penulis.
3. Pak Suryadi MT., pembimbing akademik yang selalu memberi nasihat, perhatian, dan arahan kepada penulis..
4. Bapak, terima kasih yang tak terhingga atas semua pengorbanan, perhatian, nasihat, serta do,anya kepada penulis.
5. Ibu (almh), terima kasih yang tak terhingga karena telah mendidik dan mencurahkan kasih sayang dengan sepenuh hati kepada penulis. Terima kasih telah menjadi motivasi bagi penulis.
6. Afifah Bidayah (kakakku), terima kasih atas dukungan dan dorongannya untuk segera menyelesaikan tugas akhir.

7. Nur Indah Seftiawati (Indah), terima kasih sebesar-besarnya atas perhatian, pengertian, kesabaran, semangat dan hiburan serta masukan-masukannya kepada penulis sehingga penulis selalu bersemangat.
8. Sahabat-sahabatku Abelian: Maul, RifKos, Ridwan, Chupz, Udin, Bocil (Hamdan), Aris, Trian, Buyung (Hairu), dan Dimas. Terima kasih telah membuat dan menjalani hari-hari indah bersama penulis.
9. Rekan-rekan Math ’05: Anggi, Puji, Khuri, Desti, Gyo, serta teman-teman lain yang tidak mungkin disebutkan satu persatu. Terima kasih atas dukungan dan do’anya, serta saat-saat indah di Matematika UI.
10. Kakak-kakak Math ’02, ’03, ’ 04 dan adik-adik ’06, ’07 & ’08. terima kasih telah mengisi hari-hari penulis selama kuliah di Matematika UI.
11. Karyawan & staf departemen Matematika UI, terima kasih atas bantuan dan kerjasamanya.

Penulis menyadari bahwa dalam tugas akhir ini masih terdapat kekurangan, maka dengan segala kerendahan hati, penulis mengharapkan saran dan masukan yang membangun untuk penulis di kemudian hari. Semoga tugas akhir ini dapat bermanfaat bagi para pembaca dan pihak-pihak yang akan melakukan kajian dan penelitian yang serupa.

Depok, Juli 2009

Penulis

ABSTRAK

Field sering dipelajari dan digunakan dalam beberapa bidang ilmu dan aplikasi aljabar. Dari beberapa *field* yang telah diketahui dapat dibentuk *field* lain yang lebih besar, yang disebut *extension field*. Dalam tugas akhir ini akan dibahas teori mengenai eksistensi dan cara pembentukan suatu *extension field*. Misal kita punya suatu *field* F , maka *extension field* dari F dibentuk dengan *adjoining* suatu akar dari polinomial tak tereduksi dalam $F[x]$ (himpunan polinomial dalam x atas F). Pembentukan *extension field* dibedakan berdasarkan karakteristik suatu *field*, yang terbagi menjadi dua kelompok, yaitu *field* dengan karakteristik 0 atau *field* tak hingga dan *field* dengan karakteristik p atau *field* hingga.

Kata kunci : *field, extension field,* polinomial, polinomial tak tereduksi. Akar polinomial.

vi + 70 hlm.

Bibliografi: 10 (1994-2007)

DAFTAR ISI

Halaman

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

Dalam aljabar abstrak, terdapat banyak teori mengenai suatu himpunan dan operasi-operasi yang ada didalamnya, yang disebut sistem matematika. Beberapa pembahasan mengenai suatu sistem matematika diantaranya adalah grup*, ring* dan *field.* Grup adalah suatu sistem matematika dengan sebuah operasi didalamnya, sedangkan *ring* dan *field* adalah suatu sistem matematika dengan dua buah operasi di dalamnya.

Berdasarkan jumlah elemennya, *field* dibedakan menjadi *field* tak hingga dan *field* hingga. *Field*, khususnya *field* hingga memiliki peran yang penting dalam berbagai bidang ilmu dan aplikasi, diantaranya digunakan dalam teori bilangan, *galois theory*, algoritma kriptografi, dan *coding theory*. Berdasarkan berbagai peran dan kegunaan tersebut, pembahasan mengenai *field* menjadi sangat menarik.

Sebelum ditemukannya kegunaan dan peran suatu *field* dalam berbagai bidang ilmu dan aplikasi, telah banyak berkembang teori dan gagasan tentang *field* oleh beberapa matematikawan di seluruh dunia. Beberapa diantaranya yang sangat berguna dan mendasar adalah penemuan oleh seorang matematikawan muda asal Perancis, yang bernama

Evariste Galois (1811-1832). Evariste Galois mengemukanan bahwa setiap *field* hingga memiliki jumlah elemen sebanyak $q = p^n$, dimana p adalah bilangan prima dan n adalah bilangan asli. Beberapa tahun kemudian, E. H. Moore (1862-1932) menunjukkan bahwa setiap *field* hingga dengan jumlah elemen yang sama adalah isomorfik.

Contoh *field* yang telah dikenal diantaranya adalah *field* bilangan rasional, yang dilambangkan dengan $(\mathbb{Q}, +, \bullet)$ atau untuk mempersingkat penulisan biasa juga dilambangkan $\mathbb{Q}$ saja. *Field* $\mathbb{Q}$ ini adalah *field* tak hingga terkecil. *Field* tak hingga lainnya yang telah dikenal adalah *field* bilangan riil dan *field* bilangan kompleks. Sedangkan contoh *field* hingga yang umum diketahui adalah *field* $\mathbb{Z}_p$, himpunan bilangan bulat modulo p, dimana p adalah bilangan prima.

Pada kenyataannya, *field* yang digunakan dalam berbagai bidang ilmu dan aplikasi bukan hanya *field* seperti yang disebutkan diatas. Namun, diperlukan juga *field* lain sesuai kebutuhan. *Field* lain tersebut bisa didapatkan dengan membentuk *extension field* dari suatu *field* yang telah diketahui.

1.2 PERUMUSAN MASALAH

Masalah yang dibahas pada tugas akhir ini adalah:

Bagaimana cara pembentukan *extension field*?

1.3 TUJUAN PENULISAN

Tujuan penelitian yang dilakukan dalam tugas akhir ini adalah: Menunjukkan eksistensi dari *extension field* dan cara pembentukan *extension field* tersebut.

1.4 METODE PENELITIAN

Metode penelitian yang digunakan dalam proses pembuatan tugas akhir ini adalah studi literatur, yaitu dengan cara mempelajari buku-buku referensi yang berhubungan dengan topik tugas akhir serta mengambil data-data penunjang lainnya melalui intenet.

1.5 SISTEMATIKA PENULISAN

Penulisan tugas akhir ini akan dibagi dalam empat bagian besar, yang dimulai dengan Bab I Pendahuluan, yang berisi tentang latar belakang, tujuan penulisan, rumusan masalah, metode penelitian dan sistematika penulisan.

Selanjutnya adalah Bab II Landasan Teori, yang berisi pengertian *field*, ruang vektor atas suatu *field*, polinomial atas suatu *field*, serta sifat-sifat yang diperlukan pada pembahasan tentang pembentukkan *extension field*.

Pengertian *extension field*, sifat-sifat yang berlaku pada *extension field* dan cara pembentukkan *extension field* dibahas dalam Bab III. Terakhir Bab IV Penutup berisi kesimpulan yang dapat ditarik oleh penulis dari keseluruhan isi tugas akhir dan saran dari penulis tentang tugas akhir ini.

BAB II

LANDASAN TEORI

Pada bab ini akan dibahas pengertian *field*, ruang vektor atas suatu *field*, polinomial atas suatu *field*, serta sifat-sifat yang diperlukan pada pembahasan bab selanjutnya.

Untuk memberikan pengertian *field* dan ruang vektor atas suatu *field* terlebih dahulu akan diberikan definisi suatu sistem matematika.

Definisi 2.1

Misalkan S suatu himpunan tak kosong dan terdapat operasi $\bullet$ pada S, yaitu pemetaan

$$\bullet : S \times S \to S$$

maka $(S,\bullet)$ disebut sistem matematika.

Suatu sistem matematika juga dapat didefinisikan oleh dua operasi + dan $\bullet$, ditulis $(S,+,\bullet)$

(Achmad Arifin, 2001)

Berikut diberikan pengertian grup serta sifat-sifat dalam suatu grup.

Definisi 2.2

Suatu sistem matematika $(G,*)$ disebut grup jika:

1. Jika $a,b,c \in G$, maka $a*(b*c) = (a*b)*c$. (sifat assosiatif)
2. Terdapat elemen identitas $e \in G$ sedemikian sehingga $a*e = e*a = a$ untuk setiap $a \in G$.
3. Untuk setiap $a \in G$ terdapat invers dari a, yang dinotasikan dengan $a^{-1} \in G$, sedemikian sehingga $a*a^{-1} = a^{-1}*a = e$.

(I. N. Herstein, 1996)

Definisi 2.3

Suatu grup disebut grup *abelian* atau grup komutatif jika $a*b = b*a$ untuk setiap $a,b \in G$

(I. N. Herstein, 1996)

Definisi 2.4

Suatu grup G disebut grup siklik jika terdapat elemen $g \in G$ sedemikian sehingga $G = \{g^n \mid n \in \mathbb{Z}\}$. Elemen g disebut generator dari G.

(Bhattacharya, Jain, Nagpaul, 1994)

Definisi 2.5

Misal G adalah grup dengan jumlah elemen berhingga. *Order* dari $a \in G$, dilambangkan $o(a)$, adalah bilangan bulat terkecil m sedemikian sehingga $a^m = e$, dimana e adalah elemen identitas terhadap operasi di G. (I. N. Herstein, 1996)

Suatu grup adalah sistem matematika dengan satu buah operasi. Berikut ini akan diberikan pengertian tentang *ring* dan *field*, yaitu suatu sistem matematika dengan dua buah operasi didalamnya.

Definisi 2.6

Suatu sistem matematika $(R,+,\bullet)$ disebut *ring* jika:

1. $(R,+)$ merupakan grup komutatif.
2. $(R,\bullet)$ memenuhi sifat assosiatif.
3. $(R,+,\bullet)$ memenuhi sifat distributif, artinya $a \bullet (b+c) = a \bullet b + a \bullet c$ untuk setiap $a,b,c \in R$.

(I. N. Herstein, 1996)

Definisi 2.7

Suatu himpunan bagian S dari ring $(R,+,\bullet)$ disebut disebut *subring* dari R jika S tertutup terhadap operasi penjumlahan dan perkalian di R. (Richard A. Dean, 1996)

Definisi 2.8

Ring $(R,+,\bullet)$ disebut *integral domain* jika $(R,\bullet)$ memenuhi sifat komutatif dan $a \bullet b = 0$ dalam R mengakibatkan $a = 0$ atau $b = 0$.

(I. N. Herstein, 1996)

Definisi 2.9

Suatu sistem matematika $(F,+,\bullet)$ disebut *field* jika:

1. $(F,+)$ merupakan grup komutatif.
2. $(F-\{0\},\bullet)$ merupakan grup komutatif.
3. $(F,+,\bullet)$ memenuhi sifat distributif, artinya $a \bullet (b+c) = a \bullet b + a \bullet c$ untuk setiap $a,b,c \in F$.

(I. N. Herstein, 1996)

Berdasarkan jumlah elemennya, *field* dapat dibedakan menjadi dua, yaitu *field* hingga dan *field* tak hingga. Untuk mengetahui perbedaan keduanya, diberikan definisi berikut.

Definisi 2.10

Suatu *field* $(F,+,\bullet)$ disebut *field* hingga jika banyak elemen F berhingga, yang biasa disebut dengan *Galois field*. *Galois field* dengan q elemen biasa ditulis $GF(q)$.

(Bhattacharya, Jain, Nagpaul, 1994)

Jika suatu *field* memiliki jumlah elemen tak berhingga maka *field* tersebut disebut *field* tak hingga.

Contoh *field* tak hingga adalah himpunan bilangan rasional $\mathbb{Q}$ beserta operasi penjumlahan dan perkalian yang umum padanya, dinotasikan dengan $(\mathbb{Q},+,\bullet)$. Sedangkan untuk memberikan contoh suatu *field* hingga, terlebih dahulu akan diberikan definisi tentang kelas modulo.

Definisi 2.11

Himpunan semua bilangan bulat yang menghasilkan sisa a jika dibagi dengan $n \in N$ disebut kelas a modulo n, dinotasikan $[a]_n$.

Dengan kata lain, $[a]_n = \{a + nk \mid k \in \mathbb{Z}\}$.

(Alexander Bogomolny, 1996)

Sekarang pandang $\mathbb{Z}_n = \{[a]_n \mid a \in \mathbb{Z}\}$ dengan dua operasi didefinisikan padanya, yaitu:

operasi tambah $+ : [a]_n + [b]_n = [a+b]_n$

operasi kali $\bullet : [a]_n \bullet [b]_n = [a \bullet b]_n$

Berdasarkan pengertian diatas, maka diperoleh:

1. $(\mathbb{Z}_n,+)$ merupakan grup komutatif.
2. $(\mathbb{Z}_n,\bullet)$ memenuhi sifat assosiatif dan komutatif.
3. $(\mathbb{Z}_n,+,\bullet)$ memenuhi sifat distributif, karena

$[a]_n \bullet \left([b]_n + [c]_n\right) = [a]_n \bullet [b]_n + [a]_n \bullet [c]_n$ untuk setiap $[a]_n, [b]_n, [c]_n \in \mathbb{Z}_n$.

Jadi, $\mathbb{Z}_n$ merupakan suatu *ring komutatif*. Jika $n = p$, dimana p prima, maka akan diperoleh $(\mathbb{Z}_p, \bullet)$ merupakan grup komutatif.

Untuk melihat kebenarannya, perlu diperhatikan akibat berikut ini.

Akibat 2.12 (*Fermat's Theorem*)

Jika p adalah prima dan $p \nmid a$, maka $a^{p-1} \equiv 1 \mod p$.

Untuk suatu bilangan bulat b, jika $p \mid b$ maka $b^p \equiv b \mod p$.

(I. N. Herstein, 1996)

Dari definisi $\mathbb{Z}_n$, jelas bahwa $(\mathbb{Z}_p, \bullet)$ memenuhi sifat assosiatif dan komutatif. Elemen identitas dalam $(\mathbb{Z}_p, \bullet)$ adalah $[1]_p$, karena $[a]_p \bullet [1]_p = [a \bullet 1]_p = [a]_p$ untuk setiap $[a]_p \in \mathbb{Z}_p$. Selanjutnya akan dibuktikan bahwa setiap elemen tak nol di $\mathbb{Z}_p$ mempunyai invers yang juga merupakan elemen dari $\mathbb{Z}_p$. Perhatikan jika $[a]_p \neq [0]_p \in \mathbb{Z}_p$, berarti $p \nmid a$.

Dengan demikian, berdasarkan *Fermat's Theorem*

$$a^{p-1} \equiv 1 \mod p$$

Dari definisi kelas $[.]$ didapatkan

$$\left[a^{p-1}\right]_p = [1]_p$$

Karena

$$\left[a^{p-1}\right]_p = \left[a\right]_p{}^{p-1}$$

maka

$$\left[a\right]_p{}^{p-1} = \left[1\right]_p .$$

Sehingga

$$\left[a\right]_p{}^{p-2} \bullet \left[a\right]_p = \left[1\right]_p$$

yang berarti bahwa terdapat invers dari $\left[a\right]_p \neq \left[0\right]_p \in \mathbb{Z}_p$ yaitu $\left[a\right]_p{}^{p-2}$.

Hal tersebut menunjukkan bahwa $(\mathbb{Z}_p, +, \bullet)$ adalah *field.*

Perhatikan bahwa $\mathbb{Z}_p = \left\{\left[0\right]_p, \left[1\right]_p, ..., \left[p-1\right]_p\right\}$, sehingga banyaknya elemen dari $\mathbb{Z}_p$ adalah sebanyak p. Maka $(\mathbb{Z}_p, +, \bullet)$ merupakan suatu *field* hingga.

Berikut diberikan suatu hubungan antara *field* dan grup siklik.

Teorema 2.13

Misal F adalah *field* hingga. Maka himpunan elemen-elemen tak nol dalam *field* tersebut, dilambangkan F^*, akan membentuk grup siklik terhadap operasi perkalian.

(I. N. Herstein, 1996)

Berikut ini akan diberikan pengertian mengenai karakteristik suatu *field*.

Definisi 2.14

Suatu *field* $(F,+,\bullet)$ dikatakan mempunyai karakteristik $p \neq 0$ jika untuk setiap $a \in F$ terdapat bilangan bulat positif p sedemikian sehingga $pa = 0$, dan tidak ada bilangan bulat positif lain yang lebih kecil dari p memenuhi sifat tersebut.

(I. N. Herstein, 1996)

Jika suatu *field* tidak mempunyai karakteristik $p \neq 0$ untuk suatu bilangan bulat positif p, maka *field* tersebut dikatakan mempunyai karakteristik 0.

Berikut diberikan contoh *field* dan karakteristik dari masing-masing *field* tersebut.

1. *Field* $\mathbb{Q}$, $\mathbb{R}$ dan $\mathbb{C}$ adalah *field* dengan karakteristik 0, karena tidak ada bilangan bulat positif p yang memenuhi $pa = 0$ untuk setiap elemen dalam *field* $\mathbb{Q}$, $\mathbb{R}$ dan $\mathbb{C}$ tersebut.
2. *Field* Z_p adalah *field* dengan karakteristik p, karena

$$p[a]_p = \underbrace{[a]_p + [a]_p + \ldots + [a]_p}_{p} = [0]_p$$

untuk setiap $[a]_p \in Z_p$, dimana $[0]_p$ adalah elemen identitas terhadap operasi penjumlahan di Z_p.

Berkaitan dengan definisi diatas, diberikan teorema berikut.

Teorema 2.15

Karakteristik dari suatu *field* adalah 0 atau suatu bilangan prima p.

(I. N. Herstein, 1996)

Selanjutnya akan dibahas pengertian dari *subfield* dan *prime subfield* sebagai berikut.

Definisi 2.16

Himpunan bagian *U* dari suatu *field* F disebut *subfield* dari F jika *U* adalah *field* dengan operasi-operasi dalam F.

(Rudolf Lidl & Gunter Pilz, 1994)

Definisi 2.17

Subfield terkecil dari suatu *field* F disebut *prime subfield*.

(www-math.cudenver.edu)

Berdasarkan definisi diatas, maka diperoleh setiap *field* memuat suatu *prime subfield*.

Untuk melihat hubungan antara suatu *field* dengan *prime subfield* terlebih dahulu akan diberikan pengertian homomorfisma dan isomorfisma antara dua *field*.

Definisi 2.18

Misal F_1 dan F_2 *field.* Pemetaan $\varphi : F_1 \to F_2$ disebut homomorfisma antara F_1 dan F_2, jika:

1. $\varphi(a+b) = \varphi(a) + \varphi(b)$ untuk setiap $a, b \in F_1$
2. $\varphi(a.b) = \varphi(a).\varphi(b)$ untuk setiap $a, b \in F_1$

(Antoine Chambert-Loir, 2005)

Berdasarkan definisi tersebut, diberikan teorema berikut.

Teorema 2.19

Misal F_1 dan F_2 *field* dan pemetaan $\varphi : F_1 \to F_2$ adalah homomorfisma antara F_1 dan F_2. Pemetaan φ adalah pemetaan 1-1 jika dan hanya jika $Ker(\varphi) = O$.

(Antoine Chambert-Loir, 2005)

Definisi 2.20

Misal F_1 dan F_2 *field* dan pemetaan $\varphi : F_1 \to F_2$ adalah homomorfisma antara F_1 dan F_2. F_1 dan F_2 dikatakan isomorfik jika φ adalah pemetaan 1-1 dan onto.

(Alozano, 2007)

Suatu *field* dengan karakteristik 0 memuat suatu *prime subfield* yang isomorfik dengan *field* bilangan rasional $\mathbb{Q}$. Sedangkan suatu *field* dengan karakteristik p memuat suatu *prime subfield* yang isomorfik dengan *field* $\mathbb{Z}_p$.

Berikut akan diberikan pengertian suatu ruang vektor atas suatu *field*.

Definisi 2.21

Misal V himpunan tak kosong dimana dua operasi didefinisikan padanya, yaitu operasi penjumlahan $+ : V \times V \to V$ dan operasi perkalian dengan skalar $* : F \times V \to V$. Maka sistem matematika $(V,+,*)$ disebut ruang vektor atas *field* F jika:

1. $(V,+)$ adalah group komutatif.
2. Untuk setiap $a \in F$ dan setiap $x \in V$ berlaku $ax \in V$.
3. $a(x+y) = ax + ay$ untuk setiap $a \in F$ dan $x, y \in V$.
4. $(a+b)x = ax + bx$ untuk setiap $a, b \in F$ dan $x \in V$.

5. $a(bx) = (ab)x$ untuk setiap $a, b \in F$ dan $x \in V$.

6. $1x = x$ untuk setiap $x \in V$, dimana $1 \neq 0$ adalah elemen kesatuan di F .

(I. N. Herstein, 1996)

Untuk selanjutnya penulisan F senantiasa berarti suatu *field* dan V berarti suatu ruang vektor atas *field* F .

Berikut ini diberikan pengertian tentang ruang bagian dari suatu ruang vektor V .

Definisi 2.22

Ruang bagian W dari suatu ruang vektor V adalah himpunan bagian tak kosong dari V sedemikian sehingga untuk setiap $\alpha \in F$ dan $w, v \in W$ berlaku $\alpha w \in W$ dan $w + u \in W$.

(I. N. Herstein, 1996)

Selanjutnya akan diberikan definisi tentang basis dari suatu ruang vektor V atas *field* F . Namun terlebih dahulu perlu diperhatikan definisi tentang pembangun ruang vektor V atas *field* F sebagai berikut.

Definisi 2.23

Subhimpunan $X = \{x_1, x_2, ..., x_n\} \subseteq V$ dikatakan membangun V jika setiap $y \in V$ merupakan kombinasi linier dari X.

Dengan kata lain, $y = a_1x_1 + a_2x_2 + ... + a_nx_n$ dimana $a_i \in F$.

(Achmad Arifin, 2001)

Definisi 2.24

Subhimpunan $X = \{x_1, x_2, ..., x_n\} \subseteq V$ dikatakan bebas linier jika penulisan vektor nol sebagai kombinasi linier dari X bersifat tunggal.

Dengan kata lain, kombinasi linier $a_1x_1 + a_2x_2 + ... + a_nx_n = 0$ hanya dipenuhi oleh $a_i = 0 \in F$ untuk setiap $x_i \in X$.

(Achmad Arifin, 2001)

Himpunan $X \subseteq V$ yang tidak bebas linier disebut bergantung linier. Artinya kombinasi linier $a_1x_1 + a_2x_2 + ... + a_nx_n = 0$ dipenuhi oleh $a_i \in F$ yang tidak semuanya nol, untuk setiap $x_i \in X$.

Berdasarkan definisi-definisi diatas, diberikan definisi basis dari suatu ruang vektor V atas *field* F sebagai berikut.

Definisi 2.25

Subhimpunan $X = \{x_1, x_2, ..., x_n\} \subseteq V$ disebut basis ruang vektor V jika X membangun V dan bebas linier di V.

(Achmad Arifin, 2001)

Berkaitan dengan definisi basis dari suatu ruang vektor V atas *field* F diperoleh definisi dimensi dari suatu vektor V atas *field* F sebagai berikut.

Definisi 2.26

Banyaknya elemen dalam suatu basis dari V disebut dimensi ruang vektor V atas lapangan F.

(Achmad Arifin, 2001)

Suatu ruang vektor V atas *field* F disebut ruang vektor berdimensi hingga jika banyaknya elemen dalam suatu basisnya berhingga.

Berikut ini diberikan suatu teorema yang berkaitan dengan suatu ruang vektor berdimensi hingga.

Teorema 2.27

Misal V ruang vektor atas *field* F dengan $\dim_F(V) = n$. Jika $m > n$, maka himpunan bagian dari V, dengan jumlah elemen m, bergantung linier.

(I. N. Herstein, 1996)

Berikut diberikan hubungan antara suatu *integral domain* dan ruang vektor atas suatu *field* F .

Teorema 2.28

Misal D adalah suatu *integral domain* dan memiliki elemen kesatuan didalamnya. Jika D adalah ruang vektor berdimensi hingga atas suatu *field* F , maka D adalah *field*.

(I. N. Herstein, 1996)

Selanjutnya akan kita lihat hubungan suatu *field* F dengan suatu himpunan lain, yaitu himpunan polinomial dalam x atas F yang dilambangkan $F[x]$. Berikut ini diberikan pengertian serta sifat-sifat yang berlaku dalam $F[x]$.

Definisi 2.29

Misal F *field*, maka elemen dari himpunan $F[x]$ adalah polinomial $f(x) = a_0 + a_1 x + ... + a_n x^n$ dimana $a_i \in F$, $i = 0,1,...,n$.

(I. N. Herstein, 1996)

Untuk selanjutnya, $F[x]$ melambangkan suatu himpunan polinomial dalam x atas F .

Definisi 2.30

Misal $f(x) \in F[x]$. Jika $f(x) = a_0 + a_1 x + ... + a_n x^n$ dan $a_n \neq 0$, maka derajat dari $f(x)$, dinotasikan $\deg f(x)$, adalah n.

(I. N. Herstein, 1996)

Dalam $F[x]$ terdapat operasi perkalian. Berikut diberikan suatu lemma yang berkaitan dengan perkalian dan derajat suatu polinomial dalam $F[x]$.

Lemma 2.31

Jika $f(x), g(x)$ adalah elemen tak nol dalam $F[x]$, maka $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$.

(I. N. Herstein, 1996)

Dalam $F[x]$ terdapat juga operasi pembagian. Berikut diberikan suatu teorema dan definisi yang berkaitan dengan operasi pembagian dalam $F[x]$.

Teorema 2.32 (Divisor Algorithm)

Untuk setiap $f(x), g(x) \in F[x]$ dengan $g(x) \neq 0$, terdapat $q(x), r(x) \in F[x]$ sedemikian sehingga:

$f(x) = q(x)g(x) + r(x)$; dimana $r(x) = 0$ atau $\deg r(x) < \deg g(x)$.

(I. N. Herstein, 1996)

Definisi 2.33

Misal $f(x), g(x) \in F[x]$ dengan $g(x) \neq 0$. $g(x)$ dikatakan membagi $f(x)$, ditulis $g(x) \mid f(x)$, jika $f(x) = a(x)g(x)$, untuk suatu $a(x) \in F[x]$.

(I. N. Herstein, 1996)

Salah satu bentuk khusus dari suatu polinomial $f(x) \in F[x]$ diberikan oleh definisi berikut.

Definisi 2.34

Polinomial $f(x) \in F[x]$ disebut polinomial monik jika $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$, dimana $n \geq 1$.

(I. N. Herstein, 1996)

Polinomial lain dalam $F[x]$ yang mempunyai bentuk khusus adalah polinomial yang tak tereduksi. Pengertian tentang suatu polinomial yang tak tereduksi dalam $F[x]$ dimulai dengan pengertian tentang *greatest common divisor* dari suatu polinomial dalam $F[x]$ dan definisi relatif prima dalam $F[x]$.

Definisi 2.35

Misal $f(x), g(x) \in F[x]$ dimana tidak keduanya nol. Polinomial monik $d(x) \in F[x]$ disebut *greatest common divisor* dari $f(x)$ dan $g(x)$ jika:

(a) $d(x) \mid f(x)$ dan $d(x) \mid g(x)$.

(b) Jika $h(x) \mid f(x)$ dan $h(x) \mid g(x)$, maka $h(x) \mid d(x)$.

(I. N. Herstein, 1996)

Dari definisi diatas, dapat dilihat hubungan antara dua polinomial dalam $F[x]$ sebagai berikut.

Definisi 2.36

Polinomial $f(x), g(x) \in F[x]$ dikatakan saling relatif prima jika *greatest common divisor* dari $f(x)$ dan $g(x)$ adalah 1.

(I. N. Herstein, 1996)

Berdasarkan pengertian-pengertian tersebut diperoleh definisi berikut.

Definisi 2.37

Polinomial $p(x) \in F[x]$ dengan $\deg p(x) \geq 1$ disebut tak tereduksi dalam $F[x]$ jika untuk sebarang $f(x) \in F[x]$ berlaku $p(x) \mid f(x)$ atau $p(x)$ dan $f(x)$ relatif prima.

(I. N. Herstein, 1996)

Jika $f(x) \in F[x]$ tidak tak tereduksi dalam $F[x]$, maka $f(x)$ disebut tereduksi dalam $F[x]$.

Selanjutnya diberikan pengertian suatu akar dari polinomial dalam $F[x]$.

Definisi 2.38

Suatu elemen a disebut akar dari suatu polinomial $f(x) \in F[x]$ jika $f(a) = 0$.

(I. N. Herstein, 1996)

BAB III

PEMBENTUKAN *EXTENSION FIELD*

Pada bab ini akan dibahas pengertian *extension field* dan sifat-sifat pada *extension field*, serta cara pembentukan suatu *extension field* dari suatu *field* yang diketahui.

Sebelum membahas mengenai cara pembentukan *extension field*, terlebih dahulu akan diberikan pengertian tentang *extension field* serta beberapa sifat yang berlaku pada suatu *extension field*.

3.1 *EXTENSION FIELD*

Berikut diberikan definisi *extension field* dari suatu *field*.

Definisi 3.1.1

Misal F dan E *field*. Maka E disebut *extension field* dari F jika F adalah *subfield* dari E.

(I. N. Herstein, 1996)

Untuk selanjutnya, notasi E menyatakan suatu *extension field* dari *field* F.

Teorema berikut menunjukkan hubungan antara suatu *extension field* E dari F dengan suatu ruang vektor atas suatu *field* F.

Teorema 3.1.2

Jika E adalah *extension field* dari F, maka E merupakan suatu ruang vektor atas *field* F.

(I. N. Herstein, 1996)

Bukti:

Untuk membuktikan bahwa E adalah ruang vektor atas F, maka E harus memenuhi sifat-sifat ruang vektor atas suatu *field* seperti pada Definisi 2.21. Karena E adalah *field*, maka $(E,+,\bullet)$ merupakan suatu sistem matematika dengan operasi penjumlahan dan perkalian dalam E dan $(E,+)$ merupakan group komutatif.

Karena $E \supset F$, maka untuk setiap $\alpha,\beta \in F$, berlaku $\alpha,\beta \in E$. Sehingga untuk setiap skalar $\alpha,\beta \in F$ dan vektor $a,b \in E$, maka syarat kedua sampai keenam dari Definisi 2.21 akan langsung terpenuhi. Sehingga terbukti bahwa E merupakan ruang vektor atas F.

Dengan memandang E sebagai suatu ruang vektor atas F, maka dikenal juga dimensi dari E atas F. Berkaitan dengan pengertian dimensi ruang vektor dan *extension field* dari F sebagai ruang vektor atas F, maka diberikan definisi berikut.

Definisi 3.1.3

Dimensi dari E sebagai ruang vektor atas F disebut derajat dari extension E atas F, dinotasikan dengan $[E:F]$.

(I. N. Herstein, 1996)

Berkaitan dengan definisi tersebut, diberikan teorema berikut.

Teorema 3.1.4

Misal E adalah *extension field* dari F dengan derajat n. Maka, untuk setiap $u \in E$ terdapat elemen-elemen $\alpha_0, \alpha_1, ..., \alpha_n \in F$, yang tidak semuanya nol, sedemikian sehingga

$$\alpha_0 + \alpha_1 u + ... + \alpha_n u^n = 0$$

(I. N. Herstein, 1996)

Bukti:

Ambil $u \in E$ sebarang. Sehingga dengan menggunakan operasi perkalian dalam E, maka $1, u, u^2, ..., u^n \in E$. Selanjutnya pandang E sebagai ruang vektor atas F, dengan $[E:F] = \dim_F(E) = n$. Maka berdasarkan teorema 2.27 diperoleh $\{1, u, u^2, ..., u^n\}$ bergantung linier di E. Dengan demikian dapat ditemukan $\alpha_0, \alpha_1, ..., \alpha_n \in F$, yang tidak semuanya nol, sedemikian sehingga $\alpha_0 + \alpha_1 u + ... + \alpha_n u^n = 0$.

Selanjutnya akan dibahas sifat-sifat yang diperlukan untuk membangun sebuah *extension field* E dari F.

Definisi 3.1.5

Suatu elemen $a \in E \supset F$, disebut *algebraic* atas F jika terdapat polinomial $p(x) \in F[x]$ sedemikian sehingga $p(a) = 0$.

(Neil Koblitz, 1997)

Berdasarkan Teorema 3.1.4, terlihat adanya bentuk polinomial $p(x) = \alpha_0 + \alpha_1 x + ... + \alpha_n x^n$ dalam $F[x]$ dengan $p(u) = 0$, $u \in E$. Berdasarkan hal tersebut, diberikan definisi berikut.

Definisi 3.1.6

Suatu elemen $a \in E \supset F$ disebut *algebraic* dengan derajat n atas F jika terdapat polinomial $p(x) \in F[x]$ dengan derajat n sedemikian sehingga $p(a) = 0$ dan tidak ada polinomial lain dengan derajat kurang dari n dalam $F[x]$ memenuhi sifat tersebut.

(I. N. Herstein, 1996)

Polinomial $p(x)$ pada definisi diatas adalah polinomial monik dan disebut polinomial minimal untuk a atas F.

Teorema 3.1.7

Misal $a \in E$ *algebraic* atas F dengan polinomial minimal $p(x)$ dalam $F[x]$, maka $p(x)$ tak tereduksi dalam $F[x]$

(I. N. Herstein, 1996)

Bukti:

Pembuktian dilakukan dengan menggunakan kontradiksi. Misal $p(x)$ tereduksi dalam $F[x]$, maka $p(x) = f(x)g(x)$ dimana $f(x)$ dan $g(x)$ dalam $F[x]$ dan memiliki derajat positif. Karena $0 = p(a) = f(a)g(a)$ dan karena $f(a)$ dan $g(a)$ adalah elemen dalam *field* F, maka didapat dua kemungkinan, yaitu $f(a) = 0$ atau $g(a) = 0$. Karena $p(x)$ polinomial minimal dan derajat dari $f(x)$ maupun $g(x)$ lebih kecil dari derajat $p(x)$, maka kedua kemungkinan tidak mungkin terjadi. Sehingga didapat bahwa $p(x)$ tak tereduksi dalam $F[x]$.

Jadi, dengan kata lain elemen a yang *algebraic* atas F adalah akar dari suatu polinomial monik yang tak tereduksi dalam $F[x]$.

Sekarang pandang $F(a)$, himpunan yang memuat semua kombinasi linier pangkat-pangkat dari a dengan elemen-elemen F, dimana a *algebraic* atas F dan $a \notin F$. Misal $p(x)$ adalah polinomial minimal untuk a dengan derajat n atas F. Berdasarkan *Divisor Algorithm* pada Teorema 2.31, untuk setiap $f(x) \in F[x]$, berlaku $f(x) = q(x)p(x) + r(x)$, dimana $q(x), r(x) \in F[x]$

dan $r(x)=0$ atau $\deg r(x)<\deg p(x)$. Sehingga $f(a)=q(a)p(a)+r(a)$. Karena $p(x)$ adalah polinomial minimal untuk a atas F, maka $p(a)=0$. Sehingga didapatkan $f(a)=r(a)$, dan karena $\deg r(x)<\deg p(x)$ maka derajat paling besar dari $f(a)$ adalah $n-1$. Sehingga dapat disimpulkan jika $p(x)$ adalah polinomial minimal untuk a dengan derajat n atas F, maka suatu elemen di $F(a)$, yaitu $f(a)$ dapat diekspresikan sebagai kombinasi linier dari $1, a, a^2, ..., a^{n-1}$.

Berkaitan dengan pembahasan diatas, didapatkan teorema berikut.

Teorema 3.1.8

Misal $p(x)$ adalah polinomial minimal untuk a atas F dan $a \notin F$. $F(a)$ adalah *extension field* terkecil dari F yang memuat F dan a dengan $\left[F(a):F\right]=\deg p(x)$.

(Neil Koblitz, 1997)

Bukti:

Untuk membuktikannya, terlebih dahulu akan ditunjukkan bahwa $F(a)$ merupakan suatu ruang vektor atas F. Sekarang ambil sebarang $f(a), g(a) \in F(a)$ dan $\alpha \in F$. Misal $f(a)=\alpha_0+\alpha_1 a+...+\alpha_{n-1}a^{n-1}$ dan $g(a)=\beta_0+\beta_1 a+...+\beta_{n-1}a^{n-1}$, dimana $\alpha_i, \beta_i \in F$. Dengan operasi perkalian skalar diperoleh $\alpha f(a)=\alpha\alpha_0+\alpha\alpha_1 a+...+\alpha\alpha_{n-1}a^{n-1}$. Karena $\alpha \in F$ dan $\alpha_i \in F$,

maka $\alpha\alpha_i \in F$. Sehingga $\alpha f(a) \in F(a)$. Selanjutnya dengan operasi penjumlahan dalam E diperoleh

$$f(a)+g(a)=(\alpha_0+\beta_0)+(\alpha_1+\beta_1)a+...+(\alpha_{n-1}+\beta_{n-1})a^{n-1}$$

Karena $\alpha_i, \beta_i \in F$, maka $\alpha_i + \beta_i \in F$. Sehingga didapat $f(a)+g(a) \in F(a)$. Berdasarkan definisi 2.22, diperoleh $F(a)$ adalah ruang bagian dari ruang vektor E atas F . Sehingga $F(a)$ adalah ruang vektor atas F .

Selanjutnya, untuk membuktikan $\dim_F\left(F(a)\right)=n$, harus ditunjukkan bahwa $\left\{1,a,a^2,...,a^{n-1}\right\}$ bebas linier dan membangun $F(a)$. Sekarang, jika $\alpha_0+\alpha_1 a+\alpha_2 a^2+...+\alpha_{n-1}a^{n-1}=0$, dengan $\alpha_i \in F$, maka $q(a)=0$, dimana $q(x)=\alpha_0+\alpha_1 x+\alpha_2 x^2+...+\alpha_{n-1}x^{n-1} \in F[x]$. Karena $q(x)$ berderajat lebih kecil dari $p(x)$, dan karena $p(x)$ adalah polinomial minimum untuk a atas F , maka dapat disimpulkan bahwa $q(x)=0$. Sehingga mengakibatkan $\alpha_0=\alpha_1=\alpha_2=...=\alpha_{n-1}=0$. Sehingga didapat $\{1,a,a^2,...,a^{n-1}\}$ bebas linier. Berdasarkan definisi $F(a)$, maka diperoleh bahwa $F(a)$ dibangun atas F oleh $\left\{1,a,a^2,...,a^{n-1}\right\}$. Sehingga $\left\{1,a,a^2,...,a^{n-1}\right\}$ membentuk basis untuk $F(a)$. Dengan demikian, $F(a)$ adalah ruang vektor berdimensi hingga atas F dengan $\dim_F\left(F(a)\right)=n$.

Untuk membuktikan $F(a)$ adalah *field*, terlebih dahulu akan ditunjukkan bahwa $F(a)$ adalah *integral domain*. Bardasarkan definisi $F(a)$,

karena $a \in E$ dan $E \supset F$, maka $F(a) \subset E$. Karena *field* E dapat dipandang sebagai suatu *ring*, maka untuk menunjukkan $F(a)$ adalah *ring*, cukup ditunjukkan bahwa $F(a)$ tertutup terhadap operasi penjumlahan dan perkalian dalam E.

Ambil sebarang $f(a), g(a) \in F(a)$, dengan $f(a) = \alpha_0 + \alpha_1 a + ... + \alpha_{n-1} a^{n-1}$ dan $g(a) = \beta_0 + \beta_1 a + ... + \beta_{n-1} a^{n-1}$, dimana $\alpha_i, \beta_i \in F$.

Berdasarkan pembahasan sebelumnya, telah ditunjukkan bahwa $f(a) + g(a) \in F(a)$. Selanjutnya dengan operasi perkalian dalam E diperoleh

$$f(a)g(a) = \left(\alpha_0 + \alpha_1 a + ... + \alpha_{n-1} a^{n-1}\right)\left(\beta_0 + \beta_1 a + ... + \beta_{n-1} a^{n-1}\right)$$

$$= \alpha_0 \left(\beta_0 + \beta_1 a + ... + \beta_{n-1} a^{n-1}\right) + ... + \alpha_{n-1} a^{n-1} \left(\beta_0 + \beta_1 a + ... + \beta_{n-1} a^{n-1}\right)$$

Terdapat dua kasus untuk nilai n, yaitu:

- Untuk kasus n ganjil

$$f(a)g(a) = \alpha_0\beta_0 + (\alpha_0\beta_1 + \alpha_1\beta_0)a + (\alpha_0\beta_2 + \alpha_1\beta_1 + \alpha_2\beta_0)a^2 + ...$$

$$... + (\alpha_0\beta_{n-1} + \alpha_1\beta_{n-2} + ... + \alpha_{n-2}\beta_1 + \alpha_{n-1}\beta_0)a^{n-1}$$

$$+ \left(\alpha_1\beta_{n-1} + ... + \alpha_{\lfloor n/2 \rfloor}\beta_{\lceil n/2 \rceil} + \alpha_{\lceil n/2 \rceil}\beta_{\lfloor n/2 \rfloor} + ... + \alpha_{n-1}\beta_1\right)a^n$$

$$+ \left(\alpha_2\beta_{n-1} + ... + \alpha_{(n+1)/2}\beta_{(n+1)/2} + ... + \alpha_{n-1}\beta_2\right)a^{n+1} + ... + \alpha_{n-1}\beta_{n-1}a^{2n-2}$$

- Untuk kasus n genap

$$f(a)g(a) = \alpha_0\beta_0 + (\alpha_0\beta_1 + \alpha_1\beta_0)a + (\alpha_0\beta_2 + \alpha_1\beta_1 + \alpha_2\beta_0)a^2 + \ldots$$

$$\ldots + (\alpha_0\beta_{n-1} + \alpha_1\beta_{n-2} + \ldots + \alpha_{n-2}\beta_1 + \alpha_{n-1}\beta_0)a^{n-1}$$

$$+ \left(\alpha_1\beta_{n-1} + \ldots + \alpha_{n/2}\beta_{n/2} + \ldots + \alpha_{n-1}\beta_1\right)a^n$$

$$+ \left(\alpha_2\beta_{n-1} + \ldots + \alpha_{\lfloor n+1/2 \rfloor}\beta_{\lceil n+1/2 \rceil} + \alpha_{\lceil n+1/2 \rceil}\beta_{\lfloor n+1/2 \rfloor} + \ldots + \alpha_{n-1}\beta_2\right)a^{n+1} + \ldots$$

$$\ldots + \alpha_{n-1}\beta_{n-1}a^{2n-2}$$

Berdasarkan pembahasan sebelumnya, diketahui bahwa suatu polinomial dalam a, dimana a *algebraic* dengan derajat n atas F, memiliki pangkat tertinggi $n-1$. Jika suatu polinomial derajatnya lebih besar dari $n-1$ maka dapat direduksi dengan menggunakan operasi modulo $p(x)$, yaitu polinomial minimal untuk a. Sehingga suku-suku dengan derajat lebih besar dari $n-1$ pada polinomial hasil perkalian tersebut akan digantikan dengan suku lain yang merupakan sisa pembagian suku awal dengan polinomial minimal $p(x)$, sehingga pangkatnya akan lebih kecil dari n.

Jadi, dapat ditulis

- Untuk kasus n ganjil

$$f(a)g(a) = \alpha_0\beta_0 + (\alpha_0\beta_1 + \alpha_1\beta_0)a + (\alpha_0\beta_2 + \alpha_1\beta_1 + \alpha_2\beta_0)a^2 + \ldots$$

$$\ldots + (\alpha_0\beta_{n-1} + \alpha_1\beta_{n-2} + \ldots + \alpha_{n-2}\beta_1 + \alpha_{n-1}\beta_0)a^{n-1}$$

$$+ \left(\alpha_1\beta_{n-1} + \ldots + \alpha_{\lfloor n/2 \rfloor}\beta_{\lceil n/2 \rceil} + \alpha_{\lceil n/2 \rceil}\beta_{\lfloor n/2 \rfloor} + \ldots + \alpha_{n-1}\beta_1\right)a^n \bmod p(x)$$

$$+\left(\alpha_2\beta_{n-1}+...+\alpha_{(n+1)/2}\beta_{(n+1)/2}+...+\alpha_{n-1}\beta_2\right)a^{n+1} \bmod p(x)+...$$

$$...+\alpha_{n-1}\beta_{n-1}a^{2n-2} \bmod p(x)$$

- Untuk kasus n genap

$$f(a)g(a)=\alpha_0\beta_0+(\alpha_0\beta_1+\alpha_1\beta_0)a+(\alpha_0\beta_2+\alpha_1\beta_1+\alpha_2\beta_0)a^2+...$$

$$...+(\alpha_0\beta_{n-1}+\alpha_1\beta_{n-2}+...+\alpha_{n-2}\beta_1+\alpha_{n-1}\beta_0)a^{n-1}$$

$$+\left(\alpha_1\beta_{n-1}+...+\alpha_{n/2}\beta_{n/2}+...+\alpha_{n-1}\beta_1\right)a^n \bmod p(x)$$

$$+\left(\alpha_2\beta_{n-1}+...+\alpha_{\lfloor n+1/2\rfloor}\beta_{\lceil n+1/2\rceil}+...+\alpha_{n-1}\beta_2\right)a^{n+1} \bmod p(x)+...$$

$$...+\alpha_{n-1}\beta_{n-1}a^{2n-2} \bmod p(x)$$

Karena $\alpha_i,\beta_i\in F$, maka untuk setiap kasus dari nilai n diperoleh $(\alpha_i\beta_j+...+\alpha_k\beta_l)\in F$ untuk $i,j,k,l\in\{0,1,...,n-1\}$. Sehingga, terbukti $F(a)$ adalah *ring*. $F(a)$ merupakan *ring* komutatif, karena

$$f(a)+g(a)=(\alpha_0+\beta_0)+(\alpha_1+\beta_1)a+...+(\alpha_{n-1}+\beta_{n-1})a^{n-1}$$

$$=(\beta_0+\alpha_0)+(\beta_1+\alpha_1)a+...+(\beta_{n-1}+\alpha_{n-1})a^{n-1}=g(a)+f(a)$$

Sekarang, akan ditunjukkan bahwa $F(a)$ adalah *integral domain*. Misal $f(a)g(a)=0$. Tanpa menghilangkan keumuman, dapat diambil suatu kasus dari nilai n untuk membuktikan. Misal n genap.

$$f(a)g(a) = \alpha_0\beta_0 + (\alpha_0\beta_1 + \alpha_1\beta_0)a + (\alpha_0\beta_2 + \alpha_1\beta_1 + \alpha_2\beta_0)a^2 + \ldots$$

$$\ldots + (\alpha_0\beta_{n-1} + \alpha_1\beta_{n-2} + \ldots + \alpha_{n-2}\beta_1 + \alpha_{n-1}\beta_0)a^{n-1}$$

$$+ \left(\alpha_1\beta_{n-1} + \ldots + \alpha_{n/2}\beta_{n/2} + \ldots + \alpha_{n-1}\beta_1\right)a^n \bmod p(x)$$

$$+ \left(\alpha_2\beta_{n-1} + \ldots + \alpha_{\lfloor n+1/2 \rfloor}\beta_{\lceil n+1/2 \rceil} + \ldots + \alpha_{n-1}\beta_2\right)a^{n+1} \bmod p(x) + \ldots$$

$$\ldots + \alpha_{n-1}\beta_{n-1}a^{2n-2} \bmod p(x)$$

Maka didapat

$\alpha_0\beta_0 = (\alpha_0\beta_1 + \alpha_1\beta_0) = (\alpha_0\beta_2 + \alpha_1\beta_1 + \alpha_2\beta_0) = \ldots = (\alpha_0\beta_{n-1} + \ldots + \alpha_{n-1}\beta_0) = 0$ dan

$\left(\alpha_1\beta_{n-1} + \ldots + \alpha_{n/2}\beta_{n/2} + \ldots + \alpha_{n-1}\beta_1\right) = \ldots = \alpha_{n-1}\beta_{n-1} = 0$

Karena $\alpha_i, \beta_i \in F$ dan $0 \neq a \in E$ (untuk kasus $a = 0$, diperoleh $f(a) = 0$ dan $g(a) = 0$), maka kondisi diatas terpenuhi jika dan hanya jika $\alpha_i = 0$ atau $\beta_i = 0$. Sehingga mengakibatkan $f(a) = 0$ atau $g(a) = 0$. Sehingga, diperoleh bahwa $F(a)$ adalah suatu *integral domain*. Karena $1 \in F(a)$ dan $\dim_F\left(F(a)\right) = n$, maka berdasarkan Teorema 2.28 diperoleh bahwa $F(a)$ adalah *field*. Karena $\dim_F\left(F(a)\right) = n$, maka didapatkan $\left[F(a) : F\right] = n$.

Perhatikan bahwa jika M adalah suatu *field* yang memuat F dan a, maka M memuat semua polinomial dalam a atas F, sehingga $M \supset F(a)$. Jadi, $F(a)$ adalah *field* terkecil yang memuat F dan a.

Untuk selanjutnya, *field* $F(a)$ ini disebut juga *extension field* dari F yang diperoleh dengan *adjoining* a ke dalam F.

Berdasarkan pembahasan diatas, jika kita punya suatu polinomial $p(x)$ dengan derajat n yang tak tereduksi dalam $F[x]$, dimana $p(a)=0$ dan $a \notin F$, kita dapat membangun suatu *extension field* dari F, yaitu $F(a)$.

Berkaitan dengan pembuktian Teorema 3.1.8 diatas, diberikan definisi berikut.

Definisi 3.1.9

Misal F *field* dan terdapat $p(x) \in F[x]$, polinomial minimal untuk a, dengan $p(a)=0$ dan $a \notin F$. Maka $F(a)$, *field* terkecil yang memuat F dan a, merupakan *extension field* dari F dan disebut *splitting field* untuk $p(x)$ atas F.

(Neil Koblitz, 1997)

Berikut diberikan suatu definisi untuk akar lain dari suatu polinomial minimal $p(x)$ untuk a atas F.

Definisi 3.1.10

Misal $p(x)$ polinomial minimal dari a atas F. Suatu akar lain a' dari $p(x)$ disebut konjugate dari a atas F.

(Neil Koblitz, 1997)

Hubungan antara a dan a' sebagai konjugate dari a atas F diberikan oleh teorema berikut.

Teorema 3.1.11

Jika a' adalah konjugate dari a atas F, maka *field* $F(a)$ dan $F(a')$ isomorfik.

(Neil Koblitz, 1997)

Bukti:

Berdasarkan Definisi 2.20, untuk membuktikan bahwa *field* $F(a)$ dan $F(a')$ isomorfik harus ditunjukkan terdapat homomorfisma $\varphi : F(a) \to F(a')$ yang merupakan pemetaan 1-1 dan onto.

Karena $F(a) = \left\{ \alpha_0 + \alpha_1 a + ... + \alpha_{n-1} a^{n-1} \mid \alpha_i \in F \right\}$ dan

$F(a') = \left\{ \mu_0 + \mu_1 a' + ... + \mu_{n-1} (a')^{n-1} \mid \mu_i \in F \right\}$, maka kita bisa mengaitkan suatu polinomial dalam a dan polinomial dalam a'. Pandang $\varphi : f(a) \mapsto f(a')$, dimana $f(a) \in F(a)$ dan $f(a') \in F(a')$.

Berikut akan ditunjukkan bahwa $\varphi : f(a) \mapsto f(a')$ well defined. Artinya akan ditunjukkan jika $f(a) = g(a)$, maka $\varphi(f(a)) = \varphi(g(a))$.

Ambil sebarang $f(a), g(a) \in F(a)$, dimana $f(a) = \alpha_0 + \alpha_1 a + ... + \alpha_{n-1} a^{n-1}$ dan $g(a) = \beta_0 + \beta_1 a + ... + \beta_{n-1} a^{n-1}$.

Misal $f(a) = g(a)$

Maka $\alpha_0 + \alpha_1 a + ... + \alpha_{n-1} a^{n-1} = \beta_0 + \beta_1 a + ... + \beta_{n-1} a^{n-1}$

Hal tersebut terpenuhi jika dan hanya jika $\alpha_0 = \beta_0$, $\alpha_1 = \beta_1$, ..., $\alpha_{n-1} = \beta_{n-1}$.

Sedangkan

$\varphi(f(a)) = \alpha_0 + \alpha_1 a' + ... + \alpha_{n-1}(a')^{n-1}$ dan $\varphi(g(a)) = \beta_0 + \beta_1 a' + ... + \beta_{n-1}(a')^{n-1}$.

Sehingga diperoleh

$\varphi(f(a)) = \varphi(g(a))$.

Jadi, terbukti $\varphi: f(a) \mapsto f(a')$ well defined.

Sekarang akan ditunjukkan bahwa φ adalah suatu homomorfisma, yaitu memenuhi kedua syarat pada Definisi 2.18 sebagai berikut.

1) Ambil sebarang $f(a), g(a) \in F(a)$, dimana $f(a) = \alpha_0 + \alpha_1 a + ... + \alpha_{n-1} a^{n-1}$ dan $g(a) = \beta_0 + \beta_1 a + ... + \beta_{n-1} a^{n-1}$.

   Sehingga

   $f(a) + g(a) = (\alpha_0 + \beta_0) + (\alpha_1 + \beta_1)a + ... + (\alpha_{n-1} + \beta_{n-1})a^{n-1}$.

   Sekarang

   $\varphi(f(a) + g(a)) = (\alpha_0 + \beta_0) + (\alpha_1 + \beta_1)a' + ... + (\alpha_{n-1} + \beta_{n-1})(a')^{n-1}$

   sedangkan

   $$\varphi(f(a)) + \varphi(g(a)) = \left(\alpha_0 + \alpha_1 a' + ... + \alpha_{n-1}(a')^{n-1}\right) + \left(\beta_0 + \beta_1 a' + ... + \beta_{n-1}(a')^{n-1}\right)$$

   $$= (\alpha_0 + \beta_0) + (\alpha_1 + \beta_1)a' + ... + (\alpha_{n-1} + \beta_{n-1})(a')^{n-1}$$

   Maka diperoleh,

   $\varphi(f(a) + g(a)) = \varphi(f(a)) + \varphi(g(a))$ untuk setiap $f(a), g(a) \in F(a)$.

2) Ambil sebarang $f(a), g(a) \in F(a)$, dimana $f(a) = \alpha_0 + \alpha_1 a + ... + \alpha_{n-1} a^{n-1}$ dan $g(a) = \beta_0 + \beta_1 a + ... + \beta_{n-1} a^{n-1}$.

Berdasarkan pembahasan sebelumnya dalam pembuktian $F(a)$ adalah *integral domain*, diperoleh

- Untuk kasus n ganjil

$$f(a)g(a) = \alpha_0\beta_0 + (\alpha_0\beta_1 + \alpha_1\beta_0)a + (\alpha_0\beta_2 + \alpha_1\beta_1 + \alpha_2\beta_0)a^2 + ...$$
$$... + (\alpha_0\beta_{n-1} + \alpha_1\beta_{n-2} + ... + \alpha_{n-2}\beta_1 + \alpha_{n-1}\beta_0)a^{n-1}$$
$$+ \left(\alpha_1\beta_{n-1} + ... + \alpha_{\lfloor n/2 \rfloor}\beta_{\lceil n/2 \rceil} + \alpha_{\lceil n/2 \rceil}\beta_{\lfloor n/2 \rfloor} + ... + \alpha_{n-1}\beta_1\right) a^n \bmod p(x)$$
$$+ \left(\alpha_2\beta_{n-1} + ... + \alpha_{n/2}\beta_{n/2} + ... + \alpha_{n-1}\beta_2\right) a^{n+1} \bmod p(x) + ...$$
$$... + \alpha_{n-1}\beta_{n-1} a^{2n-2} \bmod p(x)$$

- Untuk kasus n genap

$$f(a)g(a) = \alpha_0\beta_0 + (\alpha_0\beta_1 + \alpha_1\beta_0)a + (\alpha_0\beta_2 + \alpha_1\beta_1 + \alpha_2\beta_0)a^2 + ...$$
$$... + (\alpha_0\beta_{n-1} + \alpha_1\beta_{n-2} + ... + \alpha_{n-2}\beta_1 + \alpha_{n-1}\beta_0)a^{n-1}$$
$$+ \left(\alpha_1\beta_{n-1} + ... + \alpha_{n/2}\beta_{n/2} + ... + \alpha_{n-1}\beta_1\right) a^n \bmod p(x)$$
$$+ \left(\alpha_2\beta_{n-1} + ... + \alpha_{\lfloor n+1/2 \rfloor}\beta_{\lceil n+1/2 \rceil} + ... + \alpha_{n-1}\beta_2\right) a^{n+1} \bmod p(x) + ...$$
$$... + \alpha_{n-1}\beta_{n-1} a^{2n-2} \bmod p(x)$$

Sehingga

- Untuk kasus n ganjil

$$\varphi\left(f(a)g(a)\right) = \alpha_0\beta_0 + (\alpha_0\beta_1 + \alpha_1\beta_0)a' + (\alpha_0\beta_2 + \alpha_1\beta_1 + \alpha_2\beta_0)(a')^2 + \ldots$$

$$\ldots + (\alpha_0\beta_{n-1} + \alpha_1\beta_{n-2} + \ldots + \alpha_{n-2}\beta_1 + \alpha_{n-1}\beta_0)(a')^{n-1}$$

$$+\left(\alpha_1\beta_{n-1} + \ldots + \alpha_{\lfloor n/2\rfloor}\beta_{\lceil n/2\rceil} + \alpha_{\lceil n/2\rceil}\beta_{\lfloor n/2\rfloor} + \ldots + \alpha_{n-1}\beta_1\right)(a')^n \bmod p(x)$$

$$+\left(\alpha_2\beta_{n-1} + \ldots + \alpha_{n/2}\beta_{n/2} + \ldots + \alpha_{n-1}\beta_2\right)(a')^{n+1} \bmod p(x) + \ldots$$

$$\ldots + \alpha_{n-1}\beta_{n-1}(a')^{2n-2} \bmod p(x)$$

- Untuk kasus n genap

$$\varphi\left(f(a)g(a)\right) = \alpha_0\beta_0 + (\alpha_0\beta_1 + \alpha_1\beta_0)a' + (\alpha_0\beta_2 + \alpha_1\beta_1 + \alpha_2\beta_0)(a')^2 + \ldots$$

$$\ldots + (\alpha_0\beta_{n-1} + \alpha_1\beta_{n-2} + \ldots + \alpha_{n-2}\beta_1 + \alpha_{n-1}\beta_0)(a')^{n-1}$$

$$+\left(\alpha_1\beta_{n-1} + \ldots. + \alpha_{n/2}\beta_{n/2} + \ldots. + \alpha_{n-1}\beta_1\right)(a')^n \bmod p(x)$$

$$+\left(\alpha_2\beta_{n-1} + \ldots + \alpha_{\lfloor n+1/2\rfloor}\beta_{\lceil n+1/2\rceil} + \ldots + \alpha_{n-1}\beta_2\right)(a')^{n+1} \bmod p(x) + \ldots$$

$$\ldots + \alpha_{n-1}\beta_{n-1}(a')^{2n-2} \bmod p(x)$$

Sedangkan

$$\varphi\left(f(a)\right)\varphi\left(g(a)\right) = \left(\alpha_0 + \alpha_1 a' + \ldots + \alpha_{n-1}(a')^{n-1}\right)\left(\beta_0 + \beta_1 a' + \ldots + \beta_{n-1}(a')^{n-1}\right)$$

$$= \alpha_0\left(\beta_0 + \ldots + \beta_{n-1}(a')^{n-1}\right) + \ldots + \alpha_{n-1}(a')^{n-1}\left(\beta_0 + \ldots + \beta_{n-1}(a')^{n-1}\right)$$

Karena a' adalah akar lain dari $p(x)$, maka a' juga *algebraic* dengan atas F derajat n. Sehingga dapat ditulis seperti pada pembahasan polinomial dalam a.

Jadi,

- Untuk kasus n ganjil

$$\varphi\big(f(a)g(a)\big) = \alpha_0\beta_0 + (\alpha_0\beta_1 + \alpha_1\beta_0)a' + (\alpha_0\beta_2 + \alpha_1\beta_1 + \alpha_2\beta_0)(a')^2 + \ldots$$
$$\ldots + (\alpha_0\beta_{n-1} + \alpha_1\beta_{n-2} + \ldots + \alpha_{n-2}\beta_1 + \alpha_{n-1}\beta_0)(a')^{n-1}$$
$$+\Big(\alpha_1\beta_{n-1} + \ldots + \alpha_{\lfloor n/2\rfloor}\beta_{\lceil n/2\rceil} + \alpha_{\lceil n/2\rceil}\beta_{\lfloor n/2\rfloor} + \ldots + \alpha_{n-1}\beta_1\Big)(a')^n \bmod p(x)$$
$$+\big(\alpha_2\beta_{n-1} + \ldots + \alpha_{n/2}\beta_{n/2} + \ldots + \alpha_{n-1}\beta_2\big)(a')^{n+1} \bmod p(x) + \ldots$$
$$\ldots + \alpha_{n-1}\beta_{n-1}(a')^{2n-2} \bmod p(x)$$

- Untuk kasus n genap

$$\varphi\big(f(a)g(a)\big) = \alpha_0\beta_0 + (\alpha_0\beta_1 + \alpha_1\beta_0)a' + (\alpha_0\beta_2 + \alpha_1\beta_1 + \alpha_2\beta_0)(a')^2 + \ldots$$
$$\ldots + (\alpha_0\beta_{n-1} + \alpha_1\beta_{n-2} + \ldots + \alpha_{n-2}\beta_1 + \alpha_{n-1}\beta_0)(a')^{n-1}$$
$$+\big(\alpha_1\beta_{n-1} + \ldots + \alpha_{n/2}\beta_{n/2} + \ldots + \alpha_{n-1}\beta_1\big)(a')^n \bmod p(x)$$
$$+\Big(\alpha_2\beta_{n-1} + \ldots + \alpha_{\lfloor n+1/2\rfloor}\beta_{\lceil n+1/2\rceil} + \ldots + \alpha_{n-1}\beta_2\Big)(a')^{n+1} \bmod p(x) + \ldots$$
$$\ldots + \alpha_{n-1}\beta_{n-1}(a')^{2n-2} \bmod p(x)$$

Dengan demikian diperoleh

$$\varphi\big(f(a)g(a)\big) = \varphi\big(f(a)\big)\varphi\big(g(a)\big) \text{ untuk setiap } f(a), g(a) \in F(a)$$

Sehingga, terbukti bahwa φ adalah homomorfisma antara $F(a)$ dan $F(a')$.

Selanjutnya, berdasarkan Definisi 2.20, untuk membuktikan φ adalah suatu isomorfisma harus ditunjukkan bahwa φ adalah pemetaan 1-1 dan onto. Karena pemetaan φ adalah homomorfisma, maka berdasarkan Teorema 2.19, untuk menunjukkan bahwa φ adalah pemetaan 1-1, cukup dibuktikan $Ker(\varphi) = \mathrm{O}$.

Ambil sebarang $u(a) \in Ker(\varphi)$, dimana $u(a) = \gamma_0 + \gamma_1 a + ... + \gamma_{n-1} a^{n-1}$. Maka

$\varphi(u(a)) = \gamma_0 + \gamma_1 a' + ... + \gamma_{n-1}(a')^{n-1} = 0$.

Karena $\{1, a', ..., (a')^{n-1}\}$ membentuk basis untuk $F(a')$, maka $\{1, a', ..., (a')^{n-1}\}$ adalah bebas linier. Sehingga persamaan $\gamma_0 + \gamma_1 a' + ... + \gamma_{n-1}(a')^{n-1} = 0$ hanya dipenuhi oleh $\gamma_0 = \gamma_1 = ... = \gamma_{n-1} = 0$. Jadi, $u(a) = \gamma_0 + \gamma_1 a + ... + \gamma_{n-1} a^{n-1} = 0$.

Dengan demikian terbukti bahwa $Ker(\varphi) = \mathrm{O}$.

Selanjutnya harus dibuktikan bahwa φ adalah pemetaan onto. Artinya akan ditunjukkan untuk setiap $q(a') \in F(a')$ terdapat $f(a) \in F(a)$ sedemikian sehingga $\varphi(f(a)) = q(a')$.

Misal $q(a') = \alpha_0 + \alpha_1 a' + ... + \alpha_{n-1}(a')^{n-1}$ dimana $\alpha_i \in F$

pilih $f(a) = q(a) = \alpha_0 + \alpha_1 a + ... + \alpha_{n-1}a^{n-1} \in F(a)$

Sehingga diperoleh $\varphi(f(a)) = \alpha_0 + \alpha_1 a' + ... + \alpha_{n-1}(a')^{n-1} = q(a')$

Jadi, didapat bahwa φ adalah pemetaan onto.

Dari uraian diatas, diperoleh bahwa $F(a) \cong F(a')$ dengan pemetaan $\varphi : F(a) \to F(a')$ dimana $\varphi : f(a) \mapsto f(a')$.

3.2 PEMBENTUKAN *EXTENSION FIELD*

Karakteristik suatu *field* F adalah bilangan bulat terkecil p yang memenuhi $pa = \underbrace{a + a + ... + a}_{p} = 0$ dalam F. Jika hal tersebut berlaku, maka *field* F dikatakan mempunyai karakteristik p. Jika tidak terdapat p sedemikian sehingga hal tersebut berlaku, maka *field* F dikatakan mempunyai karakteristik 0. Hal ini sesuai dengan Teorema 2.15, yang menyatakan bahwa karakteristik dari suatu *field* hanya mungkin 0 atau p, dimana p prima. Maka pembentukan *extension field* dibagi ke dalam dua kelompok, yaitu pembentukan *extension field* dari suatu *field* dengan karakteristik 0 atau *field* tak hingga, yang diwakili oleh *field* $\mathbb{Q}$ dan $\mathbb{R}$, dan

pembentukan *extension field* dari suatu *field* dengan karakteristik p atau *field* hingga, yang diwakili oleh *field* $\mathbb{Z}_p$.

Secara umum, pembentukkan *extension field* dari suatu *field* F tertentu dilakukan dengan langkah-langkah sebagai berikut.

1. Cari suatu polinomial monik $p(x)$ yang tak tereduksi dalam $F[x]$.
2. Temukan akar α dari $p(x)$ dengan $\alpha \notin F$.
3. Bentuk $F(\alpha)$, yaitu himpunan yang memuat semua kombinasi linier dari α dan elemen-elemen dari F.

Maka sesuai dengan Teorema 3.1.8, $F(\alpha)$ merupakan *extension field* dari F. Jika $p(x)$ mempunyai lebih dari satu akar, maka *extension field* yang dihasilkan dari masing-masing akar akan saling isomorfik, sesuai dengan Teorema 3.1.11.

Berikut ini akan diberikan cara pembentukkan suatu *extension field* dari suatu field F berdasarkan karakteristik field F.

3.2.1 *Extension field* dari suatu *field* dengan karakteristik 0

Field $\mathbb{Q}$ atau $\mathbb{R}$ merupakan *field* berkarakteristik 0. Berikut ini diberikan beberapa contoh pembentukkan *extension field* dari suatu *field* dengan karakteristik 0.

1) Untuk $\mathbb{Q}$ *field* bilangan rasional, pilih $p(x) = x^2 - 3 \in \mathbb{Q}[x]$ sebagai polinomial monik yang tak tereduksi dalam $\mathbb{Q}$. Akar-akar dari persamaan $x^2 - 3 = 0$ adalah $\sqrt{3}$ dan $-\sqrt{3}$, yang bukan anggota $\mathbb{Q}$.

Untuk akar $\alpha = \sqrt{3}$, maka akan diperoleh suatu *extension* dari $\mathbb{Q}$, yaitu *field* $\mathbb{Q}\left(\sqrt{3}\right) = \left\{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\right\}$.

sedangkan untuk akar $\alpha = -\sqrt{3}$, maka akan diperoleh *extension field* dari $\mathbb{Q}$, yaitu $\mathbb{Q}\left(-\sqrt{3}\right) = \left\{a - b\sqrt{3} \mid a, b \in \mathbb{Q}\right\}$.

Field $\mathbb{Q}\left(\sqrt{3}\right)$ dan *field* $\mathbb{Q}\left(-\sqrt{3}\right)$ adalah isomorfik, karena terdapat pemetaan $\varphi : \mathbb{Q}\left(\sqrt{3}\right) \to \mathbb{Q}\left(-\sqrt{3}\right)$ dengan pengaitan $\varphi : a + b\sqrt{3} \mapsto a - b\sqrt{3}$ yang merupakan automorfisma. Untuk menunjukkannya, terlebih dahulu akan ditunjukkan bahwa $\varphi : a + b\sqrt{3} \mapsto a - b\sqrt{3}$ well defined.

Ambil sebarang $m, n \in \mathbb{Q}\left(\sqrt{3}\right)$, dimana $m = a + b\sqrt{3}$ dan $n = c + d\sqrt{3}$ dengan $a, b, c, d \in \mathbb{Q}$.

Misal $m = n$.

Maka $a + b\sqrt{3} = c + d\sqrt{3}$

Hal tersebut terpenuhi jika dan hanya jika $a = c$ dan $b = d$.

Sedangkan

$\varphi(m) = \varphi\left(a + b\sqrt{3}\right) = a - b\sqrt{3}$ dan $\varphi(n) = \varphi\left(c + d\sqrt{3}\right) = c - d\sqrt{3}$

Sehingga diperoleh

$\varphi(m) = \varphi(n)$

Jadi, terbukti bahwa φ well defined.

Selanjutnya akan dibuktikan bahwa φ adalah homomorfisma. Artinya φ harus memenuhi syarat-syarat seperti pada Definisi 2.18 sebagai berikut:

- Ambil sebarang $m, n \in \mathbb{Q}\left(\sqrt{3}\right)$, dimana $m = a + b\sqrt{3}$ dan $n = c + d\sqrt{3}$ dengan $a, b, c, d \in \mathbb{Q}$.

  sehingga

  $m + n = (a + c) + (b + d)\sqrt{3}$, maka $\varphi\left(m + n\right) = (a + c) - (b + d)\sqrt{3}$

  sedangkan $\varphi(m) + \varphi(n) = a - b\sqrt{3} + \left(c - d\sqrt{3}\right) = (a + b) - \left(b + d\right)\sqrt{3}$

  Sehingga diperoleh $\varphi\left(m + n\right) = \varphi\left(m\right) + \varphi\left(n\right)$

- Ambil sebarang $m, n \in \mathbb{Q}\left(\sqrt{3}\right)$, dimana $m = a + b\sqrt{3}$ dan $n = c + d\sqrt{3}$ dengan $a, b, c, d \in \mathbb{Q}$.

  sehingga

  $mn = \left(a + b\sqrt{3}\right)\left(c + d\sqrt{3}\right) = (ac + 3bd) + (ad + bc)\sqrt{3}$

  Sekarang

  $\varphi\left(mn\right) = (ac + 3bd) - (ad + bc)\sqrt{3}$

  sedangkan

$$\varphi(m)\varphi(n) = \left(a - b\sqrt{3}\right)\left(c - d\sqrt{3}\right) = (ac + 3bd) - (ad + bc)\sqrt{3}$$

Sehingga diperoleh

$$\varphi(mn) = \varphi(m)\varphi(n)$$

Jadi, terbukti bahwa φ adalah suatu homomorfisma.

Selanjutnya, berdasarkan Definisi 2.20, untuk membuktikan φ adalah suatu isomorfisma harus ditunjukkan bahwa φ adalah pemetaan 1-1 dan onto. Karena pemetaan φ adalah homomorfisma, maka berdasarkan Teorema 2.19, untuk menunjukkan bahwa φ adalah pemetaan 1-1, cukup dibuktikan $Ker(\varphi) = \mathrm{O}$.

Ambil sebarang $k \in Ker(\varphi)$, dimana $k = l + j\sqrt{3}$ dengan $l, j \in \mathbb{Q}$.

Maka

$\varphi(k) = l - j\sqrt{3} = 0$.

Karena $l, j \in \mathbb{Q}$, maka persamaan tersebut hanya dipenuhi oleh $l = 0$ dan $j = 0$. Jadi, $k = 0 - 0\sqrt{3} = 0$.

Dengan demikian terbukti bahwa $Ker(\varphi) = \mathrm{O}$.

Selanjutnya harus dibuktikan bahwa φ adalah pemetaan onto. Artinya akan ditunjukkan untuk setiap $q \in \mathbb{Q}\left(-\sqrt{3}\right)$ terdapat $m \in \mathbb{Q}\left(\sqrt{3}\right)$ sedemikian sehingga $\varphi(m) = q$.

Misal $q = a - b\sqrt{3}$ dimana $a, b \in \mathbb{Q}$

pilih $m = a + b\sqrt{3} \in \mathbb{Q}\left(\sqrt{3}\right)$

Sehingga diperoleh $\varphi(m) = \varphi\left(a + b\sqrt{3}\right) = a - b\sqrt{3} = q$

Jadi, terbukti bahwa φ adalah pemetaan onto.

Dengan demikian, didapat bahwa φ adalah isomorfisma. Namun jika diperhatikan *field* $\mathbb{Q}\left(\sqrt{3}\right)$ dan *field* $\mathbb{Q}\left(-\sqrt{3}\right)$ adalah *field* yang sama. Sehingga φ adalah suatu automorfisma.

2) Untuk $\mathbb{R}$, *field* bilangan riil, pilih $p(x) = x^2 + 1 \in \mathbb{R}[x]$ sebagai polinomial monik yang tak tereduksi dalam $\mathbb{R}$. Akar-akar dari persamaan $x^2 + 1 = 0$ adalah i dan $-i$, yang bukan anggota $\mathbb{R}$.
Jika dipilih $\alpha = i$, maka akan diperoleh suatu *extension field* dari $\mathbb{R}$, yaitu *field* $\mathbb{R}(i) = \{a + bi \mid a, b \in \mathbb{R}\}$.
Misal akar dari $p(x)$ yang diambil adalah $\alpha = -i$, maka akan diperoleh *extension field* dari $\mathbb{R}$, yaitu $\mathbb{R}(-i) = \{a - bi \mid a, b \in \mathbb{R}\}$.
Sesuai dengan uraian dari contoh sebelumnya, didapat bahwa pemetaan $\varphi : \mathbb{R}(i) \to \mathbb{R}(-i)$ dengan $\varphi : a + bi \mapsto a - bi$ merupakan suatu automorfisma, karena *field* $\mathbb{R}(i)$ dan *field* $\mathbb{R}(-i)$ adalah *field* yang sama.

3.2.2 *Extension field* dari suatu *field* dengan karakteristik p.

Pandang *field* $\mathbb{Z}_p = \{0,1,...,p-1\}$ yang merupakan field dengan karakteristik p. *Extension field* dari *field* $\mathbb{Z}_p$ dibentuk dengan *adjoining* suatu akar dari polinomial yang tak tereduksi dalam $\mathbb{Z}_p[x]$. *Extension field* dari $\mathbb{Z}_p$ dinotasikan sebagai $GF(q)$, dengan q merupakan jumlah elemen dalam *field* tersebut.

Berikut akan diberikan contoh pembentukkan *extension field* dari suatu *field* dengan karakteristik $p=3$ dan $p=2$.

1. $p=3$.

Maka *field* pembentuknya adalah $\mathbb{Z}_3$, dengan elemen-elemennya diwakili oleh 0, 1 dan 2. Selanjutnya, untuk mendapatkan *extension field* dari $\mathbb{Z}_3$ dengan derajat atas $\mathbb{Z}_3$ adalah dua, akan dicari suatu polinomial monik $p(x)$ dengan derajat $n=2$ yang tak tereduksi dalam $\mathbb{Z}_3[x]$. Berikut ini adalah daftar polinomial-polinomial monik berderajat dua yang ada dalam $\mathbb{Z}_3[x]$

- x^2
- x^2+1
- x^2+2

- $x^2 + x$
- $x^2 + x + 1$
- $x^2 + x + 2$
- $x^2 + 2x$
- $x^2 + 2x + 1$
- $x^2 + 2x + 2$

Dari daftar diatas, akan dicari polinomial- polinomial tak tereduksi dalam $\mathbb{Z}_3[x]$. Polinomial-polinomial tanpa suku konstan jelas dapat difaktorkan dalam $\mathbb{Z}_3[x]$, karena x akan merupakan salah satu faktornya. Sehingga polinomial pertama, keempat dan ketujuh pada daftar diatas dapat diabaikan. Untuk enam polinomial sisanya, dapat dilakukan pengujian dengan mensubstitusi elemen-elemen dalam $\mathbb{Z}_3$ ke dalam polinomial tersebut. Jika polinomial bernilai nol untuk satu atau lebih elemen dalam $\mathbb{Z}_3$ maka polinomial tersebut dikatakan tereduksi dalam $\mathbb{Z}_3[x]$, tetapi jika polinomial bernilai tak nol untuk semua elemen maka polinomial tersebut dikatakan tak tereduksi dalam $\mathbb{Z}_3[x]$.

Pemeriksaan ini dimulai dengan mensubstitusi semua elemen $\mathbb{Z}_3$ kedalam $x^2 + 2$ yang memberikan nilai-nilai berikut: $0^2 + 2 = 2$, $1^2 + 2 = 0$ dan $2^2 + 2 = 0$. Jadi, $x^2 + 2$ dapat difaktorkan dalam $\mathbb{Z}_3[x]$. Pada kenyataannya $x^2 + 2 = (x+1)(x+2)$.

Cara lain yang dapat digunakan adalah dengan mengalikan setiap faktor linier yang ada dalam $\mathbb{Z}_3[x]$, yaitu $(x+1)(x+1) = x^2 + 2x + 1$ dan $(x+2)(x+2) = x^2 + x + 1$. Dengan demikian, diperoleh bahwa $x^2 + 2$, $x^2 + 1$ dan $x^2 + 2x + 2$ tereduksi dalam $\mathbb{Z}_3[x]$.

Sehingga, polinomial-polinomial monik yang tak tereduksi dalam $\mathbb{Z}_3[x]$ hanya ada tiga, yaitu $x^2 + 1$, $x^2 + x + 2$, dan $x^2 + 2x + 2$.

Misal kita mengambil polinomial $x^2 + 2x + 2$ untuk membentuk *extension field* dari $\mathbb{Z}_3$. Misal α adalah akar dari polinomial tersebut, maka diperoleh

$$\mathbb{Z}_3(\alpha) = \{0, 1, 2, \alpha, \alpha + 1, \alpha + 2, 2\alpha, 2\alpha + 1, 2\alpha + 2\}$$

Jumlah anggota $\mathbb{Z}_3(\alpha)$ adalah 9, maka dinotasikan $GF(9)$. Karena *extension field* yang dihasilkan mempunyai jumlah elemen berhingga, maka menurut Teorema 2.13, elemen-elemen tak nol dalam *extension field* tersebut akan membentuk grup siklik terhadap operasi perkalian. Sehingga *extension field* yang dihasilkan akan mempunyai paling sedikit satu generator didalamnya. Berikut diberikan suatu pengertian generator secara umum dalam suatu *field* hingga $GF(q)$.

Definisi 3.2.1

Suatu generator g dalam suatu *field* hingga $GF(q)$ adalah elemen dengan order $q-1$. Ekuivalen dengan mengatakan, g adalah generator jika pangkat-pangkat dari g membentuk semua elemen tak nol dari $GF(q)$.

(Neil Koblitz, 1997)

Polinomial tak tereduksi yang akarnya merupakan generator dari suatu *field* hingga disebut polinomial primitif.

Sekarang, untuk polinomial $p(x) = x^2 + 2x + 2$, akar-akarnya akan memenuhi persamaan $\alpha^2 = -2\alpha - 2 = \alpha + 1$. Sehingga diperoleh

- $\alpha^1 = \alpha$
- $\alpha^2 = \alpha + 1$
- $\alpha^3 = \alpha^2 + \alpha = (\alpha + 1) + \alpha = 2\alpha + 1$
- $\alpha^4 = 2\alpha^2 + \alpha = 2(\alpha + 1) + \alpha = 2$
- $\alpha^5 = 2\alpha$ ..... (1)
- $\alpha^6 = 2\alpha^2 = 2\alpha + 2$
- $\alpha^7 = 2\alpha^2 + 2\alpha = 2(\alpha + 1) + 2\alpha = \alpha + 2$
- $\alpha^8 = \alpha^2 + 2\alpha = (\alpha + 1) + 2\alpha = 1$

Dari perhitungan (1) diatas, terlihat bahwa $\alpha^8 = 1$ atau α memiliki order 8. Maka akar α merupakan generator dari $GF(9)^*$. Sehingga $p(x) = x^2 + 2x + 2$ merupakan polinomial primitif.

Berikut diberikan tabel operasi penjumlahan dan perkalian dalam $GF(9)$ yang merupakan *splitting field* untuk $p(x) = x^2 + 2x + 2$ atas $\mathbb{Z}_3$. Operasi penjumlahan merupakan operasi penjumlahan biasa dalam $\mathbb{Z}_3[x]$.

Tabel 1. Penjumlahan dalam $GF(9)$ dengan $p(x) = x^2 + 2x + 2$

	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
1	1	2	0	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$
2	2	0	1	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$
x	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$	0	1	2
$x+1$	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$	1	2	0
$x+2$	$x-1$	x	$x+1$	$2x+2$	$2x$	$2x+1$	2	0	1
$2x$	$2x$	$2x+1$	$2x+2$	0	1	2	x	$x+1$	$x+2$
$2x+1$	$2x+1$	$2x+2$	$2x$	1	2	0	$x+1$	$x+2$	x
$2x+2$	$2x+2$	$2x$	$2x+1$	2	0	1	$x+2$	x	$x+1$

Sedangkan operasi perkalian dalam $GF(9)$ adalah operasi perkalian modulo $p(x) = x^2 + 2x + 2$, yaitu operasi perkalian dengan menggunakan persamaan (1). Sebagai contoh, misal $(2\alpha+1)(\alpha+2) = 2\alpha^2 + 5\alpha + 2$. Dalam $\mathbb{Z}_3$ $2\alpha^2 + 5\alpha + 2 = 2\alpha^2 + 2\alpha + 2$. Karena $\alpha^2 = \alpha + 1$, maka $2\alpha^2 + 2\alpha + 2 = 2(\alpha+1) + 2\alpha + 2 = 2\alpha + 2 + 2\alpha + 2 = \alpha + 1$. Sehingga diperoleh bahwa $(2\alpha+1)(\alpha+2) = \alpha + 1$. Operasi perkalian lainnya dalam $GF(9)$ yang merupakan *splitting field* untuk $p(x) = x^2 + 2x + 2$ diberikan dalam tabel berikut.

Tabel 2. Perkalian modulo $p(x) = x^2 + 2x + 2$

	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
2	0	2	1	2α	$2\alpha+2$	$2\alpha+1$	α	$\alpha+2$	$\alpha+1$
α	0	α	2α	$\alpha+1$	$2\alpha+1$	1	$2\alpha+2$	2	$\alpha+2$
$x+1$	0	$\alpha+1$	$2\alpha+2$	$2\alpha+1$	2	α	$\alpha+2$	2α	1
$x+2$	0	$\alpha+2$	$2\alpha+1$	1	α	$2\alpha+2$	2	$\alpha+1$	2α
$2x$	0	2α	α	$2\alpha+2$	$\alpha+2$	2	$\alpha+1$	1	$2\alpha+1$
$2x+1$	0	$2\alpha+1$	$\alpha+2$	2	2α	$\alpha+1$	1	$2\alpha+2$	α
$2x+2$	0	$2\alpha+2$	$\alpha+1$	$\alpha+2$	1	2α	$2\alpha+1$	α	2

Sekarang, misal kita mengambil polinomial tak tereduksi lainnya, yaitu polinomial x^2+x+2 untuk membentuk *extension field* dari $\mathbb{Z}_3$. Misal β adalah akar dari polinomial tersebut, maka diperoleh

$$\mathbb{Z}_3(\beta)=\{0,1,2,\beta,\beta+1,\beta+2,2\beta,2\beta+1,2\beta+2\}$$

Jumlah anggota $\mathbb{Z}_3(\beta)$ adalah 9, maka dinotasikan $GF(9)$. Untuk polinomial $p(x)=x^2+x+2$, akar-akarnya akan memenuhi persamaan $\beta^2=-\beta-2=2\beta+1$. Akar β merupakan generator dari $GF(9)^*$, karena memenuhi kondisi berikut.

- $\beta^1=\beta$
- $\beta^2=2\beta+1$
- $\beta^3=2\beta^2+\beta=2(2\beta+1)+\beta=2\beta+2$
- $\beta^4=2\beta^2+2\beta=2(2\beta+1)+2\beta=2$
- $\beta^5=2\beta$ .....(2)
- $\beta^6=2\beta^2=2(2\beta+1)=\beta+2$
- $\beta^7=\beta^2+2\beta=(2\beta+1)+2\beta=\beta+1$
- $\beta^8=\beta^2+\beta=(2\beta+1)+\beta=1$

Karena akar dari $p(x)=x^2+x+2$ adalah generator dari $GF(9)^*$, maka $p(x)=x^2+x+2$ disebut polinomial primitif.

Berikut tabel penjumlahan dan perkalian dalam $GF(9)$ yang merupakan *splitting field* untuk $p(x) = x^2 + x + 2$ atas $\mathbb{Z}_3$.

Tabel 3. Penjumlahan dalam $GF(9)$ dengan $p(x) = x^2 + x + 2$

	0	1	2	β	$\beta+1$	$\beta+2$	2β	$2\beta+1$	$2\beta+2$
0	0	1	2	β	$\beta+1$	$\beta+2$	2β	$2\beta+1$	$2\beta+2$
1	1	2	0	$\beta+1$	$\beta+2$	β	$2\beta+1$	$2\beta+2$	2β
2	2	0	1	$\beta+2$	β	$\beta+1$	$2\beta+2$	2β	$2\beta+1$
β	β	$\beta+1$	$\beta+2$	2β	$2\beta+1$	$2\beta+2$	0	1	2
$\beta+1$	$\beta+1$	$\beta+2$	β	$2\beta+1$	$2\beta+2$	2β	1	2	0
$\beta+2$	$\beta+2$	β	$\beta+1$	$2\beta+2$	2β	$2\beta+1$	2	0	1
2β	2β	$2\beta+1$	$2\beta+2$	0	1	2	β	$\beta+1$	$\beta+2$
$2\beta+1$	$2\beta+1$	$2\beta+2$	2β	1	2	0	$\beta+1$	$\beta+2$	β
$2\beta+2$	$2\beta+2$	2β	$2\beta+1$	2	0	1	$\beta+2$	β	$\beta+1$

Operasi perkalian dalam $GF(9)$ yang merupakan *splitting field* untuk $p(x) = x^2 + x + 2$ atas $\mathbb{Z}_3$ menggunakan perhitungan pada persamaan (2).

Tabel 4. Perkalian modulo $p(x) = x^2 + x + 2$

	0	1	2	β	$\beta+1$	$\beta+2$	2β	$2\beta+1$	$2\beta+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	β	2β	$\beta+1$	$\beta+2$	$2\beta+1$	$2\beta+2$
2	0	2	1	2β	β	$2\beta+2$	$2x+1$	$\beta+2$	$\beta+1$
β	0	β	2β	$2\beta+1$	$\beta+2$	1	$\beta+1$	$2x+2$	2
$\beta+1$	0	2β	β	$\beta+2$	$2\beta+1$	2	$2\beta+2$	$\beta+1$	1
$\beta+2$	0	$\beta+1$	$2\beta+2$	1	2	$\beta+2$	2β	β	$2\beta+1$
2β	0	$\beta+2$	$2\beta+1$	$\beta+1$	$2\beta+2$	2β	2	1	β
$2\beta+1$	0	$2\beta+1$	$\beta+2$	$2\beta+2$	$\beta+1$	β	1	2	2β
$2\beta+2$	0	$2\beta+2$	$\beta+1$	2	1	$2\beta+1$	β	2β	$\beta+2$

Dapat dilihat bahwa operasi penjumlahan dengan polinomial tak tereduksi yang berbeda dalam $\mathbb{Z}_3[x]$ akan menghasilkan tabel dengan bentuk yang sama. Hal ini karena operasi penjumlahan hanya dilakukan pada koefisien dari akar-akar polinomial tak tereduksi, yaitu elemen-elemen dalam $\mathbb{Z}_3$. Perbedaannya hanya terletak pada nilai akar dari masing-masing polinomial tak tereduksi tersebut. Sedangkan operasi perkalian dengan polinomial tak tereduksi yang berbeda dalam $\mathbb{Z}_3[x]$ akan menghasilkan tabel dengan bentuk yang berbeda pula.

Namun polinomial yang diambil untuk membentuk *extension field* dari $\mathbb{Z}_3$ tidak harus suatu polinomial primitif. Misal kita mengambil polinomial x^2+1 untuk membentuk *extension field* dari $\mathbb{Z}_3$. Akar dari polinomial tersebut adalah $\pm i \notin \mathbb{Z}_3$. Misal kita ambil $\alpha = i$, maka diperoleh

$$\mathbb{Z}_3(i) = \{0,1,2,i,i+1,i+2,2i,2i+1,2i+2\}$$

Jumlah anggota $F(i)$ adalah 9, maka dinotasikan $GF(9)$ juga. Untuk polinomial $p(x) = x^2+1$, $\alpha = i$ akan memenuhi persamaan $i^2 = -1$. Berdasarkan operasi perkalian, diperoleh

$$i^1 = i,\ i^2 = -1,\ i^3 = -i,\ i^4 = 1 \quad \text{..... (3)}$$

Dapat dilihat bahwa order dari elemen i adalah 4, sehingga i bukanlah generator dari $GF(9)^*$.

Tabel penjumlahan dalam $GF(9)$ yang merupakan *splitting field* untuk $p(x) = x^2+1$ atas $\mathbb{Z}_3$ akan menghasilkan bentuk yang sama dengan tabel penjumlahan dalam $GF(9)$ yang merupakan *splitting field* untuk x^2+2x+2 maupun untuk x^2+x+2. Perbedaannya hanya pada nilai akarnya saja. Sedangkan tabel perkalian akan berbeda. Berikut diberikan tabel penjumlahan dan perkalian dalam $GF(9)$ yang merupakan *splitting field* untuk $p(x) = x^2+1$ atas $\mathbb{Z}_3$.

Tabel 5. Penjumlahan dalam $GF(9)$ dengan $p(x) = x^2 + 1$

	0	1	2	i	$i+1$	$i+2$	$2i$	$2i+1$	$2i+2$
0	0	1	2	i	$i+1$	$i+2$	$2i$	$2i+1$	$2i+2$
1	1	2	0	$i+1$	$i+2$	i	$2i+1$	$2i+2$	$2i$
2	2	0	1	$i+2$	i	$i+1$	$2i+2$	$2i$	$2i+1$
i	i	$i+1$	$i+2$	$2i$	$2i+1$	$2i+2$	0	1	2
$i+1$	$i+1$	$i+2$	i	$2i+1$	$2i+2$	$2i$	1	2	0
$i+2$	$i+2$	i	$i+1$	$2i+2$	$2i$	$2i+1$	2	0	1
$2i$	$2i$	$2i+1$	$2i+2$	0	1	2	i	$i+1$	$i+2$
$2i+1$	$2i+1$	$2i+2$	$2i$	1	2	0	$i+1$	$i+2$	i
$2i+2$	$2i+2$	$2i$	$2i+1$	2	0	1	$i+2$	i	$i+1$

Tabel 6. Perkalian modulo $p(x) = x^2 + 1$

	0	1	2	i	$i+1$	$i+2$	$2i$	$2i+1$	$2i+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	i	$i+1$	$i+2$	$2i$	$2i+1$	$2i+2$
2	0	2	1	$2i$	$2i+2$	$2i+1$	i	$i+2$	$i+1$
i	0	i	$2i$	2	$i+2$	$2i+2$	1	$i+1$	$2i+1$
$i+1$	0	$i+1$	$2i+2$	$i+2$	$2i$	1	$2i+2$	2	i
$i+2$	0	$i+2$	$2i+1$	$2i+2$	1	i	$i+1$	$2i$	2
$2i$	0	$2i$	i	1	$2i+2$	$i+1$	2	$2i+2$	$i+2$
$2i+1$	0	$2i+1$	$i+2$	$i+1$	2	$2i$	$2i+2$	i	1
$2i+2$	0	$2i+2$	$i+1$	$2i+1$	i	2	$i+2$	1	$2i$

Telah diketahui bahwa i bukanlah generator dari $GF(9)^*$. Namun, karena $GF(9)^*$ merupakan grup siklik, maka pasti terdapat paling sedikit satu elemen dalam $GF(9)^*$ yang merupakan generator dari $GF(9)^*$. Elemen tersebut dapat dicari dengan mengamati Tabel 6, kemudian cari suatu elemen yang ordernya 8. Misal kita amati elemen $2i$, maka didapat $(2i)^2 = 2$. Lalu $(2i)^4 = 2^2 = 1$. Jadi, Order dari $2i$ adalah 4. Misal kita amati elemen $i+1$, maka didapat $(i+1)^2 = 2i$. Lalu $(i+1)^4 = (2i)^2 = 2$. Sehingga $(i+1)^8 = 2^2 = 1$. Jadi, $i+1$ adalah generator dari $GF(9)^*$. Dengan cara yang sama diperoleh bahwa $i+2$, $2i+1$, dan $2i+2$ juga merupakan generator dari $GF(9)^*$.

Selanjutnya akan diberikan contoh pembentukan suatu extension *field* dengan derajat tiga.

2. $p = 2$

Maka *field* pembentuknya adalah $\mathbb{Z}_2$, dengan elemen-elemennya diwakili oleh 0 dan 1. Selanjutnya, untuk mendapatkan *extension field* dari $\mathbb{Z}_2$ dengan derajat atas $\mathbb{Z}_2$ adalah tiga, harus ditemukan suatu polinomial monik $p(x)$ dengan derajat $n = 3$ yang tak tereduksi dalam $\mathbb{Z}_2[x]$. Karena koefisien dari polinomial dalam $\mathbb{Z}_2[x]$ hanya 0 dan 1, maka

kandidat polinomial yang tak tereduksi dalam $\mathbb{Z}_2[x]$ dapat dengan mudah didapatkan, yaitu:

- x^3+1
- x^3+x+1
- x^3+x^2+1
- x^3+x^2+x+1

Dengan mensubstitusi elemen 0 ke dalam polinomial-polinomial tersebut akan memberikan hasil sama dengan 1. Sedangkan jika kita substitusikan 1 ke dalam polinomial-polinomial akan diperoleh bahwa hanya polinomial dengan jumlah suku ganjil yang akan menghasilkan 1. Sehingga, terdapat dua polinomial monik kubik yang tak tereduksi dalam $\mathbb{Z}_2[x]$, yaitu x^3+x+1 dan x^3+x^2+1.

Dengan cara pemeriksaan yang sama seperti contoh sebelumnya, maka akan diperoleh bahwa x^3+x+1 dan x^3+x^2+1 adalah polinomial primitif dalam $\mathbb{Z}_2[x]$. Sekarang, misal kita mengambil polinomial x^3+x+1 untuk membentuk *extension field* dari $\mathbb{Z}_2$. Misal α adalah akar dari polinomial tersebut, maka diperoleh

$$\mathbb{Z}_2(\alpha)=\left\{0,1,\alpha,\alpha+1,\alpha^2,\alpha^2+1,\alpha^2+\alpha,\alpha^2+\alpha+1\right\}$$

Jumlah anggota $\mathbb{Z}_2(\alpha)$ adalah 8, maka dinotasikan $GF(8)$. Untuk polinomial $p(x) = x^3 + x + 1$, akar-akarnya akan memenuhi persamaan $\alpha^3 = -\alpha - 1 = \alpha + 1$. Akar α merupakan generator dari $GF(8)^*$, karena memenuhi kondisi berikut.

- $\alpha^1 = \alpha$
- $\alpha^2 = \alpha^2$
- $\alpha^3 = -\alpha - 1 = \alpha + 1$
- $\alpha^4 = \alpha^2 + \alpha$
- $\alpha^5 = \alpha^3 + \alpha^2 = (\alpha + 1) + \alpha^2 = \alpha^2 + \alpha + 1$
- $\alpha^6 = \alpha^3 + \alpha^2 + \alpha = \alpha^2 + 1$
- $\alpha^7 = \alpha^3 + \alpha = (\alpha + 1) + \alpha = 1$

Misal kita mengambil polinomial $x^3 + x^2 + 1$ untuk membentuk *extension field* dari $\mathbb{Z}_2$. Misal β adalah akar dari polinomial tersebut, maka diperoleh

$$\mathbb{Z}_2(\beta) = \{0, 1, \beta, \beta + 1, \beta^2, \beta^2 + 1, \beta^2 + \beta, \beta^2 + \beta + 1\}$$

Jumlah anggota $\mathbb{Z}_2(\beta)$ juga 8, maka dinotasikan $GF(8)$. Untuk polinomial $p(x) = x^3 + x^2 + 1$, akar-akarnya akan memenuhi persamaan $\beta^3 = -\beta^2 - 1 = \beta^2 + 1$. Akar β juga merupakan generator dari $GF(8)^*$, karena memenuhi kondisi berikut.

- $\beta^1 = \beta$
- $\beta^2 = \beta^2$
- $\beta^3 = \beta^2 + 1$
- $\beta^4 = \beta^3 + \beta = \beta^2 + \beta + 1$
- $\beta^5 = \beta^3 + \beta^2 + \beta = (\beta^2 + 1) + \beta^2 + \beta = \beta + 1$
- $\beta^6 = \beta^2 + \beta$
- $\beta^7 = \beta^3 + \beta^2 = (\beta^2 + 1) + \beta^2 = 1$

Berdasarkan pembahasan pada contoh sebelumnya, operasi penjumlahan dalam $GF(8)$ yang merupakan *splitting field* untuk $p(x) = x^3 + x + 1$ maupun untuk $p(x) = x^3 + x^2 + 1$ adalah operasi penjumlahan biasa dalam $\mathbb{Z}_2[x]$. Sehingga akan menghasilkan tabel dengan bentuk yang sama. Perbedaannya hanya pada nilai akar dari masing-masing polinomial tersebut. Sedangkan operasi perkaliannya berbeda. Operasi perkalian dalam $GF(8)$ yang merupakan *splitting field* untuk $p(x) = x^3 + x + 1$ atas $\mathbb{Z}_2$ adalah operasi perkalian modulo $p(x) = x^3 + x + 1$, sedangkan operasi perkalian dalam $GF(8)$ yang merupakan *splitting field* untuk $p(x) = x^3 + x^2 + 1$ atas $\mathbb{Z}_2$ adalah operasi perkalian modulo $p(x) = x^3 + x^2 + 1$.

Pada halaman selanjutnya diberikan tabel penjumlahan dan perkalian dalam $GF(8)$ yang merupakan *splitting field* untuk $p(x) = x^3 + x + 1$ dan $GF(8)$ yang merupakan *splitting field* untuk $p(x) = x^3 + x^2 + 1$. Dalam tabel penjumlahan digunakan notasi γ untuk mewakili α maupun β.

Tabel 7. Penjumlahan dalam $GF(8)$

	0	1	γ	$\gamma+1$	γ^2	γ^2+1	$\gamma^2+\gamma$	$\gamma^2+\gamma+1$
0	0	1	γ	$\gamma+1$	γ^2	γ^2+1	$\gamma^2+\gamma$	$\gamma^2+\gamma+1$
1	1	0	$\gamma+1$	γ	γ^2+1	γ^2	$\gamma^2+\gamma+1$	$\gamma^2+\gamma$
γ	γ	$\gamma+1$	0	1	$\gamma^2+\gamma$	$\gamma^2+\gamma+1$	γ^2	γ^2+1
$\gamma+1$	$\gamma+1$	γ	1	0	$\gamma^2+\gamma+1$	$\gamma^2+\gamma$	γ^2+1	γ^2
γ^2	γ^2	γ^2+1	$\gamma^2+\gamma$	$\gamma^2+\gamma+1$	0	1	γ	$\gamma+1$
γ^2+1	γ^2+1	γ^2	$\gamma^2+\gamma+1$	$\gamma^2+\gamma$	1	0	$\gamma+1$	γ
$\gamma^2+\gamma$	$\gamma^2+\gamma$	$\gamma^2+\gamma+1$	γ^2	γ^2+1	γ	$\gamma+1$	0	1
$\gamma^2+\gamma+1$	$\gamma^2+\gamma+1$	$\gamma^2+\gamma$	γ^2+1	γ^2	$\gamma+1$	γ	1	0

Tabel 8. Perkalian modulo $x^3 + x + 1$

	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	0	0	0	0	0	0	0
1	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
α	0	α	α^2	$\alpha^2+\alpha$	$\alpha+1$	1	$\alpha^2+\alpha+1$	α^2+1
$\alpha+1$	0	$\alpha+1$	$\alpha^2+\alpha$	α^2+1	$\alpha^2+\alpha+1$	α^2	1	α
α^2	0	α^2	$\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α	α^2+1	1
α^2+1	0	α^2+1	1	α^2	α	$\alpha^2+\alpha+1$	$\alpha+1$	$\alpha^2+\alpha$
$\alpha^2+\alpha$	0	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	1	α^2+1	$\alpha+1$	α	α^2
$\alpha^2+\alpha+1$	0	$\alpha^2+\alpha+1$	α^2+1	α	1	$\alpha^2+\alpha$	α^2	$\alpha+1$

Tabel 9. Perkalian modulo $x^3 + x^2 + 1$

	0	1	β	$\beta+1$	β^2	β^2+1	$\beta^2+\beta$	$\beta^2+\beta+1$
0	0	0	0	0	0	0	0	0
1	0	1	β	$\beta+1$	β^2	β^2+1	$\beta^2+\beta$	$\beta^2+\beta+1$
β	0	β	β^2	$\beta^2+\beta$	β^2+1	$\beta^2+\beta+1$	1	$\beta+1$
$\beta+1$	0	$\beta+1$	$\beta^2+\beta$	β^2+1	1	β	$\beta^2+\beta+1$	β^2
β^2	0	β^2	β^2+1	1	$\beta^2+\beta+1$	$\beta+1$	β	$\beta^2+\beta$
β^2+1	0	β^2+1	$\beta^2+\beta+1$	β	$\beta+1$	$\beta^2+\beta$	β^2	1
$\beta^2+\beta$	0	$\beta^2+\beta$	1	$\beta^2+\beta+1$	β	β^2	$\beta+1$	β^2+1
$\beta^2+\beta+1$	0	$\beta^2+\beta+1$	$\beta+1$	β^2	$\beta^2+\beta$	1	β^2+1	β

BAB IV

PENUTUP

4.1 KESIMPULAN

Suatu *extension field* dibentuk dari suatu *field* F yang telah diketahui. Pembentukan *extension field* dari F dilakukan dengan *adjoining* suatu elemen $\alpha \notin F$ yang merupakan akar dari suatu polinomial monik $p(x)$ tak tereduksi dalam $F[x]$, himpunan polinomial dalam x atas F. $F(\alpha)$ adalah *extension field* dari F dan merupakan *splitting field* untuk $p(x)$ atas F. Misal α' adalah akar lain dari $p(x)$, maka $F(\alpha)$ dan $F(\alpha')$ isomorfik. Pembentukan *extension field* berdasarkan karakteristik *field* pembentuknya dibagi menjadi dua, yaitu pembentukan *extension field* dari suatu *field* dengan karakteristik 0 dan pembentukan *extension field* dari suatu *field* dengan karakteristik *p*, dimana *p* prima.

Pembentukan *extension field* dari suatu *field* dengan karakteristik 0 atau *field* tak hingga, yang diwakili oleh *field* $\mathbb{Q}$ dan $\mathbb{R}$, menghasilkan suatu *field* dengan jumlah elemen tak berhingga. *Extension field* dari $\mathbb{R}$ juga merupakan *extension field* dari $\mathbb{Q}$.

Pembentukan *extension field* dari suatu *field* dengan karakteristik p atau *field* hingga, yang diwakili oleh *field* $\mathbb{Z}_p$, menghasilkan *Galois Field* dengan jumlah elemen $q = p^n$, dimana $n \in \mathbb{N}$, dilambangkan $GF(q)$. Operasi penjumlahan dalam $GF(q)$ adalah operasi penjumlahan biasa dalam $\mathbb{Z}_p$. Sedangkan operasi perkalian dalam $GF(q)$ adalah operasi perkalian modulo $p(x)$, dimana $p(x)$ adalah polinomial monik tak tereduksi dalam $\mathbb{Z}_p$.

Suatu tipe khusus dari polinomial monik tak tereduksi $\mathbb{Z}_p[x]$ adalah polinomial primitif, yaitu polinomial monik tak tereduksi yang akar-akarnya merupakan generator dari $GF(q)^*$.

4.2 SARAN

Dalam tugas akhir ini telah dibahas dan ditunjukkan eksistensi dan suatu cara pembentukan *extension field* dari suatu *field* yang telah diketahui. Berdasarkan teori yang ada dalam tugas akhir ini, diharapkan selanjutnya dapat dibentuk suatu *extension field* yang lebih rumit.

DAFTAR PUSTAKA

Herstein, I.N. 1996. *Abstract Algebra*, 3nd *edition*. Prentice-Hall Inc., New Jersey: 40-223.

Arifin, Achmad. 2001. *Aljabar Linier*, edisi kedua. Penerbit ITB Bandung., Bandung: 1-40.

Bhattacharya, P.B., S.K. Jain & S.R. Nagpaul. 1994. *Basic Abstract Algebra*, *second edition*. Cambridge University Press., Cambridge: 281-311.

Koblitz, neil. 1997. *Algebraic Aspects of Cryptography*, *volume* 3. Springer-Verlag, Berlin: 53-60.

Lidl, R. & G. Pilz. 1994. *Applied Abstract Algebra*, *second edition*. Springer-Verlag, Berlin: 117-131.

Dean, R.A. 1996. *Elements of Abstract Algebra*. John Wiley & Sons, Inc., New York: 112-119.

Chambert-Loir, Antoine. 2005. *A Field Guite to Algebra*. Springer-Verlag, Berlin: 5-7.

Bogomolny, Alexander. 1996. *Modular Arithmetic*. http://www.cut-the-knot.org/blue/Modulo.shtml, 8 Februari 2009, pkl. 16. 19.

Alozano. 2007. Field Homomorphism.

http://www.planetmath.org/FieldHomomorphism.html, 19 Februari 2009, pkl. 20. 26.

http://www-math.cudenver.edu/~wcherowi/courses/finflds.html, 2 Juni 2009, pkl. 22. 43.