Jurnal Sains & Matematika (JSM)
Volume 17 Nomor 3, Juli 2009

ISSN 0854-0675
Kajian Pustaka: 121-126

EKSISTENSI DAN KETUNGGALAN LAPANGAN HINGGA

SURYOTO
Jurusan Matematika Fakultas MIPA Universitas Diponegoro Semarang

ABSTRAK---Lapangan merupakan salah satu bentuk gelanggang yang mempunyai sifat-sifat yang cukup menarik untuk dikaji, khususnya lapangan yang banyaknya unsur berhingga atau yang lebih dikenal dengan lapangan hingga. Yang menarik dari lapangan hingga adalah banyaknya unsur yang terkandung di dalamnya, yang ditentukan sepenuhnya oleh suatu bilangan prima yang merupakan karakteristik lapangan tersebut. Pada makalah ini akan dikaji eksistensi dan ketunggalan lapangan hingga dengan order atau banyaknya unsur yang terkandung di dalamnya merupakan perpangkatan suatu bilangan prima yang merupakan karakteristiknya, melalui dua buah pendekatan, yaitu pendekatan melalui ruang vektor dan pendekatan dengan suku banyak.

Kata kunci : karakteristik, order, suku banyak monik tak-tereduksi, ruang vektor

PENDAHULUAN

Lapangan yang banyaknya unsur berhingga atau yang lebih dikenal dengan lapangan hingga, merupakan salah satu bentuk gelanggang yang mempunyai terapan yang cukup luas di bidang informasi. Menurut Koblitz [3] dan juga McEliece [4] beberapa sub-bidang di dalam teori informasi yang memanfaatkan "jasa" lapangan hingga ini antara lain : kriptografi, pemrosesan citra digital, komunikasi perambatan spektrum dan koreksi kesalahan penyandian. Di samping terapan atau peranan pentingnya di cabang matematika yang lain seperti : teori bilangan, teori grup, geometri proyeksi, dll [5, p.155]. Terlepas dari beberapa penerapannya dalam berbagai bidang di atas, makalah ini hanya membahas kajian teoritis pada lapangan hingganya saja.

Lapangan hingga senantiasa ada, hal ini dapat dilihat dari kenyataan bahwa untuk setiap bilangan prima p, gelanggang bilangan bulat modulo p merupakan lapangan hingga dengan order atau banyaknya unsur yang terkandung di dalamnya sebanyak p [5, Teorema 1.1, pp.2 – 3]. Berawal dari kenyataan ini, muncul pertanyaan mendasar : apakah lapangan hingga dengan order selain bilangan prima juga ada ? Jika ada, ada berapa banyakkah lapangan hingga yang demikian atau tunggalkah keberadaannya ? Bagaimanakah pula mengkonstruksi lapangan hingga yang demikian ?

Untuk menjawab pertanyaan-pertanyaan di atas, terdapat beberapa pendekatan yang dapat digunakan untuk mengkaji eksistensi lapangan hingga dengan order selain bilangan prima tersebut, di antaranya pendekatan melalui ruang vektor dan pendekatan dengan suku banyak. Dengan kedua pendekatan di atas akan diperlihatkan bahwa lapangan hingga dengan order selain bilangan prima juga ada, uniknya order dari lapangan hingga ini merupakan perpangkatan suatu bilangan prima dan lapangan yang demikian senantiasa tunggal. Selanjutnya dengan eksistensi suku banyak tak tereduksi, dapat dikonstruksi lapangan hingga dengan order selain bilangan prima di atas.

PEMBAHASAN

Misalkan F suatu lapangan, dengan mengingat kembali definisi karakteristik suatu gelanggang dan mengingat lapangan adalah gelanggang yang mempunyai unsur satuan, Durbin [1], memberikan definisi alternatif untuk karakteristik suatu lapangan, dimana karakteristik dari lapangan F, didefinisikan sebagai bilangan bulat positif terkecil k sedemikian hingga k1 = 0, dengan 1

menyatakan unsur satuan dari F. Jika bilangan bulat k di atas tidak ada, maka dikatakan F mempunyai karakteristik 0. Dengan definisi karakteristik lapangan di atas, dipunyai teorema berikut ini :

Teorema 1
Karakteristik suatu lapangan adalah 0 atau suatu bilangan prima.

Eksistensi Lapangan Hingga

Misal diberikan bilangan prima p, maka $\mathbf{Z}_p = \{0, 1, \ldots, p-1\}$, yaitu gelanggang bilangan bulat modulo p merupakan lapangan dengan order dan karakteristik p. Kenyataan ini mengungkapkan bahwa lapangan hingga senantiasa ada. Sekarang asumsikan dipunyai lapangan hingga dengan order q. berikut ini akan diberikan sebuah teorema yang menyatakan eksistensi lapangan hingga dengan order selain bilangan prima. Namun sebelumnya akan diberikan beberapa lema berikut ini :

Lema 1
Karakteristik suatu lapangan hingga senantiasa merupakan bilangan prima.

Lema 2
Misalkan F suatu lapangan hingga, maka F memuat sub-lapangan yang isomorfis ke $\mathbf{Z}_p$, dengan p suatu bilangan prima.

Bukti :
Misalakan F lapangan hingga dan 1 menyatakan unsur satuan dari F. Didefinisikan barisan $\{u_0, u_1, u_2, \ldots\}$ di F dengan

$u_0 = 0$, $u_n = u_{n-1} + 1$, untuk $n = 1, 2, \ldots$

Dari pendefinisian barisan di atas, untuk sebarang bilangan bulat positif s dan t berlaku :

$u_{s+t} = u_s + u_t$ (1)

dan $u_{st} = u_s \bullet u_t$ (2)

Karena F lapangan hingga, maka u_n tidak mungkin semuanya berbeda, dengan perkataan lain terdapat pengulangan unsur di dalam $\{u_0, u_1, u_2, \ldots\}$ di atas. Misalkan $u_j = u_{j+k}$ adalah pengulangan pertama, yaitu unsur-unsur $u_0, u_1, \ldots, u_{j+k-1}$ semuanya berbeda, tetapi $u_{j+k} = u_j$. Menurut persamaan (1) di atas, diperoleh $u_{j+k} - u_j = u_k$, sehingga $u_k = 0$. Dimana 0 adalah unsur pertama dari barisan $\{u_n\}$, yang berulang untuk pertama kalinya pada urutan ke-k. Dengan demikian unsur-unsur dari $\{u_0, u_1, \ldots, u_{k-1}\}$ saling berbeda dan k merupakan karakteristik dari lapangan F. Berdasarkan Lema 1, k merupakan suatu bilangan prima. Tulis k = p, dengan p suatu bilangan prima, maka dipunyai himpunan $\{u_0, u_1, \ldots, u_{p-1}\}$ yang merupakan sub-lapangan dari F yang isomorfis dengan lapangan $\mathbf{Z}_p = \{1, 2, \ldots, p-1\}$, melalui pengaitan $u_i \leftrightarrow i$.

Teorema 2
Misalkan F suatu lapangan hingga dengan dengan karakteristik p, dengan p suatu bilangan prima, maka F memuat sebanyak $q = p^n$ unsur, dengan n suatu bilangan bulat positif.

Bukti :
Misalkan F lapangan hingga, maka menurut Lema 2, F memuat sub-lapangan yang isomorf ke lapangan $\mathbf{Z}_p$. Sehingga menurut [5, Teorema 4.1, p.44], F dapat dipandang sebagai ruang vektor atas $\mathbf{Z}_p$. Karena F mempunyai order hingga, maka F sebagai ruang vektor atas $\mathbf{Z}_p$ mempunyai dimensi hingga, katakanlah $[F : \mathbf{Z}_p] = n$. Misalkan $B = \{v_1, v_2, \ldots, v_n\}$ adalah untuk F atas $\mathbf{Z}_p$, maka untuk setiap $x \in F$ dapat dinyatakan secara tunggal sebagai kombinasi linier :

$$x = \alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n,$$

untuk suatu $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbf{Z}_p$.

Karena terdapat p kemungkinan untuk setiap nilai α_i dalam kombinasi linier di atas, maka ada sebanyak p^n kombinasi linier yang menyatakan unsur-unsur yang berlainan dari F. ini memperlihatkan bahwa F memuat tepat p^n unsur berlainan atau $q = p^n$, untuk suatu bilangan prima p dan bilangan bulat positif n.

Teorema 2 di atas mengatakan bahwa jika diberikan suatu lapangan hingga, maka order lapangan hingga tersebut senantiasa

merupakan perpangkatan bulat dari suatu bilangan prima, yang merupakan karakteristiknya. Sebaliknya, jika diberikan sebarang bilangan prima p dan sebarang bilangan bulat positif n, apakah senantiasa ada lapangan hingga dengan order $q = p^n$?

Untuk menjawab pertanyaan ini, akan diberikan terlebih dahulu beberapa lema berikut ini :

Lema 3
Jika lapangan hingga F dengan order q ada, maka untuk semua bilangan bulat positif n, terdapat paling sedikit sebuah suku banyak berderajat n yang tak tereduksi atas F.

Lema 4
Jika F suatu lapangan hingga dan $F^* = F \setminus \{0\}$, maka F^* merupakan grup siklik terhadap operasi perkalian.

Lema 5
Jika F suatu lapangan hingga dengan karakteristik p, maka suku banyak $x^q - x \in \mathbf{Z}_p[x]$ teruraikan atas faktor-faktor linier pada F[x].

Bukti :
Misalkan F lapangan hingga dengan karakteristik p, maka menurut Teorema 2, order dari F adalah p^n, dengan $n = [F : \mathbf{Z}_p]$. Dengan demikian grup multiplikatif F^* dari unsur-unsur tak nol di F mempunyai order $p^n - 1$. Sehingga untuk setiap $a \in F$ berlaku $a^{q-1} = 1$, dengan $q = p^n$ dan $a^q = a$.

Dengan demikian suku banyak $x^q - x \in \mathbf{Z}_p[x]$ mempunyai $q = p^n$ akar berlainan di F. Sehingga suku banyak $x^q - x$ dapat dituliskan

$$x^q - x = (x - a_1)(x - a_2) \ldots (x - a_q),$$

dengan $a_1, a_2, \ldots, a_q \in F$,
yaitu $x^q - x$ teruraikan ke dalam faktor-faktor linier di F[x].

Lema 6
Misalkan F lapangan hingga dengan karakteristik p, maka suku banyak $f(x) = x^q - x$, dengan $q = p^n$, tidak mempunyai akar yang sama di dalam sebarang lapangan perluasan K dari F.

Teorema 3
Untuk sebarang bilangan prima p dan sebarang bilangan bulat positif n terdapat lapangan hingga dengan order p^n.

Bukti :
Pandang suku banyak $x^q - x \in \mathbf{Z}_p[x]$, dengan $q = p^n$, maka terdapat lapangan perluasan F dari $\mathbf{Z}_p$ sedemikian hingga pada F[x], suku banyak $x^q - x$ teruraikan atas faktor-faktor linier

$$x^q - x = (x - a_1)(x - a_2) \ldots (x - a_q)$$

dengan $a_1, a_2, \ldots, a_q \in F$.
Menurut Lema 6, $x^q - x$ tidak mempunyai akar-akar yang sama di F dan karena suku banyak $x^m - x$ berderajat m, maka $a_1, a_2, \ldots, a_q$ adalah q buah akar berlainan dari $x^q - x$.
Bentuk himpunan $A = \{a \in F \mid a^q = a\}$. Akan diperlihatkan bahwa A suatu lapangan. Tampak bahwa $A \neq \varnothing$ dan A memuat q buah unsur yang berlainan.
Selanjutnya misalkan $a, b \in A$, maka $a^q = a$ dan $b^q = b$, sehingga $(ab)^q = a^q b^q = ab$ atau $ab \in A$. Perhatikan bahwa

$$(a+b)^q = a^q + qa^{q-1}b + \binom{q}{2} a^{q-2}b^2 + \ldots + qab^{q-1} + b^q,$$

dimana koefisien binomial $\binom{q}{r}$ senantiasa habis dibagi oleh q, untuk $1 \leq r \leq q - 1$. Sehingga $(a + b)^q = a^q + b^q = a + b$ atau $a + b \in A$.

Dengan demikian karena A suatu himpunan bagian hingga dari suatu lapangan dan tertutup terhadap operasi penjumlahan dan perkalian, maka A merupakan sub-lapangan dari F.

Akhirnya karena A mempunyai $q = p^n$ buah unsur, maka terbukti bahwa A suatu lapangan hingga dengan order p^n.

Ketunggalan Lapangan Hingga

Dari pembahasan sebelumnya diketahui bahwa untuk sebarang bilangan prima p dan sebarang bilangan bulat positif n, lapangan hingga dengan order p^n senantiasa bisa ditemukan. Permasalahan yang muncul di sini : berapa banyakkah lapangan hingga dengan order atau banyaknya unsur merupakan perpangkatan bulat suatu bilangan prima di atas ? Di sini akan diperlihatkan bahwa dua buah lapangan hingga sebarang dengan banyaknya unsur yang terkandung di dalamnya sama senantiasa isomorfis.

Namun sebelumnya akan diberikan terlebih dahulu lema berikut ini.

Lema 7

Jika f(x) adalah suku banyak berderajat n yang tak tereduksi atas Z_p, maka f(x) membagi $x^q - x$, dengan $q = p^n$.

Teorema 4

Jika E dan F adalah lapangan-lapangan hingga dengan order yang sama, maka E dan F saling isomorfis.

Bukti :

Misalkan E dan F adalah lapangan-lapangan hingga dengan order p^n, untuk suatu bilangan prima p dan bilangan bulat positif n. Maka menurut Lema 4, F* merupakan grup siklik, katakanlah dibangun oleh sebuah unsur $b \in F$. Dengan demikian $\mathbf{Z}_p(b)$ adalah lapangan yang diperoleh dengan menggabungkan b pada $\mathbf{Z}_p$, yang tidak lain adalah F sendiri. Karena $[F : \mathbf{Z}_p] = n$, maka b adalah aljabar atas $\mathbf{Z}_p$ dengan derajat n, dimana $n = \delta(g(x))$ dan g(x) adalah suku banyak minimal untuk b di $\mathbf{Z}[x]$ serta g(x) tak tereduksi atas $\mathbf{Z}$.

Pandang pemetaan

$$\psi : \mathbf{Z}_p[x] \rightarrow F = \mathbf{Z}_p(b),$$

yang didefinisikan oleh $\psi(f(x)) = f(b)$, untuk setiap $f(x) \in \mathbf{Z}_p[x]$, maka ψ adalah homomorfisma dari $\mathbf{Z}_p[x]$ ke F yang bersifat pada dengan $\text{Ker}(\psi) = (g(x))$, yaitu ideal dari $\mathbf{Z}_p[x]$ yang dibangun oleh g(x). Dengan demikian $F \cong \mathbf{Z}_p[x] / (g(x))$.

Selanjutnya karena g(x) suku banyak berderajat n yang tak tereduksi di $\mathbf{Z}_p[x]$, maka menurut Lema 4, g(x) harus membagi suku banyak $x^q - x$, dengan $q = p^n$. Di sisi lain, karena suku banyak $x^q - x$ teruraikan atas faktor-faktor linier di E[x], yaitu :

$$x^q - x = (x - a_1)(x - a_2) \ldots (x - a_q),$$

dengan $a_1, a_2, \ldots, a_q \in E$.

Dengan demikian q(x) harus membagi

$$(x - a_1)(x - a_2) \ldots (x - a_q).$$

Menurut Herstein [2, Akibat 4.5.10, p.160], g(x) tidak mungkin relatif prima dengan semua $x - a_i$ di E[x]. Dengan perkataan lain, terdapat suatu $j \in \{1, 2, \ldots, m\}$ sedemikian hingga g(x) dan $x - a_j$ mempunyai suku banyak persekutuan dengan derajat paling sedikit satu. Atau lebih tepatnya, $x - a_j$ membagi g(x) di E[x], yaitu $g(x) = (x - a_j) h(x)$, untuk suatu $h(x) \in E[x]$. Dengan demikian $g(a_j) = 0$.

Kemudian karena g(x) tak tereduksi di $\mathbf{Z}_p[x]$ dan a_j adalah akar dari g(x), maka g(x) adalah suku banyak minimal untuk a_j di $\mathbf{Z}_p[x]$. Sehingga $\mathbf{Z}_p(a_j) \cong \mathbf{Z}_p[x] / (g(x)) \cong F$ dan diperoleh $[\mathbf{Z}_p(a_j) : \mathbf{Z}_p] = n$. Juga karena $\mathbf{Z}_p(a_j) \subseteq E$ dan $[E : \mathbf{Z}_p] = n$, maka $\mathbf{Z}_p(a_j) = E$. Akibatnya $E = \mathbf{Z}_p(a_j) \cong F$, yaitu E dan F adalah lapangan-lapangan yang isomorfis.

Pengkonstruksian Lapangan Hingga

Ide dasar untuk mengkonstruksi lapangan hingga dengan order p^n, dimana p suatu bilangan prima dan n suatu bilangan bulat positif, diberikan oleh Durbin [1, Teorema 40.1, p.180]. Di mana lapangan ini dikonstruksi dengan memanfaatkan eksistensi suku banyak monik tak tereduksi dengan derajat n. Meskipun tidak ada aturan yang baku dalam pemilihan suku banyak tak tereduksi ini untuk mengkonstruksi lapangan hingganya, suku banyak yang terpilih ataupun tidak senantiasa menghasilkan lapangan yang isomorf.

Secara garis besar, pengkonstruksian lapangan hingga di atas dapat dilakukan sebagai berikut :

1. Pilih suku banyak f(x) dengan derajat n yang tak tereduksi di $\mathbf{Z}_p[x]$.
2. Diperoleh ideal (f(x)) dari $\mathbf{Z}_p[x]$ dan $\mathbf{Z}_p[x]$ / (f(x)) adalah lapangan hingga yang diinginkan, dengan order p^n.

Contoh :
Suku banyak $1 + x + x^3 \in \mathbf{Z}_2[x]$ tak tereduksi atas $\mathbf{Z}_2$. Oleh karena itu $\mathbf{Z}_2[x] / (1 + x + x^3)$ adalah lapangan hingga dengan order $2^3 = 8$. Tabel Cayley untuk operasi-operasi lapangan diberikan oleh :

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

Tabel 1. Operasi Penjumlahan

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

Tabel 2. Operasi Perkalian

Hasil perhitungan pada kedua tabel di atas mengacu pada aturan operasi di $\mathbf{Z}_2$. Sebagai contoh $(1 + \alpha^2) + (1 + \alpha + \alpha^2) = 2 + \alpha + 2\alpha^2 = 0 + \alpha + 0 = \alpha$, yaitu di dalam operasi penjumlahan, koefisien-koefisien hasil penjumlahan direduksi dengan aturan yang berlaku pada $\mathbf{Z}_2$. Sedangkan untuk operasi perkalian, penyederhanaan hasil perhitungan mengacu aturan : Jika $f(\alpha) = (1 + \alpha + \alpha^3) q(\alpha) + r(\alpha)$, maka $f(\alpha) = r(\alpha)$. Sehingga

$$(1 + \alpha^2)(1 + \alpha + \alpha^2)$$
$$= 1 + \alpha + 2\alpha^2 + \alpha^3 + \alpha^4$$
$$= 1 + \alpha + \alpha^3 + \alpha^4 \text{ di } \mathbf{Z}_2[x].$$

Di sisi lain $1 + \alpha + \alpha^3 + \alpha^4 = (1 + \alpha + \alpha^3)(1 + \alpha) + (\alpha + \alpha^2)$ di $\mathbf{Z}_2[x]$, dengan demikian $1 + \alpha + \alpha^3 + \alpha^4 = \alpha + \alpha^2$ dan $(1 + \alpha^2)(1 + \alpha + \alpha^2) = \alpha + \alpha^2$ pada tabel.

SIMPULAN

Dari hasil pembahasan di atas dapat disimpulkan bahwa untuk sebarang bilangan prima p dan sebarang bilangan bulat positif n, lapangan hingga dengan order p^n senantiasa ada dan semua lapangan dengan order ini saling isomorf.

DAFTAR PUSTAKA

1. J. R. Durbin, **Modern Algebra**, John Wiley & Sons, Inc., New York, 2000.
2. I. N. Herstein, **Abstract Algebra**, Prentice-Hall, Upper Saddle River, New Jersey, 1996.
3. N. Koblitz, **Algebraic Aspects of Cryptography**, Springer-Verlag, Berlin Heidelberg, 1999.
4. R. J. McEliece, **Finite Field for Computer Scientists and Engineers**, Kluwer Academic Publishers, Massachusetts, 1989.
5. I. Stewart, **Galois Theory**, Chapman & Hall, London, 1994.