JURNAL MATEMATIKA DAN KOMPUTER
Vol. 4. No. 1, 41 - 45, April 2001, ISSN : 1410-8518

KETERHUBUNGAN GALOIS FIELD DAN LAPANGAN PEMISAH

Bambang Irawanto
Jurusan Matematika FMIPA UNDIP

Abstact

In this paper, it was learned of the necessary and sufficient condition for finite field with p^n elements, p prime and $n \geq 1$ an integer. A field F is an extention field of a field K if K subfield F. The extension field F of field K is Splitting field of collection polinomial $\{ f_i(x) \mid i \in I \}$ of K if F smallest subfield $\overline{K}$ containing K and all the zeros in $\overline{K}$ of the polinomial $f_i(x)$. The zeros of polinomial $f_i(x)$ are elements of field F and the elements of F is finite then F is finite field (Galois fileld). F is finite with p^n elements, p prime and $n \geq 1$ an integer if only if F is Splitting field of $x^{p^n} - x$ over Zp.

Keywords : extention fields, splitting fields, finite fields.

1. PENDAHULUAN

Lapangan adalah daerah integral yang setiap elemen yang tidak nol mempunyai invers terhadap pergandaan. Lapangan disebut lapangan berhingga jika lapangan memiliki jumlah elemen yang berhingga. Lapangan berhingga sering juga disebut dengan Galois Field (Raisinghania, M.D, 1980).

Salah satu motivasi yang melatarbelakangi pengertian dari Galois Field yaitu lapangan perluasan F atas lapangan K dan K adalah sub field dari F (Hungerford, T. W, 1984).

Misalkan lapangan K, polinomial $f(x) \in K[x]$ dan $a \in K$ adalah akar dari f (x) jka dan hanya jika $(x - a)$ faktor dari f (x) (Hungerford, 1984). Dalam tulisan ini dipelajari hubungan Galois Field dengan lapangan pemisah.

2. LAPANGAN PEMISAH

Lapangan F disebut lapangan perluasan atas lapangan K jika K subfield dari F (Hungerford,T. W, 1984). Misal lapangan F dengan karakteristik p (prima) maka F memuat sub field yang isomorfis dengan Zp, jika karakteristik F sama dengan 0 maka F memuat sub field yang isimorfis dengan Q (himpunan bilangan rasional). Jika polinomial tak nol f (x) $\in$ K [x] dan $\alpha \in$ F sedemikian hingga f (α) = 0 maka α disebut elemen aljabar sebaliknya disebut transendental (Fraleigh, J. B, 1994).

Definisi 1. F lapangan perluasan atas lapangan K. Misal himpunan $\overline{K}_F$ = {$\alpha \in$ F / α aljabar atas K} disebut penutup aljabar (aljabaraic closure).

Definisi 2. Misal K suatu lapangan dengan penutup aljabar (algebraic closure) $\overline{K}$. { f_i (x) / i $\in$ I } koleksi dari polinomial-polinomial dalam K[x]. Suatu lapangan F $\leq \overline{K}$ disebut lapangan pemisah (splitting field) dari { f_i (x) / i $\in$ I }atas K jika F adalah sub field terkecil dari $\overline{K}$ yang memuat K dan semua akar dalam $\overline{K}$ dari setiap fi(x), untuk i $\in$ I. Suatu lapangan F $\leq \overline{K}$ adalah lapangan pemisah (splitting field) atas K, jika F $\leq \overline{K}$ adalah lapangan pemisah (splitting field) dari himpunan sebarang dari polinomial-polinomial dalam K[x]. Semua lapangan K dan semua f(x) $\in$ K[x] sedemikian hingga deg (f) $\geq$ 1, terdapatlah perluasan F dari K yang merupakan lapangan pemisah untuk (f)x atas K (Dean R.A, 1996).

3. GALOIS FIELD

Lapangan dengan jumlah elemen berhingga disebut Galois Field. menulis bahwa setiap elemen dari lapangan berhingga K dengan p prima memenuhi persyaratan $x^{p^n} = x$. (Raisinghania, MD, 1980).

Teorema 1. Misal F suatu lapangan dengan p^n elemen dengan p prima yang termuat dalam penutup aljabar $\overline{Z}$ p dari Zp maka elemen-elemen F adalah akar-akar di $\overline{Z}$ p dari polinomial $x^{p^n} - x \in$ Zp[x] atau F = { a $\in \overline{Z}$ p / akar dari $x^{p^n} - x \in$ Zp[x] }

Bukti :

Pandangan himpunan F* yang merupakan himpunan elemen-elemen yang tidak nol dalam F. Jelas merupakan F* grup multiplikatif, dengan order $p^n - 1$. Untuk $\alpha \in$ F*, order dari α dalam grup multiplikatif membagi order $p^n - 1$ dari grup. Jadi untuk $\alpha \in$ F* diperoleh $\alpha^{p^n-1} = 1$, $\alpha^{p^n} = \alpha$. Sehingga untuk setiap $\alpha \in$ F adalah akar dari $(x^{p^n} - x) \in Zp\,[x]$ paling banyak p^n maka F memuat tepat akar-akar dari $x^{p^n} - x$, atau F = { a $\in \overline{Z}$ p / a akar-akar dari $(x^{p^n} - x)$ elemen $\overline{Z}$ p [x] }. Selanjutnya ditunjukkan bahwa Zp termuat di dalam F, berarti untuk setiap a $\in$ Zp merupakan akar dari $(x^{p^n} - x)$ atau untuk setiap a $\in$ Zp memenuhi $a^{p^n} = a$. Bukti dengan induksi Matematika.

(i) Benar untuk n – 1, sebab $a^{p-1} = 1$, jadi $a^p = a$.

(ii) Jika benar untuk n = k maka benar untuk n = k + 1. Menurut hipotesis induksi benar untuk n = k, maka $a^{pk} = a$, selanjutnya $a^{p(k+1)} = a^{pk.p} = (a^{pk})^p = a^p = a$. Jadi $a^{p(k+1)} = a$ sehingga benar untuk n = k + 1 jadi benar untuk setiap n, yang berarti terbukti bahwa untuk setiap a $\in$ Zp memenuhi

$a^{p^n} = a$.

Berarti F adalah subfield dari $\overline{Z}$ p terkecil yang memuat Zp dan semua akar-akar dari $(x^{p^n} - x) \in \overline{Z}$ p [x]. Jadi F lapangan pemisah dari $x^{p^n} - x$ atas Zp. Misal K suatu lapangan dengan penutup aljabar (algebraic closure) $\overline{K}$. $\{f_i(x) / i \in I\}$koleksi dari polinomial-polinomial dalam K[x]. Suatu lapangan F $\leq \overline{K}$ disebut lapangan pemisah (splitting field) dari $\{ f_i(x) / i \in I \}$ atas K jika F adalah sub field terkecil dari $\overline{K}$ yang memuat K dan semua akar dalam $\overline{K}$ dari setiap $f_i(x)$, untuk i $\in$ I. Suatu lapangan F $\leq \overline{K}$ adalah lapangan pemisah (splitting field) atas K, jika F $\leq \overline{K}$ adalah lapangan pemisah (splitting field) dari himpunan sebarang dari polinomial-polinomial dalam K [x].

Semua lapangan K dan semua f(x) $\in$ K [x] sedemikian sehingga deg (f) $\geq$ 1, terdapatlah perluasan F dari K yang merupakan lapangan pemisah untuk f(x)

atas K (Dean R. A, 1996). Sedangkan jika F suatu lapangan dengan karakteristik prima $p \neq 0$ maka polinomial $f(x) = x^{p^n} - x \in F[x]$ untuk $n \geq 1$ memiliki p^n akar-akar yang berbeda. (Raisinghania,MD, 1980).

Teorema 2. Misal p prima dan $n \geq 1$ adalah bilangan bulat, akar-akar polinomial $x^{p^n} - x \in Zp[x]$ dalam lapangan pemisah atas Zp yang semua berbeda membentuk lapangan F dengan p^n elemen.

Bukti :

Misal polinomial $f(x) = x^{p^n} - x$, maka $f^1(x) = p^n\, x^{p^n-1} - 1$, karena p prima dan f(x) polinomial dalam lapangan pemisah Zp jadi $f^1(x) = 0$. $x^{p^n-1} - 1 = -1 \neq 0$ sehingga f(x) memiliki akar-akar yang berbeda polinomial f(x) $x^{p^n-1} - x$ berderajat p^n dan memiliki akar-akar yang semua berbeda sehingga jumlah akar-akarnya p^n akar. Misal F himpunan semua akar-akar dari f(x) atau $F = \{ a \in \overline{Z}\, p \mid a$ akar dari $f(x) = x^{p^n} - x \}$ akan ditunjukkan bahwa F adalah lapangan.

Ambil $a, b \in F$ maka $a^{p^n} - a = 0$ jadi $a^{p^n} = a$ begitu juga $b^{p^n} - b = 0$ maka $b^{p^n} = b$, sehingga $(a+b)^{p^n} - (a + b) = 0$ diperoleh $(a+b)^{p^n} = (a + b)$ selanjutnya untuk $(a \cdot b^{-1})^{p^n} = a^{p^n} (b^{p^n})^{-1} = a\, b^{-1}$

Jadi F adalah lapangan, karena jumlah akarnya p^n maka F adalah lapangan dengan p^n elemen atau GF (p^n).

4. KESIMPULAN

F adalah lapangan dengan p^n elemen dimana p prima dan $n \geq 1$ bilangan bulat bila dan hanya bila F merupakan lapangan pemisah dari $x^{p^n} - x$ atas Zp.

5. UCAPAN TERIMA KASIH

Pada kesempatan ini kami menyampaikan ucapan terima kasih yang sebesar-besarnya kepada Prof. Drs. Setiadji, MS atas bimbingannya.

DAFTAR PUSTAKA

1. Dean R. A, *Element of Abstract Algebra*, John Wiley & Sons, USA, 1966.

2. Fraleigh, J. B , *A First Course in Abstract Algebra*, Addison – Wesley Publishing Company, USA, 1994.

3. Hungerford, T. W, *Graduete Text in Mathematics Algebra*, Springer Verlag, New York, 1984.

4. Raisinghania M. D, Aggarwal R. S, *Modern Algebra*, S Chand & Company Ltd, New Delhi, 1980.