SPLITTING FIELD DAN KETUNGGALANNYA ATAS POLINOMIAL *FIELD*

Corina Karim[1] dan Ari Andari[2]

[1,2]Jurusan Matematikam Universitas Brawijaya, Malang

ABSTRAK

Suatu field E disebut *extension field F*, jika $F \subset E$ di mana F merupakan field. Dengan kata lain E disebut *extension field F*, jika F subfield dari field E. Sedangkan *Splitting field* merupakan *generalisasi* dari *extension field* yang memenuhi beberapa aksioma. Field yang digunakan pada *splitting field* adalah *field finite extension*, dimana *field finite extension* adalah *extension field* yang mempunyai basis berhingga *n.*

Kata kunci: *extension field, finite extension* dan *splitting field.*

PENDAHULUAN

R ring, suatu barisan tak hingga $(a_0, a_1, a_2, \dots) \in R$ dikatakan suatu polinomial atas ring R jika terdapat suatu bilangan bulat tak negatif n sedemikian sehingga terdapat $a_i = 0 \in R, \forall i > n$. Polinomial tersebut dinotasikan sebagai berikut:

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots$$
$$= \sum_{i=1}^{\infty} a_i x^i$$

dimana *x* disebut indeterminate atas ring R.

Jika F field dan $F[x]$ ring polinomial x atas F maka $F[x]$ daerah integral dengan elemen kesatuan dan memuat subring sejati F. Polinomial $f(x) \in F[x]$ disebut *irreducible* jika *degree* $f(x) \geq 1$, dan jika $f(x) = g(x).h(x)$ dimana $g(x), h(x) \in F[x]$, maka $g(x) \in F$ atau $h(x) \in F$. Jika polinomial $f(x)$ tidak *irreducible* maka disebut *reducible* (Bhattacharya, dkk, 1986).

Selanjutnya Fraleigh (1994) menyebutkan bahwa suatu field E disebut *extension field F*, jika $F \subset E$ di mana F merupakan field. Dengan kata lain E disebut *extension field F*, jika F subfield dari field E. Dan jika E *extension field F* yang mempunyai basis berhingga n di mana E adalah ruang vektor atas F, maka E adalah suatu *finite extension* berderajat n. Selanjutnya dinotasikan $[E : F] = n$, artinya E *extension field F* berdimensi n.

Di lain pihak, menurut Gallian (1990), E *extension field* F dan $\alpha \in E$, α disebut *algebraic* atas F, jika α akar dari suatu polinomial F[*x*]. $(f(x) \in F[x], f(\alpha) = 0)$. Jika α bukan *algebraic* atas F, maka α disebut *transendental* atas F. Dan menurut Fraleigh (1994) suatu E *extension field* dari field F disebut *algebraic extension* dari F jika setiap elemen di E *algebraic* atas F. Jika E bukan *algebraic extension* maka E disebut *transcendental extension.*

Termotivasi dari pengertian *extension field* dan *finite extension*, maka dalam makalah ini akan dibahas tentang *splitting field* atas polinomial di F(x) dan membuktikan ketunggalan dari *splitting field* tersebut.

PEMBAHASAN

Definisi 1 (Bhattacharya, dkk, 1986).
Jika $f(x)$ polinomial di $F[x]$ dengan *degree* ≥ 1 maka K *extension field* F disebut *Splitting field* $f(x)$ atas F jika:

i) Faktor $f(x)$ dapat ditulis menjadi faktor linier $K[x] \ni$
$f(x) = c(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$, $\alpha_i \in K$, dengan c sebarang skalar.
ii) $K = F(\alpha_1, \alpha_2, \dots, \alpha_n) \ni K$ dibangun oleh F dengan akar-akar $\alpha_1, \alpha_2, \dots, \alpha_n \in f(x)$ dan $f(x) \in K$.

Contoh 1:
Field $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$ adalah *splitting field* dari $x^2 - 2 \in \mathbb{Q}[x]$ atas $\mathbb{Q}$.

Bukti:
Jelas $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$.
Akan dibuktikan:
(i). $\mathbb{Q}(\sqrt{2})$ *extension field* $\mathbb{Q}$.
(ii). $\mathbb{Q}(\sqrt{2})$ *splitting field* $\mathbb{Q}$ [x] atas$\mathbb{Q}$.
Bukti (i).
$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$.
Klaim $S = \{1, \sqrt{2}\}$
Akan ditunjukkan:
S adalah basis untuk ruang vektor $\mathbb{Q}$ $(\sqrt{2})$

a) Ambil sebarang $y \in \mathbb{Q}$ $(\sqrt{2})$.
Maka y dapat dinyatakan sebagai
$$y = a + b\sqrt{2}, \ \ a, b \in \mathbb{Q}$$
$$= a.1 + b.\sqrt{2},$$

Jadi S merentang $\mathbb{Q}\ (\sqrt{2})$. ▲

b) Untuk suatu $a, b \in \mathbb{Q}$, maka

$$0 = a + b\sqrt{2}$$
$$\Rightarrow 0 = a.1 + b.\sqrt{2}$$

Akan terpenuhi jika $a = 0$ dan $b = 0$

Jadi S bebas Linier. ▲

Dari a) dan b) terbukti S basis untuk $\mathbb{Q}\ (\sqrt{2})$ dan $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}\ ] = 2$. Jadi $\mathbb{Q}(\sqrt{2})$ *finite extension* $\mathbb{Q}$. Karena $\mathbb{Q}(\sqrt{2})$ *finite extension* $\mathbb{Q}$, maka $\mathbb{Q}(\sqrt{2})$ *extension field* $\mathbb{Q}$. ▲

Bukti (ii).

Akan ditunjukkan:

a) $g(x) = c(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$,
$\alpha_i \in \mathbb{Q}(\sqrt{2})$

Pilih $g(x) = x^2 - 2 \in \mathbb{Q}[x]$

$$\begin{aligned} g(x) &= x^2 - 2 \\ &= \left(x - \sqrt{2}\right)\left(x + \sqrt{2}\right) \\ &= \left(x - \sqrt{2}\right)\left(x - \left(-\sqrt{2}\right)\right) \end{aligned}$$

di mana $\pm\sqrt{2} \in \mathbb{Q}\left(\sqrt{2}\right)$ ▲

b) $\mathbb{Q}\left(\sqrt{2}\right) = \mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_n) \ni \mathbb{Q}\left(\sqrt{2}\right)$ dibangun oleh $\mathbb{Q}$ dengan akar-akar $\alpha_1, \alpha_2, \dots, \alpha_n \in g(x)$ atas $\mathbb{Q}$.

Karena $\mathbb{Q}\left(\sqrt{2}\right)$ *finite extension* atas $\mathbb{Q}$ maka $\mathbb{Q}\left(\sqrt{2}\right)$ *algebraic extension* atas $\mathbb{Q}$. Sehingga $\exists$ $g(x) \in \mathbb{Q}[x], g(x) \neq 0$ di mana $g(\alpha) = 0$.

Ambil sebarang $\alpha \in \mathbb{Q}\left(\sqrt{2}\right)$ maka

$$\begin{aligned} \alpha &= a + \sqrt{2}b \\ \alpha^2 &= \left(a + \sqrt{2}b\right)^2 \\ &= a^2 + 2\sqrt{2}ab + 2b^2 \end{aligned}$$
$$\alpha^2 - a^2 + 2\sqrt{2}ab + 2b^2 = 0$$

Sehingga $\exists$ $g(x) \in \mathbb{Q}[x]$ di mana

$$g(x) = x^2 - a^2 + 2\sqrt{2}ab + 2b^2$$

Jadi $\mathbb{Q}\left(\sqrt{2}\right)$ dibangun oleh $\mathbb{Q}$ dengan $\alpha \in \mathbb{Q}[x]$ ▲

Jadi $\mathbb{Q}\left(\sqrt{2}\right)$ *splitting field* $g(x)$atas $\mathbb{Q}$. ▲

Contoh 2

Splitting field $x^2 + 1 \in \mathbb{C}[x]$ atas $\mathbb{C}$ adalah field $\mathbb{C}$.

Teorema 2 (Bhattacharya, dkk,1986)

Jika K *splitting field* $f(x) \in F[x]$ atas F maka K *finite extension F* dan K *algebraic extension* atas *F*.

Bukti :

Karena menurut definisi 1. bagian ii) K = $F(\alpha_1, \alpha_2, \dots, \alpha_n) \ni$ K dibangun oleh F dengan $\alpha_1, \alpha_2, \dots, \alpha_n \in K$. Maka K *algebraic* atas F.

Sehingga K *finite extension F*.

Karena K *finite extension* maka K juga *algebraic extension* F. ▲

Teorema 3 (Dummit and Foote, 1991)

Misal $\varphi : F \xrightarrow{\sim} F'$ Isomorfisma Field. $f(x) \in F[x]$ polinomial dan $f'(x) \in F'[x]$ polinomial yang didapat dari φ terhadap koefisien $f(x)$. Jika *E splitting field* $f(x)$atas *F* dan *E' splitting field* $f'(x)$ atas *F'*. Maka Isomorfisma φ "*extended to*" isomorfisma $\sigma : E \xrightarrow{\sim} E'$. σ yang dibatasi (*restricted to*) *F* adalah Isomorfisma φ :

$$\begin{array}{ccc} \sigma : E & \xrightarrow{\sim} & E' \\ \downarrow & & \downarrow \\ \varphi : F & \xrightarrow{\sim} & F' \end{array}$$

Bukti:

$\varphi : F \xrightarrow{\sim} F'$ isomorfisma Field.

$$f(x) \mapsto f'(x)$$
$$\alpha_0 + \alpha_1 x \mapsto \alpha_0' + \alpha_1' x$$

E splitting field $f(x)$ atas *F*

E'*splitting field* $f'(x)$atas F'

Akan dibuktikan:

a) $$\begin{array}{ccc} \sigma : E & \xrightarrow{\sim} & E' \\ \downarrow & & \downarrow \\ \varphi : F & \xrightarrow{\sim} & F' \end{array}$$

b) σ Isomorfisma

Bukti:

a) Dengan menggunakan induksi matematika terhadap derajat *n* pada *E field extension F*.

i) Untuk *n* = 1.
Jika *n* = 1 maka *E* = *F*
Padahal

$$\begin{array}{ccc} \sigma : E & \xrightarrow{\sim} & E' \\ \downarrow & & \downarrow \\ \varphi : F & \xrightarrow{\sim} & F' \end{array}$$

maka σ = φ. ▲

ii) Andai untuk *n* = 2 benar maka akan dibuktikan *n* > 2 benar untuk sebarang *field extension*.
Bukti:

Definisikan : $\phi : F(x) \longrightarrow F(\alpha)$

$$p \mapsto p(\alpha)$$

Ambil sebarang $\alpha \in E$ *splitting field* $f(x), f(x) \notin F$.

Misal $m(x)$ polinomial terkecil yang memuat α. maka $m(x) | f(x)$, karena $\alpha \in f(x)$.

Ambil sebarang $m'^{(x)} \in F'[x] \ni m(x) = m'(x)$.

Karena $f'(x)$ *splitting field* atas F' maka ada elemen $\beta \in F'$ dan $\beta \in m'(x)$.

Jadi ada homomorfisma ring π *extending* $\varphi \ni$

$$\begin{tikzcd} \pi : F(\alpha) \arrow[r, "\sim"] \arrow[d] & F'(\beta) \arrow[d] \\ \varphi : F \arrow[r, "\sim"] & F' \end{tikzcd} \qquad (1)$$

karena $[F(\alpha): F] > 1$ maka:

$[F(\alpha): F] \geq 2$

$[E: F(\alpha)][F(\alpha): F] \geq [E: F(\alpha)].2$

$[E: F] \geq [E: F(\alpha)].2$ (karena $[E: F] = 2$ benar)

maka $[E: F(\alpha)] \leq 1$

Jadi $[E: F(\alpha)] < 1$ dan $[E: F(\alpha)] = 1$.

Jika $[E: F(\alpha)] < 1$ maka ada σ *extending* $\pi \ni$

$$\begin{tikzcd} \sigma : E \arrow[r, "\sim"] \arrow[d] & E' \arrow[d] \\ \pi : F(\alpha) \arrow[r, "\sim"] & F'(\beta) \end{tikzcd} \qquad (2)$$

karena σ *extends* π dan π *extends* φ maka σ *extends* φ.

Dari (1) dan (2) diperoleh:

$$\begin{tikzcd} \sigma : E \arrow[r, "\sim"] \arrow[d] & E' \arrow[d] \\ \pi : F(\alpha) \arrow[r, "\sim"] \arrow[d] & F'(\beta) \arrow[d] \\ \varphi : F \arrow[r, "\sim"] & F' \end{tikzcd}$$

Jadi

$$\begin{tikzcd} \sigma : E \arrow[r, "\sim"] \arrow[d] & E' \arrow[d] \\ \varphi : F \arrow[r, "\sim"] & F' \end{tikzcd}$$ ▲

Jika $[E: F(\alpha)] = 1$ maka ada σ *extending* $\pi \ni$

$$\begin{tikzcd} \sigma : E \arrow[r, "\sim"] \arrow[d] & E' \arrow[d] \\ \pi : F(\alpha) \arrow[r, "\sim"] & F'(\beta) \end{tikzcd} \quad \text{di mana } \sigma = \pi \qquad (3)$$

Dari (1) dan (3) diperoleh

$$\begin{tikzcd} \sigma : E \arrow[r, "\sim"] \arrow[d] & E' \arrow[d] \\ \varphi : F \arrow[r, "\sim"] & F' \end{tikzcd}$$ ▲

b) Andai E' *splitting field* $f'(x)$ atas F' dan φ isomorfisma.
Akan dibuktikan:
σ isomorfisma $\Rightarrow$ i) σ homomorfisma
ii) σ onto
iii) σ satu-satu

Bukti:

i) Didefinisikan:

$$\begin{tikzcd} \sigma : E \arrow[r, "\sim"] \arrow[d] & E' \arrow[d] \\ \varphi : F \arrow[r, "\sim"] & F' \end{tikzcd} \qquad \begin{array}{c} \sigma(E) = E' \\ \ni \\ \varphi(F) = F' \end{array}$$

Ambil sebarang $\alpha, \beta \in E$ *splitting field* $f(x)$ atas F dan $k \in \mathbb{Z}$, maka:

- $\sigma(\alpha\beta) = (\alpha\beta)'$
  $= \alpha'\beta'$
  $= \sigma(\alpha).\sigma(\beta)$
- $\sigma(k\alpha) = (k\alpha)'$
  $= k.\alpha'$
  $= k.\sigma(\alpha)$

Jadi σ homomorfisma. ▲

ii) Ambil sebarang $f(x) \in F[x]$, maka:

$f(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n, \ \alpha_i \in F$

Himpunan

$f^{\varphi}(x) = \varphi(\alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n)$

karena φ homomorfisma, maka:

$f^{\varphi}(x) = \varphi(\alpha_0) + \varphi(\alpha_1 x) + \cdots + \varphi(\alpha_n x^n)$
$= \varphi(\alpha_0) + \varphi(\alpha_1)x + \cdots + \varphi(\alpha_n)x^n$

Padahal E' *splitting field* $f'(x) \in F'(x)$, maka:

$f'(x) = c(x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n)$

di mana $\alpha_i \notin F'$

Sehingga

$$f'(x) = c\big(x - \varphi(a_1)\big)\big(x - \varphi(a_2)\big) \ldots \big(x - \varphi(a_n)\big) \qquad (4)$$

Disisi lain, jika ada $\beta_i \in F'$, maka:

$$f'(x) = c(x - \beta_1)(x - \beta_2) \ldots (x - \beta_n) \qquad (5)$$

dari (4) dan (5) maka himpunan

$\{\varphi(a_1), \varphi(a_2), \ldots, \varphi(a_n)\} = \{\beta_1, \beta_2, \ldots, \beta_n\}$

Karena E' *splitting field* $f'(x) \in F'(x)$maka

$E' = F'(\beta_1, \beta_2, \ldots, \beta_n)$
$= F'\big(\varphi(a_1), \varphi(a_2), \ldots, \varphi(a_n)\big)$
$= F'\big(\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_n)\big)$
$= \varphi(F)\big(\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_n)\big)$
$= \sigma(F)\big(\varphi(a_1), \varphi(a_2), \ldots, \varphi(a_n)\big)$
$= \sigma\big(F(\alpha_1, \alpha_2, \ldots, \alpha_n)\big)$

$E' = \sigma(E)$
Jadi σ Onto. ▲

iii) σ Satu-satu.
Ambil sebarang $x_1, x_1 \in E' \ni$

$$\sigma(x_1) = \sigma(x_2)$$

$\sigma(x_1) = \sigma(x_2)$
$\sigma(x_1) - \sigma(x_2) = 0$
$\sigma(x_1 - x_2) = 0$ (karena σ homomorfisma)
Jadi $x_1 - x_2 \in \ker\, \sigma$
$\sigma(x_1) = \sigma(x_2)$
$\sigma(x_1) - \sigma(x_2) = 0$
$\varphi(x_1) - \varphi(x_2) = 0$ (karena $\varphi = \sigma$)
$\varphi(x_1 - x_2) = 0$ (karena φ homomorfisma)
Jadi $x_1 - x_2 \in \ker\, \varphi$
Jadi σ Satu-satu. ▲

Akibat 4 (Ketunggalan *Splitting Field*)
Sebarang dua *splitting field* polinomial $f(x) \in F[x]$ atas field F adalah isomorfik.

Bukti:

Ambil sebarang *splitting field* $f(x) \in F[x]$.
Misal: E *splitting field* $f(x)$ atas F dan
E' *splitting field* $f'(x)$atas F'.

E *splitting field* $f(x) \in F[x]$ isomorfik dengan E' *splitting field* $f'(x) \in F'[x]$ jika ada isomorfisma ring
$\sigma : E \longrightarrow E'$ dan $\varphi : F \longrightarrow F'$

$$\begin{tikzcd}
\sigma : E \arrow[r, "\sim"] \arrow[d] & E' \arrow[d] \\
\varphi : F \arrow[r, "\sim"] & F'
\end{tikzcd}$$

komutatif ($\sigma = \varphi$).
Jelas. Dari teorema 3, di mana $F = F'$ dan $\sigma \cong \varphi$. ▲

KESIMPULAN

Dari hasil pembahasan dapat ditarik kesimpulan bahwa jika E dan E' *splitting field* atas polinomial-polinomial f(x)∈ F[x] maka kedua *splitting field* tersebut isomorfik. Dan untuk selanjutnya disebut ketunggalan *splitting field.*

DAFTAR PUSTAKA

[1] Anton,H. 1987. *Aljabar Linier Elementer*. Erlangga. Jakarta.

[2] Arifin, A. 2000. *Aljabar*. ITB. Bandung.

[3] Bhattacharya, P.B., Jain, S.K., Nagpaul, S.R. 1986. *Basic Abstract Algebra*. Second Ed., Cambridge University Press.USA.

[4] Birkhoff, G., and Mac Lane, S. 1953. *A Survey of Modern Algebra*. Mac Millan Company. New York.

[5] Deieker, P.F., and Voxman.1986. *Discrete Mathematics*. Harcourt Brace Jovanovich, Inc. New York.

[6] Dummit, David S., and Foote, Richard M. 1991. *Abstract Algebra*. Prenticehall, Inc. New Jersey.

[7] Durbin, J.R. 1992. *Modern Algebra and Introduction*. John Wiley and Sons, Inc. New york.

[8] Fraleigh, John B. 1994. *A First Course in Abstract Algebra*. Fifth Ed., Addison Wesley Publishing Company, Inc. USA.

[9] Gallian, J.A. 1990. *Contemporary Abstract Algebra*. DC Heath and Company. USA.

[10] Herstein, I.N. 1975. *Topics in Algebra*. Second Ed., John Wiley and Sons. Singapore.

[11] Hartley, B., and Hawkes, T.O. 1970. *Rings, Modules, and Linear Algebra*. Chapman and Hall. London.

[12] Leon, Steven J. 2001. *Aljabar Linear dan Aplikasinya*. Edisi kelima. Erlangga. Jakarta.

[13] Raisinghania, M.D., and Anggarwal, R.S. 1980. *Modern Algebra*. S.Chard and Company LTD. New Delhi.

[14] Roman, S. 1991. *Advanced Linear Algebra*. Springer Verlag. New York.

[15] Sims, Charles C. 1984. *Abstract A Computational Approach*. John Wiley and Sons, Inc. New York.

[16] Spindler, Karlheins. 1994. *Abstract Algebra with Application*. Volume II. Marcell Dekker, Inc. USA.

[17] Stewart, Ian. 1989. *Galois Theory*. Second Ed., Chapman and Hall. London.

[18] Whitelaw, Thomas A. 1995. *Introduction to Abstract Algebra*. Third Ed., Chapman and Hall. New York.