

# SPLITTING FIELD DAN KETUNGGALANNYA ATAS POLINOMIAL FIELD

Corina Karim<sup>1</sup> dan Ari Andari<sup>2</sup>

<sup>1,2</sup>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:

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n + \dots \\ = \sum_{i=1}^{\infty} a_i x^i$$

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  $f(x) = g(x) \cdot h(x)$  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  $\alpha \in E$ ,  $\alpha$  disebut *algebraic* atas  $F$ , jika  $\alpha$  akar dari suatu polinomial  $F[x]$ . ( $f(x) \in F[x], f(\alpha) = 0$ ). Jika  $\alpha$  bukan *algebraic* atas  $F$ , maka  $\alpha$  disebut *transcendental* 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*  $\geq 1$  maka  $K$  *extension field*  $F$  disebut *Splitting field*  $f(x)$  atas  $F$  jika:

- 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.
- $K = F(\alpha_1, \alpha_2, \dots, \alpha_n) \ni K$  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:

- $\mathbb{Q}(\sqrt{2})$  *extension field*  $\mathbb{Q}$ .
- $\mathbb{Q}(\sqrt{2})$  *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  $\mathbb{Q}(\sqrt{2})$

- Ambil sebarang  $y \in \mathbb{Q}(\sqrt{2})$ .

Maka  $y$  dapat dinyatakan sebagai

$$y = a + b\sqrt{2}, \quad a, b \in \mathbb{Q} \\ = a \cdot 1 + b \cdot \sqrt{2},$$

Created with

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

b) Untuk suatu  $a, b \in \mathbb{Q}$ , maka  
 $0 = a + b\sqrt{2}$   
 $\Rightarrow 0 = a + b \cdot \sqrt{2}$   
 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  $g(x) = x^2 - 2 \in \mathbb{Q}[x]$   
 $g(x) = x^2 - 2$   
 $= (x - \sqrt{2})(x + \sqrt{2})$   
 $= (x - \sqrt{2})(x - (-\sqrt{2}))$

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

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

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

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

$\alpha = a + \sqrt{2}b$   
 $\alpha^2 = (a + \sqrt{2}b)^2$   
 $= a^2 + 2\sqrt{2}ab + 2b^2$   
 $\alpha^2 - a^2 + 2\sqrt{2}ab + 2b^2 = 0$

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

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

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

▲  
 Jadi  $\mathbb{Q}(\sqrt{2})$  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 :**

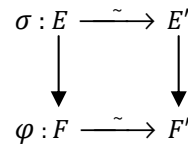
Karena menurut definisi 1. bagian ii)  $K = F(\alpha_1, \alpha_2, \dots, \alpha_n) \ni K$  dibangun oleh  $F$  dengan  $\alpha_1, \alpha_2, \dots, \alpha_n \in K$ . Maka  $K$  algebraic atas  $F$ .

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  $\varphi$  terhadap koefisien  $f(x)$ . Jika  $E$  splitting field  $f(x)$  atas  $F$  dan  $E'$  splitting field  $f'(x)$  atas  $F'$ . Maka Isomorfisma  $\varphi$  "extended to" isomorfisma  $\sigma : E \xrightarrow{\sim} E'$ .  $\sigma$  yang dibatasi (restricted to)  $F$  adalah Isomorfisma  $\varphi$  :



**Bukti:**

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

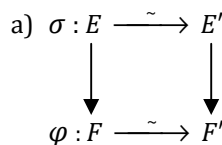
$f(x) \mapsto f'(x)$

$\alpha_0 + \alpha_1 x \mapsto \alpha_0' + \alpha_1' x$

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

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

Akan dibuktikan:



b)  $\sigma$  Isomorfisma

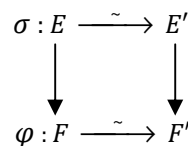
Bukti:

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

i) Untuk  $n = 1$ .

Jika  $n = 1$  maka  $E = F$

Padahal



maka  $\sigma = \varphi$ . ▲

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

Bukti:

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

$p \mapsto p(\alpha)$

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

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

Created with

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  $\pi$  *extending*  $\varphi \ni$

$$\begin{array}{ccc} \pi : F(\alpha) & \xrightarrow{\sim} & F'(\beta) \\ \downarrow & & \downarrow \\ \varphi : F & \xrightarrow{\sim} & F' \end{array} \quad (1)$$

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

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

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

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

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

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

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

$$\begin{array}{ccc} \sigma : E & \xrightarrow{\sim} & E' \\ \downarrow & & \downarrow \\ \pi : F(\alpha) & \xrightarrow{\sim} & F'(\beta) \end{array} \quad (2)$$

karena  $\sigma$  *extends*  $\pi$  dan  $\pi$  *extends*  $\varphi$  maka  $\sigma$  *extends*  $\varphi$ .

Dari (1) dan (2) diperoleh:

$$\begin{array}{ccc} \sigma : E & \xrightarrow{\sim} & E' \\ \downarrow & & \downarrow \\ \pi : F(\alpha) & \xrightarrow{\sim} & F'(\beta) \\ \downarrow & & \downarrow \\ \varphi : F & \xrightarrow{\sim} & F' \end{array}$$

Jadi

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

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

$$\begin{array}{ccc} \sigma : E & \xrightarrow{\sim} & E' \quad \text{di mana } \sigma = \pi \\ \downarrow & & \downarrow \\ \pi : F(\alpha) & \xrightarrow{\sim} & F'(\beta) \end{array} \quad (3)$$

Dari (1) dan (3) diperoleh

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

b) Andai  $E'$  *splitting field*  $f'(x)$  atas  $F'$  dan  $\varphi$  isomorfisma.

Akan dibuktikan:

- $\sigma$  isomorfisma  $\Rightarrow$  i)  $\sigma$  homomorfisma
- ii)  $\sigma$  onto
- iii)  $\sigma$  satu-satu

Bukti:

i) Didefinisikan:

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

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

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

Jadi  $\sigma$  homomorfisma. ▲

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

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

Himpunan

$$f^\varphi(x) = \varphi(\alpha_0 + \alpha_1 x + \dots + \alpha_n x^n)$$

karena  $\varphi$  homomorfisma, maka:

$$\begin{aligned} f^\varphi(x) &= \varphi(\alpha_0) + \varphi(\alpha_1 x) + \dots + \varphi(\alpha_n x^n) \\ &= \varphi(\alpha_0) + \varphi(\alpha_1)x + \dots + \varphi(\alpha_n)x^n \end{aligned}$$

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

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

di mana  $\alpha_i \notin F'$

Sehingga

$$\begin{aligned} f'(x) &= c(x - \varphi(\alpha_1))(x - \varphi(\alpha_2)) \dots \\ &\quad (x - \varphi(\alpha_n)) \end{aligned} \quad (4)$$

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

$$f'(x) = c(x - \beta_1)(x - \beta_2) \dots (x - \beta_n) \quad (5)$$

dari (4) dan (5) maka himpunan

$$\{\varphi(\alpha_1), \varphi(\alpha_2), \dots, \varphi(\alpha_n)\} = \{\beta_1, \beta_2, \dots, \beta_n\}$$

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

$$\begin{aligned} E' &= F'(\beta_1, \beta_2, \dots, \beta_n) \\ &= F'(\varphi(\alpha_1), \varphi(\alpha_2), \dots, \varphi(\alpha_n)) \\ &= F'(\sigma(\alpha_1), \sigma(\alpha_2), \dots, \sigma(\alpha_n)) \\ &= \varphi(F)(\sigma(\alpha_1), \sigma(\alpha_2), \dots, \sigma(\alpha_n)) \\ &= \sigma(F)(\varphi(\alpha_1), \varphi(\alpha_2), \dots, \varphi(\alpha_n)) \\ &= \sigma(F(\alpha_1, \alpha_2, \dots, \alpha_n)) \end{aligned}$$

Created with

$E' = \sigma(E)$   
Jadi  $\sigma$  Onto. ▲

iii)  $\sigma$  Satu-satu.

Ambil sebarang  $x_1, x_2 \in E' \ni$

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

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

$$\sigma(x_1) - \sigma(x_2) = 0$$

$$\sigma(x_1 - x_2) = 0 \quad (\text{karena } \sigma \text{ homomorfisma})$$

Jadi  $x_1 - x_2 \in \ker \sigma$

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

$$\sigma(x_1) - \sigma(x_2) = 0$$

$$\varphi(x_1) - \varphi(x_2) = 0 \quad (\text{karena } \varphi = \sigma)$$

$$\varphi(x_1 - x_2) = 0 \quad (\text{karena } \varphi \text{ homomorfisma})$$

Jadi  $x_1 - x_2 \in \ker \varphi$

Jadi  $\sigma$  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

$$\sigma : E \rightarrow E' \text{ dan } \varphi : F \rightarrow F'$$

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

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  $f(x) \in F[x]$  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.