

# Teorema Fundamental Teori Galois

**Muhamad Zaki Riyanto<sup>1</sup>**  
Mahasiswa S2 Matematika UGM  
Email: [zaki@mail.ugm.ac.id](mailto:zaki@mail.ugm.ac.id)

## Abstrak

Diberikan suatu field  $F$ , maka terdapat suatu extension berhingga  $E$  dari  $F$  sedemikian hingga jika diberikan polinomial  $f(x)$  atas  $F$ , maka  $f(x)$  mempunyai akar di  $E$ . Ide mendasar dari konsep Teori Galois adalah untuk menyelidiki hubungan antara grup permutasi dari akar-akar  $f(x)$  dengan struktur splitting field-nya.

Pada makalah ini dibahas mengenai konsep dasar pembentukan grup Galois serta Teorema Fundamental Teori Galois yang menjelaskan hubungan antara grup Galois dengan fixed field-nya.

**Kata kunci:** field extension, Galois extension, grup Galois

## 1. Pendahuluan

Solusi dan akar dari suatu persamaan polinomial telah menarik perhatian banyak matematikawan sejak 3-4 abad yang lalu. Pada awal-awal perkembangannya, untuk mencari dan mengkarakterisasi solusi-solusi dan akar-akar tersebut mereka masih menggunakan perhitungan-perhitungan aljabar seperti operasi penjumlahan, pengurangan, perkalian, pembagian, dan pengambilan akar-akar. Pada saat itu, mereka masih belum melihat hubungan di antara akar-akar tersebut dengan suatu struktur aljabar.

Pada tahun 1843, Evariste Galois menemukan sebuah cara melihat suatu solusi mengenai akar-akar dari suatu persamaan polinomial. Galois menjelaskan hubungan antara grup permutasi dari akar-akar suatu polinomial yang diberikan dengan struktur aljabar dari splitting field dari polinomial tersebut. Dia menemukan bahwa terdapat korespondensi 1-1 (bijeksi) di antara subgrup-subgrup dari grup permutasi dari akar-akar dengan field-field pertengahan dari field yang ditentukan oleh polinomial dan splitting field-nya.

Pada makalah ini dibahas mengenai konsep dasar dari Teori Galois, melalui beberapa definisi dan teorema tentang field extension dan splitting field. Selanjutnya diberikan konsep grup Galois beserta sifat-sifat pentingnya. Yang terakhir adalah mengenai

---

<sup>1</sup> Dosen Pembimbing: **Dr. Budi Surodjo, M.Si** (Jurusan Matematika UGM)

Teorema Fundamental Teori Galois, disertai dengan beberapa contohnya. Dummit (1994) telah memberikan hampir semua konsep dasar yang dibutuhkan. Secara khusus, Dummit (1999) memberikan gambaran melalui diagram latris mengenai hubungan antara grup permutasi dari akar-akar suatu polinomial dengan splitting field dari polinomial tersebut.

## 2. Field Extension

Pada bagian ini diberikan konsep-konsep dasar mengenai field extension yang digunakan untuk mendukung konsep dari grup Galois pada bagian 3.

**Definisi 2.1.** *Field prima* dari suatu field  $F$  adalah subfield dari  $F$  yang dibangun oleh elemen identitas terhadap operasi multiplikasi di  $F$ .

**Definisi 2.2.** (*Field Extension*) Jika  $K$  adalah field yang memuat subfield  $F$ , maka  $K$  disebut dengan *field extension* dari  $F$ , dinotasikan dengan  $K/F$  atau dengan diagram:

$$\begin{array}{c} K \\ | \\ F \end{array}$$

**Definisi 2.3.** *Derajat* dari field extension  $K/F$ , dinotasikan dengan  $[K:F]$ , adalah dimensi dari  $K$  sebagai ruang vektor atas  $F$ . Suatu field extension dikatakan *berhingga* jika  $[K:F]$  berhingga. Basis untuk  $K$  atas  $F$  dinotasikan dengan  $F$ -basis.

**Definisi 2.4.** Diberikan field extension  $K/F$  dan suatu koleksi  $\alpha, \beta, \dots \in K$ . Subfield terkecil dari  $K$  yang memuat  $F$  dan  $\alpha, \beta, \dots$ , dinotasikan dengan  $F(\alpha, \beta, \dots)$  disebut dengan *field yang dibangun oleh  $\alpha, \beta, \dots$  atas  $F$* .

**Definisi 2.5.** (*Extension Berhingga*) Jika suatu field  $K$  dibangun oleh elemen sebanyak berhingga atas  $F$ , maka  $K$  disebut dengan *extension berhingga* dari  $F$ . Jika  $K$  dibangun oleh satu elemen  $\alpha$  atas  $F$ , yaitu  $K = F(\alpha)$ , maka  $K$  disebut dengan *extension sederhana* dari  $F$ .

**Lemma 2.6.** Diberikan field  $F$  dan  $p(x) \in F[x]$  suatu polinomial ireduabel berderajat  $n$ . Misalkan  $K$  adalah field extension dari  $F$  yang memuat suatu akar  $\alpha$  dari  $p(x)$ . Maka

$$F(\alpha) = \{a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{n-1}\alpha^{n-1} \mid a_0, a_1, \dots, a_{n-1} \in F\} \subseteq K.$$

**Teorema 2.7.** Diberikan  $\varphi: F \xrightarrow{\sim} F'$  isomorfisma field. Diberikan  $p(x) \in F[x]$  suatu polinomial ireduabel dan  $p'(x) \in F'[x]$  polinomial ireduabel yang diperoleh dengan menggunakan pemetaan  $\varphi$  pada koefisien dari  $p(x)$ . Misalkan  $\alpha$  adalah akar dari  $p(x)$  pada suatu extension dari  $F$ , dan  $\beta$  adalah akar dari  $p'(x)$  pada suatu extension dari  $F'$ . Maka terdapat suatu isomorfisma

$$\begin{array}{ccc} \sigma: F(\alpha) & \xrightarrow{\sim} & F'(\beta) \\ & & \alpha \mapsto \beta \end{array}$$

yang memetakan  $\alpha$  ke  $\beta$  dan memperluas pemetaan  $\varphi$ , yaitu  $\sigma$  yang dibatasi ke  $F$  merupakan suatu isomorfisma  $\varphi$ .

Teorema ini jika direpresentasikan dalam bentuk diagram, diperoleh:

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

Diberikan field  $F$ , dan  $K$  suatu extension dari  $F$ .

**Definisi 2.8.** (*Algebraic*) Suatu elemen  $\alpha \in K$  disebut *algebraic* atas  $F$  jika  $\alpha$  merupakan akar dari suatu polinomial tidak nol  $f(x) \in F[x]$ . Jika  $\alpha$  tidak algebraic atas  $F$ , maka  $\alpha$  disebut *transcendental* atas  $F$ . Suatu extension  $K/F$  disebut *algebraic* jika setiap elemen dari  $K$  algebraic atas  $F$ .

**Proposisi 2.9.** Misalkan  $\alpha$  algebraic atas  $F$ . Maka terdapat dengan tunggal polinomial monik  $m_\alpha(x) \in F[x]$  dimana  $\alpha$  merupakan akarnya. Suatu polinomial  $f(x) \in F[x]$  mempunyai akar  $\alpha$  jika dan hanya jika  $m_\alpha(x)$  membagi  $f(x)$  di  $F[x]$ . Selanjutnya, polinomial  $m_\alpha(x)$  disebut dengan *polynomial minimal* untuk  $\alpha$  atas  $F$ .

**Teorema 2.10.** Diberikan  $F \subseteq K \subseteq L$  adalah field, maka

$$[L : F] = [L : K][K : F].$$

**Definisi 2.11.** (*Field Komposit*) Diberikan  $K_1$  dan  $K_2$  adalah subfield dari  $K$ . *Field komposit* dari  $K_1$  dan  $K_2$ , dinotasikan dengan  $K_1K_2$ , didefinisikan sebagai subfield terkecil dari  $K$  yang memuat  $K_1$  dan  $K_2$ .

**Proposisi 2.12.** Diberikan  $K_1$  dan  $K_2$  adalah extension berhingga dari field  $F$  yang termuat di  $K$ . Maka

$$[K_1K_2 : F] \leq [K_1 : F][K_2 : F]$$

dan bernilai sama jika dan hanya jika  $F$ -basis untuk  $K_1$  bebas linear di  $K_2$ , dan sebaliknya.

**Definisi 2.13.** (*Splitting Field*) Field extension  $K$  dari  $F$  disebut *splitting field* untuk polinomial  $f(x) \in F[x]$  jika  $f(x)$  terfaktorkan secara penuh ke dalam bentuk linear (split secara penuh) di  $K[x]$  dan  $f(x)$  tidak split secara penuh atas setiap subfield sejati dari  $K$  yang memuat  $F$ .

**Definisi 2.14.** (*Extension Normal*) Jika  $K$  adalah algebraic extension dari  $F$ , dan  $K$  merupakan splitting field untuk suatu koleksi polinomial atas  $F$ , maka  $K$  disebut dengan *extension normal* dari  $F$ .

**Teorema 2.15.** Diberikan  $\varphi : F \xrightarrow{\sim} F'$  isomorfisma field. Diberikan  $f(x) \in F[x]$  suatu polinomial dan  $f'(x) \in F'[x]$  polinomial yang diperoleh dengan menggunakan pemetaan  $\varphi$  pada koefisien dari  $f(x)$ . Misalkan  $E$  adalah splitting field untuk  $f(x)$  atas  $F$  dan  $E'$  adalah splitting field dari  $f'(x)$  atas  $F'$ . Maka isomorfisma  $\varphi$  dapat diperluas menjadi suatu isomorfisma  $\sigma : E \xrightarrow{\sim} E'$ , yaitu

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

**Akibat 2.16.** (*Ketunggalan Splitting Field*) Jika  $E_1$  dan  $E_2$  splitting field untuk suatu  $f(x) \in F[x]$  atas field  $F$ , maka  $E_1 \cong E_2$ .

Diberikan splitting field untuk polinomial  $x^n - 1$  atas  $\mathbb{Q}$ . Akar-akar dari polinomial ini disebut dengan  $n^{\text{th}}$  roots of unity. Himpunan semua  $n^{\text{th}}$  roots of unity membentuk grup siklik. Pembangun dari grup siklik tersebut dinamakan dengan *primitive  $n^{\text{th}}$  root of unity*.

**Definisi 2.17.** (*Algebraic Closure*) Suatu field  $\bar{F}$  disebut dengan *algebraic closure* dari  $F$  jika  $\bar{F}$  algebraic atas  $F$  dan setiap polinomial  $f(x) \in F[x]$  split secara penuh atas  $\bar{F}$ . Suatu field  $K$  dikatakan *algebraically closed* jika setiap polinomial di  $K[x]$  mempunyai akar di  $K$ .

**Definisi 2.18.** (*Polynomial Separabel*) Suatu polinomial atas field  $F$  dikatakan *separabel* jika tidak mempunyai akar yang sama, yaitu setiap akar-akarnya berlainan. Suatu polinomial yang tidak separabel disebut dengan *inseparabel*.

**Definisi 2.19.** (*Field Separabel*) Field  $K$  disebut *separabel* jika setiap elemen dari  $K$  merupakan akar dari suatu polinomial separabel atas  $F$ . Ekuivalen dengan mengatakan bahwa polinomial minimal atas  $F$  dari setiap elemen dari  $K$  merupakan polinomial separabel. Suatu field yang tidak separabel disebut dengan *inseparabel*.

### 3. Grup Galois

Diberikan suatu field  $F$ , maka terdapat suatu extension berhingga dari  $F$  sedemikian hingga jika diberikan  $f(x) \in F[x]$ , maka  $f(x)$  mempunyai akar di field extension-nya. Ide mendasar dari konsep Teori Galois adalah untuk menyelidiki hubungan antara grup permutasi dari akar-akar  $f(x)$  dengan struktur splitting field-nya.

**Definisi 3.1.** Diberikan field  $K$ .

- (1) Suatu isomorfisma  $\sigma : K \rightarrow K$  disebut dengan automorfisma dari  $K$ . Koleksi semua automorfisma dari  $K$  dinotasikan dengan  $\text{Aut}(K)$ .

- (2) Suatu automorfisma  $\sigma \in \text{Aut}(K)$  dikatakan *fix* untuk suatu elemen  $\alpha \in K$  jika  $\sigma(\alpha) = \alpha$ . Jika  $F$  adalah subset dari  $K$ , maka automorfisma  $\sigma$  dikatakan *fix*  $F$  jika  $\sigma(a) = a$ , untuk setiap  $a \in F$ .

Untuk setiap  $\text{Aut}(K)$  paling tidak memuat satu elemen, yaitu pemetaan identitas, dan dinotasikan dengan  $1$ , pemetaan ini sering disebut dengan automorfisma trivial. Field prima dari  $K$  merupakan field yang dibangun oleh  $1_K \in K$ , karena setiap homomorfisma memetakan  $1_K$  ke  $1_K$ , maka  $\sigma(1_K) = 1_K$ , sehingga  $\sigma(a) = a$  untuk setiap  $a$  di field prima tersebut. Oleh karena itu, setiap automorfisma dari  $K$  *fix* pada prime field-nya. Perhatikan bahwa  $\mathbb{Q}$  dan  $F_p$  hanya mempunyai automorfisma, yaitu  $\text{Aut}(\mathbb{Q}) = \{1\}$  dan  $\text{Aut}(F_p) = \{1\}$ .

**Definisi 3.2.** Diberikan field extension  $K/F$ . Didefinisikan  $\text{Aut}(K/F)$  adalah koleksi semua automorfisma dari  $K$  yang *fix*  $F$ .

Dengan kata lain,  $\text{Aut}(K/F) = \{\sigma \mid \sigma \in \text{Aut}(K) \text{ dan } \sigma(a) = a, \forall a \in F\}$ . Perhatikan bahwa jika  $F$  adalah subfield prima dari  $K$ , maka  $\text{Aut}(K) = \text{Aut}(K/F)$  sebab setiap automorfisma dari  $K$  *fix* pada  $F$ . Selanjutnya, jika  $\sigma, \tau \in \text{Aut}(K)$ , maka komposisi dari  $\sigma$  dan  $\tau$  yaitu  $\sigma\tau$  dan  $\tau\sigma$  juga merupakan automorfisma dari  $K$ .

**Proposisi 3.3.**  $\text{Aut}(K)$  merupakan grup terhadap operasi komposisi, dan  $\text{Aut}(K/F)$  merupakan subgrup dari  $\text{Aut}(K)$ .

**Bukti:**

Jelas bahwa  $\text{Aut}(K)$  tidak kosong, sebab memuat pemetaan identitas, yaitu  $1 \in \text{Aut}(K)$ . Operasi komposisi jelas bersifat asosiatif. Diambil sebarang  $\sigma \in \text{Aut}(K)$ , maka  $\sigma 1 = 1\sigma = \sigma$ , jadi  $1$  merupakan elemen identitas di  $\text{Aut}(K)$ . Karena  $\sigma$  isomorfisma, maka terdapat  $\sigma^{-1} : K \rightarrow K$  sedemikian hingga  $\sigma\sigma^{-1} = \sigma^{-1}\sigma = 1$ . Jadi,  $\text{Aut}(K)$  merupakan grup terhadap operasi komposisi. Selanjutnya, akan dibuktikan bahwa  $\text{Aut}(K/F)$  subgrup dari  $\text{Aut}(K)$ . Jelas bahwa  $1 \in \text{Aut}(K/F)$ . Diambil sebarang  $\sigma, \tau \in \text{Aut}(K/F)$  dan  $a \in F$ ,

maka  $\sigma(a) = a$  dan  $\tau(a) = a$ . Selanjutnya,  $(\sigma\tau)(a) = \sigma(\tau(a)) = \sigma(a) = a$ , diperoleh  $\sigma\tau \in \text{Aut}(K/F)$ . Diketahui  $\sigma \in \text{Aut}(K)$ , maka terdapat  $\sigma^{-1} \in \text{Aut}(K)$  sedemikian hingga  $1 = \sigma^{-1}\sigma$ . Karena  $1(a) = (\sigma^{-1}\sigma)(a) = \sigma^{-1}(\sigma(a)) = \sigma^{-1}(a)$ , maka diperoleh bahwa  $\sigma^{-1} \in \text{Aut}(K/F)$ . Jadi, terbukti bahwa  $\text{Aut}(K/F)$  subgrup dari  $\text{Aut}(K)$ . ■

Proposisi berikut ini dapat digunakan untuk menentukan automorfisma dari algebraic extension.

**Proposisi 3.4.** Diberikan field extension  $K/F$  dan  $\alpha \in K$  algebraic atas  $F$ . Maka untuk sebarang  $\sigma \in \text{Aut}(K/F)$ ,  $\sigma(\alpha)$  merupakan akar dari polinomial minimal untuk  $\alpha$  atas  $F$ , yaitu  $\text{Aut}(K/F)$  mempermutasikan akar-akar dari polinomial-polinomial ireduksibel. Pernyataan tersebut ekuivalen dengan mengatakan bahwa setiap polinomial atas  $F$  yang mempunyai  $\alpha$  sebagai akarnya, maka juga mempunyai  $\sigma(\alpha)$  sebagai akarnya.

**Bukti:**

Diketahui  $\alpha \in K$  algebraic atas  $F$ , maka terdapat suatu polinomial minimal  $m_\alpha(x) \in F[x]$  sedemikian hingga  $\alpha$  merupakan akarnya. Misalkan  $m_\alpha(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$ , maka

$$\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0 = 0. \quad (1)$$

Diambil sebarang  $\sigma \in \text{Aut}(K/F)$ , dari (1) diperoleh

$$\begin{aligned} \sigma(\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0) &= \sigma(0) \\ \Rightarrow \sigma(\alpha^n) + \sigma(a_{n-1}\alpha^{n-1}) + \dots + \sigma(a_1\alpha) + \sigma(a_0) &= 0 \\ \Rightarrow \sigma(\alpha^n) + \sigma(a_{n-1})\sigma(\alpha^{n-1}) + \dots + \sigma(a_1)\sigma(\alpha) + \sigma(a_0) &= 0 \\ \Rightarrow \sigma(\alpha)^n + \sigma(a_{n-1})\sigma(\alpha)^{n-1} + \dots + \sigma(a_1)\sigma(\alpha) + \sigma(a_0) &= 0 \end{aligned}$$

Karena  $\sigma$  fix  $F$ , maka diperoleh

$$\sigma(\alpha)^n + a_{n-1}\sigma(\alpha)^{n-1} + \dots + a_1\sigma(\alpha) + a_0 = 0,$$

atau dengan kata lain,  $\sigma(\alpha)$  merupakan akar dari  $m_\alpha(x)$ . ■

Secara umum, jika  $K$  dibangun atas  $F$  oleh suatu koleksi elemen-elemen, maka sebarang automorfisma  $\sigma \in \text{Aut}(K/F)$  ditentukan oleh pembangun dari  $K$ . Jika  $K/F$  berhingga, maka  $K$  dibangun secara hingga atas  $F$  oleh elemen-elemen algebraic. Oleh karena itu, automorfisma yang fix  $F$  sebanyak berhingga, yaitu  $\text{Aut}(K/F)$  merupakan grup hingga.

**Proposisi 3.5** Misalkan  $H$  subgrup dari  $\text{Aut}(K)$ . Jika  $F$  adalah koleksi elemen-elemen  $K$  yang fix oleh semua elemen  $H$ , yaitu  $F = \{a \in K \mid h(a) = a, \forall h \in H\}$ , maka  $F$  merupakan subfield dari  $K$ .

**Bukti:**

Jelas bahwa  $1_K \in F$ . Diambil sebarang  $h \in H$  dan  $a, b \in F$ , maka  $h(a) = a$  dan  $h(b) = b$ . Selanjutnya,  $h(a+b) = h(a) + h(b) = a + b$ ,  $h(ab) = h(a)h(b) = ab$ , dan  $h(a^{-1}) = h(a)^{-1} = a^{-1}$ . Oleh karena itu,  $F$  merupakan subfield dari  $K$ . ■

**Definisi 3.6.** Jika  $H$  merupakan subgrup dari  $\text{Aut}(K)$ , subfield dari  $K$  yang fix oleh semua elemen dari  $H$  disebut dengan *fixed field* dari  $H$ .

**Proposisi 3.7.**

- (1) Jika  $F_1 \subseteq F_2$  adalah subfield dari  $K$ , maka  $\text{Aut}(K/F_2) \leq \text{Aut}(K/F_1)$ .
- (2) Jika  $H_1 \leq H_2$  adalah subgrup dari  $\text{Aut}(K)$ , dan  $F_1$  dan  $F_2$  berturut-turut adalah fixed field-nya, maka  $F_2 \subseteq F_1$ .

**Bukti:**

- (1) Diketahui  $F_1 \subseteq F_2$  adalah subfield dari  $K$ , dan  $\text{Aut}(K/F_2)$  dan  $\text{Aut}(K/F_1)$  subgrup dari  $\text{Aut}(K)$ . Diambil sebarang  $\sigma \in \text{Aut}(K/F_2)$ , maka untuk setiap  $a \in F_2$  berlaku  $\sigma(a) = a$ . Karena  $F_1 \subseteq F_2$ , maka untuk setiap  $b \in F_1$  berlaku  $\sigma(b) = b$ . Jadi,  $\sigma \in \text{Aut}(K/F_1)$ , dengan kata lain terbukti bahwa  $\text{Aut}(K/F_2) \leq \text{Aut}(K/F_1)$ .

(2) Diketahui  $F_1$  dan  $F_2$  subfield dari  $K$ . Diambil sebarang  $a \in F_2$ , maka untuk setiap  $h_2 \in H_2$  berlaku  $h_2(a) = a$ . Karena  $H_1 \subseteq H_2$ , maka untuk setiap  $h_1 \in H_1$  berlaku  $h_1(a) = a$ . Jadi,  $a \in F_1$ , diperoleh bahwa  $F_2 \subseteq F_1$ . ■

**Proposisi 3.8.** Diberikan  $E$  splitting field atas  $F$  dari  $f(x) \in F[x]$ . Maka  $|\text{Aut}(E/F)| \leq [E:F]$ . Jika  $f(x)$  separabel, maka  $|\text{Aut}(E/F)| = [E:F]$ .

**Bukti:**

Diketahui  $E$  merupakan splitting field atas  $F$  terhadap polinomial  $f(x) \in F[x]$ . Diketahui bahwa sebarang isomorfisma (field)  $\sigma: F \xrightarrow{\sim} F'$  dapat diperluas menjadi suatu isomorfisma (field)  $\varphi: E \xrightarrow{\sim} E'$ , dengan  $E'$  adalah splitting field untuk  $f'(x) = \varphi(f(x)) \in F'[x]$ . Akan dibuktikan bahwa  $|\text{Aut}(E/F)| \leq [E:F]$  menggunakan induksi pada  $[E:F]$ . Jika  $[E:F] = 1$ , maka  $E = F$ ,  $E' = F'$ ,  $\sigma = \varphi$  dan  $|\text{Aut}(E/F)| = 1$ . Jika  $[E:F] > 1$ , maka  $f(x)$  mempunyai paling sedikit satu faktor ireduisible  $p(x)$  dengan derajat  $> 1$ , demikian juga  $f'(x)$  dan faktor ireduisible  $p'(x)$ . Misalkan  $\alpha$  adalah akar dari  $p(x)$ . Jika  $\sigma$  adalah sebarang extension dari  $\varphi$  ke  $E$ , maka  $\sigma$  dibatasi ke subfield  $F(\alpha)$  dari  $E$  merupakan suatu isomorfisma  $\tau$  dari  $F(\alpha)$  ke suatu subfield dari  $E'$ . Isomorfisma  $\tau$  ditentukan oleh aksi  $\tau$  pada  $\alpha$ , sehingga  $\tau(\alpha)$  merupakan suatu akar, yaitu  $\beta$  dari  $p'(x)$ . Diperoleh diagram berikut:

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

Sebaliknya, untuk sebarang  $\beta$  akar dari  $p'(x)$ , terdapat extension  $\tau$  dan  $\sigma$  yang mengakibatkan diagram seperti di atas. Oleh karena itu, untuk menghitung banyaknya extension  $\sigma$  cukup dengan menghitung banyaknya diagram yang mungkin. Banyaknya extension dari  $\varphi$  ke suatu isomorfisma  $\tau$  sama dengan banyaknya akar yang berbeda, yaitu  $\beta$  dari  $p'(x)$ . Karena derajat dari  $p(x)$  dan  $p'(x)$  sama dengan  $[F(\alpha):F]$ , maka

banyaknya extension dari  $\varphi$  ke  $\tau$  paling banyak  $[F(\alpha):F]$ , dan bernilai sama apabila akar-akar dari  $p(x)$  berbeda, atau  $p(x)$  separabel. Selanjutnya, karena  $E$  merupakan splitting field dari  $f(x)$  atas  $F(\alpha)$ ,  $E'$  merupakan splitting field dari  $f'(x)$  atas  $F'(\beta)$ , dan  $[E:F(\alpha)] < [E:F]$ , maka dengan asumsi induksi diperoleh bahwa banyaknya extension dari  $\tau$  ke  $\sigma$  adalah  $\leq [E:F(\alpha)]$ , dan bernilai sama jika  $f(x)$  mempunyai akar-akar yang berbeda, atau  $f(x)$  separabel. Karena diketahui bahwa  $[E:F] = [E:F(\alpha)][F(\alpha):F]$ , maka banyaknya extension dari  $\varphi$  ke  $\tau$  adalah  $\leq [E:F]$ , dan bernilai sama jika  $p(x)$  dan  $f(x)$  mempunyai akar-akar yang berbeda, hal ini sama dengan mengatakan bahwa  $f(x)$  mempunyai akar-akar yang berbeda, sebab  $p(x)$  merupakan faktor dari  $f(x)$ , atau dengan kata lain  $f(x)$  separabel. Dengan demikian teorema terbukti. ■

**Definisi 3.9.** (*Grup Galois*) Diberikan extension hingga  $K/F$ . Maka  $K$  dikatakan *Galois* atas  $F$  dan  $K/F$  adalah *Galois extension* jika  $|\text{Aut}(K/F)| = [K:F]$ . Jika  $K/F$  Galois, maka grup  $\text{Aut}(K/F)$  disebut dengan *grup Galois* dari  $K/F$ , dinotasikan dengan  $\text{Gal}(K/F)$ .

**Akibat 3.10.** Jika  $K$  adalah splitting field atas  $F$  dari polinomial separabel  $f(x) \in F[x]$ , maka  $K/F$  Galois.

**Bukti:**

Karena  $f(x)$  separabel, maka  $|\text{Aut}(K/F)| = [K:F]$ . Jadi,  $K/F$  merupakan Galois. ■

Perhatikan bahwa Akibat 3.10 mengakibatkan bahwa splitting field dari setiap polinomial atas  $\mathbb{Q}$  merupakan Galois, sebab splitting field dari  $f(x)$  sama dengan splitting field dari produk faktor-faktor ireduusibel dari  $f(x)$  yang separabel.

**Definisi 3.11.** Jika  $f(x)$  separabel atas  $F$ , maka grup Galois dari  $f(x)$  atas  $F$  adalah grup Galois dari splitting field dari  $f(x)$  atas  $F$ .

**Contoh.**

Extension  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$  Galois atas  $\mathbb{Q}$ , sebab merupakan splitting field dari polinomial  $(x^2 - 2)(x^2 - 3)$ . Setiap isomorfisma  $\sigma$  ditentukan oleh pembangunnya yaitu  $\sqrt{2}$  dan  $\sqrt{3}$ , yang dipetakan ke  $\pm\sqrt{2}$  dan  $\pm\sqrt{3}$ . Oleh karena itu, automorfisma yang mungkin adalah:

$$1: \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases} \quad \sigma: \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases} \quad \tau: \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases} \quad \sigma\tau: \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}$$

atau jika ditulis secara lebih detail, yaitu:

$$\sigma: (a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) \mapsto (a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6})$$

$$\tau: (a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) \mapsto (a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6})$$

dengan  $a, b, c, d \in \mathbb{Q}$ . Dapat dilihat bahwa  $\sigma^2 = 1$  dan  $\tau^2 = 1$ . Diperoleh bahwa

$$\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\},$$

yaitu grup Galois yang isomorfis ke grup 4-Klein. Selanjutnya, akan dilihat hubungan setiap subgrup dari  $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$  dengan fixed subfield dari  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ . Sebagai contoh, akan dicari subfield yang berkorespondensi dengan  $\{1, \sigma\tau\}$ .

Perhatikan bahwa

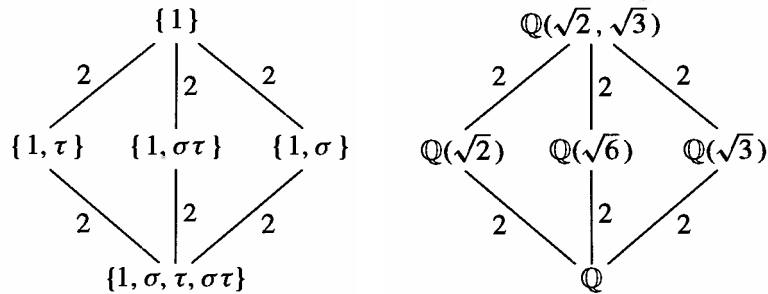
$$\sigma\tau: (a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) \mapsto (a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6})$$

menetapkan (fix) elemen  $a + d\sqrt{6}$ , yaitu field  $\mathbb{Q}(\sqrt{6})$ . Dengan cara yang sama diperoleh korespondensi antara fixed field dan subgrup dari grup Galois seperti berikut ini.

<u>Subgrup</u>	<u>Fixed Field</u>
$\{1\}$	$\mathbb{Q}(\sqrt{2}, \sqrt{3})$
$\{1, \sigma\}$	$\mathbb{Q}(\sqrt{3})$
$\{1, \sigma\tau\}$	$\mathbb{Q}(\sqrt{6})$
$\{1, \tau\}$	$\mathbb{Q}(\sqrt{2})$
$\{1, \sigma, \tau, \sigma\tau\}$	$\mathbb{Q}$

#### 4. Teorema Fundamental Teori Galois

Pada Galois extension  $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$  yang diberikan pada contoh sebelumnya, terdapat persamaan diagram dari subgrup-subgrup dari grup Galois dan fixed field-nya, yaitu



Teorema Fundamental Teori Galois menjelaskan hubungan antara subgrup dari suatu grup Galois dengan fixed field. Sebelumnya, diberikan terlebih dahulu mengenai konsep karakter dari suatu grup.

**Definisi 4.1.** (*Karakter Grup*) Suatu karakter  $\chi$  dari grup  $G$  dengan nilai di field  $L$  adalah suatu homomorfisma dari  $G$  ke  $L^*$ , yaitu grup multiplikatif dari  $L$ , dengan

$$\chi: G \rightarrow L^*$$

yaitu  $\chi(g_1 g_2) = \chi(g_1) \chi(g_2)$ , untuk setiap  $g_1, g_2 \in G$ , dan  $\chi(g)$  tidak nol di  $L$ , untuk setiap  $g \in G$ .

**Definisi 4.2.** Karakter  $\chi_1, \chi_2, \dots, \chi_n$  dari grup  $G$  dikatakan *bebas linear atas  $L$*  jika  $\chi_1, \chi_2, \dots, \chi_n$  bebas linear sebagai fungsi pada  $G$ , yaitu jika tidak ada relasi non-trivial

$$a_1 \chi_1 + a_2 \chi_2 + \dots + a_n \chi_n = 0 \tag{2}$$

dengan  $a_1, a_2, \dots, a_n \in L$  tidak semuanya nol, merupakan fungsi pada  $G$ , yaitu  $a_1 \chi_1(g) + a_2 \chi_2(g) + \dots + a_n \chi_n(g) = 0$  untuk setiap  $g \in G$ .

**Teorema 4.3.** (*Bebas Linear Karakter*) Jika  $\chi_1, \chi_2, \dots, \chi_n$  adalah karakter-karakter yang berbeda dari  $G$  dengan nilai di  $L$ , maka  $\chi_1, \chi_2, \dots, \chi_n$  bebas linear atas  $L$ .

**Bukti:**

Andaikan  $\chi_1, \chi_2, \dots, \chi_n$  tidak bebas linear. Tentukan relasi (2) yaitu  $a_1 \chi_1 + a_2 \chi_2 + \dots + a_n \chi_n = 0$  dengan  $a_i$  berindeks minimal yang tidak nol, misalkan  $m$ , yaitu

$$a_1\chi_1 + a_2\chi_2 + \dots + a_m\chi_m = 0.$$

Maka untuk sebarang  $g \in G$  diperoleh

$$a_1\chi_1(g) + a_2\chi_2(g) + \dots + a_m\chi_m(g) = 0. \quad (3)$$

Karena  $\chi_1 \neq \chi_m$ , diberikan  $g_0$  adalah suatu elemen dengan  $\chi_1(g_0) \neq \chi_m(g_0)$ . Selanjutnya, karena persamaan (3) dipenuhi, diperoleh

$$a_1\chi_1(g_0g) + a_2\chi_2(g_0g) + \dots + a_m\chi_m(g_0g) = 0,$$

yaitu

$$a_1\chi_1(g_0)\chi_1(g) + a_2\chi_2(g_0)\chi_2(g) + \dots + a_m\chi_m(g_0)\chi_m(g) = 0. \quad (4)$$

Dari sini diperoleh bahwa:

$$[\chi_m(g_0) - \chi_1(g_0)]a_1\chi_1(g) + \dots + [\chi_m(g_0) - \chi_{m-1}(g_0)]a_{m-1}\chi_{m-1}(g) = 0.$$

Karena berlaku untuk setiap  $g \in G$ , dan karena koefisien pertama ternyata tidak nol dan relasi ini lebih pendek, maka timbul kontradiksi. Jadi,  $\chi_1, \chi_2, \dots, \chi_n$  bebas linear. ■

Suatu homomorfisma (field) injektif  $\sigma: K \rightarrow L$  disebut dengan embedding (penyisipan) dari  $K$  ke dalam  $L$ . Secara khusus,  $\sigma$  merupakan homomorfisma (grup) dari grup multiplikatif  $G = K^*$  ke grup multiplikatif  $L^*$ , jadi  $\sigma$  dapat dipandang sebagai karakter dari  $K^*$  dengan nilai di  $L$ .

**Akibat 4.4.** Jika  $\sigma_1, \sigma_2, \dots, \sigma_n$  adalah embedding-embedding yang berbeda dari field  $K$  ke field  $L$ , maka  $\sigma_1, \sigma_2, \dots, \sigma_n$  bebas linear sebagai fungsi pada  $K$ . Lebih khusus, setiap automorfisma yang berbeda dari field  $K$  adalah bebas linear sebagai fungsi pada  $K$ .

**Bukti:**

Diketahui  $\sigma_1, \sigma_2, \dots, \sigma_n$  adalah embedding yang berbeda dari field  $K$  ke field  $L$ , maka  $\sigma_1, \sigma_2, \dots, \sigma_n$  dapat dipandang sebagai karakter-karakter dari  $K^*$  dengan nilai di  $L$ . Berdasarkan Teorema 4.3 diperoleh bahwa  $\sigma_1, \sigma_2, \dots, \sigma_n$  bebas linear atas  $L$ . Karena  $\sigma_1, \sigma_2, \dots, \sigma_n$  homomorfisma injektif, maka  $\sigma_1, \sigma_2, \dots, \sigma_n$  bebas linear pada  $K$ . Lebih khusus lagi, jika  $\sigma_1, \sigma_2, \dots, \sigma_n$  adalah automorfisma dari  $K$ , maka masing-masing merupakan homomorfisma injektif dari  $K$  ke  $K$ , sehingga  $\sigma_1, \sigma_2, \dots, \sigma_n$  bebas linear pada  $K$ . ■

Selanjutnya, Akibat 4.4 di atas dapat digunakan untuk menunjukkan hubungan antara order dari subgrup dari grup automorfisma dari field  $K$  dan derajat dari extension atas fixed field-nya, seperti diberikan berikut ini.

**Teorema 4.5.** Diberikan  $G = \{\sigma_1 = 1, \sigma_2, \dots, \sigma_n\}$  subgrup dari grup automorfisma dari field  $K$ , diberikan fixed field  $F$ . Maka

$$[K : F] = |G| = n .$$

**Bukti:**

Misalkan  $[K : F] = m$ . Andaikan  $n > [K : F]$  dan misalkan  $\omega_1, \omega_2, \dots, \omega_m$  adalah basis untuk  $K$  atas  $F$ . Maka sistem persamaan:

$$\begin{aligned} \sigma_1(\omega_1)x_1 + \sigma_2(\omega_1)x_2 + \dots + \sigma_n(\omega_1)x_n &= 0 \\ &\vdots \\ \sigma_1(\omega_m)x_1 + \sigma_2(\omega_m)x_2 + \dots + \sigma_n(\omega_m)x_n &= 0 \end{aligned}$$

terdiri dari  $m$  persamaan dengan variabel  $x_1, x_2, \dots, x_n$ . Karena  $m < n$ , maka terdapat solusi non-trivial  $\beta_1, \beta_2, \dots, \beta_n$  di  $K$ . Diberikan sebarang  $a_1, a_2, \dots, a_m \in F$ . Diketahui  $F$  fixed field oleh  $\sigma_1, \sigma_2, \dots, \sigma_n$ , yaitu  $\sigma_i(a_j) = a_j$ ,  $i = 1, 2, \dots, n$ ,  $j = 1, 2, \dots, m$ . Selanjutnya, dengan mengalikan persamaan pertama dengan  $a_1$ , persamaan kedua dengan  $a_2$ , dan seterusnya sampai persamaan ke- $m$  dengan  $a_m$ , maka diperoleh sistem persamaan:

$$\begin{aligned} \sigma_1(a_1\omega_1)x_1 + \sigma_2(a_1\omega_1)x_2 + \dots + \sigma_n(a_1\omega_1)x_n &= 0 \\ &\vdots \\ \sigma_1(a_m\omega_m)x_1 + \sigma_2(a_m\omega_m)x_2 + \dots + \sigma_n(a_m\omega_m)x_n &= 0 \end{aligned}$$

Selanjutnya, dengan menjumlahkan semua persamaan, maka terdapat  $\beta_1, \beta_2, \dots, \beta_n$  yang tidak semuanya nol sehingga memenuhi:

$$\sigma_1(a_1\omega_1 + \dots + a_m\omega_m)\beta_1 + \sigma_2(a_1\omega_1 + \dots + a_m\omega_m)\beta_2 + \dots + \sigma_n(a_1\omega_1 + \dots + a_m\omega_m)\beta_n = 0 ,$$

untuk setiap  $a_1, a_2, \dots, a_m \in F$ . Karena  $\omega_1, \omega_2, \dots, \omega_m$  adalah  $F$ -basis untuk  $K$ , maka untuk setiap  $\alpha \in K$  dapat dinyatakan dengan  $a_1\omega_1 + a_2\omega_2 + \dots + a_m\omega_m$ , sehingga dari persamaan sebelumnya diperoleh

$$\sigma_1(\alpha)\beta_1 + \sigma_2(\alpha)\beta_2 + \dots + \sigma_n(\alpha)\beta_n = 0 .$$

Dari sini diperoleh bahwa automorfisma yang saling berbeda  $\sigma_1, \sigma_2, \dots, \sigma_n$  tidak bebas linear atas  $K$ . Timbul kontradiksi dengan Akibat 4.4.

Andaikan  $n < [K : F]$ , maka terdapat lebih dari  $n$  elemen yang bebas linear atas  $K$ , misalkan elemen-elemen tersebut adalah  $\alpha_1, \dots, \alpha_n, \alpha_{n+1}$ . Pandang sistem yang terdiri dari  $n$  persamaan dan variabel  $x_1, \dots, x_n, x_{n+1}$  berikut

$$\begin{aligned} \sigma_1(\alpha_1)x_1 + \dots + \sigma_1(\alpha_n)x_n + \sigma_1(\alpha_{n+1})x_{n+1} &= 0 \\ &\vdots \\ \sigma_n(\alpha_1)x_1 + \dots + \sigma_n(\alpha_n)x_n + \sigma_n(\alpha_{n+1})x_{n+1} &= 0 \end{aligned} \quad (5)$$

Sistem tersebut mempunyai solusi non-trivial  $\beta_1, \dots, \beta_n, \beta_{n+1}$  di  $K$  dimana terdapat  $\beta_i$  yang tidak nol. Jika semua solusi  $\beta_1, \dots, \beta_n, \beta_{n+1}$  di  $F$ , karena  $\sigma_1 = 1$  yaitu automorfisma identitas, maka  $\alpha_1, \dots, \alpha_n, \alpha_{n+1}$  tidak bebas linear atas  $F$ . Diperoleh bahwa  $\beta_1, \dots, \beta_n, \beta_{n+1}$  bukan elemen dari  $F$ . Selanjutnya pandang semua solusi  $\beta_1, \dots, \beta_n, \beta_{n+1}$  dari sistem (5), pilih dengan solusi dengan banyaknya elemen yang tidak nol-nya minimal, misalkan  $\beta_1, \dots, \beta_r$  tidak nol. Dengan membagi persamaan-persamaan dengan  $\beta_r$ , dapat diasumsikan  $\beta_r = 1$ . Telah diketahui bahwa paling sedikit ada satu dari  $\beta_1, \dots, \beta_{r-1}, 1$  yang bukan elemen dari  $F$ , misalkan  $\beta_1 \notin F$ . Maka sistem di atas dapat ditulis sebagai berikut

$$\begin{aligned} \sigma_1(\alpha_1)\beta_1 + \dots + \sigma_1(\alpha_{r-1})\beta_{r-1} + \sigma_1(\alpha_r) &= 0 \\ &\vdots \\ \sigma_n(\alpha_1)\beta_1 + \dots + \sigma_n(\alpha_{r-1})\beta_{r-1} + \sigma_n(\alpha_r) &= 0 \end{aligned} \quad (6)$$

atau dapat ditulis dengan

$$\sigma_i(\alpha_1)\beta_1 + \dots + \sigma_i(\alpha_{r-1})\beta_{r-1} + \sigma_i(\alpha_r) = 0, \quad i = 1, 2, \dots, n \quad (7)$$

Karena  $\beta_1 \notin F$ , maka terdapat automorfisma  $\sigma_{k_0}$ ,  $1 \leq k_0 \leq n$  dengan  $\sigma_{k_0}(\beta_1) \neq \beta_1$ . Jika diterapkan pada persamaan (6), diperoleh sistem persamaan:

$$\sigma_{k_0}\sigma_j(\alpha_1)\sigma_{k_0}(\beta_1) + \dots + \sigma_{k_0}\sigma_j(\alpha_{r-1})\sigma_{k_0}(\beta_{r-1}) + \sigma_{k_0}\sigma_j(\alpha_r) = 0 \quad (8)$$

untuk  $j = 1, 2, \dots, n$ . Akan tetapi, karena  $\{\sigma_{k_0}\sigma_1, \sigma_{k_0}\sigma_2, \dots, \sigma_{k_0}\sigma_n\}$  sama dengan  $\{\sigma_1, \sigma_2, \dots, \sigma_n\}$  grup, maka persamaan (8) dapat ditulis dengan:

$$\sigma_i(\alpha_1)\sigma_{k_0}(\beta_1) + \dots + \sigma_i(\alpha_{r-1})\sigma_{k_0}(\beta_{r-1}) + \sigma_i(\alpha_r) = 0,$$

dan dengan mengurangi persamaan (7) dapat diperoleh:

$$\sigma_i(\alpha_1)[\beta_1 - \sigma_{k_0}(\beta_1)] + \dots + \sigma_i(\alpha_{r-1})[\beta_{r-1} - \sigma_{k_0}(\beta_{r-1})] = 0$$

untuk  $i = 1, 2, \dots, n$ . Diperoleh bahwa masing-masing  $x_i = \beta_i - \sigma_{k_0}(\beta_i)$  merupakan solusi dari sistem persamaan (5) dan  $x_1 = \beta_1 - \sigma_{k_0}(\beta_1)$  tidak nol. Oleh karena itu, solusi tersebut

non-trivial dan terdapat kurang dari  $r$  elemen  $x_i$  tidak nol. Timbul kontradiksi bahwa minimal ada sebanyak  $r$  elemen solusi yang tidak nol. Akibatnya, kedua pengandaian di atas salah, yaitu  $n \not\leq [K:F]$  dan  $n \not\geq [K:F]$ . Jadi, terbukti bahwa  $[K:F] = n$ . ■

**Akibat 4.6.** Diberikan extension berhingga  $K/F$ . Maka

$$|\text{Aut}(K/F)| \leq [K:F],$$

dan bernilai sama jika dan hanya jika  $F$  merupakan fixed field dari  $\text{Aut}(K/F)$ . Atau ekuivalen dengan mengatakan bahwa  $K/F$  merupakan Galois jika dan hanya jika  $F$  merupakan fixed field dari  $\text{Aut}(K/F)$ .

**Bukti:**

Berdasarkan Proposisi 3.8, diperoleh bahwa  $|\text{Aut}(K/F)| \leq [K:F]$ . Misalkan  $L$  adalah fixed field dari  $\text{Aut}(K/F)$ , maka  $F \subseteq L \subseteq K$ , sehingga  $[K:F] = [K:L][L:F]$ . Menggunakan Teorema 4.5 diperoleh bahwa  $|\text{Aut}(K/F)| = [K:L]$ , Akibatnya, diperoleh bahwa  $[K:F] = |\text{Aut}(K/F)|[L:F]$ . ■

**Akibat 4.7.** Diberikan  $G$  adalah subgroup hingga dari suatu grup automorfisma dari field  $K$ , diberikan  $F$  adalah fixed field dari  $G$ . Maka setiap automorfisma dari  $K$  yang fix  $F$  termuat di  $G$ , yaitu  $\text{Aut}(K/F) = G$ , atau dengan kata lain  $K/F$  merupakan Galois, dengan  $G$  adalah grup Galois-nya.

**Bukti:**

Diketahui  $G \leq \text{Aut}(K)$  dan  $F$  adalah fixed field dari  $G$ , maka  $G \leq \text{Aut}(K/F)$ . Oleh karena itu,  $|G| \leq |\text{Aut}(K/F)|$ . Berdasarkan Teorema 4.5 diperoleh  $|G| = [K:F]$ , dan dari Akibat 4.6 diperoleh  $|\text{Aut}(K/F)| \leq [K:F]$ . Akibatnya

$$[K:F] = |G| \leq |\text{Aut}(K/F)| \leq [K:F].$$

Dari sini diperoleh bahwa  $|G| = |\text{Aut}(K/F)|$ . Karena  $G \leq \text{Aut}(K)$ , maka terbukti bahwa  $\text{Aut}(K/F) = G$ . Jadi,  $K/F$  Galois, dan  $G$  merupakan grup Galois dari  $K/F$ . ■

**Akibat 4.8.** Jika  $G_1$  dan  $G_2$  adalah subgrup hingga yang berbeda dari grup automorfisma dari field  $K$ , maka fixed field dari  $G_1$  dan  $G_2$  juga berbeda.

**Bukti:**

Akan dibuktikan menggunakan kontraposisi. Misalkan  $F_1$  adalah fixed field dari  $G_1$ , dan  $F_2$  adalah fixed field dari  $G_2$ . Misalkan  $F_1 = F_2$ , maka  $F_1$  fix oleh  $G_2$ . Berdasarkan Akibat 4.7, setiap automorfisma yang fix  $F_1$  termuat di  $G_1$ , diperoleh  $G_2 \leq G_1$ . Selanjutnya, setiap automorfisma yang fix  $F_2$  termuat di  $G_2$ , diperoleh  $G_1 \leq G_2$ . Jadi,  $G_1 = G_2$ . ■

Berdasarkan Akibat-akibat di atas, dapat dilihat bahwa pengambilan fixed field untuk subgrup-subgrup yang berbeda dari  $\text{Aut}(K)$  memberikan subfield-subfield yang berbeda dari  $K$ . Lebih lanjut, derajat dari extension-nya dapat ditentukan melalui order dari subgrup-subgrup-nya.

**Teorema 4.9.** Suatu extension  $K/F$  merupakan Galois jika dan hanya jika  $K$  merupakan splitting field dari suatu polinomial separabel atas  $F$ . Lebih lanjut, setiap polinomial ireduisibel atas  $F$  yang mempunyai akar di  $K$  merupakan polinomial separabel dan semua akar-akarnya termuat di  $K$ , yaitu  $K/F$  merupakan extension separabel.

**Bukti:**

Dari Proposisi 3.8 diketahui bahwa splitting field dari suatu polinomial separabel merupakan Galois. Akan ditunjukkan bahwa jika  $K/F$  Galois, maka setiap polinomial ireduisibel  $p(x) \in F[x]$  yang mempunyai akar di  $K$  terfaktorkan secara penuh (splits completely) di  $K$ .

Misalkan  $G = \text{Gal}(K/F) = \{\sigma_1 = 1, \sigma_2, \dots, \sigma_n\}$ . Diberikan  $\alpha \in K$  adalah akar dari  $p(x)$ . Pandang elemen-elemen

$$\alpha, \sigma_2(\alpha), \dots, \sigma_n(\alpha) \in K. \quad (9)$$

Misalkan  $\alpha, \alpha_2, \dots, \alpha_r$  adalah elemen-elemen yang saling berbeda dari (9). Jika  $\tau \in G$ , maka  $\{\tau, \tau\sigma_2, \dots, \tau\sigma_n\} = G$ , yaitu  $\tau$  dapat dipandang sebagai permutasi pada  $G$ . Selanjutnya, gunakan permutasi tersebut pada (9). Diberikan polinomial

$$f(x) = (x - \alpha)(x - \alpha_2) \cdots (x - \alpha_r)$$

mempunyai koefisien-koefisien yang fix oleh setiap elemen dari  $G$ , sebab setiap elemen dari  $G$  mempermutasikan faktor-faktor dari  $f(x)$ . Oleh karena itu, koefisien-koefisien tersebut termuat di fixed field dari  $G$ , berdasarkan Akibat 4.6, fixed field dari  $G$  tersebut adalah  $F$ . Diperoleh bahwa  $f(x) \in F[x]$ .

Diketahui  $p(x)$  ireduksibel dan mempunyai akar  $\alpha$ , maka  $p(x)$  merupakan polinomial minimal untuk  $\alpha$  atas  $F$ , oleh karena itu  $p(x)$  membagi setiap polinomial atas  $F$  yang mempunyai  $\alpha$  sebagai akarnya. Akibatnya,  $p(x)$  membagi  $f(x)$  di  $F[x]$ , dan karena  $f(x)$  membagi  $p(x)$  di  $K[x]$ , berdasarkan Proposisi 3.4 diperoleh bahwa

$$p(x) = f(x).$$

Selanjutnya, misalkan  $K/F$  Galois dan  $\{\omega_1, \omega_2, \dots, \omega_n\}$  basis untuk  $K/F$ . Diberikan  $p_i(x)$  adalah polinomial minimal untuk  $\omega_i$  atas  $F$ , dengan  $i = 1, 2, \dots, n$ . Maka  $p_i(x)$  separabel dan akar-akarnya termuat di  $K$ . Misalkan  $g(x)$  adalah polinomial yang diperoleh dengan menghilangkan faktor yang sama pada perkalian  $p_1(x)p_2(x)\cdots p_n(x)$ . Maka splitting field dari  $g(x)$  dan  $p_1(x)p_2(x)\cdots p_n(x)$  sama, yaitu  $K$ . Jadi,  $K$  merupakan splitting field dari polinomial separabel  $g(x)$ , atau  $K/F$  merupakan extension separabel. ■

**Definisi 4.10.** (*Konjugat Galois*) Diberikan Galois extension  $K/F$ . Jika  $\alpha \in K$ , maka suatu elemen  $\sigma\alpha$  untuk  $\sigma \in \text{Gal}(K/F)$  disebut dengan *konjugat (konjugat Galois)* dari  $\alpha$  atas  $F$ . Jika  $E$  merupakan subfield dari  $K$  yang memuat  $F$ , maka field  $\sigma(E)$  disebut dengan *field konjugat* dari  $E$  atas  $F$ .

**Teorema 4.11.** (*Teorema Fundamental Teori Galois*) Diberikan suatu Galois extension  $K/F$ , misalkan  $G = \text{Gal}(K/F)$ . Maka terdapat suatu korespondensi 1-1 (bijeksi)

$$\{E \mid E \text{ subfield } K \text{ dan } F \subseteq E\} \longleftrightarrow \{H \mid H \leq G\}$$

$$\left\{ \begin{array}{c} K \\ | \\ E \\ | \\ F \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} 1 \\ | \\ H \\ | \\ G \end{array} \right\}$$

dengan definisi:

$$E \longrightarrow H = \{x \in G \mid x \text{ fix } E\}$$

$$\{E \mid E \text{ fixed field dari } H\} \longleftarrow H .$$

- (1) Diberikan  $E_1, E_2$  subfield dari  $K$  yang memuat  $F$ . Jika  $E_1$  berkorespondensi dengan  $H_1$ , dan  $E_2$  berkorespondensi dengan  $H_2$ , maka  $E_1 \subseteq E_2$  jika dan hanya jika  $H_2 \leq H_1$ .
- (2)  $[K : E] = |H|$  dan  $[E : F] = |G : H|$  (yaitu indeks dari  $H$  pada  $G$ ), jika ditulis dalam bentuk diagram:

$$\begin{array}{c} K \\ | \quad \} \quad |H| \\ E \\ | \quad \} \quad |G : H| \\ F \end{array}$$

- (3)  $K/E$  merupakan Galois, dengan  $\text{Gal}(K/E) = H$ , yaitu:

$$\begin{array}{c} K \\ | \quad H \\ E \end{array}$$

- (4)  $E$  Galois atas  $F$  jika dan hanya jika  $H$  subgrup normal di  $G$ . Jika berlaku demikian, maka:

$$\text{Gal}(E/F) \cong G/H .$$

- (5) Jika  $E_1$  berkorespondensi dengan  $H_1$ , dan  $E_2$  berkorespondensi dengan  $H_2$ , maka  $E_1 \cap E_2$  berkorespondensi dengan  $\langle H_1, H_2 \rangle$ , yaitu grup yang dibangun oleh  $H_1$  dan  $H_2$ . Oleh karena itu, lattice dari subfield-subfield dari  $K$  yang memuat  $F$  dengan lattice dari subgrup-subgrup dari  $G$  bersifat dual.

**Bukti:**

Diberikan sebarang  $H$  subgrup dari  $G$ . Berdasarkan Akibat 4.8, dapat ditentukan dengan tunggal fixed field  $E = K_H$ . Jadi, korespondensi bersifat injektif dari kiri ke kanan. Jika  $K$  merupakan splitting field dari polinomial separabel  $f(x) \in F[x]$ , maka  $f(x)$  dapat dipandang sebagai elemen dari  $E[x]$ , dengan  $E$  sebarang subfield dari  $K$  yang memuat  $F$ . Maka  $K$  merupakan splitting field dari  $f(x)$  atas  $E$ . Jadi, extension  $K/E$  merupakan Galois. Menggunakan Akibat 4.6, maka  $E$  merupakan fixed field dari  $\text{Aut}(K/E)$  yang

merupakan subgrup dari  $G$ . Diperoleh bahwa setiap subfield dari  $K$  yang memuat  $F$  berkorespondensi dengan suatu subgrup dari  $G$ . Jadi, korespondensi bersifat surjektif dari kanan ke kiri. Jadi, korespondensi tersebut merupakan suatu bikejsi (pemetaan bijektif).

(1) Diketahui  $E_1, E_2$  subfield dari  $K$  yang memuat  $F$ . Jika  $E_1$  berkorespondensi dengan  $H_1$ , dan  $E_2$  berkorespondensi dengan  $H_2$ . Misalkan  $E_1 \subseteq E_2$ , berdasarkan Proposisi 3.7(1), maka  $H_2 = \text{Aut}(K/E_2) \leq \text{Aut}(K/E_1) = H_1$ . Selanjutnya, misalkan  $H_2 \leq H_1$ , maka berdasarkan Proposisi 3.7(2), diperoleh  $E_1 \subseteq E_2$ .

(2) Diketahui  $G = \text{Gal}(K/F)$ . Misalkan  $E$  adalah fixed field dari subgrup  $H$ . Berdasarkan Teorema 4.5 diperoleh bahwa  $[K:E] = |H|$  dan  $[K:F] = |G|$ . Karena  $[K:F] = [K:E][E:F]$ , maka  $[E:F] = |G:H|$ .

(3) Pernyataan (3) terbukti berdasarkan Akibat 4.7.

(4) Misalkan  $E$  adalah fixed field dari subgrup  $H$ . Diketahui bahwa setiap  $\sigma \in G$  dapat dipandang sebagai embedding dari  $E$  ke subfield  $\sigma(E)$  dari  $K$ . Sebaliknya, diberikan  $\tau: E \xrightarrow{\sim} \tau(E) \subseteq \bar{F}$  sebarang embedding dari  $E$  ke suatu algebraic closure  $\bar{F}$  dari  $F$  yang memuat  $K$  serta fix  $F$ . Maka  $\tau(E)$  termuat di  $K$ . Jika  $\alpha \in E$  mempunyai polinomial minimal  $m_\alpha(x)$  atas  $F$ , maka  $\tau(\alpha)$  merupakan akar yang lain dari  $m_\alpha(x)$ , dari Teorema 4.9 diperoleh bahwa  $K$  memuat semua akar-akar dari  $m_\alpha(x)$ . Diketahui  $K$  adalah splitting field dari  $f(x)$  atas  $E$  dan juga merupakan splitting field dari  $\tau f(x)$  atas  $\tau(E)$ . Maka  $\tau$  dapat diperluas menjadi suatu isomorfisma  $\sigma$ , yaitu:

$$\begin{array}{ccc} \sigma: & K & \xrightarrow{\sim} & K \\ & | & & | \\ \tau: & E & \xrightarrow{\sim} & \tau(E) \end{array}$$

Karena  $\sigma$  fix  $F$ , maka setiap embedding  $\tau$  dari  $E$  yang fix  $F$  merupakan batas untuk  $E$  dari suatu automorfisma  $\sigma$  dari  $K$  yang fix  $F$ , atau dengan kata lain, setiap embedding dari  $E$  ditentukan oleh suatu  $\sigma \in G$ .

Misalkan  $\text{Emb}(E/F)$  menotasikan himpunan semua embedding dari  $E$  ke suatu algebraic closure dari  $F$  yang fix  $F$ . Diberikan automorfisma  $\sigma, \sigma' \in G$ . Maka  $\sigma$  dan  $\sigma'$  membatasi embedding yang sama dari  $E$  jika dan hanya jika  $\sigma^{-1}\sigma' = 1$  yaitu pemetaan identitas di  $E$ . Karena automorfisma dari  $K$  yang fix  $E$  merupakan elemen  $H$ , maka

$\sigma^{-1}\sigma' \in H$ . Oleh karena itu, embedding-embedding yang berbeda dari  $E$  termuat di bijeksi di atas dengan koset-koset  $\sigma H$  dari  $H$  di  $G$ . Sehingga diperoleh

$$|\text{Emb}(E/F)| = |G:H| = [E:F].$$

Perhatikan bahwa  $\text{Emb}(E/F)$  memuat grup automorfisma  $\text{Aut}(E/F)$ . Diketahui bahwa extension  $E/F$  Galois jika dan hanya jika  $|\text{Aut}(E/F)| = [E:F]$ . Berdasarkan persamaan sebelumnya, hal ini berlaku jika dan hanya jika embedding dari  $E$  merupakan suatu automorfisma dari  $E$ , yaitu  $\sigma(E) = E$  untuk setiap  $\sigma \in G$ .

Jika  $\sigma \in G$ , maka subgrup dari  $G$  yang fix  $\sigma(E)$  merupakan grup  $\sigma H \sigma^{-1}$ . Misalkan  $\sigma \alpha \in \sigma(E)$ , maka

$$(\sigma h \sigma^{-1})(\sigma \alpha) = \sigma(h\alpha) = \sigma \alpha, \text{ untuk setiap } h \in H.$$

Karena  $h$  fix  $\alpha \in E$ , maka  $\sigma H \sigma^{-1}$  fix  $\sigma(E)$ . Suatu grup yang fix  $\sigma(E)$  mempunyai order sama dengan derajat dari extension  $K$  atas  $\sigma(E)$ . Karena  $\sigma(E)$  dan  $E$  isomorfis, maka  $[K:E] = [K:\sigma(E)]$ . Akibatnya,  $|H| = [K:\sigma(E)]$ . Oleh karena itu,  $\sigma H \sigma^{-1}$  merupakan grup yang fix  $\sigma(E)$ .

Dua subfield dari  $K$  yang memuat  $F$  adalah sama jika dan hanya jika subgrup fix-nya sama. Oleh karena itu,  $\sigma(E) = E$ , untuk setiap  $\sigma \in G$  jika dan hanya jika  $\sigma H \sigma^{-1} = H$ . Dengan kata lain,  $E$  merupakan Galois atas  $F$  jika dan hanya jika  $H$  merupakan subgrup normal dari  $G$ .

Dari sini dapat dilihat bahwa suatu embedding dari  $E$  atas  $F$  dapat dipandang sebagai himpunan koset-koset dari  $H$  di  $G$ , dan jika  $H$  subgrup normal, maka embedding-embedding tersebut merupakan automorfisma. Himpunan dari koset-koset tersebut memnentuk grup  $G/H$ , oleh karena itu jika  $H$  subgrup normal, maka diperoleh bahwa

$$G/H \cong \text{Gal}(E/F).$$

- (5) Misalkan  $H_1$  adalah subgrup dari  $G$  yang fix subfield  $E_1$ , dan  $H_2$  adalah subgrup dari  $G$  yang fix subfield  $E_2$ . Maka sebarang elemen di  $H_1 \cap H_2$  fix  $E_1$  dan  $E_2$ , akibatnya fix juga pada setiap kombinasi dari elemen-elemen  $E_1$  dan  $E_2$ , yang berakibat bahwa fix pada setiap elemen di  $E_1 E_2$ . Selanjutnya, jika suatu automorfisma  $\sigma$  fix  $E_1 E_2$ , maka  $\sigma$  fix  $E_1$ , yaitu  $\sigma \in H_1$ , dan  $\sigma$  fix  $E_2$ , yaitu  $\sigma \in H_2$ , diperoleh bahwa  $\sigma \in H_1 \cap H_2$ . Jadi,  $E_1 E_2$  berkorespondensi dengan  $H_1 \cap H_2$ . Dengan cara yang sama diperoleh bahwa

$H_1 \cap H_2$  berkorespondensi dengan  $\langle H_1, H_2 \rangle$ , yaitu grup yang dibangun oleh  $H_1$  dan  $H_2$ . ■

**Contoh.**

Diketahui splitting field untuk polinomial ireduisibel  $x^3 - 2$  atas  $\mathbb{Q}$  berderajat 6. Akar-akarnya adalah  $\sqrt[3]{2}, \rho\sqrt[3]{2}, \rho^2\sqrt[3]{2}$  dengan  $\rho = \frac{-1 + \sqrt{-3}}{2}$ . Oleh karena itu splitting field dapat ditulis dengan  $\mathbb{Q}(\sqrt[3]{2}, \rho)$ . Sebarang automorfisma memetakan  $\sqrt[3]{2}, \rho\sqrt[3]{2}$  ke suatu akar dari  $x^3 - 2$ , sehingga diperoleh 9 kemungkinan. Akan tetapi, karena grup Galois hanya mempunyai order 6, maka tidak semua kemungkinan tersebut merupakan automorfisma. Misalkan

$$\sigma: \begin{cases} \sqrt[3]{2} \mapsto \rho\sqrt[3]{2} \\ \rho \mapsto \rho \end{cases} \qquad \tau: \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \rho \mapsto \rho^2 = -1 - \rho \end{cases}$$

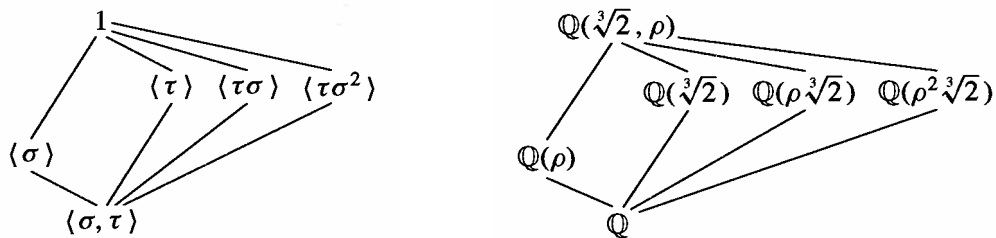
Dapat diperoleh bahwa

$$\text{Gal}(\mathbb{Q}(\sqrt[3]{2}, \rho)/\mathbb{Q}) = \langle \sigma, \tau \mid \sigma^3 = \tau^2 = 1 \rangle \cong S_3.$$

dengan korespondensi:

$$\begin{aligned} \mathbb{Q} &\longleftrightarrow \langle \sigma, \tau \rangle \\ \mathbb{Q}(\rho) &\longleftrightarrow \langle \sigma \rangle \\ \mathbb{Q}(\sqrt[3]{2}) &\longleftrightarrow \langle \tau \rangle \\ \mathbb{Q}(\rho\sqrt[3]{2}) &\longleftrightarrow \langle \tau\sigma \rangle \\ \mathbb{Q}(\rho^2\sqrt[3]{2}) &\longleftrightarrow \langle \tau\sigma^2 \rangle \\ \mathbb{Q}(\sqrt[3]{2}, \rho) &\longleftrightarrow 1 \end{aligned}$$

Selanjutnya, dapat diperoleh diagram latris:



Dapat dilihat bahwa latris dari kedua diagram diatas saling dual.

## 5. Penutup

Dari semua penjelasan di atas, diperoleh empat cara untuk mengkarakterisasi dari suatu Galois extension  $K/F$ , yaitu melalui:

- (1) suatu splitting field dari polinomial separabel atas  $F$
- (2) suatu field dimana  $F$  merupakan himpunan semua elemen yang fix oleh  $\text{Aut}(K/F)$
- (3) suatu field dengan  $[K:F] = |\text{Aut}(K/F)|$
- (4) suatu extension berhingga, normal, dan separabel.

Diberikan suatu Galois extension  $K/F$ , misalkan  $G = \text{Gal}(K/F)$ . Maka terdapat suatu bijeksi

$$\{E \mid E \text{ subfield } K \text{ dan } F \subseteq E\} \longleftrightarrow \{H \mid H \leq G\}$$

dengan definisi  $E \longmapsto H = \{x \in G \mid x \text{ fix } E\}$  dan  $\{E \mid E \text{ fixed field dari } H\} \longleftarrow H$ .

- (1) Diberikan  $E_1, E_2$  subfield dari  $K$  yang memuat  $F$ . Jika  $E_1$  berkorespondensi dengan  $H_1$ , dan  $E_2$  berkorespondensi dengan  $H_2$ , maka  $E_1 \subseteq E_2$  jika dan hanya jika  $H_2 \leq H_1$ .
- (2)  $[K:E] = |H|$  dan  $[E:F] = |G:H|$  (yaitu indeks dari  $H$  pada  $G$ ).
- (3)  $K/E$  merupakan Galois, dengan  $\text{Gal}(K/E) = H$ .
- (4)  $E$  Galois atas  $F$  jika dan hanya jika  $H$  subgrup normal di  $G$ . Jika berlaku demikian, maka:

$$\text{Gal}(E/F) \cong G/H.$$

- (5) Jika  $E_1$  berkorespondensi dengan  $H_1$ , dan  $E_2$  berkorespondensi dengan  $H_2$ , maka  $E_1 \cap E_2$  berkorespondensi dengan  $\langle H_1, H_2 \rangle$ , yaitu grup yang dibangun oleh  $H_1$  dan  $H_2$ . Oleh karena itu, latis dari subfield-subfield dari  $K$  yang memuat  $F$  dengan latis dari subgrup-subgrup dari  $G$  bersifat dual, yaitu saling terbalik.

## Daftar Pustaka

Dummit, S., Foote, M., 2004, *Abstract Algebra, Third Edition*, New Jersey, John Wiley and Sons.

Fraleigh, J.B, 2000, *A First Course in Abstract Algebra, Sixth Edition*, USA, Addison-Wesley.