TENSOR Pure and Applied Mathematics Journal

April 2022 | Vol. 3 | No. 1 Halaman 49–56

p-ISSN: 2723-0325 e-ISSN: 2723-0333

Kajian Grup Galois Isomorfis dengan Grup Alternating A_5

Fandy Sanudin[1], Henry W. M. Patty [1*], F. Y. Rumlawang[1], Dyana Patty[1]

[1] Jurusan Matematika FMIPA Universitas Pattimura, Jl. Ir. M. Putuhena, Ambon. Indonesia

*Email: henrywmpatty81@gmail.com

Manuscript submitted : Maret 2022;
Accepted for publication : April 2022.
doi : https://doi.org/10.30598/tensorvol3iss1pp49-56

Abstract: Let a trinomial $f(x) = x^5 + ax + b \in F[x]$ and irreducible over F so that an extension field E is formed where $F \subset E$ and E contain the area of the roots of $f(x)$. Furthermore, E is the splitting field of $f(x)$ if it contains a linear factor of $f(x)$ or in other words, E is the smallest wide field that only contains F and the roots of $f(x)$. In the splitting field E containing the roots of $f(x)$ there is an automorphism of E namely $\sigma: E \to E$ such that $\sigma(a) = a$ for each $a \in F$ which is an automorphism identity at F. The collection of all automorphisms are formed into a group by an operation called the Galois group, denoted by $Gal\,(E/F)$ or $gal(f(x))$. Obtaining a Galois group $f(x)$ is the same as constructing a subgroup of a symmetric group S_5 which is an alternating group A_5.

2010 Mathematical Subject Classification : 11R32, 13B05
Keywords:. alternating group, extension field, galois group, splitting field.

1. Pendahuluan

Teori galois adalah salah satu cabang dari aljabar abstrak yang menghubungkan antara teori lapangan dan teori grup dengan mereduksi masalah lapangan menjadi teori grup. Grup ini merupakan hasil pemikiran dari *Evariete Galois* (1811-1832). Untuk menghargai ide dan hasil kerjanya grup ini diberi nama grup galois. Motivasi dari grup galois adalah pencarian solusi dari persamaan polinomial berderajat lebih dari 4. *Evariete Galois* memberikan kriteria untuk penyelesaian persamaan polinomial tertentu dalam hal ini grup simetri S_n adalah akar atau solusinya.

Grup galois yang dinotasikan dengan $gal(f(x)$, merupakan grup yang memuat semua automorfisma dari lapangan pemisah yang identitasnya berada pada lapangan dari suatu polinomial $f(x)$. Menentukan suatu grup galois $gal(f(x))$ sama halnya dengan menentukan subgrup dari suatu grup simetri yang bersesuaian, sehingga grup galois, $gal\big(f(x)\big)$, isomorfis dengan subgrup dari grup simetri S_n yang disebut sebagai grup alternating. Grup alternating adalah grup yang memuat semua permutasi genap dari grup simetri S_n yang dinotasikan dengan A_n. Karena banyaknya penelitian yang membahas tentang subgrup dari grup simetri hanya sampai pada grup simetri S_4 dikarenakan semakin besar nilai n maka semakin banyak elemen maka dari itu polinomial yang akan dibahas pada tulisan ini ialah polinomial berderajat 5 sehingga

untuk mencari akar-akar dari suatu persamaan polinomial berderajat 5 sama halnya dengan menentukan subgrup dari grup simetri S_5.

Diberikan F adalah lapangan dan $f(x) \in F[x]$ yang mana $f(x)$ tak tereduksi atas $F[x]$ maka akar-akar dari polinomial $f(x)$ dapat dicari pada dengan membentuk suatu lapangan perluasan yang mana memuat akar-akar dari $f(x)$ sebelum selanjutnya membentuk lapangan pemisah dan grup galois dari $f(x)$, akar dari $f(x)$ dapat dicari dengan menghitung grup alternating A_5 jika lapangan perluasan dari $f(x)$ isomorfis dengan A_5. Sehingga muncul pertanyaan bagaimana konstruksi lapangan perluasan dari $f(x)$, lapangan pemisah dari $f(x)$ serta bagaimana isomorfisma antara grup galois dari $f(x)$ dan grup alternating A_5.

2. Hasil dan Pembahasan

Penelitian ini mengacu pada jurnal *"Galois Groups As Permutation Groups"* oleh Keith Conrad [2] sedangkan dasar teori mengenai konsep dasar grup mengacu pada [8]. Untuk konsep dasar ring seperti ideal, homomorfisma, dan automorfisma mengacu pada [7]. Terkait dengan ring polinomial mengacu pada [4], selanjutnya untuk menjelaskan tentang pembagian dan tak tereduksi dari suatu polinomial mengacu pada [6]. Konsep dasar grup galois yang isomorfis dengan subgrup dari suatu grup simetri mengacu pada [3]. Adapun teori-teori dasar yang diperlukan adalah definisi dan sifat-sifat grup, grup komutatif, grup permutasi, grup simetris, grup alternating, subgrup, subgrup normal, ring, ring komutatif, homomorfisma ring, daerah integral, lapangan, serta ring polinomial.

2.1. Lapangan Perluasan dan Lapangan Pemisah

Pembentukan grup galois diawali dengan adanya suatu polinomial $f(x)$ yang tak tereduksi atas suatu lapangan, sehingga dibentuk suatu lapangan yang dapat memuat akar dari polinomial tersebut, dapat dilihat pada definisi berikut.

Definisi 1. [5] Misalkan F lapangan, dan diberikan suatu lapangan E, jika $F \subseteq E$ dan F memiliki operasi yang sama dengan E maka E disebut sebagai lapangan perluasan dari F.

Sehingga dapat dilihat bahwa F merupakan lapangan bagian dari E, atau sama halnya dengan menyatakan bahwa F merupakan perluasan terhadap F karena $F \subseteq F$, suatu lapangan perluasan E dari F dinotasikan sebagai E/F.

Contoh 2. Karena $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ maka $\mathbb{R}$ merupakan perluasan dari $\mathbb{Q}$ dan $\mathbb{C}$ merupakan perluasan dari $\mathbb{Q}$ dan $\mathbb{R}$

Misalkan diberikan $f(x) \in F[x]$ dimana $f(x)$ tak tereduksi atas $F[x]$ maka dapat terdapat suatu lapangan perluasan E yang memuat akar-akar dari $f(x)$ dapat dilihat pada teorema berikut ini.

Teorema 3. Jika F adalah lapangan dan $f(x) \in F(x)$ polinomial tak konstan, maka terdapat E memuat F dan suatu akar dari $f(x)$.

Bukti: Misalkan $f(x) = p(x)q(x)$ dengan $p(x)$ tak tereduksi atas F. Maka $F[x]/\langle p(x)\rangle = E$ lapangan yang memuat F. Misalkan $I = \langle p(x)\rangle$. Akan dibuktikan terdapat $\alpha = I + x \in E$ sehingga $p(\alpha) = 0$.
Misalkan $p(x) = a_0 + a_1x + \cdots + a_nx^n, a_i \in F$. Homomorfisma evaluasi $\theta_a: F[x] \to E$ memberikan

$$\theta_a\big(p(x)\big) = p(\alpha) = (I + a_0) + (I + a_1)\alpha + \cdots + (I + a_n)\alpha^n$$
$$= (I + a_0) + (I + a_1)(I + x) + \cdots + (I + a_n)(I + x)^n$$

$$= (I + a_0) + (I + a_1 x) + \cdots + (I + a_n x^n)$$
$$= I + (a_0 + a_1 x + \cdots + a_n x^n)$$
$$= I + p(x)$$
$$= I$$

Karena $I = I + 0$ adalah elemen identitas dalam E, maka $\alpha \in E$ adalah akar dari $p(x)$ ini artinya α adalah akar dari $f(x)$, jadi lapangan E memuat F dan suatu akar dari $f(x)$ ■

Berdasarkan Teorema 3 di atas dapat dapat disimpulkan bahwa setiap lapangan memiliki lapangan perluasan dan setiap polinomial tak konstan memiliki akar disuatu lapangan.

Contoh 4. Diberikan polinomial $f(x) = x^3 - 3x^2 + x - 3$ atas $\mathbb{Q}$.
Karena $x^3 - 3x^2 + x - 3 = (x^2 + 1)(x - 3) = 0$ diperoleh akar-akar dari polinomial $f(x)$ berada pada $\mathbb{C}$ yaitu $\pm i$ dan 3, maka lapangan perluasan dari polinomial $f(x)$ yaitu $\mathbb{C}$.

Setelah dibahas mengenai lapangan perluasan selanjutnya akan dibahas mengenai lapangan pemisah sebagai berikut.

Definisi 5. [5] Jika E suatu lapangan perluasan dari F dan $f(x) \in F[x]$ yang mana derajatnya paling kurang adalah 1. Maka $f(x)$ memisah di E jika terdapat $a \in F$ dan $a_1, a_2, \dots, a_n \in E$ sedemikian hingga $f(x) = a(x - a_1)(x - a_2) \dots (x - a_n)$. E adalah lapangan pemisah untuk $f(x)$ atas F adalah $E = F(a_1, a_2, \dots, a_n)$.

Suatu lapangan pemisah bergantung dari polinomial dan lapangan dari polinomialnya berada. Jika $f(x) \in F(x)$ dan $f(x)$ memisah atas E, maka dapat diambil suatu akar dari $f(x)$ dan digabungkan dengan F maka diperoleh lapangan perluasan $F(a)$, sehingga dapat dilihat bahwa lapangan pemisah E dari $f(x)$ atas F adalah lapangan perluasan terkecil dari F.

Contoh 6. Diberikan polinomial $f(x) = x^3 - 3x^2 + x - 3$ atas $\mathbb{Q}$ yang mana berdasarkan contoh 4.5 mempunyai akar yaitu $\pm i$ dan 3 maka lapangan pemisah dari $f(x)$ adalah $\mathbb{Q}(i)$ yang mana juga merupakan lapangan perluasan terkecil dari $f(x)$.

Selanjutnya akan ditunjukan eksistensi dari lapangan pemisah untuk setiap $f(x) \in F[x]$ dapat dilihat dalam teorema berikut ini:

Teorema 7. Misalkan F lapangan dan $f(x)$ adalah polinomial tak konstan di $F[x]$, maka terdapat suatu lapangan pemisah untuk $f(x)$ atas F.

Bukti:
Akan dibuktikan menggunakan induksi pada derajat dari $f(x)$.
Langkah basis: jika derajat dari $f(x)$ adalah 1 maka jelas bahwa pemisah sebagai $f(x)$ linear.
Langkah induksi:

- Asumsikan bahwa terdapat suatu lapangan pemisah untuk semua polinomal dengan derajat kurang dari $f(x)$ atas F, akan ditunjukan terdapat lapangan pemisah untuk derajat lebih dari atau sama dengan $f(x)$ atas F.
- Karena F memiliki lapangan perluasan dimana $f(x)$ memiliki elemen pembuat nol, misalkan a_1 sebagai elemen pembuat nol maka dapat ditulis $f(x)$ sebagai $(x - a_1)g(x)$, dimana $g(x) \in E[x]$. Karena $\deg g(x) < \deg f(x)$, maka berdasarkan asumsi diperoleh terdapat lapangan yang memuat E

dan semua elemen pembuat nol dari $g(x), a_2, \dots, a_n$. Jadi terdapat lapangan pemisah untuk f(x) atas F yaitu $F(a_1, a_2, \dots, a_n)$■

Sehingga dari teorema 7 diketahui bahwa setiap polinomial tak konstan $f(x) \in F[x]$ memiliki lapangan pemisah.

2.2 Lapangan Automorfisma

Telah diketahui bahwa automorfisma grup merupakan isomorfisma dengan domain dan kodomain yang sama, selanjutnya akan dibahas mengenai automorfisma dari suatu lapangan dan lapangan perluasan.

Definisi 8. [10] Suatu isomorfisma $\sigma: E \to E$ disebut automorfisma dari E, yang mana $\sigma: E \to E$ adalah pemetaan bijektif, yang memenuhi kondisi berikut:

$$\sigma(a+b) = \sigma(a) + \sigma(b)$$
$$\sigma(ab) = \sigma(a)\sigma(b)$$

Koleksi dari automorfisma dari E dinotasikan dengan $Aut(E)$.

Contoh 9. Sebarang lapangan memiliki paling kurang satu automorfisma yaitu pemetaan identitas dan dinotasikan dengan id yang disebut dengan automorfisma trivial. Kumpulan dari automorfisma pada suatu lapangan dengan operasi komposisi fungsi merupakan grup dengan operasi komposisi, selanjutnya akan dijelaskan automorfisma pada lapangan perluasan.

Definisi 10. [9] Diberikan $\sigma \in Aut(E)$ disebut elemen tetap, jika $\alpha \in F$, $\sigma(\alpha) = \alpha$. Jika $F \subset E$, maka isomorfisma σ disebut tetap di F jika semua elemen tetap di F yaitu $\sigma(\alpha) = \alpha$ untuk semua $\alpha \in F$. Suatu lapangan perluasan E/F, sehingga $Aut(E/F)$ dinotasikan sebagai himpunan dari semua automorfisma dari E dengan tetap di F.

Contoh 11. $Aut(\mathbb{Q}(\sqrt{3})/\mathbb{Q})$ adalah $\{id, \tau\}$ karena $\mathbb{Q}(\sqrt{3})$ adalah lapangan pemisah dari polinomial $x^2 - 3 \in \mathbb{Q}[x]$, yang mana akar-akarnya adalah $\pm\sqrt{3}$. Jika $\tau \in Aut(\mathbb{Q}(\sqrt{3})/\mathbb{Q})$, maka $\tau(\sqrt{3}) = \pm\sqrt{3}$ karena τ tetap di $\mathbb{Q}$,

$$\tau(a + b\sqrt{3}) = a \pm b\sqrt{3}.$$

Jika $\tau(a + b\sqrt{3}) = a + b\sqrt{3}$ maka $\tau = id$ dan ,
Jika $\tau(a + b\sqrt{3}) = a - b\sqrt{3}$ maka τ bukan automorfisma identitas.
Sehingga $Aut(\mathbb{Q}(\sqrt{3})/\mathbb{Q}) = \{id, \tau\}$ dimana $\tau: \sqrt{3} \to -\sqrt{3}$.

Setelah dibentuknya automorfisma pada lapangan perluasan maka selanjutnya akan dibentuk grup galois yang mana merupakan grup dari himpunan semua automorfima, untuk lebih jelasnya dapat dilihat dari definisi dan contoh berikut.

Definisi 12. [3] Diberikan $F \subset E$ lapangan perluasan. Maka $Gal(E/F)$ adalah himpunan

$$\{\sigma: E \to E \mid \sigma\ automorfima, \sigma(a) = a, untuk\ semua\ a \in F\}.$$

Dengan kata lain, $Gal(E/F)$ memuat semua automorfisma dari E yang mana identitasnya pada F.

Diperoleh struktur dasar dari $Gal(E/F)$ adalah grup dengan operasi komposisi.

Contoh 13. Fungsi $f(x) = x^2 + 1 \in \mathbb{Q}[x]$ memiliki grup galois yaitu $Gal\ (\mathbb{Q}(i)/\mathbb{Q}) = Gal(\mathbb{Q}(i))$, karena diketahui:

$x^2+1=\left(x+\sqrt{-1}\right)\left(x-\sqrt{-1}\right)=(x+i)(x-i)=0$ sehingga $x=\pm i$ yang tak tereduksi atas $\mathbb{Q}$, maka lapangan pemisah dari $f(x)$ adalah $\mathbb{Q}(i)$ yang terdiri dari dua automorfisma yaitu $\{id,\sigma\}$ yang mana:

$\sigma(i)=i$ merupakan automorfisma identitas sehingga $\sigma=id$, dan

$\sigma(i)=-i$ yang bukan merupakan automorfisma identitas.

2.3. Grup Galois Isomorfis dengan Grup Alternating A_5

Diberikan lapangan $E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$ yang mana merupakan lapangan pemisah dari $f(x)=(x-\alpha_1)\cdots(x-\alpha_n)\in F$. Setiap σ di grup galois dari $f(x)$ atas F yang merupakan automorfisma dari lapangan pemisah $E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$ ditentukan oleh permutasi α_i karena α_i menjadi generator untuk lapangan pemisah $E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$ atas F. Permutasi dari α_i dapat dilihat sebagai suatu permutasi dari $1,2,\cdots,n$.

Setelah dibangun beberapa contoh dari grup galois dapat diihat bahwa automorfisma dari lapangan pemisah atas suatu polinomial yang merupakan permutasi dari akar-akar suatu poinomial dalam lapangan pemisah sama halnya dengan menentukan subgrup simetri dari grup simetri S_n yaitu grup alternating A_n. Selanjutnya akan dilihat bagaimana isomorfisma antara grup gaois dengan grup alternating A_n lebih khusus untuk polinomial pangkat lima terhada grup alternating A_5. Sebelumnya akan dipekenalkan terlebih dahulu tentang diskriminan dari suatu polinomial yang mana menentukan suatu grup galois berada di A_n.

Definisi 14. [2] Diberikan suatu polinomial tak konstan $f(x)\in F[x]$ berderajat n bahwa faktor-faktor atas suatu lapangan pemisah sebagai

$$f(x)=c(x-r_1)\ldots(x-r_n),$$

Diskriminan dari $f(x)$ didefinisikan dengan

$$disc\, f=\prod_{i<j}\left(r_j-r_i\right)^2. \quad (1)$$

Contoh 15. Polinomial $(x-2)(x-5)(x-7)$ memiliki diskriminan yaitu $3^2\cdot 5^2\cdot 2^2=900$.

Contoh 16. Diskriminan dari $x^2+ax+b=(x-r)(x-r')$ adalah $(r-r')^2=r^2-2rr'+r'^2=(r+r')^2-4rr'=a^2-4b$, yang mana diskriminan merupakan diskriminan dari polinomial kuadrat monik.

Jika diskriminan dari suatu polinomial $f(x)\neq 0$ maka polinomial tersebut *separable*, jika diskriminan $f(x)=0$ maka polinomial tak *separable* dimana polinomial *separable* merupakan polinomial yang memiliki faktor linear yang berbeda sehingga mengakibatkan akar dari suatu polinomial juga berbeda-beda. Secara eksplisit formula untuk menyatakan diskriminan dari beberapa trinomial sebagai berikut:

$$disc\,(x^2+ax+b)=a^2-4b \quad (2)$$
$$disc\,(x^3+ax+b)=-4a^3-27b^2 \quad (3)$$
$$disc\,(x^4+ax+b)=-27a^4-256b^3 \quad (4)$$
$$disc\,(x^5+ax+b)=256a^5+3125b^4 \quad (5)$$

Selanjutnya untuk menyatakan suatau grup galois dilihat sebagai suatu subgrup dari grup S_n dapat dilihat pada teorema-teorema berikut ini:

Teorema 17. Diberikan polinomial *separable* $f(x) \in F[x]$ dengan derajat *n*. Jika F lapangan yang bukan berkarakteristik 2, penyisipan grup galois dari $f(x)$ atas *F* ke S_n sebagai permutasi-permutasi dari akar-akar $f(x)$ memiliki bayangan (*image*) di A_n jika dan hanya jika diskriminan f *square* di E.

Bukti: Diketahui f(x) polinomial *separable* maka diskriminan $f \neq 0$ sehingga, misalkan $\delta = \prod_{i<j}(r_j - r_i) \neq 0$ yang mana $\delta \in F(r_1, \cdots, r_n)$ dan $\delta^2 = diskriminan\, f \in F$. Untuk itu diskriminan f *square* di F jika dan hanya jika $\delta \in F$.
Untuk $\sigma \in Gal(F(r_1, \cdots, r_n)/F)$, diberikan $\varepsilon_\sigma = \pm 1$ adalah tanda sebagai suatu permutasi dari r_i. Berdasarkan salah satu dari definisi dari *sign* dari suatu permutasi,

$$\sigma(\delta) = \prod_{i<j}\big(\sigma(r_j) - \sigma(r_i)\big) = \varepsilon_\sigma \prod_{i<j}(r_j - r_i) = \varepsilon_\sigma \delta,$$

Jadi $\sigma(\delta) = \pm\delta$. Karena $\delta \neq 0$ dan F tak memiliki karakteristik 2, sehingga $\delta = -\delta$. Diperoleh $\delta \in A_n$ jika dan hanya jika $\varepsilon_\sigma = 1$, jadi $\sigma \in A_n$ jika dan hanya jika $\sigma(\delta) = \delta$. Maka dari itu grup galois dari $f(x)$ atas F di A_n jika dan hanya jika δ adalah elemen tetap dari grup galois yang mana sama dengan $\delta \in K$■

Berdasarkan teorema 17 dapat diperoleh untuk suatu polinomial $f(x)$ yang memiliki diskriminan *square* atau dapat dinyatakan dalam bilangan berpangkat maka memiki permutasi akar-akar atas suatu lapangan ke grup permutasi S_n memiiki bayangan pada grup alternating A_n hal ini berarti bahwa grup galois dari suatu polinomial $f(x)$ subgrup dari grup altenating A_n.

Selanjutnya teorema berikut menjelaskan tentang penggunaan faktorisasi dari polinomial $mod\, p$ yang mana suatu grup galois atas $\mathbb{Q}$ memuat permutasi dengan struktur perputaran tertentu.

Teorema 18. Diberikan $f(x) \in \mathbb{Z}[x]$ adalah polinomial monik tak tereduksi atas $\mathbb{Q}$ dengan derajat n. Untuk suatu bilangan prima p tak dapat membagi diskriminan f, diberikan suatu faktorisasi monik tak tereduksi dari $f(x)\ mod\ p$ menjadi

$$f(x) \equiv \pi_1(x) \cdots \pi_k(x)\ mod\ p$$

dan $d_i = \deg \pi_i(x)$, jadi $d_1 + \cdots + d_k = n$. Grup galois dari $f(x)$ atas $\mathbb{Q}$, terlihat sebagai suatu subgrup dari S_n, memuat permutasi dari $(d_1, \dots, d_k)$.

Bukti: Misalkan $E = \mathbb{Q}(r_1, r_2, \dots, r_n)$, $E_P = \mathbb{Z}(\bar{r}_1, \bar{r}_2, \dots, \bar{r}_n)$, $D = \mathbb{Z}(r_1, r_2, \dots, r_n)$ adalah subring yang dibangun oleh $r_1, r_2, \dots, r_n$ dari $f(x)$ di $\mathbb{C}$
Maka:

1. Terdapat suatu homomorfisma ψ dari D ke E_P.
2. Sebarang homomorfisma ψ memberikan pemetaan bijektif dari himpunan $\mathbb{R}$ dari akar-akar f(x) di E ke himpunan $\mathbb{R}_P$ dari akar-akar $f_p(x)$ di E_P.
3. Jika ψ dan ψ' dua homomorfisma maka terdapat $\sigma \in (E/\mathbb{Q}) = Gal(f(x))$, sedimikian hingga $\psi' = \psi \circ \sigma$ dimana σ ke D adal ah automorfisma dari D.

Karena lapangan E_P memiliki orde p^m, grup $Aut(E_P)$ memiliki orde m dan $\pi: E_P \longrightarrow E_P$, dimana $\pi(a) = a^p$ untuk semua $a \in E_P$ adalah automorfisma pembangun dari $Aut(E_P)$ jadi jika $\psi: D \to E_P$ adalah sebarang homomorfisma dari E ke E_P terdapat $\sigma \in Aut(E/\mathbb{Q})$ sedemikian hingga $\pi \circ \psi = \psi \circ \sigma$ atau $\psi' \circ \pi \circ \psi = \sigma$ hal ini menunjukan bahwa aksi σ pada $\{r_1, r_2, \dots, r_n\}$ sama halnya dengan aksi dari π pada $\{\bar{r}_1, \bar{r}_2, \dots, \bar{r}_n\}$.
Berdasarkan diagram dari pemetaan

$$D \xrightarrow{\sigma} D$$

Adalah pembatas dari $\sigma \in Aut(E/\mathbb{Q})$ ke D dan dapat dilihat efek dari pemetaan-pemetaan σ, ψ, dan π pada $\{r_1, r_2, \dots, r_n\}$ dan $\{\bar{r}_1, \bar{r}_2, \dots, \bar{r}_n\}$.

$$\{r_1, r_2, \dots, r_n\} \xrightarrow{\sigma} \{\bar{r}_1, \bar{r}_2, \dots, \bar{r}_n\}$$
$$\{\bar{r}_1, \bar{r}_2, \dots, \bar{r}_n\} \xrightarrow{\pi} \{\bar{r}_1, \bar{r}_2, \dots, \bar{r}_n\}$$
$$\{r_1, r_2, \dots, r_n\} \xrightarrow{\psi} \{\bar{r}_1, \bar{r}_2, \dots, \bar{r}_n\}$$

Dimana $\psi' \circ \pi \circ \psi = \sigma$ dan $\psi' \circ \sigma \circ \psi = \pi$ efek dari σ pada $\{r_1, r_2, \dots, r_n\}$ sama halnya dengan efek dari π pada $\{\bar{r}_1, \bar{r}_2, \dots, \bar{r}_n\}$. berikut ini adalah ilustrasi lebih lanjut:

$$\sigma(r_i) = r_j \Longrightarrow \pi(\bar{r}_i) = \bar{r}_j$$
$$\bar{r}_i \xrightarrow{\psi'} r_i \xrightarrow{\sigma} r_j \xrightarrow{\psi} \bar{r}_j$$
$$\pi(\bar{r}_i) = \bar{r}_j \Longrightarrow \sigma(r_i) = r_j$$
$$r_i \xrightarrow{\psi} \bar{r}_i \xrightarrow{\pi} r_j \xrightarrow{\psi'} \bar{r}_j \ \blacksquare$$

Pada teorema 18 dengan menggunakan faktorisasi dari polinomial $mod\ \ell$ yang mana memiliki semua akar akan tetapi tiga akar berada di F_ℓ untuk suatu ℓ sehingga berakibat suatu grup galois dapat isomorf ke grup alternating A_P, dapat dilihat pada akibat berikut.

Akibat 19. Diberikan $f(x) \in \mathbb{Z}[x]$ adalah polinomial monik tak tereduksi atas $\mathbb{Q}$ dengan derajat prima $p \geq 3$ dengan diskriminan *square.* Jika terdapat bilangan prima ℓ tak habis membagi diskriminan f sedemikian hingga $f(x)$ mod ℓ memiliki semua tetapi tiga akar-akar di F_ℓ, maka grup galois dari f(x) atas $\mathbb{Q}$ isomorfis ke A_p.

Bukti: Diketahui $f(x) \in \mathbb{Z}[x]$ tak terdeduksi atas $\mathbb{Q}$ dengan derajat $p \geq 3$ dan diskriminan f *square*
Akan ditunjukan grup galois $G \cong A_P$.
Ambil sebarang G dimana G adalah grup galois dari $f(x)$, karena diskriminan f square maka G adalah subgrup dari A_p. karena $f(x)$ berderajat prima $p \geq 3$ sehingga grup galois G memiliki orde yang habis dibagi dengan p, dan G memuat $p-$putaran. Berdasarkan faktorisasi dari $f(x)$ mod ℓ dan teorema 4.8, sehingga G memuat $3-$putaran maka untuk semua bilangan prima $p \geq 3$, setiap $p-$putaran dan $3-$putaran di S_p membangun A_p, sehingga $G \cong A_P$. $\blacksquare$

Contoh 20. Misalkan diberikan $f(x) = x^5 + 20x + 16$ diskriminan $2^{16}5^6$ sehingga diskriminan dari $f(x)$ *square* diketahui $f(x)$ tak terduksi atas mod 3 sehingga $f(x)$ tak tereduksi atas $\mathbb{Q}$. Karena terdapat bilangan prima 7 dimana $f(x)$ tak tereduksi atas mod 7 dengan faktorisasi tak tereduksi adalah sebagai berikut:

$$x^5 + 20x + 16 \equiv (x-4)(x-5)(x^3 + 2x^2 + 5x + 5)\ mod\ 7$$

Yang memiliki semua tetapi tiga akar-akar di F_7, jadi grup galois dari $x^5 + 20x + 16$ atas $\mathbb{Q}$ isomorfis ke A_5.

3. Kesimpulan

Berdasarkan hasil dan pembahasan pada bab iv dapat ditarik beberapa kesimpulan sebagai berikut:

1. Misalkan $f(x) \in F[x]$ tak tereduksi atas F sehingga terdapat akar-akar yang tidak termuat dalam lapangan F, maka dikontruksi suatu lapangan E yang mana memuat akar-akar dari $f(x)$ yang disebut dengan lapangan perluasan E atas F dinotasikan dengan lapangan perluasan E/F.
2. Sutau polinomial $f(x) \in F[x]$ yang tak tereduksi atas $F[x]$ memiliki lapangan pemisah jika dan hanya jika terdapat terdapat lapangan perluasan $E[x]$, dan $f(x)$ dapat difaktorkan secara linear di dalam $E[x]$.

3. Suatu lapangan pemisah $F(a_1, a_2, \cdots a_n)$ juga merupakan lapangan perluasan terkecil, dimana hanya memuat lapangan F dan akar-akar $a_1, a_2, \cdots a_n$ dari suatu polinomial.
4. Grup galois merupakan grup yang memuat kumpulan dari automorfisma dengan operasi komposisi fungsi dari suatu lapangan pemisah dengan identitasnya di lapangan dari $f(x)$. Automorfisma dari lapangan pemisah adalah permutasi dari akar-akar polinomial dalam lapangan pemisah.
5. Syarat suatu trinomial berderajat 5 isomorfis dengan grup alternating A_5 yaitu:
    - Polinomial tak tereduksi atas suatu lapangan
    - Polinomial monik
    - Polinomial berderajat prima $p \geq 3$
    - Polinomial memiliki diskriminan square
    - Terdapat suatu bilangan prima p yang tak habis membagi diskriminan $f(x)$

Referensi

[1] Cohen, S. D., Movahhedi, A., & Salinier, A. (1999). Galois groups of trinomials. *Journal of Algebra*, *222*(2), 561–573.
[2] Conrad, K. (2015). *Galois groups as permutation groups*. 1–11. Retrieved January 10, 2021, from https://kconrad.math.uconn.edu/blurbs/galoistheory/galoisaspermgp.pdf.
[3] Cox, D. A. (2012). Second edition. *Taiwan Review*, *69*(4).
[4] Dummit. (1999). Abstract Algebra Dummit and Foote.pdf.
[5] Jiang, Y. (2018). Galois Theory and the Quintic Equation.
[6] Judson, T. W., and Austin, S. F. (2010). *Judson,Abstract Algebra Theory and Applications*. 1–438. papers2://publication/uuid/58FA28A7-7E64-4CED-BAEA-DB00DC1AAD19
[7] Khanna. (2000). Vijay K. Khanna, S.K. Bhamri - *A Course in Abstract Algebra*-Vikas (2013).pdf.
[8] Malik, D. S., & Mordeson, J. N. (2007). MTH 581-582 Introduction to Abstract Algebra. *America*, *February*.
[9] Paulsen, W. (2019). Galois Theory. *Abstract Algebra*, 523–563.
[10] Stewart, I. (2016). Field Automorphisms. *Galois Theory*, 165–170.