PARAMETER
JOURNAL OF MATHEMATICS, STATISTICS AND ITS APPLICATIONS

Vol 02 No 01, April 2023,
https://ojs3.unpatti.ac.id/index.php/parameter

KAJIAN DASAR STRUKTUR GRUP GALOIS

STUDY OF BASIC STRUCTURE GALOIS GROUP

Chrissandy Sapulete[1], Henry W. M. Patty[2], Francis Y. Rumlawang[3], Dyana Patty[4]
[1,2,3,4]Program Studi Matematika, FMIPA Universitas Pattimura
Jl. Ir. M. Putuhena, Kampus Unpatti, Poka-Ambon
e-mail: [1*]chrissandysapulete8@gmail.com

Abstrak

Terdapat lapangan polinomial satu variabel $R \in \mathbb{Q}[x]$ dan $S \in \mathbb{Q}[x]$ dimana lapangan S dimuat oleh lapangan R yang disimbolkan $S \subseteq R$ atau R/S itu berarti operasi-operasi dalam S sama dengan operasi-operasi dalam R selanjutnya disebut R merupakan lapangan perluasan dari S. Dilain sisi, terdapat polinomial $f(x)$ berderajat bulat positif di dalam $S[x]$ dan terfaktor dalam $R[x]$ serta akar – akar $f(x)$ berada dalam R. Lapangan S merupakan lapangan bagian dari R sehingga R disebut lapangan pemisah. Pada perluasan lapangan R dari S terdapat $\sigma -$ automorfisma dari R yang memetakan $R \to R$ dengan elemen dari S sehingga $S - automorfisma$ dari R yang memenuhi $\sigma(e) = e, e \in S$ sehingga himpunan automorfisma dari R membentuk suatu grup yang disebut grup galois dari R atas S dengan notasi $Gal(R/S)$. Dalam tulisan ini diperoleh himpunan automorfisma dari R dengan operasi komposisi fungsi merupakan grup galois karena setiap automorfisma pada $Gal(R/K)$ mengkontruksi akar – akar dari $f(x)$ pada R. Hal ini berarti $f(x)$ merupakan polinomial tak tereduksi sehingga akar – akar dari $f(x)$ tidak berada pada lapangan S tetapi pada perluasan lapangan S yaitu lapangan R sehingga terdapat automorfisma pada $Gal(R/S)$ yang mengkontruksi akar – akar dari $f(x)$ pada R.

Kata Kunci: *Lapangan Perluasan, Lapangan Pemisah, Lapangan Automorfisma, Grup Galois.*

Abstract

There is a polynomial field of one variable $R \in \mathbb{Q}[x]$ and $S \in \mathbb{Q}[x]$ where the field S is loaded by the field R which is symbolized $S \subseteq R$ or R/S that means the operations in S are the same as the operations in R hereinafter referred to as R is an extension field of S. On the other hand, there is a positive integer degree $f(x)$ in $S[x]$ and is factored in $R[x]$ and the roots of $f(x)$ are in R. Field S is a subfield of R so R is called the splitting field. In the extension of the field R from S there is $\sigma -$automorphism of R which maps $R \to R$ with elements of S so that the $S -$automorphism of R that satisfies $\sigma(e) = e, e \in S$ so that the set of automorphisms of R forms a group called a galois group from R over S with the notation $Gal(R/S)$. In this paper, we get the set of automorphisms from R with the function composition operation being a galois group because each automorphism in $Gal(R/K)$ constructs the roots of $f(x)$ in R. This means that $f(x)$ is an irreducible polynomial so that the roots of $f(x)$ are not in the S field but in the extension of the field S, namely the R field so that there is an automorphism in $Gal(R/S)$ which constructs the roots of $f(x)$ on R.

Keywords: *Extension Field, Splitting Field, Automorphism Field, Galois Group.*

doi: https://doi.org/10.30598/parameterv2i01pp139-144

Submitted: Desember 2022
Accepted: April 2023

1. PENDAHULUAN

Pada penelitian ini, terdapat polinomial satu variabel x yang memiliki lapangan perluasan R, seperti lapangan yang merupakan bentuk khusus dari ring, jika dalam ring terdapat subring maka demikian juga lapangan terdapat suatu sublapangan (Yusuf. M. A, 2003). Lebih jelas jika R dan S adalah lapangan, dan R memuat S maka dikatakan R merupakan lapangan perluasan dari S. Dalam suatu perluasan lapangan R dari S terdapat σ – automorfisma dari R yang memetakan $R \rightarrow R$ dengan elemen dari S selanjutnya disebut $S - \text{automorfisma}$ dari R yang memenuhi $\sigma(s) = s, s \in S$ sehingga himpunan automorfisma tersebut membentuk suatu grup yang disebut grup galois dari R atas S dengan notasi $Gal(R\,/S)$ (Yusuf. M. A, 2003). Diberikan S merupakan lapangan sehingga grup galois dari polynomial $f(x) \in S[x]$ merupakan grup $Aut_S R$, dimana R adalah lapangan pemisah dari $f(x)$ atas S (Hungerford, T. W, 1984) maka dapat dikatakan bahwa grup galois merupakan grup yang memuat himpunan automorfisma dari lapangan pemisah yang identitasnya berada pada lapangan dari suatu polinomial $f(x)$. Dalam penelitian ini, akan diselidiki kajian dasar struktur grup galois yang meliputi operasi dan syarat apa yang harus dipenuhi agar suatu polinomial merupakan grup galois.

2. METODE PENELITIAN

2.1 Tipe Penelitian

Tipe penelitian yang digunakan dalam penelitian ini yaitu studi pustaka, yaitu dengan menggunakan beberapa literatur yang berkaitan sebagai acuan untuk mengkaji topik yang akan dibahas.

2.2 Bahan dan Materi Ajar

Dalam penelitian ini, digunakan bahan atau materi berupa karya ilmiah yang disajikan dalam bentuk jurnal, skripsi, thesis, *ebook* dan media lainnya seperti video pembelajaran yang diperoleh dari internet.

2.3 Populasi dan Sampel Penelitian

Adapun prosedur yang digunakan dalam penelitian ini terdiri dari: penentuan judul penelitian, mempelajari tentang: lapangan perluasan, lapangan pemisah, lapangan automorfisma, proses identifikasi struktur dasar grup galois dan menyimpulkan penelitian.

3. HASIL DAN PEMBAHASAN

3.1 Lapangan Perluasan

Definisi 1 [3]

Lapangan R disebut lapangan perluasan atas lapangan S jika lapangan S merupakan lapangan bagian dari lapangan R ($S \subseteq R$ atau R/S).

Contoh 1

$\mathbb{Q}[\sqrt{3}]$ merupakan lapangan perluasan dari $\mathbb{Q}$ atau dapat ditulis $\mathbb{Q}[\sqrt{3}]/\mathbb{Q}$ karena jika $a \in \mathbb{Q}$ maka $a + 0\sqrt{3} \in \mathbb{Q}[\sqrt{3}]$ jadi $\mathbb{Q}[\sqrt{3}]/\mathbb{Q}$

Teorema 1 [4]
Diberikan lapangan R merupakan lapangan perluasan atas lapangan S. Jika $\alpha \in R$ merupakan elemen aljabar atas S dengan polinomial taktereduksi $p(x) \in S[x]$ untuk α berderajat n, maka $S(\alpha)$ merupakan perluasan berhingga berderajat n di mana basis dari $S(\alpha)$ atas S adalah $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$.

Bukti :
Ambil sebarang $\alpha \in R$ merupakan elemen aljabar atas S dengan polinomial tak tereduksi $p(x) \in S[x]$ untuk α berderajat n sehingga terdapat $\beta \in S(\alpha)$ maka $\beta = b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{n-1}\alpha^{n-1}$ di mana $b_i \in S$. Selanjutnya $\beta = b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{n-1}\alpha^{n-1}$ memiliki skalar yaitu $b_0 + b_1 + b_2 + \cdots + b_{n-1}$ sehingga $\beta \in S(\alpha)$ merupakan kombinasi linier dari $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$.
Akan dibuktikan bahwa basis dari $S(\alpha)$ atas S adalah $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$
Karena untuk setiap $\beta = b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{n-1}\alpha^{n-1}$ di mana $b_i \in S$ merupakan kombinasi linier dari $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ sehingga $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ merentangkan $S(\alpha)$.
$1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ bebas linier atas S karena jika $b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{n-1}\alpha^{n-1} = 0$ maka $q(\alpha) = 0$ karena $p(x)$ tak tereduksi dan mempunyai α untuk suatu $q(x) = b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{n-1}\alpha^{n-1} \in S[x]$ sehingga $q(x) = 0$. hal ini berarti $b_0 = b_1 = b_2 = \cdots = b_{n-1} = 0$.
Jadi $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ basis dari $S(\alpha)$ atas S.

Contoh 2
Basis dari $x^2 - 3$ yaitu $\{1, \sqrt{3}\}$ dimana akar dari $x^3 - 2$ adalah $\sqrt{3}$.
Ambil sebarang $a, b \in \mathbb{Q}$
Dari teorema diatas didapat a^0, a^1 dengan akarnya adalah $\sqrt{3}$ maka,

$$3^{(1/2)0}, 3^{(1/2)1} = 1, \sqrt{2}$$

Sehingga $\mathbb{Q}[\sqrt{3}] = a \cdot 1 + b \cdot \sqrt{3} = a + b\sqrt{3}$.

3.2 Lapangan Pemisah

Definisi 2 [3]
Lapangan perluasan R disebut lapangan pemisah *(splitting field)* dari polinomial $f(x) \in S[x]$ jika $f(x)$ terfaktor dalam $R[x]$ dengan akar-akar $f(x)$ berada dalam R

Contoh 3
Lapangan pemisah dari $p(x) = x^2 - 3$ adalah $\mathbb{Q}[\sqrt{3}]$ karena akar dari $x^2 - 3$ adalah $\sqrt{3}$ dimana akar ini berada pada perluasan lapangan $\mathbb{Q}[\sqrt{3}]$.

3.3 Lapangan Automorfisma

Definisi 3 [6]
Diberikan lapangan R. fungsi $f: R \to R$ dengan $a, x, y \in R$ disebut lapangan automorfisma Jika memenuhi kondisi berikut

$$f(x + y) = f(x) + f(y) \;,$$
$$f(ax) = f(a)f(x)$$
$$\text{dan } f(1/x) = 1/f(x)$$

Contoh 4

Jika didefenisikan fungsi $f: \mathbb{Q}[\sqrt{3}] \to \mathbb{Q}[\sqrt{3}]$ dengan $f(a + b\sqrt{3}) = a - b\sqrt{3}$ memenuhi ketiga kondisi diatas maka f merupakan lapangan automorfisma.

Definisi 4 [6]

Jika terdapat lapangan perluasan R dari lapangan S, maka S-automorfisma dari R adalah automorfisma f dari $R \to R$ dengan syarat tambahan yaitu $f(x) = x$ untuk semua x di S.

Dari definisi diatas dapat didefinisikan simetri akar, karena S-automorfisma menyatakan semua elemen dari S tidak berubah dan hanya memberi label ulang elemen baru yang ditambahkan ke bentuk dari R. Ternyata untuk $\mathbb{Q}[\sqrt{2}\,]$ fungsi f didefenisikan di atas adalah satu-satunya $\mathbb{Q}$-automorfisma yaitu $g(x) = x$.

Jika $p(x)$ adalah polinomial dengan koefisien rasional, $R/\mathbb{Q}$ adalah lapangan perluasan dan R adalah $\mathbb{Q}$-automorfisma dari S maka $f(p(x)) = p(f(x))$ hal ini menunjukan bahwa $\mathbb{Q}$-automorfisma dari lapangan pemisah F untuk polinomial $p(x)$ yang mengatur kembali akar dari $p(x)$. jika $p(\alpha) = 0$ maka $p(f(\alpha)) = f(p(\alpha)) = f(0) = 0$, sehingga $f(\alpha)$ merupakan akar dari $p(x)$ sehingga $\mathbb{Q}$ - automorfisma dapat mengkontruksi kembali setiap elemen dari lapangan pemisah.

3.4 Struktur Dasar Grup Galois

Definisi 5 [1]

Diberikan $S \subset R$ merupakan lapangan perluasan. Maka $Gal(R/S)$ adalah himpunan

$$\{\sigma: R \to R \mid \sigma \; adalah \; automorfisma, \sigma(a) = a \; untuk \; semua \; a \in S\}.$$

Dengan kata lain, $Gal(R/S)$ terdiri dari semua automorfisma R yang merupakan identitas di S.

Proposisi 1 [1]

$Gal(R/S)$ adalah grup dengan operasi komposisi fungsi.

Bukti :

Ambil sebarang $\sigma, \tau \in Gal(R/S)$. Maka $\sigma\tau$ adalah komposisi $\sigma \circ \tau$, yang merupakan automorfisma. Jika $a \in S$, maka $\sigma \circ \tau(a) = \sigma(\tau(a)) = \sigma(a) = a$, karena σ, τ adalah identitas pada S . oleh karena itu terdapat opoerasi komposisi pada $Gal(R/S)$, yang asosiatif dengan sifat – sifat standar komposisi.

Pemetaan identitas $1_R: R \to R$ merupakan isomorfisma yang identitas pada S, sehingga $1_R \in Gal(R/S)$. selanjutnya $\sigma \circ 1_R = 1_R \circ \sigma = \sigma$ untuk semua $\sigma \in Gal(R/S)$. Jadi 1_R merupakan elemen identitas dari $Gal(R/S)$.

Sehingga, setiap $\sigma \in Gal(R/S)$ merupakan automorfisma, hal ini berarti $\sigma^{-1}: R \to R$ juga merupakan automorfisma. Hal ini berarti juga, jika $a \in S$, maka $a = \sigma(a)$, menyiratkan $\sigma^{-1}(a) = \sigma^{-1}(\sigma(a)) = a$. Hal ini menunjukan bahwa $\sigma^{-1} \in Gal(R/S)$ sehingga terbukti $Gal(R/S)$ merupakan grup dengan operasi komposisi fungsi.

Teorema 2 [5]

Diberikan S adalah lapangan sehingga R merupakan lapangan perluasan dari S dan $f(x) \in S[x]$. Maka setiap automorfisma pada $Gal(R/S)$ mengkontruksi akar – akar dari $f(x)$ pada R.

Bukti :

Diberikan $f(x) \in S[x]$ dengan $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ dimana $a_0, a_1, \ldots, a_n \in S$, $u \in R$ merupakan akar dari f. Maka $f(u) = 0$ dan $\sigma \in Gal(R/S)$

Sehingga,

$$\sigma\big(f(u)\big) = 0$$
$$\sigma(a_0 + a_1 u + \cdots + a_n u^n) = 0$$
$$\sigma(a_0) + \sigma(a_1 u) + \cdots + \sigma(a_n u^n) = 0$$
$$\sigma(a_0) + \sigma(a_1)\sigma(u) + \cdots + \sigma(a_n)\sigma(u^n) = 0$$

Karena $a_0, a_1, \ldots, a_n \in S$ dan $\sigma \in Gal(R/S)$ sehingga $\sigma(a_0) = a_0$, $\sigma(a_1) = a_1, \ldots, \sigma(a_n) = a_n$,

Maka $\quad a_0 + a_1\sigma(u) + \cdots + a_n\sigma(u^n) = 0$

$$f\big(\sigma(u)\big) = 0$$

Karena itu $\sigma(u)$ adalah akar dari f. Hal ini berarti bahwa polinomial f memiliki akar-akar terbatas pada R dan karena σ merupakan automorfisma sehingga σ mengkontruksi akar-akar dari f pada R.

Contoh 5

Grup galois dari $x^2 - 3 \in \mathbb{Q}[x]$ adalah $Gal\big(\mathbb{Q}(\sqrt{3})/\mathbb{Q}\,\big)$ karena jika $p(x) = x^2 - 3 \in \mathbb{Q}[x]$ maka diperoleh

$$p(x) = 0$$
$$x^2 - 3 = 0$$
$$x^2 = 3$$
$$x = \sqrt{3} = a$$

Sehingga,

Basis = $a^0, a^1, a^2, a^3, \ldots, a^{n-1}$

Basis dari $x^2 - 3$ yaitu a^0, a^1 karena $x = \sqrt{3} = a$ maka,

$$\left\{3^{0/2}, 3^{1/2}\right\} = \{1, \sqrt{3}\}$$

Selanjutnya ambil sebarang $a, b \in \mathbb{Q}$

Sehingga, $\left(a.1 + b\big(\sqrt{3}\big)\right)$

Diperoleh

$\sigma\big(\,a.1 + b\big(\sqrt{3}\big)\,\big) = \sigma(a.1) + \sigma\big(b\sqrt{3}\big)$

$$= \sigma(a) + \sigma(b)\sigma(\sqrt{3})$$
$$= a + b\sigma\big(\sqrt{3}\big) = \big(\,a.1 + b\big(\sqrt{3}\big)\,\big)$$

Jadi , $\sigma\big(\,a.1 + b\big(\sqrt{3}\big)\,\big) = \left(\,a.1 + b\big(\sqrt{3}\big)\right)$

Maka grup galois dari $x^2 - 3$ adalah $Gal\big(\mathbb{Q}\big(\sqrt{3}\big)/\mathbb{Q}\,\big)$

4. SIMPULAN

Dari hasil pembahasan pada bab sebelumnya maka dapat disimpulkan bahwa strutur dasar grup galois memiliki operasi komposisi fungsi dan dikontruksi oleh lapangan perluasan, lapangan pemisah dan lapangan automorfisma sehingga grup galois memuat himpunan automorfisma dari lapangan pemisah yang identitasnya berada pada lapangan dari suatu polinomial $f(x)$. Dilain sisi setiap automorfisma pada $Gal(R/S)$ mengkontruksi akar – akar dari $f(x)$ pada R. Hal ini berarti $f(x)$ merupakan polinomial tak tereduksi sehingga akar – akar dari $f(x)$ tidak berada pada lapangan S tetapi pada perluasan lapangan S yaitu lapangan R sehingga terdapat automorfisma pada $Gal(R/S)$ yang mengkontruksi akar – akar dari $f(x)$ pada R.

DAFTAR PUSTAKA

[1] Cox, D. A. (2012).Second edition.*Taiwan Review*, 69(4).

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

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

[4] Lamhot. 2007. *Struktur Medan Galois*. Skripsi. Jogyakarta : Universitas Sanata Dharma.

[5] Mathonline learn mathematics. *Automorphisms in the Galois Group of f(x) over K Permute the Roots of f*, http://mathonline.wikidot.com/, diakses pada 2 Januari 2021 pukul 12.30 Wit.

[6] Stewart, I. (2016). Field Automorphisms. Galois Theory, 165–170. https://doi.org/10.4324/9780203489307-19

[7] Yusuf, M. A. (2003). *Grup Galois Pada Polinomial*. Undergraduate thesis. FMIPA Undip.