II. TINJAUAN PUSTAKA

Pada bab ini diberikan beberapa definisi mengenai teori grup yang mendukung proses penelitian.

2.1 Teori Grup

Definisi 2.1.1 Operasi Biner

Suatu operasi biner $*$ pada suatu himpunan S adalah fungsi yang memetakan dari $S \times S$ ke S. Untuk setiap $(a, b) \in S \times S$, $*\,((a, b))$ dinotasikan sebagai $a * b$ di S (Fraleigh, 1999).

Contoh 2.1.2

Diberikan himpunan bilangan komposit K (himpunan bilangan bulat yang lebih besar dari 1 dengan banyaknya faktor positif lebih dari 2), dilengkapi dengan operasi pangkat (^) dengan untuk setiap $a, b \in K$ didefinisikan $a \wedge b = a^b$. Himpunan K dan operasi (^) merupakan contoh himpunan yang dilengkapi dengan operasi biner.

Bukti.

Perhatikan bahwa setiap bilangan komposit $a > 1$ dan untuk setiap $b \in K$, maka $a^b > 1$. Misal faktorisasi bilangan komposit $a = p_1^{c_1} p_2^{c_2} \ldots p_k^{c_k}$ dengan

$p_1, p_2, \dots, p_k$ adalah bilangan prima yang berbeda, sehingga a memiliki faktor positif sebanyak $(c_1+1)(c_2+1)\dots(c_k+1) > 2$, maka dengan $b > 1$, $a^b = (p_1^{c_1} p_2^{c_2} \dots p_k^{c_k})^b = p_1^{c_1 b} p_2^{c_2 b} \dots p_k^{c_k b}$ memiliki faktor positif sebanyak $(c_1 b + 1)(c_2 b + 1) \dots (c_k b + 1) > (c_1+1)(c_2+1)\dots(c_k+1) > 2$. Akibatnya $a \wedge b = a^b$ merupakan bilangan komposit. Jadi operasi (^) tertutup dalam K , sehingga (^) merupakan operasi biner dalam K.

Operasi biner yang diperlengkapi pada suatu himpunan akan menjamin ketertutupan operasi elemen – elemen dalam himpunan tersebut. Lebih lanjut jika memenuhi aksioma – aksioma berikut, maka akan membentuk suatu struktur aljabar yang disebut grup.

Definisi 2.1.3 Grup

Suatu grup $\langle G, * \rangle$ adalah himpunan G, tertutup atas operasi biner $*$, sedemikian sehingga memenuhi aksioma – aksioma :

1. Untuk semua $a, b, c \in G$, berlaku

   $(a * b) * c = a * (b * c)$ (sifat asosiatif operasi $*$).

2. Terdapat suatu elemen identitas e sedemikian sehingga

   untuk semua $x \in G$, berlaku

   $e * x = x * e = x$ (identitas e atas operasi $*$).

3. Untuk setiap $a \in G$, terdapat suatu elemen a^{-1} di G sedemikian sehingga

   $a * a^{-1} = a^{-1} * a = e$.

Jika suatu himpunan G dan operasi binernya hanya memenuhi aksioma 1, maka G disebut semigrup. Suatu semigrup yang memenuhi aksioma 2 disebut monoid (Fraleigh, 1999).

Contoh 2.1.4

Himpunan string S dengan panjang minimal 1 digit yang dibentuk dari $\{0,1\}$, dilengkapi dengan operasi biner " $\cup$ " didefinisikan sebagai gabungan dua string adalah contoh semigrup.

Bukti.

Untuk sebarang $s_1, s_2 \in S$ dengan $s_1 = a_1a_2 \dots a_m$ dan $s_2 = b_1b_2 \dots b_n$, $a_i, b_j \in \{0,1\}, 1 \leq i \leq m$ dan $1 \leq j \leq n$, berlaku

$s_1 \cup s_2 = a_1a_2 \dots a_mb_1b_2 \dots b_n \in S$ dengan panjang string $m + n$, sehingga sifat tertutup operasi terpenuhi. Misalkan $s_3 \in S$ dengan $s_3 = c_1c_2 \dots c_p$, $c_p \in \{0,1\}$, $1 \leq k \leq p$, sehingga

$$
\begin{aligned}
(s_1 \cup s_2) \cup s_3 &= (a_1a_2 \dots a_mb_1b_2 \dots b_n) \cup c_1c_2 \dots c_p \\
&= a_1a_2 \dots a_mb_1b_2 \dots b_nc_1c_2 \dots c_p \\
&= a_1a_2 \dots a_m \cup (b_1b_2 \dots b_nc_1c_2 \dots c_p) \\
&= s_1 \cup (s_2 \cup s_3).
\end{aligned}
$$

Jadi, sifat asosiatif terpenuhi. Akibatnya, himpunan S dengan operasi biner " $\cup$ " membentuk semigrup.

Contoh 2.1.5

Himpunan kuasa $P(A)$ dari himpunan A, dilengkapi dengan operasi biner irisan himpunan " $\cap$ " merupakan monoid. Elemen identitas dalam monoid ini adalah A.

Bukti.

Diberikan sebarang $A_1, A_2, A_3 \in P(A)$. Oleh karena itu, $A_1, A_2, A_3 \subseteq A$. Sehingga, $A_1 \cap A_2 \subseteq A$. Akibatnya, $A_1 \cap A_2 \in P(A)$ (sifat tertutup terpenuhi). Selanjutnya, akan ditunjukkan sifat asosiatif, yaitu $(A_1 \cap A_2) \cap A_3 = A_1 \cap (A_2 \cap A_3)$.

Diberikan sebarang $a \in (A_1 \cap A_2) \cap A_3$

$\Leftrightarrow a \in (A_1 \cap A_2)$dan $a \in A_3$

$\Leftrightarrow$ $a \in A_1, a \in A_2$ dan $a \in A_3$

$\Leftrightarrow a \in A_1$dan $a \in (A_2 \cap A_3)$

$\Leftrightarrow a \in A_1 \cap (A_2 \cap A_3)$

sehingga $(A_1 \cap A_2) \cap A_3 \subseteq A_1 \cap (A_2 \cap A_3)$. Dengan cara yang serupa, diperoleh $A_1 \cap (A_2 \cap A_3) \subseteq (A_1 \cap A_2) \cap A_3$.

Akibatnya, $(A_1 \cap A_2) \cap A_3 = A_1 \cap (A_2 \cap A_3)$ (sifat asosiatif terpenuhi).

Pilih $A \in P(A)$, oleh karena untuk setiap $A_1 \in P(A)$, berlaku

$A \cap A_1 = A_1 \cap A \subseteq A_1$ dan $A_1 \subseteq A \subseteq A \cap A_1 = A_1 \cap A$ maka

$A \cap A_1 = A_1 \cap A = A_1$.

Akibatnya, A merupakan elemen identitas di $P(A)$ terhadap operasi $\cap$. Jadi, himpunan kuasa $P(A)$ dari himpunan A dengan operasi irisan himpunan " $\cap$ " membentuk monoid.

Contoh 2.1.6

Himpunan matriks berorde $n \times n$ dengan entri bilangan riil yang memiliki invers, $GL_n(R)$, yang dilengkapi dengan operasi biner $(\cdot)$ "perkalian matriks" adalah grup.

Bukti.

Diberikan sebarang $A, B \in GL_n(R)$ sehingga $\det(A), \det(B) \neq 0$.

Oleh karena $\det(AB) = \det(A) \cdot \det(B)$, maka $\det(AB) \neq 0$. Akibatnya, AB invertibel. Dengan kata lain $AB \in GL_n(R)$ (sifat tertutup terpenuhi). Sifat asosiatif jelas terpenuhi sebab $GL_n(R) \subset M_{n\times n}(R)$. Jelas bahwa matriks $I_{n\times n}$ merupakan elemen identitas dalam $GL_n(R)$. Oleh karena untuk setiap $A \in GL_n(R)$, terdapat invers dari A yaitu A^{-1} sedemikian sehingga $AA^{-1} = A^{-1}A = I$, maka setiap elemen di $GL_n(R)$ memiliki invers di $GL_n(R)$. Jadi, $GL_n(R)$ membentuk grup dengan operasi biner perkalian matriks.

Operasi biner $*$ dalam grup G memiliki kemungkinan bersifat komutatif, yaitu untuk setiap $a, b \in G$ berlaku $a * b \in G$. Hal ini yang mendasari didefinisikannya grup Abel sebagai berikut.

Definisi 2.1.7 Grup Abel (komutatif)

Suatu grup G dikatakan grup Abel (komutatif) jika dan hanya jika operasi biner $*$ bersifat komutatif (Fraleigh, 1999).

Contoh 2.1.8

Himpunan $D_{n\times n}(R)$ didefinisikan sebagai himpunan matriks diagonal berorde $n \times n$ yang invertibel dengan entri bilangan riil, yang dilengkapi dengan operasi biner $(\cdot)$ "perkalian matriks" merupakan contoh grup Abel.

Bukti.

Diberikan sebarang $A, B \in D_{n\times n}(R)$ dengan a_{ij} dan b_{ij} berturut – turut adalah entri matriks A dan B. Sehingga, untuk $i \neq j$, diperoleh $a_{ij} = 0$ dan $b_{ij} = 0$. Sementara itu, untuk $i = j$, diperoleh $a_{ij} \neq 0$ dan $b_{ij} \neq 0$. Misalkan d_{ij} adalah entri matriks AB dengan $d_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$.

Sehingga, untuk $i \neq j$:

jika $k = i$ maka $a_{ik} \neq 0$ tetapi $b_{kj} = 0$, sehingga $a_{ik}b_{kj} = 0$,

jika $k = j$ maka $a_{ik} = 0$ tetapi $b_{kj} \neq 0$, sehingga $a_{ik}b_{kj} = 0$,

jika $k \neq i$ dan $k \neq j$ maka $a_{ik} = b_{kj} = 0$, sehingga $a_{ik}b_{kj} = 0$.

Jadi, untuk $i \neq j$ dapat disimpulkan $d_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj} = 0$.

Untuk $i = j$:

jika $k = i$ dan $k = j$ maka $a_{ik} \neq 0$ dan $b_{ik} \neq 0$, sehingga $a_{ik}b_{kj} \neq 0$,

jika $k \neq i$ dan $k \neq j$ maka $a_{ik} = b_{kj} = 0$, sehingga $a_{ik}b_{kj} = 0$.

Jadi, untuk $i = j$ dapat disimpulkan $d_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj} \neq 0$.

Akibatnya, $AB \in D_{n\times n}(R)$ (sifat tertutup terpenuhi).

Selanjutnya, karena $D_{n\times n}(R) \subset GL_n(R)$, maka sifat asosiatif terpenuhi.

Jelas bahwa matriks $I_{n\times n}$ merupakan elemen identitas dalam $D_{n\times n}(R)$.

Berikutnya akan ditunjukkan bahwa setiap elemen di dalam $D_{n\times n}(R)$ memiliki invers. Untuk setiap $A \in D_{n\times n}(R)$, terdapat $A^{-1} \in D_{n\times n}(R)$ sedemikian sehingga $AA^{-1} = A^{-1}A = I$, dengan entri matriks A^{-1} adalah $a'_{ij} = \frac{1}{a_{ij}}$. Jadi, telah ditunjukkan bahwa $D_{n\times n}(R)$ adalah grup.

Selanjutnya akan ditunjukkan sifat komutatif dalam $D_{n\times n}(R)$. Diberikan sebarang $A, B \in D_{n\times n}(R)$ dengan a_{ij} entri matriks A dan b_{ij} entri matriks B, $a_{ij} = 0$ dan $b_{ij} = 0$ untuk $i \neq j$. Misal c_{ij} entri matriks AB dan d_{ij} entri matriks BA, dengan $c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj} = \sum_{k=1}^{n} b_{kj}a_{ik} = d_{ij}$. Sehingga, $AB = BA$. Akibatnya berlaku sifat komutatif pada $D_{n\times n}(R)$. Jadi, $D_{n\times n}(R)$ dengan operasi biner perkalian matriks merupakan grup Abel.

Definisi 2.1.9 Grup Abel Dasar

Grup Abel dasar adalah grup Abel berhingga dengan setiap elemen tak nol memiliki orde prima p (Dummit, 2004).

Contoh 2.1.10

Diberikan $A = \{(0,0), (0,1), (1,0), (1,1)\}$ dengan operasi biner * penjumlahan modulo 2, maka $\langle A,*\rangle$ adalah grup Abel dasar.

Himpunan bagian dari suatu grup G belum tentu memenuhi keempat aksioma – aksioma grup. Jika himpunan bagian tersebut memenuhinya maka disebut subgrup dari grup G.

Definisi 2.1.11 Subgrup

Jika suatu himpunan bagian H dari grup G tertutup atas operasi biner dari H dan G adalah grup dengan operasi biner tersebut, maka H adalah subgrup dari G yang dinotasikan dengan $H \leq G$ atau $G \geq H$ (Fraleigh, 1999).

Contoh 2.1.12

Diketahui $Z_6 = \{0, 1, 2, 3, 4, 5\}$ merupakan grup dengan operasi biner $(+_6)$ penjumlahan modulo 6. Misalkan $A = \{0, 2, 4\}$. Jelas bahwa $A \subset Z_6$. Dengan operasi biner yang sama $(+_6)$, A akan membentuk grup sehingga $A \leq Z_6$.

Dalam teori himpunan telah dikenal istilah himpunan bagian sejati dan himpunan bagian trivial. Oleh karena grup dibentuk dari suatu himpunan, maka dapat didefinisikan subgrup sejati dan subgrup trivial sebagai berikut.

Definisi 2.1.13 Subgrup Sejati dan Trivial

Jika G adalah grup, maka G sendiri adalah subgrup tak sejati dari G. Semua subgrup yang lainnya dari G disebut subgrup sejati. Dengan kata lain, H adalah subgrup sejati dari G jika dan hanya jika $H \leq G$ tetapi $H \neq G$, dinotasikan $H < G$. Subgrup $\{e\}$ disebut subgrup trivial dari G dengan e elemen identitas di G. Semua subgrup selain $\{e\}$ disebut subgrup nontrivial (Fraleigh, 1999).

Contoh 2.1.14

Diberikan $\langle Z_6, +_6 \rangle$ adalah grup, dengan $Z_6 = \{\mathbf{0}, \mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{4}, \mathbf{5}\}$.

Misal $H = \{\mathbf{0}, \mathbf{2}, \mathbf{4}\}$. Dengan operasi $+_6$, H akan membentuk grup. Sehingga H adalah subgrup dari Z_6. Karena $H \neq Z_6$, maka H adalah subgrup sejati dari Z_6 atau $H < Z_6$.

Dalam suatu grup, terdapat subgrup khusus seperti subgrup normal, karena memiliki kriteria tertentu seperti pada definisi berikut.

Definisi 2.1.15 Subgrup Normal

Diberikan H subgrup dari grup G, H dikatakan subgrup normal jika dan hanya jika $xH = Hx$ untuk setiap $x \in G$, dinotasikan $H \lhd G$ (Dummit, 2004).

Contoh 2.1.16

Diberikan grup simetri S_3. Jelas bahwa $A_3 = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$ adalah subgrup dari S_3. Sehingga, A_3 adalah subgrup normal dari S_3 atau $A_3 \lhd S_3$.

Definisi 2.1.17 *Normalizer*

Diberikan G suatu grup dan H himpunan bagian dari G, $N_G(H)$ disebut *normalizer* dari H dalam grup G jika dan hanya jika $N_G(H) = \{g \in G | gHg^{-1} = H\}$ (Dummit,2004).

Contoh 2.1.18

Diberikan grup simetri S_3. Jelas bahwa $H = \{(1)(2)(3), (1\ 2\ 3)\}$ adalah himpunan bagian dari S_3. Sehingga, $N_{S_3}(H) = \{(1)(2)(3), (1\ 2\ 3)\}$.

Definisi 2.1.19 *Centralizer*

Diberikan G suatu grup dan $z \in G$, *centralizer* dari elemen z dalam grup G adalah himpunan semua elemen G yang komutatif dengan z, dinotasikan $C_G(z)$.

Jadi, $C_G(z) = \{x \in G | xz = zx\}$.

Diberikan H subgrup dari G, *centralizer* dari subgrup H dalam grup G adalah himpunan semua elemen G yang komutatif dengan semua elemen dalam himpunan H, dinotasikan $C_G(H)$. Jadi, $C_G(H) = \{x \in G | xh = hx , \forall h \in H\}$ (Dummit,2004).

Contoh 2.1.20

Diberikan G suatu grup yang terdiri dari himpunan fungsi bernilai riil yang berbentuk $ax + b$, dengan operasi biner komposisi fungsi. Misal $f \in G$, maka $C_G(f) = \{i, f^{-1}\}$, dengan i adalah fungsi identitas dan f^{-1}fungsi invers dari f^{-1}.

Definisi 2.1.21 *Center*

Diberikan G suatu grup, *center* dari grup G adalah himpunan semua elemen G yang komutatif dengan semua elemen G, dinotasikan $Z(G)$.

Jadi, $Z(G) = \{x \in G | xg = gx , \ g \in G\}$. Ekuivalen dengan irisan dari semua *centralizer* elemen grup G (Dummit,2004).

Contoh 2.1.22

Jika G suatu grup yang terdiri dari himpunan fungsi bijektif bernilai riil, maka $Z(G) = \{i\}$, dengan i adalah fungsi identitas sedemikian sehingga $i(x) = x$, untuk setiap $x \in G$.

Grup Mathieu merupakan grup berhingga. Dalam ruang lingkupnya, dibutuhkan Teorema Lagrange sebagai berikut.

Teorema 2.1.23 Teorema Lagrange

Jika H suatu subgrup dari grup berhingga G, maka orde dari H habis membagi orde dari G (Fraleigh,1999).

Definisi 2.1.24 Subgrup Maksimal

Diberikan G suatu grup. M subgrup sejati dari G dikatakan subgrup maksimal dari G jika dan hanya jika tidak ada subgrup $N \neq M$ yang memuat M.

Definisi 2.1.25 Grup Siklik dan Subgrup Siklik

Jika G adalah suatu grup dan $a \in G$, dapat dituliskan

$\langle a \rangle = \{a^n | n \in Z\}$

$\langle a \rangle$ disebut subgrup siklik dari G yang dibangun oleh a.

Suatu grup G disebut siklik jika terdapat $a \in G$ sedemikian sehingga $G = \langle a \rangle$, dalam hal ini elemen a disebut elemen pembangun G (Rotman, 2002).

Contoh 2.1.26

$\langle Z, + \rangle$ merupakan grup siklik dengan elemen pembangunnya adalah 1 dan -1.

Tujuan penelitian ini untuk menunjukkan beberapa grup Mathieu adalah grup sederhana, maka perlu adanya definisi tentang grup sederhana sebagai berikut.

Definisi 2.1.27 Grup Sederhana

Grup sederhana adalah grup yang subgrup normalnya hanya subgrup trivial dan dirinya sendiri (Dummit,2004).

Contoh 2.1.28

Grup siklik Z_7 merupakan grup sederhana, sebab tidak memiliki subgrup normal sejati selain subgrup trivial.

2.2 Grup Permutasi

Contoh lain grup yaitu grup permutasi. Grup ini erat kaitannya dengan grup Mathieu, sebab grup Mathieu merupakan subgrup dari grup permutasi. Akan didefinisikan dahulu permutasi dari suatu himpunan.

Definisi 2.2.1 Permutasi

Suatu permutasi dari himpunan X adalah suatu fungsi bijektif dari X ke dirinya sendiri (Rotman, 2002).

Contoh 2.2.2

Diketahui $X = \{\#, \$, \%\}$. Semua permutasi dari X antara lain :

$\{\#, \$, \%\}$, $\{\#, \%, \$\}$, $\{\$, \%, \#\}$, $\{\$, \#, \%\}$, $\{\%, \#, \$\}$, dan $\{\%, \$, \#\}$

Misalkan terdapat himpunan semua permutasi dari suatu himpunan. Oleh karena permutasi merupakan fungsi bijektif, maka dua permutasi dapat dikomposisikan menjadi suatu fungsi bijektif. Sehingga, komposisi fungsi merupakan operasi biner pada himpunan semua permutasi dari suatu himpunan. Karena operasi komposisi fungsi bersifat asosiatif, himpunan permutasi ini akan membentuk semigrup. Pada himpunan permutasi ini terdapat permutasi identitas yaitu fungsi identitas yang memetakan suatu elemen $x \in X$ ke dirinya sendiri. Akibatnya, terdapat elemen identitas pada semigrup sebelumnya. Dengan kata lain, himpunan permutasi tersebut akan membentuk monoid. Oleh karena fungsi bijektif selalu mempunyai invers, yang tentunya merupakan fungsi bijektif, maka terdapat permutasi invers dalam himpunan permutasi tersebut. Dapat disimpulkan bahwa himpunan semua permutasi dari suatu himpunan akan membentuk grup yang didefinisikan sebagai berikut.

Definisi 2.2.3 Grup Simetri

Himpunan dari semua permutasi dari himpunan X, dinotasikan sebagai S_X , disebut grup simetri pada X. Jika $X = \{1, 2, 3, \dots n\}$ maka S_X dinotasikan dengan S_n dan disebut grup simetri pada n objek (Rotman, 2002).

Setelah mengetahui definisi grup permutasi, selanjutnya akan didefinisikan tentang *stabilizer*.

Definisi 2.2.4 *Stabilizer*

Diberikan G suatu grup permutasi pada himpunan Ω dan x adalah elemen Ω. *Stabilizer* dari x adalah himpunan semua permutasi dalam G yang menghasilkan titik tetap x, dinotasikan $G_x = \{g \in G | g(x) = x\}$ (Dummit,2004).

Contoh 2.2.5

Diberikan grup S_3 dan titik tetap $x = 2$. $(S_3)_2 = \{g \in S_3 | g(2) = 2\} = \{(1)(2)(3), (1\ 3)\}$.

Diberikan suatu himpunan tak kosong X. Sehingga, dapat dibentuk grup simetri S_X. Misalkan G subgrup dari S_X. Sehingga, orbit i pada grup G yang dinotasikan sebagai $orb_G(i)$, merupakan himpunan relasi ekuivalensi pada X dengan $a \sim b$, untuk setiap $a, b \in X$ jika dan hanya jika $b = g^n a$ untuk suatu $n \in \mathbb{Z}$ dan $g \in G$. Stabilizer titik i pada grup G merupakan himpunan semua $g \in G$ yang menetapkan titik i. Sehingga, dapat dirumuskan Teorema Orbit-*Stabilizer* sebagai berikut.

Teorema 2.2.6 Orbit-*Stabilizer*

Diberikan G subgrup dari grup simetri S_X, maka untuk setiap $i \in X$ berlaku

$$|G| = |orb_G(i)||G_i|$$

(Mulholland, 2011).

Dari suatu grup dan suatu himpunan tak kosong, dapat dibentuk suatu fungsi yang menghubungkan keduanya. Dengan kata lain, grup tersebut beraksi pada himpunan. Sehingga, dapat didefinisikan grup aksi sebagai berikut.

2.3 Teori Grup Aksi

Definisi 2.3.1 Grup Aksi

Diberikan X suatu himpunan dan G suatu grup. Suatu aksi dari G pada X adalah pemetaan $*: G \times X \to X$ sedemikian sehingga

1. $ex = x, \forall x \in X$; dan
2. $(g_1 g_2)(x) = g_1(g_2 x)$, untuk setiap $x \in X$ dan $\forall g_1, g_2 \in G$.

Dengan kondisi ini, X disebut G-set (Fraleigh, 1999).

Contoh 2.3.2

Diberikan S_n adalah grup simetri orde n dan himpunan X, maka S_n beraksi pada X dengan fungsi permutasi.

Dalam grup aksi dikenal istilah kernel sebagai berikut.

Definisi 2.3.3 *Kernel* Grup Aksi

Diberikan G suatu grup beraksi pada himpunan tak kosong X. Kernel dari aksi ini didefinisikan sebagai $\{g \in G | g(x) = x, \forall x \in X\}$ (Dummit,2004).

Definisi 2.3.4 Aksi *faithful*

Suatu aksi dari suatu grup disebut *faithful* jika kernelnya adalah elemen identitas (Dummit, 2004).

Contoh 2.3.5

Diberikan S_n adalah grup simetri orde n beraksi pada himpunan tak kosong X. Jika kardinalitas X adalah n, maka aksi tersebut adalah aksi *faithful*.

Definisi 2.3.6 Aksi Transitif

Diberikan G grup beraksi pada himpunan tak kosong A. Aksi grup G pada A disebut transitif jika untuk setiap $a, b \in A$, maka terdapat $g \in G$ sedemikian sehingga $ga = b$ (Dummit, 2004).

Definisi 2.3.7 G-admisibel

Diberikan (G, X) adalah grup aksi transitif dan misalkan R adalah relasi ekuivalensi pada X. R adalah G-admisibel jika dan hanya jika untuk setiap $(x, y) \in R$ berakibat $(gx, gy) \in R$ untuk setiap $g \in R$ (Biggs,1979).

Definisi 2.3.8 Relasi Δ

Relasi Δ adalah relasi ekuivalensi dengan $(x, y) \in \Delta$ jika dan hanya jika $x = y$ (Biggs, 1979).

Definisi 2.3.9 Grup Reguler

Suatu grup aksi disebut regular jika dan hanya jika *stabilizer* pada suatu titik adalah subgrup trivial (Dummit, 2004).

Definisi 2.3.10 Grup Primitif

Suatu grup aksi transitif disebut grup primitif jika dan hanya jika *stabilizer* pada suatu titik adalah subgrup maksimal (Dummit, 2004).

2.4 Grup Sylow

Definisi 2.4.1 p-grup dan p-subgrup

Suatu grup G adalah p-grup jika setiap elemen di G mempunyai orde sebesar pangkat dari p. Suatu subgrup dari grup G adalah p-subgrup dari G jika subgrup tersebut merupakan p-grup (Fraleigh,1999).

Contoh 2.4.2

Diberikan grup $\langle Z_6, +_6 \rangle$, $A = \{\mathbf{0}, \mathbf{3}\}$. Jelas bahwa $A \leq Z_6$. Karena setiap elemen tak nol dari A memiliki orde prima $p = 2$, maka $\langle A, +_6 \rangle$ adalah p-subgrup dari Z_6. Dengan demikian, $\langle A, +_6 \rangle$ adalah p-grup.

Definisi 2.4.3 Sylow p-subgrup

Suatu Sylow p-subgrup P dari grup G adalah p-subgrup maksimal dari G, yaitu p-subgrup yang tidak termuat dalam p-subgrup yang lebih besar (Fraleigh,1999).

Teorema 2.4.4

Diberikan P_1 dan P_2 adalah Sylow p-subgrup dari grup berhingga G, maka P dan P adalah konjugat subgrup dari G (Fraleigh, 1999).

2.5 Homomorfisme dan Isomorfisme

Dari dua grup dengan masing – masing operasi binernya, dapat dibentuk suatu hubungan berbentuk fungsi yang sifatnya mempertahankan operasi dari grup yang pertama pada grup yang kedua. Sehingga, dapat didefinisikan homomorfisme sebagai berikut.

Definisi 2.5.1 Homomorfisme

Suatu homomorfisme dari grup A ke grup B adalah pemetaan φ dari A ke B, sedemikian sehingga $\varphi(ab) = \varphi(a)\,\varphi(b)$ untuk semua $x, y \in A$ (Grillet,2000).

Contoh 2.5.2

Diberikan $(R, +)$ grup bilangan riil dengan operasi penjumlahan biasa dan $(Z, +)$ grup bilangan bulat dengan operasi penjumlahan biasa. Didefinisikan fungsi $\varphi: R \longrightarrow Z$ dengan $\varphi(a) = 0$, untuk setiap $a \in R$. Sehingga, untuk setiap $a, b, \in R$ berlaku $\varphi(a + b) = 0 = 0 + 0 = \varphi(a) + \varphi(b)$.

Oleh karena itu, φ merupakan homomorfisme.

Definisi 2.5.3 Monomorfisme dan Epimorfisme

Monomorfisme adalah suatu homomorfisme yang bersifat injektif. Epimorfisme adalah suatu homomorfisme yang bersifat surjektif (Grillet,2000).

Contoh 2.5.4

Diberikan $(Z, +)$ grup bilangan bulat dengan operasi penjumlahan biasa dan $(R, +)$ grup bilangan riil dengan operasi penjumlahan biasa. Didefinisikan fungsi $\varphi: R \longrightarrow Z$ dengan $\varphi(a) = a$, untuk setiap $a \in Z$.

Karena $\varphi(ab) = ab = \varphi(a)\varphi(b)$, untuk setiap $a, b \in Z$, maka φ merupakan homomorfisme. Jelas bahwa jika $\varphi(a) = \varphi(b) \Longrightarrow a = b$, φ bersifat injektif.

Oleh karena itu, φ adalah suatu monomorfisme.

Contoh 2.5.5

Diberikan $(Z, +)$ grup bilangan bulat dengan operasi penjumlahan biasa dan $(Z_n, +_n)$ grup bilangan bulat modulo n dengan operasi penjumlahan modulo n. Diberikan fungsi $\varphi: Z \longrightarrow Z_n$ dengan $\varphi(a) = a\ (mod\ n)$, untuk setiap $a \in Z$. Misal sebarang $a, b \in Z$ dengan $a = cn + k$ dan $b = dn + l$, sehingga

$$\begin{aligned}
\varphi(ab) &= \varphi(cdn^2 + dkn + cln + kl) \\
&= kl\ (mod\ n) \\
&= k(mod\ n)l(mod\ n) \\
&= \varphi(cn + k)\ \varphi(dn + l) \\
&= \varphi(a)\varphi(b).
\end{aligned}$$

Sehingga φ merupakan homomorfisme. Selanjutnya, akan ditunjukkan bahwa φ bersifat surjektif. Untuk setiap $k(mod\ n) \in Z_n$ maka terdapat $a \in Z$ sedemikian sehingga $a = cn + k$ dengan $c \in Z$. Oleh karena itu, φ adalah suatu epimorfisme.

Definisi 2.5.6 Isomorfisme dan Isomorfik

Suatu isomorfisme grup adalah suatu homomorfisme grup yang bersifat bijektif. Dua grup A dan B adalah isomorfik jika terdapat isomorfisme dari A pada B, hubungan ini dinotasikan $A \cong B$ (Grillet,2000).

Contoh 2.5.7

Diberikan $(R, +)$ grup bilangan bulat dengan operasi penjumlahan biasa dan $(R^+, \cdot)$ grup bilangan riil positif dengan operasi perkalian biasa. Didefinisikan fungsi $\varphi: R \longrightarrow R^+$ dengan $\varphi(a) = e^a$, untuk setiap $a \in R$.

Misal sebarang $a, b \in R$ sehingga $\varphi(a+b) = e^{a+b} = e^a e^b = \varphi(a)\varphi(b)$, diperoleh φ adalah suatu homomorfisme. Selanjutnya, akan ditunjukkan φ bersifat injektif.

Diberikan sebarang $a, b \in R$ dengan $\varphi(a) = \varphi(b)$, maka

$$e^a = e^b$$

$$\Leftrightarrow ln\, e^a = ln\, e^b$$

$$\Leftrightarrow \quad a = b$$

Sehingga, terbukti bahwa φ bersifat injektif.

Selanjutnya, akan ditunjukkan bahwa φ bersifat surjektif.

Untuk setiap $x \in R^+$ maka terdapat $a \in R$ sedemikian sehingga $a = \ln x$ atau $x = e^a$. Akibatnya, φ bersifat surjektif. Oleh karena itu, φ merupakan isomorfisme.

Definisi 2.5.8 Endomorfisme dan Automorfisme

Suatu endomorfisme dari grup G adalah suatu homomorfisme dari G ke G. Suatu automorfisme dari grup G adalah suatu isomorfisme dari G ke G (Grillet,2000).

Contoh 2.5.9

Diberikan G suatu grup dengan elemen identitas e. Didefinisikan fungsi $\varphi: G \longrightarrow G$ dengan $\varphi(a) = e$, untuk setiap $a \in G$. Misal sebarang $a, b \in G$ maka $\varphi(ab) = e = ee = \varphi(a)\, \varphi(b)$. Oleh karena itu, φ adalah suatu endomorfisme.

Contoh 2.5.10

Diberikan G suatu grup dan $\varphi: G \longrightarrow G$ adalah fungsi konjugasi dalam G, yaitu untuk suatu elemen tetap $g \in G$ dan untuk setiap $a \in G$ fungsi φ didefinisikan dengan $\varphi(a) = gag^{-1}$.

Untuk setiap $a, b \in G$, berlaku

$$\begin{aligned} \varphi(ab) &= gabg^{-1} \\ &= gag^{-1}gbg^{-1} \\ &= \varphi(a)\, \varphi(b). \end{aligned}$$

Sehingga, φ adalah homomorfisme.

Selanjutnya, akan dibuktikan bahwa φ bersifat injektif. Diberikan sebarang $a, b \in G$ dengan $\varphi(a) = \varphi(b)$, sehingga,

$$gag^{-1} = gbg^{-1}$$

$$g^{-1}gag^{-1}g = g^{-1}gbg^{-1}g \quad \text{(dioperasikan } g \text{ dari kanan, dan } g^{-1} \text{ dari kiri)}$$

$$a = b.$$

Oleh karena itu, terbukti bahwa φ bersifat injektif.

Selanjutnya, akan dibuktikan bahwa φ bersifat surjektif. Untuk setiap $a \in G$ diperoleh $\varphi(g^{-1}ag) = gg^{-1}agg^{-1} = a$. Sehingga, terbukti bahwa φ bersifat surjektif. Jadi, telah dibuktikan bahwa φ merupakan automorfisme.

Dalam mengkonstruksi Mathieu $M_{11}, M_{12}, M_{22}, M_{23}$ dan M_{24}, yang merupakan subgrup dari grup simetri dengan aturan yang disebut sistem Steiner sebagai berikut.

2.6 Sistem Steiner dan Grup Mathieu

Definisi 2.6.1 Sistem Steiner

Suatu $\mathcal{S}(t,k,v)$ sistem Steiner $(\Omega,\mathcal{S})$ terdiri dari himpunan berhingga Ω dan $\mathcal{S}$ merupakan koleksi himpunan bagian dari Ω yang memenuhi :

1. $|\Omega| = v$,
2. setiap $A \in \mathcal{S}$ memiliki elemen sebanyak k.
3. sebarang $B \subset \Omega$ yang memiliki elemen sebanyak t, termuat tepat satu dalam $A \in \mathcal{S}$.

Elemen dari sistem Steiner disebut blok. Elemen dari himpunan berhingga Ω disebut titik (Nickerson,2002).

Contoh 2.6.2

Elemen – elemen dari sistem Steiner $\mathcal{S}(2,3,7)$ adalah {1,2,3}, {1,4,5}, {1,6,7}, {2,4,6}, {2,5,7}, {3,4,7}, dan {3,5,6}.

Definisi 2.6.3 $M_{11}, M_{12}, M_{22}, M_{23}$ dan M_{24}

Grup Mathieu $M_{11}, M_{12}, M_{22}, M_{23}$ dan M_{24} didefinisikan sebagai berikut.

$M_{11} = \{\sigma \in S_{11} | \sigma(s) \in \mathcal{S}(4,5,11)$ untuk setiap $s \in \mathcal{S}(4,5,11)\}$.

$M_{12} = \{\sigma \in S_{12} | \sigma(s) \in \mathcal{S}(5,6,12)$ untuk setiap $s \in \mathcal{S}(5,6,12)\}$.

$M_{22} = \{\sigma \in S_{22} | \sigma(s) \in \mathcal{S}(3,6,22)$ untuk setiap $s \in \mathcal{S}(3,6,22)\}$.

$M_{23} = \{\sigma \in S_{23} | \sigma(s) \in \mathcal{S}(4,7,23)$ untuk setiap $s \in \mathcal{S}(4,7,23)\}$.

$M_{24} = \{\sigma \in S_{24} | \sigma(s) \in \mathcal{S}(5,8,24)$ untuk setiap $s \in \mathcal{S}(5,8,24)\}$.

Banyaknya elemen grup sebagai berikut :

$|M_{11}| = 7920,$

$|M_{12}| = 95040$,

$|M_{22}| = 443520$,

$|M_{23}| = 10200960$,

$|M_{24}| = 244823040$ (Rubinstein, 2011).

Misalkan suatu himpunan matriks $M(n, q)$ berukuran $n \times n$ dengan entri – entrinya elemen dari suatu lapangan berorde q. Himpunan bagian dari $M(n, q)$ yang semua elemennya memiliki determinan 1 disimbolkan sebagai $SL(n, q)$. Himpunan ini merupakan grup atas operasi perkalian matriks. Center dari grup ini yang dinotasikan sebagai $Z(SL(n, q)$ merupakan grup atas operasi perkalian matriks. Sehingga, dapat didefinisikan $PSL(n, q)$ sebagai berikut.

Definisi 2.6.4 $PSL(V)$ atau $PSL(n, q)$

Diberikan V adalah ruang vektor berdimensi n atas lapangan F berorde q. $PSL(n, q)$ didefinisikan sebagai $SL(n, q)/\, Z(SL(n, q))$ (Biggs, 1979).

Definisi 2.6.5 $PG(V)$ $atau$ $PG(n, q)$

Diberikan V adalah ruang vektor berdimensi n atas lapangan F berorde q. Misalkan relasi ekuivalensi R pada $V\backslash\{0\}$, dengan $x \sim y$ jika dan hanya jika $x = \lambda y$ untuk suatu $\lambda \in F\backslash\{0\}$, untuk setiap $x, y \in V\backslash\{0\}$. $PG(n, q)$ didefinisikan sebagai himpunan kelas – kelas ekuivalensi dari R (Biggs, 1979).