Jurnal Matematika UNAND
Vol. **VIII** No. **1** Hal. 150 – 156
Edisi Mei 2019
ISSN : 2303–291X
©Jurusan Matematika FMIPA UNAND

TEOREMA SYLOW

KHOBERLIN, I MADE ARNAWA, NOVA NOLIZA BAKAR

Program Studi S1 Matematika,
Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Andalas,
Kampus UNAND Limau Manis Padang, Indonesia.
email : khoberlin146@gmail.com

Diterima 9 Maret 2019 Direvisi 7 April 2019 Dipublikasikan 7 Mei 2019

Abstrak. Tulisan ini membahas tentang Teorema Sylow. Misalkan G suatu grup dengan orde hingga, v suatu bilangan bulat positif, dan v membagi orde dari G, yang akan dibahas adalah syarat cukup agar G memuat subgrup dengan orde v.

Kata Kunci: Grup, Orde, Subgrub, Teorema Sylow.

1. Pendahuluan

Teorema Lagrange memiliki hubungan dengan orde dalam grup hingga. Teorema Lagrange menyatakan bahwa jika G suatu grup hingga dan H subgrup dari G, maka orde dari H harus membagi orde dari G. *Converse* teorema Lagrange dalam teorema Cauchy oleh Augustin Louis Cauchy [4] dan teorema Sylow oleh matematikawan Norwegia Ludwig Sylow pada tahun 1872 [2], jika suatu bialangan bulat positif v membagi orde dari grup hingga G, maka dijamin ada H subgrup dari G dengan orde v.

2. Landasan Teori

2.1. *Teori Himpunan*

Definisi 2.1. [5] *Misalkan A dan B suatu himpunan. Himpunan A dan B saling lepas jika dan hanya jika $A \cap B = \varnothing$.*

Definisi 2.2. [3] *Misalkan A dan B suatu himpunan.*

(1) Perkalian kartesian $A \times B$ didefinisikan sebagai himpunan $A \times B = \{(a, b) \mid a \in A, b \in B\}$.
(2) Setiap subset dari $A \times B$ disebut sebagai relasi dari A ke B.
(3) Relasi dari A ke A disebut sebagai relasi di A (pada A).

Definisi 2.3. [1] *Misalkan A suatu himpunan dan $\sim$ suatu relasi pada A. Relasi $\sim$ disebut sebagai relasi ekuivalen pada A, jika:*

(1) Refleksi, jika setiap $a \in A$ *berlaku* $a \sim a$,
(2) Simetri, jika setiap $a, b \in A$ *dengan* $a \sim b$ *berlaku* $b \sim a$,
(3) Transitif, jika setiap $a, b, c \in A$ *dengan* $a \sim b$ *dan* $b \sim c$ *berlaku* $a \sim c$.

Definisi 2.4. [3] *Misalkan* X *suatu himpunan yang tak kosong dan* $\sim$ *suatu relasi ekuivalen pada* X. *Untuk setiap* $a \in X$, *didefinisikan kelas ekuivalen dari* a *sebagai* $cl(a) = \{x \in X | x \sim a\}$ *yaitu kelas ekuivalen dari* a *yang memuat semua anggota* X, *yang terkait dengan* a *pada relasi* $\sim$.

Teorema 2.5. [3] *Misalkan* X *suatu himpunan yang tak kosong dan* $\sim$ *suatu relasi ekuivalen pada* X, *maka untuk setiap* $a, b \in X$ *berlaku:*

(1) $cl(a) \neq \varnothing$,
(2) Berlaku hanya salah satu dari $cl(a) \cap cl(b) = \varnothing$ *atau* $cl(a) = cl(b)$ *yaitu dua kelas ekuivalen yang berlaku hanya salah satu dari berikut sama atau tidak mempunyai elemen,*
(3) $X = \bigcup_{a \in X} cl(a)$.

Definisi 2.6. [3] *Misalkan* X *suatu himpunan yang tidak kosong. Himpunan* K *adalah himpunan dari subset-subset yang tak kosong dari* X *sedemikian sehingga setiap dua anggota dari* K *yang berbeda saling lepas, maka* K *disebut sebagai partisi dari* X, *jika* X *sama dengan hasil gabungan atau union dari semua anggota* K.

Akibat 2.7. [3] *Misalkan* X *suatu himpunan yang tak kosong dengan suatu relasi ekuivalen yang didefinisikan pada* X, *maka himpunan semua kelas-kelas ekuivalen di* X *merupakan partisi dari* X.

2.2. *Pemetaan*

Definisi 2.8. [3] *Misalkan* A *dan* B *suatu himpunan yang tak kosong. Relasi* f *dari* A *ke* B *disebut sebagai pemetaan atau fungsi* f *dari* A *ke* B *dan ditulis sebagai* $f : A \longrightarrow B$ *jika untuk setiap* $a \in A$ *dengan tepat satu* $b \in B$ *sedemikin sehingga* $(a, b) \in f$ *(*b *disebut sebagai peta atau image dari* a *pada* f *yang ditulis sebagai* $b = f(a)$ *dan* a *disebut sebagai prapeta atau pre-image dari* b *pada* f*). Himpunan* A *disebut sebagai domain dari* f *dan* B *disebut sebagai kodomain dari* f. *Subset dari* B *yang memuat hanya anggota-anggota dari* B *yang mempunyai pre-image di* A *disebut sebagai range dari* f.

Definisi 2.9. [4] *Misalkan* A *dan* B *suatu himpunan.*

(1) Pemetaan $f : A \longrightarrow B$ *dikatakan pemetaan satu-satu atau pemetaan injektif jika setiap* $a_1, a_2 \in A$ *dengan* $f(a_1) = f(a_2)$, *maka* $a_1 = a_2$ *(atau jika setiap* $a_1, a_2 \in A$ *dengan* $a_1 \neq a_2$, *maka* $f(a_1) \neq f(a_2)$*).*
(2) Pemetaan $f : A \longrightarrow B$ *dikatakan pemetaan pada atau pemetaan surjektif jika untuk setiap* $b \in B$, *terdapat* $a \in A$ *sedemikian sehingga* $f(a) = b$.

2.3. *Bilangan Bulat*

Definisi 2.10. [3] *Misalkan a suatu bilangan bulat tak nol. Bilangan a dikatakan membagi bilangan bulat b ditulis sebagai $a \mid b$, jika $b = a\ c$ untuk suatu bilangan bulat c.*

Definisi 2.11. [3] *Misalkan p suatu bilangan bulat dan $p > 1$. Bilangan p disebut sebagai bilangan prima jika hanya 1 dan p yang membagi p.*

2.4. *Grup*

Definisi 2.12. [5] *Misalkan G suatu himpunan yang tak kosong. Pemetaan dari $G \times G$ ke G disebut operasi biner pada G.*

Definisi 2.13. [1] *Misalkan G suatu himpunan tak kosong dan $*$ suatu operasi biner yang didefinisikan di G. Unsur-unsur di G dikatakan membentuk grup terhadap operasi $*$ jika memenuhi:*

(1) Untuk setiap $a, b \in G$ berlaku $a * b \in G$ (G bersifat tertutup terhadap operasi $*$),
(2) Untuk setiap $a, b, c \in G$ berlaku $a * (b * c) = (a * b) * c$ (G bersifat asosiatif terhadap operasi $*$),
(3) Terdapat suatu unsur di G yang dilambangkan dengan e sehingga untuk setiap $a \in G$ berlaku $a * e = e * a = a$ (G memiliki unsur identitas terhadap operasi $*$),
(4) Untuk setiap $a \in G$, ada suatu unsur di G yang dilambangkan dengan a^{-1} sehingga berlaku $a * a^{-1} = a^{-1} * a = e$ (setiap unsur di G mempunyai invers terhadap operasi $*$).

Catatan:

(1) Untuk selanjutnya $a * b$ ditulis sebagai $a\ b$.
(2) Jika setiap unsur di G membentuk grup terhadap operasi biner di G, maka G suatu grup.

Definisi 2.14. [3] *Misalkan G suatu grup. Banyaknya unsur pada grup G disebut orde dari G dan dinotasikan sebagai $o(G)$ atau $|G|$.*

Lema 2.15. [3] *Misalkan G suatu grup, maka:*

(1) Elemen identitas di G tunggal,
(2) Invers dari setiap $a \in G$ tunggal,
(3) $\left(a^{-1}\right)^{-1} = a$ untuk setiap $a \in G$, dimana a^{-1} merupakan invers dari a di G,
(4) $(a\ b)^{-1} = b^{-1}\ a^{-1}$ untuk setiap $a, b \in G$,
(5)(a) Jika $a\ b = a\ c$, maka $b = c$ untuk setiap $a, b, c \in G$,
(b) Jika $b\ a = c\ a$, maka $b = c$ untuk setiap $a, b, c \in G$.

2.5. *Subgrup*

Definisi 2.16. [3] *Misalkan G suatu grup dan H subset yang tak kosong dari G. Himpunan H disebut subgrup dari G jika H membentuk grup terhadap operasi biner di G.*

Teorema 2.17. [5] *Misalkan G suatu grup dan H subgrup dari G. Unsur identitas di H sama dengan unsur identitas di G.*

Teorema 2.18. [3] *Misalkan G suatu grup dan H subset yang tak kosong dari G. Himpunan H disebut subgrup dari G jika dan hanya jika*

(1) Untuk setiap $a, b \in H$ berlaku $a\ b \in H$,
(2) Untuk setiap $a \in H$ berlaku $a^{-1} \in H$.

Definisi 2.19. [3] *Misalkan G suatu grup dan H subgrup dari G. Untuk setiap $a, b \in G$, a dikatakan kongruen dengan b mod H ditulis sebagai $a \cong b \bmod H$ jika $a\ b^{-1} \in H$.*

Teorema 2.20. [3] *Misalkan G suatu grup, H subgrup dari G, dan $a, b \in G$. Didefinisikan relasi kongruen modulo H sebagai berikut $a \cong b \bmod H$ jika $a\ b^{-1} \in H$. Relasi kongruen modulo H adalah suatu relasi ekuivalen di G.*

Definisi 2.21. [3] *Misalkan G suatu grup dan H subgrup dari G dan relasi kongruen modulo H suatu relasi ekuivalen pada G. Untuk setiap $a \in G$ didefinisikan kelas ekuivalen dari a sebagai himpunan*

$$cl\,(a) \ = \ \{x \in G | x \cong a \bmod H\}\,.$$

Definisi 2.22. [3] *Misalkan G suatu grup, H subgrup dari G, dan $a \in G$.*

(1) Himpunan $Ha \ = \ \{h\ a | h \in H\}$ disebut koset kanan dari H di G.
(2) Himpunan $aH \ = \ \{a\ h | h \in H\}$ disebut koset kiri dari H di G.

Teorema 2.23. [3] *Misalkan G suatu grup, H subgrup dari G, dan $a \in G$, maka $Ha \ = \ \{x \in G | x \cong a \bmod H\} \ = \ cl\,(a)$.*

Akibat 2.24. [3] *Misalkan G suatu grup dan H subgrup dari G, maka untuk setiap $a, b \in G$ berlaku:*

(1) $Ha \neq \varnothing$,
(2) Berlaku hanya salah satu dari $Ha \cap Hb \ = \ \varnothing$ atau $Ha \ = \ Hb$ yaitu dua kelas ekuivalen yang berlaku hanya salah satu dari berikut sama atau tidak mempunyai elemen,
(3) $G \ = \ \bigcup_{a \in G} Ha$.

Teorema 2.25. [3] *Misalkan G suatu grup hingga dan H subgrup dari G, maka $o\,(H)$ membagi $o\,(G)$.*

Lema 2.26. [1] *Misalkan G suatu grup dan H subgrup dari G. Terdapat korespondensi satu-satu antara setiap dua buah koset kanan dari H di G.*

Teorema 2.27. [3] *Misalkan G suatu grup, H subgrup dari G, dan $a, b \in G$, maka:*

(1) (a) $Ha = H$ *jika dan hanya jika* $a \in H$*;*
(b) $aH = H$ *jika dan hanya jika* $a \in H$*,*
(2) (a) $Ha = Hb$ *jika dan hanya jika* $a\, b^{-1} \in H$*;*
(b) $aH = bH$ *jika dan hanya jika* $a^{-1}\, b \in H$*.*

3. Teorema Sylow

3.1. *Teorema Sylow Pertama*

Teorema 3.1. [2] *Misalkan G suatu grup hingga, p suatu bilangan prima, dan p^α membagi orde dari G, maka G memuat subgrup dengan orde p^α.*

Bukti. Misalkan G suatu grup hingga, p suatu bilangan prima dan p^α membagi orde dari G, akan ditunjukkan G memuat subgrup dengan orde p^α. Untuk menunjukkan G memuat subgrup dengan orde p^α, dilakukan langkah-langkah pembuktian sebagai berikut:

(1) Penjelasan *combinatorial*, yaitu:
   (a) Menunjukkan bahwa terdapat s sehingga $p^s \mid (p^\alpha - k)$ dan $p^s \mid (p^\alpha m - k)$ untuk setiap $k = 1, 2, \cdots, p^\alpha - 1$,
   (b) Menunjukkan bahwa terdapat r sehingga $p^r \mid \binom{p^\alpha m}{p^\alpha}$ dan $p^r \mid m$.

(2) Pembentukan H subgrup dari G, yaitu:
   (a) Menjelaskan adanya H,
   (b) Menunjukkan bahwa H subgrup dari G.

(3) Pembuktian orde dari H adalah p^α, yaitu:
   (a) Menunjukkan bahwa $p^\alpha \leq o(H)$,
   (b) Menunjukkan bahwa $o(H) \leq p^\alpha$. □

Contoh 3.2. Himpunan K suatu grup berorde 12600 atau $o(K) = 12600$. Oleh karena $12600 = 2^3\ 3^2\ 5^4\ 7$, maka $o(K) = 2^3\ 3^2\ 5^4\ 7$. Berdasarkan Teorema 3.1 diperoleh K mempunyai paling sedikit satu subgrup yang berorde $1, 2, 2^2, 2^3, 3, 3^2, 5, 5^2, 5^3, 5^4,$ *atau* 7. Ada kemungkinan terdapat subgrup dari K yang berorde selain dari 1, 2, 2^2, 2^3, 3, 3^2, 5, 5^2, 5^3, 5^4, dan 7, namun Teorema Sylow tidak menjamin adanya subgrup tersebut.

3.2. *Sylow p-subgrup*

Definisi 3.3. [3] *Misalkan G suatu grup hingga, p suatu bilangan prima, dan n suatu bilangan bulat tak negatif. p^n membagi orde dari G dan p^{n+1} tidak membagi orde dari G, maka H subgrup dari G sedemikian sehingga $o(H) = p^n$ disebut Sylow p-subgrup dari G.*

Contoh 3.4. Himpunan $Z_{12} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}, \overline{11}\}$ suatu himpunan bilangan bulat modulo 12. Didefinisikan penjumlahan modulo 12 ($+_{12}$) di Z_{12} sebagai berikut $\overline{a} +_{12} \overline{b} = \overline{c}$ dimana c adalah sisa dari $a + b$ setelah dibagi 12. Berdasarkan

Definisi 2.14, Orde dari Z_{12} atau $o(Z_{12})$ adalah 12. Himpunan $A = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\}$ subgrup dari Z_{12}. Berdasarkan Definisi 2.14, Orde dari A atau $o(A)$ adalah 6. 6 tidak dapat dibentuk dalam perpangkatan bilangan prima, maka A bukan Sylow p-subgrup dari Z_{12}. Himpunan $B = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$ subgrup dari Z_{12}. Berdasarkan Definisi 2.14, Orde dari B atau $o(B)$ adalah 4. $4 = 2^2$ dapat dibentuk dalam perpangkatan bilangan prima, $2^2 \mid o(Z_{12})$, dan $2^{2+1} \nmid o(Z_{12})$, maka B merupakan Sylow p-subgrup dari Z_{12}. Himpunan $C = \{\overline{0}, \overline{4}, \overline{8}\}$ subgrup dari Z_{12}. Berdasarkan Definisi 2.14, Orde dari C atau $o(C)$ adalah 3. $3 = 3^1$ dapat dibentuk dalam perpangkatan bilangan prima, $3^1 \mid o(Z_{12})$, dan $3^{1+1} \nmid o(Z_{12})$, maka C merupakan Sylow p-subgrup dari Z_{12}.

Akibat 3.5. [3] *Misalkan G suatu grup hingga. Jika p suatu bilangan prima sedemikian sehingga $p^n \mid o(G)$ dan $p^{n+1} \nmid o(G)$, maka ada Sylow p-subgrup dari G.*

Bukti. Misalkan G suatu grup hingga, p suatu bilangan prima, $p^n \mid o(G)$ dan $p^{n+1} \nmid o(G)$. Berdasarkan Definisi 3.3 dan Teorema 3.1 diperoleh ada Sylow p-subgrup dari G. □

4. Kesimpulan

(1) Misalkan G suatu grup hingga dan p suatu bilangan prima. Jika $p^\alpha \mid o(G)$, maka ada H subgrup dari G sedemikian sehingga $o(H) = p^\alpha$.
(2) Misalkan G suatu grup hingga, p suatu bilangan prima, dan n suatu bilangan bulat tak negatif. p^n membagi orde dari G dan p^{n+1} tidak membagi orde dari G, maka H subgrup dari G sedemikian sehingga $o(H) = p^n$ disebut Sylow p-Subgrup dari G.
(3) Misalkan G suatu grup hingga. Jika p suatu bilangan prima sedemikian sehingga $p^n \mid o(G)$ dan $p^{n+1} \nmid o(G)$, maka ada Sylow p-subgrup dari G.

5. Ucapan Terima kasih

Penulis mengucapkan terima kasih kepada Bapak Dr. Mahdhivan Syafwan, Ibu Dr. Yanita, dan Ibu Izzati Rahmi HG, M.Si yang telah memberikan masukan dan saran dalam penyempurnaan penulisan artikel ini.

Daftar Pustaka

[1] Heirstein, I.N. 1975. *Topic in Algebra; edisi ke-2*. John Wiley and Sons, New York
[2] Kammuller, F. dan L.C. Paulson. 1999. A Formal proof of Sylow's theorem. *Journal of Automated Reasoning*. **23**: 235 – 265
[3] Khanna, V.K. dan S.K. Bhambri. 1993. *A Course in Abstract Algebra*. Vikas Publishing House PVT LTD, New Delhi
[4] Meo, M. 2004. The Mathematical Life of Cauchy's Group Theorem. *Historia Mathematica*. **31**: 196 – 221
[5] Morris, D.W. dan J. Morris. 2013. *Proofs and Concepts The Fundamental of Abstract Mathematics*. University of Lethbridge, New York

[6] Raisinghania, M.D. dan R.S. Aggarwal. 1980. *Modern Algebra; edisi ke-1*. S. Chand and Company LTD, New Delhi