SUATU BUKTI DARI WEDDERBURN'S LITTLE THEOREM

SKRIPSI

PUTRI ANGGRAYNI
07134017

JURUSAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS ANDALAS
PADANG 2012

KATA PENGANTAR

بسم الله الرحمن الرحيم

Alhamdulillah, puji syukur tak henti-hentinya diucapkan ke hadirat Allah SWT atas limpahan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan penulisan skripsi dengan judul **"Suatu Bukti dari *Wedderburn's Little Theorem*"** yang merupakan salah satu syarat untuk memperoleh gelar Sarjana Sains (S.Si.) di Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Andalas Padang. Shalawat dan salam semoga selalu tercurah kepada Rasulullah SAW yang telah menebar ilmu dan iman dalam cahaya Islam yang beliau bawa.

Penulis menyadari sepenuhnya bahwa penyusunan skripsi ini tidak terlepas dari dukungan, dorongan, kerjasama maupun bimbingan dari berbagai pihak. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Bapak Dr. Admi Nazra selaku Dosen Pembimbing yang dengan sabar mengarahkan penulis dalam menyelesaikan penulisan skripsi ini melalui bimbingan dan diskusi yang sangat bermanfaat.

2. Ibu Dr. Lyra Yulianti, Bapak Dr. Muhafzan, dan Bapak Dr. Ahmad Iqbal Baqi selaku Dosen Penguji yang telah memberi masukan dan saran kepada penulis dalam penyempurnaan penulisan skripsi ini.

3. Ibu Dr. Maiyastri selaku Dosen Pembimbing Akademik yang telah memberi pengarahan, nasehat, motivasi dan ilmu selama penulis belajar di Jurusan Matematika FMIPA Unand.

4. Bapak Dr. Admi Nazra selaku Ketua Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Andalas.

5. Seluruh Bapak/Ibu Dosen Jurusan Matematika FMIPA Universitas Andalas yang telah membagi ilmunya kepada penulis dalam proses perkuliahan, beserta seluruh Karyawan/wati Jurusan Matematika yang telah membantu selama penulis melaksanakan studi di Universitas Andalas.

6. Meri Komala Sari, S.Si., Resti Meirita, S.Si., dan Rita Gusmelia, S.Farm., yang senantiasa menyuntikkan semangat juang padaku.

7. *My Narcis Family*: Pipit Oktafia, S.Hum., Andari Yekadria, S.T., Hadi Pangestu, S.Kom., Ekho Wisa Putra, A.Md., Gusri Rahayu, Teresia, Aulia Laratika Rizal, Delsye M. Asmarani, Kartika Ramadhanty, S.T., dan Dwi Pharah Dilla.

8. Partner kerjaku yang baik hati, Uswatun Hasanah, S.Si., beserta seluruh rekan asisten Laboratorium Statistika dan Komputasi Jurusan Matematika FMIPA Universitas Andalas.

9. Semua pihak yang turut membantu hingga selesainya skripsi ini, terutama teman-teman angkatan 2007, 2008, 2009, 2010, dan 2011 di Jurusan Matematika FMIPA Unand.

Rasa hormat yang dalam kepada yang terkasih papa Syafrizal Umar dan mama Maya Sari yang senantiasa memberi kasih sayang, do'a, semangat, kekuatan luar biasa, dan dukungan. Tidak terlupa kepada ketiga adikku tersayang, Silvia

Dewi, Tri Yosi Rahmadhani, dan Yoga Fernanda Syaputra yang telah memberikan motivasi dalam menyelesaikan studiku.

Penulis selalu terbuka terhadap sumbangan pemikiran baik kritik maupun saran yang membangun untuk menyempurnakan skripsi ini. Penulis sangat menyadari bahwa skripsi ini masih jauh dari kesempurnaan dan tidak luput dari kekurangan karena terbatasnya ilmu dan pengalaman yang penulis miliki. Kritik dan saran tersebut dapat disampaikan melalui e-mail di `putri.anggrayni@gmail.com`.

Akhir kata, penulis berharap semoga skripsi ini dapat memberikan sesuatu yang bermanfaat bagi semua pihak yang membacanya. Aamiin.

Padang, Oktober 2012

Putri Anggrayni

ABSTRAK

Wedderburn's Little Theorem menyatakan bahwa setiap gelanggang pembagian yang mempunyai sejumlah berhingga unsur adalah komutatif, sehingga merupakan suatu lapangan. Teorema ini telah dibuktikan oleh banyak orang dengan berbagai ide berbeda. Dalam skripsi ini akan dikaji suatu bukti yang berdasarkan pada dua fakta mengenai lapangan berhingga.

Kata kunci: *Gelanggang pembagian, lapangan berhingga.*

DAFTAR ISI

DAFTAR NOTASI

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Gelanggang merupakan struktur penting dalam aljabar modern. Jika setiap unsur tak-nol dari suatu gelanggang R membentuk grup terhadap operasi perkalian, maka R disebut gelanggang pembagian (*division ring*). Dengan demikian satu hal yang hilang dari R untuk menjadi suatu lapangan adalah komutatifitas terhadap perkalian. Contoh gelanggang pembagian non-komutatif yang dikenal adalah gelanggang *quaternion* yang ditemukan oleh Hamilton.

Pada tahun 1905 seorang matematikawan Skotlandia, Joseph H. M. Wedderburn, membuktikan teorema yang dinyatakan sebagai berikut: "Setiap gelanggang pembagian berhingga merupakan suatu lapangan". Teorema yang lebih dikenal sebagai *Wedderburn's Little Theorem* ini telah dibuktikan oleh banyak orang dengan berbagai ide berbeda. Wedderburn sendiri telah memberikan tiga buah bukti dari teorema ini pada 1905, dan bukti lainnya diberikan oleh Leonard E. Dickson pada tahun yang sama. Selanjutnya Emil Artin, Hans Zassenhaus, Nicolas Bourbaki, dan Ernst Will adalah nama-nama terkenal yang juga telah membuktikan teorema ini.

Hingga saat ini, pembuktian *Wedderburn's Little Theorem* masih dilakukan

oleh banyak orang. Hal ini menunjukkan bahwa *Wedderburn's Little Theorem* merupakan topik yang sangat menarik untuk dikaji. Oleh karena itu, penulis tertarik untuk mengkaji suatu bukti dari *Wedderburn's Little Theorem.*

1.2 Perumusan Masalah

Berdasarkan uraian pada latar belakang, yang menjadi permasalahan dalam skripsi ini adalah bagaimanakah bukti dari *Wedderburn's Little Theorem.*

1.3 Pembatasan Masalah

Permasalahan yang akan dibahas dalam skripsi ini dibatasi tanpa melibatkan bilangan kompleks atau teori permutasi.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk mengkaji suatu bukti dari *Wedderburn's Little Theorem.*

1.5 Sistematika Penulisan

Penulisan skripsi ini terdiri atas empat bab. Bab I merupakan pendahuluan yang memuat latar belakang masalah, perumusan masalah, pembatasan masalah, tujuan penelitian, dan sistematika penulisan. Bab II merupakan landasan teori yang menjadi dasar untuk pembahasan *Wedderburn's Little Theorem.* Bab III memuat pembahasan mengenai bukti dari *Wedderburn's Little Theorem.* Bab IV

merupakan kesimpulan dari pembahasan beserta saran untuk penelitian selanjutnya.

BAB II

LANDASAN TEORI

Pada bab ini akan diberikan beberapa teori yang relevan dengan permasalahan yang telah dikemukakan di Bab I.

2.1 Teori Bilangan

Pembahasan mengenai suatu sistem aljabar tidak terlepas dari penggunaan beberapa teori bilangan. Oleh karena itu, pada subbab ini akan diberikan beberapa definisi dan teorema yang berkaitan dengan teori bilangan. Namun sebelumnya dikemukakan keberadaan bilangan bulat dalam himpunan.

Bilangan bulat adalah bilangan yang berada dalam himpunan

$$\{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\},$$

dan himpunan yang berisikan bilangan-bilangan bulat ini dilambangkan dengan $\mathbb{Z}$ [7]. Bilangan bulat memainkan peranan utama dalam pembelajaran mengenai teori bilangan. Properti di bawah ini menyatakan suatu sifat dari bilangan bulat positif.

Properti 2.1.1. [7] **Well-Ordering Property**

Setiap himpunan tak kosong dari bilangan bulat positif mempunyai unsur terkecil.

Sifat ini akan digunakan dalam pembuktian beberapa dalil.

Definisi 2.1.1. [7]

Jika a dan b adalah bilangan bulat dengan $a \neq 0$, maka a dikatakan membagi b jika terdapat suatu bilangan bulat c sedemikian sehingga $b = ac$. Jika a membagi b, a juga disebut pembagi atau faktor dari b dan b disebut kelipatan dari a.

Jika a membagi b maka ditulis $a \mid b$, dan jika a tidak membagi b maka ditulis $a \nmid b$.

Teorema 2.1.2. [7]

Jika a, b, c adalah bilangan bulat dengan $a \mid b$ dan $b \mid c$, maka $a \mid c$.

Bukti. Karena $a \mid b$ dan $b \mid c$, maka terdapat bilangan bulat e dan f sedemikian sehingga $ae = b$ dan $bf = c$. Oleh sebab itu, $c = bf = (ae)f = a(ef)$ dan disimpulkan bahwa $a \mid c$. ■

Teorema 2.1.3. [7]

Jika a, b, m, n adalah bilangan bulat, dan jika $c \mid a$ dan $c \mid b$, maka $c \mid (ma + nb)$.

Bukti. Karena $c \mid a$ dan $c \mid b$, maka terdapat bilangan bulat e dan f sedemikian sehingga $ce = a$ dan $cf = b$. Oleh sebab itu, $ma + nb = m(ce) + n(cf) = c(me + nf)$. Hal ini mengakibatkan $c \mid (ma + nb)$. ■

Teorema 2.1.4. [7]

Jika a dan b adalah bilangan bulat sedemikian sehingga $b > 0$, maka terdapat suatu bilangan bulat q dan r sedemikian sehingga $a = bq + r$ dengan $0 \leq r < b$, dimana q dan r adalah tunggal.

Bukti. Misalkan terdapat suatu himpunan $S = \{a - bk | k \in \mathbb{Z}\}$, dan misalkan

T adalah himpunan semua bilangan bulat non-negatif di S. Himpunan T tidak kosong, karena $a - bk$ positif jika k adalah suatu bilangan bulat dengan $k < \frac{a}{b}$.

Berdasarkan *Well-Ordering Property*, T mempunyai unsur terkecil $r = a - bq$. Jelaslah bahwa $r \geq 0$. Jika $r \geq b$ maka $r > r - b = a - bq - b = a - b(q+1) \geq 0$. Hal ini bertentangan dengan pemilihan $r = a - bq$ sebagai bilangan bulat non-negatif terkecil dengan bentuk $a - bk$. Oleh karena itu $0 \leq r < b$.

Untuk menunjukkan bahwa nilai q dan r tunggal, asumsikan bahwa terdapat dua persamaan $a = bq_1 + r_1$ dan $a = bq_2 + r_2$, dengan $0 \leq r_1 < b$ dan $0 \leq r_2 < b$. Dengan mensubstitusikan persamaan kedua pada persamaan pertama, diperoleh $0 = b(q_1 - q_2) + (r_1 - r_2)$. Dengan demikian, $r_2 - r_1 = b(q_1 - q_2)$. Hal ini menunjukkan bahwa b membagi $r_2 - r_1$. Karena $0 \leq r_1 < b$ dan $0 \leq r_2 < b$, diperoleh $-b < r_2 - r_1 < b$. Oleh sebab itu, b dapat membagi $r_2 - r_1$ hanya jika $r_2 - r_1 = 0$, atau dengan perkataan lain, jika $r_1 = r_2$. Karena $bq_1 + r_1 = bq_2 + r_2$ dan $r_1 = r_2$, dapat dilihat pula bahwa $q_1 = q_2$. Ini menunjukkan bahwa hasil bagi q dan sisa bagi r adalah tunggal. ■

Teorema di atas lebih dikenal sebagai Algoritma Pembagian.

Definisi 2.1.5. [7]

Suatu prima adalah suatu bilangan bulat positif yang lebih besar dari 1 *dan tidak dapat dibagi oleh bilangan bulat positif selain* 1 *dan dirinya sendiri.*

Definisi 2.1.6. [7]

Misalkan a dan b adalah bilangan bulat. Jika $n \in \mathbb{Z}$ dengan $n \mid a$ dan $n \mid b$, maka n disebut faktor persekutuan dari a dan b.

Definisi 2.1.7. [7]

Misalkan a dan b adalah bilangan bulat. Faktor persekutuan terbesar (fpb) dari a dan b, dinotasikan dengan (a, b), didefinisikan sebagai bilangan bulat non-negatif d sedemikian sehingga

1. *$d \mid a$ dan $d \mid b$ dan*
2. *jika $e \mid a$ dan $e \mid b$ maka $e \mid d$.*

Teorema 2.1.8. [7]

Faktor persekutuan terbesar dari bilangan bulat a dan b, tak keduanya 0, adalah bilangan bulat positif terkecil yang merupakan kombinasi linier dari a dan b.

Bukti. Jika $a = b = 0$, maka $(a, b) = 0 = 0s + 0t$ (untuk suatu s dan t), maka teorema benar. Dengan demikian akan diasumsikan bahwa $a \neq 0$.

Misalkan $S = \{ax + by | x, y \in \mathbb{Z}, ax + by > 0\}$. Jika $x = a$ dan $y = 0$, maka $ax + by = a^2 + b0 > 0$, sehingga $S \neq \emptyset$. Berdasarkan *Well-Ordering Property* S mempunyai bilangan bulat positif terkecil d sedemikian sehingga $d = as + bt$ untuk suatu bilangan bulat s dan t.

Berdasarkan Teorema 2.1.4, terdapat bilangan bulat q dan r sedemikian sehingga $a = dq + r, 0 \leq r < d$; akibatnya $r = a - dq = a - (as + bt)q = a(1 - sq) + b(-tq)$. Jika $0 < r$, maka $r \in S$. Namun hal ini akan bertentangan dengan fakta bahwa d adalah bilangan bulat terkecil di S. Oleh sebab itu, $r = 0$ dan $a = dq$, atau dengan perkataan lain, $d \mid a$. Dengan cara yang sama dapat diperoleh $d \mid b$. Selanjutnya dari persamaan $d = as + bt$ dan Teorema 2.1.3, jika terdapat $e \in \mathbb{Z}$ sedemikian sehingga $e \mid a$ dan $e \mid b$, maka $e \mid (as + bt) = d$. Dengan

demikian, terbukti bahwa $d = (a, b)$. ■

Definisi 2.1.9. [7]

Bilangan bulat a dan b dikatakan relatif prima jika $(a, b) = 1$.

Jelaslah bahwa jika p prima dan $p \nmid a$, maka $(a, p) = 1$ dan a dan p relatif prima.

Lema 2.1.10. [6]

Misalkan p adalah suatu bilangan prima dan $p \mid ab$, dengan $a, b \in \mathbb{Z}$, maka $p \mid a$ atau $p \mid b$.

Bukti. Andaikan $p \nmid a$, maka $(a, p) = 1$. Berdasarkan Teorema 2.1.8, terdapat bilangan bulat s dan t sedemikian sehingga $1 = as + pt$, maka $b = b(as + pt) = (ab)s + p(bt)$. Karena $p \mid ab$ dan $p \mid p$, jelaslah bahwa $p \mid (ab)s + p(bt)$, sehingga diperoleh $p \mid b$. ■

Definisi 2.1.11. [7]

Misalkan m adalah suatu bilangan bulat positif. Jika a dan b adalah bilangan bulat, maka a dikatakan kongruen ke b modulo m jika $m \mid (a - b)$.

Jika a kongruen ke b modulo m, maka ditulis $a \equiv b(\mod m)$. Jika $m \nmid (a - b)$, maka ditulis $a \not\equiv b(\mod m)$.

Teorema 2.1.12. [7]

Jika a dan b adalah bilangan bulat, maka $a \equiv b(\mod m)$ jika dan hanya jika terdapat suatu bilangan bulat k sedemikian sehingga $a = b + km$.

Bukti. Jika $a \equiv b(\mod m)$, maka $m \mid (a - b)$. Ini berarti bahwa terdapat suatu bilangan bulat k dengan $km = a - b$ sedemikian sehingga $a = b + km$.

Sebaliknya, jika terdapat suatu k dengan $a = b + km$, maka $km = a - b$. Oleh karena itu, $m \mid (a - b)$, dan mengakibatkan $a \equiv b(\mod m)$. ■

Definisi 2.1.13. [6]

Himpunan bilangan bulat $\mathbb{Z}_m = \{0, 1, \cdots, m-1\}$ *disebut sebagai himpunan dari sisaan positif terkecil modulo* m.

Contoh 2.1.1. *Misalkan* $A = \{a, 2a, \cdots, (m-1)a\}$, *maka himpunan* $\{1, 2, \cdots, (m-1)\}$ *adalah sisaan positif terkecil modulo* m *dari himpunan* A.

Teorema 2.1.14. [7]

Jika p *adalah prima dan* a *adalah suatu bilangan bulat positif dengan* $p \nmid a$, *maka* $a^{p-1} \equiv 1 (mod\ p)$.

Bukti. Misalkan terdapat suatu himpunan bilangan bulat $S = \{a, 2a, \cdots, (p-1)a\}$. Jika $p \mid ja$, dengan $j = 1, 2, \cdots, p-1$ dan $ja \in S$, maka berdasarkan Lema 2.1.10, $p \mid j$, karena $p \nmid a$. Hal ini tidaklah mungkin karena $1 \leq j \leq p-1$. Selanjutnya asumsikan bahwa $ja \equiv ka(\mod p)$, dimana $1 \leq j < k \leq p-1$. Karena $ja \equiv ka(\mod p)$, maka $p \mid (ja - ka) = a(j-k)$. Karena $p \nmid a$, maka $p \mid (j-k)$. Dengan demikian $j \equiv k(\mod p)$. Hal ini juga mustahil karena j dan k adalah bilangan bulat yang kurang dari $p-1$.

Karena setiap unsur himpunan $\{a, 2a, \cdots, (p-1)a\}$ tidak dapat dibagi oleh p dan tidak ada dua buah bilangan bulat dari himpunan tersebut yang kongruen modulo p, maka sisaan positif terkecil modulo p dari himpunan tersebut (Definisi 2.1.13) adalah $\{1, 2, \cdots, p-1\}$. Dengan demikian diperoleh

$$a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1)(\mod p),$$

sehingga

$$(p-1)!a^{p-1} \equiv (p-1)!(\mod p).$$

Karena $(p-1)!a^{p-1} \equiv (p-1)!(\mod p)$, maka $p \mid [(p-1)!a^{p-1} - (p-1)!] = (p-1)!(a^{p-1}-1)$, sehingga diperoleh $p \mid (a^{p-1}-1)$ (karena $p \nmid (p-1)!$). Oleh sebab itu, jelaslah bahwa $a^{p-1} \equiv 1(\mod p)$. ■

Teorema ini lebih dikenal dengan nama *Fermat's Little Theorem.*

2.2 Grup

Gelanggang merupakan suatu grup penjumlahan *abelian*, bersamaan dengan operasi biner kedua, yaitu perkalian. Oleh karena itu pembahasan mengenai gelanggang mestilah didahului dengan beberapa teori grup.

Definisi 2.2.15. [5]

Suatu himpunan tak kosong G dikatakan membentuk suatu grup jika di G didefinisikan suatu operasi biner yang dinotasikan dengan $*$ sedemikian sehingga

1. *Untuk setiap $a, b \in G$ berlaku $a * b \in G$ (tertutup);*
2. *Untuk setiap $a, b, c \in G$ berlaku $a * (b * c) = (a * b) * c$ (hukum asosiatif);*
3. *Terdapat suatu unsur $e \in G$ sedemikian sehingga $a * e = e * a = a$ untuk semua $a \in G$ (eksistensi unsur identitas di G);*
4. *Untuk setiap $a \in G$ terdapat suatu unsur $a^{-1} \in G$ sehingga $a * a^{-1} = a^{-1} * a = e$ (eksistensi invers di G).*

Contoh 2.2.2. *Bilangan bulat membentuk grup terhadap operasi penjumlahan biasa dari bilangan bulat.*

Definisi 2.2.16. [6]

*Suatu grup dengan sejumlah berhingga unsur disebut grup berhingga (*finite group*); jika tidak maka disebut grup takhingga (*infinite group*). Banyaknya unsur dari suatu grup G disebut orde dari G dan dinotasikan dengan $|G|$.*

Jika suatu grup G berhingga dan G memuat tepat n unsur, maka orde dari G adalah n atau $|G| = n$. Jika G tak berhingga, maka $|G| = \infty$.

Definisi 2.2.17. [5]

Suatu grup G dikatakan abelian *(atau* komutatif*) jika untuk setiap $a, b \in G$ berlaku $a * b = b * a$.*

Contoh 2.2.3. *Misalkan $\mathbb{Z}_6$ adalah himpunan bilangan bulat modulo 6 dan $+_6$ adalah operasi penjumlahan pada bilangan bulat modulo 6. Karena $+_6$ bersifat komutatif, maka $\mathbb{Z}_6$ merupakan grup* abelian.

Lema 2.2.18. [5]

Jika G adalah suatu grup, maka

1. *Unsur identitasnya tunggal;*
2. *Setiap $a \in G$ mempunyai invers yang tunggal;*
3. *Untuk setiap $a \in G$, $(a^{-1})^{-1} = a$;*
4. *Untuk semua $a, b \in G$, $(a * b)^{-1} = b^{-1} * a^{-1}$.*

Bukti. Misalkan G adalah suatu grup.

1. Misalkan e dan e' adalah unsur identitas di G. Pandang e sebagai unsur identitas dan $e' \in G$, maka $e * e' = e'$ dan $e' * e = e'$. Selanjutnya pandang e' sebagai unsur indentitas dan $e \in G$, maka $e * e' = e$ dan $e' * e = e$. Oleh sebab itu diperoleh $e = e * e' = e'$ atau $e = e'$. Dengan demikian, unsur identitas G adalah tunggal.

2. Misalkan $a \in G$, serta x dan y merupakan invers dari a. Pandang x sebagai invers dari a, maka $a * x = e$ dan $x * a = e$. Pandang y sebagai invers dari a, maka $a * y = e$ dan $y * a = e$. Perhatikan bahwa $x = x * e = x * (a * y) = (x*a)*y = e*y = y$ atau $x = y$. Dengan demikian, setiap $a \in G$ mempunyai invers yang tunggal.

3. Misalkan $a \in G$. Perhatikan bahwa $a * a^{-1} = e$ dan $a^{-1} * a = e$. Ini berarti bahwa invers dari a^{-1} adalah a atau $(a^{-1})^{-1} = a$.

4. Misalkan $a, b \in G$, maka a^{-1} dan b^{-1} berturut-turut merupakan invers dari a dan b. Perhatikan bahwa $(a*b)*(b^{-1}*a^{-1}) = a*(b*b^{-1})*a^{-1} = a*e*a^{-1} = a*a^{-1} = e$. Selanjutnya $(b^{-1}*a^{-1})*(a*b) = b^{-1}*(a^{-1}*a)*b = b^{-1}*e*b = b^{-1}*b = e$. Oleh karena itu diperoleh bahwa invers dari $(a*b) = b^{-1}*a^{-1}$ atau $(a*b)^{-1} = b^{-1}*a^{-1}$. ■

Definisi 2.2.19. [5]

Suatu subhimpunan tak kosong H dari suatu grup G dikatakan subgrup dari G jika H membentuk grup terhadap operasi biner yang didefinisikan di G.

Berdasarkan definisi di atas, jelaslah bahwa jika H merupakan subgrup dari G dan K merupakan subgrup dari H, maka K merupakan subgrup dari G.

Lema 2.2.20. [5]

Suatu subhimpunan tak kosong H dari suatu grup G merupakan suatu 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 $a^{-1} \in H$.*

Bukti. Jika H merupakan subgrup dari G, maka jelaslah bahwa (1) dan (2) dipenuhi.

Sebaliknya misalkan H adalah subhimpunan tak kosong dari G yang memenuhi sifat (1) dan (2). Akan ditunjukkan bahwa H merupakan subgrup dari G, yaitu dengan menunjukkan bahwa H memiliki unsur identitas dan memenuhi hukum asosiatif untuk setiap unsur di H. Karena hukum asosiatif dipenuhi oleh G, maka demikian pula halnya dengan H yang merupakan subhimpunan dari G. Selanjutnya jika $a \in H$, maka berdasarkan bagian (2), $a^{-1} \in H$. Karena $a, a^{-1} \in H$, maka berdasarkan bagian (1) diperoleh $a * a^{-1} \in H$ atau $e \in H$. ■

Teorema 2.2.21. [2]

Misalkan G adalah suatu grup dan H adalah suatu subhimpunan tak kosong dari G. Jika $a * b^{-1} \in H$ dimana $a, b \in H$, maka H adalah subgrup dari G.

Bukti. Misalkan G adalah suatu grup, H adalah suatu subhimpunan tak kosong dari G, dan untuk setiap $a, b \in H$ berlaku $a * b^{-1} \in H$. Akan ditunjukkan bahwa H adalah subgrup dari G.

1. Karena H adalah subhimpunan dari G, maka operasi biner $*$ di G juga berlaku di H. Jelaslah bahwa operasi $*$ ini bersifat asosiatif.

2. Selanjutnya ambil $a = x$ dan $b = x$ di H. Karena $x \in H$, maka $x \in G$, sehingga terdapat $x^{-1} \in G$. Selanjutnya karena $x * x^{-1} = e \in G$ dan $a * b^{-1} = x * x^{-1} = e \in H$, maka jelaslah bahwa H memiliki unsur identitas, yaitu $e \in H$, dimana e juga merupakan unsur identitas di G.

3. Untuk menunjukkan bahwa setiap unsur di H mempunyai invers, ambil $a = e$ dan $b = x$ di H. Karena $b = x \in H$, maka $b = x \in G$, sehingga terdapat $b^{-1} = x^{-1} \in G$. Perhatikan bahwa $a * b^{-1} = e * x^{-1} = x^{-1} \in H$. Dengan demikian jelaslah bahwa setiap unsur$x \in H$ mempunyai $x^{-1} \in H$.

4. Ambil $a = x$ dan $b = y^{-1}$ di H. Karena setiap unsur H mempunyai invers, maka $(y^{-1})^{-1} = b^{-1} \in H$. Selanjutnya perhatikan bahwa $x * y = a * b^{-1} \in H$. Dengan demikian jelaslah bahwa H bersifat tertutup terhadap operasi $*$.

Karena 1,2,3, dan 4 maka terbukti bahwa H adalah subgrup dari G. ■

Ada sebuah notasi penting yang perlu diketahui sebelum melanjutkan pembahasan mengenai subgrup. Untuk suatu unsur a dari suatu grup, notasi $\langle a \rangle$ menyatakan himpunan $\{a^n | n \in \mathbb{Z}\}$ [2].

Teorema 2.2.22. [2]

Misalkan G adalah suatu grup dan $a \in G$, maka $\langle a \rangle$ adalah subgrup dari G.

Bukti. Karena $a \in \langle a \rangle$, maka $\langle a \rangle$ adalah subhimpunan tak kosong dari G. Misalkan $a^m, a^n \in \langle a \rangle$, untuk suatu $m, n \in \mathbb{Z}$, maka $a^m * (a^n)^{-1} = a^{m-n} \in \langle a \rangle$. Dengan demikian, berdasarkan Teorema 2.2.21, $\langle a \rangle$ adalah subgrup dari G. ■

Definisi 2.2.23. [3]

Misalkan G adalah suatu grup dan H adalah suatu subgrup dari G. Untuk setiap $a \in G$, himpunan $aH = \{a * h | h \in H\}$ disebut koset kiri dari H di G yang memuat a dan himpunan $Ha = \{h * a | h \in H\}$ disebut koset kanan dari H di G yang memuat a.

Contoh 2.2.4. *Misalkan $\mathbb{Z}_9$ membentuk grup terhadap operasi penjumlahan modulo 9 dan $H = \{0, 3, 6\}$ adalah subgrup dari $\mathbb{Z}_9$, maka koset-koset (kiri) dari H di $\mathbb{Z}_9$ adalah*

1. $0 +_9 H = \{0, 3, 6\} = 3 +_9 H = 6 +_9 H$.
2. $1 +_9 H = \{1, 4, 7\} = 4 +_9 H = 7 +_9 H$.
3. $2 +_9 H = \{2, 5, 8\} = 5 +_9 H = 8 +_9 H$.

Lema 2.2.24. [8]

Misalkan H adalah suatu subgrup dari grup G, dan misalkan $a, b \in G$, maka

1. *$aH = bH$ jika dan hanya jika $b^{-1} * a \in H$. Secara khusus, $aH = H$ jika dan hanya jika $a \in H$.*
2. *Jika $aH \cap bH \neq \emptyset$, maka $aH = bH$.*
3. *$|aH| = |H|$ untuk semua $a \in G$.*

Bukti.

1. Misalkan $aH = bH$, maka $a \in aH = bH$. Selanjutnya karena $a \in bH$ maka

$a = b * h$ dengan $h \in H$. Perhatikan bahwa

$$\begin{aligned} a &= b * h \\ b^{-1} * a &= b^{-1} * b * h \\ &= e * h \\ &= h \in H. \end{aligned}$$

Dengan demikian, $b^{-1} * a \in H$.

Sebaliknya misalkan $b^{-1} * a \in H$, maka $b^{-1} * a = h$ dengan $h \in H$. Perhatikan bahwa

$$\begin{aligned} h &= b^{-1} * a \\ b * h &= b * b^{-1} * a \\ &= e * a \\ &= a. \end{aligned}$$

Karena $a = b * h$ maka $a \in bH$. Selanjutnya karena $a \in aH$ maka $a = a * h$. Dengan demikian $a * h = b * h$ atau $aH = bH$.

2. Misalkan $aH \cap bH \neq \emptyset$, maka $aH \cap bH$ memiliki sedikitnya satu unsur, sebut c. Karena $c \in aH \cap bH$ maka $c \in aH$ dan $c \in bH$. Perhatikan bahwa jika $c \in aH$ maka $c = a * h$, dan jika $c \in bH$ maka $c = b * h$; akibatnya diperoleh $a * h = b * h$. Dengan demikian $aH = bH$.

3. Definisikan suatu fungsi $f : H \to aH$ yang diberikan oleh $f(h) = a * h$. Perhatikan bahwa

- Ambil $h_1, h_2 \in H$ dengan $f(h_1) = f(h_2)$. Karena $f(h_1) = f(h_2)$ maka $a * h_1 = a * h_2$. Akibatnya

$$\begin{aligned} a^{-1} * a * h_1 &= a^{-1} * a * h_2 \\ e * h_1 &= e * h_2 \\ h_1 &= h_2. \end{aligned}$$

  Dengan demikian f adalah fungsi satu-satu.

- Ambil $a * h \in aH$ dan pilih $h \in H$, maka $f(h) = a * h$. Dengan demikian f adalah fungsi pada.

Karena f merupakan fungsi satu-satu dan pada maka f merupakan fungsi bijeksi. Oleh karena itu f mempunyai tepat satu fungsi invers $g : aH \to H$ yang diberikan oleh $g(ah) = h$. Dengan demikian $|H| = |aH|$. ■

Teorema 2.2.25. [5]

Jika G adalah suatu grup berhingga dan H adalah suatu subgrup dari G, maka $|H|$ membagi $|G|$.

Bukti. Misalkan $\{a_1H, a_2H, \ldots, a_tH\}$ menotasikan koset-koset kiri dari H di G. Karena setiap $g \in G$ berada di koset gH dan $gH = a_iH$ dengan $i = 1, 2, \ldots, t$, maka $G = a_1H \cup a_2H \cup \ldots \cup a_tH$. Selanjutnya, berdasarkan Lema 2.2.24 (2), koset-koset a_iH dan a_jH saling lepas, untuk $i \neq j$. Oleh karena itu $|G| = |a_1H| + |a_2H| + \ldots + |a_tH|$. Namun, berdasarkan Lema 2.2.24 (3), $|a_iH| = |aH|$ untuk semua nilai i. Dengan demikian $|G| = t|H|$. ■

Definisi 2.2.26. [2]

Orde dari suatu unsur $g \in G$ adalah bilangan bulat terkecil n sedemikian sehingga

$g^n = e$. *(Dalam notasi penjumlahan, ini menjadi* $ng = 0$.*) Jika tidak ada bilangan bulat yang memenuhi, maka* g *dikatakan berorde takhingga. Orde dari* g *dinotasikan dengan* $|g|$.

Akibat 2.2.27. [5]

Jika G *adalah suatu grup berhingga, maka* $|g|$ *membagi* $|G|$.

Bukti. Misalkan G adalah suatu grup berhingga dan $g \in G$. Asumsikan bahwa $|g| = n$, maka terdapat suatu subgrup $\langle g \rangle$ dari G yang dibangun oleh g. Karena $g^{|g|} = e$, maka subgrup $\langle g \rangle$ ini mempunyai paling banyak $|g| = n$ unsur.

Andaikan $\langle g \rangle$ mempunyai m unsur, dengan $m < n$. Ambil suatu unsur sebarang $g^k \in \langle g \rangle$, dengan $k < n$. Berdasarkan Teorema 2.1.4, terdapat bilangan bulat q dan r sedemikian sehingga $k = qn + r$ dengan $0 \leq r < n$. Karena $k < n$, maka jelaslah bahwa $r \leq k < n$. Dengan demikian $g^k = g^{qn+r} = g^{qn}g^r = (g^n)^q g^r = eg^r = g^r$. Karena $g^k = g^r$ maka $g^{k-r} = e$, sehingga diperoleh bahwa $k - r < n$ adalah orde dari g. Hal ini bertentangan dengan asumsi bahwa n adalah orde dari g. Dengan demikian haruslah $m = n$, atau dengan perkataan lain, $|g| = |\langle g \rangle|$. Akhirnya, karena $|\langle g \rangle|$ membagi $|G|$, maka terbukti bahwa $|g|$ membagi $|G|$. ■

Akibat 2.2.28. [5]

Jika G *adalah suatu grup berhingga, maka* $g^{|G|} = e$.

Bukti. Berdasarkan Akibat 2.2.27, $|g|$ membagi $|G|$; maka $|G| = m|g|$, untuk suatu bilangan bulat m. Oleh karena itu, $g^{|G|} = g^{m|g|} = (g^{|g|})^m = e^m = e$. ■

Definisi 2.2.29. [2]

Suatu grup G disebut siklik jika terdapat suatu unsur $a \in G$ sedemikian sehingga $G = \{a^n | n \in \mathbb{Z}\}$.

Definisi 2.2.30. [2]

Center $Z(G)$ *dari suatu grup G adalah subhimpunan dari unsur-unsur di G yang komutatif dengan setiap unsur di G, ditulis* $Z(G) = \{x \in G | x * g = g * x, \forall g \in G\}$.

Contoh 2.2.5. *Misalkan $G = \mathbb{Z}_6$ membentuk grup terhadap operasi $+_6$, maka* center *dari $\mathbb{Z}_6$ adalah* $Z(G) = \{0, 1, 2, 3, 4, 5\} = \mathbb{Z}_6$.

Definisi 2.2.31. [1]

Misalkan $a \in G$, maka himpunan $N_G(a) = \{g \in G | g^{-1} * a * g = a\}$ disebut normalizer *dari a di G.*

2.3 Gelanggang

Konsep dari suatu gelanggang diperkenalkan oleh Richard Dedekind. Istilah *ring* (*Zahlring*) dicetuskan oleh David Hilbert di dalam sebuah artikel berjudul *Die Theorie der algebraischen Zahlkörper*, Jahresbericht der Deutschen Mathematiker Vereinigung, Vol. 4, 1897. Definisi pertama dari gelanggang dipublikasikan oleh Abraham H. Fraenkel pada tahun 1914 [1,9].

Definisi 2.3.32. [5]

Suatu himpunan tak kosong R disebut sebagai suatu gelanggang asosiatif jika di R didefinisikan dua buah operasi biner, dinotasikan dengan $+$ dan $\cdot$, sedemikian sehingga untuk semua $a, b, c \in R$ berlaku

1. $a+b \in G$;

2. $a+b=b+a$;

3. $(a+b)+c=a+(b+c)$;

4. *Terdapat suatu unsur* $0 \in R$ *sedemikian sehingga* $a+0=a$ *(untuk setiap* $a \in R$*);*

5. *Terdapat suatu unsur* $-a \in R$ *sedemikian sehingga* $a+(-a)=0$;

6. $a \cdot b \in R$;

7. $a \cdot (b \cdot c)=(a \cdot b) \cdot c$;

8. $a \cdot (b+c)=a \cdot b+a \cdot c$ *dan* $(b+c) \cdot a=b \cdot a+c \cdot a$ *(dua hukum distributif).*

Aksioma-aksioma 1 sampai 5 menetapkan bahwa R merupakan suatu grup *abelian* terhadap operasi $+$. Selanjutnya aksioma-aksioma 6 dan 7 menegaskan bahwa R tertutup terhadap operasi $\cdot$ dan memenuhi hukum asosiatif. Pada aksioma 8 diberikan hubungan di antara kedua operasi di R. Pada pembahasan selanjutnya, $a \cdot b$ akan ditulis sebagai ab.

Definisi 2.3.33. [6]

Misalkan R adalah suatu gelanggang, dan S adalah suatu subhimpunan tak kosong dari R. S disebut sebagai subgelanggang dari R jika S membentuk gelanggang terhadap operasi penjumlahan dan perkalian yang didefinisikan di R.

Definisi 2.3.34. [6,9]

Misalkan R adalah suatu gelanggang. R disebut gelanggang dengan unsur identitas

jika terdapat suatu unsur $1 \in R$ *sedemikian sehingga* $a1 = 1a = a$ *untuk semua* $a \in R$.

Definisi 2.3.35. [6]

Misalkan R *adalah suatu gelanggang.* R *disebut gelanggang komutatif jika setiap* $a, b \in R$ *berlaku* $ab = ba$. *Jika tidak, maka* R *disebut gelanggang non-komutatif.*

Definisi 2.3.36. [4]

Suatu gelanggang komutatif R *adalah suatu daerah integral jika* $ab = 0$ *di* R *mengakibatkan* $a = 0$ *atau* $b = 0$.

Definisi 2.3.37. [5]

Suatu gelanggang R *disebut sebagai gelanggang pembagian (*division ring*) jika* $R - \{0\}$ *membentuk grup terhadap operasi perkalian.*

Unsur identitas terhadap perkalian ditulis sebagai 1, dan invers dari setiap $a \in R$ terhadap perkalian ditulis sebagai a^{-1}.

Definisi 2.3.38. [5]

Lapangan merupakan suatu gelanggang pembagian komutatif.

Lema 2.3.39. [5]

Jika R *merupakan suatu gelanggang, maka untuk semua* $a, b \in R$ *berlaku* $a0 = 0a = 0$.

Bukti. Jika $a \in R$, maka $a(0) = a(0 + 0) = a0 + a0$ (menggunakan hukum distributif kanan), dan karena R merupakan grup terhadap operasi penjumlahan, maka nilai $a0$ yang memenuhi persamaan tersebut tidak lain adalah 0. Dengan

cara yang sama, dan menggunakan hukum distributif kiri, dapat ditunjukkan bahwa $0a = 0$. ■

Lema 2.3.40. [5]

Suatu daerah integral berhingga merupakan suatu lapangan.

Bukti. Ingat kembali bahwa suatu daerah integral merupakan suatu gelanggang komutatif sedemikian sehingga $ab = 0$ jika dan hanya jika salah satu dari a atau b sama dengan 0. Sedangkan suatu lapangan adalah gelanggang komutatif dengan unsur identitas yang mana setiap unsur tak-nolnya mempunyai invers perkalian.

Misalkan D adalah suatu daerah integral berhingga. Untuk menunjukkan bahwa D adalah lapangan maka perlu ditunjukkan bahwa

1. Terdapat $1 \in D$ sedemikian sehingga $a1 = a, \forall a \in D$;
2. Untuk setiap $a \neq 0 \in D$ ada $b \in D$ sedemikian sehingga $ab = 1$.

Misalkan $x_1, x_2, \cdots, x_n$ adalah semua unsur di D dan andaikan bahwa jika $a \neq 0 \in D$, maka $x_1a, x_2a, \cdots, x_na \in D$. Andaikan bahwa $x_ia = x_ja$ untuk $i \neq j$, maka $(x_i - x_j)a = 0$. Karena D adalah daerah integral dan $a \neq 0$ maka hal ini mengakibatkan $x_i - x_j = 0$ sehingga $x_i = x_j$. Hal ini bertentangan dengan $i \neq j$. Dengan demikian $x_1a, x_2a, \cdots, x_na$ adalah n unsur berbeda yang berada di D, yang mana D memiliki tepat n unsur.

Misalkan setiap unsur $y \in D$ dapat ditulis sebagai x_ia untuk suatu x_i. Secara khusus, karena $a \in D$, maka $a = x_{i_0}a$ untuk suatu $x_{i_0} \in D$. Karena D komutatif, maka $a = x_{i_0}a = ax_{i_0}$. Selanjutnya perhatikan bahwa jika $y = x_ia \in D$ untuk suatu $x_i \in D$, maka $yx_{i_0} = (x_ia)x_{i_0} = x_i(ax_{i_0}) = x_ia = y$. Dengan

demikian x_{i_0} adalah unsur identitas di D dan ditulis sebagai 1. Sekarang, karena $1 \in D$, maka $1 = x_i a$ untuk suatu x_i. Misalkan $x_i = b$, maka jelaslah bahwa terdapat suatu $b \in D$ sedemikian sehingga $ab = 1$. ■

Akibat 2.3.41. [5]

Jika p adalah suatu bilangan prima maka $\mathbb{Z}_p$, gelanggang bilangan bulat mod p, *adalah suatu lapangan.*

Bukti. Karena $\mathbb{Z}_p$ adalah gelanggang dan perkalian di $\mathbb{Z}_p$ komutatif, maka $\mathbb{Z}_p$ adalah gelanggang komutatif. Selanjutnya misalkan $a, b \in \mathbb{Z}_p$ sedemikian sehingga $ab \equiv 0(\mod p)$, maka diperoleh $p \mid ab$. Karena $p \mid ab$, maka $p \mid a$ atau $p \mid b$, sehingga $a \equiv 0(\mod p)$ atau $b \equiv 0(\mod p)$. Oleh karena itu salah satu dari $a \in \mathbb{Z}_p$ atau $b \in \mathbb{Z}_p$ adalah 0. Dengan demikian, $\mathbb{Z}_p$ adalah daerah integral berhingga (karena $\mathbb{Z}_p$ mempunyai sejumlah berhingga unsur), sehingga berdasarkan Lema 2.3.40 jelaslah bahwa $\mathbb{Z}_p$ adalah suatu lapangan. ■

Definisi 2.3.42. [6]

Misalkan R adalah suatu gelanggang. Jika terdapat suatu bilangan bulat terkecil m sedemikian sehingga $ma = 0$ untuk semua $a \in R$, maka R dikatakan berkarakteristik m. Jika tidak, maka R berkarakteristik 0. m atau 0 disebut karakteristik dari R.

Definisi 2.3.43. [5]

Suatu pemetaan ϕ dari gelanggang R ke gelanggang R' dikatakan suatu homomorfisma jika untuk semua $a, b \in R$ berlaku

1. $\phi(a + b) = \phi(a) + \phi(b)$;

2. $\phi(ab) = \phi(a)\phi(b)$.

Definisi 2.3.44. [5]

Jika ϕ adalah suatu homomorfisma dari R ke R' maka kernel dari ϕ, dinotasikan dengan $I(\phi)$, adalah himpunan semua $a \in R$ sedemikian sehingga $\phi(a) = 0'$, dimana $0'$ adalah unsur identitas penjumlahan di R'.

Definisi 2.3.45. [5]

Suatu homomorfisma dari R ke R' dikatakan suatu isomorfisma jika homomorfisma tersebut merupakan suatu pemetaan satu-satu.

Definisi 2.3.46. [5]

Dua gelanggang dikatakan isomorfik jika terdapat suatu isomorfisma dari satu gelanggang pada gelanggang yang lain.

2.4 Ruang Vektor dan Lapangan

2.4.1 Ruang Vektor

Definisi 2.4.47. [5]

Suatu himpunan tak kosong V disebut sebagai suatu ruang vektor atas lapangan F jika V merupakan grup abelian *terhadap operasi penjumlahan, dan jika untuk setiap $\alpha \in F$,$v \in V$ didefinisikan suatu unsur $\alpha v \in V$ yang memenuhi*

1. $\alpha(v + w) = \alpha v + \alpha w$;

2. $(\alpha + \beta)v = \alpha v + \beta v$;

3. $\alpha(\beta v) = (\alpha\beta)v$;

4. $1v = v$;

untuk semua $\alpha, \beta \in F$ *dan* $v, w \in V$ *(dimana* 1 *merepresentasikan unsur identitas lapangan* F *terhadap operasi perkalian).*

Definisi 2.4.48. [5]

Jika V *adalah suatu ruang vektor atas* F *dan jika* $v_1, \cdots, v_n \in V$ *maka suatu unsur dengan bentuk* $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$ *dengan* $\alpha_i \in F$, *adalah suatu kombinasi linier dari* $v_1, \cdots, v_n$ *atas* F.

Definisi 2.4.49. [5]

Jika S *merupakan suatu himpunan tak kosong dari ruang vektor* V, *maka rentangan linier (*linear span*) dari* S, *dinotasikan dengan* $L(S)$, *adalah himpunan semua kombinasi linier dari unsur-unsur* S.

Definisi 2.4.50. [5]

Ruang vektor V *dikatakan berdimensi-hingga atas* F *jika terdapat suatu subhimpunan berhingga* S *di* V *sedemikian sehingga* $V = L(S)$.

Definisi 2.4.51. [5]

Jika V *adalah suatu ruang vektor dan* $v_1, \cdots, v_n \in V$, *maka vektor-vektor tersebut dikatakan bergantung linier atas* F *jika terdapat* $\lambda_1, \cdots, \lambda_n \in F$, *tak semuanya* 0, *sedemikian sehingga* $\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n = 0$.

Jika vektor-vektor $v_1, \cdots, v_n$ tidak bergantung linier atas F, maka vektor-vektor tersebut dikatakan bebas linier atas F. Jika $v_1, \cdots, v_n$ bebas linier, maka tak satupun dari vektor-vektor tersebut sama dengan 0.

Lema 2.4.52. [5]

Jika $v_1, \cdots, v_n \in V$ bebas linier, maka setiap unsur di rentangan liniernya mempunyai suatu representasi tunggal dalam bentuk $\lambda_1 v_1 + \cdots + \lambda_n v_n$ dengan $\lambda_i \in F$.

Bukti. Berdasarkan definisi, setiap unsur di rentangan linier berbentuk $\lambda_1 v_1 + \cdots + \lambda_n v_n$. Untuk memperlihatkan ketunggalannya, perlu ditunjukkan bahwa jika $\lambda_1 v_1 + \cdots + \lambda_n v_n = \mu_1 v_1 + \cdots + \mu_n v_n$ maka $\lambda_1 = \mu_1, \cdots, \lambda_n = \mu_n$.

Perhatikan bahwa jika $\lambda_1 v_1 + \cdots + \lambda_n v_n = \mu_1 v_1 + \cdots + \mu_n v_n$, maka diperoleh $(\lambda_1 - \mu_1)v_1 + \cdots + (\lambda_n - \mu_n)v_n = 0$. Karena vektor-vektor $v_1, \cdots, v_n$ bebas linier, maka hal ini mengakibatkan $\lambda_1 - \mu_1 = 0, \cdots, \lambda_n - \mu_n = 0$ sehingga jelaslah bahwa $\lambda_1 = \mu_1, \cdots, \lambda_n = \mu_n$. ■

Definisi 2.4.53. [5]

Suatu subhimpunan S dari suatu ruang vektor V disebut basis dari V jika S terdiri dari unsur-unsur yang bebas linier dan $V = L(S)$.

Teorema 2.4.54. [5]

Jika $v_1, \cdots, v_n \in V$ maka salah satu pernyataan berikut berlaku: vektor-vektor tersebut adalah bebas linier atau suatu v_k merupakan kombinasi linier dari vektor-vektor yang mendahuluinya yaitu $v_1, \cdots, v_{k-1}$.

Bukti. Jika $\{v_1, \cdots, v_n\}$ bebas linier, maka bukti selesai. Andaikan bahwa $\alpha_1 v_1 + \cdots + \alpha_n v_n = 0$ dimana tak semua α_i bernilai 0. Misalkan k adalah bilangan bulat terbesar yang mengakibatkan $\alpha_k \neq 0$. Karena $\alpha_i = 0$ untuk $i > k$, maka $\alpha_1 v_1 + \cdots + \alpha_k v_k = 0$, sehingga mengakibatkan $v_k = \alpha_k^{-1}(-\alpha_1 v_1 - \cdots - \alpha_{k-1} v_{k-1}) = (-\alpha_k^{-1}\alpha_1)v_1 + \cdots + (-\alpha_k^{-1}\alpha_{k-1})v_{k-1}$. Dengan demikian v_k merupakan kombinasi linier dari vektor-vektor yang mendahuluinya. ■

Akibat 2.4.55. [5]

Jika $\{v_1, \cdots, v_n\}$ *di* V *mempunyai suatu rentangan linier, sebut* W*, dan jika* $\{v_1, \cdots, v_k\}$ *bebas linier maka dapat ditentukan suatu subhimpunan dari* $\{v_1, \cdots, v_n\}$ *dalam bentuk* $\{v_1, v_2, \cdots, v_k, v_{i_1}, \cdots, v_{i_r}\}$ *yang terdiri dari unsur-unsur bebas linier yang rentangan liniernya juga* W*.*

Bukti. Jika $\{v_1, \cdots, v_n\}$ bebas linier maka jelaslah bahwa akibat di atas berlaku. Jika tidak, pisahkanlah unsur v_j pertama dari himpunan ini yang merupakan kombinasi linier dari vektor-vektor yang mendahuluinya. Karena $\{v_1, \cdots, v_k\}$ bebas linier, maka $j > k$. Perhatikan bahwa subhimpunan yang terbentuk setelah v_j dipisahkan, yaitu $\{v_1, \cdots, v_k, \cdots, v_{j-1}, v_{j+1}, \cdots, v_n\} = S_1$ mempunyai $n-1$ unsur. Jelaslah bahwa rentangan liniernya, sebut $L(S_1)$, termuat di W.

Selanjutnya misalkan $w \in W$, maka $w = \alpha_1 v_1 + \cdots + \alpha_{j-1} v_{j-1} + \alpha_j v_j + \cdots + \alpha_n v_n$. Namun karena $v_j = \beta_1 v_1 + \cdots + \beta_{j-1} v_{j-1}$ maka w dapat direkonstruksi menjadi $w = (\alpha_1 + \alpha_j \beta_1) v_1 + \cdots + (\alpha_{j-1} + \alpha_j \beta_{j-1}) v_{j-1} + \alpha_{j+1} v_{j+1} + \cdots + \alpha_n v_n$, sehingga W juga merupakan kombinasi linier dari unsur-unsur $v_1, \cdots, v_{j-1}, v_{j+1}, \cdots, v_n$. Dengan demikian diperoleh $L(S_1) = W$.

Jika proses pemisahan seperti di atas dilanjutkan, akan diperoleh suatu subhimpunan $\{v_1, \cdots, v_k, v_{i_1}, \cdots, v_{i_r}\}$ yang rentangan liniernya adalah W tetapi tidak ada lagi unsur dari subhimpunan tersebut yang merupakan kombinasi linier dari vektor-vektor yang mendahuluinya. Berdasarkan Teorema 2.4.54, jelaslah bahwa $\{v_1, \cdots, v_k, v_{i_1}, \cdots, v_{i_r}\}$ bebas linier. ■

Akibat 2.4.56. [5]

Jika V *adalah suatu ruang vektor berdimensi-hingga dan jika* $\{v_1, \cdots, v_n\}$ *meren-*

tang V maka suatu subhimpunan dari $\{v_1, \cdots, v_n\}$ membentuk suatu basis dari V.

Bukti. Karena V berdimensi-hingga, maka V merupakan suatu rentangan linier dari unsur-unsur $\{v_1, \cdots, v_n\}$. Berdasarkan Akibat 2.4.55, dapat ditentukan suatu subhimpunan dari $\{v_1, \cdots, v_n\}$, sebut S_2, yang unsur-unsurnya bebas linier dan $L(S_2) = V$. Karena S_2 terdiri dari unsur-unsur yang bebas linier dan $L(S_2) = V$ maka berdasarkan Definisi 2.4.53, S_2 merupakan basis dari V. ■

Definisi 2.4.57. [8]

Jika V merupakan suatu ruang vektor berdimensi-hingga atas suatu lapangan F, maka dimensi dari V, dinotasikan dengan $\dim(V)$, *adalah banyaknya unsur pada basis V.*

2.4.2 Lapangan, Lapangan Perluasan, dan Akar-akar Polinomial

Definisi 2.4.58. [6]

Misalkan F adalah suatu gelanggang komutatif. Jika $F - \{0\}$ membentuk grup terhadap operasi perkalian maka F disebut lapangan.

Definisi 2.4.59. [9]

Misalkan F adalah suatu lapangan, dan E adalah suatu subhimpunan tak kosong dari F. Jika E membentuk suatu lapangan terhadap operasi penjumlahan dan perkalian yang didefinisikan di F, maka E disebut sublapangan dari F.

Teorema 2.4.60. [4]

Karakteristik dari suatu lapangan F adalah 0 atau suatu bilangan prima.

Bukti. Jika F berkarakteristik 0, maka teorema terbukti. Selanjutnya andaikan bahwa $mx = 0$ untuk semua $x \in F$, dimana m adalah suatu bilangan bulat positif. Misalkan p adalah bilangan bulat positif terkecil sedemikian sehingga $px = 0$ untuk semua $x \in F$. Akan ditunjukkan bahwa p adalah suatu bilangan prima.

Andaikan p bukan bilangan prima, maka $p = uv$ dimana $u > 1$ dan $v > 1$ adalah bilangan bulat. Karena $1 \in F$, maka $(u1)(v1) = (uv)1 = p1 = 0$. Namun karena F adalah suatu daerah integral, maka salah satu dari dua hal ini berlaku: $u1 = 0$ atau $v1 = 0$. Jika $u1 = 0$, maka $0 = (u1)x = ux, \forall x \in F$. Demikian pula halnya jika $v1 = 0$. Namun hal ini bertentangan dengan hipotesa bahwa p adalah bilangan bulat positif terkecil yang memenuhi sifat tersebut. Dengan demikian p haruslah suatu bilangan prima. ■

Definisi 2.4.61. [5]

Misalkan F adalah suatu lapangan. Suatu lapangan K dikatakan suatu perluasan dari lapangan F jika K memuat F. Dengan perkataan lain, K adalah perluasan dari F jika F merupakan sublapangan dari K.

Jika K merupakan suatu perluasan dari F, maka K adalah suatu ruang vektor atas F terhadap operasi-operasi lapangan biasa di K.

Definisi 2.4.62. [5]

Derajat K atas F adalah dimensi dari K sebagai suatu ruang vektor atas F.

Derajat K atas F dinotasikan dengan $[K : F]$. Dalam permasalahan khusus, jika $[K : F]$ berhingga, yaitu ketika K merupakan ruang vektor berdimensi-hingga atas F, maka K dikatakan suatu perluasan berhingga dari F.

Definisi 2.4.63. [5]

Misalkan F adalah suatu lapangan dan K adalah perluasan dari F. Suatu unsur $a \in K$ dikatakan algebraic *atas F jika terdapat unsur-unsur $\alpha_0, \alpha_1, \cdots, \alpha_n$ di F, tak semuanya nol, sedemikian sehingga $\alpha_0 a^n + \alpha_1 a^{n-1} + \cdots + \alpha_n = 0$.*

Definisi 2.4.64. [4]

Misalkan F adalah suatu lapangan. Gelanggang polinomial di x atas F, dinotasikan dengan $F[x]$, adalah himpunan dari semua bentuk $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} + a_n x^n, n \geq 0$, dengan $a_i \in F$.

Definisi 2.4.65. [5]

Jika $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} + a_n x^n \neq 0, a_n \neq 0$ maka derajat dari $p(x)$, ditulis sebagai der $p(x)$, adalah n.

Lema 2.4.66. [4]

Diberikan polinomial-polinomial $f(x), g(x) \in F[x], g(x) \neq 0$, maka $f(x) = q(x)g(x) + r(x)$ dimana $q(x), r(x) \in F[x]$ dan $r(x) = 0$ atau der $r(x) <$ der $g(x)$.

Bukti. Misalkan $f(x)$ dan $g(x)$ adalah dua polinomial berderajat m dan n, berturut-turut, yang diberikan oleh $f(x) = a_0 + a_1 x + \cdots + a_m x^m, a_m \neq 0$ dan $g(x) = b_0 + b_1 x + \cdots + b_n x^n, b_n \neq 0$. Pertama-tama, akan diselesaikan suatu kasus trivial, yaitu jika der $f(x) <$ der $g(x)$ maka $f(x) = 0g(x) + r(x)$, dimana $q(x) = 0$ dan $r(x) = f(x)$, sehingga lema terbukti.

Selanjutnya pembuktian akan dilakukan dengan menggunakan induksi pada der $f(x)$. Jika der $f(x) = 0$ maka $f(x) = a_0$. Kemudian, jika der $f(x) =$ der $g(x)$ maka $g(x) = b_0$, sehingga $f(x) = g(x)q$ dimana $q = a_0/b_0$ dan $r(x) = 0$. Di sisi lain, jika der $f(x) <$ der $g(x)$, maka akan diperoleh hasil seperti kasus trivial di atas.

Sekarang misalkan der $f(x) > 0$. Andaikan lema bernilai benar untuk polinomial-polinomial berderajat lebih rendah dari $f(x)$. Akan dibuktikan bahwa lema juga bernilai benar untuk polinomial $f(x)$. Jika der $f(x) <$ der $g(x)$, maka diperoleh hasil yang sama dengan kasus trivial di atas. Oleh karena itu, andaikan bahwa der $g(x) \leq$ der $f(x)$. Selanjutnya misalkan

$$h(x) = f(x) - \frac{a_m}{b_n} x^{m-n} g(x),$$

maka

$$h(x) = (a_0 + a_1 x + \cdots + a_m x^m) - \frac{a_m}{b_n}(b_0 + b_1 x + \cdots + b_n x^n) x^{m-n},$$

sehingga der $h(x) <$ der $f(x)$. Berdasarkan asumsi induksi, terdapat $p(x)$ dan $r(x)$ sedemikian sehingga $h(x) = p(x)g(x) + r(x)$, dimana salah satu hal berikut dipenuhi: $r(x) = 0$ atau der $r(x) <$ der $g(x)$. Oleh karena itu

$$p(x)g(x) + r(x) = h(x) = f(x) - \frac{a_m}{b_n} x^{m-n} g(x),$$

sehingga

$$f(x) = g(x)(p(x) + \frac{a_m}{b_n} x^{m-n}) + r(x) = g(x)q(x) + r(x),$$

dimana $q(x) = (p(x) + \frac{a_m}{b_n} x^{m-n})$ dan $r(x) = 0$ atau der $r(x) <$ der $g(x)$. ■

Lema di atas lebih dikenal sebagai Algoritma Pembagian untuk Polinomial.

Definisi 2.4.67. [4]

Misalkan $F \subset K$ dan $F(a) = \{f(a)|f(x) \in F[x]\}$ adalah sublapangan terkecil K yang memuat F dan a. $F(a)$ disebut lapangan yang diperoleh dengan menggandengkan a ke F.

Definisi 2.4.68. [5]

Jika $p(x) \in F[x]$, maka suatu unsur a yang berada di suatu lapangan perluasan dari F disebut akar dari $p(x)$ jika $p(a) = 0$.

Lema 2.4.69. [5]

Jika $p(x) \in F[x]$ dan jika K adalah suatu perluasan dari F, maka untuk suatu unsur $b \in K, p(x) = (x-b)q(x)+p(b)$ dimana $q(x) \in K[x]$ dan dimana der $q(x) =$ der $p(x) - 1$.

Bukti. Karena $F \subset K$, maka $F[x]$ termuat di $K[x]$ sehingga $p(x)$ berada di $K[x]$. Dengan menggunakan algoritma pembagian untuk polinomial di $K[x]$ diperoleh $p(x) = (x-b)q(x)+r(x)$, dimana $q(x), r(x) \in K[x]$ dan $r(x) = 0$ atau der $r <$ der $(x-b) = 1$. Dengan demikian ($r(x) = 0$ atau der $r(x) = 0$). Kemudian perhatikan bahwa $p(b) = (b-b)q(x)+r(x) = r(x)$. Oleh karena itu, $p(x) = (x-b)q(x)+p(b)$.

Selanjutnya, karena ($p(b) = 0$ atau der $p(b) = 0$) dan $p(x) = (x-b)q(x) + p(b)$ maka terdapat dua kasus yang harus diperhatikan.

1. Jika $p(b) = 0$ maka $p(x) = (x-b)q(x) + 0 = (x-b)q(x)$. Karena der $(x-b) = 1$ maka der $q(x)$ haruslah sama dengan der $p(x) - 1$.

2. Jika der $p(b) = 0$ maka $p(b)$ merupakan suatu konstanta, sehingga $p(x) = (x-b)q(x) + p(b)$. Sama dengan kasus 1, der $q(x) =$ der $p(x) - 1$. ■

Akibat 2.4.70. [5]

Jika $a \in K$ merupakan akar dari $p(x) \in F[x]$, dimana $F \subset K$, maka di $K[x]$, $(x-a)|p(x)$.

Bukti. Dari Lema 2.4.68, di $K[x]$ berlaku $p(x) = (x-a)q(x)+p(a) = (x-a)q(x)$ karena $p(a) = 0$. Dengan demikian $(x-a)|p(x)$ di $K[x]$. ■

Definisi 2.4.71. [5]

Unsur $a \in K$ merupakan suatu akar berkelipatan m dari $p(x) \in F[x]$ jika $(x-a)^m|p(x)$, sedangkan $(x-a)^{m+1} \nmid p(x)$.

Lema 2.4.72. [5]

Suatu polinomial berderajat n atas suatu lapangan F dapat mempunyai paling banyak n akar di suatu lapangan perluasan dari F.

Bukti. Andaikan $p(x)$ berderajat n atas lapangan F dan K merupakan lapangan perluasan dari F. Akan ditunjukkan bahwa lema di atas benar dengan menggunakan induksi pada n yang merupakan derajat dari polinomial $p(x)$ atas lapangan F.

Jika $n = 1$, maka $p(x) = \alpha x + \beta$ dimana $\alpha, \beta \in F$ dan $\alpha \neq 0$. Ambil $a \in K$ sedemikian sehingga $p(a) = 0$, maka $a = (-\frac{\beta}{\alpha})$ adalah solusi dari $\alpha x + \beta = 0$. Dengan demikian, $p(x)$ mempunyai akar tunggal $-\frac{\beta}{\alpha}$.

Selanjutnya asumsikan bahwa lema benar di lapangan manapun untuk polinomial-polinomial yang berderajat kurang dari n, dan andaikan $p(x)$ berderajat n atas F. Jika $p(x)$ tidak mempunyai akar di lapangan K, maka banyaknya akar $p(x)$ di K, sebut nol, pastilah paling banyak n, sehingga bukti selesai. Oleh

karena itu, andaikan bahwa $p(x)$ mempunyai paling sedikit satu akar $a \in K$ dan a tersebut merupakan suatu akar berkelipatan m. Karena $(x-a)^m | p(x)$ maka $m \leq n$ dan $p(x) = (x-a)^m q(x)$, dimana $q(x) \in K[x]$ adalah polinomial berderajat $n-m$. Dari fakta bahwa $(x-a)^{m+1} \nmid p(x)$ maka diperoleh $(x-a) \nmid q(x)$ sehingga a bukanlah akar dari $q(x)$.

Jika $b \neq a$ merupakan suatu akar dari $p(x)$ di $K[x]$, maka $p(b) = (b-a)^m q(x) = 0$. Karena $b-a \neq 0$ dan K merupakan lapangan, maka $q(b) = 0$. Oleh karena itu, suatu akar dari $p(x)$, selain a, merupakan akar dari $q(x)$. Karena $q(x)$ berderajat $n-m < n$, maka berdasarkan hipotesa induksi, $q(x)$ mempunyai paling banyak $n-m$ akar di K, dan bersama a yang merupakan akar berkelipatan m dari $p(x)$, dapat disimpulkan bahwa $p(x)$ mempunyai paling banyak $(n-m)+m = n$ akar di K. ■

2.4.3 Lapangan Berhingga

Misalkan F adalah suatu lapangan berhingga, maka F haruslah berkarakteristik p, dengan p suatu bilangan prima, dan F memuat $0, 1, 2, \cdots, p-1$. Oleh karena itu, $F \supset \mathbb{Z}_p$, atau lebih tepatnya, F memuat suatu lapangan yang isomorfik ke $\mathbb{Z}_p$ [4].

Lema 2.4.73. [5]

Misalkan F adalah suatu lapangan berhingga dengan q unsur dan andaikan bahwa $F \subset K$ dimana K juga merupakan suatu lapangan berhingga, maka K mempunyai q^n unsur dimana $n = [K : F]$.

Bukti. K adalah ruang vektor atas F dan karena K berhingga, maka jelaslah K adalah ruang vektor berdimensi-hingga atas F. Andaikan bahwa $[K : F] = n$; maka K mempunyai suatu basis dengan n unsur atas F. Misalkan basis tersebut adalah $v_1, v_2, \cdots, v_n$, maka setiap unsur di K mempunyai suatu representasi tunggal dalam bentuk $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$ dimana $\alpha_1, \alpha_2, \cdots, \alpha_n \in F$. Dengan demikian banyaknya unsur di K adalah banyaknya bentuk $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$ sebagai barisan $\alpha_1, \alpha_2, \cdots, \alpha_n$ atas F. Karena setiap koefisien dapat mempunyai q nilai, maka jelaslah bahwa K harus mempunyai q^n unsur. ■

Akibat 2.4.74. [5]

Misalkan F adalah suatu lapangan berhingga; maka F mempunyai p^m unsur dimana bilangan prima p adalah karakteristik dari F.

Bukti. Pandanglah F sebagai suatu grup penjumlahan dan misalkan $|F| = f$; maka berdasarkan Akibat 2.2.28 diperoleh $1^f = f1 = 0$ dengan $1 \in F$. Dengan demikian F berkarakteristik p untuk suatu bilangan prima p. Oleh karena itu F memuat suatu lapangan F_0 yang isomorfik ke $\mathbb{Z}_p$. Karena F_0 mempunyai p unsur, maka berdasarkan Lema 2.4.72 F mempunyai p^m unsur dimana $m = [F : F_0]$. ■

Akibat 2.4.75. [5]

Jika lapangan berhingga F mempunyai p^m unsur maka setiap $a \in F$ memenuhi $a^{p^m} = a$.

Bukti. Jika $a = 0$, maka pernyataan akibat tersebut benar secara trivial. Di sisi lain, unsur-unsur tak-nol dari F membentuk suatu grup perkalian dengan orde $p^m - 1$, sehingga berdasarkan Akibat 2.2.28 diperoleh $a^{p^m - 1} = 1$ untuk semua

$a \neq 0 \in F$. Jika kedua ruas persamaan tersebut dikalikan dengan a, maka diperoleh $a^{p^m} = a$. ■

Lema 2.4.76. [5]

Jika lapangan berhingga F mempunyai p^m unsur maka polinomial $x^{p^m} - x$ di $F[x]$ difaktorkan di $F[x]$ sebagai $x^{p^m} - x = \prod_{\lambda \in F}(x - \lambda)$.

Bukti. Berdasarkan Lema 2.4.71 polinomial $x^{p^m} - x$ mempunyai paling banyak p^m akar di F. Akan tetapi, berdasarkan Akibat 2.4.74 diketahui bahwa p^m buah akar yang demikian adalah semua unsur dari F. Berdasarkan Akibat 2.4.69 dapat disimpulkan bahwa $x^{p^m} - x = \prod_{\lambda \in F}(x - \lambda)$. ■

Teorema 2.4.77. [5]

Grup perkalian dari unsur-unsur tak-nol dari suatu lapangan berhingga adalah siklis.

Bukti. Misalkan F adalah suatu lapangan berhingga dan G adalah grup perkalian dari unsur-unsur tak-nol F, maka suatu polinomial berderajat n di $F[x]$ mempunyai paling banyak n akar di F. Dengan demikian, secara khusus, untuk suatu bilangan bulat n, polinomial $x^n - 1$ mempunyai paling banyak n akar di F, dan demikian halnya di G.

Misalkan $|G| = q$. Andaikan suatu unsur $a \in G$ mempunyai orde sebesar mungkin yaitu q^r, untuk suatu bilangan bulat r, maka unsur-unsur $1, a, a^2, \cdots, a^{q^r-1}$ merupakan q^r solusi yang berbeda dari persamaan $x^{q^r} = 1$. Dengan demikian unsur-unsur tersebut merupakan q^r akar yang berbeda dari polinomial $x^{q^r} - 1$ di G.

Selanjutnya misalkan $b \in G$ berorde q^s, dimana $s \leq r$. Karena $(b^{q^s})^{q^{r-s}} = b^{q^r} = 1$, maka unsur-unsur $1, a, a^2, \cdots, a^{q^r-1}$ merupakan q^r akar yang berbeda dari polinomial $b^{q^r} - 1$ di G, sehingga mengakibatkan $b = a^i$, dengan $i = 0, 1, \cdots, q^{r-1}$. Dengan demikian, G adalah siklis. ■

Lema 2.4.78. [5]

Jika F adalah suatu lapangan berhingga dan $\alpha \neq 0, \beta \neq 0$ adalah dua buah unsur di F, maka terdapat unsur a dan b di F sedemikian sehingga $1 + \alpha a^2 + \beta b^2 = 0$.

Bukti. Jika char $F = 2$, maka F mempunyai 2^n unsur dan setiap $x \in F$ memenuhi $x^{2^n} = x$. Dengan demikian, setiap unsur di F berbentuk pangkat-dua. Secara khusus, $\alpha^{-1} = a^2$ untuk suatu $a \in F$. Ambil $a = 0$ dan $b = 0$, maka diperoleh $1 + \alpha a^2 + \beta b^2 = 1 + \alpha\alpha^{-1} + 0 = 1 + 1 = 2 \cdot 1 = 0$, karena char $F = 2$.

Jika karakteristik F adalah suatu bilangan prima ganjil p, maka F mempunyai p^n unsur. Misalkan $W_\alpha = \{1 + \alpha x^2 | x \in F\}$. Andaikan bahwa $1 + \alpha x^2 = 1 + \alpha y^2$, maka $\alpha x^2 = \alpha y^2$, dan karena $\alpha \neq 0$ maka $x^2 = y^2$. Dengan demikian $x = \pm y$, sehingga untuk setiap $x \neq 0$ diperoleh sebuah unsur $(1 + \alpha x^2) \in W_\alpha$ dari setiap pasangan y dan $-y$, dan untuk $x = 0$ diperoleh $1 \in W_\alpha$. Dengan demikian W_α mempunyai $1 + \frac{p^n-1}{2} = \frac{p^n+1}{2}$ unsur. Dengan cara yang sama, $W_\beta = \{-\beta x^2 | x \in F\}$ juga mempunyai $\frac{p^n+1}{2}$ unsur.

Karena setiap himpunan W_α dan W_β mempunyai lebih dari setengah unsur-unsur F, maka $W_\alpha \cap W_\beta \neq \emptyset$. Misalkan $c \in W_\alpha \cap W_\beta$. Karena $c \in W_\alpha$, maka $c = 1 + \alpha a^2$ untuk suatu $a \in F$, dan karena $c \in W_\beta$, maka $c = -\beta b^2$ untuk suatu $b \in F$. Dengan demikian, $1 + \alpha a^2 = -\beta b^2$ sehingga menghasilkan $1 + \alpha a^2 + \beta b^2 = 0$.

■

BAB III

WEDDERBURN'S LITTLE THEOREM

Pada bab ini akan dibahas tentang bukti dari *Wedderburn's Little Theorem.*

3.1 Beberapa Lema Pendukung

Pada subbab ini akan diberikan dan dibuktikan beberapa lema dan akibat yang akan digunakan untuk membuktikan *Wedderburn's Little Theorem* dalam skripsi ini.

Lema 3.1.1. [5]

Misalkan R suatu gelanggang dan misalkan $a \in R$. Misalkan pemetaan $\delta_a : R \to R$ didefinisikan oleh $\delta_a(x) = xa - ax$, maka

$$\delta_a^n(x) = xa^n - naxa^{n-1} + \frac{n(n-1)}{2}a^2xa^{n-2} - \frac{n(n-1)(n-2)}{3!}a^3xa^{n-3} + \cdots + (-1)^n a^n x.$$

Bukti. Perhatikan bahwa $\delta_a^2(x) = \delta_a(\delta_a(x)) = \delta_a(xa - ax) = (xa - ax)a - a(xa - ax) = xa^2 - 2axa + a^2x$. Kemudian $\delta_a^3(x) = \delta_a(\delta_a^2(x)) = (xa^2 - 2axa + a^2x)a - a(xa^2 - 2axa + a^2x) = xa^3 - 3axa^2 + 3a^2xa - a^3x$.

Selanjutnya diasumsikan bahwa $\delta_a^k(x) = xa^k - kaxa^{k-1} + \frac{k(k-1)}{2}a^2xa^{k-2} - \frac{k(k-1)(k-2)}{3!}a^3xa^{k-3} + \cdots + (-1)^k a^k x$, maka $\delta_a^{k+1}(x) = \delta_a(\delta_a^k(x)) = \delta_a(xa^k - kaxa^{k-1} + \frac{k(k-1)}{2}a^2xa^{k-2} - \frac{k(k-1)(k-2)}{3!}a^3xa^{k-3} + \cdots + (-1)^k a^k x) = (xa^k - kaxa^{k-1} + \frac{k(k-1)}{2}a^2xa^{k-2} - \frac{k(k-1)(k-2)}{3!}a^3xa^{k-3} + \cdots + (-1)^k a^k x)a - a(xa^k - kaxa^{k-1} + \frac{k(k-1)}{2}a^2xa^{k-2} -$

$\frac{k(k-1)(k-2)}{3!}a^3xa^{k-3}+\cdots+(-1)^k a^k x) = (xa^{k+1}-kaxa^k+\frac{k(k-1)}{2}a^2xa^{k-1}-\frac{k(k-1)(k-2)}{3!}$

$a^3xa^{k-2}+\cdots+(-1)^k a^k xa)-(axa^k-ka^2xa^{k-1}+\frac{k(k-1)}{2}a^3xa^{k-2}+\cdots+(-1)^k a^{k+1}x) =$

$xa^{k+1}-(k+1)axa^k+\frac{(k+1)k}{2}a^2xa^{k-1}-\frac{(k+1)k(k-1)}{3!}a^3xa^{k-2}+\cdots+(-1)^{k+1}a^{k+1}x.$

Dengan demikian, berdasarkan induksi, Lema 3.1.1 terbukti. ■

Akibat 3.1.2. [5]

Jika R suatu gelanggang dimana $px = 0$ untuk semua $x \in R$, dimana p adalah suatu bilangan prima, maka $\delta_a^{p^n}(x) = xa^{p^n} - a^{p^n}x$.

Bukti. Berdasarkan persamaan pada Lema 3.1.1, untuk $n = p$ diperoleh $\delta_a^p(x) = xa^p - paxa^{p-1} + \frac{p(p-1)}{2}a^2xa^{p-2} - \frac{p(p-1)(p-2)}{3!}a^3xa^{p-3} + \cdots + (-1)^p a^p x$. Karena karakteristik $R = p$ maka semua koefisien pada bagian tengah persamaan menjadi 0 dan menyisakan bentuk $\delta_a^p(x) = xa^p + (-1)^p a^p x$.

Jika $p = 2$, maka $\delta_a^2(x) = xa^2 + (-1)^2a^2x = xa^2 + a^2x = xa^2 - a^2x$ karena karakteristik $R = 2$ mengakibatkan $1 = -1$. Selanjutnya jika p merupakan bilangan prima ganjil, maka diperoleh $\delta_a^p(x) = xa^p - a^p x$. Dengan demikian $\delta_a^p(x) = xa^p - a^p x$ berlaku untuk semua bilangan prima p.

Selanjutnya, dengan induksi akan ditunjukkan bahwa $\delta_a^{p^n}(x) = xa^{p^n} - a^{p^n}x$ berlaku untuk semua bilangan bulat n. Untuk $n = 1$ diperoleh $\delta_a^{p^1}(x) = xa^{p^1} - a^{p^1}x = xa^p - a^p x$. Kemudian asumsikan bahwa untuk $n = k$ berlaku $\delta_a^{p^k}(x) = xa^{p^k} - a^{p^k}x$. Akan ditunjukkan bahwa untuk $n = k+1$ juga berlaku $\delta_a^{p^{k+1}}(x) = xa^{p^{k+1}} - a^{p^{k+1}}x$

Perhatikan bahwa $\delta_a^{p^k}(x) = xa^{p^k} - a^{p^k}x = \delta_{a^{p^k}}$, maka $\delta_a^{p^{k+1}} = (\delta_a^{p^k})^p = \delta_{a^{p^k}}^p = x(a^{p^k})^p - (a^{p^k})^p x = xa^{p^{k+1}} - a^{p^{k+1}}x$. Dengan demikian terbukti bahwa $\delta_a^{p^n}(x) = xa^{p^n} - a^{p^n}x$ berlaku untuk semua bilangan bulat n. ■

Lema 3.1.3. [3]

Misalkan D adalah suatu gelanggang pembagian dengan karakteristik $p > 0$, $Z(D) = \{z \in D | zx = xz, \forall x \in D\}$ adalah center *dari D, dan P adalah lapangan prima dengan p unsur, dimana P termuat di $Z(D)$. Andaikan $a \in D, a \notin Z(D)$ sedemikian sehingga $a^{p^n} = a$ untuk suatu $n > 0$, maka terdapat suatu $x \in D$ sedemikian sehingga*

1. $xax^{-1} \neq a$,

2. $xax^{-1} \in P(a)$, *lapangan yang diperoleh dengan menggandengkan a ke P.*

Bukti. Pertama-tama, didefinisikan suatu pemetaan $\delta_a : D \to D$ oleh $\delta_a(y) = ya - ay$ untuk semua $y \in D$. Kemudian, karena a *algebraic* atas P, maka $P(a)$ merupakan suatu lapangan berhingga dan mempunyai p^m unsur, untuk suatu bilangan bulat m. Semua unsur $P(a)$ memenuhi $u^{p^m} = u$. Berdasarkan Akibat 3.1.2, $\delta_a^{p^m}(y) = ya^{p^m} - a^{p^m}y = ya - ay = \delta_a(y)$, sehingga $\delta_a^{p^m}(y) = \delta_a(y)$.

Sekarang, jika $\lambda \in P(a)$, maka $\delta_a(\lambda x) = (\lambda x)a - a(\lambda x) = \lambda(xa - ax) = \lambda\delta_a(x)$, karena λ komutatif dengan a. Dengan demikian pemetaan $\lambda I : D \to D$, yang didefinisikan oleh $\lambda I(y) = \lambda y$, komutatif dengan δ_a untuk setiap $\lambda \in P(a)$ (dengan perkataan lain, $(\lambda I) \circ \delta_a = \delta_a \circ (\lambda I)$). Karena setiap unsur $P(a)$ memenuhi polinomial $u^{p^m} - u$, maka berdasarkan Lema 2.4.76 diperoleh $u^{p^m} - u = (u - \lambda_1)(u - \lambda_2) \cdots (u - \lambda_{p^m})$, dimana λ_i adalah p^m unsur yang berbeda di $P(a)$. Dengan menggunakan fakta bahwa $(\lambda_i I) \circ \delta_a = \delta_a \circ (\lambda_i I)$ untuk semua $\lambda_i \in P(a)$, maka diperoleh

$$0 = \delta_a^{p^m} - \delta_a = (\delta_a - \lambda_1 I) \circ (\delta_a - \lambda_2 I) \circ \cdots \circ (\delta_a - \lambda_{p^m} I)$$

dimana $(\delta_a - \lambda I)(x) = \delta_a(x) - \lambda x$.

Selanjutnya misalkan $\lambda_1 = 0$, dan andaikan untuk setiap $\lambda_i \neq 0$ diperoleh $(\delta_a - \lambda_i I) \neq 0$, $\forall y \neq 0 \in D$; maka

$$[(\delta_a - \lambda_2 I) \circ \cdots \circ (\delta_a - \lambda_{p^m} I)](x) \neq 0, \forall y \in D, x \neq 0.$$

Namun karena $0 = \delta_a^{p^m} - \delta_a = \delta_a \circ (\delta_a - \lambda_2 I) \circ \cdots \circ (\delta_a - \lambda_{p^m} I)$ maka diperoleh $\delta_a = 0$, sehingga $0 = \delta_a(y) = ya - ay$ mengakibatkan $a \in Z(D)$. Hal ini bertentangan dengan hipotesa bahwa $a \notin Z(D)$. Dengan demikian, terdapat suatu $\lambda \neq 0$ di $P(a)$ dan suatu $x \neq 0$ di D sedemikian sehingga $(\delta_a - \lambda I)(x) = 0$, yaitu $xa - ax - \lambda x = 0$. Karena $\lambda \neq 0$, maka $xax^{-1} = a + \lambda \neq a$, dan karena $\lambda \in P(a)$, maka $xax^{-1} \in P(a)$. ■

Lema 3.1.3 memberikan akibat berikut ini.

Akibat 3.1.4. [3]

$xax^{-1} = a^i \neq a$ untuk suatu bilangan bulat i.

Bukti. Misalkan a berorde s, maka semua akar dari polinomial $u^s - 1$ di lapangan $P(a)$ adalah $1, a, a^2, \cdots, a^{s-1}$. Karena $(xax^{-1})^s = xa^s x^{-1} = 1$, dan karena $xax^{-1} \in P(a)$, dengan xax^{-1} adalah suatu akar dari $u^s - 1$ di $P(a)$, maka $xax^{-1} = a^i$. ■

Lema 3.1.5. [5]

Misalkan D adalah suatu gelanggang pembagian berhingga sedemikian sehingga setiap subgelanggang pembagian sejatinya adalah komutatif. Misalkan $a, b \in D$ memenuhi $ab \neq ba$ tetapi $b^t a = ab^t$, untuk suatu bilangan bulat t, maka $b^t \in Z(D)$.

Bukti. Misalkan himpunan $N_D(b^t) = \{x \in D | xb^t = b^t x\}$. $N_D(b^t)$ merupakan suatu subgelanggang pembagian dari D. Jika $N_D(b^t) \neq D$, maka berdasarkan hipotesa, $N_D(b^t)$ adalah komutatif. Namun $a, b \in N_D(b^t)$ dan $ab \neq ba$; akibatnya $N_D(b^t)$ tidak komutatif dan haruslah $N_D(b^t) = D$. Dengan demikian $b^t \in Z(D)$.

■

Lema 3.1.6. [5]

Jika $y \in D$ sedemikian sehingga $y^r = 1$, maka $y = \lambda^i$.

Bukti. Perhatikan lapangan $C(y) = \{c \in D | cy = yc\}$ yang merupakan perluasan dari $Z(D)$. Karena r adalah prima, maka unsur-unsur $\lambda^0, \lambda^1, \lambda^2, \cdots, \lambda^{r-1} \in Z(D)$ semua berbeda dan memenuhi $\lambda^i y = y\lambda^i$. Oleh karena itu $\lambda^i \in C(y), i = 0, 1, \cdots, r-1$. Perhatikan bahwa polinomial $p(y) = y^r - 1$ berada di lapangan $Z(D)$ dan $\lambda^i \in C(y), i = 0, 1, \cdots, r-1$ mengakibatkan $p(\lambda^i) = 0$. Karena polinomial $p(y)$ memiliki paling banyak r akar di lapangan $C(y)$, maka jelaslah bahwa $y = \lambda^i, i = 0, 1, \cdots, r-1$. Dengan demikian, $y \in Z(D)$. ■

Lema 3.1.7. [6]

Misalkan D adalah suatu gelanggang pembagian berhingga dengan char $D \neq 2$ dan andaikan terdapat $a_1, b_1 \in D$ sedemikian sehingga

1. $a_1 b_1 = -b_1 a_1 \neq b_1 a_1$;
2. $a_1^2 = b_1^2 = \alpha \neq 0$;
3. *terdapat suatu $\xi, \eta \in Z(D)$ sedemikian sehingga $1 + \xi^2 - \alpha\eta^2 = 0$;*

maka $a_1 + \xi b_1 + \eta a_1 b_1 = 0$.

Bukti. Perhatikan bahwa $(a_1 + \xi b_1 + \eta a_1 b_1)^2 = a_1^2 + \xi^2 b_1^2 + \eta^2 a_1 b_1 a_1 b_1 + \xi a_1 b_1 + \xi b_1 a_1 + \eta a_1^2 b_1 + \eta a_1 b_1 a_1 + \xi\eta b_1 a_1 b_1 + \xi\eta a_1 b_1^2 = \alpha + \xi^2\alpha + \eta^2[a_1(-a_1 b_1)b_1] = \alpha[1 + \xi^2 - \alpha\eta^2] = 0.$

Karena D adalah suatu gelanggang pembagian, maka $a_1 + \xi b_1 + \eta a_1 b_1 = 0$. ■

3.2 *Wedderburn's Little Theorem*

Berikut adalah hasil utama dari skripsi ini, yakni bukti dari *Wedderburn's Little Theorem.*

Teorema 3.2.8. [3]

Setiap gelanggang pembagian berhingga merupakan suatu lapangan.

Bukti. Misalkan D adalah suatu gelanggang pembagian berhingga dan $Z(D)$ adalah *center* dari D. Jika teorema tidak benar untuk semua gelanggang pembagian berhingga D, maka D dipilih sedemikian sehingga D memiliki orde minimal di antara gelanggang-gelanggang pembagian non-komutatif. Dengan demikian, setiap gelanggang pembagian berhingga dengan orde kurang dari orde D adalah komutatif. Akan ditunjukkan bahwa asumsi mengenai gelanggang D ini akan menuju pada suatu kontradiksi.

Setiap unsur taknol di D mempunyai orde berhingga, sehingga beberapa pangkat positif dari unsur-unsur taknol tersebut berada di $Z(D)$. Misalkan $w \in D$, maka orde dari w yang relatif ke $Z(D)$ adalah bilangan bulat positif terkecil $m(w)$ sedemikian sehingga $w^{m(w)} \in Z(D)$.

Pilih suatu unsur $a \in D, a \notin Z(D)$ yang memiliki orde minimal yang tepat relatif ke Z, dan misalkan orde ini adalah r. Diklaim bahwa r adalah

suatu bilangan prima. Berdasarkan Akibat 3.1.4, terdapat suatu $x \in D$ sedemikian sehingga $xax^{-1} = a^i \neq a$, untuk suatu $i \in \mathbb{Z}$. Dengan demikian $x^2ax^{-2} = x(xax^{-1})x^{-1} = xa^ix^{-1} = (xax^{-1})^i = (a^i)^i = a^{i^2}$. Dengan cara yang sama diperoleh $x^{r-1}ax^{-(r-1)} = a^{i^{r-1}}$. Karena r adalah bilangan prima, dengan menggunakan Teorema 2.1.14, diperoleh $i^{r-1} = 1+ru$, untuk suatu bilangan bulat i, sehingga $x^{r-1}ax^{-(r-1)} = a^{i^{r-1}} = a^{1+ru} = aa^{ru} = \lambda a$ dimana $\lambda = a^{ru} \in Z(D)$. Dengan demikian, $x^{r-1}a = \lambda ax^{r-1}$. Karena $x \notin Z(D)$ dan berdasarkan sifat minimal r, diperoleh $x^{r-1} \notin Z(D)$. Hal ini mengakibatkan $\lambda \neq 1$.

Selanjutnya misalkan $b = x^{r-1}$; dengan demikian $bab^{-1} = \lambda a$; akibatnya $\lambda^r a^r = (\lambda a)^r = (bab^{-1})^r = ba^rb^{-1} = a^r$ karena $a^r \in Z(D)$. Hal ini mengakibatkan $\lambda^r = 1$. Karena $\lambda^r = 1$, maka $b^r = \lambda^r b^r = (\lambda b)^r = (a^{-1}ba)^r = a^{-1}b^ra$, sehingga $ab^r = b^ra$. Karena $ab^r = b^ra$ dan $ab \neq ba$ maka berdasarkan Lema 3.1.5 diperoleh $b^r \in Z(D)$.

Berdasarkan Teorema 2.4.77, grup perkalian dari unsur-unsur tak nol $Z(D)$ adalah siklis dan dibangun oleh suatu unsur $\gamma \in Z(D)$. Dengan demikian $a^r = \gamma^n, b^r = \gamma^m$, untuk suatu bilangan bulat n dan m. Jika $n = kr$, dengan k adalah suatu bilangan bulat, maka $(\frac{a}{\gamma^k})^r = 1$, sehingga mengakibatkan $\frac{a}{\gamma^k} = \lambda^i$ dan menuju ke $a \in Z(D)$ (Lema 3.1.6). Hal ini bertentangan dengan $a \notin Z(D)$. Dengan demikian $r \nmid n$, dan dengan cara yang sama $r \nmid m$.

Selanjutnya misalkan $a_1 = a^m$ dan $b_1 = b^n$, maka $a_1^r = a^{rm} = \gamma^{nm} = b^{rn} = b_1^r$ sehingga diperoleh $a_1^r = b_1^r = \alpha \in Z(D)$. Kemudian karena $ba = \lambda ab$ maka $b = \lambda aba^{-1}$. Dengan demikian $b^n = \lambda^n(aba^{-1})^n = \lambda^n ab^na^{-1}$, dan $b^na = \lambda^n ab^n$ sehingga $a = \lambda^n b^{-n}ab^n$; akibatnya $a^m = \lambda^{mn}(b^{-n}ab^n)^m = \lambda^{mn}b^{-n}a^mb^n$ sehingga

$b^n a^m = \lambda^{mn} a^m b^n$. Dengan demikian diperoleh $b_1 a_1 = \mu a_1 b_1, \mu = \lambda^{mn} \in Z(D)$. Karena $\lambda^r = 1$ dan r tidak membagi m maupun n, maka $\mu \neq 1$, tetapi $\mu^r = 1$.

Sekarang perhatikan bahwa $(b_1^{-1}a_1)^2 = (b_1^{-1}a_1)(b_1^{-1}a_1) = b_1^{-1}(a_1 b_1^{-1})a_1 = b_1^{-1}(\mu b_1^{-1}a_1)a_1 = \mu b_1^{-2}a_1^2$. Selanjutnya $(b_1^{-1}a_1)^3 = (b_1^{-1}a_1)^2(b_1^{-1}a_1) = (\mu b_1^{-2}a_1^2)(b_1^{-1}a_1) = \mu b_1^{-2}a_1(a_1 b_1^{-1})a_1 = \mu b_1^{-2}a_1(\mu b_1^{-1}a_1)a_1 = \mu^2 b_1^{-2}(a_1 b_1^{-1})a_1^2 = \mu^2 b_1^{-2}(\mu b_1^{-1}a_1)a_1^2 = \mu^3 b_1^{-3}a_1^3 = \mu^{1+2}b_1^{-3}a_1^3$. Jika dilanjutkan, akan diperoleh

$$(b_1^{-1}a_1)^r = \mu^{1+2+\cdots+(r-1)}b_1^{-r}a_1^r = \mu^{r(r-1)/2}.$$

Jika r adalah bilangan prima ganjil, maka $(b_1^{-1}a_1)^r = 1$. Dengan demikian diperoleh $b_1^{-1}a_1 = \lambda^i \in Z(D)$ sehingga $a_1 = \lambda^i b_1$. Perhatikan bahwa $b_1 a_1 = b_1(\lambda^i b_1) = (\lambda^i b_1)b_1 = a_1 b_1$, berkontradiksi dengan $b_1 a_1 = \mu a_1 b_1, \mu \neq 1$. Dengan demikian, teorema terbukti jika r merupakan bilangan prima ganjil.

Jika $r = 2$, maka diperoleh dua unsur $a_1^2 = b_1^2 = \alpha \in Z(D)$ dan $\mu = -1$, karena $\mu^2 = 1, \mu \neq 1$. Dengan demikian $b_1 a_1 = -a_1 b_1 \neq a_1 b_1$; sebagai konsekuensi, karakteristik D bukanlah 2. Berdasarkan Lema 2.4.77, terdapat unsur $\xi, \eta \in Z(D)$ sedemikian sehingga $1 + \xi^2 - \alpha\eta^2 = 0$. Berdasarkan Lema 3.1.7 diperoleh bahwa $a_1 + \xi b_1 + \eta a_1 b_1 = 0$. Namun

$$0 = a_1(a_1 + \xi b_1 + \eta a_1 b_1) + (a_1 + \xi b_1 + \eta a_1 b_1)a_1 = 2a_1^2 = 2\alpha \neq 0.$$

Karena $0 \neq 0$ adalah hal yang mustahil, maka kontradiksi ini mengakhiri bukti dari *Wedderburn's Little Theorem.* ■

BAB IV

PENUTUP

4.1 Kesimpulan

Dari pembahasan pada bab sebelumnya dapat disimpulkan bahwa terdapat suatu keterkaitan antara banyaknya unsur pada suatu gelanggang pembagian dan operasi perkalian pada gelanggang tersebut, yakni jika gelanggang pembagian mempunyai sejumlah berhingga unsur maka operasi perkaliannya bersifat komutatif. Dengan demikian, gelanggang pembagian tersebut merupakan suatu lapangan.

4.2 Saran

Untuk penelitian selanjutnya penulis menyarankan untuk mengkaji bukti-bukti lainnya dari *Wedderburn's Little Theorem*, terutama yang melibatkan bilangan kompleks atau teori permutasi.

DAFTAR PUSTAKA

[1] Dummit, D. S. dan R. M. Foote. 1991. *Abstract Algebra.* Prentice-Hall, New Jersey

[2] Gallian, J. A. 2006. *Contemporary Abstract Algebra. Seventh Edition.* Brook/ Cole, Cengage Learning, Australia

[3] Herstein, I. N. 1961. Wedderburn's theorem and a theorem of jacobson. *The American Mathematical Monthly.* **68**[3]:249-251

[4] Herstein, I. N. 1999. *Abstract Algebra. Third Edition.* John Wiley and Sons, New York

[5] Herstein, I. N. 1999. *Topics in Algebra. Second Edition.* John Wiley and Sons, New York

[6] Paley, H. dan P. M. Weichsel. 1966. *A First Course in Abstract Algebra.* Holt, Rinehalt and Winston Inc, New York

[7] Rosen, K. H. 2005. *Elementary Number Theory and Its Applications. Fifth Edition.* Pearson, Addison Wesley, Boston

[8] Rotman, J. J. Tanpa Tahun. *A First Course in Abstract Algebra. Third Edition.* Prentice-Hall, New Jersey

[9] Wallace, D. A. R. 1998. *Groups, Rings, and Fields.* Springer-Verlag, London

INDEKS

RIWAYAT HIDUP

Penulis bernama Putri Anggrayni, dilahirkan di Padang pada tanggal 31 Maret 1990 dari pasangan Syafrizal Umar dan Maya Sari. Penulis adalah anak pertama dari empat bersaudara. Penulis menamatkan pendidikan di TK Adabiah Padang pada tahun 1996, SD Adabiah I Padang pada tahun 2002, Kelas Akselerasi SMP Negeri 1 Padang pada tahun 2004, dan SMA Negeri 2 Padang pada tahun 2007. Pada tahun yang sama, penulis diterima sebagai mahasiswa Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Andalas melalui jalur Seleksi Penerimaan Mahasiswa Baru (SPMB).

Selama menjadi mahasiswa di Jurusan Matematika FMIPA Unand, penulis aktif sebagai anggota Himpunan Mahasiswa Matematika (HIMATIKA) FMIPA Unand dan pernah menjadi Pengurus Bidang III HIMATIKA pada periode XII, yaitu sebagai Koordinator Mading. Penulis juga pernah mengikuti Olimpiade Sains Nasional Pertamina (OSN-Pertamina) Bidang Matematika se-Sumatera Barat tahun 2011, Olimpiade Nasional Matematika dan Ilmu Pengetahuan Alam (ON-MIPA) Bidang Matematika se-Universitas Andalas tahun 2009 dan 2012, dan menjadi utusan delegasi Universitas Andalas pada ON-MIPA tingkat Koperatis Wilayah X Indonesia tahun 2012 di Pekanbaru, Riau.

Penulis juga merupakan asisten Laboratorium Statistika dan Komputasi Jurusan Matematika FMIPA Unand periode 2011/2012, serta sempat menjadi tenaga pengajar mata pelajaran Matematika di SMP Negeri 4 2×11 Kayu Tanam selama mengikuti Kuliah Kerja Nyata (KKN) pada tahun 2010 di Korong Rimbo Kalam Kenagarian Anduring Kecamatan 2×11 Kayu Tanam Kabupaten Padang Pariaman dalam rangka menyelesaikan salah satu mata kuliah wajib fakultas.