PENYELESAIAN SUATU PERSAMAAN DIOPHANTINE MENGGUNAKAN MODUL DARI MEDAN KUADRATIK

SKRIPSI

Diajukan untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Sains
Program Studi Matematika

Oleh:

Heribertus Heri Istiyanto

NIM : 003114020

PROGRAM STUDI MATEMATIKA JURUSAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS SANATA DHARMA
YOGYAKARTA

2004

SKRIPSI

PENYELESAIAN SUATU PERSAMAAN DIOPHANTINE MENGGUNAKAN MODUL DARI MEDAN KUADRATIK

Oleh:

Heribertus Heri Istiyanto

NIM: 003114020

Telah disetujui oleh:

Pembimbing

M.V. Any Herawati, S.Si., M.Si. tanggal 28 JUNI 2004

SKRIPSI

PENYELESAIAN SUATU PERSAMAAN DIOPHANTINE MENGGUNAKAN MODUL DARI MEDAN KUADRATIK

Dipersiapkan dan ditulis oleh

Heribertus Heri Istiyanto

NIM: 003114020

Telah dipertahankan di depan Panitia Penguji

pada tanggal 14 Juni 2004

dan dinyatakan memenuhi syarat.

Susunan Panitia Penguji

	Nama lengkap	Tanda tangan
Ketua	Dr. Frans Susilo, SJ	....
Sekretaris	M.V. Any Herawati, S.Si., M.Si.	....
Anggota	Prof. Drs. R. Soemantri	....
Anggota	Dr. Frans Susilo, SJ	....
Anggota	M.V. Any Herawati, S.Si., M.Si.	....

Yogyakarta, 28 Juni 2004

Fakultas MIPA

Universitas Sanata Dharma

Dekan,

Ir. Ig. Aris Dwiatmoko, M.Sc.

HALAMAN PERSEMBAHAN

Kita tidak tahu apapun tentang hari esok.
Tugas kita adalah menjadi baik dan bahagia hari ini.
-Sydney Smith-

Keinginan adalah sumber penderitaan,
tempatnya ada di dalam pikiran,
tujuan bukan utama,
yang utama adalah prosesnya,
kita hidup untuk mencari kebahagiaan.
-seperti matahari, Iwan Fals-

Kita dapat mencapai kebahagiaan
bila keinginan bukan lagi menjadi sumber penderitaan.
-heriest-

Skripsi ini kupersembahkan untuk:
Tuhan Yesus Kristus & Bunda Maria,
Bapak & Ibuku tercinta,
Mas Agus,
Erna atas segala dukungan dan doanya.

PERYATAAN KEASLIAN KARYA

Saya menyatakan dengan sesungguhnya bahwa skripsi yang saya tulis ini tidak memuat karya atau bagian karya orang lain, kecuali yang telah disebutkan dalam daftar pustaka, sebagaimana layaknya karya ilmiah.

Yogyakarta, 28 Juni 2004

Penulis

HB. Heri Istiyanto

ABSTRAK

Medan kuadratik $\mathbb{Q}(\sqrt{d})$ terdiri atas bilangan-bilangan kuadratik, yaitu bilangan-bilangan berbentuk $s + t\sqrt{d}$ dengan $s,t \in \mathbb{Q}$ dan d bilangan bulat bebas kuadrat. Bilangan $\alpha \in \mathbb{Q}(\sqrt{d})$ disebut bilangan bulat dari $\mathbb{Q}(\sqrt{d})$ jika $Tr(\alpha)$ dan $N(\alpha)$ adalah bilangan bulat. Himpunan semua bilangan bulat dari $\mathbb{Q}(\sqrt{d})$ terdiri atas bilangan-bilangan berbentuk $a + b\omega_d$ dengan $a,b \in \mathbb{Z}$ dan

$$\omega_d = \begin{cases} \sqrt{d} & \text{jika } d \equiv 2 \pmod 4 \text{ atau } d \equiv 3 \pmod 4 \\ \dfrac{1+\sqrt{d}}{2} & \text{jika } d \equiv 1 \pmod 4. \end{cases}$$

Berdasarkan teori tentang medan kuadratik, skripsi ini akan membahas algoritma untuk menentukan semua penyelesaian dari persamaan Diophantine $ax^2 + bxy + cy^2 = m$ dengan a,b,c,m bilangan rasional bulat dan $a \neq 0$. Masalah untuk menentukan semua penyelesaian dari persamaan Diophantine tersebut sama dengan masalah menentukan semua $\xi \in M$ sedemikian sehingga $N(\xi) = am$, dengan $M = \{\alpha x + \beta y \mid x, y \text{ bilangan rasional bulat}\}$, $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$, dan $\{\alpha, \beta\}$ suatu basis dari $\mathbb{Q}(\sqrt{d})$.

ABSTRACT

A quadratic field $\mathbb{Q}(\sqrt{d})$ consists of quadratic numbers, which are numbers of the form $s + t\sqrt{d}$, where s and t are rational numbers and d is a square-free integer. An element $\alpha \in \mathbb{Q}(\sqrt{d})$ is called an integer of $\mathbb{Q}(\sqrt{d})$ if $Tr(\alpha)$ and $N(\alpha)$ are integers. The set of integers of $\mathbb{Q}(\sqrt{d})$ consists of numbers of the form $a + b\omega_d$, where a and b are integers and

$$\omega_d = \begin{cases} \sqrt{d} & \text{if } d \equiv 2 \pmod 4 \text{ or } d \equiv 3 \pmod 4 \\ \dfrac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

Based on the theory of quadratic fields, this thesis will discuss an algorithm to find all solutions of a Diophantine equation of the form $ax^2 + bxy + cy^2 = m$, where a, b, c, m are rational integers and $a \neq 0$. The problem of finding all solutions of the Diophantine equation is equivalent to the problem of determining all $\xi \in M$ such that $N(\xi) = am$, where $M = \{\alpha x + \beta y \mid x, y \text{ rational integers}\}$, $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$, and $\{\alpha, \beta\}$ is a basis of $\mathbb{Q}(\sqrt{d})$.

KATA PENGANTAR

Puji dan syukur penulis panjatkan kehadirat Tuhan Yesus Kristus atas segala kasih dan perlindungan yang diberikan kepada penulis sehingga penulis akhirnya dapat menyelesaikan skipsi ini dengan baik.

Penulis menyadari bahwa skripsi ini tidak dapat terselesaikan tanpa adanya bantuan dari berbagai pihak, baik yang terlibat secara langsung maupun tidak langsung. Oleh karena itu pada kesempatan ini penulis ingin menyampaikan rasa terima kasih yang mendalam kepada:

1. Ibu M.V. Any Herawati, S.Si., M.Si. selaku dosen pembimbing skripsi dan panitia penguji, yang telah memberikan bimbingan, pengarahan, saran dan koreksi dalam penyusunan skripsi ini;
2. Romo Dr. Frans Susilo, SJ selaku Kaprodi Matematika dan panitia penguji, yang telah memberikan masukan dan saran yang bermanfaat bagi penulis dalam penyusunan skipsi ini, serta memeriksa dan merevisi abstrak yang berguna sebagai kelengkapan skripsi ini;
3. Bapak Prof. Drs. R. Soemantri, yang telah memberikan masukan dan saran yang berguna kepada penulis dalam penyelesaian skripsi ini;
4. Bapak Ir. Ig. Aris Dwiatmoko, M.Sc. dan Bapak A. Prasetyadi, S.Si., yang telah banyak membantu dalam kelancaran selama kuliah;
5. Seluruh dosen Program Studi Matematika yang selalu memberikan semangat dan dorongan kepada penulis baik selama kuliah maupun dalam penyusunan skripsi ini sehingga penulis dapat menyelesaikan studi dengan baik;

6. Ibu Ch. L. Suwarni dan Mas Tukija, serta seluruh staff perpustakaan Paingan yang telah banyak membantu penulis dalam urusan administrasi;
7. Kedua orangtuaku dan Mas Agus yang senantiasa mendukung selama kuliah dengan segenap kasih dan doanya;
8. Erna, yang dengan kesabarannya senantiasa memberikan dukungan, dorongan semangat dan doa baik selama kuliah maupun dalam penyusunan skripsi ini;
9. Teman-teman kisah klasikku di Matematika 2000: Heru, Wiwid, Bunga, Mira, Shinta, Meggy, Lissa, Anissa, Anjrah, Paula, Tanti, Lia, Dwi, Lina, Ayu, Tatik, Vincent, Widy, Deni, Ferry, Wanto, Feliks, Prast, Andi, Wahyu, Willy, Sunarta, Tony, Tika, Eros, Tini, Dewi, yang selalu mewarnai hari-hariku selama kuliah dan menyusun skripsi ini, serta memberikan semangat dan doa.
10. Mas-mas dan Mbak-mbak angkatan 98, 99 dan adik-adik angkatan 2001, 2002 dan 2003, Mas Adi'98, Ria'99, Eny'99, Tabita'01, Dani'01 yang selalu memberikan dukungan;
11. Teman-teman ikomp'00 dan PMat'00, Nyit-nyit, Dian,Temi, Lia-Sing'00, yang telah memberikan dukungan dan bantuan dalam ujian skripsi;
12. Teman-teman Mudika'46, PD Yohanes dan teman-teman kost di Gg. Buntu I, yang telah memberi dukungan moril dan doa kepada penulis.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Oleh karena itu penulis mengucapkan terima kasih bila ada kritik dan saran yang bermanfaat bagi penulis.

Penulis

DAFTAR ISI

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Dalam teori bilangan dikenal bermacam-macam persamaan Diophantine. Salah satu di antaranya, persamaan Diophantine berbentuk $ax^2 + bxy + cy^2 = m$, dengan a, b, c, m bilangan bulat yang diketahui, sedangkan x, y bilangan bulat yang akan dicari. Skripsi ini akan membahas algoritma untuk menentukan semua penyelesaian berupa bilangan bulat x, y dari persamaan Diophantine tersebut.

Meskipun persamaan Diophantine $ax^2 + bxy + cy^2 = m$ hanya merupakan persamaan yang menyangkut bilangan bulat saja baik konstanta maupun penyelesaian persamaan tersebut, namun untuk menentukan penyelesaiannya diperlukan semesta yang lebih luas dari $\mathbb{Z}$ (himpunan bilangan bulat) yaitu $\mathbb{C}$ (himpunan bilangan kompleks). Secara lebih khusus semesta yang dipakai adalah subhimpunan dari $\mathbb{C}$ yaitu $\mathbb{Q}(\sqrt{d})$ atau medan kuadratik. Skripsi ini juga akan membahas subhimpunan lain dari $\mathbb{Q}(\sqrt{d})$ yaitu himpunan bilangan bulat dari $\mathbb{Q}(\sqrt{d})$ dan modul dari $\mathbb{Q}(\sqrt{d})$.

B. Rumusan Masalah

Berdasarkan latar belakang masalah di atas maka dapat dibuat rumusan masalah sebagai berikut:

1) Apakah yang dimaksud dengan medan kuadratik?
2) Apakah yang dimaksud dengan bilangan bulat dari $Q(\sqrt{d})$ dan bagaimanakah sifat-sifatnya?
3) Apakah yang dimaksud dengan modul dari $Q(\sqrt{d})$ dan bagaimanakah sifatnya?
4) Bagaimanakah algoritma untuk menentukan semua penyelesaian dari persamaan Diophantine $ax^2 + bxy + cy^2 = m$?

C. Pembatasan Masalah

Persamaan Diophantine $ax^2 + bxy + cy^2 = m$ dapat dinyatakan dalam bentuk $\left(ax + \frac{b+\sqrt{D}}{2}y\right)\left(ax + \frac{b-\sqrt{D}}{2}y\right) = am$ dengan $D = b^2 - 4ac$. Selain itu D juga dapat dinyatakan sebagai $D = k^2 d$, dengan k bilangan bulat positif dan d bilangan bulat bebas kuadrat. Skripsi ini hanya akan membahas penyelesaian dari persamaan Diophantine $ax^2 + bxy + cy^2 = m$ dengan D bukan kuadrat bilangan bulat dan d bilangan bulat negatif bebas kuadrat.

D. Tujuan Penulisan

Tujuan dari penulisan skripsi ini adalah untuk mendeskripsikan konsep-konsep tentang medan kuadratik atau $\mathbb{Q}(\sqrt{d})$ yang digunakan untuk menentukan semua penyelesaian dari persamaan Diophantine $ax^2 + bxy + cy^2 = m$.

E. Metode Penulisan

Metode yang digunakan dalam penulisan skripsi ini adalah metode studi pustaka.

F. Sistematika Pembahasan

BAB I. PENDAHULUAN

A. Latar Belakang Masalah

B. Rumusan Masalah

C. Pembatasan Masalah

D. Tujuan Penulisan

E. Metode Penulisan

F. Sistematika Pembahasan

BAB II. KONSEP DASAR DALAM ALJABAR DAN TEORI BILANGAN

A. Gelanggang dan Medan

B. Ruang Vektor

BAB II

KONSEP DASAR DALAM ALJABAR

DAN TEORI BILANGAN

Dalam bab ini akan dibahas materi-materi prasyarat yang digunakan sebagai landasan bab-bab berikutnya. Skripsi ini menggunakan notasi $\mathbb{N}$ untuk menyatakan himpunan semua bilangan asli, notasi $\mathbb{Z}$ untuk menyatakan himpunan semua bilangan bulat, notasi $\mathbb{Q}$ untuk menyatakan himpunan semua bilangan rasional, notasi $\mathbb{R}$ untuk menyatakan himpunan semua bilangan real, dan notasi $\mathbb{C}$ untuk menyatakan himpunan semua bilangan kompleks.

A. Gelanggang dan Medan

Definisi 2.1.1:

Suatu **gelanggang** $\langle R,+,\cdot\rangle$ adalah himpunan R yang dilengkapi dengan dua operasi biner yaitu penjumlahan $(+)$ dan perkalian $(\cdot)$ yang didefinisikan di R yang memenuhi sifat-sifat:

Terhadap operasi penjumlahan $\langle R,+\rangle$:

i) $(\forall a,b \in R)\, a+b \in R$,

ii) $(\forall a,b \in R)\, a+b = b+a$,

iii) $(\forall a,b,c \in R)\, (a+b)+c = a+(b+c)$,

iv) $(\exists 0 \in R)(\forall a \in R)\, a + 0 = a,$

v) $(\forall a \in R)(\exists -a \in R)\, a + (-a) = 0.$

Terhadap operasi perkalian $\langle R, \cdot \rangle$:

i) $(\forall a, b \in R)\, a \cdot b \in R,$

ii) $(\forall a, b, c \in R)\, (a \cdot b) \cdot c = a \cdot (b \cdot c),$

iii) $(\forall a, b, c \in R)\, a \cdot (b + c) = a \cdot b + a \cdot c$ dan $(b + c) \cdot a = b \cdot a + c \cdot a.$

Dalam aksioma-aksioma di atas, selanjutnya elemen 0 disebut **elemen identitas** terhadap operasi penjumlahan, sedangkan $-a$ disebut **invers dari** a **terhadap operasi penjumlahan**.

Contoh 2.1.1:

Himpunan $\mathbb{Z}$ terhadap operasi penjumlahan $(+)$ dan perkalian $(\cdot)$ merupakan gelanggang.

Definisi 2.1.2:

Misalkan $\langle R, +, \cdot \rangle$ suatu gelanggang. Subhimpunan S dari R yang tidak kosong disebut **subgelanggang** dari R, jika S membentuk gelanggang terhadap operasi penjumlahan $(+)$ dan perkalian $(\cdot)$ yang didefinisikan di R.

Teorema berikut dapat memudahkan untuk melakukan verifikasi apakah suatu subhimpunan membentuk subgelanggang:

Teorema 2.1.1:

Misalkan $\langle R,+,\cdot\rangle$ suatu gelanggang dan S suatu subhimpunan R yang tidak kosong, maka S membentuk subgelanggang jika dan hanya jika berlaku:

i) $(\forall a,b \in S)\ ab \in S,$

ii) $(\forall a,b \in S)\ a-b \in S.$

Bukti:

($\Rightarrow$) Ambil $a,b \in S$, maka $ab \in S$ karena S subgelanggang. Sifat ii) dipenuhi karena $-b \in S$, sehingga $a+(-b)=a-b \in S.$

($\Leftarrow$) Terhadap operasi penjumlahan (+):

Ambil $a \in R$, maka $a-a=0 \in S$ (sifat ii). Sehingga $0 \in S$. Jadi S memuat elemen identitas.

Karena $0 \in S$, maka menurut sifat ii) $0-a \in S$. Sehingga:

$0-a=0+(-a)=-a \in S.$ Jadi untuk setiap $a \in S$ mempunyai invers terhadap operasi penjumlahan (+).

Bila $b \in S$, maka $-b \in S$, sehingga $a-(-b)=a+b \in S.$

Jadi operasi penjumlahan(+) di S bersifat tertutup.

Karena $S \subseteq R$ maka operasi penjumlahan(+) pada S juga komutatif dan assosiatif.

Terhadap perkalian $(\cdot)$:

Ambil $a,b \in S$, maka $ab \in S$ (sifat(i)). Sehingga S tertutup terhadap operasi perkalian$(\cdot)$.

Sifat assosiatif dan distributif pasti dipenuhi karena $S \subseteq R.$ ■

Dengan demikian sistem $\langle S,+,\cdot\rangle$ membentuk gelanggang, yaitu subgelanggang dari R.

Definisi 2.1.3:

Suatu gelanggang R yang bersifat komutatif terhadap operasi perkalian disebut **gelanggang komutatif**. Suatu gelanggang R dengan **elemen satuan** e **terhadap perkalian**, yaitu elemen yang memenuhi $ex = xe = x$ untuk setiap $x \in R$, disebut **gelanggang dengan elemen satuan**.

Definisi 2.1.4:

Misalkan R adalah gelanggang dengan elemen satuan. Suatu elemen $a \in R$ disebut **unit** jika terdapat $b \in R$ yang memenuhi $a \cdot b = b \cdot a = e$. Selanjutnya b disebut **invers dari** a **terhadap perkalian** dan ditulis a^{-1}.

Definisi 2.1.5:

Suatu gelanggang komutatif dengan elemen satuan disebut **medan** jika setiap elemen yang tidak sama dengan 0 mempunyai invers terhadap perkalian.

Subgelanggang disebut **submedan** jika komutatif dan setiap elemen yang tidak sama dengan 0 mempunyai invers terhadap perkalian.

Contoh 2.1.2:

Himpunan $\mathbb{Q}$, $\mathbb{R}$ dan $\mathbb{C}$ terhadap operasi penjumlahan $(+)$ dan perkalian $(\cdot)$ merupakan medan.

Definisi 2.1.6:

Jika a dan b dua elemen tak nol dalam gelanggang R, sehingga $ab = 0$ maka a dan b disebut **pembagi nol**.

Jadi a dan b pembagi nol bila $a \neq 0$, $b \neq 0$ dan $ab = 0$, Akibatnya gelanggang R tidak memuat pembagi nol jika

i) $ab = 0$ maka $a = 0$ atau $b = 0$, atau

ii) jika $a \neq 0$ dan $b \neq 0$ maka $ab \neq 0$, atau

iii) jika $ab = 0$ dan $a \neq 0$ maka $b = 0$.

Definisi 2.1.7:

Jika $\langle R,+,\cdot \rangle$ gelanggang komutatif dengan elemen satuan e yang tidak memuat pembagi nol, maka R disebut **daerah integral**.

Selanjutnya, subgelanggang disebut **subdaerah-integral** jika komutatif dan tidak memuat pembagi nol.

Teorema 2.1.2:

Setiap medan merupakan daerah integral.

Bukti:

Misal F suatu medan.

Tinggal dibuktikan bahwa F tidak memuat pembagi nol.

Ambil $a, b \in F$ dengan $a \neq 0$ dan $ab = 0$.

Karena $a \neq 0$ maka terdapat $a^{-1} \in F$ sehingga $aa^{-1} = a^{-1}a = e$.

Akibatnya:

$$ab = 0$$
$$a^{-1}(ab) = a^{-1}0$$
$$(a^{-1}a)b = 0$$
$$eb = 0$$
$$b = 0.$$

Hal ini berarti F tidak memuat pembagi nol, sehingga F merupakan suatu daerah integral. ■

B. Ruang Vektor

Definisi 2.2.1:

Misalkan F suatu medan. Himpunan V yang dilengkapi dengan operasi penjumlahan, yaitu $(\forall \alpha, \beta \in V)\ \alpha + \beta \in V$, dan perkalian dengan skalar, yaitu $(\forall a \in F)(\forall \alpha \in V)\ a\alpha \in V$, disebut **ruang vektor atas** F jika V terhadap operasi penjumlahan merupakan grup komutatif dan perkalian dengan skalarnya memenuhi sifat-sifat berikut:

i) $(\forall a, b \in F)(\forall \alpha \in V)(a + b)\alpha = a\alpha + b\alpha,$

ii) $(\forall a \in F)(\forall \alpha, \beta \in V)\ a(\alpha + \beta) = a\alpha + a\beta,$

iii) $(\forall a, b \in F)(\forall \alpha \in V)\ a(b\alpha) = (ab)\alpha,$

iv) $(\forall \alpha \in V)\ e\alpha = \alpha,$ e elemen satuan di F.

Elemen-elemen di V disebut **vektor** dan elemen-elemen di F disebut **skalar**.

Definisi 2.2.2:

Misalkan V ruang vektor atas medan F dan $\alpha_1, \alpha_2, \ldots, \alpha_n \in V$. Suatu elemen $\alpha \in V$ disebut **kombinasi linear** dari $\alpha_1, \alpha_2, \ldots, \alpha_n$ jika terdapat $a_1, a_2, \ldots, a_n \in F$ sedemikian sehingga

$$\alpha = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n.$$

Vektor-vektor $\alpha_1, \alpha_2, \ldots, \alpha_n \in V$ disebut **pembangun** atau **perentang** dari V jika setiap vektor dari V merupakan kombinasi linear dari $\alpha_1, \alpha_2, \ldots, \alpha_n$.

Definisi 2.2.3:

Jika V adalah ruang vektor atas medan F, maka $\alpha_1, \alpha_2, \ldots, \alpha_n \in V$ disebut **bebas linear** atas F jika

$$a_1\alpha_1 + a_2\alpha_2 + \ldots + a_n\alpha_n = 0$$

mengakibatkan $a_i = 0$ untuk setiap $i = 1,2,\ldots,n$.

Jika terdapat $a_i \neq 0$ sedemikian sehingga $a_1\alpha_1 + a_2\alpha_2 + \ldots + a_n\alpha_n = 0$, maka $\alpha_1, \alpha_2, \ldots, \alpha_n$ disebut **bergantung linear**.

Definisi 2.2.4:

Misalkan V merupakan ruang vektor atas medan F dan $\alpha_1, \alpha_2, \ldots, \alpha_n \in V$, maka himpunan $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ disebut **basis** untuk V jika $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ bebas linear dan merentang V.

C. PEMBAGIAN DAN KONGRUENSI

Pada bagian ini akan dibahas teori-teori dan sifat-sifat dasar dalam teori bilangan yang berkaitan dengan topik utama, yaitu teori tentang pembagian, dan teori kongruensi.

Definisi 2.3.1:

Misalkan $a, b \in \mathbb{Z}$. Bilangan bulat a **habis dibagi** bilangan bulat b (ditulis $b \mid a$) jika dan hanya jika terdapat $c \in \mathbb{Z}$ sedemikian sehingga $a = cb$. Jika a **tidak habis dibagi** b, ditulis $b \nmid a$.

Contoh 2.3.1:

i) $5 \mid 5$ dan $-2 \mid 8$.

ii) $7 \nmid 15$, karena tidak terdapat $c \in \mathbb{Z}$ sehingga $15 = 7c$.

Teorema 2.3.1:

Misalkan $a, b, c \in \mathbb{Z}$, maka berlaku sifat-sifat berikut:

i) Jika $a \mid b$ dan $a \mid c$ maka $a \mid (b \pm c)$.

ii) Jika $a \mid b$ dan $b \mid c$ maka $a \mid c$.

iii) Jika $a \mid b$ dan $a \mid c$ maka $a \mid (bx + cy), \forall x, y \in \mathbb{Z}$.

iv) Jika $a \mid b$ dan $c \mid d$ maka $ac \mid bd$.

v) $a \mid b$ jika dan hanya jika $ac \mid bc$, $\forall c \neq 0$.

Bukti:

i) Karena $a \mid b$ dan $a \mid c$ maka $b = ka$ dan $c = ma$, untuk suatu $k, m \in \mathbb{Z}$

sehingga:

$$b \pm c = ka \pm ma$$

$$= (k \pm m)a, \text{ dengan } k \pm m \in \mathbb{Z}.$$

Jadi $a \mid (b \pm c)$.

ii) Karena $a \mid b$ dan $b \mid c$ maka $b = ma$ dan $c = nb$, untuk suatu $m, n \in \mathbb{Z}$,

sehingga:

$$c = n(ma)$$

$$= (nm)a$$

$$= pa, \text{ dengan } p = nm \in \mathbb{Z}.$$

Jadi $a \mid c$.

iii) Ambil sembarang $x, y \in \mathbb{Z}$.

Karena $a \mid b$ dan $a \mid c$ maka terdapat $m, n \in \mathbb{Z}$ sedemikian sehingga

$b = ma$ dan $c = na$. Perhatikan bahwa:

$$bx + cy = (ma)x + (na)y$$

$= a(mx + ny)$

$= ap$, dengan $p = mx + ny \in \mathbb{Z}$.

Jadi $a \mid (bx + cy)$.

iv) Karena $a \mid b$ dan $c \mid d$ maka $b = ma$ dan $d = nc$, untuk suatu $m, n \in \mathbb{Z}$

sehingga:

$$bd = (ma)(nc)$$
$$= (mn)(ac)$$
$$= k(ac), \text{ dengan } k = mn \in \mathbb{Z}.$$

Jadi $ac \mid bd$.

v) $(\Rightarrow)$ $a \mid b$ maka $b = ma$, untuk suatu $m \in \mathbb{Z}$, sehingga:

$$bc = (ak)c, \; c \neq 0$$
$$= (ac)k.$$

Jadi $ac \mid bc$.

$(\Leftarrow)$ $ac \mid bc$ maka $bc = (ac)p$, untuk suatu $p \in \mathbb{Z}$. Karena $c \neq 0$ maka

$b = ap$. Sehingga $a \mid b$. ■

Contoh 2.3.2:

i) Dari Teorema 2.1.1 bagian (i), karena $2 \mid 4$ dan $2 \mid 6$ maka $2 \mid (4 \pm 6)$.

ii) Dari Teorema 2.1.1 bagian (iii), karena $3 \mid 6$ dan $3 \mid 12$ maka $3 \mid (6x+12y), \forall x, y \in \mathbb{Z}$. Misalkan $x = 2$ dan $y = 1$ maka $3 \mid 24$.

Definisi 2.3.2:

Misalkan n bilangan bulat positif. Bilangan bulat a dan b disebut **kongruen modulo** n ditulis $a \equiv b(\bmod n)$ jika $n \mid (a-b)$. Jika a tidak kongruen terhadap b modulo n ditulis $a \not\equiv b$ (mod n).

Contoh 2.3.3:

Bilangan $44 \equiv 8(\bmod 12)$, karena $12 \mid (44\text{-}8)$ sedangkan $40 \not\equiv 8$ (mod 12) karena $12 \nmid (40\text{-}8)$.

Definisi 2.3.3:

Misalkan himpunan A tidak kosong. Relasi $\sim$ di A disebut **relasi ekivalen** jika untuk setiap $a, b, c \in A$ berlaku:

i) a ~ a (sifat refleksif),

ii) Jika a ~ b, maka b ~ a (sifat simetris),

iii) Jika a ~ b dan b ~ c, maka a ~ c (sifat transitif).

Teorema 2.3.2:

Relasi '≡' merupakan suatu relasi ekivalen di $\mathbb{Z}$.

Bukti:

Ambil sembarang $a,b,c \in \mathbb{Z}$.

i) $a \equiv a (\bmod n)$ karena $n \mid (a-a)$.

ii) Diketahui $a \equiv b (\bmod n)$, maka $n \mid (a-b)$. Sehingga $n \mid (b-a)$ atau $b \equiv a (\bmod n)$.

iii) Diketahui $a \equiv b (\bmod n)$ dan $b \equiv c (\bmod n)$, maka $n \mid (a-b)$ dan $n \mid (b-c)$. Sehingga menurut Teorema 2.3.1 (i) $n \mid (a-b+b-c)$ atau $n \mid (a-c)$. Sehingga $a \equiv c (\bmod n)$.

Jadi relasi '≡' bersifat refleksif, simetris dan transitif. Dengan demikian relasi '≡' merupakan suatu relasi ekivalen. ■

Teorema 2.3.3:

Misalkan $a \equiv b (\bmod n)$ dan $c \equiv d (\bmod n)$, maka berlaku sifat-sifat berikut:

i) $(a+c) \equiv (b+d)(\bmod n)$,

ii) $(a-c) \equiv (b-d)(\bmod n)$,

iii) $(ac) \equiv (bd)(\bmod n)$.

Bukti:

Diketahui $a \equiv b (\bmod n)$ dan $c \equiv d (\bmod n)$. maka $n \mid (a-b)$ dan $n \mid (c-d)$.

i) Karena $n \mid (a-b)$ dan $n \mid (c-d)$ maka menurut Teorema 2.3.1(i) diperoleh $n \mid [(a-b)+(c-d)]$ atau $n \mid [(a+c)-(b+d)]$. Sehingga $(a+c) \equiv (b+d)(\text{mod}\, n)$.

ii) Karena $n \mid (a-b)$ dan $n \mid (c-d)$ maka menurut Teorema 2.3.1(i) diperoleh $n \mid [(a-b)-(c-d)]$ atau $n \mid [(a-c)-(b-d)]$ Sehingga $(a-c) \equiv (b-d)(\text{mod}\, n)$.

iii) Karena $n \mid (a-b)$ maka $n \mid [c(a-b)]$, sehingga $n \mid (ac-bc)$ yang berarti $(ac) \equiv (bc)(\text{mod}\, n)$, Karena $n \mid (c-d)$ maka $n \mid [b(c-d)]$, sehingga $n \mid (bc-bd)$ yang berarti $(bc) \equiv (bd)(\text{mod}\, n)$. Menurut Teorema 2.3.2 relasi '≡', suatu relasi ekivalen yang bersifat transitif, sehingga karena $(ac) \equiv (bc)(\text{mod}\, n)$ dan $(bc) \equiv (bd)(\text{mod}\, n)$ maka $(ac) \equiv (bc) \equiv (bd)(\text{mod}\, n)$.

Jadi $(ac) \equiv (bd)(\text{mod}\, n)$. ■

Contoh 2.3.4:

Karena $2 \equiv 5(\text{mod}\, 3)$ dan $1 \equiv 4(\text{mod}\, 3)$ maka menurut Teorema 2.3.3 berlaku:

1) $(2+1) \equiv (5+4)(\text{mod}\, 3)$ atau $3 \equiv 9(\text{mod}\, 3)$,

2) $(2-1) \equiv (5-4)(\text{mod}\, 3)$ atau $1 \equiv 1(\text{mod}\, 3)$ dan

3) $2 \equiv 20(\text{mod}\, 3)$.

Teorema 2.3.4: (Induksi Matematik)

Jika $P(n)$ merupakan suatu proposisi yang didefinisikan pada himpunan semua bilangan bulat positif $\mathbb{N}$, artinya $P(n)$ dapat bernilai benar atau salah, dan $P(n)$ mempunyai sifat:

i) $P(1)$ benar, dan

ii) Jika $P(k)$ benar, maka $P(k+1)$ benar,

maka $P(n)$ benar untuk semua $n \in \mathbb{N}$.

Teorema 2.3.5:

Jika k bulat positif dan $a \equiv b (\mathrm{mod}\ n)$, maka $a^k \equiv b^k (\mathrm{mod}\ n)$.

Bukti:

Teorema ini akan dibuktikan dengan induksi matematik.

Akan dibuktikan teorema benar untuk $k = 1$, yaitu

$$a^1 \equiv b^1 (\mathrm{mod}\ n).$$

Karena $a^1 = a$ dan $b^1 = b$, padahal diketahui $a \equiv b (\mathrm{mod}\ n)$ maka $a^1 \equiv b^1 (\mathrm{mod}\ n)$.

Jadi pernyataan benar untuk $k = 1$.

Selanjutnya, akan dibuktikan teorema benar untuk $k = 2,3,4,\ldots\ldots$

Andaikan pernyataan benar untuk $k = m$, sehingga $a^m \equiv b^m (\mathrm{mod}\ n)$.

Akan dibuktikan teorema benar untuk $k = m+1$, yaitu dibuktikan:

$$a^{m+1} \equiv b^{m+1} (\mathrm{mod}\ n).$$

Diketahui $a \equiv b(\bmod n)$ dan $a^m \equiv b^m(\bmod n)$, maka

$$aa^m \equiv bb^m(\bmod n)$$

$$a^{m+1} \equiv b^{m+1}(\bmod n)$$

Jadi, teorema benar untuk $k = m+1$. ■

Contoh 2.3.5:

Karena $2 \equiv 4(\bmod 2)$ maka $2^3 \equiv 4^3(\bmod 2)$ atau $8 \equiv 64(\bmod 2)$.

Selanjutnya dengan menggunakan pengertian kongruensi diatas berikut akan didefinisikan bilangan genap dan bilangan ganjil.

Definisi 2.3.4:

Bilangan bulat m disebut **bilangan genap** jika $m \equiv 0(\bmod 2)$, sedangkan m **bilangan ganjil** jika $m \equiv 1(\bmod 2)$.

Definisi 2.3.5:

Bilangan bulat d disebut **bilangan bulat kuadrat sempurna** jika $d = s^2$ untuk suatu bilangan bulat s.

Teorema 2.3.6:

Untuk setiap bilangan $m \in \mathrm{Z}$ berlaku:

i) m genap jika dan hanya jika $m^2 \equiv 0(\bmod 4)$.

ii) m ganjil jika dan hanya jika $m^2 \equiv 1(\text{mod}\,4)$.

Bukti:

i) ($\Rightarrow$) Untuk m genap, yaitu $m \equiv 0(\text{mod}\,2)$ maka $m = 2k_1$, untuk suatu $k_1 \in \mathbb{Z}$. Sehingga:

$$m^2 = 4k_1^2$$
$$= 4l,\ l = k_1^2 \in \mathbb{Z}.$$

Jadi $m^2 \equiv 0(\text{mod}\,4)$.

($\Leftarrow$) Andaikan m tidak genap atau m ganjil, maka $m^2 \equiv 1(\text{mod}\,4)$.

Kontradiksi, dengan yang diketahui yaitu $m^2 \equiv 0(\text{mod}\,4)$, karena untuk setiap bilangan $m \in \mathbb{Z}$ berlaku $m^2 \equiv 0(\text{mod}\,4)$ atau $m^2 \equiv 1(\text{mod}\,4)$.

ii) ($\Rightarrow$) Untuk m ganjil, yaitu $m \equiv 1(\text{mod}\,2)$ maka $m = 2k_2 + 1$, untuk suatu $k_2 \in \mathbb{Z}$. Sehingga:

$$m^2 = (2k_2 + 1)^2$$
$$= 4k_2^2 + 4k_2 + 1$$
$$m^2 - 1 = 4k_2^2 + 4k_2.$$

Jadi, $m^2 \equiv 1(\text{mod}\,4)$.

($\Leftarrow$) Andaikan m tidak ganjil atau m genap, maka $m^2 \equiv 0(\text{mod}\,4)$.

Kontradiksi, dengan yang diketahui yaitu $m^2 \equiv 1(\text{mod}\,4)$, karena untuk setiap bilangan $m \in \mathbb{Z}$ berlaku $m^2 \equiv 0(\text{mod}\,4)$ atau $m^2 \equiv 1(\text{mod}\,4)$.

■

Dengan demikian, untuk setiap bilangan $m \in \mathbb{Z}$ berlaku $m^2 \equiv 0(\text{mod}\,4)$ atau $m^2 \equiv 1(\text{mod}\,4)$. Teorema ini juga mengatakan bahwa bilangan bulat kuadrat sempurna kongruen 0 atau 1 modulo 4.

Contoh 2.3.6:

Perhatikan bahwa $2^2 \equiv 0(\text{mod}\,4)$ sehingga 2 genap.

Definisi 2.3.6:

Jika $a, b \in \mathbb{Z}$ dan $a \neq 0, b \neq 0$, maka **kelipatan persekutuan** dari a dan b adalah bilangan bulat positif m yang memenuhi $a \mid m$ dan $b \mid m$.

Contoh 2.3.7:

Salah satu kelipatan persekutuan dari 5 dan 7 adalah 35 karena $5 \mid 35$ dan $7 \mid 35$.

BAB III

MEDAN KUADRATIK

Pengertian dan sifat-sifat dasar medan kuadratik dan bilangan bulat dari medan kuadratik akan dibahas pada bab ini. Dasar teori dalam bab ini akan digunakan untuk mencari algoritma untuk menyelesaikan persamaan Diophantine pada selanjutnya. Terlebih dahulu akan didefinisikan bilangan bulat bebas kuadrat dan bilangan kuadratik.

A. Medan Kuadratik

Definisi 3.1.1:

Bilangan bulat d disebut **bilangan bulat bebas kuadrat** jika $d \neq 0$, $d \neq 1$ dan d tidak habis dibagi oleh bilangan bulat kuadrat sempurna selain 1.

Bilangan-bilangan tersebut adalah $-1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 7, \pm 10, \pm 11, \cdots$

Definisi 3.1.2:

Bilangan kuadratik adalah bilangan yang berbentuk $s + t\sqrt{d}$, dengan $s, t \in \mathbb{Q}$ dan d bilangan bulat bebas kuadrat.

Himpunan semua bilangan kuadratik dinyatakan dengan $\mathbb{Q}(\sqrt{d})$. Perhatikan bahwa jika $d > 0$, maka $s + t\sqrt{d}$ merupakan suatu bilangan real.

Sehingga $\mathbb{Q}(\sqrt{d})$ termuat dalam $\mathbb{R}$. Di lain pihak, jika $d < 0$ maka $\sqrt{d}$ merupakan suatu bilangan kompleks, sehingga $\mathbb{Q}(\sqrt{d})$ termuat dalam $\mathbb{C}$.

Jika $\mathbb{R}$, $\mathbb{Q}(\sqrt{d})$ dan $\mathbb{C}$ dibandingkan maka diperoleh hubungan sebagai berikut:

1. Jika $d > 0$ maka $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{R} \subset \mathbb{C}$.
2. Jika $d < 0$ maka $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{C}$, $\mathbb{R} \subseteq \mathbb{C}$ dan $(\mathbb{Q}(\sqrt{d}) \not\subseteq \mathbb{R}$.

Definisi 3.1.3:

Bilangan bulat Gauss adalah bilangan kompleks yang berbentuk $x + iy$, $x, y \in \mathbb{Z}$ dan $i = \sqrt{-1}$. Himpunan semua bilangan bulat Gauss dinyatakan dengan $\mathbb{Z}\,[i]$.

Perhatikan bahwa himpunan semua bilangan bulat Gauss $\mathbb{Z}[i]$ termuat dalam medan kuadratik $\mathbb{Q}(\sqrt{-1})$. Sehingga $\mathbb{Z}\,[i] \subset \mathbb{Q}(\sqrt{d}) \subset \mathbb{C}$.

Selanjutnya operasi pada $\mathbb{Q}(\sqrt{d})$ didefinisikan sesuai dengan operasi penjumlahan (+) dan perkalian $(\cdot)$ pada $\mathbb{C}$. Himpunan $\mathbb{Q}(\sqrt{d})$ yang dilengkapi dengan operasi penjumlahan (+) dan perkalian $(\cdot)$ ditulis $(\mathbb{Q}(\sqrt{d}),+,\cdot)$.

Adapun struktur yang dimiliki oleh $\mathbb{Q}(\sqrt{d})$ diberikan pada teorema berikut.

Teorema 3.1.1:

$(\mathbb{Q}(\sqrt{d}),+,\cdot)$ membentuk suatu medan.

Bukti:

Terhadap operasi penjumlahan $(\mathbb{Q}(\sqrt{d}),+)$:

i) Misalkan $\alpha,\beta \in \mathbb{Q}(\sqrt{d})$ dengan $\alpha = s+t\sqrt{d}, \beta = u+v\sqrt{d}$ maka

$$\alpha+\beta = (s+t\sqrt{d})+(u+v\sqrt{d})$$

$$=(s+u)+(t+v)\sqrt{d} \in \mathbb{Q}(\sqrt{d}).$$

Jadi, $\mathbb{Q}(\sqrt{d})$ tertutup terhadap operasi penjumlahan.

ii) Misalkan $\alpha,\beta \in \mathbb{Q}(\sqrt{d})$ dengan $\alpha = s+t\sqrt{d}, \beta = u+v\sqrt{d}$ maka

$$\alpha+\beta = (s+t\sqrt{d})+(u+v\sqrt{d})$$

$$=(s+t\sqrt{d}+u+v\sqrt{d})$$

$$=(u+v\sqrt{d}+s+t\sqrt{d})$$

$$=(u+v\sqrt{d})+(s+t\sqrt{d})$$

$$=\beta+\alpha.$$

Jadi, operasi penjumlahan pada $\mathbb{Q}(\sqrt{d})$ bersifat komutatif.

iii) Misalkan $\alpha,\beta,\gamma \in \mathbb{Q}(\sqrt{d}), \alpha = s+t\sqrt{d},\ \beta = u+v\sqrt{d}\ \ \gamma = x+y\sqrt{d}$

maka

$$(\alpha+\beta)+\gamma = (s+t\sqrt{d}+u+v\sqrt{d})+(x+y\sqrt{d})$$

$$= (s + t\sqrt{d} + u + v\sqrt{d} + x + y\sqrt{d})$$

$$= (s + t\sqrt{d}) + (u + v\sqrt{d} + x + y\sqrt{d})$$

$$= \alpha + (\beta + \gamma).$$

Jadi, operasi penjumlahan pada $\mathbb{Q}(\sqrt{d})$ bersifat assosiatif.

iv) Terdapat $0 \in \mathbb{Q}(\sqrt{d})$ sedemikian sehingga untuk setiap $\alpha \in \mathbb{Q}(\sqrt{d})$ dengan $\alpha = s + t\sqrt{d}$, berlaku:

$\alpha + 0 = s + t\sqrt{d} + 0 = s + t\sqrt{d} = \alpha$ dan

$0 + \alpha = s + t\sqrt{d} + 0 = s + t\sqrt{d} = \alpha.$

Jadi, $\mathbb{Q}(\sqrt{d})$ mempunyai elemen identitas terhadap penjumlahan.

v) Misalkan $\alpha \in \mathbb{Q}(\sqrt{d})$ dengan $\alpha = s + t\sqrt{d}$. Karena $s, t \in \mathbb{Q}$ maka $-s, -t \in \mathbb{Q}$, sehingga $-\alpha = -s - t\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ dan

$$\alpha + (-\alpha) = (s + t\sqrt{d}) + (-s - t\sqrt{d})$$

$$= (s + t\sqrt{d} - s - t\sqrt{d})$$

$$= 0.$$

Jadi, setiap elemen dalam $\mathbb{Q}(\sqrt{d})$ mempunyai invers terhadap operasi penjumlahan.

Terhadap operasi perkalian $(\mathbb{Q}(\sqrt{d}), \cdot)$:

i) Misalkan $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$ dengan $\alpha = s + t\sqrt{d}, \beta = u + v\sqrt{d}$ maka

$$\alpha\beta = (s+t\sqrt{d})(u+v\sqrt{d})$$

$$= su + tu\sqrt{d} + sv\sqrt{d} + tvd$$

$$= (su+tvd) + (tu+sv)\sqrt{d} \in \mathbb{Q}(\sqrt{d}).$$

Jadi, $\mathbb{Q}(\sqrt{d})$ tertutup terhadap operasi perkalian.

ii) Misalkan $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$ dengan $\alpha = s+t\sqrt{d}, \beta = u+v\sqrt{d}$ maka

$$\alpha\beta = (s+t\sqrt{d})(u+v\sqrt{d})$$

$$= su + tu\sqrt{d} + sv\sqrt{d} + tvd$$

$$= us + vs\sqrt{d} + ut\sqrt{d} + vtd$$

$$= (u+v\sqrt{d})(s+t\sqrt{d})$$

$$= \beta\alpha.$$

Jadi, operasi perkalian pada $\mathbb{Q}(\sqrt{d})$ bersifat komutatif.

iii) Misalkan $\alpha, \beta, \gamma \in \mathbb{Q}(\sqrt{d})$, $\alpha = s+t\sqrt{d}$, $\beta = u+v\sqrt{d}$ $\gamma = x+y\sqrt{d}$

maka

$$(\alpha\beta)\gamma = (s+t\sqrt{d})(u+v\sqrt{d})(x+y\sqrt{d})$$

$$= (su + tu\sqrt{d} + sv\sqrt{d} + tvd)(x+y\sqrt{d})$$

$$= (su)x + (tu\sqrt{d})x + (sv\sqrt{d})x + (tvd)x + (su)y\sqrt{d} + tuyd +$$

$$svyd + (tvd)y\sqrt{d}$$

$$= s(ux) + (t\sqrt{d})ux + (s\sqrt{d})vx + (td)vx + (s\sqrt{d})uy + (td)uy +$$

$$s(vyd) + (t\sqrt{d})vyd$$

$$= s(ux) + s(vyd) + (t\sqrt{d})ux + (t\sqrt{d})vyd + (s\sqrt{d})vx + (s\sqrt{d})uy +$$

$$(td)vx + (td)uy$$

$$= s(ux + vyd) + t\sqrt{d}(ux + vyd) + s(vx\sqrt{d} + uy\sqrt{d}) +$$

$$t\sqrt{d}(vx\sqrt{d} + uy\sqrt{d})$$

$$= (s + t\sqrt{d})(ux + vyd) + (s + t\sqrt{d})(vx\sqrt{d} + uy\sqrt{d})$$

$$= (s + t\sqrt{d})(ux + vyd + vx\sqrt{d} + uy\sqrt{d})$$

$$= (s + t\sqrt{d})((u + v\sqrt{d})(x + y\sqrt{d}))$$

$$= \alpha(\beta\gamma).$$

Jadi, operasi perkalian pada Q($\sqrt{d}$)bersifat assosiatif.

iv) Terdapat 1 $\in$Q($\sqrt{d}$) sedemikian sehingga untuk setiap $\alpha \in$Q($\sqrt{d}$)

dengan $\alpha = s + t\sqrt{d}$ berlaku

$$1(s + t\sqrt{d}) = (s + t\sqrt{d}) \text{ dan}$$

$$(s + t\sqrt{d})1 = (s + t\sqrt{d}).$$

Jadi, Q($\sqrt{d}$) mempunyai elemen satuan terhadap operasi perkalian.

v) Misalkan $\alpha \in$Q($\sqrt{d}$), $\alpha \neq 0$ dan $\alpha = s + t\sqrt{d}$, Perhatikan bahwa

$$\frac{1}{\alpha} = \frac{1}{s + t\sqrt{d}}$$

$$= \frac{1}{s + t\sqrt{d}} \quad \frac{s - t\sqrt{d}}{s - t\sqrt{d}}$$

$$= \frac{s}{s^2 - t^2 d} + \frac{-t}{s^2 - t^2 d}\sqrt{d} \in Q(\sqrt{d}).$$

Sehingga untuk setiap $\alpha \in Q(\sqrt{d}), \alpha \neq 0$, terdapat $\frac{1}{\alpha} \in Q(\sqrt{d})$

sedemikian sehingga $\alpha\left(\frac{1}{\alpha}\right) = 1$.

Jadi, untuk setiap elemen tak nol di $Q(\sqrt{d})$ mempunyai invers terhadap perkalian.

vi) Misalkan $\alpha, \beta, \gamma \in Q(\sqrt{d})$, $\alpha = s + t\sqrt{d}$, $\beta = u + v\sqrt{d}$ $\gamma = x + y\sqrt{d}$

maka:

$$\begin{aligned}
\alpha(\beta + \gamma) &= (s + t\sqrt{d})[(u + v\sqrt{d}) + (x + y\sqrt{d})] \\
&= (s + t\sqrt{d})[(u + x) + (v + y)\sqrt{d}] \\
&= (s + t\sqrt{d})(u + x) + (s + t\sqrt{d})((v + y)\sqrt{d}) \\
&= (u + x)(s + t\sqrt{d}) + (v + y)\sqrt{d}(s + t\sqrt{d}) \\
&= [u + x + (v + y)\sqrt{d}](s + t\sqrt{d}) \\
&= [(u + v\sqrt{d}) + (x + y\sqrt{d})](s + t\sqrt{d}) \\
&= (\alpha + \beta)\gamma.
\end{aligned}$$

Jadi, operasi perkalian pada $Q(\sqrt{d})$ bersifat distributif terhadap penjumlahan. ■

Dengan demikian telah ditunjukkan bahwa (Q($\sqrt{d}$),+,·) membentuk suatu medan. Selanjutnya medan Q($\sqrt{d}$) disebut **Medan Kuadratik**. Medan Q($\sqrt{d}$) yang terdiri dari bilangan-bilangan $s+t\sqrt{d}$ dengan $d>0$ disebut **medan kuadratik real** sedangkan jika Q($\sqrt{d}$) terdiri dari bilangan-bilangan $s+t\sqrt{d}$ dengan $d<0$ disebut **medan kuadratik imajiner**.

Teorema 3.1.2:

Misalkan $\alpha \in$ Q($\sqrt{d}$), maka α hanya dapat dinyatakan dengan satu cara sebagai $\alpha = a + b\sqrt{d}$. Dengan perkataan lain, jika $a + b\sqrt{d} = e + f\sqrt{d}$, $a,b,e,f \in$Q, maka $a = e$ atau $b = f$.

Bukti:

Misalkan $a + b\sqrt{d} = e + f\sqrt{d}$. Andaikan $b \neq f$ maka

$$\sqrt{d}(f-b) = a-e$$

$$d = \left(\frac{a-e}{f-b}\right)^2.$$

Perhatikan bahwa $\left(\frac{a-e}{f-b}\right) \in$ Z. Hal tersebut akan dijelaskan demikian.

Andaikan $\left(\frac{a-e}{f-b}\right) \notin$ Z yaitu $\left(\frac{a-e}{f-b}\right) \in$ Q-Z. Sehingga $\left(\frac{a-e}{f-b}\right)^2 \in$ Q-Z.

Karena $d = \left(\frac{a-e}{f-b}\right)^2$ maka timbul kontradiksi, karena $d \in \mathbb{Z}$. Jadi $\left(\frac{a-e}{f-b}\right) \in \mathbb{Z}$.

Selanjutnya, $d = 1 \cdot \left(\frac{a-e}{f-b}\right)^2$ habis dibagi oleh bilangan bulat kuadrat sempurna. Akibatnya d bukan bilangan bulat bebas kuadrat. Kontradiksi dengan kenyataan bahwa d bilangan bulat bebas kuadrat. Jadi haruslah $b = f$ dan mengakibatkan $a = e$. ■

Definisi 3.1.4:

Misalkan $\alpha \in Q(\sqrt{d})$ dengan $\alpha = s + t\sqrt{d}$. **Konjugat** $\overline{\alpha}$ dari α adalah bilangan $\overline{\alpha} = s - t\sqrt{d}$.

Teorema 3.1.3:

Misalkan $\alpha, \beta \in Q(\sqrt{d})$ dengan $\alpha = s + t\sqrt{d}$ dan $\beta = u + v\sqrt{d}$, maka berlaku:

i) $\overline{(\alpha + \beta)} = \overline{\alpha} + \overline{\beta}$,

ii) $\overline{(\alpha - \beta)} = \overline{\alpha} - \overline{\beta}$,

iii) $\overline{(\alpha\beta)} = \overline{\alpha}\,\overline{\beta}$,

iv) $\overline{\left(\frac{\alpha}{\beta}\right)} = \frac{\overline{\alpha}}{\overline{\beta}}$, $\beta \neq 0$,

v) $\alpha = \overline{\alpha}$ jika dan hanya jika $\alpha \in \mathbb{Q}$.

Bukti:

Karena $\alpha, \beta \in \mathbb{C}$ maka sifat(i) dan (ii) dipenuhi.

Bukti (iii):

$$(\overline{\alpha\beta}) = \overline{((s + t\sqrt{d})(u + v\sqrt{d}))}$$

$$= \overline{(su + tvd + (tu + vs)\sqrt{d})}$$

$$= su + tvd + (-tu - vs)\sqrt{d}$$

$$= (s - t\sqrt{d})(u - v\sqrt{d})$$

$$= \overline{\alpha}\,\overline{\beta}.$$

Untuk bukti iv):

Dibuktikan terlebih dahulu: $\overline{\left(\frac{1}{\beta}\right)} = \frac{1}{\overline{\beta}},\ \beta \neq 0.$

$$\overline{\left(\frac{1}{\beta}\right)} = \overline{\left(\frac{1}{u + v\sqrt{d}}\right)}$$

$$= \frac{1}{u - v\sqrt{d}}$$

$$= \frac{1}{\overline{\beta}}.$$

Sehingga, $\overline{\left(\frac{\alpha}{\beta}\right)} = \overline{\left(\alpha\frac{1}{\beta}\right)} = \overline{\alpha}\overline{\left(\frac{1}{\beta}\right)} = \overline{\alpha}\,\frac{1}{\overline{\beta}} = \frac{\overline{\alpha}}{\overline{\beta}}.$

Bukti (v):

$\alpha = \overline{\alpha}$ jika dan hanya jika $s + t\sqrt{d} = s - t\sqrt{d}$. Dengan menggunakan Teorema 3.1.2 diperoleh $t = -t$. Sehingga $t = 0$.

Jadi, $\alpha = \overline{\alpha}$ jika dan hanya jika $\alpha = s \in \mathbb{Q}$. ∎

Definisi 3.1.5:

Misalkan $\alpha \in \mathbb{Q}(\sqrt{d})$ dengan $\alpha = s + t\sqrt{d}$. **Teras** dari α, dinyatakan $Tr(\alpha)$, didefinisikan sebagai

$$Tr(\alpha) = \alpha + \overline{\alpha}.$$

Akibatnya $Tr(\alpha) = 2s$.

Definisi 3.1.6:

Misalkan $\alpha \in \mathbb{Q}(\sqrt{d})$ dengan $\alpha = s + t\sqrt{d}$. **Norma** dari α, dinyatakan $N(\alpha)$, didefinisikan sebagai

$$N(\alpha) = \alpha\overline{\alpha}.$$

Akibatnya $N(\alpha) = s^2 - t^2 d$.

Definisi 3.1.7:

Bilangan $\alpha \in \mathbb{Q}(\sqrt{d})$ disebut **akar** dari suku banyak $p(x)$ jika $p(\alpha) = 0$.

Teorema 3.1.4:

Misalkan $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$, maka berlaku

i) $Tr(\alpha+\beta) = Tr(\alpha) + Tr(\beta)$,

ii) $N(\alpha\beta) = N(\alpha)N(\beta)$,

iii) $Tr(\alpha), N(\alpha) \in \mathbb{Q}$,

iv) $N(\alpha) = 0$ jika dan hanya jika $\alpha = 0$,

v) α adalah akar dari suku banyak $p(x) = x^2 - Tr(\alpha)x + N(\alpha)$.

Bukti:

i)
$$\begin{aligned} Tr(\alpha+\beta) &= (\alpha+\beta) + \overline{(\alpha+\beta)} \\ &= (\alpha+\beta) + (\overline{\alpha} + \overline{\beta}) \\ &= (\alpha+\overline{\alpha}) + (\beta+\overline{\beta}) \\ &= Tr(\alpha) + Tr(\beta). \end{aligned}$$

ii)
$$\begin{aligned} N(\alpha\beta) &= (\alpha\beta)\overline{(\alpha\beta)} \\ &= (\alpha\beta)(\overline{\alpha}\overline{\beta}) \\ &= (\alpha\overline{\alpha})(\beta\overline{\beta}) \\ &= N(\alpha)N(\beta). \end{aligned}$$

iii)
$$\begin{aligned} Tr(\alpha) = \alpha + \overline{\alpha} &= (s + t\sqrt{d}) + (s - t\sqrt{d}) \\ &= 2s \in \mathbb{Q}. \end{aligned}$$

$$\begin{aligned} N(\alpha) = \alpha\overline{\alpha} &= (s + t\sqrt{d})(s - t\sqrt{d}) \\ &= s^2 - t^2 d \in \mathbb{Q}. \end{aligned}$$

iv) $(\Rightarrow)$

$N(\alpha) = 0$ maka $s^2 - t^2 d = 0$.

Andaikan $t \neq 0$ maka $d = \left(\frac{s}{t}\right)^2$.

Kontradiksi dengan fakta bahwa d adalah bilangan bulat bebas kuadrat. Sehingga $t = 0$ dan $s^2 = 0$, maka $s = 0$.

Jadi, $\alpha = 0$.

$(\Leftarrow)$

$\alpha = 0$ maka $N(\alpha) = 0 \cdot 0 = 0$.

v) Perhatikan bahwa $p(\alpha) = \alpha^2 - (\alpha + \bar{\alpha})\alpha + \alpha\bar{\alpha} = 0$.

Sehingga α merupakan akar dari suku banyak $p(x)$. ■

Teorema 3.1.5:

Himpunan $\mathbb{Q}(\sqrt{d})$ membentuk ruang vektor atas medan $\mathbb{Q}$.

Bukti:

i) Himpunan $\mathbb{Q}(\sqrt{d})$ terhadap operasi penjumlahan merupakan grup komutatif karena menurut Teorema 3.1.1, $\mathbb{Q}(\sqrt{d})$ merupakan medan.

ii) Misalkan $a \in \mathbb{Q}$ dan $\alpha \in \mathbb{Q}(\sqrt{d})$ dengan $\alpha = s + t\sqrt{d}$ maka

$$\begin{aligned} a\alpha &= a(s + t\sqrt{d}) \\ &= as + at\sqrt{d} \in \mathbb{Q}(\sqrt{d}). \end{aligned}$$

Jadi , $\mathbb{Q}(\sqrt{d})$ tertutup terhadap perkalian dengan skalar.

iii) Misalkan $a,b \in \mathbb{Q}$ dan $\alpha \in \mathbb{Q}(\sqrt{d})$ dengan $\alpha = s + t\sqrt{d}$ maka

$$\begin{aligned} a(b\alpha) &= a(b(s + t\sqrt{d})) \\ &= a(bs + bt\sqrt{d}) \\ &= abs + abt\sqrt{d} \\ &= ab(s + t\sqrt{d}) \\ &= (ab)\alpha. \end{aligned}$$

Jadi, $\mathbb{Q}(\sqrt{d})$ bersifat assosiatif terhadap perkalian dengan skalar.

iv) Misalkan $a,b \in \mathbb{Q}$ dan $\alpha \in \mathbb{Q}(\sqrt{d})$ dengan $\alpha = s + t\sqrt{d}$ maka

$$\begin{aligned} (a+b)\alpha &= (a+b)(s + t\sqrt{d}) \\ &= as + bs + at\sqrt{d} + bt\sqrt{d} \\ &= a(s + t\sqrt{d}) + b(s + t\sqrt{d}) \\ &= a\alpha + b\alpha. \end{aligned}$$

Jadi terhadap perkalian antara 2 skalar dengan setiap elemen di $\mathbb{Q}(\sqrt{d})$ bersifat distributif.

v) Misalkan $a \in \mathbb{Q}$ dan $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$ dengan $\alpha = s + t\sqrt{d}$, $\beta = u + v\sqrt{d}$

maka

$$\begin{aligned} a(\alpha + \beta) &= a[(s + t\sqrt{d}) + (u + v\sqrt{d})] \\ &= a(s + t\sqrt{d} + u + v\sqrt{d}) \end{aligned}$$

$$= as + at\sqrt{d} + au + av\sqrt{d})$$

$$= (as + at\sqrt{d}) + (au + av\sqrt{d})$$

$$= a(s + t\sqrt{d}) + a(u + v\sqrt{d})$$

$$= a\alpha + a\beta.$$

Jadi perkalian antara skalar dengan setiap 2 elemen di $Q(\sqrt{d})$ bersifat distributif.

vi) Perhatikan bahwa $1 \in Q$ dan untuk setiap $\alpha \in Q(\sqrt{d})$ dengan $\alpha = s + t\sqrt{d}$ berlaku

$$1\alpha = 1(s + t\sqrt{d})$$

$$= (s + t\sqrt{d})$$

$$= \alpha.$$

Jadi, untuk setiap $\alpha \in Q(\sqrt{d})$ berlaku $1\alpha = \alpha$.

Jadi, $Q(\sqrt{d})$ membentuk ruang vektor atas medan Q. ■

Contoh 3.1.1:

Himpunan $\{1, \sqrt{d}\}$ merupakan basis dari $Q(\sqrt{d})$, karena

i) Himpunan $\{1, \sqrt{d}\}$ bebas linear.

Misalkan $s_1, s_2 \in Q$ maka $\{1, \sqrt{d}\}$ bebas linear jika $s_1 + s_2\sqrt{d} = 0$ maka $s_1 = 0$ dan $s_2 = 0$.

Dengan menggunakan Teorema 3.1.2 diperoleh bahwa jika $s_1 + s_2\sqrt{d} = 0$ maka $s_1 = 0$ dan $s_2 = 0$.

ii) Himpunan $\{1, \sqrt{d}\}$ merentang $Q(\sqrt{d})$.

Misalkan $\alpha \in Q(\sqrt{d})$ dengan $\alpha = s + t\sqrt{d}$.

Perhatikan bahwa α merupakan kombinasi linear dari $1, \sqrt{d}$. Sehingga $\{1, \sqrt{d}\}$ merentang $Q(\sqrt{d})$.

Karena $\{1, \sqrt{d}\}$ bebas linear dan merentang $Q(\sqrt{d})$ maka terbukti bahwa $\{1, \sqrt{d}\}$ merupakan basis dari $Q(\sqrt{d})$.

Contoh 3.1.2:

Himpunan $\{1, \frac{1+\sqrt{d}}{2}\}$ juga merupakan basis dari $Q(\sqrt{d})$, karena

i) Himpunan $\{1, \frac{1+\sqrt{d}}{2}\}$ bebas linear.

Misalkan $s_1, s_2 \in Q$ maka $\{1, \frac{1+\sqrt{d}}{2}\}$ bebas linear jika

$$s_1 + s_2\frac{1+\sqrt{d}}{2} = 0 \text{ maka } s_1 = 0 \text{ dan } s_2 = 0.$$

Jika $s_1 + s_2\frac{1+\sqrt{d}}{2} = 0$ maka $(2s_1 + s_2) + s_2\sqrt{d} = 0$.

Dengan menggunakan Teorema 3.1.2 maka diperoleh $s_1 = 0$ dan $s_2 = 0$.

ii) Himpunan $\{1, \frac{1+\sqrt{d}}{2}\}$ merentang $\mathbb{Q}(\sqrt{d})$.

Misalkan $\alpha \in \mathbb{Q}(\sqrt{d})$ dengan $\alpha = s + t\sqrt{d}$, $s, t \in \mathbb{Q}$, d bilangan bulat bebas kuadrat.

Suatu elemen $\alpha \in \mathbb{Q}(\sqrt{d})$ merentang $\mathbb{Q}(\sqrt{d})$ jika α merupakan kombinasi linear dari $1, \frac{1+\sqrt{d}}{2}$ yaitu jika terdapat $s_1, s_2 \in \mathbb{Q}$ sedemikian sehingga

$$\alpha = s_1 + s_2 \frac{1+\sqrt{d}}{2}.$$

Perhatikan bahwa, $\alpha = s_1 + s_2 \frac{1+\sqrt{d}}{2}$ mengakibatkan

$$s_1 + s_2 \frac{1+\sqrt{d}}{2} = s + t\sqrt{d}.$$

Atau,

$$(2s_1 + s_2) + s_2\sqrt{d} = s + t\sqrt{d}.$$

Dengan menggunakan Teorema 3.1.2 diperoleh,

$$s_1 = \frac{s-t}{2} \text{ dan } s_2 = t \text{ keduanya di } \mathbb{Q}.$$

Jadi, himpunan $\{1, \frac{1+\sqrt{d}}{2}\}$ merentang $\mathbb{Q}(\sqrt{d})$.

B. Bilangan Bulat dari Medan Kuadratik

Pada sub-bab di atas telah didefinisikan mengenai medan kuadratik dan sifat-sifatnya. Selanjutnya, pada sub-bab ini akan dibicarakan mengenai bilangan bulat dari medan kuadratik dan juga sifat-sifatnya. Untuk itu, terlebih dahulu akan didefinisikan bilangan bulat dari medan kuadratik $\mathbb{Q}(\sqrt{d})$.

Definisi 3.2.1:

Bilangan $\alpha \in \mathbb{Q}(\sqrt{d})$ disebut **bilangan bulat dari** $\mathbb{Q}(\sqrt{d})$ jika $Tr(\alpha)$ dan $N(\alpha)$ di $\mathbb{Z}$. Himpunan semua bilangan bulat dari $\mathbb{Q}(\sqrt{d})$ dinyatakan dengan I_d.

Perhatikan bahwa bila $a,b \in \mathbb{Z}$ dan d adalah bilangan bulat bebas kuadrat maka bilangan $a+b\sqrt{d}$ di I_d karena:

$$Tr(a+b\sqrt{d}) = (a+b\sqrt{d})+(a-b\sqrt{d}) = 2a \in \mathbb{Z} \text{ dan}$$

$$N(a+b\sqrt{d}) = (a+b\sqrt{d})(a-b\sqrt{d}) = a^2 - db^2 \in \mathbb{Z}.$$

Namun ternyata masih terdapat bilangan lain di $\mathbb{Q}(\sqrt{d})$ yang juga memenuhi syarat sebagai anggota I_d, seperti yang akan diberikan dalam contoh berikut:

Contoh 3.2.1:

Bilangan $\frac{1+\sqrt{5}}{2}$ di I_d, sebab:

$$Tr\left(\frac{1+\sqrt{5}}{2}\right)=\frac{1+\sqrt{5}}{2}+\frac{1-\sqrt{5}}{2}=1\in\mathbb{Z} \text{ dan}$$

$$N\left(\frac{1+\sqrt{5}}{2}\right)=\frac{1-5}{4}=-1\in\mathbb{Z}.$$

Teorema 3.2.1:

Diberikan $x_1, y_1 \in \mathbb{Z}$, d bilangan bulat bebas kuadrat dan $x_1^2 - dy_1^2 \equiv 0(\text{mod } 4)$. Maka sifat-sifat berikut dipenuhi:

i) Jika $d \equiv 2(\text{mod } 4)$ atau $d \equiv 3(\text{mod } 4)$ maka x_1, y_1 keduanya genap.

ii) Jika $d \equiv 1(\text{mod } 4)$ maka x_1, y_1 keduanya genap atau x_1, y_1 keduanya ganjil.

(Catatan: karena d bilangan bulat bebas kuadrat maka $d \not\equiv 0(\text{mod } 4)$).

Bukti:

Dibuktikan dengan kontradiksi. Andaikan x_1 ganjil atau y_1 ganjil.

i) Untuk x_1 ganjil dan $d \equiv 2(\text{mod } 4)$ maka $x_1^2 - dy_1^2 \equiv 1 - dy_1^2(\text{mod } 4)$. Sehingga jika y_1 ganjil maka $1 - dy_1^2 \equiv 1 - 2y_1^2 \equiv -1(\text{mod } 4)$. Jika y_1 genap maka $1 - dy_1^2 \equiv 1 - 2y_1^2 \equiv 1(\text{mod } 4)$.

Diperoleh $x_1^2 - dy_1^2 \equiv -1(\text{mod}\,4)$ jika y_1 ganjil dan $x_1^2 - dy_1^2 \equiv 1(\text{mod}\,4)$ jika y_1 genap. Kontradiksi dengan $x_1^2 - dy_1^2 \equiv 0(\text{mod}\,4)$. Jadi x_1, y_1 keduanya genap.

Untuk x_1 ganjil dan $d \equiv 3(\text{mod}\,4)$ maka $x_1^2 - dy_1^2 \equiv 1 - 3y_1^2(\text{mod}\,4)$. Sehingga jika y_1 ganjil maka $1 - 3y_1^2 \equiv -2(\text{mod}\,4)$ dan jika y_1 genap maka $1 - 3y_1^2 \equiv 1(\text{mod}\,4)$. Diperoleh $x_1^2 - dy_1^2 \equiv -2(\text{mod}\,4)$ jika y_1 ganjil dan $x_1^2 - dy_1^2 \equiv 1(\text{mod}\,4)$ jika y_1 genap. Kontradiksi dengan $x_1^2 - dy_1^2 \equiv 0(\text{mod}\,4)$. Jadi x_1, y_1 keduanya genap.

Untuk y_1 ganjil dan $d \equiv 2(\text{mod}\,4)$ maka $x_1^2 - dy_1^2 \equiv x_1^2 - 2(\text{mod}\,4)$. Jika x_1 ganjil maka $x_1^2 - 2(\text{mod}\,4) \equiv -1(\text{mod}\,4)$. Jika x_1 genap maka $x_1^2 - 2(\text{mod}\,4) \equiv -2(\text{mod}\,4)$. Diperoleh $x_1^2 - dy_1^2 \equiv -1(\text{mod}\,4)$ jika x_1 ganjil dan $x_1^2 - dy_1^2 \equiv -2(\text{mod}\,4)$ jika x_1 genap. Kontradiksi dengan $x_1^2 - dy_1^2 \equiv 0(\text{mod}\,4)$. Jadi x_1, y_1 keduanya genap.

Untuk y_1 ganjil dan $d \equiv 3(\text{mod}\,4)$ maka $x_1^2 - dy_1^2 \equiv x_1^2 - 3(\text{mod}\,4)$. Jika x_1 ganjil maka $x_1^2 - 2(\text{mod}\,4) \equiv -2(\text{mod}\,4)$. Jika x_1 genap maka $x_1^2 - 2(\text{mod}\,4) \equiv -3(\text{mod}\,4)$. Diperoleh $x_1^2 - dy_1^2 \equiv -2(\text{mod}\,4)$ jika x_1 ganjil dan $x_1^2 - dy_1^2 \equiv -2(\text{mod}\,4)$ jika x_1 genap. Kontradiksi dengan $x_1^2 - dy_1^2 \equiv 0(\text{mod}\,4)$. Jadi x_1, y_1 keduanya genap.

ii) Jika $d \equiv 1 (\mathrm{mod}\, 4)$ maka $x_1^2 - y_1^2 \equiv 0 (\mathrm{mod}\, 4)$. Sehingga $x_1^2 \equiv y_1^2 (\mathrm{mod}\, 4)$. Jadi x_1, y_1 keduanya harus genap atau x_1, y_1 keduanya harus ganjil. ∎

Untuk mengetahui bilamana bilangan di $\mathbb{Q}(\sqrt{d})$ merupakan suatu bilangan bulat dari $\mathbb{Q}(\sqrt{d})$, akan dibuktikan dalam teorema berikut.

Teorema 3.2.2:

Himpunan bilangan bulat dari $\mathbb{Q}(\sqrt{d})$ berbentuk $a + b\omega_d$ dengan $a, b \in \mathbb{Z}$ dan

$$\omega_d = \begin{cases} \sqrt{d} & \text{jika } d \equiv 2 \text{ (mod 4) atau } d \equiv 3 \text{ (mod 4)} \\ \dfrac{1+\sqrt{d}}{2} & \text{jika } d \equiv 1 \text{ (mod 4).} \end{cases}$$

Bukti:

Misalkan $\alpha = x + y\sqrt{d}$ suatu bilangan di $\mathbb{Q}(\sqrt{d})$. Menurut Definisi 3.2.1 bilangan $\alpha \in \mathbb{Q}(\sqrt{d})$ merupakan bilangan bulat dari $\mathbb{Q}(\sqrt{d})$ jika dan hanya jika

$$Tr(\alpha) = 2x \in \mathbb{Z} \text{ dan } N(\alpha) = x^2 - dy^2 \in \mathbb{Z}.$$

Misalkan, $2x = x_1$ dan $2y = y_1$ sehingga

$$Tr(\alpha) = x_1 \in \mathbb{Z} \text{ dan } N(\alpha) = \frac{x_1^2 - dy_1^2}{4} \in \mathbb{Z}.$$

Karena $\frac{x_1^2 - dy_1^2}{4} \in \mathbb{Z}$ maka $x_1^2 - dy_1^2 \equiv 0 \pmod 4$. Andaikan $y_1 \notin \mathbb{Z}$, maka $dy_1^2 \notin \mathbb{Z}$, karena d bilangan bulat bebas kuadrat. Sehingga mengakibatkan $x_1^2 - dy_1^2 \notin \mathbb{Z}$. Kontradiksi dengan kenyataan bahwa $x_1^2 - dy_1^2 \in \mathbb{Z}$. Jadi, haruslah $y_1 \in \mathbb{Z}$.

Telah ditunjukkan bahwa untuk $d \equiv 2 \pmod 4$ atau $d \equiv 3 \pmod 4$, jika $x_1^2 - dy_1^2 \equiv 0 \pmod 4$ maka x_1, y_1 keduanya genap. Akibatnya,

$$\alpha = x + y\sqrt{d} = \frac{x_1}{2} + \frac{y_1}{2}\sqrt{d},$$

dengan keduanya $x = \frac{x_1}{2} = a$ dan $y = \frac{y_1}{2} = b$ di $\mathbb{Z}$. Dengan demikian bilangan bulat dari $\mathbb{Q}(\sqrt{d})$, untuk $d \equiv 2 \pmod 4$ atau $d \equiv 3 \pmod 4$, adalah $\alpha = a + b\sqrt{d}$ dengan a, b di $\mathbb{Z}$.

Selanjutnya, menurut Teorema 3.2.1 jika $x_1^2 - dy_1^2 \equiv 0 \pmod 4$ maka x_1, y_1 keduanya genap atau x_1, y_1 keduanya ganjil. Akibatnya, $\frac{x_1 - y_1}{2} \in \mathbb{Z}$ sehingga

$$\alpha = x + y\sqrt{d} = \frac{x_1 - y_1}{2} + y_1\left(\frac{1+\sqrt{d}}{2}\right)$$

$$= a + b\left(\frac{1+\sqrt{d}}{2}\right)$$

dengan $a = \frac{x_1 - y_1}{2}$ dan $b = y_1$ keduanya di $\mathbb{Z}$. Dengan demikian, untuk $d \equiv 1 (\bmod 4)$ bilangan bulat dari $\mathbb{Q}(\sqrt{d})$ adalah

$$\alpha = a + b\frac{1+\sqrt{d}}{2},$$

dengan a dan b suatu bilangan di $\mathbb{Z}$. ■

Jadi, telah ditunjukkan bahwa jika $d \equiv 2 (\bmod 4)$ atau $d \equiv 3 (\bmod 4)$ maka himpunan I_d terdiri dari bilangan-bilangan berbentuk $a + b\sqrt{d}$ dan jika $d \equiv 1 (\bmod 4)$ maka himpunan I_d terdiri dari bilangan-bilangan berbentuk $a + b\frac{1+\sqrt{d}}{2}$, dengan $a, b \in \mathbb{Z}$, dan d bilangan bulat bebas kuadrat.

Contoh 3.2.2:

i) $I_{-1} = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Z}\} = \mathbb{Z}[i]$, karena $-1 \equiv 3 (\bmod 4)$.

ii) $I_5 = \{a + b\frac{1+\sqrt{5}}{2} \mid a, b \in \mathbb{Z}\}$, karena $5 \equiv 1 (\bmod 4)$.

iii) $I_{-3} = \{a + b\frac{1+\sqrt{-3}}{2} \mid a, b \in \mathbb{Z}\}$, karena $-3 \equiv 1 (\bmod 4)$.

Perhatikan bahwa karena $\mathbb{Q}(\sqrt{d})$ merupakan medan, maka dengan menggunakan Teorema 2.1.2 $\mathbb{Q}(\sqrt{d})$ juga merupakan suatu daerah integral.

Teorema 3.2.3:

Himpunan I_d membentuk subdaerah-integral dalam daerah integral $\mathbb{Q}(\sqrt{d})$.

Bukti:

Terlebih dahulu dibuktikan bahwa himpunan I_d membentuk subgelanggang terhadap gelanggang $\mathbb{Q}(\sqrt{d})$.

i) Jika $d \equiv 2 \pmod 4$ atau $d \equiv 3 \pmod 4$ maka himpunan I_d terdiri dari bilangan-bilangan $x + y\sqrt{d}$, $x, y \in \mathbb{Z}$, d bilangan bulat bebas kuadrat.

Ambil $x + y\sqrt{d}$ dan $z + w\sqrt{d}$ di I_d. Sehingga:

$$(x + y\sqrt{d})(z + w\sqrt{d}) = (xz + ywd) + (yz + xw)\sqrt{d} \in I_d.$$

Selanjutnya,

$$(x + y\sqrt{d}) - (z + w\sqrt{d}) = (x - z) + (y - w)\sqrt{d} \in I_d.$$

Jadi, untuk $d \equiv 2 \pmod 4$ atau $d \equiv 3 \pmod 4$ himpunan I_d membentuk subgelanggang terhadap gelanggang $\mathbb{Q}(\sqrt{d})$.

ii) Jika $d \equiv 1 \pmod 4$ maka I_d terdiri dari bilangan-bilangan $x + y\left(\frac{1+\sqrt{d}}{2}\right)$, dengan $x, y \in \mathbb{Z}$, dan d bilangan bulat bebas kuadrat.

Ambil $x + y\left(\frac{1+\sqrt{d}}{2}\right)$ dan $z + w\left(\frac{1+\sqrt{d}}{2}\right) \in I_d$, maka:

$$\left(x+y\left(\frac{1+\sqrt{d}}{2}\right)\right)\left(z+w\left(\frac{1+\sqrt{d}}{2}\right)\right)$$

$$= xz+yw\left(\frac{1+\sqrt{d}}{2}\right)^2+(xw+yz)\left(\frac{1+\sqrt{d}}{2}\right)$$

$$= xz+yw\left(\frac{d-1}{4}\right)+(xw+yz+yw)\left(\frac{1+\sqrt{d}}{2}\right)\in I_d, \text{ dan}$$

$$\left(x+y\left(\frac{1+\sqrt{d}}{2}\right)\right)-\left(z+w\left(\frac{1+\sqrt{d}}{2}\right)\right)$$

$$= (x-z)+(y-w)\left(\frac{1+\sqrt{d}}{2}\right)\in I_d.$$

Jadi, untuk $d \equiv 1(\bmod 4)$ himpunan I_d membentuk subgelanggang terhadap gelanggang Q($\sqrt{d}$).

Dengan demikian himpunan I_d dengan $d \equiv 1(\bmod 4)$, $d \equiv 2(\bmod 4)$ atau $d \equiv 3(\bmod 4)$ membentuk subgelanggang terhadap gelanggang Q($\sqrt{d}$).

Selanjutnya ditunjukkan bahwa himpunan I_d membentuk subdaerah-integral terhadap daerah integral Q($\sqrt{d}$), yaitu tinggal dibuktikan bahwa subgelanggang I_d bersifat komutatif dan tidak memuat pembagi nol.

Karena $\alpha, \beta \in I_d$ maka $\alpha, \beta \in$ Q($\sqrt{d}$) dan $\alpha\beta = \beta\alpha$. Sehingga subgelanggang I_d bersifat komutatif. Selanjutnya, karena $\alpha, \beta \in I_d$ dan

$\alpha \neq 0, \beta \neq 0$ maka $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$ dan $\alpha \neq 0, \beta \neq 0$, karena $\mathbb{Q}(\sqrt{d})$ suatu daerah integral.

Dengan demikian subgelanggang I_d bersifat komutatif dan tidak memuat pembagi nol, sehingga himpunan I_d membentuk subdaerah-integral terhadap daerah integral $\mathbb{Q}(\sqrt{d})$. ■

Perhatikan bahwa himpunan I_d tidak membentuk submedan karena meskipun subgelanggang I_d komutatif tetapi terdapat elemen tak nol di I_d yang tidak memiliki invers terhadap perkalian di I_d. Misalnya $1+2\sqrt{3} \neq 0$ di I_d maka invers terhadap perkaliannya

$$\frac{1}{1+2\sqrt{3}} = -\frac{1}{11} + \frac{2}{11}\sqrt{3} \notin I_d.$$

Teorema 3.2.4:

Jika $\alpha \in \mathbb{Q}$ dan $\alpha \in I_d$ maka $\alpha \in \mathbb{Z}$.

Bukti:

Misal $\alpha = x$, $x \in \mathbb{Q}$. Karena $\alpha \in I_d$, maka

$$Tr(\alpha) = 2x \in \mathbb{Z} \text{ dan } N(\alpha) = x^2 \in \mathbb{Z}.$$

Misal $2x = x_1$, maka

$$Tr(\alpha) = 2\left(\frac{x_1}{2}\right) = x_1 \text{ dan } N(\alpha) = \frac{x_1^2}{4}.$$

Karena $Tr(\alpha)$ dan $N(\alpha)$ di $\mathbb{Z}$, maka x_1 di $\mathbb{Z}$ dan $\frac{x_1^2}{4}$ di $\mathbb{Z}$.

Sehingga, karena $\frac{x_1^2}{4} \in \mathbb{Z}$ maka $x_1^2 \equiv 0 (\mathrm{mod}\, 4)$ atau x_1 genap.

Sehingga, $\alpha = \frac{x_1}{2} \in \mathbb{Z}$. ■

Perhatikan bahwa untuk setiap bilangan rasional *r*, akan terdapat bilangan bulat *n* sedemikian sehingga *nr* bilangan bulat. Sifat yang sama juga dimiliki oleh I_d.

Teorema 3.2.5:

Misalkan $\alpha \in \mathbb{Q}(\sqrt{d})$, maka terdapat bilangan bulat *n* sedemikian sehingga $n\alpha \in I_d$.

Bukti:

Misalkan $\alpha \in \mathbb{Q}(\sqrt{d})$ dengan $\alpha = s + t\sqrt{d}$ maka terdapat bilangan bulat *n*, yaitu kelipatan persekutuan dari penyebutnya *s* dan *t*, sehingga $n\alpha = ns + nt\sqrt{d}$ di I_d, karena $ns, nt \in \mathbb{Z}$. ■

Contoh 3.2.3:

Misal $\alpha \in \mathbb{Q}(\sqrt{d})$ dengan $\alpha = \frac{1}{2} + \frac{2}{3}\sqrt{d}$ maka terdapat bilangan bulat n, yaitu $n = 6$ yang merupakan kelipatan persekutuan dari 2 dan 3, sehingga $n\alpha = 3 + 4\sqrt{5} \in I_d$.

Untuk selanjutnya istilah bilangan bulat diganti menjadi bilangan rasional bulat.

BAB IV

MODUL DARI MEDAN KUADRATIK

Dalam bab ini akan dibahas modul dari medan kuadratik dan sifatnya, serta algoritma untuk menentukan semua penyelesaian dari persamaan Diophantine $ax^2 + bxy + cy^2 = m$, dengan a, b, c, m bilangan rasional bulat yang diketahui, dan x, y bilangan rasional bulat yang akan dicari. Pada bab ini dan seterusnya istilah bilangan bulat diganti menjadi bilangan rasional bulat.

A. Modul dari Medan Kuadratik

Definisi 4.1.1:

Misalkan $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$ dan $\{\alpha, \beta\}$ basis dari $\mathbb{Q}(\sqrt{d})$. Misalkan pula

$$M = \{\alpha x + \beta y \mid x, y \text{ bilangan rasional bulat}\},$$

maka M disebut **modul dari** $\mathbb{Q}(\sqrt{d})$ atau **modul dari medan kuadratik**.

Contoh 4.1.1:

Himpunan I_d merupakan modul dari $\mathbb{Q}(\sqrt{d})$. Jika $d \equiv 2 \pmod 4$ atau $d \equiv 3 \pmod 4$ maka $I_d = \{1 \cdot x + \omega_d \cdot y \mid x, y \text{ bilangan rasional bulat}\}$, $\omega_d = \sqrt{d}$. Jika $d \equiv 1 \pmod 4$ maka $I_d = \{1 \cdot x + \omega_d \cdot y \mid x, y \text{ bilangan rasional bulat}\}$, dengan

$$\omega_d = \frac{1+\sqrt{d}}{2}.$$

Menurut Contoh 3.1.1 himpunan $\{1,\sqrt{d}\}$ merupakan basis dari Q($\sqrt{d}$) dan menurut Contoh 3.1.2 himpunan $\{1,\frac{1+\sqrt{d}}{2}\}$ juga merupakan basis dari Q($\sqrt{d}$) sehingga $\{1,\omega_d\}$ merupakan basis dari Q($\sqrt{d}$).

Teorema 4.1.1:

Jika $M = \{\alpha x + \beta y \mid x, y$ bilangan rasional bulat$\}$ modul dari Q($\sqrt{d}$), maka M membentuk grup komutatif terhadap operasi penjumlahan.

Bukti:

i) Ambil $\vartheta,\gamma \in M$, misalkan $\vartheta = \alpha x_1 + \beta y_1$ dan $\gamma = \alpha x_2 + \beta y_2$ untuk suatu bilangan rasional bulat x_1, x_2, y_1, y_2. Sehingga,

$$\vartheta + \gamma = \alpha(x_1 + x_2) + \beta(y_1 + y_2) \in M.$$

Jadi, M tertutup terhadap operasi penjumlahan.

ii) Ambil $\vartheta,\gamma \in M$, misalkan $\vartheta = \alpha x_1 + \beta y_1$ dan $\gamma = \alpha x_2 + \beta y_2$ untuk suatu bilangan rasional bulat x_1, x_2, y_1, y_2. Sehingga,

$$\begin{aligned}\vartheta + \gamma &= (\alpha x_1 + \beta y_1) + (\alpha x_2 + \beta y_2)\\ &= (\alpha x_1 + \beta y_1 + \alpha x_2 + \beta y_2)\\ &= (\alpha x_2 + \beta y_2) + (\alpha x_1 + \beta y_1)\\ &= \gamma + \vartheta.\end{aligned}$$

Jadi, M bersifat komutatif terhadap operasi penjumlahan.

iii) Ambil $\vartheta, \gamma, \lambda \in M$, misalkan $\vartheta = \alpha x_1 + \beta y_1$, $\gamma = \alpha x_2 + \beta y_2$ dan $\lambda = \alpha x_3 + \beta y_3$ untuk suatu bilangan rasional bulat $x_1, x_2, y_1, y_2, x_3, y_3$.

Sehingga,

$$\begin{aligned}
\vartheta + (\gamma + \lambda) &= (\alpha x_1 + \beta y_1) + ((\alpha x_2 + \beta y_2) + (\alpha x_3 + \beta y_3)) \\
&= (\alpha x_1 + \beta y_1) + (\alpha x_2 + \beta y_2 + \alpha x_3 + \beta y_3) \\
&= (\alpha x_1 + \beta y_1 + \alpha x_2 + \beta y_2) + (\alpha x_3 + \beta y_3) \\
&= ((\alpha x_1 + \beta y_1) + (\alpha x_2 + \beta y_2)) + (\alpha x_3 + \beta y_3) \\
&= (\vartheta + \gamma) + \lambda.
\end{aligned}$$

Jadi, M bersifat assosiatif terhadap operasi penjumlahan.

iv) Perhatikan bahwa $0 \in M$ karena $0 = \alpha 0 + \beta 0$, 0 bilangan rasional bulat. Sehingga untuk setiap $\vartheta \in M$, misal $\vartheta = \alpha x_1 + \beta y_1$, untuk suatu bilangan rasional bulat x_1, y_1 berlaku

$$0 + \vartheta = 0 + (\alpha x_1 + \beta y_1) = \alpha x_1 + \beta y_1 = \vartheta \text{ dan}$$

$$\vartheta + 0 = (\alpha x_1 + \beta y_1) + 0 = \alpha x_1 + \beta y_1 = \vartheta.$$

Jadi terdapat $0 \in M$ sedemikian sehingga untuk setiap $\vartheta \in M$ berlaku $0 + \vartheta = \vartheta + 0 = \vartheta$.

v) Ambil $\vartheta \in M$, misal $\vartheta = \alpha x_1 + \beta y_1$, untuk suatu bilangan rasional bulat x_1, y_1, maka terdapat $-\vartheta \in M$ yaitu $-(\alpha x_1 + \beta y_1) = -\alpha x_1 - \beta y_1$ sedemikian sehingga

$$\vartheta + (-\vartheta) = (\alpha x_1 + \beta y_1) + (-\alpha x_1 - \beta y_1) = 0.$$

Jadi untuk setiap elemen di M memiliki invers terhadap operasi penjumlahan.

Jadi, M membentuk grup komutatif terhadap operasi penjumlahan.

Perhatikan bahwa $M_1 = \{x + y\sqrt{2} \mid x, y \text{ bilangan rasional bulat}\}$ adalah sama dengan modul $M_2 = \{x + (\sqrt{2}+1)y \mid x, y \text{ bilangan rasional bulat}\}$ karena, misalkan $\gamma = x + y\sqrt{2}$ yang berada di M_1, maka γ juga dapat dinyatakan dengan $\gamma = (x-y) + (\sqrt{2}+1)y$, yang juga berada di M_2. Sebaliknya, misalkan $\lambda = x + (\sqrt{2}+1)y$ berada di M_2, maka $\lambda = (x+y) + y\sqrt{2}$ juga ada di M_1, Sehingga, $M_1 = M_2$.

Misalkan modul $M_1 = \{\alpha x + \beta y \mid x, y \text{ bilangan rasional bulat}\}$ dan modul $M_2 = \{\alpha_1 x + \beta_1 y \mid x, y \text{ bilangan rasional bulat}\}$. Selanjutnya akan diperiksa, kapan $M_1 = M_2$? Teorema berikut akan menjelaskannya.

Teorema 4.1.2:

Misalkan $\{\alpha, \beta\}$ dan $\{\alpha_1, \beta_1\}$ basis dari $\mathbb{Q}(\sqrt{d})$. Misalkan pula modul

$$M_1 = \{\alpha x + \beta y \mid x, y \text{ bilangan rasional bulat}\}$$

$$M_2 = \{\alpha_1 x + \beta_1 y \mid x, y \text{ bilangan rasional bulat}\}.$$

Modul $M_1 = M_2$ jika dan hanya jika terdapat bilangan rasional bulat x_1, y_1, z_1, w_1 sedemikan sehingga

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} x_1 & y_1 \\ z_1 & w_1 \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix}$$

dan

$$\begin{vmatrix} x_1 & y_1 \\ z_1 & w_1 \end{vmatrix} = \pm 1.$$

Bukti:

($\Rightarrow$)

Misalkan $\{\alpha, \beta\}$ dan $\{\alpha_1, \beta_1\}$ basis dari $\mathbb{Q}(\sqrt{d})$. Perhatikan bahwa α dan β di M_1. Karena $M_1 = M_2$, maka α dan $\beta \in M_2$. Sehingga,

$$\alpha = \alpha_1 x_1 + \beta_1 y_1 \qquad (1)$$

$$\beta = \alpha_1 z_1 + \beta_1 w_1 \qquad (2)$$

untuk suatu bilangan rasional bulat x_1, y_1, z_1dan w_1.

Selanjutnya, karena α_1 dan β_1 di M_2, padahal $M_1 = M_2$ maka α_1 dan β_1 di M_1. Akibatnya,

$$\alpha_1 = \alpha x + \beta y \quad (3)$$

$$\beta_1 = \alpha z + \beta w \quad (4)$$

untuk suatu bilangan rasional bulat x, y, z dan w. Dengan mensubstitusikan persamaan (3) dan (4) ke dalam persamaan (1) dan (2), diperoleh

$$\alpha = (\alpha x + \beta y)x_1 + (\alpha z + \beta w)y_1$$

$$\beta = (\alpha x + \beta y)z_1 + (\alpha z + \beta w)w_1$$

atau

$$\alpha = (xx_1 + y_1 z)\alpha + (x_1 y + y_1 w)\beta \qquad (5)$$

$$\beta = (xz_1 + w_1 z)\alpha + (yz_1 + w_1 w)\beta. \qquad (6)$$

Karena $\{\alpha, \beta\}$ basis dari $\mathbb{Q}(\sqrt{d})$ (hal ini yang membuat koefisien-koefisien dari α dan β dapat dibandingkan) persamaan (5) dan (6) dapat ditulis

$$\begin{pmatrix} xx_1 + y_1 z & x_1 y + y_1 w \\ xz_1 + w_1 z & yz_1 + w_1 w \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

atau

$$\begin{pmatrix} x_1 & y_1 \\ z_1 & w_1 \end{pmatrix}\begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Dengan mengambil determinan dari kedua ruas, diperoleh

$$(x_1 w_1 - z_1 y_1)(xw - zy) = 1. \qquad (7)$$

Akan tetapi, karena kedua faktor dalam persamaan (7) merupakan bilangan rasional bulat, maka haruslah

$$x_1 w_1 - z_1 y_1 = \pm 1$$

atau $\begin{vmatrix} x_1 & y_1 \\ z_1 & w_1 \end{vmatrix} = \pm 1.$

($\Leftarrow$)

Akan dibuktikan: $M_1 = M_2$.

Ambil $\gamma \in M_1$, maka $\gamma = \alpha s + \beta t$, untuk suatu bilangan rasional bulat s, t.

Karena $\alpha = \alpha_1 x_1 + \beta_1 y_1$ dan $\beta = \alpha_1 z_1 + \beta_1 w_1$, maka

$$\gamma = (\alpha_1 x_1 + \beta_1 y_1)s + (\alpha_1 z_1 + \beta_1 w_1)t$$
$$= (x_1 s + z_1 t)\alpha_1 + (y_1 s + w_1 t)\beta_1.$$

Sehingga, $\gamma \in M_2$.

Selanjutnya, ambil $\gamma \in M_2$, maka $\gamma = \alpha_1 k + \beta_1 m$, untuk suatu bilangan rasional bulat k, m.

Karena $\begin{vmatrix} x_1 & y_1 \\ z_1 & w_1 \end{vmatrix} = \pm 1 \neq 0$, maka $\begin{pmatrix} x_1 & y_1 \\ z_1 & w_1 \end{pmatrix}$ mempunyai invers. Sehingga,

$$\begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix} = \frac{1}{\begin{vmatrix} x_1 & y_1 \\ z_1 & w_1 \end{vmatrix}} \begin{pmatrix} w_1 & -y_1 \\ -z_1 & x_1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$$= \pm \begin{pmatrix} w_1 & -y_1 \\ -z_1 & x_1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}.$$

Akibatnya, $\alpha_1 = w_1 \alpha - y_1 \beta$ atau $\alpha_1 = -w_1 \alpha + y_1 \beta$ dan $\beta_1 = -z_1 \alpha + x_1 \beta$ atau $\beta_1 = z_1 \alpha - x_1 \beta$. Sehingga,

$$\gamma = (w_1 \alpha - y_1 \beta)k + (-z_1 \alpha + x_1 \beta)m$$

$$= (w_1 k - z_1 m)\alpha + (-y_1 k + x_1 m)\beta,$$

atau,

$$\gamma = (-w_1 \alpha + y_1 \beta)k + (z_1 \alpha - x_1 \beta)m$$

$$= (-w_1 k + z_1 m)\alpha + (y_1 k - x_1 m)\beta,$$

atau,

$$\gamma = (w_1 \alpha - y_1 \beta)k + (z_1 \alpha - x_1 \beta)m$$

$$= (w_1 k + z_1 m)\alpha + (-y_1 k + z_1 m)\beta, \text{ atau}$$

$$\gamma = (-w_1 \alpha + y_1 \beta)k + (-z_1 \alpha + x_1 \beta)m)$$

$$= (-w_1 k - z_1 m)\alpha + (y_1 k + x_1 m)\beta,$$

Sehingga, $\gamma \in M_1$. ■

Contoh 4.1.2:

Diberikan modul:

$$M_1 = \{x + y\sqrt{3} \mid x, y \text{ bilangan rasional bulat}\},$$

$$M_2 = \{(5+17\sqrt{3})x + (2+7\sqrt{3})y \mid x, y \text{ bilangan rasional bulat}\}.$$

Apakah modul $M_1 = M_2$?

Penyelesaian:

Perhatikan bahwa menurut Contoh 3.1.1 $\{1, \sqrt{3}\}$ merupakan basis dari $Q(\sqrt{3})$. Kemudian juga diperiksa bahwa $\{5+17\sqrt{3}, 2+7\sqrt{3}\}$ juga merupakan basis dari $Q(\sqrt{3})$.

Terlebih dahulu dibuktikan $\{5+17\sqrt{3}, 2+7\sqrt{3}\}$. Misalkan $s_1, s_2 \in Q$ maka $\{5+17\sqrt{3}, 2+7\sqrt{3}\}$ bebas linier yaitu jika $(5+17\sqrt{3})s_1 + (2+7\sqrt{3})s_2 = 0$ maka $s_1 = 0$ dan $s_2 = 0$. Sehingga jika $(5+17\sqrt{3})s_1 + (2+7\sqrt{3})s_2 = 0$, maka $5s_1 + 2s_2 = 0$ dan $17s_1 + 7s_2 = 0$. Dengan menstubstitusikan persamaan pertama ke dalam persamaan kedua maka diperoleh $s_1 = 0$ dan $s_2 = 0$. Sehingga $\{5+17\sqrt{3}, 2+7\sqrt{3}\}$ bebas linier.

Misalkan $\alpha \in Q(\sqrt{3})$, $\alpha = s + t\sqrt{3}$, dengan $s, t \in Q$, dan d bilangan rasional bulat bebas kuadrat. Suatu elemen $\alpha \in Q(\sqrt{3})$ merentang $Q(\sqrt{3})$ jika α

merupakan kombinasi linear dari $5+17\sqrt{3}, 2+7\sqrt{3}$ yaitu jika terdapat $s_1, s_2 \in \mathbb{Q}$ sedemikian sehingga

$$\alpha = (5+17\sqrt{3})s_1 + (2+7\sqrt{3})s_2.$$

Perhatikan bahwa : $\alpha = (5+17\sqrt{3})s_1 + (2+7\sqrt{3})s_2$ mengakibatkan

$$(5+17\sqrt{3})s_1 + (2+7\sqrt{3})s_2 = s + t\sqrt{3}.$$

Dengan menggunakan Teorema 3.1.2 diperoleh

$$5s_1 + 2s_2 = s \text{ dan}$$

$$17s_1 + 7s_2 = t.$$

Sehingga diperoleh $s_1 = 7s - 2t$ dan $s_2 = -17s + 5t$ keduanya di $\mathbb{Q}$.

Jadi, $\{5+17\sqrt{3}, 2+7\sqrt{3}\}$ basis dari $\mathbb{Q}(\sqrt{3})$.

Selanjutnya menurut Teorema 4.1.2 $M_1 = M_2$ jika dan hanya jika terdapat bilangan rasional bulat x_1, y_1, z_1, w_1 sedemikian sehingga

$$\begin{pmatrix} 1 \\ \sqrt{3} \end{pmatrix} = \begin{pmatrix} x_1 & y_1 \\ z_1 & w_1 \end{pmatrix} \begin{pmatrix} 5+17\sqrt{3} \\ 2+7\sqrt{3} \end{pmatrix} \qquad (8)$$

dan

$$\begin{vmatrix} x_1 & y_1 \\ z_1 & w_1 \end{vmatrix} = \pm 1.$$

Dari (8) diperoleh,

$$(5x_1 + 2y_1) + (17x_1 + 7y_1)\sqrt{3} = 1 \qquad (9)$$

$$(5z_1 + 2w_1) + (17z_1 + 7w_1)\sqrt{3} = \sqrt{3}. \qquad (10)$$

Menurut Teorema 3.1.2 dari persamaan (9) dapat diperoleh

$$5x_1 + 2y_1 = 1, \qquad (11)$$

$$17x_1 + 7y_1 = 0. \qquad (12)$$

Dari persaman (11) dan (12) diperoleh $x_1 = 7$ dan $y_1 = -17$. Sedangkan dari persamaan (10) dan menggunakan Teorema 3.1.2 maka diperoleh,

$$5z_1 + 2w_1 = 0 \qquad (13) \text{ dan}$$

$$17z_1 + 7w_1 = 1. \qquad (14)$$

Dari persamaan (13) dan (14) diperoleh $z_1 = -2$ dan $w_1 = 5$.

Sehingga terdapat bilangan rasional bulat $x_1 = 7$, $y_1 = -17$, $z_1 = -2$ dan $w_1 = 5$ sedemikian sehingga

$$\begin{pmatrix} 1 \\ \sqrt{3} \end{pmatrix} = \begin{pmatrix} 7 & -17 \\ -2 & 5 \end{pmatrix} \begin{pmatrix} 5+17\sqrt{3} \\ 2+7\sqrt{3} \end{pmatrix}.$$

Selain itu, $\begin{vmatrix} 7 & -17 \\ -2 & 5 \end{vmatrix} = 1$. Jadi, $M_1 = M_2$.

B. Persamaan Diophantine $ax^2 + bxy + cy^2 = m$

Dalam teori bilangan ada bermacam-macam persamaan Diophantine. Salah satu di antaranya adalah persamaan Diophantine berbentuk

$$ax^2 + bxy + cy^2 = m, \qquad (1)$$

dengan a, b, c, m bilangan rasional bulat yang diketahui, $a \neq 0$, dan x, y bilangan rasional bulat yang akan dicari.

Pada subbab ini akan diberikan algoritma untuk menentukan semua bilangan rasional bulat x, y yang memenuhi persamaan (1), dengan dasar teori yang sudah dibahas. Untuk itu, terlebih dahulu perhatikan polinomial

$$f(x,y) = ax^2 + bxy + cy^2. \qquad (2)$$

Polinomial (2) disebut **bentuk kuadrat biner**. Polinomial (2) dapat difaktorkan menjadi

$$f(x,y) = \frac{1}{a}\left(ax + \frac{b+\sqrt{D}}{2}y\right)\left(ax + \frac{b-\sqrt{D}}{2}y\right), \qquad (3)$$

dengan $D = b^2 - 4ac$ dan $a \neq 0$, yang kemudian disebut **diskriminan** dari $f(x,y)$.

Jika D bukan kuadrat bilangan rasional bulat, maka D dapat ditulis dalam bentuk $D = k^2 d$, dengan k bilangan rasional bulat positif, d bilangan rasional bulat bebas kuadrat. Jika D bukan kuadrat bilangan rasional bulat maka bilangan-bilangan D yaitu

$$\cdots\cdots,-5,-4,-3,-2,-1,2,3,5,6,7,\cdots\cdots.$$

Perhatikan bahwa D secara jelas dapat ditulis sebagai $D = k^2 d$ dengan k bilangan rasional bulat positif, d bilangan rasional bulat. Selanjutnya tinggal dibuktikan bahwa d bilangan rasional bulat bebas kuadrat, yaitu dibuktikan bahwa $d \neq 0$, $d \neq 1$ dan d bukan kelipatan kuadrat bilangan rasional bulat.

i) Dibuktikan $d \neq 0$.

Andaikan $d = 0$, maka $D = 0$.

Kontradiksi dengan D yaitu bahwa D bukan kuadrat bilangan rasional bulat.

Jadi $d \neq 0$.

ii) Dibuktikan $d \neq 1$.

Andaikan $d = 1$, maka $D = k^2$ dengan k bilangan rasional bulat positif.

Kontradiksi dengan D yaitu bahwa D bukan kuadrat bilangan rasional bulat.

Jadi $d \neq 1$.

iii) Dibuktikan d bukan kelipatan kuadrat bilangan rasional bulat.

Andaikan $d = s^2$, dengan $s \in \mathbb{Z}$.

Sehingga $D = k^2 \cdot s^2 = (ks)^2,\ ks \in \mathbb{Z}$.

Kontradiksi dengan D yaitu bahwa D bukan kuadrat bilangan rasional bulat.

Jadi d bukan kelipatan kuadrat bilangan rasional bulat.

Jadi bila $D = k^2 d$ dengan k bilangan rasional bulat positif, maka d bilangan rasional bulat bebas kuadrat. Perhatikan bahwa k dan d secara tunggal ditentukan oleh D, misalnya $D = -12 = 2^2 \cdot (-3)$, $D = -7 = 1^2 \cdot (-7)$.

Skripsi ini hanya akan membahas untuk kasus di mana D bukan kuadrat bilangan rasional bulat dan d bilangan rasional bulat negatif bebas kuadrat.

Karena $D = k^2 d$, maka persamaan (3) dapat ditulis dalam bentuk

$$f(x,y)=\frac{1}{a}\left(ax+\frac{b+k\sqrt{d}}{2}y\right)\left(ax+\frac{b-k\sqrt{d}}{2}y\right),\ a\neq 0. \qquad (4)$$

Misalkan $\alpha = a$ dan $\beta=\frac{b+k\sqrt{d}}{2}$. Perhatikan bahwa $\alpha,\beta\in \mathbb{Q}(\sqrt{d})$. Sehingga persamaan (4) juga dapat dinyatakan sebagai

$$f(x,y)=\frac{1}{a}(\alpha x+\beta y)(\overline{\alpha}x+\overline{\beta}y)$$

$$=\frac{1}{a}N(\alpha x+\beta y),$$

dengan $\overline{\alpha}$ konjugat dari α dan $\overline{\beta}$ konjugat dari β.

Karena $f(x,y)=ax^2+bxy+cy^2=m$ maka $N(\alpha x+\beta y)=am$. Sehingga masalah untuk menentukan semua penyelesaian dari persamaan Diophantine $ax^2+bxy+cy^2=m$, sama dengan menentukan semua bilangan rasional bulat x,y sedemikian sehingga $N(\alpha x+\beta y)=am$, dengan a,m bilangan rasional bulat dan $\alpha=a$ dan $\beta=\frac{b+k\sqrt{d}}{2}$. Perhatikan bahwa $\{\alpha,\beta\}$ dengan $\alpha=a$ dan $\beta=\frac{b+k\sqrt{d}}{2}$ merupakan basis dari $\mathbb{Q}(\sqrt{d})$. Hal tersebut dijelaskan demikian.

Akan dibuktikan: jika $s_1\alpha+s_2\beta=0$, $s_1,s_2\in\mathbb{Q}$ maka $s_1=0$ dan $s_2=0$. Jika $s_1\alpha+s_2\beta=0$ mengakibatkan

$$s_1a+s_2\frac{b+k\sqrt{d}}{2}=0.$$

Maka menurut Teorema 3.1.2 diperoleh $s_1 = 0$ dan $s_2 = 0$. Jadi $\{\alpha, \beta\}$ bebas linier. Himpunan $\{\alpha, \beta\}$ merentang $Q(\sqrt{d})$, sebab

Misalkan $\gamma \in Q(\sqrt{d})$ dengan $\gamma = u + v\sqrt{d}$, $u, v \in Q$, d bilangan rasional bulat bebas kuadrat. Suatu elemen $\gamma \in Q(\sqrt{d})$ merentang $Q(\sqrt{d})$ jika γ merupakan kombinasi linear dari α, β, yaitu jika terdapat $s_1, s_2 \in Q$ sedemikian sehingga

$$\gamma = s_1\alpha + s_2\beta.$$

Perhatikan bahwa: $\gamma = s_1\alpha + s_2\beta$ mengakibatkan

$$s_1 a + s_2 \frac{b + k\sqrt{d}}{2} = u + v\sqrt{d}, \text{ atau}$$

$$s_1 a + \frac{bs_2}{2} + \frac{ks_2}{2}\sqrt{d} = u + v\sqrt{d}.$$

Dengan menggunakan Teorema 3.1.2 diperoleh:

$$s_1 a + \frac{bs_2}{2} = u$$

$$\frac{ks_2}{2} = v.$$

Dari kedua persamaan diperoleh $s_1 = \frac{uk - bv}{ka}$, $s_2 = \frac{2v}{k}$, yang keduanya di Q.

Jadi, himpunan $\{\alpha, \beta\}$ merentang $Q(\sqrt{d})$.

Untuk selanjutnya, jika disebut modul M, maka yang dimaksud

$$M = \{\alpha x + \beta y \mid x, y \text{ bilangan rasional bulat}\},$$

dengan $\alpha, \beta \in Q(\sqrt{d})$ dan $\{\alpha, \beta\}$ basis dari $Q(\sqrt{d})$.

Perhatikan bahwa $\xi = \alpha x + \beta y$, dengan $\alpha = a$ dan $\beta = \dfrac{b + k\sqrt{d}}{2}$, x, y bilangan rasional bulat berada di modul M, karena $\alpha, \beta \in Q(\sqrt{d})$ dan $\{\alpha, \beta\}$ merupakan basis $Q(\sqrt{d})$. Selanjutnya, masalah untuk menentukan semua penyelesaian dari persamaan Diophantine $ax^2 + bxy + cy^2 = m$, sama dengan menentukan semua $\xi \in M$ sedemikian $N(\xi) = r$, dengan $r = am$, $r \in \mathbb{Z}$.

Misalkan M modul dari $Q(\sqrt{d})$, dengan $\alpha = s + t\sqrt{d}$, $\beta = u + v\sqrt{d}$, s, t, u, v bilangan rasional bulat, d bilangan rasional bulat negatif bebas kuadrat. Misalkan pula $\xi \in M$ dengan $\xi = \alpha x + \beta y$, Sehingga,

$$N(\xi) = N(\alpha x + \beta y) = (\alpha x + \beta y)\overline{(\alpha x + \beta y)},$$

dengan $\overline{(\alpha x + \beta y)}$ konjugat dari $\alpha x + \beta y$, dengan x, y bilangan rasional bulat. Akibatnya,

$$\begin{aligned} N(\xi) = N(\alpha x + \beta y) &= (\alpha x + \beta y)(\overline{\alpha}x + \overline{\beta}y) \\ &= ((s + t\sqrt{d})x + (u + v\sqrt{d})y)((s - t\sqrt{d})x + \\ &\quad (u - v\sqrt{d})y) \\ &= ((sx + uy) + (tx + vy)\sqrt{d})((sx + uy) - \\ &\quad (tx + vy)\sqrt{d}) \\ &= (sx + uy)^2 - d(tx + vy)^2 \\ &= (sx + uy)^2 + |d|(tx + vy)^2, \text{ karena } d < 0. \end{aligned}$$

Sehingga jika $N(\xi)=r$, maka $r\geq 0$ dan $|sx+uy|\leq\sqrt{r}$, $|tx+vy|\leq\dfrac{\sqrt{r}}{\sqrt{|d|}}$. Atau,

$$-\sqrt{r}\leq sx+uy\leq\sqrt{r} \text{ dan}$$

$$-\frac{\sqrt{r}}{\sqrt{|d|}}\leq tx+vy\leq\frac{\sqrt{r}}{\sqrt{|d|}}.$$

Karena s,t,u,v merupakan bilangan-bilangan yang diketahui dan $sx+uy$ dan $tx+vy$ terbatas maka bilangan-bilangan x,y banyaknya berhingga, karena x,y bilangan rasional bulat.

Sehingga jika $\alpha=a$ dan $\beta=\dfrac{b+k\sqrt{d}}{2}$ maka diperoleh hubungan

$$\left|ax+\frac{b}{2}y\right|\leq\sqrt{r} \text{ dan } \left|\frac{k}{2}y\right|\leq\frac{\sqrt{r}}{\sqrt{|d|}}.$$

Selanjutnya dari hubungan di atas akan diperoleh bilangan-bilangan rasional bulat x,y. Setelah diperoleh bilangan-bilangan x,y, selanjutnya diperiksa untuk masing-masing pasangan-pasangan x,y yang memenuhi $N(\xi)=r$. Pasangan-pasangan x,y yang memenuhi $N(\xi)=r$ itulah yang merupakan penyelesaian dari persamaan Diophantine (1).

Dari uraian-uraian di atas dapat dirangkum bahwa untuk menentukan penyelesaian dari persamaan Diophantine $ax^2+bxy+cy^2=m$ dapat ditentukan dengan algoritma sebagai berikut:

1) Tentukan D dengan rumus $D=b^2-4ac$ dan $r=am$.
2) Nyatakan D sebagai $D=k^2d$, dengan k bilangan rasional bulat positif dan d bilangan rasional bulat negatif bebas kuadrat.

3) Nyatakan $\alpha, \beta \in Q(\sqrt{d})$ dengan $\alpha = a$ dan $\beta = \frac{b + k\sqrt{d}}{2}$.

4) Bentuk modul M, $M = \{\alpha x + \beta y \mid x, y$ bilangan rasional bulat$\}$.

5) Tentukan bilangan rasional bulat x, y dari ketaksamaan berikut:

$$\left|ax + \frac{b}{2}y\right| \leq \sqrt{r} \text{ dan } \left|\frac{k}{2}y\right| \leq \frac{\sqrt{r}}{\sqrt{|d|}}.$$

6) Selanjutnya, tentukan $\xi \in M$ dengan $\xi = ax + \frac{b + k\sqrt{d}}{2}y$ dengan beberapa kemungkinan untuk bilangan rasional bulat x, y yang sudah diperoleh pada langkah 5).

7) Hitung $N(\xi) = \xi\bar{\xi}$, $\bar{\xi}$ konjugat dari ξ, kemudian tentukan bilangan rasional bulat x, y yang memenuhi $N(\xi) = r$. Bilangan rasional bulat x, y inilah yang merupakan penyelesaian dari persamaan Diophantine $ax^2 + bxy + cy^2 = m$.

Perhatikan bahwa algoritma diatas hanya berlaku untuk $a \neq 0$, karena jika $a = 0$ maka $\{\alpha, \beta\}$ dengan $\alpha = a$ dan $\beta = \frac{b + k\sqrt{d}}{2}$ bukan merupakan basis dari $Q(\sqrt{d})$ sehingga $\xi = ax + \frac{b + k\sqrt{d}}{2}y \notin M$.

Contoh 4.2.1:

Tentukan semua bilangan rasional bulat x, y yang memenuhi persamaan Diophantine $x^2 + xy + y^2 = 3$.

Dari persamaan Diophantine $x^2 + xy + y^2 = 3$, diperoleh $D = -3$. Sehingga D dapat ditulis $D = 1^2 \cdot (-3)$, $k = 1$ dan $d = -3$. Kemudian α, β, dinyatakan sebagai $\alpha = 1$ dan $\beta = \dfrac{1+\sqrt{-3}}{2}$. Dibentuk modul M,

$$M = \{\alpha x + \beta y \mid x, y \text{ bilangan rasional bulat}\}$$

$$= \{x + y\frac{1+\sqrt{-3}}{2} \mid x, y \text{ bilangan rasional bulat}\}.$$

Menentukan bilangan rasional bulat x, y dari ketaksamaan berikut

$$\left|x + \frac{y}{2}\right| \le \sqrt{3} \text{ dan } \left|\frac{y}{2}\right| \le \frac{\sqrt{3}}{\sqrt{3}} = 1.$$

Akibatnya,

$$-\sqrt{3} \le x + \frac{y}{2} \le \sqrt{3}, \quad (5) \text{ dan}$$

$$-2 \le y \le 2. \quad (6)$$

Karena x, y bilangan rasional bulat, maka dari (6) kemungkinan untuk y adalah $y = \pm 2$, $y = \pm 1$, dan $y = 0$. Selanjutnya akan diperiksa masing-masing kemungkinan untuk y, sehingga diperoleh beberapa pasangan (x, y) dan untuk pasangan (x, y) yang memenuhi $N(\xi) = 3$ adalah pasang (x, y) yang memenuhi persamaan Diophantine $x^2 + xy + y^2 = 3$.

1) Jika $y=-2$ maka setelah disubstitusikan ke dalam (5) diperoleh $1-\sqrt{3}\le x\le 1+\sqrt{3}$ atau $-0{,}7\le x\le 2{,}7$. Sehingga kemungkinan untuk x adalah $x=0$, $x=1$, $x=2$. Diperoleh pasangan (x,y), yaitu $(x,y)=(0,-2);(x,y)=(1,-2);(x,y)=(2,-2)$. Kemudian diperiksa untuk pasangan (x,y) yang memenuhi $N(\xi)=3$, jika $\xi=x+y\dfrac{1+\sqrt{-3}}{2}$ dan $N(\xi)=\xi\bar{\xi}$, $\bar{\xi}$ konjugat dari ξ. Untuk mempermudah melakukan pengecekan maka perhitungan akan ditampilkan dalam bentuk tabel.

Tabel 4.1

(x,y)	$\xi=x+y\dfrac{1+\sqrt{-3}}{2}$	$N(\xi)=\xi\bar{\xi}$
$(0,-2)$	$-1-\sqrt{-3}$	4
$(1,-2)$	$-\sqrt{-3}$	3
$(2,-2)$	$1-\sqrt{-3}$	4

Dari Tabel 4.1 yang memenuhi $N(\xi)=3$ hanyalah pasangan $(x,y)=(1,-2)$. Sehingga $(x,y)=(1,-2)$ merupakan penyelesaian dari persamaan Diophantine $x^2+xy+y^2=3$.

2) Jika $y=2$ maka setelah disubstitusikan ke dalam (5) diperoleh $-2-\sqrt{3}\le x\le -2+\sqrt{3}$ atau $-3{,}7\le x\le -0{,}2$. Sehingga kemungkinan untuk x adalah $x=-3$, $x=-2$, $x=-1$, $x=0$. Diperoleh pasangan (x,y), yaitu $(x,y)=(-3,2)$, $(x,y)=(-2,2)$, $(x,y)=(-1,2)$, $(x,y)=(0,2)$.

Tabel 4.2

(x,y)	$\xi = x + y\dfrac{1+\sqrt{-3}}{2}$	$N(\xi) = \xi\bar{\xi}$
$(-3,2)$	$-2+\sqrt{-3}$	7
$(-2,2)$	$-1+\sqrt{-3}$	4
$(-1,2)$	$\sqrt{-3}$	3
$(0,2)$	$1+\sqrt{-3}$	4

Dari Tabel 4.2 yang memenuhi $N(\xi) = 3$ hanyalah pasangan $(x,y) = (-1,2)$. Jadi $(x,y) = (-1,2)$ juga merupakan penyelesaian.

3) Jika $y = -1$ maka setelah disubstitusikan ke dalam (5) diperoleh $\frac{1}{2} - \sqrt{3} \le x \le \frac{1}{2} + \sqrt{3}$ atau $-1,2 \le x \le 2,2$. Sehingga kemungkinan untuk x adalah $x = -1$, $x = 0$, $x = 1$, $x = 2$. Diperoleh pasangan (x,y), yaitu $(x,y) = (-1,-1)$, $(x,y) = (0,-1)$, $(x,y) = (1,-1)$, $(x,y) = (2,-1)$.

Tabel 4.3

(x,y)	$\xi = x + y\dfrac{1+\sqrt{-3}}{2}$	$N(\xi) = \xi\bar{\xi}$
$(-1,-1)$	$-\frac{3}{2} - \frac{1}{2}\sqrt{-3}$	3
$(0,-1)$	$-\frac{1}{2} - \frac{1}{2}\sqrt{-3}$	1
$(1,-1)$	$\frac{1}{2} - \frac{1}{2}\sqrt{-3}$	1
$(2,-1)$	$\frac{3}{2} - \frac{1}{2}\sqrt{-3}$	3

Dari Tabel 4.3 yang memenuhi $N(\xi) = 3$ yaitu $(x,y) = (-1,-1)$ dan $(x,y) = (2,-1)$. Jadi $(x,y) = (-1,-1)$ dan $(x,y) = (2,-1)$ juga merupakan penyelesaian.

4) Jika $y=1$ maka setelah disubstitusikan ke dalam (5) diperoleh $-\frac{1}{2}-\sqrt{3}\leq x\leq -\frac{1}{2}+\sqrt{3}$ atau $-2{,}7\leq x\leq 1{,}2$. Sehingga kemungkinan untuk x adalah $x=-2$, $x=-1$, $x=0$, $x=1$. Diperoleh pasangan (x,y), yaitu $(x,y)=(-2,-1)$, $(x,y)=(-1,1)$, $(x,y)=(0,1)$, $(x,y)=(1,1)$.

Tabel 4.4

(x,y)	$\xi = x+y\frac{1+\sqrt{-3}}{2}$	$N(\xi)=\xi\bar{\xi}$
$(-2,1)$	$-\frac{3}{2}+\frac{1}{2}\sqrt{-3}$	3
$(-1,1)$	$-\frac{1}{2}+\frac{1}{2}\sqrt{-3}$	1
$(0,1)$	$\frac{1}{2}+\frac{1}{2}\sqrt{-3}$	1
$(1,1)$	$\frac{3}{2}+\frac{1}{2}\sqrt{-3}$	3

Dari Tabel 4.4 yang memenuhi $N(\xi)=3$ yaitu $(x,y)=(-2,1)$ dan $(x,y)=(1,1)$. Jadi $(x,y)=(-2,1)$ dan $(x,y)=(1,1)$ juga merupakan penyelesaian.

5) Jika $y=0$ maka setelah disubstitusikan ke dalam (5) diperoleh $-\sqrt{3}\leq x\leq +\sqrt{3}$ atau $-1{,}7\leq x\leq 1{,}7$. Sehingga kemungkinan untuk x adalah $x=-1$, $x=0$, dan $x=1$. Diperoleh pasangan (x,y), yaitu $(x,y)=(-1,0)$, $(x,y)=(0,0)$, $(x,y)=(1,0)$.

Tabel 4.5

(x,y)	$\xi = x + y\frac{1+\sqrt{-3}}{2}$	$N(\xi) = \xi\bar{\xi}$
$(-1,0)$	-1	1
$(0,0)$	0	0
$(1,0)$	1	1

Dari Tabel 4.5 ternyata tidak ada pasangan (x,y) yang memenuhi $N(\xi)=3$, sehingga dalam kasus ini tidak terdapat pasangan (x,y)yang merupakan penyelesaian dari persaman Diophantine $x^2 + xy + y^2 = 3$.

Dari Tabel 4.1-Tabel 4.5 dapat disimpulkan bahwa pasangan (x,y) yang merupakan penyelesaian dari persamaan Diophantine $x^2 + xy + y^2 = 3$ adalah pasangan $(x,y)=(1,-2)$; $(x,y)=(-1,2)$; $(x,y)=(-1,-1)$; $(x,y)=(2,-1)$; $(x,y)=(-2,1)$ dan $(x,y)=(1,1)$.

Contoh 4.2.2:

Tentukan semua penyelesaian bilangan rasional bulat dari persamaan Diophantine $x^2 + 2xy + 2y^2 = 17$.

Penyelesaian:

Dari persamaan Diophantine $x^2 + 2xy + 2y^2 = 17$, diperoleh $D = -4$ dan $r = 17$ sehingga D dapat ditulis dalam bentuk $D = 2^2 \cdot (-1)$, dengan $k = 2$ dan

$d=-1$. Selanjutnya, diperoleh $\alpha=1$ dan $\beta=\dfrac{2+2\sqrt{-1}}{2}=1+\sqrt{-1}$. Dibentuk modul M dengan

$$M=\{x+y(1+\sqrt{-1}) \mid x,y \text{ bilangan rasional bulat}\}.$$

Akan ditentukan $\xi \in M$ sedemikian sehingga $N(\xi)=17$.

Menentukan bilangan rasional bulat x,y dari ketaksamaan berikut

$$|x+y| \le \sqrt{17} \text{ dan}$$

$$|y| \le \frac{\sqrt{17}}{\sqrt{1}}=\sqrt{17}.$$

Atau,

$$-\sqrt{17} \le x+y \le \sqrt{17}, \qquad (7)$$

$$-\sqrt{17} \le y \le \sqrt{17}. \qquad (8)$$

Ketaksamaan (7) dapat ditulis $-4{,}1 \le x+y \le 4{,}1$ sedangkan ketaksamaan (8) dapat ditulis $-4{,}1 \le y \le 4{,}1$. Karena y rasional bulat maka kemungkinan untuk y adalah $y=\pm 4$, $y=\pm 3$, $y=\pm 2$, $y=\pm 1$ dan $y=0$. Selanjutnya akan diperiksa untuk kesembilan kemungkinan y tersebut.

1) Untuk $y=4$ maka diperoleh $-8{,}1 \le x \le 0{,}1$. Karena x bilangan rasional bulat maka kemungkinan-kemungkinan untuk x adalah $x=-8$, $x=-7$, $x=-6$, $x=-5$, $x=-4$, $x=-3$, $x=-2$, $x=-1$ dan $x=0$. Diperoleh sembilan pasangan (x,y) yang akan diberikan tabel dibawah ini, berikut perhitungan untuk ξ dan $N(\xi)$.

Tabel 4.6

(x,y)	$\xi = x + y(1+\sqrt{-1})$	$N(\xi) = \xi\overline{\xi}$
(-8,4)	$-4+4\sqrt{-1}$	32
(-7,4)	$-3+4\sqrt{-1}$	25
(-6,4)	$-2+4\sqrt{-1}$	20
(-5,4)	$-1+4\sqrt{-1}$	17
(-4,4)	$4\sqrt{-1}$	16
(-3,4)	$1+4\sqrt{-1}$	17
(-2,4)	$2+4\sqrt{-1}$	20
(-1,4)	$3+4\sqrt{-1}$	25
(0,4)	$4+4\sqrt{-1}$	32

Dari Tabel 4.6 pasangan (x,y) yang memenuhi $N(\xi)=17$ dan juga merupakan penyelesaian adalah pasangan $(x,y)=(-5,4)$ dan $(x,y)=(-3,4)$.

2) Untuk $y=-4$ maka diperoleh $-0{,}1 \le x \le 8{,}1$. Sehingga kemungkinan untuk x adalah $x=8$, $x=7$, $x=6$, $x=5$, $x=4$, $x=3$, $x=2$, $x=1$ dan $x=0$. Sehingga terdapat sembilan kemungkinan untuk pasangan (x,y), seperti yang akan diberikan dalam tabel di bawah ini,

Tabel 4.7

(x,y)	$\xi = x + y(1+\sqrt{-1})$	$N(\xi) = \xi\overline{\xi}$
(8,-4)	$4-4\sqrt{-1}$	32
(7,-4)	$3-4\sqrt{-1}$	25
(6,-4)	$2-4\sqrt{-1}$	20
(5,-4)	$1-4\sqrt{-1}$	17
(4,-4)	$-4\sqrt{-1}$	16
(3,-4)	$-1-4\sqrt{-1}$	17
(2,-4)	$-2-4\sqrt{-1}$	20
(1,-4)	$-3-4\sqrt{-1}$	25
(0,-4)	$-4-4\sqrt{-1}$	32

Dari Tabel 4.7 pasangan (x, y) yang memenuhi $N(\xi) = 17$ dan juga merupakan penyelesaian adalah pasangan $(x, y) = (5, -4)$ dan $(x, y) = (3, -4)$.

3) Untuk $y = 3$ maka diperoleh $-7{,}1 \le x \le 1{,}1$. Sehingga kemungkinan untuk x adalah $x = -7$, $x = -6$, $x = -5$, $x = -4$, $x = -3$, $x = -2$, $x = -1$, $x = 0$ dan $x = 1$. Sehingga terdapat sembilan kemungkinan untuk pasangan (x, y), seperti yang akan diberikan dalam tabel di-bawah ini,

Tabel 4.8

(x, y)	$\xi = x + y(1 + \sqrt{-1})$	$N(\xi) = \xi\bar{\xi}$
(-7,3)	$-4 + 3\sqrt{-1}$	25
(-6,3)	$-3 + 3\sqrt{-1}$	18
(-5,3)	$-2 + 3\sqrt{-1}$	13
(-4,3)	$-1 + 3\sqrt{-1}$	10
(-3,3)	$3\sqrt{-1}$	9
(-2,3)	$1 + 3\sqrt{-1}$	10
(-1,3)	$2 + 3\sqrt{-1}$	13
(0,3)	$3 + 3\sqrt{-1}$	18
(1,3)	$4 + 3\sqrt{-1}$	28

Dari Tabel 4.8 ternyata tidak ada pasangan (x, y) yang memenuhi $N(\xi) = 17$, sehingga dalam kasus ini tidak terdapat pasangan (x, y) yang merupakan penyelesaian dari persamaan Diophantine $x^2 + 2xy + 2y^2 = 17$.

4) Untuk $y=-3$ maka diperoleh $-1{,}1 \leq x \leq 7{,}1$. Sehingga kemungkinan untuk x adalah $x=7$, $x=6$, $x=5$, $x=4$, $x=3$, $x=2$, $x=1$, $x=0$, $x=-1$. Sehingga terdapat sembilan kemungkinan untuk pasangan (x,y), seperti yang akan diberikan dalam tabel di bawah ini,

Tabel 4.9

(x,y)	$\xi = x + y(1+\sqrt{-1})$	$N(\xi)=\xi\bar{\xi}$
(7,-3)	$4-3\sqrt{-1}$	25
(6,-3)	$3-3\sqrt{-1}$	18
(5,-3)	$2-3\sqrt{-1}$	13
(4,-3)	$1-3\sqrt{-1}$	10
(3,-3)	$-3\sqrt{-1}$	9
(2,-3)	$-1-3\sqrt{-1}$	10
(1,-3)	$-2-3\sqrt{-1}$	13
(0,-3)	$-3-3\sqrt{-1}$	18
(-1,-3)	$-4-3\sqrt{-1}$	25

Dari Tabel 4.9 ternyata tidak ada pasangan (x,y) yang memenuhi $N(\xi)=17$, sehingga dalam kasus ini tidak terdapat pasangan (x,y) yang merupakan penyelesaian dari persamaan Diophantine $x^2+2xy+2y^2=17$.

5) Untuk $y=2$ maka diperoleh $-6{,}1 \leq x \leq 2{,}1$. Sehingga kemungkinan untuk x adalah $x=-6$, $x=-5$, $x=-4$, $x=-3$, $x=-2$, $x=-1$, $x=0$, $x=1$ dan $x=2$. Sehingga terdapat sembilan kemungkinan untuk pasangan (x,y), seperti yang akan diberikan dalam tabel di-bawah ini,

Tabel 4.10

(x,y)	$\xi = x + y(1+\sqrt{-1})$	$N(\xi) = \xi\bar{\xi}$
(-6,2)	$-4+2\sqrt{-1}$	20
(-5,2)	$-3+2\sqrt{-1}$	13
(-4,2)	$-2+2\sqrt{-1}$	8
(-3,2)	$-1+2\sqrt{-1}$	5
(-2,2)	$2\sqrt{-1}$	4
(-1,2)	$1+3\sqrt{-1}$	10
(0,2)	$2+2\sqrt{-1}$	8
(1,2)	$3+2\sqrt{-1}$	13
(2,2)	$4+2\sqrt{-1}$	20

Dari Tabel 4.10 ternyata tidak ada pasangan (x, y) yang memenuhi $N(\xi) = 17$, sehingga dalam kasus ini tidak terdapat pasangan (x, y) yang merupakan penyelesaian dari persamaan Diophantine $x^2 + 2xy + 2y^2 = 17$.

6) Untuk $y = -2$ maka diperoleh $-2{,}1 \le x \le 6{,}1$. Sehingga kemungkinan untuk x adalah $x = 6, x = 5,$ $x = 4,$ $x = 3,$ $x = 2,$ $x = 1, x = 0,$ $x = -1$ dan $x = -2$. Terdapat sembilan kemungkinan untuk pasangan (x, y), seperti yang akan diberikan dalam tabel di bawah ini,

Tabel 4.11

(x,y)	$\xi = x + y(1+\sqrt{-1})$	$N(\xi) = \xi\bar{\xi}$
(6,-2)	$4-2\sqrt{-1}$	20
(5,-2)	$3-2\sqrt{-1}$	13
(4,-2)	$2-2\sqrt{-1}$	8
(3,-2)	$1-2\sqrt{-1}$	5
(2,-2)	$-2\sqrt{-1}$	4
(1,-2)	$-1-2\sqrt{-1}$	5

(0,-2)	$-2-2\sqrt{-1}$	8
(-1,-2)	$-3-2\sqrt{-1}$	13
(-2,-2)	$-4-2\sqrt{-1}$	20

Dari Tabel 4.11 ternyata tidak ada pasangan (x, y) yang memenuhi $N(\xi)=17$, sehingga dalam kasus ini tidak terdapat pasangan (x, y) yang merupakan penyelesaian dari persamaan Diophantine $x^2+2xy+2y^2=17$.

7) Untuk $y=1$ maka diperoleh $-5{,}1 \leq x \leq 3{,}1$. Sehingga kemungkinan untuk x adalah $x=-5$, $x=-4$, $x=-3$, $x=-2$, $x=-1$, $x=0$, $x=1$, $x=2$ dan $x=3$. Selanjutnya kemungkinan-kemungkinan untuk pasangan (x, y), akan diberikan dalam tabel di bawah ini,

Tabel 4.12

(x, y)	$\xi = x + y(1+\sqrt{-1})$	$N(\xi)=\xi\bar{\xi}$
(-4,1)	$-3+\sqrt{-1}$	10
(-3,1)	$-2+\sqrt{-1}$	5
(-2,1)	$-1+\sqrt{-1}$	2
(-1,1)	$\sqrt{-1}$	1
(0,1)	$1+\sqrt{-1}$	2
(1,1)	$2+\sqrt{-1}$	5
(2,1)	$3+\sqrt{-1}$	10
(3,1)	$4+\sqrt{-1}$	17

Dari Tabel 4.12 pasangan (x, y) yang memenuhi $N(\xi)=17$ dan juga merupakan penyelesaian adalah pasangan $(x, y)=(3{,}1)$.

8) Untuk $y=-1$ maka diperoleh $-3{,}1 \le x \le 5{,}1$. Sehingga kemungkinan untuk x adalah $x=5$, $x=4$, $x=3$, $x=2$, $x=1$, $x=0$, $x=-1$, $x=-2$ dan $x=-3$. Selanjutnya kemungkinan-kemungkinan untuk pasangan (x,y), akan diberikan dalam tabel di bawah ini,

Tabel 4.13

(x,y)	$\xi = x + y(1+\sqrt{-1})$	$N(\xi)=\xi\bar{\xi}$
(5,-1)	$4-\sqrt{-1}$	17
(4,-1)	$3-\sqrt{-1}$	10
(3,-1)	$2-3\sqrt{-1}$	13
(2,-1)	$1-\sqrt{-1}$	2
(1,-1)	$-1\sqrt{-1}$	1
(0,-1)	$-1-\sqrt{-1}$	2
(-1,-1)	$-2-\sqrt{-1}$	5
(-2,-1)	$-3-\sqrt{-1}$	10
(-3,-1)	$-4-\sqrt{-1}$	17

Dari Tabel 4.13 pasangan (x,y) yang memenuhi $N(\xi)=17$ dan juga merupakan penyelesaian adalah pasangan $(x,y)=(5,-1)$ dan $(x,y)=(-3,-1)$.

9) Untuk $y=0$ maka diperoleh $-4{,}1 \le x \le 4{,}1$. Sehingga kemungkinan untuk x adalah $x=-4$, $x=-3$, $x=-2$, $x=-1$, $x=0$, $x=1$, $x=2$, $x=3$, dan $x=4$. Selanjutnya kemungkinan-kemungkinan untuk pasangan (x,y), akan diberikan dalam tabel di bawah ini,

Tabel 4.14

(x,y)	$\xi = x + y(1+\sqrt{-1})$	$N(\xi)=\xi\bar{\xi}$
(-4,0)	-4	16
(-3,0)	-3	9

(-2,0)	-2	4
(-1,0)	-1	1
(0,0)	0	0
(1,0)	1	1
(2,0)	2	4
(3,0)	3	9
(4,0)	4	16

Karena tidak terdapat pasangan (x, y) dalam Tabel 4.14 yang memenuhi $N(\xi) = 17$, maka tidak ada penyelesaian untuk kasus ini.

Dari Tabel 4.6-Tabel 4.14 dapat disimpulkan bahwa pasangan (x, y) yang merupakan penyelesaian dari persamaan Diophantine $x^2 + 2xy + 2y^2 = 17$ adalah pasangan-pasangan $(x, y) = (-5,4)$; $(x, y) = (-3,4)$; $(x, y) = (5,-4)$; $(x, y) = (3,-4)$; $(x, y) = (3,1)$; $(x, y) = (5,-1)$ dan $(x, y) = (-3,-1)$.

BAB V

PENUTUP

Dari pembahasan pada bab-bab sebelumnya dapat disimpulkan bahwa:

1) Himpunan semua bilangan kuadratik $\mathbb{Q}(\sqrt{d})$, yaitu himpunan bilangan berbentuk $s + t\sqrt{d}$ dengan $s, t \in \mathbb{Q}$ dan d bilangan bulat bebas kuadrat, membentuk suatu medan.

2) Misalkan $\alpha \in \mathbb{Q}(\sqrt{d})$, maka α hanya dapat dinyatakan dengan satu cara sebagai $\alpha = a + b\sqrt{d}$. Dengan kata lain jika $a + b\sqrt{d} = e + f\sqrt{d}$ dengan $a, b, e, f \in \mathbb{Q}$ maka $a = e$ atau $b = f$.

3) Selanjutnya, jika $\mathbb{R}$, $\mathbb{Q}(\sqrt{d})$ dan $\mathbb{C}$ dibandingkan maka diperoleh hubungan sebagai berikut:

   a) Jika $d > 0$, maka $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{R} \subset \mathbb{C}$.

   b) Jika $d < 0$, maka $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{C}$, $\mathbb{R} \subseteq \mathbb{C}$ dan $\mathbb{Q}(\sqrt{d}) \not\subseteq \mathbb{R}$.

4) Medan kuadratik $\mathbb{Q}(\sqrt{d})$ membentuk ruang vektor atas medan $\mathbb{Q}$.

5) Diberikan $x_1, y_1 \in \mathbb{Z}$, d bilangan bulat bebas kuadrat dan $x_1^2 - dy_1^2 \equiv 0 \pmod 4$. Maka sifat-sifat berikut dipenuhi:

a) Jika $d \equiv 2(\mathrm{mod}\,4)$ atau $d \equiv 3(\mathrm{mod}\,4)$ maka x_1, y_1 keduanya genap.

b) Jika $d \equiv 1(\mathrm{mod}\,4)$ maka x_1, y_1 keduanya genap atau x_1, y_1 keduanya ganjil.

(Catatan: karena d bilangan bulat bebas kuadrat maka $d \not\equiv 0(\mathrm{mod}\ 4)$.

6) Himpunan bilangan bulat dari $\mathbb{Q}(\sqrt{d})$ yaitu I_d berbentuk

$a + b\omega_d$ dengan $a, b \in \mathbb{Z}$ dan

$$\omega_d = \begin{cases} \sqrt{d} & \text{jika } d \equiv 2 \text{ (mod 4) atau } d \equiv 3 \text{ (mod 4)} \\ \dfrac{1+\sqrt{d}}{2} & \text{jika } d \equiv 1 \text{ (mod 4).} \end{cases}$$

7) Himpunan I_d membentuk subdaerah-integral dalam daerah integral $\mathbb{Q}(\sqrt{d})$.

8) Misalkan $\{\alpha, \beta\}$ dan $\{\alpha_1, \beta_1\}$ basis dari $\mathbb{Q}(\sqrt{d})$. Misalkan pula

$$M_1 = \{\alpha x + \beta y \mid x, y \text{ bilangan rasional bulat}\} \text{ dan}$$

$$M_2 = \{\alpha_1 x + \beta y \mid x, y \text{ bilangan rasional bulat}\},$$

modul dari $\mathbb{Q}(\sqrt{d})$, maka modul $M_1 = M_2$ jika dan hanya jika terdapat bilangan rasional bulat x_1, y_1, z_1, w_1 sedemikian sehingga

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} x_1 & y_1 \\ z_1 & w_1 \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix} \text{dan} \begin{vmatrix} x_1 & y_1 \\ z_1 & w_1 \end{vmatrix} = \pm 1.$$

9) Jika $\mathbb{Z}\ [i]$ menyatakan himpunan semua bilangan bulat Gauss, yaitu bilangan kompleks berbentuk $x+iy$ dengan $x,y \in \mathbb{Z}$ dan $i=\sqrt{-1}$ maka diperoleh hubungan $\mathbb{Z}\ [i] \subseteq I_d \subseteq \mathbb{Q}(\sqrt{d})$.

10) Penyelesaian dari persamaan Diophantine $ax^2+bxy+cy^2=m$ dengan a,b,c,m bilangan rasional bulat, $a \neq 0$ dapat ditentukan dengan langkah-langkah sebagai berikut:

a) Tentukan D dengan rumus $D=b^2-4ac$ dan $r=am$.

b) Nyatakan D sebagai $D=k^2d$, dengan k bilangan rasional bulat positif dan d bilangan rasional bulat negatif bebas kuadrat.

c) Nyatakan $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$ dengan $\alpha=a$ dan $\beta=\dfrac{b+k\sqrt{d}}{2}$.

d) Bentuk modul M, $M=\{\alpha x+\beta y \mid x,y$ bilangan rasional bulat$\}$.

e) Tentukan bilangan rasional bulat x,y dari ketaksamaan berikut:

$$\left|ax+\frac{b}{2}y\right| \leq \sqrt{r} \text{ dan } \left|\frac{k}{2}y\right| \leq \frac{\sqrt{r}}{\sqrt{|d|}}.$$

f) Selanjutnya, tentukan $\xi \in M$ dengan $\xi = ax+\dfrac{b+k\sqrt{d}}{2}y$ dengan beberapa kemungkinan untuk bilangan rasional bulat x,y yang sudah diperoleh pada langkah e).

g) Hitung $N(\xi)=\xi\bar{\xi}$, $\bar{\xi}$ konjugat dari ξ, kemudian tentukan bilangan rasional bulat x,y yang memenuhi $N(\xi)=r$. Bilangan rasional bulat inilah yang merupakan penyelesaian dari persamaan Diophantine $ax^2 + bxy + cy^2 = m$.

Perhatikan bahwa algoritma tersebut khusus untuk D bukan kuadrat bilangan rasional bulat dan d bilangan rasional bulat negatif bebas kuadrat. Selainnya tidak dibahas dalam skripsi ini.

DAFTAR PUSTAKA

Adams, W.W. & Goldstein, L.J. (1976). *Introduction to Number Theory.* Englewood Cliffs: Prentice-Hall, Inc.

Arifin, A. (2000). *Aljabar.* Bandung: Penerbit ITB

Beaumont, R.A. & Pierce, R.S. (1963). *The Algebraic Foundations of Mathematics.* Reading: Addison-Wesley Publishing Company, Inc.

Budhi, W.S. (1995). *Aljabar Linear.* Jakarta: PT Gramedia Pustaka Utama

Burton, M.D. (1980). *Elementary Number Theory.* Boston: Allyn and Bacon, Inc.

Fraleigh, J.B. (1989). *A First Course in Abstract Algebra* (4th ed.). New York: Addison-Wesley Publishing Company

Niven, I. & Zuckerman, H.S. (1980). *An Introduction to the Theory of Numbers.* Edisi ke-4. New York: John Wiley & Sons, Inc.

Soemantri, R. (2000). "*Persamaan Diophantine dan Misteri yang Berabad-abad Tak Terpecahkan*". Dalam: J. Eka Priyatma, dkk. (Ed). Sains: Dari Manusia untuk Manusia. Yogyakarta: Penerbit Universitas Sanata Dharma