II. TINJAUAN PUSTAKA

Pada bab ini akan diberikan konsep dasar (pengertian) tentang bilangan sempurna, *square free,* keterbagian bilangan bulat, modulo, bilangan prima, daerah integral, ring bilangan bulat dari $\mathbb{Q}\sqrt{d}$.

2.1 Bilangan

2.1.1 Bilangan Kuadrat Sempurna

Definisi 2.1.1.1. Bilangan kuadrat sempurna adalah suatu bilangan yang jika diakar (dipangkatkan setengah) hasilnya berupa bilangan asli (Burton, 1976).

Contoh. Berikut ini merupakan bilangan kuadrat sempurna 1, 4, 9, 16, 25, 36, …
Banyak faktor dari bilangan kuadrat sempurna adalah ganjil. Karena ada satu pasang faktornya yang berpasangan dengan dirinya sendiri. Sehingga jumlah faktornya sebanyak bilangan ganjil. Faktor dari bilangan yang bukan merupakan kuadrat sempurna, misalnya bilangan 8. Faktor-faktornya yaitu 1, 8, 2 dan 4. Faktor-faktornya saling berpasangan, 1 dan 8, dan 2 dan 4.Sedangkan pada bilangan kuadrat sempurna, misalnya 9, faktor-faktornya adalah 1, 9 dan 3. Yang berpasangan adalah 1 dan 9, sedangkan 3 berpasangan dengan dirinya sendiri. Beberapa bilangan kuadrat sempurna yang pertama adalah 1, 4, 9, 16, 25, 36, 49, 64,, …

2.1.2 Bilangan Kuadrat Bebas (*Square Free Integer*)

Definisi 2.1.2.1 *Square free* adalah bilangan bulat yang tidak dapat dibagi oleh bilangan kuadrat sempurna kecuali 1 (Burton, 1976).

Contoh.

1. 10 adalah *square free*, karena 10 tidak habis dibagi dengan 4 dan 9
2. 18 bukan *square free* karena bisa dibagi $3^2 = 9$

Barisan *square free*:

1, 2, 3, 5, 6, 7, 10, 11, 13, 14, 15, 17, 19, 21, 22, 23, 26, 29, 30, 31, 34, 35, 38, 39, dan seterusnya.

Teorema 2.1.2.1. Bilangan bulat positif *n* dikatakan *square free* jika hanya jika faktor prima dari *n* tidak muncul lebih dari satu kali (Burton, 1976).

Contoh.

1. $10 = 2 \cdot 5$
2. $26 = 2 \cdot 13$

2.1.3 Keterbagian Bilangan Bulat

Definisi 2.1.3.1. Sebuah bilangan bulat *b* dikatakan terbagi atau habis dibagi oleh bilangan bulat $a \neq 0$ jika terdapat bilangan bulat c sehingga $b = ac$, ditulis $a|b$. Notasi $a \nmid b$ digunakan untuk menyatakan *b* tidak habis terbagi oleh a.

Jadi 12 terbagi oleh 4 sebab $12 = 4 \cdot 3$, tetapi 10 tidak terbagi oleh 3 sebab tidak ada bilangan bulat c sehingga $10 = 3c$, atau setiap bilangan bulat c berlaku $10 \neq 3c$. Dalam kasus ini ditulis $4|12$ dan $3 \nmid 10$ (Sukirman, 1997).

Istilah lain untuk $a|b$ adalah *a* faktor dari b, a pembagi *b* atau *b* kelipatan dari a.

Bila a pembagi b maka $-a$ juga pembagi b, sehingga pembagi suatu bilangan selalu terjadi berpasangan. Jadi dalam menentukan semua faktor dari suatu bilangan bulat cukup ditentukan faktor-faktor positifnya saja, kemudian digabungkan dengan faktor negatifnya. Fakta sederhana yang diturunkan langsung dari Definisi 2.1.3.1 adalah sebagai berikut:

$$a|0, 1|a, \text{ dan } a|a \text{ untuk } a \neq 0$$

Fakta $a|0$ dapat dijelaskan bahwa bilangan 0 selalu habis dibagi oleh bilangan apa pun yang tidak nol. Fakta $1|a$ mengatakan bahwa 1 merupakan faktor atau pembagi dari bilangan apapun termasuk bilangan 0. Fakta $a|a$ menyatakan bahwa bilangan tidak nol selalu habis membagi dirinya sendiri dengan hasil baginya adalah 1.

Berdasarkan pengertian keterbagian bilangan terdapat pada Definisi 2.1.3.1, maka berikut ini akan diberikan Teorema tentang keterbagian bilangan.

Teorema 2.1.3.1. Untuk setiap $a, b, c \in \mathbb{Z}$ berlaku pernyataan berikut

1. $a|1$ jika dan hanya jika $a = 1$ atau $a = -1$.
2. Jika $a|b$ dan $c|d$ maka $ac|bd$.
3. Jika $a|b$ dan $b|c$ maka $a|c$.
4. $a|b$ dan $b|a$ jika dan hanya jika $a = b$ atau $a = -b$.
5. Jika $a|b$ dan $b \neq 0$, maka $|a| < |b|$.
6. Jika $a|b$ dan $a|c$, maka $a|(bx + cy)$ untuk sebarang bilangan bulat x dan y (Sukirman, 1997).

Bukti

1. Jika $a = 1$ atau $a = -1$,maka jelas bahwa $a|1$, sesuai penjelasan sebelumnya. Sebaliknya, diketahui $a|1$ berarti ada $k \in \mathbb{Z}$ sehinga $1 = ka$. Persamaan ini hanya dipenuhi oleh dua kemungkinan berikut: $k = 1$, $a = 1$ atau $k = -1, a =$

-1 . Jadi berlaku jika $a|1$ maka $a = 1$ atau $a = -1$, sehingga terbukti $a|1$ jika hanya jika $a = 1$ atau $a = -1$.

2. Diketahui $a|b$ dan $c|d$ jadi terdapat $k_1, k_2 \in \mathbb{Z}$ sehingga $b = k_1 a$ dan $d = k_2 c$. Dengan mengalikan kedua persamaan tersebut diperoleh :

$$bd = (k_1 k_2)ac,$$

yaitu $ac|bd$.

3. Diketahui $a|b$ dan $b|c$,maka terdapat $k_1, k_2 \in \mathbb{Z}$ sehingga

$$b = k_1 a \quad (2.1)$$

dan

$$c = k_2 b \quad (2.2)$$

Substitusi persamaan (2.1) ke persamaan (2.2), diperoleh

$c = k_2 b = k_2(k_1 a) = (k_1 k_2)a$. Jadi $a|c$.

4. Diketahui

$$a = k_1 b \quad (2.3)$$

dan

$$b = k_2 a \quad (2.4),$$

Untuk suatu $k_1, k_2 \in \mathbb{Z}$

Persamaan (2.3) dikalikan dengan persamaan (2.4), diperoleh $ab = (k_1 k_2)(ab)$. Oleha karena itu $k_1 k_2 = 1$, yakni $k_1 = k_2 = 1$ atau $k_1 = k_2 = -1$, jadi terbukti $a = b$ atau $a = -b$.

5. Diberikan $b = ac$ untuk suatu $c \in \mathbb{Z}$. Diambil nilai mutlaknya $|b| = |ac| = |a||c|$. Karena $b \neq 0$ maka $|c| \geq 1$. Sehingga diperoleh $|b| = |a||c| \geq |a|$.

6. Diketahui $a|b$ dan $a|c$, maka terdapat $k_1, k_2 \in \mathbb{Z}$ sedemikian sehingga $b = k_1 a$ dan $c = k_2 a$. Untuk sebarang $x, y \in \mathbb{Z}$ berlaku

$$bx + cy = k_1 ax + k_2 ay = (k_1 x + k_2 y)a$$

yang berarti $a|(bx + cy)$. ■

Pernyataan terakhir Teorema 2.1.3.1 berlaku juga untuk berhingga banyak bilangan yang dibagi oleh *a*, yaitu $a|b_k, k = 1, \cdots, n$ yaitu:

$$a|(b_1 x_1 + b_2 x_2 + \cdots + b_n x_n)$$

untuk setiap bilangan bulat $x_1, x_2, \cdots, x_n$. Selanjutnya, akan dibahas pengertian faktor persekutuan terbesar.

Definisi 2.1.3.2. Misalkan *a* dan *b* dua bilangan bulat dengan minimal salah satunya tidak nol. Faktor persekutuan terbesar (FPB) atau *greatest common divisor* (gcd) dari *a* dan *b* adalah bilangan bulat *d* yang memenuhi

1**.** $d|a$ dan $d|b$;

2. Jika $c|a$ dan $c|d$ maka $c \leq d$.

Dari Definisi 2.1.3.2, kondisi 1 menyatakan bahwa *d* adalah faktor persekutuan dan kondisi 2 menyatakan bahwa *d* adalah faktor persekutuan terkecil di antara semua factor persekutuan yang ada. Selanjutnya, jika *d* faktor persekutuan terbesar dari *a* dan *b* akan ditulis *d* = gcd(a,b) (Sukirman, 1997).

2.1.4 Modulo

Modulo merupakan salah satu struktur yang digunakan pada gcd**.**

Definisi 2.1.4.1. Misalkan *a* adalah bilangan bulat dan *m* adalah bilangan bulat > 0. Operasi *a* mod *m* (dibaca "*a* modulo *m*") memberikan sisa jika *a* dibagi dengan m.

Notasi: a mod $m = r$ sedemikian sehingga $a = mq + r$, dengan $0 \leq r < m$. Bilangan m disebut modulus atau modulo, dan hasil aritmetika modulo m terletak di dalam himpunan $\{0, 1, 2, \ldots, m-1\}$ (Grillet, 2007).

Contoh. Beberapa hasil operasi dengan operator modulo:

23 mod 5 = 3 (23 = 5 • 4 + 3)

27 mod 3 = 0 (27 = 3 • 9 + 0)

Definisi 2.1.4.2 Misalkan a dan b adalah bilangan bulat dan m bilangan bulat dengan $m > 0$, a kongruen dengan b mod m, dituliskan dengan $a \equiv b \pmod{m}$ jika m habis membagi $a - b$. Jika a tidak kongruen dengan b dalam modulus m, maka dapat ditulis $a \not\equiv b \pmod{m}$ (Grillet, 2007).

Contoh .

$17 \equiv 2 \pmod{3}$ (3 habis membagi 17 – 2 = 15)

$12 \not\equiv 2 \pmod{7}$ (7 tidak habis membagi 12 -2 =10)

Kekongruenan $a \equiv b \pmod{m}$ dapat pula dituliskan dalam hubungan

$$a = b + km$$

yang dalam hal ini k adalah bilangan bulat.

Contoh

$17 \equiv 2 \pmod{3}$ dapat ditulis sebagai $17 = 2 + 5 \cdot 3$

$-7 \equiv 15 \pmod{11}$ dapat ditulis sebagai $-7 = 15 + (-2)11$

Contoh

Beberapa hasil operasi dengan relasi kongruensi berikut:

23 mod 5 = 3 dapat ditulis sebagai $23 \equiv 3 \pmod{5}$

27 mod 3 = 0 dapat ditulis sebagai $27 \equiv 0 \pmod{3}$

Berdasarkan pengertian kongruen yang terdapat pada Definisi 2.4.1.1, maka berikut ini akan diberikan teorema tentang kongruen.

Teorema 2.1.4.1. Misalkan m adalah bilangan bulat positif.

1. Jika $a \equiv b \pmod{m}$ dan c adalah sebarang bilangan bulat maka

   (i) $(a + c) \equiv (b + c) \pmod{m}$

   (ii) $ac \equiv bc \pmod{m}$

   (iii) $a^p \equiv b^p \pmod{m}$ untuk suatu bilangan bulat tak negatif p.

2. Jika $a \equiv b \pmod{m}$ dan $c \equiv d \pmod{m}$, maka

   (i) $(a + c) \equiv (b + d) \pmod{m}$

   (ii) $ac \equiv bd \pmod{m}$

(Grillet, 2007).

Bukti:

1. (i) $a \equiv b \pmod{m}$ berarti $a = b + km$ untuk suatu $k \in \mathbb{Z}$

   Untuk sebarang $c \in \mathbb{Z}$, diperoleh

   $$a + c = b + c + km$$

   $$\Leftrightarrow a + c = (b + c) (\mathrm{mod}\, m)$$

   (ii) $a \equiv b \pmod{m}$ berarti:

   $$a = b + km, \text{ untuk suatu } k \in \mathbb{Z}$$

   $$\Leftrightarrow a - b = km$$

   $$\Leftrightarrow (a - b)c = ckm$$

   $$\Leftrightarrow ac - bc = ckm$$

   $$\Leftrightarrow ac = bc + ckm$$

   $$\Leftrightarrow ac = bc + lm \text{ , dengan } l = ck$$

   $$\Leftrightarrow ac \equiv bc \pmod{m}$$

(iii) $a \equiv b$ (mod m) berarti $a = b + km$ dengan $k \in \mathbb{Z}$

$p \in \mathbb{Z}^+ \cup \{0\}$

$a^p = (b + km)^p$

$\Leftrightarrow a^p = b^p + \binom{p}{1} b^{p-1} k + \binom{p}{2} b^{p-2} k^2 m + \cdots + \binom{p}{p-1} b(km)^{p-1} + (km)^p$

$= b^p + \{\binom{p}{1} b^{p-1} km + \binom{p}{2} b^{p-2} (km)^2 + \cdots + \binom{p}{p-1} bk^{p-1} m^{p-2} + k^p m^{p-1}\} m$

$\Leftrightarrow a^p \equiv b^p (\text{mod}) m$

2. (i) $a \equiv b$ (mod m) $\Leftrightarrow a = b + k_1 m$, untuk suatu $k_1 \in \mathbb{Z}$

$c \equiv d$ (mod m) $\Leftrightarrow c = d + k_2 m$, untuk suatu $k_2 \in \mathbb{Z}$

$\Leftrightarrow (a + c) = (b + d) + (k_1 + k_2) m$

$\Leftrightarrow (a + c) = (b + d) + km \qquad (k = k_1 + k_2)$

$\Leftrightarrow (a + c) \equiv (b + d) (\text{mod } m)$

(ii) $a \equiv b$ (mod m) $\Leftrightarrow a = b + mk$, untuk suatu $k \in \mathbb{Z}$

$c \equiv d$ (mod m) $\Leftrightarrow c = d + ml$, untuk suatu $l \in \mathbb{Z}$

$\Leftrightarrow a \cdot c = (b + mk)(d + ml)$

$\Leftrightarrow a \cdot c = bd + blm + kdm + klm^2$

$\Leftrightarrow a \cdot c = bd + (bl + kd + klm) m$

$\Leftrightarrow a \cdot c \equiv bd (\text{mod } m)$ ■

2.1.5 Bilangan Prima

Definisi 2.1.5.1. Sebuah bilangan bulat $p > 1$ disebut bilangan prima, jika dan hanya jika habis dibagi dengan 1 dan bilangan itu sendiri atau p (Burton,1976).

2.2 Ring

Definisi 2.2.1.1 Misalkan R himpunan sembarang tak kosong dan + serta • adalah sebarang dua operasi pada R. Himpunan < R, +, • > disebut ring jika:

1. < R, + > grup abelian
2. Terhadap operasi • berlaku:
   a. tertutup (untuk setiap $r_1, r_2 \in R$) $r_1 \bullet r_2 \in R$
   b. asosiatif (untuk setiap $r_1, r_2 \in R$) $(r_1 \bullet r_2) \bullet r_3 = r_1 \bullet (r_2 \bullet r_3)$
3. Terhadap operasi + dan • dipenuhi:
   a. distributif kanan (untuk setiap $r_1, r_2, r_3 \in R$)$r_1 \bullet (\mathrm{r}_2 + \mathrm{r}_3) = (\mathrm{r}_1 \bullet \mathrm{r}_2) + (\mathrm{r}_1 \bullet \mathrm{r}_3)$
   b. distributif kiri (untuk setiap $r_1, r_2, r_3 \in R$)$(r_1 + r_2) \bullet r_3 = (r_1 \bullet r_3) + (r_2 \bullet r_3)$ (Fraleight, 2000).

Contoh :

1. Himpunan $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$ adalah ring.
2. Misal R adalah himpunan fungsi yang bernilai real dalam selang interval [0, 1]. Penjumlahan dan perkalian dari dua fungsi f, g diDefinisikan sebagai berikut $(f + g)\ (t) = f(t) + g\ (t)$, dan $(f \cdot g)\ (t) = f(t) \cdot g(t)$. Dengan pendefinisian ini R merupakan ring.

2.3 Daerah Integral dan Lapangan

Definisi 2.3.1. Ring komutatif dengan elemen satuan yang tak memuat pembagi nol disebut daerah integral (Fraleight, 2000).

Definisi 2.3.2. Ring Divisi adalah ring dengan setiap elemen tak nolnya adalah unit.

Definisi 2.3.3. Lapangan adalah ring divisi yang komutatif .

2.4 Unit

Definisi 2.4.1. Misalkan D adalah Daerah Integral dan 1 adalah elemen satuan di $D, u \in D$ merupakan unit jika dan hanya jika u membagi 1 sedemikian sehingga $1 = u.u^{-1}$ untuk suatu $u^{-1} \in D$. Dengan kata lain, u mempunyai invers terhadap operasi perkalian pada D (Dummit, 2004).

Contoh.

Elemen unit di $\mathbb{Z}$ adalah 1 dari -1. karena $1|1$ (1 = 1 . 1)

dan karena $-1|1$ (1 = (-1) (-1)) $\Rightarrow$ 1 = $u.u^{-1}$

2.5 Bilangan *Irreducible*

Definisi 2.5.1. Misalkan $p \neq 0$ dan p bukan unit di daerah integral D. Elemen p dikatakan *irreducible* jika $p = a \cdot b$ di D, maka a unit atau b unit di D

(Dummit, 2004).

Contoh. Misalkan D suatu daerah integral $p, q \in D$, $p, q \in$ *irreducible* dan p, q saling berasosiasi . Karena

$$p = q \cdot u$$

$$p = q \cdot u \cdot u^{-1}$$

$$p \cdot u^{-1} = q$$

Sehingga, q elemen *irreducible* (Dummit, 2004).

2.6 Lapangan Quadratic Q[$\sqrt{d}$]

Misalkan terdapat lapangan

$$\mathbb{Q}[\sqrt{d}] = \{m + n\sqrt{d} : m, n \in \mathbb{Q}\}$$

Berikut ini akan ditunjukkan bahwa himpunan $\mathbb{Q}[\sqrt{d}]$ dengan operasi penjumlahan dan perkalian membentuk ring.

Teorema 2.6.1. Jika diberikan himpunan $\mathbb{Q}[\sqrt{d}]$ sebagai berikut

$\mathbb{Q}[\sqrt{d}] = \{m + n\sqrt{d}\ ;\ m, n \in \mathbb{Q}\}$

Pada $\mathbb{Q}[\sqrt{d}]$ didefinisikan dua operasi sebagai berikut

(i) Operasi penjumlahan $(+^*)$, yaitu

$$\left(m_1 + n_1\sqrt{d}\right) +^* \left(m_2 + n_2\sqrt{d}\right) = (m_1 + n_1) + (m_2 + n_2)\sqrt{d}$$

(ii) Perkalian $(\cdot^*)$

$$\left(m_1 + n_1\sqrt{d}\right) \cdot^* \left(m_2 + n_2\sqrt{d}\right)$$

$$= (m_1 m_2 - n_1 n_2 d) + (m_1 n_2 + m_2 n_1)\sqrt{d}$$

Maka, $\langle \mathbb{Q}[\sqrt{d}], +^*, \cdot^* \rangle$ membentuk ring

Bukti

1. Harus dibuktikan bahwa $\langle \mathbb{Q}[\sqrt{d}], +^*, \cdot^* \rangle$ grup Abel atau grup komutatif

   (i) Diberikan sebarang $\left(m_1 + n_1\sqrt{d}\right), \left(m_2 + n_2\sqrt{d}\right) \in \mathbb{Q}[\sqrt{d}]$, maka diperoleh

   $\left(m_1 + n_1\sqrt{d}\right) +^* \left(m_2 + n_2\sqrt{d}\right) = (m_1 + n_1) + (m_2 + n_2)\sqrt{d}$

   Karena $(m_1 + n_1) \in \mathbb{Q}$ dan $(m_2 + n_2) \in \mathbb{Q}$, maka

   $(m_1 + n_1) +^* (m_2 + n_2)\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$

   Jadi, operasi $(+^*)$ tertutup pada $\mathbb{Q}[\sqrt{d}]$.

(ii) Diberikan sebarang $(m_1 + n_1\sqrt{d}), (m_2 + n_2\sqrt{d}), (m_3 + n_3\sqrt{d}) \in$

$\mathbb{Q}[\sqrt{d}]$, maka diperoleh

$[(m_1 + n_1\sqrt{d}) +^* (m_2 + n_2\sqrt{d})] +^* (m_3 + n_3\sqrt{d})$

$= [(m_1 + m_2) + (n_1 + n_2)\sqrt{d}] +^* (m_3 + n_3\sqrt{d})$

$= (m_1 + m_2) + (n_1 + n_2)\sqrt{d} + (m_3 + n_3\sqrt{d})$

$= (m_1 + m_2) +^* (m_3 + (n_1 + n_2 + n_3)\sqrt{d})$

$= m_1 + m_2 + m_3 + (n_1 + n_2 + n_3)\sqrt{d}$

$= (m_1 + n_1\sqrt{d}) +^* [\, (m_2 + n_2) +^* (m_3 + n_3)\sqrt{d}]$

$= (m_1 + n_1\sqrt{d}) +^* [\, (m_2 + n_2\sqrt{d}) +^* (m_3 + n_3\sqrt{d})]$

Jadi operasi $(+^*)$ bersifat asosiatif pada $\mathbb{Q}[\sqrt{d}]$.

(iii) Diberikan sebarang $m_1 + n_1\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$, maka terdapat

$(m_2 + n_2\sqrt{d}) \in \mathbb{Q}[\sqrt{d}]$ sehingga

$(m_1 + n_1\sqrt{d}) +^* (m_2 + n_2\sqrt{d})$

$= (m_2 + n_2\sqrt{d}) +^* (m_1 + n_1\sqrt{d})$

$= m_1 + n_1\sqrt{d}$

Dari persamaan

$(m_1 + n_1\sqrt{d}) +^* (m_2 + n_2\sqrt{d}) = m_1 + n_1\sqrt{d}$

$\Leftrightarrow (m_1 + m_2) + (n_1 + n_2)\sqrt{d} = m_1 + n_1\sqrt{d}$

$\Leftrightarrow m_1 + m_2 = m_1$ dan $n_1 + n_2 = n_1$

$\Leftrightarrow m_2 = 0$ dan $n_2 = 0$

Jadi $(m_2 + n_2\sqrt{d}) = 0 + 0\sqrt{d}$ merupakan elemen netral pada $\mathbb{Q}[\sqrt{d}]$.

(iv) Untuk setiap $m_1 + n_1\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$, terdapat $(m_2 + n_2\sqrt{d}) \in \mathbb{Q}[\sqrt{d}]$ sehingga

$$\begin{aligned}(m_1 + n_1\sqrt{d}) +^* (m_2 + n_2\sqrt{d}) &= (m_2 + n_2\sqrt{d}) +^* (m_1 + n_1\sqrt{d}) \\ &= 0 + 0\sqrt{d}\end{aligned}$$

Dari persamaan

$(m_1 + n_1\sqrt{d}) +^* (m_2 + n_2\sqrt{d}) = 0 + 0\sqrt{d}$

$\Leftrightarrow (m_1 + m_2) + (n_1 + n_2)\sqrt{d} = 0 + 0\sqrt{d}$

$\Leftrightarrow m_1 + m_2 = 0$ dan $n_1 + n_2 = 0$

$\Leftrightarrow m_2 = -m_1$ dan $n_2 = -n_1$

Jadi $-(m_1 + n_1\sqrt{d})$ merupakan invers pada setiap $m_1 + n_1\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$.

(v) Diberikan sebarang $(m_1 + n_1\sqrt{d}), (m_2 + n_2\sqrt{d}) \in \mathbb{Q}[\sqrt{d}]$, maka diperoleh

$$\begin{aligned}(m_1 + n_1\sqrt{d}) +^* (m_2 + n_2\sqrt{d}) &= (m_1 + m_2) + (n_1 + n_2)\sqrt{d} \\ &= (m_1 + m_2) + n_1\sqrt{d} + n_2\sqrt{d} \\ &= (m_1 + n_1\sqrt{d}) +^* (m_2 + n_2\sqrt{d})\end{aligned}$$

Jadi operasi $(+^*)$ komutatif.

Dari (i) – (v) disimpulkan $\langle \mathbb{Q}[\sqrt{d}], +^* \rangle$ grup komutatif.

2. Terhadap operasi perkalian$(\cdot^*)$.

(i) Diberikan sebarang $(m_1 + n_1\sqrt{d}), (m_2 + n_2\sqrt{d}) \in \mathbb{Q}[\sqrt{d}]$, maka

$(m_1 + n_1\sqrt{d}) \cdot^* (m_2 + n_2\sqrt{d}) = (m_1m_2 - n_1n_2) + (m_1n_2 + n_1m_2)\sqrt{d}$

Karena $(m_1m_2 - n_1n_2) \in \mathbb{Q}[\sqrt{d}]$ dan $(m_1n_2 + n_1m_2) \in \mathbb{Q}[\sqrt{d}]$, maka $(m_1m_2 - n_1n_2) + (m_1n_2 + n_1m_2)\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$.

Jadi, operasi $(\cdot^*)$ tertutup pada $\mathbb{Q}[\sqrt{d}]$.

(ii) Diberikan sebarang $(m_1 + n_1\sqrt{d}), (m_2 + n_2\sqrt{d}), (m_3 + n_3\sqrt{d}) \in \mathbb{Q}[\sqrt{d}]$, maka diperoleh

$$[(m_1 + n_1\sqrt{d}) \cdot^* (m_2 + n_2\sqrt{d})] \cdot^* (m_3 + n_3\sqrt{d})$$

$$= [(m_1m_2 - n_1n_2) + (m_1n_2 + n_1m_2)\sqrt{d}] \cdot (m_3 + n_3\sqrt{d})$$

$$= [(m_1m_2 - n_1n_2)m_3 + (-\, m_1n_2 + n_1m_2)n_3]$$

$$+[(m_1m_2 + n_1n_2)n_3 + (m_1n_2 + n_1m_2)m_3]\sqrt{d}$$

$$= m_1m_2m_3 - n_1n_2m_3 - m_1n_2n_3 - n_1m_2n_3$$

$$+m_1m_2n_3\sqrt{d} + n_1n_2n_3\sqrt{d} + m_1n_2m_3\sqrt{d} + n_1m_2m_3\sqrt{d}$$

$$= m_1m_2m_3 - m_1n_2n_3 + n_1m_2m_3\sqrt{d} - n_1n_2n_3\sqrt{d} + m_1m_2n_3\sqrt{d}$$

$$+m_1n_2m_3\sqrt{d} - n_1m_2n_3 - n_1n_2m_3$$

$$= m_1 + n_1\sqrt{d}[(m_2m_3 - n_2n_3) + (m_2n_3 + n_2m_3)\sqrt{d}]$$

$$= m_1 + n_1\sqrt{d}\,(m_2m_3 - n_2n_3 + m_2n_3 + n_2m_3)$$

$$= m_1 + n_1\sqrt{d}\,[(m_2 + n_2\sqrt{d})(m_3 + n_3\sqrt{d})]$$

3. Terhadap operasi $+^*$ dan $\cdot^*$.

(i) Diberikan sebarang $(m_1 + n_1\sqrt{d}), (m_2 + n_2\sqrt{d}), (m_3 + n_3\sqrt{d}) \in \mathbb{Q}[\sqrt{d}]$, maka diperoleh

$$[(m_1 + n_1\sqrt{d}) +^* (m_2 + n_2\sqrt{d})] \cdot^* (m_3 + n_3\sqrt{d})$$

$$= [(m_1 + n_1) +^* (m_2 + n_2)\sqrt{d}] \cdot^* (m_3 + n_3\sqrt{d})$$

$$= [(m_1 + n_1)n_3 - \ (m_2 + n_2)m_3]\sqrt{d} +^*$$

$$\left[(m_1+n_1)m_3-(m_2+n_2)n_3\sqrt{d}\right]$$

$$= m_1n_3\sqrt{d}+m_2n_3\sqrt{d}-n_1m_3\sqrt{d}-+m_1m_3+m_2m_3$$

$$+n_1n_3+n_2n_3$$

$$=(m_1m_3+m_1n_3)\sqrt{d}+n_1m_3\sqrt{d}-n_1n_3\sqrt{d}+m_2m_3+m_2n_3\sqrt{d}$$

$$+n_2m_3\sqrt{d}-n_2n_3\sqrt{d}$$

$$=(m_1+n_1\sqrt{d})\cdot^*(m_3+n_3\sqrt{d})+^*(m_2+n_2\sqrt{d})\cdot^*(m_3+n_3\sqrt{d})$$

(ii) Diberikan sebarang $(m_1+n_1\sqrt{d}),(m_2+n_2\sqrt{d}),(m_3+n_3\sqrt{d})\mathbb{Q}[\sqrt{d}]$, maka diperoleh

$$(m_1+n_1\sqrt{d})\cdot^*\left[(m_2+n_2\sqrt{d})+^*(m_3+n_3\sqrt{d})\right]$$

$$=(m_1+n_1\sqrt{d})\cdot^*\left[(m_2+m_3)+^*(n_2+n_3)\sqrt{d}\right]$$

$$=[m_1(m_2+m_3)-n_1(n_2+n_3)]+^*[m_1(n_2+n_3)+n_1(m_2+m_3)]\sqrt{d}$$

$$=m_1m_2+m_1m_3-n_1n_2-n_1n_3+(m_1n_2+m_1n_3)\sqrt{d}$$

$$+(n_1m_2+n_1m_3)\sqrt{d}$$

$$=m_1m_2+m_1n_2\sqrt{d}+n_1m_2\sqrt{d}-n_1n_2+m_1m_3+m_1n_3\sqrt{d}$$

$$+n_1m_3\sqrt{d}-n_1n_3$$

$$=(m_1+n_1\sqrt{d})\cdot^*(m_2+n_2\sqrt{d})+^*(m_1+n_1\sqrt{d})\cdot^*(m_3+n_3\sqrt{d}) \qquad \blacksquare$$

Selanjutnya ring $\mathbb{Q}[\sqrt{d}]$ merupakan daerah integral, yang dituliskan dalam teorema berikut :

Teorema 4.1.2

Ring $\mathbb{Q}[\sqrt{d}]$ merupakan daerah integral

Bukti :

Untuk membuktikan ring $\mathbb{Q}[\sqrt{d}]$ daerah integral cukup dibuktikan

(i) Ring $\mathbb{Q}[\sqrt{d}]$ komutatif

Diberikan sebarang $(m_1 + n_1\sqrt{d}), (m_2 + n_2\sqrt{d}) \in \mathbb{Q}[\sqrt{d}]$, maka diperoleh

$(m_1 + n_1\sqrt{d}) \cdot (m_2 + n_2\sqrt{d}) \in \mathbb{Q}[\sqrt{d}]$

$= (m_1m_2 - n_1n_2) + (m_1n_2 + n_1m_2)\sqrt{d}$

$= (m_2m_1 - n_2n_1) + (n_2m_1 + m_2n_1)\sqrt{d}$

$= (m_2 + n_2\sqrt{d}) \cdot (m_1 + n_1\sqrt{d})$

(ii) Ring $\mathbb{Q}[\sqrt{d}]$ tidak memuat pebagi nol

Ring $\mathbb{Q}[\sqrt{d}]$ tidak memuat pembagi nol, sebab jika diambil sebarang

$(m_1 + n_1\sqrt{d}) \neq 0, (m_2 + n_2\sqrt{d}) \neq 0$, maka

$(m_1 + n_1\sqrt{d})\,(m_2 + n_2\sqrt{d}) \neq 0$ ■