# Bab 12

# Matematika V - Algebraic Number

Di bab ini kita akan bahas konsep *algebraic number*. Kita mulai dengan penjelasan konsep ruang vektor dan *module*, diikuti oleh *separable field extension*, kemudian konsep *norm* dan *trace*, dan dikulminasi dengan *algebraic number theory*.

## 12.1 Ruang Vektor dan Module

Konsep ruang vektor banyak dipergunakan dalam ilmu pengetahuan dan teknologi, meskipun banyak orang yang menggunakannya tanpa menyadari struktur aljabar yang terdapat didalamnya. Kita akan rumuskan struktur aljabar untuk ruang vektor dan bahas konsep *module*. Jika $K$ adalah suatu *field*, maka suatu $K$*-vector space* $V$ adalah suatu *Abelian group* dengan operasi $+$ ditambah dengan *scalar multiplication*

$$\circ : K \times V \longrightarrow V$$

dimana untuk setiap $\alpha, \beta \in K$ dan $a, b \in V$:

- $\alpha \circ (a + b) = \alpha \circ a + \alpha \circ b$,
- $(\alpha + \beta) \circ a = \alpha \circ a + \beta \circ a$,
- $(\alpha \cdot \beta) \circ a = \alpha \circ (\beta \circ a)$, dan
- $1 \circ a = a$.

Sebagai contoh, jika $K$ merupakan suatu *field* dan kita definisikan

$$\begin{aligned}(v_1, v_2) + (w_1, w_2) &= (v_1 + v_2, w_1 + w_2),\\ \alpha \circ (v_1, v_2) &= (\alpha v_1, \alpha v_2),\end{aligned}$$

maka $K^2$ merupakan suatu ruang vektor ($K$-*vector space*). Berbagai konsep aljabar linear didefinisikan untuk ruang vektor sebagai berikut.

**Definisi 28** *Jika $V$ adalah suatu $K$-vector space dan $B$ adalah subset dari $V$, maka*

1. *$B$ linearly independent jika untuk setiap $n \in \mathbf{N}^+$, $v_1, v_2, \ldots, v_n \in B$ dimana setiap $v_i$ berbeda dan $\lambda_1, \lambda_2, \ldots, \lambda_n \in K$,*

$$\sum_{i=1}^{n} \lambda_i \cdot v_i = 0 \Longrightarrow \lambda_1 = \lambda_2 = \ldots = \lambda_n = 0.$$

2. *$B$ adalah generator untuk $V$ jika untuk setiap $v \in V$ terdapat $n \in \mathbf{N}^+$, $v_1, v_2, \ldots, v_n \in B$ dan $\lambda_1, \lambda_2, \ldots, \lambda_n \in K$, dimana*

$$v = \sum_{i=1}^{n} \lambda_i.$$

3. *$B$ adalah basis untuk $V$ jika $B$ adalah generator untuk $V$ yang linearly independent.*

Konsep *subspace* untuk ruang vektor dapat didefinisikan sebagai berikut. Jika $V$ adalah suatu $K$-*vector space* dan $U$ adalah subset non-kosong dari $V$ yang *closed* untuk pertambahan (jadi $U$ adalah *subgroup* dari $V$) dan $U$ *closed* untuk *scalar multiplication* (jika $\alpha \in K$ dan $a \in U$, $\alpha \circ a \in U$), maka $U$ merupakan *subspace* dari $V$.

Berikutnya kita bahas konsep *module*. Konsep *module* atas suatu *ring* sangat mirip dengan konsep ruang vektor atas suatu *field* (untuk *module*, struktur aljabar *scalar* adalah *ring* sedangkan untuk ruang vektor, struktur aljabar *scalar* adalah *field*). Jika $R$ adalah suatu *ring*, maka suatu $R$-*module* $M$ adalah suatu *Abelian group* dengan operasi + ditambah dengan *scalar multiplication*

$$\circ : R \times M \longrightarrow M$$

dimana untuk setiap $\alpha, \beta \in R$ dan $a, b \in M$:

- $\alpha \circ (a + b) = \alpha \circ a + \alpha \circ b$,
- $(\alpha + \beta) \circ a = \alpha \circ a + \beta \circ a$,

- $(\alpha \cdot \beta) \circ a = \alpha \circ (\beta \circ a)$, dan
- $1 \circ a = a$.

Berikut adalah beberapa contoh dari *module*:

- Jika $R$ adalah suatu *ring* dan $I$ adalah suatu *ideal* dalam $R$ maka tidak terlalu sulit untuk melihat bahwa $I$ adalah suatu $R$-*module*.
- Untuk $M = R^n$ berupa produk *finite* (*finite direct product*) dari *ring* $R$, jika kita abaikan perkalian dalam $M$ dan definisikan $\alpha \circ (\beta_1, \ldots, \beta_n) = (\alpha\beta_1, \ldots, \alpha\beta_n)$, maka $M$ merupakan $R$-*module* yang dinamakan *free* $R$-*module* dengan *rank* $n$.

Jika $M$ merupakan suatu $R$-*module*, $N$ merupakan *additive subgroup* dari $M$, dan $N$ *closed* untuk *scalar multiplication* (jika $\alpha \in R$ dan $a \in N$, $\alpha \circ a \in N$) maka $N$ adalah *submodule* dari $M$. Jika $B$ merupakan subset dari $M$ maka terdapat *submodule* terkecil $N$ yang mencakup $B$. $N$ terdiri dari kombinasi linear

$$\sum_{i=1}^{n} \alpha_i \circ a_i$$

dimana $\alpha_i \in R$ dan $a_i \in B$. $N$ adalah *submodule* dengan *generator* $B$ dalam $M$. Seperti halnya dengan ruang vektor, konsep *linear independence* juga berlaku untuk *module*. Jika $B$ *linearly independent* maka $B$ merupakan basis untuk $N$.

## 12.2 Separable Field Extension

Konsep *separable extension* kita bahas karena akan diperlukan dalam pembahasan *norm* dan *trace* pada bagian 12.3.

**Definisi 29** *Suatu field extension $L/K$ disebut separable jika untuk setiap $a \in L$, $\min_K^a$ tidak memiliki akar ganda dalam $L$.*

*Field extension* yang bukan berupa *separable extension* boleh dikatakan merupakan kekecualian atau anomali. Dalam buku ini, kita hanya peduli dengan *field extension* yang *separable*. Kita akan tunjukkan bahwa setiap *algebraic field extension* terhadap *field* dengan *characteristic* 0 dan setiap *algebraic field extension* terhadap *finite field* merupakan *separable field extension*. Untuk itu, kita akan gunakan konsep *perfect field*.

**Definisi 30** *Suatu field $K$ disebut perfect field jika setiap algebraic field extension $L/K$ merupakan suatu separable field extension.*

Kita juga akan gunakan konsep *square-free* (bebas dari kuadrat) dan derivatif dari *polynomial*.

**Definisi 31** *Jika $f$ merupakan polynomial sebagai berikut:*

$$f = \sum_{i=0}^{n} a_i x^i,$$

*maka derivatif dari $f$ adalah $f'$ sebagai berikut:*

$$f' = \sum_{i=1}^{n} i a_i x^{i-1}.$$

**Definisi 32** *Suatu polynomial $f$ disebut square-free jika tidak terdapat suatu polynomial non-konstan $g$ dimana $g^2 | f$.*

**Teorema 58** *Jika $K$ merupakan suatu field, $f \in K[x]$ dan tidak terdapat suatu polynomial non-konstan $g$ dimana $g|f$ dan $g|f'$, maka $f$ square-free.*

Untuk membuktikan teorema 58 mari kita lihat apa konsekuensinya jika $f$ tidak *square-free*, jadi terdapat *polynomial* $g, h \in K[x]$ dimana $g$ non-konstan dan $f = g^2 h$. Karena

$$f' = 2gg'h + g^2 h',$$

maka $g|f$ dan $g|f'$, suatu kontradiksi. Jadi jika tidak terdapat *polynomial* non-konstan $g$ dimana $g|f$ dan $g|f'$ maka $f$ *square-free*, membuktikan teorema 58. Kebalikannya (jika $f \in F[x]$ *square-free* maka tidak terdapat *polynomial* non-konstan $g$ dimana $g|f$ dan $g|f'$) tidak selalu benar, tetapi berlaku jika *characteristic* dari $F$ adalah 0 atau $F$ merupakan *finite field*. Ini akan kita tunjukkan, tetapi sebelumnya kita perlu beberapa teorema mengenai $f'$.

**Teorema 59** *Jika $F$ adalah suatu field dengan characteristic 0 dan $f \in F[x]$ maka $f' = 0$ jika dan hanya jika $f$ merupakan konstan ($f \in F$).*

Mari kita buktikan teorema 59. Jika $f$ dituliskan sebagai $f = \sum_{i=0}^{n} a_i x^i$ maka $f'$ dapat dituliskan sebagai

$$f' = \sum_{i=1}^{n} i a_i x^{i-1}$$

dan $f' = 0$ jika dan hanya jika setiap $a_i = 0$ untuk $1 \leq i \leq n$ atau dengan kata lain $f$ merupakan konstan.

**Teorema 60** *Jika $F$ adalah suatu field dengan characteristic $p \neq 0$ dan $f \in F[x]$ maka $f' = 0$ jika dan hanya jika terdapat $g \in F[x]$ dimana $f = g(x^p)$.*

Untuk *field* dengan *characteristic* $p \neq 0$, $f' = 0$ jika dan hanya jika setiap $a_i = 0$ untuk semua $i$ dimana $p \not| i$, jadi

$$f = \sum_{i=0}^{m'} a_{ip} x^{ip} = \sum_{i=0}^{m'} a_{ip} (x^p)^i,$$

atau, dengan $g = \sum_{i=0}^{m'} a_{ip} x^i$,

$$f = g(x^p),$$

membuktikan teorema 60.

**Teorema 61** *Jika $F$ merupakan finite field dengan characteristic $p \neq 0$ dan $f \in F[x]$ maka $f' = 0$ jika dan hanya jika terdapat $g \in F[x]$ dimana $f = g^p$.*

Mari kita buktikan teorema 61. Jika $f = g^p$, maka

$$\begin{aligned} f' &= p \cdot g' g^{p-1} \\ &= 0. \end{aligned}$$

Sebaliknya, jika $f' = 0$ maka menurut teorema 60 terdapat $h \in F[x]$ dimana $f = h(x^p)$. Jika $h = \sum_{i=0}^{m} a_i x^i$, kita dapat tuliskan $f$ sebagai

$$f = \sum_{i=0}^{m} a_i (x^p)^i.$$

Karena setiap elemen dari $F$ mempunyai akar pangkat $p$, maka setiap $a_i$ dapat ditulis sebagai $a_i = b_i^p$. Jadi

$$\begin{aligned} f &= \sum_{i=0}^{m} b_i^p (x^i)^p \\ &= \left( \sum_{i=0}^{m} b_i x^i \right)^p. \end{aligned}$$

Jadi dengan $g = \sum_{i=0}^{m} b_i x^i$ kita dapatkan $f = g^p$. Selesailah pembuktian teorema 61.

**Teorema 62** *Jika $F$ merupakan suatu field dengan characteristic $0$ atau $F$ merupakan suatu finite field dengan characteristic $p \neq 0$, dan $f \in F[x]$ square-free, maka tidak terdapat suatu polynomial non-konstan $g \in F[x]$ dimana $g|f$ dan $g|f'$.*

Untuk membuktikan teorema 62 mari kita lihat apa konsekuensinya jika terdapat suatu *polynomial* non-konstan $g \in F[x]$ dimana $g|f$ dan $g|f'$. Berarti terdapat suatu *polynomial* non-konstan yang *irreducible* $h \in F[x]$ dimana $h|f$ dan $h|f'$. Jadi terdapat *polynomial* $e \in F[x]$ dimana $f = he$ dan

$$f' = he' + h'e.$$

Agar $h|f'$ maka $h$ harus membagi $h'e$. Ini bisa saja terjadi jika $h' = 0$. Tetapi jika *characteristic* dari $F$ adalah 0 ini hanya bisa terjadi jika $h$ adalah suatu konstan (lihat teorema 59), suatu kontradiksi. Jika $F$ merupakan suatu *finite field* dengan *characteristic* $p \neq 0$ maka ini hanya bisa terjadi jika terdapat suatu $g \in F[x]$ dimana $f = g^p$ (lihat teorema 61), yang berarti $f$ tidak *square-free*, lagi suatu kontradiksi. Kita tinggal periksa kemungkinan lain yang dapat membuat $h|h'e$. Karena $h$ *irreducible* yang berarti $h$ adalah prima, $h|h'e$ jika $h|h'$ atau $h|e$. Tidak mungkin $h$ membagi $h'$ karena $h'$ mempunyai *degree* yang lebih kecil dari $h$. Jika $h|e$ maka terdapat suatu $d \in F[x]$ dimana $e = hd$ yang membuat $f = h^2d$, jadi $f$ tidak *square-free*, lagi suatu kontradiksi. Karena semua kemungkinan yang membuat $h|f'$ menimbulkan kontradiksi, maka konklusinya tidak terdapat suatu *polynomial* non-konstan $g \in F[x]$ dimana $g|f$ dan $g|f'$. Selesailah pembuktian teorema 62.

**Teorema 63** *Jika $F$ merupakan suatu field dengan characteristic $0$ atau $F$ merupakan suatu finite field dengan characteristic $p \neq 0$, maka $f \in F[x]$ square-free, jika dan hanya jika tidak terdapat suatu polynomial non-konstan $g \in F[x]$ dimana $g|f$ dan $g|f'$.*

Teorema 63 adalah konsekuensi teorema 58 dan teorema 62.

**Teorema 64** *Jika $F$ merupakan suatu field dan $f \in F[x]$, maka tiga proposisi berikut equivalen:*

1. *Tidak terdapat non-konstan $g \in F[x]$ dimana $g|f$ dan $g|f'$.*
2. *Untuk setiap extension field $L/F$, $f$ square-free dalam $L[x]$.*
3. *Untuk setiap extension field $L/F$, $f$ tidak memiliki akar ganda dalam $L$.*

Untuk membuktikan bahwa proposisi 2 adalah konsekuensi proposisi 1, kita gunakan fakta bahwa jika tidak terdapat non-konstan $g \in F[x]$ dimana $g|f$ dan $g|f'$ maka tidak terdapat non-konstan $h \in L[x]$ dimana $h|f$ dan $h|f'$. Ini karena jika terdapat non-konstan $h \in L[x]$ dimana $h|f$ dan $h|f'$ maka algoritma Euclid dapat digunakan untuk mendapatkan $h \in F[x]$ dimana $h|f$ dan $h|f'$ (algoritma Euclid hanya menggunakan pertambahan, perkalian dan pembagian koefisien dari $f$ dan $f'$ jadi $h$ tidak tergantung apakah sebagai *polynomial* dalam $F[x]$ atau dalam $L[x]$). Ini tentunya adalah suatu kontradiksi, jadi tidak terdapat $h \in L[x]$ dimana $h|f$ dan $h|f'$. Menggunakan teorema 58 kita dapatkan $f$

*square-free* dalam $L[x]$. Untuk membuktikan bahwa proposisi 3 adalah konsekuensi dari proposisi 2, jika $f$ memiliki akar ganda dalam $L$ maka $f$ tidak *square-free* dalam $L[x]$, suatu kontradiksi. Untuk menunjukkan bahwa proposisi 1 adalah konsekuensi dari proposisi 3, mari kita lihat apa konsekuensinya jika terdapat suatu *polynomial* non-konstan $g \in F[x]$ dimana $g|f$ dan $g|f'$. Berarti terdapat suatu *polynomial* non-konstan yang *irreducible* $h \in F[x]$ dimana $h|f$ dan $h|f'$. Jadi terdapat *polynomial* $e \in F[x]$ dimana $f = he$ dan

$$f' = he' + h'e.$$

Jadi $h|h'e$. Karena $h$ *irreducible* yang berarti $h$ prima, $h|h'$ atau $h|e$. Jika $h|e$ maka $h^2|f$ yang berarti $f$ mempunyai akar ganda dalam suatu $L$ dimana $L/F$ merupakan *field extension*, suatu kontradiksi. Jika $h|h'$ maka $h' = 0$ karena jika $h'$ mempunyai *degree* lebih kecil dari $h$ maka tidak mungkin $h|h'$, jadi $h' = 0$. Karena $h$ bukan konstan, maka ini hanya bisa terjadi jika *characteristic* dari $F$ adalah $p \neq 0$, dan $h$ dapat ditulis sebagai

$$h = \sum_{i=0}^{m} a_i x^{ip}.$$

Karena setiap elemen dari $F$ mempunyai akar pangkat $p$, maka setiap $a_i$ dapat ditulis sebagai $a_i = b_i^p$. Jadi

$$\begin{aligned} h &= \sum_{i=0}^{m} b_i^p (x^i)^p \\ &= \left( \sum_{i=0}^{m} b_i x^i \right)^p . \end{aligned}$$

Jadi $f$ mempunyai akar ganda (ada $p$ akar dari $f$ yang mempunyai nilai yang sama), suatu kontradiksi. Selesailah pembuktian teorema 64.

**Teorema 65** *Jika $F$ merupakan suatu field dan untuk setiap $f \in F[x]$, $f$ square-free jika dan hanya jika tidak terdapat suatu $g \in F[x]$ dimana $g|f$ dan $g|f'$, maka $F$ merupakan suatu perfect field.*

Mari kita buktikan teorema 65. Jika $F$ bukan merupakan *perfect field* maka terdapat suatu *algebraic field extension* $L/F$ yang bukan merupakan *separable field extension*. Jadi terdapat suatu *irreducible polynomial* (berarti *square-free*) $f \in F[x]$ yang mempunyai akar ganda dalam $L$. Berdasarkan teorema 64, terdapat suatu non-konstan $g \in F[x]$ dimana $g|f$ dan $g|f'$. Tetapi ini bertentangan dengan asumsi bahwa $f$ *square-free*. Selesailah pembuktian kita.

**Teorema 66** *Setiap field dengan characteristic* 0 *dan setiap finite field merupakan perfect field.*

Teorema ini adalah hasil kombinasi teorema 65 dengan teorema 63.

## 12.3 Norm, Trace

Kita akan bahas konsep *norm* dan *trace* untuk *separable field extension*. Kita asumsikan di bagian ini bahwa setiap *field extension* merupakan *separable field extension* terhadap suatu *perfect field*. Kita mulai dengan teorema berikut.

**Teorema 67** *Jika $K$ adalah suatu perfect field, $F$ merupakan algebraic closure dari $K$, $f(x)$ merupakan monic irreducible polynomial dalam $K[x]$ dengan degree $d$, dan $a \in F$ merupakan akar dari $f(x)$, maka terdapat tidak lebih dan tidak kurang dari $d$ ring homomorphism yang injective dari field $K(a)$ ke field $F$ dengan rumus*

- $\sigma_i(r) = r$ *untuk* $r \in K$, *dan*
- $\sigma_i(a) = a_i$

*dimana $1 \leq i \leq d$ dan $f(x)$ dapat diuraikan dalam $F[x]$ sebagai berikut:*

$$f(x) = (x - a_1)(x - a_2) \cdots (x - a_d).$$

Mari kita buktikan teorema 67. Setiap pemetaan $\sigma_i : K(a) \longrightarrow K(a_i)$ merupakan *field isomorphism*, jadi setiap $\sigma_i$ menentukan *isomorphic copy* dari $K(a)$ yang berbeda dalam $F$ (karena $K$ merupakan *perfect field*, jadi $f$ tidak memiliki akar ganda dalam $F$). Jadi sedikitnya terdapat $d$ *injective ring homomorphisms* (atau *embeddings*) dari $K(a)$ ke $F$. Untuk menunjukkan bahwa hanya terdapat $d$ *embeddings* yang telah disebutkan diatas, jika $\sigma : K(a) \longrightarrow F$ merupakan *injective ring homomorphism*, maka $\sigma(r) = r$ untuk $r \in K$ dan $\sigma(a) = \theta \in F$. Karena

$$f(x) = x^d + c_{d-1}x^{d-1} + \ldots + c_1 x + c_0,$$

maka

$$\begin{aligned} f(\theta) &= \theta^d + c_{d-1}\theta^{d-1} + \ldots + c_1\theta + c_0 \\ &= \sigma(a)^d + c_{d-1}\sigma(a)^{d-1} + \ldots + c_1\sigma(a) + c_0 \\ &= \sigma(a^d + c_{d-1}a^{d-1} + \ldots + c_1 a + c_0) \\ &= \sigma(0) \\ &= 0. \end{aligned}$$

Jadi $\theta = a_i$ dan $\sigma = \sigma_i$ untuk suatu $i$ dengan $1 \leq i \leq d$. Jadi *embedding* harus salah satu dari $\sigma_i$ dan ada tidak lebih dan tidak kurang dari $d$ *embeddings*. Selesailah pembuktian teorema 67.

**Teorema 68 (Dedekind)** *$\sigma_1, \sigma_2, \ldots, \sigma_d$ diatas linearly independent, dengan kata lain jika terdapat $c_1, c_2, \ldots, c_d \in K$ dimana*

$$c_1\sigma_1(b) + c_2\sigma_2(b) + \ldots + c_d\sigma_d(b) = 0$$

*untuk setiap $b \in K(a)$, maka setiap $c_i = 0$ untuk $1 \leq i \leq d$.*

Kita buktikan teorema 68 menggunakan induksi pada $d$. Untuk $d = 1$ maka sangat jelas bahwa jika

$$c_1\sigma_1(b) = 0$$

untuk setiap $b \in K(a)$, maka $c_1 = 0$ karena ada $b_0 \in K(a)$ dimana $\sigma_1(b_0) \neq 0$. Untuk $d \geq 2$, kita dapat asumsikan setiap $d - 1$ *homomorphism* $\sigma_i$ yang berbeda adalah *linearly independent*. Kita lihat apa konsekuensinya jika terdapat $c_1, c_2, \ldots, c_d$ dimana untuk setiap $b \in K(a)$:

$$c_1\sigma_1(b) + c_2\sigma_2(b) + \ldots + c_d\sigma_d(b) = 0. \tag{12.1}$$

Karena $\sigma_1 \neq \sigma_d$ maka terdapat $b_0 \in K(a)$ dimana $\sigma_1(b_0) \neq \sigma_d(b_0)$. Karena persamaan 12.1 berlaku untuk setiap $b \in K(a)$ maka persamaan juga berlaku untuk $b_0b$. Jadi kita dapatkan

$$c_1\sigma_1(b_0)\sigma_1(b) + c_2\sigma_2(b_0)\sigma_2(b) + \ldots + c_d\sigma_d(b_0)\sigma_d(b) = 0. \tag{12.2}$$

Jika kita kalikan persamaan 12.1 dengan $\sigma_d(b_0)$ maka kita dapatkan

$$c_1\sigma_d(b_0)\sigma_1(b) + c_2\sigma_d(b_0)\sigma_2(b) + \ldots + c_d\sigma_d(b_0)\sigma_d(b) = 0. \tag{12.3}$$

Jika kita kurangkan persamaan 12.3 dari persamaan 12.2 maka kita dapatkan

$$c_1(\sigma_1(b_0) - \sigma_d(b_0))\sigma_1(b) + \ldots + c_{d-1}(\sigma_{d-1}(b_0) - \sigma_{d-1}(b_0))\sigma_{d-1}(b) = 0.$$

Dengan $e_i = c_i(\sigma_i(b_0) - \sigma_d(b_0))$ untuk $1 \leq i \leq d-1$, kita dapatkan

$$e_1\sigma_1(b) + e_2\sigma_2(b) + \ldots + e_{d-1}\sigma_{d-1}(b) = 0.$$

Berdasarkan hipotesis induksi, $\sigma_1, \sigma_2, \ldots, \sigma_{d-1}$ *linearly independent*, jadi setiap $e_i = 0$. Jadi $c_1(\sigma_1(b_0) - \sigma_d(b_0)) = 0$, dan karena $\sigma_1(b_0) \neq \sigma_d(b_0)$ maka $c_1 = 0$. Menggunakan cara yang sama kita akan dapatkan $c_2 = 0, \ldots, c_{d-1} = 0$. Persamaan 12.1 menjadi $c_d\sigma_d(b) = 0$ untuk setiap $b \in K(a)$, dan karena terdapat $e_0 \in K(a)$ dimana $\sigma_d(e_0) \neq 0$, maka $c_d = 0$. Selesailah pembuktian teorema 68.

Sekarang kita definisikan konsep *norm*:

**Definisi 33** *Jika $f(x)$ merupakan monic irreducible polynomial dalam $K[x]$ dengan degree $d$, $a \in F$ merupakan akar dari $f(x)$, dan $\theta \in K(a)$, maka norm dari elemen $\theta$ untuk field extension $K(a)/K$, yang diberi notasi $N_K^{K(a)}(\theta)$, didefinisikan sebagai berikut:*

$$N_K^{K(a)}(\theta) = \sigma_1(\theta)\sigma_2(\theta)\cdots\sigma_d(\theta)$$

*dimana setiap $\sigma_i$ merupakan embedding yang berbeda seperti yang berada dalam teorema 67.*

Tidak terlalu sulit untuk menunjukkan bahwa $N_K^{K(a)}$ bersifat *multiplicative*:

$$N_K^{K(a)}(\theta_1\theta_2) = N_K^{K(a)}(\theta_1)N_K^{K(a)}(\theta_2).$$

Berikutnya kita definisikan konsep *trace*:

**Definisi 34** *Jika $f(x)$ merupakan monic irreducible polynomial dalam $K[x]$ dengan degree $d$, $a \in F$ merupakan akar dari $f(x)$, dan $\theta \in K(a)$, maka trace dari elemen $\theta$ untuk field extension $K(a)/K$, yang diberi notasi $T_K^{K(a)}(\theta)$, didefinisikan sebagai berikut:*

$$T_K^{K(a)}(\theta) = \sigma_1(\theta) + \sigma_2(\theta) + \ldots + \sigma_d(\theta)$$

*dimana setiap $\sigma_i$ merupakan embedding yang berbeda seperti yang berada dalam teorema 67.*

Tidak terlalu sulit untuk menunjukkan bahwa $T_K^{K(a)}$ bersifat *additive*, jika $a, b \in K$ dan $x, y \in K(a)$, maka:

$$T_K^{K(a)}(ax + by) = aT_K^{K(a)}(x) + bT_K^{K(a)}(y).$$

Selanjutnya kita bahas efek komposisi *field extension* terhadap *norm*. Jika $x = N_K^L(u)$ dan $E/L$ adalah *field extension* dengan dimensi $n$, maka

$$N_K^E(u) = x^n.$$

Ini karena *field extension* menghasilkan $n$ pemetaan $\sigma LE_1, \sigma LE_2, \ldots \sigma LE_n$ yang *injective* dan setiap pemetaan menghasilkan

$$\sigma LE_i(x) = x.$$

Jika *field extension* $L/K$ mempunyai dimensi $m$ make terdapat $mn$ pemetaan *injective* dari $K$ ke $E$ yang merupakan komposisi pemetaan

$$K \xrightarrow{\sigma KL_j} L \xrightarrow{\sigma LE_i} E$$

dimana $1 \leq i \leq n$ dan $1 \leq j \leq m$. Jadi

$$\begin{aligned} N_K^E(u) &= \prod_{i=1}^{n} \sigma LE_i(\prod_{j=1}^{m} \sigma KL_j(u)) \\ &= \prod_{i=1}^{n} \sigma LE_i(x) \\ &= x^n. \end{aligned}$$

Untuk *trace*, jika $x = T_K^L(u)$, rumusnya adalah:

$$T_K^E(u) = nx.$$

Berikutnya, kita akan lihat bahwa *norm* juga bisa didapat menggunakan determinan. Kita gunakan matrik pengali untuk elemen dalam $K(a)$. Dengan basis sebagai berikut

$$\begin{bmatrix} 1 \\ a \\ a^2 \\ \vdots \\ a^{d-1} \end{bmatrix},$$

jika $v$ adalah vektor untuk suatu elemen $x \in K(a)$, matrik pengali $A$ untuk suatu elemen $e \in K(a)$ adalah matrik yang jika dikalikan dengan vektor $v$:

$$Av = v'$$

menghasilkan vektor $v'$ yang merepresentasikan $ex$. Jika basis yang digunakan adalah $b_1, b_2, \ldots, b_n$, maka setiap kolom $i$ merepresentasikan $eb_i$ sebagai kombinasi linear $b_1, b_2, \ldots, b_n$. Tidak terlalu sulit untuk melihat bahwa matrik pengali untuk $a$ adalah *companion matrix* untuk $f(x) = x^d + c_{d-1}x^{d-1} + \ldots + c_1x + c_0$ sebagai berikut:

$$C(f) = \begin{bmatrix} 0 & 0 & \ldots & 0 & -c_0 \\ 1 & 0 & \ldots & 0 & -c_1 \\ 0 & 1 & \ldots & 0 & -c_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -c_{d-1} \end{bmatrix}.$$

Kolom pertama dalam matrik merepresentasikan $a$, kolom kedua merepresentasikan $a^2$, dan seterusnya sampai dengan kolom terahir yang merepresentasikan $a^d$. Perhatikan bahwa kolom untuk $a^d$ didapat dari

$$0 = a^d + c_{d-1}a^{d-1} + \ldots + c_1a + c_0,$$

jadi

$$a^d = -c_{d-1}a^{d-1} \ldots - c_1a - c_0.$$

Matrik menghasilkan determinan

$$\det(C(f)) = (-1)^{d-1}(-c_0) = (-1)^d c_0.$$

Menggunakan determinan kita dapatkan *norm*

$$N_K^{K(a)}(a) = \det(C(f)) = (-1)^d c_0.$$

Mari kita periksa apakah ini sesuai dengan *norm* yang didapatkan menggunakan definisi 33.

$$\begin{aligned} f(x) &= (x-a_1)(x-a_2)\cdots(x-a_d) \\ &= x^d + \ldots + (-1)^d(a_1a_2\cdots a_d). \end{aligned}$$

Jadi karena $(-1)^d(a_1a_2\cdots a_d) = c_0$ maka menggunakan definisi 33:

$$\begin{aligned} N_K^{K(a)}(a) &= \sigma_1(a)\sigma_2(a)\cdots\sigma_d(a) \\ &= a_1a_2\cdots a_d \\ &= (-1)^d(-1)^d(a_1a_2\cdots a_d) \\ &= (-1)^d c_0. \end{aligned}$$

Jadi *norm* yang didapatkan menggunakan determinan matrik sesuai dengan *norm* yang didapatkan menggunakan definisi 33. Demikian juga *trace* bisa didapatkan dari matrik pengali, yaitu dari penjumlahan elemen-elemen diagonal. Jadi menggunakan *companion matrix* kita dapatkan

$$T_K^{K(a)}(a) = -c_{d-1}.$$

Mari kita periksa apakah ini sesuai dengan *trace* yang didapatkan menggunakan definisi 34.

$$\begin{aligned} f(x) &= (x-a_1)(x-a_2)\cdots(x-a_d) \\ &= x^d - (a_1+a_2+\ldots+a_d)x^{d-1} + \ldots. \end{aligned}$$

Jadi karena $-(a_1+a_2+\ldots a_d) = c_{d-1}$ maka menggunakan definisi 34:

$$\begin{aligned} T_K^{K(a)}(a) &= \sigma_1(a)+\sigma_2(a)+\ldots+\sigma_d(a) \\ &= a_1+a_2+\ldots+a_d \\ &= -c_{d-1}. \end{aligned}$$

Jadi *trace* yang didapatkan menggunakan matrik sesuai dengan *trace* yang didapatkan menggunakan definisi 34.

*Norm* dan *trace* tidak tergantung pada basis yang digunakan. Jika basis lain digunakan (bukan 1, $a$, $a^2$, ...), maka terdapat matrik *change of basis* $Q$, dan karena

$$Q^{-1}QC(f)Q^{-1}Q = C(f)$$

maka $QC(f)Q^{-1}$ *similar* dengan $C(f)$ yang berarti $QC(f)Q^{-1}$ dan $C(f)$ mempunyai determinan yang sama dan *trace* yang sama. Jadi *norm* dan *trace* adalah *invariant* dari basis.

Mari kita periksa apakah penggunaan determinan berlaku untuk sembarang elemen $u \in K(a)$. Jika $u \in K$ maka matrik pengali adalah

$$\begin{bmatrix} u & 0 & \dots & 0 & 0 \\ 0 & u & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & u & 0 \\ 0 & 0 & \dots & 0 & u \end{bmatrix}$$

yang menghasilkan determinan $u^d$. Menggunakan definisi 33 kita dapatkan:

$$\begin{aligned} N_K^{K(a)}(u) &= \sigma_1(u)\sigma_2(u)\cdots\sigma_d(u) \\ &= \underbrace{uu\cdots u}_{d\times} \\ &= u^d \end{aligned}$$

jadi sesuai dengan hasil yang didapat menggunakan deteminan. Jika $u \notin K$ maka terdapat *irreducible polynomial* $g(x)$ dengan *degree* $n|d$ dimana $u$ merupakan akar dari $g(x)$. Jika

$$g(x) = x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0,$$

maka matrik pengali $u$ untuk $K(u)$ adalah

$$C(g) = \begin{bmatrix} 0 & 0 & \dots & 0 & -b_0 \\ 1 & 0 & \dots & 0 & -b_1 \\ 0 & 1 & \dots & 0 & -b_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -b_{n-1} \end{bmatrix}$$

dan $\det(C(g)) = (-1)^n b_0$. Jika $K(u) = K(a)$ maka kita selesai karena

$$g = \min_K^u = \min_K^a = f,$$

jadi $n = d$, $b_0 = c_0$ dan $u$ sama dengan $a$ atau merupakan suatu *conjugate* dari $a$ atas $f$. Jika $K(u) \subset K(a)$ maka $N_K^{K(u)}(u) = \det(C(g)) = (-1)^n b_0$ dan $K(a)/K(u)$ adalah *field extension* dengan dimensi $m = \frac{d}{n}$, jadi

$$\begin{aligned} N_K^{K(a)}(u) &= (N_K^{K(u)}(u))^m \\ &= ((-1)^n b_0)^m. \end{aligned}$$

Bagaimana dengan determinan matrik pengali $u$ untuk $K(a)/K$? Sebagai basis kita dapat gunakan *cross product* basis $K(u)/K$ dengan basis $K(a)/K(u)$:

$$1, u, u^2, \ldots, u^d, v, uv, u^2v, \ldots, u^dv, \ldots, v^m, uv^m, u^2v^m, \ldots, u^dv^m$$

dimana $1, v, \ldots, v^m$ merupakan basis untuk $K(a)/K(u)$. Matrik pengali menjadi

$$U = \begin{bmatrix} C(g) & 0 & \ldots & 0 & 0 \\ 0 & C(g) & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & C(g) & 0 \\ 0 & 0 & \ldots & 0 & C(g) \end{bmatrix}$$

dimana terdapat $m$ salinan dari submatrik $C(g)$ dan setiap 0 merupakan submatrik 0 yang dimensinya sama dengan $C(g)$. Kita dapatkan

$$\begin{aligned} \det(U) &= (\det(C(g)))^m \\ &= ((-1)^n b_0)^m \end{aligned}$$

sesuai dengan *norm* diatas. Jadi untuk sembarang $u \in K(a)$, $N_K^{K(a)}(u)$ bisa didapat menggunakan determinan matrik pengali untuk $u$.

Sekarang mari kita periksa apakah rumus untuk *trace* berlaku untuk sembarang elemen $u \in K(a)$. Jika $u \in K$ maka matrik pengali adalah

$$\begin{bmatrix} u & 0 & \ldots & 0 & 0 \\ 0 & u & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & u & 0 \\ 0 & 0 & \ldots & 0 & u \end{bmatrix}$$

yang menghasilkan *trace* $du$. Menggunakan definisi 34 kita dapatkan:

$$\begin{aligned} T_K^{K(a)}(u) &= \sigma_1(u) + \sigma_2(u) + \ldots + \sigma_d(u) \\ &= \underbrace{u + u + \ldots u}_{d\times} \\ &= du \end{aligned}$$

jadi sesuai dengan hasil yang didapat menggunakan *trace* matrik. Jika $u \notin K$ maka terdapat *irreducible polynomial* $g(x)$ dengan *degree* $n|d$ dimana $u$ merupakan akar dari $g(x)$. Jika

$$g(x) = x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0,$$

maka matrik pengali $u$ untuk $K(u)$ adalah

$$C(g) = \begin{bmatrix} 0 & 0 & \ldots & 0 & -b_0 \\ 1 & 0 & \ldots & 0 & -b_1 \\ 0 & 1 & \ldots & 0 & -b_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -b_{n-1} \end{bmatrix}$$

dan *trace* matrik adalah $-b_{n-1}$. Jika $K(u) = K(a)$ maka kita selesai karena

$$g = \min_K^u = \min_K^a = f,$$

jadi $n = d$, $b_{n-1} = c_{n-1}$ dan $u$ sama dengan $a$ atau merupakan suatu *conjugate* dari $a$ atas $f$. Jika $K(u) \subset K(a)$ maka $T_K^{K(u)}(u) = trace(C(g)) = -b_{n-1}$ dan $K(a)/K(u)$ adalah *field extension* dengan dimensi $m = \frac{d}{n}$, jadi

$$\begin{aligned} T_K^{K(a)}(u) &= m(T_K^{K(u)}(u)) \\ &= -mb_{n-1}. \end{aligned}$$

Bagaimana dengan *trace* matrik pengali $u$ untuk $K(a)/K$? Sebagai basis kita dapat gunakan *cross product* basis $K(u)/K$ dengan basis $K(a)/K(u)$:

$$1, u, u^2, \ldots, u^d, v, uv, u^2v, \ldots, u^dv, \ldots, v^m, uv^m, u^2v^m, \ldots, u^dv^m$$

dimana $1, v, \ldots, v^m$ merupakan basis untuk $K(a)/K(u)$. Matrik pengali menjadi

$$U = \begin{bmatrix} C(g) & 0 & \ldots & 0 & 0 \\ 0 & C(g) & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & C(g) & 0 \\ 0 & 0 & \ldots & 0 & C(g) \end{bmatrix}$$

dimana terdapat $m$ salinan dari submatrik $C(g)$ dan setiap 0 merupakan submatrik 0 yang dimensinya sama dengan $C(g)$. Kita dapatkan

$$\begin{aligned} trace(U) &= m(trace(C(g))) \\ &= -mb_{n-1} \end{aligned}$$

sesuai dengan *trace* diatas. Jadi untuk sembarang $u \in K(a)$, $T_K^{K(a)}(u)$ bisa didapat menggunakan *trace* matrik pengali untuk $u$.

## 12.4 Algebraic Number Theory

Teori mengenai *algebraic numbers* diperlukan dalam pembahasan metode *number field sieve*, yaitu metode tercepat hingga saat ini untuk menguraikan bilangan sangat besar (lebih dari 100 digit). Pembahasan *algebraic number theory* biasanya melibatkan 4 komponen:

- suatu *Dedekind domain* yaitu **Z** (bilangan bulat),
- suatu *fraction field*[1] untuk **Z** yaitu **Q** (bilangan rasional),

[1] *Fraction field* untuk suatu *ring* terdiri dari semua pecahan dimana *numerator* dan *denominator* (kecuali 0 tidak dapat menjadi *denominator*) berasal dari *ring*.

- suatu *number field* $\mathbf{Q}(\alpha)$ yang merupakan *algebraic field extension* dari $\mathbf{Q}$, dan
- suatu *Dedekind domain* $\mathfrak{D}$ terdiri dari semua *algebraic integers* dalam $\mathbf{Q}(\alpha)$ (semua elemen dalam $\mathbf{Q}(\alpha)$ yang *integral* atas $\mathbf{Z}$).

Pertama kita akan bahas konsep *Dedekind domain* yaitu struktur *ring* dimana setiap *proper ideal* dapat diuraikan secara unik (*unique factorization*). Untuk itu kita perlu definisikan terlebih dahulu beberapa konsep dimulai dengan *integral closure*. Konsep *integral closure* untuk *ring* adalah generalisasi dari konsep *algebraic closure* untuk *field*

**Definisi 35** *Jika $A$ dan $B$ keduanya merupakan ring dengan $A$ subring dari $B$ dan $b \in B$, maka $b$ disebut integral atas $A$ jika terdapat monic polynomial $f$ dengan koefisien dalam $A$ dimana $f(b) = 0$.*

Jadi *integral* untuk *ring* serupa dengan konsep *algebraic* untuk *field*.

**Definisi 36 (Integral Closure)** *Jika $A$ dan $B$ keduanya merupakan ring dengan $A \subseteq B$, maka subset $C$ dari $B$ yang berisi semua elemen $B$ yang integral atas $A$ merupakan subring dari $B$ yang mencakup $A$ dan disebut integral closure dari $A$ dalam $B$. Jika $C = A$ maka $A$ disebut integrally closed dalam $B$. Jika $A$ disebut integrally closed tanpa menyebut dalam ring apa, maka yang dimaksud adalah integrally closed dalam fraction field untuk $A$.*

Contoh dari suatu *ring* yang *integrally closed* adalah $\mathbf{Z}$:

**Teorema 69** $\mathbf{Z}$ *(himpunan bilangan bulat) adalah suatu ring yang integrally closed.*

Mari kita buktikan teorema 69. Kita tunjukkan bahwa setiap elemen dalam *fraction field* $\mathbf{Q}$ yang *integral* atas $\mathbf{Z}$ berada dalam $\mathbf{Z}$. Jika $x$ adalah elemen sebagaimana diatas, maka $x$ dapat dituliskan sebagai $x = \frac{a}{b}$ dimana $a, b \in \mathbf{Z}$ dan $a$ koprima dengan $b$. Karena $x$ *integral* atas $\mathbf{Z}$ maka terdapat persamaan sebagai berikut

$$(\frac{a}{b})^n + a_{n-1}(\frac{a}{b})^{n-1} + \ldots + a_1(\frac{a}{b}) + a_0 = 0$$

dimana setiap $a_i \in \mathbf{Z}$. Jika persamaan kita kalikan dengan $b^n$ kita dapatkan

$$a^n + bc = 0$$

untuk suatu $c \in \mathbf{Z}$. Jadi $b$ membagi $a^n$ yang, karena $a$ koprima dengan $b$, hanya bisa terjadi jika $b$ merupakan suatu *unit*. Jika $b$ merupakan *unit*, maka

$$x = ab^{-1} \in \mathbf{Z}.$$

Jadi $\mathbf{Z}$ *integrally closed*.

**Teorema 70** *Jika $x \in \mathfrak{D}$, maka setiap*

$$\sigma_i(x) \in \mathbf{Z}$$

*untuk $0 \leq i \leq d$, dimana setiap $\sigma_i$ adalah homomorphism sesuai teorema 67 dengan $f = \min_{\mathbf{Q}}^{\alpha}$ dan $d$ adalah degree dari $\min_{\mathbf{Q}}^{\alpha}$.*

Mari kita buktikan teorema 70. Pertama kita ingin tunjukkan bahwa setiap

$$x_i = \sigma_i(x)$$

*integral* atas $\mathbf{Z}$. Karena $x \in \mathfrak{D}$ maka $x$ *integral* atas $\mathbf{Z}$, jadi terdapat *polynomial* $f$ dengan koefisien dalam $\mathbf{Z}$ dimana $f(x) = 0$. Kita dapatkan

$$\sigma_i(f(x)) = f(\sigma_i(x)) = f(x_i)$$

jadi setiap $x_i$ *integral* atas $\mathbf{Z}$. Karena menurut teorema 69, $\mathbf{Z}$ *integrally closed*, maka $x_i \in \mathbf{Z}$ membuktikan teorema 70.

Konsep berikutnya yang diperlukan untuk *Dedekind domain* adalah konsep *Noetherian ring.*

**Definisi 37 (Noetherian Ring)** *Suatu ring $R$ adalah Noetherian jika tidak terdapat deretan yang infinite dari ideal $I_0, I_1, I_2, \ldots$ dalam $R$:*

$$I_0 \subset I_1 \subset I_2 \subset \ldots$$

Jadi setiap himpunan non-kosong berisi *ideals* dari suatu *Noetherian ring* mempunyai elemen maksimal. Karena $\subset$ untuk *ideal* bersifat *partial order*, elemen maksimal tidak unik. Himpunan dapat memiliki lebih dari satu elemen maksimal. Suatu *Noetherian ring* juga mempunyai sifat bahwa setiap *ideal* dalam *ring* mempunyai *generator* yang *finite* (*finitely generated*). Artinya setiap *ideal* $I$ dalam *Noetherian ring* $R$ mempunyai *generator* dengan bentuk

$$A = \{a_0, a_1, \ldots, a_n\},$$

jadi setiap elemen dalam *ideal* $I$ dapat ditulis sebagai

$$\sum_{i=0}^{n} a_i r_i$$

dimana setiap $r_i \in R$. Notasi $\mathrm{Id}(a_0, a_1 \ldots, a_n)$ kerap digunakan untuk *ideal* dengan *generator* $A$. Untuk menunjukkan bahwa setiap *ideal* $I$ dalam suatu *Noetherian ring* $R$ mempunyai *generator* yang *finite*, diperlukan penggunaan *axiom of choice*. Pembuktian dilakukan dengan menunjukkan bahwa jika *generator* tidak *finite* maka kita akan dapatkan kontradiksi. Dengan $\varphi$ berupa fungsi *choice* yang jika diaplikasikan pada $0 \neq A \in \mathcal{P}(R)$ ($A$ adalah subset non-kosong dari $R$) menghasilkan suatu elemen dalam $A$, dan dengan $a_0 \in I$ sembarang elemen dalam $I$, kita definisikan

$$a_{i+1} = \varphi(I \setminus \mathrm{Id}(a_0, a_1, \ldots, a_i))$$

dan

$$I_i = \mathrm{Id}(a_0, a_1, \ldots, a_i)$$

untuk setiap $i \in \mathbf{N}$. Maka terdapat deretan *infinite*

$$I_o \subset I_1 \subset I_2 \subset \ldots$$

yang kontradiksi dengan definisi *Noetherian ring* untuk $R$. Sekarang kita buktikan sebaliknya, yaitu jika setiap *ideal* dalam *ring* $R$ adalah *finitely generated*, maka $R$ adalah *Noetherian ring*. Pertama, kita buktikan terlebih dahulu bahwa jika setiap *ideal* dalam *ring* $R$ adalah *finitely generated*, maka untuk setiap $B \subseteq R$ terdapat *finite subset* $C \subseteq B$ dimana $\mathrm{Id}(C) = \mathrm{Id}(B)$. Karena $\mathrm{Id}(B)$ *finitely generated*, berarti terdapat *subset* $D = \{d_1, \ldots, d_n\} \subseteq \mathrm{Id}(B)$ yang *finite* dimana $\mathrm{Id}(D) = \mathrm{Id}(B)$. Kita dapat tuliskan setiap $d_i$ sebagai:

$$d_i = \sum_{j=1}^{k_i} r_{ij} b_{ij} \text{ dengan } r_{ij} \in R, b_{ij} \in B,$$

untuk $1 \leq i \leq n$. Jika kita buat

$$C = \{b_{ij} | 1 \leq i \leq n, 1 \leq j \leq k_i\}$$

maka $C$ adalah *finite subset* $B$ yang menjadi *generator* untuk $\mathrm{Id}(B)$ karena untuk setiap $b \in \mathrm{Id}(B)$ terdapat $s_1, \ldots, s_n$ dimana setiap $s_i \in R$ dan

$$\begin{aligned} b &= \sum_{i=1}^{n} s_i d_i \\ &= \sum_{i=1}^{n} s_i \sum_{j=1}^{k_i} r_{ij} b_{ij} \\ &= \sum_{i=1}^{n} \sum_{j=1}^{k_i} s_i r_{ij} b_{ij}. \end{aligned}$$

Jadi $C$ merupakan *finite subset* $B$ dengan $\mathrm{Id}(C) = \mathrm{Id}(B)$. Berikutnya kita akan tunjukkan bahwa jika setiap *ideal* dalam $R$ *finitely generated*, maka untuk setiap deretan elemen dalam $R$

$$a_0, a_1, a_2, \ldots$$

($\{a_i\}_{i\in\mathbf{N}}$) terdapat $n \in \mathbf{N}$ dimana $a_{n+1} \in \mathrm{Id}(a_o, a_1, \ldots, a_n)$. Dengan

$$I = \mathrm{Id}(\{a_i | i \in \mathbf{N}\})$$

hasil sebelumnya mengatakan bahwa terdapat *finite subset* $B \subset \{a_i | i \in \mathbf{N}\}$ dimana $\mathrm{Id}(B) = I$. Jadi terdapat $n \in \mathbf{N}$ dimana $B \subseteq \{a_0, \ldots, a_n\}$. Alhasil $\mathrm{Id}(a_0, \ldots, a_n) = I$, jadi

$$a_{n+1} \in \mathrm{Id}(a_0, \ldots, a_n).$$

Sekarang kita tunjukkan bahwa jika setiap *ideal* dalam $R$ *finitely generated* maka $R$ adalah *Noetherian ring.* Kita lihat apa konsekuensi jika $R$ bukan *Noetherian ring*, jadi terdapat deretan *infinite*

$$I_0 \subset I_1 \subset I_2 \subset \ldots$$

Kita gunakan *axiom of choice* dengan fungsi *choice* $\varphi$ untuk mendefinisikan dereten

$$a_0, a_1, a_2, \ldots$$

dengan $a_0 = \varphi(I_0)$ dan $a_{i+1} = \varphi(I_{i+1} \setminus I_i)$. Menggunakan hasil sebelumnya, terdapat $n \in \mathbf{N}$ dimana $a_{n+1} \in \mathrm{Id}(a_0, \ldots, a_n)$, suatu kontradiksi. Jadi kita telah membuktikan teorema berikut.

**Teorema 71** *Suatu ring $R$ adalah Noetherian ring jika dan hanya jika setiap ideal dalam $R$ finitely generated.*

Sekarang kita definisikan konsep *Dedekind domain.*

**Definisi 38 (Dedekind Domain)** *Suatu Dedekind domain adalah suatu integral domain $A$ dimana*

- *$A$ integrally closed.*
- *$A$ merupakan suatu Noetherian ring.*
- *Setiap ideal prima yang bukan 0 merupakan ideal maksimal.*

Tidak terlalu sulit untuk menunjukkan bahwa $\mathbf{Z}$ merupakan suatu *Dedekind domain*:

- Berdasarkan teorema 69, $\mathbf{Z}$ *integrally closed.*
- Berikutnya, karena $\mathbf{Z}$ merupakan *principal ideal domain* dimana setiap *ideal* $I$ mempunyai bentuk $n\mathbf{Z}$ dengan $n \in \mathbf{Z}$, jadi $I$ *finitely generated* oleh
$$\{n\},$$
maka $\mathbf{Z}$ merupakan *Noetherian ring.*

- Yang terahir, karena **Z** merupakan suatu *principal ideal domain*, maka menurut teorema 18 setiap *non-trivial ideal* prima dalam **Z** merupakan *ideal* maksimal.

Sebelum menunjukkan bahwa $\mathfrak{D}$ juga merupakan *Dedekind domain*, kita definisikan terlebih dahulu konsep *Noetherian module*.

**Definisi 39 (Noetherian Module)** *Suatu module $M$ adalah Noetherian jika tidak terdapat deretan infinite submodule $M_0, M_1, M_2, \ldots$ dari $M$:*

$$M_0 \subset M_1 \subset M_2 \subset \ldots$$

Jika suatu *ring* $R$ adalah *Noetherian* sebagai *module*, jelas bahwa $R$ merupakan *Noetherian ring* karena setiap *ideal* dalam $R$ adalah *submodule* dari $R$. Juga sangat jelas bahwa jika *module* $M$ *Noetherian*, maka *submodule* $G$ dari $M$ juga *Noetherian*. Konsep *quotient module* $M/G$ didefinisikan mirip dengan *quotient ring*, hanya saja *ideal* diganti oleh *submodule* sebagai modulo.

**Teorema 72** *Jika $M$ adalah suatu module dan $G$ adalah submodule dari $M$, maka $M$ Noetherian jika dan hanya jika $G$ dan $M/G$ Noetherian.*

Jika $M$ *Noetherian*, sangat jelas bahwa $G$ juga *Noetherian*, dan *submodule* dari $M/G$ dapat ditulis sebagai

$$G_0/G,\ G_1/G,\ G_2/G,\ \ldots$$

dimana setiap $G_i$ adalah *submodule* dari $M$ yang mencakup $G$ ($G$ merupakan subset dari $G_i$). Karena tidak terdapat deretan *infinite*

$$G_0 \subset G_1 \subset G_2 \subset \ldots$$

maka tidak terdapat deretan *infinite*

$$G_0/G \subset G_1/G \subset G_2/G \subset \ldots$$

jadi $M/G$ *Noetherian*. Jika $G$ dan $M/G$ *Noetherian*, mari kita tunjukkan bahwa $M$ juga *Noetherian*. Jika

$$M_0 \subseteq M_1 \subseteq M_2 \subseteq \ldots$$

merupakan sembarang deretan *infinite* dimana setiap $M_i$ merupakan *submodule* dari $M$, maka terdapat $k_1$ dimana

$$M_0 \cap G \ \subset\ \ldots\ \subset\ M_{k_1} \cap G \ =\ M_{k_1+1} \cap G \ =\ \ldots$$

dan $k_2$ dimana

$$(G + M_0)/G \ \subset\ \ldots\ \subset\ (G + M_{k_2})/G \ =\ (G + M_{k_2+1})/G \ =\ \ldots$$

Jika $k = \max(k_1, k_2)$, maka

$$M_k \cap G = M_{k+i} \cap G \text{ dan } G + M_k = G + M_{k+i}$$

untuk setiap $i \in \mathbf{N}$. Kita ketahui bahwa $M_k \subseteq M_{k+i}$. Jika $g \in M_{k+i}$, maka $g \in G + M_{k+i} = G + M_k$. Jadi terdapat $a \in G$ dan $b \in M_k$ dimana $g = a + b$, dan kita dapatkan

$$a = g - b \in M_{k+i} \cap G = M_k \cap G.$$

Ini menghasilkan $a, b \in M_k$, yang berarti $g = a + b \in M_k$, jadi $M_{k+i} \subseteq M_k$, dan bersama dengan $M_k \subseteq M_{k+i}$ menghasilkan $M_k = M_{k+i}$. Jadi $M$ *Noetherian*, dan selesailah pembuktian teorema 72. Satu konsekuensi dari teorema 72 adalah *direct product* dari dua *Noetherian module* juga *Noetherian* (komponen pertama adalah $G$, komponen kedua adalah $M/G$, dan produk adalah $M$). *Direct product* $P$ dari dua $R$-*module* $M$ dan $N$ didefinisikan sebagai berikut:

- $P = \{(x_1, x_2) | x_1 \in M, x_2 \in N\}$ (jadi elemen-elemen $P$ membentuk himpunan yang merupakan *Cartesian product* dari $M$ dan $N$).
- $(x_1, x_2) + (y_1, y_2) = (x_1 + x_2, y_1 + y_2)$.
- $\alpha \circ (x_1, y_1) = (\alpha \circ x_1, \alpha \circ x_2)$.

Dengan menggunakan induksi kita dapatkan teorema berikut:

**Teorema 73** *Finite direct product dari Noetherian modules juga Noetherian.*

Kembali ke $\mathfrak{D}$, sifat pertama yang harus dipenuhi $\mathfrak{D}$ agar menjadi suatu *Dedekind domain* adalah bahwa $\mathfrak{D}$ *integrally closed*. Untuk itu kita perlukan dua teorema.

**Teorema 74** *Terdapat basis untuk field extension* $\mathbf{Q}(\alpha)/\mathbf{Q}$ *yang seluruhnya terdiri dari elemen-elemen* $\mathfrak{D}$.

Mari kita buktikan teorema 74. Jika $x_1, x_2, \ldots, x_n$ merupakan basis untuk $\mathbf{Q}(\alpha)/\mathbf{Q}$, maka setiap $x_i$ *algebraic* atas $\mathbf{Q}$ (karena *extension* bersifat *algebraic*), jadi terdapat *polynomial* sebagai berikut:

$$a_m x_i^m + \ldots + a_1 x_i + a_0$$

dimana $a_m \neq 0$ dan $a_j \in \mathbf{Z}$ (*polynomial* dengan koefisien dalam $\mathbf{Z}$ didapat dari *polynomial* dengan koefisien dalam $\mathbf{Q}$ dengan mengalikan *common denominator*). Dengan $y_i = a_m x_i$ kita kalikan *polynomial* dengan $a_m^{m-1}$ untuk mendapatkan

$$\begin{aligned} (a_m x_i)^m + \ldots + a_1 a_m^{m-2}(a_m x_i) + a_0 a_m^{m-1} &= \\ y_i^m + \ldots - a_1 a_m^{m-2} y_i + a_0 a_m^{m-1} &= 0. \end{aligned}$$

Jadi terdapat basis $y_1, y_2, \ldots, y_n$ untuk $\mathbf{Q}(\alpha)/\mathbf{Q}$ dimana setiap $y_i$ *integral* atas $\mathbf{Z}$ (dengan kata lain setiap $y_i$ adalah elemen dari $\mathfrak{O}$), jadi terdapat basis yang seluruhnya terdiri dari elemen-elemen $\mathfrak{O}$. Selesailah pembuktian teorema 74.

**Teorema 75** $\mathbf{Q}(\alpha)$ *merupakan fraction field untuk* $\mathfrak{O}$.

Jika $x \in \mathbf{Q}(\alpha)$, maka terdapat $0 \neq a \in \mathbf{Z}$ dan $y \in \mathfrak{O}$ dimana $x = \frac{y}{a}$ (gunakan pembuktian teorema 74 dengan $y_i = y, x_i = x, a_m = a$). Jadi $\mathbf{Q}(\alpha)$ merupakan *fraction field* untuk $\mathfrak{O}$.

Sifat kedua yang harus dipenuhi oleh $\mathfrak{O}$ adalah *Noetherian ring*. Untuk itu, selain konsep *module* kita gunakan juga *trace form*.

**Definisi 40 (Trace Form)** *Untuk separable field extension $L/K$, trace form untuk $L/K$ adalah suatu bilinear form dengan pemetaan sebagai berikut:*

$$(x, y) \mapsto T_K^L(xy)$$

*dimana $x, y \in L$.*

**Teorema 76** *Jika $L/K$ merupakan separable field extension, maka trace form dari $L/K$ non-degenerate. Dengan kata lain, jika $(x, y) \mapsto 0$ untuk semua $y \in L$, maka $x = 0$.*

Untuk membuktikan teorema 76, kita tunjukkan terlebih dahulu bahwa jika $L/K$ merupakan *separable field extension* maka $T_K^L(x)$ tidak mungkin 0 untuk semua $x \in L$. Jika $T_K^L(x) = 0$ untuk semua $x \in L$, maka $\sum_{i=0}^{d} \sigma_i(x) = 0$ untuk semua $x \in L$. Tetapi ini bertentangan dengan teorema 68, jadi tidak mungkin $T_K^L(x) = 0$ untuk semua $x \in L$. Sekarang kita lihat apa konsekuensinya jika $(x, y) \mapsto 0$ untuk semua $y \in L$ dan $x \neq 0$. Kita pilih $x_0 \in L$ dimana $T_K^L(x_0) \neq 0$, lalu pilih $y \in L$ yang membuat $x_0 = xy$. Karena kita dapatkan kontradiksi, yaitu

$$T_K^L(x_0) = T_K^L(xy) = 0$$

dan

$$T_K^L(x_0) \neq 0,$$

maka selesailah pembuktian teorema 76.

**Teorema 77** *Jika $b_1, b_2, \ldots, b_d$ adalah suatu basis untuk $\mathbf{Q}(\alpha)/\mathbf{Q}$ sebagai ruang vektor, maka terdapat basis $c_1, c_2, \ldots, c_d$ untuk $\mathbf{Q}(\alpha)/\mathbf{Q}$ (yang didapat menggunakan dual basis) dimana*

$$(b_i, c_j) = \delta_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j. \end{cases}$$

Untuk membuktikan teorema 77, pertama perhatikan bahwa untuk setiap $y \in \mathbf{Q}(\alpha)$, pemetaan

$$l = f(y) : x \mapsto (x, y)$$

merupakan *linear form*, atau secara formal:

$$\begin{aligned} l(x_1 + x_2) &= l(x_1) + l(x_2), \\ l(ax_1) &= al(x_1) \end{aligned}$$

untuk setiap $x_1, x_2 \in \mathbf{Q}(\alpha)$ dan setiap $a \in \mathbf{Q}$. Ini dapat ditunjukkan sebagai berikut:

$$\begin{aligned} l(x_1 + x_2) &= \sum_{i=1}^{d} \sigma_i((x_1 + x_2)y) \\ &= \sum_{i=1}^{d} (\sigma_i(x_1 y) + \sigma_i(x_2 y)) \\ &= \sum_{i=1}^{d} \sigma_i(x_1 y) + \sum_{i=1}^{d} \sigma_i(x_2 y) \\ &= l(x_1) + l(x_2) \end{aligned}$$

dan

$$\begin{aligned} l(ax_1) &= \sum_{i=1}^{d} \sigma_i(ax_1) \\ &= \sum_{i=1}^{d} a\sigma_i(x_1) \\ &= a\sum_{i=1}^{d} \sigma_i(x_1) \\ &= al(x_1). \end{aligned}$$

Pemetaan

$$y \mapsto f(y)$$

merupakan suatu *linear map* dari $\mathbf{Q}(\alpha)$ ke $\mathbf{Q}(\alpha)^*$ (ruang untuk *linear form* pada $\mathbf{Q}(\alpha)$). Berikutnya kita tunjukkan bahwa *linear map* $y \mapsto f(y)$ *injective*, yaitu $f(y_1) \neq f(y_2)$ untuk setiap $y_1, y_2 \in \mathbf{Q}(\alpha)$ jika $y_1 \neq y_2$. Mari kita lihat apa konsekuensinya jika $f(y_1) = f(y_2)$ dan $y_1 \neq y_2$. Jadi

$$(x \mapsto \sum_{i=1}^{d} \sigma_i(xy_1)) = (x \mapsto \sum_{i=1}^{d} \sigma_i(xy_2))$$

atau

$$\sum_{i=1}^{d} \sigma_i(x(y_1 - y_2)) = 0$$

yang, karena $x$ sembarang jadi bisa pilih $x \neq 0$, dan berdasarkan teorema 68 berarti $(y_1 - y_2) = 0$ atau $y_1 = y_2$, suatu kontradiksi. Jadi jika $y_1 \neq y_2$ maka $f(y_1) \neq f(y_2)$, membuktikan bahwa $y \mapsto f(y)$ *injective*. Kita juga ingin tunjukkan bahwa *linear map* $y \mapsto f(y)$ *surjective*: untuk setiap *linear form* $l$ pada $\mathbf{Q}(\alpha)$, terdapat $y \in \mathbf{Q}(\alpha)$ dimana $l = f(y)$. Jika $b_1, b_2, \ldots, b_d$ merupakan basis untuk $\mathbf{Q}(\alpha)/\mathbf{Q}$ sebagai ruang vektor maka $x = x_1b_1 + x_2b_2 + \ldots + x_db_d$ dapat ditulis dengan vektor kolom sebagai berikut:

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_d \end{bmatrix}.$$

Jadi setiap *linear form* dapat ditulis dengan perkalian matrik sebagai berikut:

$$\begin{bmatrix} a_1 & a_2 & \ldots & a_d \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_d \end{bmatrix}$$

yang menghasilkan $a_1x_1 + a_2x_2 + \ldots a_dx_d$. Jadi kita ingin tunjukkan bahwa terdapat $y \in \mathbf{Q}(\alpha)$ dimana $T_{\mathbf{Q}}^{\mathbf{Q}(\alpha)}(xy)$ juga menghasilkan $a_1x_1 + a_2x_2 + \ldots a_dx_d$. Jika $y = y_1b_1 + y_2b_2 + \ldots + y_db_d$, maka kita dapatkan

$$\begin{aligned}
T_{\mathbf{Q}}^{\mathbf{Q}(\alpha)}(xy) &= \sum_{i=1}^{d} \sigma_i(xy) \\
&= \sum_{i=1}^{d} \sigma_i((x_1b_1 + \ldots + x_db_d)(y_1b_1 + \ldots + y_db_d)) \\
&= \sum_{i=1}^{d} \sigma_i(x_1y_1b_1^2) + \sum_{i=1}^{d} \sigma_i(x_1y_2b_1b_2) + \ldots \sum_{i=1}^{d} \sigma_i(x_1y_db_1b_d) + \\
&\quad \sum_{i=1}^{d} \sigma_i(x_2y_1b_1b_2) + \sum_{i=1}^{d} \sigma_i(x_2y_2b_2^2) + \ldots \sum_{i=1}^{d} \sigma_i(x_2y_db_2b_d) + \\
&\quad \vdots \\
&\quad \sum_{i=1}^{d} \sigma_i(x_dy_1b_1b_d) + \sum_{i=1}^{d} \sigma_i(x_dy_2b_2b_d) + \ldots \sum_{i=1}^{d} \sigma_i(x_dy_db_d^2)
\end{aligned}$$

$$\begin{aligned}
= \quad & x_1(y_1T_{\mathbf{Q}}^{\mathbf{Q}(\alpha)}(b_1^2) + y_2T_{\mathbf{Q}}^{\mathbf{Q}(\alpha)}(b_1b_2) + \ldots + y_dT_{\mathbf{Q}}^{\mathbf{Q}(\alpha)}(b_1b_d)) + \\
& x_2(y_1T_{\mathbf{Q}}^{\mathbf{Q}(\alpha)}(b_1b_2) + y_2T_{\mathbf{Q}}^{\mathbf{Q}(\alpha)}(b_2^2) + \ldots + y_dT_{\mathbf{Q}}^{\mathbf{Q}(\alpha)}(b_2b_d)) + \\
& \vdots \\
& x_d(y_1T_{\mathbf{Q}}^{\mathbf{Q}(\alpha)}(b_1b_d) + y_2T_{\mathbf{Q}}^{\mathbf{Q}(\alpha)}(b_2b_d) + \ldots + y_dT_{\mathbf{Q}}^{\mathbf{Q}(\alpha)}(b_d^2)).
\end{aligned}$$

Agar hasil diatas sama dengan $a_1x_1 + a_2x_2 + \ldots a_dx_d$, untuk $1 \leq j \leq d$ kita dapatkan

$$a_jx_j = x_j(\sum_{i=1}^{d} y_iT_{\mathbf{Q}}^{\mathbf{Q}(\alpha)}(b_jb_i))$$

atau

$$a_j = \sum_{i=1}^{d} y_iT_{\mathbf{Q}}^{\mathbf{Q}(\alpha)}(b_jb_i).$$

Setiap $a_j$ dan $T_{\mathbf{Q}}^{\mathbf{Q}(\alpha)}(b_jb_i)$ merupakan konstan, dan karena ada $d$ persamaan dengan $d$ variabel $(y_1, y_2, \ldots, y_d)$ maka setiap $y_i$ dapat ditemukan, jadi terdapat $y \in \mathbf{Q}(\alpha)$ dimana $l = f(y)$, jadi *linear map* $y \mapsto f(y)$ *surjective.* Karena *linear map* tersebut juga *injective* maka $y \mapsto f(y)$ adalah suatu *bijection.* Menggunakan *bijection* ini, kita dapatkan *dual basis* dari $b_1, b_2, \ldots, b_d$ dalam *dual space* (yaitu ruang untuk *linear form*):

$$z_1, z_2, \ldots, z_d.$$

Jadi $z_j(b_i) = \delta_{ij}$. Jika $z_j = f(c_j)$ maka

$$\begin{aligned}
(b_i, c_j) &= f(c_j)(b_i) \\
&= z_j(b_i) \\
&= \delta ij.
\end{aligned}$$

Selesailah pembuktian teorema 77.

**Teorema 78** $\mathfrak{D}$ *merupakan free* $\mathbf{Z}$*-module dengan rank* $d$*, dimana* $d$ *adalah degree dari* $\min_{\mathbf{Q}}^{\alpha}$.

Mari kita buktikan teorema 78. Teorema 74 mengatakan bahwa terdapat basis $b_1, b_2, \ldots, b_d$ untuk $\mathbf{Q}(\alpha)/\mathbf{Q}$ dimana setiap $b_i \in \mathfrak{D}$. Menurut teorema 77 terdapat basis $c_1, c_2, \ldots, c_d$ dimana $(b_i, c_j) = \delta_{ij}$. Jika $z \in \mathfrak{D}$ maka $z$ dapat ditulis sebagai $z = \sum_{j=1}^{d} a_jc_j$. Kita dapatkan

$$T_{\mathbf{Q}}^{\mathbf{Q}(\alpha)}(b_iz) = T_{\mathbf{Q}}^{\mathbf{Q}(\alpha)}(\sum_{j=1}^{d} a_jb_ic_j)$$

$$\begin{aligned} &= \sum_{j=1}^{d} a_j T_{\mathbf{Q}}^{\mathbf{Q}(\alpha)}(b_i c_j) \\ &= \sum_{j=1}^{d} a_j \delta_{ij} \\ &= a_i. \end{aligned}$$

Karena $T_{\mathbf{Q}}^{\mathbf{Q}(\alpha)}(b_i z) \in \mathbf{Z}$ maka setiap $a_i \in \mathbf{Z}$, jadi $\mathfrak{D}$ merupakan *submodule* dari *free* $\mathbf{Z}$*-module* $\bigoplus_{j=1}^{d} \mathbf{Z}c_j$. Karena $\mathfrak{D}$ juga mencakup *free* $\mathbf{Z}$*-module* $\bigoplus_{j=1}^{d} \mathbf{Z}b_j$ maka $\mathfrak{D}$ merupakan *free* $\mathbf{Z}$*-module* dengan rank $d$, membuktikan teorema 78.

**Teorema 79** *$\mathfrak{D}$ adalah suatu Noetherian ring.*

Berdasarkan teorema 78, $\mathfrak{D}$ merupakan suatu *free* $\mathbf{Z}$*-module* dengan *rank d*. Karena $\mathbf{Z}$ adalah suatu *Noetherian ring*, maka berdasarkan teorema 73, $\mathfrak{D}$ yang merupakan *direct product* dari $d$ salinan $\mathbf{Z}$ juga *Noetherian*, membuktikan teorema 79.

**Teorema 80** *Setiap non-trivial ideal prima $I$ dalam $\mathfrak{D}$ maksimal.*

Untuk membuktikan teorema 80, kita pilih $x \in I$ dimana $x \neq 0$. Karena $x \in \mathfrak{D}$ maka terdapat *polynomial*

$$x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0 = 0$$

dimana setiap $a_i \in \mathbf{Z}$ dan $m$ adalah bilangan bulat positif yang sekecil mungkin (minimal). Jadi $a_0 \neq 0$ dan kita dapatkan

$$a_0 \in \mathfrak{D}x \cap \mathbf{Z} \subseteq I \cap \mathbf{Z},$$

jadi $I \cap \mathbf{Z}$ merupakan *non-trivial ideal* dalam $\mathbf{Z}$. Untuk setiap $a, b \in \mathbf{Z}$, jika $ab \in I \cap \mathbf{Z}$, maka $ab \in I$, dan karena $I$ adalah *ideal* prima, maka $a \in I$ atau $b \in I$. Akibatnya

$$a \in I \cap \mathbf{Z} \text{ atau } b \in I \cap \mathbf{Z},$$

jadi $I \cap \mathbf{Z}$ adalah *ideal* prima dalam $\mathbf{Z}$. Berdasarkan teorema 18, $I \cap \mathbf{Z}$ adalah *ideal* maksimal dalam $\mathbf{Z}$. Sekarang kita lihat apa konsekuensinya jika $I$ bukan *ideal* maksimal dalam $\mathfrak{D}$. Berarti terdapat *ideal* $J$ dimana $I \subset J$ dan $J \neq \mathfrak{D}$. Jika kita pilih $y \in J$ dengan $y \notin I$, maka kita akan dapatkan suatu $b_0$ dimana

$$b_0 \in \mathfrak{D}y \cap \mathbf{Z} \subseteq J \cap \mathbf{Z}.$$

Kita juga ketahui bahwa $b_0 \notin I$, jadi $b_0 \notin I \cap \mathbf{Z}$. Jadi $I \cap \mathbf{Z} \subset J \cap \mathbf{Z}$. Karena $1 \notin J \cap \mathbf{Z}$ maka $J \cap \mathbf{Z} \neq \mathbf{Z}$, jadi $I \cap \mathbf{Z}$ bukan suatu *ideal* maksimal, suatu kontradiksi. Selesailah pembuktian teorema 80.

Sekarang kita tunjukkan bahwa $\mathfrak{D}$ merupakan suatu *Dedekind domain*:

- Berdasarkan definisinya, $\mathfrak{D}$ *integrally closed* dalam $\mathbf{Q}(\alpha)$. Teorema 75 mengatakan bahwa $\mathbf{Q}(\alpha)$ merupakan *fraction field* untuk $\mathfrak{D}$. Jadi $\mathfrak{D}$ *integrally closed.*

- Berdasarkan teorema 79, $\mathfrak{D}$ adalah suatu *Noetherian ring.*

- Yang terahir, berdasarkan teorema 80, setiap *non-trivial ideal* prima dalam $\mathfrak{D}$ maksimal.

Selanjutnya kita jelaskan konsep penguraian *ideal*, karena itulah fokus dari teori mengenai *algebraic numbers*, bukan aritmatika dalam *number field.* Kita mulai dengan penjelasan konsep produk dari *ideal.* Secara formal, produk dari *ideal* $I$ dan $J$ didefinisikan sebagai berikut:

$$IJ = \{a_1b_1 + \ldots a_nb_n | a_i \in I, b_i \in J, i = 1, 2, \ldots, n; n = 1, 2, 3, \ldots\}$$

dengan kata lain produk *ideal* adalah himpunan yang isinya adalah semua penjumlahan produk $a_ib_i$ yang *finite.* Tidak terlalu sulit untuk melihat bahwa:

$$IJ \subseteq I \cap J.$$

Juga, jika

$$IJ \subseteq P$$

dimana $P$ adalah suatu *ideal* prima, maka

$$I \subseteq P \text{ atau } J \subseteq P.$$

**Teorema 81** *Jika $I$ merupakan non-trivial ideal dari suatu Noetherian integral domain $R$, maka $I$ mencakup produk dari non-trivial ideal prima.*

Untuk membuktikan teorema 81 mari kita lihat apa konsekuensinya jika $I$ tidak mencakup produk dari *non-trivial ideal* prima. Jika $S$ merupakan himpunan semua *non-trivial ideal* dari $R$ yang tidak mencakup produk dari *non-trivial ideal* prima maka, karena $R$ adalah suatu *Noetherian ring*, $S$ mempunyai elemen maksimal, sebut saja $J$. Karena $J \in S$ maka $J$ tidak mungkin prima, jadi terdapat $a, b \in R$ dimana $a \notin J$ dan $b \notin J$ tetapi $ab \in J$. Karena $J$ adalah elemen maksimal dari $S$, maka $J + aR$ dan $J + bR$ masing-masing merupakan *non-trivial ideal* yang mencakup produk dari *non-trivial ideal* prima, jadi $(J + aR)(J + bR)$ juga mencakup produk dari *non-trivial ideal* prima. Karena

$$(J + aR)(J + bR) \subseteq (J + abR) = J$$

maka $J$ juga mencakup produk dari *non-trivial ideal* prima, suatu kontradiksi. Jadi $I$ harus mencakup produk dari *non-trivial ideal* prima dan selesailah pembuktian teorema 81.

Sebelum kita bahas teorema mengenai penguraian *ideal*, kita perlu konsep *fractional ideal*. Kita gunakan himpunan $I = (\frac{5}{3})\mathbf{Z}$ sebagai motivasi. Karena bukan merupakan *subset* dari $\mathbf{Z}$, $I$ bukan suatu *ideal*. Akan tetapi $I$ mempunyai sifat mirip dengan *ideal* yaitu

- Jika $a, b \in I$ maka $a + b \in I$.
- Jika $a \in I$ dan $n \in \mathbf{Z}$ maka $na \in I$.

Juga, jika kita kalikan setiap elemen $I$ dengan 3 kita akan dapatkan suatu *ideal* yaitu $5\mathbf{Z}$. Kita katakan bahwa $I$ merupakan suatu *fractional ideal* yang mempunyai definisi sebagai berikut:

**Definisi 41 (Fractional Ideal)** *Jika $R$ merupakan suatu integral domain dengan fraction field $K$ dan $I$ merupakan $R$-submodule dari $K$, dan jika terdapat suatu $0 \neq r \in R$ dimana $rI \subseteq R$, maka $I$ disebut fractional ideal dan $r$ merupakan denominator dari $I$.*

Jadi $(\frac{5}{3})\mathbf{Z}$ merupakan *fractional ideal* dengan *denominator* $r = 3$. Tentunya *ideal* biasa juga merupakan *fractional ideal* dengan *denominator* $r = 1$. Produk untuk *fractional ideal* didefinisikan serupa dengan produk untuk *ideal* biasa.

**Teorema 82** *Jika $I$ merupakan non-trivial ideal prima dari suatu Dedekind domain $R$, $K$ merupakan fraction field dari $R$, dan $J = \{x \in K | xI \subseteq R\}$, maka $J$ merupakan fractional ideal dan $IJ = R$.*

Mari kita buktikan teorema 82. Karena untuk $0 \neq r \in I$ dan $x \in J$ kita dapatkan $rx \in R$, maka $rJ \subseteq R$ jadi $J$ merupakan suatu *fractional ideal*. Berikutnya kita akan tunjukkan bahwa

$$R \subset J.$$

Jika $x \in R$ maka $xI \subseteq R$ dan $x \in K$, yang berarti $R \subseteq J$. Untuk suatu $0 \neq a \in I$, terdapat *principal ideal* $aR \subseteq I$. Karena $R$ *Noetherian*, teorema 81 menjamin bahwa terdapat bilangan positif $n$ yang terkecil dengan

$$P_1 P_2 \cdots P_n \subseteq aR \subseteq I$$

dimana setiap $P_i$ merupakan *ideal* prima dan $P_i \neq 0$. Karena $I$ prima, maka $I$ mencakup salah satu $P_i$ sebut saja $P_1$. Untuk $n \geq 2$ kita buat

$$I_1 = P_2 \cdots P_n.$$

Karena $n$ adalah bilangan positif terkecil dengan $P_1 \cdots P_n \subseteq aR$, maka $I_1 \nsubseteq aR$. Jika kita pilih $b \in I_1$ dimana $b \notin aR$, maka karena $II_1 = P_1 P_2 \cdots P_n \subseteq aR$,

$bI \subseteq aR$. Jadi $ba^{-1}I \subseteq R$ yang berarti $ba^{-1} \in J$. Tetapi $ba^{-1} \notin R$ karena $b \notin R$, jadi $R \subset J$. Untuk $n = 1$,

$$P_1 \subseteq aR \subseteq I = P_1,$$

jadi $aR = I$. Karena $aR$ merupakan *ideal* prima, maka terdapat $b \in R$ dimana $b \notin aR$, jadi $ba^{-1} \notin R$. Tetapi

$$ba^{-1}I = ba^{-1}aR = bR \subseteq R,$$

yang berarti $ba^{-1} \in J$. Jadi untuk $n = 1$ kita dapati juga $R \subset J$. Melanjutkan pembuktian teorema 82, karena $IJ \subseteq R$ berdasarkan definisi $J$, berarti $IJ$ merupakan *ideal* dari $R$ dan kita dapatkan

$$I = IR \subseteq IJ \subseteq R.$$

Karena $I$ adalah maksimal ($I$ prima), maka $IJ = I$ atau $IJ = R$. Jadi kita tinggal tunjukkan bahwa $IJ \neq I$. Untuk itu kita lihat apa konsekuensinya jika $IJ = I$. Jika $x \in J$ maka $xI \subseteq IJ$ dan karena asumsi $IJ = I$ maka $xI \subseteq I$. Menggunakan induksi kita dapatkan

$$x^n I \subseteq I$$

untuk $n = 1, 2, \ldots$. Untuk $0 \neq r \in I$, $rx^n \in x^n I \subseteq I \subseteq R$, jadi $R[x]$ merupakan *fractional ideal*. Karena $rR[x] \subseteq R$ maka $R[x] \subseteq r^{-1}R$, dan karena $r^{-1}R$ *isomorphic* dengan $R$ sebagai $R$*-module* (yang berarti $r^{-1}R$ *Noetherian* jadi *finitely generated*), maka $R[x]$ merupakan *finitely generated* $R$*-submodule* dari $K$. Berarti $x$ *integral* atas $R$. Karena $R$ *integrally closed* ($R$ adalah *Dedekind domain*) maka $x \in R$, jadi $J \subseteq R$. Tetapi ini merupakan kontradiksi dengan $R \subset J$, jadi tidak mungkin $IJ = I$. Jadi $IJ = R$ dan selesailah pembuktian teorema 82.

**Teorema 83** *Jika $I$ merupakan suatu non-trivial ideal dari suatu Dedekind domain $R$ maka $I$ dapat diuraikan secara unik sebagai*

$$I = P_1 P_2 \cdots P_n$$

*dimana setiap $P_i$ merupakan ideal prima (dan bisa terdapat repetisi dalam produk).*

Mari kita buktikan teorema 83. Untuk membuktikan bahwa setiap *non-trivial ideal* dapat diuraikan sebagai produk, kita buat himpunan $S$ sebagai himpunan dari semua *non-trivial proper ideal* dari $R$ yang tidak dapat diuraikan sebagai produk dari *ideal* prima. Karena $R$ merupakan suatu *Noetherian ring*, jika $S$ tidak kosong, maka $S$ mempunyai elemen yang maksimal, sebut saja $I_0$. Tentu saja $I_0$ tercakup dalam suatu *ideal* maksimal (dan prima) $I_1$ dan berdasarkan teorema 82, $I_1$ mempunyai *inverse* berupa *fractional ideal* sebut saja $J$ (jadi $I_1 J = R$). Kita dapatkan

$$I_0 = I_0 R \subseteq I_0 J \subseteq I_1 J = R.$$

Jadi $I_0 J$ merupakan suatu *ideal*. Mengunakan cara yang sama dengan yang berada dalam pembuktian teorema 82 kita dapat tunjukkan bahwa $I_0 \subset I_0 J$. Karena $I_0$ adalah elemen maksimal $S$, maka $I_0 J$ dapat diuraikan sebagai produk dari *ideal* prima, sebut saja

$$I_0 J = Q_1 Q_2 \cdots Q_m$$

dimana setiap $Q_i$ merupakan *ideal* prima. Jika kita kalikan persamaan dengan $I_1$ kita dapatkan

$$\begin{aligned} I_0 I_1 J &= I_1 Q_1 Q_2 \cdots Q_m, \\ I_0 R &= I_1 Q_1 Q_2 \cdots Q_m, \\ I_0 &= I_1 Q_1 Q_2 \cdots Q_m. \end{aligned}$$

Jadi $I_0$ merupakan produk dari *ideal* prima, suatu kontradiksi karena $I_0 \in S$. Berarti $S$ adalah himpunan kosong, jadi setiap *non-trivial ideal* dalam *Dedekind domain* dapat diuraikan sebagai produk dari *ideal* prima. Untuk menunjukkan bahwa produk tersebut unik (hanya urutannya yang dapat diubah), kita ingin tunjukkan bahwa jika

$$P_1 P_2 \cdots P_n = Q_1 Q_2 \cdots Q_m$$

dimana setiap $P_i$ dan $Q_i$ merupakan *ideal* prima, maka $m = n$ dan urutan faktor bisa diubah hingga $P_i = Q_i$ untuk setiap $1 \leq i \leq n$. Untuk itu kita gunakan induksi. Untuk $n = 1$, $m = 1 = n$ dan $P_1 = Q_1$ karena $P_1$ tidak mungkin diuraikan sebagai produk *ideal* prima. Untuk $n > 1$, jika

$$P_1 P_2 \cdots P_{n-1} = Q_1 Q_2 \cdots Q_{n-1}$$

dimana $P_i = Q_i$ untuk setiap $1 \leq i \leq n-1$, maka $m = n$ dan $P_n = Q_n$ karena $P_n$ tidak mungkin diuraikan sebagai produk *ideal* prima. Jadi $m = n$ dan $P_i = Q_i$ untuk setiap $1 \leq i \leq n-1$. Selesailah pembuktian teorema 83.

Selanjutnya kita akan bahas hubungan antara *ideal* prima dalam $\mathfrak{D}$ dengan *ideal* prima dalam $\mathbf{Z}$. Jika $I$ merupakan *ideal* prima dalam $\mathbf{Z}$ maka $I\mathfrak{D}$ merupakan ekstensi (disebut juga *lifting*) dari $I$ ke $\mathfrak{D}$. Meskipun $I\mathfrak{D}$ belum tentu prima, berdasarkan teorema 83, $I\mathfrak{D}$ dapat diuraikan menjadi

$$I\mathfrak{D} = \prod_{i=1}^{n} P_i^{e_i}$$

dimana setiap $P_i$ merupakan *ideal* prima yang berbeda (*ideal* prima yang sama dikumpulkan menjadi pemangkatan dari *ideal* tersebut). Sebaliknya jika $Q$ merupakan *ideal* prima dalam $\mathfrak{D}$ maka kita dapatkan

$$P = Q \cap \mathbf{Z}$$

sebagai kontraksi dari $Q$ ke $\mathbf{Z}$. Tidak terlalu sulit untuk melihat bahwa $P$ merupakan *ideal* prima dalam $\mathbf{Z}$.

**Teorema 84** *Jika $Q$ merupakan ideal prima dalam $\mathfrak{D}$, maka $Q$ tampil dalam penguraian $P\mathfrak{D}$ jika dan hanya jika $Q \cap \mathbf{Z} = P$.*

Mari kita buktikan teorema 84. Jika $Q \cap \mathbf{Z} = P$ maka $P \subseteq Q$, jadi $P\mathfrak{D} \subseteq Q$ karena $Q$ merupakan *ideal*, yang berarti $Q$ membagi $P\mathfrak{D}$. Jadi $Q$ tampil dalam penguraian $P\mathfrak{D}$. Sebaliknya jika $Q$ membagi $P\mathfrak{D}$ maka $P\mathfrak{D} \subseteq Q$. Jadi

$$P = P \cap \mathbf{Z} \subseteq P\mathfrak{D} \cap \mathbf{Z} \subseteq Q \cap \mathbf{Z}.$$

Karena dalam $\mathbf{Z}$ setiap *ideal* prima juga *ideal* maksimal, maka $P = Q \cap \mathbf{Z}$. Selesailah pembuktian teorema 84.

Selanjutnya kita perlu konsep *norm* dari suatu *ideal*. Jika $H$ adalah suatu *ideal* dalam *ring* $\mathfrak{D}$ maka *norm* dari $H$ adalah banyaknya *coset* $H$ dalam $\mathfrak{D}$ dengan notasi

$$|\mathfrak{D}/H|.$$

**Teorema 85** *Jika $\langle u \rangle$ merupakan principal ideal dengan generator $u$, maka*

$$N(\langle u \rangle) = |N(u)|.$$

Untuk membuktikan teorema 85 kita perlu melihat $\mathfrak{D}$ sebagai *lattice*. Yang dimaksud dengan *lattice* disini adalah ruang titik-titik integral, bukan suatu *partial order*, dan suatu *principal ideal* menjadi *sublattice* dari $\mathfrak{D}$. *Principal ideal* $\langle u \rangle$ ditentukan oleh vektor-vektor yang *linearly independent* sebagai berikut:

$$u, u\alpha, u\alpha^2, \ldots, u\alpha^{d-1}.$$

Jadi $\langle u \rangle$ adalah *sublattice* dari $\mathfrak{D}$ (dengan dimensi $d$). Lebih dari itu,

$$u, u\alpha, u\alpha^2, \ldots, u\alpha^{d-1}$$

adalah basis untuk $\langle u \rangle$. *Covolume* dari suatu *lattice* adalah determinan dari matrik generator. Untuk $\langle u \rangle$, matrik generator adalah matrik pengali untuk $u$, sedangkan untuk $\mathfrak{D}$ matrik generator adalah matrik identitas dengan dimensi $d \times d$:

$$\begin{bmatrix} 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & \ldots & 0 & 1 \end{bmatrix}.$$

*Volume* dari *lattice* adalah nilai mutlak dari *covolume*, dan dapat dipandang sebagai *unit volume* yang dibuat menggunakan basis dari *lattice*. Banyaknya *coset* $\langle u\rangle$ dalam $\mathfrak{D}$ sama dengan *index* $\langle u\rangle$ dalam $\mathfrak{D}$ yaitu rasio *volume* $\langle u\rangle$ dengan *volume* $\mathfrak{D}$. Jika $U$ adalah matrik pengali untuk $u$ dan $I$ adalah matrik identitas, maka

$$\begin{aligned} |\mathfrak{D}/\langle u\rangle| &= \frac{|\det(U)|}{|\det(I)|} \\ &= |\det(U)|. \end{aligned}$$

Jadi

$$\begin{aligned} N(\langle u\rangle) &= |\det(U)| \\ &= |N(u)|. \end{aligned}$$

Berikutnya kita ingin tunjukkan bahwa *norm* untuk *ideal* juga bersifat *multiplicative.*

**Teorema 86** *Jika $I$ dan $J$ merupakan non-trivial ideal dalam ring $\mathfrak{D}$, maka*

$$N(IJ) = N(I)N(J).$$

Untuk membuktikan teorema 86, karena $J$ dapat diuraikan menjadi produk *ideal* prima, kita cukup menunjukkan bahwa

$$N(IP) = N(I)N(P)$$

dimana $P$ merupakan *ideal* prima. Menggunakan teorema 43, kita dapatkan

$$\mathfrak{D}/I \simeq (\mathfrak{D}/IP)/(I/IP).$$

Jadi

$$|\mathfrak{D}/IP| = |\mathfrak{D}/I||I/IP|.$$

Karena $N(IP) = |\mathfrak{D}/IP|$ dan $N(I) = |\mathfrak{D}/I|$, kita tinggal menunjukkan bahwa

$$|I/IP| = |\mathfrak{D}/P| = N(P).$$

Karena *unique factorization* (teorema 83), maka

$$I \neq IP,$$

jadi terdapat $\alpha \in I \setminus IP$. Jika kita buat pemetaan

$$\begin{aligned} f : \mathfrak{D} &\longrightarrow I/IP \\ x &\mapsto x\alpha + IP, \end{aligned}$$

maka tidak terlalu sulit untuk melihat bahwa $f$ merupakan suatu *homomorphism* antara $\mathfrak{D}$-*modules*. Karena $P$ merupakan *ideal* maksimal, maka menggunakan *homomorphism theorem* untuk *modules* yang serupa dengan teorema 39, $f$ *surjective* dengan $\ker(f) = P$, dan kita dapatkan

$$\mathfrak{D}/P \simeq I/IP$$

jadi

$$|I/IP| = |\mathfrak{D}/P| = N(P)$$

dan selesailah pembuktian kita.

Berikutnya adalah teorema yang menghubungkan *ideal* prima dalam $\mathfrak{D}$ dengan bilangan prima dalam $\mathbf{Z}$.

**Teorema 87**

- *Jika $\mathfrak{p}$ adalah ideal dalam $\mathfrak{D}$ dengan $N(\mathfrak{p}) = p$ dimana $p$ merupakan bilangan prima, maka $\mathfrak{p}$ adalah ideal prima dalam $\mathfrak{D}$.*
- *Sebaliknya jika $\mathfrak{p}$ adalah ideal prima dalam $\mathfrak{D}$, maka $N(\mathfrak{p}) = p^f$ untuk suatu bilangan bulat positif $f$.*

Jika $\mathfrak{p}$ merupakan *ideal* dalam $\mathfrak{D}$ dengan $N(\mathfrak{p}) = p$ untuk suatu bilangan prima $p$ maka, karena $|\mathfrak{D}/\mathfrak{p}| = p$,

$$\mathfrak{D}/\mathfrak{p} \simeq \mathbf{Z}/p\mathbf{Z}.$$

Jadi $\mathfrak{D}/\mathfrak{p}$ merupakan suatu *field*, yang berarti $\mathfrak{p}$ adalah *ideal* maksimal, dan karena $\mathfrak{D}$ adalah suatu *Dedekind domain* berarti $\mathfrak{p}$ merupakan *ideal* prima. Jadi kita telah buktikan bagian pertama dari teorema 87. Untuk membuktikan bagian kedua, jika $\mathfrak{p}$ merupakan *ideal* prima dalam $\mathfrak{D}$, maka $\mathfrak{p} \cap \mathbf{Z}$ merupakan *ideal* prima dalam $\mathbf{Z}$ dengan *generator* bilangan prima, sebut saja $p$ (jadi $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$). Kita dapat membuat *principal ideal* $\langle p \rangle$ dalam $\mathfrak{D}$ dan berdasarkan *unique factorization* maka $\langle p \rangle$ dapat ditulis sebagai

$$\langle p \rangle = P_1^{e_1} P_2^{e_2} \cdots P_n^{e_n}$$

dimana $P_1, P_2, \ldots, P_n$ masing-masing adalah *ideal* prima yang berbeda dalam $\mathfrak{D}$ dan $e_1, e_2, \ldots, e_n$ merupakan bilangan bulat positif. Tentunya $p \in P_i$ untuk setiap $1 \leq i \leq n$. Kita juga dapatkan

$$P_1^{e_1} P_2^{e_2} \cdots P_n^{e_n} \subseteq \mathfrak{p}$$

jadi $P_j \subseteq \mathfrak{p}$ untuk suatu $1 \leq j \leq n$. Karena $P_j$ maksimal maka $P_j = \mathfrak{p}$. Jika kita ambil *norm* dari $\langle p \rangle$ maka kita dapatkan

$$N(\langle p \rangle) = N(P_1)^{e_1} N(P_2)^{e_2} \cdots N(P_n)^{e_n}.$$

Kita juga dapatkan

$$N(\langle p \rangle) = |N(p)| = p^d$$

dimana $d$ merupakan dimensi dari $\mathfrak{D}$. Jadi untuk setiap $1 \leq i \leq n$ terdapat bilangan bulat positif $f_i$ dimana $N(P_i) = p^{f_i}$. Jadi

$$N(\mathfrak{p}) = N(P_j) = p^{f_j}.$$

Selesailah pembuktian teorema 87.

## 12.5 Ringkasan

Di bab ini kita telah bahas konsep *algebraic number*. Bab ini dimulai dengan pembahasan struktur aljabar untuk ruang vektor dan *module*, kemudian diikuti oleh konsep *separable field extension*, lalu konsep *norm* dan *trace*, dan terahir *algebraic number theory*. Teori mengenai *algebraic numbers* digunakan dalam metode penguraian *number field sieve*.