BAB II

TEORI PENUNJANG

Dalam bab ini akan dibahas mengenai beberapa teori yang dapat menunjang materi pada bab III dan IV antara lain himpunan, grup, finite field, matriks, serta relasi dan fungsi.

2.1. Himpunan

Definisi 2.1.1.

Himpunan adalah daftar, kumpulan atau kelas obyek yang didefinisikan secara jelas. Obyek-obyek tersebut dapat berupa bilangan, orang, surat, sungai, dan sebagainya. Obyek-obyek tersebut biasa disebut elemen-elemen atau anggota-anggota dari himpunan.

Himpunan-himpunan dinotasikan dengan huruf besar, sedangkan elemen-elemen dengan huruf kecil.

Jika suatu obyek a adalah elemen dari sebuah himpunan A, ditulis

$$a \in A$$

Sedangkan jika suatu obyek a bukan elemen sebuah himpunan A, ditulis

$$a \notin A$$

Definisi 2.1.2.

A disebut subhimpunan dari B, jika semua elemen sebuah himpuan A adalah juga sebuah himpunan B. Secara simbolis,

$$A \subseteq B$$

Selanjutnya, jika A bukanlah subhimpunan B, ditulis $A \not\subset B$.

Definisi 2.1.3.

Dua himpunan A dan B adalah sama, jika dan hanya jika $A \subseteq B$ dan $B \subseteq A$.

Definisi 2.1.4.

B adalah subhimpunan sejati dari A, jika B adalah subhimpunan A dan B tidak sama dengan A. Secara simbolis,

$$B \subseteq A \text{ dan } B \neq A$$

Dua himpunan A dan B dikatakan dapat diperbandingkan (*comparable*) jika,

$$A \subseteq B \text{ atau } B \subseteq A$$

Yaitu, jika salah satu himpunan adalah subhimpunan dari himpunan lainnya. Lainnya, jika himpunan A dan B dikatakan tidak dapat diperbandingkan jika,

$$A \not\subset B \text{ dan } B \not\subset A$$

Yaitu, ada anggota A yang tidak terdapat dalam B dan juga ada anggota B yang tidak terdapat dalam A.

Contoh 2.1.1.

Misalkan $A = \{ 1, 2 \}$ dan $B = \{ 1, 2, 3 \}$. Maka A dapat diperbandingkan dengan B, karena A adalah subhimpunan B.

Contoh 2.1.2.

Misalkan $R = \{ 1, 2 \}$ dan $S = \{ 2, 3, 4 \}$. Maka R dan S tidak dapat diperbandingkan karena $1 \in R$ tetapi $1 \notin S$, dan $3 \in S$ tetapi $3 \notin R$

Teorema 2.1.1.

Jika A adalah subhimpunan B dan B subhimpunan C maka, A adalah subhimpunan C yaitu jika

$$A \subseteq B \text{ dan } B \subseteq C \text{ maka berati } A \subseteq C$$

Bukti :

Misalkan a adalah anggota A, yaitu $a \in A$. Karena A adalah subhimpunan B, maka a juga termasuk B, yaitu $a \in B$. Tetapi, menurut hipotesa, $B \subseteq C$; oleh karena itu setiap anggota B termasuk a adalah juga anggota C. Maka terbukti bahwa $A \subseteq C$.

Definisi 2.1.5.

Himpunan dari himpunan-himpunan disebut keluarga himpunan. Keluarga himpunan dinotasikan dengan huruf-huruf tulisan tangan (script).

$$\mathcal{A}, \mathcal{B}, \ldots.$$

Contoh 2.1.3.

Himpunan {{2, 3}, {2}, {5, 6}} adalah keluarga himpunan-himpunan. Anggota-anggotanya adalah himpunan-himpunan {2, 3}, {2}, dan {5, 6}.

Definisi 2.1.6.

Semua himpunan yang ditinjau adalah subhimpunan dari sebuah himpunan tertentu disebut himpunan semesta.

Himpunan semesta dinyatakan dengan **S**

Definisi 2.1.7.

Keluarga dari semua subhimpunan sebuah himpunan A disebut himpunan kuasa dari A.

Himpunan kuasa dari A biasanya dinyatakan dengan,

$$2^A$$

Contoh 2.1.4.

Misalkan T = { 4, 7, 8 } maka himpunan kuasa dari T adalah :

$$2^T = \{ \{ 4, 7, 8 \}, \{ 4, 7 \}, \{ 4, 8 \}, \{ 7, 8 \}, (4 \}, \{ 7 \}, \{ 8 \}, \{ \varnothing \} \}$$

Definisi 2.1.8.

Himpunan A dan B disebut saling asing, jika himpunan-himpunan A dan B tidak mempunyai elemen-elemen yang dimiliki bersama, artinya tidak ada elemen A yang terdapat dalam B dan tidak ada elemen B yang terdapat dalam A.

Contoh 2.1.5.

Misalkan E = { x, y, z } dan F = { r, s, t }. Maka E dan F saling asing.

2.2. Grup

Definisi 2.2.1.

Operasi biner * pada himpunan A adalah suatu aturan yang menentukan suatu elemen dari A untuk setiap pasangan terurut (a , b) dari elemen-elemen dalam A.

Operasi biner * pada himpunan A dikatakan :

1. Komutatif jika $a * b = b * a$, $\forall\ a, b \in$ A.
2. Assosiatif jika $(a * b) * c = a * (b * c)$, $\forall\ a, b \in$ A.

Definisi 2.2.2.

Misalkan * merupakan operasi biner pada A dan $e \in$ A maka :

1. e disebut elemen identitas kanan untuk * jika $a * e = a$, $\forall\ a \in$ A.
2. e disebut elemen identitas kiri untuk * jika $e * a = a$, $\forall\ a \in$ A.
3. e disebut elemen identitas dua sisi untuk * jika $a * e = e * a = a$, $\forall\ a \in$ A.

Jika e merupakan elemen identitas dua sisi maka cukup disebut elemen identitas.

Definisi 2.2.3.

Misalkan * merupakan operasi biner pada A dan e adalah elemen identitas untuk * dan $a, b \in$ A.

1. Jika $b * a = e$, maka b disebut invers kiri dari a terhadap * dan elemen identitas e.
2. Jika $a * b = e$, maka b disebut invers kanan dari a terhadap * dan elemen identitas e.
3. Jika $b * a = a * b = e$, maka b disebut invers dua sisi dari a terhadap * dan elemen identitas e.
4. Jika b merupakan invers dua sisi dari a, maka cukup disebut b invers dari a. Invers dari a dinotasikan dengan a^{-1}.

Definisi 2.2.4.

Suatu grup (**G**, *) adalah suatu himpunan **G**, dengan suatu operasi biner *, sedemikian sehingga aksioma-aksioma berikut terpenuhi :

1. Operasi biner * bersifat assosiatif.
2. Terdapat elemen identitas $e \in$ **G** terhadap *.

3. Setiap elemen $a \in \mathbf{G}$ mempunyai invers $a^{-1} \in \mathbf{G}$ terhadap elemen identitas e dan *.

Contoh 2.2.1.

Misalkan $\mathbf{G} = \{ a, b, c \}$ dengan operasi biner * sebagai berikut :

*	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Maka (**G**, *) adalah sebuah grup, karena ketiga aksioma grup terpenuhi, yaitu :

1. Operasi biner * bersifat assosiatif

$(a * b) * c = b * c = a$

$a * (b * c) = a * a = a$

2. Terdapat elemen identitas, yaitu a

3. Setiap elemen dalam **G** mempunyai invers, yaitu $a^{-1} = a$, $b^{-1} = c$, $c^{-1} = b$

Definisi 2.2.5.

Suatu grup (**G**, *) disebut abelian jika operasi biner * bersifat komutatif, yaitu $a * b = b * a$, $\forall\ a, b \in \mathbf{G}$.

Definisi 2.2.6.

Misalkan grup (**G**, *), dan misalkan $\mathbf{H} \subseteq \mathbf{G}$. **H** disebut subgrup **G**, jika * merupakan operasi biner pada **H** dan (**H**, *) membentuk grup.

Jika **H** subgrup **G**, dinotasikan $\mathbf{H} < \mathbf{G}$

Contoh 2.2.2.

(**R**, +) adalah suatu grup, $Z \subset \mathbf{R}$ dan (Z, +) adalah grup. Maka (Z, +) adalah subgrup dari (**R**, +).

2.3. Finite Field

Definisi 2.3.1.

Suatu ring $\boldsymbol{R}$ adalah suatu himpunan $\boldsymbol{R}$ dengan dua operasi biner + (penjumlahan) dan • (pergandaan) yang tidak kosong memenuhi aksioma-aksioma dibawah ini :

I. $\boldsymbol{R}$ merupakan grup abelian terhadap operasi penjumlahan, yaitu :

1. Untuk semua a, b, c dalam $\boldsymbol{R}$ berlaku $(a + b) + c = a + (b + c)$.
2. Di dalam $\boldsymbol{R}$ terdapat elemen 0 sedemikian sehingga untuk setiap a dalam $\boldsymbol{R}$ berlaku $0 + a = a + 0 = a$.
3. Untuk setiap a dalam $\boldsymbol{R}$ dapat ditemukan elemen $-a$ sedemikian sehingga $-a + a = a + (-a) = 0$.
4. Untuk setiap a, b dalam $\boldsymbol{R}$ berlaku $a + b = b + a$.

II. Pergandaan mempunyai sifat assosiatif, yaitu :

1. Untuk semua a, b dalam $\boldsymbol{R}$ berlaku $(a \bullet b) \bullet c = a \bullet (b \bullet c)$.

III. Kedua aturan komposisi di atas dihubungkan dengan aksioma distributivitas.

1. Untuk semua a, b, c dalam $\boldsymbol{R}$ berlaku $a \bullet (b + c) = a \bullet b + a \bullet c$ dan $(b + c) \bullet a = b \bullet a + c \bullet a$.

Untuk selanjutnya pergandaan antara $a \bullet b$ cukup ditulis dengan ab.

Definisi 2.3.2.

Field **F** adalah suatu struktur aljabar yang memenuhi aksioma-aksioma ring serta aksioma-aksioma berikut ini :

II. Pergandaan mempunyai sifat assosiatif, yaitu :

2. Adanya elemen e dalam $\boldsymbol{R}$ sedemikian sehingga $ae = ea = a$ untuk setiap a dalam $\boldsymbol{R}$.

3. Untuk setiap a, b dalam $\boldsymbol{R}$ berlaku $ab = ba$.

4. Setiap a dalam $\boldsymbol{R}$ yang tidak sama dengan nol mempunyai invers a^{-1} dalam $\boldsymbol{R}$ yaitu $a^{-1}\, a = a\, a^{-1} = e$.

Jadi **F** merupakan suatu field, jika **F** adalah grup abelian terhadap operasi penjumlahan dan **F** – { 0 } adalah grup abelian terhadap operasi pergandaan.

Definisi 2.3.3.

Daerah integral adalah suatu struktur aljabar yang memenuhi aksioma-aksioma field (selain II.4) dan tidak memuat pembagi nol sejati.

Definisi 2.3.4.

Suatu elemen $a \in \boldsymbol{R}$ dinamakan pembagi nol bila terdapat $b \neq 0 \in \boldsymbol{R}$ sedemikian sehingga $ab = ba = 0$. Apabila $a \neq 0$, maka a disebut pembagi nol sejati.

Contoh 2.3.1.

Jika **F** adalah himpunan dari integer-integer modulo 7 dibawah operasi penjumlahan dan perkalian mod 7. Elemen-elemen dari **F** adalah 7 simbol 0, 1, 2, 3, 4, 5, 6. Maka :

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

.	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

F merupakan grup abelian terhadap penjumlahan dan **F** – { 0 } merupakan grup abelian terhadap pergandaan. Jadi **F** merupakan suatu field. Karena elemen-elemennya hanya terdiri atas bilangan-bilangan terbatas maka disebut suatu finite field.

Teorema 2.2.1.

Ring dari bilangan-bilangan bulat modulo p, yaitu $I_p = \{ \bar{0}, \bar{1}, \bar{2}, \ldots, \overline{p-1} \}$ merupakan field jika hanya jika p prime.

Bukti :

($\Rightarrow$) I_p suatu field maka p prime.

Andaikan p tidak prime maka $p = p_1 p_2$ dengan $p_1 > 1$, $p_2 > 1$. Sehingga $\overline{p_1}\ \overline{p_2} = \overline{p_1 p_2} = \overline{p} = \bar{0}$. Maka terdapat pembagi nol sejati. Jadi I_p bukan field.

($\Leftarrow$) p prime maka I_p suatu field. Ambil dua anggota $\overline{p_1} \neq \bar{0}$ dan $\overline{p_2} \neq \bar{0}$ dari $I_p = \{ \bar{0}, \bar{1}, \bar{2}, \ldots, \overline{p-1} \}$. Jelas hasil pergandaannya, yaitu $\overline{p_1}\ \overline{p_2} = \overline{p_1 p_2}$.

$p_1 p_2$ pasti bukan kelipatan p. Sebab p prime dan suatu hasil ganda itu habis dibagi oleh faktor prime p, hanya apabila sekurang-kurangnya satu faktor habis dibagi oleh p. Karena $p_1 p_2$ bukan kelipatan p maka $\overline{p_1}\ \overline{p_2} \neq \bar{0}$.

Terbukti $\overline{p_1} \neq \overline{0}$ dan $\overline{p_2} \neq \overline{0}$ sehingga $\overline{p_1}\ \overline{p_2} \neq \overline{0}$. Maka I_p tidak memuat pembagi nol sejati, akibatnya I_p suatu field.

Definisi 2.3.5.

Suatu finite field yang terdiri atas p kelas-kelas residu sebagai sisa pembagian (mod p) dengan p adalah bilangan prime disebut Galoid Field berorde p dan dinotasikan dengan GF_p.

Untuk menyederhanakan penulisan maka, untuk selanjutnya elemen-elemen dari suatu Galoid Field akan dituliskan sebagai { 0, 1, 2, ..., p-1 }.

Dalam GF_p terdapat suatu elemen yang disebut sebagai akar primitif dari GF_p.

Definisi 2.3.6.

Suatu integer x disebut sebagai akar primitif dari GF_p, jika x merupakan elemen dari GF_p sedemikian sehingga semua pangkat dari x yang kurang dari ($p - 1$) modulo p adalah semua elemen dalam GF_p kecuali elemen nol yang berbeda satu sama lain dan $x^{p-1} \equiv 1 \pmod{p}$.

Contoh 2.3.2.

Untuk $p = 3$, GF_p mempunyai elemen-elemen { 0, 1, 2 }. Elemen-elemen 2 dan 5 adalah akar primitif dari GF_3 karena hasil pangkat dari 2 dan 5 modulo 3 adalah semua elemen dari GF_3.

$2^0 = 1$ $\quad$ $5^0 = 1$

$2^1 = 2$ $\quad$ $5^1 = 2$

$2^2 = 1$ $\quad$ $5^2 = 1$

Berikut diberikan sebuah tabel dari akar-akar primitif untuk beberapa nilai p.

p	Primitive Root
3	2
5	2
7	3
11	2
13	2
17	3
19	2
23	5

Misalkan ring $\boldsymbol{R}$ dan sebarang simbol x. Dengan $f(x)$, $g(x)$ adalah polinomial-polinomial dalam x,

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots.$$

$$g(x) = b_0 + b_1 x + b_2 x^2 + \ldots.$$

dimana koefisien-koefisiennya berasal dari field GF_p.

Definisi 2.3.7.

Derajat dari polinomial adalah pangkat tertinggi x yang mempunyai koefisien taknol.

Didefinisikan operasi-operasi penjumlahan dan pergandaan dari ring komutatif GF_p [] x [], yaitu :

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \ldots..$$

$$f(x).\, g(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \ldots..$$

Jika derajat $f(x) \geq$ derajat $g(x)$, maka pembagian $f(x)$ dengan $g(x)$ sedemikian sehingga :

$$f(x) = q(x).\, g(x) + r(x).$$

Dengan derajat $r(x)$ < derajat $q(x).g(x)$, dengan $q(x).g(x)$ adalah hasil bagi dan $r(x)$ adalah sisa pembagian $f(x)$ dengan $g(x)$. Apabila $r(x) = 0$ maka $f(x) = q(x).g(x)$ habis dibagi oleh $g(x)$.

Contoh 2.3.3.

Misalkan $p = 5$,

$f(x) = x^4 + 3x^3 + 2x^2 + x + 3$

$g(x) = x^2 + 4x + 2$

Sehingga didapat,

$f(x) = q(x).g(x) + r(x)$

$(x^2 + 4x + 4).(x^2 + 4x + 2) + 2x$

Polinomial $f(x)$ dari $GF_p[|x|]$ disebut reducible dari GF_p apabila dapat dibagi oleh polinomial-polinomial $\phi_1(x)$ dan $\phi_2(x)$ dari $GF_p[|x|]$ berderajat m dan n dengan $m \geq 1, n \geq 1$ sedemikian sehingga :

$$f(x) = \phi_1(x).\phi_2(x)$$

Polinomial $f(x)$ dari $GF_p[|x|]$ disebut irreducible dari GF_p apabila tidak dapat dibagi oleh polinomial-polinomial $\phi_1(x)$ dan $\phi_2(x)$ dari $GF_p[|x|]$ berderajat m dan n dengan $m \geq 1, n \geq 1$.

Contoh 2.3.4.

Polinomial $x^2 + 1$ dari $GF_5[|x|]$ merupakan reducible GF_5, karena $(x^2 + 1)$ dapat dibagi oleh polinomial-polinomial $\phi_1(x) = (x + 2)$ dan $\phi_2(x) = (x + 3)$, sedemikian sehingga :

$$f(x) = x^2 + 1 = (x + 2).(x + 3)$$

Contoh 2.3.5.

Polinomial $x^2 + 2$ dari GF_5 [| x |] merupakan irreducible GF_5, karena $(x^2 + 2)$ tidak dapat dibagi oleh polinomial-polinomial $\phi_1(x)$ dan $\phi_2(x)$.

Definisi 2.3.8.

Polinomial-polinomial $f_1(x)$ dan $f_2(x)$ disebut kongruen modulo $\phi(x)$ jika $f_1(x) - f_2(x)$ dapat dibagi oleh $\phi(x)$ yang merupakan polinomial dari GF_p [| x |]. Secara simbolis,

$$f_1(x) \equiv f_2(x) \text{ [| mod } \phi(x) \text{ |]}$$

Contoh 2.3.6.

Misalkan $p = 5$,

$f_1(x) = x^3 + 2x^2 + x$

$f_2(x) = x^3 + x^2 + x + 4$

karena $f_1(x) - f_2(x) = x^2 + 1$ dapat dibagi oleh $(x + 2)$ atau $(x + 3)$ maka $f_1(x)$ $\equiv f_2(x)$ [| mod $\phi(x)$ |].

Pandang $\phi(x)$ adalah modulus polinomial dan [| $f(x)$ |] adalah kelas semua polinomial yang kongruen dengan $f(x)$. Didefinisikan operasi penjumlahan dan pengandaan kelas-kelas residu tersebut :

$$[|f_1(x)|] + [|f_2(x)|] = [|f_1(x) + f_2(x)|]$$

$$[|f_1(x)|]\,[|f_2(x)|] = [|f_1(x).f_2(x)|]$$

Apabila modulus polinomial $\phi(x)$ adalah irreducible GF_p, maka didapatkan field dari kelas-kelas residu. Misalkan derajat $\phi(x)$ adalah m, dan sebarang kelas $[|f(x)|]$ didefinisikan sebagai :

$$f(x) = \phi(x).q(x) + f_1(x)$$

Dimana derajat $f_1(x)$ < derajat $\phi(x)$. Sedemikian der $f_1(x) \leq m - 1$. Maka $f_1(x)$ disebut sebagai standard representative $[|f(x)|]$, dapat ditulis :

$$f_1(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{m-1} x^{m-1}.$$

Koefisien a_i berasal dari GF_p, sehingga didapatkan nilai p yang berbeda. Sehingga banyaknya standard representative dan kelas-kelas residu modulo $\phi(x)$ adalah p^m sedemikian order dari field GF_p dan $\phi(x)$ terdiri tepat p^m elemen yang berbeda.

Contoh 2.3.7.

Pandang ring komutatif GF_3 $[|x|]$ dengan modulus polinomial $\phi(x)$ adalah $x^2 + 1$. Jelas bahwa $x^2 + 1$ adalah irreducible GF_3. Karena $p = 3$ dan pangkat tertinggi $\phi(x) = 2$, maka order dari field kelas residu $[|\text{mod}(x^2 + 1)|]$ terdiri tepat 9 elemen yang berbeda yaitu :

$|[0|], [|1|], [|2|], [|x|], [|x+1|], [|x+2|], [|2x|], [|2x+1|], [|2x+2|]$

ambil 6 elemen sebarang yaitu $[|x|], [|x+1|], [|x+2|], [|2x|], [|2x+1|], [|2x+2|]$ dan operasikan ke dalam bentuk penjumlahan dan pengandaan.

(i). $[|x|] + [|x+1|] = [|2x+1|]$.

(ii). $[|2x+1|] + [|2x+2|] = [|x|]$.

(iii). $[|x+1|].[|x+2|] = [|1|]$.

(iv). $[|x+1|].[|2x+2|] = [|2x^2 + x + 2|] = [|x|]$.

Definisi 2.3.9.

Suatu finite field yang terdiri atas p^m, dengan p^m adalah bilangan pangkat prime disebut Galoid Field berorde p^m dan dinotasikan dengan GF_p^m .

Definisi 2.3.10.

Suatu elemen taknol θ disebut sebagai elemen primitif dari GF_p^m dan setiap θ memenuhi $\theta^{p^m-1} = 1$ jika semua pangkat dari θ kurang dari $p^m - 1$ adalah berbeda.

Apabila θ adalah elemen primitif, maka :

$\theta^0 (= 1), \theta^1, \theta^2, ..., \theta^{p^m-2}$ mempunyai elemen-elemen yang berbeda. Dengan mengambil $\theta^i \neq 1$, dengan $0 < i < p^m - 1$, kelas $[| x |]$ dapat atau tidak dapat mempunyai elemen primitif, tergantung dari modulus polinomial yang diberikan.

Contoh 2.3.8.

Misalkan field GF_3^2 dan modulus polinomial $\phi(x) = x^2 + x + 2$. Karena hasil semua pangkat dari θ kurang dari $p^m - 1 = 8$ adalah berbeda, maka $[| x |]$ mempunyai elemen primitif.

$$[| x^0 |] = [| 1 |]$$

$$[| x^1 |] = [| x |]$$

$$[| x^2 |] = [| 2x + 1 |]$$

$$[| x^3 |] = [| 2x^2 + x |] = [| 2x + 2 |]$$

$$[| x^4 |] = [| 2x^2 + 2x |] = [| 2 |]$$

$$[| x^5 |] = [| 2x |]$$

$$[|\, x^6 \,|] = [|\, 2x^2 \,|] = [|\, x + 2 \,|]$$

$$[|\, x^7 \,|] = [|\, x^2 + 2x \,|] = [|\, x + 1 \,|]$$

$$[|\, x^8 \,|] = [|\, 1 \,|]$$

Berikut diberikan beberapa fungsi minimum dari modulus polinomial yang telah diketahui agar field GF_p^m mempunyai elemen primitif.

Field	Fungsi Minimum
GF_2^2	$x^2 + x + 1$
GF_2^3	$x^3 + x^2 + 1$
GF_3^2	$x^2 + x + 2$

2.4. Matriks

Definisi 2.4.1.

Matriks adalah himpunan skalar (bilangan riil atau kompleks) yang disusun secara empat persegi panjang (menurut baris-baris dan kolom-kolom).

Skalar-skalar itu disebut elemen matriks. Dan untuk batasannya diberikan:

$$\begin{bmatrix} \quad \end{bmatrix} \text{ atau } \begin{pmatrix} \quad \end{pmatrix} \text{ atau } \begin{Vmatrix} \quad \end{Vmatrix}$$

Matriks diberi nama dengan huruf besar. Secara lengkap ditulis A = (a_{ij}), artinya suatu matriks A dengan elemen baris ke- i dan kolom ke-j adalah a_{ij}.

Pandang suatu matriks A = (a_{ij}), $i = 1, 2, \ldots, m$ dan $j = 1, 2, \ldots, n$; yang berarti bahwa banyaknya baris adalah m serta banyaknya kolom adalah n. Maka dapat dituliskan matriks $A_{(m \times n)}$ = (a_{ij}). ($m \times n$) disebut ukuran (ordo) dari matriks, dengan :

$$A = \begin{bmatrix} a_{11} & a_{12} & .. & a_{1n} \\ a_{21} & a_{22} & .. & a_{2n} \\ : & : & .. & : \\ a_{m1} & a_{m2} & .. & a_{nn} \end{bmatrix}$$

Dua matriks A = (a_{ij}) dan B = (b_{ij}) dikatakan sama A = B, bila ukurannya sama ($m \times n$) dan berlaku $a_{ij} = b_{ij}$ untuk setiap i dan j ($i = 1, 2, .., m$; $j = 1, 2, .., n$).

Pandang suatu matriks A = (a_{ij}) berordo ($m \times n$) maka transpose dari A adalah matriks A^T berukuran ($n \times m$) yang didapatkan dari A dengan menuliskan baris ke-i dari A, $i = 1, 2, .., m$, sebagai kolom ke-i dari A^Tdan kolom ke-j dari A, $j = 1, 2, .., n$, sebagai baris ke-j dari A^T. Maka dapat dituliskan $A^T = (a_{ji})$.

Ada beberapa jenis matriks khusus, antara lain :

1. Matriks bujur sangkar berordo n adalah suatu matriks dengan banyaknya baris sama dengan banyaknya kolom yaitu n. Barisan elemen-elemen $a_{11}, a_{22}, \ldots, a_{nn}$ disebut sebagai diagonal utama dari matriks bujur sangkar tersebut.
2. Matriks diagonal adalah matriks bujur sangkar yang semua elemen diluar diagonal utama adalah nol.
3. Matriks identitas adalah matriks diagonal yang elemen-elemen diagonal utamanya semua = 1. Matriks identitas biasanya ditulis I atau I_n dengan n menyatakan ordo matriks tersebut.
4. Matriks simetris adalah matriks bujur sangkar yang tranposenya sama dengan dirinya sendiri, sehingga $A = A^T$.

Transformasi elementer pada baris dan kolom suatu matriks A adalah sebagai berikut :

1a). Penukaran tempat baris ke-*i* dan baris ke-*j* (baris ke-*i* dijadikan baris ke-*j* dan baris ke-*j* dijadikan baris ke-*i*).

1b). Penukaran tempat kolom ke-*i* dan kolom ke-*j* (kolom ke-*i* dijadikan kolom ke-*j* dan kolom ke-*j* dijadikan kolom ke-*i*).

2a). Memperkalikan baris ke-*i* dengan skalar $\lambda \neq 0$.

2b). Memperkalikan kolom ke-*i* dengan skalar $\lambda \neq 0$.

3a). Menambah baris ke-*i* dengan λ kali baris ke-*j*.

3b). Menambah kolom ke-*i* dengan λ kali kolom ke-*j*.

Definisi 2.4.2.

Matriks A dan B disebut ekivalen (A $\approx$ B) apabila salah satunya dapat diperoleh dari yang lain dengan tranformasi-transformasi elementer terhadap baris dan atau kolom.

Definisi 2.4.3.

Barisan bilangan-bilangan $(j_1, j_2, \ldots, j_n)$ dimana berlaku $j_i \neq j_k$, untuk $i \neq k$ (i dan $k = 1, 2, .., n$) serta j_i salah satu dari bilangan asli (1, 2, .., n) disebut permutasi.

Apabila terdapat n buah bilangan asli 1, 2, .., n, maka banyaknya permutasi yang dapat dibentuk adalah $n ! = n (n - 1) (n - 2) \ldots .2.1$.

Definisi 2.4.4.

Sebuah inversi pada suatu permutasi $(j_1, j_2, \ldots, j_n)$ adalah jika $j_k \prec j_i$ (j_k mendahului j_i) padahal $j_i < j_k$ ($i =$ dan $k = 1, 2, \ldots, n$).

Contoh 2.4.1.

Permutasi (4 3 1 2), banyaknya inversi ada lima yaitu :

(1). $j_1 = 4$ mendahului $j_2 = 3$ padahal $3 < 4$

(2). $j_1 = 4$ mendahului $j_3 = 1$ padahal $1 < 4$

(3). $j_1 = 4$ mendahului $j_4 = 2$ padahal $2 < 4$

(4). $j_2 = 3$ mendahului $j_3 = 1$ padahal $1 < 3$

(5). $j_2 = 3$ mendahului $j_4 = 2$ padahal $2 < 3$

Definisi 2.4.5.

Jika banyaknya inversi dari suatu permutasi adalah bilangan ganjil maka disebut permutasi ganjil dan sebaliknya disebut permutasi genap.

Apabila terdapat n bilangan asli 1, 2, .., n maka banyaknya permutasi n !, yaitu ½ (n !) adalah permutasi genap dan ½ (n !) adalah permutasi ganjil.

2.5. Relasi dan Fungsi

Definisi 2.5.1.

Secara simbolis kalimat " a berada dalam relasi R dengan b " dapat disajikan dengan " a R b " atau " R (a, b) ".

Definisi 2.5.2.

Relasi R disebut refleksif jika dan hanya jika untuk setiap anggota dari semesta **S** berlaku a R a. Secara simbolis,

R refleksif jika dan hanya jika ($\forall a \in \mathbf{S}$). a R a.

Definisi 2.5.3.

Relasi R disebut simetris jika dan hanya jika untuk setiap a, b dalam **S** berlaku jika a R b maka b R a. Secara simbolis,

R simetris jika dan hanya jika ($\forall a, b \in \mathbf{S}$). a R $b \Rightarrow b$ R a.

Definisi 2.5.4.

Relasi R disebut transitif jika dan hanya jika untuk setiap triple a, b, c dari semesta **S**, berlaku apabila a R b dan b R c maka a R c. Secara simbolis,

R transitif jika dan hanya jika ($\forall a, b, c \in \mathbf{S}$). a R b dan b R $c \Rightarrow a$ R c.

Definisi 2.5.5.

Suatu relasi yang sekaligus mempunyai ketiga sifat refleksif, simetris, dan transitif disebut relasi ekuivalensi.

Contoh 2.5.1.

Relasi kesejajaran antara garis-garis lurus pada bidang datar adalah relasi ekuivalensi karena memenuhi ketiga sifat refleksif, simetris, dan transitif.

Teorema 2.5.1.

Suatu relasi ekuivalensi antara anggota-anggota dari suatu semesta **S** mengakibatkan adanya penggolongan (partisi) di dalam **S**.

Penggolongan di dalam **S** dimaksudkan bahwa, **S** terbagi atas himpunan-subhimpunan (golongan-golongan, kelas-kelas) masing-masing bukan himpunan kosong, yang saling asing sedemikian sehingga anggota dari **S** berada dalam salah satu (dan hanya satu) golongan dari **S**.

Bukti :

Misalkan relasi di atas disebut R, maka R memiliki sifat-sifat refleksif, simetris, dan transitif. Semua elemen-elemen yang berada dalam relasi R dengan a, dikumpulkan dalam suatu himpunan Sa. Jadi Sa = $\{ x \in \mathbf{S} \mid x \text{ R } a \}$. Himpunan Sa tidak kosong, karena R refleksif, jadi a R a. Sehingga $a \in$ Sa dan Sa sekurang-kurangnya mempunyai satu anggota. Dari sini disimpulkan bahwa setiap anggota

pasti berada dalam sekurang-kurangnya satu kelas, yaitu kelas yang memuat dirinya sendiri.

Sekarang dibuktikan bahwa apabila dua golongan itu berserikat satu elemen saja maka kedua golongan itu berimpitan .....(1)

Andaikan Sa dan Sb berserikat elemen *c*. Karena $c \in$ Sa maka *c* R *a*. karena R simetris, maka *a* R *c*. $c \in$ Sb maka *c* R b. Dari *a* R *c* dan *c* R *b*, dengan mempergunakan sifat transitif maka *a* R *b*. sehingga $a \in$ Sb. Selanjutnya, untuk setiap $p \in$ Sa berlaku *p* R *a*, dan karena *a* R *b*, dengan mempergunakan sifat R transitif, maka *p* R *b*. Jadi, $p \in$ Sb. Maka terbukti, setiap anggota dari Sa menjadi anggota dari Sb. Yaitu, Sa $\subseteq$ Sb .....(2)

Selanjutnya, karena $c \in$ Sb, maka *c* R *b*. Karena R simetris maka *b* R *c*. $c \in$ Sa maka *c* R *a*. Dari *b* R *c* dan *c* R *a* dengan mempergunakan sifat transitif maka *b* R *a* sehingga $b \in$ Sa. Selanjutnya, untuk setiap $q \in$ Sb berlaku *q* R *b*, dan karena *b* R *a*, dengan mempergunakan sifat R transitif, maka *q* R *a*. Jadi, $q \in$ Sa. Maka terbukti, setiap anggota dari Sb menjadi anggota dari Sa. Jadi Sb $\subseteq$ Sa .....(3)

Dari (2) dan (3) menghasilkan Sa = Sb. Dengan demikian kalimat (1) terbukti. Kontraposisi dari (1) adalah apabila kelas-kelas itu tidak berimpitan maka kedua kelas itu tidak berserikat satu elemen pun, jadi saling asing (disjoint).

Kelas-kelas atau golongan-golongan yang terbentuk karena relasi ekuivalensi disebut kelas-kelas atau golongan-golongan ekuivalensi atau *equivalensi classes.*

Definisi 2.5.6.

Misalkan g merupakan suatu integer positif. Sebarang dua integer a dan b (positif, negatif, atau nol) dikatakan kongruen modulo g jika $a - b$ adalah kelipatan g ditulis,

$a \equiv b \pmod{g}$ bila dan hanya bila $a - b = kg$ ($k = 0, \pm 1, \pm 2, ..$)

Sebaliknya, jika $a - b$ bukan kelipatan g maka a dan b dikatakan tidak kongruen modulo g dan ditulis $a \not\equiv b \pmod{g}$.

Contoh 2.5.2.

$15 \equiv 1 \pmod{7}$, karena $15 - 1 = 14 = 2.7$

$-3 \equiv 11 \pmod{7}$, karena $-3 - 11 = -14 = -2.7$

$13 \not\equiv 2 \pmod{7}$, karena $13 - 2 = 11$, bukan kelipatan 7.

Teorema 2.5.2.

Untuk setiap integer a dan g maka $a \equiv a \pmod{g}$

Bukti :

$a \equiv a \pmod{g}$ karena $a - a = 0 \,.\, g$

Teorema 2.5.3.

Jika $a \equiv b \pmod{g}$ maka $b \equiv a \pmod{g}$

Bukti :

Karena $a - b = k \,.\, g$ maka $b - a = -k\,g$ (suatu kelipatan (negatif) dari g juga). Sehingga $b \equiv a \pmod{g}$.

Teorema 2.5.4.

Jika $a \equiv b \pmod{g}$ dan $b \equiv c \pmod{g}$ maka $a \equiv c \pmod{g}$.

Bukti :

Karena $a \equiv b \pmod{g}$ maka $a - b = k_1 g$ dan karena $b \equiv c \pmod{g}$ maka $b - c = k_2 g$, dengan k_1 dan k_2 adalah integer. Sehingga $a - c = (k_1 + k_2)$ g dan $a \equiv c \pmod{g}$.

Teorema 2.5.5.

Jika $a \equiv b \pmod{g}$, $n > 0$, $g = k_2 g$ maka $a \equiv b \pmod{n}$

Bukti :

Karena $a \equiv b \pmod{g}$ maka $a - b = k_1 g$ dan karena $g = k_2 n$ maka

$$a - b = k_1 (k_2 n)$$

$$a - b = (k_1 \; k_2) n$$

$$a \equiv b \pmod{n}$$

Contoh 2.5.3.

Jika $a = 15$, $b = 3$, $n = 2$, $g = 4 = 2n$ maka

$15 \equiv 3 \pmod{4}$ karena $15 - 3 = 12 = 3.4$.

$15 \equiv 3 \pmod{2}$ karena $15 - 3 = 12 = 6 . 2$

Teorema 2.5.6.

Jika $a \equiv b \pmod{g}$ dan $c \equiv d \pmod{g}$ maka $a + c \equiv b + d \pmod{g}$.

Bukti :

Karena $a \equiv b \pmod{g}$ maka $a - b = k_1 g$ dan karena $c \equiv d \pmod{g}$ maka $c - d = k_2 g$ sehingga :

$$(a + c) - (b + d) = (k_1 + k_2) g$$

$$a + c \equiv b + d \pmod{g}$$

Berdasarkan teorema 2.5.2, 2.5.3 , dan 2.5.4 maka relasi kongruensi adalah suatu relasi ekuivalensi karena memenuhi sifat-sifat refleksif, simetris, dan transitif. Sehingga berdasarkan teorema 2.5.1, maka himpunan integer dapat dibagi kedalam kelas-kelas ekuivalensi yang saling asing sedemikian sehingga sebarang dua integer yang ada dalam satu kelas yang sama adalah kongruen satu sama lain. Kelas tempat integer a berada dinotasikan dengan (a). Jadi, jika a dan b ada dalam satu kelas yang sama maka (a) = (b).

Contoh 2.5.4.

Jika $g = 7$, maka

$$(15) = (1) \text{ karena } 15 \equiv 1 \pmod 7$$

$$(-3) = (11) \text{ karena } -3 \equiv 11 \pmod 7$$

Definisi 2.5.7.

Suatu fungsi / pemetaan / mapping dari suatu himpunan S ke himpunan T (atau S sebagai daerah sumber / domain dan T sebagai daerah kawan / co-domain) adalah suatu aturan yang pada setiap anggota dari S menentukan dengan tunggal satu anggota dalam T.

Setiap fungsi dari S ke T disebut juga fungsi dari S into T. Jika elemen-elemen dari T juga dihabiskan, jadi jika setiap t dalam T mempunyai kawan di dalam S, atau dengan kata lain jika setiap t dalam T berasal dari suatu s dalam S, maka fungsi itu disebut fungsi dari S onto T. Sehingga setiap fungsi yang onto adalah fungsi into, tetapi belum tentu sebaliknya.

Untuk suatu fungsi yang onto berlaku $f(S) = T$. Yaitu daerah hasil berimpitan dengan daerah kawannya. Pemetaan yang onto disebut juga surjektif.

Jika elemen-elemen dari T yang mempunyai kawan dalam S, hanya mempunyai kawan 1, maka pemetaannya disebut injektif. Dan jika setiap elemen dari S menentukan dengan tunggal satu elemen dari T dan sebaliknya, maka pemetaannya disebut bijektif. Dapat dikatakan juga bahwa pada fungsi bijektif, terdapat korespodensi satu-satu bertimbal balik antara elemen-elemen dari S dengan elemen-elemen dari T.