BAB II

TEORI PENUNJANG

2. 1. Bilangan Bulat.

Definisi 2. 1. 1.

Misalkan a dan b bilangan – bilangan bulat, a membagi habis b jika terdapat bilangan bulat c sedemikian sehingga $b = ac$, ditulis $a \mid b$ dan dikatakan a faktor dari b, b kelipatan dari a atau a pembagi dari b.

Teorema 2. 1. 2. Algoritma Pembagian.

Jika a, b bilangan – bilangan bulat dengan $b > 0$, maka terdapat dengan tunggal bilangan – bilangan bulat q dan r sedemikian sehingga

$$a = bq + r, \text{ dengan } 0 \leq r < b.$$

Bukti.

Misalkan S himpunan dari semua bilangan – bilangan bulat x yang dapat ditulis dalam bentuk $x = a - bn$ untuk $n \in Z$, dan misalkan S' himpunan dari semua bilangan – bilangan bulat nonnegatif pada S. Himpunan $S' \neq \phi$. Jika $0 \in S'$ didapat :

$$a - bq = 0 \text{ atau } a = bq + 0.. \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(2.\ 1.\ 1)$$

untuk beberapa q. Jika $0 \notin S'$, maka S' mempunyai elemen terkecil yaitu :

$$r = a - bq \text{ atau } a = bq + r \text{ dengan } r \text{ positif.}$$

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

Sekarang,

$$a - b(q+1) = a - bq - b = r - b \ldots\ldots\ldots\ldots\ldots\ldots\ldots (2.1.2)$$

sehingga $r - b \in S$. Karena r elemen terkecil dalam S' dan $r - b < r$, maka $r - b$ adalah negatif atau $r - b < 0$ dan $r < b$. Kombinasi dari (2. 1. 1) dan (2 1. 2) didapat :

$$a = bq + r \text{ dengan } 0 \le r < b.$$

Akan ditunjukkan bahwa q dan r tunggal.

Andaikan $a = bq_1 + r_1$ dan $a = bq_2 + r_2$ dengan $0 \le r_1 < b$ dan $0 \le r_2 < b$.

Diasumsikan bahwa $r_1 \le r_2$. Ini berarti :

$$0 \le r_2 - r_1 \le r_2 < b.$$

Bagaimanapun, didapat :

$$0 \le r_2 - r_1 = (a - bq_2) - (a - bq_1) = b(q_1 - q_2).$$

Karena $r_2 - r_1$ kelipatan dari b yang lebih kecil dari b, berarti $r_2 - r_1 = 0$ dan $r_1 = r_2$, sehingga $bq_1 = bq_2$ dengan $b \ne 0$. Ini berarti $q_1 = q_2$. Ini membuktikan bahwa q dan r tunggal. ■

Contoh 2. 1. 1.

Misalkan $a = 357$ dan $b = 13$, dengan Algoritma Pembagian didapat $q = 27$ dan $r = 6$ sedemikian sehingga $357 = (13)(27) + 6$. Jika a negatif maka persamaan menjadi $-357 = (13)(-28) + 7$ dengan $q = -28$ dan $r = 7$.

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

Definisi 2. 1. 3.

Suatu bilangan bulat positif d disebut pembagi persekutuan terbesar dari a dan b jika memenuhi sifat – sifat berikut :

1. d / a dan d / b
2. c / a dan c / b berarti c / d.

Selanjutnya pembagi persekutuan terbesar dari a dan b ditulis PPT (a, b).

Teorema 2. 1. 4.

Jika a, b bilangan - bilangan bulat dengan $b \neq 0$, maka terdapat PPT (a, b) sehingga

$$d = am + bn$$

dengan m, n bilangan - bilangan bulat dan d bilangan bulat positif terkecil yang dapat ditulis dalam bentuk ini.

Bukti.

Misalkan a dan b bilangan – bilangan bulat yang salah satunya bukan 0. Jika $b = 0$, maka $a \neq 0$, sehingga $|a| > 0$, $d =$ PPT (a, b) dan

$$d = a \cdot 1 + b \cdot 0 \text{ atau } d = a \cdot (-1) + b \cdot 0.$$

Andaikan $b \neq 0$. Perhatikan S himpunan semua bilangan – bilangan bulat yang dapat ditulis dalam bentuk $ax + by$ untuk beberapa bilangan bulat x dan y. Misalkan S^+ himpunan semua bilangan – bilangan bulat positif dalam S. Himpunan S memuat :

$$b = a \cdot 0 + b \cdot 1 \text{ dan } -b = a \cdot 0 + b \cdot (-1).$$

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

Jadi $S^+ \neq 0$ dan mempunyai elemen positif terkecil d, $d = am + bn$, dan akan ditunjukkan bahwa d adalah PPT (a, b). Dengan Algoritma Pembagian, terdapat bilangan bilangan bulat q dan r sedemikian sehingga $a = dq + r$ dengan $0 \leq r < d$. Dari persamaan ini didapat :

$$r = a - dq = a - (am + bn)q = a(1 - mq) + b(-nq).$$

Jadi r dalam $S = \{ax + by\}$, dan $0 \leq r < d$. Pilih d elemen terkecil dalam S^+, sehingga $r = 0$ dan d / a. Dengan cara yang sama didapat d / b. Jika c / a dan c / b maka $a = ch$ dan $b = ck$ untuk bilangan – bilangan bulat h dan k sehingga

$$\begin{aligned} d &= am + bn \\ &= chm + ckn \\ &= c(hm + kn). \end{aligned}$$

Ini membuktikan bahwa c / d. Dengan definisi 2. 1. 3, d = PPT (a, b).

Akan ditunjukkan bahwa d tunggal.

Andaikan d_1 dan d_2 PPT (a, b), maka d_1 / d_2 dan d_2 / d_1. Karena d_1 dan d_2 bilangan bulat positif. Ini berarti $d_1 = d_2$. ■

PPT $(a, b) = d$ didapat dengan menggunakan Algoritma Euclidean yaitu pengulangan Algoritma Pembagian seperti berikut :

$$a = bq_0 + r_1 \text{ dengan } 0 \leq r_1 < b$$

$$b = q_1 r_1 + r_2 \text{ dengan } 0 \leq r_2 < r_1$$

$$\vdots$$

$$r_k = r_{k+1} \cdot q_{k+1} + r_{k+2} \text{ dengan } r_{k+2} = 0 \text{ atau } 0 \leq r_{k+2} < r_{k+1}.$$

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

Contoh 2. 1. 2.

PPT (1492, 1776) = 4 dan 4 = (1776)(-21) + (1492)(25).

Definisi 2. 1. 5.

Dua bilangan bulat a dan b adalah relatif prima jika PPT $(a, b) = 1$

Definisi 2. 1. 6.

Suatu bilangan bulat p adalah bilangan prima jika $p \geq 1$ dan pembagi dari p adalah ± 1 dan $\pm\ p$.

2. 2. Relasi dan Modulo.

Definisi 2. 2. 1.

Suatu relasi R pada suatu himpunan $A \neq \phi$ adalah suatu himpunan $R \neq \phi$ yang elemen - elemennya adalah pasangan berurutan (x, y) dengan x, y dari A.

Contoh 2. 2. 1.

Misalkan $A = \{-2, -5, 2, 5\}$ dan relasi R pada A didefinisikan sebagai berikut :

$$xRy \Leftrightarrow |x| > |y|.$$

Jadi R = {(5, -2), (5, 2), (-5, -2), (-5, 2)}.

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

Definisi 2. 2. 2.

Suatu relasi R pada himpunan A adalah suatu relasi ekuivalensi jika memenuhi sifat- sifat berikut :

1. Refleksif : xRx, $\forall\ x \in A$

2. Simetris : $xRy \Rightarrow yRx$, $\forall\ x, y \in A$

3. Transitif : xRy dan $yRz \Rightarrow xRz$, $\forall\ x, y, z \in A$.

Contoh 2. 2. 2.

Relasi R pada A didefinisikan sebagai berikut :

$xRy \Leftrightarrow |x| = |y|$ adalah suatu relasi ekuivalensi pada A.

Definisi 2. 2. 3.

Misalkan R suatu relasi ekuivalensi pada himpunan $A \neq \phi$. Himpunan :

$$[a] = \{x \in A / xRa\}$$

disebut klas ekuivalensi yang memuat a.

Dengan adanya relasi ekuivalensi R pada A, maka A terpartisi atas klas - klas ekuivalensi yang saling asing.

Definisi 2. 2. 4.

Misalkan n suatu bilangan bulat positif. Untuk sebarang bilangan bulat a dan b, $(a + b)$ mod n disebut sisa pembagian $(a + b)$ oleh n ; $(a \cdot b)$ mod n disebut sisa pembagian $(a \cdot b)$ oleh n.

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

Contoh 2. 2. 3.

(-2) + (-3) mod 2 = 1 dan (-2)(-3) mod 2 = 0.

Definisi 2. 2. 5.

Misalkan n bilangan bulat positif, $n > 1$ dan x, y bilangan – bilangan bulat, x adalah kongruen y modulo n jika dan hanya jika $x - y$ adalah kelipatan dari n atau $x \equiv y \pmod{n} \Leftrightarrow x - y = kn$, untuk suatu bilangan bulat k.

Teorema 2. 2. 6.

Relasi kongruensi modulo n adalah suatu relasi ekuivalensi pada Z.

Bukti.

Akan ditunjukkan bahwa kongruensi modulo n adalah (1) refleksif, (2) simetris, (3) transitif.

Ambil $n > 1$ dan x, y, z sebarang elemen di Z.

1. $x \equiv x \pmod{n}$ sebab $x - x = (n)(0)$.

2. $x \equiv y \pmod{n} \Rightarrow x - y = nq$ dengan $q \in Z$.

$\Rightarrow y - x = n(-q)$ dengan $-q \in Z$.

$\Rightarrow y \equiv x \pmod{n}$,

sehingga $x \equiv y \pmod{n} \Rightarrow y \equiv x \pmod{n}$.

3. $x \equiv y \pmod{n}$ dan $y \equiv z \pmod{n}$

$\Rightarrow x - y = nq$ dan $y - z = nk$ dengan $q, k \in Z$.

$\Rightarrow x - z = x - y + y - z$

$= n(q + k)$, dengan $(q + k) \in Z$.

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

sehingga $x \equiv y \pmod{n}$ dan $y \equiv z \pmod{n} \Rightarrow x \equiv z \pmod{n}$. ■

Contoh 2. 2. 4.

Relasi kongruensi modulo 4 pada Z didefinisikan sebagai berikut :

$xRy \Leftrightarrow x \equiv y \pmod{4}$,

adalah suatu relasi ekuivalensi pada Z.

Dengan adanya relasi ekuivalensi R pada Z, klas – klas ekuivalensi untuk kongruensi modulo 4 membentuk suatu partisi dari Z yang memisahkan Z ke dalam himpunan – himpunan bagian yang saling asing. Himpunan – himpunan bagian yang saling asing ini disebut klas – klas kongruensi atau klas – klas sisa. Relasi kongruensi ini memuat 4 klas - klas kongruensi modulo 4 yang saling asing yaitu :

$[0] = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$

$[1] = \{\ldots, -7, -3, 1, 5, 9, \ldots\}$

$[2] = \{\ldots, -6, -2, 2, 6, 10, \ldots\}$

$[3] = \{\ldots, -5, -1, 3, 7, 11, \ldots\}$.

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

2. 3. Grup

Definisi 2. 3. 1.

Suatu himpunan $G \neq \phi$ dengan suatu operasi * di dalam G disebut grup jika memenuhi sifat - sifat berikut :

1. Tertutup :

$(\forall x,y \in G)(\exists z \in G)\, x * y = z.$

2. Assosiatif :

$(\forall x, y, z \in G)\, (x * y) * z = x * (y * z).$

3. $(\forall x \in G)(\exists e \in G)\, e * x = x * e = x.$

Selanjutnya elemen e disebut elemen identitas.

4. $(\forall a \in G)(\exists b \in G)\, a * b = b * a = e.$

Selanjutnya elemen b disebut invers dari elemen a.

Contoh 2. 3. 1.

$Z_7 - \{[0]\} = \{ [1], [2],\ldots, [6]\}$pada klas – klas kongruensi modulo 7 membentuk suatu grup terhadap penggandaan modulo 7.

Definisi 2. 3. 2.

Jika dalam grup G memenuhi sifat :

$$x * y = y * x, \forall x, y \in G,$$

maka G disebut grup komutatif atau grup abelian.

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

Contoh 2. 3. 2.

Z_8 = {[0], [1], [2],..., [7]} pada klas – klas kongruensi modulo 8 membentuk suatu grup abelian terhadap penjumlahan modulo 8.

Definisi 2. 3. 3.

Grup G disebut grup siklik jika terdapat $a \in G$ sedemikian sehingga

$$G = \langle a \rangle = \{x \in G / x = a^n; n \in G\}.$$

Selanjutnya a disebut pembangun dari grup G.

Contoh 2 . 3. 3.

H = {[1], [2], [4]} dari Z_7. $H \subset Z_7$ dan H membentuk subgrup abelian terhadap penggandaan modulo 7 dan H adalah grup siklik dengan elemen pembagun [2] dan [4].

Definisi 2. 3. 4.

Misalkan $H \neq \phi$, $H \subset G$. H disebut subgroup G jika H adalah grup dengan operasi * yang sama dengan grup G.

Contoh 2. 3. 4.

H = {[0], [2], [4], [6]} dari Z_8. $H \subset Z_8$ dan H membentuk suatu grup terhadap penjumlahan modulo 8.

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

Definisi 2. 3. 5.

Misalkan H suatu subgrup dari grup G. Untuk sebarang elemen a di G,

$aH = \{x \in G / x = ah ; h \in H\}$ disebut koset kiri dari H di G,

$Ha = \{x \in G / x = ha ; h \in H\}$ disebut koset kanan dari H di G.

Contoh 2. 3. 5.

Koset – koset dari $H = \{[1], [2], [4]\}$ di Z_7 : [1]H = [2]H = [4]H ={[1], [2], [4]}

dan [3]H = [5]H = [6]H = {[3], [5], [6]}.

2. 4. Ring dan Lapangan

Definisi 2. 4. 1.

Suatu himpunan R dengan operasi penjumlahan dan penggandaan disebut Ring jika memenuhi sifat – sifat berikut :

I. R grup abelian terhadap penjumlahan.

II. 1. Tertutup : $(\forall x, y \in R)(\exists z \in R)\, x \cdot y = z$.

2. Assosiatif : $(\forall a, b, c \in R)\, a \cdot (b \cdot c) = b \cdot (a \cdot c)$.

III. 1. Distributif kiri : $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$, $\forall x, y, z \in R$.

2. Distributif kanan : $x \cdot (y + z) = (x \cdot y) + (x \cdot z), \forall\, x, y, z \in R$.

Jika ring R memenuhi sifat $x * y = y * x$, $\forall\, x, y \in R$, maka R disebut ring komutatif.

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

Definisi 2. 4. 2.

Suatu ring F disebut Lapangan jika F - $\{0\}$ adalah grup abelian terhadap penggandaan.

Jadi setiap elemen $a \neq 0$ dalam F memuat invers terhadap penggandaan yang ditulis : a^{-1}.

Contoh 2. 4. 1.

$(Q, +, \cdot)$ dan $(R, +, \cdot)$ adalah lapangan.

2. 5. Ruang Vektor

Definisi 2. 5. 1.

Himpunan V disebut suatu ruang vektor atas lapangan F jika V adalah grup abelian terhadap penjumlahan dan untuk setiap $x \in V$ dan $a \in F$, terdapat suatu elemen $ax \in V$ sedemikian sehingga, untuk setiap $a, b \in F$ dan $x, y \in V$ berlaku :

1. $a \cdot (x + y) = a \cdot x + a \cdot y$.
2. $(a + b) \cdot x = a \cdot x + b \cdot x$.
3. $(ab) \cdot x = a(b \cdot x)$.
4. $(\exists\, e \in F)\ e \cdot x = x$.

Selanjutnya elemen – elemen dalam V disebut vektor dan elemen – elemen dalam F disebut skalar.

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

Contoh 2. 5. 1.

$V = \left\{ \begin{bmatrix} a & a+b \\ a+b & b \end{bmatrix} / a, b \in R \right\}$ adalah suatu ruang vektor atas R.

Definisi 2. 5. 2.

Himpunan vektor - vektor $\{ v_1, v_2, \ldots, v_n \}$ dikatakan membangun ruang vektor V jika setiap elemen v di V dapat dinyatakan sebagai kombinasi linier dari $\{ v_1, v_2, \ldots, v_n \}$ yaitu : $a_1v_1 + a_2v_2 + \ldots - a_nv_n = V$,

dengan $a_1, a_2, \ldots, a_n$ adalah skalar.

Contoh 2. 5. 2.

Vektor – vektor $i = (1, 0, 0)$, $j = (0, 1, 0)$, $k = (0, 0, 1)$ membangun R^3 .

Definisi 2. 5. 3.

Himpunan vektor - vektor $\{ v_1, v_2, \ldots, v_n \}$ dikatakan tak bebas linier atas lapangan F, jika ada elemen – elemen $a_1, a_2, \ldots, a_n$ dari F yang tidak semuanya nol, sedemikian sehingga $a_1v_1 + a_2v_2 + \ldots + a_nv_n = 0$. Jika $a_1 = a_2 = \ldots = a_n = 0$ sedemikian sehingga $a_1v_1 + a_2v_2 + \ldots + a_nv_n = 0$, maka$\{ v_1, v_2, \ldots, v_n \}$ disebut bebas linier atas F.

Contoh 2. 5. 3.

$B = \left\{ \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \right\}$ adalah bebas linier atas R.

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

Definisi 2. 5. 4.

Misalkan V suatu ruang vektor atas F. Suatu himpunan bagian B pada V disebut basis untuk V jika B adalah bebas linier atas F dan B membangun V.

Contoh 2. 5. 4.

$B = \left\{ \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \right\}$ adalah suatu basis untuk V atas R.

2. 6. Ring Polinomial

Definisi 2. 6. 1.

Misalkan R suatu ring komutatif dengan elemen satuan e dan x suatu simbol yang disebut indeterminate. Dibentuk $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x^1 + a_0 x^0 = \sum_{i=0}^{n} a_i x^i$, dengan a_i dalam R dan n bilangan bulat nonnegatif. Ditetapkan $a_i x^i = x^i a$, $0 \leq i \leq n$. Selanjutnya $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x^1 + a_0 x^0$ disebut polinomial atas R dalam indeterminate x(polinomial dalam x dengan koefisien – koefisien dalam R). Jika setiap koefisien dari $f(x)$ berharga nol maka $f(x)$ disebut polinomial nol. Bilangan bulat terbesar n dimana koefisien dari x^n tidak nol disebut derajat dari $f(x)$ dengan notasi deg $f(x)$ dan koefisien a_n disebut koefisien utama dari $f(x)$. Jika $a_n = 1$,

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

maka $f(x)$ disebut polinomial monic. Misalkan $f(x) = \sum_{i=0}^{n} a_i x^i$, $f(x)$ dikatakan mempunyai derajat n jika $a_n \neq 0$. Jika $f(x) = \sum_{i=0}^{n} a_i x^i$ dan $g(x) = \sum_{i=0}^{n} b_i x^i$ maka $f(x) = g(x)$ jika dan hanya jika $a_i = b_i$, untuk setiap i.

Contoh 2. 6. 1.

$f(x) = 5x^3 + 0\,x^2 - -4x^1 + 2x^0$ suatu polinomial dalam x atas ring Z.

Definisi 2. 6. 2.

Misalkan R suatu ring komutatif dengan elemen satuan dan $R[x]$ himpunan semua polinomial – polinomial dalam x atas R. Misalkan $f(x) = \sum_{i=0}^{n} a_i x^i$ dan $g(x) = \sum_{i=0}^{m} b_i x^i$ dalam R[x], maka

$$f(x) + g(x) = \sum_{i=0}^{k} (a_i + b_i) x^i ,$$

dengan k bilangan bulat terbesar antara m, n,

dan

$$f(x) \cdot g(x) = \sum_{i=0}^{n+m} c_i x^i ,$$

dengan $c_i = a_0 b_0 + a_1 b_1 + \ldots + a_{i-1} b_1 + a_i b_0$.

Selanjutnya $R[x]$ dengan operasi penjumlahan dan penggandaan seperti di atas adalah suatu ring dan disebut ring polinomial atas R dalam indeterminate x.

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

Contoh 2. 6. 2.

Misalkan $f(x) = 1x^0 + 5x^1 + 3x^3$ dan $g(x) = 4x^0 + 2x^1$ dalam Z_6

$$f(x) + g(x) = \sum_{i=0}^{k}(a_i + b_i)x^i = (1+4)x^0 + (5+2)x^1 + (0+0)x^2 + (3+0)x^3$$

$$= 5x^0 + x^1 + 3x^3$$

$$f(x) \cdot g(x) = 4x^0 + 4x^1 + 4x^2.$$

Teorema 2. 6. 3. Algoritma Pembagian untuk $F[x]$

Jika F adalah lapangan dan $f(x)$, $g(x) \in F[x]$ dengan $g(x) \neq 0$, maka terdapat dengan tunggal polinomial - polinomial $q(x)$ dan $r(x)$ di dalam $F[x]$ sedemikian sehingga

$$f(x) = g(x)q(x) + r(x) \qquad \ldots(1)$$

dengan $r(x) = 0$ atau deg $r(x) <$ deg $g(x)$.

Bukti.

1. Jika $f(x) = 0$ atau deg $f(x) <$ deg $g(x)$ maka persamaan (1) menjadi

$$f(x) = g(x)(0) + f(x)$$

berarti $q(x) = 0$ dan $r(x) = f(x)$ memenuhi sifat yang ditentukan.

2. Jika deg $g(x) = 0$, maka $g(x) = c$ untuk suatu konstanta c. Persamaan (1) menjadi $f(x) = c[c^{-1}f(x)] + 0$, berarti $q(x) = c^{-1}f(x)$ dan $r(x) = 0$ memenuhi sifat yang ditentukan.

Andaikan $f(x) \neq 0$ dan $1 \leq$ deg $g(x) \leq$ deg $f(x)$. Bukti dengan induski matematika.Untuk setiap bilangan bulat positif n, misalkan S_n suatu pernyataan

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

bahwa jika $f(x) \in F[x]$ mempunyai derajat n dan $1 \leq \deg g(x) \leq \deg f(x)$, maka ada $q(x)$ dan $r(x) \in F[x]$ sedemikian sehingga

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

dengan $r(x) = 0$ atau $\deg r(x) < \deg g(x)$.

Jika $n = 1$, maka sifat $1 \leq \deg g(x) \leq \deg f(x) = n$ memerlukan $g(x)$ dan $f(x)$ yang berderajat 1, misalkan $g(x) = ax + b$ dan $f(x) = cx + d$

dengan $a \neq 0$ dan $c \neq 0$. Persamaan

$cx + d = (ax + b)(ca^{-1}) + (d - bca^{-1})$,

berarti $q(x) = ca^{-1}$ dan $r(x) = d - bca^{-1}$ memenuhi sifat yang ditentukan, dan S_1 benar.

Jika k bilangan bulat positif sedemikian sehingga S_m benar untuk semua bilangan bulat positif $m < k$. Untuk membuktikan bahwa S_k benar, misalkan $f(x) \in F[x]$ dengan $\deg f(x) = k$ dan $g(x) \in F[x]$ dengan

$1 \leq \deg g(x) \leq \deg f(x)$,

maka

$g(x) = ax^j + \ldots, f(x) = cx^k + \ldots$

dengan $a \neq 0$, $c \neq 0$, dan $j \leq k$. Langkah pertama dengan menggunakan pembagian panjang $f(x)$ oleh $g(x)$ seperti ditunjukkan dibawah,

$$\begin{array}{r|l} & ca^{-1}x^{k-j} \\ \hline ax^j + \cdots & cx^k + \cdots \\ & \underline{ca^{-1}x^{k-j}g(x)} \\ & f(x) - ca^{-1}x^{k-j}g(x) \end{array}$$

menghasilkan

$$f(x) = ca^{-1}x^{k-j}g(x) + [f(x) - ca^{-1}x^{k-j}g(x)].$$

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

Jika $h(x) = f(x) - ca^{-1}x^{k-j}g(x)$, maka koefisien x^k dalam $h(x)$ adalah nol, dan deg $h(x) < k$. Dengan hipotesa induksi, ada polinomial – polinomial $q_0(x)$ dan $r(x)$ sedemikian sehingga

$h(x) = g(x)q_0(x) + r(x)$ dengan $r(x) = 0$ atau deg $r(x) <$ deg $g(x)$. Ini menghasilkan persamaan $f(x) = ca^{-1}x^{k-j}g(x)$

$$= ca^{-1}x^{k-j}g(x) + g(x)q_0(x) + r(x)$$

$$= g(x)[f(x) - ca^{-1}x^{k-j} + q_0(x)] + r(x),$$

berarti $q(x) = ca^{-1}x^{k-j} + q_0(x)$ dan $r(x)$ adalah polinomial – polinomial yang memenuhi sifat yang ditentukan. Oleh karena itu S_k adalah benar,

Akan ditunjukkan bahwa $q(x)$ dan $r(x)$ tunggal. Andaikan $f(x) = g(x)q_1(x) + r_1(x)$ dan $f(x) = g(x)q_2(x) + r_2(x)$ dengan $r_i(x) = 0$ atau deg $r_i(x) <$ deg $g(x)$ untuk $i = 1, 2$, maka

$$r_1(x) - r_2(x) = [f(x) - g(x)q_1(x)] - [f(x) - g(x)q_2(x)]$$

$$= g(x)[q_2(x) - q_1(x)].$$

Pada persamaan sisi kanan, $g(x)[q_2(x) - q_1(x)]$ adalah nol atau mempunyai derajat lebih besar atau sama dengan deg $g(x)$. Pada sisi kiri, $r_1(x) - r_2(x)$ adalah nol atau mempunyai derajat lebih kecil daripada deg $g(x)$ karena deg $r_1(x) <$ deg $g(x)$ dan deg $r_2(x) <$ deg $g(x)$. Ini menunjukkan bahwa $r_1(x) = r_2(x)$ dan $q_1(x) = q_2(x)$ sebab $g(x)$ bukan harga nol. Oleh karena itu $q(x)$ dan $r(x)$ adalah tunggal. ■

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

Contoh 2. 6. 3.

Misalkan $f(x) = 4x^4 + 2x^3 + 6x^2 + 4x + 5$ dan $g(x) = 3x^2 + 2$ dalam $Z_7[x]$, dengan Algoritma Pembagian didapat $q(x) = 6x^2 + 3x + 5$ dan $(x) = 5x + 2$, sehingga

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

atau

$$4x^4 + 2x^3 + 6x^2 + 4x + 5 = (6x^2 + 3x + 5)(3x^2 + 2) + 5x + 2.$$

Definisi 2. 6. 4.

Misalkan $f(x) \neq 0$, $g(x) \neq 0$, $d(x)$ dalam $F[x]$. Suatu polinomial monic $d(x)$ disebut pembagi persekutuan terbesar dari $f(x)$ dan $g(x)$ jika memenuhi sifat- sifat berikut :

1. $d(x) / f(x)$ dan $d(x) / g(x)$
2. $h(x) / f(x)$ dan $h(x) / g(x) \Rightarrow h(x) / d(x)$.

Selanjutnya pembagi persekutuan terbesar dari $f(x)$ dan $g(x)$ ditulis PPT $(f(x), g(x))$

Teorema 2. 6. 5.

Jika $f(x) \neq 0$ dan $g(x) \neq 0$ dalam $F[x]$, maka terdapat dengan tunggal polinomial monic derajat terkecil $d(x)$ = PPT $(f(x), g(x))$ dalam $F[x]$ sedemikian sehingga $d(x) = f(x)s(x) + g(x)t(x)$ dengan $s(x)$ dan $t(x)$ dalam $F[x]$.

Untuk mendapatkan $d(x)$ = PPT $(f(x), g(x))$, digunakan Algoritma Euclidean yaitu pengulangan Algoritma Pembagian seperti berikut ini :

$f(x) = q_0(x)g(x) + r_1(x)$, dengan $0 < \deg r_1(x) < \deg q_0(x)$,

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

$$g(x) = q_1(x)r_1(x) + r_2(x), \text{ dengan } 0 < \deg r_2(x) < \deg r_1(x),$$

$$\vdots$$

$$r_{i-1}(x) = q_i(x)r_i(x) + r_{i+1}(x),$$

dengan $\deg r_{i+1}(x) = 0$ atau $0 < \deg r_{i+1}(x) < \deg r_i(x)$, untuk $0 \le i < n$.

Contoh 2. 6. 4.

Perhatikan polinomial - polinomial dalam $GF(5)[x]$.

$$f(x) = x^8 + 4x^7 + 4x^6 + 4x^5 + 4x^4 + 2x^3 + x + 2.$$

$$g(x) = x^6 + 3x^5 + 4x^4 + 2x^3 + 3x^2 + 2.$$

PPT $(f(x), g(x)) = 2x^2 + x + 4$.

PPT monic $(f(x), g(x)) = 3(2x^2 + x + 4) = x^2 + 3x + 4$.

$s(x) = 4x^2 + x + 1$ dan $t(x) = x^4 + 4x + 1$.

2. 7. Faktorisasi dalam $F[x]$

Definisi 2. 7. 1.

Misalkan $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1x^1 + a_0x^0 = \sum_{i=0}^{n} a_i x^i$ dalam $F[x]$.

Jika c suatu elemen dalam F sedemikian sehingga $f(c) = 0$, maka c disebut harga nol dari $f(x)$, atau c disebut akar atau solusi dari persamaan $f(x) = 0$. Jika $(x - c) / f(x)$ maka $(x - c)$ disebut faktor dari $f(x)$.

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

Contoh 2. 7. 1.

Perhatikan $f(x) = x^2 + 1$ dalam $Z_5[x]$. Karena $f(3) = 3^2 + 1 = 0$ dalam Z_5, maka 3 adalah harga nol dari $x^2 + 1$ atau 3 adalah akar dari $x^2 + 1$atas Z_5.

Teorema 2. 7. 2. Teorema Sisa

Jika $f(x)$ suatu polinomial dalam $F[x]$ dan c dalam F, maka sisa pembagian dari $f(x)$ oleh $(x - c)$ adalah $f(c)$.

Bukti.

Karena (x - c) dan $f(x)$ dalam $F[x]$ maka menurut Algoritma Pembagian

$$f(x) = (x - c)q(x) + r, \text{ dengan deg } r < \text{deg } (x - c).$$

Karena $(x - c)$ berderajat satu, maka deg $r = 0$ atau r suatu konstanta.

Jadi $r = f(c)$. ■

Teorema 2. 7. 3. Teorema faktor

Suatu polinomial $f(x)$ atas lapangan berhingga F memuat suatu faktor $(x - c)$ dalam $F[x]$ jika dan hanya jika c dalam F adalah harga nol dari $f(x)$.

Bukti.

Dari Teorema Sisa , didapat :

$f(x) = (x - c)q(x) + f(c)$

Jadi $(x - c)$ suatu faktor dari $f(x)$ jika dan hanya jika $f(c) = 0$. ■

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

Teorema 2. 7. 4.

Misalkan $f(x)$ suatu polinomal dalam $F[x]$ yang mempunyai derajat n dan koefisien utama a. Jika $c_1, c_2, c_3, \ldots, c_n$ adalah n harga nol yang berlainan dari $f(x)$ dalam F, maka

$$f(x) = a(x - c_1)(x - c_2)(x - c_3)\cdots(x - c_n)$$

Bukti.

Bukti dengan induksi matematika pada $n = \deg f(x)$. Untuk setiap bilangan bulat positif n, misalkan S_n suatu pernyataan dari Teorema .

Untuk $n = 1$, $f(x)$ mempunyai derajat 1 dan koefisien utama a, dan misalkan c_1 suatu penghasil nol dari $f(x)$ dalam F, maka $f(x) = ax + b$ dengan $a \neq 0$ dan $f(c_1) = 0$. Ini berarti $ac_1 + b = 0$ dan $b = -ac$. Karena itu

$f(x) = ax_1 - ac_1 = a(x - c_1)$ dan S_1 benar.

Diasumsikan bahwa S_k benar, dan misalkan $f(x)$ suatu polinomial dengan koefisien utama a dan berderjat $k + 1$ harga nol yang berlainan

$c_1, c_2, c_3, \ldots, c_k, c_{k+1}$ dalam F. Karena c_{k+1} suatu harga nol dari $f(x)$, maka

$$f(x) = (x - c_{k+1})q(x),$$

dengan Teorema Faktor dan Definisi 2. 6. 2, $q(x)$ mempunyai derajat k. Karena faktor $(x - c_{k+1})$ monic, maka $q(x)$ dan $f(x)$ mempunyai koefisien utama yang sama. Untuk $i = 1, 2, 3, \ldots, k$, didapat :

$(c_i - c_{k+1})q(c_i) = f(c_i) = 0$ dengan $(c_i - c_{k+1}) \neq 0$,

sehingga $q(c_i) = 0$ untuk $i = 1, 2, \ldots, k$, maka $c_1, c_2, c_3, \ldots, c_k$ adalah harga nol dari $q(x)$ dalam F, sehingga

$$q(x) = a(x - c_1)(x - c_2)(x - c_3)\cdots(x - c_k).$$

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

Substitusikan $q(x)$ ke dalam $f(x) = (x - c_{k+1})q(x)$ menghasilkan $f(x) = a(x - c_1)(x - c_2)(x - c_3) \cdots (x - c_k)(x - c_{k+1})$. Karena S_k benar ketika S_{k+1} benar, maka S_n benar untuk semua bilangan bulat.

Jadi $f(x) = a(x - c_1)(x - c_2)(x - c_3)\cdots(x - c_k)(x - c_{k+1})$. ■

Akibat 2. 7. 4.

Suatu polinomial derajat n dalam $F[x]$ paling banyak mempunyai n harga nol yang berlainan dalam F.

Contoh 2. 7. 2.

Diketahui 1 harga nol dari $f(x) = x^4 + 3x^3 + 2x + 4$ dalam $Z_5[x]$, sehingga faktorisasinya : $f(x) = (x - 1)^3(x + 1)$ dalam $Z_5[x]$.

Definisi 2. 7. 5.

Suatu polinomial $f(x) \in F[x]$ disebut tak tereduksi atas F jika $f(x)$ tidak dapat dinyatakan sebagai penggandaan dua polinomial $h(x)$ dan $g(x)$ dalam $F[x]$ dengan deg $h(x)$ dan deg $g(x)$ kurang dari deg $f(x)$. Jika $f(x) = h(x)g(x)$ maka $f(x)$ disebut tereduksi atas F.

Contoh 2. 7. 3.

$f(x) = x^3 + 3x + 2$ dalam $Z_5[x]$ tak tereduksi atas Z_5.

$f(x) = x^2 - 2$ dalam $R[x]$ tereduksi atas R, sebab $x^2 - 2 = (x - 2^{1/2})(x + 2^{1/2})$.

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

Teorema 2. 7. 6.

Jika $f(x)$ berderajat 2 atau 3 dalam $F[x]$, maka $f(x)$ tereduksi atas F jika dan hanya jika $f(x)$ mempunyai harga nol dalam F.

Bukti.

Karena $f(x)$ tereduksi maka $f(x) = h(x)g(x)$, dengan deg $g(x)$ dan deg $h(x) <$ deg $f(x)$. Karena $f(x)$ kuadratik atau kubik maka $g(x)$ atau $h(x)$ mempunyai derajat 1.

Jika $g(x)(x - c)$ maka $g(c) = 0$, sehingga

$f(c) = h(c)g(c) = h(c)0 = 0$,

$f(x)$ mempunyai harga nol dalam F. Jadi c harga nol dari $f(x)$.

Sebaliknya, dari Teorema Sisa didapat : $f(x) = (x - c)q(x) + f(c)$. Jika $f(c) = 0$ untuk c dalam F, maka $(x - c)$ faktor dari $f(x)$. Jadi $f(x)$ tereduksi atas F. ■

Contoh 2. 7. 4.

$f(x) = x^3 + 2x^2 - 3x + 4$ dalam $Z_5[x]$, $f(x)$ tereduksi atas Z_5 karena 3 suatu harga nol dari $f(x)$.

Teorema 2. 7. 7.

Jika $f(x)$ suatu polinomial tak tereduksi atas lapangan F dan $f(x)$ membagi habis $f(x)g(x)$ dalam $F[x]$, maka $p(x) / f(x)$ atau $p(x) / g(x)$ dalam $F[x]$.

Bukti

Misalkan $p(x)$ tak tereduksi atas F dan $p(x)$ membagi habis $f(x)g(x)$ yaitu

$f(x)g(x) = p(x)q(x)$ untuk suatu $q(x)$ dalam $F[x]$.....(2.7.1).

Jika $p(x) / f(x)$, persamaan (2.7.1) terpenuhi . Misalkan $p(x)$ tidak membagi habis

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)

$f(x)$. Ini berarti bahwa PPT $(f(x), p(x)) = 1$. Dengan Teorema 2. 7. 5, terdapat $s(x)$ dan $t(x)$ dalam $F[x]$ sedemikian sehingga

$$1 = f(x)s(x) + p(x)t(x)$$

sehingga

$$\begin{aligned} g(x) &= g(x)[f(x)s(x) + p(x)t(x)] \\ &= f(x)g(x)s(x) + g(x)p(x)t(x) \\ &= p(x)q(x)s(x) + p(x)g(x)t(x) \\ g(x) &= p(x)[q(x)s(x) + g(x)t(x)], \end{aligned}$$

sehingga $p(x)$ membagi habis $g(x)$.

Jadi $p(x)$ membagi habis $g(x)$ jika $p(x)$ tidak membagi habis $f(x)$. ■

Contoh 2. 7. 5.

Faktorisasi $f(x) = 2x^4 + x^3 + 3x^2 + 2x + 4$ atas lapangan Z_5.

$f(0) = 4, f(1) = 2, f(2) = 0, f(3) = 1, f(4) = 1$. Jadi 2 harga nol dari $f(x)$.

$f(x) = 2(x - 2)^2(x^2 + 2x + 3) = a(x)b(x)$.

$a(x) = 2(x - 2)^2$ dan $b(x) = x^2 + 2x + 3$

$p(x) = x^2 + 2x + 3$ membagi habis $f(x)$, $p(x)$ tidak membagi habis $a(x)$ tetapi membagi habis $b(x)$.

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)