DADU SICHERMAN

(Suatu Aplikasi dari Faktorisasi Tunggal Pada Z[X])

Elah Nurlaelah

Jurusan Pendidikan Matematika
Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam
Universitas Pendidikan Indonesia

ABSTRACT

An interesting application of unique factorization in Z[X] is Sicherman dice. The dice is a pair of dice whose has different number from ordinary dice which faces are labeled 1 through 6. But probability the sum of faces are same as the sum of ordinary dices. Sicherman dice is obtained by using one to one correspondence between the two polynomials and the face of two dice of ordinary dice.

Kata Kunci **:** *ring R[X], daerah Integral, polynomial irreducible, Faktorisasi tunggal pada Z[X].*

PENDAHULUAN

Pada makalah ini akan disajikan suatu aplikasi yang menarik dari teorema faktorisasi tunggal pada Z[X]. Dan dengan menggunakan sifat korespondensi satu-satu antara dua polinomial dan dua mata dari dua buah dadu yang permukaannya diberi nomor dari 1 sampai 6, dapat dihasilkan sepasang dadu lain yang mempunyai probabilitas sama dengan dua buah dadu dengan nomor terurut .

Sebagai materi prasyarat untuk mempelajari bahan tersebut terlebih dahulu diuraikan beberapa definisi, teorema dan lemma yang menunjang.

MATERI PRASYARAT

Teorema 1: (Teorema Fundamental Aritmatika)

Setiap bilangan bulat lebih besar daripada satu adalah prima atau hasil kali bilangan prima. Hasil kali tersebut tunggal, kecuali urutan di mana bilangan –bilangan tersebut

*) Reviewer: Dian Usdiyana,
Jurusan Pendidikan
Matematika FPMIPA UPI

muncul. Jadi jika $n = p_1p_2\ldots p_r$ dan $n = q_1q_2\ldots q_s$ dimana p_i dan q_j masing-masing prima, maka r = s dan setelah q_j diurutkan kembali diperoleh $p_i = q_j$, untuk setiap i.

Definisi 2: Polinomial Atas Ring R

Misalkan R suatu Ring komutatif , Himpunan R[X] = { $a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \mid a_{ii} \in R$, n bilangan bulat positif } disebut ring polinomial atas R dengan indeterminate X.

Misalkan $f(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$

dan

$g(x) = b_mx^m + b_{m-1}x^{m-1} + \ldots + b_1x + b_0$ dengan f(x) dan g(x) $\in$ R[X], maka :

$f(x) + g(x) = (a_s + b_s)x^s + (a_{s-1} + b_{s-1})x^{s-1} + \ldots + (a_1 + b_1) x + a_0 + b_0$

dimana $a_i = 0$ untuk $i > n$ dan $b_i = 0$ untuk $i > m$. Juga,

$f(x).g(x) = c_{m+n} x^{m+n} + c_{m+n-1}x^{m+n-1} + \ldots + c_1x + c_0$

dimana $c_k = a_kb_0 + a_{k-1}b_1 + \ldots + a_1b_{k-1} + a_0b_k$ untuk k = 0,…, m+n.

Definisi 3 : (Daerah Integral)

Suatu ring komutatif dengan elemen satuan disebut **daerah integral** jika tidak memuat elemen pembagi nol.

Teorema 4 :

Jika D suatu daerah integral, maka D[X] suatu daerah integral.

Bukti:

Jika D suatu daerah integral maka D adalah suatu ring, dan akibatnya D[X] suatu ring. Untuk membuktikan bahwa D[X] suatu daerah integral tinggal menunjukkan bahwa D[X] memenuhi sifat komutatif, memuat elemen satuan dan tidak memuat elemen pembagi nol.

Sifat komutatif pada D[X] langsung dipenuhi jika D bersifat komutatif. Dan jika 1 elemen satuan pada D , maka f(x) = 1 adalah elemen satuan pada D[x] sebab $\forall$ g(x) $\in$ D[X], g(x).1 = 1.g(x) = g(x). Selanjutnya misalkan

$f(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_0$

dan

$g(x) = b_mx^m + b_{m-1}x^{m-1} + \ldots + b_0$

di mana $a_n \neq 0$ dan $b_m \neq 0$. Maka f(x).g(x) mempunyai koefisien utama a_nb_m dan karena D daerah integral maka $a_nb_m \neq 0$.

Definisi 5 :

Misalkan D suatu daerah integral.

Suatu polinomial f(x) $\in$ D[X] yang bukan polinomial nol dan bukan polinomial satuan dalam D[X] disebut **polinomial irreducible atas D,** jika f(x) = g(x)h(x) dengan g(x) dan h(x) $\in$ D[X], maka f(x) atau g(x) adalah elemen satuan dalam D[X]. Polinomial tak nol atau polinomial yang bukan satuan dalam D[x] yang tidak irreducible atas D disebut **reducible** atas D.

Definisi 6: (Konten Dari Polinomial, dan Polinomial Primitif)

Konten dari suatu polinomial $a_nx^n + a_{n-1}x^{n-1} + \ldots + a_0$ dengan $a_i \in Z$, i = 0,1,2,…n adalah pembagi persekutuan terbesar dari a_n , a_{n-1} , …, a_0. Suatu **polinomial primitif** adalah polinomial pada Z[X] dengan konten 1.

Lemma 7 : (Lemma Gauss).

Hasil kali dua buah polinomial primitif adalah primitif.

Bukti :

Misalkan f(x) dan g(x) masing-masing adalah polinomial primitif, dan misalkan f(x)g(x) bukan polinomial primitif.

Misalkan p adalah konten prima dari f(x)g(x), dan misalkan $\bar{f}$ (x) , $\bar{g}$ (x) dan $\overline{f(x)g(x)}$ adalah polinomial yang diperoleh dari f(x),g(x) dan f(x)g(x) dengan mereduksi koefisien-koefisiennya ke modulo p. Maka $\bar{f}$ (x) dan $\bar{g}$ (x) adalah elemen-elemen dari $Z_p[X]$ dan $\bar{f}$ (x) $\bar{g}$ (x) = $\overline{f(x)g(x)}$ = 0 elemen nol pada $Z_p[X]$. Akibatnya $\bar{f}$ (x) = 0 atau $\bar{g}$ (x) = 0. Ini berarti bahwa p membagi setiap koefisien dari f(x) atau p membagi setiap koefisien dari g(x). Dengan demikian maka baik f(x) maupun g(x) tidak primitif.

Teorema 8 :

Misalkan F suatu field dan p(x) polinomial irreducible atas F, maka F[X]/(p(x)) adalah field.

Teorema 9:

Misalkan F suatu field dan misalkan p(x), a(x), b(x) $\in$ F[X] . Jika p(x) polinomial irreducible atas F dan p(x) $|$ a(x)b(x) maka p(x) $|$ a(x) atau p(x) $|$ b(x).

Bukti:

Karena p(x) polinomial irreducible dan F[X]/(p(x)) suatu field maka F[X]/(p(x)) suatu integral domain. Misalkan $\bar{a}$ (x) dan $\bar{b}$(x) adalah image dari homomorfisma dari F[X] ke

F[X]/(p(x)). Karena p(x) | a(x)b(x), diperoleh $\bar{a}(x)\,\bar{\phi}(x) = \bar{0}$ elemen nol pada F[X]/(p(x)). Jadi $\bar{a}(x) = \bar{0}$ atau $\phi(x) = 0$, dan ini berarti bahwa p(x) | a(x) atau p(x) | b(x).

Faktorisasi Tunggal Pada Z[X]

Teorema :

Setiap polinomial dalam Z[X] yang bukan polinomial nol dan bukan polinomial satuan dalam Z[X] dapat ditulis dalam bentuk $b_1b_2 \ldots b_sp_1(x)p_2(x)\ldots p_m(x)$ dimana setiap b_i adalah prima (yaitu polinomial dengan derajat nol), dan $p_i(x)$ adalah polinomial irreducible dengan derajat positif. Selanjutnya jika;

$$b_1b_2 \ldots b_sp_1(x)p_2(x)\ldots p_m(x) = c_1c_2\ldots c_tq_1(x)q_2(x)\ldots q_n(x)$$

dimana b_i dan c_j untuk setiap i dan j polinomial irreducible dengan derajat nol, dan $p_i(x)$ dan $q_j(x)$ maing-masing polinomial irreducible dengan derajat positif, maka s = t , m= n , dan setelah c_j dan $q_j(x)$ diurutkan kembali diperoleh $b_i = \pm c_i$ untuk i = 1,2, …,s dan $p_i(x) = \pm q_i(x)$ untuk i = 1,2, …, m.

Bukti :

Misalkan f(x) suatu polinomial tak nol dan bukan elemen satuan dalam Z[X]. Jika derajat f(x) = 0, maka f(x) suatu konstanta dengan menggunakan teorema 1, teorema terbukti.

Jika derajat f(x) > 0, misalkan konten dari f(x) adalah b dan $b = b_1b_2 \ldots b_s$ adalah faktorisasi prima dari b, maka $f(x) = b_1b_2 \ldots b_s\, f_1(x)$, dengan $f_1(x) \in Z[X]$ adalah polinomial primitif dengan derajat positif .

Jadi untuk membuktikan teorema tersebut cukup ditunjukkan bahwa polinomial primitif $f_1(x)$ dapat ditulis sebagai hasil kali polinomial- polinomial irreducible dengan derajat positif. Dengan menggunakan induksi dibuktikan sebagai berikut;

Jika derajat $f_1(x) = 1$, maka $f_1(x)$ adalah polinomial irreducible. Selanjutnya misalkan setiap polinomial primitif dengan derajat lebih kecil dari f(x) dapat ditulis sebagai hasil kali polinomial irreducible dengan derajat positif. Jika $f_1(x)$ irreducible , ini berarti tidak perlu dibuktikan lebih lanjut. Sebaliknya jika $f_1(x) = g(x)h(x)$ dimana g(x) dan h(x) adalah polinomial primitif dan mempunyai derajat lebih kecil dari $f_1(x)$.Sehingga dengan induksi baik g(x) maupun h(x) dapat ditulis sebagai hasil kali dari polinomial irreducible dengan derajat positif. Maka demikian juga dengan f(x).

Untuk membuktikan ketunggalan dari teorema, misalkan ;

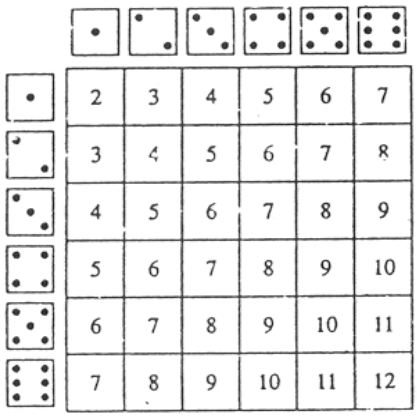
$f(x) = b_1b_2 \ldots b_sp_1(x)p_2(x)\ldots p_m(x) = c_1c_2\ldots c_tq_1(x)q_2(x)\ldots q_n(x)$ di mana b_i dan c_j untuk

i = 1,2,…,s dan j = 1,2,…,t adalah polinomial irreducible dengan derajat nol, $p_i(x)$, dan $q_j(x)$ untuk i = 1,2,…,m dan j = 1,2,…,n adalah polinomial irreduble dengan derajat positif. Misalkan $b = b_1b_2 \ldots b_s$ dan $c = c_1c_2\ldots c_t$. Karena $p_i(x)$ dan $q_j(x)$ masing-masing polinomial primitif, dengan menggunakan lemma 7 maka $p_1(x)p_2(x)\ldots p_m(x)$ dan $q_1(x)q_2(x)\ldots q_n(x)$ adalah polinomial primitif. Selanjutnya b dan c harus sama dengan plus dan minus dari

konten f(x), dan ini berarti sama dengan nilai mutlaknya. Dengan menggunakan teorema 1 maka s = t dan setelah diurutkan kembali $b_i = \pm c_i$, untuk i = 1, 2,…, s. jadi dengan mengkensel bagian konstanta dalam dua bagian faktorisasi dari f(x) diperoleh $p_1(x)p_2(x)\ldots p_m(x) = \pm q_1(x)q_2(x)\ldots q_n(x)$. Selanjutnya dengan memandang $p_i(x)$ dan $q_j(x)$ sebagai elemen-elemen dari Q[X] dan $p_1(x)$ membagi $q_1(x)q_2(x)\ldots q_n(x)$, maka dengan teorema 8 bahwa $p_1(x) \mid q_i(x)$ untuk suatu i. Dengan mengurutkan kembali misalkan diasumsikan i = 1, maka karena $q_i(x)$ polinomial irreducible , diperoleh $q_1(x) = r/s\ p_1(x)$, dengan r, s $\in$ Z. Karena baik $p_1(x)$ dan $q_1(x)$ keduanya polinomial primitif , maka haruslah r/s = ± 1. Sehingga $q_1(x) = \pm p_1(x)$, setelah dikensel diperoleh $p_2(x)\ldots p_m(x) = \pm q_2(x)\ldots q_n(x)$. Prosedur yang sama diulangi untuk $p_2(x)$ untuk menggantikan $p_1(x)$. Jika m < n, setelah m langkah, pada ruas kiri sama dengan 1 sedangkan pada ruas kanan terdiri dari suatu polinomial nonkonstan. Jelas ini tidak mungkin. Sebaliknya jika m > n, setelah n langkah akan diperoleh ± 1 pada ruas kanan dan suatu polinomial tak konstan pada ruas kiri, juga ini tidak mungkin. Dengan demikian haruslah m = n dan $p_i(x) = \pm q_i(x)$ setelah $q_i(x)$ diurutkan kembali.

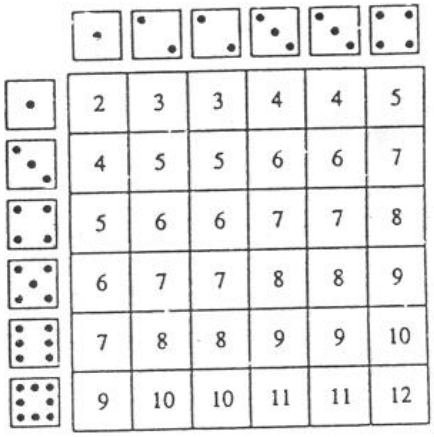
Dadu Sicherman (Suatu Aplikasi Dari Faktorisasi Tunggal)

Perhatikan dua buah dadu bersisi 6 dimana setiap permukaannya diberi nomor dari 1 sampai 6. Probabilitas muncul jumlah 7 pada pelemparan dua dadu tersebut adalah 6/36 , probabilitas jumlah 6 adalah 5/36 dan seterusnya. Selanjutnya dua buah dadu bersisi enam yang lain diberi nomor 1,2,2,3,3,4 dan 1,3,4,5,6,8,(selanjutnya kedua dadu ini disebut dadu Sicherman) maka probabilitas muncul jumlah 7 dan 6 masing-masing adalah 6/36 dan 5/36 sama dengan probabilitas dari jumlah dadu dengan nomor berurutan 1 sampai 6. Perhatikan gambar berikut;



2	3	4	5	6	7
3	4	5	6	7	8
4	5	6	7	8	9
5	6	7	8	9	10
6	7	8	9	10	11
7	8	9	10	11	12

Dadu Biasa



2	3	3	4	4	5
4	5	5	6	6	7
5	6	6	7	7	8
6	7	7	8	8	9
7	8	8	9	9	10
9	10	10	11	11	12

Dadu Sicherman

Dalam contoh ini akan ditunjukkan bahwa label pada dadu sicherman dapat diturunkan dan hanya urutan nomor tersebut yang mungkin, yaitu dengan menggunakan sifat faktorisasi tunggal pada Z[X].

Berdasarkan gambar diatas ternyata pasangan dadu yang menghasilkan jumlah enam adalah (5,1), (4,2), (3,3), (2,4), (1,5). Selanjutnya perhatikan suatu polinomial yang berderajat sama dengan urutan dadu , yaitu 1 sampai 6. Polinomial tersebut adalah ;

$X^6 + X^5 + X^4 + X^3 + X^2 + X$. Hasil kali dua polinomial tersebut adalah;

$$(X^6 + X^5 + X^4 + X^3 + X^2 + X) \qquad (X^6 + X^5 + X^4 + X^3 + X^2 + X).$$

Dalam perkalian ini X^6 diperoleh dari $X^5.X^1$, $X^4.X^2$, $X^3.X^3$, $X^2.X^4$, $X^1.X^5$. Ternyata terdapat korespondensi satu-satu antara jumlah dua buah dadu bernilai 6 dengan X^6. Disamping jumlah tersebut korespondensi satu-satu inipun dapat digunakan untuk jumlah dua buah dadu yang lain dengan pangkat yang lain. Demikian juga untuk dadu sichermen atau dadu lain yang menghasilkan probabilitas yang sama.

Selanjutnya misalkan $\{ a_1, a_2, a_3, a_4, a_5, a_6 \}$ dan $\{b_1, b_2, b_3, b_4, b_5, b_6 \}$ dua himpunan label bernilai positif untuk suatu kubus yang mempunyai sifat seperti dua buah dadu dengan nomor terurut.

Dan misalkan ;

$$(X^6 + X^5 + X^4 + X^3 + X^2 + X)(X^6 + X^5 + X^4 + X^3 + X^2 + X)$$

$$= (x^{a_1} + x^{a_2} + x^{a_3} + x^{a_4} + x^{a_5} + x^{a_6})(x^{b_1} + x^{b_2} + x^{b_3} + x^{b_4} + x^{b_5} + x^{b_6}). \quad (1)$$

Selanjutnya persamaan ini akan diselesaikan untuk semua a_i dan b_i. Disini faktorisasi tunggal pada Z[X] akan digunakan ;

Faktor yang irreducible dari polinomial $X^6 + X^5 + X^4 + X^3 + X^2 + X$ adalah

$$X(X + 1)(X^2 + X + 1)(X^2 - X + 1)$$

Sehingga ruas kiri dari persamaan (1) mempunyai faktor irreducible sebagai berikut;

$$X^2 (X + 1)^2 (X^2 + X + 1)^2 (X^2 - X + 1)^2.$$

Dengan menggunakan teorema faktorisasi tunggal ini berarti bahwa

$P(X) = x^{a_1} + x^{a_2} + x^{a_3} + x^{a_4} + x^{a_5} + x^{a_6}$ mempunyai faktor irreducible yang sama dengan polinomial $X^6 + X^5 + X^4 + X^3 + X^2 + X$. Jadi P(X) mempunyai bentuk ;

$$X^q (X + 1)^r (X^2 + X + 1)^s (X^2 - X + 1)^t \text{ dengan } 0 \le q, r, s, t \le 2.$$

Pembatasan untuk kemungkinan keempat parameter tersebut adalah dengan mengevaluasi P(X) pada nilai X = 1 dan X = 0 pada dua cara, sebagai berikut;

$P(1) = 1^{a_1} + 1^{a_2} + 1^{a_3} + 1^{a_4} + 1^{a_5} + 1^{a_6} = 6$ dan $P(1) = 1^q 2^r 3^s 1^t$, dari sini jelas bahwa r = 1 dan t = 1, tetapi bagaimana dengan nilai q ?. Untuk itu persamaan P(X) dievaluasi pada X = 0, dari sini jelas $q \neq 0$, karena jika q = 0 maka P(0) tidak terdefinisi. Selanjutnya jika q = 2 , maka $P(1) = 1^2 2^1 3^1 1^t = 6$ untuk nilai $0 \le t \le 2$, tetapi jumlah pangkat terkecil perkalian dua

polinomialnya adalah 3, dan ini bertentangan dengan jumlah dadu yang terkecil yaitu 2, dengan demikian haruslah q = 1.

Di bawah ini akan disajikan polinomial-polinomial dengan nilai q= 1,r = 1,s= 1,dan t = 0,1,2. Sebagai berikut;

Jika t = 0, maka $P(X) = X^1 (X + 1)^1 (X^2 + X + 1)^1(X^2 - X + 1)^0$

$= X^1 (X + 1)^1(X^2 + X + 1)^1$

$= X^4 + X^3 + X^3 + X^2 + X^2 + X.$

Ini berarti dadu mempunyai label (4, 3, 3, 2, 2, 1) yang merupakan **dadu sicherman**.

Jika t = 1, maka $P(X) = X^1 (X + 1)^1 (X^2 + X + 1)^1 (X^2 - X + 1)^1$

$= X^6 + X^5 + X^4 + X^3 + X^2 + X.$

Ini berarti dadu mempunayi label (6, 5, 4, 3, 2, 1) yang merupakan dadu biasa.

Jika t = 2, maka $P(X) = X^1 (X + 1)^1 (X^2 + X + 1)^1 (X^2 - X + 1)^2$

$= X^8 + X^6 + X^5 + X^4 + X^3 + X.$

Ini berarti dadu mempunyai label (8, 6, 5, 4, 3, 2, 1) yang merupakan **dadu sicherman** yang lain.

Ini membuktikan bahwa dadu sicherman memberikan probabilitas yang sama dengan dadu dengan nomor terurut, dan hanya urutan dua dadu tersebut yang mempunyai sifat seperti itu.

DAFTAR PUSTAKA

Chaudhuri,N.P. *Abstract Algebra.*McGraw-Hill Offices. New York. 1969.

Durbin. John.R. . *Modern Algebra An Introduction.* John Wiley & Sons. New York. *3rd Edition.1992.*

Gallian,A.J. *Contemporary Abstract Algebra.*D.C. Heath and Company. Toronto. *Second Edition.1990.*