Jurnal Penelitian Sains ; hal 11 - 17
No.5. April 1999 ISSN: 1410-7058

MENENTUKAN FAKTOR PERSEKUTUAN TERBESAR [FPB] SUATU RING POLINOM $B_n[x]$ DENGAN MENGGUNAKAN ALGORITMA EUCLID

Sugandi Yahdin dan Wenny Rosita WR
Jurusan Matematika FMIPA Universitas Sriwijaya

ABSTRAK

Algoritma Pembagian merupakan generalisasi konsep pembagi-pembagi dan konsep Faktor Persekutuan Terbesar [FPB] untuk suatu himpunan dalam Ring Euclid. Salah satu himpunan yang merupakan Ring Euclid adalah Ring Polinom dengan koefisien-koefisien dalam bilangan bulat modulo n dimana n merupakan bilangan prima. Faktor Persekutuan Terbesar suatu Ring Polinom dalam Ring Euclid dapat dihitung dengan menggunakan Algoritma Euclid yang merupakan proses iterasi atau pengulangan dari Algoritma Pembagian Polinom.

PENDAHULUAN

Aljabar Abstrak terdiri dari struktur-struktur aljabar, salah satu di antaranya adalah *Grup* (Wahyudin, 1989). Grup terdiri dari himpunan dan operasi biner yang didefinisikan pada himpunan. Grup merupakan dasar untuk mempelajari struktur aljabar *Ring, Field* dan *Integral Domain*.

Teori Grup belum cukup untuk merangkum semua struktur aljabar karena suatu grup hanya berkaitan dengan satu operasi biner saja. Suatu struktur aljabar yang mempunyai dua operasi biner yaitu " penjumlahan " dan " perkalian " disebut *Ring* atau *Gelanggang*.

Jurnal Penelitian Sains ; hal 11 - 17
No.5. April 1999 ISSN: 1410-7058

Ring adalah himpunan R yang tak kosong dengan operasi biner + dan × yang setiap elemen-elemennya bersifat **Grup Abelian** terhadap penjumlahan, mempunyai sifat distributif dan mempunyai sifat asosiatif terhadap perkalian. Salah satu himpunan yang dapat memenuhi aksioma-aksioma ring adalah bilangan bulat dan polinom.

Definisi 1. Misalkan R adalah ring dan x adalah variabel. Polinom dalam x dengan koefisien di R ditunjukkan pada bentuk

$$a_0x^0 + a_1x^1 + a_2x^2 + \ldots + a_nx^n,$$

dimana $n \geq 0$ dan $a_i \in R$; $i = 0, 1, 2, \ldots, n$. Himpunan dari semua polinom dalam x dengan koefisien di R dinotasikan dengan **R[x].**

Ring Polinom memiliki beberapa sifat yang sama dengan ring dari bilangan-bilangan bulat; yaitu keduanya merupakan integral domain tetapi keduanya bukan field (lapangan). Selain itu pula, kedua ring tersebut memiliki algoritma-algoritma yang berlaku didalamnya yaitu Algoritma Pembagian dan Algoritma Euclid dan ring dengan algoritma tersebut disebut dengan Ring Euclid.

Salah satu kegunaan dari Algoritma Euclid adalah dapat menetukan FPB dari suatu **Ring Polinom $B_n[x]$**, yaitu ring polinom yang memiliki koefisien dalam bilangan bulat modulo n dimana n merupakan bilangan prima.

Ada dua metode yang telah dikenal sebelumnya bahwa untuk memperoleh FPB dari pasangan bilangan bulat a dan b yang keduanya tidak nol, yaitu dengan **faktorisasi prima (pohon faktor)** atau dengan menentukan **faktor-faktor** dari bilangan itu sendiri. Tidak begitu sulit untuk mencari faktor-faktor dari pasangan bilangan bulat a dan b sehingga diperoleh faktor persekutuan terbesar dari a dan b, tidak demikian halnya dengan dua polinom a(x) dan b(x) yang keduanya tidak nol.

Untuk memperoleh faktor persekutuan terbesar dari dua polinom tersebut seringkali menemui kesulitan untuk mendapatkan faktor-faktor persekutuan dari dua polinom di atas. Karena itu

Jurnal Penelitian Sains ; hal 11 - 17
No.5. April 1999 ISSN: 1410-7058

melalui proses *iterasi* atau *pengulangan Algoritma Pembagian Polinom* dapat diperoleh faktor-faktor persekutuan dari dua polinom a(x) dan b(x).

Definisi 2. Misalkan a(x) dan b(x) adalah polinom-polinom tidak nol di dalam **R[x]** dan disebut **Faktor Persekutuan Terbesar** d(x) dari a(x) dan b(x) bila memenuhi kondisi berikut:

(i). d(x) adalah polinom monic.

(ii). d(x) | a(x) dan d(x) | b(x).

(iii). Jika c(x) ∈ **R[x]** sedemikian hingga c(x) | a(x) dan c(x) | b(x), maka c(x) | d(x).

HASIL DAN PEMBAHASAN

ALGORITMA PEMBAGIAN POLINOM

Bila suatu polinom dibagi oleh polinom yang lainnya maka diperoleh suatu hasil bagi (faktor) dan sisa hasil bagi, ternyata hal ini selalu mungkin. Proses pembagian polinom ditunjukkan dari pembuktian teorema sebagai berikut.

Teorema 1. {Algoritma Pembagian Polinom}

Misalkan a(x), b(x) ∈ **R[x]** yang keduanya tidak nol maka ada polinom q(x) dan r(x) yang unik dalam **R[x]** sedemikian hingga **b(x) = a(x).q(x) + r(x)** dimana r(x) = 0 atau deg r(x) < deg a(x).

Bukti.

Akan ditunjukkan keberadaan dari q(x) dan r(x). Jika b(x) = 0 atau deg b(x) < deg a(x) maka diperoleh q(x) = 0 dan r(x) = b(x). Jadi sekarang dapat diasumsikan bahwa m = deg b(x) ≥ deg a(x) = n dan dimisalkan $a(x) = a_n x^n + ... + a_0$ dan $b(x) = b_m x^m + ... + b_0$. Inti dari pembuktian ini untuk

menunjukkan jika kita akan membagi a(x) ke dalam b(x). Dari pembagian b(x) oleh a(x) maka diperoleh $b_1(x) = b(x) - a_n^{-1}b_m x^{m-n}a(x)$ dan dapat dilihat pada bagan berikut.

$$\begin{array}{r} a_n^{-1}b_m x^{m-n} \\ a_n x^n + \ldots \overline{)\, b_m x^m + \ldots} \\ \underline{b_m x^m + \ldots} \\ b_1(x) \end{array}$$

$$b_1(x) = (b_m x^m + \ldots + b_0) - a_n^{-1}b_m x^{m-n}(a_n x^n + \ldots + a_0).$$

Kemudian jika $b_1(x) = 0$ atau deg $b_1(x)$ < deg a(x) maka ada $q_1(x)$ dan $r_1(x)$ dalam **R[x]** sedemikian hingga $b_1(x) = a(x)\, q_1(x) + r_1(x)$ dimana $r_1(x) = 0$ atau deg $r_1(x)$ < deg a(x) sehingga diperoleh

$$\begin{aligned} b(x) &= a_n^{-1}b_m x^{m-n}a(x) + b_1(x) \\ &= a_n^{-1}b_m x^{m-n}a(x) + q_1(x)a(x) + r_1(x) \\ &= [a_n^{-1}b_m x^{m-n} + q_1(x)]\, a(x) + r_1(x) \end{aligned}$$

sehingga diperoleh polinom $q(x) = a_n^{-1}b_m x^{m-n} + q_1(x)$ dan $r(x) = r_1(x)$.

Untuk pembuktian keunikan, diberikan $b(x) = a(x).q(x) + r(x)$ dan $b(x) = a(x).q^*(x) + r^*(x)$ dimana $r(x) = 0$ atau deg r(x) < deg a(x) dan $r^*(x) = 0$ atau deg $r^*(x)$ < deg a(x), maka pengurangan dua persamaan ini diperoleh

$$0 = a(x)[\, q(x) - q^*(x)\,] + [\, r(x) - r^*(x)\,] \text{ atau}$$

$$r^*(x) - r(x) = a(x)[q(x) - q^*(x)]$$

dengan demikian $r^*(x) - r(x)$ adalah nol atau derajat dari $[r^*(x) - r(x)]$ adalah lebih kecil dari a(x). Jelas ini tidak mungkin karena $r^*(x) = r(x)$ dan $q(x) = q^*(x)$. Maka q(x) dan r(x) adalah unik dan pembuktian terpenuhi.

Contoh.

Bagilah $x^3 + 2x^2 + x + 2$ oleh $x^2 + 2$ dalam $\mathbf{B_3[x]}$.

Penyelesaian.

Dengan menggunakan pembagian panjang polinom diperoleh polinom q(x) dan r(x).

$$
\begin{array}{r}
x+2 \\
x^2+2\overline{)\,x^3+2x^2+x+2} \\
\underline{x^3 \qquad +2x} \\
2x^2+2x+2 \\
\underline{2x^2 \qquad +1} \\
2x+1
\end{array}
$$

Jadi $q(x) = (x + 2)$ dan $r(x) = (2x + 1)$.

Dalam Algoritma Pembagian, polinom q(x) disebut hasil bagi atau faktor dan r(x) disebut sisa dari pembagian dari b(x) oleh a(x).

ALGORITMA EUCLID

Misalkan a(x) dan b(x) merupakan polinom-polinom dari suatu Ring Euclid yang keduanya tidak nol, pengulangan Algoritma Pembagian Polinom ditulis

$b(x) = a(x).q_1(x) + r_1(x)$ dengan deg $r_1(x) <$ deg $a(x)$.

$a(x) = r_1(x).q_2(x) + r_2(x)$ dengan deg $r_2(x) <$ deg $r_1(x)$.

$r_1(x) = r_2(x).q_3(x) + r_3(x)$ dengan deg $r_3(x) <$ deg $r_2(x)$.

.

.

.

$r_{n-2}(x) = r_{n-1}(x).q_n(x) + r_n(x)$ dengan deg $r_n(x) <$ deg $r_{n-1}(x)$

$r_{n-1}(x) = r_n(x).q_{n+1}(x) + 0$.

Jurnal Penelitian Sains ; hal 11 - 17
No.5. April 1999 ISSN: 1410-7058

Sisa hasil bagi selalu berkurang derajatnya, sehingga akhirnya sisa hasil bagi akan bernilai nol. Dapat dilihat bahwa

$$\mathbf{FPB[a(x), b(x)] = FPB\ [a(x), r_1(x)] = ... = FPB\ [r_{n-1}(x), r_n(x)] = FPB\ [r_n(x), 0].}$$

Karena $r_n(x)$ adalah pembagi dari $r_{n-1}(x)$ yang menjadi FPB dari $r_n(x)$ dan $r_{n-1}(x)$ sehingga

$$\mathbf{r_n(x) = FPB\ [a(x), b(x)].}$$

KESIMPULAN DAN SARAN

Dari hasil dan pembahasan dapat disimpulkan sebagai berikut

1. **Algoritma Euclid** dapat memberikan kemudahan untuk memperoleh FPB dari Ring Polinom.
2. $\mathbf{B_n[x]}$ merupakan polinom yang memiliki koefisien-koefisien dalam bilangan bulat modulo n yang diperoleh dengan menggantikan setiap koefisien-koefisien polinom dalam bilangan bulat modulo n nya.
3. $\mathbf{B_n[x]}$ digunakan untuk mempermudah dan mempercepat melakukan perhitungan pada pembagian panjang polinom agar koefisien polinom tetap berada dalam bilangan bilangan bulat.

DAFTAR PUSTAKA

Alexanderson, L., G. , and Hilman, P., A., 1994, ***Abstract Algebra A First Undergraduate,*** Fifth Edition, Boston : PWS Publishing Company.

Dummit, D., and Richard, M. F., 1991, *Abstract Algebra,* Prentice-Hall, Inc.

Ehrlich, G, 1991, *Fundamental Concepts of Abstract Algebra, PWS*-Kent Publishing Company Boston.

Flat, E., D., 1989, *Introduction to Number Theory,* New York: John Wiley & Sons, Inc.

Fraleigh, B. and John, 1994, *A First Course in Abstract Algebra,* Fifth Edition, USA:Addison-Wesley Publishing Company, Inc.

Hartley, B. and Hawkes, T.O., 1994, *Rings, Modules and Linear Algebra..*

Suradi, 1985, *Diktat Kuliah Struktur Aljabar I,* Jurusan Matematika FMIPA ITS.

Wahyudin, 1989, *Aljabar Modern,* Edisi Pertama, Bandung:Tarsito.

Whitelaw, A., T., 1985, *Introduction to Abstract Algebra,* Third Edition, Glasgow: Chapman & Hall.