Rantai Kompleks, U-Kompleks, dan (U,U')-Pemetaan dari $\mathbb{Z}_n$

Utih Amartiwi*, Gustina Elfiyanti

Abstrak

Suatu rantai R-modul dan R-homorfisma

$$\ldots \to C_{n+1} \xrightarrow[d_{n+1}]{} C_n \xrightarrow[d_n]{} C_{n-1} \xrightarrow[d_{n-1}]{} C_{n-2} \to \ldots$$

disebut barisan eksak jika $\mathrm{Im} d_{n+1} = \ker d_n$. *Rantai ini disebut juga rantai kompleks jika* $d_n d_{n+1}(C_{n+1}) = \{0\}$. *Davvaz dan Parnian memperkenalkan generalisasi konsep barisan gmaieksak dengan menggantikan {0} dengan* U_{n-1} *suatu submodul dari* C_{n-1} *yang disebut dengan U-eksak. Kemudian, Davvaz dan Shabani mengembangkan konsep ini dengan mendefinisikan konsep rantai U-kompleks, U-homologi, rantai (U,U')-pemetaan, rantai (U,U')- homotopi, dan U-fungtor.* $\mathbb{Z}_n$ *adalah himpunan bilangan bulat modulo n, dimana* $n \in \mathbb{Z}$. *merupakan modul atas* $\mathbb{Z}$ *dengan operasi penjumlahan dan perkalian skalar. Sehingga,* $\mathbb{Z}_n$ *dapat dikatakan* $\mathbb{Z}$ *-modul. Dalam makalah ini, penulis membuat rantai kompleks, U-kompleks, dan (U, U')-pemetaan dari* $\mathbb{Z}_n$ *dengan memanfaatkan sifat-sifat di aritmatika modulo.*

Kata-kata kunci: rantai kompleks, rantai U-kompleks, rantai (U,U')- pemetaan, aritmatika modulo.

Pendahuluan

Suatu rantai R-modul dan R-homorfisma

$$\ldots \to C_{n+1} \xrightarrow[d_{n+1}]{} C_n \xrightarrow[d_n]{} C_{n-1} \xrightarrow[d_{n-1}]{} C_{n-2} \to \ldots$$

disebut barisan eksak jika $\mathrm{Im} d_{n+1} = \ker d_n$. Rantai ini disebut juga rantai kompleks jika. $d_n d_{n+1}(C_{n+1}) = \{0\}$. Dalam [2] Davvaz dan Parnian memperkenalkan generalisasi konsep barisan eksak dengan menggantikan {0} dengan U_{n-1} suatu submodul dari C_{n-1} yang disebut dengan U-eksak. Kemudian, Davvaz dan Shabani [1] mengembangkan konsep ini dengan mendefinisikan konsep rantai U-kompleks, U-homologi, rantai (U,U′)- pemetaan, rantai (U,U′)-homotopi, dan U-fungtor.

$\mathbb{Z}_n$ adalah himpunan bilangan bulat modulo n, dimana $n \in \mathbb{Z}$. $\mathbb{Z}_n$ merupakan modul atas $\mathbb{Z}$ dengan operasi penjumlahan dan perkalian skalar. Pada awalnya, penulis membuat beberapa contoh rantai kompleks, U-kompleks, dan (U,U')-pemetaan dari $\mathbb{Z}_n$. Setelah membuat beberapa contoh, penulis menemukan bahwa contoh-contoh tersebut membentuk suatu pola yang dapat diperumum dan dibuktikan dengan menggunakan konsep dari teori bilangan. Pada makalah ini, penulis membahas perumuman dari contoh tersebut dan membuat pembuktiannya. Penulis berharap teori ini dapat terus mendukung perkembangan ilmu pengetahuan khususnya di bidang aljabar, teori bilangan, dan kriptografi.

Teori

1. Definisi Modul

   Misalkan R suatu gelanggang komutatif dengan identitas, yang elemen-elemennya disebut skalar. Sebuah R-modul adalah himpunan tak kosong M, dengan dua operasi yang memenuhi :

   1.(M,+) grup abel.

   2.Untuk setiap $m_1, m_2 \in M$ dan $r,s \in R$ berlaku :

   a.$m_1 r \in M$

   b.$m_1(rs)=(m_1 r)s$

   c.$m_1(r+s)=m_1 r+m_1 s$

   d.$(m_1+m_2)r=m_1 r+m_2 r$

   e.$m_1 \cdot 1=m_1$

2. Homomorfisma Modul

   Misalkan M dan N merupakan R-modul. Suatu pemetaan $f : M \to N$ dikatakan homomorfisma R-modul jika $f(rx+sy) = rf(x)+sf(y), \forall x, y \in M,$ dan $r, s \in R$

3. Aritmatika Modulo

   Definisi: Misalkan $a, b, m \in \mathbb{Z}$, a dikatakan kongruen dengan b modulo m jika (a-b) habis dibagi m atau m|(a-b), ditulis: $a \equiv b (\mathrm{mod}\, m)$.

   Teorema: $\forall$a, b, c, n$\in \mathbb{Z}$ berlaku

   • (a+b) mod n=(a mod n)+(b mod n)

- (axb) mod n = (a mod n)x(b mod n)
- a ≡ b mod n → ac ≡ bc mod n

Definisikan $\mathbb{Z}_n$ adalah himpunan bilangan bulat modulo n. $\mathbb{Z}_n$ merupakan modul atas $\mathbb{Z}$ dengan operasi penjumlahan dan perkalian skalar.

4. Rantai Kompleks

Suatu rantai R-modul dan R-homorfisma

$$\ldots \to C_{n+1} \xrightarrow[d_{n+1}]{} C_n \xrightarrow[d_n]{} C_{n-1} \xrightarrow[d_{n-1}]{} C_{n-2} \to \ldots$$

disebut Rantai kompleks jika $d_n d_{n+1}(C_{n+1}) = \{0\}$, ∀n

5. Rantai U-Kompleks

Diberikan dua koleksi R-modul $\{C_n\},\{U_n\},n\in\mathbb{Z}$, dimana setiap C_n mengandung U_n dan homomorfisma R-modul $\{d_n:C_n\to C_{n-1}\}$. Rantai (C_n, U_n, d_n) dikatakan rantai U-kompleks jika $d_n d_{n+1}(C_{n+1}) \subseteq U_{n-1}$ dan $\mathrm{Im} d_n \supseteq U_{n-1}$

6. Rantai (U,U')-Pemetaan

Misalkan (C,U,∂) rantai U-kompleks, dan (C',U',∂') rantai U'-kompleks. Barisan $F=\{F_n : C_n \to C_n'\}$ dikatakan rantai (U,U')-pemetaan jika diagram berikut komutatif, yaitu $F_n(U_n) \subseteq U_n'$, dan $\partial_n' F_n = F_{n-1}\partial_n$

$$\begin{array}{ccccccc} (C,U,\partial) \ldots \to & C_{n+1} & \xrightarrow{\partial_{n+1}} & C_n & \xrightarrow{\partial_n} & C_{n-1} & \to \ldots \\ & \downarrow F_{n+1} & & \downarrow F_n & & \downarrow F_{n-1} & \\ (C,U,\partial) \ldots \to & C'_{n+1} & \xrightarrow{\partial'_{n+1}} & C'_n & \xrightarrow{\partial'_n} & C'_{n-1} & \to \ldots \end{array}$$

Hasil dan diskusi

Teorema 1

Misalkan a∈$\mathbb{Z}_n$, jika faktor persekutuan terbesar dari a dan n ditulis GCD(a,n)=b, dimana n=bc, untuk suatu b,c∈$\mathbb{Z}$ maka $\langle \bar{a} \rangle$ ={ $p\bar{a}$ |$\bar{p}\in$ $\mathbb{Z}_n$ } = {0, 1.b,...,(c-1)b}

Bukti

Misalkan GCD(a,n)=b, maka ∃c,d∈$\mathbb{Z}$ sedemikian sehingga n=cb dan a=db. Ambil sebarang $\bar{p}$ ∈$\mathbb{Z}_n$. Perhatikan:

$p\bar{a}$ =pa mod n

=pdb mod n (1)

Pandang menjadi 3 kasus:

1. Jika $pd \le c$, maka persamaan (1) menjadi:

   pdb mod n∈{0 mod cb, 1.b mod cb,...,(c-1) mod cb}= $\{\bar{0},\overline{1.b},\ldots,\overline{(c-1)b}\}$

2. Jika pd>c, maka pd=kc+m, untuk suatu k,m∈$\mathbb{Z}$ dan m<c. Persamaan (1) menjadi:

   pdb mod cb =(kc+m)b mod cb

   =(kcb+mb) mod cb

   =mb mod cb

   ∈{0 mod cb, 1.b mod cb,...,(c-1) mod cb}= $\{\bar{0},\overline{1.b},\ldots,\overline{(c-1)b}\}$

∎ Terbukti

Teorema 2

Jika $\bar{a}$ ∈$\mathbb{Z}_n$ dan k∈$\mathbb{Z}$, maka $\langle \overline{ka} \rangle \subseteq \langle \bar{a} \rangle$

Bukti

Ambil sebarang $\bar{b}$ ∈ $\langle \overline{ka} \rangle$, maka:

$\bar{b} = m.ka \bmod n = la \bmod n \in \langle \bar{a} \rangle$ untuk suatu m,l∈$\mathbb{Z}$

∎ Terbukti

Teorema 3

Misalkan untuk setiap m berlaku d_m: $\mathbb{Z}_n \to \mathbb{Z}_n$ dengan:

$d_m : \bar{x} \mapsto \bar{x}l\sqrt{n}$	Untuk n bilangan kuadrat, l∈$\mathbb{Z}$
$d_m : \bar{x} \mapsto \bar{x}l\sqrt{kn}$	Untuk n bukan bilangan kuadrat, dapat dicari k∈$\mathbb{Z}$ sehingga kn bilangan kuadrat, dan l∈$\mathbb{Z}$

Maka rantai berikut rantai kompleks

$$\ldots \to \mathbb{Z}_n \xrightarrow[d_{m+1}]{} \mathbb{Z}_n \xrightarrow[d_m]{} \mathbb{Z}_n \xrightarrow[d_{m-1}]{} \ldots \qquad (2)$$

Bukti

Ambil sebarang $\bar{x}$ ∈$\mathbb{Z}_n$

1. Untuk n bilangan kuadrat, maka:

   $d_m d_{m+1}(\bar{x}) = xl^2 n \bmod n = \bar{0}$

2. Untuk n bukan bilangan kuadrat, dapat dicari k□ℤ sehingga kn bilangan kuadrat, maka:

$$d_m d_{m+1}(\bar{x}) = xl^2 kn \bmod n = \bar{0}$$

□ Terbukti rantai (2) rantai kompleks

Teorema 4

Misalkan untuk setiap m berlaku

d_m: $\mathbb{Z}_n \rightarrow \mathbb{Z}_n$ d_m: $\bar{x} \mapsto lk\bar{x}$	$U_m = \langle \overline{lk^2} \rangle$ dengan $\bar{l}, \bar{k} \in \mathbb{Z}_n$

Maka rantai berikut rantai $\langle \overline{lk^2} \rangle$-kompleks

$$\dots \rightarrow \mathbb{Z}_n \xrightarrow[d_{m+1}]{} \mathbb{Z}_n \xrightarrow[d_m]{} \mathbb{Z}_n \xrightarrow[d_{m-1}]{} \dots \qquad (3)$$

Bukti

Perhatikan bahwa $U_{m-1} = \langle \overline{lk^2} \rangle$, $\mathrm{Im} d_m = \langle \overline{lk} \rangle$, $d_m d_{m+1}(\mathbb{Z}_n) = \langle \overline{l^2 k^2} \rangle$ untuk setiap m. Maka menurut Teorema 2, $d_m d_{m+1}(\mathbb{Z}_n) \subseteq U_{m-1}$ dan $\mathrm{Im} d_m \supseteq U_{m-1}$

□ Terbukti rantai (3) rantai U-kompleks

Teorema 5

Misalkan 2 rantai U-kompleks

$$\begin{array}{ccccccccc} (\mathbb{Z}_p, U^{\mathbb{Z}_p}, \partial) & \dots & \longrightarrow & \mathbb{Z}_p & \xrightarrow{\partial_{n+1}} & \mathbb{Z}_p & \xrightarrow{\partial_n} & \mathbb{Z}_p & \longrightarrow \dots \\ & & & \downarrow f_{n+1} & & \downarrow f_n & & \downarrow f_{n-1} & \\ (\mathbb{Z}_m, U^{\mathbb{Z}_m}, d) & \dots & \longrightarrow & \mathbb{Z}_m & \xrightarrow{d_{n+1}} & \mathbb{Z}_m & \xrightarrow{d_n} & \mathbb{Z}_m & \longrightarrow \dots \end{array}$$

dengan:

$\partial_n : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ $\bar{a} \longmapsto k\bar{a}$	$d_n : \mathbb{Z}_m \rightarrow \mathbb{Z}_m$ $\forall n$ $\bar{\bar{b}} \mapsto l\bar{\bar{b}}$

Misalkan pula f=$(f_n)_{n\square\mathbb{Z}}$ rantai (U,U')-pemetaan dengan:

$$f_n : \mathbb{Z}_p \rightarrow \mathbb{Z}_m \quad \forall n$$
$$\bar{a} \mapsto ra \bmod m$$

Maka berlaku:

1. Jika Jika l mod m=k mod m, maka nilai r yang memenuhi adalah semua anggota himpunan ℤ
2. Jika l mod m≠k mod m, maka nilai r yang memenuhi adalah 0 atau kelipatan dari m

Bukti:

Ambil sebarang $\bar{a} \in \mathbb{Z}_p$, karena f rantai (U,U')-pemetaan, maka:

$$d_n f_n(\bar{a}) = f_{n-1} \partial_n(\bar{a})$$

lra mod m=kra mod m

Berdasarkan sifat aritmatika modul, diperoleh nilai r yang memenuhi adalah:

1. Jika Jika l mod m=k mod m, maka nilai r yang memenuhi adalah semua anggota himpunan ℤ
2. Jika l mod m≠k mod m, maka nilai r yang memenuhi adalah 0 atau kelipatan dari m

Kesimpulan

Dengan memanfaatkan sifat-sifat aritmatika modulo, kita bisa membuat suatu bentuk umum dari rantai kompleks, U-kompleks dan (U,U')-pemetaan dari $\mathbb{Z}_n$, yaitu:

1. Misalkan untuk setiap m berlaku

   d_m: $\mathbb{Z}_n \rightarrow \mathbb{Z}_n$ dengan:

$d_m : \bar{x} \mapsto \bar{x}l\sqrt{n}$	Untuk n bilangan kuadrat, l□ℤ
$d_m : \bar{x} \mapsto \bar{x}l\sqrt{kn}$	Untuk n bukan bilangan kuadrat, dapat dicari k□ℤ sehingga kn bilangan kuadrat, dan l□ℤ

   Maka rantai berikut rantai kompleks

$$\dots \rightarrow \mathbb{Z}_n \xrightarrow[d_{m+1}]{} \mathbb{Z}_n \xrightarrow[d_m]{} \mathbb{Z}_n \xrightarrow[d_{m-1}]{} \dots$$

2. Misalkan untuk setiap m berlaku

d_m: $\mathbb{Z}_n \rightarrow \mathbb{Z}_n$ d_m: $\bar{x} \mapsto lk\bar{x}$	$U_m = \langle \overline{lk^2} \rangle$ dengan $\bar{l}, \bar{k} \in \mathbb{Z}_n$

   Maka rantai berikut rantai $\langle \overline{lk^2} \rangle$-kompleks

$$\dots \rightarrow \mathbb{Z}_n \xrightarrow[d_{m+1}]{} \mathbb{Z}_n \xrightarrow[d_m]{} \mathbb{Z}_n \xrightarrow[d_{m-1}]{} \dots$$

3. Misalkan 2 rantai U-kompleks

$$
\begin{array}{ccccccccc}
(\mathbb{Z}_p, U^{\mathbb{Z}_p}, \partial) & .... & \longrightarrow & \mathbb{Z}_p & \xrightarrow{\partial_{n+1}} & \mathbb{Z}_p & \xrightarrow{\partial_n} & \mathbb{Z}_p & \longrightarrow \ ... \\
 & & & \downarrow f_{n+1} & & \downarrow f_n & & \downarrow f_{n-1} & \\
(\mathbb{Z}_m, U^{\mathbb{Z}_m}, d) & .... & \longrightarrow & \mathbb{Z}_m & \xrightarrow{d_{n+1}} & \mathbb{Z}_m & \xrightarrow{d_n} & \mathbb{Z}_m & \longrightarrow \ ...
\end{array}
$$

dengan:

$\partial_n : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ $\overline{a} \longmapsto k\overline{a}$	$d_n : \mathbb{Z}_m \rightarrow \mathbb{Z}_m$ $\overline{\overline{b}} \mapsto l\overline{\overline{b}}$ $\forall n$

Misalkan pula rantai (U,U')-pemetaan $f=(f_n)_{n\square\mathbb{Z}}$ dengan:

$$f_n : \mathbb{Z}_p \rightarrow \mathbb{Z}_m \quad \forall n$$
$$\overline{a} \mapsto ra \mod m$$

Maka berlaku:

1. Jika Jika l mod m=k mod m, maka nilai r yang memenuhi adalah semua anggota himpunan $\mathbb{Z}$
2. Jika l mod m≠k mod m, maka nilai r yang memenuhi adalah 0 atau kelipatan dari m

4. Teori bilangan merupakan dasar dari ilmu kriptografi. Karena itu, hasil penelitian ini masih bisa dikembangkan untuk mendukung perkembangan ilmu kriptografi.

Ucapan terima kasih

Penulis mengucapkan terima kasih kepada civitas akademika program studi matematika Fakultas Sains dan Teknologi UIN Syarif Hidayatullah Jakarta yang telah mendidik dan mendukung penulis mengembangkan penelitian ini

Referensi

[1] B.Davvaz and H.Shabani-Solt, A generalization of Homological Algebra, J.Korean Math. Soc, 39 (2002), 6, 881-898
[2] B.Davvaz dan Y.A Parnian - Gramaleky, A Note on Exact Sequence, Bull. Malaysian Math. Soc. (2) 22 (1999), 53-56
[3] C.A Weibel, An Introduction to Homological Algebra, Cambridge University Press, United Kingdom, 1994
[4] I. Niven, H.S. Zuckerman, H.L. Montgomery, An Introduction to the Theory of Numbers, John Wiley & Sons, Inc. New York, 1960
[5] S.M. Anvariyeh dan B.Davvaz, U-Split Exact Sequence, Far East J. Math. Sci. (FJMS) 4 (2002), 2, 209-219

Utih Amartiwi*
Faculty of Science and Technology
UIN Syarif Hidayatullah Jakarta
utih.amartiwi@gmail.com

Gustina Elfiyanti
Faculty of Science and Technology
UIN Syarif Hidayatullah Jakarta
gustina.elfiyanti@uinjkt.ac.id

*Corresponding author