KARAKTERISTIK SUBMODUL SIKLIK PRIMA, PRIMA LEMAH DAN HAMPIR PRIMA PADA $\mathbb{Z} -$ MODUL $\mathbb{Z}_n[i]$

SKRIPSI

Oleh
RINA JULIANA
NIM : G1D016040
(Program Studi : Matematika)

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS MATARAM
2020

KARAKTERISTIK SUBMODUL SIKLIK PRIMA, PRIMA LEMAH DAN HAMPIR PRIMA PADA $\mathbb{Z} -$ MODUL $\mathbb{Z}_n[i]$

SKRIPSI

Karya tulis sebagai salah satu syarat untuk mendapatkan gelar Sarjana dari Universitas Mataram.

Oleh

RINA JULIANA
NIM : G1D016040
(Program Studi : Matematika)

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS MATARAM
2020

ABSTRAK

KARAKTERISTIK SUBMODUL SIKLIK PRIMA, PRIMA LEMAH DAN HAMPIR PRIMA PADA $\mathbb{Z}-$ MODUL $\mathbb{Z}_n[i]$

Oleh

RINA JULIANA

NIM: G1D016040

Kriptografi adalah salah satu cabang ilmu matematika yang digunakan pada sistem keamanan digital. Beberapa algoritma kriptografi yang terkenal seperti RSA, sangat bergantung pada faktorisasi prima dari bilangan bulat. Tetapi, kehadiran komputer kuantum dapat menjadi ancaman bagi sebagian algoritma dalam kriptografi. Sehingga salah satu usaha matematikawan dalam mencari alternatif untuk menciptakan teknologi keamanan baru dalam kriptografi adalah dengan mempelajari abstraksi bilangan prima. Salah satu bentuk abstraksi bilangan prima ialah submodul prima yang diperkenalkan oleh Dauns pada tahun 1978. Submodul prima kemudian diperumum menjadi submodul prima lemah dan submodul hampir prima. Pada penelitian ini dikaji karakteristik submodul siklik prima, prima lemah, dan hampir prima pada $\mathbb{Z}-$ modul $\mathbb{Z}_n[i]$. Salah satu hasilnya ialah jika n bilangan prima, maka setiap submodul siklik dari $\mathbb{Z}-$ modul $\mathbb{Z}_n[i]$ merupakan submodul prima.

Kata kunci: submodul siklik, submodul prima, submodul prima lemah, submodul hampir prima, $\mathbb{Z}-$ modul $\mathbb{Z}_n[i]$

ABSTRACT

THE CHARACTERISTICS OF PRIME, WEAKLY PRIME AND ALMOST PRIME CYCLIC SUBMODULES ON $\mathbb{Z} -$ MODULE $\mathbb{Z}_n[i]$

By

RINA JULIANA

NIM: G1D016040

Cryptography is a branch of mathematics that used in digital security systems. Some cryptographic algorithms, such as RSA, depend on prime factorization of integers. However, quantum computers might be a threat to some algorithms in cryptography. One of the mathematicians' efforts in finding alternatives to create new security technologies in cryptography is to study the abstraction of prime numbers. Prime submodule is one of the prime numbers abstraction which was introduced by Dauns in 1978. Lately, prime submodules were generalized into weakly prime submodules and almost prime submodules. This study will examine the characteristics of prime, weakly prime, and almost prime cyclic submodules in $\mathbb{Z} -$ module $\mathbb{Z}_n[i]$. One of the results is if n is a prime number then the cyclic submodule of $\mathbb{Z} -$ module $\mathbb{Z}_n[i]$ is prime submodule.

Keywords: cyclic submodules, prime submodules, weakly prime submodules, almost prime submodules, $\mathbb{Z} -$ module $\mathbb{Z}_n[i]$

PERNYATAAN

Dengan ini saya menyatakan bahwa skripsi ini murni karya saya sendiri dan di dalam skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu perguruan tinggi serta tidak terdapat karya atau pendapat yang pernah dituliskan atau dipublikasikan oleh orang lain, kecuali yang tertulis pada situasi dalam naskah ini dan disebutkan di dalam daftar pustakanya.

Mataram, Juli 2020
Yang menyatakan,

RINA JULIANA
NIM. G1D 016 040

HALAMAN PERSETUJUAN

KARAKTERISTIK SUBMODUL SIKLIK PRIMA, PRIMA LEMAH DAN HAMPIR PRIMA PADA $\mathbb{Z}$ – MODUL $\mathbb{Z}_n[i]$

RINA JULIANA
NIM : G1D016040

Menyetujui

Tim Pembimbing

Tanggal : Juli 2020

Pembimbing I,

Dr. I Gede Adhitya Wisnu Wardhana, S.Si., M.Si.
NIP. 19800429 200801 1 008

Pembimbing II,

Dr. Irwansyah, S.Si., M.Si.
NIP. 19890707 201504 1 004

HALAMAN PENGESAHAN

Skripsi yang berjudul:

KARAKTERISTIK SUBMODUL SIKLIK PRIMA, PRIMA LEMAH DAN HAMPIR PRIMA PADA $\mathbb{Z}$ – MODUL $\mathbb{Z}_n[i]$

RINA JULIANA
(G1D016040)

Telah dipertahankan di depan Tim Penguji Program Studi Matematika
Fakultas Matematika dan Ilmu Penegtahuan Alam
Pada tanggal : 24 Juli 2020

Tim Penguji

Dr. I Gede Adhitya Wisnu Wardhana, S.Si., M.Si. (Ketua)
NIP. 19800429 200801 1 008

Dr. Irwansyah, S.Si., M.Si. (Sekretaris)
NIP. 19890707 201504 1 004

Qurratul Aini, S.Si., M.Sc. (Anggota I)
NIP. 19870830 201404 2 002

Ni Wayan Switrayni, S.Pd., M.Si. (Anggota II)
NIP. 19890517 201504 2 002

Mengetahui,

Fakultas MIPA Universitas Mataram	Program Studi Matematika
Dekan,	Ketua,
Prof. Dedy Suhendra, Ph.D.	Dr. Marwan, S.Si., M.Si.
NIP. 19671207 199603 2 001	NIP. 19711005 200003 1 002

KATA PENGANTAR

Puji syukur kehadirat Allah SWT atas limpahan rahmat dan karunia-Nya sehingga penulis dapat merampungkan skripsi dengan judul : “Karakteristik Submodul Siklik Prima, Prima Lemah, dan Hampir Prima pada $\mathbb{Z} -$ modul $\mathbb{Z}_n[i]$”. Skripsi ini untuk memenuhi salah satu syarat menyelesaikan studi serta dalam rangka memperoleh gelar Sarjana Matematika pada Program Studi Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Mataram.

Penghargaan dan terima kasih yang setulus-tulusnya kepada Ibunda tercinta Suhaebah dan Ayahanda tercinta Syahrun yang telah mencurahkan segenap cinta dan kasih sayang serta perhatian moril maupun materil. Semoga Allah SWT selalu melimpahkan rahmat, kesehatan, karunia, dan keberkahan di dunia dan di akhirat atas budi baik yang telah diberikan kepada penulis.

Penghargaan dan terima kasih juga penulis berikan kepada Bapak Dr. I Gede Adhitya Wisnu Wardhana selaku Pembimbing I dan Bapak Dr. Irwansyah, M. Si. selaku Pembimbing II atas bimbingannya selama penulisan skripsi ini. Serta ucapan terima kasih kepada :

1. Bapak Prof. Dr. Lalu Husni, SH., M.Hum., selaku Rektor Universitas Mataram, atas kesempatan yang diberikan kepada penulis untuk mengikuti dan menyelesaikan pendidikan Strata Satu (S1) di Universitas Mataram.
2. Bapak Dedy Suhendra, Ph.D., selaku Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Mataram.
3. Bapak Dr. Marwan, S.Si., M.Si., selaku Ketua Program Studi Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Mataram.
4. Bapak/ Ibu Dosen pada Program Studi Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Mataram, atas ilmu dan pengetahuan yang diberikan kepada penulis.
5. Kakak-kakak tercinta yang selalu memberi dukungan moril maupun materiil.
6. Kawan-kawan seperjuangan Program Studi Matematika Angkatan 2016 (*COS 16),* atas dukungan dan kebersamaannya.

7. Kawan-kawan Donat the geng yang selalu mendukung, memberikan nasihat, dan pelajaran-pelajaran berharga.
8. Keluarga BPH Gamatika Research Club (GRC) 2019 yang selalu menemani dan memberi motivasi.

Akhir kata penulis menyadari bahwa dalam penulisan skripsi ini masih jauh dari kesempurnaan. Karena itu, penulis memohon saran dan kritik yang sifatnya membangun demi kesempurnaannya dan semoga bermanfaat bagi kita semua. Aamiin.

Mataram, Juli 2020

Penulis

DAFTAR ISI

DAFTAR GAMBAR

BAB I
PENDAHULUAN

Pada bab ini akan dijelaskan latar belakang yang mendasari perlunya dilakukan penelitian ini dan menetapkan rumusan masalah serta tujuan dari penelitian ini.

1.1 Latar Belakang

Bilangan prima pada bilangan bulat merupakan bilangan yang memiliki sifat unik. Saat ini, bilangan prima memiliki banyak aplikasi pada sistem keamanan digital. Hal ini tidak terlepas dari pekembangan komputer yang sangat pesat, yang kemudian memunculkan suatu masalah yaitu keamanan data. Kriptografi adalah salah satu cabang ilmu matematika yang banyak digunakan pada sistem keamanan digital. Kriptografi mempelajari ilmu enkripsi yang memanfaatkan sifat keunikan bilangan prima untuk membangkitkan kunci enkripsi. Di bidang ini, bilangan prima memegang peran yang sangat penting untuk menjaga kerahasiaan informasi. Salah satu usaha matematikawan dalam mencari alternatif untuk menciptakan teknologi keamanan baru dalam kriptografi adalah dengan mempelajari abstraksi bilangan prima.

Abstraksi bilangan prima ke dalam teori ring telah dilakukan sejak tahun 1871 oleh Dedekind, hasilnya ialah diperkenalkannya istilah ideal prima. Kemudian pada tahun 1978, Dauns memperkenalkan sistem matematika baru yang disebut submodul prima, yang merupakan abstraksi bilangan prima pada sistem matematika yang lebih kompleks. Selanjutnya pada tahun 2009, konsep submodul prima diperumum oleh Hadi menjadi submodul prima lemah. Kemudian pada tahun 2012, konsep submodul prima lemah ini diperumum kembali menjadi submodul hampir prima oleh Khashan.

Sifat-sifat bilangan prima pada ring bilangan bulat tidak sama dengan bilangan prima pada ring bilangan bulat Gauss ($\mathbb{Z}[i]$), hal ini dibahas oleh Maulana dkk pada tahun 2018. Salah satu fakta yang menarik yang ditemukan adalah tidak semua bilangan prima pada bilangan bulat juga merupakan bilangan prima pada bilangan bulat Gauss. Bilangan prima pada ring bilangan bulat merupakan bilangan prima pada ring bilangan bulat Gauss jika dan hanya jika bilangan tersebut dibagi 4 bersisa 3. Wardhana dan Astuti pada tahun 2014 memberikan karakteristik submodul prima lemah dan submodul hampir prima dengan mengambil studi kasus pada modul bilangan bulat modulo yaitu $\mathbb{Z}-$ modul $\mathbb{Z}_n$.

Konsep submodul prima, prima lemah dan submodul hampir prima pada $\mathbb{Z}-$ modul $\mathbb{Z}$ ekuivalen. Tetapi pada $\mathbb{Z}-$ modul $\mathbb{Z}_n$ terdapat banyak contoh submodul hampir prima yang bukan merupakan submodul prima lemah. Sehingga submodul prima lemah dan submodul hampir prima adalah dua konsep yang berbeda. Wardhana dan Astuti telah memberikan karakteristik submodul prima, submodul prima lemah, dan submodul hampir prima pada $\mathbb{Z}-$ modul $\mathbb{Z}_n$ pada tahun 2014. Oleh karena itu, timbul ketertarikan untuk mengetahui tentang konsep submodul prima, prima lemah dan hampir prima pada modul yang lebih kompleks yaitu bilangan bulat Gauss modulo $(\mathbb{Z}_n[i])$. Sehingga, pada tulisan ini akan dikaji karakteristik submodul prima, prima lemah dan submodul hampir prima pada modul bilangan bulat Gauss modulo atas ring bilangan bulat.

1.2 Rumusan Masalah

Dari latar belakang yang telah diuraikan sebelumnya, maka masalah yang dibahas dalam tulisan ini yaitu bagaimana karakteristik submodul siklik prima, prima lemah, dan hampir prima pada $\mathbb{Z}-$ modul $\mathbb{Z}_n[i]$?

1.3 Tujuan

Dari rumusan masalah di atas, dapat ditentukan tujuan dari penelitian ini yaitu untuk menentukan karakteristik submodul siklik prima, prima lemah, dan hampir prima pada $\mathbb{Z}-$ modul $\mathbb{Z}_n[i]$.

1.4 Manfaat

Adapun manfaat dari penelitian ini, antara lain ialah penelitian ini diharapkan dapat:

1. Menjadi pengembangan ilmu pengetahuan dalam bidang teori modul.
2. Menjadi tambahan pengetahuan bagi pembaca dan penulis sendiri.

1.5 Batasan Masalah

Pembahasan dalam penelitian ini dibatasi hanya pada submodul sejati yang siklik dari $\mathbb{Z} -$ modul $\mathbb{Z}_n[i]$.

BAB II
LANDASAN TEORI

Pada bagian ini akan dijabarkan beberapa teori yang menjadi dasar dalam penelitian ini, yaitu grup, ring, modul, submodul dan bilangan bulat Gauss modulo.

2.1 Grup

Struktur aljabar terdiri dari suatu himpunan objek, satu atau lebih operasi pada himpunan yang disertai dengan hukum tertentu yang dipenuhi oleh operasi. Berikut akan dijabarkan definisi operasi biner dan beberapa istilah yang berlaku pada operasi tersebut.

Definisi 2.1.1 (Dummit & Foote, 2004)

1. *Sebuah operasi biner* $*$ *pada himpunan* G *adalah sebuah fungsi* $*: G \times G \to G$.
2. *Sebuah operasi biner* $*$ *pada himpunan* G *dikatakan asosiatif jika* $\forall a, b, c \in G$ *berlaku* $(a * b) * c = a * (b * c)$.
3. *Sebuah operasi biner* $*$ *pada himpunan* G *dikatakan komutatif jika* $\forall a, b \in G$, $a * b = b * a$.

Selanjutnya definisi grup akan dijabarkan sebagai berikut.

Definisi 2.1.2 (Dummit & Foote, 2004)

Grup adalah suatu pasangan terurut $(G,*)$ *yang terdiri atas himpunan* G *yang disertai dengan operasi biner* $*$ *yang didefinisikan pada* G *dan memenuhi sifat berikut:*

1. *Untuk setiap* $\forall a, b, c \in G$ *berlaku* $(a * b) * c = a * (b * c)$.
2. *Terdapat suatu elemen* $e \in G$, *yang dinamakan dengan identitas pada* G *sehingga untuk setiap* $a \in G$ *berlaku* $e * a = a * e$.
3. *Untuk setiap* $a \in G$, *terdapat* $a^{-1} \in G$ *sehingga* $a * a^{-1} = a^{-1} * a = e$.

Grup $(G,*)$ *dikatakan abelian (komutatif) jika untuk semua* $a, b \in G, a * b = b * a$.

Contoh 2.1.1

1. Himpunan bilangan bulat yaitu $\mathbb{Z}$, terhadap operasi penjumlahan merupakan grup komutatif, dengan $e = 0$ dan $a^{-1} = -1$ untuk setiap $a \in \mathbb{Z}$.
2. Himpunan bilangan bulat yaitu $\mathbb{Z}$ terhadap operasi perkalian biasa bukan grup, karena $2 \in \mathbb{Z}$ tidak memiliki invers.

2.2 Ring

Sistem matematika yang dilengkapi oleh dua operasi yaitu penjumlahan dan perkalian, sehingga terhadap operasi penjumlahan membentuk grup abelian, dapat membentuk suatu ring. Selanjutnya akan dijabarkan definisi ring sebagai berikut.

Definisi 2.2.1 (Dummit & Foote, 2004)

1. *Suatu himpunan* G *dengan dua operasi biner yaitu penjumlahan* $(+)$ *dan perkalian* $(*)$ *yang didefinisikan pada* G *dinamakan* ring *apabila memenuhi sifat berikut:*
   a. $(G, +)$ *merupakan grup abelian.*
   b. *Operasi* $*$ *bersifat asosiatif* $(a * b) * c = a * (b * c)$, $\forall\, a, b, c \in G$.
   c. *Berlaku sifat distributif pada* $G: \forall\, a, b, c \in G, a * (b + c) = (a * b) + (a * c)$ *dan* $(a + b) * c = (a * c) + (b * c)$
2. *Ring G dikatakan komutatif jika operasi* $*$ *bersifat komutatif.*
3. *Ring G dikatakan memiliki elemen satuan terhadap operasi perkalian jika terdapat elemen* $1 \in G$ *sehingga* $a * 1 = 1 * a = a, \forall\, a \in G$.

Contoh 2.2.1

Himpunan bilangan bulat $(\mathbb{Z})$, himpunan bilangan bulat modulo $(\mathbb{Z}_n)$, dan himpunan bilangan bulat Gauss modulo $(\mathbb{Z}_n[i])$ dengan operasi penjumlahan dan perkalian merupakan ring komutatif dengan elemen satuan.

Pada uraian selanjutnya, notasi $a * b$ ditulis dengan ab. Selanjutnya akan dijabarkan definisi ideal yang merupakan bentuk khusus dari subhimpunan sebuah *ring*.

Definisi 2.2.2 (Dummit & Foote, 2004)

Misalkan R ring dan $I \subseteq R$, I disebut ideal dari ring R jika memenuhi :

1. *Untuk setiap $a, b \in I$ maka $a - b \in I$.*
2. *Untuk setiap $a \in I$ dan $r \in R$, maka $ar \in I$ dan $ra \in I$.*

Selanjutnya $I \subseteq R$ disebut ideal kanan jika memenuhi sifat pada poin 1 di atas, dan $Ir \subseteq I$ untuk setiap $r \in R$, dimana $Ir = \{ar \mid a \in I\}$. $I \subseteq R$ disebut ideal kiri jika memenuhi sifat pada poin 1 di atas, dan $rI \subseteq I$ untuk setiap $r \in R$, dimana $rI = \{ra \mid a \in I\}$.

Definisi 2.2.3 (Dummit & Foote, 2004)

Diberikan $(R, +, *)$ suatu ring, Ideal I disebut ideal utama jika I dapat dibangun oleh suatu elemen dalam R atau dengan kata lain, terdapat $a \in R$ sedemikian hingga $I = \langle a \rangle$.

Contoh 2.2.2

1. Himpunan bilangan bulat genap yakni $2\mathbb{Z}$ merupakan ideal utama dari ring $\mathbb{Z}$ yang dibangun oleh 2.
2. Ideal $\langle 2, x \rangle$ dari ring $\mathbb{Z}[x]$ bukan merupakan ideal utama. Pandang $\langle 2, x \rangle = \{2p(x) + xq(x) \mid p(x), q(x) \in \mathbb{Z}[x]\}$, sehingga ideal ini memuat polinomial dengan koefisien bilangan bulat dengan suku konstan nya genap. Jelas bahwa $1 \notin \langle 2, x \rangle$, sehingga ideal tersebut ideal sejati. Andaikan ideal $\langle 2, x \rangle$ merupakan ideal utama, yaitu $\langle 2, x \rangle = \langle a(x) \rangle$ untuk suatu $a(x) \in \mathbb{Z}[x]$. Karena $2 \in \langle a(x) \rangle$, maka terdapat $p(x) \in \mathbb{Z}[x]$ sehingga $2 = p(x)a(x)$. Derajat polinomial $p(x)a(x)$ yaitu derajat $p(x) +$ derajat $a(x) = 0$. Dengan demikian $p(x), a(x)$ haruslah suatu konstanta. Karena ideal tersebut ideal sejati maka kemungkinan $a(x) = \pm 2$. Tetapi $x \in \langle a(x) \rangle = \langle 2 \rangle = \langle -2 \rangle$, sehingga $x = 2q(x)$ untuk suatu $q(x) \in \mathbb{Z}[x]$, jelas

tidak mungkin terjadi. Dengan demikian pengandaian salah, sehingga haruslah ideal $\langle 2, x \rangle$ bukan ideal utama.

Definisi 2.2.4 (Dummit & Foote, 2004)
Misalkan R suatu ring komutatif. Suatu ideal I disebut ideal prima jika $I \neq R$ dan untuk $ab \in I$ dengan $a, b \in R$, maka $a \in I$ atau $b \in I$.

Suatu ideal I dari ring R dikatakan ideal maksimal bila I berbeda dengan R dan tidak ada ideal lain selain R yang mengandung I. Berikut definisinya.

Definisi 2.2.5 (Dummit & Foote, 2004)
Suatu ideal I dari R dinamakan ideal maksimal jika $I \neq R$ dan apabila ada ideal J dari R dimana $I \subseteq J \subseteq R$ maka $I = J$ atau $J = R$.

Contoh 2.2.3

1. Ideal $I = \langle 2 \rangle$ merupakan ideal maksimal dari ring $\mathbb{Z}$, karena tidak ada ideal lain yang mengandung I kecuali $\mathbb{Z}$ itu sendiri.
2. Ideal $I = \langle 4 \rangle$ bukan merupakan ideal maksimal dari ring $\mathbb{Z}$ karena ada ideal $J = \langle 2 \rangle \neq \mathbb{Z}$ dimana $I \subset J$.

Selanjutnya akan dijabarkan definisi dari beberapa istilah dalam ring, seperti pembagi nol, unit, dan daerah integral.

Definisi 2.2.6 (Dummit & Foote, 2004)
Misalkan R adalah sebuah ring. Suatu elemen tak nol $a \in R$ dinamakan pembagi nol jika terdapat suatu elemen tak nol $b \in R$ sehingga berlaku $ab = 0$ atau $ba = 0$.

Definisi 2.2.7 (Fraleigh, 2014)
Suatu elemen u dari ring komutatif R dengan unsur satuan disebut unit jika u habis membagi 1 atau dengan kata lain u memiliki invers perkalian. Dua elemen $a, b \in R$ berasosiasi di R jika $a = bu$ dimana u adalah suatu unit di R.

Contoh 2.2.4

1. Elemen $\overline{2} \in \mathbb{Z}_6$ merupakan pembagi nol, karena terdapat $\overline{3} \in \mathbb{Z}_6$ sehingga $\overline{2} \cdot \overline{3} = \overline{0}$
2. Elemen $\overline{2} \in \mathbb{Z}_5$ merupakan unit, karena terdapat $\overline{3} \in \mathbb{Z}_5$ sehingga $\overline{2} \cdot \overline{3} = \overline{1}$. Himpunan semua unit pada ring $\mathbb{Z}_5$ terdiri dari $\{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$

Definisi 2.2.7 (Dummit & Foote, 2004)

Suatu ring komutatif dengan elemen satuan dinamakan daerah integral jika ring tersebut tidak memuat pembagi nol.

Contoh 2.2.5

1. Ring $\mathbb{Z}$ merupakan salah satu contoh daerah integral karena tidak memuat pembagi nol.
2. Ring $\mathbb{Z}_6$ dengan operasi penjumlahan dan perkalian modulo 6 bukan merupakan daerah integral, karena memuat pembagi nol yaitu $\overline{2}$ dan $\overline{3}$.

Definisi 2.2.8 (Dummit & Foote, 2004)

Suatu daerah integral R dinamakan Daerah Ideal Utama jika setiap ideal di R merupakan ideal utama.

Contoh 2.2.6

1. Ring $\mathbb{Z}$ merupakan salah satu contoh daerah ideal utama karena setiap idealnya merupakan ideal utama.
2. Ring $\mathbb{Z}[x]$ bukan merupakan daerah ideal utama karena terdapat Ideal $\langle 2, x \rangle$ yang dibangun oleh 2 dan x.

Dalam daerah integral, bilangan prima dan bilangan tak tereduksi dapat didefinisikan sebagai berikut.

Definisi 2.2.9 (Fraleigh, 2014)

Suatu elemen taknol dan bukan unit p dari suatu daerah integral R disebut tak tereduksi di R jika setiap pemfaktoran $p = ab$ di R hanya terpenuhi bila a atau b adalah unit.

Untuk suatu daerah integral R, elemen $r \in R$ dikatakan membagi $s \in R$ (ditulis $r|s$) jika terdapat suatu elemen $x \in R$ sedemikian sehingga $s = xr$. Pada daerah integral R, dapat didefinisikan elemen prima sebagai berikut.

Definisi 2.2.10 (Fraleigh, 2014)

Suatu elemen taknol dan bukan unit p dari suatu daerah integral R disebut prima jika untuk setiap $a, b \in R$, $p|ab$ berimplikasi $p|a$ atau $p|b$.

Contoh 2.2.7

1. Pada bilangan bulat, 5 merupakan salah satu bilangan tak tereduksi karena semua faktornya berbentuk $5 = 5 \cdot 1$ atau $5 = (-5) \cdot (-1)$ dimana 1 dan -1 merupakan unit.
2. Pada bilangan bulat, 6 bukan merupakan bilangan tak tereduksi karena ada faktornya yang berbentuk $6 = 2 \cdot 3$ dimana 2 dan 3 keduanya bukan unit.

Dalam daerah ideal utama, ideal maksimal dan bilangan tak tereduksi saling berkaitan. Berikut teoremanya.

Teorema 2.2.1 (Fraleigh, 2014)

Suatu ideal $\langle p \rangle$ pada daerah ideal utama merupakan ideal maksimal jika dan hanya jika p tak tereduksi.

Bukti.

Diberikan p ideal maksimal dari suatu daerah ideal utama R. Andaikan $p = ab$ di R, maka $\langle p \rangle \subseteq \langle a \rangle$. Jika $\langle p \rangle = \langle a \rangle$ maka a dan p berasosiasi, sehingga b merupakan unit. Jika $\langle p \rangle \neq \langle a \rangle$ maka haruslah $\langle a \rangle = \langle 1 \rangle = R$ karena $\langle p \rangle$ ideal maksimal, sehingga a dan 1 berasosiasi. Akibatnya a unit. Dari dua kasus tersebut diperoleh a atau b unit. Jadi p tak tereduksi.

Sebaliknya, andaikan p tak tereduksi di R. Jika $\langle p \rangle \subseteq \langle a \rangle$ kita dapatkan $p = ab$. Jika a unit, maka $\langle a \rangle = \langle 1 \rangle = R$. Jika a bukan unit, maka b harus unit, sehingga terdapat $u \in R$ sehingga $bu = 1$. Akibatnya $pu = abu = a1 = a$, jadi $\langle a \rangle \subseteq \langle p \rangle$ dan kita dapatkan $\langle p \rangle = \langle a \rangle$. Dari dua kasus tersebut diperoleh $\langle a \rangle = R$ atau $\langle a \rangle = \langle p \rangle$. Jadi $\langle p \rangle$ ideal maksimal.

■

Dalam daerah ideal utama, elemen tak tereduksi dan elemen prima ekivalen. Lebih jelasnya berikut teorema yang diberikan.

Teorema 2.2.2 (Roman, 2008)

Misalkan R daerah ideal utama, $p \in R$ prima jika hanya jika p tak tereduksi.

Bukti.

Misalkan p prima dan $p = ab$, artinya $p|ab$. Karena p prima berlaku $p|a$ atau $p|b$. Tanpa mengurangi keumuman, misalkan hanya berlaku $p|a$, artinya $a = pk$ untuk suatu $k \in R$. Selanjutnya $p = ab = pkb$, diperoleh $p(1 - kb) = 0$. Karena daerah ideal utama merupakan daerah integral dan $p \neq 0$ maka haruslah $1 - kb = 0$ diperoleh $kb = 1$. Akibatnya b suatu unit di R. Jadi p tak tereduksi.

Sebaliknya, misalkan p tak tereduksi dan $p|ab$. Berdasarkan Teorema 2.2.1 diperoleh $\langle p \rangle$ ideal maksimal. Akibatnya $\langle p, a \rangle = \langle p \rangle$ atau $\langle p, a \rangle = R = \langle 1 \rangle$. Untuk $\langle p, a \rangle = \langle p \rangle$ diperoleh $p|a$. Untuk $\langle p, a \rangle = R = \langle 1 \rangle$ diperoleh $1 = xp + ya$ untuk suatu $x, y \in R$. Dengan mengalikan kedua ruas dengan b diperoleh $b = bxp + bya$. Karena $p|bxp$ dan $p|bya$ maka $p|b$. Dari kedua kasus tersebut maka $p|a$ atau $p|b$. Jadi p prima.

■

Selanjutnya dalam daerah ideal utama, dua elemen dikatakan saling prima jika kedua elemen tersebut tidak mempunyai faktor bersama yang bukan unit.

Teorema 2.2.3 (Roman, 2008)

Misalkan R daerah ideal utama. Elemen $a, b \in R$ relatif prima, yaitu tidak mempunyai faktor bersama yang bukan unit, jika dan hanya jika terdapat $r, s \in R$ sedemikian sehingga $ra + sb = 1$, yang dinotasikan dengan $(a, b) = 1$.

Bukti.

Misalkan $a, b \in R$ relatif prima. Pandang ideal $\langle a, b\rangle$, karena R daerah ideal utama maka ideal tersebut merupakan ideal utama. Akibatnya, terdapat $d \in R$ sehingga $\langle a, b\rangle = \langle d\rangle$, diperoleh $d|a$ dan $d|b$. Karena a dan b relatif prima, maka diperoleh d merupakan unit. Akibatnya $\langle a, b\rangle = R$. Dengan demikian terdapat $r, s \in R$ sedemikian sehingga $ra + sb = 1$.

Sebaliknya, jika $(a, b) = 1$ atau $ra + sb = 1$ untuk suatu $r, s \in R$, maka jelas a dan b relatif prima.

■

Contoh 2.2.8

Pada daerah ideal utama $\mathbb{Z}$, 5 relatif prima dengan 7 karena terdapat $3, (-2) \in \mathbb{Z}$ sehingga $3 \cdot 5 + (-2) \cdot 7 = 1$.

Setiap bilangan bulat, dapat ditulis sebagai perkalian hingga bilangan bilangan prima. Secara umum, pada daerah integral yang setiap elemennya dapat ditulis sebagai perkalian hingga bilangan-bilangan tak tereduksi dikatakan daerah faktorisasi tunggal. Berikut definisi yang diberikan.

Definisi 2.2.11 (Roman, 2008)

Suatu daerah integral R disebut daerah faktorisasi tunggal bila memenuhi kondisi berikut:

a. *Setiap elemen R yang bukan nol ataupun unit bisa difaktorkan menjadi perkalian hingga bilangan tak tereduksi.*
b. *Jika $p_1 p_2 \dots p_r$ dan $q_1 q_2 \dots q_s$ adalah dua faktorisasi berbeda dari suatu unsur di R maka $r = s$ dan faktorisasi q_j dapat diurutkan kembali sehingga p_i dan q_i berasosiasi.*

Telah diketahui bahwa pada ruang vektor, skalar-skalarnya berasal dari suatu lapangan. Selanjutnya akan dijabarkan definisi lapangan.

Definisi 2.2.12 (Dummit & Foote, 2004)
Suatu ring dengan elemen satuan disebut ring hasil bagi jika setiap elemen tak nol $a \in R$ memiliki invers terhadap operasi perkalian, dengan kata lain, terdapat $b \in R$ sehingga $ab = ba = 1$. Ring hasil bagi yang memenuhi sifat komutatif dinamakan dengan lapangan.

Contoh 2.2.9

1. Ring $\mathbb{Z}_5$ merupakan lapangan karena semua elemen tak nol pada $\mathbb{Z}_5$ memiliki invers terhadap operasi perkalian.
2. Ring $\mathbb{Z}$ bukan lapangan, karena $2 \in \mathbb{Z}$ tidak memiliki invers terhadap operasi perkalian.

2.3 Modul

Dalam ruang vektor, diketahui bahwa skalar-skalarnya berasal dari lapangan, dengan kata lain suatu ruang vektor V terbentuk apabila V adalah grup aditif abelian yang dilengkapi dengan skalar yang berasal dari suatu lapangan F dan memenuhi beberapa aksioma. Pada modul, syarat skalar cukup berasal dari suatu ring. Berikut akan dijabarkan definisi modul.

Definisi 2.3.1 (Roman, 2008)
Diberikan R ring komutatif dengan elemen satuan. Suatu $R -$ modul atau modul atas R adalah himpunan M dengan dua operasi, yaitu penjumlahan yang dinotasikan dengan $+$, yang menghubungkan setiap elemen $(u, v) \in M\ x\ M$ terhadap elemen $u + v \in M$, dan perkalian scalar yang menghubungkan elemen $(r, v) \in R \times M$ terhadap elemen $rv \in M$. Lebih jauh sifat-sifat berikut harus terpenuhi:

1. *$(M, +)$ merupakan grup abelian*
2. *Untuk setiap $r, s \in R$ dan untuk setiap $m, n \in M$ berlaku*
   a. $(r + s)m = rm + sm$

b. $(rs)m = r(sm)$

c. $r(m+n) = rm + rn$

d. $1m = m$

Contoh 2.3.1

$\mathbb{Z}-$modul $\mathbb{Z}$, $\mathbb{Z}-$modul $\mathbb{Z}_n$, $\mathbb{Z}-$modul $\mathbb{Z}_n[i]$ merupakan modul atas ring bilangan bulat.

Pada suatu ruang vektor V atas lapangan F, himpunan yang terdiri dari satu elemen $\{v\}$ dengan $v \neq 0$ merupakan himpunan bebas linear. Himpunan bebas linear pada suatu $R-$modul M didefinisikan sebagai berikut.

Definisi 2.3.2 (Roman, 2008)

Suatu himpunan S subset dari $R-$modul M dikatakan bebas linear jika untuk setiap $v_1, \dots, v_n \in S$ dan $r_1, \dots, r_n \in R$ berlaku

$$r_1v_1 + \cdots + r_nv_n = 0 \Longrightarrow r_i = 0 \text{ untuk setiap } i = 1,2, \dots, n.$$

Himpunan S yang tidak bebas linear disebut bergantung linear.

Jika pada ruang vektor himpunan tunggal pasti bebas linear, pada modul tidak selalu terjadi, contohnya pada $\mathbb{Z}-$modul $\mathbb{Z}_6$, $\{\bar{2}\}$ tidak bebas linear karena terdapat $3 \neq 0 \in \mathbb{Z}$ sedemikian sehingga $3 \cdot \bar{2} = \bar{0}$. Hal ini mendasari definisi modul torsi, yang diuraikan sebagai berikut.

Definisi 2.3.3 (Roman, 2008)

Misalkan M suatu $R-$modul. Suatu elemen tak nol $v \in M$ sedemikian hingga $rv = 0$ untuk suatu $r \in R$ yang tak nol disebut elemen torsi dari M. Modul yang tidak mempunyai elemen torsi selain nol disebut bebas torsi. Jika setiap elemen dari M merupakan elemen torsi, maka M disebut modul torsi. Himpunan semua elemen torsi dari M digabungkan dengan nol dinotasikan dengan M_{tor}.

Contoh 2.3.2

$\mathbb{Z}-$modul $\mathbb{Z}_n$ dan $\mathbb{Z}-$modul $\mathbb{Z}_n[i]$ merupakan modul torsi, karena semua elemennya merupakan elemen torsi.

2.4 Submodul

Seperti halnya ruang vektor yang memiliki subhimpunan yang membentuk ruang vektor atas lapangan yang sama, modul juga memiliki subhimpunan yang membentuk modul atas ring yang sama dan disebut submodul. Berikut ini dijabarkan definisi submodul.

Definisi 2.4.1 (Roman, 2008)

Suatu subhimpunan S dari $R-$ modul M dinamakan submodul dari M jika S membentuk $R-$ modul terhadap operasi yang sama dengan operasi yang didefinisikan pada M. Selanjutnya $S \leq M$ digunakan untuk menotasikan S submodul dari M.

Submodul dari M merupakan subhimpunan M yang membentuk modul terhadap operasi yang berlaku pada M. Dapat diperhatikan, jika R adalah suatu lapangan, maka submodul sama dengan subruang. Setiap $R-$modul M pasti memiliki setidaknya dua buah submodul yaitu M dan $\{0\}$ (disebut dengan submodul trivial).

Teorema 2.4.1 (Switrayni, 2015)

Misalkan diberikan suatu R-modul M dan $N \subseteq M$, maka N adalah submodul dari M jika dan hanya jika memenuhi dua syarat berikut:

1. $n_1 - n_2 \in N, \forall\, n_1, n_2 \in N$

2. $rn \in N, \forall\, n \in N;\ \forall\, r \in R$

Bukti.

($\Rightarrow$) Diketahui bahwa N adalah submodul dari modul M, maka N membentuk grup abelian terhadap operasi penjumlahan, sehingga N merupakan subgrup dari M, akibatnya untuk setiap $n_1, n_2 \in N$, berlaku $n_1 - n_2 \in N$. Karena N merupakan submodul dari M akibatnya operasi perkalian skalar yang berlaku pada M juga berlaku pada N, sehingga untuk setiap $r \in R$ dan $n \in N$ maka $rn \in N$.

($\Leftarrow$) Diketahui untuk setiap $n_1, n_2 \in N$ berlaku $n_1 - n_2 \in N$, maka N merupakan subgrup dari M. Selanjutnya, karena sifat abelian pada M juga berlaku pada N, maka N merupakan subgrup abelian. Diketahui pula bahwa untuk setiap $n \in N$ dan $r \in R$, berlaku $rn \in N$, maka operasi skalar di M juga berlaku di N, sehingga untuk setiap $n_1, n_2 \in N$, dan $r, s \in R$ berlaku:

a. $(r+s)n = rn + sn$

b. $(rs)n = r(sn)$

c. $r(n_1 + n_2) = rn_1 + rn_2$

d. $1n = n$

Jadi, N membentuk suatu modul di bawah operasi yang sama dengan M. Dengan demikian N merupakan submodul dari M.

■

Contoh 2.4.1

1. $2\mathbb{Z}$ merupakan submodul dari $\mathbb{Z}-$modul $\mathbb{Z}$ karena membentuk modul terhadap operasi yang sama atas ring $\mathbb{Z}$.
2. Subhimpunan $N = \{0,1,3\}$ dari $\mathbb{Z}-$modul $\mathbb{Z}$ bukan submodul, karena $3 - 1 = 2 \notin N$.

Selanjutnya akan dijabarkan definisi himpunan pembangun pada submodul, sebagai berikut.

Definisi 2.4.2 (Roman, 2008)

Submodul yang dibangun oleh suatu himpunan S subset dari modul M merupakan himpunan semua kombinasi linear dari elemen-elemen S, yaitu:

$$\langle\langle S\rangle\rangle = \{r_1v_1 + r_2v_2 + \cdots + r_nv_n | r_i \in R, v_i \in S, n \geq 1\}.$$

Himpunan S dikatakan membangun modul M jika $M = \langle\langle S\rangle\rangle$.

Submodul yang memiliki himpunan pembangun, yang terdiri dari satu elemen disebut submodul siklik. Definisinya diberikan sebagai berikut.

Definisi 2.4.3 (Roman, 2008)

Misalkan M merupakan R-modul, suatu submodul yang berbentuk

$$\langle\langle v\rangle\rangle = Rv = \{rv \mid r \in R\}$$

untuk $v \in M$, disebut submodul siklik yang dibangun oleh v.

Contoh 2.4.2

1. $\langle\langle 2\rangle\rangle$ merupakan submodul siklik pada $\mathbb{Z}-$ modul $\mathbb{Z}$ karena dibangun oleh satu elemen yaitu 2.
2. $\langle\langle \overline{1} + \overline{2}i\rangle\rangle$ merupakan submodul siklik pada $\mathbb{Z}-$modul $\mathbb{Z}_3[i]$ karena dibangun oleh satu elemen yaitu $\overline{1} + \overline{2}i$.

Pada ruang vektor dikenal istilah hasil tambah langsung. Begitu juga dengan modul, dapat didefinisikan hasil tambah langsung pada suatu $R-$modul M. Namun sebelumnya, diberikan definisi penjumlahan dua submodul dari suatu $R-$modul M sebagai berikut.

Definisi 2.4.4 (Dummit & Foote, 2004)

Diberikan A, B submodul dari suatu $R-$modul M. Jumlahan dari A dan B merupakan himpunan

$$A + B = \{a + b \mid a \in A, b \in B\}.$$

Selanjutnya, definisi hasil tambah langsung pada suatu $R-$modul M diberikan sebagai berikut.

Definisi 2.4.5 (Roman, 2008)

Suatu R-modul M merupakan hasil tambah langsung dalam dari himpunan $\digamma = \{S_i \mid i \in I\}$ submodul dari M, dapat dinyatakan sebagai

$$M = \bigoplus \digamma \text{ atau } M = \bigoplus_{i\in I} S_i$$

Jika berlaku:

1. *M merupakan jumlah dari keluarga himpunan $\digamma$*

$$M = \sum_{i\in I} S_i$$

2. *Untuk setiap $i \in I$ berlaku*

$$S_i \cap \left(\sum_{j \neq i} S_j \right) = \{0\}$$

Dalam hal ini setiap S_i disebut jumlah langsung dari M. Jika $\digamma = \{S_1, \dots, S_n\}$ *keluarga himpunan yang berhingga, jumlah langsung biasanya dituliskan sebagai*

$$M = S_1 \oplus \dots \oplus S_n$$

Contoh 2.4.3

$\mathbb{Z}-$modul $\mathbb{Z}_6$ dapat dituliskan sebagai hasil tambah langsung submodul $N_1 = \langle\langle \bar{2} \rangle\rangle = \{\bar{0}, \bar{2}, \bar{4}\}$ dan $N_2 = \langle\langle \bar{3} \rangle\rangle = \{\bar{0}, \bar{3}\}$. Karena $N_1 + N_2 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\} = \mathbb{Z}_6$ dan $N_1 \cap N_2 = \{\bar{0}\}$.

Selanjutnya akan dijabarkan definisi submodul prima, submodul prima lemah dan submodul hampir prima. Pada bagian ini, ring yang dimaksud selalu ring komutatif dengan unsur satuan. Diberikan dua buah submodul N dan K dari $R-$modul M. Sisa dari N oleh K dinotasikan dengan $(N: K)$ didefinisikan dengan himpunan $(N: K) = \{r \in R \mid rK \subseteq N\}$.

Contoh 2.4.4

1. Misalkan $M = \mathbb{Z}_3$ modul atas $\mathbb{Z}$ dan $N = \langle\langle \bar{0} \rangle\rangle$ submodul dari M. Didapatkan sisa N oleh M sebagai berikut, $(N: M) = \{r \in \mathbb{Z} \mid rM \subseteq N\} = \{r \in \mathbb{Z} \mid r\bar{a} \in N, \ \forall\, \bar{a} \in \mathbb{Z}_3\} = 3\mathbb{Z}$.
2. Misalkan $M = \mathbb{Z}_6$ modul atas $\mathbb{Z}$ dan $N = \langle\langle \bar{2} \rangle\rangle$ submodul dari M. Didapatkan sisa N oleh M sebagai berikut, $(N: M) = \{r \in \mathbb{Z} \mid rM \subseteq N\} = \{r \in \mathbb{Z} \mid r\bar{a} \in N, \ \forall\, \bar{a} \in \mathbb{Z}_6\} = 2\mathbb{Z}$.
3. Misalkan $M = \mathbb{Z}_4$ modul atas $\mathbb{Z}$ dan $N = \langle\langle \bar{0} \rangle\rangle$ submodul dari M. Didapatkan sisa N oleh M sebagai berikut, $(N: M) = \{r \in \mathbb{Z} \mid rM \subseteq N\} = \{r \in \mathbb{Z} \mid r\bar{a} \in N, \ \forall\, \bar{a} \in \mathbb{Z}_4\} = 4\mathbb{Z}$.

Definisi 2.4.6 (Dauns, 1978)

Misalkan M adalah suatu R −modul, submodul sejati N dikatakan submodul prima apabila untuk setiap $r \in R$ dan $m \in M$ dengan $rm \in N$, berlaku $r \in (N: M)$ atau $m \in N$.

Contoh 2.4.5

1. $N = \langle\langle \bar{0} \rangle\rangle$ merupakan submodul prima pada $\mathbb{Z}$ −modul $\mathbb{Z}_3$, karena untuk setiap $r \in \mathbb{Z}$ dan $\bar{m} \in \mathbb{Z}_3$ dengan $r\bar{m} \in N$, berlaku $r \in (N: M) = 3\mathbb{Z}$ atau $\bar{m} = \bar{0} \in \mathbb{Z}_3$.
2. $N = \langle\langle \bar{2} \rangle\rangle$ merupakan submodul prima pada $\mathbb{Z}$ −modul $\mathbb{Z}_6$, karena untuk setiap $r \in \mathbb{Z}$ dan $\bar{m} \in \mathbb{Z}_6$ dengan $r\bar{m} \in N$, berlaku $r \in (N: M) = 2\mathbb{Z}$ atau $\bar{m} \in \mathbb{Z}_6$.
3. $N = \langle\langle \bar{0} \rangle\rangle$ bukan submodul prima pada $\mathbb{Z}$ −modul $\mathbb{Z}_4$, karena terdapat $2 \notin (N: M) = 4\mathbb{Z}$ dan $\bar{2} \notin N$ sehingga $\bar{2}.\bar{2} = \bar{0} \in N$.

Submodul prima lemah adalah perumuman submodul prima, yang didefinisikan sebagai berikut.

Definisi 2.4.7 (Hadi, 2009)

Misalkan N adalah submodul sejati dari R −modul M. Submodul N dikatakan submodul prima lemah apabila untuk setiap $r \in R$ dan $m \in M$ dengan $rm \in N - \{0\}$, berlaku $r \in (N : M)$ atau $m \in N$.

Berdasarkan definisi di atas, dapat diketahui bahwa submodul nol pasti merupakan submodul prima lemah dan setiap submodul prima pasti merupakan submodul prima lemah. Sebaliknya submodul prima lemah belum tentu merupakan submodul prima. Beberapa contohnya diuraikan pada contoh berikut.

Contoh 2.4.5

1. $N = \langle\langle \bar{0} \rangle\rangle$ merupakan submodul prima lemah pada $\mathbb{Z}$ −modul $\mathbb{Z}_6$, tetapi bukan submodul prima karena terdapat $2 \notin (N: M) = 6\mathbb{Z}$ dan $\bar{3} \notin N$ sedemikian sehingga $2 \cdot \bar{3} = \bar{0}$.

2. $N = \langle\langle\bar{1} + i\rangle\rangle$ merupakan submodul prima lemah pada $\mathbb{Z}$ −modul $\mathbb{Z}_3[i]$ karena untuk setiap $r \in \mathbb{Z}$ dan $m \in M = \mathbb{Z}_3[i]$ dengan $rm \in N - \{0\}$, berlaku $r \in (N : M) = 3\mathbb{Z}$ atau $m \in N$.
3. $N = \langle\langle\bar{0}\rangle\rangle$ merupakan submodul prima lemah pada $\mathbb{Z}$ −modul $\mathbb{Z}_3$ karena untuk setiap $r \in \mathbb{Z}$ dan $m \in M = \mathbb{Z}_3$ dengan $rm \in N - \{0\}$, berlaku $r \in (N : M) = 3\mathbb{Z}$ atau $m \in N$.

Selanjutnya, perumuman dari submodul prima lemah yaitu submodul hampir prima dijabarkan dalam definisi berikut.

Definisi 2.4.8 (Khashan, 2012)
Misalkan N adalah submodul sejati dari R −modul M. Submodul N dikatakan submodul hampir prima apabila untuk setiap $r \in R$ dan $m \in M$ dengan $rm \in N - (N:M)N$, berlaku $r \in (N : M)$ atau $m \in N$.

Berdasarkan definisi di atas, diketahui bahwa submodul prima dan submodul prima lemah pasti merupakan submodul hampir prima. Sebaliknya, submodul hampir prima belum tentu merupakan submodul prima lemah. Beberapa contohnya diuraikan sebagai berikut.

Contoh 2.4.6
1. $N = \langle\langle\bar{4}\rangle\rangle$ merupakan submodul hampir prima pada $\mathbb{Z}$ −modul $\mathbb{Z}_{36}$, tetapi bukan submodul prima lemah, karena terdapat $2 \cdot \bar{7} = \overline{14} \neq \bar{0} \in N$ tetapi $2 \notin (N:M) = 4\mathbb{Z}$ dan $\bar{7} \notin N$.
2. $N = \langle\langle\bar{0}\rangle\rangle$ merupakan submodul hampir prima pada $\mathbb{Z}$ −modul $\mathbb{Z}_4[i]$ karena untuk setiap $r \in \mathbb{Z}$ dan $m \in M = \mathbb{Z}_4[i]$ dengan $rm \in N - (N:M)N = N - \{0\}$, berlaku $r \in (N : M) = 4\mathbb{Z}$ atau $m \in N$.
3. $N = \langle\langle\bar{1} + \bar{2}i\rangle\rangle$ merupakan submodul hampir prima pada $\mathbb{Z}$ −modul $\mathbb{Z}_5[i]$ karena untuk setiap $r \in \mathbb{Z}$ dan $m \in \mathbb{Z}_5[i]$ dengan $rm \in N - (N:M)N = N - \{0\}$, berlaku $r \in (N : M) = 5\mathbb{Z}$ atau $m \in N$.

2.5 Bilangan Bulat Gauss Modulo

Ring bilangan bulat Gauss merupakan salah satu sistem matematika yang dibentuk dari ring bilangan bulat. Himpunan bilangan bulat Gauss didefinisikan sebagai $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$ dengan $i^2 = -1$. Himpunan bilangan bulat Gauss tersebut tertutup terhadap operasi tambah dan kali. Ring bilangan bulat Gauss modulo $\mathbb{Z}_n[i]$ merupakan salah satu ring yang dikontruksi dari $\mathbb{Z}[i]$. Himpunan ini didefinisikan sebagai $\mathbb{Z}_n[i] = \{\overline{a} + \overline{b}i \,|\overline{a}, \overline{b} \in \mathbb{Z}_n\}$. Himpunan $\mathbb{Z}_n[i]$ dilengkapi dengan operasi tambah dan kali yang didefinisikan sebagai berikut. Untuk setiap $v, w \in \mathbb{Z}_n[i]$, dengan $v = \overline{a} + \overline{b}i, w = \overline{c} + \overline{d}i$, $(\overline{a} + \overline{b}i) + (\overline{c} + \overline{d}i) \coloneqq (\overline{a} + \overline{c}) + (\overline{b} + \overline{d})i$ dan $(\overline{a} + \overline{b}i)(\overline{c} + \overline{d}i) \coloneqq (\overline{ac} - \overline{bd}) + (\overline{ad} + \overline{bc})i$ (Rosiyanti, 2015).

BAB III
METODE PENELITIAN

3.1 Jenis Penelitian

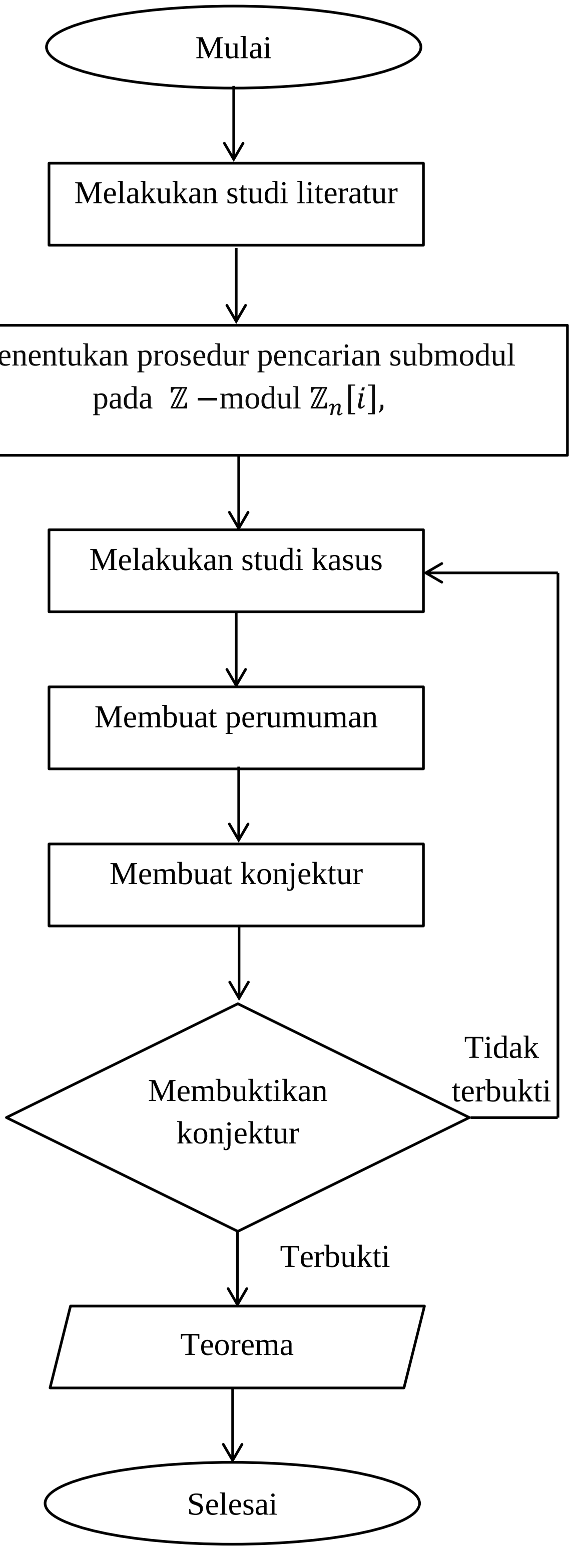
Jenis penelitian dalam tulisan ini adalah penelitian kajian pustaka (studi literatur), yaitu dilakukan dengan mempelajari buku-buku maupun sumber bacaan lain yang berkaitan dengan judul yang diangkat oleh penulis. Penelitian dilakukan dengan membaca, mengkaji dan memahami referensi yang berasal dari buku maupun sumber bacaan yang lain seperti majalah, jurnal, dan makalah-makalah yang memuat topik ataupun materi yang berkaitan dengan grup, ring, modul, dan beberapa teori yang dibutuhkan untuk menunjang tulisan ini.

3.2 Langkah-Langkah Penelitian

Adapun langkah-langkah yan dilakukan dalam penelitian ini adalah:

1. Melakukan studi literatur, yaitu mencari dan mempelajari sumber literatur yang berhubungan dengan modul, submodul prima, submodul prima lemah, submodul hampir prima, bilangan bulat gauss modulo dan beberapa teori lain yang dapat menunjang penelitian ini.
2. Menentukan prosedur pencarian submodul pada $\mathbb{Z}-$modul $\mathbb{Z}_n[i]$, pada langkah ini akan dilakukan pencarian submodul-submodul dari $\mathbb{Z}-$modul $\mathbb{Z}_n[i]$ untuk mendapatkan gambaran secara umum.
3. Melakukan studi kasus, yaitu mencari contoh dan mengelompokkan submodul siklik prima, prima lemah dan hampir prima pada $\mathbb{Z}-$modul $\mathbb{Z}_n[i]$, mempelajari bentuk-bentuknya, sehingga dapat diperumum.
4. Membuat perumuman, yaitu merumuskan submodul siklik prima, prima lemah dan hampir prima pada $\mathbb{Z}-$modul $\mathbb{Z}_n[i]$, secara umum.
5. Membuat konjektur, yaitu menduga karakteristik submodul siklik prima, prima lemah, dan hampir prima pada $\mathbb{Z}-$modul $\mathbb{Z}_n[i]$.
6. Membuktikan konjektur, yakni membuktikan dugaan sehingga didapatkan karakteristik submodul siklik prima, prima lemah, dan hampir prima pada $\mathbb{Z}-$modul $\mathbb{Z}_n[i]$.

Adapun langkah-langkah yang akan dilakukan dalam penelitian ini dapat diamati dalam diagram alir berikut:



Gambar 3.1 Diagram alir langkah-langkah penelitian

BAB IV

HASIL DAN PEMBAHASAN

Pada bagian ini akan dibahas mengenai submodul prima, submodul prima lemah, dan submodul hampir prima pada $\mathbb{Z}$ −modul $\mathbb{Z}_n[i]$.

4.1 Submodul dan Sifatnya

Pada bagian ini akan dibahas beberapa contoh submodul sejati dan sisa submodul tersebut terhadap modulnya pada $\mathbb{Z}$ −modul $\mathbb{Z}_n[i]$. Beberapa contoh submodul sejati dari $\mathbb{Z}$ −modul $\mathbb{Z}_n[i]$ diuraikan pada contoh berikut .

Contoh 4.1.1

1. Misalkan $n = 2$, submodul sejati dari $\mathbb{Z}$ −modul $\mathbb{Z}_n[i]$ yaitu

   $N_1 = \langle\langle\bar{0}\rangle\rangle$

   $N_2 = \langle\langle\bar{1}\rangle\rangle$

   $N_3 = \langle\langle i\rangle\rangle$

   $N_4 = \langle\langle\bar{1} + i\rangle\rangle$

2. Misalkan $n = 3$, beberapa submodul sejati dari $\mathbb{Z}$ −modul $\mathbb{Z}_n[i]$ yaitu

   $N_1 = \langle\langle\bar{0}\rangle\rangle$

   $N_2 = \langle\langle\bar{1}\rangle\rangle$

   $N_3 = \langle\langle i\rangle\rangle$

   $N_4 = \langle\langle\bar{1} + i\rangle\rangle$

   $N_5 = \langle\langle\bar{1} + \bar{2}i\rangle\rangle$

3. Misalkan $n = 6$, beberapa submodul sejati dari $\mathbb{Z}$ −modul $\mathbb{Z}_n[i]$ yaitu

   $N_1 = \langle\langle\bar{0}\rangle\rangle$

   $N_2 = \langle\langle\bar{1}\rangle\rangle$

   $N_3 = \langle\langle i\rangle\rangle$

   $N_4 = \langle\langle\bar{1} + i\rangle\rangle$

   $N_5 = \langle\langle\bar{2} + \bar{3}i\rangle\rangle$

Selanjutnya akan dibahas sisa dari submodul N oleh M $(N: M)$ pada $\mathbb{Z}$ −modul $\mathbb{Z}_n[i]$. Beberapa contohnya diuraikan sebagai berikut.

Contoh 4.1.2

1. Misalkan $n = 2$, dan $N = \langle\langle\bar{0}\rangle\rangle$ submodul dari $M = \mathbb{Z}_n[i]$ modul atas $\mathbb{Z}$. Didapatkan sisa N oleh M sebagai berikut, $(N: M) = \{r \in \mathbb{Z} \mid rM \subseteq N\} = \{r \in \mathbb{Z} \mid r(\bar{c} + \bar{d}i) \in N,\ \forall\, \bar{c}, \bar{d} \in \mathbb{Z}_n\} = 2\mathbb{Z}$.
2. Misalkan $n = 2$, dan $N = \langle\langle\bar{1}\rangle\rangle$ submodul dari $M = \mathbb{Z}_n[i]$ modul atas $\mathbb{Z}$. Didapatkan sisa N oleh M sebagai berikut, $(N: M) = \{r \in \mathbb{Z} \mid rM \subseteq N\} = \{r \in \mathbb{Z} \mid r(\bar{c} + \bar{d}i) \in N,\ \forall\, \bar{c}, \bar{d} \in \mathbb{Z}_n\} = 2\mathbb{Z}$.
3. Misalkan $n = 3$, dan $N = \langle\langle\bar{1} + i\rangle\rangle$ submodul dari $M = \mathbb{Z}_n[i]$ modul atas $\mathbb{Z}$. Didapatkan sisa N oleh M sebagai berikut, $(N: M) = \{r \in \mathbb{Z} \mid rM \subseteq N\} = \{r \in \mathbb{Z} \mid r(\bar{c} + \bar{d}i) \in N,\ \forall\, \bar{c}, \bar{d} \in \mathbb{Z}_n\} = 3\mathbb{Z}$.
4. Misalkan $n = 6$, dan $N = \langle\langle\bar{2} + \bar{3}i\rangle\rangle$ submodul dari $M = \mathbb{Z}_n[i]$ modul atas $\mathbb{Z}$. Didapatkan sisa N oleh M sebagai berikut, $(N: M) = \{r \in \mathbb{Z} \mid rM \subseteq N\} = \{r \in \mathbb{Z} \mid r(\bar{c} + \bar{d}i) \in N,\ \forall\, \bar{c}, \bar{d} \in \mathbb{Z}_n\} = 6\mathbb{Z}$.

Dari beberapa contoh tersebut, dapat dibuat konjektur/dugaan bahwa sisa dari submodul N oleh M pada $\mathbb{Z}$ −modul $\mathbb{Z}_n[i]$ yaitu $(N: M) = n\mathbb{Z}$. Konjektur ini dibuktikan dalam teorema berikut.

Teorema 4.1.1

Misalkan $M = \mathbb{Z}_n[i]$ modul atas ring $\mathbb{Z}$, dengan $n = p_1^{k_1} p_2^{k_2} \ldots p_j^{k_j}$, $p_1, p_2, \ldots, p_j$ bilangan prima berbeda dan $k_1, k_2, \ldots, k_j$ bilangan asli. Jika N submodul siklik dari modul M, maka $(N: M) = n\mathbb{Z}$.

Bukti.

Misalkan $N = \langle\langle\bar{a} + \bar{b}i\rangle\rangle$ dengan $\bar{a}, \bar{b} \in \mathbb{Z}_n$, tanpa mengurangi perumuman, a dan b bisa dipilih sehingga $a, b < n$. Untuk $n = 2$ dan $n = 3$, jelas bahwa $(N: M) = n\mathbb{Z}$, sehingga akan dibuktikan untuk $n > 3$. Untuk setiap $r \in (N: M)$, a dan b dapat dibagi menjadi empat kasus sebagai berikut.

Kasus 1: $a \nmid n$ dan $b \nmid n$

Pilih $\bar{a} \in M$, maka $r\bar{a} = s\bar{a} + s\bar{b}i$ untuk suatu $s \in \mathbb{Z}$. Karena $b \nmid n$ dan $b < n$, maka $\gcd(b, n) = 1$. Diperoleh $s\bar{b} = \bar{0}$, akibatnya $sb = nk_1$ untuk suatu $k_1 \in \mathbb{Z}$, dengan kata lain $n \mid sb$. Karena $\gcd(b, n) = 1$, maka $n \mid s$, dengan kata lain $s = nk_2$ untuk suatu $k_2 \in \mathbb{Z}$. Akibatnya $s\bar{a} = \bar{0} = r\bar{a}$. Karena $a \nmid n$ dan $a < n$ maka $\gcd(a, n) = 1$. Karena $r\bar{a} = \bar{0}$, maka $ra = nk_3$ untuk suatu $k_3 \in \mathbb{Z}$, dengan kata lain $n \mid ra$. Karena $\gcd(a, n) = 1$, maka $n \mid r$, dengan kata lain $r = nk_4$ untuk suatu $k_4 \in \mathbb{Z}$.

Kasus 2: $a \mid n$ dan $b \nmid n$

Pilih $\bar{b} \in M$, maka $r\bar{b} = s\bar{a} + s\bar{b}i$ untuk suatu $s \in \mathbb{Z}$. Karena $b \nmid n$ dan $b < n$, maka $\gcd(b, n) = 1$. Diperoleh $s\bar{b} = \bar{0}$, akibatnya $sb = nk_1$ untuk suatu $k_1 \in \mathbb{Z}$, dengan kata lain $n \mid sb$. Karena $\gcd(b, n) = 1$, maka $n \mid s$, dengan kata lain $s = nk_2$ untuk suatu $k_2 \in \mathbb{Z}$. Akibatnya $s\bar{a} = \bar{0} = r\bar{b}$. Karena $r\bar{b} = \bar{0}$, maka $rb = nk_3$ untuk suatu $k_3 \in \mathbb{Z}$, dengan kata lain $n \mid rb$. Karena $\gcd(b, n) = 1$, maka $n \mid r$, dengan kata lain $r = nk_4$ untuk suatu $k_4 \in \mathbb{Z}$.

Kasus 3: $a \nmid n$ dan $b \mid n$

Pilih $\bar{a}i \in M$, maka $r\bar{a}i = s\bar{a} + s\bar{b}i$ untuk suatu $s \in \mathbb{Z}$. Karena $a \nmid n$ dan $a < n$, maka $\gcd(a, n) = 1$. Diperoleh $s\bar{a} = \bar{0}$ akibatnya $sa = nk_1$ untuk suatu $k_1 \in \mathbb{Z}$, dengan kata lain $n \mid sa$. Karena $\gcd(a, n) = 1$, maka $n \mid s$, dengan kata lain $s = nk_2$ untuk suatu $k_2 \in \mathbb{Z}$. Akibatnya $s\bar{b}i = \bar{0} = r\bar{a}i$. Karena $r\bar{a} = \bar{0}$, maka $ra = nk_3$ untuk suatu $k_3 \in \mathbb{Z}$, dengan kata lain $n \mid ra$. Karena $\gcd(a, n) = 1$, maka $n \mid r$, dengan kata lain $r = nk_4$ untuk suatu $k_4 \in \mathbb{Z}$.

Kasus 4: $a \mid n$ dan $b \mid n$

- $\bar{a} = \bar{b}$

  Pilih $\overline{n-1} \in M$, maka $r\overline{(n-1)} = s\bar{a} + s\bar{b}i$ untuk suatu $s \in \mathbb{Z}$. Diperoleh $s\bar{b} = s\bar{a} = \bar{0}$, sehingga $r\overline{(n-1)} = \bar{0}$. Akibatnya $r(n-1) = nk$ untuk suatu $k \in \mathbb{Z}$, dengan kata lain $n \mid r(n-1)$. Karena $\gcd(n-1, n) = 1$ untuk $n > 3$, maka $n \mid r$, dengan kata lain $r = nl$ untuk suatu $l \in \mathbb{Z}$.

- $\bar{a} \neq \bar{b}$

  Pilih $\overline{n-1} + \overline{n-1}i \in M$, maka $r\overline{(n-1)} + r\overline{(n-1)}i = s\bar{a} + s\bar{b}i$ untuk suatu $s \in \mathbb{Z}$. Akibatnya $s\bar{a} = s\bar{b} = r\overline{(n-1)}$. Karena $a \neq b$ dan $a, b < n$, maka $s\bar{a} = s\bar{b} = \bar{0}$, akibatnya $r\overline{(n-1)} = \bar{0}$. Sehingga $r(n-1) = nk$ untuk suatu $k \in \mathbb{Z}$, dengan kata lain $n \mid r(n-1)$. Karena $\gcd(n-1, n) = 1$ untuk $n > 3$, maka $n \mid r$, dengan kata lain $r = nl$ untuk suatu $l \in \mathbb{Z}$.

Sehingga diperoleh $r \in n\mathbb{Z}$. Sebaliknya, untuk setiap $r \in n\mathbb{Z}$, jelas bahwa $r \in (N: M)$. Dengan demikian, $(N: M) = n\mathbb{Z}$.

■

Selanjutnya akan dibahas sifat-sifat khusus pada $\mathbb{Z} -$ modul $\mathbb{Z}_n[i]$. Sifat yang pertama ialah ketika terdapat dua submodul sejati yang tidak sama, yang diuraikan pada teorema berikut.

Teorema 4.1.2

Misalkan $M = \mathbb{Z}_n[i]$ modul atas ring $\mathbb{Z}$, dengan $n = {p_1}^{k_1}{p_2}^{k_2} \dots {p_j}^{k_j}$, $p_1, p_2, \dots, p_j$ bilangan prima berbeda dan $k_1, k_2, \dots, k_j$ bilangan asli. Misalkan a,$b \in M$, maka $a \neq kb$ atau $b \neq la$ untuk setiap $k, l \in \mathbb{Z}$, jika dan hanya jika $\langle\langle a \rangle\rangle \neq \langle\langle b \rangle\rangle$.

Bukti.

($\Longrightarrow$) Diberikan $a \neq kb$ atau $b \neq la$ untuk setiap $k, l \in \mathbb{Z}$. Andaikan $\langle\langle a \rangle\rangle = \langle\langle b \rangle\rangle$. Maka diperoleh $a \in \langle\langle b \rangle\rangle$ dan $b \in \langle\langle a \rangle\rangle$, sedemikian sehingga $a = \alpha b$ dan $b = \beta a$ untuk suatu $\alpha, \beta \in \mathbb{Z}$. Kontradiksi dengan $a \neq kb$ atau $b \neq la$ untuk setiap $k, l \in \mathbb{Z}$. Jadi haruslah $\langle\langle a \rangle\rangle \neq \langle\langle b \rangle\rangle$.

($\Longleftarrow$) Diberikan $\langle\langle a \rangle\rangle \neq \langle\langle b \rangle\rangle$. Andaikan $a = \alpha b$ dan $b = la$ untuk suatu $\alpha \in \mathbb{Z}$. Sehingga diperoleh $a \in \langle\langle b \rangle\rangle$ dan $b \in \langle\langle a \rangle\rangle$. Akibatnya $\langle\langle a \rangle\rangle = \langle\langle b \rangle\rangle$. Kontradiksi dengan $\langle\langle a \rangle\rangle \neq \langle\langle b \rangle\rangle$. Jadi haruslah $a \neq kb$ atau $b \neq la$ untuk setiap $k, l \in \mathbb{Z}$.

■

Pada suatu ruang vektor V atas lapangan F dikenal istilah hasil tambah langsung, hal yang sama juga berlaku pada $\mathbb{Z}-$ modul $\mathbb{Z}_n[i]$, khususnya ketika n bilangan prima. Jika terdapat dua submodul siklik yang berbeda pada $\mathbb{Z}-$ modul $\mathbb{Z}_n[i]$, maka modul tersebut dapat dinyatakan dengan hasil tambah langsung dua submodul tersebut. Hal ini dibuktikan pada Teorema 4.1.3 dan Teorema 4.1.4.

Teorema 4.1.3

Misalkan $M = \mathbb{Z}_n[i]$ modul atas ring $\mathbb{Z}$, dengan n bilangan prima. Misalkan a,b $\in M$ dengan $a, b \neq \bar{0}$, maka $\langle\langle a\rangle\rangle \neq \langle\langle b\rangle\rangle$ jika dan hanya jika $\langle\langle a\rangle\rangle \cap \langle\langle b\rangle\rangle = \{\bar{0}\}$.

Bukti.

($\Longrightarrow$) Diberikan $\langle\langle a\rangle\rangle \neq \langle\langle b\rangle\rangle$. Andaikan $\langle\langle a\rangle\rangle \cap \langle\langle b\rangle\rangle \neq \{\bar{0}\}$. Maka terdapat $c \neq \bar{0}$, $c \in \langle\langle a\rangle\rangle \cap \langle\langle b\rangle\rangle$ sehingga $c = \gamma_1 a = \gamma_2 b$ untuk suatu $\gamma_1, \gamma_2 \in \mathbb{Z}$, tanpa mengurangi perumuman dapat dipilih $\gamma_1, \gamma_2 < n$. Diperoleh $\gamma_1 \neq 0$, karena $\gamma_1 < n$ dan n bilangan prima, maka $(\gamma_1, n) = 1$. Akibatnya terdapat $p, q \in \mathbb{Z}$ sehingga $1 = p\gamma_1 + qn$, dengan kata lain $\bar{p}\gamma_1 = \bar{1}$. Misalkan $a = \overline{a_1} + \overline{a_2}i$ dan $b = \overline{b_1} + \overline{b_2}i$, maka $\gamma_1(\overline{a_1} + \overline{a_2}i) = \gamma_2(\overline{b_1} + \overline{b_2}i)$. Sehingga $\bar{p}\gamma_1(\overline{a_1} + \overline{a_2}i) = \bar{p}\gamma_2(\overline{b_1} + \overline{b_2}i)$, karena $\bar{p}\gamma_1 = \bar{1}$ maka $(\overline{a_1} + \overline{a_2}i) = \bar{p}\gamma_2(\overline{b_1} + \overline{b_2}i)$. Sehingga diperoleh $a = p\gamma_2 b$, dengan kata lain $a \in \langle\langle b\rangle\rangle$. Akibatnya, $\langle\langle a\rangle\rangle \subseteq \langle\langle b\rangle\rangle$. Dengan cara yang sama, diperoleh $b \in \langle\langle a\rangle\rangle$. Sehingga $\langle\langle b\rangle\rangle \subseteq \langle\langle a\rangle\rangle$. Dengan demikian, $\langle\langle a\rangle\rangle = \langle\langle b\rangle\rangle$. Kontradiksi dengan $\langle\langle a\rangle\rangle \neq \langle\langle b\rangle\rangle$. Jadi haruslah $\langle\langle a\rangle\rangle \cap \langle\langle b\rangle\rangle = \{\bar{0}\}$.

($\Longleftarrow$) Jika $\langle\langle a\rangle\rangle \cap \langle\langle b\rangle\rangle = \{\bar{0}\}$, maka jelas bahwa $\langle\langle a\rangle\rangle \neq \langle\langle b\rangle\rangle$.

■

Teorema 4.1.4

Misalkan $M = \mathbb{Z}_n[i]$ modul atas ring $\mathbb{Z}$, dengan n bilangan prima. Misalkan a,b $\in M$, $a, b \neq \bar{0}$ dengan $\langle\langle a\rangle\rangle \neq \langle\langle b\rangle\rangle$, maka $\langle\langle a\rangle\rangle \oplus \langle\langle b\rangle\rangle = M$.

Bukti.

Jelas bahwa $\langle\langle a\rangle\rangle + \langle\langle b\rangle\rangle \subseteq M$. Diketahui bahwa kardinalitas M yaitu $|M| = n^2$. Berdasarkan definisi dan karena n bilangan prima, diperoleh $\langle\langle a\rangle\rangle =$

$\{ra \mid r \in \mathbb{Z}\} = \{\bar{0}, x_1, \dots, x_{n-1}\}$ dan $\langle\langle b\rangle\rangle = \{rb \mid r \in \mathbb{Z}\} = \{\bar{0}, y_1, \dots, y_{n-1}\}$, sehingga $|\langle\langle a\rangle\rangle| = |\langle\langle b\rangle\rangle| = n$. Berdasarkan Teorema 4.1.3, diperoleh $\langle\langle a\rangle\rangle \cap \langle\langle b\rangle\rangle = \{\bar{0}\}$. Misalkan $A = \{x_i + y_j | i, j = 1, \dots, n-1\}$, karena $\langle\langle a\rangle\rangle \cap \langle\langle b\rangle\rangle = \{\bar{0}\}$ maka $x_i + y_j \notin \langle\langle a\rangle\rangle \cup \langle\langle b\rangle\rangle$ dan $|A| = (n-1)^2 = n^2 - 2n + 1$. Sehingga $|\langle\langle a\rangle\rangle + \langle\langle b\rangle\rangle| = |A \cup \langle\langle a\rangle\rangle \cup \langle\langle b\rangle\rangle| = n^2 - 2n + 1 + 2n - 1 = n^2 = |M|$. Dengan demikian $M \subseteq \langle\langle a\rangle\rangle + \langle\langle b\rangle\rangle$. Jadi, $\langle\langle a\rangle\rangle + \langle\langle b\rangle\rangle = M$. Selanjutnya berdasarkan Teorema 4.1.3, diperoleh $\langle\langle a\rangle\rangle \cap \langle\langle b\rangle\rangle = \{\bar{0}\}$. Dengan demikian, $\langle\langle a\rangle\rangle \oplus \langle\langle b\rangle\rangle = M$.

■

Berdasarkan Teorema 4.1.3 dan Teorema 4.1.4, diketahui bahwa modul $M = \mathbb{Z}_n[i]$ dengan n bilangan prima, dapat dituliskan sebagai hasil tambah langsung dua submodul siklik tak nol yang tidak sama. Hal ini memberikan dugaan bahwa submodul sejati dari M hanya terdiri dari submodul siklik, yang diuraikan dalam proposisi berikut.

Teorema 4.1.5

Misalkan $M = \mathbb{Z}_n[i]$ modul atas ring $\mathbb{Z}$, dengan n bilangan prima, maka

1. *Setiap submodul sejati dari M merupakan submodul siklik*
2. *Untuk setiap N submodul sejati dari M, berlaku $(N\colon M) = n\mathbb{Z}$.*

Bukti.

1. Misalkan $N = \langle\langle a, b\rangle\rangle$ submodul sejati dari M yang dibangun oleh dua unsur $a, b \in M$. Maka berdasarkan Teorema 4.1.3, diperoleh $\langle\langle a\rangle\rangle \cap \langle\langle b\rangle\rangle = \{\bar{0}\}$. Selanjutnya berdasarkan Teorema 4.1.4, diperoleh $\langle\langle a\rangle\rangle + \langle\langle b\rangle\rangle = M$. Sehingga $N = \langle\langle a, b\rangle\rangle$ bukan submodul sejati dari M. Dengan demikian, submodul N haruslah siklik.
2. Berdasarkan bukti pada poin 1 diperoleh N merupakan submodul siklik. Dengan demikian, berdasarkan Teorema 4.1.1, diperoleh $(N\colon M) = n\mathbb{Z}$.

■

4.2 Submodul Prima

Pada bagian sebelumnya telah dijabarkan definisi submodul prima dari suatu R −modul M. Diketahui bahwa tidak semua submodul sejati merupakan submodul prima. Beberapa contoh submodul siklik yang merupakan submodul prima dan bukan prima pada $\mathbb{Z}$ − modul $\mathbb{Z}_n[i]$ diuraikan pada contoh berikut.

Contoh 4.2.1

1. Misalkan $M = \mathbb{Z}_2[i]$ modul atas ring $\mathbb{Z}$. Submodul siklik dari M yaitu

   $N_1 = \langle\langle\bar{0}\rangle\rangle$

   $N_2 = \langle\langle\bar{1}\rangle\rangle$

   $N_3 = \langle\langle\bar{\imath}\rangle\rangle$

   $N_4 = \langle\langle\bar{1} + i\rangle\rangle$

   Merupakan submodul prima karena untuk setiap $r \in \mathbb{Z}$ dan $m \in \mathbb{Z}_2[i]$ dengan $rm \in N_i$, berlaku $r \in (N_i: M)$ atau $m \in N_i$.

2. Misalkan $M = \mathbb{Z}_3[i]$ modul atas ring $\mathbb{Z}$. Submodul siklik dari M yaitu

   $N_1 = \langle\langle\bar{0}\rangle\rangle$

   $N_2 = \langle\langle\bar{1} + i\rangle\rangle$

   $N_3 = \langle\langle\bar{1}\ + \bar{2}\mathrm{i}\rangle\rangle$

   …

   dan seterusnya

   Merupakan submodul prima karena untuk setiap $r \in \mathbb{Z}$ dan $m \in \mathbb{Z}_3[i]$ dengan $rm \in N_i$, berlaku $r \in (N_i: M)$ atau $m \in N_i$.

3. Misalkan $M = \mathbb{Z}_4[i]$ modul atas ring $\mathbb{Z}$, submodul $N = \langle\langle\bar{0}\rangle\rangle$ bukan submodul prima, karena terdapat $r = 2 \notin (N: M)$ dan $m = \bar{2} \notin N$ sehingga $rm = \bar{0} \in N$.

Dari beberapa contoh tersebut, dapat dibuat konjektur/dugaan bahwa ketika n bilangan prima, setiap submodul sejati pada $\mathbb{Z}$ −modul $\mathbb{Z}_n[i]$ merupakan submodul prima. Konjektur ini dibuktikan dalam teorema berikut.

Teorema 4.2.1

Misalkan $M = \mathbb{Z}_n[i]$ modul atas ring $\mathbb{Z}$, dengan n bilangan prima, maka semua submodul sejati dari M adalah submodul prima.

Bukti.

Berdasarkan Teorema 4.1.5, submodul sejati dari M hanya submodul siklik. Misalkan $N = \langle\langle \overline{n_1} + \overline{n_2} i \rangle\rangle$ untuk $\overline{n_1}, \overline{n_2} \in \mathbb{Z}_n$ submodul sejati dari M, tanpa mengurangi perumuman, n_1 dan n_2 bisa dipilih sehingga $n_1, n_2 < n$. Berdasarkan Teorema 4.1.1, diketahui $(N: M) = n\mathbb{Z}$. Karena n bilangan prima, maka $n_1, n_2 = 0$ atau $n_1, n_2 \neq 0$ yang ekuivalen dengan $\gcd(n, n_1) = \gcd(n, n_2) = 1$ Ambil $r \in \mathbb{Z}$ dan $m = \overline{m_1} + \overline{m_2} i \in M$ sehingga $rm \in N$.

Kasus 1: $n_1 = 0$ dan $n_2 = 0$

Maka berlaku $\overline{n_1} = \bar{0}$ dan $\overline{n_2} = \bar{0}$. Karena $rm \in N$, maka diperoleh $r\overline{m_1} = \bar{0}$ dan $r\overline{m_2} = \bar{0}$, akibatnya $rm_1 = k_1 n$ dan $rm_2 = k_2 n$ untuk suatu $k_1, k_2 \in \mathbb{Z}$. Sehingga $n \mid rm_1$ dan $n \mid rm_2$. Karena n bilangan prima, maka diperoleh $n \mid r$ atau $n \mid m_1$ dan $n \mid m_2$. Sehingga berlaku $r = k_3 n$ untuk suatu $k_3 \in \mathbb{Z}$ atau $\overline{m_1} = \overline{m_2} = \bar{0}$. Dengan demikian, berlaku $r \in (N: M)$ atau $m = \overline{m_1} + \overline{m_2} i \in N$.

Kasus 2: $n_1 \neq 0$ dan $n_2 \neq 0$

Maka berlaku $r\overline{m_1} + r\overline{m_2} i = s\overline{n_1} + s\overline{n_2} i$ untuk suatu $s \in \mathbb{Z}$. Jika $r\overline{m_1} = \bar{0}$ maka $r \in (N: M)$ atau $\overline{m_1} = \bar{0}$. Jika $r\overline{m_2} = \bar{0}$, maka $r \in (N: M)$ atau $\overline{m_2} = \bar{0}$. Sehingga, jika $r\overline{m_1} = \bar{0}$ atau $r\overline{m_2} = \bar{0}$, berlaku $r \in (N: M)$. Selanjutnya misalkan $r\overline{m_1} \neq \bar{0}$ dan $r\overline{m_2} \neq \bar{0}$, maka $\bar{r} \neq \bar{0}$. Karena n bilangan prima, maka terdapat $\bar{w}$ sedemikian hingga $\bar{r}\bar{w} = \bar{1}$. Karena $r\overline{m_1} = s\overline{n_1}$ dan $r\overline{m_2} = s\overline{n_2}$, maka $\overline{m_1} = sw\overline{n_1}$ dan $\overline{m_2} = sw\overline{n_2}$. Dengan demikian diperoleh $m = sw\overline{n_1} + sw\overline{n_2} i \in N$.

Kasus 3: $n_1 = 0$ dan $n_2 \neq 0$

Maka berlaku $r\overline{m_1} + r\overline{m_2} i = s\overline{n_2} i$, diperoleh $r\overline{m_1} = \bar{0}$ dan $r\overline{m_2} = s\overline{n_2} i$. Jika $r\overline{m_2} = \bar{0}$, maka $r \in (N: M)$ atau $\overline{m_2} = \bar{0}$. Selanjutnya misalkan $r\overline{m_2} \neq \bar{0}$, maka $\bar{r} \neq \bar{0}$. Karena n bilangan prima, maka terdapat $\bar{w}$ sedemikian hingga $\bar{r}\bar{w} = \bar{1}$. Karena $r\overline{m_2} = s\overline{n_2}$, maka $\overline{m_2} = sw\overline{n_2}$. Akibatnya, diperoleh $\overline{m_1} = \bar{0}$, sehingga $m = sw\overline{n_2} i \in N$.

Kasus 4: $n_1 \neq 0$ dan $n_2 = 0$

Dengan cara yang serupa seperti Kasus 3, diperoleh hasil yang sama yaitu jika $r\overline{m_1} = \overline{0}$, maka $r \in (N: M)$ atau $\overline{m_1} = \overline{0}$. Jika $r\overline{m_1} \neq \overline{0}$ maka $m = sw\overline{n_1}i \in N$.

Jadi, N submodul prima dari M.

■

4.3 Submodul Prima Lemah

Pada bagian sebelumnya telah diuraikan definisi dari submodul prima lemah. Berdasarkan definisi, diketahui bahwa setiap submodul prima pasti merupakan submodul prima lemah. Selanjutnya submodul nol dari suatu $R-$ modul M juga merupakan submodul prima lemah. Pada modul torsi yang dibangun secara hingga atas daerah ideal utama, submodul prima lemah hanya terdiri dari submodul prima atau submodul nol. Sifat tersebut diuraikan dalam teorema berikut ini.

Teorema 4.3.1 (Wardhana, Astuti dan Muchtadi-Alamsyah, 2016)
Misalkan M modul torsi yang dibangun secara hingga atas daerah ideal utama, submodul sejati N merupakan submodul prima lemah jika dan hanya jika N submodul prima atau submodul nol.

Berdasarkan definisi, diketahui bahwa $\mathbb{Z}-$modul $\mathbb{Z}_n[i]$ merupakan modul torsi yang dibangun secara hingga atas daerah ideal utama. Akibatnya, berdasarkan Teorema 4.3.1 submodul prima lemah pada $\mathbb{Z}-$modul $\mathbb{Z}_n[i]$ hanya terdiri dari submodul prima atau submodul nol, yang diuraikan dalam akibat berikut.

Akibat 4.3.1
Misalkan $M = \mathbb{Z}_n[i]$ modul atas ring $\mathbb{Z}$, maka submodul sejati N merupakan submodul prima lemah jika dan hanya jika N submodul prima atau submodul nol.

4.4 Submodul Hampir Prima

Pada bagian sebelumnya, definisi submodul hampir prima telah diuraikan. Selanjutnya, beberapa contoh submodul siklik hampir prima pada $\mathbb{Z}$ −modul $\mathbb{Z}_n[i]$ diberikan pada contoh berikut.

Contoh 4.4.1

1. Misalkan $M = \mathbb{Z}_2[i]$ modul atas ring $\mathbb{Z}$, submodul siklik dari M

   $N_1 = \langle\langle\bar{0}\rangle\rangle$

   $N_2 = \langle\langle\bar{1}\rangle\rangle$

   $N_3 = \langle\langle i\rangle\rangle$

   $N_4 = \langle\langle\bar{1} + i\rangle\rangle$

   merupakan submodul hampir prima karena untuk setiap $r \in \mathbb{Z}$ dan $m \in \mathbb{Z}_2[i]$ dengan $rm \in N_i - (N_i: M)N_i$, berlaku $r \in (N_i: M)$ atau $m \in N_i$.

2. Misalkan $M = \mathbb{Z}_3[i]$ modul atas ring $\mathbb{Z}$, submodul siklik dari M

   $N_1 = \langle\langle\bar{0}\rangle\rangle$

   $N_2 = \langle\langle\bar{1} + i\rangle\rangle$

   $N_3 = \langle\langle\bar{1} + \bar{2}i\rangle\rangle$

   …

   dan seterusnya

   merupakan submodul hampir prima karena untuk setiap $r \in \mathbb{Z}$ dan $m \in \mathbb{Z}_3[i]$ dengan $rm \in N_i - (N_i: M)N_i$, berlaku $r \in (N_i: M)$ atau $m \in N_i$.

3. Misalkan $M = \mathbb{Z}_4[i]$ modul atas ring $\mathbb{Z}$, submodul $N = \langle\langle\bar{0}\rangle\rangle$ merupakan submodul hampir prima karena untuk setiap $r \in \mathbb{Z}$ dan $m \in \mathbb{Z}_4[i]$ dengan $rm \in N - (N: M)N$, berlaku $r \in (N: M)$ atau $m \in N$.

Dari beberapa contoh tersebut, diketahui bahwa submodul prima lemah pada $\mathbb{Z}$ −modul $\mathbb{Z}_n[i]$ juga merupakan submodul hampir prima. Hal ini dikarenakan submodul siklik yang prima lemah dan submodul siklik yang hampir prima pada $\mathbb{Z}$ −modul $\mathbb{Z}_n[i]$ ekuivalen, yang dibuktikan dalam teorema berikut.

Teorema 4.4.1

Misalkan $M = \mathbb{Z}_n[i]$ modul atas ring $\mathbb{Z}$, dengan $n = p_1^{k_1} p_2^{k_2} \dots p_j^{k_j}$, $p_1, p_2, \dots, p_j$ bilangan prima berbeda dan $k_1, k_2, \dots, k_j$ bilangan asli. Himpunan N merupakan submodul siklik dari M. Submodul N merupakan submodul prima lemah jika dan hanya jika N submodul hampir prima.

Bukti.

($\Longrightarrow$) Misalkan N submodul prima lemah. Maka untuk setiap $r \in \mathbb{Z}$ dan $m \in M$ dengan $rm \in N - \{\bar{0}\}$, berlaku $r \in (N : M)$ atau $m \in N$. Berdasarkan Teorema 4.1.1, diperoleh $(N : M) = n\mathbb{Z}$. Perhatikan bahwa $(N: M)N = n\mathbb{Z}N = \bar{0}$. Sehingga bedasarkan definisi, N submodul hampir prima.
($\Longleftarrow$) Sebaliknya, jika N submodul hampir prima maka untuk setiap $r \in \mathbb{Z}$ dan $m \in M$ dengan $rm \in N - (N: M)N$, berlaku $r \in (N : M)N$ atau $m \in N$. Diketahui bahwa $(N: M)N = n\mathbb{Z}N = \bar{0} = (N: M)$. Dengan demikian, berdasarkan definisi, N submodul prima lemah.

■

Berdasarkan Akibat 4.3.1, diketahui bahwa submodul prima lemah dari $\mathbb{Z}$ −modul $\mathbb{Z}_n[i]$ hanya terdiri dari submodul prima dan submodul nol. Selanjutnya dari Teorema 4.4.1, diketahui bahwa submodul siklik yang prima lemah ekuivalen dengan submodul siklik yang hampir prima. Akibatnya, pada $\mathbb{Z}$ −modul $\mathbb{Z}_n[i]$ dengan n tak prima, submodul siklik yang hampir prima yang bukan submodul prima hanya submodul nol. Hal ini diuraikan dalam Akibat 4.4.1, sebagai berikut.

Akibat 4.4.1

Misalkan $M = \mathbb{Z}_n[i]$ modul atas ring $\mathbb{Z}$, dengan $n = p_1^{k_1} p_2^{k_2} \dots p_j^{k_j}$, $p_1, p_2, \dots, p_j$ bilangan prima berbeda dan $k_1, k_2, \dots, k_j$ bilangan asli. Maka satu-satunya submodul siklik yang hampir prima yang bukan submodul prima ialah submodul nol.

BAB V
PENUTUP

5.1 Kesimpulan

Penelitian ini menghasilkan karakteristik submodul siklik prima, submodul prima lemah dan submodul hampir prima pada $\mathbb{Z}-$modul $\mathbb{Z}_n[i]$ yang diuraikan sebagai berikut:

1. Submodul siklik N merupakan submodul prima pada $\mathbb{Z}-$modul $\mathbb{Z}_n[i]$ jika n bilangan prima.
2. Submodul prima lemah pada $\mathbb{Z}-$modul $\mathbb{Z}_n[i]$ terdiri dari submodul nol dan submodul primanya.
3. Submodul siklik hampir prima pada $\mathbb{Z}-$modul $\mathbb{Z}_n[i]$ ekuivalen dengan submodul prima lemah.

5.2 Saran

Setelah membahas submodul siklik prima, prima lemah dan hampir prima pada $\mathbb{Z}-$modul $\mathbb{Z}_n[i]$, penulis ingin menyampaikan saran bagi para pembaca ataupun peneliti selanjutnya agar dapat melakukan penelitian pada submodul tak siklik dari $\mathbb{Z}-$modul $\mathbb{Z}_n[i]$ dan sistem matematika lainnya yang lebih kompleks.

DAFTAR PUSTAKA

Dauns, J., 1978, ***Prime Submodules***, J. Rine Angew Math., **1978:298**, pp. 156-181.

Dummit, S. D., Foote, M. R., 2004, ***Abstract Algebra**, **3rd ed***., John Wiley & Sons, Inc., USA.

Fraleigh, J. B., 2014, ***A First Course in Abstract Algebra 7th ed***, Pearson Education Limited, USA.

Hadi, I.M.A., 2009, ***On Weakly Prime Submodules***., Ibn Al-Haitham Journal for Pure and Applied Science, **22(3)**, pp. 183-190.

Juliana, R., Wardhana, I. G. A. W., Irwansyah, 2020, ***Some Characteristics of Prime Submodules of Gaussian Integer Modulo over Integer***, Proceedings International Conference on Science and Technology (ICST), **Vol 1**, pp. 209-213.

Khashan, H.A., 2012, ***On Almost Prime Submodules***, Acta Mathematica Scientia, **32(2)**, pp. 645-651.

Maulana, F., Wardhana, I. G. A. W., Switrayni, N. W., Aini, Q., 2018, ***Bilangan Prima dan Bilangan Tak Tereduksi pada Bilangan Bulat Gauss***, Dipresentasikan pada Seminar Nasional APPPI II, NTB, 27 Oktober 2019

Roman, Steven. 2008. ***Advanced Linier Algebra***, ***3rd ed***, Springer, New York.

Rosiyanti, H., 2015, ***Wakil Unsur Pembangun Ideal dari Bilangan Bulat Gauss Modulo*** $\mathbb{Z}_m[i]$**,** Jurnal Pendidikan Matematika & Sains, **1(1)**, pp.97-100.

Switrayni, N.W., 2015, ***Pengantar Teori Modul***, Universitas Mataram, Mataram.

Wardhana, I.G.A.W., Astuti, P., 2014, ***Karakteristik Submodul Prima Lemah dan Hampir Prima dari*** $\mathbb{Z}$ ***−modul*** $\mathbb{Z}_n$**,** Jurnal Matematika & Sains, **19(1)**, pp.16-20.

Wardhana, I.G.A.W., Astuti, P., Muchtadi-Alamsyah, I., 2016, ***On Almost Prime Submodule of a Finitely Generated Module Over Principal Ideal Domain,*** JP Journal of Algebra, Number Theory and Applications, pp.121-128.