KETERBAGIAN DAN
SIFAT-SIFAT DAERAH FAKTORISASI TUNGGAL $\mathbb{Z}_p$

SKRIPSI

Oleh:

MOH. ZUHDI KURNIAWAN
NIM. 06510046

JURUSAN MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2012

KETERBAGIAN DAN
SIFAT-SIFAT DAERAH FAKTORISASI TUNGGAL $\mathbb{Z}_p$

SKRIPSI

Diajukan Kepada:
Fakultas Sains dan Teknologi
Universitas Islam Negeri Maulana Malik Ibrahim Malang
Untuk Memenuhi Salah Satu Persyaratan dalam
Memperoleh Gelar Sarjana Sains (S.Si)

Oleh:
MOH. ZUHDI KURNIAWAN
NIM. 06510046

JURUSAN MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2012

KETERBAGIAN DAN
SIFAT-SIFAT DAERAH FAKTORISASI TUNGGAL $\mathbb{Z}_p$

SKRIPSI

Oleh:
MOH. ZUHDI KURNIAWAN
NIM. 06510046

Telah Diperiksa dan Disetujui untuk Diuji

Tanggal: 15 Desember 2012

Dosen Pembimbing I,	**Dosen Pembimbing II,**
Drs. H. Turmudi, M.Si	**Fachrur Rozi, M.Si**
NIP. 19571005 198203 1 006	**NIP. 19800527 200801 1 012**

Mengetahui,
Ketua Jurusan Matematika

Abdussakir, M.Pd
NIP. 19751006 200312 1 001

KETERBAGIAN DAN
SIFAT-SIFAT DAERAH FAKTORISASI TUNGGAL $\mathbb{Z}_p$

SKRIPSI

Oleh:
MOH. ZUHDI KURNIAWAN
NIM. 06510046

Telah Dipertahankan di Depan Dewan Penguji Skripsi
dan Dinyatakan Diterima sebagai Salah Satu Persyaratan
untuk Memperoleh Gelar Sarjana Sains (S.Si)

Tanggal: 29 Desember 2012

Susunan Dewan Penguji		Tanda Tangan
1. Penguji Utama	: Abdussakir, M.Pd NIP. 19751006 200312 1 001	________
2. Ketua Penguji	: Hairur Rahman, M.Si NIP. 19800429 200604 1 003	________
3. Sekretaris Penguji	: Drs. H. Turmudi, M.Si NIP. 19571005 198203 1 006	________
4. Anggota	: Fachrur Rozi, M.Si NIP. 19800527 200801 1 012	________

Mengetahui dan Mengesahkan,
Ketua Jurusan Matematika,

Abdussakir, M.Pd
NIP. 19751006 200312 1 001

PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan di bawah ini:

Nama	: Moh. Zuhdi Kurniawan
NIM	: 06510046
Jurusan	: Matematika
Fakultas	: Sains dan Teknologi
Penulis Skripsi berjudul	: Keterbagian dan Sifat-sifat Daerah Faktorisasi Tunggal $\mathbb{Z}_p$

menyatakan dengan sebenarnya bahwa skripsi yang saya tulis ini benar-benar merupakan hasil karya saya sendiri, bukan merupakan pengambilalihan data, tulisan, atau pikiran orang lain yang saya akui sebagai hasil tulisan atau pikiran saya sendiri, kecuali dengan mencantumkan sumber cuplikan pada daftar pustaka. Apabila dikemudian hari terbukti atau dapat dibuktikan skripsi ini hasil jiplakan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Malang, 29 Desember 2012
Yang membuat pernyataan,

Moh. Zuhdi Kurniawan
NIM. 06510046

MOTTO

فَإِنَّ مَعَ ٱلۡعُسۡرِ يُسۡرًا ٥ إِنَّ مَعَ ٱلۡعُسۡرِ يُسۡرٗا ٦

"*Karena sesungguhnya sesudah kesulitan itu ada kemudahan.*

Sesungguhnya sesudah kesulitan itu ada kemudahan."

(QS. Al-Insyirah:6)

PERSEMBAHAN

Alhamdulillah, dengan segenap rasa syukur karya tulis ini dipersembahkan kepada ayah, ibu, dan keluarga tercinta.

KATA PENGANTAR

Alhamdulillah, puji dan syukur hanya milik Allah SWT Yang Maha Pengasih dan Maha Penyayang. Shalawat dan salam semoga senantiasa dilimpahkan kepada Nabi Muhammad SAW. Dengan hidayah dan pertolongan Allah, skripsi yang berjudul **"Keterbagian dan Sifat-sifat Daerah Faktorisasi Tunggal $\mathbb{Z}_p$"** dapat selesai dengan baik. Skripsi ini disusun sebagai salah satu syarat untuk meraih gelar sarjana pada Jurusan Matematika Fakultas Sain dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang.

Penulisan skripsi ini dapat terwujud karena bantuan, bimbingan, dan motivasi dari berbagai pihak. Oleh karena itu, ungkapan terimakasih disampaikan kepada:

1. Prof. Dr. H. Imam Suprayogo, selaku rektor Universitas Islam Negeri Maulana Malik Ibrahim Malang.
2. Prof. Drs. Sutiman Bambang Sumitro, S.U, D.Sc, selaku dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang.
3. Abdussakir, M.Pd, selaku ketua Jurusan Matematika Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang.
4. Drs. H. Turmudi, M.Si dan Fachrur Rozi, M.Si, sebagai dosen pembimbing skripsi.
5. Bapak dan ibu dosen di Jurusan Matematika, dan seluruh *civitas academica* Jurusan Matematika Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang.

6. Ayah dan ibu atas doa, bimbingan, dan ridlonya selama ini.
7. Prof. Dr. KH. Ahmad Mudlor, S.H, sebagai Pengasuh Lembaga Tinggi Pesantren Luhur Malang, segenap Dewan *Asatidz*, dan seluruh guru-guru yang telah mendidik penulis dengan ikhlas.
8. Segenap keluarga besar MTs. Al-Hidayah Wajak.
9. Kepada semua pihak yang telah membantu dalam penyelesaian skripsi ini.

Semoga skripsi ini dapat memberikan kontribusi yang berarti di masa mendatang.

Malang, 29 Desember 2012

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR SIMBOL

$\forall$	: untuk semua
$\exists$	: ada
$\in$	: unsur dari
$\notin$	: bukan unsur dari
$\subseteq$	: subhimpunan dari
$A \times B$	: hasil kali kartesius A dan B
$*: S \times S \to S$	: $*$ adalah pemetaan dari $S \times S$ ke S
$\mathbb{N}$	: himpunan semua bilangan asli
$\mathbb{Z}$	: himpunan semua bilangan bulat
$\mathbb{R}$	: himpunan semua bilangan riil
$\langle a \rangle$	: ideal yang dibangun oleh unsur a
$a \mid b$	: a membagi b
$a \nmid b$	: a tidak membagi b
$a \sim b$	: a sekawan dengan b
$\Leftrightarrow$	: jika dan hanya jika
FPB	: faktor persekutuan terbesar
KPK	: kelipatan persekutuan terkecil
$\mathbb{Z}_n$	: koleksi semua kelas kongruensi modulo n (bilangan asli)
$\mathbb{Z}_p$	: koleksi semua kelas kongruensi modulo p (bilangan prima)
$\overline{a}$	: kelas kongruensi yang diwakili unsur a

DAFTAR ISTILAH

Bahasa Indonesia	Bahasa Inggris	Bahasa Arab
Sifat-sifat keterbagian	Divisibility properties	خصائص القسمة
Daerah faktorisasi tunggal	Unique factorization domain	حلقة التحليل الفريدة
Daerah integral	Integral domain	حلقة الصحيحة
Lapangan	Field	حلق
Daerah ideal utama	Principal ideal domain	مجال المثالى الرئيسة
Teori bilangan	Number theory	نظرية الأعداد
Bilangan prima	Prime number	عدد الأولى
Refleksif	Reflective	معكس
Transitif	Transitive	متعدية
Simetris	Symmetry	متماثل
Unsur unit	Unit element	عنصر الواحدة
Sekawan	Associates	رابط
Unsur tereduksi	Reducible element	العنصر القابل للتخفيض
Unsur tak tereduksi	Irreducible element	العنصر المتعذر رفضه
Unsur prima	Prime element	عنصر الرئيس
Ideal	Ideal	المثالى
Ring komutatif dengan unsur kesatuan	Commutative ring with unity	حلقة التبادلية بعنصر الوحدانية

ABSTRAK

Kurniawan, Moh. Zuhdi. **Keterbagian dan Sifat-sifat Daerah Faktorisasi Tunggal** $\mathbb{Z}_p$. Skripsi. Jurusan Matematika. Fakultas Sains dan Teknologi. Universitas Islam Negeri Maulana Malik Ibrahim Malang.
Pembimbing: (1) Drs. H. Turmudi, M.Si
(2) Fachrur Rozi, M.Si

Kata Kunci: daerah integral $(\mathbb{Z}_p, +, \times)$, sifat-sifat keterbagian, daerah faktorisasi tunggal, daerah ideal utama

Dalam teori bilangan sifat-sifat keterbagian diperkenalkan sebagai dasar faktorisasi (pemfaktoran). Sifat-sifat keterbagian dan faktorisasi tersebut selanjutnya diperumum dalam kajian aljabar abstrak, khususnya pada daerah integral $(\mathbb{Z}_p, +, \times)$ dimana $\mathbb{Z}_p$ adalah himpunan yang memuat koleksi semua kelas kongruensi modulo p (bilangan prima), yaitu $\mathbb{Z}_p = \{\bar{0}, \bar{1}, \dots, \overline{(p-1)}\}$.

Penelitian ini difokuskan pada kajian sifat-sifat keterbagian dan sifat-sifat daerah faktorisasi tunggal (DFT) pada daerah integral $\mathbb{Z}_p$.

Analisis sifat-sifat DFT $\mathbb{Z}_p$ dimulai dengan menguraikan sifat-sifat keterbagian pada $\mathbb{Z}_p$ dan membuktikan bahwa $\mathbb{Z}_p$ merupakan DFT. Kemudian diuraikan dan dibuktikan sifat-sifat DFT $\mathbb{Z}_p$.

Sifat-sifat keterbagian pada $\mathbb{Z}_p$ yaitu: (1) refleksif; (2) transitif; (3) simetris; (4) Jika $\bar{a}|\bar{b}$ maka $\bar{a}|(\bar{b}+\bar{c})$ dan $\bar{a}|(\bar{b}-\bar{c})$, untuk setiap $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_p$ dan $\bar{a} \neq \bar{0}$; (5) jika $\bar{a}|\bar{b}$ maka $\bar{a}|\bar{b}\bar{c}$, untuk setiap $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_p$ dan $\bar{a} \neq \bar{0}$; (6) jika $\bar{a}\bar{c}|\bar{b}$ maka $\bar{a}|\bar{b}$, untuk setiap $\bar{b} \in \mathbb{Z}_p$ dan $\bar{a}, \bar{c} \in \mathbb{Z}_p - \{\bar{0}\}$. Adapun sifat-sifat DFT $\mathbb{Z}_p$, yaitu: (1) setiap unsur tak nol di $\mathbb{Z}_p$ adalah unit; (2) setiap unsur tak nol di DFT $\mathbb{Z}_p$ adalah sekawan bagi semua unsur tak nol di DFT $\mathbb{Z}_p$; (3) FPB dari dua unsur tak nol di DFT $\mathbb{Z}_p$ adalah sembarang unsur tak nol di DFT $\mathbb{Z}_p$; (4) KPK dari dua unsur tak nol di DFT $\mathbb{Z}_p$ adalah sembarang unsur tak nol di DFT $\mathbb{Z}_p$; (5) DFT $\mathbb{Z}_p$ tidak memuat unsur tereduksi; (6) DFT $\mathbb{Z}_p$ tidak memuat unsur tak tereduksi; (7) DFT $\mathbb{Z}_p$ tidak memuat unsur prima.

ABSTRACT

Kurniawan, Moh. Zuhdi. **Divisibility and The Properties of Unique Factorization Domain $\mathbb{Z}_p$**. Thesis. Mathematics Department. Faculty of Science and Technology. Maulana Malik Ibrahim State Islamic University, Malang.
Advisor: (1) Drs. H. Turmudi, M.Si
(2) Fachrur Rozi, M.Si

Keywords: integral domain $(\mathbb{Z}_p, +, \times)$, divisibility properties, unique factorization domain, principal ideal domain

In the number theory, divisibility properties is described as basic of factorization. The divisibility properties and factorization will be generalized in abstract algebra, especially on integral domain $(\mathbb{Z}_p, +, \times)$ which $\mathbb{Z}_p$ is a set of collection of congruence class modulo p (prime number). It is denoted $\mathbb{Z}_p = \{\bar{0}, \bar{1}, \dots, \overline{(p-1)}\}$.

This research focused on the properties of divisibility and unique factorization domain (UFD) on integral domain $\mathbb{Z}_p$.

Analyzing of the UFD $\mathbb{Z}_p$ properties begins by describing the divisibility properties of $\mathbb{Z}_p$ and proofing that $\mathbb{Z}_p$ is UFD. Then, describing and proofing the properties of UFD $\mathbb{Z}_p$.

The divisibility properties of $\mathbb{Z}_p$ are: (1) reflective; (2) transitive; (3) symmetry; (4) if $\bar{a}|\bar{b}$ then $\bar{a}|(\bar{b}+\bar{c})$ and $\bar{a}|(\bar{b}-\bar{c})$ for all $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_p$ and $\bar{a} \neq \bar{0}$; (5) if $\bar{a}|\bar{b}$ then $\bar{a}|\bar{b}\bar{c}$ for all $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_p$ and $\bar{a} \neq \bar{0}$; (6) if $\bar{a}\bar{c}|\bar{b}$ then $\bar{a}|\bar{b}$ for all $\bar{b} \in \mathbb{Z}_p$ and $\bar{a}, \bar{c} \in \mathbb{Z}_p - \{\bar{0}\}$. The properties of UFD $\mathbb{Z}_p$ are: (1) each nonzero elements of UFD $\mathbb{Z}_p$ is unit; (2) every nonzero element of UFD $\mathbb{Z}_p$ is associate by all nonzero elements of UFD $\mathbb{Z}_p$; (3) GCD of two nonzero elements of UFD $\mathbb{Z}_p$ is any nonzero elements of UFD $\mathbb{Z}_p$; (4) LCM of two nonzero elements of UFD $\mathbb{Z}_p$ is any nonzero elements of UFD $\mathbb{Z}_p$; (5) UFD $\mathbb{Z}_p$ does not contain reducible element; (6) UFD $\mathbb{Z}_p$ does not contain irreducible element; (7) UFD $\mathbb{Z}_p$ does not contain prime.

الملخص

محمد زهدى كورنياوان. **القسمة وخصائص حلقة التحليل الفريدة $\mathbb{Z}_p$**. بحث العلم . قسم الرياضيات. كلية العلوم والتكنولوجيا. جامعة مولانا مالك إبراهيم الإسلامية الحكومية مالانج.

مشرف: (١) دوكتور أندوس الحج تورمودى الماجيستير

(٢) فخر الرازى الماجستير

الكلمة الرئيسة: حلقة الصحيحة $\mathbb{Z}_p$ ، خصائص القسمة، حلقة التحليل الفريدة، مجال المثالى الرئيسة

في نظرية الأعداد، يكون بحث خصائص القسمة أساسا للتحليل. و هذه الخصائص والتحليل سوف تعم فى الجبر المجرد، وخاصة على حلقة الصحيحة $(\mathbb{Z}_p, +, \times)$ الذي $\mathbb{Z}_p$ هو مجمع من فئة التطابق مودولو p (عدد الأولى). وتكتب عليه $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \dots, \overline{(p-1)}\}$.

و هذا البحث يركز على خصائص القسمة و حلقة التحليل الفريدة (UFD) في حلقة الصحيحة $\mathbb{Z}_p$.

يبتدأ هذا البحث بشرح خصائص القسمة $\mathbb{Z}_p$ و تدليل أن $\mathbb{Z}_p$ هى UFD. ثم تشريح و تدليل خصائص UFD $\mathbb{Z}_p$. خصائص القسمة هى: (١) معكس؛(٢) متعدية؛(٣) متماثل؛(٤) إذا $\bar{a}|\bar{b}$ ثم $\bar{a}|(\bar{b}+\bar{c})$ و $\bar{a}|(\bar{b}-\bar{c})$ لكل $\bar{a},\bar{b},\bar{c} \in \mathbb{Z}_p$ و $\bar{a} \neq \bar{0}$؛(٥) إذا $\bar{a}|\bar{b}$ ثم $\bar{a}|\bar{b}\bar{c}$ لكل $\bar{a},\bar{b},\bar{c} \in \mathbb{Z}_p$ و $\bar{a} \neq \bar{0}$؛(٦) إذا $\bar{a}\bar{c}|\bar{b}$ ثم $\bar{a}|\bar{b}$ لكل $\bar{b} \in \mathbb{Z}_p$ و $\bar{a},\bar{c} \in \mathbb{Z}_p - \{\bar{0}\}$. و خصائص UFD $\mathbb{Z}_p$، هى: (١) كل العناصر غير صفرية في UFD $\mathbb{Z}_p$ هو الواحدة؛ (٢) كل العناصر غير صفرية في UFD $\mathbb{Z}_p$ هو رابط بعضها البعض؛ (٣) GCD لغير صفرية عنصرين هو كل العناصر غير صفرية في UFD $\mathbb{Z}_p$؛(٤) LCM لغير صفرية عنصرين ه و كل العناصر غير صفرية في UFD $\mathbb{Z}_p$؛(٥) UFD $\mathbb{Z}_p$ لا تحتوى العنصر القابل للتخفيض؛ (٦) UFD $\mathbb{Z}_p$ لا تحتوى العنصر المتعذر رفضه؛ (٧) UFD $\mathbb{Z}_p$ لا تحتوى عنصر الرئيس.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Matematika merupakan salah satu ilmu pengetahuan dasar (*basic science*) yang banyak bermanfaat dalam perkembangan berbagai disiplin ilmu. Matematika telah banyak mengajarkan manusia mengenal dan menjelaskan fenomena-fenomena yang terjadi di sekelilingnya. Hal ini karena matematika mampu memodelkan dunia nyata ke dalam bahasa metematika sehingga dapat lebih mudah dipahami secara universal.

Secara historis, Islam pada masa kejayaannya mempunyai peran besar dalam perkembangan ilmu pengetahuan, termasuk matematika. Abu Abdullah Muhammad Ibn Musa Al-Khawarizmi atau yang dikenal sebagai Al-Khawarizmi adalah salah satu intelektual muslim yang memberikan banyak karya orisinil dalam bidang matematika. Karyanya *Kitab Al-Jabr wa Al-Muqabalah (The Book of Restoring and Balancing)* menjadi titik awal matematika aljabar, sehingga Al-Khawarizmi dikenal sebagai "Bapak Ilmu Pengetahuan Aljabar". Terjemahannya dalam bahasa latin digunakan sebagai buku wajib matematika dasar di daratan Eropa hingga abad keenam belas (Mohamed, 2001:17).

Aktivitas intelektual, tradisi ilmiah dan produktivitas karya ilmiah pada zaman keemasan Islam lebih dari sekedar tujuan untuk mengembangkan ilmu pengetahuan, namun kebutuhan religi menjadi dorongan yang kuat untuk terus berkarya. Salah satu motivasi dan inspirasi untuk mengembangkan ilmu pengetahuan disampaikan oleh Allah SWT melalui Al-Qur’an surat Al-‘Alaq ayat 1-5, yaitu:

ٱقۡرَأۡ بِٱسۡمِ رَبِّكَ ٱلَّذِي خَلَقَ ﴿١﴾ خَلَقَ ٱلۡإِنسَٰنَ مِنۡ عَلَقٍ ﴿٢﴾ ٱقۡرَأۡ وَرَبُّكَ ٱلۡأَكۡرَمُ ﴿٣﴾

ٱلَّذِي عَلَّمَ بِٱلۡقَلَمِ ﴿٤﴾ عَلَّمَ ٱلۡإِنسَٰنَ مَا لَمۡ يَعۡلَمۡ ﴿٥﴾

Artinya: (1) Bacalah dengan (menyebut) nama Tuhanmu yang menciptakan; (2) Dia telah menciptakan manusia dari segumpal darah; (3) Bacalah, dan Tuhanmulah Yang Maha Mulia; (4) Yang mengajar (manusia) dengan perantaran kalam[1589]; (5) Dia mengajarkan kepada manusia apa yang tidak diketahuinya.

[1589] Maksudnya: Allah mengajar manusia dengan perantaraan tulis baca.

Lima ayat yang pertama kali diwahyukan oleh Allah SWT kepada Nabi Muhammad SAW ini memuat motivasi untuk belajar melalui membaca dan inspirasi untuk berkarya dengan menulis. Hal ini sesuai dengan fakta bahwa berkembangnya ilmu pengetahuan melalui dua kegiatan ilmiah tersebut, yaitu membaca dan menulis. Kata *iqro’* memiliki pengertian yang lebih luas, yaitu membaca semesta alam, berpikir, dan tadabbur. Begitu pula menulis di sini juga berarti berkarya secara universal. Mohamed (2001:7) menyebutkan bahwa motivasi senada disampaikan Al-Qur’an dalam sekitar 750 ayat (hampir $\frac{1}{8}$ dari isi Al-Qur’an) yang berisi dorongan untuk mempelajari alam.

Selain itu, dalam satu hadis yang diriwayatkan oleh Ibnu Maajah, Nabi Muhammad SAW pernah menyampaikan motivasi dan inspirasi untuk mengembangkan ilmu pengetahuan, yaitu:

طَلَبُ الْعِلْمِ فَرِيْضَةٌ عَلَى كُلِّ مُسْلِمٍ (رواه إبن ماجه)

Artinya: Mencari ilmu adalah amat sangat wajib bagi setiap Muslim.

Hadis di atas menyampaikan ide pentingnya mengembangkan ilmu pengetahuan, yang disimbolkan dengan kata *fariidhoh* berbentuk *mubaalaghah*, yang artinya amat sangat wajib.

Abdussakir (2007:99) menyampaikan bahwa Al-Qur'an merupakan kalam Allah yang berbicara mengenai beberapa topik matematika. Al-Qur'an berbicara tentang bilangan, aljabar, geometri dan pengukuran serta statistika. Sekalipun begitu, menurut M. Quraish Shihab (1992:24) memahami hubungan antara Al-Qur'an dan ilmu pengetahuan bukan dinilai dari banyaknya cabang-cabang ilmu pengetahuan yang tersimpul di dalamnya, bukan pula dengan menunjukkan kebenaran teori-teori ilmiah, tetapi dengan melihat adakah Al-Qur'an atau jiwa (motivasi) ayat-ayatnya menghalangi kemajuan ilmu pengetahuan atau mendorong lebih maju. Hal ini sesuai dengan tujuan Al-Qur'an adalah sebagai kitab hidayah yang memberikan petunjuk kepada manusia seluruhnya dalam persoalan akidah, *tasyri'*, dan akhlak demi kebahagiaan hidup di dunia dan di akhirat.

Di antara tema yang banyak dikembangkan dalam aljabar adalah aljabar abstrak, yaitu suatu pembahasan yang dimulai dengan memperkenalkan konsep sistem matematika dan sifat-sifatnya. Bhattacharya dkk. (1990:61) menyebutkan bahwa sistem matematika atau disebut juga struktur aljabar adalah suatu himpunan tak kosong yang dilengkapi dengan paling sedikit satu operasi biner. Sistem matematika dari suatu himpunan tak kosong yang dilengkapi satu operasi biner disebut grup, adapun yang dilengkapi dua operasi biner disebut ring.

Daerah integral dalam aljabar abstrak merupakan ring komutatif dengan unsur kesatuan dan tidak memuat pembagi nol. Himpunan bilangan bulat dengan penjumlahan sebagai operasi pertama dan perkalian sebagai operasi kedua merupakan daerah integral. Dalam teori bilangan yang semesta pembicaraannya adalah daerah integral bilangan bulat, telah diperkenalkan sifat-sifat keterbagian sebagai dasar konsep faktorisasi. Sifat-sifat keterbagian pada himpunan bilangan bulat berbeda dengan sifat-sifat keterbagian pada himpunan bilangan rasional, begitu pula dengan himpunan bilangan riil.

Sifat keterbagian dan faktorisasi pada himpunan bilangan bulat tersebut selanjutnya diperumum dalam kajian aljabar abstrak pada objek daerah integral, khususnya pada $(\mathbb{Z}_p, +, \times)$ dimana $\mathbb{Z}_p$ adalah himpunan yang memuat koleksi semua kelas kongruensi modulo bilangan prima p, yaitu $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \dots, \overline{(p-1)}\}$. Daerah integral $\mathbb{Z}_p$ yang juga merupakan lapangan terhingga memiliki sifat-sifat khusus yang berbeda dengan daerah integral lainnya. Oleh karena itu, penelitian ini akan mengkaji lebih dalam mengenai sifat-sifat keterbagian pada $\mathbb{Z}_p$ dan sifat-sifat daerah faktorisasi tunggal $\mathbb{Z}_p$.

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, permasalahan yang akan dibahas dalam skripsi ini adalah:

1. Bagaimanakah sifat-sifat dan pembuktian keterbagian pada $\mathbb{Z}_p$?
2. Bagaimanakah sifat-sifat dan pembuktian daerah faktorisasi tunggal $\mathbb{Z}_p$?

1.3 Tujuan Penelitian

Tujuan penyusunan skripsi ini adalah:

1. Mendeskripsikan sifat-sifat dan pembuktian keterbagian pada $\mathbb{Z}_p$.
2. Mendeskripsikan sifat-sifat dan pembuktian daerah faktorisasi tunggal $\mathbb{Z}_p$.

1.4 Manfaat Penelitian

Adapun manfaat penelitian dalam skripsi ini adalah:

1. Bagi Penulis

   Sebagai tambahan pengetahuan dalam penelitian matematika murni, khususnya mengenai keterbagian pada $\mathbb{Z}_p$ dan sifat-sifat daerah faktorisasi tunggal $\mathbb{Z}_p$.

2. Bagi Lembaga

   Sebagai tambahan referensi untuk penelitian maupun perkuliahan mengenai keterbagian pada $\mathbb{Z}_p$ dan sifat-sifat daerah faktorisasi tunggal $\mathbb{Z}_p$.

3. Bagi Pembaca

   Sebagai tambahan wawasan materi aljabar abstrak, yaitu mengenai keterbagian pada $\mathbb{Z}_p$ dan sifat-sifat daerah faktorisasi tunggal $\mathbb{Z}_p$.

1.5 Metode Penelitian

Metode penelitian yang dipakai untuk menyelesaikan masalah di atas adalah metode kepustakaan atau disebut juga studi literatur, yaitu penelitian yang dilakukan dengan mengumpulkan teori dan informasi yang berhubungan dengan penelitian dengan bantuan referensi seperti buku maupun jurnal ilmiah. Adapun langkah-langkah yang dilakukan dalam penelitian ini adalah sebagai berikut:

1. Membahas definisi keterbagian pada $\mathbb{Z}_p$.
2. Mencari sifat-sifat keterbagian pada $\mathbb{Z}_p$ sekaligus membuktikannya.
3. Membuktikan bahwa $\mathbb{Z}_p$ merupakan daerah faktorisasi tunggal.
4. Menganalisis dan membuktikan sifat-sifat daerah faktorisasi tunggal $\mathbb{Z}_p$.
5. Merumuskan kesimpulan dari hasil pembahasan.

1.6 Sistematika Penulisan

Untuk mempermudah pembaca memahami tulisan ini, penulis membagi tulisan ini ke dalam empat bab sebagai berikut:

1. **BAB I PENDAHULUAN:** Bab ini memuat latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, dan sistematika penulisan.

2. **BAB II KAJIAN PUSTAKA:** Dalam bab ini dikemukakan landasan teori yang akan digunakan dalam membahas sifat-sifat keterbagian pada $\mathbb{Z}_p$ dan sifat-sifat daerah faktorisasi tunggal $\mathbb{Z}_p$, diantaranya yaitu teori grup, teori ring, ring $\mathbb{Z}_p$, ideal, keterbagian pada ring komutatif, dan definisi daerah faktorisasi tunggal.
3. **BAB III PEMBAHASAN:** Bab ini memaparkan sifat-sifat keterbagian pada $\mathbb{Z}_p$ dan sifat-sifat daerah faktorisasi tunggal $\mathbb{Z}_p$.
4. **BAB IV PENUTUP:** Dalam bab ini dikemukakan kesimpulan dari hasil penelitian dan beberapa saran.

BAB II

KAJIAN PUSTAKA

2.1 Grup

2.1.1 Definisi Hasil Kali Kartesius

Hasil kali kartesius dari himpunan A dan B adalah $A \times B = \{(x, y) | x \in A, y \in B\}$, yaitu koleksi dari pasangan terurut unsur-unsur dari A dan B (Dummit dan Foote, 1991:1).

Contoh 2.1

Misalkan $A = \{a, b\}$ dan $B = \{1, 2, 3\}$, maka $A \times B = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$.

2.1.2 Definisi Operasi Biner

Operasi biner $*$ pada himpunan G adalah fungsi $*: G \times G \to G$. Untuk sembarang $a, b \in G$ bisa dituliskan $a * b$ untuk $*(a, b)$ (Dummit dan Foote, 1991:17).

Contoh 2.2

1. Operasi pengurangan di $\mathbb{Z}$ merupakan operasi biner, karena untuk semua $a, b \in \mathbb{Z}$ memenuhi $(a - b) \in \mathbb{Z}$.
2. Operasi pengurangan di $\mathbb{N}$ bukan operasi biner, karena ada $(1 - 2) \notin \mathbb{N}$. Untuk semua $a, b \in \mathbb{N}$ dan $a < b$, maka $(a - b) \notin \mathbb{N}$.

2.1.3 Definisi Struktur Aljabar

Struktur aljabar adalah suatu himpunan tak kosong yang dilengkapi satu atau lebih operasi biner pada himpunan itu (Bhattacharya, dkk., 1995:61).

$(G,*)$ adalah suatu struktur aljabar dari himpunan tak kosong G yang dilengkapi satu operasi biner, yaitu $*$. Sedangkan $(R,*,\circ)$ adalah suatu struktur aljabar dari himpunan tak kosong R yang dilengkapi dua operasi biner, secara berurutan yaitu $*$ dan $\circ$.

Contoh 2.3

1. $(\mathbb{Z},+)$ merupakan struktur aljabar, karena untuk semua $a,b \in \mathbb{Z}$ berlaku $(a+b) \in \mathbb{Z}$.
2. $(\mathbb{N},+)$ merupakan struktur aljabar, karena untuk semua $a,b \in \mathbb{N}$ berlaku $(a+b) \in \mathbb{N}$.
3. $(\mathbb{N},-)$ bukan struktur aljabar. Contoh 2.2 menunjukkan bahwa operasi pengurangan di $\mathbb{N}$ bukan operasi biner.

2.1.4 Definisi Grup

Grup adalah pasangan terurut $(G,*)$ dimana G adalah himpunan dan $*$ adalah operasi biner pada G yang memenuhi beberapa aksioma berikut:

1. $(a*b)*c = a*(b*c)$ untuk semua $a,b,c \in G$ (dengan kata lain $*$ bersifat asosiatif),
2. Terdapat unsur e di G sedemikian hingga $a*e = e*a = a$, untuk semua $a \in G$ (e disebut unsur identitas dari G),
3. Untuk setiap $a \in G$ terdapat unsur a^{-1} di G sedemikian hingga $a*a^{-1} = a^{-1}*a = e$ (a^{-1} disebut invers dari a),

(Dummit dan Foote, 1991:17).

Penyebutan $(G,*)$ adalah grup, selanjutnya dapat disederhanakan dengan cukup menulis grup G, ataupun G adalah grup (dengan asumsi G dilengkapi satu operasi biner tertentu).

Contoh 2.4

1. $(\mathbb{Z},+)$ adalah grup, karena memenuhi:
   a) Sifat asosiatif.
      Untuk semua $a,b,c \in \mathbb{Z}$ berlaku $a+(b+c)=(a+b)+c$.
   b) Terdapat 0 di $\mathbb{Z}$ sebagai unsur identitas penjumlahan di $\mathbb{Z}$, sedemikian hingga untuk semua $a \in \mathbb{Z}$, berlaku $a+0=0+a=a$.
   c) Untuk setiap $a \in \mathbb{Z}$, selalu terdapat invers penjumlahannya yaitu $-a \in \mathbb{Z}$, sehingga $a+(-a)=-a+a=0$.
2. $(\mathbb{N},+)$ bukan grup, karena tidak ada unsur identitas penjumlahan di $\mathbb{N}$.

2.1.5 Definisi Grup Komutatif

Grup $(G,*)$ dikatakan komutatif jika $a*b=b*a$ untuk semua $a,b \in G$ (Dummit dan Foote, 1991:17).

Contoh 2.5

1. $(\mathbb{Z},+)$ adalah grup komutatif, karena untuk semua $a,b \in \mathbb{Z}$ berlaku $a+b=b+a$.
2. Misalkan M adalah himpunan matriks yang didefinisikan sebagai $M=\left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| \, a,b,c,d \in \mathbb{R}; ad-bc \neq 0\right\}$. Pada himpunan M, diberikan suatu operasi perkalian matriks, yang didefinisikan sebagai $\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} p & q \\ r & s \end{bmatrix}=\begin{bmatrix} ap+br & aq+bs \\ cp+dr & cq+ds \end{bmatrix}$, untuk semua $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ dan $\begin{bmatrix} p & q \\ r & s \end{bmatrix}$ unsur di M. Dengan

perkalian matriks tersebut, struktur aljabar $(M,\times)$ merupakan grup tak komutatif, karena:

a) Bersifat asosiatif

Untuk semua $\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \begin{bmatrix} e & f \\ g & h \end{bmatrix}$ dan $\begin{bmatrix} i & j \\ k & l \end{bmatrix}$ di M berlaku:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\left(\begin{bmatrix} e & f \\ g & h \end{bmatrix}\begin{bmatrix} i & j \\ k & l \end{bmatrix}\right)$$

$$= \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} ei + fk & ej + fl \\ gi + hk & gj + hl \end{bmatrix}$$

$$= \begin{bmatrix} a(ei) + a(fk) + b(gi) + b(hk) & a(ej) + a(fl) + b(gj) + b(hl) \\ c(ei) + c(fk) + d(gi) + d(hk) & c(ej) + c(fl) + d(gj) + d(hl) \end{bmatrix}$$

$$= \begin{bmatrix} (ae)i + (bg)i + (af)k + (bh)k & (ae)j + (bg)j + (af)l + (bh)l \\ (ce)i + (dg)i + (cf)k + (dh)k & (ce)j + (dg)j + (cf)l + (dh)l \end{bmatrix}$$

$$= \begin{bmatrix} (ae + bg)i + (af + bh)k & (ae + bg)j + (af + bh)l \\ (ce + dg)i + (cf + dh)k & (ce + dg)j + (cf + dh)l \end{bmatrix}$$

$$= \begin{bmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{bmatrix}\begin{bmatrix} i & j \\ k & l \end{bmatrix}$$

$$= \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} e & f \\ g & h \end{bmatrix}\right)\begin{bmatrix} i & j \\ k & l \end{bmatrix}$$

Sehingga $\begin{bmatrix} a & b \\ c & d \end{bmatrix}\left(\begin{bmatrix} e & f \\ g & h \end{bmatrix}\begin{bmatrix} i & j \\ k & l \end{bmatrix}\right) = \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} e & f \\ g & h \end{bmatrix}\right)\begin{bmatrix} i & j \\ k & l \end{bmatrix}$.

b) Terdapat $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in M$ sebagai unsur identitas, sedemikian hingga untuk semua $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M$ berlaku: $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

c) Untuk setiap $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M$ terdapat inversnya di M yang didefinisikan sebagai $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}$

dengan $\frac{a}{ad-bc}, \frac{-b}{ad-bc}, \frac{-c}{ad-bc}, \frac{d}{ad-bc} \in \mathbb{R}$.

Sehingga $\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

dan $\begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

d) Tidak berlaku sifat komutatif di M, karena ada $\begin{bmatrix} 3 & 1 \\ 0 & 2 \end{bmatrix}$ dan $\begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix}$ di M, sedemikian hingga:

$\begin{bmatrix} 3 & 1 \\ 0 & 2 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix} = \begin{bmatrix} 6 & 7 \\ 6 & 2 \end{bmatrix}$ dan $\begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix}\begin{bmatrix} 3 & 1 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 3 & 5 \\ 9 & 5 \end{bmatrix}$.

2.1.6 Definisi Grup Terhingga dan Grup Tak Terhingga

Grup G dikatakan terhingga jika memuat unsur yang banyaknya terhingga. Sebaliknya, grup G dikatakan tak terhingga jika memuat unsur yang banyaknya tak terhingga (Arifin, 2000:36).

Contoh 2.6

1. $(\mathbb{Z}, +)$ adalah grup tak terhingga. Contoh 2.4 menunjukkan bahwa $(\mathbb{Z}, +)$ merupakan grup. $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$ memuat unsur yang banyaknya tak terhingga.

2. Misalkan $H = \left\{\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}, \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}, \begin{bmatrix}-1 & 0\\0 & 1\end{bmatrix}, \begin{bmatrix}-1 & 0\\0 & -1\end{bmatrix}\right\}$, maka $(H,\times)$ adalah grup terhingga karena memenuhi:

   a) Sifat asosiatif.

   Untuk semua $\begin{bmatrix}a & 0\\0 & b\end{bmatrix}, \begin{bmatrix}c & 0\\0 & d\end{bmatrix}$ dan $\begin{bmatrix}e & 0\\0 & f\end{bmatrix}$ di H berlaku:

   $$\begin{bmatrix}a & 0\\0 & b\end{bmatrix}\left(\begin{bmatrix}c & 0\\0 & d\end{bmatrix}\begin{bmatrix}e & 0\\0 & f\end{bmatrix}\right)$$

   $$= \begin{bmatrix}a & 0\\0 & b\end{bmatrix}\begin{bmatrix}ce & 0\\0 & df\end{bmatrix}$$

   $$= \begin{bmatrix}a(ce) & 0\\0 & b(df)\end{bmatrix}$$

   $$= \begin{bmatrix}(ac)e & 0\\0 & (bd)f\end{bmatrix}$$

   $$= \begin{bmatrix}ac & 0\\0 & bd\end{bmatrix}\begin{bmatrix}e & 0\\0 & f\end{bmatrix}$$

   $$= \left(\begin{bmatrix}a & 0\\0 & b\end{bmatrix}\begin{bmatrix}c & 0\\0 & d\end{bmatrix}\right)\begin{bmatrix}e & 0\\0 & f\end{bmatrix}$$

   Sehingga $\begin{bmatrix}a & 0\\0 & b\end{bmatrix}\left(\begin{bmatrix}c & 0\\0 & d\end{bmatrix}\begin{bmatrix}e & 0\\0 & f\end{bmatrix}\right) = \left(\begin{bmatrix}a & 0\\0 & b\end{bmatrix}\begin{bmatrix}c & 0\\0 & d\end{bmatrix}\right)\begin{bmatrix}e & 0\\0 & f\end{bmatrix}$.

   b) Terdapat $\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix} \in H$ sebagai unsur identitas, sedemikian hingga untuk semua $\begin{bmatrix}a & 0\\0 & b\end{bmatrix} \in H$ berlaku $\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}\begin{bmatrix}a & 0\\0 & b\end{bmatrix} = \begin{bmatrix}a & 0\\0 & b\end{bmatrix}\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix} = \begin{bmatrix}a & 0\\0 & b\end{bmatrix}$.

   c) Untuk setiap $\begin{bmatrix}a & 0\\0 & b\end{bmatrix}$ di H selalu memiliki invers perkaliannya di H yang didefinisikan sebagai $\begin{bmatrix}a & 0\\0 & b\end{bmatrix}^{-1} = \frac{1}{ab}\begin{bmatrix}b & 0\\0 & a\end{bmatrix} = \begin{bmatrix}\frac{1}{a} & 0\\0 & \frac{1}{b}\end{bmatrix}$. Karena $\frac{1}{1} = 1$

$$\text{dan } \frac{1}{-1} = -1, \text{ maka } \begin{bmatrix} \frac{1}{a} & 0 \\ 0 & \frac{1}{b} \end{bmatrix} \text{ selalu ada di } H.$$

Karena $(H,\times)$ merupakan grup dan himpunan H memuat unsur yang banyaknya terbatas, maka grup H disebut grup terhingga.

2.2 Ring

2.2.1 Definisi Ring

Ring R adalah himpunan yang dilengkapi dengan dua operasi biner $+$ dan $\times$ (disebut penjumlahan dan perkalian) yang memenuhi aksioma berikut:

1. $(R,+)$ adalah grup komutatif,
2. $\times$ bersifat asosiatif: $(a \times b) \times c = a \times (b \times c)$ untuk semua $a, b, c \in R$,
3. Dalil distributif berlaku di R: untuk semua $a, b, c \in R$

   $(a + b) \times c = (a \times c) + (b \times c)$ dan $a \times (b + c) = (a \times b) + (a \times c)$,

(Dummit dan Foote, 1991:225).

Selanjutnya, perkalian unsur $a \in R$ dan $b \in R$, yaitu $a \times b$ ditulis ab.

Contoh 2.7

1. $(\mathbb{Z},+,\times)$ merupakan ring, karena memenuhi:
   a) $(\mathbb{Z},+)$ adalah grup komutatif. Telah ditunjukkan pada contoh 2.5.
   b) $(\mathbb{Z},\times)$ bersifat asosiatif, yaitu: $a(bc) = (ab)c$ untuk semua $a, b, c \in \mathbb{Z}$.
   c) Dalil distributif berlaku di $\mathbb{Z}$. Untuk semua $a, b, c \in \mathbb{Z}$ berlaku:

      $a(b + c) = ab + ac$ dan $(a + b)c = ac + bc$.
2. $(\mathbb{N},+,\times)$ bukanlah ring, karena $(\mathbb{N},+)$ bukan merupakan grup.

2.2.2 Definisi Ring Komutatif

Ring R disebut komutatif jika perkaliannya bersifat komutatif (Dummit dan Foote, 1991:225).

Contoh 2.8

1. Ring $(\mathbb{Z},+,\times)$ merupakan ring komutatif, karena untuk semua $a,b \in \mathbb{Z}$ berlaku $ab = ba$.
2. Misalkan M adalah himpunan matriks yang didefinisikan sebagai $M = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| \, a,b,c,d \in \mathbb{R}; ad - bc \neq 0\right\}$. Pada himpunan M, diberikan operasi penjumlahan dan perkalian matriks, yang didefinisikan sebagai $\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} p & q \\ r & s \end{bmatrix} = \begin{bmatrix} a+p & a+q \\ c+r & d+s \end{bmatrix}$ dan $\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} p & q \\ r & s \end{bmatrix} = \begin{bmatrix} ap+br & aq+bs \\ cp+dr & cq+ds \end{bmatrix}$, untuk semua $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ dan $\begin{bmatrix} p & q \\ r & s \end{bmatrix}$ unsur di M. Dengan penjumlahan dan perkalian matriks tersebut, struktur aljabar $(M,+,\times)$ merupakan ring tak komutatif, karena:
   a) $(M,+)$ merupakan grup komutatif
      i) Bersifat asosiatif

      Untuk semua $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $\begin{bmatrix} e & f \\ g & h \end{bmatrix}$ dan $\begin{bmatrix} i & j \\ k & l \end{bmatrix}$ di M, berlaku:

$$\begin{aligned}
\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \left(\begin{bmatrix} e & f \\ g & h \end{bmatrix} + \begin{bmatrix} i & j \\ k & l \end{bmatrix}\right) &= \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e+i & f+j \\ g+k & h+l \end{bmatrix} \\
&= \begin{bmatrix} a+(e+i) & b+(f+j) \\ c+(g+k) & d+(h+l) \end{bmatrix} \\
&= \begin{bmatrix} (a+e)+i & (b+f)+j \\ (c+g)+k & (d+h)+l \end{bmatrix}
\end{aligned}$$

$$= \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix} + \begin{bmatrix} i & j \\ k & l \end{bmatrix}$$

$$= \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} \right) + \begin{bmatrix} i & j \\ k & l \end{bmatrix}$$

ii) Terdapat $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in M$ sebagai unsur identitas penjumlahan di M, sehingga untuk semua $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M$ berlaku:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

iii) Untuk setiap $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M$ selalu memiliki invers penjumlahannya di M, yaitu $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$, sehingga:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

iv) Untuk semua $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ dan $\begin{bmatrix} e & f \\ g & h \end{bmatrix}$ di M, memenuhi:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix}$$

$$= \begin{bmatrix} e+a & f+b \\ g+c & h+d \end{bmatrix}$$

$$= \begin{bmatrix} e & f \\ g & h \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

b) $(M,\times)$ bersifat asosiatif. Telah ditunjukkan pada contoh 2.5.

c) Dalil distributif berlaku di M, untuk semua $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $\begin{bmatrix} e & f \\ g & h \end{bmatrix}$ dan $\begin{bmatrix} i & j \\ k & l \end{bmatrix}$ di M, berlaku:

i) $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \left(\begin{bmatrix} e & f \\ g & h \end{bmatrix} + \begin{bmatrix} i & j \\ k & l \end{bmatrix} \right)$

$$= \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e+i & f+j \\ g+k & h+l \end{bmatrix}$$

$$= \begin{bmatrix} (ae+ai)+(bg+bk) & (af+aj)+(bh+bl) \\ (ce+ci)+(dg+dk) & (cf+cj)+(dh+dl) \end{bmatrix}$$

$$= \begin{bmatrix} (ae+bg)+(ai+bk) & (af+bh)+(aj+bl) \\ (ce+dg)+(ci+dk) & (cf+dh)+(cj+dl) \end{bmatrix}$$

$$= \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix} + \begin{bmatrix} ai+bk & aj+bl \\ ci+dk & cj+dl \end{bmatrix}$$

$$= \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} i & j \\ k & l \end{bmatrix}$$

ii) $\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} \right) \begin{bmatrix} i & j \\ k & l \end{bmatrix}$

$$= \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix} \begin{bmatrix} i & j \\ k & l \end{bmatrix}$$

$$= \begin{bmatrix} (ai+ei)+(bk+fk) & (aj+ej)+(bl+fl) \\ (ci+gi)+(dk+hk) & (cj+gj)+(dl+hl) \end{bmatrix}$$

$$= \begin{bmatrix} (ai+bk)+(ei+fk) & (aj+bl)+(ej+fl) \\ (ci+dk)+(gi+hk) & (cj+dl)+(gj+hl) \end{bmatrix}$$

$$= \begin{bmatrix} ai+bk & aj+bl \\ ci+dk & cj+dl \end{bmatrix} + \begin{bmatrix} ei+fk & ej+fl \\ gi+hk & gj+hl \end{bmatrix}$$

$$= \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} i & j \\ k & l \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} \begin{bmatrix} i & j \\ k & l \end{bmatrix}$$

d) Pada $(M,\times)$ tidak berlaku sifat komutatif. Telah ditunjukkan pada contoh 2.5.

2.2.3 Definisi Ring dengan Unsur Kesatuan

Ring R dikatakan memiliki unsur kesatuan (memuat 1) jika terdapat unsur $1 \in R$ dengan $1a = a1 = a$ untuk semua $a \in R$ (Dummit dan Foote, 1991:225).

Pada pembahasan selanjutnya, unsur identitas penjumlahan di ring R dinotasikan dengan 0, sedangkan pada perkalian dinotasikan dengan 1. Invers unsur a terhadap penjumlahan dinotasikan dengan $-a$, sedangkan invers terhadap perkalian dinotasikan dengan a^{-1}.

Contoh 2.9

1. Ring komutatif $(\mathbb{Z},+,\times)$ merupakan ring dengan unsur kesatuan. Ring $(\mathbb{Z},+,\times)$ memuat $1 \in \mathbb{Z}$ yang memenuhi $a1 = 1a = a$ untuk semua $a \in \mathbb{Z}$.
2. Misalkan $E = \{2k|k \in \mathbb{Z}\} = \{\dots,-6,-4,-2,0,2,4,6,\dots\}$. Maka struktur aljabar $(E,+,\times)$ merupakan ring tanpa unsur kesatuan.

   a) $(E,+)$ merupakan grup komutatif, karena memenuhi:

      i) Sifat asosiatif. Untuk semua $a,b,c \in E$, misalkan $a = 2k_1$, $b = 2k_2$ dan $c = 2k_3$, untuk suatu $k_1,k_2,k_3 \in \mathbb{Z}$, berlaku:

      $a + (b + c) = 2k_1 + (2k_2 + 2k_3)$ $[2k_1, 2k_2, 2k_3 \in \mathbb{Z}]$

      $= (2k_1 + 2k_2) + 2k_3$ [sifat asosiatif penjumlahan

      $= (a + b) + c$ di $\mathbb{Z}$]

      ii) Terdapat $0 \in E$ sebagai unsur identitas penjumlahan di E. Untuk semua $a = 2k \in E$, $k \in \mathbb{Z}$, berlaku:

      $a + 0 = 2k + 0 = 0 + 2k = 0 + a = a.$

      iii) Untuk semua $a \in E$ memiliki invers penjumlahan di E. Misalkan invers dari $a = 2k_1 \in E$ adalah $b = 2k_2 \in E$. Akan ditunjukkan bahwa $a + b = b + a = 0$.

      $a + b = 0 \Leftrightarrow 2k_1 + 2k_2 = 0$

      $\Rightarrow 2(k_1 + k_2) = 0$

$$\Longrightarrow \quad k_1 + k_2 = 0$$

$$\Longrightarrow \quad k_2 = -k_1 \in \mathbb{Z}$$

Maka $b = 2k_2 = 2(-k_1) = -2k_1 = -a \in E$.

Sehingga $a + (-a) = 2k_1 + (-2k_1)$

$= (-2k_1) + 2k_1$

$= (-a) + a$

$= 0$

iv) Untuk semua $a, b \in E$, misalkan $a = 2k_1$ dan $b = 2k_2$ dengan $k_1, k_2 \in \mathbb{Z}$, maka berlaku:

$a + b = 2k_1 + 2k_2$ [$2k_1, 2k_2 \in \mathbb{Z}$]

$= 2k_2 + 2k_1$ [sifat komutatif penjumlahan di $\mathbb{Z}$]

$= b + a$

b) $(E,\times)$ memenuhi sifat asosiatif. Untuk semua $a, b, c \in E$, misalkan $a = 2k_1$, $b = 2k_2$ dan $c = 2k_3$, dimana $k_1, k_2, k_3 \in \mathbb{Z}$, berlaku:

$a(bc) = 2k_1(2k_2 2k_3)$ [$2k_1, 2k_2, 2k_3 \in \mathbb{Z}$]

$= (2k_1 2k_2)2k_3$ [sifat asosiatif perkalian di $\mathbb{Z}$]

$= (ab)c$

c) Dalil distributif berlaku di E. Untuk semua $a, b, c \in E$, misalkan $a = 2k_1$, $b = 2k_2$ dan $c = 2k_3$, dimana $k_1, k_2, k_3 \in \mathbb{Z}$, berlaku:

$a(b + c) = 2k_1(2k_2 + 2k_3) = 2k_1 2k_2 + 2k_1 2k_3 = ab + ac$.

$(a + b)c = (2k_1 + 2k_2)2k_3 = 2k_1 2k_3 + 2k_2 2k_3 = ac + bc$.

d) E tidak memuuat unsur kesatuan. Misalkan $a = 2k_1 \in E$ dimana $k_1 \in \mathbb{Z}$. Andaikan terdapat $b \in E$ sebagai unsur kesatuan dimana $b = 2k_2$ untuk $k_2 \in \mathbb{Z}$, maka $ab = ba = a$. Faktanya:

$$ab = 2k_1 2k_2 \neq 2k_1.$$

Pengandaian salah, jadi tidak ada unsur kesatuan di E.

2.2.4 Definisi Lapangan

Ring R dengan unsur kesatuan, dimana $1 \neq 0$, disebut *division ring* (atau *skew field*) jika setiap unsur tak nol $a \in R$ mempunyai invers perkalian, artinya ada $b \in R$ sedemikian hingga $ab = ba = 1$. *Division ring* yang komutatif disebut lapangan (Dummit dan Foote, 1991:226).

Jika definisi lapangan di atas dituliskan secara terpisah, maka redaksinya adalah: Ring komutatif R dengan unsur kesatuan, dimana $1 \neq 0$, disebut lapangan jika setiap unsur tak nol $a \in R$ mempunyai invers perkalian, artinya ada $b \in R$ sedemikian hingga $ab = ba = 1$.

Contoh 2.10

1. $(\mathbb{R}, +, \times)$ merupakan lapangan.

   a) $(\mathbb{R}, +)$ merupakan grup komutatif, karena memenuhi:

      i) Sifat asosiatif. Untuk setiap $a, b, c \in \mathbb{R}$ berlaku $a + (b + c) = (a + b) + c$.

      ii) Terdapat $0 \in \mathbb{R}$ sebagai unsur identitas penjumlahan di $\mathbb{R}$, sedemikian hingga untuk semua $a \in \mathbb{R}$ berlaku $a + 0 = 0 + a = a$.

      iii) Untuk setiap $a \in \mathbb{R}$ selalu terdapat invers penjumlahannya, yaitu $-a \in \mathbb{R}$, sehingga memenuhi $a + (-a) = (-a) + a = 0$.

iv) Untuk semua $a, b \in \mathbb{R}$ berlaku $a + b = b + a$.

b) $(\mathbb{R},\times)$ bersifat asosiatif. Untuk setiap $a, b, c \in \mathbb{R}$ berlaku $a(bc) = (ab)c$.

c) Dalil distributif berlaku di $\mathbb{R}$. Untuk setiap $a, b, c \in \mathbb{R}$ berlaku: $a(b + c) = ab + ac$ dan $(a + b)c = ac + bc$.

d) $(\mathbb{R},\times)$ memenuhi sifat komutatif. Untuk setiap $a, b \in \mathbb{R}$ berlaku $ab = ba$.

e) Terdapat $1 \in \mathbb{R}$ sebagai unsur identitas perkalian di $\mathbb{R}$, sedemikian hingga untuk setiap $a \in \mathbb{R}$ berlaku $a1 = 1a = a$.

f) $1 \neq 0$.

g) Untuk setiap unsur tak nol $a \in \mathbb{R}$ selalu terdapat invers perkaliannya, yaitu $a^{-1} = \frac{1}{a} \in \mathbb{R}$, sehingga memenuhi $aa^{-1} = a^{-1}a = 1$.

2. Daerah integral $(\mathbb{Z}, +,\times)$ bukan merupakan lapangan. Karena ada $3 \in \mathbb{Z}$, sedangkan $3^{-1} = \frac{1}{3} \notin \mathbb{Z}$.

2.2.5 Definisi Pembagi Nol

Misalkan R adalah ring. Unsur tak nol a di R disebut pembagi nol jika ada unsur tak nol b di R sedemikian hingga memenuhi salah satu dari $ab = 0$ ataupun $ba = 0$ (Dummit dan Foote, 1991:228).

2.2.6 Definisi Daerah Integral

Ring komutatif dengan unsur kesatuan $1 \neq 0$ disebut daerah integral jika tidak memuat pembagi nol (Dummit dan Foote, 1991:229).

Contoh 2.11

1. Ring komutatif dengan unsur kesatuan $(\mathbb{Z}, +,\times)$ merupakan daerah integral. Unsur kesatuan itu $1 \neq 0$. Ring $\mathbb{Z}$ tidak memuat pembagi nol, karena perkalian

dua unsur tak nol di $\mathbb{Z}$ selalu tidak pernah menghasilkan nol, artinya untuk setiap $a, b \in \mathbb{Z}$, jika $a \neq 0$ dan $ab = 0$ maka $b = 0$.

2. Untuk $M = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| a, b, c, d \in \mathbb{R} \right\}$ maka ring $(M, +, \times)$ bukan merupakan daerah integral, karena $(M, +, \times)$ memuat pembagi nol. $\begin{bmatrix} 1 & 0 \\ 2 & 0 \end{bmatrix} \in M$ dimana $\begin{bmatrix} 1 & 0 \\ 2 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, unsur $\begin{bmatrix} 1 & 0 \\ 2 & 0 \end{bmatrix}$ adalah pembagi nol di M karena ada $\begin{bmatrix} 0 & 0 \\ 1 & 2 \end{bmatrix} \in M$ dimana $\begin{bmatrix} 0 & 0 \\ 1 & 2 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ sedemikian hingga $\begin{bmatrix} 1 & 0 \\ 2 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

Teorema 2.1

Misalkan R adalah ring, maka:

1. $0a = a0 = 0$ untuk semua $a \in R$.
2. $(-a)b = a(-b) = -(ab)$ untuk semua $a, b \in R$.

(Dummit dan Foote, 1991:228).

Bukti

1.

$0a = (0 + 0)a$	$[0a \in R]$
$0a = 0a + 0a$	[sifat distributif di R]
$0a + (-0a) = (0a + 0a) + (-0a)$	$[-0a \in R]$
$0 = 0a + \big(0a + (-0a)\big)$	[sifat asosiatif di R]
$0 = 0a + 0$	[sifat invers penjumlahan di R]
$0 = 0a$	[sifat identitas penjumlahan di R]

2. $ab + (-a)b = \big(a + (-a)\big)b = 0b = 0$,

   sedangkan $ab + a(-b) = a\big(b + (-b)\big) = a0 = 0$.

   Jadi $(-a)b = a(-b) = -(ab)$.

Teorema 2.2

Asumsikan a, b dan c adalah unsur dari sembarang ring dengan a bukan pembagi nol. Jika $ab = ac$, maka berlaku salah satu dari $a = 0$ atau $b = c$ (dengan kata lain jika $a \neq 0$ maka a bisa dikansel). Dalam hal ini, jika a, b, c adalah sembarang unsur di daerah integral dan $ab = ac$, maka berlaku salah satu dari $a = 0$ atau $b = c$ (Dummit dan Foote, 1991:229).

Bukti

$$ab = ac$$

$$ab + \left(a(-c)\right) = ac + (-ac) \qquad [a(-c) = -ac]$$

$$a(b - c) = 0 \qquad \text{[sifat invers penjumlahan di daerah integral]}$$

Karena a, b, c adalah unsur di daerah integral (tidak memuat pembagi nol), maka berlaku salah satu dari $a \neq 0$ sehingga $b - c = 0$, atau $b - c \neq 0$ sehingga $a = 0$.

2.2.7 Definisi Unit

Misalkan R adalah ring dengan unsur kesatuan $1 \neq 0$. Unsur u di R disebut unit di R jika terdapat suatu v di R sedemikian hingga $uv = vu = 1$. Himpunan unit-unit di R dinotasikan $R^{\times}$ (Dummit dan Foote, 1991:228).

Corollary 2.1

Setiap unsur tak nol di lapangan F adalah unit (Dummit dan Foote, 1991:228).

Bukti

Lapangan F adalah ring komutatif F yang memuat unsur kesatuan $1 \neq 0$. Untuk setiap unsur tak nol $a \in F$ selalu ada $b \neq 0$ di F dimana $ab = ba = 1$. Jadi, setiap unsur tak nol di F adalah unit, $F^{\times} = F - \{0\}$.

Corollary 2.2

Misalkan R adalah ring. Pembagi nol di R bukanlah unit (Dummit dan Foote, 1991:228).

Bukti

Andaikan a adalah unit di R. Jika a adalah pembagi nol di R, akan ditunjukkan ada unsur tak nol $b \in R$ yang memenuhi $ab = 0$ ataupun $ba = 0$.

a adalah unit di R, artinya terdapat $va = 1$ untuk $v \in R$. Selanjutnya $b = 1b = (va)b = v(ab) = v0 = 0$, kontradiktif dengan $b \neq 0$.

Selain itu, terdapat $av = 1$ untuk $v \in R$. Selanjutnya $b = b1 = b(av) = (ba)v = 0v = 0$, juga kontradiktif dengan $b \neq 0$.

Jadi, jika $ab = 0$ ataupun $ba = 0$ untuk $b \neq 0$, maka a bukan unit. Sehingga, sembarang lapangan F tidak memuat pembagi nol.

Teorema 2.3

Sembarang daerah integral terhingga adalah lapangan (Raisinghania dan Aggarwal, 1980:328).

Bukti

Daerah integral adalah ring komutatif dengan unsur kesatuan $1 \neq 0$ dan tak memuat pembagi nol. Lapangan adalah ring komutatif dengan unsur kesatuan $1 \neq 0$ dimana setiap unsur tak nol mempunyai invers perkalian. Untuk membuktikan teorema ini, cukup ditunjukkan bahwa di daerah integral terhingga, setiap unsur tak nol mempunyai invers perkalian.

Misalkan D adalah daerah integral dengan banyak unsur terhingga n. Misalkan a adalah sembarang unsur tak nol di D.

Ambil sebuah himpunan $D^* = \{ax |\ x \in D$ dan $x \neq 0\}$.

Maka dengan sifat ketertutupan pada perkalian di D, berakibat setiap unsur di D^* adalah unsur di D dan karena D adalah ring tanpa pembagi nol, maka kanselasi berlaku di D.

Konsekuensinya, $ax = ay$ dan $a \neq 0$ maka $x = y$. Ini menunjukkan bahwa semua unsur di D^* adalah unsur yang berbeda dari D, oleh karena itu D^* memuat semua unsur tak nol sebanyak $(n-1)$ unsur di D. Karena 1 (identitas perkalian) pasti merupakan salah satu dari $(n-1)$ unsur di D, maka: $ax = 1$ untuk semua $x \in D$, dimana $x \neq 0$. Akibatnya $a^{-1} = x$. Sehingga setiap unsur tak nol di D mempunyai invers perkalian di D. Karena itu, D merupakan lapangan.

2.2.8 Definisi Subring

Subring dari ring R adalah subgrup dari R yang tertutup pada perkalian. Dengan kata lain, subhimpunan S dari ring R adalah subring jika operasi penjumlahan dan perkalian di R berlaku untuk S, membentuk struktur ring S. Untuk menunjukkan bahwa subhimpunan dari ring R adalah subring, cukup dengan memeriksa bahwa subhimpunan itu tidak kosong dan tertutup pada pengurangan dan perkalian (Dummit dan Foote, 1991:230).

Contoh 2.12

Untuk $E = \{2k | k \in \mathbb{Z}\}$, struktur aljabar $(E, +, \times)$ adalah subring dari ring $(\mathbb{Z}, +, \times)$. Jelas bahwa E subhimpunan dari $\mathbb{Z}$, dan E tidak kosong. Akan ditunjukkan bahwa E tertutup pada pengurangan (invers penjumlahan) dan perkalian. Ambil $a, b \in E$ dimana $a = 2k_1$ dan $b = 2k_2$ untuk suatu $k_1, k_2 \in \mathbb{Z}$. $a - b = 2k_1 - 2k_2 = 2(k_1 - k_2) \in E$, dimana $(k_1 - k_2) \in \mathbb{Z}$. Selanjutnya, $ab = (2k_1)(2k_2) = 2(2k_1k_2) \in E$, dimana $2k_1k_2 \in \mathbb{Z}$.

2.3.1 Definisi Keterbagian

Misalkan R ring komutatif dan $a, b \in R$ dengan $b \neq 0$. Unsur a disebut kelipatan dari b jika ada unsur $x \in R$ dengan $a = bx$. Dalam hal ini b disebut membagi a, atau pembagi dari a, ditulis $b|a$ (Dummit dan Foote, 1991:273).

Jika tidak ada $x \in R$ yang memenuhi $a = bx$, maka dikatakan b tidak membagi a, ditulis $b \nmid a$.

Contoh 2.13

$(\mathbb{Z}, +, \times)$ adalah ring komutatif. Dikatakan $3|6$, karena ada 2 di $\mathbb{Z}$ sehingga $6 = (3)(2)$. Sedangkan $3 \nmid 5$, karena tidak ada $x \in \mathbb{Z}$ yang memenuhi $5 = 3x$.

2.3.2 Definisi FPB

Misalkan R ring komutatif dan $a, b \in R$ dengan $b \neq 0$. Faktor persekutuan terbesar dari a dan b adalah unsur tak nol d sedemikian hingga:

(i) $d|a$ dan $d|b$, dan

(ii) Jika $d'|a$ dan $d'|b$ maka $d'|d$.

Faktor persekutuan terbesar dari a dan b selanjutnya dinotasikan (a, b).

(Dummit dan Foote, 1991:273).

Contoh 2.14

Pada daerah integral $\mathbb{Z}$, faktor dari $4 = \{\pm 1, \pm 2, \pm 4\}$, dan $6 = \{\pm 1, \pm 2, \pm 3, \pm 6\}$. Sehingga faktor persekutuan dari 4 dan 6 adalah $\{\pm 1, \pm 2\}$. Jadi FPB $(4, 6) = \{\pm 2\}$.

2.3.3 Definisi KPK

Misalkan R ring komutatif dengan unsur kesatuan 1, misalkan a dan b unsur tak nol di R. Kelipatan persekutuan terkecil dari a dan b adalah unsur e di R sedemikian hingga:

(i) $a|e$ dan $b|e$, dan

(ii) Jika $a|e'$ dan $b|e'$ maka $e|e'$.

(Dummit dan Foote, 1991:278).

Kelipatan persekutuan terkecil dari a dan b selanjutnya ditulis KPK (a, b).

Contoh 2.15

Pada daerah integral $\mathbb{Z}$, kelipatan dari $2 = \{\pm 2, \pm 4, \pm 6, \pm 8, \pm 10, \pm 12, \ldots\}$, dan $3 = \{\pm 3, \pm 6, \pm 9, \pm 12, \ldots\}$. Kelipatan persekutuan dari 2 dan 3 adalah $\{\pm 6, \pm 12, \ldots\}$. Jadi KPK dari 2 dan 3 adalah $\{\pm 6\}$.

2.3 Ideal

2.3.4 Definisi Ideal

Misalkan R adalah ring, I adalah subhimpunan dari R, dan $r \in R$.

1. $rI = \{ra |\ a \in I\}$ dan $Ir = \{ar |\ a \in I\}$.
2. Subhimpunan I dari R adalah ideal kiri dari R jika

   (i) I adalah subring dari R, dan

(ii) I tertutup pada perkalian kiri dengan unsur-unsur di R, dengan kata lain $rI \subseteq I$ untuk semua $r \in R$.

Dengan cara yang sama I adalah ideal kanan jika (i) berlaku dan syarat (ii) diganti dengan

(ii)' I tertutup pada perkalian kanan dengan unsur-unsur di R, dengan kata lain $Ir \subseteq I$ untuk semua $r \in R$.

3. Subhimpunan I yang merupakan ideal kiri dan ideal kanan disebut ideal (atau, untuk menambahkan penekanan, disebut ideal dua sisi) dari R.

(Dummit dan Foote, 1991:242).

Untuk membuktikan bahwa subset I dari ring R adalah ideal cukup dengan membuktikan bahwa I tak kosong, tertutup pada pengurangan dan tertutup pada perkalian dengan semua unsur di R (dan tidak hanya dengan unsur di I).

(Dummit dan Foote, 1991:242)

Contoh 2.16

Misalkan n adalah bilangan bulat positif. Akan ditunjukkan bahwa $n\mathbb{Z}$ adalah ideal dari ring $\mathbb{Z}$.

Jelas bahwa $n\mathbb{Z}$ adalah subhimpunan dari $\mathbb{Z}$, dan $n\mathbb{Z}$ tak kosong.

a) Akan ditunjukkan $a - b \in n\mathbb{Z}$ untuk semua $a, b \in n\mathbb{Z}$

Ambil $a, b \in n\mathbb{Z}$ dimana $a = nm$ dan $b = np$ untuk suatu $m, p \in \mathbb{Z}$

$a - b = nm - np = n(m - p) \in n\mathbb{Z}$

b) Akan ditunjukkan $ar \in n\mathbb{Z}$ dan $ra \in n\mathbb{Z}$ untuk semua $a \in n\mathbb{Z}$ dan $r \in \mathbb{Z}$

Ambil $a \in n\mathbb{Z}$ dimana $a = nm$ untuk suatu $m \in \mathbb{Z}$

(i) $ra = r(nm) = n(rm) \in n\mathbb{Z}$ [ideal kiri]

(ii) $ar = (nm)r = n(mr) \in n\mathbb{Z}$ [ideal kanan]

Terbukti bahwa $n\mathbb{Z}$ adalah ideal dari ring $\mathbb{Z}$.

2.3.5 Definisi Ideal Utama

Misalkan R adalah ring dengan unsur kesatuan $1 \neq 0$. Misalkan A adalah subhimpunan dari ring R.

1. Misalkan $\langle A \rangle$ merupakan ideal terkecil dari R yang memuat A, selanjutnya $\langle A \rangle$ disebut ideal yang dibangun oleh A.
2. Misalkan RA merupakan himpunan dari semua penjumlahan terhingga unsur-unsur dari bentuk ra dengan $r \in R$ dan $a \in A$, artinya $RA = \{r_1 a_1 + r_2 a_2 + \cdots + r_n a_n \mid r_i \in R, a_i \in A, n \in \mathbb{Z}^+\}$ (dimana $RA = 0$ jika $A \neq \emptyset$).
3. Dengan cara yang sama, $AR = \{a_1 r_1 + a_2 r_2 + \cdots + a_n r_n \mid r_i \in R, a_i \in A, n \in \mathbb{Z}^+\}$ dan $RAR = \{r_1 a_1 r_1' + r_2 a_2 r_2' + \cdots + r_n a_n r_n' \mid r_i, r_i' \in R, a_i \in A, n \in \mathbb{Z}^+\}$.
4. Ideal yang dibangun oleh satu (tunggal) unsur disebut ideal utama.
5. Ideal yang dibangun oleh himpunan terhingga disebut *finitely generated ideal*.

(Dummit dan Foote, 1991:250).

Jika a dan b adalah unsur tak nol di ring komutatif R sedemikian hingga sebuah ideal dibangun oleh a dan b adalah ideal utama $\langle d \rangle$, maka d adalah faktor persekuatuan terbesar dari a dan b (Dummit dan Foote, 1991:274).

Perlu dipertegas bahwa arti notasi $\langle a \rangle = \langle b \rangle$ berbeda dengan $\langle a, b \rangle$. Notasi pertama, $\langle a \rangle = \langle b \rangle$ bermakna bahwa secara tunggal (berdiri sendiri) unsur a

membangun sebuah ideal yang sama dengan ideal yang dibangun oleh unsur b. Notasi kedua, $\langle a, b\rangle$ bermakna unsur a dan b bersama-sama (berpasangan) membangun suatu ideal.

Contoh 2.17

Contoh 2.15 menjamin bahwa $2\mathbb{Z} = \{2n | n \in \mathbb{Z}\} = \{0, \pm 2, \pm 4, \dots\}$ adalah ideal dari $\mathbb{Z}$. Faktanya, $(-2)\mathbb{Z} = \{-2n | n \in \mathbb{Z}\} = \{0, \pm 2, \pm 4, \dots\}$, yaitu $2\mathbb{Z} = (-2)\mathbb{Z}$. Artinya ideal $\{0, \pm 2, \pm 4, \dots\} = 2\mathbb{Z} = (-2)\mathbb{Z} = \langle 2\rangle = \langle -2\rangle$ karena pembangkitnya selalu tunggal, maka ideal itu disebut ideal utama.

2.3.6 Definisi Ideal Prima

Asumsikan R ring komutatif. Suatu ideal P disebut ideal prima jika $P \neq R$ dan bila hasil perkalian ab dari dua unsur $a, b \in R$ adalah unsur di P, maka sedikitnya satu dari a dan b adalah unsur di P (Dummit dan Foote, 1991:254).

Contoh 2.18

1. $5\mathbb{Z}$ adalah ideal prima dari $\mathbb{Z}$.

   $5\mathbb{Z} = \{5n |\ n \in \mathbb{Z}\} = \{0, \pm 5, \pm 10, \pm 15, \dots\}$, jadi $5\mathbb{Z} \neq \mathbb{Z}$.

   Ambil $a, b \in \mathbb{Z}$ dan $ab \in 5\mathbb{Z}$, maka $ab = 5n$. Karena $n \in \mathbb{Z}$ maka n dapat dinyatakan sebagai $n = pq$ untuk semua $p, q \in \mathbb{Z}$. Sehingga $ab = 5n = 5(pq) = (5p)(q)$ dan $5p \in 5\mathbb{Z}$. Karena $q \in \mathbb{Z}$ maka ada q yang merupakan unsur di $5\mathbb{Z}$.

2. $6\mathbb{Z}$ adalah ideal dari $\mathbb{Z}$, tetapi $6\mathbb{Z}$ bukan ideal prima.

   Misalkan $6\mathbb{Z} = \{6n |\ n \in \mathbb{Z}\}$. Ambil $a, b \in \mathbb{Z}$ dan $ab \in 6\mathbb{Z}$, maka $ab = 6n$. Jika $n \in \mathbb{Z}$ maka n bisa dinyatakan sebagai $n = pq$ untuk semua $p, q \in \mathbb{Z}$. Sehingga $ab = 6n = 6(pq) = (2p)(3q)$. Jadi ada $ab \in 6\mathbb{Z}$ dimana $a, b \notin 6\mathbb{Z}$.

2.3.7 Definisi Daerah Ideal Utama

Daerah ideal utama adalah daerah integral yang setiap idealnya adalah ideal utama (Dummit dan Foote, 1991:279).

Contoh 2.19

$(\mathbb{Z}, +, \times)$ adalah daerah ideal utama. Untuk suatu $m \in \mathbb{Z}$, terdapat $m\mathbb{Z} = (-m)\mathbb{Z}$. Contoh 2.15 menunjukkan bahwa setiap $m\mathbb{Z}$ merupakan ideal dari ring $\mathbb{Z}$.

Ideal $m\mathbb{Z} = (-m)\mathbb{Z} = \langle m \rangle = \langle -m \rangle$. Karena setiap ideal $m\mathbb{Z}$ yang dibangun oleh unsur tunggal m adalah ideal utama, maka daerah integral $(\mathbb{Z}, +, \times)$ adalah daerah ideal utama.

Teorema 2.4

Di daerah ideal utama setiap pasangan unsurnya selalu mempunyai FPB (Raisinghania dan Aggarwal, 1980:402).

Bukti

Misalkan a dan b sembarang dua unsur tak nol di daerah ideal utama D dan misal $\langle a \rangle$ dan $\langle b \rangle$ masing-masing menunjukkan ideal utama yang dibangun oleh a dan b. Karena penjumlahan dua ideal menghasilkan ideal, $\langle a \rangle + \langle b \rangle$ adalah ideal.

Karena D daerah ideal utama, maka selalu terdapat ideal utama yang dibangun oleh unsur tak nol d, sedemikian hingga $\langle a \rangle + \langle b \rangle = \langle d \rangle$.

Asumsikan $d =$ FPB (a, b), karena $\langle a \rangle + \langle b \rangle = \langle d \rangle$ maka $\langle a \rangle \subset \langle d \rangle$ dan $\langle b \rangle \subset \langle d \rangle$. Jika $\langle a \rangle \subset \langle d \rangle$, maka $a \subset \langle d \rangle$ dan $a = dx$ untuk beberapa $x \in D$, akibatnya $d|a$. Jika $\langle b \rangle \subset \langle d \rangle$, maka $b \subset \langle d \rangle$ dan $b = dy$ untuk beberapa $y \in D$, akibatnya $d|b$. Karena $d|a$ dan $d|b$, maka $d =$ FPB (a, b).

Misalkan ada lagi FPB dari a dan b, yaitu e. Maka $e|a$ dan $e|b$ sehingga $a = em_1$ dan $b = em_2$ diman $m_1, m_2 \in D$. Akibatnya:

$x \in \langle a \rangle \Rightarrow x = ax_1$ untuk beberapa $x_1 \in D$

$\Rightarrow x = (em_1)x_1$

$\Rightarrow x = e(m_1 x_1)$

$\Rightarrow x \subset \langle e \rangle$, jadi $\langle a \rangle \subset \langle e \rangle$.

Selanjutnya,

$y \in \langle b \rangle \Rightarrow y = by_1$ untuk beberapa $y_1 \in D$

$\Rightarrow y = (em_2)y_1$

$\Rightarrow y = e(m_2 y_1)$

$\Rightarrow y \subset \langle e \rangle$, jadi $\langle b \rangle \subset \langle e \rangle$.

Karena $e|a$ dan $e|b$, maka $\langle a \rangle \subset \langle e \rangle$ dan $\langle b \rangle \subset \langle e \rangle$ sehingga$\langle d \rangle = \langle a \rangle + \langle b \rangle$ dan $\langle d \rangle \subset \langle e \rangle$. Jelas, $d \subset \langle e \rangle$ sedemikian hingga $d = ex$ untuk beberapa $x \in D$. dan $e|d$.

Terbukti $d =$ FPB (a, b), karena setiap faktor persekutuan dari a dan b selalu merupakan pembagi (faktor) dari d.

Teorema 2.5

Di daerah ideal utama setiap pasangan unsurnya selalu mempunyai KPK (Raisinghania dan Aggarwal, 1980:404).

Bukti

Misalkan a dan b sembarang dua unsur tak nol di daerah ideal utama D dan misal $\langle a \rangle$ dan $\langle b \rangle$ masing-masing menunjukkan ideal utama yang dibangun oleh a dan b. Karena irisan dari dua ideal juga adalah ideal, $\langle a \rangle \cap \langle b \rangle$ adalah ideal utama dari D, sedemikian hingga terdapat unsur e di D sedemikian hingga $\langle a\rangle \cap \langle b\rangle = \langle e\rangle$.

Asumsikan $e =$ KPK (a, b), karena $\langle a\rangle \cap \langle b\rangle = \langle e\rangle$ maka $\langle e\rangle \subset \langle a\rangle$ dan $\langle e\rangle \subset \langle b\rangle$. Jika $a \subset \langle d\rangle$ dan $b \subset \langle d\rangle$, maka $e = ax$ dan $e = by$ untuk beberapa $x, y \in D$. Akibatnya $a|e$ dan $b|e$.

Misalkan ada lagi KPK dari a dan b, yaitu n. Maka $a|n$ dan $b|n$ sehingga $n = am_1$ dan $n = bm_2$ diman $m_1, m_2 \in D$. Akibatnya:

$x \in \langle n\rangle \Rightarrow x = nx_1$ untuk beberapa $x_1 \in D$

$\Rightarrow x = (am_1)x_1$

$\Rightarrow x = a(m_1x_1)$

$\Rightarrow x \subset \langle a\rangle$, jadi $\langle n\rangle \subset \langle a\rangle$.

Selanjutnya,

$y \in \langle n\rangle \Rightarrow y = ny_1$ untuk beberapa $y_1 \in D$

$\Rightarrow y = (bm_2)y_1$

$\Rightarrow y = b(m_2y_1)$

$\Rightarrow y \subset \langle b\rangle$, jadi $\langle n\rangle \subset \langle b\rangle$.

Karena $\langle n\rangle \subset \langle a\rangle$ dan $\langle n\rangle \subset \langle b\rangle$, maka $\langle n\rangle \subset \{\langle a\rangle \cap \langle b\rangle\} = \langle e\rangle$. Sehingga, $\langle n\rangle \subset \langle e\rangle$ dan $n \in \langle e\rangle$ sedemikian hingga $n = ek$ untuk beberapa $k \in D$. Jadi, $e|n$.

Terbukti $e =$ KPK (a, b), karena setiap kelipatan persekutuan dari a dan b selalu merupakan kelipatan dari e.

2.4 Daerah Faktorisasi Tunggal

2.4.1 Definisi Kesekawanan

Misalkan D adalah daerah integral. Dua unsur a dan b di D disebut sekawan di D jika dua unsur itu berbeda pada unit. Dengan kata lain, $a = ub$ untuk beberapa unit u di D (Dummit dan Foote, 1991:282).

Bentuk $a = ub$ berarti $b|a$. Karena u adalah invertibel maka $u^{-1}a = b$, yang berarti $a|b$. Selanjutnya dua unsur tak nol a dan b sekawan di D, ditulis $a \sim b \Leftrightarrow a|b$ dan $b|a$.

Contoh 2.20

1. Di daerah integral $\mathbb{Z}$, $-2 \sim 2$ karena $-2|2$ dan $2|-2$.
2. Di daerah integral $\mathbb{Z}$, $2 \nsim 4$ karena $2|4$ tetapi $4 \nmid 2$.

2.4.2 Definisi Unsur Tereduksi dan Tak Tereduksi

Misalkan D adalah daerah integral. Misalkan $d \in D$ adalah unsur tak nol dan bukan unit. Maka d dikatakan tak tereduksi di D jika $d = ab$ dengan $a, b \in D$, sedikitnya satu dari a atau b harus merupakan unit di d. Jika sebaliknya, d dikatakan tereduksi (Dummit dan Foote, 1991:282).

Dengan kata lain, d disebut tereduksi jika ada $a, b \in D$ dan $a, b \notin D^{\times}$.

Contoh 2.21

Himpunan unit di daerah integral $\mathbb{Z}$ adalah $\mathbb{Z}^{\times} = \{\pm 1\}$.

1. 7 merupakan unsur tak tereduksi di $\mathbb{Z}$, karena $7 = (1)(7) = (-1)(-7)$. Faktanya, salah satu unsur dari pasangan perkalian itu adalah unit.
2. 6 merupakan unsur tereduksi di $\mathbb{Z}$, karena 6 bisa dinyatakan dalam perkalian dua unsur yang bukan unit, yaitu $6 = (2)(3)$.

2.4.3 Definisi Unsur Prima

Misalkan D adalah daerah integral. Unsur tak nol $p \in D$ disebut prima di D jika ideal $\langle p \rangle$ yang dibangun oleh p adalah ideal prima. Dengan kata lain, unsur tak nol p adalah prima jika bukan unit dan ketika $p|ab$ untuk sembarang $a, b \in D$, maka berlaku salah satu dari $p|a$ atau $p|b$ (Dummit dan Foote, 1991:282).

Contoh 2.22

1. 5 merupakan unsur prima di $\mathbb{Z}$. Contoh 2.18 menunjukkan bahwa ideal $5\mathbb{Z} = \langle 5 \rangle$ adalah ideal prima yang dibangun oleh 5.
2. 6 bukan merupakan unsur prima di $\mathbb{Z}$. Contoh 2.18 menunjukkan bahwa ideal $6\mathbb{Z} = \langle 6 \rangle$ merupakan ideal yang dibangun oleh 6, tetapi ideal $\langle 6 \rangle$ bukan ideal utama.

2.4.4 Definisi Daerah Faktorisasi Tunggal

Daerah integral D disebut daerah faktorisasi tunggal (DFT) jika setiap unsur di D yang bukan nol memenuhi salah satu dari aksioma berikut:

1. Merupakan unit,
2. Dapat dinyatakan secara tunggal sebagai hasil kali sejumlah terhingga unsur-unsur prima di D. Dikatakan tunggal adalah jika semua hasil kalinya hanya berbeda dalam urutan atau pada unsur sekawannya.

(Raisinghania dan Aggarwal, 1980:405).

Contoh 2.23

1. Bilangan 6 di $\mathbb{Z}$ dapat dinyatakan dalam perkalian faktor-faktor primanya sebagaimana berikut:

   $6 = (2)(3)$

$= (3)(2)$

$= (-2)(-3)$

$= (-3)(-2)$

Perhatikan bahwa semua hasil kalinya hanya berbeda dalam urutan atau unsur sekawannya, sehingga disebut hasil kali yang tunggal.

2. Bilangan 12 di $\mathbb{Z}$ bisa dinyatakan dalam perkalian faktor-faktor primanya sebagaimana berikut:

$12 = (2)(2)(3)$

$= (2)(3)(2)$

$= (3)(2)(2)$

$= (-2)(-2)(3)$

$= (-2)(2)(-3)$

$= (2)(-2)(-3)$

$= (-2)(-3)(2)$

$= (-2)(3)(-2)$

$= (2)(-3)(-2)$

$= (-3)(-2)(2)$

$= (-3)(2)(-2)$

$= (3)(-2)(-2)$

Perhatikan bahwa semua hasil kalinya hanya berbeda dalam urutan atau unsur sekawannya, sehingga disebut hasil kali yang tunggal.

3. Daerah integral $\mathbb{Z}$ merupakan DFT, karena setiap unsur di $\mathbb{Z}$ selain $-1, 0, 1$ bisa dinyatakan secara tunggal sebagai hasil kali dari sejumlah terhingga unsur prima di $\mathbb{Z}$.

2.5 Ring $\mathbb{Z}_p$

Sebelum membahas himpunan $\mathbb{Z}_p$, terlebih dahulu akan diberikan definisi mengenai kelas kongruensi modulo.

2.5.1 Definisi Kelas Kongruensi Modulo

Untuk sembarang $k \in \mathbb{Z}$ dinotasikan kelas ekivalen dari a, sebagai $\bar{a}$. Selanjutnya $\bar{a}$ disebut kelas kongruensi dari a mod n dan memuat bilangan bulat yang berbeda dengan a oleh kelipatan dari n, dengan kata lain:

$$\bar{a} = \{nk + a | k \in \mathbb{Z}\}$$
$$= \{a, a \pm n, a \pm 2n, a \pm 3n, \dots\}$$

(Dummit dan Foote, 1991:8).

Arifin (2000:29) menyampaikan bahwa himpunan semua kelas kongruensi modulo n ditandai dengan $\mathbb{Z}_n = \{\bar{a} | \ a \in \mathbb{Z}\}$. Adapun Bhattacharya dkk (1995:12) menyatakan bahwa $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{(n-1)}\}$.

Contoh 2.23

$\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ mempunyai unsur-unsur:

$\bar{0} = \{\dots, -8, -4, 0, 4, 8, \dots\}$

$\bar{1} = \{\dots, -7, -3, 1, 5, 9, \dots\}$

$\bar{2} = \{\dots, -6, -2, 2, 6, 10, \dots\}$

$\bar{3} = \{\dots, -5, -1, 3, 7, 11, \dots\}$

2.5.2 Definisi Operasi Tambah dan Operasi Kali pada $\mathbb{Z}_n$

Operasi tambah dan operasi kali pada $\mathbb{Z}_n$ berturut-turut adalah pemetaan $+: \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ yang didefinisikan oleh pengaitan

$$+: (\bar{a}, \bar{b}) \mapsto \bar{a} + \bar{b} = \overline{a+b},$$

dan pemetaan $\times: \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ yang didefinisikan oleh pengaitan

$$\times: (\bar{a}, \bar{b}) \mapsto \bar{a}\bar{b} = \overline{ab},$$

untuk semua $\bar{a}, \bar{b} \in \mathbb{Z}_n$,

(Arifin, 2000:29).

Contoh 2.24

1. Hasil operasi tambah dan kali setiap unsur di $\mathbb{Z}_4$ dinyatakan sebagai berikut.

Tabel 2.1: Tabel Penjumlahan dan Perkalian Unsur-unsur di $\mathbb{Z}_4$

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$\times$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

2. Sistem matematika $(\mathbb{Z}_n, +, \times)$ dengan n bilangan asli adalah ring komutatif dengan unsur kesatuan.
   a) Akan ditunjukkan bahwa $(\mathbb{Z}_n, +)$ adalah grup komutatif, karena memenuhi:
      i) Sifat asosiatif. $\forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$ berlaku:

$\bar{a} + (\bar{b} + \bar{c}) = \bar{a} + \overline{b+c}$ [definisi penjumlahan di $\mathbb{Z}_n$]

$= \overline{a(b+c)}$ [definisi penjumlahan di $\mathbb{Z}_n$]

$= \overline{(a+b)+c}$ [sifat asosiatif penjumlahan di $\mathbb{Z}$]

$= \overline{a+b} + \bar{c}$ [definisi penjumlahan di $\mathbb{Z}_n$]

$= (\bar{a} + \bar{b}) + \bar{c}$ [definisi penjumlahan di $\mathbb{Z}_n$]

ii) Terdapat $\bar{0} \in \mathbb{Z}_n$ sebagai unsur identitas penjumlahan di $\mathbb{Z}_n$, sehingga untuk semua $a \in \mathbb{Z}_n$, berlaku $\bar{a} + \bar{0} = \bar{0} + \bar{a} = \bar{a}$.

iii) Untuk setiap $\bar{a} \in \mathbb{Z}_n$ terdapat invers penjumlahan $\bar{a}$ yaitu $\overline{n-a} \in \mathbb{Z}_n$ yang memenuhi $\bar{a} + \overline{n-a} = \overline{n-a} + \bar{a} = \bar{0}$.

iv) Memenuhi sifat komutatif. $\forall \bar{a}, \bar{b} \in \mathbb{Z}_n$ berlaku:

$\bar{a} + \bar{b} = \overline{a+b}$ [definisi penjumlahan di $\mathbb{Z}_n$]

$= \overline{b+a}$ [sifat komutatif penjumlahan di $\mathbb{Z}$]

$= \bar{b} + \bar{a}$ [definisi penjumlahan di $\mathbb{Z}_n$]

b) Akan ditunjukkan bahwa $(\mathbb{Z}_n, \times)$ memenuhi sifat asosiatif. $\forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$ berlaku:

$\bar{a}(\bar{b}\bar{c}) = \bar{a}\overline{bc}$ [definisi perkalian di $\mathbb{Z}_n$]

$= \overline{a(bc)}$ [definisi perkalian di $\mathbb{Z}_n$]

$= \overline{(ab)c}$ [sifat asosiatif perkalian di $\mathbb{Z}$]

$= \overline{ab}\bar{c}$ [definisi perkalian di $\mathbb{Z}_n$]

$= (\bar{a}\bar{b})\bar{c}$ [definisi perkalian di $\mathbb{Z}_n$]

c) Sifat distributif perkalian terhadap penjumlahan. $\forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$ berlaku:

$\bar{a}(\bar{b} + \bar{c}) = \bar{a}\overline{b+c}$ [definisi penjumlahan di $\mathbb{Z}_n$]

$= \overline{a(b+c)}$ [definisi perkalian di $\mathbb{Z}_n$]

$= \overline{ab+ac}$ [sifat distributif perkalian terhadap penjumlahan di $\mathbb{Z}$]

$= \overline{ab} + \overline{ac}$ [definisi penjumlahan di $\mathbb{Z}_n$]

$= \bar{a}\bar{b} + \bar{a}\bar{c}$ [definisi perkalian di $\mathbb{Z}_n$]

begitu pula,

$(\bar{a} + \bar{b})\bar{c} = \overline{a+b}\bar{c}$ [definisi penjumlahan di $\mathbb{Z}_n$]

$= \overline{(a+b)c}$ [definisi perkalian di $\mathbb{Z}_n$]

$= \overline{ac + bc}$ [sifat distributif perkalian terhadap penjumlahan di $\mathbb{Z}$]

$= \overline{ac} + \overline{bc}$ [definisi penjumlahan di $\mathbb{Z}_n$]

$= \bar{a}\bar{c} + \bar{b}\bar{c}$ [definisi perkalian di $\mathbb{Z}_n$]

d) Ring $\mathbb{Z}_n$ merupakan ring komutatif, karena untuk semua $\bar{a}, \bar{b} \in \mathbb{Z}_n$ berlaku $\bar{a}\bar{b} = \overline{ab} = \overline{ba} = \bar{b}\bar{a}$.

e) Ring $\mathbb{Z}_n$ merupakan ring dengan unsur kesatuan, karena terdapat $\bar{1} \in \mathbb{Z}_n$ sebagai unsur identitas perkalian, sehingga berlaku $\bar{a}\bar{1} = \bar{1}\bar{a} = \bar{a}$.

Selanjutnya notasi $\mathbb{Z}_n$ mewakili ring $(\mathbb{Z}_n, +, \times)$.

3. Ring $(\mathbb{Z}_p, +, \times)$ dengan p bilangan prima, adalah daerah integral.

Bukti

$\mathbb{Z}_p$ adalah subring dari $\mathbb{Z}_n$, sehingga sifat-sifat para ring $\mathbb{Z}_n$ juga berlaku di ring $\mathbb{Z}_p$, yaitu ring komutatif dengan unsur kesatuan. Selanjutnya akan ditunjukkan, jika p adalah bilangan prima maka ring $\mathbb{Z}_p$ tidak memuat pembagi nol.

Andaikan $\mathbb{Z}_p$ memuat pembagi nol, maka ada unsur $\bar{a} \neq \bar{0}$ di $\mathbb{Z}_p$ yang diwakili oleh bilangan bulat a dan ada unsur $\bar{b} \neq \bar{0}$ di $\mathbb{Z}_p$ yang diwakili oleh bilangan bulat b, sedemikian hingga $\overline{ab} = \bar{0}$. Beberapa asumsi yang timbul yaitu:

a) Karena untuk semua $\bar{a} \neq \bar{0}$ dan $\bar{b} \neq \bar{0}$ berlaku $\overline{ab} = \bar{0}$. maka $\bar{a} \neq \bar{1}$ atau $\bar{b} \neq \bar{1}$.

b) Karena $\bar{p} = \bar{0}$ maka $\overline{ab} = \bar{p}$ sehingga $\bar{a} \neq \bar{p}$ dan $\bar{b} \neq \bar{p}$.

Asumsi di atas menunjukkan bahwa ada $a \neq p$ dan $b \neq p$ sedemikian hingga berlaku $ab = p$. Akibatnya, p bukanlah bilangan prima, karena memiliki dua buah faktor bilangan asli yang bukan 1 dan p itu sendiri. Kesimpulan ini bertentangan dengan hipotesis awal, bahwa p adalah bilangan prima. Sehingga pengandaian $\mathbb{Z}_p$ memuat pembagi nol adalah salah.

Dari sini telah terbukti benar jika p adalah bilangan prima maka ring $\mathbb{Z}_p$ tidak memuat pembagi nol. Karena $\mathbb{Z}_p$ juga merupakan ring komutatif dengan elemen kesatuan, maka $\mathbb{Z}_p$ merupakan daerah integral.

4. Daerah integral $\mathbb{Z}_p$ adalah lapangan.

Bukti

$\mathbb{Z}_p$ adalah himpunan dengan unsur terhingga, sehingga daerah integral $\mathbb{Z}_p$ merupakan daerah integral terhingga. Dengan mengikuti teorema 2.4, maka ring $\mathbb{Z}_p$ merupakan lapangan.

BAB III

PEMBAHASAN

3.1 Keterbagian pada $\mathbb{Z}_p$

Ring $\mathbb{Z}_p$ adalah ring modulo dengan p bilangan prima, yaitu $p = \{2, 3, 5, 7, 11, \dots\}$. Ring $\mathbb{Z}_p$ merupakan lapangan, setiap lapangan merupakan daerah integral, dan setiap daerah integral adalah ring komutatif. Definisi 2.3.1 adalah definisi keterbagian pada ring komutatif, selanjutnya definisi tersebut akan digunakan pada $\mathbb{Z}_p$.

3.1.1 Definisi Keterbagian pada $\mathbb{Z}_p$

Pada sembarang lapangan $\mathbb{Z}_p$, unsur $\bar{a} \in \mathbb{Z}_p$ dimana $\bar{a} \neq \bar{0}$ dikatakan membagi unsur $\bar{b} \in \mathbb{Z}_p$ jika ada unsur $\bar{c} \in \mathbb{Z}_p$ sedemikian hingga $\bar{b} = \bar{a}\bar{c}$. Unsur $\bar{a}$ membagi $\bar{b}$ ditulis $\bar{a}|\bar{b}$, tetapi jika $\bar{a}$ tidak membagi $\bar{b}$, maka ditulis $\bar{a} \nmid \bar{b}$.

3.1.2 Sifat-sifat Keterbagian pada $\mathbb{Z}_p$

Untuk semua unsur di $\mathbb{Z}_p$, berlaku sifat keterbagian berikut:

1. Refleksif, yaitu: $\bar{a}|\bar{a}$ untuk $\bar{a} \neq \bar{0}$.

   Bukti

   $\mathbb{Z}_p$ adalah ring dengan unsur kesatuan. Untuk unsur tak nol $\bar{a} \in \mathbb{Z}_p$ berlaku $\bar{a} = \bar{a}\bar{1}$, yaitu sifat unsur kesatuan di $\mathbb{Z}_p$.

   Jadi terbukti benar $\bar{a}|\bar{a}$ untuk $\bar{a} \neq \bar{0}$.

2. Transitif, yaitu: jika $\bar{a}|\bar{b}$ dan $\bar{b}|\bar{c}$, maka $\bar{a}|\bar{c}$ untuk $\bar{a} \neq \bar{0}$ dan $\bar{b} \neq \bar{0}$.

   Bukti

   $\bar{a}|\bar{b}$, artinya ada unsur tak nol $\bar{d} \in \mathbb{Z}_p$ sedemikian hingga $\bar{b} = \bar{a}\bar{d}$.

   $\bar{b}|\bar{c}$, artinya ada $\bar{e} \in \mathbb{Z}_p$ sedemikian hingga $\bar{c} = \bar{b}\bar{e}$.

   Oleh karena itu:

   $\bar{c} = \bar{b}\bar{e}$

   $= (\bar{a}\bar{d})\bar{e}$ [$\bar{b} = \bar{a}\bar{d}$]

   $= \bar{a}(\bar{d}\bar{e})$ [sifat asosiatif perkalian di $\mathbb{Z}_p$, dan $\bar{d}\bar{e} \in \mathbb{Z}_p$]

   Karena itu, $\bar{a}|\bar{c}$.

   Jadi terbukti benar, jika $\bar{a}|\bar{b}$ dan $\bar{b}|\bar{c}$, maka $\bar{a}|\bar{c}$ untuk $\bar{a} \neq \bar{0}$ dan $\bar{b} \neq \bar{0}$.

3. Simetris, yaitu: jika $\bar{a}|\bar{b}$ maka $\bar{b}|\bar{a}$ untuk $\bar{a} \neq \bar{0}$ dan $\bar{b} \neq \bar{0}$.

   Bukti

   $\bar{a}|\bar{b}$, artinya ada unsur tak nol $\bar{c} \in \mathbb{Z}_p$ sedemikian hingga $\bar{b} = \bar{a}\bar{c}$.

   Selanjutnya:

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

   $\bar{b}(\bar{c})^{-1} = \bar{a}\bar{c}(\bar{c})^{-1}$ [unsur tak nol di $\mathbb{Z}_p$ selalu punya invers perkalian]

   $\bar{b}(\bar{c})^{-1} = \bar{a}\bar{1}$ [dijamin oleh definisi lapangan, $\bar{c}(\bar{c})^{-1} = \bar{1}$]

   $\bar{a} = \bar{b}(\bar{c})^{-1}$

   Jadi terbukti benar, jika $\bar{a}|\bar{b}$ maka $\bar{b}|\bar{a}$ untuk $\bar{a} \neq \bar{0}$ dan $\bar{b} \neq \bar{0}$.

4. Jika $\bar{a}|\bar{b}$ dan $\bar{a}|\bar{c}$ maka $\bar{a}|(\bar{b} + \bar{c})$ dan $\bar{a}|(\bar{b} - \bar{c})$ untuk $\bar{a} \neq \bar{0}$.

   Bukti

   $\bar{a}|\bar{b}$, artinya ada $\bar{d} \in \mathbb{Z}_p$ sehingga $\bar{b} = \bar{a}\bar{d}$.

Sedangkan $\bar{a}|\bar{c}$, artinya ada $\bar{e} \in \mathbb{Z}_p$ sehingga $\bar{c} = \bar{a}\bar{e}$.

$\bar{b} + \bar{c} = \bar{a}\bar{d} + \bar{a}\bar{e} = \bar{a}(\bar{d} + \bar{e})$ berakibat $\bar{a}|(\bar{b} + \bar{c})$ karena $(\bar{b} + \bar{c}) \in \mathbb{Z}_p$.

$\bar{b} - \bar{c} = \bar{a}\bar{d} - \bar{a}\bar{e} = \bar{a}(\bar{d} - \bar{e})$ berakibat $\bar{a}|(\bar{b} - \bar{c})$ karena $(\bar{b} - \bar{c}) \in \mathbb{Z}_p$.

Jadi terbukti benar, jika $\bar{a}|\bar{b}$ dan $\bar{a}|\bar{c}$ maka $\bar{a}|(\bar{b} + \bar{c})$ dan $\bar{a}|(\bar{b} - \bar{c})$ untuk $\bar{a} \neq \bar{0}$.

5. Jika $\bar{a}|\bar{b}$ maka $\bar{a}|\bar{b}\bar{c}$ untuk $\bar{a} \neq \bar{0}$.

Bukti

$\bar{a}|\bar{b}$, artinya ada $\bar{d} \in \mathbb{Z}_p$ sedemikian hingga $\bar{b} = \bar{a}\bar{d}$. Ambil $\bar{c} \in \mathbb{Z}_p$, maka:

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

$(\bar{b})\bar{c} = (\bar{a}\bar{d})\bar{c}$

$\bar{b}\bar{c} = \bar{a}(\bar{d}\bar{c})$ [sifat asosiatif perkalian di $\mathbb{Z}_p$, dan $\bar{b}\bar{c} \in \mathbb{Z}_p$]

Sehingga, $\bar{a}|\bar{b}\bar{c}$.

Jadi terbukti benar, jika $\bar{a}|\bar{b}$ maka $\bar{a}|\bar{b}\bar{c}$.

6. Jika $\bar{a}|\bar{b}$ maka $\bar{a}\bar{c}|\bar{b}$ untuk $\bar{a} \neq \bar{0}$ dan $\bar{c} \neq \bar{0}$.

Bukti

$\bar{a}|\bar{b}$, artinya ada $\bar{d} \in \mathbb{Z}_p$ sedemikian hingga $\bar{b} = \bar{a}\bar{d}$. Ambil $\bar{c} \in \mathbb{Z}_p$ dan $\bar{c} \neq \bar{0}$, maka:

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

$\bar{b} = (\bar{a}\bar{d})(\bar{c}(\bar{c})^{-1})$ [$\bar{c}(\bar{c})^{-1} = \bar{1} \in \mathbb{Z}_p$]

$\bar{b} = (\bar{a}\bar{c})(\bar{d}(\bar{c})^{-1})$ [sifat asosiatif dan komutatif perkalian di $\mathbb{Z}_p$]

Karean $\bar{a} \neq \bar{0}$ dan $\bar{c} \neq \bar{0}$, maka $\bar{a}\bar{c} \neq \bar{0}$. Sehingga, $\bar{a}\bar{c}|\bar{b}$.

Jadi terbukti benar, jika $\bar{a}|\bar{b}$ maka $\bar{a}\bar{c}|\bar{b}$.

3.2 Daerah Faktorisasi Tunggal $\mathbb{Z}_p$

3.4.1 DFT $\mathbb{Z}_p$

Sebagai dasar bukti bahwa $\mathbb{Z}_p$ adalah DFT, terlebih dahulu diketengahkan corollary 3.1 yang juga merupakan karakter sifat unsur-unsur di $\mathbb{Z}_p$.

Corollary 3.1

Setiap unsur tak nol di $\mathbb{Z}_p$ adalah unit.

Bukti

$\mathbb{Z}_p$ adalah daerah integral. Selain itu, $\mathbb{Z}_p$ adalah lapangan yang berakibat setiap unsur tak nol di $\mathbb{Z}_p$ selalu mempunyai invers perkalian, maka setiap unsur tak nol di $\mathbb{Z}_p$ adalah unit

Corollary 3.2

$\mathbb{Z}_p$ adalah daerah faktorisasi tunggal (DFT).

Bukti

$\mathbb{Z}_p$ memenuhi aksioma pertama dari definisi 2.3.11 (definisi DFT), karena setiap unsur tak nol di $\mathbb{Z}_p$ adalah unit. Jadi, $\mathbb{Z}_p$ adalah DFT.

3.4.2 Sifat-sifat DFT $\mathbb{Z}_p$

Corollary 3.3

Setiap unsur tak nol di DFT $\mathbb{Z}_p$ adalah sekawan bagi semua unsur tak nol di DFT $\mathbb{Z}_p$.

Bukti

Definisi 2.3.8 (definisi kesekawanan) menunjukkan bahwa dua unsur tak nol a dan b di daerah integral dikatakan sekawan, jika dan hanya jika $a|b$ dan

$b|a$. Keterbagian di $\mathbb{Z}_p$ bersifat simetris, yaitu untuk $\bar{a} \neq \bar{0}$ dan $\bar{b} \neq \bar{0}$ selalu berlaku $\bar{a}|\bar{b}$ dan $\bar{b}|\bar{a}$. Jadi setiap $\bar{a}$ yang tak nol selalu sekawan dengan semua unsur tak nol $\bar{b}$.

Teorema 2.4 dan 2.5 menjamin bahwa setiap daerah ideal utama memiliki FPB dan KPK. Selanjutnya akan ditunjukkan FPB dan KPK di DFT $\mathbb{Z}_p$. Namun sebelumnya diketengahkan corollary 3.4 sampai dengan 3.9 yang menjamin bahwa DFT $\mathbb{Z}_p$ adalah daerah ideal utama.

Corollary 3.4

Di DFT $\mathbb{Z}_p$, jika $\langle\bar{a}\rangle = \{\bar{0}\}$ maka $\bar{a} = \bar{0}$.

Bukti

Diberikan $\langle\bar{a}\rangle = \left\{\bar{a}\bar{r}_1 + \bar{a}\bar{r}_2 + \cdots + \bar{a}\bar{r}_n \middle|\ \bar{a}, \bar{r}_i \in \mathbb{Z}_p, n \in \mathbb{Z}^+\right\} = \{\bar{0}\}$. Pada $\mathbb{Z}_p = \left\{\bar{r}_1, \bar{r}_2, \dots, \bar{r}_n \middle|\ \bar{r}_i \in \mathbb{Z}_p, n \in \mathbb{Z}^+\right\}$ hanya ada satu unsur ideantitas penjumlahan, yaitu $\bar{0}$. Misalkan $\bar{r}_1 = \bar{0}$, maka unsur-unsur $\{\bar{r}_2, \bar{r}_3, \dots, \bar{r}_n\}$ pasti bukan nol. Andaikan $\bar{a} \neq \bar{0}$, maka diperoleh barisan $\{\bar{a}\bar{0} + \bar{a}\bar{r}_2 + \cdots + \bar{a}\bar{r}_n\} = \{\bar{0} + \bar{a}\bar{r}_2 + \cdots + \bar{a}\bar{r}_n\} \neq \{\bar{0}\}$. Jadi, pengandaian $\bar{a} \neq \bar{0}$ adalah salah. Sehingga ideal $\langle\bar{a}\rangle = \{\bar{0}\}$ maka $\bar{a} = \bar{0}$.

Corollary 3.5

$\langle\bar{0}\rangle$ dan $\mathbb{Z}_p$ adalah ideal dari DFT $\mathbb{Z}_p$.

Bukti

Corollary 3.4 menunjukkan bahwa $\langle\bar{0}\rangle$ adalah ideal utama yang dibangun oleh $\bar{0}$. Dan, $\mathbb{Z}_p$ juga merupakan ideal dari $\mathbb{Z}_p$ sendiri, karena:

(i) Untuk semua $\bar{a}, \bar{b} \in \mathbb{Z}_p$ berlaku $\bar{a} - \bar{b} = \bar{a} + (-\bar{b}) = \overline{a + (b)} = \overline{a - b}$ dimana $(a - b) \in \mathbb{Z}$.

(ii) Untuk semua $\bar{a}, \bar{b} \in \mathbb{Z}_p$ berlaku $\bar{a}\bar{b} \in \mathbb{Z}_p$.

Corollary 3.6

Di DFT $\mathbb{Z}_p$, $\langle \bar{a} \rangle = \langle \bar{b} \rangle$ jika dan hanya jika $\bar{a} \sim \bar{b}$.

Bukti

($\Rightarrow$) Akan ditunjukkan, jika $\langle \bar{a} \rangle = \langle \bar{b} \rangle$ maka $\bar{a} \sim \bar{b}$.

Mengikuti definisi 2.3.5 (definisi ideal utama dan unsur pembangun ideal), jika $\langle \bar{a} \rangle = \langle \bar{b} \rangle$, maka ada $\bar{a} \in \langle \bar{b} \rangle$ sehingga $\bar{a} = \bar{b}\bar{r}$ untuk suatu $\bar{r} \in \mathbb{Z}_p$, jadi $\bar{b} | \bar{a}$. Dengan langkah yang sama, $\bar{a} \in \langle \bar{b} \rangle$ berimplikasi $\bar{a} | \bar{b}$. Karena $\bar{b} | \bar{a}$ dan $\bar{a} | \bar{b}$, maka $\bar{a} \sim \bar{b}$.

($\Leftarrow$) Akan ditunjukkan, jika $\bar{a} \sim \bar{b}$ maka $\langle \bar{a} \rangle = \langle \bar{b} \rangle$.

Definisi 2.3.8 (definisi kesekawanan) menjamin bahwa $\bar{a} \sim \bar{b}$ maka $\bar{a} = \bar{b}\bar{u}$ dan $\bar{b} = \bar{a}\bar{v}$, dengan $\bar{u}$ dan $\bar{v}$ suatu unit. Semua elemen di DFT $\mathbb{Z}_p$ adalah unit,, dengan mengikuti definisi 2.3.5, maka $\bar{a} = \bar{b}\bar{u}$ berakibat $\bar{a} \in \langle \bar{b} \rangle$ sehingga $\langle \bar{a} \rangle \subseteq \langle \bar{b} \rangle$. Dengan langkah yang sama, $\bar{b} = \bar{a}\bar{v}$ berakibat $\bar{b} \in \langle \bar{a} \rangle$ sehingga $\langle \bar{b} \rangle \subseteq \langle \bar{a} \rangle$. Jadi, $\langle \bar{a} \rangle = \langle \bar{b} \rangle$.

Corollary 3.7

DFT $\mathbb{Z}_p$ hanya memiliki dua ideal, yaitu $\langle \bar{0} \rangle$ dan $\mathbb{Z}_p = \langle \bar{a} \rangle$ untuk $\bar{a} \neq \bar{0}$ dan $\bar{a} \in \mathbb{Z}_p$.

Bukti

Corollary 3.5 menjamin bahwa ideal $\langle\bar{0}\rangle$ selalu ada di $\mathbb{Z}_p$. Selanjutnya akan ditunjukkan bahwa selain $\langle\bar{0}\rangle$ tidak ada ideal yang lainnya kecuali hanya $\mathbb{Z}_p$ sendiri.

Misalkan $\langle\bar{a}\rangle$ ideal dari $\mathbb{Z}_p$ dan $\langle\bar{a}\rangle \neq \langle\bar{0}\rangle$, akan dibuktikan bahwa $\langle\bar{a}\rangle = \mathbb{Z}_p$. Asumsikan $\bar{a} \in \langle\bar{a}\rangle$ dan $\bar{a} \neq \bar{0}$. Karena $\mathbb{Z}_p$ adalah lapangan, maka $\bar{a}$ selalu mempunyai invers perkalian di $\mathbb{Z}_p$. Sehingga diperoleh: $\bar{1} = \bar{a}(\bar{a})^{-1} \in \langle\bar{a}\rangle$, karena $\langle\bar{a}\rangle$ adalah ideal.

Ambil $\bar{r}$ yaitu sembarang unsur di $\mathbb{Z}_p$, maka kita peroleh:

$$\begin{aligned}\bar{r} &= \bar{1}\bar{r}\\ &= (\bar{a}(\bar{a})^{-1})\bar{r}\\ &= \bar{a}((\bar{a})^{-1}\bar{r}) \in \langle\bar{a}\rangle \qquad \text{dimana } ((\bar{a})^{-1}\bar{r}) \in \mathbb{Z}_p \text{ dan } \langle\bar{a}\rangle \text{ adalah ideal.}\end{aligned}$$

Jadi, sembarang ideal dari $\mathbb{Z}_p$ yaitu ideal $\langle\bar{a}\rangle \neq \langle\bar{0}\rangle$ adalah $\mathbb{Z}_p$ itu sendiri. Kesimpulannya, terbukti bahwa tidak ada ideal dari $\mathbb{Z}_p$ selain $\langle\bar{0}\rangle$ dan $\mathbb{Z}_p = \langle\bar{a}\rangle$ untuk $\bar{a} \neq \bar{0}$.

Corollary 3.8

$\langle\bar{0}\rangle$ satu-satunya ideal prima dari $\mathbb{Z}_p$.

Bukti

Akan ditunjukkan bahwa $\langle\bar{0}\rangle$ adalah ideal prima dari $\mathbb{Z}_p$. Jelas bahwa $\langle\bar{0}\rangle = \{\bar{0}\} \neq \mathbb{Z}_p$. Misalkan $\bar{a}, \bar{b} \in \mathbb{Z}_p$ dan $\bar{a}\bar{b} = \bar{0} \in \langle\bar{0}\rangle$. Karena berlaku $\bar{a}\bar{b} = \bar{0}$, hanya jika $\bar{a} = \bar{0}$ atau $\bar{b} = \bar{0}$, dengan kata lain tidak ada $\bar{a} \neq \bar{0}$ dan $\bar{b} \neq \bar{0}$

sehingga $\bar{a}\bar{b} = \bar{0}$. Hal ini karena $\mathbb{Z}_p$ adalah daerah integral (tidak memuat pembagi nol). Jadi, $\langle\bar{0}\rangle$ adalah ideal prima.

Ideal dari $\mathbb{Z}_p$ selain $\langle\bar{0}\rangle$ adalah $\langle\bar{a}\rangle$ untuk $\bar{a} \neq \bar{0}$. Jelas $\langle\bar{a}\rangle = \mathbb{Z}_p$, sehingga $\langle\bar{a}\rangle$ untuk $\bar{a} \neq \bar{0}$ bukan ideal prima.

Corollary 3.9

DFT $\mathbb{Z}_p$ adalah daerah ideal utama.

Bukti

Corollary 3.7 menunjukkan bahwa DFT $\mathbb{Z}_p$ hanya memiliki dua ideal yaitu $\langle\bar{0}\rangle$ dan $\mathbb{Z}_p = \langle\bar{a}\rangle$ yang masing-masing dibangun oleh $\bar{0}$ dan $\bar{a} \neq \bar{0}$. Sehingga DFT $\mathbb{Z}_p$ adalah daerah ideal utama.

Corollary 3.10

FPB dari dua unsur tak nol di DFT $\mathbb{Z}_p$ adalah sembarang unsur tak nol di DFT $\mathbb{Z}_p$.

Bukti

Misalkan $\bar{d}$ adalah FPB dari $\bar{a}$ dan $\bar{b}$ untuk sembarang $\bar{a}, \bar{b} \in \mathbb{Z}_p - \{\bar{0}\}$. Karena FPB $(\bar{a}, \bar{b}) = \bar{d}$, maka $\bar{d}|\bar{a}$ dan $\bar{d}|\bar{b}$. Hal ini menjamin bahwa $\bar{d} \neq \bar{0}$. Selain itu, jika terdapat $\bar{x} \in \mathbb{Z}_p - \{\bar{0}\}$ dimana $\bar{x}|\bar{a}$ dan $\bar{x}|\bar{b}$, maka $\bar{x}|\bar{d}$ sedemikian hingga $\bar{d} = \bar{x}\bar{y}$ ada $\bar{y} \in \mathbb{Z}_p$. Karena $\bar{d} \neq \bar{0}$ dan $\bar{x} \neq \bar{0}$, ini berakibat $\bar{y} \neq \bar{0}$. Hasil perkalian setiap $\bar{x}$ dan $\bar{y}$ adalah semua unsur $\mathbb{Z}_p - \{\bar{0}\}$.

Corollary 3.11

KPK dari dua unsur tak nol di DFT $\mathbb{Z}_p$ adalah sembarang unsur tak nol di DFT $\mathbb{Z}_p$.

Bukti

Misalkan $\bar{e}$ adalah KPK dari $\bar{a}$ dan $\bar{b}$ untuk sembarang $\bar{a}, \bar{b} \in \mathbb{Z}_p - \{\bar{0}\}$. Karena KPK $(\bar{a}, \bar{b}) = \bar{e}$, maka: (i) $\bar{a}|\bar{e}$ dan $\bar{b}|\bar{e}$; (ii) $\bar{a}|\bar{m}$ dan $\bar{b}|\bar{m}$; dan (iii) $\bar{e}|\bar{m}$. Jelas $\bar{e} \neq \bar{0}$. Selanjutnya, untuk $\bar{a}|\bar{e}$ dan $\bar{b}|\bar{e}$ selalu ada $\bar{c}, \bar{d} \in \mathbb{Z}_p - \{\bar{0}\}$ sedemikian hingga $\bar{e} = \bar{a}\bar{c} = \bar{b}\bar{d}$. Jadi KPK $(\bar{a}, \bar{b}) = \bar{e}$ dimana $\bar{e} \in \mathbb{Z}_p - \{\bar{0}\}$.

Corollary 3.12

DFT $\mathbb{Z}_p$ tidak memuat unsur tereduksi dan tak tereduksi.

Bukti

Semua unsur tak nol di DFT $\mathbb{Z}_p$ adalah unit. Mengikuti definisi 2.3.9 (definisi unsur tereduksi dan tak tereduksi), maka semua unsur-unsur itu bukan unsur tereduksi dan bukan pula unsur tak tereduksi.

Corollary 3.13

DFT $\mathbb{Z}_p$ tidak memuat unsur prima.

Bukti

Definisi 2.3.10 (definisi unsur prima) mengatakan bahwa unsur prima adalah unsur tak nol yang membangun suatu ideal prima. Corollary 3.8 menunjukkan bahwa $\langle\bar{0}\rangle$ satu-satunya ideal prima dari $\mathbb{Z}_p$. Jadi, jelas bahwa $\bar{0}$ bukan unsur prima.

3.3 Kajian Keagamaan

3.3.1 Relasi Al-Qur'an dan Ilmu Pengetahuan

Al-Qur'an dan As-Sunnah keduanya mutlak menjadi pedoman bagi manusia yang mendambakan kebahagiaan hidup di dunia dan akhirat. Menentang arus keduanya hanya akan bermuara pada jurang kesengsaraan dan ketidakbahagiaan. Hal ini telah disampaikan oleh Nabi Muhammad SAW dalam sebuah hadis riwayat Imam Al-Hakim (Ibrahim, 2010:vii), yang berbunyi:

تَرَكْتُ فِيْكُمْ أَمْرَيْنِ لَنْ تَضِلُّوا مَا تَمَسَّكْتُمْ بِهِمَا كِتَابَ اللهِ وَ سُنَّتِيْ

Artinya: "Telah kutinggalkan bagi kalian dua perkara, niscaya kalian takkan tersesat jika berpegang kepadanya, (yaitu) Kitabullah (Al-Qur'an) dan Sunnahku (Al-Hadits)".

Salah satu kegiatan terpenting dalam sejarah perkembangan peradaban manusia adalah membaca, yang dalam bahasa arab diartikan *qara'a* atau juga *tala*. Kedua kata ini masing-masing digunakan dalam Al-Qur'an, kata *qara'a* salah satunya terdapat dalam surat ke-96 ayat 1, sedangkan *tala* salah satunya di surat ke-2 ayat 252. Namun keduanya memiliki arti membaca yang berbeda. Shihab (1992:168) mengatakan bahwa *tala* merujuk pada makna membaca bacaan-bacaan yang sifatnya suci dan pasti benar. Adapun *qara'a* memiliki arti dasar "menghimpun", yang juga berarti kegiatan membaca tanpa mengharuskan ada suatu teks tertulis yang dibaca, tidak harus diucapkan. Artinya, membaca mencakup segala apa yang bisa dijangkau manusia, tidak hanya persoalan agama, namun juga mencakup alam raya. Mempelajari berbagai bidang ilmu pengetahuan yang tidak bertentangan dengan perintah Allah adalah bentuk dari kegiatan membaca.

Tujuan utama Al-Qur'an adalah sebagai kitab petunjuk yang menuntun manusia menuju jalan keselamatan di dunia dan akhirat. Selain itu, Al-Qur'an juga memberikan motivasi besar dan dorongan kuat kepada manusia untuk selalu belajar, melakukan kegiatan ilmiah dan penelitian salah satunya melalui perintah membaca (*iqra'*) sebagaimana yang telah disampaikan. Di sinilah letak hubungan erat Al-Qur'an dengan ilmu pengetahuan, yaitu pada motivasi mengembangkan ilmu.

Dalam masa dakwahnya, Nabi Muhammad SAW berhasil membentuk budaya (iklim) ilmiah, yaitu menekankan nilai pentingnya ilmu pengetahuan alam kepada masyarakat. Al-Qur'an menyampaikan pertanyaan-pertanyaan yang menjadi sebuah ujian, di antaranya ada dalam surat Az-Zumar ayat 9: *Tanyakanlah hai Muhammad! Adakah sama orang-orang yang mengetahui dengan mereka yang tidak mengetahui?* Ayat ini menekankan kepada masyarakat betapa besar nilai ilmu pengetahuan dan kedudukan cendekiawan. Selain itu, surat Ali Imran ayat 66 berbunyi: *Inilah kamu (wahai Ahlul Kitab), kamu ini membantah tentang hal-hal yang kamu ketahui (Nabi Musa, Isa, dan Muhammad), maka mengapakah membantah pula dalam hal-hal yang kalian tidak ketahui (Nabi Ibrahim)?* Ayat ini merupakan kritik terhadap mereka yang berbicara ataupun membantah suatu persoalan tanpa adanya data objektif dan ilmiah.

Ayat-ayat seperti ini yang selanjutnya akan membentuk iklim ilmiah dalam masyarakat dan mendorong kemajuan ilmu pengetahuan. Shihab (1992:44) mengatakan bahwa iklim ilmiah seperti itu telah menumbuhkan tokoh-tokoh besar seperti Ibnu Sina, Al-Farabi, Al-Ghazali, dan sebagainya. Bahkan, ayat-ayat seperti itulah yang menginspirasi Muhammad bin Ahmad menemukan angka nol, yang akhirnya mendorong Muhammad bin Musa Al-Khawarizmiy menemukan perhitungan aljabar. Tanpa penemuan-penemuan itu, terutama perkembangan ilmu matematika akan tetap merangkak dan meraba-raba dalam alam gelap gulita. Shihab juga mengatakan bahwa mewujudkan iklim ilmiah jauh lebih penting daripada menemukan teori ilmiah, karena tanpa wujudnya iklim ilmu pengetahuan, para ahli yang menemukan teori itu akan mendapatkan pertentangan hebat dari lingkungannya, seperti halnya nasib Galileo yang menjadi korban hasil penemuannya.

Karena itu, pendapat Shihab (1992:44) mengenai hubungan Al-Qur’an dan ilmu pengetahuan sejauh ini bagi penulis adalah teori yang paling sesuai. Beliau menegaskan bahwa Al-Qur’an sebagai kitab petunjuk yang memberikan petunjuk kepada manusia untuk kebahagiaan hidupnya di dunia dan akhirat, yang dalam hubungannya dengan ilmu pengetahuan adalah mendorong manusia seluruhnya untuk mempergunakan akal pikirannya serta menambah ilmu pengetahuannya sebisa mungkin. Kemudian juga menjadikan observasi atas alam semesta sebagai alat untuk memperkuat keimanan.

Shihab mengatakan bahwa praktik mencari ayat-ayat Al-Qur’an untuk membenarkan ataupun membantah teori ilmiah dan penemuan baru adalah tidak tepat. Bukan saja karena tidak sejalan dengan tujuan-tujuan pokok Al-Qur’an, tetapi juga karena menjadikan Al-Qur’an yang absolut sebagai dasar untuk menghakimi teori ilmiah yang kebenarannya relatif dinilai sebagai tindakan yang kurang hati-hati. Boleh jadi ketika Al-Qur’an telah membenarkan suatu teori ilmiah, dikemudian hari ditemukan bahwa teori ilmiah itu terbukti salah, hal ini yang anggap dapat mencederai keabsolutan Al-Qur’an.

Namun usaha ulama dan ilmuan lainnya yang mencoba menguraikan hubungan Al-Qur'an dengan ilmu pengetahuan dari pintu sains juga memberikan sumbangsih besar bagi kemajuan dunia islam. Seperti usaha-usaha yang dilakukan Harun Yahya dalam menjelaskan Al-Qur'an, menjelaskan kejadian alam telah mendorong banyak pihak dan kalangan untuk semakin terbuka dalam mempelajari Al-Qur'an. Semua ini adalah hal yang positif yang akan semakin melengkapi wawasan keislaman dan memperkuat keimanan kita.

3.3.2 Ulama dalam Al-Qur'an

Shihab (1992:382) mengatakan bahwa Al-Qur'an menyebutkan kata *'ulama* disebutkan dalam Al-Qur'an sebanyak dua kali. Pertama, dalam konteks ajakan Al-Qur'an untuk memperhatikan turunnya hujan dari langit, beraneka ragamnya buah-buahan, gunung, binatang, dan manusia, yang kemudian diakhiri dengan ayat: *Sesungguhnya yang takut kepada Allah di antara hamba-hamba-Nya hanyalah ulama* (QS. Fathir:28). Ayat ini menggambarkan bahwa yang dinamakan ulama adalah orang-orang yang memiliki pengetahuan tentang ayat-ayat Allah yang bersifat *kawniyyah* (fenomena alam). Kedua, dalam konteks pembicaraan Al-Qur'an yang kebenaran dan kandungannya telah diakuai (diketahui) oleh ulama Bani Israil (QS. Asyu'araa':197).

Selanjutnya menurut Shihab, definisi ulama berdasarkan kedua ayat tersebut adalah orang yang mempunyai pengetahuan tentang ayat-ayat Allah, baik yang bersifat *kawniyyah* maupun *qur'aniyyah*. Selain itu, dibatasi bahwa orang yang takut kepada Allah hanyalah ulama (apapun disiplin ilmunya). Sebab, pada dasarnya semua ilmu selama bermanfaat dapat menghantarkan pemiliknya pada pengetahuan tentang kekuasaan Tuhan (*khasyyah*) dan terbuka untuk kepentingan semua manusia (sebagaimana ilmu Islam). Di sini dapat ditarik garis pemisah antara sarjana, cendekiawan, orang yang banyak ilmu agama, dengan ulama. Namun dalam tata bahasa Indonesia, kata ulama mengalami penyempitan makna yang dikhususkan pada ilmu agama.

BAB IV

PENUTUP

4.1 Kesimpulan

Berdasarkan pembahasan pada bab ketiga, maka dapat disimpulkan:

1. Sifat-sifat keterbagian pada $\mathbb{Z}_p$

   Berikut ini adalah sifat-sifat keterbagian pada $\mathbb{Z}_p$ yang telah dibuktikan dalam pembahasan.

Tabel 4.1: Tabel Sifat-sifat Keterbagian pada $\mathbb{Z}_p$

No.	Sifat Keterbagian
1.	Refleksif, yaitu: $\bar{a}\|\bar{a}$ untuk setiap $\bar{a} \in \mathbb{Z}_p - \{\bar{0}\}$
2.	Transitif, yaitu: jika $\bar{a}\|\bar{b}$ dan $\bar{b}\|\bar{c}$, maka $\bar{a}\|\bar{c}$ untuk setiap $\bar{c} \in \mathbb{Z}_p$ dan $\bar{a}, \bar{b} \in \mathbb{Z}_p - \{\bar{0}\}$
3.	Simetris, yaitu: jika $\bar{a}\|\bar{b}$ maka $\bar{b}\|\bar{a}$ untuk setiap $\bar{a}, \bar{b} \in \mathbb{Z}_p - \{\bar{0}\}$
4.	Jika $\bar{a}\|\bar{b}$ maka $\bar{a}\|(\bar{b} + \bar{c})$ dan $\bar{a}\|(\bar{b} - \bar{c})$ untuk setiap $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_p$ dan $\bar{a} \neq \bar{0}$
5.	Jika $\bar{a}\|\bar{b}$ maka $\bar{a}\|\bar{b}\bar{c}$ untuk setiap $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_p$ dan $\bar{a} \neq \bar{0}$
6.	Jika $\bar{a}\|\bar{b}$ maka $\bar{a}\bar{c}\|\bar{b}$ untuk setiap $\bar{b} \in \mathbb{Z}_p$ dan $\bar{a}, \bar{c} \in \mathbb{Z}_p - \{\bar{0}\}$

2. Sifat-sifat dan pembuktian daerah faktorisasi tunggal $\mathbb{Z}_p$

   a. Telah dibuktikan bahwa $\mathbb{Z}_p$ merupakan daerah faktorisasi tunggal (DFT).

b. Sifat-sifat DFT $\mathbb{Z}_p$.

Berikut ini adalah sifat-sifat DFT $\mathbb{Z}_p$ yang telah dibuktikan dalam pembahasan.

Tabel 4.1: Tabel Sifat-sifat DFT $\mathbb{Z}_p$

No.	Unsur-unsur di DFT $\mathbb{Z}_p$	Keterangan
1.	Unit	Setiap unsur tak nol di $\mathbb{Z}_p$ adalah unit
2.	Sekawan	Setiap unsur tak nol di DFT $\mathbb{Z}_p$ adalah sekawan bagi semua unsur tak nol di DFT $\mathbb{Z}_p$
3.	FPB	FPB dari dua unsur tak nol di DFT $\mathbb{Z}_p$ adalah sembarang unsur tak nol di DFT $\mathbb{Z}_p$
4.	KPK	KPK dari dua unsur tak nol di DFT $\mathbb{Z}_p$ adalah sembarang unsur tak nol di DFT $\mathbb{Z}_p$
5.	Unsur tereduksi	DFT $\mathbb{Z}_p$ tidak memuat unsur tereduksi
6.	Unsur tak tereduksi	DFT $\mathbb{Z}_p$ tidak memuat unsur tak tereduksi
7.	Prima	DFT $\mathbb{Z}_p$ tidak memuat unsur prima

4.2 Saran

Penelitian ini dapat dilanjutkan pada ring $\mathbb{Z}_k$ untuk k bilangan komposit, dan diperumum pada ring $\mathbb{Z}_n$ untuk n bilangan asli, tetap dengan topik yang sama yaitu menguraikan sifat-sifat keterbagian dan faktorisasinya.

DAFTAR PUSTAKA

Abdussakir. 2007. *Ketika Kiai Mengajar Matematika*. Malang: UIN Malang Press

Arifin, Achmad. 2000. *Aljabar*. Bandung: ITB Bandung

Bhattacharya, P.B., dkk. 1995. *Basic Abstract Algebra*. New York: Cambridge University Press

Dummit, David S. dan Foote, Richard M. 1991. *Abstract Algebra*. New Jersey: Prentice-Hall, Inc

Ibrahim, Ahmad Syawqi. 2010. *Ensiklopedi Mukjizat Ilmiah Hadits Nabi: Kebenaran Risalah Muhammad, SAW*. Bandung: Sygma Publishing

Raisinghania, M.D dan Aggarwal, R.S. 1980. *Modern Algebra*. New Delhi: Ram Nagar

Shihab, Quraish. 1992. *"Membumikan" Al-Qur'an: Fungsi dan Peran Wahyu dalam Kehidupan Masyarakat*. Bandung: Mizan

KEMENTERIAN AGAMA RI
UNIVERSITAS ISLAM NEGERI
MAULANA MALIK IBRAHIM MALANG
FAKULTAS SAINS & TEKNOLOGI
Jalan Gajayana No. 50 Malang Telp. (0341) 558933 Fax. (0341) 558933

BUKTI KONSULTASI SKRIPSI

Nama : **Moh. Zuhdi Kurniawan**
NIM : **06510046**
Fakultas/ Jurusan: **Sains dan Teknologi/ Matematika**
Judul Skripsi : **Keterbagian dan Sifat-sifat Daerah Faktorisasi Tunggal $\mathbb{Z}_p$**
Pembimbing I : **Drs. H. Turmudi, M.Si**
Pembimbing II : **Fachrur Rozi, M.Si**

No	Tanggal	Materi Konsultasi	Tanda Tangan
1	12 Desember 2011	Konsultasi BAB I dan perubahan redaksi judul	1.
2	1 September 2012	Revisi BAB I	2.
3	17 September 2012	Revisi BAB II dan penyesuaian istilah-istilah pada BAB I dan II	3.
4	26 September 2012	Revisi BAB III	4.
5	20 Nopember 2012	Revisi Abstrak	5.
6	3 Desember 2012	Revisi BAB IV	6.
7	5 Desember 2012	Arah kajian agama	7.
8	12 Desember 2012	Konsultasi kajian agama	8.
9	13 Desember 2012	Konsultasi hasil revisi kajian agama	9.
10	13 Desember 2012	Revisi abstrak dan BAB IV	10.
11	14 Desember 2012	ACC kajian agama	11.
12	14 Desember 2012	ACC Keseluruhan	12.

Malang, 15 Desember 2012
Mengetahui,
Ketua Jurusan Matematika

Abdussakir, M.Pd
NIP. 19751006 200312 1 001