

**APLIKASI BASIS GRÖBNER PADA PENYELESAIAN SISTEM
KONGRUENSI ATAS RING POLINOMIAL MULTIVARIABEL
DAN IMPLEMENTASI PADA SINGULAR-CAS**

SKRIPSI

**OLEH
MOHAMMAD ZAENAL FANANI
NIM. 220601110091**



**PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM MALANG
2026**

**APLIKASI BASIS GRÖBNER PADA PENYELESAIAN SISTEM
KONGRUENSI ATAS RING POLINOMIAL MULTIVARIABEL
DAN IMPLEMENTASI PADA SINGULAR-CAS**

SKRIPSI

**Diajukan Kepada
Fakultas Sains dan Teknologi
Universitas Islam Negeri Maulana Malik Ibrahim Malang
untuk Memenuhi Salah Satu Persyaratan dalam
Memperoleh Gelar Sarjana Matematika (S.Mat)**

**Oleh
Mohammad Zaenal Fanani
NIM. 220601110091**

**PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM MALANG
2026**

APLIKASI BASIS GRÖBNER PADA PENYELESAIAN SISTEM KONGRUENSI ATAS RING POLINOMIAL MULTIVARIABEL DAN IMPLEMENTASI PADA SINGULAR-CAS

SKRIPSI

Oleh
Mohammad Zaenal Fanani
NIM. 220601110091

Telah Disetujui Untuk Diuji

Malang, 3 Maret 2026

Dosen Pembimbing I



Dewi Ismiarti, M.Si.
NIPPPK. 19870505 202521 2 077

Dosen Pembimbing II



Ari Kusumastuti, M.Si.
NIP. 19770521 200501 2 004

Mengetahui,
Ketua Program Studi Matematika



Dr. Fachrud Rozi, M.Si.
NIP. 19800527 200801 1 012

APLIKASI BASIS GRÖBNER PADA PENYELESAIAN SISTEM KONGRUENSI ATAS RING POLINOMIAL MULTIVARIABEL DAN IMPLEMENTASI PADA SINGULAR-CAS

SKRIPSI

Oleh
Mohammad Zaenal Fanani
NIM. 220601110091

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

Tanggal 28 April 2026

Ketua Penguji : Prof. Dr. H. Turmudi M.Si., Ph.D.

Anggota Penguji 1 : Intan Nisfulaila, M.Si

Anggota Penguji 2 : Dewi Ismiarti, M.Si.

Anggota Penguji 3 : Ari Kusumastuti, M.Si.

Mengetahui,
Ketua Program Studi Matematika



Dr. Fachrur Rozi, M.Si.
NIP. 19800527 200801 1 012

PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan di bawah ini:

Nama : Mohammad Zaenal Fanani

NIM : 220601110091

Program Studi : Matematika

Fakultas : Sains dan Teknologi

Judul Skripsi : Aplikasi Basis Gröbner pada Penyelesaian Sistem Kongruensi
atas Ring Polinomial Multivariabel dan Implementasi pada
Singular-CAS

Menyatakan dengan sebenarnya bahwa skripsi yang saya tulis ini merupakan hasil karya sendiri, bukan pengambilan tulisan atau pemikiran orang lain yang saya akui sebagai pemikiran saya, kecuali dengan mencantumkan sumber cuplikan pada daftar rujukan di halaman terakhir. Apabila dikemudian hari terbukti skripsi ini adalah hasil jiplakan atau tiruan, maka saya akan bersedia menerima sanksi yang berlaku atas perbuatan tersebut.

Malang, 28 April 2026



Mohammad Zaenal Fanani
NIM. 220601110091

MOTO

“Alon-alon waton kelaton”

“The mathematician does not study pure mathematics because it is useful; he studies it because he delights in it and he delights in it because it is beautiful”

Henri Poincaré

“I can illustrate the second approach with the same image of a nut to be opened. The first analogy that came to my mind is of immersing the nut in some softening liquid, and why not simply water? From time to time you rub so the liquid penetrates better, and otherwise you let time pass. The shell becomes more flexible through weeks and months—when the time is ripe, hand pressure is enough, the shell opens like a perfectly ripened avocado!”

Alexander Grothendieck

PERSEMBAHAN

Skripsi ini dipersembahkan kepada kedua orang tua yang telah membesarkan penulis dengan kesabaran dan kasih sayang, yang mendidik penulis hingga menjadi pribadi berbudi luhur, dan yang mendukung penuh penulis untuk melanjutkan pendidikan tingkat lanjut pada bidang yang diminati.

KATA PENGANTAR

Puji dan syukur kehadiran Allah SWT. atas segala kemurahan dan limpahan rahmat serta karunia-Nya sehingga naskah skripsi berjudul "*Aplikasi Basis Gröbner pada Penyelesaian Sistem Kongruensi atas Ring Polinomial Multivariabel dan Implementasi pada Singular-CAS*" dapat disusun dengan baik. Shalawat serta salam semoga senantiasa tercurahkan kepada junjungan kita Nabi Muhammad SAW. Skripsi ini disusun untuk memenuhi salah satu persyaratan dalam memperoleh gelar Sarjana Matematika (S.Mat) Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. terselesaikannya skripsi ini tidak lepas dari dorongan berbagai pihak, oleh karena itu penulis ucapkan terima kasih yang sebesar-besarnya kepada:

1. Prof. Dr. Hj. Ilfi Nur Diana, M.Si., selaku Rektor Universitas Islam Negeri Maulana Malik Ibrahim Malang.
2. Dr. Agus Mulyono, M.Kes., selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang.
3. Dr. Fachrur Rozi, M.Si., selaku Ketua Program Studi Matematika Universitas Islam Negeri Maulana Malik Ibrahim Malang.
4. Dewi Ismiarti, M.Si., selaku Dosen Pembimbing I yang telah memberikan bimbingan dan arahan yang sangat baik kepada penulis dari masa penentuan topik sampai selesai pengerjaan skripsi.
5. Ari Kusumastuti, M.Si., selaku Dosen Pembimbing II yang telah memberikan bimbingan dan arahan terkait kepenulisan kajian integrasi topik dengan Al-Qur'an.
6. Prof. Dr. H. Turmudi M.Si., Ph.D., selaku Ketua Penguji yang telah memberikan kritik dan saran yang membangun terkait struktur kepenulisan skripsi ini.
7. Intan Nisfulaila, M.Si., selaku Anggota Penguji I yang telah memberikan koreksi terhadap penggunaan kata dan kalimat yang tepat pada skripsi ini.
8. Seluruh dosen Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim yang telah memberikan bekal ilmu pengetahuan dan pengalaman akademik yang sangat bermanfaat selama masa perkuliahan.

9. Kedua orang tua yang selalu mendukung penuh penulis dalam melaksanakan kegiatan perkuliahan hingga akhirnya penulis bisa menuntaskan skripsi ini dengan baik.
10. Teman-teman penulis yang sama-sama memiliki semangat bermatematika yang tinggi, sehingga penulis dapat menikmati setiap aktivitas perkuliahan dengan sepenuh hati.
11. Diri sendiri yang patut diapresiasi karena telah melalui banyak hal, suka maupun duka sepanjang masa perkuliahan ini maupun saat pengerjaan skripsi.

Penyusunan skripsi ini disusun dengan sebaik-baiknya, namun masih terdapat kekurangan dalam penyusunannya. Oleh karena itu, saran dan kritik yang sifatnya membangun dari semua pihak sangatlah diharapkan untuk membantu penulis menjadi lebih baik.

Malang, 28 April 2026

Penulis

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGANTAR	ii
HALAMAN PERSETUJUAN	iii
HALAMAN PENGESAHAN	iv
PERNYATAAN KEASLIAN TULISAN	v
MOTO	vi
PERSEMBAHAN	vii
KATA PENGANTAR	viii
DAFTAR ISI	x
DAFTAR GAMBAR	xii
ABSTRAK	xiii
ABSTRACT	xiv
البحث مستخلص	xv
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	4
1.3 Tujuan Penelitian	4
1.4 Manfaat Penelitian	5
1.5 Batasan Masalah	5
BAB II KAJIAN TEORI	7
2.1 Ring	7
2.1.1 Ideal	8
2.1.2 Ring Polinomial Multivariabel, Order Suku, dan Algoritma Pembagian	10
2.1.3 Pembagian Polinomial dengan Ideal	25
2.2 Basis Gröbner	25
2.2.1 Algoritma Buchberger	28
2.2.2 Basis Gröbner Tereduksi	32
2.3 Kongruensi	33
2.3.1 Bentuk Normal dari Polinomial Multivariabel	34
2.3.2 Sistem Kongruensi atas Ring Polinomial Multivariabel	35
2.4 Singular-CAS	36
2.5 Kajian Integrasi Topik dengan Al-Qur'an	37
2.6 Kajian Topik dengan Teori Pendukung	40
BAB III METODE PENELITIAN	41
3.1 Jenis Penelitian	41
3.2 Pra Penelitian	41
3.3 Tahapan Penelitian	42
BAB IV HASIL DAN PEMBAHASAN	45
4.1 Penyelesaian Sistem Kongruensi atas Ring Polinomial Multivariabel	45
4.2 Implementasi pada Singular-CAS	59
BAB V PENUTUP	65
5.1 Kesimpulan	65
5.2 Saran untuk Penelitian Lanjutan	67
DAFTAR PUSTAKA	68
LAMPIRAN	69

RIWAYAT HIDUP	71
----------------------------	-----------

DAFTAR GAMBAR

Gambar 2.1 Tampilan Awal dari Singular-CAS	37
Gambar 4.1 Langkah-langkah Penyelesaian Sistem Kongruensi	52
Gambar 4.2 Pendeklarasian Ring, Polinomial, dan Ideal dari Contoh 4.2.1.....	60
Gambar 4.3 Proses menjalankan prosedur “solveCongruences”	61
Gambar 4.4 <i>Output</i> dari Prosedur untuk Sistem Kongruensi Contoh 4.2.1.....	61
Gambar 4.5 Hasil Perhitungan yang Disimpan oleh Prosedur.....	62
Gambar 4.6 <i>Output</i> dari Prosedur untuk Sistem Kongruensi Contoh 4.2.2.....	63
Gambar 4.7 Hasil Pengecakan untuk $h = 2x^2 - 1$	64
Gambar 4.8 Hasil Pengecekan untuk $u = z^3 + yz$	64

ABSTRAK

Fanani, Mohammad Zaenal. 2026. **Aplikasi Basis Gröbner pada Penyelesaian Sistem Kongruensi atas Ring Polinomial Multivariabel dan Implementasi pada Singular-CAS**. Skripsi. Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing (I) Dewi Ismiarti, M.Si., (II) Ari Kusumastuti, M.Si.

Kata Kunci: basis Gröbner, kongruensi, ring polinomial multivariabel, Singular-CAS, sistem kongruensi atas ring polinomial multivariabel.

Diberikan ring polinomial multivariabel $k[x_1, x_2, \dots, x_n]$ dengan k adalah suatu lapangan dan n adalah bilangan bulat positif. Basis Gröbner bagi ideal $I \subseteq k[x_1, x_2, \dots, x_n]$ adalah suatu himpunan pembangun bagi I yang memiliki sifat penting dalam pembagian polinomial, yaitu sisa pembagian polinomial oleh basis Gröbner bersifat tunggal. Konsep basis Gröbner dapat digunakan untuk menyelesaikan sistem persamaan polinomial pada $k[x_1, x_2, \dots, x_n]$. Misalkan $f, g \in k[x_1, x_2, \dots, x_n]$. Polinomial f dikatakan kongruen g modulo I jika $f - g \in I$. Diberikan sistem kongruensi atas $k[x_1, x_2, \dots, x_n]$, yakni kumpulan kongruensi polinomial modulo ideal yang simultan. Masing-masing kongruensi pada sistem kongruensi tersebut dapat diubah menjadi persamaan polinomial, sehingga terbentuk sistem persamaan polinomial. Oleh karena itu, tujuan dari penelitian ini adalah mengkaji cara menyelesaikan sistem kongruensi atas $k[x_1, x_2, \dots, x_n]$ dengan basis Gröbner. Kemudian metode dari penyelesaian sistem kongruensi atas $k[x_1, x_2, \dots, x_n]$ dengan basis Gröbner diimplementasikan pada Singular-CAS. Berdasarkan hasil dan pembahasan, untuk menyelesaikan sistem kongruensi atas $k[x_1, x_2, \dots, x_n]$, pertama bentuk ideal J dan polinomial g yang bersesuaian dengan sistem kongruensi. Kemudian cari basis Gröbner G bagi ideal J dengan menetapkan terlebih dahulu order eliminasi. Setelah itu cari sisa pembagian dari g oleh G . Sisa pembagian ini menentukan eksistensi dari solusi bagi sistem kongruensi yang diberikan. Langkah penyelesaian ini kemudian diimplementasikan dalam bentuk dua prosedur yang berbeda pada Singular-CAS. Kesimpulan pada penelitian ini adalah diperoleh metode penyelesaian sistem kongruensi atas $k[x_1, x_2, \dots, x_n]$ dengan basis Gröbner dan metode penyelesaian tersebut berhasil diimplementasikan pada Singular-CAS dalam bentuk dua prosedur.

ABSTRACT

Fanani, Mohammad Zaenal. 2026. **Application of Gröbner Bases for Solving System of Congruence over Multivariable Polynomial Rings and Singular-CAS Implementation.** Undergraduate Thesis. Mathematics Study Program, Faculty of Science and Technology, Universitas Islam Negeri Maulana Malik Ibrahim Malang.

Advisors: (I) Dewi Ismiarti, M.Si., (II) Ari Kusumastuti, M.Si.

Keywords: congruence, Gröbner bases, multivariable polynomial rings, Singular-CAS, system of congruence over multivariable polynomial rings.

Given a multivariable polynomial ring $k[x_1, x_2, \dots, x_n]$ where k is a field and n is a positive integer. A Gröbner basis for an ideal $I \subseteq k[x_1, x_2, \dots, x_n]$ is a generating set for I that has an important property in polynomial division, namely that the remainder of a polynomial division by a Gröbner basis is unique. The concept of Gröbner bases can be used to solve systems of polynomial equations in $k[x_1, x_2, \dots, x_n]$. Let $f, g \in k[x_1, x_2, \dots, x_n]$. The polynomial f is said to be congruent to g modulo I if $f - g \in I$. Given a system of congruence equations over $k[x_1, x_2, \dots, x_n]$, that is a collection of simultaneous polynomial congruences modulo an ideal. each congruence in the congruence system can be transformed into a polynomial equation, thus forming a system of polynomial equations. Therefore, the purpose of this research is to examine how to solve systems of congruence equations over $k[x_1, x_2, \dots, x_n]$ using Gröbner bases. Then, the method for solving systems of congruence equations over $k[x_1, x_2, \dots, x_n]$ using Gröbner bases is implemented in Singular-CAS. Based on the results and discussion, to solve a system of congruence equations over $k[x_1, x_2, \dots, x_n]$, first form an ideal J and a polynomial g corresponding to the congruence system. Then, compute the Gröbner basis G for J by first determining the elimination order. After that, find the remainder of the division of g by G . The remainder of the division process determines the existence of a solution for the given congruence system. These methods then implemented in the form of two different procedures in Singular-CAS.

مستخلص البحث

الفناني، محمد زين. ٢٠٢٦. تطبيق قواعد جروبنر في حل أنظمة معادلات التطابق على حلقات كثيرات الحدود متعددة المتغيرات وتطبيقه في برنامج *Singular-CAS* البحث الجامعي. قسم الرياضيات، كلية العلوم والتكنولوجيا، جامعة مولانا مالك إبراهيم الإسلامية الحكومية مالانج.
المشرفان: (I) ديوي إسمياري، ماجستير في العلوم، (II) آري كوسوماستوتي، ماجستير في العلوم.

الكلمات الأساسية: قاعدة جروبنر، التطابق، حلقات كثيرات الحدود متعددة المتغيرات، نظام معادلات التطابق على حلقات كثيرات الحدود متعددة المتغيرات، *Singular-CAS*

بفرض وجود حلقة كثيرة حدود متعددة المتغيرات $k[x_1, x_2, \dots, x_n]$ حيث k يمثل حقلاً و n عدد صحيح موجب. قاعدة جروبنر للمثالي $I \subseteq k[x_1, x_2, \dots, x_n]$ هي مجموعة مولدة I تمتلك خاصية مهمة في قسمة كثيرات الحدود، وهي أن باقي قسمة كثيرة الحدود على قاعدة جروبنر يكون وحيداً. يمكن استخدام مفهوم قواعد جروبنر لحل أنظمة معادلات كثيرات الحدود في $k[x_1, x_2, \dots, x_n]$. نظام معادلات التطابق على $k[x_1, x_2, \dots, x_n]$ هو مجموعة من تطابقات كثيرات الحدود المتزامنة بمقياس مثالي. بينما بالنسبة لكثيرتي الحدود $f, g \in k[x_1, x_2, \dots, x_n]$ ، يُقال إن كثيرة الحدود f تطابق g بمقياس I إذا كان $f - g \in I$. إذا أُعطي نظام من معادلات التطابق على $k[x_1, x_2, \dots, x_n]$ ، يمكن تحويل كل تطابق في هذا النظام إلى معادلة كثيرة حدود، مما يشكل نظاماً من معادلات كثيرات الحدود. لذلك، هدف هذا البحث إلى دراسة كيفية حل أنظمة معادلات التطابق على $k[x_1, x_2, \dots, x_n]$ باستخدام قواعد جروبنر. بعد ذلك، تم تطبيق طريقة حل أنظمة معادلات التطابق على $k[x_1, x_2, \dots, x_n]$ باستخدام قواعد جروبنر في برنامج *Singular-CAS*. بناءً على النتائج والمناقشة، لحل نظام معادلات التطابق على $k[x_1, x_2, \dots, x_n]$ ، كَوْن أولاً المثالي J وكثيرة الحدود g المتوافقة مع نظام التطابق. ثم أوجد قاعدة جروبنر G للمثالي J بتحديد ترتيب الحذف أولاً. بعد ذلك، أوجد باقي قسمة g على G . يحدد باقي القسمة هذا وجود حل لنظام التطابق المعطى. ثم طبقت خطوات الحل هذه في شكل إجراءاتين مختلفتين في برنامج *Singular-CAS*.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Aljabar komputer adalah salah satu cabang pada matematika yang membahas tentang pengembangan algoritma dan *software computer* untuk memanipulasi ekspresi dan objek matematika. Hal ini juga termasuk komputasi untuk mendapatkan solusi eksak dari sistem persamaan polinomial. Meskipun solusi numerik lebih sering digunakan untuk menyelesaikan sistem persamaan yang muncul di berbagai bidang sains karena efisiensi dari komputasi, solusi eksak dapat memberikan informasi yang lebih menarik tentang sistem persamaan polinomial daripada solusi numerik (Gathen & Gerhard, 2003).

Salah satu topik yang dibahas pada aljabar komputer adalah basis Gröbner. Basis Gröbner merupakan himpunan pembangun dengan sifat tertentu bagi suatu ideal I pada ring komutatif $k[x_1, x_2, \dots, x_n]$ di mana k adalah lapangan. Sifat khusus ini adalah setiap suku utama dari polinomial pada I dapat dibagi oleh suatu suku utama dari anggota basis Gröbner. Basis Gröbner diperkenalkan oleh Bruno Buchberger pada tahun 1965 untuk mencari solusi dari sistem persamaan polinomial. Buchberger juga memperkenalkan algoritma untuk mengkomputasikan basis Gröbner, yang kemudian disebut sebagai algoritma Buchberger (Buchberger, 2006). Sejak saat itu, kajian tentang basis Gröbner dan aplikasinya terus berkembang hingga saat ini.

Basis Gröbner dapat diaplikasikan pada bidang-bidang matematika yang lain. Salah satu yang mendasar adalah mencari himpunan solusi dari sistem persamaan polinomial. Basis Gröbner juga dapat diaplikasikan pada bidang teori graf terkait

masalah pewarnaan, pada teori modul terkait masalah keanggotaan modul, pada riset operasi terkait *integer programming*, dan masih banyak lagi (Adams & Loustaunau, 1996). Di luar matematika, basis Gröbner dapat diaplikasikan ke bidang robotik terkait permasalahan kinematik (Cox, Little, & O'Shea, 2015) dan bidang pemrosesan sinyal dan gambar terkait *wavelet* (Lin, Xu, & Wu, 2004).

Salah satu konsep yang mendasar pada teori bilangan adalah kongruensi. Misalkan a, b , dan m adalah bilangan bulat dengan m bilangan bulat positif. Bilangan bulat a dikatakan kongruen b modulo m jika m membagi $a-b$. Dari beberapa kongruensi dapat dibentuk sebuah sistem kongruensi. Salah satu cara untuk menyelesaikan sistem kongruensi adalah dengan mengubah setiap kongruensi menjadi sebuah persamaan, atau yang biasa disebut sebagai persamaan diophantine (Rosen, 2005).

Konsep kongruensi ini kemudian didefinisikan pada ring polinomial multivariabel. Misalkan f, g adalah polinomial pada $k[x_1, x_2, \dots, x_n]$ dan I adalah ideal pada $k[x_1, x_2, \dots, x_n]$. Polinomial f dikatakan kongruen g modulo I jika $f - g \in I$. Dari beberapa kongruensi dapat dibentuk sistem kongruensi atas ring polinomial multivariabel. Setiap kongruensi pada sistem tersebut dapat diubah menjadi persamaan polinomial, kemudian akan membentuk sistem persamaan polinomial. Penelitian kali ini bertujuan untuk mengetahui kapan suatu sistem kongruensi memiliki solusi dengan menggunakan basis Gröbner. Jika ya, akan dikaji bagaimana himpunan solusi dari sistem kongruensi tersebut (Adams & Loustaunau, 1996).

Aljabar komputer dalam hal ini dapat dipandang sebagai cabang matematika yang memberikan pedoman untuk menyelesaikan berbagai macam permasalahan

yang ada di cabang matematika yang lain, salah satunya adalah pedoman untuk menyelesaikan sistem kongruensi atas ring polinomial multivariabel. Alat utama yang dipakai adalah basis Gröbner. Dalam perspektif Islam, seorang muslim harus menempatkan Al-Qur'an sebagai pedoman bagi kehidupan manusia, sebagaimana tertuang dalam Surat Al-Jatsiyah ayat 20

هَذَا بَصَائِرُ لِلنَّاسِ وَهُدًى وَرَحْمَةٌ لِّقَوْمٍ يُوقِنُونَ ﴿٢٠﴾

“Ini (Al-Qur'an) adalah pedoman bagi manusia, petunjuk, dan rahmat bagi kaum yang meyakini(-nya).”

Berdasarkan tafsir Al-Muyassar dari Kementerian Agama Saudi Arabia, berikut ini tafsir dari ayat tersebut. Al-Quran yang Kami turunkan kepadamu ini (wahai Rasul) adalah penerang, dengannya manusia melihat antara yang haq dengan yang bathil, dengannya mereka mengetahui jalan yang lurus, petunjuk dan rahmat bagi kaum yang meyakini kebenaran sejatinya dan bahwa ia diturunkan dari Allah yang Maha perkasa lagi Maha bijaksana.

Salah satu yang ditekankan dari tafsir tersebut adalah Al-Qur'an merupakan pedoman bagi umat manusia untuk melihat secara gamblang perbedaan dari haq dan bathil. Melalui paradigma integrasi ini, metode penyelesaian sistem kongruensi atas ring polinomial multivariabel dengan basis Gröbner dapat dipandang sebagai representasi rasional dari ikhtiar manusia dalam menciptakan pedoman untuk menyingkirkan ambiguitas matematika sehingga solusi sistem kongruensi yang valid didapatkan.

Bersamaan dengan berkembangnya teori basis Gröbner, dikembangkan juga *software* untuk melakukan komputasi basis Gröbner, seperti CoCoA, Macaulay, dan Singular. *Software* semacam ini disebut sebagai *Computer Algebra System* (CAS). Khususnya Singular, salah satu dari CAS dirancang untuk komputasi dalam

aljabar komutatif, geometri aljabar, dan teori singularitas. Sistem ini terutama digunakan untuk perhitungan yang melibatkan polinomial multivariabel, ideal, modul, dan varietas aljabar. Singular sangat efisien dalam menghitung basis Gröbner, yang merupakan fondasi untuk banyak algoritma dalam aljabar komutatif dan geometri aljabar komputasional (Greuel & Pfister, 2007). Oleh karena itu pada penelitian ini, akan dibuat prosedur untuk menyelesaikan sistem kongruensi atas ring polinomial multivariabel menggunakan Singular-CAS.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, rumusan masalah penelitian kali ini adalah sebagai berikut:

1. Bagaimana penyelesaian sistem kongruensi atas ring polinomial multivariabel dengan basis Gröbner?
2. Bagaimana implementasi dari metode penyelesaian sistem kongruensi atas ring polinomial multivariabel dengan basis Gröbner pada Singular-CAS?

1.3 Tujuan Penelitian

Berdasarkan latar belakang di atas, rumusan masalah penelitian kali ini adalah sebagai berikut:

1. Untuk mengetahui penyelesaian sistem kongruensi atas ring polinomial multivariabel dengan basis Gröbner.
2. Untuk mengimplementasikan metode penyelesaian sistem kongruensi atas ring polinomial multivariabel dengan basis Gröbner pada Singular-CAS.

1.4 Manfaat Penelitian

Penelitian ini diharapkan memberikan manfaat sebagai berikut:

1. Bagi penulis yaitu dapat mengetahui proses penyelesaian sistem kongruensi atas ring polinomial multivariabel dengan basis Gröbner dan implementasinya pada Singular-CAS.
2. Bagi peneliti selanjutnya yaitu dapat dijadikan rujukan penelitian bidang Matematika khususnya mengenai topik yang berhubungan dengan aljabar komputer dan aplikasinya.

1.5 Batasan Masalah

Adapun batasan masalah pada penelitian ini adalah sebagai berikut:

1. Ring polinomial yang dikaji adalah ring polinomial multivariabel atau ring polinomial dalam n variabel dengan koefisiennya merupakan suatu lapangan k , dengan n adalah sebarang bilangan bulat positif. Ring polinomial multivariabel ini dapat ditulis sebagai ring komutatif $k[x_1, x_2, \dots, x_n]$.
2. Basis Gröbner yang dikaji adalah basis Gröbner bagi sebarang ideal I dari $k[x_1, x_2, \dots, x_n]$.
3. Kongruensi yang dikaji adalah kongruensi dari sebarang polinomial f modulo polinomial g ideal I pada $k[x_1, x_2, \dots, x_n]$, yang dinotasikan sebagai $f \equiv g \pmod{I}$. Sistem kongruensi adalah kumpulan beberapa kongruensi, dalam bentuk $f \equiv f_i \pmod{I_i}$ beserta himpunan solusinya untuk $i = 1, 2, \dots, m$ dengan f, f_i merupakan polinomial dan I_i merupakan ideal pada $k[x_1, x_2, \dots, x_n]$.

4. Solusi dari sistem kongruensi atas ring $k[x_1, x_2, \dots, x_n]$ adalah kumpulan polinomial yang memenuhi sistem kongruensi tersebut.
5. Penyelesaian sistem kongruensi pada penelitian ini adalah metode mencari solusi dari sistem kongruensi atas ring $k[x_1, x_2, \dots, x_n]$.
6. *Software* Singular-CAS digunakan untuk membuat prosedur penyelesaian sistem kongruensi atas ring $k[x_1, x_2, \dots, x_n]$ dengan bantuan komputer.

BAB II

KAJIAN TEORI

2.1 Ring

Pada penelitian ini, sistem kongruensi dinyatakan dalam bahasa ring. Sehingga dibutuhkan definisi dasar ring.

Definisi 2.1.1 Misalkan R adalah himpunan tak kosong yang dilengkapi dengan dua operasi biner, penjumlahan dan perkalian. Himpunan R disebut sebagai ring jika untuk setiap $a, b, c \in R$ berlaku

1. Penjumlahan pada R bersifat asosiatif, yaitu $(a + b) + c = a + (b + c)$.
2. Himpunan R memiliki identitas penjumlahan, yaitu terdapat $0 \in R$ sehingga $a + 0 = 0 + a = a$.
3. Setiap anggota R memiliki invers terhadap penjumlahan, yaitu untuk setiap $a \in R$, terdapat $-a \in R$ sehingga $a + (-a) = 0$.
4. Penjumlahan pada R bersifat komutatif, yaitu $a + b = b + a$.
5. Perkalian pada R bersifat asosiatif, yaitu $a(bc) = (ab)c$.
6. Penjumlahan dan perkalian pada R memenuhi sifat distributif, yaitu $a(b + c) = ab + ac$ dan $(a + b)c = ac + bc$.

Kemudian pada ring R , didefinisikan $a - b$ sebagai $a + (-b)$ untuk setiap $a, b \in R$, di mana $-b$ adalah invers dari b terhadap penjumlahan. Lebih lanjut jika untuk setiap $a, b \in R$, $ab = ba$ maka R disebut ring komutatif. Jika R memiliki identitas perkalian, yang dinotasikan sebagai 1, maka R disebut ring dengan kesatuan. Ring R yang memenuhi keduanya disebut sebagai ring komutatif dengan kesatuan. Pada ring dengan kesatuan, suatu $r \neq 0$ dikatakan unit jika terdapat $r^{-1} \in R$ sedemikian sehingga $rr^{-1} = 1$. Jika setiap elemen tak nol dari ring komutatif dengan kesatuan

merupakan unit, maka R disebut sebagai lapangan. Lapangan dalam pembahasan kali ini dinotasikan sebagai k (Gallian, 2013).

Contoh 2.1.2 Berikut ini beberapa contoh dari ring.

1. Himpunan $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, dan $\mathbb{C}$ semuanya merupakan ring. Himpunan $\mathbb{Q}$, $\mathbb{R}$, dan $\mathbb{C}$ merupakan lapangan tetapi $\mathbb{Z}$ bukan lapangan, karena $2 \in \mathbb{Z}$ bukan merupakan unit.
2. Himpunan bilangan bulat modulo n , dinotasikan sebagai $\mathbb{Z}_n$, merupakan ring.
3. Himpunan polinomial dalam satu variabel x dengan koefisiennya berada di lapangan k , yang dinotasikan sebagai $k[x]$, merupakan ring.

Definisi 2.1.3 Subhimpunan S dari ring R , dikatakan sebagai subring dari R jika S juga merupakan ring dengan operasi yang sama seperti pada R (Gallian, 2013).

Berikut adalah teorema yang dapat digunakan untuk menentukan apakah suatu subhimpunan dari R merupakan subring dari R .

Teorema 2.1.4 Subhimpunan tak kosong S dari ring R merupakan subring dari R jika untuk setiap $a, b \in S$ berlaku

1. $a - b \in S$;
2. $ab \in S$

(Gallian, 2013).

2.1.1 Ideal

Pada teori ring, terdapat satu jenis subring yang memiliki sifat khusus. Sifat khusus ini yang memegang peran penting dalam penelitian mengenai sistem persamaan kongruensi.

Definisi 2.1.1.1 Misalkan I adalah subring dari ring R . Subring I merupakan ideal pada R jika untuk setiap $r \in R$ dan $s \in I$, $rs \in I$ dan $sr \in I$. Jika untuk setiap anggota dari ideal I dapat dinyatakan sebagai kombinasi linier dari $a_1, a_2, \dots, a_s \in R$, yaitu untuk setiap $a \in I$ terdapat $r_1, r_2, \dots, r_s \in R$ sehingga

$$a = r_1 a_1 + r_2 a_2 + \dots + r_s a_s,$$

maka I dikatakan dibangun secara hingga oleh $a_1, a_2, \dots, a_s$. Ideal ini dilambangkan sebagai $I = \langle a_1, a_2, \dots, a_s \rangle = \{\sum_{i=1}^s r_i a_i \mid r_i \in R\}$ (Gallian, 2013).

Contoh 2.1.1.2 Berikut ini adalah beberapa contoh dari ideal.

1. Misalkan $\mathbb{Z}$ adalah ring. Himpunan bilangan genap dari $\mathbb{Z}$ adalah ideal pada $\mathbb{Z}$.
2. Misalkan S adalah himpunan bilangan ganjil dari $\mathbb{Z}$. Himpunan S bukan merupakan ideal, karena $3 \in S$ dan $2 \in \mathbb{Z}$, tetapi $3 \cdot 2 = 6 \notin S$.

Berikut adalah teorema yang dapat digunakan untuk menentukan apakah suatu subhimpunan dari R merupakan ideal pada R .

Teorema 2.1.1.3 Misalkan I adalah subhimpunan dari ring R . Subhimpunan I merupakan ideal pada R jika untuk setiap $a, b \in I$ dan $r \in R$ berlaku

1. $a - b \in I$;
2. $ra \in I$ dan $ar \in I$.

(Gallian, 2013).

Pada penelitian ini, terdapat dua objek yang berkaitan dengan ideal yang akan digunakan pada pembahasan.

Definisi 2.1.1.4 Misalkan R adalah ring, I adalah ideal pada R , dan $r \in R$. Didefinisikan koset dari I sebagai

$$r + I = \{r + a \mid a \in I\}$$

(Gallian, 2013).

Definisi 2.1.1.5 Misalkan R adalah ring, I adalah ideal pada R , dan $r \in R$.

Didefinisikan rI sebagai

$$rI = \{ra | a \in I\}$$

(Gallian, 2013).

Teorema 2.1.1.6 Misalkan R adalah ring, I adalah ideal pada R . Untuk setiap $r \in R$, rI adalah ideal pada R . Lebih lanjut jika $I = \langle a_1, a_2, \dots, a_s \rangle$ di mana $a_1, a_2, \dots, a_s \in R$, maka $rI = \langle ra_1, ra_2, \dots, ra_s \rangle$ (Gallian, 2013).

2.1.2 Ring Polinomial Multivariabel, Order Suku, dan Algoritma Pembagian

Sistem kongruensi terdefinisi pada polinomial multivariabel. Oleh karena itu dibutuhkan definisi dari ring polinomial multivariabel. Sebelum itu ada satu definisi yang dibutuhkan.

Definisi 2.1.2.1 Misalkan $x_1, x_2, \dots, x_n$ adalah variabel. Hasil kali perpangkatan pada $x_1, x_2, \dots, x_n$ adalah ekspresi dalam bentuk

$$x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$$

dengan $\alpha_i \in \mathbb{Z}_{\geq 0}$, untuk $1 \leq i \leq n$. Himpunan hasil kali perpangkatan pada $x_1, x_2, \dots, x_n$, yang dilambangkan sebagai $\mathbb{T}^n$, didefinisikan sebagai

$$\mathbb{T}^n = \{x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n} \mid \alpha_i \in \mathbb{Z}_{\geq 0}, 1 \leq i \leq n\}.$$

Hasil kali perpangkatan $x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$ juga dapat ditulis dalam bentuk $\mathbf{x}^\alpha$ dengan $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n$. Sedangkan untuk lapangan k , ekspresi dalam bentuk $ax_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$ di mana $a \in k$ disebut sebagai suku (*term*) (Adams & Loustaunau, 1996).

Definisi 2.1.2.2 Misalkan $x_1, x_2, \dots, x_n$ adalah variabel dan $\mathbb{T}^n$ adalah hasil kali perpangkatan pada $x_1, x_2, \dots, x_n$.

1. Polinomial f dalam n variabel atau polinomial multivariabel dengan koefisiennya berada di lapangan k adalah jumlahan berhingga dari suku-suku dalam bentuk $a_\alpha x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$, yaitu

$$f = \sum_{\alpha} a_{\alpha} x^{\alpha} = \sum_{\alpha \in \mathbb{Z}_{\geq 0}^n}^{\text{berhingga}} a_{\alpha_1 \alpha_2 \dots \alpha_n} x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}.$$

2. Himpunan semua polinomial dalam n variabel dengan koefisiennya berada di lapangan k berbentuk

$$\left\{ \sum_{\alpha \in \mathbb{Z}_{\geq 0}^n}^{\text{berhingga}} a_{\alpha_1 \alpha_2 \dots \alpha_n} x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n} \mid a_{\alpha_1 \alpha_2 \dots \alpha_n} \in k, \alpha_i \in \mathbb{Z}_{\geq 0}, 1 \leq i \leq n \right\}.$$

3. Misalkan $f = \sum_{\alpha} a_{\alpha} x^{\alpha}$ dan $g = \sum_{\beta} b_{\beta} x^{\beta}$ adalah polinomial dalam n variabel. Didefinisikan penjumlahan sebagai

$$f + g = \sum_{\alpha} a_{\alpha} x^{\alpha} + \sum_{\beta} b_{\beta} x^{\beta} = \sum_{\gamma} (a_{\gamma} + b_{\gamma}) x^{\gamma}$$

dengan

$$a_{\gamma} = \begin{cases} a_{\alpha}, & x^{\gamma} = x^{\alpha} \\ 0, & x^{\gamma} \neq x^{\alpha} \end{cases}$$

$$b_{\gamma} = \begin{cases} b_{\beta}, & x^{\gamma} = x^{\beta} \\ 0, & x^{\gamma} \neq x^{\beta} \end{cases}$$

Didefinisikan perkalian pada polinomial dalam n variabel sebagai

$$fg = \sum_{\alpha} a_{\alpha} x^{\alpha} \sum_{\beta} b_{\beta} x^{\beta} = \sum_{\gamma} \left(\sum_{\alpha+\beta=\gamma} (a_{\alpha} b_{\beta}) x^{\gamma} \right)$$

(Greuel & Pfister, 2007).

Teorema 2.1.2.3 Himpunan polinomial dalam n variabel yang dilengkapi dengan dua operasi yang didefinisikan pada Definisi 2.1.2.2. merupakan ring komutatif dengan kesatuan. Ring ini dilambangkan sebagai $k[x_1, x_2, \dots, x_n]$.

Bukti. Misalkan $f, g, h \in k[x_1, x_2, \dots, x_n]$ dengan $f = \sum_{\alpha} a_{\alpha} \mathbf{x}^{\alpha}, g = \sum_{\beta} b_{\beta} \mathbf{x}^{\beta}$, dan $h = \sum_{\gamma} c_{\gamma} \mathbf{x}^{\gamma}$ di mana $a_{\alpha}, b_{\beta}, c_{\gamma} \in k$ dan $\mathbf{x}^{\alpha}, \mathbf{x}^{\beta}, \mathbf{x}^{\gamma}$ hasil perpangkatan pada $x_1, x_2, \dots, x_n$.

1. Penjumlahan pada $k[x_1, x_2, \dots, x_n]$ bersifat asosiatif. Perhatikan bahwa

$$\begin{aligned} (f + g) + h &= \sum_{\delta} (a_{\delta} + b_{\delta}) \mathbf{x}^{\delta} + \sum_{\gamma} c_{\gamma} \mathbf{x}^{\gamma} \\ &= \sum_{\delta} (a_{\delta} + b_{\delta} + c_{\delta}) \mathbf{x}^{\delta} \\ &= \sum_{\alpha} a_{\alpha} \mathbf{x}^{\alpha} + \sum_{\delta} (b_{\delta} + c_{\delta}) \mathbf{x}^{\delta} \\ &= f + (g + h). \end{aligned}$$

2. Terdapat $0 \in k[x_1, x_2, \dots, x_n]$ sebagai identitas penjumlahan pada $k[x_1, x_2, \dots, x_n]$.

3. Invers dari f terhadap penjumlahan adalah $-f = \sum_{\alpha} -a_{\alpha} \mathbf{x}^{\alpha}$.

4. Penjumlahan pada $k[x_1, x_2, \dots, x_n]$ bersifat komutatif. Perhatikan bahwa

$$f + g = \sum_{\delta} (a_{\delta} + b_{\delta}) \mathbf{x}^{\delta} = \sum_{\delta} (b_{\delta} + a_{\delta}) \mathbf{x}^{\delta} = g + f.$$

5. Perkalian pada $k[x_1, x_2, \dots, x_n]$ bersifat asosiatif. Perhatikan bahwa

$$\begin{aligned} (fg)h &= \sum_{\delta} \left(\sum_{\alpha+\beta=\delta} (a_{\alpha} b_{\beta}) \mathbf{x}^{\delta} \right) \sum_{\gamma} c_{\gamma} \mathbf{x}^{\gamma} \\ &= \sum_{\epsilon} \left(\sum_{\alpha+\beta+\gamma=\epsilon} (a_{\alpha} b_{\beta} c_{\gamma}) \mathbf{x}^{\epsilon} \right) \end{aligned}$$

$$\begin{aligned}
&= \sum_{\alpha} a_{\alpha} \mathbf{x}^{\alpha} \sum_{\delta} \left(\sum_{\beta+\gamma=\delta} (b_{\beta} c_{\gamma}) \mathbf{x}^{\delta} \right) \\
&= f(gh).
\end{aligned}$$

6. Penjumlahan dan perkalian pada $k[x_1, x_2, \dots, x_n]$ bersifat distributif.

Perhatikan bahwa

$$\begin{aligned}
f(g+h) &= \sum_{\alpha} a_{\alpha} \mathbf{x}^{\alpha} \sum_{\delta} (b_{\delta} + c_{\delta}) \mathbf{x}^{\delta} \\
&= \sum_{\epsilon} \left(\sum_{\alpha+\delta=\epsilon} (a_{\alpha} (b_{\delta} + c_{\delta})) \mathbf{x}^{\epsilon} \right) \\
&= \sum_{\epsilon} \left(\sum_{\alpha+\delta=\epsilon} (a_{\alpha} b_{\delta} + a_{\alpha} c_{\delta}) \mathbf{x}^{\epsilon} \right) \\
&= \sum_{\epsilon} \left(\sum_{\alpha+\delta=\epsilon} a_{\alpha} b_{\delta} \mathbf{x}^{\epsilon} \right) + \sum_{\epsilon} \left(\sum_{\alpha+\delta=\epsilon} a_{\alpha} c_{\delta} \mathbf{x}^{\epsilon} \right) \\
&= fg + gh \\
(f+g)h &= \sum_{\delta} (a_{\delta} + b_{\delta}) \mathbf{x}^{\delta} \sum_{\gamma} c_{\gamma} \mathbf{x}^{\gamma} \\
&= \sum_{\epsilon} \left(\sum_{\alpha+\delta=\epsilon} ((a_{\delta} + b_{\delta}) c_{\gamma}) \mathbf{x}^{\epsilon} \right) \\
&= \sum_{\epsilon} \left(\sum_{\alpha+\delta=\epsilon} (a_{\alpha} b_{\delta} + a_{\alpha} c_{\delta}) \mathbf{x}^{\epsilon} \right) \\
&= \sum_{\epsilon} \left(\sum_{\alpha+\delta=\epsilon} a_{\alpha} b_{\delta} \mathbf{x}^{\epsilon} \right) + \sum_{\epsilon} \left(\sum_{\alpha+\delta=\epsilon} a_{\alpha} c_{\delta} \mathbf{x}^{\epsilon} \right) \\
&= fg + gh.
\end{aligned}$$

7. Terdapat $1 \in k[x_1, x_2, \dots, x_n]$ sebagai identitas perkalian pada $k[x_1, x_2, \dots, x_n]$.

8. Perkalian pada $k[x_1, x_2, \dots, x_n]$ bersifat komutatif. Perhatikan bahwa

$$fg = \sum_{\delta} \left(\sum_{\alpha+\beta=\delta} (a_{\alpha}b_{\beta}) \right) x^{\delta} = \sum_{\delta} \left(\sum_{\beta+\alpha=\delta} (b_{\beta}a_{\alpha}) \right) x^{\delta} = gf.$$

Jadi, $k[x_1, x_2, \dots, x_n]$ merupakan ring komutatif dengan kesatuan.

Pembagian pada polinomial multivariabel sedikit berbeda dengan pembagian polinomial satu variabel. Perbedaan ini terletak pada aturan pengurutan suku polinomial sebelum melakukan proses pembagian. Hal ini dilakukan agar proses pembagian dapat berhenti dan menghasilkan hasil bagi beserta sisa bagi. Pada polinomial satu variabel, pengurutan dari suku pada polinomial dapat dilakukan dengan melihat perpangkatan terbesar. Pada polinomial multivariabel, terdapat beberapa aturan untuk pengurutan dari suku pada polinomial. Aturan pengurutan ini disebut sebagai order suku.

Definisi 2.1.2.4 Suatu order suku $<$ pada $\mathbb{T}^n$ disebut orde total jika memenuhi kondisi berikut:

1. $1 < x^{\beta}$, untuk setiap $x^{\beta} \in \mathbb{T}^n$ dan $x^{\beta} \neq 1$;
2. Jika $x^{\alpha} < x^{\beta}$, maka $x^{\alpha}x^{\gamma} < x^{\beta}x^{\gamma}$, untuk setiap $x^{\gamma} \in \mathbb{T}^n$

(Adams & Loustaunau, 1996).

Pada $k[x_1, x_2, \dots, x_n]$ terdapat berbagai macam orde suku yang dapat digunakan untuk melakukan komputasi pembagian. Berikut ini adalah tiga diantaranya yang akan digunakan pada penelitian ini.

Definisi 2.1.2.5 Misalkan $x^{\alpha}, x^{\beta} \in \mathbb{T}^n$ dengan $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$ dan $\beta = (\beta_1, \beta_2, \dots, \beta_n)$. Didefinisikan order leksikografis pada $\mathbb{T}^n$ dengan $x_1 > x_2 > \dots > x_n$ sebagai

$$x^\alpha < x^\beta \Leftrightarrow \begin{cases} \alpha_i < \beta_i \text{ untuk suatu } i \in \{1, 2, \dots, n\} \text{ dan} \\ \alpha_j = \beta_j \text{ untuk setiap } j < i \end{cases}$$

(Adams & Lousaunau, 1996).

Definisi 2.1.2.6 Misalkan $x^\alpha, x^\beta \in \mathbb{T}^n$ dengan $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$ dan $\beta = (\beta_1, \beta_2, \dots, \beta_n)$. Didefinisikan order leksikografis derajat pada $\mathbb{T}^n$ dengan $x_1 > x_2 > \dots > x_n$ sebagai

$$x^\alpha < x^\beta \Leftrightarrow \begin{cases} \sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i \\ \text{atau} \\ \sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i \text{ dan } x^\alpha < x^\beta \text{ terhadap derajat leksikografis} \\ \text{dengan } x_1 > x_2 > \dots > x_n \end{cases}$$

(Adams & Lousaunau, 1996).

Definisi 2.1.2.7 Misalkan $x^\alpha, x^\beta \in \mathbb{T}^n$ dengan $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$ dan $\beta = (\beta_1, \beta_2, \dots, \beta_n)$. Didefinisikan order leksikografis balikan derajat pada $\mathbb{T}^n$ dengan $x_1 > x_2 > \dots > x_n$ sebagai

$$x^\alpha < x^\beta \Leftrightarrow \begin{cases} \sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i \\ \text{atau} \\ \sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i \text{ dan } \alpha_i > \beta_i \text{ untuk suatu } i \in \{1, 2, \dots, n\} \text{ dan} \\ \alpha_j = \beta_j \text{ untuk setiap } j > i \end{cases}$$

(Adams & Lousaunau, 1996).

Teorema 2.1.2.8 Setiap order suku pada $\mathbb{T}^n$ terurut dengan baik, yaitu untuk setiap subhimpunan A dari $\mathbb{T}^n$ terdapat $x^\alpha \in A$ yang memenuhi $x^\alpha \leq x^\beta$ untuk setiap $x^\beta \in A$ (Adams & Lousaunau, 1996).

Contoh 2.1.2.9 Misalkan $f = x^2yz^3$ dan $g = xy^3z^2$ adalah hasil kali perpangkatan dalam variabel x, y, z dengan $x > y > z$. Misalkan perpangkatan

dari variabel pada f adalah $\alpha = (2,1,3) = (\alpha_1, \alpha_2, \alpha_3)$ dan perpangkatan dari variabel pada g adalah $\beta = (1,3,2) = (\beta_1, \beta_2, \beta_3)$. Berdasarkan order leksikografis, karena $\beta_1 < \alpha_1$, maka

$$xy^3z^2 < x^2yz^3.$$

Berdasarkan order leksikografis derajat, karena $\alpha_1 + \alpha_2 + \alpha_3 = 2 + 2 + 2 = 6 = 2 + 1 + 3 = \beta_1 + \beta_2 + \beta_3$ dan $x^2yz^3 < x^2y^2z^2$ terhadap derajat leksikografis, maka

$$xy^3z^2 < x^2yz^3.$$

Berdasarkan order leksikografis balikan derajat, karena $\alpha_1 + \alpha_2 + \alpha_3 = \beta_1 + \beta_2 + \beta_3$ dan $\beta_3 < \alpha_3$, maka

$$xy^3z^2 > x^2yz^3.$$

Misalkan terdapat dua himpunan variabel $\{x_1, x_2, \dots, x_n\}$ dan $\{y_1, y_2, \dots, y_m\}$. Tulis hasil kali perpangkatan pada variabel $\{x_1, x_2, \dots, x_n\}$ sebagai hasil kali perpangkatan pada variabel x dan hasil kali perpangkatan pada variabel $\{y_1, y_2, \dots, y_m\}$ sebagai hasil kali perpangkatan pada variabel y . Tulis $<_x$ dan $<_y$ berturut-turut sebagai order suku pada x dan y . Didefinisikan order suku $<$ pada variabel x dan y sebagai berikut.

Definisi 2.1.2.10 Misalkan X_1, X_2 adalah suku pada variabel x dan Y_1, Y_2 adalah suku pada variabel y . Didefinisikan

$$X_1Y_1 < X_2Y_2 \Leftrightarrow \begin{cases} X_1 <_x X_2 \\ \text{atau} \\ X_1 = X_2, Y_1 <_y Y_2 \end{cases}$$

Order suku di atas disebut sebagai order eliminasi dengan variabel x lebih besar dari variabel y (Adams & Lousaunau, 1996).

Teorema 2.1.2.11 Order eliminasi merupakan order suku. Lebih lanjut $Y_1 < XY_2$ untuk sebarang hasil kali perpangkatan Y_1, Y_2 pada variabel y dan hasil kali pangkat pada X variabel x dengan suatu x_i memiliki pangkat positif (Adams & Lousstaunau, 1996).

Jika x dan y masing-masing berorder leksikografis, maka eliminasi order juga berorder leksikografis dengan variabel y lebih kecil dari variabel x . Sehingga order eliminasi dapat dipandang sebagai perumuman dari order leksikografis.

Berikut ini adalah contoh perbandingan hasil kali perpangkatan terhadap order eliminasi.

Contoh 2.1.2.12 Misalkan x_1, x_2, y_1 , dan y_2 adalah variabel. Tetapkan order leksikografis derajat pada x_1 dan x_2 dengan $x_1 > x_2$. Tulis $<_x$ sebagai order suku pada x_1 dan x_2 . Tetapkan order leksikografis pada y_1 dan y_2 dengan $y_1 > y_2$. Tulis $<_x$ sebagai order suku pada y_1 dan y_2 . Tetapkan order eliminasi dengan variabel x_1, x_2 lebih besar dari variabel y_1, y_2 . Misalkan $x_1^2 x_2^3 y_1^5$ dan $x_1^4 x_2^4 y_2$ adalah hasil kali perpangkatan pada x_1, x_2, y_1 , dan y_2 . Maka

$$x_1^2 x_2^3 y_1^5 < x_1^4 x_2^4 y_2$$

karena $x_1^2 x_2^3 <_x x_1^4 x_2^4$. Sedangkan untuk $x_1^2 x_2^3 y_2^6$,

$$x_1^2 x_2^3 y_1^5 > x_1^2 x_2^3 y_2^6$$

$x_1^2 x_2^3 = x_1^2 x_2^3$ dan $y_1^5 > y_2^6$.

Setelah ditentukan order suku yang dipakai pada $k[x_1, x_2, \dots, x_n]$, maka pembagian pada $k[x_1, x_2, \dots, x_n]$ dapat dilakukan secara efektif. Sebelum itu,

berikut ini beberapa notasi dan istilah yang digunakan sesudah memilih order suku.

Definisi 2.1.2.13 Tetapkan sebuah order pada $k[x_1, x_2, \dots, x_n]$. Untuk setiap $f \neq 0 \in k[x_1, x_2, \dots, x_n]$ dapat ditulis sebagai

$$f = a_1 \mathbf{x}^{\alpha_1} + a_2 \mathbf{x}^{\alpha_2} + \dots + a_r \mathbf{x}^{\alpha_r}$$

dengan $a_i \neq 0 \in k, \mathbf{x}^{\alpha_i} \in \mathbb{T}^n$ untuk setiap $i \in \{1, 2, \dots, r\}$ dan $\mathbf{x}^{\alpha_1} > \mathbf{x}^{\alpha_2} > \dots > \mathbf{x}^{\alpha_r}$. Lebih lanjut

1. $\text{lp}(f) = \mathbf{x}^{\alpha_1}$ adalah hasil kali perpangkatan utama (*leading power product*) dari f ;
2. $\text{lc}(f) = a_1$ adalah koefisien utama (*leading coefficient*) dari f ;
3. $\text{lt}(f) = a_1 \mathbf{x}^{\alpha_1}$ adalah suku utama (*leading term*) dari f

(Adams & Loustaunau, 1996).

Contoh 2.1.2.14 Tetapkan order leksikografis derajat pada $\mathbb{Q}[x, y, z]$ dengan $x > y > z$. Misalkan $f = -\frac{1}{2}x^6z^2 + 4x^5y^3z + 3x^2y$. Maka

$$\text{lp}(f) = x^5y^3z$$

$$\text{lc}(f) = 4$$

$$\text{lt}(f) = 4x^5y^3z$$

Selanjutnya akan didefinisikan terlebih dahulu kapan suatu suku polinomial dikatakan membagi suku polinomial lain dan kapan suatu polinomial dikatakan membagi polinomial lain.

Definisi 2.1.2.15 Misalkan X dan Y adalah suku pada variabel $x_1, x_2, \dots, x_n$ dalam bentuk $X = ax_1^{\alpha_1}x_2^{\alpha_2} \dots x_n^{\alpha_n}$ dan $Y = bx_1^{\beta_1}x_2^{\beta_2} \dots x_n^{\beta_n}$ dengan $a, b \in k$. Suku Y dikatakan membagi X jika $\beta_i \leq \alpha_i$ untuk setiap $i \in \{1, 2, \dots, n\}$.

Definisi 2.1.2.16 Misalkan $f, g \in k[x_1, x_2, \dots, x_n]$. Polinomial g dikatakan membagi f jika terdapat $q \in k[x_1, x_2, \dots, x_n]$ sehingga

$$f = qg.$$

Berikut ini kasus khusus dari pembagian suatu polinomial f dengan polinomial g dalam satu langkah.

Definisi 2.1.2.17 Misalkan $k[x_1, x_2, \dots, x_n]$ adalah ring polinomial pada $x_1, x_2, \dots, x_n$ dengan koefisien pada lapangan k . Untuk $f, g, h \in k[x_1, x_2, \dots, x_n]$ dengan $g \neq 0$, polinomial f dikatakan tereduksi ke h modulo g pada satu langkah jika dan hanya jika $\text{lp}(g)$ membagi suatu hasil kali perpangkatan X pada f dan

$$h = f - \frac{X}{\text{lt}(g)}g$$

Polinomial f tereduksi ke h modulo g dapat ditulis sebagai

$$f \xrightarrow{g} h$$

atau

$$f \xrightarrow{Y, g} h$$

dengan $Y = \frac{X}{\text{lt}(g)}$ (Adams & Loustaunau, 1996).

Proses mendapatkan polinomial h dari polinomial f dan g berdasarkan Definisi 2.1.2.17 inilah yang disebut sebagai pembagian polinomial f dengan polinomial g dalam satu langkah.

Contoh 2.1.2.18 Misalkan $f = 3x^2y^2z - x^2y$ dan $g = 2xy - 4y$ adalah polinomial pada $\mathbb{Q}[x, y, z]$ terhadap order leksikografis derajat dengan $x > y >$

z. Misalkan $X = x^2y^2z$ adalah salah satu dari hasil kali perpangkatan pada f .

Karena $\text{lp}(g) = xy$ membagi X dan

$$\begin{aligned} h &= f - \frac{X}{\text{lt}(g)}g \\ &= (3x^2y^2z - x^2y) - \frac{3x^2y^2z}{2xy}(2xy - 4y) \\ &= (3x^2y^2z - x^2y) - \frac{3}{2}xyz(2xy - 4y) \\ &= (3x^2y^2z - x^2y) - (3x^2y^2z - 6xy^2z) \\ &= 6xy^2z - x^2y \end{aligned}$$

maka

$$f \xrightarrow{\frac{3}{2}xyz, g} 6xy^2z - x^2y$$

Pembagian polinomial yang sudah didefinisikan sebelumnya dapat diperumum sehingga pembagian dapat dilakukan dengan lebih dari satu polinomial pembagi. Yaitu, polinomial f dapat dibagi dengan sekumpulan polinomial tak nol $f_1, f_2, \dots, f_s$ dalam beberapa langkah.

Definisi 2.1.2.19 Misalkan f, h , dan $f_1, f_2, \dots, f_s$ adalah polinomial di $k[x_1, x_2, \dots, x_n]$ dengan $f_1, f_2, \dots, f_s \neq 0$ dan $F = \{f_1, f_2, \dots, f_s\}$. Polinomial f dikatakan tereduksi ke h modulo F , yang ditulis sebagai

$$f \xrightarrow{F}_+ h$$

jika dan hanya jika terdapat barisan indeks $i_1, i_2, \dots, i_t \in \{1, 2, \dots, s\}$ dan barisan polinomial $h_1, h_2, \dots, h_{t-1} \in k[x_1, x_2, \dots, x_n]$ sehingga

$$f \xrightarrow{f_{i_1}} h_1 \xrightarrow{f_{i_2}} h_2 \xrightarrow{f_{i_3}} \dots \xrightarrow{f_{i_{t-1}}} h_{t-1} \xrightarrow{f_{i_t}} h$$

(Adams & Lousstaunau, 1996).

Pembagian dari sebuah polinomial f dengan sekumpulan polinomial tak nol $f_1, f_2, \dots, f_s$ dapat dilakukan dengan memilih f_i sehingga $\text{lp}(f_i)$ membagi $\text{lp}(f)$. Karena f_i yang memenuhi bisa lebih dari satu, maka cara melakukan pembagian f dengan $f_1, f_2, \dots, f_s$ tidak tunggal. Berikut ilustrasi dari pembagian dalam beberapa langkah.

Contoh 2.1.2.20 Misalkan $f = 3x^2y^2z - x^2y$ dan $F = \{f_1, f_2\}$ dengan $f_1 = 2xy - 4y$ dan $f_2 = -y^2z + 1$ adalah polinomial pada $\mathbb{Q}[x, y, z]$ terhadap order leksikografis derajat dengan $x > y > z$. Maka

$$f \xrightarrow{F}_+ -2xy - 6x$$

karena

$$f \xrightarrow{\frac{3}{2}xyz, f_1} 6xy^2z - x^2y \xrightarrow{-6x, f_2} -x^2y - 6x \xrightarrow{-\frac{1}{2}x, f_1} -2xy - 6x$$

Terdapat istilah khusus ketika tidak ada f_i pada polinomial $f_1, f_2, \dots, f_s$ sehingga $\text{lp}(f_i)$ membagi polinomial r .

Definisi 2.1.2.21 Polinomial r di $k[x_1, x_2, \dots, x_n]$ dikatakan tereduksi atas himpunan polinomial tak nol $F = \{f_1, f_2, \dots, f_s\} \subseteq k[x_1, x_2, \dots, x_n]$ jika $r = 0$ atau tidak ada hasil pangkat di r yang dapat dibagi oleh salah satu dari $\text{lp}(f_i)$ pada F (Adams & Loustaunau, 1996).

Definisi 2.1.2.22 Jika $f \xrightarrow{F}_+ r$ dan r tereduksi atas F , maka r disebut sebagai sisa pembagian dari f atas F (Adams & Loustaunau, 1996).

Contoh 2.1.2.23 Pada Contoh 2.1.2.20 karena $-2xy - 6x \xrightarrow{-1, f_1} -6x - 4y$ dan $\text{lp}(f_1)$ maupun $\text{lp}(f_2)$ tidak membagi $-6x - 4y$, maka $-6x - 4y$ tereduksi atas F . Lebih lanjut

$$f \xrightarrow{F} -6x - 4y$$

Sehingga $-6x - 4y$ adalah sisa pembagian dari f atas F .

Dari proses pembagian yang sudah didefinisikan sebelumnya, dapat didefinisikan algoritma pembagian sebagai berikut.

Algoritma 2.1.2.24 Berikut ini adalah algoritma pembagian pada $k[x_1, x_2, \dots, x_n]$

Input: $f_1, f_2, \dots, f_s \in k[x_1, x_2, \dots, x_n]$ dengan $f_i \neq 0, i \in \{1, 2, \dots, s\}$

Output: $u_1, u_2, \dots, u_s, r \in k[x_1, x_2, \dots, x_n]$ sehingga $f = u_1 f_1 + u_2 f_2 + \dots + u_s f_s + r$ dengan r tereduksi atas $\{f_1, f_2, \dots, f_s\}$ dan $\max(\max_{1 \leq i \leq s} (\text{lp}(u_i), \text{lp}(f_i)), \text{lp}(r)) = \text{lp}(f)$

Initialization: $u_1 := 0, u_2 := 0, \dots, u_s := 0, r := 0, h := f$

While $h \neq 0$ **do**

If terdapat i sehingga $\text{lp}(f_i)$ membagi $\text{lp}(h)$ **then**

pilih i terkecil sehingga $\text{lp}(f_i)$ membagi $\text{lp}(h)$

$u_i := u_i + \frac{\text{lt}(h)}{\text{lt}(f_i)}$

$h := h - \frac{\text{lt}(h)}{\text{lt}(f_i)} f_i$

Else

$r := r + \text{lt}(h)$

$h := h - \text{lt}(h)$

Berdasarkan (Adams & Loustaunau, 1996), algoritma di atas pasti berhenti dan akan menghasilkan polinomial $u_1, u_2, \dots, u_s, r \in k[x_1, x_2, \dots, x_n]$

$$f = u_1 f_1 + u_2 f_2 + \dots + u_s f_s + r$$

dengan

$$\text{lp}(f) = \max(\max_{1 \leq i \leq s}(\text{lp}(u_i), \text{lp}(f_i)), r)$$

Contoh 2.1.2.25 Pada contoh ini, algoritma pembagian akan diterapkan untuk mencari u_1, u_2 , dan r seperti pada Contoh 2.1.2.20 sehingga

$$f = u_1 f_1 + u_2 f_2 + r$$

dan

$$\text{lp}(f) = \max(\max(\text{lp}(u_1)\text{lp}(f_1), \text{lp}(u_2)\text{lp}(f_2)), r)$$

Dari Contoh 2.1.2.20, $f = 3x^2y^2z - x^2y$, $f_1 = 2xy - 4y$, dan $f_2 = -y^2z + 1$.

Inisialisasi: $u_1 := 0, u_2 := 0, r := 0, h := 3x^2y^2z - x^2y$

Iterasi pertama, $h \neq 0$

$$\text{lp}(f_1) = xy \text{ membagi } \text{lp}(h) = x^2y^2z$$

$$u_1 := u_1 + \frac{\text{lt}(h)}{\text{lt}(f_1)} = 0 + \frac{3}{2}xyz = \frac{3}{2}xyz$$

$$h := h - \frac{\text{lt}(h)}{\text{lt}(f_1)} f_1 = 3x^2y^2z - x^2y - \frac{3}{2}xyz(2xy - 4y) = 6xy^2z - x^2y$$

Iterasi kedua, $h \neq 0$

$$\text{lp}(f_1) = xy \text{ membagi } \text{lp}(h) = xy^2z$$

$$u_1 := u_1 + \frac{\text{lt}(h)}{\text{lt}(f_1)} = \frac{3}{2}xyz + \frac{6xy^2z}{2xy} = \frac{3}{2}xyz + 3yz$$

$$h := h - \frac{\text{lt}(h)}{\text{lt}(f_1)} f_1 = 6xy^2z - x^2y - 3yz(2xy - 4y) = -x^2y + 12y^2z$$

Iterasi ketiga, $h \neq 0$

$$\text{lp}(f_1) = xy \text{ membagi } \text{lp}(h) = x^2y$$

$$u_1 := u_1 + \frac{lt(h)}{lt(f_1)} = \frac{3}{2}xyz + 3yz + \frac{(-x^2y)}{2xy} = \frac{3}{2}xyz + 3yz - \frac{1}{2}x$$

$$h := h - \frac{lt(h)}{lt(f_1)} f_1 = -x^2y + 12y^2z + \frac{1}{2}x(2xy - 4y) = 12y^2z - 2xy$$

Iterasi keempat, $h \neq 0$

$$lp(f_1) = xy \text{ tidak membagi } lp(h) = y^2z$$

$$lp(f_2) = y^2z \text{ membagi } lp(h) = y^2z$$

$$u_2 := u_1 + \frac{lt(h)}{lt(f_2)} = 0 + \frac{12y^2z}{-y^2z} = -12$$

$$h := h - \frac{lt(h)}{lt(f_2)} f_2 = 12y^2z - 2xy + 12(-y^2z + 1) = -2xy + 12$$

Iterasi kelima, $h \neq 0$

$$lp(f_1) = xy \text{ membagi } lp(h) = xy$$

$$u_1 := u_1 + \frac{lt(h)}{lt(f_1)} = \frac{3}{2}xyz + 3yz - \frac{1}{2}x + \frac{(-2xy)}{2xy} = \frac{3}{2}xyz + 3yz - \frac{1}{2}x - 1$$

$$h := h - \frac{lt(h)}{lt(f_1)} f_1 = -2xy + 12 + 1(2xy - 4y) = -4y + 12$$

Iterasi keenam, $h \neq 0$

$$lp(f_1) = xy \text{ tidak membagi } lp(h) = y$$

$$lp(f_2) = y^2z \text{ tidak membagi } lp(h) = y$$

$$r := r + lt(h) = 0 - 8y = -8y$$

$$h := h - lt(h) = -8y + 12 - 8y = 12$$

Iterasi ketujuh, $h \neq 0$

$$lp(f_1) = xy \text{ tidak membagi } lp(h) = 1$$

$$lp(f_2) = y^2z \text{ tidak membagi } lp(h) = 1$$

$$r := r + lt(h) = -8y + 12$$

$$h := h - \text{lt}(h) = 12 - 12 = 0$$

Iterasi kedelapan, $h = 0$

Jadi f dapat ditulis dalam bentuk

$$f = \left(\frac{3}{2}xyz + 3yz - \frac{1}{2}x - 1 \right) (2xy - 4y) - 12(-y^2z + 1) - 4y + 12$$

Pada penelitian ini, untuk mempersingkat penulisan, algoritma pembagian akan ditulis seperti dalam bentuk Definisi 2.1.2.17 dan 2.1.2.19.

2.1.3 Pembagian Polinomial dengan Ideal

Misalkan $f \in k[x_1, x_2, \dots, x_n]$ dan $F = \{f_1, f_2, \dots, f_s\} \subseteq k[x_1, x_2, \dots, x_n]$ dengan setiap $f_i \in F$ merupakan polinomial tak nol. Berdasarkan algoritma pembagian, f dapat ditulis dalam bentuk

$$f = u_1f_1 + u_2f_2 + \dots + u_sf_s + r$$

untuk suatu $u_1, u_2, \dots, u_s \in k[x_1, x_2, \dots, x_n]$. Hal ini mengakibatkan $f - r \in \langle f_1, f_2, \dots, f_s \rangle$. Sehingga untuk suatu ideal $J = \langle f_1, f_2, \dots, f_s \rangle \subseteq k[x_1, x_2, \dots, x_n]$, pembagian f dengan ideal J dapat didefinisikan sebagai pembagian f dengan pembangun dari J , yaitu $\{f_1, f_2, \dots, f_s\}$. Berdasarkan Adams & Lousaunau (1996), setiap ideal I pada $k[x_1, x_2, \dots, x_n]$ dibangun secara berhingga. Artinya pembagian f dengan I terdefinisi dengan baik.

2.2 Basis Gröbner

Pembahasan utama pada penelitian ini didasarkan pada suatu pembangun dari ideal pada $k[x_1, x_2, \dots, x_n]$ yang memiliki sifat khusus.

Definisi 2.2.1 Misalkan I adalah ideal dari $k[x_1, x_2, \dots, x_n]$ dan $G = \{g_1, g_2, \dots, g_t\}$ merupakan subhimpunan tak nol dari I . Himpunan G merupakan basis Gröbner bagi

I jika dan hanya jika untuk setiap $f \neq 0 \in I$, terdapat $1 \leq i \leq t$ sedemikian sehingga $lp(g_i)$ membagi $lp(f)$ (Adams & Lousaunau, 1996).

Salah satu perbedaan basis Gröbner dengan pembangun dari ideal yang lebih umum adalah, sisa pembagian dari $f \in k[x_1, x_2, \dots, x_n]$ dengan basis Gröbner G bagi ideal I adalah tunggal.

Teorema 2.2.2 Misalkan $G = \{g_1, g_2, \dots, g_t\}$ adalah himpunan yang berisi polinomial tak nol dari $k[x_1, x_2, \dots, x_n]$. Maka G adalah basis Gröbner jika dan hanya jika untuk setiap $f \in k[x_1, x_2, \dots, x_n]$, sisa pembagian dari f dengan G tunggal (Adams & Lousaunau, 1996).

Pembuktian mengenai penyelesaian sistem kongruensi dengan basis Gröbner menggunakan dua teorema berikut yang memanfaatkan sifat dari order eliminasi.

Teorema 2.2.3 Misalkan I adalah ideal pada $k[y_1, y_2, \dots, y_m, x_1, x_2, \dots, x_n]$ dan $<$ adalah order eliminasi dengan variabel x lebih besar dari variabel y . Jika G merupakan basis Gröbner bagi I , maka $G \cap k[y_1, y_2, \dots, y_m]$ merupakan basis Gröbner bagi $I \cap k[y_1, y_2, \dots, y_m]$ (Adams & Lousaunau, 1996).

Bukti. Karena $G \subseteq I$, maka $G \cap k[y_1, y_2, \dots, y_m] \subseteq I \cap k[y_1, y_2, \dots, y_m]$. Misalkan $f \in I \cap k[y_1, y_2, \dots, y_m]$. Karena G merupakan basis Gröbner bagi I , maka terdapat $g_j \in G$ sehingga $lp(g_j)$ membagi $lp(f)$. Berdasarkan order eliminasi, maka g_j hanya memuat variabel y saja. Akibatnya $g_j \in G \cap k[y_1, y_2, \dots, y_m]$. Jadi $G \cap k[y_1, y_2, \dots, y_m]$ merupakan basis Gröbner bagi $I \cap k[y_1, y_2, \dots, y_m]$.

Teorema 2.2.4 Misalkan $I_1, I_2, \dots, I_m$ adalah ideal pada $k[x_1, x_2, \dots, x_n]$. Untuk setiap $i \in \{1, 2, \dots, m\}$, misalkan w_i adalah variabel baru. Misalkan $J = \langle 1 - (w_1 + w_2 + \dots + w_m), w_1 I_1, w_2 I_2, \dots, w_m I_m \rangle$. Maka

$$I_1 \cap I_2 \cap \dots \cap I_m = J \cap k[x_1, x_2, \dots, x_n]$$

(Adams & Loustaunau, 1996).

Bukti. Akan ditunjukkan $I_1 \cap I_2 \cap \dots \cap I_m = J \cap k[x_1, x_2, \dots, x_n]$ dengan menunjukkan $I_1 \cap I_2 \cap \dots \cap I_m \subseteq J \cap k[x_1, x_2, \dots, x_n]$ dan $J \cap k[x_1, x_2, \dots, x_n] \subseteq I_1 \cap I_2 \cap \dots \cap I_m$. Akan ditunjukkan terlebih dahulu $I_1 \cap I_2 \cap \dots \cap I_m \subseteq J \cap k[x_1, x_2, \dots, x_n]$. Misalkan $f \in I_1 \cap I_2 \cap \dots \cap I_m$. Perhatikan bahwa f dapat ditulis dalam bentuk

$$\begin{aligned} f &= f \left(1 - \sum_{i=1}^m w_i + \sum_{i=1}^m w_i \right) \\ &= f \left(1 - \sum_{i=1}^m w_i \right) + f \sum_{i=1}^m w_i \\ &= f \left(1 - \sum_{i=1}^m w_i \right) + \sum_{i=1}^m f w_i \end{aligned}$$

Karena $f \in I_1 \cap I_2 \cap \dots \cap I_m$, maka $f w_i \in w_i I_i$, untuk setiap $i \in \{1, 2, \dots, n\}$.

Artinya $f \in J$, sehingga $f \in J \cap k[x_1, x_2, \dots, x_n]$. Akibatnya $I_1 \cap I_2 \cap \dots \cap I_m \subseteq J \cap k[x_1, x_2, \dots, x_n]$. Sebaliknya misalkan $f \in J \cap k[x_1, x_2, \dots, x_n]$. Maka f dapat ditulis dalam bentuk

$$f = g \left(1 - \sum_{i=1}^m w_i \right) + \sum_{i=1}^m h_i w_i f_i$$

untuk suatu $g, h_i \in k[x_1, x_2, \dots, x_n, w_1, w_2, \dots, w_m]$ dan $f_i \in k[x_1, x_2, \dots, x_n]$ dengan $i \in \{1, 2, \dots, n\}$. Tetapkan $k \in \{1, 2, \dots, n\}$. Evaluasi f saat $w_k = 1$ dan $w_j = 0$, untuk setiap $j \in \{1, 2, \dots, n\}, j \neq k$ menghasilkan

$$f = h_k(x_1, \dots, x_n, 0, 0, \dots, 1, \dots, 0, 0) f_k$$

Karena $f_k \in I_k$, maka $f \in I_k$. Karena untuk setiap $k \in \{1, 2, \dots, n\}$ berlaku $f \in I_k$, maka $f \in I_1 \cap I_2 \cap \dots \cap I_m$. Akibatnya $J \cap k[x_1, x_2, \dots, x_n] \subseteq I_1 \cap I_2 \cap \dots \cap I_m$.

2.2.1 Algoritma Buchberger

Ketika sudah ditentukan pembangun bagi suatu ideal I pada $k[x_1, x_2, \dots, x_n]$ bukan merupakan basis Gröbner, bagaimana cara mendapatkan basi Gröbner bagi ideal tersebut agar bisa memanfaatkan sifat-sifat khusus dari basis Gröbner? Terdapat beberapa algoritma yang dikembangkan untuk mendapatkan basis Gröbner bagi I . Salah satu yang paling awal dikembangkan dan paling sederhana adalah algoritma Buchberger. Sebelum mengenalkan algoritma Buchberger, terdapat beberapa istilah yang harus diketahui.

Definisi 2.2.1.1 Misalkan $f, g \in k[x_1, x_2, \dots, x_n]$. Didefinisikan kelipatan persekutuan terkecil dari f dan g adalah sebagai polinomial d yang memenuhi

1. Polinomial d membagi f dan g .
2. Jika $h \in k[x_1, x_2, \dots, x_n]$ membagi f dan g , maka h membagi d .

Kelipatan persekutuan terkecil dari f dan g dinotasikan sebagai $\text{lcm}(f, g)$ (Adams & Lousaunau, 1996).

Definisi 2.2.1.2 Misalkan $f, g \in k[x_1, x_2, \dots, x_n]$ adalah polinomial tak nol. Misalkan $L = \text{lcm}(\text{lp}(f), \text{lp}(g))$. Didefinisikan S -polinomial dari f dan g sebagai

$$S(f, g) = \frac{L}{\text{lt}(f)}f - \frac{L}{\text{lt}(g)}g$$

(Adams & Lousaunau, 1996).

S -polinomial ini digunakan sebagai kriteria untuk menentukan apakah himpunan pembangun bagi suatu ideal I merupakan basis Gröbner.

Teorema 2.2.1.3 Misalkan $G = \{g_1, g_2, \dots, g_t\}$ adalah polinomial tak nol pada $k[x_1, x_2, \dots, x_n]$ dan ideal $I = \langle G \rangle$. Maka G adalah basis Gröbner bagi I jika dan hanya jika untuk setiap $i, j \in \{1, 2, \dots, t\}, i \neq j$ berlaku

$$S(f_i, f_j) \xrightarrow{G}_+ 0$$

(Adams & Loustaunau, 1996).

Contoh 2.2.1.4 Misalkan $f_1 = x + y - z$ dan $f_2 = y + 4z$ adalah polinomial pada $\mathbb{Q}[x, y]$ berorde leksikografis dengan $x > y > z$ dan $G = \{f_1, f_2\}$. Misalkan $I = \langle G \rangle$ adalah ideal pada $\mathbb{Q}[x, y]$. Perhatikan bahwa

$$L = \text{lcm}(\text{lp}(f_1), \text{lp}(f_2)) = xy,$$

sehingga S -polinomial dari f_1 dan f_2 adalah

$$\begin{aligned} S(f_1, f_2) &= \frac{L}{\text{lt}(f_1)} f_1 - \frac{L}{\text{lt}(f_2)} f_2 \\ &= \frac{xy}{x} (x + y - z) - \frac{xy}{y} (y + 4z) \\ &= y(x + y - z) - x(y + 4z) \\ &= -4xz + y^2 - yz. \end{aligned}$$

Reduksi $S(f_1, f_2)$ dengan G diperoleh

$$S(f_1, f_2) \xrightarrow{-4z, f_1} y^2 + 3yz - 4z^2 \xrightarrow{y, f_2} -yz - 4z^2 \xrightarrow{-z, f_2} 0.$$

Akibatnya G merupakan basis Gröbner bagi I .

Contoh 2.2.1.5 Misalkan $f_1 = xy - y$ dan $f_2 = -x + y^2$ adalah polinomial pada $\mathbb{Q}[x, y]$ berorde leksikografis dengan $x > y$ dan $G = \{f_1, f_2\}$. Misalkan $I = \langle G \rangle$ adalah ideal pada $\mathbb{Q}[x, y]$. Perhatikan bahwa

$$L = \text{lcm}(\text{lp}(f_1), \text{lp}(f_2)) = xy,$$

sehingga S -polinomial dari f_1 dan f_2 adalah

$$\begin{aligned}
S(f_1, f_2) &= \frac{L}{\text{lt}(f_1)} f_1 - \frac{L}{\text{lt}(f_2)} f_2 \\
&= \frac{xy}{xy} (xy - y) - \frac{xy}{-x} (-x + y^2) \\
&= xy - y + y(-x + y^2) \\
&= y^3 - y.
\end{aligned}$$

Reduksi $S(f_1, f_2)$ dengan G

$$y^3 - y \xrightarrow{G}_+ y^3 - y$$

Karena sisa pembagian dari $S(f_1, f_2)$ tidak sama dengan 0, maka G bukan basis Gröbner bagi I .

Kriteria berdasarkan Teorema 2.2.1.3 inilah yang menjadi ide utama pada algoritma Buchberger untuk mencari basis Gröbner. Pertama, reduksi semua S -polinomial pada G . Jika semuanya 0, maka G adalah basis Gröbner bagi ideal I . Jika suatu S -polinomial direduksi oleh G tidak menghasilkan 0, maka tambahkan sisa pembagian tersebut ke dalam G . Lakukan hal yang sama seperti sebelumnya. Maka anggota dari G akan terus bertambah hingga semua S -polinomial pada G ketika direduksi oleh G akan menghasilkan 0.

Algoritma 2.2.1.6 Berikut ini algoritma Buchberger, algoritma untuk mengkomputasikan basis Gröbner bagi ideal I dari $k[x_1, x_2, \dots, x_n]$ (Adams & Lousaunau, 1996).

Input: $F = \{f_1, f_2, \dots, f_s\} \subseteq k[x_1, x_2, \dots, x_n]$ dengan $f_i \neq 0$ untuk setiap $1 \leq i \leq s$

Output: Basis Gröbner $G = \{g_1, g_2, \dots, g_t\}$ bagi $I = \langle f_1, f_2, \dots, f_s \rangle$

Initialization: $G := F, \mathcal{G} := \{\{f_i, f_j\} \mid f_i \neq f_j \in G\}$

While $\mathcal{G} \neq \emptyset$ **do**

Pilih sebarang $\{f, g\} \in \mathcal{G}$

$\mathcal{G} := \mathcal{G} - \{\{f, g\}\}$

$S(f, g) \xrightarrow{G}_+ h$, di mana h tereduksi terhadap G

If $h \neq 0$ **then**

$\mathcal{G} := \mathcal{G} \cup \{\{u, h\} \mid u \in G\}$

$G := G \cup \{h\}$

Berdasarkan (Adams & Lousaunau, 1996), algoritma di atas pasti berhenti dan akan menghasilkan sebuah basis Gröbner bagi suatu ideal I pada $k[x_1, x_2, \dots, x_n]$.

Contoh 2.2.1.7 Misalkan $f_1 = xy - y$ dan $f_2 = -x + y^2$ adalah polinomial pada $\mathbb{Q}[x, y]$ berorde leksikografis dengan $x > y$ dan $F = \{f_1, f_2\}$. Misalkan $I = \langle F \rangle$ adalah ideal pada $\mathbb{Q}[x, y]$. Akan dicari basis Gröbner bagi I .

Inisialisasi: $G := F$ dan $\mathcal{G} := \{\{f_1, f_2\}\}$

Iterasi pertama, $\mathcal{G} \neq \emptyset$

Pilih $\{f_1, f_2\} \in \mathcal{G}$

$\mathcal{G} := \emptyset$

$S(f_1, f_2) = f_1 + yf_2 = y^3 - y$

$S(f_1, f_2) \xrightarrow{G}_+ y^3 - y$

Karena $y^3 - y \neq 0$, maka

Misalkan $f_3 = y^3 - y$

$$\mathcal{G} := \{\{f_1, f_2\}, \{f_1, f_3\}\}$$

$$G := \{f_1, f_2, f_3\}$$

Iterasi kedua, $\mathcal{G} \neq \emptyset$

Pilih $\{f_1, f_3\} \in \mathcal{G}$

$$\mathcal{G} := \{\{f_2, f_3\}\}$$

$$S(f_1, f_3) = y^2 f_1 - x f_3 = -y^3 + xy = xy - y^3$$

$$S(f_1, f_3) \xrightarrow{1, f_1} -y^3 + y \xrightarrow{-1, f_3} 0$$

Iterasi ketiga, $\mathcal{G} \neq \emptyset$

Pilih $\{\{f_2, f_3\}\} \in \mathcal{G}$

$$\mathcal{G} := \emptyset$$

$$S(f_2, f_3) = y^3 f_2 - x f_3 = y^5 - xy = -xy + y^5$$

$$S(f_2, f_3) \xrightarrow{-1, f_1} y^5 - y \xrightarrow{y^2, f_3} y^3 - y \xrightarrow{1, f_3} 0$$

Jadi, $G = \{f_1, f_2, f_3\}$ adalah basis Gröbner bagi $I = \langle f_1, f_2 \rangle$ dengan $f_3 = y^3 - y$.

2.2.2 Basis Gröbner Tereduksi

Komputasi basis Gröbner dengan algoritma Buchberger mengindikasikan basis Gröbner G yang didapatkan akan memiliki lebih banyak anggota daripada himpunan pembangun awal yang diberikan. Oleh karena itu, adakalanya suku utama dari suatu anggota G dapat dibagi oleh suku utama anggota G yang lain. Terdapat istilah khusus saat hal ini tidak terjadi.

Definisi 2.2.2.1 Misalkan $G = \{g_1, g_2, \dots, g_t\}$ adalah basis Gröbner bagi ideal I pada $k[x_1, x_2, \dots, x_n]$. Basis Gröbner G dikatakan minimal jika untuk setiap $i \in \{1, 2, \dots, t\}$, $\text{lc}(g_i) = 1$ dan untuk setiap $i \neq j$, $\text{lp}(g_i)$ tidak membagi $\text{lp}(g_j)$.

Definisi 2.2.2.2 Misalkan $G = \{g_1, g_2, \dots, g_t\}$ adalah basis Gröbner bagi ideal I pada $k[x_1, x_2, \dots, x_n]$. Basis Gröbner G dikatakan tereduksi jika untuk setiap $i \in \{1, 2, \dots, t\}$, $\text{lc}(g_i) = 1$ dan g_i tereduksi modulo $G - \{g_i\}$ (Adams & Lousaunau, 1996).

2.3 Kongruensi

Sebelum didefinisikan sistem kongruensi atas ring polinomial multivariabel, akan didefinisikan terlebih dahulu konsep kongruensi pada ring polinomial multivariabel.

Definisi 2.3.1 Misalkan I adalah ideal tidak nol pada $k[x_1, x_2, \dots, x_n]$ dan $f, g \in k[x_1, x_2, \dots, x_n]$. Polinomial f dikatakan kongruen g modulo I , yang dinotasikan sebagai $f \equiv g \pmod{I}$, jika $f - g \in I$ (Adams & Lousaunau, 1996).

Contoh 2.3.2 Misalkan $I = \langle x^2y + y, y^2 \rangle$ adalah ideal pada $\mathbb{Q}[x, y]$. Diberikan $f = 5x^3y + 3xy + 3y^3$ dan $g = 2x^3y + y^3$. Karena

$$f - g = 3x^3y + 3xy + 2y^3 = 3x(x^2y + y) + 2y(y^2) \in I,$$

maka $f \equiv g \pmod{I}$.

Berikut beberapa sifat kongruensi pada ring polinomial multivariabel.

Teorema 2.3.3 Misalkan I adalah ideal pada $k[x_1, x_2, \dots, x_n]$. Misalkan $f \in k[x_1, x_2, \dots, x_n]$. Maka berlaku pernyataan berikut.

1. Jika $f \equiv g \pmod{I}$ untuk suatu $g \in k[x_1, x_2, \dots, x_n]$, maka $g \equiv f \pmod{I}$.
2. Jika $f \equiv g \pmod{I}$ dan $h \equiv i \pmod{I}$ untuk suatu $g, h, i \in k[x_1, x_2, \dots, x_n]$, maka $f + h \equiv g + i \pmod{I}$.

Bukti.

1. Misalkan $f \equiv g \pmod{I}$. Maka terdapat $q \in I$ sehingga

$$f = q + g$$

$$g = (-q) + f.$$

Akibatnya $g \equiv f \pmod{I}$.

2. Misalkan $f \equiv g \pmod{I}$ dan $h \equiv i \pmod{I}$. Maka terdapat $q_1, q_2 \in I$ sehingga

$$f = q_1 + g$$

$$h = q_2 + i.$$

Jumlahkan keduanya

$$f + h = q_1 + q_2 + g + i.$$

Karena $q_1 + q_2 \in I$, maka

$$f + h \equiv g + i \pmod{I}.$$

2.3.1 Bentuk Normal dari Polinomial Multivariabel

Berikut ini adalah sifat kongruensi yang berkaitan dengan pembagian polinomial dengan basis Gröbner. Sebelum itu, didefinisikan terlebih dahulu sisa pembagian polinomial dengan basis Gröbner.

Definisi 2.3.1.1 Misalkan G adalah basis Gröbner bagi ideal I pada $k[x_1, x_2, \dots, x_n]$ dan $f \in k[x_1, x_2, \dots, x_n]$. Jika r adalah sisa pembagian dari f oleh G , maka r disebut sebagai bentuk normal dari f atas G , yang dilambangkan sebagai $N_G(f) = r$ (Adams & Loustaunau, 1996).

Contoh 2.3.1.2 Berdasarkan Contoh 2.2.1.7., $G = \{f_1, f_2, f_3\}$ adalah basis Gröbner bagi $I = \langle f_1, f_2 \rangle$ dengan $f_1 = xy - y$, $f_2 = -x + y^2$, dan $f_3 = y^3 - y$. Misalkan $h_1 = 3xy^5 - 7y^2$. Reduksi h_1 dengan G menghasilkan

$$3xy^5 - 7y^2 \xrightarrow{3y^4, f_1} 3y^5 - 7y^2 \xrightarrow{3y^2, f_3} 3y^3 - 7y^2 \xrightarrow{3, f_3} -7y^2 + 3y.$$

Karena G adalah basis Gröbner, maka $-7y^2 + 3y$ bentuk normal dari f atas G .

Teorema 2.3.1.3 Misalkan $f, g \in k[x_1, x_2, \dots, x_n]$ dan G adalah basis Gröbner bagi ideal I pada $k[x_1, x_2, \dots, x_n]$. Maka $f \equiv g \pmod{I}$ jika dan hanya jika $N_G(f) = N_G(g)$ (Adams & Loustaunau, 1996).

Bukti. ($\Rightarrow$) Misalkan $f \equiv g \pmod{I}$. Maka terdapat $q \in I$ sehingga

$$f = q + g.$$

Artinya $N_G(f) = N_G(q) + N_G(g)$. Karena G adalah basis Gröbner dan $q \in I$, maka $N_G(q) = 0$. Akibatnya $N_G(f) = N_G(g)$.

($\Leftarrow$) Misalkan $N_G(f) = N_G(g)$. Perhatikan bahwa

$$\begin{aligned} f - g &= f - N_G(f) + N_G(g) - g \\ &= (f - N_G(f)) - (g - N_G(g)). \end{aligned}$$

Karena $f - N_G(f), g - N_G(g) \in I$, maka $f - g \in I$. Akibatnya $f \equiv g \pmod{I}$.

Contoh 2.3.1.4 Berdasarkan Contoh 2.2.1.7., $G = \{f_1, f_2, f_3\}$ adalah basis Gröbner bagi $I = \langle f_1, f_2 \rangle$ dengan $f_1 = xy - y, f_2 = -x + y^2$, dan $f_3 = y^3 - y$. Misalkan $h_1 = 3xy^5 - 7y^2$ dan $h_2 = 4x^2y^2 + xy^4$. Reduksi h_1 dengan G menghasilkan $N_G(h_1) = -7y^2 + 3y$, berdasarkan Contoh 2.3.1.2. Reduksi h_2 dengan G menghasilkan

$$4x^2y^2 + xy^4 \xrightarrow{4xy, f_1} xy^4 + 4xy^2 \xrightarrow{y^3, f_1} 4xy^2 + y^4 \xrightarrow{4y, f_1} y^4 + 4y^2 \xrightarrow{y, f_3} 5y^2.$$

Didapatkan $N_G(h_2) = 5y^2$. Karena $N_G(h_1) \neq N_G(h_2)$, maka berdasarkan Teorema 2.3.1.3, h_1 tidak kongruen h_2 modulo I .

2.3.2 Sistem Kongruensi atas Ring Polinomial Multivariabel

Berikut adalah definisi dari sistem kongruensi atas ring polinomial multivariabel.

Definisi 2.3.2.1 Misalkan $I_1, I_2, \dots, I_m$ adalah ideal tak nol yang berbeda pada $k[x_1, x_2, \dots, x_n]$. Misalkan $f, f_1, f_2, \dots, f_m \in k[x_1, x_2, \dots, x_n]$. Didefinisikan sistem kongruensi atas ring polinomial multivariabel sebagai kumpulan kongruensi-kongruensi

$$\begin{aligned} f &\equiv f_1 \pmod{I_1} \\ f &\equiv f_2 \pmod{I_2} \\ &\vdots \\ f &\equiv f_m \pmod{I_m} \end{aligned} \tag{2.1}$$

(Adams & Loustaunau, 1996).

Definisi 2.3.2.2 Diberikan sistem kongruensi

$$\begin{aligned} f &\equiv f_1 \pmod{I_1} \\ f &\equiv f_2 \pmod{I_2} \\ &\vdots \\ f &\equiv f_m \pmod{I_m} \end{aligned} \tag{2.2}$$

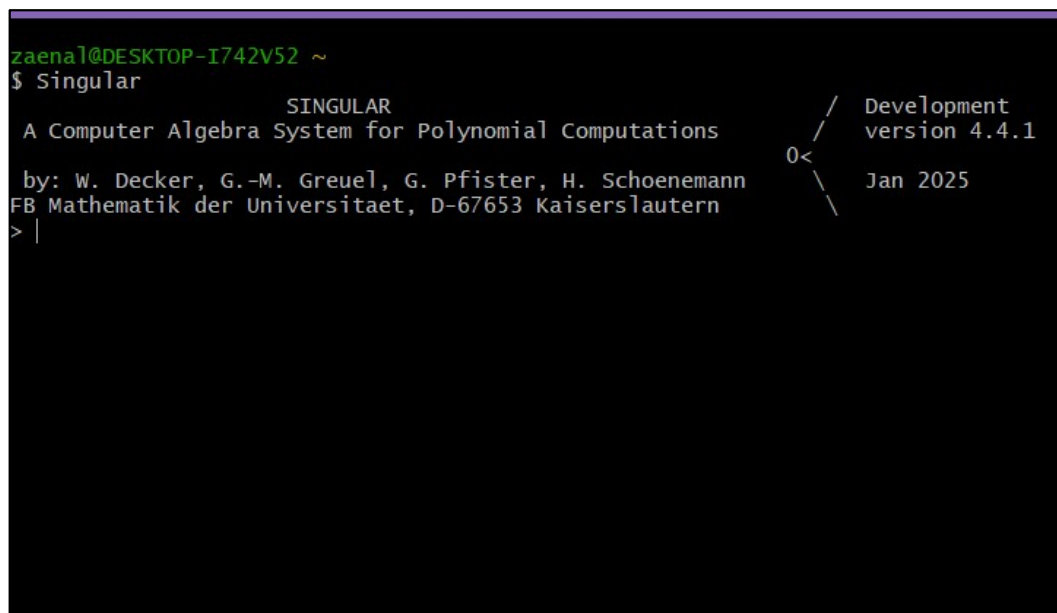
Suatu polinomial $u \in k[x_1, x_2, \dots, x_n]$ disebut sebagai suatu solusi dari sistem kongruensi (2.2) jika $u - f_i \in I_i$, untuk setiap $i \in \{1, 2, \dots, m\}$ (Adams & Loustaunau, 1996).

2.4 Singular-CAS

Singular-CAS dalam konteks kajian teori aljabar komutatif dan geometri aljabar berperan sebagai realisasi komputasional dari struktur-struktur teoretis yang dikembangkan dalam matematika murni. Sistem ini mengimplementasikan algoritma-algoritma fundamental yang berdasar pada teori basis Gröbner, yang merupakan generalisasi dari pembagian polinomial multivariat dan menjadi landasan untuk menyelesaikan masalah ideal dalam ring polinomial. Dalam ranah geometri aljabar, Singular digunakan untuk mempelajari varietas aljabar melalui korespondensi dengan ideal-ideal radikal, menghitung invarian seperti dimensi

Krull dan derajat varietas, serta menganalisis singularitas melalui resolusi desingularisasi (Greuel & Pfister, 2007).

Dengan demikian, Singular tidak hanya menjadi alat bantu hitung, tetapi juga media eksplorasi teoretis yang menghubungkan abstraksi matematika dengan verifikasi empiris, sekaligus media untuk menguji dugaan dan mengembangkan teori baru dalam aljabar komutatif dan geometri aljabar. Berikut ini adalah tampilan awal dari Singular-CAS.



```

zaenal@DESKTOP-I742V52 ~
$ Singular
          SINGULAR
A Computer Algebra System for Polynomial Computations
by: W. Decker, G.-M. Greuel, G. Pfister, H. Schoenemann
FB Mathematik der Universitaet, D-67653 Kaiserslautern
> |
Development
version 4.4.1
Jan 2025
  
```

Gambar 2.1 Tampilan Awal dari Singular-CAS

2.5 Kajian Integrasi Topik dengan Al-Qur'an

Seperti yang sudah dijabarkan pada latar belakang, salah satu yang ditekankan dari Surat Al-Jatsiyah ayat 20 adalah Al-Qur'an sebagai pedoman untuk melihat antara yang haq dan bathil. Antara haq dan bathil tidak boleh dicampuradukan, karena akan menimbulkan kekacauan moral dan intelektual. Mencampurkan keduanya berarti mengaburkan batas antara yang benar dan salah, yang pada

akhirnya melahirkan kezaliman. Sebagaimana firman Allah SWT dalam Surat Al-Baqarah ayat 42

وَلَا تَلْبِسُوا الْحَقَّ بِالْبَاطِلِ وَتَكْتُمُوا الْحَقَّ وَأَنْتُمْ تَعْلَمُونَ

“Janganlah kamu campuradukkan kebenaran dengan kebatilan dan (jangan pula) kamu sembunyikan kebenaran, sedangkan kamu mengetahui(-nya).”

Jika ditinjau dari asbabun nuzulnya, ayat ini turun dalam satu rangkaian pada surat Al-Baqarah ayat 40-44. Yaitu teguran Allah SWT terhadap Bani Israil di Madinah, yang mengetahui kebenaran kenabian Nabi Muhammad dari kitab mereka tetapi menolak menyampaikannya kepada kaumnya. Untuk Al-Baqarah ayat 42 terdapat dua larangan dari Allah SWT yang ditujukan ke Bani Israil.

Pertama, agar mereka jangan mencampuradukkan yang haq dengan yang bathil. Maksudnya, pemimpin-pemimpin Bani Israil suka memasukkan pendapat-pendapat pribadi ke dalam Kitab Taurat, sehingga sukarlah untuk membedakan mana yang benar.

Kedua, agar mereka tidak menyembunyikan kebenaran, padahal mereka mengetahuinya. Maksudnya, Bani Israil itu telah menyembunyikan kebenaran yang telah mereka ketahui dari kitab suci mereka. Antara lain ialah berita dari Allah tentang Nabi Muhammad saw yang akan diutus sebagai penutup dari semua rasul Allah untuk seluruh umat manusia.

Hal ini sengaja mereka tutupi dari masyarakat umum, bahkan mereka berusaha menjelekkan Nabi Muhammad saw, untuk menghalangi manusia beriman kepadanya. Ayat ini mencela perbuatan mereka yang demikian itu, dan setiap orang yang dengan sengaja menyembunyikan sesuatu yang benar.

Kembali pada basis Gröbner. Salah satu hal yang membedakan basis Gröbner G dengan pembangun bagi ideal I yang lain terletak pada ketunggalan dari

pembagian polinomial dengan basis Gröbner, berdasarkan Teorema 2.2.2. Sifat ini menjamin tidak adanya keambiguitas saat melakukan pembagian polinomial dengan basis Gröbner. Sebaliknya tidak ada jaminan ketunggalan sisa pembagian dari f dengan suatu pembangun dari I .

Hal ini selaras dengan larangan pertama yang dijabarkan di atas. Ketunggalan sisa pembagian dalam hal ini dapat dimaknai sebagai perbuatan haq. Sehingga sifat sebaliknya sebagai perbuatan bathil. Maka keambiguitas dari sisa pembagian suatu polinomial f anggota dari I dengan suatu pembangun dari I inilah yang dapat dimaknai sebagai mencampurkan antara haq dan bathil. Hal ini akan berakibat tidak dapat ditentukan apakah suatu sistem kongruensi atas ring polinomial multivariabel memiliki solusi.

Diantara contoh dari perbuatan mencampurkan antara haq dan bathil terletak pada surat Ali Imran ayat 71

﴿٧١﴾ يَا أَهْلَ الْكِتَابِ لِمَ تَلْبِسُونَ الْحَقَّ بِالْبَاطِلِ وَتَكْتُمُونَ الْحَقَّ وَأَنْتُمْ تَعْلَمُونَ

“Wahai Ahlulkitab, mengapa kamu mencampurkan yang hak dengan yang batil dan kamu menyembunyikan kebenaran, padahal kamu mengetahui?”

Berikut adalah tafsir dari ayat tersebut berdasarkan Tafsir Wajiz Kementerian Agama RI. Setelah ayat sebelumnya menjelaskan sikap penolakan Ahli Kitab terhadap kebenaran yang dibawa Rasulullah, maka ayat ini kembali menjelaskan perilaku buruk mereka yang lainnya, antara lain upaya penyesatan terhadap kaum muslim. Dalam hal ini, mereka menutup-nutupi beberapa firman Allah yang termaktub di dalam Taurat dan Injil dengan perkataan-perkataan yang dibuat-buat oleh mereka sendiri. Mereka juga menyembunyikan kebenaran tentang kenabian Muhammad yang disebut dalam Taurat dan Injil, meskipun mereka tahu tentang kebenaran dan akibatnya, yaitu siksa yang sangat pedih.

Ayat ini memberi tahu tentang teguran secara langsung dari Allah SWT ke ahli kitab. Mereka menyembunyikan kebenaran yang dibawa dari Nabi dan Rasul yang tertuang pada kitab Taurat dan Injil dan menambahkan perkataan mereka sendiri.

2.6 Kajian Topik dengan Teori Pendukung

Teorema berikut dapat digunakan untuk menentukan apakah suatu sistem kongruensi atas $k[x_1, x_2, \dots, x_n]$ memiliki solusi. Lebih lanjut, himpunan solusi dari sistem persamaan kongruensi juga dapat diketahui. Terakhir, diberikan kriteria mengenai polinomial yang berada dalam himpunan solusi.

Teorema 2.6.1 Misalkan $I_1, I_2, \dots, I_m$ adalah ideal yang berbeda pada $k[x_1, x_2, \dots, x_n]$. Misalkan $f_1, f_2, \dots, f_m \in k[x_1, x_2, \dots, x_n]$ dengan

$$\begin{aligned} f &\equiv f_1 \pmod{I_1} \\ f &\equiv f_2 \pmod{I_2} \\ &\vdots \\ f &\equiv f_m \pmod{I_m} \end{aligned} \tag{2.3}$$

adalah sistem kongruensi. Maka berlaku pernyataan berikut.

1. Misalkan $g = \sum_{i=1}^m w_i f_i \in k[x_1, x_2, \dots, x_n, w_1, w_2, \dots, w_m]$. Sistem (2.3) memiliki solusi jika dan hanya jika $h = N_G(g) \in k[x_1, x_2, \dots, x_n]$. Lebih lanjut h adalah solusi dari sistem (2.3).
2. Jika sistem (2.3) memiliki solusi, maka $h + \cap_{i=1}^m I_i = \{h + v \mid v \in \cap_{i=1}^m I_i\}$ adalah himpunan solusi dari sistem (2.3).
3. Khususnya, $u \in k[x_1, x_2, \dots, x_n]$ adalah solusi dari sistem (2.3) jika dan hanya jika $h = N_{G \cap k[x_1, x_2, \dots, x_n]}(u)$,

di mana G adalah basis Gröbner bagi ideal $J = \langle 1 - \sum_{i=1}^m w_i, w_1 I_1, w_2 I_2, \dots, w_m I_m \rangle$ pada $k[x_1, x_2, \dots, x_n, w_1, w_2, \dots, w_m]$ terhadap order eliminasi dengan variabel x lebih kecil dari variabel w (Adams & Loustaunau, 1996).

BAB III

METODE PENELITIAN

3.1 Jenis Penelitian

Metode yang digunakan dalam penelitian ini adalah studi literatur, yaitu penelitian dilakukan dengan mengumpulkan dan mengkaji data dari sumber literatur seperti jurnal dan buku. Data yang dikumpulkan adalah yang berkaitan dengan basis Gröbner dan sistem kongruensi atas ring polinomial multivariabel.

3.2 Pra Penelitian

Penelitian ini mengumpulkan berbagai macam jurnal, artikel, dan buku yang berkaitan dengan topik yang dibahas pada penelitian ini. Berikut ini rujukan yang digunakan pada penelitian ini.

Rujukan utama dari penelitian ini adalah buku karangan Adams & Loustaunau (1996). Buku tersebut membahas tentang pengantar dari basis Gröbner dan aplikasinya. Definisi dari ring polinomial, order suku, algoritma pembagian, basis Gröbner, dan algoritma Buchberger dijelaskan pada buku tersebut. Setelahnya dibahas berbagai macam aplikasi basis Gröbner, salah satunya adalah penyelesaian sistem persamaan polinomial. Kemudian salah satu subbab pada buku tersebut membahas tentang order eliminasi yang juga akan digunakan pada penelitian ini untuk menyelesaikan sistem kongruensi atas ring polinomial multivariabel.

Ide mengenai penyelesaian sistem kongruensi atas polinomial multivariabel didapatkan pada *exercises* dari subbab pembahasan order eliminasi ini. Karena penelitian ini berkaitan dengan konsep ring, maka buku karangan Gallian (2013) dan Dummit & Foote (2004) digunakan sebagai referensi konsep dasar ring.

Konsep mengenai ideal dan homomorfisma ring pada buku tersebut juga digunakan sebagai referensi.

Rujukan pendukung lain yang digunakan untuk mendefinisikan ring polinomial didapatkan dari buku karangan Greuel & Pfister (2007). Sementara rujukan mengenai konsep dasar dari kongruensi pada bilangan bulat didapatkan dari Rosen (2005). Rujukan-rujukan lain mengenai teori basis Gröbner dan aplikasinya adalah Cox, Little, & O'Shea (2015) dan Lin, Xu, & Wu (2004).

3.3 Tahapan Penelitian

Setelah selesai mempelajari dan memahami konsep yang berkaitan dengan penelitian, yaitu konsep basis Gröbner dan sistem kongruensi atas ring polinomial multivariabel beserta teori pendukungnya, berikut ini tahapan penelitian yang akan dilakukan. Berikut ini adalah tahapan penelitian mengenai bagaimana menyelesaikan sistem kongruensi atas ring polinomial multivariabel dengan basis Gröbner.

1. Mengkaji teorema yang akan digunakan untuk menyelesaikan sistem kongruensi atas ring polinomial multivariabel berikut.

Misalkan $I_1, I_2, \dots, I_m$ adalah ideal yang berbeda pada $k[x_1, x_2, \dots, x_n]$,

$f_1, f_2, \dots, f_m \in k[x_1, x_2, \dots, x_n]$, dan

$$\begin{aligned} f &\equiv f_1 \pmod{I_1} \\ f &\equiv f_2 \pmod{I_2} \\ &\vdots \\ f &\equiv f_m \pmod{I_m} \end{aligned} \tag{3.1}$$

adalah sistem kongruensi atas $k[x_1, x_2, \dots, x_n]$. Misalkan $J = \langle 1 - (w_1 + w_2 + \dots + w_m), w_1 I_1, w_2 I_2, \dots, w_m I_m \rangle$ adalah ideal pada $k[x_1, x_2, \dots, x_n, w_1, w_2, \dots, w_m]$ dan G adalah basis Gröbner bagi J terhadap

order eliminasi dengan variabel x lebih kecil dari variabel w . Misalkan $g = \sum_{i=1}^m w_i f_i$.

- a. Misalkan $g = \sum_{i=1}^m w_i f_i \in k[x_1, x_2, \dots, x_n, w_1, w_2, \dots, w_m]$. Sistem (3.1) memiliki solusi jika dan hanya jika $h = N_G(g) \in k[x_1, x_2, \dots, x_n]$. Lebih lanjut h adalah suatu solusi dari sistem (3.1).
- b. Jika $h = N_G(g)$ dan $h \in k[x_1, x_2, \dots, x_n]$, maka $h + \cap_{i=1}^m I_i = \{h + v | v \in \cap_{i=1}^m I_i\}$ adalah himpunan solusi dari sistem (3.1).
- c. Khususnya, $u \in k[x_1, x_2, \dots, x_n]$ adalah solusi dari sistem (3.1) jika dan hanya jika $h = N_{G \cap k[x_1, x_2, \dots, x_n]}(u)$.

2. Membuktikan teorema tersebut menggunakan sifat-sifat basis Gröbner, kongruensi, dan order eliminasi. Berikut ini adalah gambaran umum dari pembuktian teorema tersebut.

- a. Menunjukkan jika $f \in k[x_1, x_2, \dots, x_n]$ merupakan solusi bagi sistem (3.1), maka akan didapatkan

$$g \equiv f \pmod{J}$$

- b. Tulis g dalam bentuk

$$g - h = c \left(1 - \sum_{i=1}^m w_i \right) + \sum_{i=1}^m a_i w_i q_i$$

- c. Memverifikasi bahwa

$$h \equiv f_k \pmod{I_k}$$

untuk setiap $k \in \{1, 2, \dots, m\}$.

- d. Memverifikasi solusi dengan mensubstitusi $h + \cap_{i=1}^m I_i$ ke sistem (3.1).
- e. Menunjukkan bahwa solusi dari sistem (3.1) merupakan anggota dari $h + \cap_{i=1}^m I_i$.

- f. Membuktikan poin nomor tiga dengan Teorema 2.2.3, 2.2.4, dan 2.3.1.3.
3. Menunjukkan secara eksplisit langkah-langkah penyelesaian sistem kongruensi atas ring polinomial multivariabel berdasarkan teorema yang sudah dikaji dan dibuktikan pada poin satu dan dua. Komputasi basis Gröbner pada langkah-langkah ini dilakukan dengan algoritma Buchberger.

Selanjutnya langkah-langkah penyelesaian sistem kongruensi atas ring polinomial dengan basis Gröbner akan diimplementasikan dalam pada Singular-CAS dalam bentuk prosedur Singular-CAS. Berikut ini adalah langkah-langkah implemenentasinya.

1. Membuat prosedur pada Singuar-CAS untuk menentukan apakah sistem kongruensi atas ring polinomial multivariabel memiliki solusi dan menunjukan himpunan solusinya.
2. Membuat prosedur untuk menentukan apakah suatu polinomial merupakan solusi bagi sistem kongruensi pada sistem kongruensi atas ring polinomial multivariabel.
3. Menunjukkan bagaimana cara menjalankan dua prosedur pada Singular-CAS yang sudah dibuat untuk menyelesaikan sistem kongruensi atas ring polinomial multivariabel.
4. Memberikan contoh penyelesaian sistem kongruensi atas ring polinomial multivariabel dengan prosedur pada Singular-CAS yang sudah dibuat.

BAB IV

HASIL DAN PEMBAHASAN

4.1 Penyelesaian Sistem Kongruensi atas Ring Polinomial Multivariabel

Misalkan $I_1, I_2, \dots, I_m$ adalah ideal yang berbeda pada $k[x_1, x_2, \dots, x_n]$.

Misalkan $f, f_1, f_2, \dots, f_m \in k[x_1, x_2, \dots, x_n]$. Diberikan sistem kongruensi

$$\begin{aligned} f &\equiv f_1 \pmod{I_1} \\ f &\equiv f_2 \pmod{I_2} \\ &\vdots \\ f &\equiv f_m \pmod{I_m} \end{aligned} \tag{4.1}$$

Pertanyaanya adalah apakah ada $f \in k[x_1, x_2, \dots, x_n]$ yang memenuhi sistem (4.1)?

Jika ada, bagaimana himpunan solusinya? Pada subbab ini akan dibahas metode untuk menjawab pertanyaan-pertanyaan tersebut. Berikut ini adalah salah satu contoh dari sistem persamaan kongruensi yang memiliki solusi.

Contoh 4.1.1 Misalkan $I_1 = \langle x^2y + z \rangle, I_2 = \langle xz, xy, y^2z + z \rangle, I_3 = \langle x^3 + y, z^3 + z \rangle$ adalah ideal pada $\mathbb{Q}[x, y, z]$ terhadap order leksikografis derajat dengan $x > y > z$. Diberikan sistem kongruensi

$$\begin{aligned} f &\equiv y^2z + z^2 + z + 2 \pmod{I_1} \\ f &\equiv 2 \pmod{I_2} \\ f &\equiv -xy^3 + y^2z + z + 2 \pmod{I_3} \end{aligned} \tag{4.2}$$

Misalkan $f_1 = y^2z + z^2 + z + 2, f_2 = 2, f_3 = -xy^3 + y^2z + z + 2$. Misalkan $f = x^4y^2 + y^2z + z + 2$. Akan ditunjukkan f merupakan solusi bagi sistem (4.2) dengan menunjukkan sisa pembagian dari f dengan I_1, I_2 , dan I_3 secara berurutan adalah f_1, f_2, f_3 . Misalkan $I_1 = \langle x^2y + z \rangle = \langle p_1 \rangle$. Reduksi f oleh I_1 menghasilkan

$$f \xrightarrow{x^2y, p_1} -x^2yz + y^2z + z + 2 \xrightarrow{-z, p_1} y^2z + z^2 + z + 2.$$

Karena $lp(g_i)$ tidak membagi setiap suku pada polinomial $y^2z + z^2 + z + 2$, maka sisa pembagian dari f dengan I_1 adalah $y^2z + z^2 + z + 2 = f_1$. Misalkan $I_3 = \langle xz, xy, y^2z + z \rangle = \langle q_1, q_2, q_3 \rangle$. Reduksi f oleh I_2 menghasilkan

$$f \xrightarrow{x^3y, q_2} y^2z + z + 2 \xrightarrow{1, q_3} 2.$$

Didapatkan sisa pembagian dari f dengan I_2 adalah $2 = f_2$. Misalkan $I_3 = \langle x^3 + y, z^3 + z \rangle = \langle r_1, r_2 \rangle$. Reduksi f oleh I_3 menghasilkan

$$f \xrightarrow{xy^2, r_1} -xy^3 + y^2z + z + 2.$$

Didapatkan sisa pembagian dari f dengan I_3 adalah $-xy^3 + y^2z + z + 2 = f_3$.

Jadi, f merupakan solusi bagi sistem (4.2).

Teorema berikut dapat digunakan untuk menunjukkan eksistensi solusi dari sistem (4.1) dan mendeskripsikan solusi dari sistem (4.1) secara spesifik. Lebihlanjut kriteria apakah suatu polinomial $u \in k[x_1, x_2, \dots, x_n]$ termasuk solusi juga diberikan.

Teorema 4.1.2 Misalkan $I_1, I_2, \dots, I_m$ adalah ideal yang berbeda pada $k[x_1, x_2, \dots, x_n]$. Misalkan $f_1, f_2, \dots, f_m \in k[x_1, x_2, \dots, x_n]$ dengan

$$\begin{aligned} f &\equiv f_1 \pmod{I_1} \\ f &\equiv f_2 \pmod{I_2} \\ &\vdots \\ f &\equiv f_m \pmod{I_m} \end{aligned} \tag{4.3}$$

adalah sistem kongruensi. Maka berlaku pernyataan berikut.

1. Misalkan $g = \sum_{i=1}^m w_i f_i \in k[x_1, x_2, \dots, x_n, w_1, w_2, \dots, w_m]$. Sistem (4.3) memiliki solusi jika dan hanya jika $h = N_G(g) \in k[x_1, x_2, \dots, x_n]$. Lebih lanjut h adalah solusi dari sistem (4.3).

2. Jika sistem (4.3) memiliki solusi, maka $h + \cap_{i=1}^m I_i = \{h + v | v \in \cap_{i=1}^m I_i\}$ adalah himpunan solusi dari sistem (4.3).

3. Khususnya, $u \in k[x_1, x_2, \dots, x_n]$ adalah solusi dari sistem (4.3) jika dan hanya jika $h = N_{G \cap k[x_1, x_2, \dots, x_n]}(u)$,

di mana G adalah basis Gröbner bagi ideal $J = \langle 1 - \sum_{i=1}^m w_i, w_1 I_1, w_2 I_2, \dots, w_m I_m \rangle$ pada $k[x_1, x_2, \dots, x_n, w_1, w_2, \dots, w_m]$ terhadap order eliminasi dengan variabel x lebih kecil dari variabel w (Adams & Lousaunau, 1996).

Bukti.

1. ($\Rightarrow$) Misalkan sistem (4.3) memiliki solusi. Artinya terdapat $f \in k[x_1, x_2, \dots, x_n]$ sehingga untuk setiap $i \in \{1, 2, \dots, m\}$

$$f \equiv f_i \pmod{I_i}.$$

Maka terdapat $q_i \in I_i$ sehingga

$$f - f_i = q_i.$$

Tinjau f, f_i , dan q_i sebagai polinomial pada $k[x_1, x_2, \dots, x_n, w_1, w_2, \dots, w_m]$.

Perhatikan bahwa

$$\begin{aligned} w_i(f - f_i) &= w_i q_i \\ w_i f - w_i f_i &= w_i q_i. \end{aligned}$$

Didapatkan $w_i f \equiv w_i f_i \pmod{w_i I_i}$. Karena $w_i I_i \in J$, maka $w_i f_i \equiv w_i f \pmod{J}$. Akibatnya untuk $g = \sum_{i=1}^m w_i f_i$

$$g = \sum_{i=1}^m w_i f_i \pmod{J} \equiv \sum_{i=1}^m w_i f \pmod{J} \equiv f \sum_{i=1}^m w_i \pmod{J}.$$

Karena $1 - \sum_{i=1}^m w_i \in J$, maka berdasarkan Teorema 2.3.3. $\sum_{i=1}^m w_i \equiv 1 \pmod{J}$ sehingga

$$g \equiv f \sum_{i=1}^m w_i \pmod{J} \equiv f \pmod{J}.$$

Misalkan $h = N_G(g)$. Berdasarkan Teorema 2.3.1.3., $g \equiv f \pmod{J}$ jika dan hanya jika $N_G(g) = N_G(f)$. Karena $f \in k[x_1, x_2, \dots, x_n]$ dan variabel x lebih kecil dari w , maka $h \in k[x_1, x_2, \dots, x_n]$.

($\Leftarrow$) Misalkan $h = N_G(g) \in k[x_1, x_2, \dots, x_n]$. Artinya sebagai polinomial pada $k[x_1, x_2, \dots, x_n, w_1, w_2, \dots, w_m]$, polinomial g dengan sisa pembagian terhadap G adalah h dapat ditulis dalam bentuk

$$g - h = c \left(1 - \sum_{i=1}^m w_i \right) + \sum_{i=1}^m a_i w_i q_i \quad (4.4)$$

untuk suatu $c, a_i \in k[x_1, x_2, \dots, x_n, w_1, w_2, \dots, w_m]$, dan $q_i \in I_i$. Tetapkan $k \in \{1, 2, \dots, m\}$. Evaluasi persamaan (4.4) saat $w_k = 1$ dan $w_j = 0$ untuk $j \in \{1, 2, \dots, m\}, j \neq k$. Misalkan $g' = g(x_1, \dots, x_n, 0, \dots, 1, \dots, 0)$ dan $h' = h(x_1, \dots, x_n, 0, \dots, 1, \dots, 0)$. Evaluasi ruas kiri dari persamaan (4.4) menghasilkan

$$g' - h' = f_k(x_1, x_2, \dots, x_n) - h(x_1, x_2, \dots, x_n).$$

Misalkan $c' = c(x_1, \dots, x_n, 0, \dots, 1, \dots, 0)$ dan $q'_i = q_i(x_1, \dots, x_n, 0, \dots, 1, \dots, 0)$, untuk $i = \{1, 2, \dots, m\}$. Evaluasi ruas kanan dari persamaan (4.4) menghasilkan

$$\begin{aligned} c' \left(1 - \sum_{i=1}^m w_i \right) + \sum_{i=1}^m a_i w_i q'_i &= c'(1 - 1) + a_k q'_k \\ &= a_k q'_k. \end{aligned}$$

Didapatkan persamaan (4.4) akan menjadi

$$f_k(x_1, x_2, \dots, x_n) - h(x_1, x_2, \dots, x_n) = a_k q'_k.$$

Karena $q'_k \in I$, maka $a_k q'_k \in I$. Akibatnya berdasarkan definisi kongruensi, $f_k \equiv h \pmod{I_k}$. Berdasarkan Teorema 2.3.3

$$h \equiv f_k \pmod{I_k}.$$

Karena untuk setiap $k \in \{1, 2, \dots, m\}$ berlaku $h \equiv f_k \pmod{I_k}$, maka sistem (4.3) memiliki solusi. Dalam hal ini solusinya adalah h .

2. Akan ditunjukkan $h + \cap_{i=1}^m I_i = \{h + v | v \in \cap_{i=1}^m I_i\}$ merupakan himpunan solusi bagi (4.3) dengan menunjukan $h + \cap_{i=1}^m I_i$ termasuk ke dalam solusi bagi (4.3) dan setiap solusi bagi (4.3) merupakan anggota dari $h + \cap_{i=1}^m I_i$.

Akan ditunjukkan terlebih dahulu $h + \cap_{i=1}^m I_i$ termasuk ke dalam solusi dari sistem (4.3). Misalkan $v \in \cap_{i=1}^m I_i$. Berdasarkan Teorema 2.2.4. karena $\cap_{i=1}^m I_i = J \cap k[x_1, x_2, \dots, x_n]$, maka $v \xrightarrow{G} 0$. Artinya sebagai polinomial dalam $k[x_1, x_2, \dots, x_n, w_1, w_2, \dots, w_m]$, polinomial v yang habis dibagi oleh G dapat ditulis dalam bentuk

$$v = d \left(1 - \sum_{i=1}^m w_i \right) + \sum_{i=1}^m b_i w_i r_i \quad (4.5)$$

untuk suatu $d, b_i \in k[x_1, x_2, \dots, x_n, w_1, w_2, \dots, w_m]$, $r_i \in I_i$. Tetapkan $k \in \{1, 2, \dots, m\}$. Evaluasi (4.5) saat $w_k = 1$ dan $w_j = 0$ untuk $j \in \{1, 2, \dots, m\}, j \neq k$. Misalkan $v' = v(x_1, \dots, x_n, 0, \dots, 1, \dots, 0)$ dan $d' = d(x_1, \dots, x_n, 0, \dots, 1, \dots, 0)$, dan $r'_i = r_i(x_1, \dots, x_n, 0, \dots, 1, \dots, 0)$, untuk $i \in \{1, 2, \dots, m\}$. Evaluasi (4.5) menghasilkan

$$\begin{aligned} v' &= d' \left(1 - \sum_{i=1}^m w_i \right) + \sum_{i=1}^m b_i w_i r'_i \\ &= d'(1 - 1) + b_k r'_k \\ &= b_k r'_k. \end{aligned}$$

Karena $r'_k \in I$, maka $b_k r'_k \in I$. Akibatnya berdasarkan definisi kongruensi

$$v \equiv 0 \pmod{I_k}$$

Karena untuk setiap $k \in \{1, 2, \dots, m\}$ berlaku $v \equiv 0 \pmod{I_k}$, berdasarkan Teorema 2.3.3.

$$h + v \equiv f_k \pmod{I_k}$$

Akibatnya $h + \cap_{i=1}^m I_i$ termasuk dalam himpunan solusi dari sistem (4.3).

Kemudian akan ditunjukkan solusi dari sistem (4.3) merupakan anggota dari $h + \cap_{i=1}^m I_i$. Misalkan u adalah solusi dari sistem (4.3), yaitu

$$u \equiv f_i \pmod{I_i}$$

untuk setiap $i \in \{1, 2, \dots, m\}$. Maka u dapat ditulis dalam bentuk $u = q_i + f_i$, untuk suatu $q_i \in I_i$. Karena h merupakan solusi, maka h dapat ditulis dalam bentuk $h = r_i + f_i$, untuk suatu $r_i \in I_i$. Perhatikan bahwa

$$\begin{aligned} u &= q_i + f_i \\ &= q_i + (h - r_i) \\ &= h + (q_i - r_i). \end{aligned}$$

Akibatnya $u \in h + \cap_{i=1}^m I_i$. Jadi himpunan solusi dari sistem (4.3) adalah $h + \cap_{i=1}^m I_i = \{h + v \mid v \in \cap_{i=1}^m I_i\}$.

3. Misalkan u adalah solusi dari sistem (4.3), yaitu $u \in h + \cap_{i=1}^m I_i$. Artinya $u - h \in \cap_{i=1}^m I_i$ sehingga

$$u \equiv h \pmod{\cap_{i=1}^m I_i}.$$

Misalkan $G' = G \cap k[x_1, x_2, \dots, x_n]$, dan $J' = J \cap k[x_1, x_2, \dots, x_n]$.

Berdasarkan Teorema 2.2.3 dan Teorema 2.2.4, karena G merupakan basis Gröbner bagi J , maka G' merupakan basis Gröbner bagi J' dan $J' = \cap_{i=1}^m I_i$.

Karena h tereduksi terhadap G terhadap order eliminasi dan $G' \subseteq G$, maka $N_{G'}(h) = N_G(h) = h$. Berdasarkan Teorema 2.3.1.3., $u \equiv h \pmod{\cap_{i=1}^m I_i}$ jika dan hanya jika $N_{G'}(u) = N_{G'}(h)$. Jadi $u \in k[x_1, x_2, \dots, x_n]$ adalah solusi dari sistem (4.3) jika dan hanya jika $h = N_{G'}(u)$.

Dari dua poin pertama pada Teorema 4.1.2, diperoleh prosedur untuk menyelesaikan sistem kongruensi atas ring polinomial multivariabel. Misalkan

$$\begin{aligned} f &\equiv f_1 \pmod{I_1} \\ f &\equiv f_2 \pmod{I_2} \\ &\vdots \\ f &\equiv f_m \pmod{I_m} \end{aligned} \tag{4.6}$$

dengan $I_1, I_2, \dots, I_m$ adalah ideal yang berbeda pada $k[x_1, x_2, \dots, x_n]$ dan $f, f_1, f_2, \dots, f_m \in k[x_1, x_2, \dots, x_n]$. Langkah-langkah untuk menyelesaikan sistem (4.6) adalah sebagai berikut.

1. Bentuk ideal

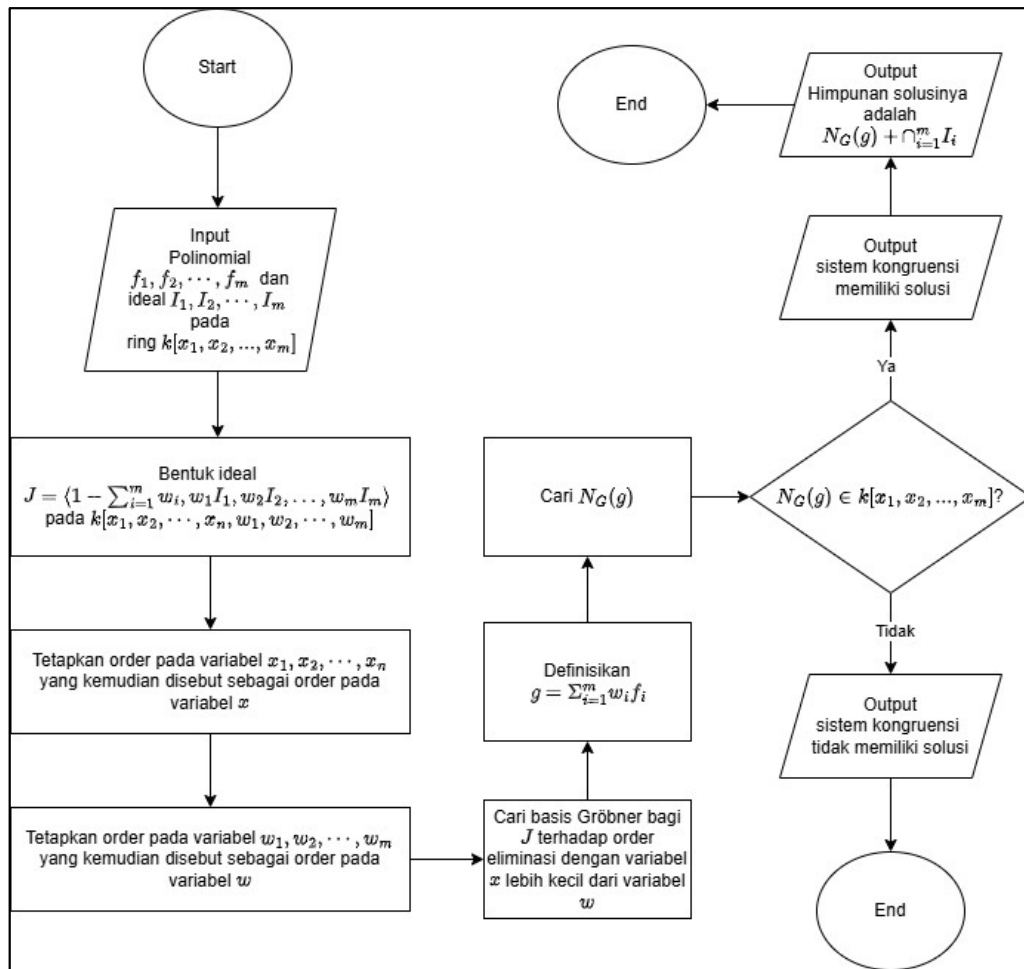
$$J = \langle 1 - \sum_{i=1}^m w_i, w_1 I_1, w_2 I_2, \dots, w_m I_m \rangle$$

pada $k[x_1, x_2, \dots, x_n, w_1, w_2, \dots, w_m]$.

2. Tetapkan order pada $x_1, x_2, \dots, x_n$, yang kemudian disebut sebagai order pada variabel x . Tetapkan sebuah order pada $w_1, w_2, \dots, w_m$, yang kemudian disebut sebagai order pada variabel w .
3. Cari basis Gröbner G bagi J terhadap order eliminasi dengan variabel x lebih kecil daripada variabel w .
4. Cari $N_G(\sum_{i=1}^m w_i f_i)$.
5. Jika $N_G(\sum_{i=1}^m w_i f_i) \notin k[x_1, x_2, \dots, x_n]$, maka sistem (4.6) tidak memiliki solusi. Jika $h = N_G(\sum_{i=1}^m w_i f_i) \in k[x_1, x_2, \dots, x_n]$, maka sistem (4.6) memiliki

solusi. Lebih lanjut himpunan solusinya adalah $h + \cap_{i=1}^m I_i = h + \langle G \cap k[x_1, x_2, \dots, x_n] \rangle$.

Langkah-langkah penyelesaian sistem kongruensi atas ring polinomial multivariabel diilustrasikan dalam diagram alir sebagai berikut.



Gambar 4.1 Langkah-langkah Penyelesaian Sistem Kongruensi

Contoh 4.1.3 Diberikan sistem kongruensi pada $\mathbb{Q}[x, y]$

$$\begin{aligned} f &\equiv x - 1 \pmod{\langle x, y \rangle} \\ f &\equiv x \pmod{\langle x - 1, y \rangle}. \end{aligned} \tag{4.7}$$

1. Bentuk ideal

$$J = \langle 1 - (w_1 + w_2), w_1 \langle x, y \rangle, w_2 \langle x - 1, y \rangle \rangle \subseteq \mathbb{Q}[x, y, w_1, w_2].$$

2. Tetapkan order leksikografis balikan derajat pada variabel x, y dengan $x < y$ dan order leksikografis balikan derajat pada variabel w_1, w_2 dengan $w_1 < w_2$.
3. Tetapkan order eliminasi dengan variabel x, y lebih kecil dari variabel w_1, w_2 .

Misalkan $F = \{g_1, g_2, g_3, g_4, g_5\}$ dengan $g_1 = -w_2 - w_1 + 1$, $g_2 = w_1x$, $g_3 = w_1y$, $g_4 = w_2x - w_2$, dan $g_5 = w_2y$ adalah pembangun dari J . Akan dicari basis Gröbner dari J dengan algoritma Buchberger.

Inisialisasi: $G := F$ dan $\mathcal{G} := \{\{g_1, g_2\}, \{g_1, g_3\}, \{g_1, g_4\}, \{g_1, g_5\}, \{g_2, g_3\}, \{g_2, g_4\}, \{g_2, g_5\}, \{g_3, g_4\}, \{g_3, g_5\}, \{g_4, g_5\}\}$

Iterasi pertama, $\mathcal{G} \neq \emptyset$

Pilih $\{g_1, g_2\} \in \mathcal{G}$

$\mathcal{G} := \mathcal{G} - \{\{g_1, g_2\}\}$

$$S(g_1, g_2) = \frac{w_2 w_1 x}{-w_2} g_1 - \frac{w_2 w_1 x}{w_1 x} g_2 = w_1^2 x - w_1 x$$

$$S(g_1, g_2) \xrightarrow{w_1, g_2} w_1 x \xrightarrow{-1, g_2} 0$$

Iterasi kedua, $\mathcal{G} \neq \emptyset$

Pilih $\{g_1, g_3\} \in \mathcal{G}$

$\mathcal{G} := \mathcal{G} - \{\{g_1, g_3\}\}$

$$S(g_1, g_3) = \frac{w_2 w_1 y}{-w_2} g_1 - \frac{w_2 w_1 y}{w_1 y} g_2 = w_1^2 y - w_1 y$$

$$S(g_1, g_3) \xrightarrow{w_1, g_3} w_1 y \xrightarrow{-1, g_3} 0$$

Iterasi ketiga, $\mathcal{G} \neq \emptyset$

Pilih $\{\{g_1, g_4\}\} \in \mathcal{G}$

$\mathcal{G} := \mathcal{G} - \{\{g_1, g_4\}\}$

$$S(g_1, g_4) = \frac{w_2 x}{-w_2} g_1 - \frac{w_2 x}{w_2 x} g_4 = w_1 x - w_2 - x$$

$$S(g_1, g_4) \xrightarrow{1, g_2} -w_2 - x \xrightarrow{1, g_1} w_1 + x - 1$$

Karena $w_1 + x - 1 \neq 0$

$$\text{Misalkan } g_6 := w_1 + x - 1$$

$$G := G \cup \{g_6\}$$

$$\mathcal{G} := \mathcal{G} \cup \{\{g_1, g_6\}, \{g_2, g_6\}, \dots, \{g_5, g_6\}\}$$

Iterasi keempat, $\mathcal{G} \neq \emptyset$

$$\text{Pilih } \{g_1, g_5\} \in \mathcal{G}$$

$$\mathcal{G} := \mathcal{G} - \{\{g_1, g_5\}\}$$

$$S(g_1, g_5) = \frac{w_2 y}{-w_2} g_1 - \frac{w_2 y}{w_2 y} g_5 = w_1 y - y$$

$$S(g_1, g_5) \xrightarrow{1, g_3} -y$$

Karena $-y \neq 0$

$$\text{Misalkan } g_7 := -y$$

$$G := G \cup \{g_7\}$$

$$\mathcal{G} := \mathcal{G} \cup \{\{g_1, g_7\}, \{g_2, g_7\}, \dots, \{g_6, g_7\}\}$$

Iterasi kelima, $\mathcal{G} \neq \emptyset$

$$\text{Pilih } \{g_2, g_3\} \in \mathcal{G}$$

$$\mathcal{G} := \mathcal{G} - \{\{g_2, g_3\}\}$$

$$S(g_2, g_3) = \frac{w_1 x y}{w_1 x} g_2 - \frac{w_1 x y}{w_1 y} g_3 = 0$$

Iterasi keenam, $\mathcal{G} \neq \emptyset$

$$\text{Pilih } \{g_2, g_4\} \in \mathcal{G}$$

$$\mathcal{G} := \mathcal{G} - \{\{g_2, g_4\}\}$$

$$S(g_2, g_4) = \frac{w_2 w_1 x}{w_1 x} g_2 - \frac{w_2 w_1 x}{w_2 x} g_4 = w_2 w_1$$

$$S(g_2, g_4) \xrightarrow{-w_1, g_1} -w_1^2 + w_1 \xrightarrow{-w_1, g_6} w_1 x \xrightarrow{x, g_6} -x^2 + x$$

Karena $-x^2 + x \neq 0$

Misalkan $g_8 := -x^2 + x$

$$G := G \cup \{g_8\}$$

$$\mathcal{G} := \mathcal{G} \cup \{\{g_1, g_8\}, \{g_2, g_8\}, \dots, \{g_6, g_8\}\}$$

Setelahnya untuk setiap $\{g_i, g_j\}$ pada $\mathcal{G}$ yang tersisa, $S(g_i, g_j) \xrightarrow{G} 0$. Artinya

$$G = \{-w_2 - w_1 + 1, w_1 x, w_1 y, w_2 x - w_2, w_2 y, w_1 + x - 1, -y, -x^2 + x\}$$

merupakan basis Gröbner bagi J .

4. Misalkan $g = w_1 f_1 + w_2 f_2 = w_1(x - 1) + w_2 x = w_2 x + w_1 x - w_1$.

Reduksi g terhadap G

$$g \xrightarrow{1, g_4} w_1 x + w_2 - w_1 \xrightarrow{1, g_2} w_2 - w_1 \xrightarrow{-1, g_1} -2w_1 + 1 \xrightarrow{-2, g_6} 2x - 1.$$

5. Karena $N_G(g) = 2x - 1 \in \mathbb{Q}[x, y]$, maka sistem (4.7) memiliki solusi.

Himpunan solusinya adalah $2x - 1 + \langle x, y \rangle \cap \langle x - 1, y \rangle = 2x - 1 + \langle -y, -x^2 + x \rangle$.

Kemudian poin ketiga pada Teorema 4.1.2 dapat digunakan untuk menguji apakah suatu polinomial pada $k[x_1, x_2, \dots, x_n]$ merupakan solusi bagi sistem (4.7).

Contoh 4.1.4 Dari Contoh 4.1.3. diperoleh $G \cap \mathbb{Q}[x, y] = \{-y, -x^2 + x\}$ dan $h = 2x - 1$. Misalkan $h_1 = -y$ dan $h_2 = -x^2 + x$. Misalkan $u_1 = 2x^2 - 1$. Reduksi u_1 oleh $G \cap \mathbb{Q}[x, y]$ menghasilkan

$$u_1 \xrightarrow{-2, h_2} 2x - 1.$$

Artinya $N_{G \cap \mathbb{Q}[x,y]}(u_1) = 2x - 1 = h$. Karena $N_{G \cap \mathbb{Q}[x,y]}(u_1) = h$, maka u_1 adalah suatu solusi dari sistem kongruensi pada Contoh 4.1.3. Misalkan $u_2 = 2x^2 + y$. Reduksi u_2 oleh $G \cap \mathbb{Q}[x, y]$ menghasilkan

$$u_2 \xrightarrow{-2, h_2} y + 2x \xrightarrow{-1, h_1} 2x.$$

Karena $N_{G \cap \mathbb{Q}[x,y]}(u_2) = 2x \neq h$, maka u_2 bukan solusi dari sistem kongruensi pada Contoh 4.1.3.

Berikut ini adalah contoh sistem kongruensi atas ring polinomial multivariabel yang tidak memiliki solusi.

Contoh 4.1.5 Diberikan sistem kongruensi pada $\mathbb{Q}[x, y]$

$$\begin{aligned} f &\equiv x \pmod{\langle x^2y, y - 1 \rangle} \\ f &\equiv x + 1 \pmod{\langle x^3y, y - 1 \rangle} \end{aligned} \tag{4.8}$$

1. Bentuk ideal

$$J = \langle 1 - (w_1 + w_2), w_1 \langle x^2y, y - 1 \rangle, w_2 \langle x^3y, y - 1 \rangle \rangle \subseteq \mathbb{Q}[x, y, w_1, w_2].$$

2. Tetapkan order leksikografis derajat pada variabel x, y dengan $x < y$ dan order leksikografis derajat pada variabel w_1, w_2 dengan $w_1 < w_2$.

3. Tetapkan order eliminasi dengan variabel x, y lebih kecil dari variabel w_1, w_2 .

Misalkan $F = \{g_1, g_2, g_3, g_4, g_5\}$ dengan $g_1 = -w_2 - w_1 + 1$, $g_2 = w_1x^2y$, $g_3 = w_1y - w_1$, $g_4 = w_2x^3y$, dan $g_5 = w_2y - w_2$ adalah pembangun dari J .

Akan dicari basis Gröbner dari J dengan algoritma Buchberger

Inisialisasi: $G := F$ dan $\mathcal{G} := \{\{g_1, g_2\}, \{g_1, g_3\}, \{g_1, g_4\}, \{g_1, g_5\}, \{g_2, g_3\}, \{g_2, g_4\}, \{g_2, g_5\}, \{g_3, g_4\}, \{g_3, g_5\}, \{g_4, g_5\}\}$

Iterasi pertama, $\mathcal{G} \neq \emptyset$

Pilih $\{g_1, g_2\} \in \mathcal{G}$

$$\mathcal{G} := \mathcal{G} - \{\{g_1, g_2\}\}$$

$$S(g_1, g_2) = \frac{w_2 w_1 x^2 y}{-w_2} g_1 - \frac{w_2 w_1 x^2 y}{w_1 x^2 y} g_2 = w_1^2 x^2 y - w_1 x^2 y$$

$$S(g_1, g_2) \xrightarrow{w_1, g_2} w_1 x \xrightarrow{-1, g_2} 0$$

Iterasi kedua, $\mathcal{G} \neq \emptyset$

Pilih $\{g_1, g_3\} \in \mathcal{G}$

$$\mathcal{G} := \mathcal{G} - \{\{g_1, g_3\}\}$$

$$S(g_1, g_3) = \frac{w_2 w_1 y}{-w_2} g_1 - \frac{w_2 w_1 y}{w_1 y} g_2 = w_1^2 y + w_2 w_1 - w_1 y$$

$$S(g_1, g_3) \xrightarrow{w_1, g_3} w_2 w_1 + w_1^2 - w_1 y \xrightarrow{-w_1, g_3} -w_1 y + w_1 \xrightarrow{-1, g_3} 0$$

Iterasi ketiga, $\mathcal{G} \neq \emptyset$

Pilih $\{\{g_1, g_4\}\} \in \mathcal{G}$

$$\mathcal{G} := \mathcal{G} - \{\{g_1, g_4\}\}$$

$$S(g_1, g_4) = \frac{w_2 x^3 y}{-w_2} g_1 - \frac{w_2 x^3 y}{w_2 x^3 y} g_4 = w_1 x^3 y - x^3 y$$

$$S(g_1, g_4) \xrightarrow{x, g_2} -x^3 y$$

Karena $-x^3 y \neq 0$

Misalkan $g_6 := -x^3 y$

$$G := G \cup \{g_6\}$$

$$\mathcal{G} := \mathcal{G} \cup \{\{g_1, g_6\}, \{g_2, g_6\}, \dots, \{g_5, g_6\}\}$$

Iterasi keempat, $\mathcal{G} \neq \emptyset$

Pilih $\{\{g_1, g_5\}\} \in \mathcal{G}$

$$\mathcal{G} := \mathcal{G} - \{\{g_1, g_5\}\}$$

$$S(g_1, g_5) = \frac{w_2 y}{-w_2} g_1 - \frac{w_2 y}{w_2 y} g_5 = w_1 y + w_2 - y$$

$$S(g_1, g_5) \xrightarrow{1, g_3} w_2 + w_1 - y \xrightarrow{-1, g_1} -y + 1$$

Karena $-y + 1 \neq 0$

Misalkan $g_7 := -y + 1$

$$G := G \cup \{g_7\}$$

$$\mathcal{G} := \mathcal{G} \cup \{\{g_1, g_7\}, \{g_2, g_7\}, \dots, \{g_6, g_7\}\}$$

Iterasi kelima, $\mathcal{G} \neq \emptyset$

Pilih $\{\{g_2, g_3\}\} \in \mathcal{G}$

$$\mathcal{G} := \mathcal{G} - \{\{g_2, g_3\}\}$$

$$S(g_2, g_3) = \frac{w_1 x^2 y}{w_1 x^2 y} g_2 - \frac{w_1 x^2 y}{w_1 y} g_3 = w_1 x^2$$

$$S(g_2, g_3) \xrightarrow{G}_+ w_1 x^2$$

Karena $w_1 x^2 \neq 0$

Misalkan $g_8 := w_1 x^2$

$$G := G \cup \{g_8\}$$

$$\mathcal{G} := \mathcal{G} \cup \{\{g_1, g_8\}, \{g_2, g_8\}, \dots, \{g_7, g_8\}\}$$

Iterasi keenam, $\mathcal{G} \neq \emptyset$

Pilih $\{\{g_4, g_5\}\} \in \mathcal{G}$

$$\mathcal{G} := \mathcal{G} - \{\{g_4, g_5\}\}$$

$$S(g_4, g_5) = \frac{w_2 x^3 y}{w_2 x^3 y} g_4 - \frac{w_2 x^3 y}{w_2 y} g_5 = w_2 x^3$$

$$S(g_2, g_3) \xrightarrow{-x^3, g_1} -w_1 x^3 + x^3 \xrightarrow{-1, g_1} x^3$$

Karena $x^3 \neq 0$

Misalkan $g_9 := x^3$

$$G := G \cup \{g_9\}$$

$$\mathcal{G} := \mathcal{G} \cup \{\{g_1, g_9\}, \{g_2, g_9\}, \dots, \{g_8, g_9\}\}$$

4. Setelahnya untuk setiap $\{g_i, g_j\}$ pada $\mathcal{G}$ yang tersisa, $S(g_i, g_j) \xrightarrow{G}_+ 0$. Artinya

$$G = \{-w_2 - w_1 + 1, w_1x^2y, w_1y - w_1, w_2x^3y, w_2y - w_2, -x^3y, -y \\ + 1, w_1x^2, x^3\}$$

merupakan basis Gröbner bagi J .

5. Misalkan $g = w_1f_1 + w_2f_2 = w_1x + w_2(x + 1) = w_2x + w_1x + w_2$.

Reduksi g terhadap G

$$g \xrightarrow{-x, g_1} w_2 + x \xrightarrow{-1, g_1} -w_1 + x + 1.$$

6. Karena $N_G(g) = -w_1 + x + 1 \notin \mathbb{Q}[x, y]$, maka sistem (4.8) tidak memiliki solusi.

4.2 Implementasi pada Singular-CAS

Langkah-langkah penyelesaian sistem kongruensi atas ring polinomial multivariabel dengan basis Gröbner berdasarkan Teorema 4.1.2. akan diimplementasikan pada Singular-CAS dalam bentuk prosedur. Prosedur ini ditulis menggunakan *software* Notepad bawaan Windows dan disimpan dalam format .txt. Terdapat dua prosedur yang dibuat. Berikut ini adalah deskripsi dari kedua prosedur tersebut.

1. Prosedur pertama bernama “solveCongruences”. Prosedur ini memiliki dua parameter. Parameter pertama adalah polinomial-polinomial dari sistem kongruensi. Parameter kedua adalah ideal-ideal dari sistem kongruensi. Saat dijalankan, prosedur ini akan menunjukkan apakah sistem kongruensi yang diberikan memiliki solusi atau tidak dan menunjukkan himpunan solusinya jika sistem kongruensi yang diberikan memiliki solusi.

2. Prosedur kedua bernama “checkSolution”. Prosedur ini memiliki tiga paramter.

Parameter pertama adalah suatu polinomial u . Parameter kedua dan ketiga diambil dari prosedur pertama. Prosedur ini akan menentukan apakah u termasuk ke dalam solusi bagi sistem kongruensi.

Dari prosedur yang sudah dibuat, berikut ini langkah-langkah untuk menjalankan prosedur pertama.

1. Salin prosedur yang disimpan ke dalam Singular-CAS.
2. Deklarasikan ring yang terdiri dari lapangan k , variabel, dan order eliminasi dengan variabel x lebih kecil dari variabel w .
3. Deklarasikan polinomial $f_1, f_2, \dots, f_m$ dan ideal $I_1, I_2, \dots, I_m$ dari sistem kongruensi.
4. Himpun $f_1, f_2, \dots, f_m$ dalam sebuah *list*. Himpun juga $I_1, I_2, \dots, I_m$ dalam sebuah *list*.
5. Panggil prosedur untuk menentukan apakah sistem kongruensi memiliki solusi dan menunjukkan himpunan solusinya dengan parameterya adalah *list* dari $f_1, f_2, \dots, f_m$ dan *list* dari $I_1, I_2, \dots, I_m$.

Contoh 4.2.1 Diberikan sistem kongruensi pada $\mathbb{Q}[x, y, z]$

$$\begin{aligned} f &\equiv x^2 - 1 \pmod{\langle x^2, y, 2z + x \rangle} \\ f &\equiv x^2 \pmod{\langle x^2 - 1, y \rangle} \\ f &\equiv y - z \pmod{\langle x^2 - 2, x - 1 \rangle}. \end{aligned} \tag{4.9}$$

Tetapkan order leksikografis balikan derajat dengan $x < y < z$. Karena terdapat tiga kongruensi, maka terdapat tiga variabel baru w_1, w_2, w_3 berorde derajat leksikografis balikan derajat dengan $w_1 < w_2 < w_3$. Deklarasikan ring, polinomial, dan ideal dari sistem kongruensi

```
> ring r = 0, (w3,w2,w1,z,y,x), (dp(3),dp(2));
ideal I1 = x^2,y,2z+x;
ideal I2 = x^2-1,y;
ideal I3 = x^2-2,x-1;
poly f1 = x^2-1;
poly f2 = x^2;
poly f3 = y-z;
```

Gambar 4.2 Pendeklarasian Ring, Polinomial, dan Ideal dari Contoh 4.2.1.

Gabungkan ideal I_1, I_2, I_3 dalam sebuah *list*. Begitupun juga untuk f_1, f_2, f_3 .

Kemudian jalankan prosedur dengan parameter *list* dari f_1, f_2, f_3 dan *list* dari I_1, I_2, I_3 .

```
list idealCong= I1,I2,I3;
list polyCong = f1,f2,f3;
list result = solveCongruences(polyCong, idealCong);
```

Gambar 4.3 Proses Menjalankan Prosedur “solveCongruences”

Berikut ini adalah hasil akhir dari prosedur yang dijalankan

```
Ideal J dibangun oleh:
J[1]=-w3-w2-w1+1
J[2]=w3*x^2-2*w3
J[3]=w3*x-w3
J[4]=w2*x^2-w2
J[5]=w2*y
J[6]=w1*x^2
J[7]=w1*y
J[8]=2*w1*z+w1*x
Basis Groebner GJ dari J:
GJ[1]=y
GJ[2]=2*z*x^2+x^3-2*z-x
GJ[3]=x^4-x^2
GJ[4]=w1+x^2-1
GJ[5]=w2+w1-1
GJ[6]=w3+w2+w1-1
Polinomial g yang terbentuk:
-w3*z+w3*y+w2*x^2+w1*x^2-w1
Reduksi g oleh GJ:
2*x^2-1
Karena bentuk normal dari g tidak memiliki suku dengan variabel w,
maka sistem persamaan kongruensi memiliki solusi
```

Gambar 4.4 *Output* dari Prosedur untuk Sistem Kongruensi Contoh 4.2.1.

Terlihat bahwa basis Gröbner dari ideal $J = \langle 1 - (w_1 + w_2 + w_3), w_1 I_1, w_2 I_2, w_3 I_3 \rangle$ adalah

$$G = \{y, 2zx^2 + x^3 - 2z - x, x^4 - x^2, w_1 + x^2 - 1, w_2 + w_1 - 1, w_3 + w_2 + w_1 - 1\}.$$

Saat $g = w_1f_1 + w_2f_2 + w_3f_3$ direduksi oleh G , hasilnya adalah $g = 2x^2 - 1 \in \mathbb{Q}[x, y, z]$. Maka sistem (4.9) memiliki solusi.

Mengapa G memiliki elemen yang lebih sedikit daripada pembangun J ? Hal ini dikarenakan Singular mengkomputasikan basis Gröbner yang tereduksi bagi J , berbeda seperti pada pembahasan sebelumnya, komputasi basis Gröbner dengan algoritma Buchberger tidak memungkinkan untuk mendapatkan basis Gröbner G dengan banyak elemen yang lebih sedikit dari pada pembangun J . Tetapi setelah didapatkan basis Gröbner G dengan algoritma Buchberger, dapat dilakukan penghapusan beberapa elemen sehingga akan didapatkan sebuah basis Gröbner yang tereduksi bagi J .

Prosedur ini menyimpan empat hal jika sistem persamaan kongruensi memiliki solusi.

```
> result[1];
2*x^2-1
> result[2];
_[1]=y
_[2]=2*z*x^2+x^3-2*z-x
_[3]=x^4-x^2
_[4]=w1+x^2-1
_[5]=w2+w1-1
_[6]=w3+w2+w1-1
> result[3];
_[1]=y
_[2]=2*z*x^2+x^3-2*z-x
_[3]=x^4-x^2
> result[4];
Himpunan solusi: 2*x^2-1 + <y, 2*z*x^2+x^3-2*z-x, x^4-x^2>
```

Gambar 4.5 Hasil Perhitungan yang Disimpan oleh Prosedur

Hal pertama yang disimpan adalah bentuk normal dari g . Kedua adalah basis Gröbner G bagi ideal J . Ketiga adalah irisan dari ideal I_1, I_2 , dan I_3 . Keempat adalah himpunan solusi dari sistem kongruensi. Dalam hal ini, himpunan solusi dari sistem (4.9) adalah $2x^2 - 1 + \langle y, 2x^2z + x^3 - 2z - x, x^4 - x^2 \rangle$.

Berikut adalah contoh suatu sistem kongruensi yang tidak memiliki solusi.

Contoh 4.2.2 Diberikan sistem kongruensi pada $\mathbb{Q}[x, y]$

$$\begin{aligned} f &\equiv 0 \pmod{\langle x, y \rangle} \\ f &\equiv 1 \pmod{\langle x, y^2 \rangle}. \end{aligned} \quad (4.10)$$

Tetapkan order leksikografis balikan derajat pada variabel x, y dengan $x < y$ dan pada variabel w_1, w_2 dengan $w_1 < w_2$. Hasil dari prosedur yang dijalankan adalah

```

Ideal J dibangun oleh:
J[1]=-w2-w1+1
J[2]=w2*x
J[3]=w2*y^2
J[4]=w1*x
J[5]=w1*y
Basis Groebner GJ dari J:
GJ[1]=x
GJ[2]=y^2
GJ[3]=w1*y
GJ[4]=w2+w1-1
Polinomial g yang terbentuk:
w2
Reduksi g oleh GJ:
-w1+1
Karena bentuk normal dari g memiliki suku bervariasi w,
maka sistem persamaan kongruensi tidak memiliki solusi

```

Gambar 4.6 *Output* dari Prosedur untuk Sistem Kongruensi Contoh 4.2.2.

Terlihat bahwa pada sistem (4.10), $N_G(g) = -w_1 + 1 \notin \mathbb{Q}[x, y]$. Jadi sistem (4.10) tidak memiliki solusi.

Setelah diketahui bahwa sistem kongruensi atas ring polinomial multivariabel yang diberikan memiliki solusi, kemudian dicari himpunan solusinya. Selanjutnya dapat ditentukan apakah suatu polinomial solusi dari sistem kongruensi. Langkah ini juga diimplementasikan pada Singular-CAS pada prosedur kedua. Pengecekan dilakukan berdasarkan poin ketiga dari Teorema 4.1.2. Misalkan u adalah suatu polinomial. Jika bentuk normal dari u sama dengan bentuk normal dari g ketika

direduksi oleh $G \cap k[x_1, x_2, \dots, x_n]$, maka u juga merupakan solusi bagi sistem kongruensi yang diberikan.

Contoh 4.2.3 Diberikan sistem kongruensi seperti pada Contoh 4.2.1. Bentuk normal dari g pada sistem tersebut adalah $h = 2x^2 - 1$. Maka h juga merupakan solusi. Definisikan h pada Singular. Panggil prosedur dengan parameternya adalah u , bentuk normal dari g , dan irisan dari ideal I_1, I_2, I_3 untuk apakah h merupakan solusi dari sistem kongruensi pada Contoh 4.2.1.

```
> poly u = 2*x^2-1;
checkSolution(u,result[1],result[3]);
// ** GJ is no standard basis
2*x^2-1
u termasuk solusi
```

Gambar 4.7 Hasil Pengecekan untuk $h = 2x^2 - 1$

Jika dimisalkan $u = z^3 - yz$, maka

```
> poly u = z^3 - y*z;
checkSolution(u,result[1],result[3]);
// ** GJ is no standard basis
z^3
u bukanlah solusi
```

Gambar 4.8 Hasil Pengecekan untuk $u = z^3 + yz$

bentuk normal dari u adalah z^3 . Artinya u bukan solusi dari sistem kongruensi pada Contoh 4.2.1.

BAB V

PENUTUP

5.1 Kesimpulan

1. Berdasarkan pembahasan, diperoleh langkah-langkah penyelesaian sistem kongruensi atas ring polinomial multivariabel dengan basis Gröbner sebagai berikut.

Misalkan

$$\begin{aligned} f &\equiv f_1 \pmod{I_1} \\ f &\equiv f_2 \pmod{I_2} \\ &\vdots \\ f &\equiv f_m \pmod{I_m} \end{aligned} \tag{5.1}$$

adalah sistem kongruensi atas $k[x_1, x_2, \dots, x_n]$ dengan $I_1, I_2, \dots, I_m$ adalah ideal yang berbeda pada ring polinomial $k[x_1, x_2, \dots, x_n]$ dan $f, f_1, f_2, \dots, f_m \in k[x_1, x_2, \dots, x_n]$. Maka langkah-langkah penyelesaian dari sistem (5.1) adalah sebagai berikut.

- a. Membentuk ideal

$$J = \langle 1 - \sum_{i=1}^m w_i, w_1 I_1, w_2 I_2, \dots, w_m I_m \rangle$$

pada $k[x_1, x_2, \dots, x_n, w_1, w_2, \dots, w_m]$.

- b. Menetapkan order pada $x_1, x_2, \dots, x_n$, yang kemudian disebut sebagai order pada variabel x . Tetapkan sebuah order pada $w_1, w_2, \dots, w_m$, yang kemudian disebut sebagai order pada variabel w .
- c. Mencari basis Gröbner G bagi J terhadap order eliminasi dengan variabel x lebih kecil daripada variabel w .
- d. Menentukan $N_G(\sum_{i=1}^m w_i f_i)$.

- e. Jika $N_G(\sum_{i=1}^m w_i f_i) \notin k[x_1, x_2, \dots, x_n]$, maka sistem (5.1) tidak memiliki solusi. Jika $h = N_G(\sum_{i=1}^m w_i f_i) \in k[x_1, x_2, \dots, x_n]$, maka sistem (5.1) memiliki solusi. Lebih lanjut himpunan solusinya adalah $h + \cap_{i=1}^m I_i = h + \langle G \cap k[x_1, x_2, \dots, x_n] \rangle$.

2. Implementasi dari metode penyelesaian sistem kongruensi atas ring polinomial multivariabel dengan basis Gröbner pada Singular-CAS dilakukan dengan membuat dua prosedur pada Singular-CAS. Berikut ini adalah deskripsi dari dua prosedur tersebut.

- a. Prosedur pertama bernama “solveCongruences”. Prosedur ini memiliki dua parameter. Parameter pertama adalah polinomial-polinomial dari sistem kongruensi. Parameter kedua adalah ideal-ideal dari sistem kongruensi. Saat dijalankan, prosedur ini akan menunjukkan apakah sistem kongruensi yang diberikan memiliki solusi atau tidak dan menunjukkan himpunan solusinya jika sistem kongruensi yang diberikan memiliki solusi.

Berikut ini langkah-langkah untuk menjalankan prosedur pertama.

- i. Menyalin prosedur yang disimpan ke dalam Singular-CAS.
- ii. Mendeklarasikan ring yang terdiri dari lapangan k , variabel, dan order eliminasi dengan variabel x lebih kecil dari variabel w .
- iii. Mendeklarasikan polinomial $f_1, f_2, \dots, f_m$ dan ideal $I_1, I_2, \dots, I_m$ dari sistem kongruensi.
- iv. Menghimpun $f_1, f_2, \dots, f_m$ dalam sebuah *list*. Himpun juga $I_1, I_2, \dots, I_m$ dalam sebuah *list*.

- v. Panggil prosedur untuk menentukan apakah sistem kongruensi memiliki solusi dan menunjukkan himpunan solusinya dengan parameternya adalah *list* dari $f_1, f_2, \dots, f_m$ dan *list* dari $I_1, I_2, \dots, I_m$.
- b. Prosedur kedua bernama “checkSolution”. Prosedur ini memiliki tiga parameter. Parameter pertama adalah suatu polinomial u . Parameter kedua dan ketiga diambil dari prosedur pertama. Prosedur ini akan menentukan apakah u termasuk ke dalam solusi bagi sistem kongruensi. Dari prosedur pertama, jalankan prosedur kedua untuk menentukan apakah suatu polinomial u termasuk ke dalam solusi bagi sistem kongruensi atas ring polinomial multivariabel.

5.2 Saran untuk Penelitian Lanjutan

Dalam penelitian ini, koefisien dari ring polinomial yang ditinjau pada sistem kongruensi adalah suatu lapangan k . Peneliti selanjutnya disarankan untuk mengkaji apakah metode dengan basis Gröbner dapat diaplikasikan untuk menyelesaikan sistem kongruensi atas ring polinomial saat koefisien dari ring polinomial adalah ring komutatif yang bukan lapangan.

DAFTAR PUSTAKA

- Adams, W. W., & Loustaunau, P. (1996). *An Introduction to Gröbner Bases*. American Mathematical Society.
- Buchberger, B. (2006). Bruno Buchberger's PhD thesis 1965: An Algorithm for Finding The Basis Elements of The Residue Class Ring of a Zero Dimensional Polynomial Ideal. *Journal of Symbolic Computation*, 475-511.
- Cox, D. A., Little, J., & O'Shea, D. (2015). *Ideals, Varieties, and Algorithms Fourth Edition*. Springer.
- Dummit, D. S., & Foote, R. M. (2004). *Abstract Algebra Third Edition*. John Wiley and Sons.
- Gallian, J. A. (2013). *Contemporary Abstract Algebra*. Boston: Cengage Learning.
- Gathen, J. v., & Gerhard, J. (2003). *Modern Computer Algebra Second Edition*. Cambridge: Cambridge University Press.
- Greuel, G.-M., & Pfister, G. (2007). *A Singular Introduction to Commutative Algebra*. Springer Berlin.
- Kementerian Agama Saudi Arabia. (2021). *Tafsir Al-Muyassar*.
- Kemenag RI. (2022). *Al-Qur'an dan Terjemahannya*. Jakarta: Lajnah Pentasihan Mushaf Al-Qur'an Kementerian Agama Republik Indonesia
- Lin, Z., Xu, L., & Wu, Q. (2004). Applications of Gröbner Bases to Signal and Image Proccesing: A Survey. *Linear Algebra and its Applications*, 169-202.
- Rosen, K. H. (2005). *Elementary Number Theory and Its Applications Fifth Edition*. Pearson.

LAMPIRAN

Lampiran 1. Prosedur untuk menguji eksistensi dan himpunan solusi dari sistem kongruensi atas ring polinomial multivariabel dengan basis Gröbner.

```
proc solveCongruences(list congruences_poly, list congruences_ideal)
{
    int m = size(congruences_ideal);

    // Build ideal J
    ideal J;
    poly sum_w = 0;

    for (int i = 1; i <= m; i++) {
        sum_w = sum_w + var(i);
    }
    J[1] = 1 - sum_w;
    int counter = 2;
    for (i = 1; i <= m; i++) {
        ideal I = congruences_ideal[m+1-i];
        for (int j = 1; j <= ncols(I); j++) {
            J[counter] = var(i) * I[j];
            counter++;
        }
    }
    print("Ideal J dibangun oleh:");
    J;

    // Compute Gröbner basis
    ideal GJ = std(J);
    print("Basis Groebner GJ dari J:");
    GJ;

    // Build polynomial g
    poly g = 0;
    for (i = 1; i <= m; i++) {
        g = g + var(i) * congruences_poly[m+1-i];
    }
    print("Polinomial g yang terbentuk: ");
    g;

    // Reduce g
    poly reduceg = reduce(g, GJ);
    print("Reduksi g oleh GJ:");
    reduceg;

    // Check if solution exists - simpler approach
    // Just check if reduceg is in the subring of x-variables
    // We can do this by checking if it's unchanged when we map w_i -> 0
    poly check = reduceg;
    for (i = 1; i <= m; i++) {
        check = subst(check, var(i), 0);
    }

    if (check != reduceg) {
        print("Karena bentuk normal dari g memiliki suku bervariasi w,");
        print("maka sistem persamaan kongruensi tidak memiliki solusi");
        return(reduceg);
    }

    print("Karena bentuk normal dari g tidak memiliki suku bervariasi w,");
    print("maka sistem persamaan kongruensi memiliki solusi");

    //intersection ideal
    ideal intersection_ideal = eliminate(GJ, 1..m);

    // solution set
    string solution_set = "Himpunan solusi: " + string(reduceg) + " + <" + string(intersection_ideal) + ">";

    return(list(reduceg, GJ, intersection_ideal, solution_set));
}
```

Lampiran 2. Prosedur untuk mengecek apakah suatu polinomial merupakan solusi bagi sistem kongruensi atas ring polinomial.

```
proc checkSolution (u,reduceg,GJ)
{
    poly normal_u = reduce(u,GJ);
    normal_u;
    if (normal_u == reduceg)
    {
        return("u termasuk solusi");
    }
    return("u bukanlah solusi");
}
```

RIWAYAT HIDUP



Penulis bernama Mohammad Zaenal Fanani, lahir pada 5 Mei 2003. Penulis berasal dari Desa Denanyar Kabupaten Jombang. Penulis merupakan anak kedua dari pasangan Anis Samsul Huda dan Anisatun Nihlah. Pendidikan formal yang ditempuh diawali dengan pendidikan sekolah dasar di MIN 1 Jombang dan lulus pada tahun 2016. Kemudian pendidikan sekolah menengah pertama di MTsN 4 Jombang dan lulus pada tahun 2019. Selanjutnya penulis menempuh pendidikan sekolah menengah atas di MAN 4 Jombang dan lulus pada tahun 2022. Setelah lulus, penulis melanjutkan studinya pada Jurusan Matematika, Fakultas Sains dan Teknologi, UIN Maulana Malik Ibrahim Malang. Selain kegiatan perkuliahan penulis juga aktif mengikuti kepanitian olimpiade matematika dan menjadi guru privat.



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

BUKTI KONSULTASI SKRIPSI

Nama : Mohammad Zaenal Fanani
NIM : 220601110091
Fakultas / Jurusan : Sains dan Teknologi / Matematika
Judul Skripsi : Aplikasi Basis Gröbner pada Penyelesaian Sistem Kongruensi atas Ring Poinomial Multivariabel dan Implementasi pada Singular-CAS
Pembimbing I : Dewi Ismiarti, M.Si.
Pembimbing II : Ari Kusumastuti, M.Si.

No	Tanggal	Hal	Tanda Tangan
1.	8 September 2025	Konsultasi Bab I	1.
2.	18 September 2025	Konsultasi Bab IV	2.
3.	25 September 2025	Konsultasi Bab I, II, dan III	3.
4.	14 Oktober 2025	Konsultasi Kajian Integrasi Bab I	4.
5.	21 Oktober 2025	Konsultasi Kajian Integrasi Bab I	5.
6.	29 Oktober 2025	Konsultasi Kajian Integrasi Bab I dan II	6.
7.	4 November 2025	ACC Kajian Integrasi Bab I dan II	7.
8.	6 November 2025	Konsultasi Bab IV	8.
9.	19 November 2025	Konsultasi Bab IV	9.
10.	26 November 2025	ACC Seminar Proposal	10.
11.	3 Desember 2025	Konsultasi Revisi Seminar Proposal	11.
12.	9 Desember 2025	Konsultasi Revisi Seminar Proposal	12.
13.	6 Februari 2026	ACC Seminar Hasil	13.
14.	13 Februari 2026	Konsultasi Revisi Seminar Hasil	14.
15.	3 Maret 2026	ACC Kajian Integrasi Bab I dan II	15.



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

16.	3 Maret 2026	Konsultasi Sebelum Sidang	16.
17.	30 Maret 2026	Konsultasi Sebelum Sidang	17.
18.	28 April 2026	ACC Akhir Keseluruhan	18.

Malang, 28 April 2026

Mengetahui,

Ketua Program Studi Matematika



Dr. Fachrur Rozi, M.Si.

NIP. 19800527 200801 1 012