5-2017

Problem Book on Higher Algebra and Number Theory

Ryanto Putra
The University of Texas Rio Grande Valley

PROBLEM BOOK ON HIGHER ALGEBRA AND NUMBER THEORY

A Thesis

by

RYANTO PUTRA

Submitted to the Graduate College of
The University of Texas Rio Grande Valley
In partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

May 2017

Major Subject: Mathematics

PROBLEM BOOK ON HIGHER ALGEBRA AND NUMBER THEORY

A Thesis
by
RYANTO PUTRA

COMMITTEE MEMBERS

Dr. habil. Paul-Hermann Zieschang
Chair of Committee

Dr. Timothy Huber
Committee Member

Dr. Elena Poletaeva
Committee Member

Dr. Sergey Grigorian
Committee Member

May 2017

ABSTRACT

Putra, Ryanto, Problem Book on Higher Algebra and Number Theory. Master of Science (MS), May, 2017, 121 pp., references, 7 titles.

This book is an attempt to provide relevant end-of-section exercises, together with their step-by-step solutions, to Dr. Zieschang's classic class notes *Higher Algebra* and *Number Theory.* It's written under the notion that active hands-on working on exercises is an important part of learning, whereby students would see the nuance and intricacies of a math concepts which they may miss from passive reading. The problems are selected here to provide background on the text, examples that illuminate the underlying theorems, as well as to fill in the gaps in the notes.

DEDICATION

I wholeheartedly dedicate this thesis to my dear wife, Jade S. Putra, for her sacrifices, understanding, support, faith, wisdom and unlimited patience; to my late mother Mrs. Liem, whose hardship, hard work and sacrifices that I came to appreciate only after her passing. Rest in peace; we all love you.

ACKNOWLEDGEMENT

I would like to devote this acknowledgement to thank Dr. Zieschang for giving me this opportunity to compile problems and their solutions to his two elegant class notes, *Higher Algebra* and *Number Theory.* His encouragements, admonition and support that have carried me through. May this set be useful to his future students. I am doubtful that I would be able to write this thesis without these virtues from him.

Likewise, I am grateful to Dr. Timothy Huber, not only for agreeing to sit as committee member, but for his gentle guidance on transitioning from Brownsville to RGV thesis requirement. Finally, to the rest of committee members, Dr. Elena Poletaeva and Dr. Sergey Grigorian, for graciously agreeing to sit as committee members.

TABLE OF CONTENTS

Page

ABSTRACT iii

DEDICATION iv

ACKNOWLEDGEMENT v

TABLE OF CONTENTS vii

CHAPTER I. INTRODUCTION 1

CHAPTER II. HIGHER ALGEBRA 5

2.1 Basic Facts on Commutative Rings with 1 5

2.2 Modules 11

2.3 The Field of Fractions of an Integral Domain 15

2.4 Integrality 21

2.5 Integrality and Fields 24

2.6 Prime Ideals 28

2.7 The Krull Dimension 31

2.8 Noetherian Modules 35

2.9 Noetherian Integral Domain 40

2.10 Commutative Artinian Rings 44

2.11 Noetherian Domain of Dimension 1 49

2.12 Dedekind Domain 53

2.13 The Field of Fractions of a Dedekind Domain 57

CHAPTER III. NUMBER THEORY 61

3.1 Commutative Rings 61

3.2 Some Basic Arithmetic 68

3.3 Theorems of Euler, Fermat and Wilson 72

3.4 Quadratic Number Fields 79

3.5 The Ring of the Gaussian Integers 87

3.6 Pythagorean Triples 92

3.7 Fermat’s Theorem for Multiples of Four 107

3.8 Fermat’s Theorem for Multiples of Three 114

REFERENCES 120

BIOGRAPHICAL SKETCH 121

CHAPTER I

INTRODUCTION

This problems and solutions set is written to accompany Dr. Zieschang's class note on *Higher Algebra* and *Number Theory*, to satisfy my degree requirement for MS degree from UT-RGV. I am planning to use this introduction to lay out my case for providing these problems and solutions set to the class notes, and explaining the methods that I compiled these exercises with. I would like to begin with the story of my late mother.

My mother was an elementary teacher at a village in southern China in 1930s. She told me that on the first day of her job, the principal handed her a stack of writing slates for her students, a worn-out textbook for her and pointed to a worn-out poster pinned to the wall written by Confusius, the 550 BC Chinese sage, as the only guide:

I hear and I forget;
I see and I remember;
I do and therefore I understand.

Years passed by quickly. When I was in primary school, I remembered my homework on Chinese class consisted mostly of the so-called *Chao-Xie*, which literally means copying by longhand the assigned text to workbook. This practice, of course, was understandable because the Chinese is character-based, thus the longhand copying enhanced memorization of the number of strokes, whereas in schools of alphabetic language such practice is unknown of. I knew it was tedious, laborious and time-consuming, but it was effective beyond any measurement. That was my first encounter with learning-by-doing.

Years later I found out interestingly that the Cistercian monastery there required its Trappist monks to copy Bible daily in longhand – word by word, page by page, supposedly to internalize the godly words deep into their mind and soul. Therefore even in my early age, I was an unapologetic believer in the merit of hand-on learning.

Moving fast forward to my years of high school math teacher in the US. In a workshop I attended, I was vindicated learning that the ancient proverb is affirmed not only by a few separate, incidental and anecdotal evidences as above, but has since become the subject of many modern studies, the most notable being the Cone of Experience developed by an American educationist Edgar Dale (1900 – 1987) while he was professor of education at the Ohio State University. At its simplest description, the research found that students tend to remember only about 10% to 20% of what they hear and see as depicted at the narrowing tip of the cone, versus about 90% of what they do hands-on, as depicted at the wider bottom of the cone.

Moving fast forward again to this present tense as math graduate student at UT-RGV, I am very excited to know that this ancient 2,500-year old proverb is not only still resonating well but has surfaced in so many situations and forms. First and foremost, of course, is the legend of Srinivasa Ramanujan (1887 – 1920.) Because he is so central in this writing, his brief biography sketch is in order here.

Ramanujan was an Indian mathematician who, with almost no formal schooling in mathematics, made extraordinary contributions to mathematical analysis, number theory, infinite series, etc. He initially did his research in isolation, but eventually went to England and forged a historical partnership with the mathematician G. H. Hardy there. Plagued by health problems throughout his life and obsessively involved with his works, Ramanujan's health deteriorated. He returned to India and died soon thereafter at the age of 32 in 1920. During his short life, he independently compiled nearly 3,900 identities and equations, nearly all his claims have now been proven correct.

It's said that Ramanujan taught himself pure mathematics not by formalism, but by systematically working through 6,000s problems of George S. Carr's *Synopsis of Elementary Results in Pure and Applied Mathematics*, and derived much of his intuition from the patterns he observed from those computations. (The book is actually not a problem book, it's an exam-prep book for taking Cambridge Tripos. Ramanjuan made it famous by using it as problem book.) In a lighter case, I can relate also to Freeman Dyson, the American mathematician and theoretical physicist, who spent his long summer months of his youth working through hundreds and hundreds of problems in differential equations, to eventually become a master in the field.

In another front, I am gratified to learn that the Confusius proverb is the favorite quote of Robert L. Moore (1882 – 1974), the Texas-born topologist who pioneered the famous Moore method of teaching higher math. In its most basic form, the Moore method is a hand-on way of learning higher math that he discovered while teaching the subject at the University of Pennsylvania in 1911.

And traditional longhand learning even excels digital. There was a research in 2014 as reported by this article: *The Pen Is Mightier Than the Keyboard: Advantages of Longhand Over Laptop Note-Taking*, written by Princeton researcher Pam Mueller and Daniel Oppenheimer of UCLA. Their studies followed the note-taking habits of Princeton students and tested the knowledge retention of those pupils who used a laptop to take notes against those who wrote longhand. Here is their result: Note-takers who used laptops created nearly verbatim records of the lectures in the study, but scored lower on tests of retention than those who wrote their notes longhand, even when the test was given one week later.

Finally, here are these trivia: Googling the search word “I hear and I forget” gets 210,000,000 hits; “*ich hore und ich vergesse*” in German gets 169,000; “*Oigo y olvido*” in Spanish gets 392,000; “*Je entends et je l’oublie*” in French gets 16,400,000; “*Ik hoor en ik vergeet*” in Dutch gets 559,000, etc. Unfortunately I do not have the keyboards to search in Chinese – the native language of the ancient sage.

While I am unquestionably a firm believer of the learning-by-doing, but I am fully aware that this learning style is not the only one. Without being judgmental, there is at least one style that is diametrically opposite of my style. It is the so-called Bourbaki formalism, named after Nicolas Bourbaki, which is the collective pseudonym for a group of mainly French 20th-century mathematicians, characterized by their stringent adherence to the sequence of definition –

theorem – proof writing, providing very few if any examples. Everything is presented as general as possible without any diagram or geometric illustration, with little narration on motivation.

When reading Dr. Zieschang's class notes, I realized that they are mostly leaning toward Bourbaki styles, hence my desire to complement them with exercises so that they are adaptable also to students who are conversant in learning-by-doing. It would be a waste of resource if these elegant class notes are fruitful only to learners of Bourbaki style.

In composing the exercises, I followed these four patterns. First, I provide background to what the chapter is about. For example, on chapter about Commutative Ring with unity, I provided questions about which rings form Commutative Ring with unity and which do not, thus giving students backdrops to understand the materials further. Secondly, I looked for small components of proof that Dr. Zieschang omitted because they are too simple to be discussed in the note. For instance, where the notes state that "... it is obvious that T is also a R-module..., " or that "... it is easy to see that R is a noetherian ring..." etc., then I will pick them up and compose them as end-of-section exercises.

Thirdly, I provided instantiation of an abstract math concept, in that I provide a real and concrete instance of an abstraction. For example, students may have difficulties internalize the concept of a field, but can easily visualize it by giving ring of rational numbers as an example. Finally, I composed exercises incorporating the theorems or lemmas in the note. Of these four methods, this fourth one is the hardest since theorems in abstract algebra are not as straightforward as in lower math.

It has been my sincere hope that these exercises are useful to future students in understanding the materials, and instrumental in appreciating the beauty of abstract algebra. It is also hoped that this problem set is suitable for independent study. If even only one single student benefits from my endeavor, I will feel amply rewarded. Finally, I would like to conclude this preface by once again thanking Dr. Zieschang for allowing me this opportunity. Any error or omission in the problem sets, however, should always be attributed to me.

CHAPTER II

HIGHER ALGEBRA

2.1 Basic Facts on Commutative Rings with 1

Problem 2.1.1

Find out if each of the following rings is commutative ring with unity by analyzing each in terms multiplicative identity, commutativity and multiplicative inverse:

(a) $(\mathbb{Z}, +, \times)$, (b) $(2\mathbb{Z}, +, \times)$, (c) $(\mathbb{Q}, +, \times)$, (d) $(\mathbb{R}, +, \times)$, (e) $(\mathbb{Z}_5, +, \times)$ and (f) $(\mathbb{Z}_6, +, \times)$.

Solution: (a) For $(\mathbb{Z}, +, \times)$, we have:

Identity: Yes; $1 \in \mathbb{Z}$.

Commutativity: Yes; $\forall a, b \in \mathbb{Z}, ab = ba.$

Zero divisor: None; $ab = 0$ implies $a = 0$ or $b = 0$.

Multiplicative inverse: None; $\forall a \in \mathbb{Z} \setminus \{1, -1\}, a \in \mathbb{Z}$ but $\frac{1}{a} \notin \mathbb{Z}$.

Conclusion: $(\mathbb{Z}, +, \times)$ is commutative ring with 1. (Analyzing even further down, we find that it is an integral domain but not a field.)

(b) For $(2\mathbb{Z}, +, \times)$, we have:

Identity: None; $1 \notin 2\mathbb{Z}$.

Commutativity: Yes.

Zero divisor: None.

Multiplicative inverse: None.

Conclusion: $(2\mathbb{Z}, +, \times)$ is commutative ring but without unity.

(c) For $(\mathbb{Q}, +, \times)$, we have:

Identity: Yes; $1 \in \mathbb{Q}$.

Commutativity: Yes.

Zero divisor: None.

Multiplicative inverse: Yes; $\forall\ \frac{p}{q} \in \mathbb{Q}$, $\frac{p}{q} \neq 0$, there exists $\frac{q}{p} \in \mathbb{Q}$.

Conclusion: $(\mathbb{Q}, +, \times)$ is commutative ring with 1. (Analyzing even further, we find that it is an integral domain and it is a field.)

(d) For $(\mathbb{R}, +, \times)$, we have:

Identity: Yes; $1 \in \mathbb{R}$.

Commutativity: Yes.

Zero divisor: None.

Multiplicative inverse: Yes.

Conclusion: $(\mathbb{R}, +, \times)$ is commutative ring with 1. (Analyzing even further, it is an integral domain and it is a field.)

(e) For $(\mathbb{Z}_6, +, \times)$, we have:

Identity: Yes; $[1] \in \mathbb{Z}_6$.

Commutativity: Yes; [a][b] = [ab] = [ba] = [b][a].

Zero divisor: Yes; [2][3] = [6] = [0].

Multiplicative inverse: None.

Conclusion: $(\mathbb{Z}_6, +, \times)$ is commutative ring with 1.

(f) For $(\mathbb{Z}_5, +, \times)$, we have:

Identity: Yes; $[1] \in \mathbb{Z}_5$.

Commutativity: Yes.

Zero divisor: None.

Multiplicative inverse: Yes; $[1][1] = [1], [2][3] = [1], [3][2] = [1]$, etc.

Conclusion: $(\mathbb{Z}_5, +, \times)$ is commutative ring with 1. (Analyzing even further down, we find that it is an integral domain and a field.)

■

Problem 2.1.2

Show that the set of the following form:

$$I = \{ \begin{pmatrix} a & a \\ b & b \end{pmatrix} \mid a, b \in \mathbb{R} \}$$

is not an ideal of the ring $M_{2\times2}(\mathbb{R})$.

Solution: Consider an arbitrary

$$A = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \in M_{2\times2}(\mathbb{R}).$$

The product

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} a & a \\ b & b \end{pmatrix} = \begin{pmatrix} xa + yb & xa + yb \\ zb + wb & za + wb \end{pmatrix} \in M_{2\times2}(\mathbb{R}),$$

but

$$\begin{pmatrix} a & a \\ b & b \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} ax + az & ay + aw \\ bx + bz & by + bw \end{pmatrix} \notin M_{2\times2}(\mathbb{R}).$$

Therefore I is only a left ideal of M but not an ideal of M.

$\blacksquare$

Problem 2.1.3

Show that the following subset

$$I = \{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \mid b \in \mathbb{Z} \}$$

of a non-commutative ring

$$S = \{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{Z} \}$$

is an ideal of S.

Solution: I is clearly closed under addition since

$$\begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & y \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & x+y \\ 0 & 0 \end{pmatrix}.$$

I contains an additive inverse of each of its element since

$$-\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -b \\ 0 & 0 \end{pmatrix}.$$

Finally for an arbitrary element $\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \in S$, we have

$$\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} 0 & bz \\ 0 & 0 \end{pmatrix} \in I$$

and

$$\begin{pmatrix} x & y \\ 0 & z \end{pmatrix}\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & xb \\ 0 & 0 \end{pmatrix} \in I.$$

Thus I is an ideal of S.

■

Problem 2.1.4

Let R be a commutative ring with 1. Show that every maximal ideal is a prime ideal.

Solution: Let M be a maximal ideal of R with $xy \in M$, we need to show that either $x \in M$ or $y \in M$. Suppose that $x \in M$, then we are done. Suppose, on the other hand, that $x \notin M$. Let $A = \{ax + b \mid a \in R, b \in M\}$, then A is an ideal and $M \subsetneq A$. But maximality of M dictates that $A = R$. Thus $1_R \in A$, then $1_R = ax + b$ for some $a \in R$ and $b \in M$. From $1_R = ax + b$ and

$y \in R$, we have

$$\begin{aligned} y &= yax + yb \\ &= axy + yb. \end{aligned}$$

We know that $b \in M$, and by definition of ideal therefore $yb \in M$ and also $axy \in M$. Hence $(axy + yb) \in M$, and thus $y \in M$, as desired.

■

Problem 2.1.5

Find out all the prime and maximal ideals in $\mathbb{Z}_8, \mathbb{Z}_9$ and $\mathbb{Z}_{10}$.

Solution: (a) First, for $\mathbb{Z}_8$: We know that the ideals in $\mathbb{Z}_n$ are all principal ideals and if $\mathbb{J} = (j)$ is such an ideal, with $j \in Z^+$, then $j \mid n$. The positive divisors of 8 are 1, 2, 4 and 8, so the principal ideal generators in $\mathbb{Z}_8$ are

$$\begin{aligned} &(1) = \{0,1,2,3,4,5,6,7\} = \mathbb{Z}_8, \\ &(2) = \{0,2,4,6\}, \\ &(4) = \{0,4\} \\ &(8) = \{0\}. \end{aligned}$$

Of these, by inspection, (2) is maximal and therefore prime, whereas (1) and (8) are trivial, so they are neither prime nor maximal. Also notice that $(4) \subset (2)$ therefore (4) is not maximal. Additionally, since $2(2) \in (4)$ but 2 $\notin (4)$, therefore (4) is not prime.

(b) Secondly for $\mathbb{Z}_9$: The positive divisors of 9 are 1, 3, 9, so the principal ideal generators in $\mathbb{Z}_9$ are

$$\begin{aligned} &(1) = \{0,1,2,3,4,5,6,7,8\} = \mathbb{Z}_9, \\ &(3) = \{0,3,9\}, \\ &(9) = \{0\}. \end{aligned}$$

Of these, by inspection, (3) is maximal and therefore prime, whereas (1) and (9) are trivial thus they are neither prime or maximal.

(c) Finally for $\mathbb{Z}_{10}$: The positive divisors of 10 are 1, 2, 5 and 10, so the principal ideal generators in $\mathbb{Z}_{10}$ are these followings:

$$\begin{aligned}
(1) &= \{0,1,2,3,4,5,6,7,8,9\} = \mathbb{Z}_{10},\\
(2) &= \{0,2,4,6,8\},\\
(5) &= \{0,5\}\\
(10) &= \{0\}.
\end{aligned}$$

Of these, by inspection (2) and (5) are maximal and therefore prime, whereas (1) and (10) are trivial therefore they are neither prime nor maximal.

■

2.2 Modules

Problem 2.2.1

Complex product plays an important role not only in this section, but also throughout commutative algebra. *Complex product* is defined in the class note as follow:

> Let P and Q be non-empty subsets of R, a commutative ring with 1. Define PQ to be the set of all elements
>
> $$p_1q_1 + \ldots + p_nq_n$$
>
> with $p_1, \ldots, p_n \in P$ and $q_1, \ldots, q_n \in Q$. Then the set PQ is called the *complex product* of P and Q.

Consider $R = \mathbb{R}_6 = \{0, 1, 2, 3, 4, 5\}$, the classic example of commutative ring with 1, with $R \supset P = \{4, 5\}$ and $R \supset Q = \{0, 1, 2\}$. Compute and show that $PQ = \mathbb{Z}/\mathbb{Z}_6$.

Solution: First we need to consider all pairwise products of elements of P and Q:

$$\{4, 5\}\{0, 1, 2\} = \{4 \cdot 0, 4 \cdot 1, 4 \cdot 2, 5 \cdot 0, 5 \cdot 1, 5 \cdot 2\} = \{0, 2, 4, 5\}$$

Next, we need to consider all possible sums of a finite number of these products:

(a) One-term sums:

$$\{0, 2, 4, 5\}$$

(b) Two-term sums:

$$\{0 + 2, 0 + 4, 0 + 5, 2 + 0, 2 + 4, 2 + 5, 4 + 0, 4 + 2, 4 + 5, 5 + 0, 4 + 2, 4 + 5, \}$$
$$= \{0, 1, 2, 3, 4, 5\}$$

(c) Three-term sums and four-term sums: Since the set of two-term sums has all elements of R, therefore the three- and four-term sums are no longer relevant.

Hence $PQ = \{0, 1, 2, 3, 4, 5\} = \mathbb{Z}/6\mathbb{Z}$.

■

Problem 2.2.2

Complete the proof on Dr. Zieschang's Lemma 2.2 by proving the second step of containment, i.e., $L(PQ) \subseteq (LP)Q$.

Solution: Let m be an element in $L(PQ)$. Then we find a positive integer n, elements $m_1, \ldots, m_n$ in PQ and elements $l_1, \ldots, l_n$ in L such that

$$m = l_1 m_1 + \ldots + l_n m_n.$$

For each element $i \in \{1, \ldots, n\}$, we find a positive integer k_i, elements $p_1, \ldots, p_{k_i}$ in P and elements $q_1, \ldots, q_{k_i}$ in Q such that

$$m_i = p_1 q_1, \ldots, p_{k_i} q_{k_1}.$$

Thus

$$\begin{aligned} m &= l_1(p_1 q_1, \ldots, p_{k_i} q_{k_i}) + \ldots + l_n(p_1 q_1, \ldots, p_{k_n} q_{k_n}) \\ &= [l_1(p_1 q_1) + \ldots + l_1(p_{k_1} q_{k_1})] + \ldots + [l_n(p_1 q_1) + \ldots + l_n(p_{k_n} q_{k_n})] \\ &= [(l_1 p_1) q_1 + \ldots + (l_1 p_{k_i}) q_{k_i}] + \ldots + [(l_n p_1) q_1 + \ldots + (l_n p_{k_n}) q_{k_n}] \\ &\in (LP)Q. \end{aligned}$$

Since $m \in L(PQ)$ implies $m \in (LP)Q$, therefore $L(PQ) \subseteq (LP)Q$ as desired.

$\blacksquare$

Problem 2.2.3

Let M be an R-module. A subgroup L of the additive group M is called *submodule* of M if, for any two elements $l \in L$ and $r \in R$, $lr \in L$. Prove that $\{0\}$ and M are submodules of M.

Solution: Let $r \in R$ and $0 \in \{0\}$. Since $0r = 0 \in \{0\}$, therefore $\{0\}$ is submodule of M. Next, let's fix $r \in R$ and $m \in M$. Since $lm \in M$ by definition of module M, therefore M is submodule of M.

$\blacksquare$

Problem 2.2.4

If R is any ring, and $n \in \mathbb{N}$. Prove that the following Cartesian product defined as $\mathbb{R}^n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in R\}$ is a right R-module, based on the following operations for $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in R^n$, and $r \in R$:

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$$

$$(a_1, \ldots, a_n)r = (a_1 r, \ldots, a_n r).$$

Solution: We need to satisfy all of the four conditions of module as stated in the class note.

(a) Here is the first condition: For $s, t \in R$,

$$\begin{aligned}(a_1, \ldots, a_n)(st) &= (a_1 st, \ldots, a_n st)\\ &= (a_1 s, \ldots, a_n s)(t).\end{aligned}$$

(b) Next, the second condition:

$$\begin{aligned}(a_1, \ldots, a_n)(s+t) &= (a_1(s+t), \ldots, a_n(s+t))\\ &= ((a_1 s + a_1 t), \ldots, (a_n s + a_n t))\\ &= (a_1 s + \ldots + a_n s) + (a_1 t + \ldots + a_n t)\\ &= (a_1, \ldots, a_n)s + (a_1, \ldots, a_n)t.\end{aligned}$$

(c) The third condition:

$$[(a_1, \ldots, a_n) + (b_1, \ldots, b_n)]r = (a_1, \ldots, a_n)r + (b_1, \ldots, b_n)r.$$

(d) Finally for the fourth condition: For $1 \in R$,

$$(a_1, \ldots, a_n)1 = (a_1, \ldots, a_n).$$

■

Problem 2.2.5

Let $C[0,1]$ be an additive group of continuous $\mathbb{R}$-valued functions defined on the interval $[0,1]$, and define its operations by:

$$(f+g)(x) = f(x) + g(x), \text{ for } f, g \in C[0,1]$$
$$(kf)(x) = kf(x), \text{ for } k \in \mathbb{R}.$$

By recalling from calculus that the sum of continuous functions is again a continuous function, prove that $C[0,1]$ is an $\mathbb{R}$-module.

Solution: Similar to the above problem, here we need to satisfy the four conditions of module as stated in the class note. Let $f, g \in C[0,1]$ and $r, s \in \mathbb{R}$.

(a) For the first condition:

$$\begin{aligned} f(x) \cdot rs &= r \cdot f(x) \cdot s \\ &= (rf)(x) \cdot s. \end{aligned}$$

(b) Next, the second condition:

$$\begin{aligned} f(x)(r+s) &= r \cdot f(x) + s \cdot f(x) \\ &= (rf)(x) + (sf)(x). \end{aligned}$$

(c) The third condition:

$$\begin{aligned} (f(x)+g(x))r &= r \cdot f(x) + r \cdot g(x) \\ &= (rf)(x) + (rg)(x). \end{aligned}$$

(d) Finally, the fourth condition:

$$f(x) \cdot 1 = f(x).$$

■

2.3 The Field of Fractions of an Integral Domain

Problem 2.3.1

In Dr. Zieschang's note, $[s, t]$ is defined as the equivalence class containing (s, t). Find $[2, 3] \in \mathbb{Z}_{11} \times (\mathbb{Z}_{11} \setminus \{0\})$.

Solution: We note that $\mathbb{Z}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ is an integral domain since there is no zero divisor. Here we have

$$[2, 3] = \{(a, b) \in \mathbb{Z}_{11} \times (\mathbb{Z}_{11} \setminus \{0\}) \mid 2b = 3a\},$$

$$\begin{aligned} 2b &= 3a \\ b &= \frac{3}{2}a. \end{aligned}$$

And by inspection, for $a \in \{2, 4, 6, 8, 10\}$ we have

$$\begin{aligned} b &\in \{3, 6, 9, 12, 15\} \\ &= \{3, 6, 9, 1, 4\}. \end{aligned}$$

Hence we have

$$[2, 3] = \{(2, 3), (4, 6), (6, 9), (8, 1), (10, 4), (1, 7), (3, 10), (5, 2), (7, 5), (9, 8)\}.$$

Verifying:

$$\begin{aligned} (2, 3) \sim (2, 3) &\iff 2 \cdot 3 = 2 \cdot 3 \\ (2, 3) \sim (4, 6) &\iff 2 \cdot 6 = 4 \cdot 3, 12 = 12, 1 = 1 \\ (2, 3) \sim (6, 9) &\iff 2 \cdot 9 = 6 \cdot 3, 18 = 18, 7 = 7 \\ (2, 3) \sim (8, 1) &\iff 2 \cdot 1 = 8 \cdot 3, 2 = 24, 2 = 2 \\ (2, 3) \sim (10, 4) &\iff 2 \cdot 4 = 10 \cdot 3, 8 = 30, 8 = 8 \end{aligned}$$

■

Problem 2.3.2

In the class note, $F(R)$ is defined as the set of all equivalence class of $\sim$, with R an integral domain. Find $F(\mathbb{Z}_3)$, where $\mathbb{Z}_3$ an integral domain.

Solution: Notice that $\mathbb{Z}_3 = \{0, 1, 2\}$. Let's fix $[s, t] \in \mathbb{Z}_3 \times (\mathbb{Z}_3 \setminus \{0\})$, then by preliminary observation, we have

$$F(\mathbb{Z}_3) = \{[0, 1], [1, 1], [1, 2]\}.$$

Each equivalence class has the following elements:

$[0, 1] = \{(0, 1), (0, 2)\}$. Verifying: $0 \cdot 1 = 0 \cdot 1;\ 0 \cdot 2 = 0 \cdot 1.$

$[1, 1] = \{(1, 1), (2, 2)\}$. Verifying: $1 \cdot 1 = 1 \cdot 1;\ 1 \cdot 2 = 2 \cdot 1.$

$[1, 2] = \{(1, 2), (2, 1)\}$. Verifying: $1 \cdot 2 = 1 \cdot 2;\ 1 \cdot 1 = 2 \cdot 2.$

■

Problem 2.3.3

Dr. Zieschang's note defines the operations on the equivalence classes $F(R)$, with R is an integral domain, as:

$$[s, t] + [u, v] := [sv + tu, tv]$$

$$[s, t][u, v] := [su, tv],$$

where $[s, t], [u, v] \in R \times R \setminus \{0\}$. They are called *fractional addition* and *fractional multiplication* respectively. Prove that these two opertions are well-defined.

Solution: (a) In proving that the fractional addition is well-defined, we need to prove that $+$ is unambiguous:

$$[s, t] = [a, b], [u, v] = [c, d] \Rightarrow [sv + tu, tv] = [ad + bc, bd],$$

where $[s, t]$, $[u, v]$, $[a, b]$ and $[c, d]$ are arbitrary elements of $R \times R \setminus \{0\}$.

We notice that

$$[s, t] = [a, b] \to (s, t) \sim (a, b)$$

$$\to sb = ta,$$

and also

$$\begin{aligned}[u,v]=[c,d]&\rightarrow (u,v)\sim(c,d)\\ &\rightarrow ud=vc.\end{aligned}$$

We observe that

$$\begin{aligned}(sv+tu)bd&=svbd+tubd\\ &=sbvd+udtb\\ &=tavd+vctb\\ &=(ad+bc)tv,\end{aligned}$$

implying that

$$\begin{aligned}(sv+tu,tv)&\sim(ad+bc,bd)\\ [sv+tu,tv]&=[ad+bc,bd],\end{aligned}$$

which further implying that the additive operation + is well-defined, as desired.

(b) In proving that the multiplicative operation $\cdot$ is well-defined, we need to show that $\cdot$ is unambiguous:

$$[s,t]=[a,b],[u,v]=[c,d]\Rightarrow[sv,tv]=[ac,bd],$$

where as in the above, $[s,t]$, $[u,v]$, $[a,b]$ and $[c,d]$ are arbitrary elements of $R\times R\setminus\{0\}$. From the above, we have shown that

$$\begin{aligned}sb&=ta\\ ud&=vc.\end{aligned}$$

We observe that

$$\begin{aligned}(su)bd&=sbud\\ &=tavc\\ &=(tv)ac,\end{aligned}$$

implying that

$$(su, tv) \sim (ac, bd)$$

$$[su, tv] = [ac, bd],$$

which further implying that the multiplication operation $\cdot$ is well-defined, as desired.

$\blacksquare$

Problem 2.3.4

Prove that $F(R)$ is commutative ring with unity.

Solution: (a) First, consider $[a, b], [c, d], [e, f] \in F(R)$ where $b, d, f \neq 0$. Here $F(R)$ is $+$ associative:

$$\begin{aligned}([a, b] + [c, d]) + [e, f] &= [ad + bc, bd] + [e, f] \\ &= [(ad + bc)f + (bd)e, (bd)f] \\ &= [a(df) + b(cf + de), b(bf)] \\ &= [a, b] + [cf + de, df] \\ &= [a, b] + ([c, d] + [e, f]).\end{aligned}$$

(b) Secondly, $F(R)$ is $\cdot$ associative:

$$\begin{aligned}([a, b][c, d])[e, f] &= ([ac, bd])[e, f] \\ &= [ace, bdf] \\ &= [a(ce), b(bf)] \\ &= [a, b]([ce, df]) \\ &= [a, b]([c, d][e, f]).\end{aligned}$$

(c) Thirdly, $F(R)$ is $+$ commutative:

$$\begin{aligned}[a, b] + [c, d] &= [ad + bc, bd] \\ &= [cb + da, db] \\ &= [c, d] + [a, b].\end{aligned}$$

(d) $F(R)$ is $\cdot$ commutative:

$$\begin{aligned}[a,b][c,d] &= [ac,bd] \\ &= [ca,db] \\ &= [c,d][a,b].\end{aligned}$$

(e) $F(R)$ is closed in $+$:

$$[a,b]+[c,d]=[ad+bc,bd].$$

Since $b,d \neq 0$ and R does not have zero divisor, therefore $bd \neq 0$ and hence

$$[ad+bc,bd] \in F(R).$$

(f) $F(R)$ is closed in $+$:

$$[a,b][c,d]=[ac,bd].$$

Since $bd \neq 0$ therefore

$$[ac,bd] \in F(R).$$

(g) And distributivity law holds in $F(R)$:

$$\begin{aligned}[a,b]([c,d]+[e,f]) &= [a,b][cf+de,df] \\ &= [a(cf+de),b(df)] \\ &= [acf+ade,bdf] \\ &= [bacf+bade,bbdf] \\ &= [acbf+bdae,bdbf] \\ &= [ac,bd]+[ae,bf] \\ &= [a,b][c,d]+[a,b][e,f].\end{aligned}$$

(h) Next, $F(R)$ has $+$ neutral element $[0,1]$:

$$
\begin{aligned}
[a,b]+[0,1] &= [a\cdot 1 + b\cdot 0, b\cdot 1] \\
&= [a,b]
\end{aligned}
$$

(i) Finally, $\forall [a,b] \in F(R)$, $[a,b]$ has $+$ inverse $[-a,b]$:

$$
\begin{aligned}
[a,b]+[-a,b] &= [ab-ab, bb] \\
&= [0,b^2] \\
&= [0,1]
\end{aligned}
$$

■

Problem 2.3.5

Show that $F(R)$ is a field.

Solution: (a) Frist, we note that $F(R)$ has multiplicative neutral element $[1,1]$:

$$
\begin{aligned}
[a,b][1,1] &= [a\cdot 1, b\cdot 1] \\
&= [a,b].
\end{aligned}
$$

(b) Here $\forall a,b \in R\setminus\{0\}$, $[b,a]$ is a multiplicative inverse of $[a,b]$ since

$$
\begin{aligned}
[a,b][b,a] &= [ab,ab] \\
&= [1,1].
\end{aligned}
$$

■

2.4 Integrality

Problem 2.4.1

Show that the *Gaussian* integers, $\mathbb{Z}[i]$, is integral over $\mathbb{Z}$. Show also the same for $\mathbb{Z}[\sqrt{2}]$.

Solution : (a) For $\mathbb{Z}[i]$: For all $(a+bi) \in \mathbb{Z}[i]$, there exists a *monic* polynomial

$$P(x) = x^2 - 2ax + (a^2 + b^2),$$

where $2a$ is the so-called the trace of $a+bi$ and a^2+b^2 is the so-called norm of $a+bi$, such that

$$\begin{aligned} P(a+bi) &= (a+bi)^2 - 2a(a+bi) + (a^2+b^2) \\ &= a^2 + 2abi - b^2 - 2a^2 - 2abi + a^2 + b^2 \\ &= 0. \end{aligned}$$

Hence $\mathbb{Z}[i]$ is integral over $\mathbb{Z}$.

(b) Next, for $\mathbb{Z}[\sqrt{2}]$: For all $(a+b\sqrt{2}) \in \mathbb{Z}[\sqrt{2}]$, a slightly modified *monic* polynomial as in (a) above has $a+b\sqrt{2}$ as its root:

$$P(x) = x^2 - 2ax + (a^2 - 2b^2),$$

where $2a$ is the so-called the trace of $a+b\sqrt{2}$ and a^2+b^2 is the so-called norm of $a+b\sqrt{2}$, that is,

$$\begin{aligned} P(a+bi) &= (a+b\sqrt{2})^2 - 2a(a+b\sqrt{2}) + (a^2-2b^2) \\ &= a^2 + 2ab\sqrt{2} + 2b^2 - 2a^2 - 2ab\sqrt{2} + a^2 - 2b^2 \\ &= 0. \end{aligned}$$

Hence $\mathbb{Z}[\sqrt{2}]$ is integral over $\mathbb{Z}$.

$\blacksquare$

Problem 2.4.2

Prove the assertion found in Dr. Zieschang's class note:

$$S \subseteq I_R(S) \subseteq R,$$

where $I_R(S)$ is defined as the set of all elements in R which are integral over $S \subseteq R$, with R being a commutative ring with unity.

Solution : For $\forall a \in S$, there exists a *monic* polynomial

$$P_a(x) = x - a,$$

such that

$$P_a(a) = a - a = 0.$$

Therefore for all $a \in S$, a is the root of a *monic* polynomial $P_a(x)$, thus $a \in I_R(S)$. Hence $S \subseteq I_R(S)$. Since $I_R(S)$ is defined as set of all elements in R which are integral over S, therefore $I_R(S) \subseteq R$.

By combining the results from above, therefore we have $S \subseteq I_R(S) \subseteq R$, as desired.

■

Problem 2.4.3

Prove the assertion found in Dr. Zieschang's note:

$$I_R(S) \subseteq I_R(T),$$

where S and T are subrings of a commutative ring with unity R, and $S \subset T$.

Solution : Here we have $S \subseteq T$, therefore

$$\forall a \in S \Rightarrow a \in T.$$

For $I_R(S)$, from Exercise 4.2 above we have

$$S \subseteq I_R(S) \subseteq R,$$

hence

$$\forall a \in S \Rightarrow a \in I_R(S).$$

For $I_R(T)$, from the same Exercise 4.3 above, we have

$$T \subseteq I_R(T) \subseteq R,$$

hence

$$\forall a \in T \Rightarrow a \in I_R(T).$$

Therefore, by combining all of the above, we finally have the following, as desired.

$$\forall a \in I_R(S) \Rightarrow a \in I_R(T)$$

$$I_R(S) \subseteq I_R(T).$$

■

2.5 Integrality and Fields

Problem 2.5.1

Show that integral domain $\mathbb{Z}$ is integrally closed in the rational field $\mathbb{Q}$.

Solution: According to Dr. Zieschang's note, for each subring $S \subseteq R$, where R is a commutative ring with unity, $I_R(S)$ is defined to be the set of all elements of R which are integral over S, thus,

$$S \subseteq I_R(S) \subseteq R.$$

If $S = I_R(S)$, S is said to be *integrally closed* in R.

Consider

$$I_{\mathbb{Q}}(\mathbb{Z}) = \{\frac{a}{b} \mid a \in \mathbb{Z}, b = 1\}.$$

Obviously $I_{\mathbb{Q}}(\mathbb{Z})$ consists of all elements of $\mathbb{Q}$ which are integral over $\mathbb{Z}$. For every $x \in I_{\mathbb{Q}}(\mathbb{Z})$, there exists polynomial $P(x)$ with coefficient in $\mathbb{Z}$, such that

$$P(x) = x - a = 0.$$

Hence

$$\mathbb{Z} \subseteq I_{\mathbb{Q}}(\mathbb{Z}) \subseteq \mathbb{Q}.$$

Now, consider $c \in I_{\mathbb{Q}}(\mathbb{Z})$. Since $I_{\mathbb{Q}}(\mathbb{Z})$ is the set of elements of $\mathbb{Q}$ which are integral over $\mathbb{Z}$, therefore $P(c) = c - a = 0$, consequently $c = a$, implying that c is an element of $\mathbb{Z}$. Thus
$\forall c \in I_{\mathbb{Q}}(\mathbb{Z})$ we have $c \in \mathbb{Z}$, hence $I_{\mathbb{Q}}(\mathbb{Z}) \subseteq \mathbb{Z}$.
Since $I_{\mathbb{Q}}(\mathbb{Z}) \subseteq \mathbb{Z}$ and $\mathbb{Z} \subseteq I_{\mathbb{Q}}\mathbb{Z}$, therefore $I_{\mathbb{Q}}(\mathbb{Z}) = \mathbb{Z}$. Hence $\mathbb{Z}$ is integrally closed in the field $\mathbb{Q}$, as desired.

■

Problem 2.5.2

Show that $\mathbb{Z}[\sqrt{5}]$ is *not* integrally closed in $\mathbb{Q}[\sqrt{5}]$.

Solution: Again from Dr. Zieschang's class note, we learned that for each subring $S \subseteq R$, where

R is commutative ring with unity, $I_R(S)$ is defined to be the set of all elements in R which are integral over S. Thus we have

$$S \subseteq I_R(S) \subseteq R.$$

If $S = I_R(S)$, then S is said to be *integrally closed* in R.

Here we are going to prove by counterexample: We know that $q = \frac{1}{2} + \frac{1}{2}\sqrt{5} \in \mathbb{Q}[\sqrt{5}]$ is integral over $\mathbb{Z}$ because $\mathbb{Z}[\sqrt{5}] \subset \mathbb{Q}[\sqrt{5}]$, and there exists a *monic* polynomial with coefficient from $\mathbb{Z}[\sqrt{5}]$,

$$P(x) = x^2 - x - 1$$

such that q is its root:

$$\begin{aligned} P(x) &= (\frac{1}{2} + \frac{1}{2}\sqrt{5})^2 - (\frac{1}{2} + \frac{1}{2}\sqrt{5}) - 1 \\ &= \frac{1}{4} + \frac{2}{4}\sqrt{5} + \frac{5}{4} - \frac{1}{2} + \frac{1}{2}\sqrt{5} - 1 \\ &= 0 \end{aligned}$$

Hence $q \in I_{Q[\sqrt{5}]}(\mathbb{Z}[\sqrt{5}])$ but $q \notin \mathbb{Z}[\sqrt{5}]$, consequently $\mathbb{Z}[\sqrt{5}] \neq I_{Q[\sqrt{5}]}(\mathbb{Z}[\sqrt{5}])$, that is, $\mathbb{Z}[\sqrt{5}]$ is *not* integrally closed in $\mathbb{Q}[\sqrt{5}]$, as desired.

■

Problem 2.5.3

Show that $\mathbb{Z}$ is integrally closed in field $\mathbb{C}$.

Solution: Consider

$$I_{\mathbb{C}}\mathbb{Q} = \{a + bi \mid a \in \mathbb{Z}, b = 0\}.$$

Obviously $I_{\mathbb{C}}(\mathbb{Z})$ consists of all elements of $\mathbb{C}$ which are integral over $\mathbb{Z}$. For every $x \in I_{\mathbb{C}}(\mathbb{Z})$, there exists polynomial $P(x)$ with coefficient in $\mathbb{Z}$, such that

$$P(x) = x - a = 0.$$

Hence

$$\mathbb{Z} \subseteq I_{\mathbb{C}}(\mathbb{Z}) \subseteq \mathbb{C}.$$

Now, consider $c \in I_{\mathbb{C}}(\mathbb{Z})$. Since $I_{\mathbb{C}}(\mathbb{Z})$ is the set of elements of $\mathbb{C}$ which are integral over $\mathbb{Z}$, therefore $P(c) = c - a = 0$, consequently $c = a$, implying that c is an element of $\mathbb{Z}$. Thus $\forall c \in I_{\mathbb{C}}(\mathbb{Z})$ we have $c \in \mathbb{Z}$, hence $I_{\mathbb{C}}(\mathbb{Z}) \subseteq \mathbb{Z}$.

Since $I_{\mathbb{C}}(\mathbb{Z}) \subseteq \mathbb{Z}$ and $\mathbb{Z} \subseteq I_{\mathbb{C}}\mathbb{Z}$, therefore $I_{\mathbb{C}}(\mathbb{Z}) = \mathbb{Z}$. Hence $\mathbb{Z}$ is integrally closed in the field $\mathbb{C}$, as desired.

■

Problem 2.5.4

Dr. Zieschang concludes this chapter by making reference in Lemma 5.8 to UFD, the Unique Factorization Domain. Show that the ring integer $\mathbb{Z}[\sqrt{-6}]$ is *not* a UFD.

Solution: UFD is a commutative ring in which every non-zero, non-unit element is a product of prime (or irreducible) elements, uniquely up to order and unit. This is a generalization to the Fundamental Theorem of Arithmetic.

Here, $\mathbb{Z}[\sqrt{-6}]$ is *not* UFD because we have these followings:

$$(6 + 0 \cdot [\sqrt{-6}]) = (2 + 0 \cdot [\sqrt{-6}])(3 + 0 \cdot [\sqrt{-6}]),$$

and

$$(6 + 0 \cdot [\sqrt{-6}]) = (0 + [\sqrt{-6}])(0 + [\sqrt{-6}])$$

as our counterexamples. But we need to show that $2, 3$ and $[\sqrt{-6}]$ are irreducibles in $\mathbb{Z}[\sqrt{-6}]$. We begin with the first one, which is 2. Suppose to the contrary that 2 is reducible, therefore for some $r, s, t, u \in \mathbb{Z}$:

$$2 = (r + s\sqrt{-6})(t + u\sqrt{-6}),$$

where $(r + s\sqrt{-6})$ and $(t + u\sqrt{-6})$ are not units since the only units are -1 and 1.

Consequently the product of their conjugates is also 2:

$$\begin{aligned} 2 &= (r - s\sqrt{-6})(t - u\sqrt{-6}) \\ 4 &= (r - s\sqrt{-6})(r + s\sqrt{-6})(t - u\sqrt{-6})(t + u\sqrt{-6}) \\ &= (r^2 + 6s^2)(t^2 + 6u^2). \end{aligned}$$

Hence

$$(r^2 + 6s^2) \in \{1, 2, 4\}.$$

(a) From the set $\{1, 2, 4\}$, first we consider

$$(r^2 + 6s^2) = 1,$$

which implies $r = 1$ and $s = 0$, thus forcing 2 to be irreducible.

(b) Secondly we consider

$$(r^2 + 6s^2) = 2,$$

which implies that $r, s \notin \mathbb{Z}$ hence not possible.

(c) Consider finally

$$(r^2 + 6s^2) = 4,$$

which implies that $r = \{-2, 2\}$ and $s = 0$, thus forcing $(t^2 + 6u^2) \in \{-1, 1\}$.

Hence there is no non-trivial factorization of 2 in $\mathbb{Z}[\sqrt{-6}]$.

Using the same steps as above, we can similarly show that 3, $\sqrt{-6}$ are also irreducible in $\mathbb{Z}[\sqrt{-6}]$, as desired.

■

2.6 Prime Ideals

Problem 2.6.1

Show that $\mathbb{Z} \times \{0\}$ is prime ideal of $\mathbb{Z} \times \mathbb{Z}$.

Solution: Recall from Dr. Zieschang's *Algebra I* that an ideal T of a commutative ring with unity R is called a *prime* if the following conditions hold:

(1) $T \neq R$,

(2) If $a, b \in R$ and $ab \in T$, then either $a \in T$ or $b \in T$.

Obviously $\mathbb{Z} \times \mathbb{Z} \neq \mathbb{Z} \times \{0\}$. Suppose that $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}$, and $(a, b)(c, d) \in \mathbb{Z} \times \{0\}$, then $bd = 0 \in \mathbb{Z}$. And then since $\mathbb{Z}$ is an integral domain, hence either

$$b = 0 \longrightarrow (a, b) \in \mathbb{Z} \times \{0\}$$

or

$$d = 0 \longrightarrow (c, d) \in \mathbb{Z} \times \{0\}.$$

Hence $\mathbb{Z} \times \{0\}$ is prime ideal of $\mathbb{Z} \times \mathbb{Z}$.

■

Problem 2.6.2

Consider $\mathbb{E}$ as set of even integers. Show that the ideal $(4) \subset \mathbb{E}$ is not a prime ideal of $\mathbb{E}$, but (10) and (14) are prime ideals of $\mathbb{E}$.

Solution: (a) For (4), we have

$$\begin{aligned}(4) &= \{4z \mid z \in \mathbb{Z}\} \\ &= \{\ldots, -12, -8, -4, 0, 4, 8, 12, \ldots\}\end{aligned}$$

Let's take $2, 6 \in \mathbb{E}$ as counterexamples. Here we have $2 \cdot 6 = 12 \in (4)$ but $2 \in (4)$ and $6 \in (4)$. Hence (4) is not a prime ideal.

(b) For (10), we have

$$\begin{aligned}(10) &= \{10z \mid z \in \mathbb{Z}\} \\ &= \{\ldots, -30, -20, -10, 0, 10, 20, 30, \ldots\}\end{aligned}$$

Suppose that $a, b \in \mathbb{E}$ and that $ab \in (10)$. This implies that $10 \mid ab$, implying further that either $10 \mid a$ or $10 \mid b$. This is because a and b are even integers which effectively exclude 5 that is the generator of 10, hence proving that (10) is a prime ideal, as desired.

(c) And finally for (14), we have

$$\begin{aligned}(14) &= \{14z \mid z \in \mathbb{Z}\} \\ &= \{\ldots, -42, -28, -14, 0, 14, 28, 42, \ldots\}\end{aligned}$$

Suppose that $a, b \in \mathbb{E}$ and that $ab \in (14)$. This implies that $14 \mid ab$, implying further that either $14 \mid a$ or $14 \mid b$. This is because a and b are even integers which effectively exclude 7 that is the generator of 14, hence proving that (14) is a prime ideal, as desired.

■

Problem 2.6.3

Prove Dr. Zieschang's assertion in the note that commutative ring with unity R is an integral domain if and only if $\{0\}$ is prime ideal of R.

Solution: Here we need to prove both ways:

(a) For proving $\Longrightarrow$: Suppose that R is an integer domain, which means that R does not have zero divisor. If $a, b \in R$ and $ab \in \{0\}$, then either $a \in \{0\}$ or $b \in \{0\}$ since R does not have zero divisor.

(b) Next, for proving $\Longleftarrow$: Suppose that $\{0\}$ is prime ideal of R. If $ab \in \{0\}$, then either $a \in \{0\}$ or $b \in \{0\}$, implying that R does not have zero divisor.

■

Problem 2.6.4

Complete Lemma 6.1 in Dr. Zieschang's note by proving (b) ⇒ (c), (d) ⇒ (b) and (b) ⇒ (d).

Solution: From Dr. Zieschang's class note, we have Lemma 6.1 that reads as follow: For each ideal T different from $R,$ the following conditions are equivalent:

(a) The ideal T is a prime ideal of $R.$

(b) For any two ideal U and V of R with $UV \subseteq T$ we have $U \subseteq T$ or $V \subseteq T.$

(c) For any two ideals U and V of R with $T \subseteq U, T \subset V$, and $UV \subseteq T$, we have $U = T$ or $V = T.$

(d) Let $U_1, ..., U_n$ be ideals of R with $U_1 \cdots U_n \subseteq T.$ Then there exists an element i in $\{1, ..., n\}$ such that $U_i \subseteq T.$

(1) Proving (b) ⇒ (c): Given that $U \subseteq T$ in (b) and given that $T \subseteq U$ in (c), we have therefore $U = T$. Given that $V \subseteq T$ in (b) and $T \subseteq V$ in (c), we therefore have $V = T.$

(2) Proving (d) ⇒ (b): Set $n = 2$ for n in (d), then we have $U_1 \cdot U_2 \subseteq T$ and either $U_1 \subseteq T$ or $U_2 \subseteq T.$ All of these translate perfectly to (b).

(3) Proving (b) ⇒ (d): Proof by mathematical induction: Let $P(n)$ be the proposition as stated in the point (d).

(3a) For $n = 2$, $P(2)$ is true: For any two ideal U and V of R with $UV \subseteq T$, we have $U \subseteq T$ or $V \subseteq T.$

(3b) For $n = k$, assume that $P(k)$ is true: For any $U_1, ..., U_k$ ideals of R with $U_1 \cdots U_k \subseteq T.$ Then there exists an element $i \in \{1, ..., k\}$ such that $U_i \subseteq T.$

(3c) We need to prove $P(k + 1)$ for $n = k + 1$ is true. Consider any $U_1, ..., U_k, U_{k+1}$ ideals of R with $U_1 \cdots U_k \cdot U_{k+1} \subseteq T.$ Recall that by assumption $U_1 \cdots U_k \subseteq T$, therefore let $U_1 \cdots U_k = V$, and hence $V \cdot U_{k+1} \subseteq T.$ By $P(2)$ we have $V \subseteq T$ or $U_{k+1} \subseteq T$, and by $P(k)$ we have U_i, an ideal that makes up the V, such that $U_i \subseteq T.$ Hence $P(k + 1)$ is true, as desired.

■

2.7 The Krull Dimension

Problem 2.7.1

Find $\dim(\mathbb{Z}_6)$.

Solution: Recall Lemma 7.3 from Dr. Zieschang's *Algebra I*: Let R be commutative ring with unity and let s be an element of R, then the following statements hold:

(i) If s is a prime element in R, sR is a prime ideal of R.

(ii) Assume that $s \neq 0$ and sR is a prime ideal of R, then s is a prime element.

Here, first of all we need to find the prime elements of $\mathbb{Z}_6$. Again according to *Algebra I*, an element r of a unital commutative ring R is called a *prime* if it meets the following two conditions:

(i) $r \in R \setminus U(R) \setminus \{0\}$, where $U(R)$ is the set of units of R.

(ii) If r divides a product of two elements of $R \setminus \{0\}$, then r divides one of the two factors.

From $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$, we have the units of $\mathbb{Z}_6$, that is $U(\mathbb{Z}_6) = \{1, 5\}$. Consequently we have

$$\mathbb{Z}_6 \setminus U(\mathbb{Z}_6) \setminus \{0\} = \{2, 3, 4\}.$$

Of the above, the element 2 does not meet the condition (ii) because, for instance, we have $2 \mid 2 \cdot 4$, where $2 \cdot 4$ is the product of two elements of $\mathbb{Z}_6$, but we have $2 \mid 2$ *and* at the same time $2 \mid 4$. Accordingly, the prime elements of $\mathbb{Z}_6$ are 3 and 4 only.

We have therefore the prime ideals of $\mathbb{Z}_6$:

$$\begin{aligned} 3\mathbb{Z}_6 &= \{0, 3, 6, 9, 12, 15\} \\ &= \{0, 3\}. \\ 4\mathbb{Z}_6 &= \{0, 4, 8, 12, 16, 20\} \\ &= \{0, 4, 2, 0, 4, 2\} \\ &= \{0, 2, 4\}. \end{aligned}$$

Since $\{0\}$ is the prime ideal of $\mathbb{Z}_6$, and since

$$\{0\} \subsetneq 3\mathbb{Z}_6$$

and also

$$\{0\} \subsetneq 4\mathbb{Z}_6,$$

therefore the order of the non-empty set of chain of prime ideals $\mathcal{S}$, that is $|\mathcal{S}|$, is 2. Then

$$\begin{aligned}\dim(\mathbb{Z}_6) &= |\mathcal{S}| - 1\\ &= 2 - 1\\ &= 1.\end{aligned}$$

■

Problem 2.7.2

Show that $\dim(\mathbb{Z}) = 1, \dim(\mathbb{R}) = 1$ and $\dim(\mathbb{Q}) = 0$.

Solution: (a) Consider p_i, with $i \in \{1, 2, ..., n\}$, as prime numbers of $\mathbb{Z}$. According to Lemma 7.3 again, then $p_i\mathbb{Z}$ are the prime ideals of $\mathbb{Z}$. Since $p_i\mathbb{Z}$ are also the maximal ideals of $\mathbb{Z}$, therefore $\mathbb{Z}$ has only chain set of prime ideals $\mathcal{S}$ of oder 2:

$$\{0\} \subsetneq p_i\mathbb{Z}.$$

Hence,

$$\begin{aligned}\dim(\mathbb{Z}) &= |\mathcal{S}| - 1\\ &= 2 - 1\\ &= 1.\end{aligned}$$

(b) Using similar argument like the above, we can derive

$$\begin{aligned}\dim(\mathbb{R}) &= |\mathcal{S}| - 1\\ &= 2 - 1\\ &= 1.\end{aligned}$$

(c) We know that $\mathbb{Q}$ is a field, and field does not have any prime ideal except $\{0\}$, hence the order of chain set of prime ideals $\mathcal{S}$ is $|\mathcal{S}| = 1$. Therefore

$$\begin{aligned}\dim(\mathbb{Q}) &= |\mathcal{S}| - 1\\ &= 1 - 1\\ &= 0.\end{aligned}$$

■

Problem 2.7.3

Find $\dim(\mathbb{Z}[i])$, the Krull dimension of the *Gaussian* integer.

Solution: We have learned from exercise 4.3 that *Gaussian* integer $\mathbb{Z}[i]$ is integral over $\mathbb{Z}$. At the same time we also learned from section 4 that if S is a subring of R, R being commutative ring with unity, and $I_R(S)$ denotes the set of all elements in R which are integral over S, then

$$S \subseteq I_R(S) \subseteq R.$$

If $I_R(S) = R$, we say that R is *integral over* S.

Hence,

$$\mathbb{Z} \subseteq I_{\mathbb{Z}[i]}(\mathbb{Z}) \subseteq \mathbb{Z}[i],$$

and also

$$I_{\mathbb{Z}[i]}(\mathbb{Z}) = \mathbb{Z}[i].$$

Recall from Lemma 7.9 that if $I_R(S) = R$, then $\dim(S) = \dim(R)$. Consequently

$$\begin{aligned} \dim(\mathbb{Z}[i]) &= \dim(\mathbb{Z}) \\ &= 1. \end{aligned}$$

■

Problem 2.7.4

Show that the polynomial ring over integral domain $\mathbb{Z}[x_1, \ldots, x_n]$ has dimension of n.

Solution: We know that $\mathbb{Z}$ is integral domain, then so is its polynomial ring $\mathbb{Z}[x_1, \ldots, x_n]$.
Proof: Consider $f(x_1, \ldots, x_n)$ and $g(x_1, \ldots, x_n)$ be any two non-zero polynomial in $\mathbb{Z}[x_1, \ldots, x_n]$, and let a_f and a_g be the leading coefficients of the f and g. Thus as $a_f \neq 0$ and $a_g \neq 0$, we have $a_f \cdot a_g \neq 0$. But as $a_f \cdot a_g$ is the leading coefficient of $f \cdot g$, therefore $f \cdot g$ can not be a zero polynomial. Consequently $\mathbb{Z}[x_1, \ldots, x_n]$ has no zero divisor, hence $\mathbb{Z}[x_1, \ldots, x_n]$ is an integral domain.
Having proven the above, we then call from Lemma 7.1 of Dr. Zieschang's *Algebra I*, that if T is an ideal of R and $T \neq R$, then the ideal T is prime if and only if R/T is an integral domain.
$\mathbb{Z}[x_1, \ldots, x_n]$ is an integral domain, and so are (x_1), the subset of $\mathbb{Z}[x_1, \ldots, x_n]$, and $\mathbb{Z}[x_1, \ldots, x_n]/(x_1)$. Hence by Lemma 7.1, (x_1) is a prime ideal.
By similar argument, we can prove that $(x_1, x_2), (x_1, x_2, x_3), \ldots, (x_1, \ldots, x_n)$ are all prime ideals of $\mathbb{Z}[x_1, \ldots, x_n]$. Since $0 \subsetneq (x_1) \subsetneq (x_1, x_2), \ldots, \subsetneq (x_1, \ldots, x_n)$, therefore we have $\dim(\mathbb{Z}[x_1, \ldots, x_n]) = n$, as desired.

■

2.8 Noetherian Modules

Problem 2.8.1

Show that R^n, the set of all n-tuples with components in unitary ring R, is R-module under the usual definition of addition and scalar multiplication:

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = \big((x_1 + y_1), \ldots, (y_n + y_n)\big)$$
$$r(x_1, \ldots, x_n) = (rx_1, \ldots, rx_n).$$

Solution: Recall the formal definition of module: Let R be a ring and M an additively written group, then M is a R-module if for $r, s \in R$, and $x, y \in M$:

(a) $r(x + y) = rx + ry$

(b) $(r + s)x = rx + sx$

(c) $r(sx) = (rs)x$

(d) $1_R x = x$.

(a) For the first condition, consider $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in R^n$, and $r, s \in R$, then

$$\begin{aligned} r\big((x_1, \ldots, x_n) + (y_1, \ldots, y_n)\big) &= r\big((x_1 + y_1), \ldots, (x_n + y_n)\big) \\ &= \big(r(x_1 + y_1), \ldots, r(x_n + y_n)\big) \\ &= \big((rx_1 + ry_1), \ldots, (rx_n + ry_n)\big) \\ &= \big((rx_1, \ldots, ry_1) + (ry_n, \ldots, ry_n)\big) \\ &= \big(r(x_1, \ldots, x_1) + r(y_n, \ldots, y_n)\big). \end{aligned}$$

(b) For the second condition, we have:

$$\begin{aligned} (r + s)(x_1, \ldots, x_n) &= \big((r + s)x_1, \ldots, (r + s)x_n\big) \\ &= \big((rx_1 + sx_1), \ldots, (rx_n + sx_n)\big) \\ &= \big((rx_1, \ldots, rx_n) + (sx_1, \ldots, sx_n)\big) \\ &= r(x_1, \ldots, x_n) + s(x_1, \ldots, x_n). \end{aligned}$$

(c) And for the third condition, we have:

$$\begin{aligned} r\big(s(x_1, \dots, x_n)\big) &= r(sx_1, \dots, sx_n) \\ &= rsx_1, \dots, rsx_n \\ &= (rs)(x_1, \dots, x_n). \end{aligned}$$

(d) Finally for the last condition, we have:

$$\begin{aligned} 1_R(x_1, \dots, x_n) &= (1_R x_1, \dots, 1_R x_n) \\ &= (x_1, \dots, x_n). \end{aligned}$$

Consequently M is R-module under the usual definition of addition and scalar multiplication, as desired.

■

Problem 2.8.2

Prove the assertion Dr. Zieschang made in the note: Let M be a R-module, and S be subring of R, then M is also an S-module.

Solution: Let's fix $s, t \in S$, and $x, y \in M$. Since S is subring of R hence $\forall s \in S \to s \in R$, therefore we have $s(x + y) = sx + sy$, which satisfies the first condition of the definition of a module.

And for the same reason that $\forall s, t \in S \to s, t \in R$, we have the second, the third and the fourth condition satisfied:

$$(s + t)x = sx + tx$$

$$s(tx) = (st)x$$

$$1_S x = x.$$

Consequently M is an S-module, as desired.

■

Problem 2.8.3

Show that $\mathbb{Z}$ is a noetherian module.

Solution: Recall that an R-module is called noetherian if each non-empty ascending chain of submodules of M,

$$L_1 \subseteq L_2 \subseteq L_3 \subseteq \dots$$

possess a maximal element with respect to set theoretic inclusion.

Notice that $\mathbb{Z}$ is a $\mathbb{Z}$-module, and $\mathbb{Z}$ is a principal ideal domain. If we have $a, b \in \mathbb{Z}$ and $(a) \subset (b)$, then b must divides a. As an illustration:

$$(2) = \{\dots - 4, -2, 0, 2, 4, 6, 8, \dots\}$$
$$(4) = \{\dots - 4, 0, 4, 8, 12, 16 \dots\}$$

then obviously $(4) \subset (2)$ and $2 \mid 4$.

If we have $a_i \in \mathbb{Z}$ and

$$(a_1) \subset (a_2) \subset (a_3) \subset (a_4) \subset \dots$$

then

$$a_2 \mid a_1, \ a_3 \mid a_1, \ a_4 \mid a_1 \dots$$

implying that the submodules (a_i) must eventually stabilizes, i.e., possesses a maximal element since a_i has only finite number of divisors. Consequently $\mathbb{Z}$ is a noetherian module, as desired.

■

Problem 2.8.4

Show that field F as a ring, i.e., F of F-module, is always noetherian.

Solution: First we note that field F has only trivial ideals $\{0\}$ and F itself as ideals. Proof by contradiction:

Suppose that by contradiction F possess an ideal I, with $I \neq \{0\}$ and $I \neq F$, therefore I must contain an element x, with $x \notin \{0\}$.

Since F is a field, x must possess a multiplicative inverse, i.e., there is $x^{-1} \in F$ such that

$xx^{-1} = 1_F$. This implies that $1_F \in I$ by definition of ideal, since $x \in I$ and $x^{-1} \in F$, therefore $xx^{-1} = 1_F$ must be in I.

But for $\forall y \in F, y1_F \in I$ since $1_F \in I$. Hence $F \subseteq I$. However as an ideal of F, $I \subseteq F$. Consequently $I = F$. Because field F has only $\{0\}$ and F itself as ideals, therefore F as an F-module is always noetherian, as desired.

■

Problem 2.8.5

Show that $\mathbb{Z}$-module $\mathbb{Q}$ is not noetherian.

Solution: Proof by counterexample: Suppose that $(\frac{1}{p})$ is a submodule of $\mathbb{Q}$ generated by $\frac{1}{p}$, thus there exists a sequence of submodules with respect to set-theoritic inclusion:

$$\left(\frac{1}{p}\right) \subset \left(\frac{1}{p^2}\right) \subset \left(\frac{1}{p^3}\right) \subset \dots$$

As an illustration:

$$\begin{aligned}\left(\frac{1}{2}\right) &= \{\frac{1}{2}, \frac{2}{2}, \frac{3}{2}, \frac{4}{2}, \frac{5}{2}, \frac{6}{2} \dots\} \\ &= \{\frac{1}{2}, 1, \frac{3}{2}, 2, \frac{5}{2}, 3, \dots\}\end{aligned}$$

$$\begin{aligned}\left(\frac{1}{2^2}\right) &= \{\frac{1}{4}, \frac{2}{4}, \frac{3}{4}, \frac{4}{4}, \frac{5}{4}, \frac{6}{4}, \frac{7}{4}, \frac{8}{4}, \dots\} \\ &= \{\frac{1}{4}, \frac{1}{2}, \frac{3}{4}, 1, \frac{5}{4}, \frac{3}{2}, \frac{7}{4}, 2, \dots\}\end{aligned}$$

$$\begin{aligned}\left(\frac{1}{2^3}\right) &= \{\frac{1}{8}, \frac{2}{8}, \frac{3}{8}, \frac{4}{8}, \frac{5}{8}, \frac{6}{8}, \frac{7}{8}, \frac{8}{8}, \dots\} \\ &= \{\frac{1}{8}, \frac{1}{4}, \frac{3}{8}, \frac{1}{2}, \frac{5}{8}, \frac{3}{4}, \frac{7}{8}, 1, \dots\}\end{aligned}$$

$$\begin{aligned}\left(\frac{1}{2^4}\right) &= \dots \\ &= \dots\end{aligned}$$

Thus $(\frac{1}{2}) \subset (\frac{1}{2^2}) \subset (\frac{1}{2^3}) \subset \dots$ Since the sequence does not stabilize, therefore it does not have maximal element. Hence $\mathbb{Z}$-module $\mathbb{Q}$ is not noetherian, as desired.

$\blacksquare$

2.9 Noetherian Integral Domain

Problem 2.9.1

Show that every principal ideal domain is noetherian.

Solution: We start by proving this Lemma: If every ideal of commutative ring R is finitely generated, then R is noetherian. Proof:

> Let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ be an ascending chain of ideals in R, then $I = \bigcup_{n=1}^{\infty} I_n$ is an ideal of R. Since I is finitely generate, we have
>
> $$I = (x_1, \ldots, x_n),$$
>
> with $x_i \in R$. For each $j \in [1, k], x_j \in I$, therefore $x_j \in I_{n_j}$ for some positive integer n_j. Thus
>
> $$\{x_1, \ldots, x_k\} \subseteq I_{max(n_1,\ldots,n_k)},$$
>
> from which it follows that $I \subseteq I_{max(n_1,\ldots,n_k)}$ and hence $I = I_{max(n_1,\ldots,n_k)}$. Let's take $N = max(n_1, \ldots, n_k)$ then we have $I_N = I_{(N+s)}$ for $s \in \mathbb{N}$, hence the chain stabilizes and thus R is noetherian, as desired.

Having proven the above lemma, we recall that in principal ideal domain, every ideal is generated by one single element and thus it is finitely generated. By the above lemma, then every principal ideal domain is noetherian.

■

Problem 2.9.2

Show that polynomial of one inderminate over $\mathbb{Z}$, that is $\mathbb{Z}[x]$, is noetherian integral domain.

Solution: Obviously $\mathbb{Z}$ is an integral domain because $\mathbb{Z}$ does not have zero divisor: $\forall a, b \in \mathbb{Z}$, $ab = 0$ means either $a = 0$ or $b = 0$. At the same time, we know that $\mathbb{Z}$ is principal ideal domain. Proof:

> Suppose I is an ideal of $\mathbb{Z}$. If $I = 0$ then 0 generates I and we are done. Suppose instead that $I \neq 0$ and suppose further a is the least positive element of I. We need to prove that a

generates I, that is, $(a) = I$. Obviously $a \in I$. In set-builder form: $(a) = \{ar \mid r \in \mathbb{Z}\}$, hence $ar \in I$. Let $b \in I$. If $b = 0$, we have $b = a \cdot 0 \in (a)$. But if $b \neq 0$, we assume $b > 0$ and by Euclidean algorithm we have

$$b = aq + r,$$

where the quotient $q \in \mathbb{Z}$ and remainder $r \in \mathbb{Z}$ and $0 \leq r \leq a$.

Now we have $r = b - aq \in I$ since $a \in I$ and $b \in I$. This implies $r = 0$ since $r < a$ and a is the least positive element in $\mathbb{Z}$. Hence $b = aq \in I$, thus $(a) = I$, as desired.

The fact that $\mathbb{Z}$ is principal ideal domain means that every ideal of $\mathbb{Z}$ is finitely generated. By Lemma in the previous exercise, if every ideal of a commutative ring is finitely generated, then the ring is noetherian. Combined with the fact that $\mathbb{Z}$ is integral domain, consequently $\mathbb{Z}$ is noetherian integral domain.

By Hilbert's Basis Theorem: If R is a noetherian ring, then $R[x]$ is noetherian ring. The corollary of this theorem is that if R is a noetherian integral domain, then $R[x]$ is noetherian. Consequently, since $\mathbb{Z}$ is noetherian integral domain, therefore $\mathbb{Z}[x]$ is noetherian integral domain, as desired.

■

Problem 2.9.3

Show that $\mathbb{Z}[x]$ is a noetherian integral domain which is not principal ideal domain.

Solution: By previous exercise, $\mathbb{Z}[x]$ is a noetherian integral domain. We need only to prove that $\mathbb{Z}[x]$ is not principal ideal domain. We will prove it by showing a counterexample. Let's consider ideal generated by integer 2 and indeterminate x:

$$\begin{aligned} I &= (2, x) \\ &= (2) + (x) \end{aligned}$$

First we need to show that I is an ideal of $\mathbb{Z}[i]$.

Let's consider these arbitrary elements of I where $a, b \in \mathbb{Z}$.:

$$p_1(x) = 2a + f(x),$$
$$p_2(x) = 2b + g(x),$$

Then

$$\begin{aligned} p_1(x) - p_2(x) &= 2(a-b) + (f(x) - g(x)) \\ &\in I, \end{aligned}$$

this is because $2(a-b) \in (2)$ and $\big(f(x) - g(x)\big) \in \mathbb{Z}[x]$.

Now, let's consider $r(x)$ an arbitrary element of $\mathbb{Z}[x]$, not necessarily has to be in I:

$$r(x) = c_n x^n + \ldots + c_1 x + c_0$$

with $c_i \in \mathbb{Z}$. Then

$$r(x)p(x) = (c_n x^n + \ldots + c_1 x + c_0)(2a + f(x)).$$

Here, $2ac_0 \in (2)$ and the rest of the terms will be elements of (x). Therefore $r(x)p(x) \in I$, and consequently $I = (2) + (x)$ is ideal of $\mathbb{Z}[x]$, as desired.

Assume that I is generated by a polynomial $h(x)$. Then $h(x)$ will have to divide 2, so there are two possible scenarios:

(a) First scenario: $h(x)$ will have to be a unit, which is not possible since obviously $I = (2) + (x)$ is not a unit ideal.

(b) Alternatively, $h(x)$ will have to be the product of a unit and 2, which again generates a different ideal since the indeterminate x is not suppose to be in (2).

Hence with $I = (2) + (x)$ as a counterexample, we conclude that $\mathbb{Z}[x]$ does not form principal ideal domain.

■

Problem 2.9.4

Show that $\mathbb{C}(x_1, x_2, \ldots)$ is a noetherian ring that contains a subring that is not noetherian.

Solution: Consider polynomial ring over complex number

$$R = \mathbb{C}[x_1, x_2, \ldots]$$

with infinitely many indeterminates. Then

$$(x_1) = \{x_1 f(x_1, x_2, \ldots) \mid f(x_1, x_2, \ldots) \in R\}$$

is obviously an ideal of R because, among other things, (x_1) absorbs multiplication, i.e., $\forall f \in (x_1), \forall g \in R, fg \in (x_1)$. And by similar argument,

$$(x_1, x_2), (x_1, x_2, x_3), (x_1, x_2, x_3, \ldots)$$

are also ideals of R.

Here, R is not noetherian because the chain of ideals,

$$(x_1, x_2) \subset (x_1, x_2, x_3) \subset (x_1, x_2, x_3, x_4) \subset \ldots$$

does not stabilize. On the other hand, R is contained in $\mathbb{C}(x_1, x_2, \ldots)$, the field of fraction of the polynomial ring $\mathbb{C}[x_1, x_2, \ldots]$. Since according to problem 8.5 every field is noetherian, hence $\mathbb{C}(x_1, x_2, \ldots)$ is noetherian. Therefore, $\mathbb{C}(x_1, x_2, \ldots)$ is a noetherian ring that contains a subring $\mathbb{C}[x_1, x_2, \ldots]$ that is not noetherian.

■

2.10 Commutative Artinian Rings

Problem 2.10.1

Show that $\mathbb{Z}$ and any polynomial ring $K[x]$ is not artinian.

Solution: Be definition, a commutative ring R with unity is called *artinian* if *each* descending chain

$$T_1 \subseteq T_2 \subseteq T_3 \subseteq \dots$$

of ideals of R possess a minimal element with respect to set theoretic inclusion.

In integer $\mathbb{Z}$, for $x \in \mathbb{Z}$, (x) is an ideal of $\mathbb{Z}$. Sketch of proof:

(a) The identity element $0 \in (x)$ obviously, since $0 \in \mathbb{Z}$.

(b) For $a, b \in (x), a + b \in (x)$.

(c) The ideal (x) obsorbs multiplication: $\forall y \in \mathbb{Z}$ and $\forall z \in (x)$, we have $yz = zy \in (x)$.

Using similar argument, we have also

$$(x^2), (x^3), (x^4) \dots$$

as ideals of $\mathbb{Z}$. However, the chain of descending ideals

$$(x) \supseteq (x^2) \supseteq (x^3) \supseteq (x^4) \supseteq \dots$$

is strictly descending and does not stabilize. Hence $\mathbb{Z}$ is not artinian.

In polynomial ring over K with one indeterminate $K[x]$, we have

$$(x) = \{xf(x) \mid f(x) \in K[x]\}$$

as ideal of $K[x]$. Sketch of proof:

(a) The identity element $0 \in (x)$.

(b) For $a, b \in (x), a + b \in (x)$.

(c) For $a \in (x)$ and $c \in K[x]$, (x) absorbs multiplication, i.e., $ac \in (x)$.

Using similar argument, we have

$$(x^2), (x^3), (x^4) \dots$$

also as ideals of $K[x]$. However, the chain of descending ideals,

$$(x) \supseteq (x^2) \supseteq (x^3) \supseteq (x^4) \supseteq \dots$$

is strictly descending and does not stabilize. Hence polynomial ring $K[x]$ is nor artinian.

■

Problem 2.10.2

Show that field $\mathbb{Q}$ is both artinian and noetherian.

Solution: Recall that R, a commutative ring with unity, is called *noetherian* if each ascending chain of ideals

$$T_1 \subseteq T_2 \subseteq T_3 \subseteq \dots$$

possesses a maximal element with respect to set theoretic inclusion.

Recall also that the same ring R is *artinian* if each descending chain of ideals

$$T_1 \supseteq T_2 \supseteq T_3 \supseteq \dots$$

possesses a minimal element with respect to set theoretic inclusion.

First we need to show that $\mathbb{Q}$ has only trivial ideals, which are $\{0\}$ and $\mathbb{Q}$ itself. Proof:

(a) We will assume by contrary that $\mathbb{Q}$ has a non-trial ideal I. Since I is an ideal, then I has multiplication absorbing property, that is

$$\forall q \in \mathbb{Q} \Rightarrow qI \subseteq I.$$

(b) Since $I \subset \mathbb{Q}$, therefore $\forall x \in I \Rightarrow x \in \mathbb{Q}$. Consequently x has an inverse x^{-1}. Therefore

$x^{-1}x = 1 \in I$.

(c) Since $1 \in I$ and $\forall q \in \mathbb{Q} \Rightarrow qI \subseteq I$, it is easy to see that $I = \mathbb{Q}$. Hence $\mathbb{Q}$ has only tirival ideal $\{0\}$ and $\mathbb{Q}$ itself, as desired.

Since the *ascending* chain of the two ideals in $\mathbb{Q}$ stabilizes,

$$\{0\} \subset \mathbb{Q},$$

hence $\mathbb{Q}$ is *noetherian*. At the same time, since the *descending* chain is also stabilizes,

$$\mathbb{Q} \supset \{0\},$$

consequently $\mathbb{Q}$ is *artinian*.

■

Problem 2.10.3

Show that $\mathbb{Q}/\mathbb{Z}$ as $\mathbb{Z}$-module is not noetherian but it is artinian.

Solution: Consider $(\frac{1}{p}) \subset \mathbb{Q}/\mathbb{Z}$ with p a prime number of $\mathbb{Z}$. Sketch of proving that $(\frac{1}{p})$ is ideal of $\mathbb{Q}/\mathbb{Z}$:

(a) Obviously $0 \in (\frac{1}{p})$ and 0 is the neutral number of $(\frac{1}{p})$.

(b) If $a, b \in (\frac{1}{p})$ then it is easy to see that $a + b \in (\frac{1}{p})$.

(c) If $x \in Q/\mathbb{Z}$ and $a \in (\frac{1}{p})$, again it is obvious that $ax \in (\frac{1}{p})$. Hence $(\frac{1}{p})$ is an ideal of $\mathbb{Q}/\mathbb{Z}$.

By the same reasoning, we take $(\frac{1}{p^2}), (\frac{1}{p^3}), \ldots$ as ideals of $\mathbb{Q}/\mathbb{Z}$. Then we have

$$(\frac{1}{p}) \subset (\frac{1}{p^2}) \subset (\frac{1}{p^3}) \subset \ldots$$

as an increasing chain of ideals which goes on forever without being stationary. Hence $\mathbb{Q}/\mathbb{Z}$ is not noetherian.

Now consider $(\frac{1}{n})$ as subgroup of $\mathbb{Q}/\mathbb{Z}$, with $n \in \mathbb{Z}$. By the same argument as above, $(\frac{1}{n})$ is an ideal of $\mathbb{Q}/\mathbb{Z}$. With $(\frac{1}{n})$ and $(\frac{1}{m})$ as ideals of $\mathbb{Q}/\mathbb{Z}$, we have

$$(\frac{1}{n}) \supset (\frac{1}{m}) \Rightarrow mn.$$

(Here is an illustration of the above claim: Since $(\frac{1}{4}) \supset (\frac{1}{2})$, therefore $2 \mid 4$.)

Consequently the descending chain of ideals

$$(\frac{1}{n_1}) \supset (\frac{1}{n_2}) \supset (\frac{1}{n_3}) \supset \dots$$

will eventually stabilize since there are only finite number of factors of n_1. Therefore $\mathbb{Q}/\mathbb{Z}$ is artinian, as desired.

■

Problem 2.10.4

Show that simple modules are both artinian and noetherian.

Solution: Recall that simple module is analogues to a simple group. A module is called *simple* if the only submodules are $\{0\}$ and the module itself.

Recall from the previous Section 2 in Dr. Zieschang's note, that if R is a commutative ring with unity, then an additive group M is called R-module if the followings hold for $\forall a, b \in R$ and $x, y \in M$:

(a) $a(x + y) = ax + ay$

(b) $(a + b)x = ax + by$

(c) $(ab)x = a(bx)$

(d) $1_R x = x$.

By comparing this definition with that of a ring, we see that moduel is in fact generalization of ring.

Recall also that if N is a subgroup of M, then N is R-submodule if N has the absorbing property, that is, for $\forall n \in N, r \in R \Longrightarrow rn = nr \in N$. Again, by contrasting this definition with that of an ideal, we see that submodule is in fact a generalization of ideal.

With these definitions in hand, we can now generalize the ACC (Ascending Chain Condition) and DCC (Descending Chain Condition) to modules by generalizing ring with module and by generalizing ideal with submodule.

From here, we have submodules in a simple modules, S, stablizing in both ascending chain:

$$\{0\} \subset S,$$

and stabilizing in descending chain:

$$S \subset \{0\}.$$

Consequently, simple module is both noetherian as well as artinian.

$\blacksquare$

2.11 Noetherian Domain of Dimension 1

Problem 2.11.1

Prove Dr. Zieschang's assertion in the note that for a unital commutative ring R, with T and U being the ideals of R, that

$$N_R(U/T) := \{r \in R \mid Ur \subseteq T\}$$

is an ideal of R.

Solution: We first need to show that $N_R(U/T)$ is an additive subgroup of R. Let's denote $N_R(U/T)$ simply as N for simplicity.

Here N has additive identity element 0, because $0 \in R$ and also because $U0 = 0$ and also $\{0\} \subseteq T$. If $r \in R$ and $Ur \subseteq T$, then of course we have these as their additive inverses: $-r \in R$ and $U(-r) \subseteq T$. If $a, b \in R$ and $Ua, Ub \subseteq T$, then

$$a + b \in R$$

and

$$\begin{aligned} U(a+b) &= Ua + Ub \\ &\subseteq T + T \\ &= T, \end{aligned}$$

hence $U(a+b) \subseteq T$.

Secondly, we need to show that N "absorbs" multiplication by any element $a \in R$. Here, if $a \in R$ and $r \in N$, then

$$ra \in R$$

and

$$\begin{aligned} U(ra) &= (Ur)a \\ &\subseteq Ta \\ &= T, \end{aligned}$$

this is because T being an ideal of R, hence T ”absorbs” multiplication by $a \in R$. Therefore $U(ra) \subseteq T$. Consequently $N := N_R(U/T)$ is an ideal of R, as desired.

■

Problem 2.11.2

Show that the ring $\mathbb{Z}$ is a noetherian domain of dimension 1.

Solution: From Section 7 about Krull Dimension, we have learned that the Krull dimension of $\mathbb{Z}$, that is $\dim(\mathbb{Z})$, is 1. Very briefly: The prime ideals of ring of $\mathbb{Z}$ are of the form $p_i\mathbb{Z}$, where p_i are prime numbers of $\mathbb{Z}$. Recall also that $\{0\}$ is a prime ideal of $\mathbb{Z}$ and that each non-zero prime ideal is maximal ideal. Consequently there is a strictly increasing chain

$$\{0\} \subsetneq P_i\mathbb{Z}$$

of prime ideals for each prime number P_i, thus

$$\dim(\mathbb{Z}) = 1.$$

(More generally, we say that any principal ideal domain that is not a field has Krull dimension of 1, because every non-zero prime ideal is maximal ideal.) From Section 9 about Noetherian Integral Domain, we also learned that $\mathbb{Z}$ is noetherian. Very briefly: $\mathbb{Z}$ is principal ideal domain by which each ideal of $\mathbb{Z}$ is generated by one single element, which further means that ideals of $\mathbb{Z}$ are finitely generated. Recall Dr. Zieschang’s Lemma 8.1: If M is an R-module, then the module M is noetherian if and only if each submodule of M is finitely generated. Here, because $\mathbb{Z}$ is finitely generated, therefore $\mathbb{Z}$ is noetherian. Thus $\mathbb{Z}$ is noetherian domain of dimension 1, as desired.

■

Problem 2.11.3

Show that the *Gaussian* integer $\mathbb{Z}[i]$ is a noetherian domain of dimension 1.

Solution: First we need to prove that $\mathbb{Z}[i]$ forms an integral domain. Proof by contradiction:

(a) We know that $\mathbb{Z}[i]$ is commutative ring. Suppose that $(a+bi) \in \mathbb{Z}[i]$ and suppose also that $(c+di) \in \mathbb{Z}[i]$, with $a, b, c, d \in \mathbb{Z} \setminus \{0\}$.

(b) Suppose further that there is zero divisor in $\mathbb{Z}[i]$:

$$\begin{aligned} 0 &= (a+bi)(c+di) \\ &= (ac-bd)+(ad+bc)i \\ &\in \mathbb{Z}[i], \end{aligned}$$

implying that

$$\begin{aligned} ac-bd &= 0 \\ ac &= bd, \end{aligned} \tag{1}$$

and also

$$\begin{aligned} ad+bc &= 0 \\ ad &= -bc. \end{aligned} \tag{2}$$

(c) If we multiple the above (1) and (2), then we have

$$\begin{aligned} a^2cd &= -b^2cd \\ a^2 &= -b^2 \end{aligned}$$

which is impossible to be true. Hence we have to conclude that $\mathbb{Z}[i]$ does not have zero divisor, consequently $\mathbb{Z}[i]$ is integral domain.

Secondly, we need to prove that $\mathbb{Z}[i]$ forms a principal ideal domain.

(a) By corollary to Lemma 8.5 of Dr. Zieschang's *Algebra I*, $\mathbb{Z}[i]$ is euclidean with respect to the degree function:

$$\delta : \mathbb{Z}[i] \to \mathbb{N}, \quad x + yi \mapsto x^2 + y^2.$$

(b) Recall Dr. Zieschang's Theorem 8.6 in *Algebra I* which states that euclidean rings are principal ideal domain. Hence $\mathbb{Z}[i]$ forms a principal ideal domain.

Since $\mathbb{Z}[i]$ is a principal ideal domain, hence its ideals are finitely generated, resulting in conclusion that $\mathbb{Z}[i]$ is noetherian.

We recall from Lemma 8.2 of *Algebra I* again: That in principal ideal domain, all prime ideals different from $\{0\}$ are maximal. Consequently if I is an ideal of $\mathbb{Z}[i]$, then there is a strictly increasing chain of prime ideals

$$\{0\} \subsetneq I$$

such that

$$\dim(\mathbb{Z}[i]) = 1.$$

Hence $\mathbb{Z}[i]$ is noetherian domain of dimension 1, as desired.

■

2.12 Dedekind Domain

Problem 2.12.1

Show that each of rings of $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$ and $\mathbb{Z}$ is Dedekind domain.

Solution: First we recall the following chain of class inclusion:

$$\text{Field} \subset \text{PID} \subset \text{UFD} \subset \text{Integral Domain},$$

and also Corollary 12.6 from Dr. Zieschang's class note: The Principal Ideal Domains are exactly the Dedekind domains which are Unique Factorization Domains. Here, for proving $\mathbb{R}$, $\mathbb{Q}$ and $\mathbb{C}$, we will go down the shortest route by finding out if each of them is a field.

(a) The real number ring $\mathbb{R}$ does not have zero divisor, has multiplicative identity of 1, and each element has multiplicative inverse, hence $\mathbb{R}$ is a field and consequently $\mathbb{R}$ is a Dedekind domain.

(b) The rational number $\mathbb{Q}$ does not have zero divisor, has multiplicative identity of 1, and each element has multiplicative inverse, hence as in the case of $\mathbb{R}$, $\mathbb{Q}$ is a field and consequently it is a Dedekind domain.

(c) The complex number $\mathbb{C}$ has multiplicative inverse of $1 + 0 \cdot i = 1$, which we can easily confirm. Additionally, $\forall (a + bi) \in \mathbb{C}$, with $a, b \in \mathbb{R}$, it has

$$\begin{aligned}\frac{1}{(a+bi)} &= \frac{1}{(a+bi)} \cdot \frac{(a-bi)}{(a-bi)} \\ &= \frac{(a-bi)}{(a^2+b^2)} \\ &= \frac{a}{(a^2+b^2)} - \frac{bi}{(a^2+b^2)}\end{aligned}$$

as its multiplicative inverse. Therefore $\mathbb{C}$ forms a field and consequently $\mathbb{C}$ is a Dedekind domain.

(d) The integer $\mathbb{Z}$ is of course not a field, because $\mathbb{Z}$ does not have multiplicative inverse. However, we do know that $\mathbb{Z}$ forms a Principal Ideal Domain. Proof:

> Suppose I is an ideal of $\mathbb{Z}$. If $I = 0$ then 0 generates I and we are done. Suppose instead that $I \neq 0$ and suppose further a is the least positive element of I. We need to prove that a

> generates I, that is, $(a) = I$. Obviously $a \in I$. In set-builder form: $(a) = \{ar \mid r \in \mathbb{Z}\}$, hence $ar \in I$. Let fix $b \in I$. If $b = 0$, we have $b = a \cdot 0 \in (a)$. But if $b \neq 0$, we assume $b > 0$ and by Euclidean algorithm we have
>
> $$b = aq + r,$$
>
> where the quotient $q \in \mathbb{Z}$ and remainder $r \in \mathbb{Z}$ and $0 \leq r \leq a$. Now we have $r = b - aq \in I$ since $a \in I$ and $b \in I$. This implies $r = 0$ since $r < a$ and a is the least positive element in $\mathbb{Z}$. Hence $b = aq \in I$, thus $(a) = I$, as desired.

Since $\mathbb{Z}$ is a Principal Ideal Domain hence it's a Dedekind domain.

■

Problem 2.12.2

Find out if each of these polynomial rings with one indeterminate is Dedekind domain: $\mathbb{R}[x]$, $\mathbb{Q}[x]$, $\mathbb{C}[x]$ and $\mathbb{Z}[x]$.

Solution: We will use the Corollary 12.6 as in the previous exercise by first showing that each of the above polynomial rings is Principal Ideal Domain. To do that, first we need the following Lemma: Let $\mathcal{K}$ be a field, then the polynomial ring $\mathcal{K}[x]$ is a Principal Ideal Domain. Proof:

> Let $I \subset \mathcal{K}[x]$ be an ideal. We want to prove that I is principal. If $I = 0$, then I is trivial and we are done. If, on the other hand, $I \neq 0$, then let's fix $f(x) \in I$ be a non-zero polynomial of the least degree. Here we are claiming that $I = (f(x))$. For any given $g(x) \in I$, we have
>
> $$\frac{g(x)}{f(x)} = q(x) \cdot f(x) + r(x),$$
>
> where $q(x)$ and $r(x)$ are the quotient and remainder polynomials respectively, and where $r(x)$ has strictly smaller degree then $f(x)$. However, $r(x) = g(x) - q(x) \cdot f(x)$, where $f(x)$ has been set in the above to have the least possible degree. Hence the minimality of the

degree of $f(x)$ forces $r(x)$ to be 0. Therefore

$$\begin{aligned} g(x) &= q(x) \cdot f(x) \\ &\in (f(x)). \end{aligned}$$

Since we have set $g(x) \in I$ as arbitrary, hence $I = (f(x))$, as desired.

Having proven the lemma, we now turn our attention to previous exercise, where we have shown $\mathbb{R}$, $\mathbb{Q}$ and $\mathbb{C}$ are fields. Because of this result, therefore we conclude that polynomial rings with one indeterminate $\mathbb{R}[x]$, $\mathbb{Q}[x]$ and $\mathbb{C}[x]$ are Principal Ideal Domains and hence they are Dedekind domains, as desired.

Having done with $\mathbb{R}[x]$, $\mathbb{Q}[x]$ and $\mathbb{C}[x]$, we will now focus on $\mathbb{Z}[x]$. Since $\mathbb{Z}$ is not a field and therefore $\mathbb{Z}[x]$ is not a Principal Ideal Domain. Consequently $\mathbb{Z}[x]$ is not a Dedekind domain.

■

Problem 2.12.3

Find $\dim(\mathbb{R})$, $\dim(\mathbb{Q})$ and $\dim(\mathbb{Z})$ to confirm the validity of Dr. Zieschang's Lemma 12.3.

Solution: Here is the Lemma 12.3 from Dr. Zieschang's class note: Dedekind domains have exactly Krull dimension of either 0 or 1.

First we would like to show that $\dim(\mathbb{Z}) = 1, \dim(\mathbb{R}) = 1$ and $\dim(\mathbb{Q}) = 0$.

(a) Consider p_i, with $i \in \{1, 2, ..., n\}$, as prime numbers of $\mathbb{Z}$. According to Lemma 7.3 of Dr. Zieschang's *Algebra I*, then $p_i\mathbb{Z}$ are the prime ideals of $\mathbb{Z}$. Since $p_i\mathbb{Z}$ are also the maximal ideals of $\mathbb{Z}$, therefore $\mathbb{Z}$ has only chain set of prime ideals $\mathcal{S}$ of oder 2:

$$\{0\} \subsetneq p_i\mathbb{Z}.$$

Hence,

$$\begin{aligned} \dim(\mathbb{Z}) &= |\mathcal{S}| - 1 \\ &= 2 - 1 \\ &= 1. \end{aligned}$$

(b) Using similar argument like the above, we can derive

$$\dim(\mathbb{R}) = |\mathcal{S}| - 1 = 2 - 1 = 1.$$

(c) We know that $\mathbb{Q}$ is a field, and field does not have any prime ideal except $\{0\}$, hence the order of chain set of prime ideals $\mathcal{S}$ is $|\mathcal{S}| = 1$. Therefore

$$\dim(\mathbb{Q}) = |\mathcal{S}| - 1 = 1 - 1 = 0.$$

Since we now have had $\dim(\mathbb{Z}) = 1$, $\dim(\mathbb{R}) = 1$ and $\dim(\mathbb{Q}) = 0$, and since by Problem 12.1 we have shown that the rings of $\mathbb{R},\ \mathbb{Q}$ and $\mathbb{Z}$ are Dedekind domains, thus we confirm the validity of Dr. Zieschang's Lemma 12.3, as desired.

■

Problem 2.12.4

By using ring of integer $\mathbb{Z}$, give an example to illustrate the validity of Dr. Zieschang's Corollary 12.1 in his class note.

Solution: Here is the Corollary 12.1: Let T be an ideal of Dedekind domain R, and let p be a non-zero element in T. Then T possesses an element q such that $pR + qR = T$.

From previous exercise, we have known that $\mathbb{Z}$ is Dedekind domain. Consider $\mathbb{Z}$ as the R in the Corollary 12.1, and the set of even integers $2\mathbb{Z}$, an ideal of $\mathbb{Z}$, as T in the Corollary 12.1. Let's take as an example $p = 8 \in 2\mathbb{Z}$, then we need to find $q \in 2\mathbb{Z}$. Since $q \in 2\mathbb{Z}$, hence there exists $\bar{q} \in \mathbb{Z}$ such that $q = 2\bar{q}$.

$$8\mathbb{Z} + q\mathbb{Z} = 2 \cdot 4\mathbb{Z} + 2\bar{q}\mathbb{Z} = 2\mathbb{Z}.$$

Here, p can be any arbitrary element of the set of even integer $2\mathbb{Z}$.

■

2.13 The Field of Fractions of a Dedekind Domain

Problem 2.13.1

Verify Dr. Zieschang's Lemma 13.2 by using $\mathbb{Z}$ as an illustration.

Solution: Recall Lemma 13.2 from Dr. Zieschang's class note: Assume that R is integrally closed noetherian domain of Krull dimension 1. Then each non-zero prime ideal of R is invertible.

From previous exercise 11.2, we have learned that the ring $\mathbb{Z}$ is a noetherian domain of dimension 1. We will show that $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$. Proof:

> Take any element of $\mathbb{Q}$ which is integral over $\mathbb{Z}$, and reduce it in the form of $\frac{x}{y}$, with $x, y \in \mathbb{Z}$ and $\gcd(x, y) = 1$. Then $\left(\frac{x}{y}\right)^n + a_1 \left(\frac{x}{y}\right)^{n-1} + \ldots + a_n = 0$ with $a_i \in \mathbb{Z}$. Multiplying both sides by y^n, then
>
> $$x^n + a_1 x^{n-1} y + \ldots + a_n y^n = 0$$
> $$x^n + (a_1 x^{n-1} + \ldots + a_n y^{n-1})y = 0.$$
>
> This implies that y divides x^n. So $y = \{-1, 1\}$ and hence $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$, as desired.

Having proven that $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$, next we need to show that for each prime number $p \in \mathbb{Z}$, then $p\mathbb{Z}$ is prime ideal of $\mathbb{Z}$. According to Dr. Zieschang's *Algebra I* note, the proof is as follow:

> Obviously $p\mathbb{Z} \neq \mathbb{Z}$. We know that $p \in \mathbb{Z}$, if $a \in \mathbb{Z}$ then obviously $pa \in p\mathbb{Z}$. Hence $p\mathbb{Z}$ is prime ideal of $\mathbb{Z}$.

Then prime ideal $p\mathbb{Z}$ of $\mathbb{Z}$ is invertible:

$$\begin{aligned}(\mathbb{Z} : (p)) &= \{x \in \mathbb{Q} \mid (p)x \subset \mathbb{Z}\} \\ &= \frac{1}{p}\mathbb{Z} \subset \mathbb{Q},\end{aligned}$$

as desired.

■

Problem 2.13.2

Repeat the previous exercise by using *Gaussian* integer $\mathbb{Z}[i]$ as illustration.

Solution: From Dr. Zieschang's Corollary 4.11 in his class note on Number Theory, we learn that $\mathbb{Z}[i]$ forms Euclidean domain, and since

$$\text{Euclidean domain} \subset \text{Principal Ideal Domain},$$

therefore $\mathbb{Z}[i]$ forms Principal Ideal Domain.

From Corollary 12.6 of this class note, we have learned that the principal ideal domains are exactly the gaussian Dedekind domain. Consequently $\mathbb{Z}[i]$ forms Dedekind domain.

From Proposition 13.1 of this chapter, we learn that Dedekind domains are integrally closed. Specifically $\mathbb{Z}[i]$ is integrally closed in $\mathbb{Q}[i]$. Therefore the ring of *Gaussian* integer $\mathbb{Z}[i]$ is an integrally closed noetherian domain of dimension 1.

From Theorem 5.4 of Number Theory class note, we have (p) as prime element of $\mathbb{Z}[i]$, with prime number $p \in \mathbb{Z}$ and $p \equiv 3(\mod 4)$:

$$(p) = p\mathbb{Z}[i].$$

Then prime ideal $(p) = p\mathbb{Z}[i]$ of $\mathbb{Z}[i]$ is invertible, as desired:

$$\begin{aligned}(\mathbb{Z}[i] : (p)) &= \big\{x \in \mathbb{Q}[i] \mid (p)x \subset \mathbb{Z}[i]\big\} \\ &= \frac{1}{p}\mathbb{Z}[i] \subset \mathbb{Q}[i].\end{aligned}$$

■

Problem 2.13.3

Using only Dr. Zieschang's Lemma 13.3, prove that $\mathbb{Z}$ is a Dedekind domain.

Solution: Recall Lemma 13.3: Let R be an integral domain, and assume that $\mathcal{F}(R) \setminus \{\{0\}\}$ is a group. Then R is a Dedekind domain.

Recall also from this class note's section 3: *The Field of Fractions of an Integral Domain*, that

$$\frac{m}{n}\mathbb{Z} := \{\frac{mz}{n} \mid m, z \in \mathbb{Z}, n \in \mathbb{Z} \setminus \{0\}\}$$

is called the fractional ideal of $\mathbb{Z}$ in $\mathbb{Q}$, and that $\mathcal{F}_{\mathbb{Q}}(\mathbb{Z})$ is the set of all fractional ideals of $\mathbb{Z}$ in $\mathbb{Q}$. Let $F_i \in \mathcal{F}_{\mathbb{Q}}(\mathbb{Z})$ with $i \in \mathbb{N}$, and that

$$F_i = \{\frac{m_i z}{n_i} \mid m_i, z \in \mathbb{Z},\ n_i \in \mathbb{Z} \setminus \{0\}\}.$$

We then need to prove that $\mathcal{F}_{\mathbb{Q}}(\mathbb{Z}) \setminus \{\{0\}\}$ is a group.

Let's denote $\mathcal{F} := \mathcal{F}_{\mathbb{Q}}(\mathbb{Z}) \setminus \{\{0\}\}$ for simplicity. Then obviously $\mathcal{F}$ can't be additive group because it does not contain additive neutral element $\{0\}$. We then proceed to prove that $(\mathcal{F}, \cdot)$ is a group.

(a) The neutral element of $(\mathcal{F}, \cdot)$ is $\{\{\frac{1}{1}\}\} = \{\{1\}\}$.

(b) The inverse element of F_i is

$$F_i^{-1} = \{\frac{n_i}{m_i z} \mid n_i \in \mathbb{Z},\ m_i, z \in \mathbb{Z} \setminus \{0\}\},$$

because $F_i \cdot F_i^{-1} = \{\{1\}\}$.

(c) If $F_1, F_2 \in \mathcal{F}$, then

$$\begin{aligned} F_1 \cdot F_2 &= \{\{\frac{m_1}{n_1}\mathbb{Z}\} \cdot \{\frac{m_2}{n_2}\mathbb{Z}\}\} \\ &= \{\{\frac{m_1 \cdot m_2}{n_1 \cdot n_2}\mathbb{Z}\}\} \\ &\in \mathcal{F}, \end{aligned}$$

hence the closure property.

(d) If F_1, F_2 and $F_3 \in \mathcal{F}$, then

$$(F_1 \cdot F_2) \cdot F_3 = \Big\{ \big(\{\frac{m_1}{n_1}\mathbb{Z}\} \cdot \{\frac{m_2}{n_2}\mathbb{Z}\}\big) \cdot \{\frac{m_3}{n_3}\mathbb{Z}\} \Big\}$$

$$= \Big\{ \big(\{\frac{m_1 \cdot m_2}{n_1 \cdot n_2}\mathbb{Z}\}\big) \cdot \{\frac{m_3}{n_3}\mathbb{Z}\} \Big\}$$

$$= \Big\{ \{\frac{m_1 \cdot m_2 \cdot m_3}{n_1 \cdot n_2 \cdot n_3}\mathbb{Z}\} \Big\}$$

$$= \Big\{ \{\frac{m_1}{n_1}\mathbb{Z}\} \cdot \big(\{\frac{m_2 \cdot m_3}{n_2 \cdot n_3}\mathbb{Z}\}\big) \Big\}$$

$$= \Big\{ \{\frac{m_1}{n_1}\mathbb{Z}\} \cdot \big(\{\frac{m_2}{n_2}\mathbb{Z}\} \cdot \{\frac{m_3}{n_3}\mathbb{Z}\}\big) \} \Big\}$$

$$= F_1 \cdot (F_2 \cdot F_3),$$

hence the associative property and consequently, $\mathcal{F}$ is a group, as desired.

Since $\mathbb{Z}$ is an integral domain and since $\mathcal{F}_{\mathbb{Q}}(\mathbb{Z}) \setminus \{\{0\}\}$ is a group, therefore $\mathbb{Z}$ is a Dedekind domain per Lemma 13.3.

■

CHAPTER III

NUMBER THEORY

3.1 Commutative Rings

Problem 3.1.1

Using only the concept of coprime, provide alternative proof of Lemma 1.7 as stated in the class note.

Solution: Here is the Lemma 1.7 from class note: There are infinitely many prime elements in $\mathbb{Z}$. Before we start with the proof, let's recall also that for $m, n \in \mathbb{Z}$, m and n are said to be coprime if $gcd(m, n) = 1$. (The following proof is adopted from Filip Saidak, 2005.)

First, we will prove and use this little lemma: Consecutive integers are coprime. Proof:

> Let's assume that for $n \in \mathbb{Z}, n$ and $(n+1)$ are not coprime, implying that there exists $d \in \mathbb{Z}$, such that if $d \mid n$, then $d \mid (n+1)$. Consequently,
>
> $$\begin{aligned} & d \mid (n+1) - n \\ = \quad & d \mid 1, \end{aligned}$$
>
> which is not possible. Hence $gcd\big(n, (n+1)\big) = 1$.

Having proven the lemma, let's denote $n \in \mathbb{Z}$ and $n > 1$. Since n and $(n+1)$ are consecutive integers, they must be coprime, and hence the number

$$N_2 = n(n+1)$$

must have at least two different prime factors.

Similarly, since N_2 and $(N_2 + 1)$ are consecutive integers, they must be coprime and hence the number

$$N_3 = N_2(N_2 + 1)$$

must have at least 3 different prime factors. And this process can be continued indefinitely, thus proving our case.

Indeed, using concrete integer, if $n = 5$ then $n + 1 = 6$, and

$$\begin{aligned} 5 \cdot 6 &= 30 \\ &= 2 \cdot 3 \cdot 5, \end{aligned}$$

and

$$\begin{aligned} 30 \cdot 31 &= 930 \\ &= 2 \cdot 3 \cdot 5 \cdot 31, \end{aligned}$$

and

$$\begin{aligned} 930 \cdot 931 &= 865,830 \\ &= 2 \cdot 3 \cdot 5 \cdot 31 \cdot 7^2 \cdot 19 \\ &= 2 \cdot 3 \cdot 5 \cdot 7^2 \cdot 19 \cdot 31, \end{aligned}$$

and this operation can be carried on indefinitely.

■

Problem 3.1.2

Prove that a right triangle of Pythagorean triple dilated by an integer factor is still a right triangle of Pythagorean triple.

Solution: Recall from Lemma 1.8 in Dr. Zieschang's class note: Let R be a Unique Factorization

Domain, let x, y and z be elements in R, and let m and n be positive integers. Then we have

$$x^n + y^n = z^n$$

if and only if

$$(mx)^n + (my)^n = (mz)^n.$$

Next, we recall from Dr. Zieschang's *Algebra I* that $\mathbb{Z}$ forms Unique Factorization Domain due to the Fundamental Theorem of Arithmetic. Now, let's fix $x, y, z \in \mathbb{Z}^+$ as Pythagorean triple such that

$$x^2 + y^2 = z^2,$$

and let's assume that right tringle is dilated by factor of m, where $m \in \mathbb{Z}^+$. Hence

$$x' = mx$$

$$y' = my,$$

$$z' = mz.$$

Since Lemma 1.8 asserts that $(mx)^2 + (my)^2 = (mz)^2$, therefore $(x')^2 + (y')^2 = (z')^2$, and hence it is still Pythagorean triple.

■

Problem 3.1.3

Use examples of *Gaussian* integers $\mathbb{Z}[i]$ to illustrate the Lemma 1.9 from the class note.

Solution: First, we need to mention these following four facts:

(a) Recall the Lemma 1.9 from class note: Let R be a Unique Factorization Domain, $x, y \in R$, and $n \in \mathbb{Z}^+$ such that $x^n \mid y^n$. Then $x \mid y$.

(b) We have learned from Dr. Zieschang's *Algebra I*, that *Gaussian* integers $(a + bi) \in \mathbb{Z}[i]$, where $a, b \in \mathbb{Z}$, forms Unique Factorization Domain. And that the norm $\mathcal{N}$ of *Gaussian* integer $\alpha = (a + bi)$ is defined as the product of the *Gaussian* integer and its conjugate:

$$\begin{aligned}\mathcal{N}(\alpha) &= \alpha\bar{\alpha} \\ &= (a+bi)(a-bi) \\ &= a^2+b^2.\end{aligned}$$

(c) Additionally, we recall the *Gaussian* integer's division theorem: For $\alpha, \beta \in \mathbb{Z}[i]$, with $\beta \neq 0$,

$$\frac{\alpha}{\beta} = \beta q + r,$$

where $q, r \in \mathbb{Z}[i]$ are the quotient and remainder, with $\mathcal{N}(r) < \mathcal{N}(\beta)$. If $r = 0$, we say that $\beta \mid \alpha$.

(d) Finally, we recall the divisibility of $\mathbb{Z}[i]$: For $\alpha, \beta \in \mathbb{Z}[i]$, if $\beta \mid \alpha \in \mathbb{Z}[i]$ then

$\mathcal{N}(\beta) \mid \mathcal{N}(\alpha) \in \mathbb{Z}$.

Having recalled the above four facts, we take these as examples of *Gaussian* integers $\mathbb{Z}[i]$:

$$\begin{aligned}\alpha &= -8+6i, \\ \beta &= \ \ 3+4i.\end{aligned}$$

Here apparently $\beta \mid \alpha$, as demonstrated by the followings:

$$\begin{aligned}\frac{-8+6i}{3+4i} &= \frac{-8+6i}{3+4i} \cdot \frac{3-4i}{3-4i} \\ &= \frac{50i}{25} \\ &= 2i.\end{aligned}$$

And indeed, since $\mathcal{N}(\alpha) = 100, (\beta) = 25$, hence $\mathcal{N}(\beta) \mid \mathcal{N}(\alpha)$.

Then, expressing the α and β in perfect square terms, we have

$$\begin{aligned}\alpha &= -8+6i \\ &= (1+3i)^2,\end{aligned}$$

and

$$\begin{aligned}\beta &= 3 + 4i \\ &= (2+i)^2.\end{aligned}$$

If we divide the square root of α by the square root of β, we have

$$\begin{aligned}\frac{\sqrt{\alpha}}{\sqrt{\beta}} = \frac{\alpha'}{\beta'} &= \frac{1+3i}{2+i} \\ &= \frac{(1+3i)}{(2+i)} \cdot \frac{(2-i)}{(2-i)} \\ &= \frac{5-5i}{5} \\ &= 1 - i\end{aligned}$$

Since the remainder $r = 0$, therefore $\beta' \mid \alpha'$ and indeed, since $\mathcal{N}(\alpha') = 10$ and $\mathcal{N}(\beta') = 5$, consequently $\mathcal{N}(\beta') \mid \mathcal{N}(\alpha')$.

■

Problem 3.1.4

Similar to previous exercise, use the example of polynomial ring to illustrate the Lemma 1.9.

Solution: As we have learned from *Algebra I* that $P[x]$ forms Unique Factorization Domain, where P is a field. We have learned also the division of polynomial rings:

$$\frac{P_1[x]}{P_2[x]} = P_2[x] \cdot Q[x] + R[x],$$

where $P_2[x] \neq 0$, and $\deg(P_2[x]) > \deg(R[x])$. Additionally, $P_2[x] \mid P_1[x]$ if and only if $R[x] = 0$.

Here, we take these as our examples:

$$\begin{aligned}P_1[x] &= x^4 + \frac{7}{3}x^3 + \frac{73}{36}x^2 + \frac{7}{9}x + \frac{1}{9}, \\ P_2[x] &= x^2 + x + \frac{1}{4}.\end{aligned}$$

By polynomial long division, we have

$$\begin{aligned}\frac{P_1[x]}{P_2[x]} &= x^2 + \frac{4}{3}x + \frac{4}{9}\\ &= (x + \frac{2}{3})^2.\end{aligned}$$

Since the remainder $R[x] = 0$ we have $P_2[x] \mid P_1[x]$.

By expressing the $P_1[x]$ and $P_2[x]$ in perfect square terms, we then have

$$\begin{aligned}P_1[x] &= x^4 + \frac{7}{3}x^3 + \frac{73}{36}x^2 + \frac{7}{9}x + \frac{1}{9}\\ &= (x^2 + \frac{7}{9}x + \frac{1}{3})^2.\\ P_2[x] &= x^2 + x + \frac{1}{4}\\ &= (x + \frac{1}{2})^2.\end{aligned}$$

We then square root the $P_1[x]$ and $P_2[x]$ and divide $P_1[x]$ by $P_2[x]$, we have

$$\begin{aligned}\frac{\sqrt{P_1[x]}}{\sqrt{P_2[x]}} = \frac{P_1'[x]}{P_2'[x]} &= \frac{x^2 + \frac{7}{6}x + \frac{1}{3}}{x + \frac{1}{2}}\\ &= x + \frac{2}{3}.\end{aligned}$$

Since the remainder $R[x] = 0$, we have $P_2'[x] \mid P_1'[x]$, as desired.

■

Problem 3.1.5

Show that the difference of two square of odd integers is always divisible by 4.

Solution: Recall Lemma 1.12 from Dr. Zieschang's note: Let z be an odd integer. We have $z^2 \equiv 1 \pmod 4$. Recall also that for $a_i, b_i, m \in \mathbb{Z}$, if

$$\begin{aligned}a_1 &\equiv b_1 \pmod m,\\ a_2 &\equiv b_2 \pmod m,\end{aligned}$$

then we have

$$a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m}.$$

Having recalled those results, suppose that z_1 and z_2 are odd integers, then based on Lemma 1.12:

$$z_1^2 \equiv 1 \pmod{4},$$
$$z_2^2 \equiv 1 \pmod{4},$$

consequently

$$z_1^2 - z_2^2 \equiv 0 \pmod{4}.$$

Therefore $4 \mid (z_1^2 - z_2^2)$, as desired.

■

Problem 3.1.6

Show that the sum of n square of odd integers is congruent to n modulo 4.

Solution: Recall Lemma 1.12 from the note and the two properties of modulo arithmetic we referred to in previous problem.

Let's fix z_i as an odd integer, with $i = \{1, 2, \dots, n\}$. Then we have

$$z_1^2 \equiv 1 \pmod{4},$$
$$z_1^2 \equiv 1 \pmod{4},$$
$$\dots$$
$$\dots$$
$$z_n^2 \equiv 1 \pmod{4},$$

hence

$$\sum_{i=1}^{n} z_i^2 \equiv n \pmod{4},$$

as desired.

■

3.2 Some Basic Arithmetic

Problem 3.2.1

Using Lemma 2.11 from Dr. Zieschang's class note, find all the subgroups of $\mathbb{Z}_4, \mathbb{Z}_7$ and $\mathbb{Z}_{12}$.

Solution: Recall that according to the note's Lemma 2.1 on Lagrange Theorem, the order of subgroup divides the order of the group. Recall also that in order to be a subgroup, each element has to have inverse and to close under the operation.

(a) First, we have $\mathbb{Z}_4 = \{0, 1, 2, 3\}$. Since its order $|\mathbb{Z}_4| = 4$, therefore the order of any subgroup of $\mathbb{Z}_4$ has to be the factors of 4, which are $1, 2$ and 4. By observation and trial and error, we have the following subgroups:

(a_1) The first subgroup is the trivia $\{0\}$, its order is 1. Here 0 has itself as inverse, and it closes under the operation.

(a_2) The second is $\{0, 2\}$, its order is 2. Here, 2 has itself as the inverse, and the subgroup is closed under the opration.

(a_3) The third is $\mathbb{Z}_4$ itself, its order is 4. Here since the subgroup is the group itself, therefore we do not have to investigate each element's inverse and the subgroup's closure.

(b) Next we have $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$. Because its order $|\mathbb{Z}_7| = 7$, hence the order of each of its subgroup has to be either 1 or 7. Again by observation and trial and error, we have

(b_1) The trivia subgroup $\{0\}$, its order is 1.

(b_2) The Z_7 itself, its order is 7.

(c) Finally we have $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$. Since its order $|\mathbb{Z}_{12}|$ is 12, therefore each of its subgroups' order must be $1, 2, 3, 4, 6$ or 12.

(c_1) The trivia subgroup $\{0\}$, its order is 1.

(c_2) The second subgroup is $\{0, 6\}$, its order is 2. Here 6 has itself as the inverse, and the subgroup closes under the operation.

(c_3) The third is $\{0, 4, 8\}$, with order of 3. Here 4 and 8 have each other as the inverse, and the subgroup closes under the operation.

(c_4) The fourth is $\{0, 3, 6, 9\}$, with order of 4. Here 3 and 9 have each other as the inverse, and 6 has itself as the inverse, and the subgroup closes under the operation.

(c_5) The fifth one is $\{0, 2, 4, 6, 8, 10\}$, with order of 6. Here 2 and 10, 4 and 8 have each other as the inverse, 6 has itself as the inverse, and the subgroup closes under the operation.

(c_6) The last one is the $\mathbb{Z}_{12}$ itself with order of 12.

■

Problem 3.2.2

Use the order of each element of $\mathbb{Z}_{10}$ to validate the Lemma 2.2 in the class note.

Solution: Recall Dr. Zieschang's Lemma 2.2: Let G be a finite group, and $g \in G$, then the order of g divides the order of G. Recall also that the order of an element of a finite group is the smallest positive integer n, such that $g^n = e$.

We have $\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

Since $0^1 = 0,$ therefore the order $\mathcal{O}(0) = 1$;

$1^{10} = 0,$ the order $\mathcal{O}(1) = 10$;

$2^5 = 0,$ the order $\mathcal{O}(2) = 5$;

$3^{10} = 0,$ the order $\mathcal{O}(3) = 10$;

$4^5 = 0,$ the order $\mathcal{O}(4) = 5$;

$5^2 = 0,$ the order $\mathcal{O}(5) = 2$;

$\ldots$

$9^{10} = 0,$ the order $\mathcal{O}(9) = 10$.

The order of each element of $\mathbb{Z}_{10}$ is therefore $1, 2, 5$ and 10, and each of these divides the order of $\mathbb{Z}_{10}$.

■

Problem 3.2.3

With respect to Dr. Zieschang's Lemma 2.5, show that if $p_i > 2$ are the prime numbers, with $i = \{1, 2, \ldots, n\}$, and if it is established that $p_i \equiv 1 \pmod 4$ and the existence of $z_i \in \mathbb{Z}$ such that $p_i \mid (z_i^2 + 1)$, then

(a) the product of p_i is also congruent to $1 \pmod 4$;

(b) the product of p_i divides the product of their respective $(z_i^2 + 1)$.

Solution: (a) Recall that one of the properties of modular arithmetic is that if $a_1 \equiv b_1 \pmod n$ and $a_2 \equiv b_2 \pmod n$, then we have

$$a_1 a_2 \equiv b_1 b_2 \pmod n.$$

Here we have

$$\begin{aligned} p_1 &\equiv 1 \pmod 4, \\ p_2 &\equiv 1 \pmod 4, \\ &\dots \\ p_n &\equiv 1 \pmod 4, \end{aligned}$$

and consequently

$$\begin{aligned} \prod_{i=1}^{n} p_i &\equiv 1^n \pmod 4 \\ &\equiv 1 \pmod 4, \end{aligned}$$

as desired.

(b) If $p_i \mid (z_i^2 + 1)$, then $(z_i^2 + 1)$ must be k_i multiples of p_i, where k_i are positive integers:

$$k_i p_i = z_i^2 + 1.$$

Therefore we have

$$\begin{aligned} k_1 p_1 &= z_1^2 + 1, \\ k_2 p_2 &= z_2^2 + 1, \\ &\dots \\ k_n p_n &= z_n^2 + 1, \end{aligned}$$

and consequently

$$\prod_{i=1}^{n} k_i p_i = \prod_{i=1}^{n} (z_i^2 + 1),$$

implying that the product of p_i divides the product of $(z_i^2 + 1)$, as desired.

■

Problem 3.2.4

With respect to Dr. Zieschang's Lemma 2.5, find out the z numbers for prime numbers $101, 113, 157, 137$ and 149.

Solution: (a) For prime number 101, we observe that $101 \equiv 1 \pmod{4}$. Lemma 2.5 guarantees that $\exists z \in \mathbb{Z}$ such that $101 \mid z^2 + 1$. This implies that $z^2 + 1$ must be an n-multiple of 101, with $n \in \mathbb{Z}$:

$$\begin{aligned} 101n &= z^2 + 1 \\ n &= \frac{z^2 + 1}{101}. \end{aligned}$$

Substituting y for n and x for z, we observe that $y = \frac{x^2+1}{101}$ is actually a simple quadratic function with x as independent variable and y as dependent variable. Using graphic calculator's simple table feature, we can easily input integers into x, and specifically look for y values that are integers. Here we find that $y(10) = 1$. Hence $z = 10$ for prime number 101.

(b) Similarly for prime number 113, we have $113 \equiv 1 \pmod{4}$, and from

$$y = \frac{x^2 + 1}{113}$$

we find out that its z values is 15.

(c) Using the same method, we have 28, 100 and 44 as z values for prime numbers $157, 137$ and 149, respectively.

■

3.3 Theorems of Euler, Fermat and Wilson

Problem 3.3.1

Using Lemma 3.4 (i) from Dr. Zieschang's class note, find the last digit of expansion of 55^5.

Solution: Recall Lemma 3.1 (i) on Euler's theorem: If a and n are positive integers such that $gcd(a, n) = 1$, then

$$a^{\varphi(n)} \equiv 1 \pmod{n},$$

where $\varphi(n)$ is the Euler's totient function that counts the positive integers less than or equal to n that are relatively prime to n. For examples, $\varphi(5) = 4$ because out of 5 digits of $1, 2, 3, 4, 5$, there are only 4 of them relatively prime to 5:

$$gcd(5, 1) = 1,$$
$$gcd(5, 2) = 1,$$
$$gcd(5, 3) = 1,$$
$$gcd(5, 4) = 1,$$
$$gcd(5, 5) = 5,$$

where 5 is the only one that is not co-prime with 5.

Here we need to solve $55^5 \equiv x \pmod{10}$ for x by using the Euler's theorem:

$$a^{\varphi(n)} \equiv 1 \pmod{10}.$$

We note that $\varphi(10) = 4$ because only 4 out of the 10 numbers are co-prime with 10. Note also since $\gcd(55, 10) \neq 1$, we have to break up 55 into $5 \cdot 11$ and use only 11:

$$11^{\varphi(n)} \equiv 1 \pmod{10}$$
$$11^4 \equiv 1 \pmod{10}.$$

Then we have

$$\begin{aligned} 55^5 &= 5^5 \cdot 11^5 \\ &= 5^5 \cdot 11^4 \cdot 11 \\ &\equiv 5^5 \cdot 1 \cdot 11 \pmod{10} \\ &\equiv 5^5 \cdot 11 \pmod{10} \\ &\equiv 34375 \pmod{10} \\ &\equiv (34370 + 5) \pmod{10} \\ &\equiv 5 \pmod{10}, \end{aligned}$$

consequently the last digit of 55^5 is 5.

■

Problem 3.3.2

Using the same lemma as above, find the last two digits of 3333^{4444}.

Solution: Here we first have to solve $3333^{4444} \equiv x \pmod{100}$ for x using Euler's theorem:

$$a^{\varphi(100)} \equiv 1 \pmod{100}.$$

Since we note that $gcd(3333, 100) = 1$, we can use 3333 for the a in Lemma 3.4 (i):

$$3333^{\varphi(100)} \equiv 1 \pmod{100}.$$

Next we need to find $\varphi(100)$:

$$\varphi(100) = \varphi(2^2)\varphi(5^2).$$

Recall the theorem for finding $\varphi(p^k)$:

$$\varphi(p^k) = p^k(1 - \frac{1}{p}),$$

hence

$$\begin{aligned}\varphi(2^2) &= 2^2(1-\frac{1}{2})\\ &= 4(\frac{1}{2})\\ &= 2,\end{aligned}$$

and

$$\begin{aligned}\varphi(5^2) &= 5^2(1-\frac{1}{5})\\ &= 25(\frac{4}{5})\\ &= 20,\end{aligned}$$

consequently

$$\begin{aligned}\varphi(100) &= \varphi(2^2)\varphi(5^2)\\ &= 2\cdot 20\\ &= 40.\end{aligned}$$

Therefore we have

$$3333^{40} \equiv 1 \pmod{100}.$$

Then we have

$$\begin{aligned}3333^{4444} &= (3333^{40})^{111}\cdot(3333)^4\\ &\equiv (1)^{111}\cdot(3333)^4 \pmod{100}\\ &\equiv (3333)^4 \pmod{100}\\ &\equiv (3300+33)^4 \pmod{100}\\ &\equiv 33^4 \pmod{100}\\ &\equiv 1185921 \pmod{100}\\ &\equiv (1185900+21) \pmod{100}\\ &\equiv 21 \pmod{100},\end{aligned}$$

consequently, the last 2 digits of 3333^{4444} is 2 and 1.

■

Problem 3.3.3

Show that the inverse of $5 \pmod{101}$ is 5^{99}.

Solution: Recall Lemma 3.4 (ii) on Fermat's theorem: If p is a prime, a any integer and $p \nmid a$, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Since 101 is prime and $5 \nmid 101$, then according to Fermat's theorem

$$\begin{aligned} 5^{101-1} &\equiv 1 \pmod{101} \\ 5^{100} &\equiv 1 \pmod{101} \\ 5 \cdot 5^{99} &\equiv 1 \pmod{101}, \end{aligned}$$

implying that the inverse of $5 \pmod{101}$ is 5^{99}.

■

Problem 3.3.4

Calculate $2^{234} \pmod{11}$, using only Fermat's theorem.

Solution: Since $gcd(2, 11) = 1$, therefore by Fermat's theorem

$$\begin{aligned} 2^{11-1} &\equiv 1 \pmod{11}, \\ 2^{10} &\equiv 1 \pmod{11}. \end{aligned}$$

We now break down the exponent as quotient and remainder:

$$345 = 34 \cdot 10 + 5,$$

therefore

$$\begin{aligned}2^{345} &= 2^{34\cdot 10+5}\\ &= (2^{10})^{34}\cdot 2^5\\ &\equiv 1^{34}\cdot 2^5 \pmod{11}\\ &\equiv 32 \pmod{11}\\ &\equiv (22+10) \pmod{11}\\ &\equiv 10 \pmod{11}.\end{aligned}$$

■

Problem 3.3.5

Using only the modular multiplicative inverse and Wilson's theorem, verify that 13 is a prime number.

Solution: Recall Lemma 3.6 on Wilson's theorem: A positive integer n is prime if and only if $(n-1)! \equiv -1 \pmod{n}$. Recall also that the modular multiplicative inverse of an integer a modulo m is an integer a^{-1} such that

$$aa^{-1} \equiv 1 \pmod{m}.$$

Having recalled the above results, we need to prove that

$$(13-1)! \equiv -1 \pmod{13}.$$

Here we have

$$\begin{aligned}(13-1)! &= 12!\\ &= 1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8\cdot 9\cdot 10\cdot 11\cdot 12,\end{aligned}$$

and the modulo 13 inverse of some of the numbers are:

$$\begin{aligned}
2 \cdot 7 &\equiv 1 \pmod{13} \\
3 \cdot 9 &\equiv 1 \pmod{13} \\
4 \cdot 10 &\equiv 1 \pmod{13} \\
5 \cdot 8 &\equiv 1 \pmod{13} \\
6 \cdot 11 &\equiv 1 \pmod{13}.
\end{aligned}$$

Rearranging the numbers, we have

$$\begin{aligned}
(13-1)! &\equiv 1 \cdot (2 \cdot 7) \cdot (3 \cdot 9) \cdot (4 \cdot 10) \cdot (5 \cdot 8) \cdot (6 \cdot 11) \cdot 12 \pmod{13} \\
&\equiv 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 12 \pmod{13} \\
&\equiv 12 \pmod{13} \\
&\equiv (12 - 13) \pmod{13} \\
&\equiv -1 \pmod{13},
\end{aligned}$$

as desired.

■

Problem 3.3.6

What is the remainder of $97!$ when it is divided by 101?

Solution: Here we need to apply Wilson's theorem:

$$\begin{aligned}(101-1)! &\equiv -1 \pmod{101}\\ 100! &\equiv -1 \pmod{101}\\ 97!\cdot 98\cdot 99\cdot 100 &\equiv -1 \pmod{101}\\ 97!(98-101)(99-101)(100-101) &\equiv -1 \pmod{101}\\ 97!(-3)(-2)(-1) &\equiv -1 \pmod{101}\\ 97!\cdot 6 \equiv 1 &\pmod{101}.\end{aligned}$$

We know that the modular inverse of 6 modulo 101 is 17:

$$17\cdot 6\equiv 1 \pmod{101},$$

therefore

$$\begin{aligned}97!\cdot 17\cdot 6 &\equiv 17 \pmod{101}\\ 97!\cdot 1 &\equiv 17 \pmod{101}\\ 97! &\equiv 17 \pmod{101}.\end{aligned}$$

Therefore, $97!$ has remainder of 17 when divided by 101.

■

3.4 Quadratic Number Fields

Problem 3.4.1

If $\alpha, \beta \in \mathbb{Q}[\sqrt{2}]$, prove the following properties of conjugation σ:

(a) $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$,

(b) $\sigma(\alpha \cdot \beta) = \sigma(\alpha) \cdot \sigma(\beta)$,

(c) $\sigma(\sigma(\alpha)) = \alpha$.

Solution: (a) Recall that Dr. Zieschang's note defines

$$\sigma(x + y\sqrt{d}) := x - y\sqrt{d},$$

where the elements $x + y\sqrt{d}$ and $x - y\sqrt{d}$ are called the conjugates.

Let's assume the followings:

$$\alpha = a_1 + b_1\sqrt{d},$$

$$\beta = a_2 + b_2\sqrt{d}.$$

$$\alpha + \beta = (a_1 + a_2) + (b_1 + b_2)\sqrt{d}.$$

Therefore

$$\begin{aligned}\sigma(\alpha + \beta) &= (a_1 + a_2) - (b_1 + b_2)\sqrt{d} \\ &= (a_1 - b_1\sqrt{d}) + (a_2 - b_2\sqrt{d}) \\ &= \sigma(\alpha) + \sigma(\beta),\end{aligned}$$

as desired.

(b) For multiplication of α and β, we have

$$\begin{aligned}\alpha\beta &= (a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d}) \\ &= (a_1a_2 + b_1b_2d) + (a_1b_2 + a_2b_1)\sqrt{d},\end{aligned}$$

and there

$$\begin{aligned}\sigma(\alpha\beta) &= (a_1a_2 + b_1b_2d) - (a_1b_2 + a_2b_1)\sqrt{d} \\ &= a_1a_2 - a_1b_2\sqrt{d} - a_2b_1\sqrt{d} + b_1b_2(\sqrt{d})^2 \\ &= (a_1 - b_1\sqrt{d})(a_2 - b_2\sqrt{d}) \\ &= \sigma(\alpha)\sigma(\beta),\end{aligned}$$

as desired.

(c) For conjugate of α:

$$\begin{aligned}\sigma(\alpha) &= a_1 - b_1\sqrt{d} \\ \sigma(\sigma(\alpha)) &= \sigma(a_1 - b_1\sqrt{d}) \\ &= a_1 + b_1\sqrt{d} \\ &= \alpha,\end{aligned}$$

as desired.

■

Problem 3.4.2

For any $\alpha \in \mathbb{Q}[\sqrt{d}]$ and $\beta \in \mathbb{Q}[\sqrt{d}]$, show that trace τ is additive while norm ν is multiplicative, that is:

$$\tau(\alpha + \beta) = \tau(\alpha) + \tau(\beta)$$

but

$$\nu(\alpha\beta) = \nu(\alpha)\nu(\beta).$$

Solution: We recall that in Dr. Zieschang's note, trace τ and norm ν are defined respectively as

$$\begin{aligned}\tau(z) &:= z + \sigma(z) \\ \nu(z) &:= z\sigma(z),\end{aligned}$$

where $\sigma(z)$ denotes the conjugate of $z = (x + y\sqrt{d})$.

Let's assume, as in the previous exercise, that

$$\begin{aligned}\alpha &= a_1 + b_1\sqrt{d},\\ \beta &= a_2 + b_2\sqrt{d},\\ (\alpha+\beta) &= (a_1+a_2) + (b_1+b_2)\sqrt{d}.\end{aligned}$$

Therefore

$$\begin{aligned}\tau(\alpha) &= a_1 + b_1\sqrt{d} + a_1 - b_1\sqrt{d}\\ &= 2a_1,\\ \tau(\beta) &= a_2 + b_2\sqrt{d} + a_2 - b_2\sqrt{d}\\ &= 2a_2,\\ \sigma(\alpha+\beta) &= (a_1+a_2) - (b_1+b_2)\sqrt{d}.\end{aligned}$$

Consequently,

$$\begin{aligned}\tau(\alpha+\beta) &= (a_1+a_2) + (b_1+b_2)\sqrt{d} + (a_1+a_2) - (b_1+b_2)\sqrt{d}\\ &= 2a_1 + 2a_2\\ &= \tau(\alpha) + \tau(\beta),\end{aligned}$$

as desired.

For product of α and β, we have

$$\begin{aligned}\alpha\beta &= (a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d})\\ &= (a_1a_2 + b_1b_2d) + (a_1b_2 + a_2b_1)\sqrt{d},\end{aligned}$$

and

$$\begin{aligned}\nu(\alpha) &= (a_1 + b_1\sqrt{d})(a_1 - b_1\sqrt{d}) \\ &= a_1^2 - b_1^2 d, \\ \nu(\beta) &= (a_2 + b_2\sqrt{d})(a_2 - b_2\sqrt{d}) \\ &= a_2^2 - b_2^2 d.\end{aligned}$$

Consequently,

$$\begin{aligned}\nu(\alpha\beta) &= \left[(a_1a_2 + b_1b_2d) + (a_1b_2 + a_2b_1)\sqrt{d}\right]\left[(a_1a_2 + b_1b_2d) - (a_1b_2 + a_2b_1)\sqrt{d}\right] \\ &= (a_1a_2 + b_1b_2)^2 - (a_1b_2 + a_2b_1)^2 d \\ &= (a_1a_2)^2 + 2(a_1a_2b_1b_2) + (b_1b_2)^2 - (a_1b_2)^2 d - 2(a_1a_2b_1b_2)d - (a_2b_1)^2 d \\ &= (a_1a_2)^2 - (a_1b_2)^2 d - (a_2b_1)^2 d + (b_1b_2)^2 \\ &= (a_1^2 - b_1^2 d)(a_2^2 - b_2^2 d) \\ &= \nu(\alpha)\nu(\beta),\end{aligned}$$

as desired.

■

Problem 3.4.3

Show that

$$z = (\frac{73}{2} + \frac{3}{2}\sqrt{109}) \in \mathbb{Q}[\sqrt{109}]$$

is integral over $\mathbb{Z}$.

Solution: (a) Recall Dr. Zieschang's theorem 4.5 (ii): If $d \equiv 1 \pmod 4$, then

$$I_{\mathbb{Q}[\sqrt{d}]}(\mathbb{Z}) = \left\{\frac{v}{2} + \frac{w}{2}\sqrt{d} \mid v, w \in \mathbb{Z};\ v \equiv w \pmod 2\right\}.$$

Here we have square-free $d = 109 \equiv 1 \pmod 4$, with $v = 73$, $w = 3$ and $73 \equiv 3 \pmod 2$. Thus theorem 4.8 (ii) guarantees that z is integral over $\mathbb{Z}$.

Indeed,

$$
\begin{aligned}
\sigma(z) &= \left(\frac{73}{2} - \frac{3}{2}\sqrt{109}\right), \\
\tau(z) &= z + 6z \\
&= \left(\frac{73}{2} + \frac{3}{2}\sqrt{109}\right) + \left(\frac{73}{2} - \frac{3}{2}\sqrt{109}\right) \\
&= 73 \in \mathbb{Z},
\end{aligned}
$$

and

$$
\begin{aligned}
\nu(z) &= z\sigma(z) \\
&= \left(\frac{73}{2} + \frac{3}{2}\sqrt{109})(\frac{73}{2} - \frac{3}{2}\sqrt{109}\right) \\
&= \left(\frac{73}{2}\right)^2 - \left(\frac{3}{2}\sqrt{109}\right)^2 \\
&= \frac{5329}{4} - \frac{981}{4} \\
&= 1087 \in \mathbb{Z}.
\end{aligned}
$$

Here, since $\tau(z)$ and $\nu(z)$ are integral, Lemma 7.3 guarantees that $\mathbb{Z}$ is integral over $\mathbb{Z}$.

■

Problem 3.4.4

Show that z, as defined below, is integral over $\mathbb{Z}$:

$$
z \in \left\{ a + b(\frac{1+\sqrt{d}}{2}) \ \mid \ a, b \in \mathbb{Z};\ d \equiv 1 \pmod 4 \right\}.
$$

Solution: To solve this problem, we will use Dr. Zieschang's Lemma 4.7: An element $z \in \mathbb{Q}[\sqrt{d}]$ is integral over $\mathbb{Z}$ if and only if $\tau(z)$ and $\nu(z)$ are integral.

Here we have

$$
\begin{aligned}
z &= \left(a + b(\frac{1+\sqrt{d}}{2})\right) \\
&= \left((a + \frac{b}{2}) + \frac{b}{2}\sqrt{d}\right),
\end{aligned}
$$

and

$$\sigma(z) = \left((a + \frac{b}{2}) - \frac{b}{2}\sqrt{d}\right),$$

hence the trace of z:

$$\begin{aligned}\tau(z) &= z + \sigma(z)\\ &= \left[(a + \frac{b}{2}) + \frac{b}{2}\sqrt{d}\right] + \left[(a + \frac{b}{2}) - \frac{b}{2}\sqrt{d}\right]\\ &= \left(a + \frac{b}{2}\right) + \left(a + \frac{b}{2}\right)\\ &= (2a + b) \in \mathbb{Z}.\end{aligned}$$

Additionally, we have the norm of z:

$$\begin{aligned}\nu(z) &= z\sigma(z)\\ &= \left[(a + \frac{b}{2}) + \frac{b}{2}\sqrt{d}\right]\left[(a + \frac{b}{2}) - \frac{b}{2}\sqrt{d}\right]\\ &= \left(a + \frac{b}{2}\right)^2 - \frac{b^2 d}{4}\\ &= a^2 + ab + \frac{b^2}{4} - \frac{b^2 d}{4}\\ &= a^2 + ab + \frac{b^2(1-d)}{4}.\end{aligned}$$

Since $d \equiv 1 \pmod 4$, therefore $4 \mid (d-1)$, hence $4 \mid b^2(1-d)$ and also

$$\nu(z) = a^2 + ab + \frac{b^2(1-d)}{4} \in \mathbb{Z},$$

consequently z is integral over $\mathbb{Z}$, as desired.

■

Problem 3.4.5

Show that the sum of $z_1 \in \mathbb{Q}[\sqrt{d}]$ and $z_2 \in \mathbb{Q}[\sqrt{d}]$, as defined below, with each of them integral over $\mathbb{Z}$, is again integral over $\mathbb{Z}$:

$$\begin{aligned} z_1 &= \left(a + b\left(\frac{1+\sqrt{d}}{2}\right)\right), \\ z_2 &= \left(\frac{v}{2} + \frac{w}{2}\sqrt{d})\right), \end{aligned}$$

where $a, b, v, w, d \in \mathbb{Z}$, and $d \equiv 1 \pmod 4),\ v \equiv w \pmod 2)$.

Solution: Again as in the previous solutions, we will take the advantage of Lemma 4.7:

$$\begin{aligned} z_1 + z_2 &= \left(a + b\left(\frac{1+\sqrt{d}}{2}\right)\right)\left(\frac{v}{2} + \frac{w}{2}\sqrt{d}\right) \\ &= \left(a + \frac{b}{2} + \frac{v}{2}\right) + \left(\frac{b}{2} + \frac{w}{2}\right)\sqrt{d}, \end{aligned}$$

and

$$\sigma(z_1 + z_2) = \left(a + \frac{b}{2} + \frac{v}{2}\right) - \left(\frac{b}{2} + \frac{w}{2}\right)\sqrt{d}.$$

First we need to find the trace of $z_1 + z_2$:

$$\begin{aligned} \tau(z_1 + z_2) &= (z_1 + z_2) + \sigma(z_1 + z_2) \\ &= 2\left(a + \frac{b}{2} + \frac{v}{2}\right) \\ &= 2a + b + v \\ &\in \mathbb{Z}. \end{aligned}$$

Next, we compute the norm of $z_1 + z_2$:

$$\begin{aligned} \nu(z_1 + z_2) &= (z_1 + z_2)\sigma(z_1 + z_2) \\ &= \left(a + \frac{b}{2} + \frac{v}{2}\right)^2 - \left((\frac{b}{2} + \frac{w}{2})\sqrt{d}\right)^2 \\ &= \left(a^2 + b + v + \frac{(b+v)^2}{4} - \frac{(b+w)^2 d}{4}\right) \\ &= \left(a^2 + b + v + \frac{(v^2 - w^2) + 2b(v-w)}{4}\right). \end{aligned}$$

Since $a^2, b, v \in \mathbb{Z}$, we need only to prove that the last term from the above expression is integral, more specifically we need to prove:

$$4 \mid (v^2 - w^2) + 2b(v - w).$$

Here we will take advantage of the fact given by the problem that $v \equiv w \pmod 2$, implying that $2 \mid (v - w)$ and $2 \mid (v + w)$. Then we have

$$\frac{(v^2 - w^2) + 2b(v - w)}{4} = \frac{(v - w)(v + w) + 2b(v - w)}{4}.$$

Since $2 \mid (v - w)$ and $2 \mid (v + w)$, therefore $4 \mid (v - w)(v + w)$. Since $2 \mid (v - w)$, therefor $4 \mid 2b(v - w)$. Hence $\sigma(z_1 + z_2) \in \mathbb{Z}$. Consequently $z_1 + z_2$ is integral over $\mathbb{Z}$ since both its trace and norm are integral, as desired.

■

3.5 The Ring of the Gaussian Integers

Problem 3.5.1

Show that the equations

$$x^2 + 4x - 22 = 0,$$

$$x^2 + 2xy + y^2 - 63 = 0$$

where $x, y \in \mathbb{Z}^+$, do not have integer solution.

Solution: Recall Dr. Zieschang's Theorem 5.8 in his classnote: Let x be a positive integer. Then $x^2 + 1$ is not a cube.

(a) In the first equation, we have

$$\begin{aligned} x^2 + 4x - 22 &= 0 \\ (x^2 + 4x + 4) + 1 &= 27 \\ (x+2)^2 + 1 &= 3^3, \end{aligned}$$

which does not have positive integer solution according to Theorem 5.8. Indeed, let $\mathcal{D}$ be the discriminant of the above quadratic equation, then

$$\mathcal{D} = b^2 - 4ac = 4^2 - (4)(1)(-22) = 104,$$

which is not a perfect square number, implying that the equation does not have integer solution.

(b) On the second equation, we have

$$\begin{aligned} x^2 + 2xy + y^2 - 63 &= 0 \\ (x^2 + 2xy + y^2) + 1 &= 64 \\ (x+y)^2 + 1 &= 4^3, \end{aligned}$$

which according to Theorem 5.8 does not have integer solution for x and y.

■

Problem 3.5.2

Show that

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2 = 35$$

has integer solutions that are unique.

Solution: Recall Dr. Zieschang's Corollary 5.6 on Fermat Theorem: Let p be an odd prime number. Then p is the sum of two integer squares if and only if $p \equiv 1 \pmod 4$.

We have 35 as the sum of three prime numbers:

$$35 = 5 + 13 + 17,$$

and each of the above primes is congruent to 1 modulo 4:

$$\begin{aligned} 5 &\equiv 1 \pmod 4, \\ 13 &\equiv 1 \pmod 4, \\ 17 &\equiv 1 \pmod 4. \end{aligned}$$

Therefore, Corollary 5.6 guarantees that these equations have integer solutions:

$$\begin{aligned} x_1^2 + x_2^2 &= 5, \\ x_3^2 + x_4^2 &= 13, \\ x_5^2 + x_6^2 &= 17, \end{aligned}$$

hence $x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2 = 35$ has integer solution, as desired. Indeed,

$$\begin{aligned} (\pm 1)^2 + (\pm 2)^2 &= 5, \\ (\pm 2)^2 + (\pm 3)^2 &= 13, \\ (\pm 1)^2 + (\pm 4)^2 &= 17. \end{aligned}$$

Next, we need to show that the solutions are unique. Recall Lemma 5.7 in Dr. Zieschang's note:

Let p be a prime with $p \equiv 1 \pmod 4$. Then there is only one way to write p as a sum of two squares. Consequently, solutions to x_1, x_2, x_3, x_4, x_5, and x_6 are unique up to their parity.

■

Problem 3.5.3

Find out if the followings are *Gaussian* primes:

$$3 + 4i,\ 3 - 4i,\ 5i,\ -11i,\ 13 + 2i.$$

Solution: Recall Dr. Zieschang's Theorem 5.2, 5.3 and 5.4 which can be summarized as follows: For $z = (a + bi) \in \mathbb{Z}[i]$, then z is prime:

(i) if $a \neq 0$ and $b = 0$ and if $|a|$ is prime number satisfying $|a| \equiv 3 \pmod 4$. The associates of z after multiplication by units ± 1 are also prime.

(ii) if $a = 0$ and $b \neq 0$ and if $|b|$ is prime number satisfying $|b| \equiv 3 \pmod 4$. Its associates after multiplication by units $\pm i$ are also prime.

(iii) if $a \neq 0$ and $b \neq 0$ and if the norm of z, $\mathcal{N}(a + bi)$, is prime number.

(a) For $3 + 4i$, we have

$$\begin{aligned} \mathcal{N}(3 + 4i) &= 9 + 16 \\ &= 25 \\ &= 5^2. \end{aligned}$$

Since 25 is not real prime therefore $3 + 4i$ is not *Gaussian* prime. For the same reason, its conjugate $3 - 4i$ is also not prime.

(b) Next, for $5i$, since

$$|5| \not\equiv 3 \pmod 4$$

therefore $5i$ is not prime.

(c) For $-11i$, however, since

$$|-11| \equiv 3 \pmod 4,$$

therefore $-11i$ is prime. Its associates:

$$(-11i)(i) = 11,$$
$$(-11i)(-i) = -11$$

are also prime.

(d) Finally for $13 + 2i$, since

$$\begin{aligned}\mathcal{N}(13+2i) &= 13^2 + 2^2 \\ &= 173,\end{aligned}$$

which is real prime, therefore $13 + 2i$ is *Gaussian* prime.

■

Problem 3.5.4

Find out all *Gaussian* primes with norm $\mathcal{N}$ less than 30.

Solution: Here we need to recall again summary of Theorem 5.2, 5.3 and 5.4 from the previous exercise.

For $z = (a + 0i)$, we have to find real prime a such that $a \equiv 3 \pmod 4$ and $a^2 < 30$. Here we have

$$a = 4k + 3$$

where $k \in \mathbb{Z}^+$. Therefore we have

$$(4k+3)^2 < 30.$$

By observation, from $k \in \{0, 1\}$ we get $a \in \{3, 7\}$ together with their associates.

Using the same analysis, for $z = (0 + bi)$ we get $b \in \{3i, 7i\}$ together with their associates.

For $z = (a + bi)$, we have to find out $a, b \in \mathbb{Z}$ such that

$$\begin{aligned}\mathcal{N}(a+bi) &= a^2 + b^2 \\ &= p \\ &< 30,\end{aligned}$$

where p is prime number. Recall that by Corollary 5.6 of Fermat Theorem, p has to satisfy $p \equiv 1 \pmod 4$ in order to be the sum of two square integrals.

Here we have

$$p = 4k + 1:$$

(a) For $k = 1$, we get $p = 5$. Since $2^2 + 1^2 = 5 < 30$, we have $1 \pm 2i$ and $2 \pm i$ and their respective associates as solutions.

(b) For $k = 2$, we get $p = 9$ which is not prime number.

(c) For $k = 3$, we get $p = 13 < 30$, where $3^2 + 2^2 = 13$. Therefore we have $3 \pm 2i$ and $2 \pm 3i$ and their respective associates as solutions.

(d) For $k = 4$, we get $p = 17 < 30$, where $4^2 + 1^2 = 17$. Therefore we have $4 \pm i$ and $1 \pm 4i$ and their respective associates as solutions.

(e) For $k = 5$, we get $p = 21$ which is not prime.

(f) For $k = 6$, we get $p = 25$ which is not prime.

(g) For $k = 7$, we get $p = 29 < 30$ where $5^2 + 2^2 = 29$, hence we have $5 \pm 2i$ and $2 \pm 5i$ and their respective associates as solutions.

■

3.6 Pythagorean Triples

Problem 3.6.1

Show that $(3, 4, 5)$ is the only Pythagorean triple consisting of consecutive integers .

Solution: Assume that $((n-k), n, (n+k))$ is the consecutive Pythagorean triple, with $n, k \in \mathbb{Z}^{+}$. Therefore we have

$$(n-k)^2 + n^2 = (n+k)^2$$

$$n^2 - 2kn + k^2 + n^2 = n^2 + 2kn + k^2$$

$$n^2 = 4kn$$

$$n = 4k.$$

Next, substituting the result from above to the triple, we then have

$$((4k-k), 4k, (4k+k)),$$

which simplifies into

$$(3k, 4k, 5k).$$

Finally, substituting the smallest value of k, that is $k = 1$, will give us the primitive $(3, 4, 5)$. Substituting with $k > 1$ will only give us k-multiple of the above primitive. Hence $(3, 4, 5)$ is the only Pythagorean triple consisting of consecutive integers.

■

Problem 3.6.2

Show that where (x, y, z) is a Pythagorean triple, then $12 \mid xy$.

Solution: Recall from Dr. Zieschang's Lemma 6.1, that the generators of Pythagorean triple are

$$x = b^2 - a^2,$$

$$y = 2ab,$$

$$z = b^2 + a^2,$$

where $a, b \in \mathbb{Z}^+$, $gcd(a, b) = 1$, and $b \not\equiv a \pmod 2$.

First, we need to prove that $4 \mid xy$, that is, the following is true:

$$4 \mid 2ab(b^2 - a^2).$$

Here, we see that if both a and b are even, or if either a or b is even, then we are done because obviously $4 \mid 2ab$. If, on the other hand, a and b are both odd, then suppose that

$$a = 2p + 1, p \in \mathbb{Z},$$

$$b = 2q + 1, q \in \mathbb{Z}.$$

These lead to

$$\begin{aligned} b^2 - a^2 &= (2p + 1)^2 - (2q + 1)^2 \\ &= (4p^2 + 4p + 1) - (4q^2 + 4q + 1) \\ &= 4(p^2 + p - q^2 - q), \end{aligned}$$

consequently $4 \mid (b^2 - a^2)$, as desired.

Secondly we need to show that $3 \mid 2ab(b^2 - a2)$. Here we will use the fact that for any $z \in \mathbb{Z}$, then it is either

$$z \equiv 0 \pmod 3 \Longrightarrow z = 3p, \text{ where } p \in \mathbb{Z}$$

or

$$z \equiv \pm 1 \pmod 3 \Longrightarrow z = 3p \pm 1.$$

Here we see that if both a and b are 0 modulo 3, or if either one of them is 0 modulo 3, then we are done because then obviously $3 \mid 2ab$.

If, on the other hand, $a \equiv \pm 1 \pmod 3$ and also $b \equiv \pm 1 \pmod 3$, then obviously $3 \nmid 2ab$. But looking at $(b^2 - a^2)$, assuming that

$$a = 3p \pm 1, p \in \mathbb{Z},$$

$$b = 3q \pm 1, q \in \mathbb{Z},$$

then we have

$$\begin{aligned} b^2 - a^2 &= (3p \pm 1)^2 - (3q \pm 1)^2 \\ &= 9p^2 \pm 6p + 1 - (9q^2 \pm 6q + 1) \\ &= 9p^2 \pm 6p - 9q^2 \pm 6q \\ &= 3(3p^2 \pm 2p - 3q^2 \pm 2q), \end{aligned}$$

hence $3 \mid (b^2 - a^2)$, as desired.

Having proven that $4 \mid 2ab(b^2 - a^2)$ and $3 \mid 2ab(b^2 - a^2)$, then $12 \mid 2ab(b^2 - a^2)$, that is, $12 \mid xy$, as desired.

$\blacksquare$

Problem 3.6.3

Prove that where (x, y, z) is Pythagorean triple, then $60 \mid xyz$.

Solution: Recall the generators of Pythagorean triple from previous exercise:

$$x = b^2 - a^2,$$

$$y = 2ab,$$

$$z = b^2 + a^2,$$

where $a, b \in \mathbb{Z}^+$, $gcd(a, b) = 1$, and $b \not\equiv a \pmod 2$.

Recall also from the previous exercise, that we have shown that $12 \mid xy$, therefore we need only to prove that $5 \mid xyz$. We will still be using Dr. Zieschang's Lemma 6.1 referred to by the previous exercise. As in the previous problem, here we will take advantage of the fact that for any $z \in \mathbb{Z}$, then z has to be one of the followings:

$$\begin{aligned} z &\equiv 0 \pmod 5 \Longrightarrow z = 5p, \text{ where } p \in \mathbb{Z}, \\ z &\equiv \pm 1 \pmod 5 \Longrightarrow z = 5p \pm 1, \text{or} \\ z &\equiv \pm 2 \pmod 5 \Longrightarrow z = 5p \pm 2. \end{aligned}$$

We will present 4 possible cases as follows:

(a) The first case: Either $a \equiv 0 \pmod 5$ or $b \equiv 0 \pmod 5$, or both $a \equiv 0 \pmod 5$ and $b \equiv 0 \pmod 5$. Then we are done because this implies:

$$5 \mid 2ab \Longrightarrow 5 \mid y \Longrightarrow 60 \mid xyz,$$

as desired.

(b) The second case: Both $a \equiv \pm 1 \pmod 5$ and $b \equiv \pm 1 \pmod 5$, that is $a = 5p \pm 1$ and $b = 5q \pm 1$. Then we have

$$\begin{aligned} b^2 - a^2 &= (5p \pm 1)^2 - (5q \pm 1)^2 \\ &= 25p^2 \pm 10p + 1 - (25q^2 \pm 10q + 1) \\ &= 25p^2 \pm 10p - 25q^2 \pm 10q \\ &= 5(5p^2 \pm 2p - 5q^2 \pm 2q), \end{aligned}$$

hence we conclude

$$5 \mid (b^2 - a^2) \Longrightarrow 5 \mid x \Longrightarrow 60 \mid xyz.$$

(c) The third case: Both $a \equiv \pm 2 \pmod 5$ and $b \equiv \pm 2 \pmod 5$, that is $a = 5p \pm 2$ and $b = 5q \pm 2$. If this is the case then the analysis will proceed similar to the second case above, leading again to conclusion that

$$5 \mid (b^2 - a^2) \Longrightarrow 5 \mid x \Longrightarrow 60 \mid xyz.$$

(d) The final case: One of them is congruent to ± 1 modulo 5 while the other is congruent to ± 2

modulo 5. Without loss of generality, let's us assume that

$$a = 5p \pm 1,$$
$$b = 5q \pm 2.$$

Then

$$\begin{aligned} z &= b^2 + a^2 \\ &= (5q \pm 2)^2 + (5p \pm 1)^2 \\ &= (25q^2 \pm 20q + 4) + (25p^2 \pm 10p + 1) \\ &= 5(5q^2 \pm 4q + 5p^2 \pm 2p + 1), \end{aligned}$$

implying that

$$5 \mid (b^2 + a^2) \Longrightarrow 5 \mid z \Longrightarrow 60 \mid xyz,$$

as desired.

■

Problem 3.6.4

Suppose that (x, y, z) is a set of Pythagorean triple. Show that $y + z$ is always a perfect square number.

Solution: Recall the generators of Pythagorean triple from previous exercise:

$$x = b^2 - a^2,$$
$$y = 2ab,$$
$$z = b^2 + a^2,$$

where $a, b \in \mathbb{Z}^+$, $gcd(a, b) = 1$, and $b \not\equiv a \pmod 2$. Then it's easy to see that $y + z = a^2 + 2ab + b^2 = (a + b)^2$. Hence the sum of y and z is always a perfect square number, as desired.

■

Problem 3.6.5

Suppose that 115 and 277 belong to a Pythagorean triple, find out the triple's a and b integers.

Solution: Recall Dr. Zieschang's Lemma 6.1: The triple

$$\big((b^2 - a^2), 2ab, (b^2 + a^2)\big)$$

where $a, b \in \mathbb{Z}^+$, is the generator of a Pythagorean triple if and only if $gcd(a, b) = 1$ and $b \not\equiv a \pmod 2$.

Here, since both 115 and 227 are odd, they can't be generated from $2ab$. Since $115 < 277$, therefore we have

$$a^2 - b^2 = 115$$

$$a^2 + b^2 = 277.$$

Adding up the two above equations, we obtain

$$2a^2 = 392$$

$$a = 14,$$

and therefore

$$b = 9.$$

■

Problem 3.6.6

One of the value in a certain Pythagorean triple is 84, find all possible values of the other two.

Solution: Recall the generator of Pythagorean triple cited in the previous exercise. Since 84 is an even number, it must be generated from $2ab$. Therefore we have

$$2ab = 84$$

$$ab = 42,$$

which can be factored into the following four possibilities:

(a) First, $42 = 2 \cdot 21$. Since $gcd(2, 21) = 1$ and $21 \not\equiv 2 \pmod 2$, therefore they are valid values for a and b. Hence:

$$x = 21^2 - 2^2 = 437$$

$$y = 84$$

$$z = 21^2 + 2^2 = 445.$$

Verifying:

$$437^2 + 84^2 = 198,025$$

$$445^2 = 198,025.$$

(b) Secondly, $42 = 3 \cdot 14$. Since $gcd(3, 14) = 1$ and $14 \not\equiv 3 \pmod 2$, therefore:

$$x = 14^2 - 3^2 = 187$$

$$y = 84$$

$$z = 14^2 + 3^2 = 205.$$

Verifying:

$$187^2 + 84^2 = 42,025$$

$$205^2 = 42,025.$$

(c) Next, $42 = 6 \cdot 7$. Since $gcd(6, 7) = 1$ and $7 \not\equiv 6 \pmod 2$, therefore:

$$x = 7^2 - 6^2 = 13$$

$$y = 84$$

$$z = 7^2 + 6^2 = 85.$$

Verifying:

$$13^2 + 84^2 = 7,225$$
$$85^2 = 7,225.$$

(d) Finally, $42 = 42 \cdot 1$. Since $gcd(42, 1) = 1$ and $42 \not\equiv 1 \pmod 2$, therefore:

$$x = 42^2 - 1^2 = 1763$$
$$y = 84$$
$$z = 42^2 + 1^2 = 1765.$$

Verifying:

$$1763^2 + 84^2 = 3,115,225$$
$$1765^2 = 3,115,225.$$

■

Problem 3.6.7

Repeat the above exercise with 228.

Solution: We will repeat the same steps like above for 228:

$$2ab = 228$$
$$ab = 114,$$

which can be factored int the following four possibilities:

(a) First, $114 = 2 \cdot 57$. Since $gcd(2, 57) = 1$ and $57 \not\equiv 2 \pmod 2$, therefore they are valid values for a and b. Hence:

$$x = 57^2 - 2^2 = 3,245$$
$$y = 228$$
$$z = 57^2 + 2^2 = 3,253.$$

Verifying:

$$3,245^2 + 228^2 = 10,582,009$$

$$3,253^2 = 10,582,009$$

.

(b) Secondly, $114 = 3 \cdot 38$. Since $gcd(3, 38) = 1$ and $38 \not\equiv 3 \pmod 2$, therefore:

$$x = 38^2 - 3^2 = 1,435$$

$$y = 228$$

$$z = 38^2 + 3^2 = 1,453.$$

Verifying:

$$1,435^2 + 228^2 = 2,111,209$$

$$1,453^2 = 2,111,209.$$

(c) Next, $114 = 6 \cdot 19$. Since $gcd(6, 19) = 1$ and $19 \not\equiv 6 \pmod 2$, therefore:

$$x = 19^2 - 6^2 = 325$$

$$y = 228$$

$$z = 19^2 + 6^2 = 397.$$

Verifying:

$$325^2 + 228^2 = 157,609$$

$$397^2 = 157,609.$$

(d) Finally $114 = 114 \cdot 1$. Since $gcd(114, 1) = 1$ and $114 \not\equiv 1 \pmod 2$, therefore:

$$x = 114^2 - 1^2 = 12,995$$
$$y = 228$$
$$z = 114^2 + 1^2 = 12,997.$$

Verifying:

$$12,995^2 + 228^2 = 168,922,009$$
$$12,997^2 = 168,922,009.$$

■

Problem 3.6.8

The middle value of a Pythagorean triple is 325, find out the other two values.

Solution: Since 325 is odd and a Pythagorean's middle value, therefore it must be generated by $b^2 - a^2$:

$$\begin{aligned} 325 &= b^2 - a^2 \\ &= (b-a)(b+a). \end{aligned}$$

Next, we factor 325 into three sets of pair of factors:

(a) First, $325 = 5 \cdot 65$. We set up a system of linear equations:

$$b - a = 5$$
$$b + a = 65.$$

By elimination we have $b = 35$ and $a = 30$. However these are not valid values since $gcd(35, 30) \neq 1$.

(b) Secondly, $325 = 25 \cdot 13$. The system of equations is

$$b - a = 13$$
$$b + a = 25,$$

from which we obtain $b = 19$ and $a = 6$. Since $gcd(19, 6) = 1$ and $19 \not\equiv 6 \pmod 2$, they are valid values.

Therefore,

$$x = 325$$
$$y = 2 \cdot 19 \cdot 6 = 228$$
$$z = 19^2 + 6^2 = 397.$$

Verifying: $325^2 + 228^2 = 157,609 = 397^2$.

$$325^2 + 228^2 = 157,609$$
$$397^2 = 157,609.$$

(b) Finally, $325 = 325 \cdot 1$. The system of equations is

$$b - a = 1$$
$$b + a = 325,$$

from which we obtain $b = 163$ and $a = 162$. Since $gcd(163, 162) = 1$ and $163 \not\equiv 162 \pmod 2$, they are valid values.

Therefore,

$$x = 325$$
$$y = 2 \cdot 163 \cdot 162 = 52,812$$
$$z = 163^2 + 162^2 = 52,813.$$

Verifying: $325^2 + 52,812^2 = 2,789,212,969 = 512,813^2$.

$$325^2 + 52,812^2 = 2,789,212,969$$
$$52,813^2 = 2,789,212,969.$$

■

Problem 3.6.9

Repeat the same above exercise with 575.

Solution: Since 575 is odd and a Pythagorean's middle value, therefore it must be generated by $b^2 - a^2$:

$$\begin{aligned} 575 &= b^2 - a^2 \\ &= (b-a)(b+a). \end{aligned}$$

Next, we factor 325 into three sets of pair of factors:

(a) First, we have $575 = 5 \cdot 115$. We set up a system of linear equations:

$$\begin{aligned} b - a &= 5 \\ b + a &= 115. \end{aligned}$$

By elimination we have $b = 60$ and $a = 55$. However these are not valid values since $gcd(60, 55) \neq 1$.

(b) Secondly, we have $575 = 25 \cdot 23$. The system of equations is

$$\begin{aligned} b - a &= 23 \\ b + a &= 25, \end{aligned}$$

from which we obtain $b = 24$ and $a = 1$. Since $gcd(24, 1) = 1$ and $24 \not\equiv 1 \pmod 2$, they are valid values.

Therefore,

$$x = 575$$
$$y = 2 \cdot 24 \cdot 1 = 48$$
$$z = 24^2 + 1^2 = 577.$$

Verifying:

$$575^2 + 48^2 = 167,281$$
$$577^2 = 167,281.$$

(b) Finally we have $575 = 575 \cdot 1$. The system of equations is

$$b - a = 1$$
$$b + a = 575,$$

from which we obtain $b = 288$ and $a = 287$. Since $gcd(288, 287) = 1$ and $288 \not\equiv 287 \pmod 2$, they are valid values.

Therefore,

$$x = 575$$
$$y = 2 \cdot 288 \cdot 287 = 165,312$$
$$z = 288^2 + 287^2 = 165,313.$$

Verifying:

$$575^2 + 165,312^2 = 27,328,387,970$$
$$165,313^2 = 27,328,387,970.$$

■

Problem 3.6.10

The largest value in a Pythagorean triple is 409. Find the sets of the other two values.

Solution: Since 409 is the largest value in the triple, we have

$$a^2 + b^2 = 409,$$

hence

$$b^2 = 409 - a^2$$
$$b = \sqrt{409 - a^2},$$

where $a \in [1, 20]$. By using a graphic calculator's table function, we have these two sets of solution:

(a) The first set is $a = 3$ and $b = 20$. Since $b > a$, $gcd(20, 3) = 1$ and $20 \not\equiv 3 \pmod 2$, the values are valid. We therefore have

$$x = 20^2 - 3^2 = 391$$
$$y = 2 \cdot 20 \cdot 3 = 120$$
$$z = 409.$$

Verifying:

$$391^2 + 120^2 = 167,281$$
$$409^2 = 167,281.$$

(b) The second set is $a = 20$ and $b = 3$. But since $b < a$ therefore this set is not valid for Pythagorean triple.

■

Problem 3.6.11

Repeat the same above exercise for 545.

Solution: Since 545 is the largest value in the triple, we have

$$a^2 + b^2 = 545,$$

hence

$$b^2 = 545 - a^2$$
$$b = \sqrt{545 - a^2},$$

where $a \in [1, 23]$. By using graphic calculator's table function, we have four sets of solution:

(a) The first set is $a = 4$ and $b = 23$. Since $b > a$, $gcd(23, 4) = 1$ and $23 \not\equiv 4 \pmod 2$, these values are valid. We therefore have

$$\begin{aligned} x &= 23^2 - 4^2 = 513 \\ y &= 2 \cdot 4 \cdot 23 = 124 \\ z &= 545. \end{aligned}$$

Verifying:

$$\begin{aligned} 513^2 + 184^2 &= 297,025 \\ 545^2 &= 297,025. \end{aligned}$$

(b) The second set is $a = 16$ and $b = 17$. Since $b > a$, $gcd(17, 16) = 1$ and $17 \not\equiv 16 \pmod 2$, these values are valid. We therefore have

$$\begin{aligned} x &= 17^2 - 16^2 = 33 \\ y &= 2 \cdot 7 \cdot 16 = 344 \\ z &= 545. \end{aligned}$$

Verifying:

$$\begin{aligned} 33^2 + 544^2 &= 297,025 \\ 545^2 &= 297,025. \end{aligned}$$

(c) The third and fourth sets are respectively the interchanged values between a and b from the first and second sets in paragraph (a) and (b), i.e., $a = 23,\ b = 4$ in the first set and $a = 17,\ b = 16$ in the second set. They are not Pythagorean triple's valid values since $a > b$.

■

3.7 Fermat's Theorem for Multiples of Four

Problem 3.7.1

Show that

$$x^4 - 4y^4 = z^2$$

does not have solution in positive integers.

Solution: Recall Dr. Zieschang's Lemma 6.1 on the generators of Pythagorean triple:

$$\begin{aligned} x &= b^2 - a^2, \\ y &= 2ab, \\ z &= b^2 + a^2, \end{aligned}$$

where $a, b \in \mathbb{Z}^+$, $gcd(a, b) = 1$, and $b \not\equiv a \pmod 2$.

Recall also Dr. Zieschang's Proposition 7.2: There do not exist positive integers x, y and z satisfying

$$x^4 + y^4 = z^2.$$

Having recalled the above two results, here we have

$$\begin{aligned} x^4 - 4y^4 &= z^2 \\ x^4 &= z^2 + 4y^4 \\ (x^2)^2 &= z^2 + (2y^2)^2. \end{aligned}$$

The last equation above implies that x^2, z and $2y^2$ are Pythagorean triples, thus per Lemma 6.1 there must exisst $a, b \in \mathbb{Z}^+, gcd(b, a) = 1$ and $b \not\equiv a \pmod 2$ such that

$$\begin{aligned} z &= b^2 - a^2, \\ 2y^2 &= 2ab, \\ x^2 &= b^2 + a^2. \end{aligned}$$

But $2y^2 = 2ab$ implies that there exist $p, q \in \mathbb{Z}$ such that

$$a = p^2$$
$$b = q^2.$$

By substitution,

$$\begin{aligned} x^2 &= b^2 + a^2 \\ &= (q^2)^2 + (p^2)^2 \\ &= q^4 + p^4, \end{aligned}$$

which does not have positive integer solution per Proposition 7.1.

■

Problem 3.7.2

Using the method of infinite descent, prove that

$$x^4 - y^4 = z^2$$

does not have positive integer solution.

Solution: Here we have

$$z^2 + (y^2)^2 = (x^2)^2.$$

Since z, y^2 and x^2 are Pythagorean triple, therefore there exist $p, q \in \mathbb{Z}^+, gcd(p, q) = 1$ and $p \not\equiv q \pmod 2$, such that

$$x^2 = p^2 + q^2$$
$$y^2 = p^2 - q^2, \text{ or } y^2 = 2pq$$
$$z = 2pq, \text{ or } z = p^2 - q^2.$$

Here we chose a solution that minimize $x^2 + y^2$. Factoring the original equation $x^4 - y^4 = z^2$, we have

$$(x^2 - y^2)(x^2 + y^2) = z^2.$$

Case I: First we assume that $y^2 = p^2 - q^2$. Therefore

$$\begin{aligned} x^2y^2 &= (p^2+q^2)(p^2-q^2) \\ &= p^4 - q^4. \end{aligned}$$

Clearly

$$\begin{aligned} p^2+q^2 &= x^2 \\ &< x^2+y^2 \\ &= p^2+q^2+p^2-q^2 \\ &= 2p^2, \end{aligned}$$

so we have found a solution that is smaller than the assumed nominal solution, contradicting the hypothesis.

Case II: We assume therefore that $y^2 = 2pq$ instead. Now we have

$$x^2 = p^2 + q^2$$

as Pythagorean triple. Therefore there exist $a, b \in \mathbb{Z}, gcd(a,b) = 1$ and $b \not\equiv a \pmod 2$, such that

$$\begin{aligned} p &= a^2 - b^2 \\ q &= 2ab \\ x &= a^2 + b^2. \end{aligned}$$

Then we have

$$\begin{aligned} ab(a^2-b^2) &= \frac{1}{2}qp \\ &= \frac{y^2}{4}, \end{aligned}$$

which is perfect square. It follows that a, b and $(a^2 - b^2)$ are perfect squares. Therefore there must exist $r, s, t \in \mathbb{Z}^+$, such that

$$\begin{aligned} a &= r^2 \\ b &= s^2 \\ a^2 - b^2 &= t^2. \end{aligned}$$

Next, we have

$$\begin{aligned} t^2 &= a^2 - b^2 \\ &= (r^2)^2 - (s^2)^2 \\ &= r^4 - s^4, \end{aligned}$$

and

$$\begin{aligned} r^2 + s^2 &= a + b \\ &< (a+b)(ab)(a-b) \\ &= \frac{1}{2}pq \\ &= \frac{y^2}{4} \\ &\leq y^2 \\ &< x^2 + y^2. \end{aligned}$$

Again we have thus found a smaller solution in positive integers, contradicting the hypothesis. Thus we are forced to conclude that $x^4 - y^4 = z^2$ does not have integer solution, as desired.

■

Problem 3.7.3

Show that a right triangle with Pythagorean triple sides can *not* have area that is a perfect square integer.

Solution: Recall from the previous exercise that

$$x^4 - y^4 = z^2$$

does not have positive integer solution.

Recall again Lemma 6.1 on the generators of Pythagorean triple:

$$x = b^2 - a^2,$$
$$y = 2ab,$$
$$z = b^2 + a^2,$$

where $a, b \in \mathbb{Z}^+$, $gcd(a, b) = 1$, and $b \not\equiv a \pmod 2$.

For the area of a right triangle of Pythagorean triple, we have

$$\begin{aligned} A &= \frac{1}{2}xy \\ &= \frac{1}{2}(2ab)(b^2 - a^2) \\ &= ab(b^2 - a^2). \end{aligned}$$

Suppose that A is a perfect square integer. This implies that a, b and $(b^2 - a^2)$ have to be perfect square integers:

$$\begin{aligned} a &= p^2 \\ b &= q^2 \\ (b^2 - a^2) &= r^2 \end{aligned}$$

for certain $p, q, r \in \mathbb{Z}^+$. Thus, substituting b^2 with $(q^2)^2$ and a^2 with $(p^2)^2$, we have

$$\begin{aligned} A &= ab(b^2 - a^2) \\ &= p^2q^2(q^4 - p^4) \\ &= p^2q^2r^2. \end{aligned}$$

But this is not possible since $q^4 - p^4 = r^2$ does not have integer solution from the previous problem.

$\blacksquare$

Problem 3.7.4

Show that

$$x^4 + 4y^4 = z^2$$

does not have solution in positive integers.

Solution: Recall Lemma 6.1 on generators of Pythagorean triples and the result from previous exercise 7.2 that

$$x^4 - y^4 = z^2$$

does not have integer solution.

Here we have

$$x^4 + 4y^4 = z^2$$
$$(x^2)^2 + (2y^2)^2 = z^2.$$

Since $x^2, 2y^2$ and z are Pythagorean triple, therefore per Lemma 6.1 there must exist $a, b \in \mathbb{Z}$, $gcd(a, b) = 1$ and $b \not\equiv a \pmod 2$, such that

$$x^2 = b^2 - a^2$$
$$2y^2 = 2ab$$
$$z = b^2 + a^2.$$

Since $2y^2 = 2ab$, there must exist $p, q \in \mathbb{Z}$,

$$a = p^2$$
$$b = q^2$$

such that $2y^2 = 2p^2q^2$.

Substituting $a = p^2$ and $b = q^2$, we have

$$\begin{aligned} x^2 &= b^2 - a^2 \\ &= (p^2)^2 - (q^2)^2 \\ &= p^4 - q^4, \end{aligned}$$

which according to problem 7.2 does not have integer solution. Therefore $x^4 + 4y^4 = z^2$ does not have integer solution, as desired.

■

3.8 Fermat's Theorem for Multiples of Three

Problem 3.8.1

Show that the equation

$$x^{3m} + y^{3m} = z^{3m}$$

does not have any integer solution with $xyz \neq 0$.

Solution: Recall that the Fermat's theorem for multiple of 3 that states

$$x^3 + y^3 = z^3$$

does not have any integer solution with $xyz \neq 0$. Next, we transform the equation in this exercise into

$$(x^m)^3 + (y^m)^3 = (z^m)^3.$$

Substituting $x^m = r, y^m = s$ and $z^m = t$, we then have

$$r^3 + s^3 = t^3,$$

which does not have integer solution according to Fermat's theorem.

■

Problem 3.8.2

Compute x and y for non-trivial integer solution from this equation:

$$(y^2 + x^2)^3 = (2xy)^3 + (y^2 - x^2)^3.$$

Solution: Recall Fermat's theorem on multiple of 3 cited in the previous exercise. Since the above equation is one with exponent of multiple of 3, therefore there will be no integer solution *unless* one of the term is zero. Since the first term, $y^2 + x^2$, will never be zero, hence we have only the following two possibilities:

Case I: $2xy = 0$, which means, first, that x is zero and y is a free variable:

$$(x, y) = \{(0, y) \mid y \in \mathbb{Z}\}.$$

Secondly, $y = 0$ and x is a free variable. But this $(x, y) = \{(x, 0) \mid x \in \mathbb{Z}\}$ is not possible since it leads to $x^6 \neq -x^6$.

Case II: $y^2 - x^2 = 0$, therefore

$$y^2 = x^2$$

$$y = x,$$

therefore the solution is

$$(x, y) = \{(z, z) \mid z \in \mathbb{Z}\}.$$

Alternatively, we can also pursue this second case as follow: Since $y^2 - x^2 = 0$, therefore

$$(y^2 + x^2)^3 = (2xy)^3$$

$$y^2 + x^2 = 2xy$$

$$y^2 - 2xy + x^2 = 0$$

$$(y - x)^2 = 0$$

$$y = x,$$

hence the same solution as before:

$$(x, y) = \{(z, z) \mid z \in \mathbb{Z}\}.$$

■

Problem 3.8.3

Prove that the equation

$$x^6 - y^3 = z^6$$

does not have integer solution for $xyz \neq 0$.

Solution: Recall Fermat's theorem on multiple of 3 cited in the previous exercise. Here, we can transform the equation into one with exponent of multiple of 3:

$$x^6 - y^3 = z^6$$

$$x^6 = y^3 + z^6$$

$$(x^2)^3 = (y)^3 + (z^2)^3,$$

which implies that it does not have integer solution.

■

Problem 3.8.4

Show that the equation

$$x^6 + 4y^6 = z^{18}$$

does not have integer solution for $xyz \neq 0$.

Solution: Recall again the Fermat's theorem for exponent of multiple of 3, and recall also Lemma 6.1 on the generator of Pythagorean triple:

$$x = b^2 - a^2,$$

$$y = 2ab,$$

$$z = b^2 + a^2,$$

where $a, b \in \mathbb{Z}^+$, $gcd(a, b) = 1$, and $b \not\equiv a \pmod 2$.

Here we have

$$x^6 + 4y^6 = z^{18}$$

$$(x^3)^2 + (2y^3)^2 = (z^9)^2,$$

which is a set of Pythagorean triple. Hence there must exist $a, b \in \mathbb{Z}^+$, $gcd(b, a) = 1$ and $b \not\equiv a$

$(\mathrm{mod}\ 2)$, such that

$$x^3 = b^2 - a^2$$
$$2y^3 = 2ab$$
$$z^9 = b^2 + a^2.$$

Since $2y^3 = 2ab$, therefore ab must be a perfect cube, which means that there must exist $p, q \in \mathbb{Z}^+$, such that, whithout loss of generality:

$$a = p^3$$
$$b = q^3.$$

Substituting, we have

$$\begin{aligned} x^3 &= b^2 - a^2, \\ x^3 &= (q^3)^2 - (p^3)^2 \\ &= (q^2)^3 - (p^2)^3. \end{aligned}$$

Since the equation is one with exponent of multiple of 3, therefore per Fermat's theorem it does not have integer solution. Using similar argument, we can also show that

$$(z^3)^3 = (p^2)^3 + (q^2)^3$$

does not have integer solution. Thus $x^6 + 4y^6 = z^{18}$ does not have integer solution, as desired.

■

Problem 3.8.5

Solve for non-trivial integer solution of $2x^3 + 6xy^2 = z^3$.

Solution: Recall the sum and difference of cube:

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

Here we have

$$\begin{aligned}z^3 &= 2x^3 + 6xy^2\\ &= (x^3 + 3x^2y + 3xy^2 + y^3) + (x^3 - 3x^2y + 3xy^2 - y^3)\\ &= (x+y)^3 + (x-y)^3.\end{aligned}$$

Since this equation represents one with exponent of multiple of 3, therefore per Fermat's theorem it does not have integer solution, unless of the term is zero. Hence we have these three cases here.

(a) Case I: $(x+y)^3 = 0$. Here we have

$$\begin{aligned}(x+y)^3 &= 0\\ x+y &= 0\\ x &= -y,\end{aligned}$$

and then we express z in term of y:

$$\begin{aligned}(x-y)^3 &= z^3\\ x-y &= z\\ -2y &= z.\end{aligned}$$

Consequently the solution in the first case is

$$(x, y, z) = \{(-k, k, -2k) \mid k \in \mathbb{Z}\}.$$

(b) Case II: $(x-y)^3 = 0$. Here we have

$$\begin{aligned}(x-y)^3 &= 0\\ x-y &= 0\\ x &= y,\end{aligned}$$

and we z we proceed as follow:

$$\begin{aligned}(x+y)^3 &= z^3\\ x+y &= z\\ 2y &= z.\end{aligned}$$

Consequently the solution is

$$(x,y,z) = \{(k,k,2k) \mid k \in \mathbb{Z}\}.$$

(c) Case III: $z^3 = 0$. Here we have $z = 0$. To solve for x and y, we set

$$\begin{aligned}(x+y)^3 + (x-y)^3 = 0&\\ (x+y)^3 &= -(x-y)^3\\ x+y &= -(x-y)\\ x+y &= -x+y\\ x &= 0.\end{aligned}$$

Hence the integer solution is

$$(x,y,z) = \{(0,k,0) \mid k \in \mathbb{Z}\}.$$

■

REFERENCES

Zieschang, Paul-Hermann, *Algebra I*, class notes for MATH-3321: Algebra I at University of Texas - Brownsville, Department of Mathematics.

Zieschang, Paul-Hermann, *Higher Algebra*, class notes for MATH-5321: Higher Algebra at University of Texas - Brownsville, Department of Mathematics.

Zieschang, Paul-Hermann, *Number Theory*, class notes for MATH-4329: Number Theory at University of Texas - Brownsville, Department of Mathematics.

Gilbert, Linda, Jimmy Gilbert, *Elements of Modern Algebra,* 7th edition, Belmont, Cal, Brook/Cole, 2009.

Fraleigh, John B., *A First Course in Abstract Algebra,* 7th edition, New York, NY., Pearson, 2003.

Rosen, Kenneth H., *Elementary Number Theory and Its Applications,* 5th edition, New York, NY., Pearson-Addison Wesley, 2003.

Tattersal, James J., *Elementary Number Theory in Nine Chapters,* 2nd edition, New York, NY., Cambridge University Press, 2005.

BIOGRAPHICAL SKETCH

Ryanto (Ryan) Putra started working on his BS degree in his late adulthood by 1984 while he was still living oversea, enrolling in then Regents College's Independent Study Degree Program, an external degree program of the University of the State of New York in Albany. The institution is the oldest and hailed as the pioneer in distant degree program catering mainly toward oversea military personnel. In 2001 the college was renamed as Excelsior College. Upon graduation in 1992 with BS degree in General Business, Ryan then went to the University of Houston to graduate with an MBA degree in Accounting in 1995.

After some years of careers in various businesses in Texas, he finally succumbed to the callings of long lineage of family members who were once educators, especially from his mother, of being an educator himself. He returned to his study and obtained a Texas teacher license in 2009, certified in high school mathematics, physics and chemistry. His first assignment was teaching Geometry at Hardin HS, a small school district northeast of Houston. Aside from state credential, he is also certified by the College Board to teach AP Calculus I and II.

Even while he was still teaching HS, he had had his next goal set to teach at college level, for which a master degree in mathematics is required. Since he did not have enough undergraduate credits in math, he began the long journey, one credit hour at a time, by taking various prerequisite undergraduate math classes from various independent study programs. Once he earned enough prerequisite credits, he then applied to the online math program at the UT-Brownsville. After the university was merged to the UT-Rio Grande Valley, he graduated with an MS degree in Math in 2017.

In total, Ryan has combined 8 years of teaching experience. He is currently an instructor at the local Tarrant County Community College's Northeast campus, teaching subjects ranging from College Algebra to Calculus III. He can be reached by email at ryanto.putra@tccd.edu.