INTRODUCTORY ALGEBRAIC NUMBER THEORY

ŞABAN ALACA
Carleton University, Ottawa

KENNETH S. WILLIAMS
Carleton University, Ottawa

CAMBRIDGE UNIVERSITY PRESS

PUBLISHED BY THE PRESS SYNDICATE OF THE UNIVERSITY OF CAMBRIDGE
The Pitt Building, Trumpington Street, Cambridge, United Kingdom

CAMBRIDGE UNIVERSITY PRESS
The Edinburgh Building, Cambridge CB2 2RU, UK
40 West 20th Street, New York, NY 10011-4211, USA
477 Williamstown Road, Port Melbourne, VIC 3207, Australia
Ruiz de Alarcón 13, 28014 Madrid, Spain
Dock House, The Waterfront, Cape Town 8001, South Africa

http://www.cambridge.org

First published 2004

Printed in the United States of America

Typeface Times 11/14 pt. *System* LaTeX 2_ε [TB]

A catalog record for this book is available from the British Library.

Library of Congress Cataloging in Publication Data
Alaca, Saban, 1964–
Introductory algebraic number theory / Saban Alaca, Kenneth S. Williams.
p. cm.
Includes bibliographical references and index.
ISBN 0-521-83250-0 (hb.) – ISBN 0-521-54011-9 (pbk.)
1. Algebraic number theory. I. Williams, Kenneth S. II. Title.
QA247 .A43 2003
512′.74 – dc21 2003051243

ISBN 0 521 83250 0 hardback
ISBN 0 521 54011 9 paperback

Contents

List of Tables *page* xi
Notation xiii
Introduction xv
1 Integral Domains 1
1.1 Integral Domains 1
1.2 Irreducibles and Primes 5
1.3 Ideals 8
1.4 Principal Ideal Domains 10
1.5 Maximal Ideals and Prime Ideals 16
1.6 Sums and Products of Ideals 21
Exercises 23
Suggested Reading 25
Biographies 25
2 Euclidean Domains 27
2.1 Euclidean Domains 27
2.2 Examples of Euclidean Domains 30
2.3 Examples of Domains That are Not Euclidean 37
2.4 Almost Euclidean Domains 46
2.5 Representing Primes by Binary Quadratic Forms 47
Exercises 49
Suggested Reading 51
Biographies 53
3 Noetherian Domains 54
3.1 Noetherian Domains 54
3.2 Factorization Domains 57
3.3 Unique Factorization Domains 60
3.4 Modules 64
3.5 Noetherian Modules 67
Exercises 71

Suggested Reading 72
Biographies 73
4 Elements Integral over a Domain 74
4.1 Elements Integral over a Domain 74
4.2 Integral Closure 81
Exercises 86
Suggested Reading 87
Biographies 87
5 Algebraic Extensions of a Field 88
5.1 Minimal Polynomial of an Element Algebraic over a Field 88
5.2 Conjugates of α over K 90
5.3 Conjugates of an Algebraic Integer 91
5.4 Algebraic Integers in a Quadratic Field 94
5.5 Simple Extensions 98
5.6 Multiple Extensions 102
Exercises 106
Suggested Reading 108
Biographies 108
6 Algebraic Number Fields 109
6.1 Algebraic Number Fields 109
6.2 Conjugate Fields of an Algebraic Number Field 112
6.3 The Field Polynomial of an Element of an Algebraic Number Field 116
6.4 The Discriminant of a Set of Elements in an Algebraic Number Field 123
6.5 Basis of an Ideal 129
6.6 Prime Ideals in Rings of Integers 137
Exercises 138
Suggested Reading 140
Biographies 140
7 Integral Bases 141
7.1 Integral Basis of an Algebraic Number Field 141
7.2 Minimal Integers 160
7.3 Some Integral Bases in Cubic Fields 170
7.4 Index and Minimal Index of an Algebraic Number Field 178
7.5 Integral Basis of a Cyclotomic Field 186
Exercises 189
Suggested Reading 191
Biographies 193
8 Dedekind Domains 194
8.1 Dedekind Domains 194
8.2 Ideals in a Dedekind Domain 195

8.3 Factorization into Prime Ideals 200
8.4 Order of an Ideal with Respect to a Prime Ideal 206
8.5 Generators of Ideals in a Dedekind Domain 215
Exercises 216
Suggested Reading 217
9 Norms of Ideals 218
9.1 Norm of an Integral Ideal 218
9.2 Norm and Trace of an Element 222
9.3 Norm of a Product of Ideals 228
9.4 Norm of a Fractional Ideal 231
Exercises 233
Suggested Reading 234
Biographies 235
10 Factoring Primes in a Number Field 236
10.1 Norm of a Prime Ideal 236
10.2 Factoring Primes in a Quadratic Field 241
10.3 Factoring Primes in a Monogenic Number Field 249
10.4 Some Factorizations in Cubic Fields 253
10.5 Factoring Primes in an Arbitrary Number Field 257
10.6 Factoring Primes in a Cyclotomic Field 260
Exercises 261
Suggested Reading 262
11 Units in Real Quadratic Fields 264
11.1 The Units of $\mathbb{Z} + \mathbb{Z}\sqrt{2}$ 264
11.2 The Equation $x^2 - my^2 = 1$ 267
11.3 Units of Norm 1 271
11.4 Units of Norm -1 275
11.5 The Fundamental Unit 278
11.6 Calculating the Fundamental Unit 286
11.7 The Equation $x^2 - my^2 = N$ 294
Exercises 297
Suggested Reading 298
Biographies 298
12 The Ideal Class Group 299
12.1 Ideal Class Group 299
12.2 Minkowski's Translate Theorem 300
12.3 Minkowski's Convex Body Theorem 305
12.4 Minkowski's Linear Forms Theorem 306
12.5 Finiteness of the Ideal Class Group 311
12.6 Algorithm to Determine the Ideal Class Group 314
12.7 Applications to Binary Quadratic Forms 331
Exercises 341

	Suggested Reading	343
	Biographies	343
13	Dirichlet's Unit Theorem	344
13.1	Valuations of an Element of a Number Field	344
13.2	Properties of Valuations	346
13.3	Proof of Dirichlet's Unit Theorem	359
13.4	Fundamental System of Units	361
13.5	Roots of Unity	363
13.6	Fundamental Units in Cubic Fields	369
13.7	Regulator	378
	Exercises	382
	Suggested Reading	383
	Biographies	384
14	Applications to Diophantine Equations	385
14.1	Insolvability of $y^2 = x^3 + k$ Using Congruence Considerations	385
14.2	Solving $y^2 = x^3 + k$ Using Algebraic Numbers	389
14.3	The Diophantine Equation $y(y+1) = x(x+1)(x+2)$	401
	Exercises	410
	Suggested Reading	411
	Biographies	411
List of Definitions		413
Location of Theorems		417
Location of Lemmas		421
Bibliography		423
Index		425

List of Tables

1 Integral bases and discriminants for $\mathbb{Q}(\sqrt[3]{k}),\ 2 \le k \le 20$, k cubefree. *page* 177
2 Integral bases and discriminants for $\mathbb{Q}(\sqrt[4]{k})$, $x^4 - k$ irreducible in $\mathbb{Q}[x], 2 \le k \le 10$. 177
3 Integral bases and discriminants for $\mathbb{Q}(\sqrt[4]{-k})$, $x^4 + k$ irreducible in $\mathbb{Q}[x], 1 \le k \le 10$. 178
4 Fundamental units of $O_{\mathbb{Q}(\sqrt{m})},\ 2 \le m < 40$, m squarefree. 280
5 Nontrivial ideal class groups $H(\mathbb{Q}(\sqrt{k})),\ -30 < k < 0$, k squarefree. 322
6 Nontrivial ideal class groups $H(\mathbb{Q}(\sqrt{k})),\ 2 \le k < 100$, k squarefree. 323
7 Class numbers of imaginary quadratic fields $K = \mathbb{Q}(\sqrt{k})$, $-195 \le k < 0$, k squarefree. 325
8 Class numbers of real quadratic fields $K = \mathbb{Q}(\sqrt{k})$, $0 < k \le 197$, k squarefree. 326
9 Class numbers of $\mathbb{Q}(\sqrt[3]{k}),\ 2 \le k \le 101$, k cubefree. 329
10 Class numbers of cyclotomic fields $K_m,\ 3 \le m \le 45$, $m \not\equiv 2 \pmod 4$. 331
11 Fundamental unit (> 1) of $\mathbb{Q}(\sqrt[3]{m})$ for a few values of $m \in \mathbb{N}$. 375
12 Fundamental unit of cubic fields K with exactly one real embedding and $-268 \le d(K) < 0$. 376
13 Units of totally real cubic fields K with $0 < d(K) \le 1101$. 377
14 Fundamental unit of some pure quartic fields $\mathbb{Q}(\sqrt[4]{-m})$. 378
15 Solutions $(x, y) \in \mathbb{Z}^2$ of $y^2 = x^3 + k,\ -20 \le k < 0$. 402
16 Solutions $(x, y) \in \mathbb{Z}^2$ of $y^2 = x^3 + k,\ 0 < k \le 20$. 403

1

Integral Domains

1.1 Integral Domains

In this chapter we recall the definition and properties of an integral domain and develop the concept of divisibility in such a domain. We expect the reader to be familiar with the elementary properties of groups, rings, and fields and to have a basic knowledge of both elementary number theory and linear algebra over a field.

Definition 1.1.1 (Integral domain) *An integral domain is a commutative ring that has a multiplicative identity but no divisors of zero.*

An integral domain D is called a field if for each $a \in D,\ a \neq 0$, there exists $b \in D$ with $ab = 1$.

Example 1.1.1 *The ring $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$ of all integers is an integral domain.*

Example 1.1.2 *$\mathbb{Z} + \mathbb{Z}i = \{a + bi \mid a, b \in \mathbb{Z}\}$ is an integral domain. The elements of $\mathbb{Z} + \mathbb{Z}i$ are called Gaussian integers after the famous mathematician Carl Friedrich Gauss (1777–1855), who developed their properties in his work on biquadratic reciprocity. $\mathbb{Z} + \mathbb{Z}i$ is called the Gaussian domain.*

Example 1.1.3 *$\mathbb{Z} + \mathbb{Z}\omega = \{a + b\omega \mid a, b \in \mathbb{Z}\}$, where ω is the complex cube root of unity given by $\omega = (-1 + \sqrt{-3})/2$, is an integral domain. The elements of $\mathbb{Z} + \mathbb{Z}\omega$ are called Eisenstein integers after Gotthold Eisenstein (1823–1852), who introduced them in his pioneering work on the law of cubic reciprocity. $\mathbb{Z} + \mathbb{Z}\omega$ is called the Eisenstein domain. The other complex cube root of unity is $\omega^2 = \overline{\omega} = (-1 - \sqrt{-3})/2$. Note that $\mathbb{Z} + \mathbb{Z}\omega = \mathbb{Z} + \mathbb{Z}\omega^2$ as $\omega^2 = -\omega - 1$. Also $\mathbb{Z} + \mathbb{Z}\omega = \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{-3}}{2}\right)$.*

Example 1.1.4 *$\mathbb{Z} + \mathbb{Z}\sqrt{m} = \{a + b\sqrt{m} \mid a, b \in \mathbb{Z}\}$, where m is a positive or negative integer that is not a perfect square, is an integral domain. As $\sqrt{m}$ is a root of an irreducible quadratic polynomial (namely $x^2 - m$), $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ is called* *a quadratic domain. If k is a nonzero integer such that k^2 divides m then*

$$\mathbb{Z}+\mathbb{Z}\sqrt{m} \subseteq \mathbb{Z}+\mathbb{Z}\sqrt{m/k^2}$$

with equality if and only if $k^2 = 1$. $\mathbb{Z}+\mathbb{Z}\sqrt{m}$ is called a subdomain of $\mathbb{Z}+\mathbb{Z}\sqrt{m/k^2}$. Thus $\mathbb{Z}+2\mathbb{Z}i \subset \mathbb{Z}+\mathbb{Z}i$.

Example 1.1.5 $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right) = \{a+b\left(\frac{1+\sqrt{m}}{2}\right) \mid a, b \in \mathbb{Z}\}$*, where m is a nonsquare integer (positive or negative), which is congruent to 1 modulo 4, is an integral domain. We emphasize that $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ is not an integral domain if $m \not\equiv 1 \pmod 4$ since in this case it is not closed under multiplication as*

$$\left(\frac{1+\sqrt{m}}{2}\right)\left(1-\left(\frac{1+\sqrt{m}}{2}\right)\right) = \left(\frac{1+\sqrt{m}}{2}\right)\left(\frac{1-\sqrt{m}}{2}\right) = \frac{1-m}{4} \notin \mathbb{Z}.$$

Again as $\frac{1+\sqrt{m}}{2}$ is a root of an irreducible quadratic polynomial (namely $x^2 - x + \left(\frac{1-m}{4}\right)$), $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ is called a quadratic domain. We note that the elements of the integral domain $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ can also be written in the form $\frac{1}{2}(x+y\sqrt{m})$, where x and y are integers such that $x \equiv y \pmod 2$. Clearly the domain $\mathbb{Z}+\mathbb{Z}\sqrt{m}$ is a subdomain of $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$.

Example 1.1.6 $F[x]$ = *the ring of polynomials in the indeterminate x with coefficients from a field F is an integral domain.*

Example 1.1.7 $\mathbb{Z}[x]$ = *the ring of polynomials in the indeterminate x with integral coefficients is an integral domain.*

Example 1.1.8 $D[x]$ = *the ring of polynomials in the indeterminate x with coefficients from the integral domain D is an integral domain.*

Example 1.1.9 $F[x, y]$ = *the ring of polynomials in the two indeterminates x and y with coefficients from the field F is an integral domain.*

Example 1.1.10 $\mathbb{Z}+\mathbb{Z}\theta+\mathbb{Z}\theta^2 = \{a+b\theta+c\theta^2 \mid a, b, c \in \mathbb{Z}\}$*, where θ is a root of the cubic equation $\theta^3+\theta+1=0$, is an integral domain. It is called a cubic domain.*

Example 1.1.11 $D = \{a+b\sqrt{2}+ci+di\sqrt{2} \mid a, c$ *integers; b, d both integers or both halves of odd integers$\}$ is an integral domain. Clearly $\mathbb{Z}+\mathbb{Z}\sqrt{2} \subset D$, $\mathbb{Z}+\mathbb{Z}i \subset D$, $\mathbb{Z}+\mathbb{Z}i\sqrt{2} \subset D$.*

Properties of an Integral Domain

Let D be an integral domain. Then the following properties hold.

(a) The identity element of D is unique, for if 1 and $1'$ are two identities for D then

$$1 = 1 \cdot 1' \text{ (as } 1' \text{ is an identity)} = 1' \text{ (as 1 is an identity).}$$

(b) D possesses a left cancellation law, that is,

$$ab = ac,\ a \neq 0 \Longrightarrow b = c\ (a, b, c \in D)$$

as well as a right cancellation law

$$ac = bc,\ c \neq 0 \Longrightarrow a = b\ (a, b, c \in D).$$

(c) It is well known that if D is an integral domain then there exists a field F, called the field of quotients of D or the quotient field of D, that contains an isomorphic copy D' of D (see, for example, Fraleigh [3]). In practice it is usual to identify D with D' and so consider D as a subdomain of F. The quotient field of $\mathbb{Z}$ is the field of rational numbers $\mathbb{Q}$. The quotient field of the polynomial domain $F[X]$ (where F is a field) is the field $F(X)$ of rational functions in X.

Definition 1.1.2 (Divisor) *Let a and b belong to the integral domain D. The element a is said to be a divisor of b (or a divides b) if there exists an element c of D such that $b = ac$. If a is a divisor of b, we write $a \mid b$. If a is not a divisor of b, we write $a \nmid b$.*

Example 1.1.12 $1 + i \mid 2$ *in* $\mathbb{Z} + \mathbb{Z}i$ *as* $2 = (1 + i)(1 - i)$.

Example 1.1.13 $x^2 + x + 1 \mid x^4 + x^2 + 1$ *in* $\mathbb{Z}[x]$ *as* $x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 - x + 1)$.

Example 1.1.14 $(1 - \omega)^2 \mid 3$ *in* $\mathbb{Z} + \mathbb{Z}\omega$ *as* $3 = (1 - \omega)^2(1 + \omega)$ (*see Example 1.1.3*).

Example 1.1.15 $1 + \theta - \theta^2 \mid -\theta - 2\theta^2$ *in* $\mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2$ *as* $-\theta - 2\theta^2 = (1 + \theta - \theta^2)(1 - \theta)$ (*see Example 1.1.10*).

Example 1.1.16 $2 + \sqrt{2} \nmid 3$ *in* $\mathbb{Z} + \mathbb{Z}\sqrt{2}$ *as* $3/(2 + \sqrt{2}) = 3 - \frac{3}{2}\sqrt{2} \notin \mathbb{Z} + \mathbb{Z}\sqrt{2}$.

Properties of Divisors

Let $a, b, c \in D$, where D is an integral domain. Then the following properties hold.

(a) $a \mid a$ (reflexive property).
(b) $a \mid b$ and $b \mid c$ implies $a \mid c$ (transitive property).

(c) $a \mid b$ and $a \mid c$ implies $a \mid xb + yc$ for any $x \in D$ and $y \in D$.
(d) $a \mid b$ implies $ac \mid bc$.
(e) $ac \mid bc$ and $c \neq 0$ implies $a \mid b$.
(f) $1 \mid a$.
(g) $a \mid 0$.
(h) $0 \mid a$ implies $a = 0$.

Definition 1.1.3 (Unit) *An element a of an integral domain D is called a unit if $a \mid 1$. The set of units of D is denoted by $U(D)$.*

Properties of Units

Let D be an integral domain. Then $U(D)$ has the following properties.

(a) $\pm 1 \in U(D)$.
(b) If $a \in U(D)$ then $-a \in U(D)$.
(c) If $a \in U(D)$ then $a^{-1} \in U(D)$.
(d) If $a \in U(D)$ and $b \in U(D)$ then $ab \in U(D)$.
(e) If $a \in U(D)$ then $\pm a^n \in U(D)$ for any $n \in \mathbb{Z}$.

Example 1.1.17

(a) $i \in U(\mathbb{Z} + \mathbb{Z}i)$.
(b) $\omega \in U(\mathbb{Z} + \mathbb{Z}\omega)$ (*see Example 1.1.3*).
(c) $\theta \in U(\mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2)$ *as* $1 = \theta(-1 - \theta^2)$ (*see Example 1.1.10*).

Theorem 1.1.1 *If D is an integral domain then $U(D)$ is an Abelian group with respect to multiplication.*

Proof: $U(D)$ is closed under multiplication by property (d). Multiplication of elements of $U(D)$ is both associative and commutative as D is an integral domain. $U(D)$ possesses an identity element, namely 1, by property (a). Every element of $U(D)$ has a multiplicative inverse by property (c). Thus $U(D)$ is an Abelian group with respect to multiplication. ■

Abelian groups are named after the Norwegian mathematician Niels Henrik Abel (1802–1829), who proved in 1824 the impossibility of solving the general quintic equation by means of radicals.

Example 1.1.18 *Let $\mathbb{Z}_n$ denote the cyclic group of order n.*

(a) $U(\mathbb{Z}) = \{\pm 1\} \simeq \mathbb{Z}_2$.
(b) $U(\mathbb{Z} + \mathbb{Z}i) = \{\pm 1, \pm i\} \simeq \mathbb{Z}_4$.
(c) $U(F[x]) = F^*$, *where F is a field and* $F^* = F \setminus \{0\}$.

(d) $U(\mathbb{Z}[x]) = \{\pm 1\} \simeq \mathbb{Z}_2$.
(e) $\pm(1+\sqrt{2})^n \in U(\mathbb{Z}+\mathbb{Z}\sqrt{2})$, *for all* $n \in \mathbb{Z}$.
(f) $\frac{1}{2}\sqrt{2} + \frac{1}{2}i\sqrt{2} \in U(D)$, *where* D *is defined in Example 1.1.11.*

We remark that in Chapter 11 we will show that

$$U(\mathbb{Z}+\mathbb{Z}\sqrt{2}) = \{\pm(1+\sqrt{2})^n \mid n \in \mathbb{Z}\} \simeq \mathbb{Z}_2 \times \mathbb{Z}.$$

Definition 1.1.4 (Associate) *Two nonzero elements* a *and* b *of an integral domain* D *are called associates, or said to be associated, if each divides the other. If* a *and* b *are associates we write* $a \sim b$. *If* a *and* b *are not associates we write* $a \not\sim b$.

Properties of Associates

Let $a, b, c \in D^* = D \setminus \{0\}$, where D is an integral domain. The following properties hold.

(a) $a \sim a$ (reflexive property).
(b) $a \sim b$ implies $b \sim a$ (symmetric property).
(c) $a \sim b$ and $b \sim c$ imply $a \sim c$ (transitive property).
(d) $a \sim b$ if and only if $ab^{-1} \in U(D)$.
(e) $a \sim 1$ if and only if a is a unit.

Properties (a), (b), and (c) show that $\sim$ is an equivalence relation. The equivalence class containing $a \in D$ is just the set $\{ua \mid u \in U(D)\}$.

Example 1.1.19

(a) *In* $\mathbb{Z}$, $a \sim b$ *if and only if* $a = \pm b$, *equivalently* $|a| = |b|$.
(b) *In* $\mathbb{Z}+\mathbb{Z}i$ *we have* $1+i \sim 1-i$ *as* $\frac{1+i}{1-i} = i \in U(\mathbb{Z}+\mathbb{Z}i)$.
(c) *In* $\mathbb{Z}+\mathbb{Z}\sqrt{2}$ *we have* $1+3\sqrt{2} \sim 5-2\sqrt{2}$ *as* $\frac{1+3\sqrt{2}}{5-2\sqrt{2}} = 1+\sqrt{2} \in U(\mathbb{Z}+\mathbb{Z}\sqrt{2})$.

1.2 Irreducibles and Primes

In $\mathbb{Z}$ an integer p (≥ 2) that is divisible only by the positive integers 1 and p is called a prime. Each prime p in $\mathbb{Z}$ has the following two properties:

$$p = ab \;\; (a, b \in \mathbb{Z}) \Longrightarrow a \text{ or } b = \pm 1 \tag{1.2.1}$$

and

$$p \mid ab \;\; (a, b \in \mathbb{Z}) \Longrightarrow p \mid a \text{ or } p \mid b. \tag{1.2.2}$$

Our next definition generalizes property (1.2.1) to an arbitrary integral domain D, and an element of D with this property is called an irreducible element.

Definition 1.2.1 (Irreducible) *A nonzero, nonunit element a of an integral domain D is called an irreducible, or said to be irreducible, if $a = bc$, where $b, c \in D$, implies that either b or c is a unit.*

A nonzero, nonunit element that is not irreducible is called reducible.

Example 1.2.1 2 *is irreducible in $\mathbb{Z}$, for if $2 = ab$ with $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$ then either $a = \pm 1$ or $b = \pm 1$.*

Example 1.2.2 2 *is irreducible in $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$. To show this, suppose that $2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$, where $a, b, c, d \in \mathbb{Z}$. Taking the modulus of both sides of this equation, we obtain $4 = (a^2 + 5b^2)(c^2 + 5d^2)$. Thus $a^2 + 5b^2$ is a positive integral divisor of 4 and so we must have*

$$a$$

Example 1.2.5 *2 is not a prime in* $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$ *as* $2 \mid (1+\sqrt{-5})(1-\sqrt{-5})$ *yet* $2 \nmid 1 \pm \sqrt{-5}$.

Example 1.2.6 $1+i$ *is a prime in* $\mathbb{Z} + \mathbb{Z}i$. *To show this, suppose that* $1+i \mid (a+bi)(c+di)$, *where* $a, b, c, d \in \mathbb{Z}$. *Then there exist integers* x *and* y *such that*

$$(a+bi)(c+di) = (1+i)(x+yi).$$

Taking the modulus of both sides of this equation, we obtain

$$(a^2+b^2)(c^2+d^2) = 2(x^2+y^2).$$

As 2 is a prime in $\mathbb{Z}$, *we have either* $2 \mid a^2+b^2$ *or* $2 \mid c^2+d^2$. *Interchanging* $a+bi$ *and* $c+di$, *if necessary, we may suppose that* $2 \mid a^2+b^2$. *Thus, either* a *and* b *are both even or they are both odd. In the former case* $a = 2r$ *and* $b = 2s$, *where* r *and* s *are integers, and*

$$a+bi = 2(r+si) = (1+i)((r+s)+(-r+s)i),$$

so that $1+i \mid a+bi$. *In the latter case* $a = 2r+1$ *and* $b = 2s+1$, *where* r *and* s *are integers, and*

$$a+bi = 2(r+si)+(1+i) = (1+i)((r+s+1)+(-r+s)i),$$

so that $1+i \mid a+bi$. *Hence* $1+i$ *is a prime in* $\mathbb{Z}+\mathbb{Z}i$.

Theorem 1.2.1 *In any integral domain* D *a prime is irreducible.*

Proof: Let $p \in D$ be a prime and suppose that $p = ab$, where $a, b \in D$. As $ab = p \cdot 1$ we have $p \mid ab$, and so, as p is prime, we deduce that $p \mid a$ or $p \mid b$, that is, $a/p \in D$ or $b/p \in D$. Since $1 = a/p \cdot b$ or $1 = a \cdot b/p$, either b is a unit or a is a unit of D. This proves that p is an irreducible element of D. ■

The converse of Theorem 1.2.1 is not true. From Examples 1.2.2 and 1.2.5 we see that the element 2 of $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$ is irreducible but not prime.

Waterhouse [6] has recently given a class of integral domains in which every irreducible is prime.

Theorem 1.2.2 *Let* D *be an integral domain that has the following property:*

Every quadratic polynomial in $D[X]$ *having roots in the quotient field* F *of* D *is a product of linear polynomials in* $D[X]$. (1.2.3)

Then every irreducible in D *is prime.*

Proof: Let p be an irreducible element in D, which is not prime. Then there exist $a, b \in D$ such that

$$p \mid ab, \;\; p \nmid a, \;\; p \nmid b.$$

Let $r = ab/p \in D$, and consider the quadratic polynomial

$$f(X) = pX^2 - (a+b)X + r.$$

In $F[X]$ we have

$$f(X) = p(X - a/p)(X - b/p).$$

We show that $f(X)$ does not factor into linear factors in $D[X]$. Indeed, suppose on the contrary that

$$f(X) = (cX + s)(dX + t)$$

in $D[X]$. Then $cd = p$. As p is irreducible, one of c and d is a unit of D, say d, so that $c = d^{-1}p$. Then the roots of $f(X)$ in F are $-ds/p$ and $-d^{-1}t$. But $-d^{-1}t \in D$, while neither a/p nor b/p is in D. Thus no such factorization can exist. Hence every irreducible in D is prime. ■

1.3 Ideals

Subsets of an integral domain D that are closed under addition and under multiplication by elements of D play a special role and are called ideals.

Definition 1.3.1 (Ideal) *An ideal I of an integral domain D is a nonempty subset of D having the following two properties:*

$$a \in I, \; b \in I \Longrightarrow a + b \in I,$$

$$a \in I, r \in D \Longrightarrow ra \in I.$$

It is clear that if $a_1, \ldots, a_n \in I$ then $r_1a_1 + \cdots + r_na_n \in I$ for all $r_1, \ldots, r_n \in D$. In particular if $a \in I$ and $b \in I$ then $-a \in I$ and $a - b \in I$. Also $0 \in I$, and if $1 \in I$ then $I = D$.

Example 1.3.1 *If $\{a_1, \ldots, a_n\}$ is a set of elements of the integral domain D then the set of all finite linear combinations of $a_1, \ldots, a_n$*

$$\left\{ \sum_{i=1}^{n} r_i a_i \mid r_1, \ldots, r_n \in D \right\}$$

is an ideal of D, which we denote by $\langle a_1, \ldots, a_n \rangle$.

Definition 1.3.2 (Principal ideal) *An ideal I of an integral domain D is called a principal ideal if there exists an element $a \in I$ such that $I = \langle a \rangle$. The element a is called a generator of the ideal I.*

If D is an integral domain the principal ideal $\langle a \rangle$ generated by $a \in D$ is just the set $\{ra \mid r \in D\}$. Clearly the principal ideal $\langle 0 \rangle$ is just the singleton set $\{0\}$ and the principal ideal $\langle 1 \rangle$ is D.

Definition 1.3.3 (Proper ideal) *An ideal I of an integral domain D is called a proper ideal of D if $I \neq \langle 0 \rangle, \langle 1 \rangle$.*

Thus a proper ideal of an integral domain D is an ideal I such that $\{0\} \subset I \subset D$.

Example 1.3.2 *For any positive integer k, the set*

$$k\mathbb{Z} = \{0, \pm k, \pm 2k, \ldots\}$$

is an ideal of $\mathbb{Z}$. Indeed $k\mathbb{Z}$ is a principal ideal generated by k (or $-k$) so that

$$k\mathbb{Z} = \langle k \rangle = \langle -k \rangle.$$

Example 1.3.3 *Let*

$$I = \{f(x) \in \mathbb{Z}[x] \mid f(0) = 0\}.$$

Then I is an ideal of $\mathbb{Z}[x]$ and $I = \langle x \rangle$.

Example 1.3.4 *Let*

$$J = \{f(x) \in \mathbb{Z}[x] \mid f(0) \equiv 0 \pmod 2\}.$$

Then J is an ideal of $\mathbb{Z}[x]$ and $J = \langle 2, x \rangle$. However, J is not a principal ideal.

Theorem 1.3.1 *Let D be an integral domain and let $a, b \in D^* = D \setminus \{0\}$. Then*

$$\langle a \rangle = \langle b \rangle \textit{ if and only if } a/b \in U(D).$$

Proof: If $a/b \in U(D)$ then $a = bu$ for some $u \in U(D)$. Let $x \in \langle a \rangle$. Then $x = ac$ for some $c \in D$. Hence $x = buc$ with $uc \in D$. Thus $x \in \langle b \rangle$. We have shown that $\langle a \rangle \subseteq \langle b \rangle$. As $a/b \in U(D)$ and $U(D)$ is a group with respect to multiplication, we have $b/a = (a/b)^{-1} \in U(D)$. Then, proceeding exactly as before with the roles of a and b interchanged, we find that $\langle b \rangle \subseteq \langle a \rangle$. Thus $\langle a \rangle = \langle b \rangle$.

Conversely, suppose that $\langle a \rangle = \langle b \rangle$. Then $a = bc$ for some $c \in D$ and $b = ad$ for some $d \in D$. Hence $b = bcd$. As $b \neq 0$ we deduce that $1 = cd$ so that $c \in U(D)$. Thus $a/b = c \in U(D)$. ■

1.4 Principal Ideal Domains

An important class of integral domains are those in which every ideal is principal.

Definition 1.4.1 (Principal ideal domain) *An integral domain D is called a principal ideal domain if every ideal in D is principal.*

We begin by giving an example of an integral domain in which every ideal is principal.

Theorem 1.4.1 *$\mathbb{Z}$ is a principal ideal domain.*

Proof: Let I be an ideal of $\mathbb{Z}$. If $I = \{0\}$ then $I = \langle 0 \rangle$ is a principal ideal. Thus we may suppose that $I \neq \{0\}$. Hence I contains a nonzero element a. As both a and $-a$ belong to I, we can suppose that $a > 0$. Hence I contains at least one positive integer, namely a.

We let m denote the least positive integer in I. Dividing a by m, we obtain integers q and r such that $a = mq + r$ and $0 \leq r < m$. As $a \in I$ and $m \in I$, we have $r = a - mq \in I$. This contradicts the minimality of m unless $r = 0$, in which case $a = mq$; that is, $I = \langle m \rangle = m\mathbb{Z}$. ■

Theorems 1.3.1 and 1.4.1 show that the set of ideals of $\mathbb{Z}$ is $\{k\mathbb{Z} \mid k \in \{0, 1, 2, \ldots\}\}$. Moreover, if I is an ideal of $\mathbb{Z}$ then it is generated by the least positive integer in I.

Other examples of principal ideal domains will be given in Chapter 2 where we discuss Euclidean domains.

Theorem 1.4.2 *In a principal ideal domain, an irreducible element is prime.*

Proof: Let p be an irreducible element in a principal ideal domain D. Suppose that $p \mid ab$, where $a, b \in D$. If $p \nmid a$ we let I be the ideal $\langle p, a \rangle$ of D. As D is a principal ideal domain there is an element $c \in D$ such that $I = \langle c \rangle$. As $a \in I$ and $p \in I$ we must have $c \mid a$ and $c \mid p$. If $c \sim p$ then $p \mid a$, contradicting $p \nmid a$. Hence $c \not\sim p$, and as p is irreducible, c must be a unit. Thus there exists $d \in D$ such that $cd = 1$. Now $c \in \langle a, p \rangle$ so there exist $x, y \in D$ such that $c = xa + yp$. Hence

$$1 = cd = dxa + dyp,$$

and so

$$b = (dx)ab + (bdy)p.$$

Since $p \mid ab$ this shows that $p \mid b$. Thus $p \mid a$ or $p \mid b$ and p is a prime element of D. ■

Theorem 1.4.3 *In a principal ideal domain, an element is irreducible if and only if it is prime.*

Proof: This follows immediately from Theorems 1.2.1 and 1.4.2. ■

Example 1.4.1 *It was noted in Section 1.2 that* 2 *is irreducible but not prime in* $\mathbb{Z}+\mathbb{Z}\sqrt{-5}$. *Hence, by Theorem 1.4.3, the integral domain* $\mathbb{Z}+\mathbb{Z}\sqrt{-5}$ *is not a principal ideal domain. Indeed the ideal* $\langle 2, 1+\sqrt{-5}\rangle$ *of* $\mathbb{Z}+\mathbb{Z}\sqrt{-5}$ *is not principal. This can be shown directly as follows. Suppose, on the contrary, that the ideal* $\langle 2, 1+\sqrt{-5}\rangle$ *is principal, that is,* $\langle 2, 1+\sqrt{-5}\rangle = \langle \alpha\rangle$ *for some* $\alpha \in \mathbb{Z}+\mathbb{Z}\sqrt{-5}$. *Hence* $2 \in \langle\alpha\rangle$ *and* $1+\sqrt{-5} \in \langle\alpha\rangle$ *so that* $\alpha \mid 2$ *and* $\alpha \mid 1+\sqrt{-5}$. *From the first of these, as* 2 *is irreducible in* $\mathbb{Z}+\mathbb{Z}\sqrt{-5}$, *it must be the case that* $\alpha \sim 1$ *or* $\alpha \sim 2$. *If* $\alpha \sim 2$ *then* $2 \mid 1+\sqrt{-5}$, *which is impossible as* $\frac{1+\sqrt{-5}}{2} = \frac{1}{2}+\frac{1}{2}\sqrt{-5} \notin \mathbb{Z}+\mathbb{Z}\sqrt{-5}$. *Hence* $\alpha \sim 1$, *and so* $\langle 2, 1+\sqrt{-5}\rangle = \langle 1\rangle$. *This shows that* 1 *is a linear combination of* 2 *and* $1+\sqrt{-5}$ *with coefficients from* $\mathbb{Z}+\mathbb{Z}\sqrt{-5}$; *that is, there exist* $x, y, z, w \in \mathbb{Z}$ *such that*

$$1 = (x+y\sqrt{-5})2 + (z+w\sqrt{-5})(1+\sqrt{-5}).$$

Equating coefficients of 1 *and* $\sqrt{-5}$, *we obtain*

$$1 = 2x+z-5w,\ 0 = 2y+z+w.$$

The difference of these equations yields

$$1 = 2(x-y-3w),$$

which is clearly impossible as the left-hand side is an odd integer and the right-hand side is an even integer. Hence the ideal $\langle 2, 1+\sqrt{-5}\rangle$ *is not principal in* $\mathbb{Z}+\mathbb{Z}\sqrt{-5}$.

Definition 1.4.2 (Greatest common divisor) *Let* D *be a principal ideal domain and let* $\{a_1,\ldots,a_n\}$ *be a set of elements of* D. *Then the ideal* $\langle a_1,\ldots,a_n\rangle$ *is a principal ideal. A generator of this ideal is called a greatest common divisor of* $a_1,\ldots,a_n$.

Let D be a principal ideal domain. If a and b are greatest common divisors of $a_1,\ldots,a_n \in D$ then

$$\langle a\rangle = \langle a_1,\ldots,a_n\rangle = \langle b\rangle,$$

so that, by Theorem 1.3.1, $a \sim b$. We write $(a_1,\ldots,a_n)$ for a greatest common divisor of $a_1,\ldots,a_n$, understanding that $(a_1,\ldots,a_n)$ is only defined up to a unit. We note that $(a_1,\ldots,a_n)=0$ if $a_1=\cdots=a_n=0$. Also $(a_1,\ldots,a_n) = (a_1,\ldots,a_{n-1})$ if $a_n=0$. Furthermore,

$$a \in \langle a\rangle = \langle a_1,\ldots,a_n\rangle,$$

so that

$$a = r_1 a_1 + \cdots + r_n a_n$$

for some $r_1, \ldots, r_n \in D$. Thus if $c \in D$ is such that

$$c \mid a_j \ (j = 1, 2, \ldots, n)$$

then

$$c \mid a.$$

Moreover, for $j = 1, 2, \ldots, n$, we have

$$a_j \in \langle a_1, \ldots, a_n \rangle = \langle a \rangle$$

so that

$$a \mid a_j.$$

This justifies calling a "a greatest common divisor" of $a_1, \ldots, a_n$. The elements $a_1, \ldots, a_n$ are called relatively prime if $(a_1, \ldots, a_n)$ is a unit, that is,

$$\langle a_1, \ldots, a_n \rangle = \langle 1 \rangle = D.$$

It is easy to verify that

$$(a_1, \ldots, a_{n-1}, a_n) = ((a_1, \ldots, a_{n-1}), a_n),$$

so that a greatest common divisor can be obtained by finding a succession of greatest common divisors of pairs of elements, that is, if $(a_1, a_2) = b$ then $(a_1, a_2, a_3) = (b, a_3)$, etc.

In the next theorem we use our knowledge of primes and irreducibles in a principal ideal domain to give conditions under which a prime p can be expressed as $u^2 - mv^2$ or $mv^2 - u^2$ for some integers u and v, where m is a given nonsquare integer.

Theorem 1.4.4 *Let m be a nonsquare integer such that $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ is a principal ideal domain. Let p be an odd prime for which the Legendre symbol*

$$\left(\frac{m}{p} \right) = 1.$$

Then there exist integers u and v such that

$$p = u^2 - mv^2 \textit{ if } m < 0, \textit{ or if } m > 0,$$

and there are integers T, U such that $T^2 - mU^2 = -1$,

$$p = u^2 - mv^2 \textit{ or } mv^2 - u^2, \textit{ if } m > 0,$$

and there are no integers T, U with $T^2 - mU^2 = -1$.

Proof: As $\left(\frac{m}{p}\right) = 1$, there exists an integer x such that $x^2 \equiv m \pmod{p}$. Thus

$$p \mid (x + \sqrt{m})(x - \sqrt{m})$$

in $\mathbb{Z} + \mathbb{Z}\sqrt{m}$. Clearly $\frac{x \pm \sqrt{m}}{p} = \frac{x}{p} \pm \frac{1}{p}\sqrt{m} \notin \mathbb{Z} + \mathbb{Z}\sqrt{m}$ so that

$$p \nmid x \pm \sqrt{m}.$$

Hence p is not a prime in $\mathbb{Z} + \mathbb{Z}\sqrt{m}$. As $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ is a principal ideal domain, by Theorem 1.4.3 p is not irreducible in $\mathbb{Z} + \mathbb{Z}\sqrt{m}$. Hence

$$p = (u + v\sqrt{m})(w + t\sqrt{m}) \tag{1.4.1}$$

for some $u + v\sqrt{m} \in \mathbb{Z} + \mathbb{Z}\sqrt{m}$ and $w + t\sqrt{m} \in \mathbb{Z} + \mathbb{Z}\sqrt{m}$, where neither $u + v\sqrt{m}$ nor $w + t\sqrt{m}$ is a unit in $\mathbb{Z} + \mathbb{Z}\sqrt{m}$. From (1.4.1) we deduce that

$$p - (uw + tvm) = (ut + vw)\sqrt{m}.$$

As m is not a square, $\sqrt{m} \notin \mathbb{Q}$, so that

$$p - (uw + tvm) = ut + vm = 0.$$

Then

$$p^2 = (uw + tvm)^2 = (uw + tvm)^2 - m(ut + vm)^2$$

so that

$$p^2 = (u^2 - mv^2)(w^2 - mt^2). \tag{1.4.2}$$

As $m, u, v, w, t \in \mathbb{Z}$ and $m \in \mathbb{N}$, we see that $u^2 - mv^2 \in \mathbb{Z}$ and $w^2 - mt^2 \in \mathbb{Z}$. Moreover, $u^2 - mv^2 \neq \pm 1$ and $w^2 - mt^2 \neq \pm 1$, as $u + v\sqrt{m}$ and $w + t\sqrt{m}$ are not units in $\mathbb{Z} + \mathbb{Z}\sqrt{m}$. Thus, from (1.4.2), as p is a prime, we must have $\pm p = u^2 - mv^2 = w^2 - mt^2$. Hence there are integers u and v such that $p = u^2 - mv^2$ or $-(u^2 - mv^2)$.

If $m < 0$ then $u^2 - mv^2 > 0$, so we must have $p = u^2 - mv^2$.

If $m > 0$, $p = -(u^2 - mv^2)$, and there exist integers T and U such that $T^2 - mU^2 = -1$ then $p = u'^2 - mv'^2$ with $u' = Tu + mUv$, $v' = Uu + Tv$. ∎

In Chapter 2 we give some nonsquare values of m for which $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ is a principal ideal domain. Then, by Theorem 1.4.4, we know that for those odd primes p for which $\left(\frac{m}{p}\right) = 1$ there are integers u and v such that $p = u^2 - mv^2$ or $mv^2 - u^2$. For a general positive integer m it is a difficult problem to decide which primes are expressible as $u^2 - mv^2$ with $u, v \in \mathbb{Z}$. The reader interested in knowing more about this problem should consult Cox [2].

In the next theorem we give conditions that ensure that a prime p can be expressed in the form $u^2 + uv + \frac{1}{4}(1 - m)v^2$ or $-(u^2 + uv + \frac{1}{4}(1 - m)v^2)$