Foundations of Ring Arithmetic

Stephanie N. Reyes

Last Updated: December 11, 2019

This treatise is adapted from the thesis
submitted by the author as partial fulfillment of the requirements
for her degree of Master of Science in Pure Mathematics
in the Graduate College of the
University of Illinois at Chicago, 2019

Chicago, Illinois

This treatise **has not been approved** by the MS Thesis Defense Committee members:

Alina Carmen Cojocaru, *Chair and Advisor*;
Nathan Jones; and
Ramin Takloo-Bighash

assembled as partial fulfillment of the requirements for the author's degree of Master of Science in Pure Mathematics. Any nonstandard typesetting, grammar and terminology included in this treatise reflects the stylistic preferences of the author and **does not** necessarily imply any lack of expertise or common sense on the part of the committee members; the committee's sensible recommendations were followed in the submitted version of the author's thesis, but the author chose to respectfully ignore the committee's recommendations on *style* in completing this treatise.

Contents

Summary

This treatise explores the "galaxy" of integrally closed domains through arithmetic properties of rings, starting with standard domain class inclusions

$$\{\text{Euclidean domains}\} \subsetneq \{\text{PIDs}\} \subsetneq \{\text{UFDs}\} \subsetneq \{\text{GCDDs}\},$$

and with a special emphasis on square number fields and their rings of integers, square number rings.

Through this treatise, the author demonstrates the breadth of her background, training and ability in writing mathematics; some portions are written and typeset as standard mathematical prose, others are structured to break and flow like poetry. In the latter case, exposition is secondary to symbolic manipulation.

Acknowledgements

Sponsors

Diversifying Faculty in Illinois (DFI) Fellowship, 2020–YY;

Graduate Assistance in Areas of National Need (GAANN) Fellowship, 2016–17;

Mellon-Mays Undergraduate Fellowship (MMUF), 2010–16;

Mentors

Ramin Takloo-Bighash, 2020–YY;

Rodrigo Bañuelos, FA2017;

Edray Goins, AY2016–17;

Education

California Institute of Technology

BS, Mathematics, 2016

Advisors

Alina Carmen Cojocaru (UIC);

Matthias Flach (Caltech)

Commutative algebra and number theory

Selected Research Projects

- Lattice-based Fully Homomorphic Encryption

  Mellon-Mays Summer Research, 2014

  Mentor: Lily Khadjavi

  - Presentation: Infinite Possibilities Conference, 2015
  - Presentation: Mellon-Mays Regional Conference, 2014

- Cohomology of Hilbert scheme points on K3 surfaces

  Mellon-Mays Summer Research, 2012

  Mentor: Andrei Jorza

- Algebraic Hecke characters which are rational over $\mathbb{Q}$

  Caltech SURF, 2011

  Mentor: Matthias Flach

  - Presentation: Caltech SURF Seminar Day, 2011

Selected Conferences Attended

- Underrepresented Students in Topology and Algebra Research Symposium (USTARS). 2018, 2019;
- Algebra Extravaganza. Philadelphia, 2018;
- Mellon-Mays Regional Conference. UCLA, 2013;
- AMS/MAA Joint Mathematics Meetings. San Diego, 2013;
- Southern California Number Theory Day. Pasadena, 2011

Dedication

To my loving spouse and life partner, Christopher Perez. We did it, man.

USTARS (2018, 2019);

EDGE 2016;

MMUF (Grad Studies Grant 2017);

MMUF REU (2012, 2013, 2014);

SURF (2011);

FSRI (2010);

SMaRT (2010).

Service

AWMath Student Chapter (President, 2019–YY);

SMaRT Camp Counselor and TA (2012);

FSRImath TA (2012, 2013).

I. Catalog of Arithmetic Properties in Domains

Throughout this part, I use A to denote an *integral domain.* That is, I take A to be a *commutative, unital ring with* $1_A \neq 0$ *and no zero divisors.* I use the term *domain* to mean *integral domain* for convenience. One should assume domains are commutative unless otherwise specified. For such a domain, I use $U(A)$ to denote its group of units.

Any corrections or suggestions should be sent to stephanie @ math.uic.edu.

1 Divisibility Class Arithmetic

In this section, we formally explore *divisibility* as a relational property between domain elements. In particular, this section contains a rigorous proof that *divisibility association* gives an equivalence relation on a domain.

Definition 1.1. An element $a \in A$ **divides** an element $b \in A$
(equivalently, an element $b \in A$ **is a multiple of** an element $a \in A$)
if there exists $c \in A$ such that $b = a\,c.$

Notational Note. If $a,\ b \in A$ are such that a divides b
(equivalently, if $b \in A$ is a multiple of $a \in A$), we write $a \mid b.$
Further, if $a \mid b,$ we may say that "a is a **divisor** or **factor** of $b.$"

1.1 Domain Divisibility Properties

Proposition 1.2 (Domain Divisibility Properties)**.** For $a,\ b,\ c,\ d_1, \ldots, d_n \in A$, the following divisibility properties hold:

i. (*Reflexivity*) Any element $a \in A$ divides itself. That is, if $a \in A$ then $a \mid a$.

Proof. There is an identity element $1 \in A$ such that, for every $a \in A$,

$$a \quad = \quad a\,1 \quad = \quad 1 \cdot a. \qquad (*)$$

Note that $(*)$ is equivalent to "a is a multiple of a" which is equivalent to "a divides a" by Definition 1.1. Thus, if $a \in A$ then $a \mid a$. □

ii. (*Symmetry*) The elements $a \in A$ and $b \in A$ divide each other if and only if they differ by a unit factor. That is, $a \mid b$ and $b \mid a$ if and only if there exists $u \in U(A)$ such that $b = u \cdot a$.

$\overset{Proof}{\Longrightarrow}$. First, assume $a \mid b$ and $b \mid a$. Then, there exist $c, c' \in A$ such that

$$a \quad = \quad b\,c' \quad = \quad c'\,b \qquad (\mathbf{a})$$

$$\text{and} \qquad b \quad = \quad a\,c \quad = \quad c\,a. \qquad (\mathbf{b})$$

Substituting Equation (**a**) into Equation (**b**), we have

$$1 \cdot b \quad = \quad b \quad = \quad c\,(c'\,b) \quad = \quad (c'\,c)\,b. \qquad (\mathbf{c})$$

Since $1 \in A$ is unique, Equation (**c**) implies that $1 = c'\,c$ which further implies that $c =: u \in U(A)$. Thus, $b = u \cdot a$, as desired. □

$\overset{Proof}{\Longleftarrow}$. Now, assume there is some $u \in U(A)$ such that

$$b \quad = \quad u \cdot a \quad = \quad a\ u. \tag{$*$}$$

Since $b = a\ u$, we can say that $a \mid b$ by Definition 1.1.

Further, since $u \in U(A)$, there is some $u' \in A$ such that

$$u\ u' \quad = \quad u'\ u \quad = \quad 1.$$

Multiplying both sides of Equation $(*)$ by u' gives

$$\begin{aligned} b\ u' \quad &= \quad (a\ u)\ u' \\ &= \quad a\ (u\ u') \\ &= \quad a\ 1 \\ &= \quad a. \end{aligned}$$

Thus, $a = b\ u'$ which means that $b \mid a$ by Definition 1.1. □

iii. (*Transitivity*) All divisors of an element divide all multiples of that element.

That is, if $a \mid b$ and $b \mid c$ then $a \mid c$.

Proof. Since $a \mid b$, there is some $d \in A$ such that

$$b \quad = \quad a\ d \tag{\textbf{a}}$$

and, since $b \mid c$, there is some $d' \in A$ such that

$$c \quad = \quad b\ d'. \tag{\textbf{b}}$$

We now use Equation (**a**) to re-express Equation (**b**) as

$$c \quad = \quad (a\ d)\ d' \quad = \quad a\ (d\ d').$$

Thus, there is an element $c' := dd' \in A$ such that $c \ = \ a\ c'$.

Thus, $a \mid c$. □

iv. If an element divides all elements of a finite subset of A, then that element divides any A-linear combination of subset elements.

That is, if $a \mid d_i$ for all $1 \leqslant i \leqslant n$, then $a \ \mid \ a_1\ d_1 + \cdots + a_n\ d_n$ for any subset $\{a_1, \ldots, a_n\} \subset A$.

Proof. Given that $a \mid d_i$ for all $1 \leqslant i \leqslant n$, we know that there exists some $c_i \in A$ such that $d_i \ = \ a\ c_i$ for all $1 \leqslant i \leqslant n$. Thus, for any subset $\{a_1, \ldots, a_n\} \subset A$, we have

$$\begin{aligned} a_1\ d_1 + \cdots + a_n\ d_n \quad &= \quad a_1\ (a\ c_1) + \cdots + a_n\ (a\ c_n) \\ &= \quad (a_1\ a)\ c_1 + \cdots + (a_n\ a)\ c_n \\ &= \quad (a\ a_1)\ c_1 + \cdots + (a\ a_n)\ c_n \\ &= \quad a\ (a_1\ c_1) + \cdots + a\ (a_n\ c_n) \\ &= \quad a\ (a_1\ c_1 + \cdots + a_n\ c_n). \end{aligned}$$

Since $c := a_1 c_1 + \cdots + a_n c_n \in A$ for any subset $\{a_1, \ldots, a_n\} \subset A$, we have

$$(a_1\ d_1 + \cdots + a_n\ d_n) \quad = \quad a\ c$$

which means that $a \ \mid \ a_1\ d_1 + \cdots + a_n\ d_n$. □

v. If A is a domain and $a,\ b \in A$ then $a \mid b$ if and only if $Ab \subseteq Aa$.

$\overset{Proof}{\Longrightarrow}$. Assuming $a \mid b$, we know that there exists $c \in A$ such that $c\ a = b$. This implies that $b \in Aa \quad := \quad \{\ c\ a\ :\ c \in A\ \}$ and further implies

$$\begin{aligned} Ab \subseteq AAa \quad &:= \quad \{d\ c\ a\ :\ d,\ c \in A\} \\ &= \quad \{(d\ c)\ a\ :\ d,\ c \in A\} \\ &= \quad \{a'\ a\ :\ a' = d\ c \in A \quad \forall d,\ c \in A\} \\ &= \quad \{a'\ a\ :\ a' \in A\} \\ &= \quad Aa, \end{aligned}$$

concluding the proof. □

$\overset{Proof}{\Longleftarrow}$. Assuming $Ab \subseteq Aa$, we know that for all $\beta \in Ab$ there exists an $\alpha \in A$ such that $\beta = \alpha\ a$. Since $1 \in A$ and since $b = 1 \cdot b \in Ab$, this means that there exists an $\alpha_b \in A$ such that $b = \alpha_b\ a$, implying that $a \mid b$. □

1.2 Divisibility Associate Equivalence

In this subsection, we explicate the *reflexive*, *symmetric* and *transitive* properties of divisibility given above into a formal equivalence relation, called *divisibility association*.

Definition 1.3. If $a \in A$ and $b \in A$ differ by a unit factor, we call a and b **associates** with respect to divisibility
(equivalently, we say a and b are **associated in divisibility**).
In other words, if $a,\ b \in A$ are such that $u \cdot b = a$ for some unit $u \in U(A)$, we say that "a is **associate** to b with respect to divisibility" and write $a \doteqdot b$.

Proposition 1.4. Divisibility association gives an equivalence relation on A.

Remark. The following proofs are analogous to the proofs in Proposition 1.2.

i. Reflexive. For every element $a \in A$, we have that $a \doteqdot a$.

Recall. Divisibility is a *reflexive* property.

That is, for every $a \in A$, we have $a \mid a$.

Proof. The multiplicative identity element $1 \in A$ is a unit and satisfies

$$a = a\,1 = 1 \cdot a.$$

Thus, $a \doteqdot a$ by Definition 1.3. □

ii. Symmetric. For any two elements $a,\ b \in A$ such that $a \doteqdot b$, we also have that $b \doteqdot a$.

Recall. Divisibility is a *symmetric* property.

That is, $a \mid b$ and $b \mid a$ if and only if there exists $u \in U(A)$ such that $u \cdot a = b$.

Proof. If $a \doteqdot b$, there exists $u \in U(A)$ such that $u \cdot a = b$.
Further, since $u \in U(A)$, there is some $u^{-1} \in U(A)$ such that

$$u\,u^{-1} = u^{-1}\,u = 1.$$

Thus, $u^{-1} \cdot b = u^{-1} \cdot (u \cdot a) = (u^{-1}\,u) \cdot a = 1 \cdot a = a$,
implying that $u^{-1} \cdot b = a$. Hence, $b \doteqdot a$. □

iii. Transitive. If $a, b, c \in A$ are such that $a \doteqdot b$ and $b \doteqdot c$, then $a \doteqdot c$.

Recall. Divisibility is a *transitive* property.

That is, if $a \mid b$ and $b \mid c$ then $a \mid c$.

Proof. Since $a \doteqdot b$, there is some $u \in U(A)$ such that

$$u \cdot a \quad = \quad b \tag{\textbf{a}}$$

and, since $b \doteqdot c$, there is some $u' \in U(A)$ such that

$$u' \cdot b \quad = \quad c. \tag{\textbf{b}}$$

Using Equation ($\mathbf{a}$), we re-express Equation ($\mathbf{b}$) as

$$c \quad = \quad u' \cdot (u \cdot a) \quad = \quad (u' \; u) \cdot a.$$

Thus $u' \, u \in U(A)$, which means that $a \doteqdot c$. □

We now encounter the first distinctive class of divisibility associates covered in this treatise. The following remark states that the group of units $U(A)$ of a domain A form an equivalence class of elements which are associate to the multiplicative identity element $1 \in A$. In other words, divisibility association classifies all invertible elements in a domain as equivalent to the multiplicative identity.

Remark 1.5. An element of A is an associate of the multiplicative identity in A if and only if it is a unit (equivalently, $a \doteqdot 1$ if and only if $a \in U(A)$).

$\overset{Proof}{\Longrightarrow}$. First, assume $a \doteqdot 1$. By Definition 1.3, this means that there is some $u \in U(A)$ such that $u \cdot a \; = \; 1$. Thus, $a \in U(A)$. □

$\overset{Proof}{\Longleftarrow}$. Now, assume $a \in U(A)$. This means there exists some $a' \in U(A)$ such that $a \, a' \; = \; a' \, a \; = \; 1$. Thus, $a \doteqdot 1$ by definition. □

Remark 1.6. If A is a domain and $a,\ b \in A$ then

i. $a \doteqdot b$ if and only if $Ab = Aa$; and

ii. Remark 1.5 holds $\iff$ $Aa = A$.

i. $\overset{Proof}{\Longrightarrow}$. First, assume $a \doteqdot b$ (similarly, $b \doteqdot a$). Then, there exists $u \in U(A)$ such that $u\ a = b$ (similarly, there exists $u' \in u(A)$ such that $u'\ b = a$). This implies that $b \in Aa$ (similarly, $a \in Aa$). Thus $Ab \subseteq Aa$ (similarly, $Aa \subseteq Ab$), implying that $Ab = Aa$. □

i. $\overset{Proof}{\Longleftarrow}$. Now, assume $Ab = Aa$. This implies that $Ab \subseteq Aa$ (and that $Ab \supseteq Aa$), further implying that for all $\beta \in Ab$ there exists $\alpha \in A$ such that $\beta = \alpha\ a$ (and further implying that for all $\alpha \in Aa$ there exists $\beta \in A$ such that $\alpha = \beta\ b$). Since $b = 1 \cdot b \in Ab$, this means that there exists an $\alpha_b \in A$ such that $b = \alpha_b\ a$ (and since $a = 1 \cdot a \in Aa$, this means that there exists $\beta_a \in A$ such that $a = \beta_a\ b$). Thus,

$$\begin{aligned} b &= \alpha_b\ (\beta_a\ b), \\ 1 \cdot b &= (\alpha_b\ \beta_a)\ b, \\ 1 &= \alpha_b\ \beta_a, \end{aligned}$$

implying that $\alpha_b,\ \beta_a \in U(A)$ and, finally, implying that $a \doteqdot b$. □

ii. $\overset{Proof}{\Longrightarrow}$. Assume there exists $u \in U(A) \subseteq A$ such that $u \cdot a = 1$. This implies that $1 \in Aa$ which further implies that $A \subseteq AAa$. Thus, $A \subseteq Aa$. Further, assuming Remark 1.5, it is clear that $Aa \subseteq A$. Thus, since $Aa \subseteq A$ and $A \subseteq Aa$ we have $Aa = A$. □

ii. $\overset{Proof}{\Longleftarrow}$. If $Aa = A$, there exists $b \in A$ such that $b\ a = 1$ which implies that $a \in U(A)$ if and only if $a = 1$. □

2 Specific Classes of Associates

In the previous section, we formally defined divisibility as an equivalence relation. Now, we deepen our understanding of this relational property by defining specific divisibility classes of shared factors/multiples for pairs of domain elements.

In this discussion of *greatest common divisors* and *least common multiples* we take care to emphasize that the existence of such classes of associates is not always guaranteed for any given pair of elements in an arbitrary domain. We introduce *greatest common divisor domains*, domains for which there exists a greatest common divisor for every pair of elements, and give an example of a domain which is not a greatest common divisor domain.
Any corrections or suggestions should be sent to stephanie @ math.uic.edu.

2.1 Greatest Common Divisors

Definition 2.1. An element $d \in A$ is called a **greatest common divisor** of two elements $a,\ b \in A$ if

i. d divides a $(d \mid a)$,

ii. d divides b $(d \mid b)$ and

iii. any element which divides both a and b also divides d

(any $d' \in A$ such that $d' \mid a$ and $d' \mid b$ is also such that $d' \mid d$).

(Clarifying) Remark 2.2. If such an element $d \in A$ exists for the pair $a,\ b \in A$, then it is unique *only up to association in divisibility.* I use $\mathbf{gcd}(a,b)$ to denote the *equivalence class* of associates of d. I may also say that $d \in \mathbf{gcd}(a,b)$. To denote a *representative element* of the equivalence class, I may use $\gcd(a,b)$.

Proposition 2.3. Suppose A is a domain for which there exists $\gcd(a,b) \in A$ for every pair of elements $a,\ b \in A$.

Then, letting $a,\ b,\ c \in A$, the following properties hold:

i. Any greatest common divisor of an arbitrary nonzero element and the additive identity, zero, is associate to the nonzero arbitrary element $(\gcd(a,0)\ \doteqdot\ a)$;

Proof. Since $a \mid a$ and $a \mid 0$, it follows that $a \mid \gcd(a,0)$.

Since $\gcd(a,0) \mid a$ by definition, we conclude $\gcd(a,0) \doteqdot a$. □

ii. $\gcd(a,b) \doteqdot a$ if and only if $a \mid b$;

$\overset{Proof}{\Longrightarrow}$. If $\gcd(a,b) \doteqdot a$, there exists $u \in U(A)$ such that $\gcd(a,b) = u \cdot a$. Thus, $a \mid \gcd(a,b)$ and, because $\gcd(a,b) \mid b$, we can conclude $a \mid b$. □

$\overset{Proof}{\Longleftarrow}$. Suppose $a \mid b$. Then $a \mid a$, $a \mid b$, and any d' such that $d' \mid a$ and $d' \mid b$ trivially satisfies $d' \mid a$. So $\gcd(a,b) \doteqdot a$. □

iii. if $d\ =\ \gcd(a,b)$ is a representative greatest common divisor of distinct, nonzero elements $a,\ b \in A$ and if $a',\ b' \in A$ are such that $a\ =\ d\,a'$ and $b\ =\ d\,b'$, then $\gcd(a',b') \doteqdot 1$;

Proof. Let d' be such that $d' \mid a'$ and $d' \mid b'$. Then $d\,d' \mid\ d\,a' = a$ and $d\,d' \mid\ d\,b' = b$, so $d\,d' \mid d$ because $d = \gcd(a,b)$. Then there exists $c \in A$ such that $d\ =\ c\,d\,d'$, so $c\,d' = 1$ and thus $d' \in U(A)$. Thus we have that $\gcd(a',b') \doteqdot 1$. □

iv. $\gcd(ac,bc)\ \doteqdot\ c \cdot \gcd(a,b)$; and

Proof. Let $d\ :=\ \gcd(a,b)$ and let d' be such that $d' \mid a\,c$ and $d' \mid b\,c$. By part **iii.**, there exists a' and b' such that $a\ =\ d\,a'$, $b\ =\ d\,b'$, and $\gcd(a',b') \doteqdot 1$. Then $d' \mid c\,d\,a'$ and $d' \mid c\,d\,b'$. If $d' \nmid c\,d$ there would exist d'' which is not a unit such that $d' \mid c\ d\ d''$, $d'' \mid a'$, and $d'' \mid b'$. But, because $\gcd(a', b') \doteqdot 1$, d'' would be a unit. Thus $d' \mid c\ d$, so $\gcd(ac, bc) \doteqdot c \cdot \gcd(a, b)$. □

v. $\gcd(a,\ \gcd(b, c)) \doteqdot \gcd(\ \gcd(a, b),\ c)$.

Proof. Let $d := \gcd(a, b)$ and $e := \gcd(b, c)$. Then $\gcd(d, c) \mid d$ and $\gcd(d, c) \mid c$, so $\gcd(d, c) \mid a$ and $\gcd(d, c) \mid b$ and thus $\gcd(d, c) \mid e$. Then $\gcd(d, c) \mid \gcd(a, e)$. Let d' be such that $d' \mid a$ and $d' \mid e$. Then $d' \mid b$ and $d' \mid c$, so $d' \mid d$ and thus $d' \mid \gcd(d, c)$. Thus $\gcd(a,\ \gcd(b, c)) \doteqdot \gcd(\ \gcd(a, b),\ c)$. □

Definition 2.4. If A is a domain for which there exists at least one greatest common divisor $\gcd(a, b)$ of every pair of elements $a,\ b \in A$ up to association by division, we define **the greatest common divisor of a finite subset** $\{a_1, \ldots, a_n\} \subset A$ of nonzero, nonunital elements inductively. That is, we define the following association

$$\gcd(a_1, \ldots, a_n) \doteqdot \gcd(\ \gcd(a_1, \ldots, a_{n-1}),\ a_n).$$

2.2 Least Common Multiples

Definition 2.5. An element $m \in A$ is called a **least common multiple** of two elements $a,\ b \in A$ if

i. m is a multiple of a, $(a \mid m)$

ii. m is a multiple of b, $(b \mid m)$ and

iii. any $m' \in A$ such that $a \mid m$ and $b \mid m$ is also such that $m' \mid m$.

(Clarifying) Remark 2.6. If such an element $m \in A$ exists for the pair $a,\ b \in A$, then it is unique *only up to association in divisibility.* We use $\mathbf{lcm}(a,b)$ to denote the *equivalence class* of associates of m. We may also say that $m \in \mathbf{lcm}(a,b)$. To denote a *representative element* of the equivalence class, we use $\operatorname{lcm}(a,b)$.

2.3 Greatest Common Divisor Domains

Definition 2.7. If A is a domain for which there exists a greatest common divisor for any two elements $a,\ b, \in A$, then we call A a **greatest common divisor domain** (abbr. **GCDD**)

Arithmetic Characterization Theorem for Greatest Common Divisor Domains

Theorem 2.8. Let A be a domain. Then the following are equivalent:

i. For any $a,\ b \in A$ there exists $d := \gcd(a,b) \in A$.

ii. For any $a,\ b \in A$ there exists $\mu := \operatorname{lcm}(a,b) \in A$.

iii. For any $a,\ b \in A$ there exists $\mu \in A$ such that
$Aa \cap Ab \ = \ A\mu$.

Claim 2.8.1 (ii. ⇒ iii.). Let $a,\ b \in A$. If there exists some

$$\mu := \operatorname{lcm}(a,b) \in \mathbf{lcm}(a,b)$$

then $Aa \cap Ab = A\mu$.

Proof. First, we want to show that $Aa \cap Ab \supseteq A\mu$. By Definition 2.5, this means $a \mid \mu$ and $b \mid \mu$ which, by Proposition 1.2, implies that $A\mu \subseteq Aa$ and that $A\mu \subseteq Ab$. Thus, $Aa \cap Ab \supseteq A\mu$.

Now, we want to show that $Aa \cap Ab \subseteq A\mu$. Note that $\mu \in Aa$ and $\mu \in Ab$ which implies that there exist elements $\alpha,\ \beta \in A$ such that $\mu = \alpha a$ and $\mu = \beta b$; in other words, it implies that $a \mid \mu$ and $b \mid \mu$. Since $\mu = \operatorname{lcm}(a, b)$, we have $\mu \mid m$ for any $m \in Aa \cap Ab$. So, $Am \subseteq A\mu$ and, in particular, $m \in A\mu$. Then we conclude that $Aa \cap Ab \subseteq A\mu$. Thus, $Aa \cap Ab = A\mu$. □

Claim 2.8.2 (iii. ⇒ ii.). If there exists some $\mu \in A$ such that $Aa \cap Ab = A\mu$ for all pairs $a,\ b \in A$ then $\mu := \operatorname{lcm}(a, b) \in \mathbf{lcm}(a, b)$.

Proof. Let $a, b \in A$. Assume there is an element $\mu \in A$ such that $Aa \cap Ab = A\mu$ for all pairs $a,\ b \in A$. By basic set theory, this implies that $\mu \in Aa$ and that $\mu \in Ab$. So, $a \mid \mu$ and $b \mid \mu$, by Proposition 1.2. (Note that we have shown that μ satisfies Definition 2.5.i. and 2.5.ii.)

Now, take any $m \in A$ such that $a \mid m$ and $b \mid m$, that is, take $m \in A$ to be an arbitrary common divisor of both a and b. Then $m \in Aa$ and $m \in Ab$ which implies that $m \in Aa \cap Ab$ and, by assumption, that $m \in A\mu$. So, there is some $c \in A$ such that $m = c\ \mu$ implying that $\mu \mid m$. (Note that we have shown that μ satisfies Definition 2.5.iii.) Thus, there is a least common multiple $\mu := \operatorname{lcm}(a, b) \in \mathbf{lcm}(a, b)$ for every pair of elements $a,\ b \in A$. □

Claim 2.8.3 (i. ⇒ ii.). If there exists an element $d \in A$ such that $d \in \mathbf{gcd}(a, b)$ for all pairs $a,\ b \in A$ then there exists $\mu \in A$ such that $\mu \in \mathbf{lcm}(a, b)$ for all pairs $a,\ b \in A$.

Proof. In the case where $a,\ b \in A$ are such that $ab = 0$, we have $\operatorname{lcm}(a, b) = 0$.

So, assume there is some nonzero element $d := \gcd(a, b) \in A$ satisfying Definition 2.1 for an arbitrary pair $a,\ b \in A$ such that $ab \neq 0$. Then, by Proposition 2.3, there exist elements $a',\ b' \in A$ such that

$$a = d\ a', b = d\ b' \text{ and } \gcd(a', b') \doteqdot 1. \qquad (*)$$

Substituting (1) $a = da'$ and (2) $b = db'$ into the product $a\ b$ results in

$$a\ b = (d\ a')\ b = d\ (a'\ b) = d\ m \qquad (1)$$

$$a\ b = a\ (b'\ d) = (a\ b')\ d = m\ d, \qquad (2)$$

where $m = a'\ b = a\ b'$. But then $b \mid m$ and $a \mid m$ by Definition 1.1.

Now, let $m' \in A$ be any multiple of both a and b. That is, assume $m' \in A$ is such that $a \mid m'$ and $b \mid m'$. So, there exist $\alpha,\ \beta \in A$ such that $m' = a\ \alpha$ and $m' = b\ \beta$, which implies $m' = (d\ a')\ \alpha$ and $m' = (d\ b')$. Thus, $m' = d\ a'\ \alpha = d\ b'\ \beta$ implying that $a'\ \alpha = b'\ \beta$. This, along with Proposition 2.3, implies that

$$b'\ \gcd(\beta,\ \alpha) \doteqdot \gcd(b'\ \beta,\ b'\ \alpha) = \gcd(a'\ \alpha,\ b'\ \alpha)$$

which further implies that

$$b' \ \gcd(\beta,\ \alpha) \doteqdot \alpha \ \gcd(a',\ b') \doteqdot \alpha \ 1 \doteqdot \alpha$$

because $\gcd(a', b') \doteqdot 1$ (see $(*)$). Now, since $b' \ \gcd(a', b') \doteqdot \alpha$, we get that $b' \mid \alpha$. So, there is some $\alpha' \in A$ which is such that $\alpha = b' \ \alpha'$. Thus,

$$m' = a \ \alpha = a \ (b' \ \alpha') = (a \ b') \ \alpha' = m \ \alpha'$$

which, by Definition 1.1, means that $m \mid m'$ for any such $m' \in A$. We conclude that $m \in \mathbf{lcm}(a, b)$, as desired. □

Claim 2.8.4 (ii. ⇒ i.). If there exists an element $\mu \in A$ such that $\mu \in \mathbf{lcm}(a, b)$ for all pairs $a,\ b \in A$ then for all pairs $a,\ b \in A$ there exists $d \in A$ such that $d \in \mathbf{gcd}(a, b)$.

Proof. Let $a,\ b \in A$ be such that $ab = 0$. In this case, we have $\gcd(a, b) = 0$.

So, assume there is some nonzero element $m := \operatorname{lcm}(a, b) \in A$ satisfying Definition 2.5 for an arbitrary pair $a,\ b \in A$ such that $ab \neq 0$. Then, there exist elements $a',\ b' \in A$ such that

$$m = a \ a' = b \ b'.$$

Now, since $m = \operatorname{lcm}(a, b)$, $a \mid ab$ and $b \mid ab$, there is some $d \in A$ such that

$$a \ b = m \ d = (a \ a') \ d.$$

Thus, by left cancellation, $b = a' \; d$, which implies that $d \mid b$ by Definition 1.1.

Similarly, since $m = \operatorname{lcm}(a, b)$, $a \mid ab$ and $b \mid ab$, the $d \in A$ from above is also such that

$$a \; b = m \; d = (b' \; b) \; d = b' \; (b \; d) = b' \; d \; b.$$

So, by right cancellation, $a = b' \; d$ which implies that $d \mid a$ by Definition 1.1. Thus, d is a divisor of both a and b.

Now, let $d' \in A$ be any divisor of both a and b. That is, assume $d' \in A$ is such that $d' \mid a$ and $d' \mid b$. So, there exist α, $\beta \in A$ such that

$$a = d' \; \alpha \text{ and } b = d' \; \beta.$$

Setting $m' := d' \; \alpha \; \beta$, we obtain

$$m' = a \; \beta = \alpha \; b.$$

which implies that

$$d' \; m' = (d')^2 \; \alpha \; \beta = (d' \; \alpha) \; (d' \; \beta) = a \; b$$

and that a, $b \mid m'$. Further, since $m = \operatorname{lcm}(a, b)$, we know that $m' \mid m$ which implies that there is some $\gamma \in A$ such that $m' = m \, \gamma$.

Thus,

$$a\ b = d'\ m' = d'\ (m\ \gamma)$$

$$m\ d = (d'\ m)\ \gamma$$

$$= m\ d'\ \gamma.$$

So, $d = d'\gamma$ implying that $d' \mid d$. Therefore, by Definition 2.1 and Remark 2.2, $d \in \mathbf{gcd}(a,b)$, as desired. □

Theorem 2.9. If A is a domain satisfying any of the properties in Theorem 2.8, then

$$\gcd(a,b)\ \operatorname{lcm}(a,b) \doteqdot a\ b \text{ for any } a,\ b \in A.$$

Proof. If $d := \gcd(a,b) \in A$ is a greatest common divisor of nozero elements $a,\ b \in A,$ then there exist elements $a',\ b' \in A$ such that $a = d\ a'$ and $b = d\ b'$ with $\gcd(a',b') \doteqdot 1.$ Also, there exist $x,\ y \in A$ with $d = a\ x\ +\ b\ y. \ldots\ldots$ (1)

Thus, $d\ a'\ b = d\ a\ b' = d\ \mu$ with $a'\ b = a\ b' =: \mu \in A$ which implies that $a \mid \mu$ and $b \mid \mu$ and, in particular, $\mu\ d = a\ b. \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$ (2)

Similarly, if $m \in A$ is any common multiple of the $a,\ b \in A$ from above, then there exist elements $\alpha,\ \beta \in A$ such that $m = a\ \alpha$ and $m = b\ \beta. \ldots\ldots$ (3)

$$\begin{aligned} \text{Thus, } m\, d &= m\ (a\ x\ +\ b\ y) && \text{by (1)} \\ &= m\ a\ x\ +\ m\ b\ y \\ &= b\ \beta\ a\ x\ +\ a\ \alpha\ b\ y \\ &= a\ b\ (\beta\ x\ +\ \alpha\ y) && \text{by (3)} \\ &= \mu\ d\ (\beta\ x\ +\ \alpha\ y) && \text{by (2)} \\ \Longrightarrow\ m &= \mu(\beta\ x\ +\ \alpha\ y). \end{aligned}$$

So, $a \mid \mu$, $b \mid \mu$, and $\mu \mid m$ for any common multiple $m \in A$ of $a,\ b \in A$ which implies that $\mu \in \mathbf{lcm}(a,b)$ by Definition 2.5 and Remark 2.6.

Thus, $a\ b = d\ \mu \doteqdot \gcd(a,b)\ \operatorname{lcm}(a,b)$, as desired. □

Remark 2.10. If A is a domain for which there exists at least one greatest common divisor $\gcd(a,b) \in A$ (up to association by division) for every pair of elements $a,\ b \in A$, then we can express the **least common multiple of a finite subset** $\{a_1,\ldots,a_n\} \subset A$ of nonzero, nonunital elements in terms of the inductive definition of greatest common divisor. That is, given Definition 2.4, the following association holds

$$\operatorname{lcm}(a_1,\ldots,a_n)\ \gcd(a_1,\ldots,a_n) \doteqdot a_1\cdots a_n.$$

A Clarifying Non-Example

Theorem 2.11 ([Khu03]). There exist domains which are not GCDDs: for an integer $d \geqslant 3$ such that $d+1$ is not prime, and writing

$d+1=pk$ for some prime p and some integer $k \geqslant 2$, the domain

$$Z[\sqrt{-d}] := \{a + b\sqrt{-d}\}$$

has the property that p and $1+\sqrt{-d}$ have a greatest common divisor but not a least common multiple. In particular, as a consequence of Theorem 2.8, $\mathbb{Z}[\sqrt{-d}]$ is not a GCDD.

2.4 Primes and Irreducibles

Definition 2.12. A nonzero element $p \in A \setminus U(A)$ is called **prime** if, for any $a,\ b \in A$ such that $p \mid ab$, we have $p \mid a$ or $p \mid b$.

Definition 2.13. A nonzero element $q \in A \setminus U(A)$ is called **irreducible** if, for any $a, b \in A$ such that $q = ab$, we have $a \in U(A)$ or $a \doteqdot q$.

Note the following equivalent definition for an irreducible element.

Definition. A nonzero element $q \in A \setminus U(A)$ is called **irreducible** if, for any $a, b \in A$ such that $q = ab$, we have $a \in U(A)$ or $b \in U(A)$.

Arithmetic Characterization of Primes and Irreducibles

Theorem 2.14. Let A be a domain and $p,\ q \in A \setminus \{0\}$. Then, the following hold:

i. Prime Element $\iff$ Generates Prime Ideal. An element $p \in A \setminus \{0\}$ is prime if and only if Ap is a prime ideal;

$\overset{Proof}{\Longrightarrow}$. Assume $p \in A \setminus U(A)$ is prime and let $a,\ b \in A$ be such that $ab \in Ap$. This means that there is some $c \in A$ such that $(a\ b) = c\ p$ which implies that $p \mid ab$. Thus, $p \mid a$ or $p \mid b$ by Definition 2.12. This means that there exists $\alpha \in A$ such that $\alpha\, p = a$ or that there exists $\beta \in A$ such that $\beta\, p = b$. Thus, either $a \in Ap$ or $b \in Ap$ which implies that Ap is a prime ideal. □

$\overset{Proof}{\Longleftarrow}$. Now, assume $Ap \lhd A$ is prime and let $a,\ b \in A$ be such that $p \mid ab$. This means that there is some $c \in A$ such that $(a\ b) = c\ p$ which implies that $ab \in Ap$. Thus, a or $b \in Ap$ which implies there exists $\alpha \in A$ such that $\alpha\ p = a$ or there exists $\beta \in A$ such that $\beta\ p = b$. Thus, either $p \mid a$ or $p \mid b$ which implies that $p \in A$ is prime. □

ii. Irreducible Element $\Longleftrightarrow$ Generates Maximal Ideal. An element $q \in A \setminus \{0\}$ is irreducible if and only if Aq is maximal among principal ideals;

$\overset{Proof}{\Longrightarrow}$. Assume $q \in A \setminus U(A)$ is irreducible. We want so show that, if a principal ideal $Aa \lhd A$ is such that $Aa \supseteq Aq$ then $Aq = Aa$. If $a \in U(A)$, then $Aa = A$. So, let $a \in A \setminus U(A)$ be such that $Aq \subseteq Aa$. This means that any element $q' \in Aq$ can be written $q' = \alpha' a$ for some $\alpha' \in A$ and, in particular, there is some $\alpha \in A$ such that $\alpha\ a = q$. Since $q \in A$ is irreducible by assumption and since $a \notin U(A)$, then $a \div q$. Thus, $Aq = Aa$, implying that Aq is maximal among $Aa \lhd A$. □

$\overset{Proof}{\Longleftarrow}$. Assume $Aq \lhd A$ is maximal among all $Aa \lhd A$ and let $a,\ b \in A$ be such that $q = ab$. Then, either $a \in U(A)$, in which case $q \in A$ is irreducible, or $a \in A \setminus U(A)$, in which case $Aa \neq A$. So, consider the latter case. Since $a \in A$ is given to be such that $a \mid q$, the above implies $Aq \subseteq Aa \subsetneq A$. Since Aq was assumed to be maximal, this implies that $Aa = Aq$, which further implies that $q \doteqdot a$. We have shown that, if $a,\ b \in A$ are such that $q = a\ b$, then either $a \in U(A)$ or $a \doteqdot q$. Thus, q is irreducible by Definition 2.13. □

iii. Prime Elements are Irreducible in Domains. Any prime element p of a domain A is also an irreducible element;

Proof. Let $a,\ b \in A$ be nonzero and $p \in A \setminus U(A)$ be nonzero and prime such that $p = a\ b$. Thus, $p \mid a\ b$ which means that **(1)** $p \mid a$ or **(2)** $p \mid b$ by Definition 2.12.

(1) First, assume $p \mid a$. Then, there is some $\alpha \in A$ such that $a = p\ \alpha$ and, thus, $p = p\ 1 = a\ b = (p\ \alpha)\ b$ which implies that $1 = \alpha\ b$ and that $b \in U(A)$.

(2) Similarly, assuming $p \mid b$, there is some $\beta \in A$ such that $b = \beta\ p$ and, thus, $p = 1\ p = a\ b = a\ (\beta\ p)$ which implies that $1 = a\ \beta$ and that $a \in U(A)$.

So, any such prime p is also irreducible. □

iv. Irreducible Elements are Prime in GCDDS. If A is a domain in which a greatest common divisor $\gcd(a,b) \in A$ exists for any pair of nonzero elements $a,\ b \in A \setminus U(A)$, then any irreducible element $q \in A$ is also a prime element. (See Theorem 2.8 for more on *greatest common divisor domains*)

Proof. Let A be a domain in which there exists a greatest common divisor for any pair of nonzero elements. Let $a,\ b \in A \setminus U(A)$ be nonzero elements and let $q \in A$ be irreducible such that $q \ | \ a\ b$.

There exists $d := \gcd(q, a) \in A$ which is such that $d \mid q$. So, there is some $u \in A$ such that $q = u\ d$ which implies that **(1)** $d \in U(A)$ or **(2)** $u \in U(A)$.

(1) If $d \in U(A)$, then $\gcd(q, a) \doteqdot q \doteqdot 1$. Thus,

$$b\ \gcd(q, a) \ \doteqdot\ \gcd(bq, ba)\ \doteqdot\ b.$$

Now, since $q \mid qb$ and $q \mid ab$, we deduce that $q \mid \gcd(qb, ab) \doteqdot b$ which implies that $q \mid b$.

(2) If $u \in U(A)$, then $\gcd(q, a) \doteqdot d \doteqdot q$. Since, $\gcd(q, a) \doteqdot q$, then $q \ | \ a$.

Thus, q is prime. □

(Clarifying) Remark. Note that the converse of Theorem 2.14.iii. is not necessarily true for arbitrary domains. This is reflected in Theorem 2.14.iv. by the stricter hypothesis that A be a GCDD. (see Example 3.9)

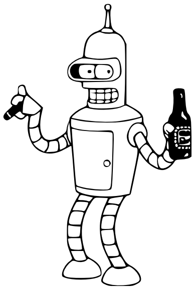
(Clarifying) Remark. One may, for example, be tempted to assert that every domain contains infinitely many prime classes or, equivalently, infinitely many prime elements which are not associated in divisibility. However, the number of distinct prime classes in an arbitrary domain may not be infinite. We will revisit this remark in the context of *unique factorization domains* (UFDs), where we prove that a UFD A has infinitely many prime classes if $\#U(A) < \infty$.

II. Survey of Specific Domains

3 Survey of Subclasses

3.0 Arithmetic in Square Number Rings

Terminology Apology. I must now caution that my departure from convention in this section—in particular, the substitution of "square" for the more commonly used "quadratic"—is fairly drastic and *very* "extra" of me. That is, don't try this, kids at home! □



Now that we have catalogued relevant arithmetic properties of domains, we introduce the notion of a square number field in order to access a class of arithmetically-relevant domains: the rings of integers of square number fields. That is, we define a *square number field* in order to discuss the associated *square number ring*. Square number rings are algebraically-motivated but are arithmetically concrete; one can explicitly manipulate their elements as symbols to check if they satisfy arithmetic characterizations of domain subclasses.

Spoiler Alert. Square number rings are, most importantly, dedekind domains. However, we will not discuss dedekind domains in depth. Instead, we use arithmetic in square number rings to illustrate, in concrete examples and counter-examples, a broad charting of properties as arithmetically-characterized domain subclass inclusions.

Terminology Note. I choose to include the modifier "number" in the terms "square number field" and "square number ring" to indicate the strict context of a rational base field and, in so doing, emphasizing the number theoretical significance of this topic.

Square Number Fields

Definition 3.1. A **number field** $K \subseteq \mathbb{C}$ is a finite extension of $\mathbb{Q}$. A number field $K \supseteq \mathbb{Q}$ is called a **square number field** if $[K : \mathbb{Q}] = 2$.

Corollary 3.1.1. If K is a square number field then there is a uniquely determined, nonzero and squarefree integer d such that

$$K = \mathbb{Q}(\sqrt{\,d\,}\,) := \{a + b\sqrt{d} \ : \ a,\ b \in \mathbb{Q}\}.$$

Proof. Let $\alpha \in K \setminus \mathbb{Q}$. Since K is assumed to be a square number field,

$$[K : \mathbb{Q}] \quad = \quad \dim_{\mathbb{Q}} K \quad = \quad 2$$

and, since $\{1,\ \alpha\}$ is a $\mathbb{Q}$-linearly independent set, we deduce that $\{1,\ \alpha\}$ is a $\mathbb{Q}$-basis for K.

Now, consider $\mathbf{m}(X) := \min_{\mathbb{Q}}^{\alpha}(X) \in \mathbb{Q}[X]$. Since $[K : \mathbb{Q}] = 2$, we know $\deg_{\mathbb{Q}} \mathbf{m} = 2$ and that $\mathbf{m}(X) \quad = \quad X^2 + aX + b$

$$= \quad \left(X + \tfrac{a}{2}\right)^2 - \left(\tfrac{a^2}{4} - b\right).$$

Note that, if $a = 0$ then $b = 0$ implies that $\mathbf{m}(X) = X^2$ which is not irreducible over $\mathbb{Q}$. Thus, if $a = 0$, then $b \neq 0$. Note also that, if $b = 0$ then $\mathbf{m}(X) = X^2 + aX = X(X - a)$ which is not irreducible over $\mathbb{Q}$. So, we eliminate the possibility that $a \neq 0$ and $b = 0$. Note in particular $b \neq 0$ implies $r := \dfrac{a^2}{4} - b$ is nonzero and rational. Thus, we can express $r = \dfrac{r_1}{r_2}$ for $r_1,\ r_2 \neq 0$ which implies $r = \dfrac{r_1}{r_2} \cdot \dfrac{r_2}{r_2} = \dfrac{1}{r_2^2}\, r_1\, r_2$.

Letting $\delta^2 = r_1\, r_2$, we express $r = \left(\dfrac{\delta}{r_2}\right)^2$ .... (1)

Now, since $\mathbf{m}(X)$ is the minimal polynomial of α over $\mathbb{Q}$, we have

$$\begin{aligned} 0 \quad = \quad \mathbf{m}(\alpha) \quad &= \quad \left(\alpha + \frac{a}{2}\right)^2 - \left(\frac{a^2}{4} - b\right) \\ &= \quad \left(\alpha + \frac{a}{2}\right)^2 - r \\ &= \quad x^2 - r \\ &= \quad p(x) \end{aligned}$$

where $p(X) := X^2 - r \in \mathbb{Q}[X]$ is satisfied by the value $x := \alpha + \dfrac{a}{2}$.

Thus, by above, $p(x) = x^2 - \left(\dfrac{\delta}{r_2}\right)^2$.

Recalling Line (1) from above, we set $\delta \doteqdot \sqrt{r_1 r_2}$ giving

$$\sqrt{r} \quad \doteqdot \quad \frac{1}{r_2}\sqrt{r_1 r_2} \quad \doteqdot \quad c \cdot \sqrt{d}\,.$$

$\square$

Corollary 3.1.2. There are two injective field homomorphisms

$$\mathrm{id},\ \sigma \quad : \quad K \hookrightarrow \mathbb{C}$$

defined by

$$\mathrm{id} : \sqrt{d} \ \mapsto \sqrt{d} \qquad \text{and} \qquad \sigma : \sqrt{d} \mapsto -\sqrt{d}\,.$$

Corollary 3.1.3. The **trace map** $\mathrm{TR}^{K/\mathbb{Q}} : K \hookrightarrow \mathbb{Q}$ is defined by $a + b\sqrt{d} \ \mapsto \ 2a$ and the **norm map** $\mathrm{N}^{K/\mathbb{Q}} : K \hookrightarrow \mathbb{Q}$ is defined by $a + b\sqrt{d} \mapsto a^2 - db^2$.

Remark 3.2. Let $d \in \mathbb{Z} \setminus \{0, 1\}$ be such that $d > 0$ and d is squarefree. As a consequence of the preceding discussion, we can define the following two subclasses of square number fields in terms of d:

i. Real square number fields. have the form $\mathbb{Q}(\sqrt{\ d\ })$;

ii. Imaginary square number fields. have the form $\mathbb{Q}(\sqrt{-d})$.

Definition 3.3. Let $A \subseteq B$ be an extension of domains. An element $b \in B$ is **integral over** A if there exists a monic polynomial $f(X) \in A[X]$ such that $f(b) = 0$. The extension $A \subseteq B$ is called **integral** if every element of B is integral over A. Define the **integral closure of** A **in** B,

$$A'_B \ := \ \{b \in B \ : \ b \text{ integral over } A\}.$$

Then A is **integrally closed in** B if $A'_B = A$, and A is **integrally closed** if it is integrally closed in its field of fractions.

Definition 3.4. Let K be a number field. We denote the **integer elements of** K by $\mathcal{O}_K := \mathbb{Z}'_K$, i.e. the integral closure of $\mathbb{Z}$ in K. A domain consisting of integer elements in a number field is called a **number ring** and is denoted $\mathcal{O}_K$, regardless of whether the associated number field K is specified. If K is a square number field, we will refer to $\mathcal{O}_K$ as a **square number ring** (abbr. SNR).

Theorem 3.5. If $d \in \mathbb{Z} \setminus \{0,1\}$ is the squarefree and uniquely determined integer guaranteed by Corollary 3.1.1 for a square number field $K = \mathbb{Q}(\sqrt{d}\,)$ then the set of integer elements of K is given by

$$\mathcal{O}_K \quad = \quad \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & d \;\equiv\; 1 \pmod 4 \\ \\ \mathbb{Z}[\sqrt{d}\,] & d \;\not\equiv\; 1 \pmod 4 \end{cases}$$

where given $\alpha \in K$ we define

$$\mathbb{Z}[\alpha] \quad := \quad \{a + b\alpha \;:\; a,\; b \in \mathbb{Z}\} \;\subseteq\; K,$$

and the **discriminant** of the extension K with respect to the base field $\mathbb{Q}$ is given by

$$\operatorname{disc}_{\mathbb{Q}} K \quad = \quad \begin{cases} d & d \;\equiv\; 1 \pmod 4 \\ \\ 4\,d & d \;\not\equiv\; 1 \pmod 4 \end{cases}$$

Proof. Observe that $\sqrt{d} \in \mathcal{O}_K$ because $\sqrt{d}$ is a root of the polynomial $X^2 - d \in \mathbb{Z}[X]$. Moreover, $\{1,\ \sqrt{d}\,\}$ is $\mathbb{Z}$-linearly independent since $d \in \mathbb{Z} \setminus \{0,1\}$ is squarefree. Thus, $\mathbb{Z}[\sqrt{d}\,] \subseteq \mathcal{O}_K$. If $d \equiv 1 \pmod 4$ then $\dfrac{1+\sqrt{d}}{2} \in \mathcal{O}_K$,

since $\dfrac{1+\sqrt{d}}{2}$ is a root of $X^2 - X + \dfrac{1-d}{4} \in \mathbb{Z}[X]$.
As above, $\dfrac{1+\sqrt{d}}{2}$ and 1 are $\mathbb{Z}$-linearly independent, so $\mathbb{Z}\left[\dfrac{1+\sqrt{d}}{2}\right] \subseteq \mathcal{O}_K$.
Now let $\alpha \in \mathcal{O}_K$. Since $\{1, \sqrt{d}\}$ is a $\mathbb{Q}$-basis for $\mathbb{Q}(\sqrt{d})$, there exist $a,\ b \in \mathbb{Q}$ such that $\alpha = a + b\sqrt{d}$. Calculating the trace and the norm of α, we infer that

$$2a \in \mathbb{Z} \tag{3}$$

and that

$$a^2 - db^2 \in \mathbb{Z}. \tag{4}$$

Moreover, after multiplying (4) by 4, we infer that

$$(2a)^2 - d(2b)^2 \in \mathbb{Z}, \tag{5}$$

and, upon using (3) and that d is a squarefree integer, we infer further that

$$2b \in \mathbb{Z}. \tag{6}$$

Indeed, to verify (6), suppose that $2b \notin \mathbb{Z}$. Then there exist $s,\ p,\ t \in \mathbb{Z}$, with $p \nmid s$ a prime, such that $2b = \dfrac{s}{p\ t}$. Recalling (3) and (5), we deduce that, for some $n \in \mathbb{Z}$, $d\ s^2 = p^2\ t^2\ n$. Since $p \nmid s$, this implies that $p^2 \mid d$, which contradicts the squarefreeness of d. Thus (6) is true. Denoting $u := 2a$ and $v := 2b$, observe that we have shown

$$\alpha \in \mathcal{O}_K \quad \Longrightarrow \quad u, v \in \mathbb{Z} \quad \text{and} \quad u^2 - dv^2 \equiv 0 \pmod 4.$$

(NB: The converse is also true. The element $a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ is a root of the monic polynomial $X^2 - uX + \dfrac{u^2 - dv^2}{4}$ which is integral if $u,\ v \in \mathbb{Z}$ and

$$u^2 - dv^2 \equiv 0 \pmod 4.$$

Thus we have the equivalence

$$\alpha \in \mathcal{O}_K \quad \Longleftrightarrow \quad u, v \in \mathbb{Z} \quad \text{and} \quad u^2 - dv^2 \equiv 0 \pmod 4.$$

Now, recall that the square of an integer is either 0 or $1 \pmod 4$. Thus the condition $u^2 - dv^2 \equiv 0 \pmod 4$ holds

if u and v are both even or

if $d \equiv 1$ and $u \equiv v \pmod 2$.

If $d \equiv 2, 3 \pmod 4$, we infer from this remark that u, v are both even.

Thus $\alpha = a + b\sqrt{d} = \dfrac{u}{2} + \dfrac{v}{2}\sqrt{d} \in \mathbb{Z}[\sqrt{d}\,]$.

If $d \equiv 1 \pmod 4$, we infer from the remark that $u,\ v$ have the same parity.

Thus $\alpha = a + b\sqrt{d} = \dfrac{u-v}{2} + \dfrac{v\,(1 + \sqrt{d}\,)}{2} \in \mathbb{Z}\left[\dfrac{1+\sqrt{d}}{2}\right]$. □

Proof. To calculate the discriminant, proceed as follows. If $d \equiv 2, 3 \pmod 4$, then

$$\operatorname{disc}_{\mathbb{Q}} K = \begin{vmatrix} \mathrm{id}(1) & \mathrm{id}(\sqrt{d}\,) \\ \sigma(1) & \sigma(\sqrt{d}\,) \end{vmatrix}^2 = \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 = 4d.$$

If $d \equiv 1 \pmod 4$, then

$$\operatorname{disc}_{\mathbb{Q}} K = \begin{vmatrix} \mathrm{id}(1) & \mathrm{id}\left(\frac{1+\sqrt{d}}{2}\right) \\ \sigma(1) & \sigma\left(\frac{1+\sqrt{d}}{2}\right) \end{vmatrix}^2 = \begin{vmatrix} 1 & \frac{1+\sqrt{d}}{2} \\ 1 & \frac{1-\sqrt{d}}{2} \end{vmatrix}^2 = d.$$

□

Units of an Imaginary Square Number Ring

Remark 3.6. Let $K = \mathbb{Q}(\sqrt{d}\,)$ be a square number ring. We will denote the norm map of K as $N(x) := \mathrm{N}^{K}/_{\mathbb{Q}}(x)$.

Lemma 3.7. Let $K = \mathbb{Q}(\sqrt{d}\,)$ be a square number ring. Then

i. $N(x \cdot y) = N(x) \cdot N(y)$ for all $x,\ y \in K$;

ii. $N(x) \in \mathbb{Z}$ for all $x \in \mathcal{O}_K$ (in particular $N(x) \in \mathbb{N}$ if $d < 0$); and

iii. $x \in U(\mathcal{O}_K)$ if and only if $N(x) = \pm 1$.

i. *Proof.* Given $x = a + b\sqrt{d}$ and $y = c + e\sqrt{d} \in K$,

$$\begin{aligned} N(x \cdot y) &= N((a + b\sqrt{d}) \cdot (c + e\sqrt{d})) \\ &= N((ac + bde) + (ae + bc)\sqrt{d}) \\ &= (ac + bde)^2 - d(ae + bc)^2 \\ &= (a^2c^2 + 2abcde + b^2d^2e^2) - d(a^2e^2 + 2abce + b^2c^2) \\ &= (a^2c^2 + b^2d^2e^2) - d(a^2e^2 + b^2c^2) \\ &= (a^2 - db^2) \cdot (c^2 - de^2) \\ &= N(x) \cdot N(y). \end{aligned}$$

□

ii. *Proof.* Clear from definition. □

iii. $\overset{Proof}{\Longrightarrow}$. Suppose that $x \in U(\mathcal{O}_K)$ and let $y \in U(\mathcal{O}_K)$ such that $x \cdot y = 1$. Then $1 = N(1) = N(x \cdot y) = N(x) \cdot N(y)$, so $N(x) = \pm 1$. □

$\overset{Proof}{\Longleftarrow}$. Suppose that $x = a + b\sqrt{d} \in \mathcal{O}_K$ such that $N(x) = \pm 1$ and let $y = a - b\sqrt{d}$. Then

$$x \cdot y = (a + b\sqrt{d}\,) \cdot (a - b\sqrt{d}\,) = a^2 - d\,b^2 = N(x) = \pm 1,$$

so $x \in U(\mathcal{O}_K)$. □

Theorem 3.8. Let K be an imaginary square field. That is, let $K = \mathbb{Q}(\sqrt{d}\,)$ for some squarefree $d \in \mathbb{Z} \setminus \{0, 1\}$ with $d < 0$. Then

$$U(\mathcal{O}_K) = \begin{cases} \{\pm 1,\ \pm i\} & d = -1 \\ \{\pm 1, \pm\frac{1}{2}\left(1 \pm i\sqrt{3}\right)\} & d = -3 \\ \{-1,\ 1\} & d \neq -1,\ -3. \end{cases}$$

Proof. Let $K = \mathbb{Q}(\sqrt{d})$. By Theorem 3.5, any element of $\mathcal{O}_K$ will have the form

i. $x = a + b\sqrt{d}$ if $d \not\equiv 1 \pmod 4$; or

ii. $x = a + b\left(\frac{1+\sqrt{d}}{2}\right)$ if $d \equiv 1 \pmod 4$,

for some $a,\ b \in \mathbb{Z}$. Note that we do not consider $d \equiv 0 \pmod 4$, as such d are not squarefree.

i. Supposing that $d \equiv 2, 3 \pmod 4$ and that $d \notin \{-1, -3\}$, we have $d \leq -2$ which implies $-d \geq 2$. Then, since any $x \in \mathcal{O}_K$ will have the form $x = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}\,]$, and, since any $x \in U(\mathcal{O}_K)$ will be such that $N(x) = 1$, we have $1 = N(x) = a^2 - db^2 \geq a^2 + 2b^2$ which implies $(a, b) = (\pm 1, 0)$ and, thus, $U(\mathcal{O}_K) = \{-1, 1\}$. Now, suppose that $d = -1$. Then any $x \in U(\mathcal{O}_K)$ will have the form

$x = a + bi \in U(\mathcal{O}_K)$ and will be such that $N(x) = 1$. Thus, $1 = N(x) = a^2 + b^2$, which implies $(a, b) \in \{(\pm 1, 0), (0, \pm 1)\}$ and, further, that $U(\mathcal{O}_K) = \{\pm 1, \pm i\}$.

ii. Supposing that $d \equiv 1 \pmod 4$ such that $d \neq -3$, we have $d \leq -7$ which implies $-d \geq 7$. Then, since any $x \in U(\mathcal{O}_K)$ will have the form

$$x = a + b\left(\frac{1+\sqrt{d}}{2}\right) = \left(a + \frac{b}{2}\right) + \frac{b}{2}\sqrt{d} \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right],$$

and, since any $x \in U(\mathcal{O}_K)$ will be such that $N(x) = 1$, we have $1 = N(x) = \left(a + \frac{b}{2}\right)^2 - \frac{db^2}{4}$ which implies

$$4 = (2a+b)^2 - db^2 \geq (2a+b)^2 + 7b^2.$$

Thus, $(a, b) = (\pm 1, 0)$ and $U(\mathcal{O}_K) = \{-1, 1\}$. Now, suppose that $d = -3$. Then any $x \in U(\mathcal{O}_K)$ will have the form

$$x = a + b\left(\frac{1+\sqrt{-3}}{2}\right) = \left(a + \frac{b}{2}\right) + \frac{b}{2}\sqrt{-3} \in \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right],$$

and will be such that $N(x) = 1$. Thus, $1 = N(x) = \left(a + \frac{b}{2}\right)^2 + \frac{3b^2}{4}$ which implies $4 = (2a+b)^2 + 3b^2 = 4a^2 + 4ab + 4b^2$ and further implies that $1 = a^2 + ab + b^2$. Thus, $(a, b) \in \{(\pm 1, 0), (0, \pm 1), (\pm 1, \mp 1)\}$ and thus

$$U(\mathcal{O}_K) = \left\{\pm 1,\ \pm\frac{1}{2}\left(1 \pm i\sqrt{3}\right)\right\}.$$

□

Example 3.9. There is a domain for which an irreducible element is not necessarily prime: Consider the square number field $K := \mathbb{Q}(\sqrt{-5})$ and its ring of integers $A := \mathcal{O}_K = \mathbb{Z}\left[\sqrt{-5}\right]$. In A, we have the following two factorizations of 6: $6 = 2 \cdot 3 = \left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right)$. We will prove:

Claim 1: The elements 2, 3, $1+\sqrt{-5}$ and $1-\sqrt{-5}$ are irreducible in A.

Claim 2: The elements 2, 3, $1+i\sqrt{5}$ and $1-i\sqrt{5}$ are not prime in A.

Proof of Claim 1. We will give the proof only for 2 being irreducible. Let $\alpha = a + b\sqrt{-5}$ and $\beta = c + i\sqrt{-5} \in A$ such that $2 = \alpha\beta$. Applying N, we deduce that $4 = (a^2+5b^2)(c^2+5d^2)$. Thus either $a^2+5b^2 = 1$ and $c^2+5d^2 = 4$, or $a^2+5b^2 = 2$ and $c^2+5d^2 = 2$, or $a^2+5b^2 = 4$ and $c^2+5d^2 = 1$. Recalling that $a, b, c, d \in \mathbb{Z}$, we deduce that only the first and thirds situations can occur, respectively implying $a = \pm 1, b = 0, c = \pm 2, d = 0$, and $a = \pm 2, b = 0, c = \pm 1, d = 0$. In particular, we obtain that either $\alpha \in U(A)$, or that $\beta \in U(A)$. Thus 2 is indeed irreducible in A, as desired. □

Proof of Claim 2. We will give the proof only for 2 not being prime. Observe that $2 \mid 6 = \left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right)$. So, if $2 \mid \left(1+\sqrt{-5}\right)$ or $2 \mid \left(1-\sqrt{5}\right)$, then, by applying N, we deduce that $4 \mid 6$, a contradiction. Consequently, $2 \nmid \left(1 \pm \sqrt{-5}\right)$, which means that 2 is not a prime in A, as desired. □

3.1 Unique Factorization Domains

Proposition 3.10 (Prime Irreducible Decomposition)**.** Let A be a domain. If $p_1, \ldots, p_n$ are prime elements and $q_1, \ldots, q_m$ are irreducible elements of A such that

$$p_1 \cdots p_n = q_1 \cdots q_m \ ,$$

then $m = n$ and for every $1 \leq i \leq n$, there is a $1 \leq j \leq m$ such that $p_i \doteqdot q_j$.

Proof. We proceed by induction on n.

If $n = 1$ then $p_1 = q_1 \cdots q_m$. So, because p_1 is prime, there exists a $1 \leq j \leq m$ such that $p_1 \mid q_j$. Without loss of generality we may assume $j = 1$. Also $q_1 \mid p_1$, so $p_1 \doteqdot q_1$ and there exists $u \in U(A)$ such that $p_1 = u \cdot q_1$. Suppose that $m > 1$. Then

$$u \cdot q_1 = p_1 = q_1 q_2 \cdots q_m \implies u = q_2 \cdots q_m,$$

but each q_j is irreducible and hence cannot be a unit. Thus $m = 1$.

Suppose that the result holds for $n < N$ and that

$$p_1 \cdots p_N = q_1 \cdots q_m.$$

Then because p_1 is prime there exists a $1 \leq j \leq m$ such that $p_1 \mid q_j$, and without loss of generality we may assume $j = 1$. There exists $u \in A$ such that $q_1 = u p_1$, so $u \in U(A)$ because q_1 is irreducible and p_1 cannot be a unit.

Then $p_1 \doteqdot q_1$ and

$$u \cdot q_1 \cdots q_m = u \cdot p_1 p_2 \cdots p_N = q_1 p_2 \cdots p_N \implies p_2 \cdots p_N = u \cdot q_2 \cdots q_m,$$

so by the inductive hypothesis we have that $m - 1 = N - 1 \implies m = N$ and for every $2 \leq i \leq N$ there is a $2 \leq j \leq m$ such that $p_i \doteqdot q_j$. Thus the result holds for all n. □

Definition 3.11. We call a domain A a **unique factorization domain (UFD)** if for every nonzero element $a \in A \setminus U(A)$ there exist prime elements $p_1, \ldots, p_n \in A$ such that $a = p_1 \cdots p_n$.

Definition 3.12. Let A be a domain and let $p_i \in A$ be prime for all $i \in I$, where I is an arbitrary indexing set. The subset $\{p_i\}_{i \in I} \subseteq A$ is called a **system of prime representatives** in A if

i. for any pair of distinct indexing elements $i,\ j \in I$, we have $p_i \not\doteqdot p_j$;

ii. for any prime element $p \in A$, there is an indexing element $i \in I$ such that $p \doteqdot p_i$.

Remark 3.13. If A is a UFD with a system of prime representatives $\{p_i\}_{i \in I} \subseteq A$ then for any nonzero element $a \in A \setminus U(A)$ there exist unique indexing subsets $\{i_1, \ldots, i_n\} \subseteq I$ and $\{\alpha_{i_1}, \ldots, \alpha_{i_n}\} \subsetneq \mathbb{N} \setminus \{0\}$ such that

$$a = u \cdot p_{i_1}^{\alpha_{i_1}} \cdots p_{i_n}^{\alpha_{i_n}} \text{ for some } u \in U(A).$$

Proposition 3.14. If A is a UFD with a system $\{p_i\}_{i \in I} \subseteq A$ of prime representatives, then any pair $a,\ b \in A$ of nonzero and nonunital elements with prime factorizations

$$a = u \cdot \prod_{i \in I} p_i^{\alpha_i} (\text{where } \alpha_i = 0 \text{ if } \ p_i \nmid a),$$

$$\text{and } b = v \cdot \prod_{i \in I} p_i^{\beta_i} (\text{where } \beta_i = 0 \text{ if } \ p_i \nmid b),$$

i. will have a greatest common divisor satisfying $\gcd(a, b) \doteqdot \prod_{i \in I} p_i^{\min\{\alpha_i, \beta_i\}}$, and

ii. will have a least common multiple satisfying $\operatorname{lcm}(a, b) \doteqdot \prod_{i \in I} p_i^{\max\{\alpha_i, \beta_i\}}$.

i. *Proof.* Let $d = \prod_{i \in I} p_i^{\min\{\alpha_i, \beta_i\}}$. First note that $p_i^{\min\{\alpha_i, \beta_i\}} \mid a$ and $p_i^{\min\{\alpha_i, \beta_i\}} \mid b$ for all i, so $d \mid a$ and $d \mid b$. Let d' such that $d' \mid a$ and $d' \mid b$. Then d' has a unique factorization

$$d' = w \cdot \prod_{i \in I} p_i^{\gamma_i}$$

where $\gamma_i \leq \min\{\alpha_i, \beta_i\}$ for all i, otherwise d' could not divide both a and b. Then $d' \mid d$, so

$$\gcd(a, b) \doteqdot \prod_{i \in I} p_i^{\min\{\alpha_i, \beta_i\}}.$$

□

ii. *Proof omitted.* □

Corollary 3.14.1. If A is a UFD, then A is a GCDD. In other words,$\{$ GCDDs $\} \supseteq \{$ UFDs $\}$.

Definition 3.15. A domain A is a **Bézout domain** if, for all ideals $(a,\ b) \trianglelefteq A$ there exists $d \in A$ such that $(a,\ b) = (d)$. Note that a Bézout domain is not necessarily a PID, but it is a GCDD with $\gcd(a, b) = d$.

Definition 3.16. The **ring of algebraic integers**, denoted by $\Omega := \mathbb{Z}'_{\mathbb{C}}$, is the integral closure of $\mathbb{Z}$ in $\mathbb{C}$.

Example 3.17. Let $A := \Omega$ be the ring of algebraic integers. Because A is a Bézout domain (see [DF04, Exercise 16.3.24]) it is a GCCD. However, A is not a UFD because it contains no irreducible elements, as any nonzero $a \in A \setminus U(A)$ can be factorized $a = \sqrt{a} \cdot \sqrt{a}$.

Arithmetic Characterization Theorem for Unique Factorization Domains

Theorem 3.18. Let A be a domain. Then the following statements are equivalent:

i. The domain A is a UFD (see Definition 3.11);

ii. every nonzero element of $A \setminus U(A)$ can be written *uniquely* as a product of *irreducible* elements;

iii. a. every nonzero element of $A \setminus U(A)$ can be written as a product of irreducible elements;

b. every irreducible element of A is also prime;

iv. a. every nonzero element of $A \setminus U(A)$ can be written as a product of irreducible elements;

b. a greatest commmon divisor exists for every pair of elements $a,\ b \in A$;

v. every nonzero prime ideal $P \lhd A$ contains a prime element;

vi. a. every chain of principal ideals of A stabilizes;

b. for all $a,\ b \in A$, there exists $c \in A$ such that $Aa \cap Ab = Ac$.

Claim 3.18.1 (**i.** $\Rightarrow$ **ii.**). Assume that A is a UFD. Since all prime elements are irreducible in domains and since A is a UFD, any nonzero

$a \in A \setminus U(A)$ will factor into prime and, hence, irreducible elements. Thus, by Proposition 3.10 and Remark 3.13, any nonzero $a \in A \setminus U(A)$ will factor *uniquely* as a product of irreducible elements. □

Claim 3.18.2 (**ii.** ⇒ **iii. a.** ⇒ **iii. b.**). We want to show **ii.** ⇒ **iii. b.** So, let $q \in A$ be an irreducible and let $a, b \in A$ be such that $q \mid a\, b$. Then there exists $c \in A$ such that $a\, b = q\, c$. Applying (ii), we write the unique irreducible factorizations of a, b, and c as

$$a = \prod_{1 \leq i \leq m} q_i^{\alpha_i}, \;\; b = \prod_{1 \leq i \leq n} \overline{q}_i^{\beta_i},$$

$$\text{and } c = \prod_{1 \leq i \leq k} \widetilde{q}_i^{\gamma_i}.$$

Thus

$$\prod_{1 \leq i \leq m} q_i^{\alpha_i} \cdot \prod_{1 \leq i \leq n} \overline{q}_i^{\beta_i} = q \prod_{1 \leq i \leq k} \widetilde{q}_i^{\gamma_i}.$$

Recalling that (ii) ensures the uniqueness of the irreducible factorization of an element of A, we deduce that $q \sim q_i$ for some $1 \leq i \leq m$ or that $q \sim \overline{q}_i$ for some $1 \leq i \leq n$. Thus $q \mid a$ or $q \mid b$, proving that q is a prime.

Claim 3.18.3 (**iii.** ⇒ **i.**). *Proof is obvious.* □

Claim 3.18.4 (**i.** ⇒ **iv. a.** ⇒ **iv. b.**). *Claim follows from Proposition 3.14.* □

Claim 3.18.5 (**iv.** ⇒ **i.**). *Claim follows from Proposition 2.14.* □

Claim 3.18.6 (**i.** ⇒ **v.**). Let $P \lhd A$ be a nonzero prime ideal and let $a \in P$ be a nonzero element. Since $a \notin U(A)$, we know a has a prime factorization, say, $a = \prod_{1 \leq i \leq n} p_i^{\alpha_i}$. Then, since P is a prime ideal, it follows that $p_i \in P$ for some $1 \leq i \leq n$. □

Claim 3.18.7 (v. $\Rightarrow$ i.). Recalling Theorem 2.8 and part (iv) of Theorem 2.14, it suffices to show that every nonzero $a \in A \setminus U(A)$ can be written as a product of irreducibles. Suppose that this is not true, i.e. suppose that the subset

$$X := \{a \in A \setminus (U(A) \cup \{0\}) : a \text{ is not a product of irreducibles}\}$$

is nonempty. Thus there exists $a \in X$. Clearly, a is not irreducible. Thus, it can be written as $a = a_1 \, b_1$ for some nonzero $a_1, b_1 \in A \setminus U(A)$. At least one of a_1 or b_1 is not in X, for otherwise a is a product of irreducibles, a contradiction. Say that $a_1 \in X$. Reasoning as above, a_1 is not irreducible, and, thus, can be written as $a_1 = a_2 b_2$ for some nonzero $a_2,\ b_2 \in A \setminus U(A)$ with $a_2 \in X$.

Continuing in the same way, we obtain two sequences of nonzero elements $(a_n)_{n \geq 1}, (b_n)_{n \geq 1} \subseteq A \setminus U(A)$ with $a_n = a_{n+1} b_{n+1}$. Consequently, we obtain a strictly ascending sequence of principal ideals, $Aa_1 \subsetneq Aa_2 \subsetneq \ldots \subsetneq Aa_n \subsetneq \ldots$, a contradiction with (vi1). Thus $X = \emptyset$, confirming (i). □

Remark 3.19. Let A be a UFD which is not a field.

i. If $|U(A)| < \infty$, then A has infinitely many non-associated primes.

Proof. [1] Because A is a UFD but not a field, it contains at least one prime element. Suppose that A contains only finitely many non-associated primes $p_1, \ldots, p_n$. For

[1] This proof due to Gregory Taylor.

any $e = (e_1, \ldots, e_n) \in \mathbb{N}^n$, define $a_e := p_1^{e_1} \cdots p_n^{e_n} + 1$. Note that each a_e is uniquely determined by e because A is a UFD: if $a_e = a_{e'}$, then $e = e'$ by unique factorization. Because $|U(A)| < \infty$, there exists some e such that a_e is not a unit and $e_i > 0$ for all i, so there is a unique factorization

$$p_1^{e_1} \cdots p_n^{e_n} + 1 = a_e = u \cdot p_1^{f_1} \cdots p_n^{f_n},$$

where $f_j > 0$ for some j. But then $e_j > 0$ by assumption, so

$$1 \equiv a_e \equiv 0 \pmod{p_j}.$$

This is a contradiction, so A must have infinitely many non-associated primes. □

Note that this proof would fail if $|U(A)| = \infty$.

ii. If $|U(A)| = \infty$, then A may have only finitely many non-associated primes.

Proof. Let $p \in \mathbb{Z}$ be prime, let $S := \mathbb{Z} \setminus (p)$, and let $A := S^{-1}\mathbb{Z}$. Then A is a PID (see Theorem 5.1) and has a unique maximal ideal generated by $\frac{p}{1}$. All prime ideals in PIDs are maximal, so $\frac{p}{1}$ is is the only prime in A up to associates. □

3.2 Principal Ideal Domains

Definition 3.20. A domain A is called a **principal ideal domain** if, for any ideal $I \trianglelefteq A$, there exists an element $a \in A$ such that $I = Aa$. In other words, every ideal in a principal ideal domain can be generated by a single element.

Theorem 3.21. If A is a principal ideal domain, then A is a unique factorization domain. In other words, ... $\{\text{ UFDs }\} \supseteq \{\text{ PIDs }\}$.

Proof. Since A is a PID, using part (vi) of Theorem 3.18, it suffices to prove that every ascending sequence of ideals of A terminates. Let $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$ be an ascending sequence of ideals and define $I := \bigcup_{n \geq 1} I_n$. It is clear that I is closed under multiplication by elements of A, and for all $x, y \in I$ there exists $n \geq 1$ such that $x, y \in I_n$, so $x + y \in I_n \subseteq I$. Thus $I \trianglelefteq A$. Further, since A is a PID, there exists $a \in A$ such that $I = Aa$. In particular, $a \in I$, so there exists $k \geq 1$ such that $a \in I_k$. Then $I_k \subseteq I = Aa \subseteq I_k$, and so $I = I_k$. Consequently, $I_k = I_{k+1} = I_{k+2} = \cdots$, completing the proof. □

Theorem 3.22. If A is a PID and $a,\ b \in A$, then $\gcd(a, b)$ exists and there exist elements $\gamma,\ \delta \in A$ such that $\gamma\, a + \delta b = \gcd(a, b)$.

Proof. Consider the ideal $Aa + Ab \trianglelefteq A$. Since A is a PID, there exists $d \in A$ such that $Aa + Ab = Ad$. Observing that $d \in Ad$, we deduce that there exist $\lambda,\ \mu \in A$ such that $\lambda a + \mu b = d$. We claim that $d = \gcd(a, b)$. Observing that $Aa \subseteq Aa + Ab = Ad$ and that $Ab \subseteq Aa + Ab = Ad$, we deduce that $d \mid a$ and that $d \mid b$. Moreover, letting $d' \in A$ be such that $d' \mid a$ and $d' \mid b$, we see that $d' \mid \lambda a + \mu b$, i.e. $d' \mid d$, completing the proof. □

Example 3.23. The polynomial ring $A := \mathbb{Z}[X]$ is a UFD (see Theorem 4.3), but it is not a PID because the ideal $(2, X)$ is not principal.

3·3 Euclidean Domains

Definition 3.24. A domain A is called **Euclidean** (or a **Euclidean domain**) if there exists a function $\varphi : A \setminus \{0\} \longrightarrow \mathbb{N}$ such that, for any $a,\ b \in A \setminus \{0\}$ there exist $q, r \in A$ satisfying $a = b\ q\ +\ r$ with **i.** $r = 0$ or **ii.** $\varphi(r) < \varphi(b)$. Such a function φ is called a **Euclidean function**.

(Clarifying) Remark. A Euclidean function does not need to be a multiplicative norm! There exists a Euclidean Domain on which a multiplicative norm cannot be defined. [CNT19, Theorem 1.3]

Proposition 3.25. If A is a Euclidean domain with respect to the Euclidean function φ, then there exists an associated norm $\overline{\varphi} : A \setminus \{0\} \longrightarrow \mathbb{N}$ such that for any $a,\ b \in A \setminus \{0\}$

1. there exist $q,\ r \in A$ satisfying $a = b\ q\ +\ r$ with **i.** $r = 0$ or **ii.** $\overline{\varphi}(r) < \overline{\varphi}(b)$; and
2. if $a \mid b$, we have $\overline{\varphi}(a) \leq \overline{\varphi}(b)$.

Proof. We define $\varphi'(a) := \min\{\varphi(c)\ :\ c \doteqdot a\}$ and show that such a map satisfies the above properties. That is, we show $\varphi' = \overline{\varphi}$. Let $a, b \in A \setminus \{0\}$ and let $u \in U(A)$ such that $\varphi(u \cdot b) = \varphi'(b)$. Then there exists $q, r \in A$ such that $u \cdot a = (u \cdot b)\ q + r$ with $r = 0$ or $\varphi(r) < \varphi(u \cdot b) = \varphi'(b)$. Then $a = bq + u^{-1} \cdot r$ with $u^{-1} \cdot r = 0$ or $\varphi'(u^{-1} \cdot r) \leq \varphi(r) < \varphi(u \cdot b) = \varphi'(b)$. □

(Clarifying) Remark. The $q,\ r \in A$ given in Definition 3.24 and Remark 3.25 (for a domain A which is Euclidean with respect to a norm φ) are not necessarily uniquely determined by a and b.

Theorem 3.26 ([Rha62]). If A is a Euclidean domain with respect to a Euclidean function φ and the $q, r \in A$ are uniquely determined by a and b, then there exists a field K such that either $A \cong K$ or $A \cong K[X]$.

Proposition 3.27. If A is Euclidean with respect to the norm $\overline{\varphi}$ (see Remark 3.25) then

i. for all $a,\ b \in A \setminus \{0\}$ such that $a \doteqdot b$, we have $\overline{\varphi}(a) = \overline{\varphi}(b)$;

ii. for all $a,\ b \in A \setminus \{0\}$ such that $a \mid b$ and $\overline{\varphi}(a) = \overline{\varphi}(b)$, we have $a \doteqdot b$;

iii. for all $u \in U(A)$, we have $\overline{\varphi}(u) = \overline{\varphi}(1)$.

Theorem 3.28. If A is a Euclidean domain, then A is a principal ideal domain. In other words, ... { PIDs } $\supseteq$ { EDs }.

Proof. Let A be a Euclidean domain. So, there exists $\varphi : A \setminus \{0\} \longrightarrow \mathbb{N}$ with the property: for all $a,\ b \in A$ with $b \neq 0$ there exist $q,\ r \in A$ such that $a = bq + r$ and $r = 0$ or $\varphi(r) < \varphi(b)$. Now, let $0 \neq I \lhd A$ and set $\mathcal{I} := \{\varphi(x) \ :\ x \in I \setminus \{0\}\}$. Observing that $\emptyset \neq \mathcal{I} \subseteq \mathbb{N}$, we deduce

$$\text{there exists } x_0 \in I \setminus \{0\} \text{ such that } \varphi(x_0) \text{ is the smallest element of } \mathcal{I}. \tag{7}$$

We claim that $I = Ax_0$ and proceed by proving double inclusion. First, it is clear that $I \supseteq Ax_0$ since $x_0 \in I$ and $I \lhd A$. Now, we want to show $I \subseteq Ax_0$. So, let $x \in I$. Since $x_0 \in A \setminus \{0\}$ and since A is Euclidean, there exist $q,\ r \in A$ such that

$$x = x_0\, q\ +\ r \tag{8}$$

and

$$r = 0 \tag{9}$$

or

$$\varphi(r) < \varphi(x_0). \tag{10}$$

By (8), we know $r \in I$. Further, if (10) held, we would get a contradiction with (7). Thus (9) must hold instead, implying that $x \in Ax_0$ and completing the proof. □

Theorem 3.29 ([AW04, §2.2])**.** Let $K = \mathbb{Q}(\sqrt{d})$ for some squarefree $d \in \mathbb{Z} \setminus \{0, 1\}$ be a square number field. Then $\mathcal{O}_K$ is a Euclidean domain with respect to the norm $\mathrm{N}^{K}\!/\!_{\mathbb{Q}}$ if and only if

$$d \in \{-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}.$$

Theorem 3.30 ([Har04])**.** Let $K = \mathbb{Q}(\sqrt{14})$. Then $\mathcal{O}_K$ is a Euclidean domain, but not with respect to the norm $\mathrm{N}^{K}\!/\!_{\mathbb{Q}}$.

Example 3.31. The domain $A := \mathbb{Z}\left[\dfrac{1 + \sqrt{-19}}{2}\right]$ is a PID (see [AW04, Example 12.6.1]). However, A is *not* a Euclidean domain with respect to any function (see [AW04, Theorem 2.3.8]).

III. Preserved Properties

4 Polynomial and Power Series Rings Over Domains

4.1 Polynomial Rings Over Domains

Lemma 4.0. If A is a domain, then $A[X]$ is a domain and $U(A[X]) = U(A)$.

Proof. Suppose that there exist

$$f(X) = a_nX^n + \cdots + a_1X + a_0, g(X) = b_mX^m + \cdots + b_1X + b_0 \in A[X] \setminus \{0\}$$

such that $f(X)\ g(X) = 0$. Without loss of generality we may assume $a_0, b_0 \neq 0$, otherwise we may factor out the lowest power of X from all terms to obtain polynomials that satisfy this. Then $0 = f(X)\ g(X) = c_{m+n}X^{m+n} + \cdots + c_1X + c_0$, where $c_i = \sum\limits_{j=0}^{i} a_jb_{i-j} = 0$ for all i. But then $0 = c_0 = a_0b_0 \neq 0$, which is a contradiction because A is a domain. Thus no such f and g exist, so $A[X]$ is a domain.

Note that for any $f, g \in A[X]$ we have that $\deg(f \cdot g) = \deg(f) + \deg(g)$, so if $f, g \in U(A[X])$ such that $f \cdot g = 1$ we have $0 = \deg(1) = \deg(f) + \deg(g)$, so $\deg(f) = \deg(g) = 0$ and thus $f, g \in U(A)$. It is also clear that $U(A) \subseteq U(A[X])$, so $U(A[X]) = U(A)$. □

Theorem 4.1. If K is a field, then $K[X]$ is a Euclidean Domain.

Proof. Let $f(X),\ g(X) \in K[X]$ such that $g(X) \neq 0$. We claim that there exist $q(X),\ r(X) \in K[X]$ such that $f(X) = q(X)\ g(X)\ +\ r(X) \ldots\ldots\ldots\ldots\ldots\ldots (*)$ with $r(X) = 0$ or $\deg r(X) < \deg g(X)$. If $f(X) = 0$, we can choose $q(X) = r(X) = 0$. So, suppose $f(X) \in K[X]$ is such that $f(X) \neq 0$. In particular, assume $f(X) \in K[X]$ is such that $n := \deg f(X)\ \geqslant\ 0$.

If $n = 0$ then $\deg f(X) = 0$ implies $f \in K$. Thus, there exist $q,\ r \in K$ such that $f = q \cdot g(X)\ +\ r \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (**)$ In particular, there exist $r\ :=\ f$ and $q\ :=\ 0$ for which $(**)$ holds. Further, if $m\ :=\ \deg g(X)\ >\ n$, there exist $q(X)\ :=\ 0$ and $r(X) := f(X)$ which satisfy $(*)$. So, without loss of generality, take $f(X),\ g(X) \in K[X]$ to be such that

$$\deg f(X)\ :=\ \underline{n \geqslant m}\ :=\ \deg g(X).$$

Then, for appropriate $a_0,\ \ldots,\ a_n, b_0,\ \ldots,\ b_n \in K$ (with $a_n,\ b_m \neq 0$) we can express

$$f(X) := a_n \cdot X^n\ + \cdots +\ a_1 \cdot X\ +\ a_0 \in K[X]$$

and

$$g(X) := b_m \cdot X^m\ + \cdots +\ b_1 \cdot X\ +\ b_0 \in K[X]$$

to define

$$h(X) := f(X)\ -\ \frac{a_n}{b_m} \cdot X^{n-m}\ g(X).$$

Since $\deg h < n$, there exist $p(X),\ r(X) \in K[X]$ such that $h(X) = p(X)g(X) + r(X)$ with $r(X) = 0$ or $\deg r(X) < \deg g(X)$, *assuming a strong induction hypothesis*, that is, assuming our claim holds for every $h(X) \in K[X]$ such that $\deg h(X) < \deg f(X)$.

Thus, there exists $q(X) \in K[X]$ such that $q(X) = p(X)\ +\ \dfrac{a_n}{b_m}\ X^{n-m}$ and there exists $r(X) \in K[X]$ satisfying $(*)$ for all such $f(X),\ g(X) \in K[X]$. □

Corollary 4.1.1. By Theorem 3.28, since, for any field K, the polynomial ring $A := K[X]$ is a Euclidean Domain, then A is also a principal ideal domain.

Lemma 4.2.0 (Gauss, [DF04, Proposition 9.5])**.** If A is a UFD with field of fractions $K = \mathrm{Frac}(A)$ and $f(X) \in A[X]$ is irreducible in $A[X]$, then it is also irreducible in $K[X]$.

Corollary 4.2.2. If A is a UFD with field of fractions $K = \mathrm{Frac}(A)$ and $f(X) \in A[X]$ is a polynomial such that the greatest common divisor of its coefficients is 1, then $f(X)$ is irreducible in $A[X]$ if and only if it is irreducible in $F[X]$.

Proof. Suppose that $f(X) = g(X)h(X)$ is reducible in $A[X]$. Then by the condition on the coefficients of $f(X)$ neither $g(X)$ nor $h(X)$ are constant, so $f(X) = g(X)h(X)$ is also reducible in $K[X]$. □

Theorem 4.3. If A is a UFD, then $A[X]$ is a UFD.

Proof. Let $f(X) \in A[X] \setminus \{0\}$, and without loss of generality we may assume that the greatest common divisor of its coefficients is 1. Because $K[X]$ is a Euclidean domain (and hence a UFD) there exists a factorization over $K[X]$ into irreducibles. By Gauss's lemma we obtain a factorization in $A[X]$. The greatest common divisor of the coefficients of each of these factors is also 1, so by the previous lemma these factors are also irreducible in $A[X]$. Thus there exists a factorization of $f(X)$ in $A[X]$ into irreducibles, and uniqueness follows from the uniqueness of factorization in $K[X]$. □

Corollary 4.4. If A is a Euclidean domain or PID, then $A[X]$ is a UFD.

4.2 Rings of Formal Power Series

Lemma 4.5. If A is a domain, then $A[[X]]$ is a domain and

$$U(A[[X]]) = \left\{ \sum_{i\geqslant 0} a_i X^i \in A[[X]] \ : \ a_0 \in U(A) \right\}.$$

Proof. Suppose that

$$f(X) = \sum_{i\geqslant 0} a_i X^i, \ g(X) = \sum_{i\geqslant 0} b_i X^i \in A[[X]]$$

such that $f(X)\ g(X) = 0.$

Without loss of generality we may assume that $a_0, b_0 \neq 0,$ otherwise we may factor out the lowest power of X from all terms to obtain series that satisfy this. But then $0 = f(X)\ g(X) = \sum_{i\geqslant 0} c_i X^i$ where $c_i = \sum_{j=0}^{i} a_j b_{i-j} = 0$ for all $i,$ so $0 = c_0 = a_0 b_0 \neq 0,$ which is a contradiction because A is a domain. Thus $A[[X]]$ is a domain.

Suppose that $f(X) = \sum_{i\geqslant 0} a_i X^i \in U(A[[X]])$ and let $g(X) = \sum_{i\geqslant 0} b_i X^i \in U(A[[X]])$ such that $f(X)\ g(X) = 1.$ Then $1 = f(X)\ g(X) = \sum_{i\geqslant 0} c_i X^i$ where $c_0 = a_0 b_0 = 1$ and $c_i = \sum_{j=0}^{i} a_j b_{i-j} = 0$ for all $i > 1,$ so $a_0 \in U(A).$

Conversely, suppose that $f(X) = \sum_{i\geqslant 0} a_i X^i \in A[[X]]$ with $a_0 \in U(A).$ Let $g(X) = \sum_{i\geqslant 0} b_i X^i \in A[[X]]$ with

$$b_0 := \frac{1}{a_0} \text{ and, for all } i > 0, \ b_i := -\frac{1}{a_0} \sum_{j=1}^{i} a_j b_{i-j}.$$

Then one may verify that $f(X)\, g(X) = 1$, so $f(X) \in U(A[[X]])$. Thus

$$U(A[[X]]) = \left\{ \sum_{i \geqslant 0} a_i X^i \in A[[X]] \ : \ a_0 \in U(A) \right\}.$$

□

Theorem 4.6. If K is a field, then $K[[X]]$ is a Euclidean domain.

Proof. By Lemma 4.5, any $f(X) \in K[[X]] \setminus \{0\}$ may be written as $f(X) = X^n \widetilde{f}(X)$ for some uniquely determined $n \in \mathbb{N}$ and $\widetilde{f}(X) \in U(K[[X]])$, so define

$$\varphi : K[[X]] \setminus \{0\} \longrightarrow \mathbb{N} \text{ by } \varphi(f) := n.$$

Let $f(X), g(X) \in K[[X]]$ such that $g(X) \neq 0$. We claim that there exist $q(X), r(X) \in K[[X]]$ such that $f(X) = q(X)g(X) + r(X)$ with $r(X) = 0$ or $\varphi(r) < \varphi(g)$.

If $\varphi(f) < \varphi(g)$, we can choose $q(X) = 0$ and $r(X) = f(X)$. Otherwise, suppose $\varphi(f) \geq \varphi(g)$ and let $n = \varphi(f), m = \varphi(g)$. Then there exist $\widetilde{f}(X), \widetilde{g}(X) \in U(K[[X]])$ such that $f(X) = X^n \widetilde{f}(X)$, $g(X) = X^m \widetilde{g}(X)$, and thus we can choose $q(X) = X^{n-m} \widetilde{f}(X) \widetilde{g}(X)^{-1}$ and $r(X) = 0$. Thus $K[[X]]$ is a Euclidean domain. □

Theorem 4.7. If A is a PID, then $A[[X]]$ is a UFD.

Proof. We will show that for any non-zero prime ideal $P \trianglelefteq A[[X]]$, there exists a prime element $p \in A$ such that $p \in P$. We'll do this with the help of the function

$$\begin{aligned} \varphi : A[[X]] &\longrightarrow A, \\ \sum_{i \geq 0} a_i X^i &\mapsto a_0, \end{aligned}$$

which is a surjective ring homomorphism. Fix an arbitrary non-zero prime ideal $P \trianglelefteq A[[X]]$. If $X \in P$, then we may take $p := X$. If $X \notin P$, consider the ideal $P^* := \varphi(P) \trianglelefteq A$. Since A is a PID, there exists $a \in A$ such that $P^* = A\ a$. Thus there exists $f \in P$ such that $a = \varphi(f)$. In particular, f satisfies $f(X) = a + a_1 X + \dots$.

Claim 4.7.1. $P = fA[[X]]$.

Proof. We prove double inclusion.

First, it is clear that $P \supseteq fA[[X]]$ because $f(X) \in P$.

Now, we want to show $P \subseteq fA[[X]]$. So, let $g(X) := b_0 + b_1 X + \dots \in P$. Then $b_0 = \varphi(g) \in P^* = Aa$, which implies that there exists $\alpha_0 \in A$ such that $b_0 = \alpha_0\ a$. In turn, this implies that

$$g(X) - \alpha_0 f(X) = X g_1(X) \tag{11}$$

for some $g_1 \in A[[X]]$. But $g(X) - \alpha_0 f(X) \in P$, a prime ideal which satisfies $X \notin P$. Thus

$$g_1 \in P.$$

We deduce that there exists $\alpha_1 \in A$ such that

$$g_1(X) - \alpha_1 f(X) = X g_2(X) \tag{12}$$

for some $g_2 \in A[[X]]$. Putting together (11) and (12), we deduce that

$$g(X) = (\alpha_0 + \alpha_1 X) f(X) + X^2 g_2(X).$$

Proceeding similarly for $g_2 \in P$, we find $\alpha_3 \in A$ and $g_3 \in A[[X]]$ such that

$$g(X) = \left(\alpha_0 + \alpha_1 X + \alpha_2 X^2\right) f(X) + X^3 g_3(X).$$

Continuing, we find $\alpha_4, \alpha_5, \ldots \in A$ such that

$$h(X) := \alpha_0 + \alpha_1 X + \alpha_2 X^2 + \ldots \in A[[X]]$$

satisfies

$$g(X) = h(X) f(X).$$

Thus

$$g \in A[[X]]f.$$

□

Since P is a principal prime ideal of $A[[X]]$, its generator f must be a prime element of $A[[X]]$ and also of P. This completes the proof. □

Remark 4.8. If A is a UFD, then $A[[X]]$ is not necessarily a UFD. For example, in the paper *"On unique factorization domains,"* Pierre Samuel shows that $A := K[a, b, c]$, with K a perfect field of characteristic 2 and with $a^3 + b^7 = c^2$, is a UFD, but $A[[X]]$ is not (see page 14, second paragraph; this example arises from Samuel's Theorem 4.1 on page 9 and Theorem 4.3 on page 11).

Corollary 4.9. If K is a field, then $K[[X, Y]]$ is a UFD.

Proof. Because $K[[X]]$ is a Euclidean domain it is a PID, so $K[[X, Y]] = K[[X]][[Y]]$ is a UFD. □

5 Localizations of Domains

5.1 An Arithmetic Characterization of Domain Localizations

Theorem 5.1 (Localization Preserves PID Structure)**.** If A is a PID and $S \subseteq A$ is a multiplicatively closed system, then $S^{-1}A$ is a PID.

Proof. Let $I = \left(\frac{a_1}{s_1}, \frac{a_2}{s_2}, \ldots\right) \trianglelefteq S^{-1}A$ be an ideal. Because $\frac{1}{s_1}, \frac{1}{s_2}, \ldots \in U(S^{-1}A)$ we have $I = \left(\frac{a_1}{1}, \frac{a_2}{1}, \ldots\right)$. Because A is a PID there exists $d \in A$ such that $(d) = (a_1, a_2, \ldots)$ and, in particular, $d \mid a_i$ for all i. Thus, $I = \left(\frac{d}{1}\right)$ is principal, so $S^{-1}A$ is a PID. □

Theorem 5.2 (Localization Preserves UFD Structure)**.** If A is a UFD and $S \subseteq A$ is a multiplicatively closed subset, then $S^{-1}A$ is a UFD.

Proof. Suppose that $q \in A$ is irreducible. If there exists $s \in S$ such that $q \mid s$, then there exists $a \in A$ such that $s = q\,a$, so $\frac{q}{1} \cdot \frac{a}{s} = \frac{q\,a}{s} = 1$, and, hence, $\frac{q}{1}$ is a unit.

Now suppose that q does not divide any element of S, and suppose that $\frac{q}{1} = \frac{a}{s} \cdot \frac{b}{t}$. Then $a\,b = q\,s\,t$, so $q \mid ab$ and hence $q \mid a$ or $q \mid b$ because $q \in A$ is prime. Without loss of generality assume $a = q\,c$. Then $\frac{q}{1} = \frac{qc}{s} \cdot \frac{b}{t} = \frac{q}{1} \cdot \frac{bc}{st}$, so $\frac{bc}{st} = 1$ which implies $\frac{b}{t} \in U(A)$ is a unit and, hence, $\frac{q}{1}$ is irreducible. Suppose that $\frac{a}{s} \in S^{-1}A$ is irreducible. If a is irreducible in A it is clear that $\frac{a}{s}$ is associate to $\frac{a}{1}$, so suppose that a is not irreducible in A. If every irreducible dividing a in A also divides an element of S, then $\frac{a}{s}$ would be a unit and could not be irreducible, so there must exist an irreducible $q \in A$ such that $a = q\,b$ and such that q does not divide any element of S. Then $\frac{a}{s} =$

$\frac{q}{1} \cdot \frac{b}{s}$, so $\frac{b}{s}$ is a unit by the irreducibility of $\frac{a}{s}$ and $\frac{q}{1}$. Thus, any irreducible $\frac{a}{s} \in S^{-1}A$ is associate to $\frac{q}{1}$ for some irreducible $q \in A$.

Now let $\frac{a}{s} \in S^{-1}A \setminus \{0\}$. There exists a unique factorization

$$a = u \cdot p_1^{e_1} \cdots p_m^{e_m} \; q_1^{f_1} \cdots q_n^{f_n} \in A,$$

where $p_1, \ldots, p_m$ are the prime factors of a which divide elements of S and $q_1, \ldots, q_n$ are the factors of a which do not divide an element of S. Then, there is a factorization into irreducibles

$$\frac{a}{s} = \frac{u \cdot p_1^{e_1} \cdots p_m^{e_m}}{s} \cdot \left(\frac{q_1}{1}\right)^{f_1} \cdots \left(\frac{q_n}{1}\right)^{f_n}.$$

Because all irreducibles of $S^{-1}A$ are associate to some $\frac{q}{1}$, this factorization is unique by the uniqueness of factorization in A. □

Theorem 5.3. Let A be a domain such that every ascending chain of principal ideals of A stabilizes. Let $(p_i)_{i \in I}$ be a set of prime elements of A and denote by S the multiplicatively closed system generated by this set. If $S^{-1}A$ is a UFD, then A is a UFD.

Proof. Observe that it is enough to prove the statement for S such that $0 \notin S$. Otherwise, $S^{-1}A = \{0\}$ and there is nothing to prove. So, let $p \in A$ be a prime element which does divide any element of S. We want to show that $\frac{p}{1}$ is prime in $S^{-1}A$. Clearly, $\frac{p}{1} \neq \frac{0}{1}$. Moreover, since p does not divide any element of S, we have $\frac{p}{1} \notin U\left(S^{-1}A\right)$.

Let $a,\ b \in A$ and $s,\ t \in S$ be such that $\frac{p}{1} \bigm| \frac{a}{s} \cdot \frac{b}{t}$ in $S^{-1}A$. Then there exists $\frac{c}{r} \in S^{-1}A$ such that $\frac{a}{s} \cdot \frac{b}{t} = \frac{p}{1} \cdot \frac{c}{r}$. In other words, there exist $u,\ v \in S$ such that $u\,a\,b = p\,c\,v$. This gives $p \mid u \cdot a\,b$ in A, and since p is a prime in A, we get $p \mid u$, or $p \mid a$, or $p \mid b$. Recall that p does not divide any element of S. Thus $p \mid a$ or $p \mid b$. This, in turn, implies that $\dfrac{p}{1} \,\Big|\, \dfrac{a}{s}$ or $\dfrac{p}{1} \,\Big|\, \dfrac{b}{s}$ in $S^{-1}A$, which implies that $\dfrac{p}{1}$ is prime in $S^{-1}A$, as desired.

Now, let $\dfrac{a}{s} \in (S^{-1}A) \setminus U\left(S^{-1}A\right)$ such that $\dfrac{a}{s} \neq \dfrac{0}{1}$. Since A is a UFD, any element $a \in A$ can be written as a product of primes of A, say, $a = p_1 \dots p_n$. Upon reindexing the prime factors in the decomposition of a, assume that p_j for $1 \leqslant j \leqslant r$ do not divide any element of S, while p_k for $(r+1) \leqslant k \leqslant n$ divide some element of S. That is, assume that there exist $s_{r+1}, \dots, s_n \in S$ and $a_{r+1}, \dots, a_n \in A \setminus \{0\}$ such that $p_{r+1}a_{r+1} = s_{r+1}$, $\dots$, $s_n = p_n a_n$. Then

$$\frac{a}{s} = \frac{p_1}{1} \cdot \ldots \cdot \frac{p_r}{1} \cdot \frac{p_{r+1}}{1} \cdots \frac{p_n}{1} = \frac{p_1}{1} \cdot \ldots \cdot \frac{p_r}{1} \cdot \frac{s_{r+1}}{a_{r+1}} \cdots \frac{s_n}{a_n}.$$

Observe that $u := \dfrac{s_{r+1}}{a_{r+1}} \cdots \dfrac{s_n}{a_n} \in U(S^{-1}A)$ and that, by above, $\dfrac{p_1}{1}, \dots, \dfrac{p_r}{1}$ are prime in $S^{-1}A$. $\square$

References

[AW04] Şaban Alaca and Kenneth S. Williams. *Introductory algebraic number theory.* Cambridge University Press, Cambridge, 2004.

[Buc61] David A. Buchsbaun. Some remarks on factorization in power series rings. *J. Math. Mech.*, 10:749–753, 1961.

[CE59] E. D. Cashwell and C. J. Everett. The ring of number theoretic functions. *Pacific J. Math.*, 9:975–985, 1959.

[Cla94] David A. Clark. A quadratic field which is Euclidean but not norm-Euclidean. *Manuscripta Math.*, 83(3-4):327–330, 1994.

[CNT19] Chris J. Conidis, Pace P. Nielsen, and Vandy Tombs. Transfinitely valued Euclidean domains have arbitrary indecomposable order type. *Communications in Algebra*, 47(3):1105–1113, 2019.

[Coh73] P. M. Cohn. Unique factorization domains. *Amer. Math. Monthly*, 80:1–18, 1973.

[DF04] D.S. Dummit and R.M. Foote. *Abstract Algebra.* Wiley, 2004.

[Gol04] Dorian Goldfeld. The Gauss class number problem for imaginary quadratic fields. In *Heenger points and Rankin L-series*, volume 49 of *Math. Sci. Res. Inst. Publ.*, pages 25–36. Cambridge Univ. Press, Cambridge, 2004.

[Har04] Malcom Harper. $\mathbb{Z}[\sqrt{14}]$ is Euclidean. *Canadian Journal of Mathematics*, 56(1):55–70, 2004.

[HM04] Malcolm Harper and M. Ram Murty. Euclidean rings of algebraic integers. *Canadian Journal of Mathematics*, 56(1):71–76, 2004.

[Khu03] Dinesh Khurana. On GCD and LCM in domains — a conjecture of Gauss. *Resonance*, 8(6):72–79, June 2003.

[Rha62] Tong-Shieng Rhai. Mathematical Notes: A Characterization of Polynomial Domains Over a Field. *American Mathematical Monthly*, 69(10):984–986, December 1962.

[RMSS18] M. Ram Murty, Kotyada Srinivas, and Muthukrishnan Subramani. Admissible primes and Euclidean quadratic fields. *J. Ramanujan Math. Soc.*, 33(2):135–147, 2018.

[Sam61] Pierre Samuel. On unique factorization domains. *Illinois Journal of Mathematics*, 5:1–17, 1961.

[Sou07] K. Soundararajan. The number of imaginary quadratic fields with a given class number. *Hardy-Ramanujan J.*, 30:13–18, 2007.