FACTORISATION THEORY IN A NON-COMMUTATIVE ALGEBRA

Stephen Ozvatic

Supervised by Dr Daniel Chan

School of Mathematics,
The University of New South Wales.

October 30, 2009

Submitted in partial fulfillment of the requirements of the degree of
Bachelor of Science with Honours

I hereby declare that this submission is my own work and to the best of my knowledge it contains no materials previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any other degree or diploma at UNSW or any other educational institution, except where due acknowledgement is made in the thesis. Any contribution made to the research by others, with whom I have worked at UNSW or elsewhere, is explicitly acknowledged in the thesis.

I also declare that the intellectual content of this thesis is the product of my own work, except to the extent that assistance from others in the project's design and conception or in style, presentation and linguistic expression is acknowledged.

Stephen Ozvatic

Acknowledgements

I don't really know what my mum wanted me to be when I grew up. She might say a pilot among other things since she has always liked traveling, planes and Europe, her birthplace. She was told by one of my primary school teachers many years ago that I was good at maths, so perhaps she had hope for a few short years that it would eventuate, but I quickly threw that idea out. Now I'm not saying I'm good at maths (I found out I'm probably the opposite), but I've always been interested in it and it was probably a surprise when my mum found out I decided I was going to study it at university, since my family migrated here to Australia from a farm in Europe. Now four years later I'm here and have this thesis to show for it. It may only be an honours thesis to some, but whether this thesis is good or terrible, trivial or complicated, or if I get a mark of 50 (hopefully I won't get below this) or 95, it wont impact on how proud I am to have completed this; though 95 would be nice.

I'd like to thank my supervisor Daniel along with Hendrik, Gary, Ian and Anthony who helped me along the way during my studies. My thanks also go to my support and distraction Sonia, my colleagues Hugh, Oliver and Roland among others, my friends, and my family: Ana, Maria and Joe.

Stephen Ozvatic

Prerequisites

Though most definitions and the proofs of theorems are included within, at least an elementary knowledge of ring theory, factorisation theory and module theory is required. If you have not heard the words homomorphism, integral domain or module, then refer to the references page for a list of suitable sources. For any proofs that are not included here, there will be references pointing to proofs in widely accepted sources; and for any material that is required conceptually, there will be references given when required.

Introduction

The theory of *Dedekind domains* comes from the studies of the factorisation properties of the ring of algebraic integers $\mathcal{O}_K$ in an algebraic number field K. Richard Dedekind (1831-1916) in the latter half of his life, knowing that $\mathcal{O}_K$ was not always a *unique factorisation domain*, looked at 'fractional ideals' of $\mathcal{O}_K$ rather than elements and saw that there was always a unique factorisation of them. Through his work, he provided the concepts of *ideals*, *modules* (though he wrote *modul*), defined *prime ideals* (that is, generalised prime numbers), introduced the word *field* and perhaps most importantly, the concept of a ring is due to him, though the term 'ring' first appears due to Hilbert and our axiomatic definitions were not introduced until the 1920's by Emmy Noether and Krull.

The work done on these rings by Dedekind were part of the third (1879) and fourth (1894) editions of *Vorlesungen ber Zahlentheorie* and the notions created eventually lead to be fundamental to ring theory, allowing him to provide an algebraic proof to the *Riemann-Roch Theorem* after only three years.

So what is a Dedekind domain? They are basically rings where each ideal is able to be factorised into prime ideals. If this sounds familiar it probably is since each integer, an element of $\mathbb{Z}$, has that same property. That is, each integer can be factorised into prime integers. It turns out that the integers are also a Dedekind domain themselves, but this understates their usefulness. If we look at roots of monic polynomials

$$x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0$$

with coefficients in $\mathbb{Z}$, then the set of these roots are called *algebraic integers* and denoted B. If we now look at a finite extension K of the field $\mathbb{Q}$, then the set $K \cap B$ is actually a Dedekind domain denoted by $\mathcal{O}_K$ and called the *ring of algebraic integers* of K. This is the ring studied by Dedekind in which he found the unique factorisation property of ideals, even though the unique factorisation of elements in this ring does not always hold.

With a more modern theory available, this construction which is now often used as an introduction to algebraic number theory, is mainly used as an example as Dedekind domains are more powerful than this. For example, every *principal ideal domain* is a Dedekind domain. So in Chapter 1 we will look at Dedekind domains and see their remarkable property of ideal factorisation and furthermore we will see that in fact the set of all these ideals, to be called *fractional ideals*, forms an abelian group and is generated by the prime ideals of the Dedekind domain and their *inverses*, which will also be looked at.

This theory will then act as background knowledge as in the next two chapters we generalise it to a non-commutative setting. We do this by defining *orders* in

semisimple algebras, which can be conceptually thought of as a subring that is a lattice in space (the space here being a semisimple algebra). The theory of orders here depends heavily on the requirement that they be 'maximal' in the sense that there is no other order larger than it (perhaps other than the algebra it is in). Using this conceptual definition, a Dedekind domain also forms a lattice in space that is a subring of its quotient field. For example the integers $\mathbb{Z}$ form a lattice in the rationals $\mathbb{Q}$ and are a Dedekind domain, as has been mentioned.

However when moving to orders, there is actually two kinds of ideal factorisation to consider. The first is two-sided ideals, the second one-sided ideals. Obviously the one-sided case encompasses the two-sided case, but there are certain properties in the two-sided case that can be related back to Dedekind domains, where these fail in the one-sided case. More specifically, the set of all two-sided ideals in a maximal order is an abelian group generated by the prime ideals of the maximal order. However, in the one-sided case no such nicety occurs. The set of one-sided ideals of a single maximal order can not even be considered. It turns out that we have to consider all ideals of all maximal orders and in that case it turns out to be a *groupoid*, a generalisation of a group, which will be called the *Brandt Groupoid* associated to the semisimple algebra.

Finally, we will look briefly at some nice results due to the theory from Chapter's 1,2 and 3. This will be in regard to seeing when the factorisation of elements in Dedekind domains and orders occurs (and also when unique factorisation of elements in an arbitrary ring implies the same for ideals), as well as looking at the first case of a Dedekind domain, the ring of algebraic integers. But nicest of all (for the author of this thesis anyway), we will look at the rational quaternions, an extension of the complex numbers, and then finish with a proof due to the preceding theory in Chapter's 1,2 and 3 of Lagrange's *Four Squares Theorem*: That every natural number can be written in the form

$$a^2 + b^2 + c^2 + d^2$$

for integers a, b, c and d.

Contents

Chapter 1

Dedekind Domains and Fractional Ideals

To start with, we will look at a standard view of the theory, with the end of the rainbow not being home to an Irishman with a pot of gold, but rather a uniqueness result about Dedekind domains. Chapter 1 is mainly to do with the commutative case, however a more general case will be done after this. So to keep a standard, unless defined or stated otherwise commutativity is not assumed and every ring is unital. Firstly though, some preliminaries must be carried out, but most of these should be familiar to the reader. If R is a *domain*, it is meant that R is a ring with no zero divisors. A ring is then an *integral domain* if it is a commutative domain. Assume hereon for the whole document that R is a ring with quotient ring K where $R \neq K$ and note that if R is an integral domain then K is a field. For clarity, the notation $\subset$ will denote a strict subset whereas $\subseteq$ indicates the possibility of equality.

1.1 Background

For a ring R, not necessarily commutative, a left *R-module* M is an additive abelian group with a map $R \times M \to M : (r, m) \mapsto rm$ such that for $r, s, 1 \in R$ and $m, n \in M$

- $(r + s)m = rm + sm$
- $r(m + n) = rm + rn$
- $(rs)m = r(sm)$
- $1m = m$.

Similarly, a right and two-sided module can be defined. The left R-module M is called *finitely generated* if it can be written as $M = Rx_1 + Rx_2 + \cdots + Rx_n$ for a finite number, n, of elements $x_i \in M$. An *R-algebra* is a ring A such that there exists a homomorphism $\phi : R \to Z(A)$ where $Z(A) = \{x \in A \mid xa = ax \text{ for every } a \in A\}$ is the centre of A. In this document, an algebra is always assumed to be associative. To see an A as an R-module, we define $r \cdot x = \phi(r)x$ for $r \in R$ and $x \in A$. The *dimension* of a K-algebra A over the field K is its dimension as a vector space over K.

Given an integral domain R, let A be a finite dimensional K-algebra. An element $\alpha \in A$ is *integral* over R if there is some monic polynomial $f(X) \in R[X]$ with $f(\alpha) = 0$ and similarly a subring $B \subseteq A$ is *integral* over R if every element of B is integral over R. Hence the set of all elements of A integral over R is called the *integral closure* of R in A and is denoted $\overline{R}^A$. R is then called *integrally closed* if the integral closure of R in K is R itself. For an integral domain R and finite dimensional K-algebra A, the following two results will be useful at times throughout this document. They are standard results so will not be proved here, but proofs can be found in Reiner [1, p.3-6], Jacobson [6, p.408-409] and Janusz [7, p.5-7].

Proposition 1.1.1 *The following are equivalent for an element $\alpha \in A$.*

a) *α is integral over R.*

b) *$R[\alpha]$ is a finitely generated R-module.*

c) *There is finitely generated R-module M that is a subring of A containing α.*

Proposition 1.1.2 *If R is integrally closed, then $\alpha \in A$ is integral over R if and only if the minimal polynomial of α over K, $p(X)$, is an element of $R[X]$.*

Some concepts of factorisation theory are required in a later chapter, but are also needed conceptually at times throughout the document, so a basic introduction will be given here. For the reader not familiar with this material, it can be found in Jacobson [5, p.140-149], Stewart & Tall [8, p.81-99] and Sivaramakrishnan [10, §2,3]. For an integral domain R, an element $u \in R$ is called a *unit* if there is some $v \in R$ such that $uv = vu = 1_R$. The set of units in R, $u(R)$, is then an abelian subgroup of R under multiplication. Then if two elements $a, b \in R$ satisfy $a = ub$ for some $u \in u(R)$ we call a and b *associates*. If $a = bc$ for $a, b, c \in R$, we say that b (or equivalently c) *divides* a and denote this by $b \mid a$. An element $p \in R$ is called *prime* when for two elements $a, b \in R$, if $p \mid ab$ then either $p \mid a$ or $p \mid b$. A non-zero non-unit element $r \in R$ is *irreducible* if for every factorisation $r = ab$ for $a, b \in R$, either $a \in u(R)$ or $b \in u(R)$. See that both a and b can not be in $u(R)$ since this forces $r \in u(R)$. Also note that irreducible elements are prime, but the converse is not necessarily true.

Example 1.1.3 Every irreducible element p in an integral domain R is prime since a factorisation $p = ab$ with $a, b \in R$ has, without loss of generalisation, $b \in u(R)$. So p and a are associates and $p \mid a$. □

Now we can define certain types of rings. Here they are commutative, but the definitions can be generalised to a non-commutative case. The integral domain R is called an *Unique Factorisation Domain* (or UFD) when for every element $r \in R$, there exists a factorisation of r into irreducible elements of R and if there are two factorisations $r = a_1 \cdots a_n = b_1 \cdots b_m$ with $a_i, b_j \in R$ irreducible for all i and j, then $n = m$ and $a_i = u_i b_{\pi(i)}$ for some permutation $\pi \in \text{perm}\{1, \cdots, n\}$ and unit $u_i \in u(R)$ for every i. That is, we can swap around the b_i's and multiply them by units to get $a_1 \cdots a_n$.

Certain rings have a nice property when looking at their ideals, so we will define those rings here. Given a subset $S \subseteq R$, the *ideal generated by* S is $\sum_{s \in S} sR$ and is denoted $\langle S \rangle$. An ideal I is then called a principal ideal if $I = \langle r \rangle = rR$ for some $r \in R$. That is, it is generated by one element of R. An integral domain R is thus called a *Principal Ideal Domain* (or PID) if every ideal of R is a principal ideal. It turns out that the following results hold, but note importantly that the converse of Theorem 1.1.5 does not hold.

Proposition 1.1.4 *Every prime element in a UFD is irreducible.*

Proof. Let R be a UFD and $p \in R$ be prime. If $p = ab$ for two elements $a, b \in R$, then $p \mid ab$ and without loss of generality say that $p \mid a$. Then $a = pc$ for some $c \in R$. But then $p = ab = pcb$ and hence $cb = 1$ since R is an integral domain, implying $b \in u(R)$ and p is irreducible. □

Theorem 1.1.5 *Every PID is a UFD.*

Proof. Let R be a PID and first suppose that there is some $r \in R$ that is not expressible as a product of irreducibles and so can not be irreducible itself. Then $r = a_1 b_1$ for some non-units a_1 and b_1 where at least one is not expressible as a product of irreducibles as well. Suppose without loss of generalisation this is a_1. Then we can write $a_1 = a_2 b_2$ for some non-units a_2 and b_2 where a_2 is not expressible as a product of irreducibles. Continuing this gets an infinite chain of proper ideals $\langle r \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle \subset \cdots$. Using Proposition 1.1.7 from ahead gets that this chain eventually stabilises, so one of the a_i's must be ireeducible, contradictiong that a_i is not expressible as a product of irreducibles.

Secondly, write $r \in R$ as $r = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$ for irreducible p_i and q_j. Since they are also prime we have $p_1 \mid q_1 q_2 \cdots q_m$, so $p_1 \mid q_k$ for some k and since p_1 and q_k are irreducible, $p_1 = u_1 q_k$ for some unit $u_1 \in u(R)$. Now $p_2 \cdots p_n = q_1 \cdots q_{k-1} q_{k+1} \cdots q_m$, so doing this repeatedly gets $n = m$ and each p_i an associate of some q_j with $1 = u_1 \cdots u_n$. Thus r is uniquely expressible as a product of irreducible elements of R up to rearrangement and associates, so R is a UFD. □

Example 1.1.6 The integers $\mathbb{Z}$ have ideals of the form $n\mathbb{Z}$, so they are a PID and thus a UFD. The units of $\mathbb{Z}$ are $u(\mathbb{Z}) = \{1, -1\}$ and the irreducible integers are the prime integers. □

Finally, a ring R is called left *noetherian* if its left ideals satisfy the ascending chain condition (that is, a chain of left ideals $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$ of R eventually has $I_n = I_N$ for every $N \geq n$.) and left *artinian* if its left ideals satisfy the descending chain condition (similarly to before but with a decreasing chain instead). This similarly holds for right noetherian and artinian, and a ring is just called noetherian or artianian if the respective chain conditions hold for both right and left ideals. Similarly, an R-module M is called *noetherian* or *artinian* if its submodules satisfy those same conditions. A *prime* ideal of an integral domain R is a non-zero proper ideal P such that R/P has no zero divisors. This definition is equivalent to saying that given ideals A, B and P, if $AB \subseteq P$ implies $A \subseteq P$ or $B \subseteq P$, then P is prime (which is analogous to the 'usual' definition of an element being prime, as given above). The following result about a PID will be useful. In fact, we have already used it.

Proposition 1.1.7 *Any PID is noetherian.*

Proof. Let R be a PID, $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$ be an infinite chain of ideals in R and $I = \cup_{i \geq 0} I_i$. Let $a, b \in R$, so $a \in I_i$ and $b \in I_j$ for some i and j and without loss of generality suppose that $i \leq j$. Then since $I_i \subseteq I_j, a + b \in I_j \subseteq I$ since I_j is a group and for $r \in R, rb \in I_j \subseteq I$ also, showing I is in fact an ideal of R. Since R is a PID, every ideal is principal, so $I = \langle p \rangle$ for some irreducible $p \in R$. Now $p \in I$, so $p \in I_k$ for some k and $I_0 \subseteq I_1 \subseteq \cdots \subseteq I_k = I_{k+1} = \cdots$, showing R is noetherian. □

Example 1.1.8 A maximal ideal I of an integral domain R is a prime ideal since R/I is a field. □

1.2 Dedekind Domains

Now using these definitions we can define a certain sort of ring, called a Dedekind domain or Dedekind ring, which is the assumption taken upon many rings in this document. As will be found by the end of the document, these types of rings all have a property that can help when trying to establish when elements of R can be expressed uniquely in terms of its irreducible elements, that is, when R is a unique factorisation domain. But their main property, as we will find, is their ability to factorise of ideals.

The theory of Dedekind domains comes from the studies of the factorisation properties of the ring of algebraic integers $\mathcal{O}_K$ in an algebraic number field K. Dedekind (1831-1916) in the latter half of his life, knowing that $\mathcal{O}_K$ was not always a UFD, looked at 'fractional ideals' of $\mathcal{O}_K$ rather than elements and saw that there was always a unique factorisation of them. This lead to the use of the word *ideal* in its common usage and the use of his name for the ring we are about to define.

References for the rest of this chapter are Reiner [1, p.44-50], Curtis & Reiner [4, §18], Jacobson [6, §10], Janusz [7, p.8-18], Samuel [9, p.47-52] and Sivaramakrishnan [10, p.394-410]. There are other definitions of a Dedekind ring involving projectivity and localizations and discrete valuation rings, but they will not be looked at. Our definition will be as follows.

Definition 1.2.1 An integral domain R is called a *Dedekind domain* if it is noetherian, integrally closed and such that every non-zero prime ideal is maximal.

This definition is equivalent to a remarkable fact about the 'factorisation' of ideals in the integral domain R into 'irreducibles.' You might guess that these irreducibles are the maximal ideals of R and in that case, you would be right. Except when R is a Dedekind domain prime ideals coincide with the maximal ideals, or 'irreducible' ideals, which is reminiscent of the property in unique factorisation domains that prime elements are irreducible and every element can be written as a unique product of prime elements. The reader may also guess that principal ideal domains may be important here, and again they would be right as the following examples give an indication of.

Example 1.2.2 As with many things in number theory, some concepts are vast generalisations of properties held by the integers. The PID $\mathbb{Z}$ is a noetherian integrally closed integral domain with quotient field $\mathbb{Q}$. Since its prime ideals are of the form $p\mathbb{Z}$ for p a non-zero prime integer, the prime ideals coincide with the maximal ideals of $\mathbb{Z}$ and hence it is a Dedekind domain. □

Proposition 1.2.3 *Every PID is a Dedekind domain.*

Proof. Proposition 1.1.7 shows us every PID is noetherian, so we only need to show the other two requirements. Let R be a PID and $\langle p \rangle$ be a prime ideal in R. Then for two ideals $\langle a \rangle$ and $\langle b \rangle$ of R that have $\langle a \rangle \langle b \rangle = \langle ab \rangle \subseteq \langle p \rangle$, it follows that $p \mid ab$. But then $\langle a \rangle \subseteq p$ or $\langle b \rangle \subseteq \langle p \rangle$ since $\langle p \rangle$ is prime, so we have either $p \mid a$ or $p \mid b$, showing p is prime as an element of R. Theorem 1.1.4 then implies p is irreducible, so $\langle p \rangle$ is actually a maximal ideal.

For the proof of being integrally closed, the usual proof will do. Let $x \in K$ and suppose it is a root of a polynomial $X^n + c_{n-1}X^{n-1} + \cdots + c_1 X + c_0 \in R[X]$. Then

since K is a UFD, $x = \frac{p}{q}$ where p and q are coprime. Then substituting $\frac{p}{q}$ into the polynomial and multiplying by q^n gets

$$p^n + c_{n-1}qp^{n-1} + \cdots + c_1q^{n-1}p + c_0q^n = 0.$$

Thus $q \mid p$ must follow and $q = \pm 1$, so $x \in R$ and R is integrally closed, proving the proposition. □

Example 1.2.4 The ring $\mathbb{Z}[\sqrt{-5}] = \mathbb{Z} \oplus \sqrt{-5}\mathbb{Z}$ is a Dedekind domain. Firstly, it is noetherian since $\mathbb{Z}$ is noetherian. Secondly, it is integrally closed since if $q = \frac{a}{b} + \frac{c}{d}\sqrt{-5} \in \mathbb{Q}[\sqrt{-5}]$ with (a, b) and (c, d) pairwise coprime is a root of a monic polynomial $X^n + c_{n-1}X^{n-1} + \cdots + c_1X + c_0 \in \mathbb{Z}[\sqrt{-5}][X]$, then substituting $X = q$ and multiplying by $(bd)^n$ gets

$$(bdq)^n + c_{n-1}(bd)(bdq)^{n-1} + \cdots + c_1(bd)^{n-1}(bdq) + c_0(bd)^n = 0,$$

a ploynomaial in $\mathbb{Z}[\sqrt{-5}][bdq]$ But bd divides 0, so it must divide the left hand side, so must divide $(bdq)^n$. But $bdq = ad + cb\sqrt{-5}$, so bd must divide both ad and cb, implying both b and d are either 1 or -1, so $q \in \mathbb{Z}[\sqrt{-5}]$.

Thirdly, let P be a prime ideal of $\mathbb{Z}[\sqrt{-5}]$. If $a + b\sqrt{-5} \in P$, then both of $5ab + 5b^2\sqrt{-5}, a^2\sqrt{-5} - 5ab \in P$, so adding gets $a^2 + 5b^2 \in P$ also. But an integer $n \in P$ if and only if $n\sqrt{-5} \in P$ too. Thus P is of the form $p\mathbb{Z}+\sqrt{-5}p\mathbb{Z}$ for some $p \in \mathbb{Z}$. If $n = ab$ for some $a, b \in \mathbb{Z}[\sqrt{-5}]$, then $P = (a\mathbb{Z}+a\sqrt{-5}\mathbb{Z})(b\mathbb{Z}+b\sqrt{-5}\mathbb{Z}) = AB$, so $AB \subseteq P$ (Note the multiplication of ideals is given by (1.2) ahead, if required). But $P \subset A$ and $P \subset B$, so P can not be prime. Thus p must be an irreducible in $\mathbb{Z}[\sqrt{-5}]$. Let I be an ideal of $\mathbb{Z}[\sqrt{-5}]$ such that $P \subset I$. Then there is some $a \in \mathbb{Z} \cap I$ such that $p \nmid a$. But by the Euclidean algorithm there exists $x, y \in \mathbb{Z}$ such that $xp + ya = 1$, so $I = R$ and P is maximal.

This example was given for a particular reason. Since $6 = (1+\sqrt{-5})(1-\sqrt{-5}) = 2.3$, it is not a UFD and thus not a PID. This shows the converse of Proposition 1.2.3 does not necessarily hold. □

Example 1.2.5 For another example, given a finite field extension $L/\mathbb{Q}$ consider the integral closure of $\mathbb{Z}$ in L and let $\mathcal{O}_L = \overline{\mathbb{Z}}^L$. Then $\mathcal{O}_L$ is a ring called the algebraic integers of L (or the ring of integers of L) and is in fact a Dedekind domain. This example will be reintroduced later in Chapter 4 when talking about the class number. □

However from here the relationship between unique factorisation of elements and of ideals will be left until Chapter 4. What we need to focus on is what we are trying to look at. If we want to factorise ideals lets make sure that we know exactly what we mean when we say an ideal. Before we do this, we again need to build up some standard theory. Tensor products will be used here, but not in their full power, so only a small notion of them is required. For readers unfamiliar with tensor product see Curtis and Reiner [4, §12] and Jacobson [6, p.125-133]. For a basic view of a construction of a tensor product of two modules, let R be an integral domain and

consider a right R-module M, left R-module N, and the module T generated by their product $M \times N$

$$T = \{\text{finite sums} \sum_i r_i(m_i, n_i) \mid m_i \in M, n_i \in N, r_i \in R\}.$$

Now look at the subgroup V of T generated by the following subset of T, for all $m, m' \in M$, $n, n' \in N$ and $r \in R$.

$$\begin{cases} (m + m', n) - (m, n) - (m', n) \\ (m, n + n') - (m, n) - (m, n') \\ (mr, n) - r(m, n) \\ (m, rn) - r(m, n) \end{cases}$$

Then we define the *tensor product* of M and N over R to be $M \otimes_R N = T/V$. Here the tensor product $M \otimes_R N$ is actually an R-module. This is because for $r, s \in R$ and $m \in M, n \in N$,

$$r(s(m, n)) = r(ms, n) = ((ms)r, n) = (m(sr), n) = (sr)(m, n).$$

So since R is an integral domain, $rs = sr$ allows $M \otimes_R N$ to be an R-module. If the tensor product is over the quotient field K, then $M \otimes_K N$ is more specifically a vector space. In the case we deal with, $M = K$, the quotient field of R, and N is commutative. So it is actually just the vector space $K \otimes_R N$ and for ease ignore the $\otimes_R$ and just write

$$K \otimes_R N = K \cdot N = \{\text{finite sums} \sum_i k_i n_i \mid k_i \in K, n_i \in N\}. \tag{1.1}$$

That is all that is required of tensor products here (actually (1.1) is the the main point), so we will move onto some more definitons. For an integral domain R and R-module M, the *annihilator* of M is defined by $ann_R M = \{r \in R \mid rM = 0\}$ and similarly the *annihilator* of an element $m \in M$ is defined by $ann_R m = \{r \in R \mid rm = 0\}$. The element $m \in M$ is called an *R-torsion* element if $ann_R m \neq 0$ and M is called *R-torsionfree* if the only R-torsion element in M is 0.

The point here of torsion elements is that we want to visualize M as $1 \otimes_R M$ inside $K \otimes_R M$. If there is a R-homomorphism $\phi : M \to K \otimes_R M : m \mapsto (1, m)$, then $ker\{\phi\}$ is the submodule of these torsion elements in M, and M being R-torsionfree sets $ker\{\phi\} = 0$, giving us what we want. See Reiner [1, p.32-34, 44] for more details on this. Now we can define the following for an integral domain R. An *R-lattice* is a finitely generated R-torsionfree R-module. Each R-lattice L is an R-submodule of the finite dimensional vector space $V = K \otimes_R L = K \cdot L$. Hence L is called a *full R-lattice* in V to emphasize that L has a K-basis of V. This leads us to the following, as descibed in Reiner [1, p.47-48] and Swan & Evans [2, p.83-84], which turns out to be the same as the other references listed earlier.

Definition 1.2.6 For a Dedekind domain R, a non-zero full R-lattice in K is called a *fractional R-ideal*.

Note here that since the vector space V of a fractional R-ideal L is actually the field K, it trivially follows that a finitely generated R-submodule of K is R-torsionfree (since R is an integral domain) and satisfies $K \cdot L = V = K$ (since K is a field). So a fractional R-ideal can be defined more simply to be just a finitely generated R-submodule in K. Some important things to note are that for a fractional R-ideal L there is an $r \in R$ satisfying $rL \subseteq R$ since L is finitely generated in K. Secondly, every ideal I of R is itself a fractional R-ideal since it is a R-submodule of $R \subset K$ which is noetherian. Thirdly, the multiplication of two fractional ideals J and L is defined by

$$JL = \{\text{finite sums} \sum_i j_i l_i \mid j_i \in J, l_i \in L\}. \tag{1.2}$$

Since J and L are finitely generated, JL must be finitely generated and is thus a fractional ideal too.

These fractional ideals are the key part of the theory for factorisation of ideals into prime ideals in a Dedekind domain. But to show this requires a bit more work. It turns out to be of immeasurable use to look at the set of elements of K that send a fractional ideal inside R. The reason being that the product of two fractional ideals is another fractional ideal and R is istelf a fractional R-ideal, so this set of elements gives the possible notion of a group with identity R. As we will soon see in the next section, this indeed gives us what we want. So to finish this section, given a Dedekind domain R define for a fractional R-ideal L

$$L^{-1} = \{x \in K \mid xL \subseteq R\}. \tag{1.3}$$

L^{-1} is clearly an R-module in K and by the note above there is an $r \in R$ such that $rL \subseteq R$, so $L^{-1} \neq 0$. Now a non-zero $x \in L$ satisfies $L^{-1}x \subseteq R$, so $yx \in R$ for every $y \in L^{-1}$. So $y \in Rx^{-1}$ and L^{-1} is an R-submodule of the principal R-module Rx^{-1} and is thus finitely generated itself. So L^{-1} is also a fractional R-ideal.

Example 1.2.7 As before, take the Dedekind domain $\mathbb{Z}$. Then $(p/q)\mathbb{Z}$ is a fractional ideal for non-zero $p, q \in \mathbb{Z}$ and $((p/q)\mathbb{Z})^{-1}$ is given by $(q/p)\mathbb{Z}$. Actually, all fractional ideals of $\mathbb{Z}$ are of that form. More generally, for any Dedekind domain R, xR is a fractional ideal for a non-zero $x \in K$ and $(xR)^{-1}$ is given by $x^{-1}R$. But all ideals of R are of that form only if R is a PID. □

1.3 The Factorisation of Ideals

From here we can start to think about if we can factorise ideals of a Dedekind domain R into maximal (or prime) ideals and even better if we can factorise all fractional ideals of R into prime ideals, which will be the aim of the rest of this chapter. The order of the results here is sometimes in the opposite direction of the order given in sources containing this material, but the content is often the same. References for this section were mentioned at the definition of a Dedekind domain and are Reiner [1, p.44-50], Curtis & Reiner [4, §18], Jacobson [6, §10], Janusz [7, p.8-18], Samuel [9, p.49-52] and Sivaramakrishnan [10, p.394-410]. From here, only a few results are needed to get the group structure that was mentioned before, but they also are our stepping stones towards our aim of factorising ideals.

Proposition 1.3.1 *Every proper ideal I of a Dedekind domain R contains a product of prime ideals of R and has $R \subset I^{-1}$.*

Proof. For completeness, note the ideal $I = R$ contains any product of prime ideals, but $I^{-1} = R^{-1} = R$. Let A be the set of proper ideals of R that do not contain a product of prime ideals. Since R is noetherian there must exist an ideal I in A that is contained in no other ideal in A, that is, a maximal element of A. Now I cannot be prime and any ideal properly containing I must contain a product of prime ideals. Since I is not prime, there are elements $r, s \in R - I$ such that $rs \in I$ and hence $I + rR$ and $I + sR$ are ideals properly containing I, so each contains a product of prime ideals. But

$$(I + rR)(I + sR) \subseteq II + rI + sI + rsR \subseteq I$$

and so I must contain a product of prime ideals, contradicting the existence of a maximal element of the set A, and A is empty.

For the second part of the proposition let I be a proper ideal of R. Then clearly $I^{-1} \supseteq R$, so we must show $I^{-1} - R$ is not empty. Let $i \in I$ be non-zero. Then by the previous part there are prime ideals $P_1, \ldots, P_n$ such that $P_1 \ldots P_n \subseteq iR \subseteq I$, and select $P_1, \ldots, P_n$ such that n is minimal. As R is noetherian and $I \subset R$ there is some maximal ideal P with $P_1 \ldots P_n \subset P$. If $P_k \neq P$ for every k, then there are $p_k \in P_k$ where $p_k \notin P$ and $p_1 \ldots p_n \in P$, so $p_k R \not\subseteq P$ and $p_1 R \ldots p_n R = p_1 \ldots p_n R \subseteq P$, contradicting P being prime (since maximal ideals are prime ideals). Thus $P = P_k$ for some k and

$$P_1 \ldots P_n = P_1 \ldots P_{k-1} P_{k+1} \ldots P_n P \subseteq iR \subseteq I \subseteq P.$$

Now since n is minimal, $P_1 \ldots P_{k-1} P_{k+1} \ldots P_n \not\subseteq iR$, so select some element $p \in P_1 \ldots P_{k-1} P_{k+1} \ldots P_n - iR$. Thus $i^{-1} p \notin R$ and

$$i^{-1} pI \subseteq i^{-1} pP \subseteq i^{-1} P_1 \ldots P_{k-1} P_{k+1} \ldots P_n P \subseteq i^{-1}(iR) = R$$

and hence $i^{-1} p \in I^{-1} - R$. □

Proposition 1.3.2 *For a Dedekind domain R and fractional R-ideal L, the set $\{x \in K \mid xL \subseteq L\} = R$.*

Proof. Let $S = \{x \in K \mid xL \subseteq L\}$ and note that $R \subseteq S$ since L is an R-module, so we only need to show the reverse inclusion. Let $s \in S$, then for $n \in \mathbb{N}$

$$s^n L = s^{n-1}(sL) \subseteq s^{n-1} L \subseteq \ldots \subseteq sL \subseteq L,$$

so $L[s]$ is an R-submodule of L and is thus finitely generated. If $L \subseteq R$, then since R is integrally closed it follow by Proposition 1.1.1 that $s \in R$. If $L \supset R$ then $R[s]$ is a finitely generated submodule of $L[s]$ and similarly $s \in R$. □

Corollary 1.3.3 *For a fractional ideal L of a Dedekind domain R, $L^{-1} L = L L^{-1} = R$.*

Proof. By definition $L^{-1}L \subseteq R$ and since $L^{-1}L$ is itself a fractional ideal, it is an ideal in R and so $(L^{-1}L)^{-1}(L^{-1}L)$ is also an ideal in R. By Proposition 1.3.1, if $L^{-1}L$ is proper in R then $(L^{-1}L)^{-1} \supset R$. Now since $(L^{-1}L)^{-1}(L^{-1}L) \subseteq R$ we have $(L^{-1}L)^{-1}L^{-1} \subseteq L^{-1}$ and thus $(L^{-1}L)^{-1} \subseteq R$ by Proposition 1.3.2. So $L^{-1}L$ can not be proper and we must have $L^{-1}L = R$. Also, $LL^{-1} = R$ since R is commutative. □

Note also that for a fractional R-ideal L, this imples that $(L^{-1})^{-1} = L$. Now do we have a group structure? Firstly, the product of two fractional ideals is a fractional ideal (and is commutative since R is). Secondly the product of fractional ideals is clearly associative since R is. Thirdly and finally; R is the unity element and there exist inverses for every fractional ideal that satisfy Corollary 1.3.3. Thus we have just proven the following theorem.

Theorem 1.3.4 *For a Dedekind domain R, the set of fractional R-ideals $\mathcal{L}_R$ is a multiplicative abelian group with identity R and the inverse of $L \in \mathcal{L}_R$ given by L^{-1}.*

But what about our aim? If we want to be able to factorise every ideal of a Dedekind domain R, or even better, every fractional ideal of R in terms of prime ideals of R, then it makes sense that the set of fractional R-ideals $\mathcal{L}_R$ would be generated by the prime ideals of R. Indeed this is the case and the following results lead to its proof. But first, say for two fractional ideals L and J that L *divides* J when there is an ideal $I \subseteq R$ such that $J = LI$ and denote this by $L \mid J$. Then there is the following equivalence.

Proposition 1.3.5 *Let J and L be fractional ideals of the Dedekind domain R. Then $J \subset L$ if and only if there is a proper ideal $I \subset R$ such that $J = LI$.*

Proof. One way is trivial since if $J = LI$ then $L = LR \supset LI = J$. So let $J \subset L$. Then $R = L^{-1}L \supset L^{-1}J$ and $L^{-1}J$ is a proper ideal in R. Letting $I = L^{-1}J$ gets $LI = LL^{-1}J = J$ as required. □

Lemma 1.3.6 *The ideals in a Dedekind domain can be written uniquely in terms of its prime ideals up to rearrangement.*

Proof. First show an ideal in the Dedekind domain R can be written as a product of prime ideals and afterwards show this expression is unique up to rearrangement. We define the ideal R of R to be an empty multiplication of primes, so exclude this case. Let S be the set of proper ideals in R that can not be expressed as a product of prime ideals and suppose it is not empty. Since R is noetherian there is a maximal element $K \in S$ that can not be a maximal ideal in R (since maximal ideals are prime). Let J be a maximal ideal of R strictly containing K. By Proposition 1.3.5 there is a proper ideal I in R such that $K = JI$. Now $I = RI \supset JI = K$, so we have $R \supset J, I \supset K$ and by the maximality of K both J and I are products of prime ideals. But then so is $JI = K$ and thus S must be empty.

Now suppose that two products of prime ideals are equal, say $P_1P_2 \dots P_n = Q_1Q_2 \dots Q_m$ for prime ideals P_i, Q_j and positive integers n, m. As in Proposition 1.3.1, let P be a maximal ideal in R such that $P_1P_2 \dots P_n \subseteq P$. Then if $P \neq P_i$ for

every i there are $p_i \in P_i$ where $p_i \notin P$ such that $p_1 p_2 \dots p_n \in P$. So $p_i R \nsubseteq P_i$ for every i and $p_1 R p_2 R \dots p_n R = p_1 p_2 \dots p_n R \subseteq P$, contradicting P being prime. So let $P = P_k$ for some k. Similarly $Q_1 Q_2 \dots Q_m \subseteq P$ and thus $P = Q_l$ for some l. So $P_k = Q_l$ and we get

$$\begin{aligned} P_1 P_2 \dots P_k \dots P_n &= Q_1 Q_2 \dots Q_l \dots Q_m \\ P^{-1} P_k P_1 P_2 \dots P_{k-1} P_{k+1} \dots P_n &= P^{-1} Q_l Q_1 Q_2 \dots Q_{l-1} Q_{l+1} \dots Q_m \\ P_1 P_2 \dots P_{k-1} P_{k+1} \dots P_n &= Q_1 Q_2 \dots Q_{l-1} Q_{l+1} \dots Q_m. \end{aligned}$$

By doing this procedure another $n-2$ times it is clear that $n = m$ and each P_i coincides with some Q_j. Thus the factorisation is unique up to rearrangement. □

We now know every proper ideal I of a Dedekind domain R can be written in the form $I = Q_1 Q_2 \dots Q_m$ for some positive integer m and prime ideals Q_j, so we can rewrite this as $I = P_1^{e_1} P_2^{e_2} \dots P_n^{e_n}$ for some positive integer $n \leq m$ where all the P_i are distinct and $e_i > 0$. This remarkable (and only slightly set up) property as mentioned earlier is reminiscent of the integers and principal ideal domains and is where the this theory, the theory of Dedekind domains, was born. Also, it gives us a nice generalisation of the greatest common divisor and lowest common multiple.

Corollary 1.3.7 *The greatest common divisor of two ideals I, J of R, denoted gcd(I, J), and lowest common multiple, denoted lcm(I, J), both exist and are a product of prime ideals of R.*

Proof. Write $I = P_1^{e_1} \dots P_n^{e_n}$ and $J = P_1^{f_1} \dots P_n^{f_n}$ where e_i and f_j are natrural numbers as in the previous lemma. Then $\gcd(I, J) = P_1^{\min\{e_1, f_1\}} \dots P_n^{\min\{e_n, f_n\}}$ and $\operatorname{lcm}(I, J) = P_1^{\max\{e_1, f_1\}} \dots P_n^{\max\{e_n, f_n\}}$. □

This last Lemma also gives us a nice fact. If $I = P_1^{e_1} P_2^{e_2} \dots P_n^{e_n}$ is a proper ideal in R, then can we use this to write I^{-1} in a similar form? Consider $P_1^{-e_1} P_2^{-e_2} \dots P_n^{-e_n}$ where $P_i^{-e_i} = \underbrace{P_i^{-1} \cdots P_i^{-1}}_{e_i \text{ times}}$. Then

$$I P_1^{-e_1} P_2^{-e_2} \dots P_n^{-e_n} = P_1^{e_1} P_2^{e_2} \dots P_n^{e_n} P_1^{-e_1} P_2^{-e_2} \dots P_n^{-e_n} = R$$

and it follows that $I^{-1} = P_1^{-e_1} P_2^{-e_2} \dots P_n^{-e_n}$. This then allows us to extend the preceding Lemma to get one of the main theorems of this chapter.

Theorem 1.3.8 *The abelian group of fractional ideals $\mathcal{L}_R$ of a Dedekind domain R is generated by the prime ideals of R and their inverses.*

Proof. This will be proved by showing every fractional ideal can be written as a product of primes and prime inverses. Let L be any fractional ideal of R. If $L \subseteq R$, then this is immediate by Lemma 1.3.6 so let $L \nsubseteq R$. As mentioned earlier, since L is finitely generated there is a non-zero $r \in R$ such that $rL \subseteq R$, so rL is an ideal in R. By Lemma 1.3.6 we can write this as $rL = P_1^{e_1} P_2^{e_2} \dots P_n^{e_n}$ for some non-negative integer n, positive integers e_i and prime ideals P_i. Similarly $rR = Q_1^{f_1} Q_2^{f_2} \dots Q_m^{f_m}$ for some non-negative integer m, positive integers f_j and prime ideals Q_j. So $rL =$

$(rR)L$ and thus $L = (rR)^{-1}P_1^{e_1}P_2^{e_2}\dots P_n^{e_n} = Q_1^{-f_1}Q_2^{-f_2}\dots Q_m^{-f_m}P_1^{e_1}P_2^{e_2}\dots P_n^{e_n}$. That is, L can be written as the product of prime ideals and inverses of prime ideals and this factorisation is unique (up to rearrangement) since the factorizations of rL and rR are themselves. Thus the set of fractional ideals $\mathcal{L}_R$ is generated by the prime ideals of R and their inverses. □

Example 1.3.9 As in Example 1.2.7, fractional ideals of $\mathbb{Z}$ are of the form $\frac{p}{q}\mathbb{Z}$ for $\frac{p}{q} \in \mathbb{Q}$. So let p and q be coprime and write p and q as their prime factorisations $p = x_1^{i_1}\cdots x_n^{i_n}$ and $q = y_1^{j_1}\cdots y_m^{j_m}$. Then

$$\begin{aligned}\frac{p}{q}\mathbb{Z} = \frac{x_1^{i_1}\cdots x_n^{i_n}}{y_1^{j_1}\cdots y_m^{j_m}}\mathbb{Z} &= (x_1^{i_1}\mathbb{Z})\cdots(x_n^{i_n}\mathbb{Z})(y_1^{-j_1}\mathbb{Z})\cdots(y_m^{-j_m}\mathbb{Z}) \\ &= (x_1\mathbb{Z})^{i_1}\cdots(x_n\mathbb{Z})^{i_n}(y_1\mathbb{Z})^{-j_1}\cdots(y_m\mathbb{Z})^{-j_m}.\end{aligned}$$

Also, the abelian group of fractional ideals $\mathcal{L}_\mathbb{Z}$ is just the group generated by

$$\{\mathbb{Z}\} \cup \{2\mathbb{Z}, 3\mathbb{Z}, 5\mathbb{Z}, 7\mathbb{Z}, 11\mathbb{Z}, \cdots\} \cup \{\frac{1}{2}\mathbb{Z}, \frac{1}{3}\mathbb{Z}, \frac{1}{5}\mathbb{Z}, \frac{1}{7}\mathbb{Z}, \frac{1}{11}\mathbb{Z}\cdots\}.$$

□

So in a similar fashion to the previous Lemma, we can now write any fractional ideal $L \in \mathcal{L}_R$ uniquely in the form $L = P_1^{e_1}P_2^{e_2}\dots P_n^{e_n}$ for some non-negative integer n with each P_i distinct. But this time each e_i is a non-zero integer, not necessarily positive. This theorem effectively gives us a characterisation of Dedekind domains and to conclude the chapter, it turns out that if we went backwards, then everything works out nicely. But as the next chapters will show us, the uniqueness result about Dedekind domains that we have found can be generalised. So if we are at the end of the rainbow now, then maybe the pot of gold would of been better?

Theorem 1.3.10 *The following are equivalent for an integral domain R.*

- **a)** *The ring R is a Dedekind domain.*
- **b)** *The ring R is noetherian, integrally closed and every non-zero prime ideal in R is maximal.*
- **c)** *Every proper ideal L in R is expressible as a product of prime ideals of R uniquely up to rearrangement as $P_1^{e_1}\dots P_n^{e_n}$ with each P_i distinct and $e_i > 0$.*
- **d)** *The set of fractional ideals $\mathcal{L}_R$ of R is generated by the prime ideals of R and their inverses.*

Proof. By definition, a) and b) are equivalent and Theorem 1.3.8 c) and d) must be equivalent. Also, we have just shown that b) implies c), so we only need to show that c) or d) implies b) to get the theorem. Assume d) and consider an infinite chain of ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$. Then write $I = P_1\cdots P_n$ for prime ideals P_i not necessarily distinct. Then the chain can have at most n distinct proper ideals, so eventually stabilizes and thus R is noetherian. Secondly, let $\alpha \in K$ be a root of the polynomial $X^n + c_{n-1}X^{n-1} + \cdots c_1X + c_0 \in R[X]$. Then $\alpha^n = -c_{n-1}\alpha^{n-1} - \cdots - c_1\alpha - c_0$, so letting $L = \langle \alpha^{n-1}, \cdots, \alpha, 1\rangle$ we see that $\alpha^n \in L$ and thus $\alpha L \subseteq L$. But $L = P_1\cdots P_k$ is a product of prime ideals P_i of R, so multiplying

both sided by $P_1^{-1} \cdots P_k^{-1}$ gets $\alpha R \subseteq R$, so $\alpha \in R$. Finally, clearly the prime ideals coincide with the maximal ideals. So R is a Dedekind domain, showing d) implies b) and proving the theorem. $\square$

Chapter 2

Dedekind Domains and Orders

In Chapter 1, we went through what a Dedekind domain was and how ideals in Dedekind domains could be written as a product of prime ideals. But what about doing this more generally? What do we mean here by more generally? We mean for much larger rings than Dedekind domains, say for rings containing Dedekind domains. Dedekind domains are of course commutative, so to do this more generally, we generalise the ideas in Chapter 1 to a non-commutative setting. So as mentioned at the beginning of Chapter 1, commutativity is not assumed. To start, we extend our reach and consider algebras over a Dedekind domain's quotient field, then take a subring of this algebra and see if this subring (which is not necessarily commutative or a domain) has a similar type of factorisation into 'prime' ideals.

Some preliminaries are required to move forward, so we will say these here. Recalling a definition from Chapter 1, For a commutative ring S, an *S-algebra* is a ring A such that there exists a homomorphism $h : S \to Z(A)$ where $Z(A) = \{x \in A \mid xa = ax \text{ for every } a \in A\}$ is the centre of A. So to see A as an S-module, we define $s \cdot x = h(s)x$ for $s \in S$ and $x \in A$. An S-algebra A is then called *simple* if it has no non-trivial two-sided ideals and *semisimple* if A is the direct product of simple subalgebras.

The use of fields in this chapter require some properties, so again let us define them here. Let F be a field and K/F be a field extension. Then K is called *separable* over F if the minimal polynomial of every $\alpha \in K$ over F factors into distinct linear factors over K. The *dimension* of an F-algebra A over F is its dimension as a vector space over F. For the finite dimensional F-algebra A, if A is semisimple and the centre of each simple simple summand of A is a separable field extension of F, then A is called *separable* over F.

Also recall from Chapter 1 that for a Dedekind domain R with quotient field K and vector space V over K, a *full R-lattice* in V is a finitely generated R-torsionfree R-module M in V that satisfies $K \otimes_R M = K \cdot M = V$ by the equality (1.1). This allows us to define a major part of the theory from hereon. So for the rest of this chapter let R be a Dedekind domain with quotient field K, A be a finite dimensional separable semisimple K-algebra and M be a full R-lattice in A. Note that A is always associative, but not necessarily commutative and that K is a subring of $Z(A)$.

2.1 Orders

In Chapter 1 we defined an integral domain to be a Dedekind domain if

I It was noetherian.

II It was integrally closed.

III Every prime ideal was maximal.

If we use these three properties as a hint to help find subrings of A able to factorise ideals as we can in Dedekind domains, then these subrings might not be as complicated or hard to find as first thought. Actually, as references Reiner [1, p.108-110], Swan & Evans [2, p.83-84], Bass [3, p.152-156] and Curtis & Reiner [4, p.515-517] point out, these types of subrings are starring us in the face; as the next seemingly abstract definition of an *R-order* points out.

Definition 2.1.1 A unital subring Λ of A that is a full R-lattice in A is called an *R-order* in A.

As with Dedekind domains there are also other definitions of an R-order that involve Krull rings and primary ideals, but they will not be looked at. So for this reason Reiner [1] and Swan & Evans [2] are the main references for this chapter, though Bass [3] and Curtis & Reiner [4] still provide some input, but not as much. (Note that conceptually orders can be thought of as follows: Starting with a finite number of points in space, we can extend these by adding an subtracting points from each other to make a lattice in that space, and if that lattice turns out to be a subring of the space without needing infinitely many points to generate it, then it is an order).

So does this definition satisfy the three properties above? Since R is noetherian and the R-order Λ is finitely generated, Λ must also be noetherian for both left and right ideals. So we will just call Λ noetherian to indicate both left and right noetherian. Thus property I above is satisfied for Λ and we are off to a good start. After a few examples of some orders we will focus our aims at the next two properties.

Example 2.1.2 If we let A be the $n \times n$ matrices over K, $M_n(K)$, then the homomorphism $K \to A : x \mapsto xI_n$ shows A is a K-algebra. Let Λ be the subring and R-module $M_n(R)$. See that Λ is generated by $\{(1)_{ij} \mid 0 \leq i, j \leq n\}$ where $(1)_{ij}$ is the matrix with a 1 in the ij^{th} position and zero's elsewhere and so is finitely generated by n^2 elements. Since $K \cdot \Lambda = A$ and Λ contains the identity I_n with 1's in the main diagonal and zero's elsewhere, it is a unital subring and a full R-lattice in A, so an R-order in A. □

Example 2.1.3 Let $R = \mathbb{Z}$ and $A = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k \subset \mathbb{H}$ be the rational quaternions, where $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$ is an extension of $\mathbb{C}$ called the quaternions where $i^2 = j^2 = k^2 = ijk = -1$. This is a $\mathbb{Q}$-algebra since $\mathbb{Q}$ is embedded in A. If we let Λ be the subring $\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}k$, then Λ is also a finitely generated $\mathbb{Z}$-module containing the identity $1 \in \mathbb{Z}$ with $\mathbb{Q} \cdot \Lambda = A$, so it is a $\mathbb{Z}$-order in A. □

Example 2.1.4 It is important to note that both the algebras in the previous two examples were separable and semisimple. In fact, both were simple algebras. But if orders are to generalise the notion of a Dedekind domain, then letting $A = K$ and $\Lambda = R$ should work and as expected, it does. □

In Chapter 1 we defined the inverse of a fractional R-ideal L in (1.3) by elements $x \in K$ that sent xL inside R, and then showed in Proposition 1.3.2 that $\{x \in K \mid xL \subseteq L\} = R$. So what if we consider something similar for a full R-lattice M in A? Take the set $S = \{x \in A \mid xM \subseteq M\}$. Then S is a unital subring of A and clearly an R-module. But what else can we say about it?

Since M is a full R-lattice in A, xM is an R-lattice in A for every $x \in A$ (not necessarily a full R-lattice). Now we can write $x = k_1m_1 + \cdots k_nm_n$ for some $k_i \in K$ and $m_i \in M$ since $K \cdot M = A$. Since $k_i \in K$, there is an $r_i \in R$ such that $r_ik_i \in R$. Thus there is an $r \in R$ such that $rx = rk_1m_1 + \cdots + rk_nm_n \in M$ and thus $rx \in S$. So $x = r^{-1}rx \in K \cdot S$ and we have $A \subseteq K \cdot S$. Hence $A = K \cdot S$. If we now take $x = 1$, then there is an $r \in R$ with $r \in M$. So $Sr \subseteq M$ and $S \subseteq r^{-1}M$. Since $r^{-1}M$ is an R-lattice by above thus so is S. Hence S is actually an R-order in A. Similarly, the set $\{x \in A \mid Mx \subseteq M\}$ is an R-order and we can define the following.

Definition 2.1.5 The *left* and *right orders* of M are defined respectively as

$$O_l(M) = \{x \in A \mid xM \subseteq M\},$$
$$O_r(M) = \{x \in A \mid Mx \subseteq M\}.$$

Now returning to before to see if the other two properties hold, we first note that they do not quite do what we want them to at the moment. Looking at the second property, 'integrally closed' is defined for a ring with respect to its quotient field, but we only want to look at an R-order of A, not the whole of A or of the integral closure of A. So we just want an R-order to be integral over A. This query is then solved by the following theorem.

Theorem 2.1.6 *The R-order Λ is integral over R and thus the minimal polynomial of every $\alpha \in \Lambda$ over K, $p_\alpha(X)$, is in $R[X]$.*

Proof. Let $x \in \Lambda$. Since Λ is an R-lattice and $R[x] \subseteq \Lambda$, then $R[x]$ is a finitely generated R-module. By Proposition 1.1.1 it follows that x is integral over R. Since x was arbitrary, we have Λ integral over R. The second statement is then a result of Proposition 1.1.2. □

Example 2.1.7 As in Example 2.1.4, letting $A = K$ and $\Lambda = R$ gets R being integral over K as expected. □

We now have properties I and II and look at the third. From here we let Λ be an R-order in A and M be a full R-lattice in A. We defined a prime ideal of an integral domain in Chapter 1 and here we define one in an order, referencing Reiner [1, p.190] and Swan & Evans [2, p.89]. Since R is commutative, ideals in R are both left and right ideals. In Λ however, left ideals are not necessarily right ideals. So at first we will stick only to two-sided ideals (unless stated otherwise) and look at one-sided ideals later in the chapter. When prime ideals are spoken about it will be clear what kind of prime is being referred to, to avoid confusion. We assume that all ideals of Λ are full R-lattices in A.

Definition 2.1.8 A *prime ideal* of Λ is a proper two-sided ideal $B \subset \Lambda$ that is a full R-lattice in A such that for two-sided ideals I, J in Λ, if $IJ \subseteq B$ then $I \subseteq B$ or $J \subseteq B$.

The multiplication of ideals here is the same as in (1.2) and note that the last part of the definition is equivalent to saying for two-sided ideals I, J in Λ/B,

$$\text{if } IJ = 0 \text{ then } I = 0 \text{ or } J = 0, \tag{2.1}$$

reminiscent of an (possibly integral) domain.

Example 2.1.9 Every maximal two-sided ideal M of Λ is a prime ideal of Λ. By maximal, it is meant that M is a proper ideal of Λ that is not contained in any other proper ideal of Λ. □

Proof. This example requires some proof, so we sill do it here. Let M be a two-sided maximal ideal of Λ. Two two-sided ideals I, J of Λ that have $IJ \subseteq M$, fall into the following cases:

1. If one of the ideals contains M, say $I \supseteq M$, then either $I = M$ or $I = \Lambda$. The first shows $I \subseteq M$ and the second shows $J = \Lambda J = IJ \subseteq M$, so M is prime.
2. Otherwise let $I \not\supseteq M$ and $J \not\supseteq M$. Since $IJ \subseteq M$, $(I + M)J \subseteq M$. But $I + M \supseteq M$ and so $I + M$ falls into the first case. So if $I + M = M$, then $I \subseteq M$ and if $I + M = \Lambda$, then $J \subseteq M$ and again M is prime.

□

This example can also be proven a different way by using (2.1) and the following Lemma, which will be proven for ideals in general, not just two-sided ideals.

Lemma 2.1.10

a) *For an ideal M of Λ, N/M is an ideal of Λ/M if and only if N is an ideal of Λ containing M.*

b) *Λ/M is simple if and only if M is a maximal two-sided ideal in Λ.*

Proof. Consider left ideals and let M be one such of Λ. To Prove part a, first let N/M be an ideal of Λ/M. Note that $N \supseteq M$ since otherwise N/M is not well defined. Let $n \in N$ and $x \in \Lambda$, so $n + M \in N/M$ and $x + M \in \Lambda/M$. Then $(x + M)(n + M) = xn + xM + Mn + MM \in N/M$. But $Mn + xM + MM \subseteq M$, so $xn \in N$ must follow. Thus N is an ideal of Λ containing M. Now to prove the converse, let N be an ideal of Λ containing M and show N/M is an ideal in Λ/M. Again let $n \in N$ and $x \in \Lambda$, so $n + M \in N/M$ and $x + M \in \Lambda/M$. Then $(x + M)(n + M) = xn + xM + Mn + MM \in N/M$ with $Mn + xM + MM \subseteq M$ and $xn \in N$. Thus $(x + M)(n + M) \in N/M$ and N/M is an ideal in Λ/M, proving part a.

The proof of part b follows from part a since if Λ/M is simple then there are no proper two-sided ideals of Λ strictly containing M, so M is a maximal two-sided ideal. Conversely, if M is a maximal two-sided ideal, then the only two-sided ideals of Λ/M are M/M and Λ/M, that is, the trivial ones. So Λ/M has no non-trivial two-sided ideals and is thus simple, proving part b. □

This proves the Example 2.1.9 trivially since simple algebras have no non-trivial ideals, but it also gives us an important application of the next Theorem, which can be found in Reiner [1, p.190-191] and also in Swan & Evans [2, p.95-96]. The latter, however, uses a different proof to the one given here, instead using the Chinese

Remainder Theorem. But first we must state a standard theorem from the theory of modules, which can be found in Curtis & Reiner [4, §25].

Theorem 2.1.11 *The ring R is semisimple as a left R-module if and only if every left R-module is semisimple. Every semisimple ring R can be decomposed into a sum of minimal left ideals Re_i of R where e_i are orthogonal idempotents. That is $e_i^2 = e_i$ and for $i \neq j, e_i e_j = 0$.*

Theorem 2.1.12 *If B is a prime ideal of Λ then*

- **a)** *$P = B \cap R$ is a prime ideal of R. Moreover $B \to P$ gives a surjective relation between the prime ideals of Λ and the prime ideals of R.*
- **b)** *Λ/B is a finite dimensional simple algebra over the field R/P.*

Proof. Let B be a prime ideal of Λ, $P = B \cap R$ and $\Delta = \Lambda/B$. We prove part a first as we need R/P to be a field. Since B is a full R-lattice in A, by the argument before Definition 2.1.5 there is an $r \in R$ such that $r \in B$, so P is not empty. Also, since $B \subset \Lambda, 1 \notin B$ and hence $1 \notin P$, implying $P \subset R$. Now P is an ideal of R since $RP = R(B \cap R) = (RB) \cap R = B \cap R = P$ since B is a full R-lattice in A. Now if $\alpha, \beta \in R$ satisfy $\alpha\beta \in P$, then $(\alpha\Lambda)(\beta\Lambda) \subseteq B$. So $\alpha\Lambda \subseteq B$ or $\beta\Lambda \subseteq B$, implying that $\alpha \in P$ or $\beta \in P$ and P is a prime ideal of R.

Now let P be a prime ideal of R. Since Λ is an R-lattice and $P \subset R$, $P\Lambda$ is a proper two-sided ideal of Λ and so is contained in some maximal ideal B in Λ. Now $P \subseteq B \cap R \subset R$ and since both P and $B \cap R$ are prime in R it follows that $P = B \cap R$ proving the surjectivity of the relation $B \to P = B \cap R$ and thus part a.

For the proof of part b, R/P is a field so is trivially artinian as a ring. Now Λ is a finitely generated R-module, so Λ/B must be a finitely generated R/P-module and is thus artinian, as well as a finite dimensional R/P-algebra since $R/P \subseteq Z(\Lambda/B)$. Suppose first that Λ/B is semisimple. Now two separate simple components Δ_i and Δ_j of Λ have $\Delta_i\Delta_j \subseteq \Delta_i \cap \Delta_j = 0$, so by (2.1) one of them must be zero. Thus there can only be one simple component and Λ/B is actually simple. So it suffices to show that Λ/B is semisimple.

Suppose that there is a two-sided ideal $X \supset B$ such that $X/B \supset 0$ is minimal. Such an X exists since Λ/B is artinitan. Now $(X/B)^2 \subseteq X/B$, so since X/B is minimal either $(X/B)^2 = 0$ or $(X/B)^2 = X/B$. The first implies $X/B = 0$ via (2.1) so it must be the latter. But in that case, it must be also that $X^2 = X$ in Λ. Let $X = Rx_1 + \cdots Rx_n$ for some $x_i \in A$, $n \in \mathbb{Z}^+$ and no x_i equal to a sum $\sum_{j\neq i} r_j x_j$ or product $\sum_{j\neq i} r_j x_j \sum_{k\neq i} r_k x_k$ involving the other terms of X since if any x_i is, removing that x_i will not affect the ideal X (so we have a 'minimal' amount of x_i). Then $X^2 = Rx_1^2 + \cdots Rx_n x^1 + Rx_1x_2 + \cdots Rx_n x_2 + \cdots + Rx_1 x_n + \cdots Rx_n^2$ and thus since each x_i cannot be expressed in terms of the other elements of X, they must all be idempotent (that is $x_i^2 = x_i$). But as $X^2 = X$ then $x_i x_j = 0$ (and so they are orthogonal idempotents) must also be the case for all $i \neq j$. By Theorem 2.1.2.1 this means X is actually semisimple. Doing similarly for another minimal two-sided ideal $Y \supset X$ it follows that Y is a direct product of ideals generated by idempotents of A that cancel each other so is semisimple as well. Thus every two-sided ideal in Λ/B is semisimple, so by Theorem 2.1.2.1Λ/B is semisimple itself. □

This result is quite remarkable and provides a correspondence between the original definition of a prime ideal in Chapter 1 and the abstracted definition here in Chapter 2. Just as importantly, the succeeding corollary of Theorem 2.1.12 allows us to get the last property we require of Λ, property III.

Corollary 2.1.13 *The prime ideals of Λ are maximal two-sided ideals in Λ.*

Proof. For a prime ideal B of Λ, Theorem 2.1.12 says that Λ/B is simple and Lemma 2.1.10 then implies B is maximal. □

This gives us the equivalence of maximal ideals and prime ideals of Λ, so the order Λ satisfies the three properties held by a Dedekind domain and we are off to a good start. Though this is very nice, it still does not mean too much to us about the factorisation of ideals in this order without actually looking at the ideals of Λ. So next we will discuss the ideals of Λ, with references for the next section Reiner [1, p.108-111,192,204-205], Swan & Evans [2, p.83-84,88] and Bass [3, p.152-156].

2.2 Maximal Orders

In the last section, we went briefly into the ideals of Λ to show property III of a Dedekind domain held for Λ. Left ideals M in Λ all have $\Lambda \cdot M = M$ and are assumed to be full R-lattices in A, but what if we consider such M not contained in Λ. We did this in Chapter 1 with the definition of a fractional ideal and saw that each fractional ideal could be factorised uniquely as a product of prime ideals and inverses of prime ideals and also that the set of these fractional ideals was an abelian group generated by the prime ideals and their inverses. So we search for the Irishman the the end of the rainbow and again we do it here with a similar definition with the aim of seeing if a similar factorisation occurs in an R-order Λ.

Definition 2.2.1 For the R-order Λ, a non-zero full R-lattice in A that is a finitely generated Λ-module is called a *fractional Λ-ideal* of A.

Example 2.2.2 As in Example 2.1.7, letting $A = K$ and $\Lambda = R$ gets the fractional Λ-ideals here and the fractional R-ideals in Chapter 1 coinciding. □

We will denote fractional Λ-ideals as we did in Chapter 1 by using L, J and so on and as usual the product of two fractional Λ-ideals is another fractional Λ-ideal given by (1.2). We do however drop the word fractional for ease and just refer to them as ideals of Λ, assuming that they are in fact fractional Λ-ideals of A. If a full R-lattice is a two-sided ideal of Λ, it is then just an ideal of Λ that is a two-sided Λ-module. We will soon only look at two-sided ideals and then look at a more general case later, but for now this two-sidedness is not assumed. First note the useful fact via the argument given before Definition 2.1.5, that for every ideal L of Λ, the intersection $R \cap L \neq 0$.

The ideals considered from Definition 2.1.8 until this point are all fractional Λ-ideals since they are full R-lattices in A and are contained in Λ, an R-lattice itself, implying they are finitely generated Λ-modules. To emphasize when an ideal L of Λ is contained in Λ we call L an *integral ideal of* Λ. As usual, L is a *maximal integral ideal of* Λ when it is contained properly in no other integral ideal of Λ.

So now we have generalised some of the definitions of Chapter 1, in particular Dedekind domains and the corresponding fractional ideals. But is this all that is

required to generalise the results for Dedekind domains from Chapter 1? At the moment there are no restrictions on the order we choose. In particular, as we will soon find to be important, we have not established any sort of maximality for orders, which leads to the following.

Definition 2.2.3 An R-order that is not properly contained in any other R-order is called a *maximal* R-order.

Example 2.2.4 As in Example 2.2.2 (and as mentioned just before the previous definition), if $A = K$ and $\Lambda = R$ then Λ is a maximal R-order in A since adding any element $q \in K - R$ to R gets an infinitely generated R-module, so $R+q$ cannot be an R-order. □

Example 2.2.5 As in Example 2.1.2, letting $A = M_n(K)$ and $\Lambda = M_n(R)$, then Λ was an R-order in A. Actually, λ is a maximal R-order in A since if you add another matrix $M \in A - \Lambda$ to Λ with, say, an element $q \in K - R$ in the lk^th position. Since Λ is generated by the matrices $\{(1)_{ij} \mid 0 \leq i, j \leq n\}$ where $(1)_{ij}$ is the matrix with a 1 in the ij^{th} position and zero's elsewhere, the element q can be placed in any position. Thus any multiple of q can be placed in any position and similarly to Example 2.2.4 $\Lambda + M$ is not an R-order. □

Example 2.2.6 As in Example 2.1.3 with $A = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$ and $\Lambda = \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}k$, then Λ was an order in A. But Λ is not a maximal order. Let $\alpha = (1+i+j+k)/2$ and $\Lambda' = \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}\alpha$. Then Λ' is a subring (since it can be written as $\Lambda' = \{(a+bi+cj+dk)/2 \mid a \equiv b \equiv c \equiv d \equiv \mod 2\}$ that contains Λ (since $k = 2\alpha - 1 - i - j$) and is generated by $1, i, j, \alpha$, so is an $\mathbb{Z}$-order of A. Further, it is maximal. This follows since Λ' is a non-commutative PID, which will be looked at in Chapter 4. So suppose there is an order $\Delta \supseteq \Lambda'$, then Δ is a Λ-ideal also. There turns out to be an $r \in R$ such that $r\Delta \subseteq \Lambda'$ (which will be an element of Δ^{-1}). So $r\Delta = \Lambda' x$ for some $x \in \Lambda$. But then $\Delta = O_l(\Delta) = O_l(r\Delta) = O_l(\Lambda' x) = O_l(\Lambda') = \Lambda'$ and Λ' is maximal. □

The reason we need maximal orders will soon become apparent as we look into the ideals of Λ. But first we must make one more extrapolation from Chapter 1. As mentioned earlier, in (1.3) we defined for a fractional R-ideal L a set of elements $x \in K$ that sent xL inside R, which happened to be the inverse of L in $\mathcal{L}_R$. This becomes a slight problem here due to the issue of non-commutativity, since for a fractional Λ-ideal L and element $x \in A$, xL is not necessarily the same as Lx. So let $S_l = \{x \in A \mid xL \subseteq \Lambda\}$ and $S_r = \{x \in A \mid Lx \subseteq \Lambda\}$. For arguments sake, let L be a two-sided ideal, so for $x \in S_l$ we have $xL \subseteq \Lambda$, so $LxL \subseteq L$ and similarly for any $x \in S_r, LxL \subseteq L$ also. So let $S = \{x \in A \mid LxL \subseteq L\}$. We have just seen that $S_l \cup S_r \subseteq S$, but are they equal? In general the answer is no.

The most we can say is that, since $LSL \subseteq L$, we have $LS \subseteq O_l(L)$ and $SL \subseteq O_r(L)$. But if Λ is a maximal order the the answer is better than yes. In this case $O_l(L) \supseteq \Lambda$, so $O_l(L) = \Lambda$ and similarly $O_r(L) = \Lambda$. So we have $S = \{x \in A \mid L \cdot x \subseteq O_l(L)\} = \{x \in A \mid L \cdot x \subseteq \Lambda\} = S_r$ and also $S = \{x \in A \mid x \cdot L \subseteq O_r(L)\} = \{x \in A \mid x \cdot L \subseteq \Lambda\} = S_l$, exactly what we want since it is the counterpart to (1.3) in a maximal order. That is, when Λ is maximal we get $S_l = S_r = S$. So we will use this

idea as motivation and define in general for an ideal L (not necessarily two-sided) of Λ

$$L^{-1} = \{x \in A \mid L \cdot x \cdot L \subseteq L\}, \tag{2.2}$$

or equivalently

$$L^{-1} = \{x \in A \mid L \cdot x \subseteq O_l(L)\} = \{x \in A \mid x \cdot L \subseteq O_r(L)\}. \tag{2.3}$$

So we then see that when Λ is maximal and L is strictly two-sided

$$L^{-1} = \{x \in A \mid L \cdot x \subseteq \Lambda\} = \{x \in A \mid x \cdot L \subseteq \Lambda\}. \tag{2.4}$$

We see that L^{-1} is clearly an R-module, but is it an ideal in Λ? Since there is an $r \in L \cap R$, then $rL^{-1} \subseteq O_l(L)$. Thus $L^{-1} \subseteq r^{-1}O_l(L)$, which shows L^{-1} is finitely generated and R-torsionfree and thus an R-lattice. If $\Lambda = O_l(L)$, then as in the discussion before Defintion 2.1.5 there is an $r \in R \cap L$ such that $rL \subseteq \Lambda$. So $L \subseteq r^{-1}\Lambda$ and $r\Lambda = (r^{-1}\Lambda) = \{x \in A \mid r^{-1}\Lambda x \subseteq \Lambda\} \subseteq \{x \in A \mid Lx \subseteq \Lambda\} = L^{-1}$. So L^{-1} is full and indeed an ideal of Λ itself. Similarly, L^{-1} is an Λ-ideal also when $\Lambda = O_r(L)$.

We know now that L^{-1} is an ideal, but what else do we know? Using (2.3) we have that $LL^{-1} \subseteq O_l(L)$, so $L(L^{-1}O_l(L)) \subseteq O_l(L)$ and thus $L^{-1}O_l(L) \subseteq L^{-1}$ which shows L^{-1} is a right $O_l(L)$-module. Similarly, $L^{-1}L \subseteq O_r(L)$ gets $(O_r(L)L^{-1})L \subseteq O_r(L)$ and $O_r(L)L^{-1} \subseteq L^{-1}$ which shows that L^{-1} is a left $O_r(L)$-module. These also give us two nice containments,

$$O_r(L^{-1}) \supseteq O_l(L) \text{ and } O_l(L^{-1}) \supseteq O_r(L). \tag{2.5}$$

This allows us to think of the ideals of an order as a set that contains inverses, but we want to see if it is a group. Before we see if this is the case, we use the preceding results to aquire the following useful facts. For the full R-lattice L, if $O_l(L)$ is maximal we have $LL^{-1} \subseteq O_l(L)$ by definition. Firstly, since L^{-1} is an ideal and the product of two ideals is another ideal, it follows that LL^{-1} is an integral ideal in $O_l(L)$. Now by (2.5) $O_r(L^{-1}) = O_l(L)$ and thus LL^{-1} is actually a two-sided integral ideal of $O_l(L)$. Secondly, if $J \subseteq L$, then $JL^{-1} \subseteq LL^{-1} \subseteq O_l(L)$ and so $L^{-1} \subseteq J^{-1}$. Reiterating this instead with $O_r(L)$ maximal gets $L^{-1}L$ a two-sided integral ideal of $O_r(L)$ and for $J \subseteq L$, yet again $L^{-1} \subseteq J^{-1}$. Repeating the second fact here, we get

$$\text{if } J \subseteq L \text{ then } L^{-1} \subseteq J^{-1}. \tag{2.6}$$

2.3 The Factorisation of Two-Sided Ideals

So now we have the necessary utensils to see if the set of these fractional ideals is a group. We do however have to revert to the case of two-sided ideals (two-sidedness will be stated explicitly), like in the previous section. But this turns out to be necessary here for our new aim, to see if the two-sided ideals of Λ can be factorised in a similar fashion to the ideals in a Dedekind domain (which may not be the case for one-sided ideals). So we continue on with this, trying to establish a group

structure along the way. The method we will use to see if these cases hold may seem familiar to the reader and can be found in Reiner [1, p.204-207], Swan & Evans [2, p.88-92] and Bass [3, p.155-159]. In fact most of the results (and proofs) in this section naturally follow from their counterparts in Chapter 1. For example, the next three results resemble Proposition 1.3.1 and Corollary 1.3.3 and are again our first stepping stones.

Lemma 2.3.1 *Every two-sided ideal of* Λ *contains a product of prime ideals of* Λ.

Proof. Note first that ideal here means two-sided ideal and any ideal $L \supseteq \Lambda$ contains any product of prime ideals of Λ, so only consider integral ideals from hereon. Let S be the set of proper ideals of Λ that do not contain a product of prime ideals. Since Λ is noetherian there must exist a maximal ideal M in S. Now M cannot be prime and any ideal properly containing M must contain a product of prime ideals. Since M is not prime, there are two two-sided ideals $L, J \subseteq \Lambda$ such that $L, J \nsubseteq M$ and $LJ \subseteq M$. But then $(L+M)(J+M) \subseteq M$ also and both $L+M, J+M \supset M$. Both $L+M$ and $J+M$ are two-sided ideals and by the maximality of M they contain a product of prime ideals. But then so does M since $(L+M)(J+M) \subseteq M$, contradicting the existence of a maximal element of the set S, and S is empty. □

Lemma 2.3.2 *Let* L *be a two-sided ideal of the maximal order* Λ. *If* $L \subset \Lambda$, *then* $L^{-1} \supset \Lambda$.

Proof. Let $L \subset \Lambda$ be a two-sided ideal of Λ. Clearly $L^{-1} \supseteq \Lambda$, so suppose $L^{-1} = \Lambda$. Then there is a maximal ideal B such that $L \subseteq B \subset \Lambda$ and let $r \in R \cap B$. Then by Lemma 2.3.1, $r\Lambda$ contains a product of prime ideals B_i

$$B \supseteq r\Lambda \supseteq B_1 B_2 \cdots B_n$$

and choose these prime ideals such that n is minimal. If $B \neq B_i$ for every i, then there are $x_i \in B_i$ where $x_i \notin B$ for every i but $x_1 x_2 \cdots x_n \in B$. So $x_1 \Lambda x_2 \lambda \cdots x_n \Lambda \subseteq B$ but $x_i \Lambda \nsubseteq B$ for every i. So since B is prime and $x_1 \Lambda \nsubseteq B$, then $x_2 \Lambda \cdots x_n \Lambda \subseteq B$ must follow. But then $x_2 \Lambda \nsubseteq B$, so again $x_3 \Lambda \cdots x_n \Lambda \subseteq B$ follows. Doing this another $n-3$ times gets either $x_{n-1}\Lambda \subseteq B$ or $x_n \Lambda \subseteq B$, which is a contradiction. Thus $B = B_j$ for some j and

$$B \supseteq r\Lambda \supseteq B_1 \cdots B_{j-1} B B_{j+1} \cdots B_n.$$

Let $D = B_1 \cdots B_{j-1}$ and $C = B_{j+1} \cdots B_n$ and see that D and C are both two-sided ideals of Λ. So $DBC \subseteq r\Lambda$ gets $r^{-1}DBC \subseteq \Lambda$ and $Dr^{-1}BCD \subseteq D$. Thus $r^{-1}BCD \subseteq O_r(D) = \Lambda$ and so by (2.6) we get $r^{-1}CD \subseteq B^{-1} \subseteq L^{-1} = \Lambda$. But this gets $CD \subseteq r\Lambda$, so $r\Lambda$ contains a product of $n-1$ prime ideals of Λ, contradicting the minimality of n. Thus $L^{-1} \neq \Lambda$. □

Theorem 2.3.3 *Let* L *be a full* R*-lattice of* A. *If* $O_l(L)$ *is a maximal order then* $L \cdot L^{-1} = O_l(L)$. *Similarly, if* $O_r(L)$ *is a maximal order then* $L^{-1} \cdot L = O_r(L)$.

Proof. Suppose $O_l(L)$ is maximal. We know that LL^{-1} is a two-sided ideal contained in $\Lambda = O_l(L)$. Then we also get $(LL^{-1})(LL^{-1})^{-1} \subseteq \Lambda$, implying $L^{-1}(LL^{-1})^{-1} \subseteq L^{-1}$ and thus $(LL^{-1})^{-1} \subseteq O_r(L^{-1})$. But by (2.5) $O_r(L^{-1}) \supseteq \Lambda$, a maximal order, so $O_r(L^{-1}) = \Lambda$ and we get $(LL^{-1})^{-1} \subseteq \Lambda$. By Lemma 2.3.2 it follows that $LL^{-1} = \Lambda$. The second part of the theorem works similarly, but will be shown to indicate the importance of this result. Again, $L^{-1}L$ is a two-sided ideal contained in $\Lambda' = O_r(L)$, so $(L^{-1}L)^{-1}(L^{-1}L) \subseteq \Lambda'$ gets $(L^{-1}L)^{-1}L^{-1} \subseteq L^{-1}$ and hence $(L^{-1}L)^{-1} \subseteq O_l(L^{-1})$. By (2.5) $O_l(L^{-1}) \supseteq \Lambda'$, a maximal order, so $O_l(L^{-1}) = \Lambda'$ and $(LL^{-1})^{-1} \subseteq \Lambda'$, where Lemma 2.3.2 again finishes off the proof. □

The preceding theorem (which was proven for a full R-lattice, not a two-sided ideal) gives us exactly what we want when Λ is a maximal order since if Λ is maximal, for every two-sided ideal L of Λ we have $O_l(L) = O_r(L) = \Lambda$. Also, see that $LL^{-1} = (L^{-1})^{-1}L^{-1}$. But does $(L^{-1})^{-1} = L$? In fact it does, not only for two-sided ideals, but also for one-sided ideals as the following result shows.

Proposition 2.3.4 *Let L be a full R-lattice in A and $\Lambda = O_l(L)$ or $O_r(L)$. If Λ is a maximal order then $(L^{-1})^{-1} = L$. Also, any ideal of Λ that contains Λ is the inverse of an integral ideal of Λ.*

Proof. Let $\Lambda = O_l(L)$ be maximal. Since L is a full R-lattice, then so is L^{-1}. So by Theorem 2.3.3 and (2.5) we have $(L^{-1})^{-1}L^{-1} = O_r(L^{-1}) = \Lambda$. So $(L^{-1})^{-1}L^{-1}L = (L^{-1})^{-1}O_r(L) = L$ and thus $(L^{-1})^{-1} \subseteq L$ since $O_r(L)$ is a unital subring. To show the reverse inclusion, by (2.5) we get

$$(L^{-1})^{-1} = O_l((L^{-1})^{-1})(L^{-1})^{-1} \supseteq O_r(L^{-1})(L^{-1})^{-1} = \Lambda(L^{-1})^{-1}.$$

This then gets

$$(L^{-1})^{-1} \supseteq LL^{-1}(L^{-1})^{-1} = LO_l(L^{-1}) \supseteq LO_r(L) = L,$$

and the reverse inclusion holds, implying $(L^{-1})^{-1} = L$. The proof is done similarly for $\Lambda = O_r(L)$.

For the second part, again let $\Lambda = O_l(L)$ be maximal but also $\Lambda \subset L$. Then $\Lambda L^{-1} \subseteq LL^{-1} = \Lambda$, so $L^{-1} \subseteq O_r(\Lambda) = \Lambda$ and L^{-1} is integral. Letting $J = L^{-1}$, we get $J^{-1} = (L^{-1})^{-1} = L$, so L is the inverse of an integral ideal of Λ. Again, the proof is done similarly for $\Lambda = O_r(L)$. □

So now we only need one more lemma to get what we want, and then our objective of ideal factorisation into prime ideals is done. Unlike the Dedekind domain case, we have the answer to our aim before before we certify that the set of fractional ideals is a group. By what we have so far, products of ideals of Λ are also ideals and this is associative since A is, Λ acts as an identity and there is an inverse for every ideal of Λ. So we have a group structure, but we want to know if it is abelian since at the moment there is no reason to see that it is. Referencing Reiner [1, p.206-207], Swan & Evans [2, p.91-92] and Bass [3, p.158], this query is also answered by the following, which achieves our aim.

Lemma 2.3.5 *Let Λ be a maximal order. Then multiplication of prime ideals of Λ is commutative and every integral two-sided ideal of Λ can be written uniquely as a product of prime ideals of Λ up to rearrangement.*

Proof. Let B an C be distinct prime ideals of Λ. Then see that $B^{-1}CB \subseteq B^{-1}\Lambda B = \Lambda$ by Theorem 2.3.3. Now $B(B^{-1}CB) = CB \subseteq C$, but since C is prime either $B \subseteq C$ or $B^{-1}CB \subseteq C$. The first implies $B = C$, which cannot be true, so we must have $B^{-1}CB \subseteq C$ and thus $CB \subseteq BC$. Doing exactly the same procedure with B and C swapped gets the reverse inclusion and thus $BC = CB$, showing multiplication of prime ideals is commutative.

Now for the second part of the proof, suppose that there are two-sided Λ-ideals that cannot be written as a product of prime ideals and let the set of these be S. Then there is a maximal two-sided ideal $M \in S$ which obviously is not prime. So there is a prime ideal B such that $M \subset B \subset \Lambda$ and hence $\Lambda \subset B^{-1} \subset M^{-1}$ and multiplying by M gets $M \subseteq MB^{-1} \subseteq \Lambda$. If $M = MB^{-1}$ then $B^{-1} \subseteq O_r(M) = \Lambda$, contradicting Lemma 2.3.2. So $M \subset MB^{-1}$ and thus MB^{-1} is a two-sided ideal strictly containing M, so by the maximality of M MB^{-1} is expressible as a product of prime ideals, say $MB^{-1} = B_1B_2\cdots B_n$ for some n. But then $M = B_1\cdots B_nB$, a product of prime ideals, contradicting the existence of a maximal element of S and thus S is empty.

Finally we must show that if two expressions of prime ideals are equal then they are the same prime ideals, but rearranged. So for prime ideals B_i and Q_j, let $B_1B_2\cdots B_k = Q_1Q_2\cdots Q_l$. since both expressions are a product of prime ideals, they are contained in some prime ideal, say B. So $B \supseteq B_1B_2\cdots B_k$ and by the proof of Lemma 2.3.2 it follows that $B = B_r$ for some r. Similarly $B \supseteq Q_1Q_2\cdots Q_l$ and so $B = Q_s$ for some s, so we get

$$\begin{aligned} B_1\cdots B_{r-1}BB_{r+1}\cdots B_k &= Q_1\cdots Q_{s-1}BQs+1\cdots Q_l \\ B^{-1}BB_1\cdots B_{r-1}B_{r+1}\cdots B_k &= B^{-1}BQ_1\cdots Q_{s-1}Bs+1\cdots Q_l \\ B_1\cdots B_{r-1}B_{r+1}\cdots B_k &= Q_1\cdots Q_{s-1}Qs+1\cdots Q_l. \end{aligned}$$

Doing this another $k-2$ times gets $k = l$ and each B_i coinciding with some Q_j. Thus the factorisation is unique up to rearrangement. □

So as in Chapter 1 we can write two-sided ideals L of Λ in the form $L = B_1^{q_1}B_2^{q_2}\cdots B_n^{q_n}$ for distinct prime ideals B_i of Λ and positive integers q_i. But how do we write L^{-1}? If we look only when Λ is maximal so $LL^{-1} = \Lambda$, then similarly to Chapter 1 yet again, we see that due to the commutativity of the prime ideals, $L^{-1} = B^{-q_1}B^{-q_2}\cdots B^{-q_n}$. This observation then leads to the major theorem of this section and our aim, the generalisation of Theorem 1.3.8. But first, we state a corollary, which yet again generalises the notion of a greatest common divisor and lowest commom multiple from Chapter 1.

Corollary 2.3.6 *The greatest common divisor of two ideals I, J of Λ, denoted $gcd(I, J)$, and lowest common multiple, denoted $lcm(I, J)$, both exist and are a product of prime ideals of Λ.*

Proof. Write $I = B_1^{e_1} \dots B_n^{e_n}$ and $J = B_1^{f_1} \dots B_n^{f_n}$ where e_i and f_j are natrural numbers as in the previous lemma. Then $\gcd(I, J) = B_1^{\min\{e_1,f_1\}} \dots B_n^{\min\{e_n,f_n\}}$ and $\operatorname{lcm}(I, J) = B_1^{\max\{e_1,f_1\}} \dots B_n^{\max\{e_n,f_n\}}$. □

Theorem 2.3.7 *Let Λ be a maximal order. Then the set of two-sided ideals of $\Lambda, \mathcal{B}_\Lambda$, is an abelian group under multiplication generated by the prime ideals of Λ with identity Λ and inverse of two-sided ideal $L \in \mathcal{B}_\Lambda$ given by L^{-1}.*

Proof. This will be proved by showing every two-sided ideal of Λ can be written as a product of prime ideals of Λ and prime inverses. Let L be an ideal of Λ. If $L \subseteq \Lambda$, then this follows straight away from Lemma 2.3.5 so let $L \nsubseteq \Lambda$. Let $r \in R \cap L^{-1}$ so $rL \subseteq \Lambda$ is integral and by Lemma 2.3.5 can be written as a product $rL = B_1 \cdots B_n$ of prime B_i ideals of Λ. But $rL = (r\Lambda)L$, so since Λ is an R-module we can also write $r\Lambda = Q_1 \cdots Q_m$ for prime ideals Q_j of Λ. Thus $L = (r\Lambda)^{-1} B_1 \cdots B_n = Q_1^{-1} \cdots Q_m^{-1} B_1 \cdots B_n$ is written as a product of prime ideals of Λ and prime inverses. This proves the theorem. □

So just like the fractional ideals of a Dedekind domain, Theorem 2.3.7 shows every two-sided fractional ideal L of a maximal order Λ can be written as $L = P_1^{e_1} P_2^{e_2} \cdots P_n^{e_n}$ for distinct prime ideals P_i of Λ and each integer $e_i \neq 0$. That is, there is unique factorisation of two-sided fractional Λ-ideals up to rearrangement.

Example 2.3.8 We look at factorising some two-sided ideals in a maximal order in the rational quaternions given in Example 2.2.6. So we let $A = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$ and $\Lambda = \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}\alpha$ where $\alpha = (1 + i + j + k)/2$. Then we saw that Λ was a maximal order (note the change in notation from that example) that could also be written as $\Lambda = \{(a + bi + cj + dk)/2 \mid a \equiv b \equiv c \equiv d \bmod 2\}$.

So what are the maximal two-sided ideals in Λ? It turns out that Λ is actually a non-commutative version of a PID (see Chapter 4), so every left ideal in Λ can be written as Λx for some $x \in \Lambda$. As it is a PID, there are 'irreducible' elements in Λ also. It turns out (which will be proven again in Chapter 4) that if $x \in \Lambda$ is irreducible, then writing $x = a + bi + cj + dk$ gets the 'norm' of x to be

$$|x| = x\overline{x} = (a + bi + cj + dk)\overline{(a - bi - cj - dk)} = a^2 + b^2 + c^2 + d^2.$$

Furthermore, it is a positive prime integer. So from this we see that all maximal ideals and maximal two-sided ideals are either of the form Λx or $\Lambda\,|x|$ for some irreducible $x \in \Lambda$. Visually,

$$\{\text{Maximal Left } \Lambda\text{ -ideals}\} \cup \{\text{Maximal Two-sided } \Lambda\text{-ideals}\}$$

$$\shortmid\cap$$

$$\{\Lambda\text{-ideals of form } \Lambda x \text{ or } \Lambda\,|x| \mid \text{ Irreducible } x \in \Lambda\}.$$

So when is an an ideal two-sided? Clearly the ones of the form $\Lambda\,|x|$ are two-sided, but are there any irreducible $x \in \Lambda$ such that Λx is a two-sided ideal? Straight away we can see that $\Lambda(1+i)$ is actually two-sided since $(1+i)(w+xi+yj+zk) = (w+xi-zj+yk)(1+i)$. So are there any more? If we let $x = a+bi+cj+dk \in \Lambda$

be irreducible, if $|x| = 2$, then two of a, b, c and d are 1 and the other two 0, so it is identical to the case $1 + i$, so lets look when $|x| > 2$.

If Λx is two-sided, then for every $z \in \Lambda$ there must be a $\lambda \in \Lambda$ such that $zx = x\lambda$, so $\lambda = \frac{xz\overline{x}}{|x|}$. That is, $\frac{x\Lambda\overline{x}}{|x|} = \Lambda$. When substituting $z = 1 + j$ and rearranging, we get that $a^2+b^2+c^2+d^2 \mid bc-ad$. When $z = i$ we get that $a^2+b^2+c^2+d^2 \mid ad+bc, ac-bd$. Thus it must be that $a^2 + b^2 + c^2 + d^2 \mid bc$ (since $a^2 + b^2 + c^2 + d^2 > 2$), implying that one of b and c is 0. But then $a^2 + b^2 + c^2 + d^2 \mid ad + bc = ad$ implying that one of a and d is 0. So without loss of generality $x = a + bi$. By substituting $z = 1 + j$ again yields $a^2 + b^2 \mid 2ab$ so one of a and b must be zero, implying a prime number is an integer squared which is obviously nonsense.

So by this long-winded argument every ideal of the form Λx for $x \in \Lambda$ irreducible with $|x| > 2$ a maximal left ideal. Thus $\Lambda\,|x|$ are the maximal two-sided Λ-ideals, that is, the prime ideals of Λ in addition to $\Lambda(1 + i)$. But what about 2Λ? Lets apply some of the theory. Since $2 = (1 + i)(1 - i)$ we have that

$$2\Lambda = \Lambda(1 + i)\Lambda(1 - i) = (\Lambda(1 + i))^2.$$

Now for any positive rational n, write $n = 2^a \frac{p_1^{e_1} \cdots p_b^{e_b}}{q_1^{f_1} \cdots q_c^{f_c}}$ where each p_l and q_l is a positive odd prime and $e_l, f_l > 0$ (assuming no common factors on numerator and denominator), but a a non-zero integer. Then we have

$$\begin{aligned} n\Lambda &= (2^a\Lambda)(p_1^{e_1}\Lambda) \cdots (p_b^{e_b}\Lambda)(q_1^{-f_1}\Lambda) \cdots (q_b^{-f_c}\Lambda) \\ &= (2\Lambda)^a(p_1\Lambda)^{e_1} \cdots (p_b\Lambda)^{e_b}(q_1\Lambda)^{-f_1} \cdots (q_b\Lambda)^{-f_c} \\ &= (\Lambda(1 + i))^{2a}(p_1\Lambda)^{e_1} \cdots (p_b\Lambda)^{e_b}(q_1\Lambda)^{-f_1} \cdots (q_b\Lambda)^{-f_c}. \end{aligned}$$

Which seems almost identical to the factorisation of the ideals in the Dedekind domain $\mathbb{Z}$ given in Example 1.3.9. Note if n is negative, then there is no difference since $n\Lambda = (-n)\Lambda$. Finally the set of two-sided ideals in Λ, $\mathcal{B}_\Lambda$, is just the set

$$\{\Lambda, \Lambda(1 + i), \Lambda\frac{1 + i}{2}\} \cup \{3\Lambda, 5\Lambda, 7\Lambda, 11\Lambda, \cdots\} \cup \{\frac{1}{3}\Lambda, \frac{1}{5}\Lambda, \frac{1}{7}\Lambda, \frac{1}{11}\Lambda, \cdots\}.$$

□

Chapter 3

Maximal Orders and Groupoids

The final result of the last chapter is indeed a nice consequence for two-sided ideals in a maximal R-order over a finite dimensional separable semisimple K-algebra, but if that is the only gold at the end of the rainbow, then the Irishman has run away with our gold and left only a few pieces behind. So we chase after him by now considering one-sided ideals to see yet again if they can be factorised uniquely in terms of 'irreducible' ideals and not only this, but we will again see if the set of all these one-sided ideals forms a group. So now we focus at both of these aims. Strictly one-sided ideals, however, cannot be a product of prime ideals since prime ideals here are by defintion two-sided. But there is still a relation between the prime ideals and maximal one-sided ideals, and this lends a hand later in the piece. So from hereon we let all ideals be one-sided unless stated otherwise.

3.1 One-Sidedness

To start ourselves off, we will actually give a conclusion to the previous chapter that shall give us some preliminary argument towards our new aim. In the previous chapter we saw that the set of two-sided ideals, $\mathcal{B}_\Lambda$, of the maximal R-order Λ in the finite dimensional separable semisimple K-algebra A was actually an abelian group generated by the prime ideals of Λ. But if we look at two different maximal orders, do we get two different groups? This query will be answered shortly, but first we need some requisites. The reference for this section is Reiner [1, p.197-199,204-205]. So similarly to last section, let R be a Dedekind domain with quotient field K, A a finite dimensional separable semisimple K-algebra and Λ an order of A.

If we take a full R-lattice M in A, then $O_l(M)$ is not necessarily the same as $O_r(M)$. In fact, if $\Lambda' = O_l(M) = O_r(M)$ then M is a two-sided fractional Λ'-ideal, so if M is strictly a one-sided Λ-ideal for some order Λ, then $O_l(M) \neq O_r(M)$. This then introduces some problems. Firstly, what is an integral ideal now in the one-sided case? Secondly, given two orders Λ and Λ', is there an Λ-ideal (also Λ'-ideal) L with $O_l(L) = \Lambda$ and $O_r(L) = \Lambda'$ and does the multiplication of ideals now change since $O_l(L) \neq O_r(L)$?

Upon considering the definition of an integral ideal: a Λ-ideal L is an *integral ideal* of Λ if $L \subseteq \Lambda$; It is seen that this is independent of left or right multiplication, so still holds in the one-sided case. Similarly, so does the definition for a *maximal integral ideal*. However, it would be nice to know when integrality holds for an order on each side. We get some insight into this if the left ideal L has $\Lambda = O_l(L)$, allowing us the following result, taken for a full R-lattice in A.

Proposition 3.1.1 *For any full R-lattice M in A, $M \subseteq O_l(M)$ if and only if $M \subseteq O_r(M)$. That is, M is an integral ideal of $O_l(M)$ if and only if M is an integral ideal of $O_r(M)$.*

Proof. Let M be a full R-lattice in A and let $M \subseteq O_l(M)$. Then $MM \subseteq O_l(M)M = M$ and it follows by definiton that $M \subseteq O_r(M)$. Similarly, if $M \subseteq O_r(M)$, then $MM \subseteq MO_r(M) = M$ and $M \subseteq O_l(M)$, completing the proof. □

Now looking at the second problem, we see that the multiplication of ideals is as usual defined by (1.2) since we are in the algebra A. But for the full R-lattices M and N, $MN = (MO_r(M))N = M(O_r(M)N)$. So it would again seem optimal that $O_r(M) = O_l(N)$. Thus for full R-lattices $M_1, M_2, \cdots, M_n$ the product $M_1M_2\cdots M_n$ is called *proper* if $O_r(M_i) = O_l(M_{i+1})$ for every $i \in \{1, 2, \cdots, n-1\}$. It is then seen that

$$O_l(M_1M_2\cdots M_n) \supseteq O_l(M_1) \text{ and } O_r(M_1M_2\cdots M_n) \supseteq O_r(M_n). \tag{3.1}$$

Now for two orders Λ and Λ', is there a full R-lattice M with $O_l(M) = \Lambda$ and $O_r(M) = \Lambda'$? The answer in general is not clear, but this is not needed. If Λ and Λ' are maximal, then the answer is yes. Let $M = \Lambda \cdot \Lambda'$, then $O_l(M) \supseteq \Lambda$, so $O_l(M) = \Lambda$ and similarly $O_r(M) = \Lambda'$, so M shows this (Note that the fact M was not constructed via a proper product is not important, since all we wanted was for M to be a left Λ-ideal and right Λ'-ideal).

Using this, we create some notation by writing a full R-lattice M as M_{ij} where we denote $\Lambda_i = O_l(M)$ and $\Lambda_j = O_r(M)$. Thus a proper product of full R-lattices can be written as $M_{12}M_{23}\cdots M_{n\,n+1}$. So for a full R lattice $M = M_{ij}$ with both Λ_i and Λ_j maximal, we still have the inverse defined by (2.2) or (2.3). But can we write M^{-1} in the same way? By (2.5), we have $O_l(M^{-1}) \supseteq O_r(M) = \Lambda_j$, so $O_l(M^{-1}) = \Lambda_j$ and similarly $O_r(M^{-1}) = \Lambda_i$. Hence inverting M swaps the orders over and we write $M^{-1} = (M_{ij})^{-1} = M_{ij}^{-1}$ seeing in fact that $O_l(M_{ij}^{-1}) = \Lambda_j$ and $O_r(M_{ij}^{-1}) = \Lambda_i$.

One final thing to note for a proper product is given in the following result.

Proposition 3.1.2 *A proper product of integral ideals is an integral ideal.*

Proof. Let $M_{12}M_{23}\cdots M_{r\,r+1}$ be a proper product of integral ideals. Then

$$\begin{aligned} M_{12}M_{23}\cdots M_{r\,r+1} &\subseteq \Lambda_2 M_{23}\cdots M_{r\,r+1} = M_{23}\cdots M_{r\,r+1} \\ &\subseteq \Lambda_3 M_{34}\cdots M_{r\,r+1} = M_{34}\cdots M_{r\,r+1} \\ &\vdots \\ &\subseteq \Lambda_r M_{r\,r+1} = M_{r\,r+1} \subseteq \Lambda_{r+1}. \end{aligned}$$

Thus $M_{12}M_{23}\cdots M_{r\,r+1}$ is an integral ideal, proving the proposition. □

Now returning to see if $\mathcal{B}_{\Lambda_i} = \mathcal{B}_{\Lambda_j}$ for two maximal orders Λ_i and Λ_j, the following result gives us the answer to our query.

Theorem 3.1.3 *Let Λ_i and Λ_j be maximal orders in A. For an ideal N_{ij} with $O_l(N_{ij}) = \Lambda_i$ and $O_r(N_{ij}) = \Lambda_j$, the map*

$$\phi_{ij} : \mathcal{B}_{\Lambda_i} \to \mathcal{B}_{\Lambda_j} : L \mapsto N_{ij}^{-1} L N_{ij}$$

is an isomorphism. Furthermore, ϕ_{ij} is independent of the choice of N_{ij}.

Proof. Let $\phi = \phi_{ij}$ and the ideal $N = N_{ij}$ have $O_l(N_{ij}) = \Lambda_i$ and $O_r(N_{ij}) = \Lambda_j$. Then for $L \in \mathcal{B}_{\Lambda_i}$, by (3.1) we have $O_l(N^{-1}LN) = O_l(N^{-1}) = \Lambda_j$ and $O_r(N^{-1}LN) = O_r(N) = \Lambda_j$, so $N^{-1}LN$ is a two-sided Λ_j ideal and $N^{-1}LN \in \mathcal{B}_{\Lambda_j}$. Also see that $\phi(\Lambda_i) = N^{-1}\Lambda_i N = N^{-1}N = \Lambda_j$, so the identity in $\mathcal{B}_{\Lambda_i}$ is sent to the identity in $\mathcal{B}_{\Lambda_j}$. Now to show ϕ is a homomorphism, let $L, L' \in \mathcal{B}_{\Lambda_i}$. Then $\phi(LL') = N^{-1}LL'N = N^{-1}L\Lambda_i L'N = N^{-1}LNN^{-1}L'N = \phi(L)\phi(L')$ and ϕ is a homomorphism.

Considering similarly the homomorphism $\phi' = \phi_{ji}$ sending $J \in \mathcal{B}_{\Lambda_j}$ to $NJN^{-1} \in \mathcal{B}_{\Lambda_i}$, then it is seen that $\phi'\phi(L) = NN^{-1}LNN^{-1} = L$ and $\phi\phi'(J) = N^{-1}NJN^{-1}N = J$. So ϕ_{ji} is the inverse of ϕ_{ij} and they are both isomorphisms. Now for another ideal $M = M_{ij}$, see that NM^{-1} and MN^{-1} are two-sided Λ_i-ideals since they both have left and right orders equal to Λ_i, so they are elements of $\mathcal{B}_{\Lambda_i}$. Thus since $\mathcal{B}_{\Lambda_i}$ is abelian, for $L \in \mathcal{B}_{\Lambda_i}$ we have

$$L = L\Lambda_i = LNN^{-1} = LN\Lambda_j N^{-1} = LNM^{-1}MN^{-1} = NM^{-1}LMN^{-1}.$$

So using this with ϕ gets

$$N^{-1}LN = \phi(L) = \phi(NM^{-1}LMN^{-1}) = N^{-1}NM^{-1}LMN^{-1}N = M^{-1}LM.$$

So ϕ is independent of the choice of $N = N_{ij}$, proving the theorem. □

So we see that $\mathcal{B}_{\Lambda_i} = \mathcal{B}_{\Lambda_j}$ does not quite hold, but $\mathcal{B}_{\Lambda_i} \cong \mathcal{B}_{\Lambda_j}$ always does, showing us that the group generated by the prime ideals of a maximal order essentially does not depend on the maximal order. This is a wonderful result and it will guide us in the right direction via two of its corollaries. However, we cannot go into these at the moment without some further theory, so they will be left to the next section. Instead, we start with some results about one-sided ideals, some of which generalise further the results of Chapter 2. As before, the reference for the remaineder of this section is Reiner [1, p.195-196,204]. This will focus on left ideals, but the right case follows equivalently.

Getting back to one of our usual and aforementioned aims of seeing if the set of the one-sided ideals is a group, we see that ideals are actually Λ-ideals for some order Λ, so they are dependent on Λ. Since a full R-lattice M in A does not necessarily have $O_l(M) = O_r(M)$, we see that for another full R-lattice N such that $O_l(M) = O_l(N)$ and $O_r(M) \neq O_r(N)$, M and N are left $O_l(M)$-ideals, but one is a right $O_r(M)$-ideal, and the other a $O_r(N)$-ideal, so considering the set of 'ideals' is not quite what we want. Now we want $O_l(M)$ or $O_r(M)$ to be maximal so that Theorem 2.3.3 gets one of the products $M \cdot M^{-1} = O_l(M)$ or $M^{-1} \cdot M = O_r(M)$ equal to a maximal order, allowing an order to be the 'identity' of the potential

group. Thus we must consider a more general case than an ideal over a maximal order and define the following.

Definition 3.1.4 A full R-lattice N_{ij} in A is called a *normal ideal* of A if Λ_i is a maximal order in A.

Example 3.1.5 For a maximal order Λ, left ideals L of Λ are normal ideals since $O_l(L) = \Lambda$. So this definition is extending the reach of all the ideals we are considering to all arbitrary maximal orders. □

It will be seen more clearly why this definition is needed later. The definition, which says the left order is maximal, however says nothing about the maximality of Λ_j, so though we want the identity to be a maximal order, this is currently only plausible for left multiplication. We soon see that for a normal ideal N_{ij} that Λ_j must also be maximal, but we first need to state the following theorem, which actually needs another standard theorem, which can be found in Jacobson [6, p.200-201].

Theorem 3.1.6 *R is a simple artinian ring if and only if R is artinian and has a simple module M such that* $\mathrm{ann}_R M = 0$.

Now the following theorem is a remarkably important result and will be used throughout the following sections. So for L and B as in the theorem below, we say that *L belongs to B*.

Theorem 3.1.7 *Let L be a maximal left integral ideal of maximal order Λ. Then*

- **a)** *There is a unique prime ideal B of Λ such that $B \subseteq L \subset \Lambda$ and $B = ann_\Lambda \Lambda/L$. Moreover $L \to B$ gives a surjective relation between the maximal integral ideals of Λ and the prime ideals of Λ.*
- **b)** *The simple ring Λ/B has simple left module Λ/L.*
- **c)** *Each prime ideal determines a maximal left integral ideal that belongs to it.*

Proof. Since L is a maximal left integral Λ-ideal we see that $B = \mathrm{ann}_\Lambda \Lambda/L = \{x \in \Lambda \mid x\Lambda \subseteq L\}$ and it is a two-sided ideal. Choose an $\alpha \in R \cap L$, then $\Lambda r = r\Lambda \subseteq L$. But $r\Lambda$ is a two-sided ideal, so write it as $Q_1^{e_1} \cdots Q_k^{e_k}$ for disctinct prime ideals Q_i and non-zero e_i. Then $\Lambda/r\Lambda \subseteq \Lambda/L$ has only a finite number of two-sided ideals and is thus artinian, so Λ/B is artinian also. Now

$$\mathrm{ann}_{\Lambda/B}\Lambda/L = \{x \in \Lambda/B \mid x(\Lambda/L) = (\Lambda/L)x = 0\} = \{x \in \Lambda/B \mid x\Lambda, \Lambda x \subseteq L\} = 0$$

(note this is 0 in Λ/B), so since Λ/L is a simple module (since L is maximal) by Theorem 3.1.6 Λ/B is simple, proving part b and implying B is actually a prime ideal of Λ. This is unique since if Q is another prime ideal contained in L, then $Q \subseteq \mathrm{ann}_\Lambda \Lambda/L$, implying $Q = B$.

Now given any prime ideal B of Λ there is a maximal left integral ideal L such that $B \subseteq L$. Since $\Lambda/(\mathrm{ann}_\Lambda \Lambda/L)$ is simple, then $B \subseteq \mathrm{ann}_\Lambda \Lambda/L$ and thus $B = \mathrm{ann}_\Lambda \Lambda/L$, proving part c and the surjectivity of the relation $L \to B$, proving part a. □

3.2 Generalising a Familiar Sight

So now we want to look at our aims of factorising ideals of maximal orders into 'irreducible' ideals and looking to see if the set of them is a group. But as we needed to do in Chapter 2 when generalising Chapter 1, we need to extend the results of Chapter 2 to one-sided ideals here, where the main reference is Reiner [1, p.201,207-209]. Also, since we introduced normal ideals and intend on using them, we had better look at them to see their properties. As we have suggested, this section is mainly for the creation of utensils to use for looking at our aims in the next section. Also, as suggested by the name of this section, Theorem 3.1.7 will have its first use in the following very familiar Lemma, which is courtesy of Reiner [1, p.207-208].

Lemma 3.2.1 *Let L be a proper integral ideal of Λ. Then $L^{-1} \supset \Lambda$.*

Proof. If L is not maximal then $L \subset J$ for some maximal integral ideal J. But then $J^{-1} \subset L^{-1}$. So it suffices to prove the lemma for L a maximal integral ideal. Let $B = \mathrm{ann}_\Lambda(\Lambda/L)$ be the prime ideal to which L belongs. Then Λ/L is a simple left module over the simple ring $\overline{\Lambda} = \Lambda/B$. Hence L is the inverse image, under the map $\Lambda \to \overline{\Lambda}$, of some maximal left ideal of Λ. Therefore we may write $L = \Lambda(1-e) + B$, where $e \in \Lambda$ is such that its image $\overline{e}$ is a primitive idempotent in $\overline{\Lambda}$. Set $N = e\Lambda + B$, a right ideal in Λ. Since $(1-e)e \in B$, it follows that $LN \subseteq B$. On the other hand, LN is a two-sided ideal of Λ containing B^2. It follows that LN is either B or B^2. If $LN = B^2$, then $Be \subseteq B^2$; multiplying by B^{-1}, we deduce that $e \in B$, which is impossible. This shows $LN = B$.

Now choose a non-zero $\alpha \in R \cap B$ and write $\alpha\Lambda$ as a product of prime ideals of Λ. Since $\alpha\Lambda \subseteq B$, one of the factors must equal B, and so we may write $\alpha\Lambda = BQ = LNQ$, where Q is some two-sided ideal of Λ. If $L^{-1} = \Lambda$, then $\alpha^{-1}NQ \subseteq L^{-1} = \Lambda$ implies $NQ \subseteq \alpha\Lambda$, which in turn implies $N\Lambda \subseteq \alpha\Lambda Q^{-1} = B$, so $N \subseteq B$. But $N = e\Lambda + B$, so the last inclusion is impossible. This shows that $L^{-1} \supset \Lambda$ and completes the proof of the lemma. □

This then allows the following fundamental result, which was alluded to earlier and allows the notion of a proper product to be more familiar and not a rare novelty.

Theorem 3.2.2 *For a full R-lattice M_{ij} in A, Λ_i is a maximal order if and only if Λ_j is a maximal order.*

Proof. Let $M = M_{ij}$ be a normal ideal. We first prove the theorem for integral ideals, but see that if $M = \Lambda_i$, then $\Lambda_j = O_r(M) = \Lambda_i$ is trivially maximal. So assume from hereon that M is proper integral. For a contradiction, suppose that M is a maximal counterexample to the theorem. That is, Λ_j is not maximal and if $L_{ik} \supset M_{ij}$ is also a left Λ_i-ideal, then Λ_k is maximal. In fact, let $L = L_{ik}$ be one such that L/M is simple, that is, L is a minimal left ideal in Λ_i/M. Let $N = L^{-1}M$, then $N \subset L^{-1}L = \Lambda_k$ since if $N = L^{-1}M = L^{-1}L = \Lambda_k$ then $M = L$, a contradiction. Also, since L/M is simple it follows that N is a maximal integral ideal in Λ_k. Now $O_l(N) \supseteq O_r(L) = \Lambda_k$, so $O_l(N) = \Lambda_k$ and $O_r(N) \supseteq O_r(M) = \Lambda_j$. But if $x \in O_r(N)$, then $Mx = L(Nx) \subseteq L(N) = M$, so $x \in O_r(M)$ and $O_r(N) = O_r(M) = \Lambda_j$ and $N = N_{kj}$.

Since Λ_j is not maximal, let $\Lambda_j' \supset \Lambda_j$ be maximal and consider the product $N\Lambda_j'N^{-1}$. It is a full R-lattice containing the unity since $N\Lambda_j'N^{-1} \supseteq NN^{-1} = \Lambda_k$, and Λ_k is a unital full R-lattice. It is also a subring of A since $N\Lambda_j'N^{-1} \cdot N\Lambda_j'N^{-1} \subseteq N\Lambda_j'\Lambda_j\Lambda_j'N^{-1} \subseteq N\Lambda_j'N^{-1}$ and hence $N\Lambda_j'N^{-1}$ is actually an order. In fact since $N\Lambda_j'N^{-1} \supseteq \Lambda_k$ it follows that $N\Lambda_j'N^{-1} = \Lambda_k$ is a maximal order.

Now from Lemma 3.2.1 we get the following chain of inclusions, $N \subseteq N\Lambda_j' \subseteq N\Lambda_j'N^{-1} = \Lambda_k$ and since N is a maximal left Λ_k-ideal it follows that either $N\Lambda_j' = N$ or $N\Lambda_j' = \Lambda_k$. If the first was true, then $\Lambda_j' \subseteq O_r(N) = \Lambda_j$ and so Λ_j is maximal, which is a contradiction and so $N\Lambda_j' = \Lambda_k$ must hold. But in this case, $\Lambda_k = N\Lambda_j'N^{-1} = \Lambda_kN^{-1}$ and thus $N^{-1} \subseteq O_r(\Lambda_k) = \Lambda_k$, contradicting Lemma 3.2.1. Therefore the maximal normal ideal M_{ij} with Λ_j not maximal is fictitious. By doing the converse similarly to above, the theorem then follows for all integral ideals.

Finally if M_{ij} is not integral, then $M \supset \Lambda_i$ and by Proposition 2.3.4 $M = J^{-1}$ for some integral Λ_i-ideal J with $\Lambda_j = O_r(J^{-1}) = O_l(J)$ and $\Lambda_i = O_l(J^{-1}) = O_r(J)$. So it suffices to show that J (which has maximal right order) has a maximal left order, which is covered by above. Again this similarly holds for a non-integral M_{ij} with Λ_j maximal and proves the theorem. □

From this we see that a normal ideal N_{ij} has both Λ_i and Λ_j maximal, so the ideals that have their left order maximal actually coincide with the ideals that have their right order maximal. At this point we mention that these normal ideals now replace the fractional ideals in a maximal order Λ in our train of thought and see that, as mentioned earlier, that all fractional Λ-ideals are actually normal ideals. So we are actually looking to see if the set of normal ideals is a group, and the previous theorem simplifies remarkably our considerations of the set of normal ideals of A since the right orders of each element of the set are also maximal, allowing us to have a maximal order as both a left and right identity element. However, there seems to be the problem that there may be several identities, since left and right multiplication by a maximal order may not acquire the same answer. Thus we might need to consider a larger set than the previous sections, and the set may actually be a *groupoid* rather than a group, where we define a groupoid as following, referencing Reiner [1, p.201]. First, a *partial function* $G \times G \to G$, is an operation that is not defined on the whole of $G \times G$. Then define the following.

Definition 3.2.3 A set G with partial function $G \times G \to G : (N_{ij}, N_{kl}) \mapsto N_{ij}N_{kl}$ is called a *groupoid* if it satisfies the following axioms. For elements $N_{ij}, N_{kl}, N_{mn} \in G$,

- There are unique $e_i, e_j \in G$, called the *left* and *right units* of N_{ij} respectively, such that the following are defined and hold true: $e_iN_{ij} = N_{ij} = N_{ij}e_j$, $e_ie_i = e_i$ and $e_je_j = e_j$.
- $N_{ij}N_{kl}$ is defined if and only if $j = k$, that is, when $e_j = e_k$.
- For any two units $e_i, e_j \in G$, there is an element $N_{ij} \in G$ with left unit e_i and right unit e_j.
- If $N_{ij}N_{kl}$ and $N_{kl}N_{mn}$ are both defined, then so are both $(N_{ij}N_{kl})N_{mn}$ and $N_{ij}(N_{kl}N_{mn})$ and they are equal.
- There is another element $N_{ij}^{-1} \in G$ with left unit e_j, right unit e_i and such that $N_{ij}N_{ij}^{-1} = e_i$ and $N_{ij}^{-1}N_{ij} = e_j$ both hold.

So a groupoid is just a generalisation of a group, with possibly multiple identity elements and a partial function replacing the binary operation. Thus a group is a specific case of a groupoid and we see that the set of fractional ideals over a Dedekind domain R, $\mathcal{L}_R$, and the set of two-sided ideals of a maximal order Λ, $\mathcal{B}_\Lambda$, are actually groupoids themselves. Now leaving the group (or groupoid) structure on the backburner, for the remainder of the section we look at some properties of normal ideals, referencing again Reiner [1, p.197-198,202,209]. We firstly prove an uniqueness property for normal ideals and then show a generalisation for divisors of an ideal given in Proposition 1.3.5.

Proposition 3.2.4 *For normal ideals N and M, the product NM is proper if and only if $NM \subset NM'$ for every normal ideal M' strictly containing M, or equivalently $NM \subset N'M$ for every normal ideal N' strictly containing N.*

Proof. Let $N = N_{12}, M = M_{34}$ and $M' = M'_{56}$. Suppose $NM \subset NM'$ for all normal ideals $M \subset M'$. Then $NM = (N\Lambda_2)M = N(\Lambda_2 M)$ implies that $M = \Lambda_2 M$ so $\Lambda_3 = \Lambda_2$ and NM is proper. Now let NM be proper and suppose that $M \subset M'$. Clearly $NM \subseteq NM'$, but if $NM = NM'$ then $M' \subseteq \Lambda_2 M' = N^{-1}NM' = N^{-1}NM = \Lambda_2 M = M$. This is a contradiction, so $NM \subset NM'$. The proof for $NM \subset N'M$ for every normal ideal N' containing N follows similarly. □

Proposition 3.2.5 *Let N and M be normal ideals.*

- **a)** *If $N = N_{12}$ and $M = M_{34}$, then $N \subseteq M$ if and only if there are integral ideals X_{13} and Y_{42} such that $N_{12} = X_{13}M_{34}Y_{42}$.*
- **b)** *If $N = N_{12}$ and $M = M_{14}$, then $N \subseteq M$ if and only if there is an integral ideal Y_{42} such that $N_{12} = M_{14}Y_{42}$.*
- **c)** *If $N = N_{12}$ and $M = M_{32}$, then $N \subseteq M$ if and only if there is an integral ideal X_{13} such that $N_{12} = X_{13}M_{32}$.*

Proof. Let N_{12} and M_{34} be normal ideals. If $N_{12} = X_{13}M_{34}Y_{42}$ for some integral ideals X_{13} and Y_{42}, then $N_{12} \subseteq \Lambda_3 M_{34}\Lambda_4 = M_{34}$ as required. Now suppose that $N = N_{12} \subseteq M_{34} = M$. We of course want $N_{12} = X_{13}M_{34}Y_{42}$ for some integral ideals $X = X_{13}$ and $Y = Y_{42}$, so we let $X = N_{12}(\Lambda_3 N_{12})^{-1}$ and $Y = M_{34}^{-1}N_{12}$. Then it is seen that X and Y are both normal ideals and have left and right orders as indicated by their subscripts. Since $N \subseteq \Lambda_3 N$, we have $(\Lambda_3 N)^{-1} \subseteq N^{-1}$ and so $X \subseteq NN^{-1} = \Lambda_1$, so X is an integral ideal. Also, $Y \subseteq M^{-1}M = \Lambda_4$ so Y is an integral ideal. Now we get

$$XMY = N(\Lambda_3 N)^{-1}MM^{-1}N = N(\Lambda_3 N)^{-1}\Lambda_3 N = N\Lambda_2 = N$$

and part a) of the the proposition is proven.

To prove b), see that when $\Lambda_3 = \Lambda_1$ in a), then $X = N_{12}(\Lambda_1 N_{12})^{-1} = \Lambda_1$ getting $N_{12} = M_{14}Y_{42}$. Similarly, if we prove a) instead by letting $X = N_{12}M_{34}^{-1}$ and $Y = (N_{12}\Lambda_4)^{-1}N_{12}$, then when $\Lambda_4 = \Lambda_2$ we get $Y = (N_{12}\Lambda_2)^{-1}N_{12} = \Lambda_2$ and so $N_{12} = X_{13}M_{32}$, proving c). □

These results then get us the following theorem, which is essential if we are to look at factorising ideals of a maximal order Λ into 'irreducible' ideals of Λ. By irreducible we of course mean maximal integral ideals in Λ, so the next theorem shows that if an ideal is maximal as a left ideal, then it must be maximal as a right ideal also and vice versa.

Theorem 3.2.6 *The normal ideal N_{12} is a maximal left integral ideal in Λ_1 if and only if it is a maximal right integral ideal in Λ_2.*

Proof. Let the normal ideal $N = N_{12}$ be a maximal left integral ideal in Λ_1. By Proposition 3.1.1, $N \subseteq \Lambda_2$. If $N = \Lambda_2$, then $\Lambda_1 = O_l(N) = \Lambda_2 = N$, contradicting N being a maximal ideal, so $N \subset \Lambda_2$. Suppose there is a normal ideal $M = M_{32}$ such that $N \subset M \subset \Lambda_2$. If $M = \Lambda_3$, then again $\Lambda_2 = O_r(M) = \Lambda_3 = M$, so $M \subset \Lambda_3$. Now by Proposition 3.2.5 we can write N as $N_{12} = X_{13}M_{32}$ for some integral ideal $X = X_{13}$. But then

$$N = X_{13}M_{32} \subseteq X_{13}\Lambda_3 = X_{13} \subseteq \Lambda_1$$

and so $X = N$ or $X = \Lambda_1$. If $X = N$, then $\Lambda_3 = \Lambda_2$ and $M = N^{-1}NM = N^{-1}N = \Lambda_2$, which is a contradiction. So $X = \Lambda_1$ must hold. But then $\Lambda_3 = O_r(X_{13}) = \Lambda_1$ and thus $N = M$. This is a contradiction and proves that N_{12} is also a maximal right integral ideal in Λ_2. Similarly, the reverse statement holds and the theorem is proven. □

So a normal ideal N_{ij} that is either a maximal left or right integral ideal can just be called a maximal integral ideal, indicating by the theorem above that it is indeed both a left and right maximal integral in its left and right orders respectively. With this theorem we now have the required tools to look at our aims of factorising ideals and seeing if the set of these ideals is a group or groupoid. So in the next section this is what we do.

3.3 The Factorisation of One-Sided Ideals

Now we use the technical results of the previous section to see if a the factorisation of ideals in Dedekind domains and for two-sided ideals in maximal orders holds similarly for one-sided ideals in maximal orders, but without the use of prime ideals, replacing them with maximal integral ideals. The main reference for this section is again Reiner [1, p.196-201]. As mentioned in the first section of this chapter, there are two important corollaries to Theorem 3.1.3. These are given here.

Corollary 3.3.1 *Let the normal ideal N_{12} be a maximal integral ideal which belongs to the prime ideals B_1 of Λ_1 and B_2 of Λ_2. Then $B_2 = \phi_{12}(B_1)$.*

Proof. First let $N = N_{12}$ and see that $\phi_{12}(B_1) = N^{-1}B_1N$. Let $J, K \in \mathcal{B}_{\Lambda_2}$ such that $JK \subseteq \phi_{12}(B_1) = N^{-1}B_1N$. Then $NJ\Lambda_2KN^{-1} = NJN^{-1}NKN^{-1} \subseteq B_1$. Since $NJN^{-1}, NKN^{-1} \in \mathcal{B}_{\Lambda_1}$ and B_1 is prime, without loss of generality we have $NJN^{-1} \subseteq B_1$. But then $J \subseteq N^{-1}B_1N$ and thus $\phi_{12}(B_1)$ is prime in Λ_2. Now since $B_1 \subseteq N$, we have $N^{-1} \subseteq B_1^{-1}$. Thus $N^{-1}B_1N \subseteq B_1^{-1}B_1N = N$ and so $N_1^{-1}B_1N$ is a prime ideal in Λ_2 containing N. By the uniqueness of B_2 it follows that $\phi_{12}(B_1) = N_1^{-1}B_1N = B_2$ and the corollary is proven. □

This corollary gives us a notion of similarity between ideals of differing orders. So with ϕ_{12} as in Corollary 3.3.1 and for an ideal L in Λ_1 we say that L and $\phi_{12}(L)$ are *similar*. So this corollary shows that each maximal integral ideal identifies a pair of similar prime ideals. However, it is not always the case that the converse holds. That is, if there are two prime ideals that are similar, there is not always a maximal integral ideal belonging to both of them. The second corollary is given here, and will be used later.

Corollary 3.3.2 *Let $N = N_{23}$ be a normal maximal integral ideal belonging to the prime ideal B_2 of Λ_2. Then for each normal ideal $M = M_{12}$, M/MN is a simple left Λ_1-module and $ann_{\Lambda_1} M/MN$ is similar to B_2.*

Proof. First we see that $\mathrm{ann}_{\Lambda_1} M/MN = \{x \in \Lambda_1 \mid xM \subseteq MN\}$. Now if there is an Λ_1-module L such that $MN \subseteq L \subseteq M$, then $N \subseteq M^{-1}L \subseteq \Lambda_2$. Thus $M^{-1}L$ is either N or Λ_2, implying $L = MN$ or $L = M$ and M/MN is a simple left Λ_1-module.

Now similarly to the proof of Theorem 3.1.7 we have

$$\begin{aligned}\mathrm{ann}_{\Lambda_1/MN}(M/MN) &= \{x \in \Lambda_1/MN \mid x(M/MN) = (M/MN)x = 0\} \\ &= \{x \in \Lambda_1/MN \mid xM, Mx \subseteq MN\} = 0\end{aligned}$$

(note this is 0 in Λ_1/MN) so $\mathrm{ann}_{\Lambda_1} M/MN$ is a prime ideal of Λ_1, say B_1. But considering $\phi_{21}(B_2) = MB_2M^{-1}$, we see that $\phi_{21}(B_2)M = MB_2 \subseteq MN$, so $\phi_{21}(B_2) \subseteq B_1$ and thus $\phi_{21}(B_2) = P_1 = \mathrm{ann}_{\Lambda_1} M/MN$, proving the corollary. □

Finally the Irishman is in sight and we can look at trying to factorise one-sided ideals. Unfortunately due to the non-commutativity of A and order Λ, if there is a factorisation then it will probably not be unique. This will be remedied somewhat in the next few results, but first we show that there is a factorisation of integral one-sided ideals into maximal integral ideals via the proper product and that the number of factors stays the same.

Lemma 3.3.3 *Let N_{ij} be a normal integral ideal, and Λ be either Λ_i or Λ_j. If the composition length of Λ/N_{ij} is s, then N_{ij} can be written as a proper product of s normal maximal integral ideals $M_1M_2\cdots M_s$ where $O_l(N) = O_l(M_1)$ and $O_r(N) = O_r(M_s)$. Also, s is uniquely determined by N_{ij} and is independent of the choice of Λ_i or Λ_j.*

Proof. For the first statement, let $\Lambda = \Lambda_i$ and see that if N is itself maximal then the result trivially holds true, so taking this as the $s = 1$ case we prove the theorem by induction on s. Suppose the result is true for $s \geq 1$ and let N be such that Λ_i/N_{ij} has composition length $s+1$. Then there is a normal maximal integral ideal $M = M_{ik}$ such that $N \subset M \subset \Lambda_i$ and M/N has composition length s. Consider

$M^{-1}N$, a left ideal of Λ_k, and suppose $\Lambda_k/M^{-1}N$ has composition length t. Then there is an unrefinable chain of t left Λ_k-modules

$$M^{-1}N = L_1 \subset L_2 \subset \cdots \subset L_t \subset \Lambda_k.$$

But then by Proposition 3.2.4

$$N = MM^{-1}N = ML_1 \subset ML_2 \subset \cdots \subset ML_t \subset M\Lambda_k = M.$$

and $t \leq s$ since M/N has composition length s. Similarly there is an unrefinable chain of s Λ_i-modules from N to Λ_k, so multiplying by M^{-1} on the left gets $s \leq t$, showing $s = t$ and so $\Lambda_k/M^{-1}N$ has composition length s also. By induction there are s normal maximal integral ideals M_l such that $M^{-1}N = M_2 \cdots M_{t+1}$ and $O_l(M^{-1}N) = O_l(M_2)$ and $O_r(M^{-1}N) = O_r(M_{s+1})$. But then $N = MM_2 \cdots M_{s+1}$ is a product of $s+1$ normal maximal integral ideals. Finally, $O_l(M) = \Lambda_i = O_l(N)$ and $O_r(M_{s+1}) = \Lambda_j = O_r(N)$. The case where $\Lambda = \Lambda_j$ holds similarly to above.

For the second statement, suppose that N can be written as a proper product of normal maximal integral ideals $N = M_1M_2 \cdots M_s$ with $O_l(N) = O_l(M_1)$ and $O_r(N) = O_r(M_s)$. Then by Proposition 3.2.4

$$N = M_1 \cdots M_s \subset M_1 \cdots M_{s-1} \subset \cdots \subset M_1M_2 \subset M_1 \subset \Lambda_i \tag{3.2}$$

and

$$N = M_1 \cdots M_s \subset M_2 \cdots M_s \subset \cdots \subset M_{s-1}M_s \subset M_s \subset \Lambda_j \tag{3.3}$$

are unrefinable chains of s left Λ_i and Λ_j-modules. So the composition length of Λ/N_{ij} for either $\Lambda = \Lambda_i$ or Λ_j is s and by the Jordan-Holder Theorem all decompositions are isomorphic to either (3.2) or (3.3), thus s is uniquely determined by N_{ij}, proving the lemma. □

So this shows that every normal integral ideal can be expressed as a product of maximal normal integral ideals. But what about ideals that are not integral? First consider what the inverse of an integral ideal would look like. If we write an normal integral ideal L_{ij} out as a proper product as in Lemma 3.3.3 $L = L_{ij} = M_1 \cdots M_s$. Then if we let $L^{-1} = M_s^{-1} \cdots M_1^{-1}$, which is still a proper product, then everything works out as we want it to. For instance,

$$\begin{aligned} LL^{-1} &= M_1 \cdots M_s M_s^{-1} \cdots M_1^{-1} \\ &= M_1 \cdots M_{s-1} O_l(M_s) M_{s-1}^{-1} \cdots M_1^{-1} \\ &\quad \vdots \\ &= M_1 O_l(M_2) M_1^{-1} \\ &= O_l(M_1) = \Lambda_i \end{aligned}$$

and similarly, $L^{-1}L = \Lambda_j$. We can now use this new found property to achieve our aim, catch the Irishman and get a factorisation of every normal ideal in A.

Theorem 3.3.4 *Every normal ideal in A can be written as a proper product of maximal normal integral ideals and inverses of maximal normal integral ideals in A.*

Proof. Let $N = N_{ij}$ be a normal ideal in A. If $N \subseteq \Lambda_i$, then the result follows immediately from Lemma 3.3.3, so let $N \nsubseteq \Lambda_i$. Since there is an $r \in R \cap N^{-1}$, then $rN \subseteq \Lambda_i$ and by Lemma 3.3.3 write $rN = M_1 \cdots M_s$ for maximal normal integral ideals M_l. But since $rN = (r\Lambda_i)N$, then we can write $N = (r\Lambda_i)^{-1}rN$. Since $r\Lambda_i \subseteq \Lambda_i$ and it is two-sided, we can write $r\Lambda_i = L_1 \cdots L_k$ for maximal normal integral ideals L_l with $O_l(L_1) = O_r(L_k) = \Lambda_i$. But then $(r\Lambda_i)^{-1} = L_k^{-1} \cdots L_1^{-1}$, so we can write $N = L_k^{-1} \cdots L_1^{-1} M_1 \cdots M_s$. That is, N is a proper product of maximal normal integral ideals and inverses of maximal normal integral ideals. □

So we have caught the Irishman, taken his gold and found that every normal ideal in A can be factorised, even though it is not unique. We have thus achieved one of our aims, but what of the second? What can we say about the set of all these normal ideals in A? The answer is given in the following theorem, which follows from the preceding theorem.

Theorem 3.3.5 *The set of all normal ideals in A is a groupoid when endowed with the proper product. It is called the Brandt Groupoid assosciated with A and is generated by the maximal normal integral ideals of A and the inverses of maximal normal integral ideals of A, where the proper product is defined.*

As expected, the units of the Brandt Groupoid associated with A are the maximal orders in A and the inverse of the normal ideal L_{ij} in A with left unit Λ_i and right unit Λ_j is L_{ij}^{-1}. But returning to the corollaries stated earleier, how do they help us? Though the factorisation of a normal ideal of A is not unique, the factors do however belong to the same prime ideals, up to similarity.

Corollary 3.3.6 *Let N_{ij} be a normal integral ideal written as a proper product $N = M_1 M_2 \cdots M_s$ of normal maximal integral ideals M_l, where s is the composition length of Λ_i/N_{ij}. Then the prime ideals that each M_l belongs to is uniquely determined by N_{ij} up to similarity and order of occurrence.*

Proof. Relabeling the product as $N = N_{1\,s+1} = M_{12}M_{23} \cdots M_{s\,s+1}$, consider the series of composition factors of Λ_1/N

$$\Lambda_1/M_{12}, M_{12}/M_{12}M_{23}, \cdots, M_{12} \cdots M_{s-1\,s}/M_{12} \cdots M_{s\,s+1}.$$

If we let B_i be a prime ideal of Λ_i such that $M_{i\,i+1}$ belongs to it, then by Corollary 3.3.2 we get that

$$\begin{aligned}
\phi_{11}(B_1) &= B_1 = \mathrm{ann}_{\Lambda_1}(\Lambda_1/M_{12}), \\
\phi_{21}(B_2) &= \mathrm{ann}_{\Lambda_1}(M_{12}/M_{12}M_{23}), \\
&\vdots \\
\phi_{s1}(B_s) &= \mathrm{ann}_{\Lambda_1}(M_{12} \cdots M_{s-1\,s}/M_{12} \cdots M_{s\,s+1}).
\end{aligned}$$

So the prime ideals B_i are determined up to similarity and order of occurence by L, proving the corollary. □

But what else can we say about the factorisation, or at least a factorisation? It turns out that we can specify the composition factors of Λ_1/L_{1s} in advance, as the following theorem states. For the proof of this theorem, see Reiner [1, p.200-201].

Theorem 3.3.7 *Let $L = L_{ij}$ be a normal ideal with the composition lenngth of Λ_i/L equal to s and let $\{S_1, S_2, \cdots, S_s\}$ be the composition factors of the Λ_i-module Λ_i/L, arranged in any preassigned order. Then there is a factorisation $L = M_1 \cdots M_s$ of L into a product of maximal normal integral ideals M_k such that the factor modules*

$$\Lambda_i/M_1, M_1/M_1M_2, \cdots, M_1 \cdots M_{s-1}/L$$

are precisely $S_1, S_2, \cdots, S_k$, in that order.

To conclude our look on the factorisation of ideals we will look at, yet again, the rational quaternions and state a theorem, which is included more for aesthetic reasons rather than for usefulness.

Theorem 3.3.8 *Let Λ be a maximal order in A. There are surjective relations from the maximal integral ideals of Λ to the prime ideals of Λ and from the prime ideals of Λ to the prime ideals of R,*

$$\{\text{Maximal Integral Ideals of } \Lambda\} \to \{\text{Prime Ideals of } \Lambda\} \to \{\text{Prime Ideals of } R\}.$$

Proof. These are given by Theorems 2.1.12 and 3.1.7. □

Example 3.3.9 We look at factorising some one-sided ideals in a maximal order in the rational quaternions. So let $A = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$ and $\Lambda = \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}\alpha$ where $\alpha = (1+i+j+k)/2$. Then we saw that Λ was a maximal order that could also be written as $\Lambda = \{(a+bi+cj+dk)/2 \mid a \equiv b \equiv c \equiv d \bmod 2\}$. By Example 2.3.8, we also saw that all the maximal left ideals of Λ are of the form Λx for irreducible $x \in \Lambda$. This was because Λ was a non-commutative version of a PID.

Since Λ is a PID, it follows that every element can be expressed as a product of irreducible elements (for more on this see Chapter 4). So let $z \in \Lambda$ be a non-zero non-unit element. Then we can write $z = x_1x_2 \cdots x_n$ for some n irreducible elements $x_i \in \Lambda$. Thus we can write $\Lambda z = \Lambda x_1 \cdots x_n$. But Λx is a maximal left ideal, so relabeling $\Lambda = \Delta_1$, suppose $\Delta_1 x_1$ has right order Δ_2. Then Δ_2 must also be a

maximal order and $x_1\Delta_2$ must be a maximal right ideal since $\Delta_1 x_1$ is a maximal left ideal. So x_1 is irreducible in Δ_2 and hence we can write

$$\Lambda z = (\Delta_1 x_1 \Delta_2) x_2 \cdots x_n = (\Delta_1 x_1)(\Delta_2 x_2) x_3 \cdots x_n.$$

Similarly we can say $\Delta_2 x_2$ has right order Δ_3 and x_2 is irreducible in Δ_3 so

$$\Lambda z = (\Delta_1 x_1)(\Delta_2 x_2)(\Delta_3 x_3) x_4 \cdots x_n.$$

Continuing this we then express the left ideal Λz as a product of normal maximal integral ideals

$$\Lambda z = (\Delta_1 x_1)(\Delta_2 x_2) \cdots (\Delta_n x_n).$$

The Brandt Groupoid associated with A is however hard to find, as *all* maximal orders in A must be considered. So it will just be left as a thought. □

Chapter 4

Factorisation...of Elements

So far we have just considered factorising ideals of specific rings into a product of 'irreducibles', or maximal ideals, in that ring. But what about factorising elements in the ring? More specifically, we pose the question: Do the results we have found about Dedekind domains and orders allow us to uniquely factorise elements? Before we answer this question, we recall some definitions at the beginning of Chapter 1 as they will be used here.

4.1 Background

Let R be an integral domain and $u(R)$ be the multiplicative subgroup of units of R. An element $p \in R$ is called *prime* if for two elements $a, b \in R$, if $p \mid ab$ then either $p \mid a$ or $p \mid b$. A non-zero non-unit element $r \in R$ is *irreducible* if for every factorisation $r = ab$ for $a, b \in R$, either $a \in u(R)$ or $b \in u(R)$ (see that both a and b can not be in $u(R)$ since this forces $r \in u(R)$). Call R an *Unique Factorisation Domain* (or UFD) when for every element $r \in R$, if there are two factorisations $r = a_1 \cdots a_n = b_1 \cdots b_m$ with $a_i, b_j \in R$ for all i and j, then $n = m$ and $a_i = u_i b_{\pi(i)}$ for some permutation $\pi \in \{1, \cdots, n\}$ and unit $u_i \in u(R)$ for every i. That is, we can swap around the b_i's and multiply them by units to get $a_1 \cdots a_n$. Call R a *Principal Ideal Domain* (or PID) if every ideal of R is a principal ideal.

If for the integral domain R there is a function $\nu : R - 0 \to \mathbb{N}$ such that the following are satisfied

- For $a \in R$ and $b \in R - 0$ there are $q, r \in R$ such that $a = bq + r$ and $\nu(r) < \nu(b)$,
- For $a, b \in R - 0$, $\nu(a) \leq \nu(ab)$,

then R is called an *Euclidean domain*. The definition shows us that every Euclidean domain has an 'Euclidean algorithm' and this can be used to find the greatest common divisor of two elements of R. From this it we can establish the following result.

Theorem 4.1.1 *Every Euclidan domain R with function ν is a PID and all proper ideals I in R are generated by an element $x \in I$ with $\nu(x) = \min_{i \in I}\{\nu(i)\}$. That is, $\nu(x)$ is minimal.*

Proof. Let I be a proper ideal of R. Since $\nu : R \to \mathbb{N}$, then there is a minimal value of $\{\nu(x) \mid x \in I\}$, and let $z \in I$ be one such that $\nu(z)$ is minimal. Then $I \supseteq \langle z \rangle$. But for any $x \in I$ there are $q, r \in R$ such that $x = zq + r$ and $\nu(r) < \nu(z)$. The minimality of $\nu(z)$ implies $\nu(r) = 0$ and so $r = 0$ since R is an integral domain. So $x \in \langle z \rangle$ and thus $I = \langle z \rangle$. This also proves that R is a PID. □

There are the following examples of Euclidean domains.

Example 4.1.2 All fields F are Euclidean domains via the function $\nu(x) = 1$ for all $x \in F - 0$. But not all Euclidean domains are fields, as the Euclidean domain $\mathbb{Z}$ with function $\nu(x) = |x|$ indicates. □

Now returning to the question: Do the results we have found about Dedekind domains and orders allow us to uniquely factorise elements in that Dedekind domain? The answer is actually very easy to get, as we have already seen in Example 1.2.4 and as repeated below.

Example 4.1.3 The ring $R = \mathbb{Z}[\sqrt{-5}]$ is a Dedekind domain, but $6 = (1+\sqrt{-5})(1-\sqrt{-5}) = 2.3$, so R is not a UFD. □

So the answer is no. But it turns out that it is pretty close. The number 6 above was expressed twice above and it turns out that

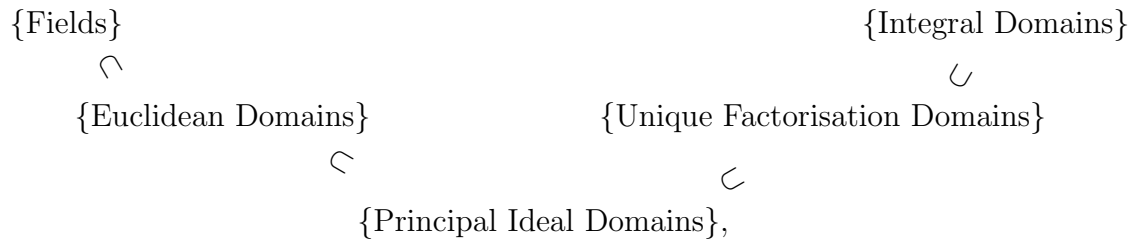
$$6 = (1 + \sqrt{-5})(1 - \sqrt{-5}) = 2.3$$

are the only expressions that equal it except for rearrangement or multiplication by units in $\mathbb{Z}[\sqrt{-5}]$. So even though $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, it seems to be within arms reach of being one.

Of course when we say 'factorise elements', we are being very informal when this is in regard to orders since they are not necessarily commutative. So First we consider if it is the case in Dedekind domains and then move onto orders later, redefining some factorisation theory notions with non-commutativity allowed. Note though that this chapter is more a summary of some nice results rather than an in depth account, so many theorems will not have proofs provided, but references to proofs will be given.

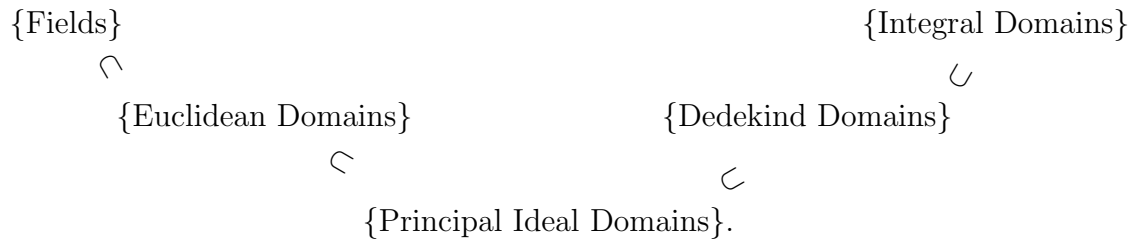
4.2 Factorisation, the Class Group and The Class Number

Back in Chapter 1 we showed every PID was a Dedekind domain via Proposition 1.2.3. So if we look at the following chain of inclusions,



do {Dedekind domains} fit in somewhere? As we see by Example 4.1.3, if it does then it is in between UFD's and integral domains. However, the next proposition shows us that it does not fit into the chain since not all UFD's are Dedekind domains, but if we replace UFD's with Dedekind domaains in the chain above then

the resulting chain of inclusions below still holds.



Theorem 4.2.1 *A Dedekind domain is a UFD if and only if it is a PID.*

Proof. See Sivaramakrishnan [10, p.406]. □

But how do we actually know when a Dedekind domain R is a PID? To do this we must consider classes of set of Fractional ideals $\mathcal{L}_R$ of R, a Dedekind domain from hereon. These classes are defined as following. Two fractional ideals $L, J \in \mathcal{L}_R$ are elements of the same ideal class if $L = xJ$ for some $x \in K$ and this ideal class can then be denoted $[L]$ (or equivalently $[J]$). See here that $L \cong J$ as modules via $L \to J : a \mapsto xa$ with inverse $xa \mapsto x^{-1}xa = a$, so these ideal classes can be thought of as isomorphism classes. Ideal classes can be multiplied together to get another ideal class by $[L][J] = [LJ]$. This works since if $xL \in [L]$ and $yJ \in [J]$ for some $x, y \in K$, then $xLyJ = (xy)LJ \in [LJ]$. Thus we have proven the following.

Definition 4.2.2 The ideal classes of $\mathcal{L}_R$ form an abelian multiplicative group with identity element $[R]$ called the *ideal class group* of R. This is denoted by $\mathcal{H}_R$.

Now if a fractional ideal of R is generated by one element it is, as expected, called a *principal* fractional ideal. So by Theorem 1.3.8 if R is a PID, then the ideal class group of R is actually just $\{[R]\}$, an one element set. Conversely, if the ideal class group of R is just $\{[R]\}$ then R is obviously a PID, so R is a PID if and only if its ideal class group is just the class $[R]$. But what if it is not just $[R]$, that is, if R is not a PID? If this is the case, we can use $\mathcal{H}_R$ as a 'measure' of how far R is from being one, if it happens to be finite. So when $\mathcal{H}_R$ is indeed finite, we let $h(R) = |\mathcal{H}_R|$ (and say $h(R)$ is infinite otherwise) and call this number the *class number* of R. From the preceding discussion we see that R is a PID if and only if $h(R) = 1$ and thus we get the following corollary.

Corollary 4.2.3 *A Dedekind domain is a UFD if and only if the class number of R is* 1.

Proof. By above a Dedekind domain is a PID if and only if $h(R) = 1$. Theorem 4.2.1 then proves the corollary. □

This corollary says that in the case of a Dedekind domain R with class number 1, there is actually more than just a unique factorisation of ideals, there is a unique factorisation of elements. So when looking at R, one can use the ideals of R instead of the elements of R, and vice versa. Class group are discussed more in delpth see Reiner [1, p.48], Jacobson [6, 643-649], Janusz [7, p.16-18], Stewart & Tall [8, §9] and Sivaramakrishnan [10, p.436-441].

4.3 Finiteness of The Class Number of the Ring of Integers

Algebraic number theory is, obviously, a large part of number theory and uses vast amounts of algebraic techniques. Here we take a certain type of Dedekind domain that is important to algebraic number theory and see that its class number is finite. More detailed accounts of what will be discussed here can be found in Janusz [7, p.52-65], Stewart & Tall [8, §9], Samuel [9, p.57-59] and Sivaramakrishnan [10, p.436-441]. This certain type of ring is the ring of integers of a number field and was a motivating example for the definition of a Dedekind domain. For this section we ignore the use of K and A in the rest of the document as the quotient field of R and K-algebra, since they will soon be redefined.

To start with, we must take a specific case of integrality over a ring R. A complex number α is an *algebraic number* if there is a polynomial $p(X) \in \mathbb{Q}[X]$ such that $p(\alpha) = 0$. The ring $\mathbb{Q}$ could actually be replaced by $\mathbb{Z}$ since multiplying the polynomial by all the denominators of the coefficients gets a polynomial with integer coefficients. The set of all algebraic numbers is denoted by A and is actually a subfield of $\mathbb{C}$.

Corollary 4.3.1 *A complex number α is an algebraic number if and only if $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is finite.*

Proof. If $\alpha \in A$, then α is a root of a polynomial $p(X) \in \mathbb{Q}[X]$ of say degree n. Making this polynomial monic in $\mathbb{Q}[X]$ and multiplying by α we get $\alpha p(\alpha) = 0$, so α^{n+1} is expressible as a polynomial of α of degree n, thus $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is finite. Conversely if $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is finite of say degree n, then $1, \alpha, \cdots, \alpha^n$ are linearly dependent over $\mathbb{Q}$, so $\alpha \in A$. □

Theorem 4.3.2 *The set of all algebraic numbers A is a subfield of $\mathbb{C}$.*

Proof. For $\alpha, \beta \in A$

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}],$$

which is finite. Since $\alpha \pm \beta, \alpha\beta, \alpha/\beta \in \mathbb{Q}(\alpha, \beta)$, then each is an algebraic number by Corollary 4.3.1. □

It turns out that $[A : \mathbb{Q}]$ is not finite, so to make life easier we define the following. A subfield $K \subset \mathbb{C}$ is an *algebraic number field* if $[K : \mathbb{Q}]$ is finite. Now obviously $K \subset A$ and since $[K : \mathbb{Q}]$ is finite we may write $K = \mathbb{Q}(\alpha_1, \cdots, \alpha_n)$ for some algebraic numbers α_i, but can we say anything else? Since K is a field it is an Euclidean domain and there is a gcd algorithm applicable in K. So letting $\alpha = \gcd(\alpha_1, \cdots, \alpha_n)$ we see that $K = \mathbb{Q}(\alpha)$, showing us every algebraic number field is just a finite extension of $\mathbb{Q}$ generated by one algebraic number.

Given the algebraic numbers A, lets look at a subset of them as follows. For an $\alpha \in A$, it was mentioned that there is a polynomial in $\mathbb{Z}[X]$ with α as a root. But this polynomial may not be monic. We then call $\beta \in A$ an *algebraic integer* if there is a monic polynomial $p(X) \in \mathbb{Z}[X]$ such that $p(\beta) = 0$ and let the set of all algebraic integers be denoted by B. This subset actually turns out to be a subring, as the following shows.

Theorem 4.3.3 *The set of algebraic integers, B, is a subring of the algebraic numbers A.*

Proof. An algebraic integer is just an element $x \in \mathbb{C}$ that is integral over $\mathbb{Z}$. So by Proposition 1.1.1 x is an algebraic integer if and only if $\mathbb{Z}[x]$ is a finitely generated $\mathbb{Z}$-module. Now for two algebraic integers $x, y \in \mathbb{C}$, $\mathbb{Z}[x]$ and $\mathbb{Z}[y]$ are finitely generated $\mathbb{Z}$-modules. Thus $\mathbb{Z}[x, y]$ must be a finitely generated $\mathbb{Z}$-module also. But since $x + y, xy \in \mathbb{Z}[x, y]$, then they are also algebraic integers and thus B is a subring of A. □

This set is useful to us in the following way. Let K be an algebraic number field and let $\mathcal{O}_K = K \cap B$. Then $\mathcal{O}_K$ is called the *ring of integers* of K. As the definition suggests, $\mathcal{O}_K$ is a subring of K since both K and B are rings. But $\mathcal{O}_K$ turns out to be more than just a ring, it is a Dedekind domain. If this sounds familiar, it may be because it was mentioned back in Example 1.2.5 where it was defined as the integral closure of $\mathbb{Z}$ in a finite extension $K/\mathbb{Q}$, $\mathcal{O}_K = \overline{\mathbb{Z}}^K$. Both of these definitions create the same ring, which the following theorem shows.

Theorem 4.3.4 *For an algebraic number field K, the ring of integers $\mathcal{O}_K$ of K is a Dedekind domain.*

Proof. See Sivaramakrishnan [10, p.409-410]. □

Now we look at the ideas discussed in the previous section and consider the ideal class group of $\mathcal{O}_K$. Is the ideal class group of $\mathcal{O}_K$ finite? The answer to this is given in the following theorem, which will not be proved here. One proof, though not straightforward, uses fairly straightforward ideas from geometry, lattices and Minkowski's theorem to get bounds on the 'norm' of an ideal using the discriminant of a matrix formed by a basis of K over $\mathbb{Q}$ and monomorphisms $K \to \mathbb{C}$ (this proof can be found in the references listed at the beginning of this section). But the previous seemingly complicated sentence is remedied by the next seemingly simple one.

Theorem 4.3.5 *The ideal class group of $\mathcal{O}_K$ is finite.*

Theorem 4.3.5 shows that the class group of K is finite, but how small is it? There is one nice property associated with $\mathcal{O}_K$ that can be found without too much work. It is not always the case that $\mathcal{O}_K$ is a PID, so an ideal is not always generated by one element. However, if it is not generated by one element then it is generated by two.

Theorem 4.3.6 *Every ideal in $\mathcal{O}_K$ is generated by at most two elements.*

Proof. See Stewart & Tall [8, p.131-132] and Sivaramakrishnan [10, p.426-427]. □

As we mentioned before, one proof of Theorem 4.3.5 uses geometric ideas. But there is another way using the definitions in Chapter's 2 and 3 and algebraic techniques. A benefit of this more complicated theorem is that it is a generalised version of the finiteness theorem above.

4.4 Factorisation in an Order and the Jordan-Zassenhaus Theorem

Theorem 4.3.5 shows us that the ideal class number is finite for algebraic number fields. But the proof that was mentioned uses ideas different from Chapter's 2 and 3. If similar ideas to Chapter's 2 and 3 are to be used, it turns out that a more general theorem can be established, named the *Jordan-Zassenhaus Theorem*. So to start, as usual we let A be a separable semisimple K-algebra and Λ an R-order in A.

As shown earlier, the set of fractional ideals of a Dedekind domain R can be partitioned into ideal classes, with the set of all these classes called the ideal class group. This was done by saying two R-ideals L and J are in the same class when $L = xJ$ for some $x \in K$. But this says that $L \cong J$ as R-modules. So we use the latter to classify ideals of Λ for R-orders Λ in A. Two fractional left Λ-ideals L and J are elements of the same *ideal class* if $L \cong J$ as Λ-modules. But each isomorphism between L and J can be extended to an automorphism $KL \cong KJ$ from A to A. Hence the ideal class containing L, denoted $[L]$ as previously, is actually $[L] = \{Lx \mid x \in u(A)\}$. When $A = K$ this coincides with the ideal classes looked at previously, but in that case the multiplication by a unit can be on either side of the ideal. In an arbitrary A, however, the multiplication must be on the right to keep Lx a left Λ-ideal. The set of these ideal classes, denoted $\mathcal{H}_\Lambda$, is not always a group due to this right multiplcation by an element in $u(A)$, but as we did with Dedekind domains, we only want to see if it is finite. So if it is finite we let $h(\Lambda) = |\mathcal{H}_\Lambda|$ (and say $h(\Lambda)$ infinite otherwise) and call this the *ideal class number* of Λ. See Reiner [1, p.224] for more details on this.

In a Dedekind domain R, when we had $h(R) = 1$ then we knew R was a PID. So can we get something similar for an order in an algebra? First we need to clear up some concepts, for instance, a PID is by definition commutative so it will need to be generalised (see Sivaramakrishnan [10, p.244-246]). The concept of an integral domain being a PID, however, can be easily defined for a non-commutative ring, so until we revert back to orders, let Λ be any arbitrary non-commutative ring and not necessarily an order (or a domain). The ring Λ is a left *principal ideal ring* (or left PIR) if every left integral ideal in Λ is generated by one element. That is, every left integral ideal I of Λ can be written as $I = \Lambda x$ for some $x \in \Lambda$. Similarly the definition holds for a ring being a right PIR and if the ring is both a left and right PIR, then it is just called a PIR.

A *unit* in the ring Λ is an element $u \in \Lambda$ such that there exists a $v \in \Lambda$ where $uv = 1$. Note this also implies that $vu = 1$ since $vuv = v$, so $v(vu - 1) = 0$ and multiplying by u on the left gets $vu = 1$. The set of units of Λ, $u(\Lambda)$, is then a subgroup of Λ under multiplication. The element $x \in \Lambda$ is then called *irreducible* if every factorisation $x = ab$ for $a, b \in \Lambda$, has either $a \in u(\Lambda)$ or $b \in u(\Lambda)$. This gets the following result on irreducibility.

Proposition 4.4.1 *For the ring Λ, $x \in \Lambda$ is irreducible if and only if Λx is a maximal left integral ideal.*

Proof. Suppose that $x \in \Lambda$ is not irreducible, then $x = ab$ for some non-zero non-units $a, b \in \Lambda$. Then $\Lambda x = \Lambda ab \subset \Lambda b$, showing one implication. If Λx is not

maximal, then $\Lambda x \subset \Lambda b$ for some non-zero non-unit $b \in \Lambda$. So $x = ab$ for some non-zero non-unit $a \in \Lambda$ and x is not irreducible, proving the proposition. $\square$

Note the result could equally have been proven for $x\Lambda$ a maximal right ideal, but we continue on our path. Two elements $x, y \in \Lambda$ are called left *associates* if $x = yu$ for some $u \in u(\Lambda)$ and right associates if $x = uy$. This is equivalent to saying that x and y are left associates when $\Lambda/\Lambda x \cong \Lambda/\Lambda y$ and similarly right associates when $\Lambda/x\Lambda \cong \Lambda/y\Lambda$. It turns out that when defining a UFD, or in this case a UFR, this is the more useful way. When looking at a factorisation of an element $x \in \Lambda$ into irreducibles of Λ, say $x = p_1 \cdots p_n$ with p_i irreducible for every i, then there is the following chain of inclusions

$$\Lambda x = \Lambda p_1 \dots p_n \subseteq \Lambda p_2 \cdots p_n \subseteq \cdots \subseteq \Lambda p_n \subseteq \Lambda. \tag{4.1}$$

Each subset, though, must be strict since $\Lambda p_{i-1} \cdots p_n / \Lambda p_i \cdots p_n \cong \Lambda/\Lambda p_i$ and Λp_i is a maximal left ideal in Λ. Thus we get the following series of non-zero quotient rings

$$\Lambda/\Lambda p_1, \Lambda/\Lambda p_2, \cdots, \Lambda/\Lambda p_n. \tag{4.2}$$

This allows us to define the following. A ring Λ is an *unique factorisation ring* (or UFR) if for every non-zero element $x \in \Lambda$, there is a factorisation of x as a product of irreducible elements of Λ and if there are two factorisations $x = p_1 \cdots p_n = q_1 \cdots q_m$ for irreducibles $p_i, q_j \in \Lambda$, then $n = m$ and their series of ideals as in (4.2) are isomorphic in the sense that $\Lambda/\Lambda p_i \cong \Lambda/\Lambda q_{\pi(i)}$ for some $\pi \in \text{perm}\{1, \cdots, n\}$ for every i. That is, p_i is a left associate of $q_{\pi(i)}$.

Finally, call a set W well-ordered if there is a partial order (a reflexive, anti-symmetric and transitive binary relation) on W such that every subset of W has a minimal element according to this order. We will call the ring Λ a left *Euclidean ring* if there is a function $\nu : \Lambda \to W$ where W is a well-ordered set (usually $\mathbb{N}$) such that for $x \in \Lambda$ and $y \in \Lambda - 0$, there exist $q, r \in \Lambda$ such that $x = qy + r$ and $\nu(r) < \nu(b)$ (see Brungs [11]). Similarly Λ is a right Euclidean ring if the same conditions hold but the multiplication by q is on the right, so $x = yq + r$. These definitions do not always coincide, so if a ring is both a left and right Eudlcidean ring, then it is just called an Euclidean ring. Similarly to the commutative case, a division ring D is an Euclidean ring with $\nu(x) = 1$ for all $x \in D - 0$ and Theorems 1.1.5 and 4.1.1 hold, allowing a similar chain of inclusions

$$\begin{array}{ccccc} \{\text{Division Rings}\} & & & & \{\text{Unique Factorisation Rings}\} \\ & \cap & & & \cup \\ & \{\text{Euclidean Rings}\} & \subset & \{\text{Principal Ideal Rings}\} & \end{array}$$

Returning to looking at R-orders in the algebra A, we let Λ again be an R-order in A. So what can we now say when $h(\Lambda) = 1$? When $h(R) = 1$ for the Dedekind domain R then R was a PID, when replacing R with Λ, we get the following Theorem.

Theorem 4.4.2 *The R-order Λ in A is a left PIR if and only if $h(\Lambda) = 1$ for left Λ-ideals.*

Proof. If Λ has $h(\Lambda) = 1$ for left ideals, then since Λ is a left Λ-ideal itself, the only class of left Λ-ideals in $\mathcal{H}_\Lambda$ must be $[\Lambda] = \{\Lambda u \mid u \in u(A)\}$, showing Λ is a left PIR. Secondly, if Λ is a left PIR then take an integral ideal of the form Λx for some $x \in \Lambda$. By the Brandt Groupoid associated with A, there is an inverse to Λx, say L, which will be a right Λ-ideal. But $\Lambda x L = \Lambda$, so there are some $y \in \Lambda$ and $z \in L$ such that $yxz = 1$, implying that $yx \in u(A)$. Similary, there is a $u \in u(A)$ such that $uyx = 1$, implying that $x \in u(A)$ and thus Λx is in the class $[\Lambda]$, so $h(\Lambda) = 1$ for left ideals. □

That is, if the ideal class number for left ideals is 1, then there is a factorisation of elements of Λ and not just ideals, just like the Dedekind domain scenario, even though it is non-commutative (see Reiner [1, p.230]). If $h(\Lambda) = 1$, then for an element $x \in \Lambda$, find a chain as in (4.1)

$$\Lambda x = \Lambda x_1 \subset \Lambda x_2 \subset \cdots \subset \Lambda x_n = \Lambda$$

where $x = x_1$ and $x_n = 1$. Then as in Proposition 4.4.1 we can write $x_i = z_i x_{i+1}$ for some non-zero non-unit $z_i \in \Lambda$. Since $\Lambda x_{i+1}/\Lambda x_i \cong \Lambda/\Lambda z_i$ then Λz_i is a maximal ideal and by Proposition 4.4.1 z_i is irreducible. But then $x = z_1 z_2 \cdots z_{n-1} x_n = z_1 z_2 \cdots z_{n-1}$, a product of irreducible elements of Λ. Furthermore, we get a series of quotient rings as in (4.2)

$$\Lambda/\Lambda u_1, \Lambda/\Lambda u_2, \cdots, \Lambda/\Lambda u_n.$$

So when looking at Λ, one can use the ideals of Λ instead of the elements of Λ, and vice versa, as in the Dedekind domain case. Moreover, Corollary 3.3.6 gives us the prime ideals that each Λz_i belongs to up to similarity and occurrence. So each z_i is associated with some prime ideal of Λ and these prime ideals can actually be uniquely determined by the element x up to similarity and occurence.

More generally, however, seeing just when $h(\Lambda)$ is finite is not always easy. So when can we say it is finite? We have seen previously that when A is an algebraic number field K and Λ the ring of integers $\mathcal{O}_K$, then $h(\mathcal{O}_K)$ is finite. This was in fact Theorem 4.3.5 and it was stated that a standard proof of this uses ideas from geometry and lattices and is relatively unrelated to the material here. However there is another proof that uses Chapter's 2 and 3 that actually establishes a more general result. The proof (including Lemma 4.4.3), which is somewhat more complicated than the standard proof of Theorem 4.3.5, will not be given, but it can be found in Reiner [1, p.224-229], Swan & Evans [2, p.43-54], Curtis & Reiner [4, §79] and Bass [3, p.539-548].

To state the theorem we first need to give some definitions. Recall that a full R-lattice M in A is an R-lattice such that $KM = A$ and fractional ideals in the R-order Λ are full R-lattices in A that are finitely generated Λ-modules. The R-rank of a R-lattice M in Λ is then defined as $\text{rank}_R M = \dim_K(KM)$. For the R-order Λ, the *Jordan-Zassenhaus condition*, denoted $JZ(\Lambda)$ holds true if for each $t \in \mathbb{Z}^+$, the number of Λ-isomorphism classes of left R-lattices of R-rank at most t is finite.

Note that if $t = [A : K]$ then clearly the Λ-isomorphism classes of rank t are the left ideal classes of Λ and so if $JZ(\Lambda)$ holds then indeed $h(\Lambda)$ is finite. In fact, we get the following lemma, which is proven when A is a skewfield over K, which is defined as follows. The division ring D is called a *skewfield* over K if $K \subseteq Z(D)$ and $[D : K]$ is finite, where $Z(D)$ is the centre of D.

Lemma 4.4.3 *Let Λ be an R-order in a skewfield D over K. Then $JZ(\Lambda)$ holds if and only if $h(\Lambda)$ is finite.*

This lemma then gives us the generalisation of Theorem 4.3.5 by its use in the following theorem, the Jordan-Zassenhaus Theorem, which uses the following definition, allowing it to expand its reach. A *function field* is a finite extension of the field $k(X)$ of rational functions in an indeterminate X over a finite field k. The theorem will just be stated without any discussion, but note that it can also be proven for certain S-orders where S is a commutative ring, not necessarily a Dedekind domain, see Reiner [1, p.228-229].

Theorem 4.4.4 *Let R be a Dedekind domain such that K is an algebraic number field or function field. Then for each R-order Λ in a semisimple K-algebra A, $JZ(\Lambda)$ holds true.*

4.5 Quaternions and a Sum of Four Squares

Now we look at a specific example. We have seen already in Examples 3.3.9, 2.3.8 and 2.2.6 that the rational quaternions give good examples of all the theoretical aspects discussed up to Chapter 3. But certain facts about them have been used so that they can be such a good example. So here we will show these facts, with the rational quaternions yet again providing a good example of the theory looked at in this chapter so far. For this section, refer to Reiner [1, p.229-231]. As a historical note, Hamilton was the inventor of the quaternions in 1843. He intended to extend the complex number to three dimensions over $\mathbb{R}$ for applied purposes, but it took him several years to find out that this would not work. He realised that he needed four dimensions and that commutativity does not hold, which prompted the start of non-commutative ring theory, a pure topic.

So from hereon let $A = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$ be the separable semisimple $\mathbb{Q}$-algebra of rational quaternions, recalling that it is an extension of the rational complex numbers $\mathbb{Q} \oplus \mathbb{Q}i$ where elements j and k act as roots of -1 and multiplication follows the rule $i^2 = j^2 = k^2 = ijk = -1$. Let $\Delta = \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}k$ and $\Lambda = \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}\alpha$ where $\alpha = (1 + i + j + k)/2$. We have seen that Δ is an order and Λ is a maximal order containing Δ. Also, it is easy to show that we can rewrite Λ as

$$\Lambda = \{(a + bi + cj + dk)/2 \mid a, b, c, d \in \mathbb{Z} \text{ such that } a \equiv b \equiv c \equiv d \bmod 2\}. \quad (4.3)$$

Also, it is easy to see that for every $x \in \Lambda$ there is a $u \in u(\Lambda)$ such that $ux \in \Delta$. This will actually become a key point in our dicussions.

We will show that the class number of Λ is finite. In fact, we will see it is 1 and do this by proving A is an Euclidean ring. To do this we first define the function

$\nu : A \to \mathbb{Q}^+ \cup \{0\} : x \mapsto |x|$, where $|\cdot|$ acts as a 'norm' like in the complex numbers. That is, if $x = a + bi + cj + dk \in A$, then

$$\begin{aligned}\nu(x) = |x| &= (a + bi + cj + dk)\overline{(a + bi + cj + dk)} \\ &= (a + bi + cj + dk)(a - bi - cj - dk) \\ &= a^2 + b^2 + c^2 + d^2.\end{aligned}$$

The function ν is also multiplicative since for $x, y \in \Lambda$

$$\nu(xy) = xy\overline{xy} = xy\overline{xy} = y\nu(x)\overline{y} = \nu(x)y\overline{y} = \nu(x)\nu(y).$$

But what if we restrict ν to Λ? Let $x = (a + bi + cj + dk)/2 \in \Lambda$ as in (4.3), then $v(x) = \frac{1}{4}(a^2 + b^2 + c^2 + d^2)$. If the integers a, b, c and d are all congruent to 0 mod 2, then their squares are congruent to 0 mod 4 and $\nu(x) \in \mathbb{N}$. Otherwise if they are congruent to 1 mod 2, then for some integers a', b', c' and d' we can write

$$\begin{aligned}\frac{1}{4}(a^2 + b^2 + c^2 + d^2) &= \frac{1}{4}((2a' + 1)^2 + (2b' + 1)^2 + (2c' + 1)^2 + (2d' + 1)^2) \\ &= a'^2 + a' + b'^2 + b' + c'^2 + c' + d'^2 + d' + 1.\end{aligned}$$

Getting $v(x) \in \mathbb{N}$ yet again. Thus ν restricted to Λ always achieves a non-negative integer, so we can say $\nu : \Lambda \to \mathbb{N}$ instead.

This allows us to look at the units of Λ, since if $u \in u(\Lambda)$, then there is a $v \in u(\Lambda)$ such that $uv = 1$. So $1 = \nu(uv) = \nu(u)\nu(v)$ and since $\nu(u)$ and $\nu(v)$ must be non-negative integers, they are both 1. Thus the group of units of Λ is exactly the following 24 elements

$$u(\Lambda) = \{u \in \Lambda \mid \nu(u) = 1\} = \{\pm 1, \pm i, \pm j, \pm k, (\pm 1 \pm i \pm j \pm k)/2\}.$$

Now we have all we need to know about ν to show that Λ is an Euclidean ring, and thus $h(\Lambda) = 1$. So we do it here.

Theorem 4.5.1 *The maximal order $\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}\alpha$ in $\mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$ where $\alpha = (1 + i + j + k)/2$ is an Euclidean ring*

Proof. Let $\Lambda = \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}\alpha$ and $A = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$ as usual an let $x \in \Lambda$ and $y \in \Lambda - 0$. Since A is a division ring, we look at the quotient xy^{-1} in A. Since Λ is a full $\mathbb{Z}$-lattice in A there is some $q \in \Lambda$ and $r' \in A$ such that $xy^{-1} = q + r'$ where $r' = a_1 + a_2 i + a_3 j + a_4 k$ with $|a_i| \leq \frac{1}{2}$ for every i. In fact, if $|a_i| = \frac{1}{2}$ for every i then $r' \in \Lambda$ and we can write $xy^{-1} = q' + r''$ where $q' = q + r' \in \Lambda$ and $r'' = 0$. Thus at least one of the a_i has $a_i < \frac{1}{2}$ and $v(r) < \frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = 1$. So multiplying by y we get $x = qy + r$ where $r = r'y$. But both x and qy are in Λ, so $r \in \Lambda$ also. Finally, since $\nu(r) = \nu(r'y) = \nu(r')\nu(y) < \nu(y)$ it follows that Λ is a left Euclidean ring and by considering $y^{-1}x$ it follows that Λ is actually an Euclidean ring. □

Furthermore, since A is a domain, Λ is actually a non-commutative version of a Euclidean domain and thus a principal ideal domain. So the following corollary is now trivial.

Corollary 4.5.2 *The maximal order $\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}\alpha$ in $\mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$ where $\alpha = (1 + i + j + k)/2$ has $h(\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}\alpha) = 1$.*

Proof. Theorem 4.5.1 says that $\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}\alpha$ is an Euclidean ring, so it is a PIR and thus $h(\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}\alpha) = 1$. □

But now that we know Λ is a PID, every integral ideal of Λ can be written as Λx for some $x \in \Lambda$. This unexpectedly allows us to prove a nice number theoretic result (with inspiration from Reiner [1, p.215]) that was first proved in 1770 by Lagrange (obviously via a different proof), the *Four Squares Theorem*. The theorem also allows us to relate the theory of orders back to arithmetic, and even non-commutative arithmetic, even though it seems to be an abstract algebraic being. This theorem is given here.

Theorem 4.5.3 *Every natural number can be expressed as a sum of four squares.*

Proof. Let $p \in \mathbb{N}$ be prime. Then there exists an irreducible $x \in \Lambda$ so that Λx is a maximal integral ideal such that $\Lambda p \subseteq \Lambda x$. Now intersecting these ideal with $\mathbb{Z}$ we get $p\mathbb{Z} = \mathbb{Z} \cap \Lambda p \subseteq \mathbb{Z} \cap \Lambda x$. Now if $z \in \mathbb{Z} \cap \Lambda x$, then $z \in \mathbb{Z}$ and $z \in \Lambda x$, so $z = yx$ for some $y \in \Lambda$. But then $y\,|x| = yx\overline{x} = z\overline{x}$ and thus $y = \frac{z}{|x|}\overline{x}$. Thus $\mathbb{Z} \cap \Lambda x \subseteq \mathbb{Z}\,|x|$, so $\mathbb{Z}p \subseteq \mathbb{Z}\,|x|$. But p is prime, so either $|x| = 1$ or $|x| = p$. The first implies that x is a unit, contradicting that x is irreducible, so it must be that $|x| = p$. But now there is a $u \in u(\Lambda)$ such that $ux \in \Delta$, so $ux = a + bi + cj + dk$ for some $a, b, c, d \in \mathbb{Z}$. So we have

$$p = |x| = |u|\,|x| = |ux| = a^2 + b^2 + c^2 + d^2.$$

That is, each prime is a sum of four squares. Finally, if $n = p_1^{e_1} \cdots p_k^{e_k} \in \mathbb{N}$ where each p_i is prime and $e_i > 0$, then there are irreducible $x_i \in \Lambda$ such that $p_i = |x_i|$ for every i. So by the multiplicative property of $|\cdot|$ and for some unit $v \in u(\Lambda)$ such that $vx_1^{e_1} \cdots x_k^{e_k} = a + bi + cj + dk \in \Delta$, we have

$$\begin{aligned} n = p_1^{e_1} \cdots p_k^{e_k} &= |x_1|^{e_1} \cdots |x_k|^{e_k} = |x_1^{e_1}| \cdots |x_k^{e_k}| \\ &= |x_1^{e_1} \cdots x_k^{e_k}| = |v|\,|x_1^{e_1} \cdots x_k^{e_k}| = |vx_1^{e_1} \cdots x_k^{e_k}| \\ &= a^2 + b^2 + c^2 + d^2, \end{aligned}$$

proving the theorem. □

To conclude we state a similar result to the Four Squares Theorem above, which can be shown via a similar method. Also, it seems plausible that the changes in the setup between this next theorem and the previous theorem can be continued for other values. However Ramanujan [12, §20] and Kloosterman [13] show that there are at most 54 different combinations of $w, x, y, z \in \mathbb{Z}^+$ such that expressions of the form $wa^2 + xb^2 + yc^2 + zd^2$ can express every natural number. From this the only values that make Λ an order, up to rearrangement, are $w = 1, x = 3, y = 1$ and $z = 3$.

Theorem 4.5.4 *Let* $A = \mathbb{Q} \oplus \mathbb{Q}\sqrt{3}i \oplus \mathbb{Q}j \oplus \mathbb{Q}\sqrt{3}k$ *and* $\Lambda = \mathbb{Z} \oplus \mathbb{Z}\sqrt{3}i \oplus \mathbb{Z}j \oplus \mathbb{Z}\alpha$ *where* $\alpha = (a + \sqrt{3}i + j + \sqrt{3}k)/2$. *Then* Λ *is a non-commutative Euclidean domain and every natural number can be written in the form* $a^2 + 3b^2 + c^2 + 3d^2$ *for integers* a, b, c *and* d.

References

[1] Reiner, I., Maximal Orders, Academic Press, 1975.

[2] Swan, R. and Evans, E,. K-Theory of Finite Groups and Orders, Springer-Verlag, 1970.

[3] Bass, H., Algebraic K-Theory, W.A. Benjamin, Inc , 1968.

[4] Curtis, C. and Reiner, I., Representation Theory of Finite Groups and Associative Algebras, John Wiley & Sons, Inc, 1962.

[5] Jacobson, N., Basic Algebra I, Dover Publications, Inc, 2009.

[6] Jacobson, N., Basic Algebra II, Dover Publications, Inc, 2009.

[7] Janusz, G., Algebraic Number Fields, Academic Press, 1973.

[8] Stewart, I. and Tall, D., Algebraic Number Theory, Chapman & Hall, 1987.

[9] Samuel, P., Silberger, A., Algebraic Theory of Numbers, Dover Publications, Inc, 2008.

[10] Sivaramakrishnan, R., Certain Number-Theoretic Episodes in Algebra, Chapman & Hall, 2007.

[11] Brungs, H., Left Euclidean rings, Pacific Journal of Mathematics, Volume 45, No. 1, 1973.

[12] Ramanujan, S., Collected papers of Srinivasa Ramanujan, Cambridge University Press, 1927.

[13] Kloosterman, H., On the Representation of Numbers in the Form $ax^2 + by^2 + cz^2 + dt^2$, London Mathematical Society, 1926.

[14] The MacTutor History of Mathematics archive, http://www-history.mcs.st-and.ac.uk/, School of Mathematics and Statistics, University of St Andrews, Scotland, October 2009.