David Husert

Similarity of Integer Matrices

Dissertation

Paderborn 2017

Based on a true story

Abstract

The thesis at hand deals with the question of how to decide whether two integer matrices are similar. To answer it, a module-theoretic approach will be pursued. In the first part of the work, a one-to-one correspondence will be established between classes of semisimple matrices and classes of modules which are defined over certain orders. For two such modules it then has to be examined whether they are isomorphic. In general, this problem can be solved by a principal ideal test, where the ideal concerned is a right ideal of a typically noncommutative matrix order. In a first approximation, the problem will be considered over a maximal order. It is well known how to conduct the test in this situation. Upon a positive outcome, it can be decided in a finite number of steps whether the original ideal is principal. Under suitable conditions, this can be done by methods for finite abelian groups. For instance, the ideal needs to be coprime to the conductor of an extension of matrix orders. Among other things, it will be shown how to ensure that this condition is satisfied.

The second part will deal with nilpotent elements of matrix orders. While the close connection between matrices and modules will not persist in this case, it will suffice to consider a finite family of modules to decide similarity. Combining the methods of both parts will result in a complete algorithm.

—

Die vorliegende Arbeit beschäftigt sich mit der Frage, wie sich entscheiden lässt, ob zwei ganzzahlige Matrizen ähnlich sind. Zu ihrer Beantwortung wird ein modultheoretischer Ansatz verfolgt. Im ersten Teil der Arbeit wird eine Eins-zu-eins-Korrespondenz hergeleitet zwischen Klassen halbeinfacher Matrizen und Klassen von Moduln, die über bestimmten Ordnungen definiert sind. Für zwei solcher Moduln muss anschließend untersucht werden, ob sie isomorph sind. Im Allgemeinen lässt sich dieses Problem mithilfe eines Hauptidealtests lösen, wobei das betreffende Ideal ein Rechtsideal einer typischerweise nicht kommutativen Matrizenordnung ist. Als erste Annäherung wird das Problem über einer Maximalordnung betrachtet. Es ist wohlbekannt, wie sich der Test in dieser Situation durchführen lässt. Bei einem positiven Ergebnis kann in endlich vielen Schritten entschieden werden, ob ursprünglich ein Hauptideal vorlag. Unter geeigneten Bedingungen kann dies mit Methoden für endliche abelsche Gruppen bewerkstelligt werden. Beispielsweise muss das Ideal koprim sein zum Führer einer Erweiterung von Matrizenordnungen. Unter anderem wird gezeigt werden, wie sich gewährleisten lässt, dass diese Bedingung erfüllt ist.

Der zweite Teil wird sich mit nilpotenten Elementen von Matrizenordnungen beschäftigen. Zwar wird die enge Verbindung zwischen Matrizen und Moduln in diesem Fall nicht bestehen bleiben, doch wird es genügen, eine endliche Familie von Moduln zu betrachten, um Ähnlichkeit nachzuweisen. Die Kombination der Methoden aus beiden Teilen wird einen vollständigen Algorithmus liefern.

Contents

Introduction

The subject of the thesis at hand is the following problem: Given two integer matrices A and B, decide whether they are similar, that is, decide whether there is an invertible integer matrix C such that

$$CA = BC.$$

Our goal is to develop a method by which this question can be answered and which computes a suitable matrix C if the outcome is positive.

Over a field, such as the rational numbers, it is well known that this problem can be solved by comparing the (generalized) Jordan normal forms of both matrices. For integer matrices, however, this is not true. In fact, there are matrices with the same Jordan normal form over the rational numbers which are not similar over the integers. To make things worse, it is uncertain how a canonical form for similarity classes of integer matrices could look like; it seems rather unlikely that such a form exists.

It was first shown, independently, by Sarkisjan (1979) and Grunewald (1980) that the problem of integral similarity is decidable in computational terms. In their papers, they actually proposed working algorithms, albeit not very efficient ones. Some more work was done on matrices of the size 2×2 and 3×3, for instance by Applegate and Onishi (1981, 1982) and Behn and Van der Merwe (2002), but their methods strongly rely on the given size and cannot be generalized readily to higher dimensions. As a matter of fact, new difficulties arise when dealing with matrices of the size 4×4.

At the time of writing, there is no implemented algorithm which solves our problem in general. In the computer algebra system Magma, there is a function called `IsGLZConjugate` which works for matrices of finite order and matrices of the size 2×2. The first case is based on results by Opgenorth, Plesken and Schulz (1998), the second case was implemented by the author as part of his diploma thesis. As we will see, our method will reduce the computational effort for matrices of finite order by a considerable amount.

The basic strategy of this work will be as follows. By the Jordan–Chevalley theorem, we have unique decompositions

$$A = S + N \qquad \text{and} \qquad B = S' + N'$$

where S, S' are semisimple and N, N' nilpotent matrices satisfying $SN = NS$ and $S'N' = N'S'$. Without restriction we may assume that all matrices are integral. Then, in a first step, we can examine whether S and S' are similar. Afterwards, we can pay attention to the nilpotent summands. Accordingly, our work will be separated into two parts.

For semisimple matrices, we will show that there is a one-to-one correspondence between their similarity classes and the equivalence (or isomorphy) classes of certain modules. To be more precise, if

$$\mu = \mu_1 \cdots \mu_s \qquad \text{and} \qquad \chi = \mu_1^{n_1} \cdots \mu_s^{n_s}$$

are the minimal and characteristic polynomials of the matrices at hand, we consider the algebra

$$\boldsymbol{\mathcal{K}} = \mathcal{K}_1 \oplus \cdots \oplus \mathcal{K}_s \quad \text{where } \mathcal{K}_\iota = \mathbb{Q}(\vartheta_\iota) = \mathbb{Q}[X]/(\mu_\iota).$$

The similarity classes of our matrices then correspond to the classes of full $\mathcal{O}$-modules in $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}} = \mathcal{K}_1^{n_1} \oplus \cdots \oplus \mathcal{K}_s^{n_s}$ where $\mathcal{O} = \mathbb{Z}[\vartheta] = \mathbb{Z}[\vartheta_1 \oplus \cdots \oplus \vartheta_s]$. This theorem was proved by Latimer and MacDuffee (1933) under the assumption $n_1 = \cdots = n_s = 1$, and we will prove its validity in the general case. Deciding similarity of semisimple matrices will then be equivalent to deciding whether two full modules are isomorphic.

If the modules are defined over the maximal order $\mathcal{O}_{\boldsymbol{\mathcal{K}}}$, it is well known how to decide whether they are equivalent, namely by reducing the problem to a principal ideal test in $\mathcal{O}_{\boldsymbol{\mathcal{K}}}$. However, this special case already illustrates that deciding similarity has to be considered a hard problem, as principal ideal testing certainly is. If the modules are defined over a nonmaximal order, further difficulties should be expected, as the theory of finitely generated modules is much less well understood in this case. For instance, the reduction indicated over $\mathcal{O}_{\boldsymbol{\mathcal{K}}}$ cannot be realized in general. As it turns out, any nonmaximal order of $\boldsymbol{\mathcal{K}}$ can occur in our context (as multiplier ring of a suitable module).

To find a solution in the nonmaximal case, we will need to decide whether a right ideal $\mathfrak{C}$ of a matrix order

$$\Lambda \subset \mathrm{M}(\boldsymbol{n}, \boldsymbol{\mathcal{K}}) = \bigoplus_{\iota=1}^{s} \mathrm{M}(n_\iota, \mathcal{K}_\iota)$$

is principal. Unless $n_1 = \cdots = n_s = 1$, this order is of course noncommutative. It is also nonmaximal unless its center is equal to $\mathcal{O}_{\boldsymbol{\mathcal{K}}}$. To decide whether $\mathfrak{C}$ is principal, we will devise an algorithm which will resemble an approach known for ideals in number fields. First, we will examine whether $\mathfrak{C}\Lambda_{\boldsymbol{\mathcal{K}}}$ is principal for a suitable maximal order $\Lambda_{\boldsymbol{\mathcal{K}}} \supset \Lambda$. This is obviously necessary for $\mathfrak{C}$ to be principal. If $\mathfrak{C}\Lambda_{\boldsymbol{\mathcal{K}}} = \varGamma\Lambda_{\boldsymbol{\mathcal{K}}}$, checking whether $\mathfrak{C}$ is principal will become a finite problem. Given that $\mathfrak{C}$ is coprime to the conductor $\mathfrak{F}$ of the extension $\Lambda \subset \Lambda_{\boldsymbol{\mathcal{K}}}$, we will have to check whether the residue class $[\varGamma + \mathfrak{F}]$ belongs to the image of the canonical map

$$\Lambda_{\boldsymbol{\mathcal{K}}}^\times \to (\Lambda/\mathfrak{F})^\times \backslash (\Lambda_{\boldsymbol{\mathcal{K}}}/\mathfrak{F})^\times.$$

In good cases, we will be able to solve this problem using standard methods for finitely presented abelian groups, as it is actually a question about determinants. However, as we will see in an example, $\det(\Lambda/\mathfrak{F})$ does not have to be a ring. Naturally, this will complicate things for us. Nevertheless, we can obtain an answer by searching the finite codomain of the map above. Unfortunately, it is not a group in general.

Furthermore, we will explain why it is always possible to assume that $\mathfrak{C}$ is coprime to the conductor. Suppose $\mathcal{O}$ is the center of Λ and $\mathfrak{f}$ the conductor of the extension $\mathcal{O} \subset \mathcal{O}_{\boldsymbol{\mathcal{K}}}$. Under the assumption that $\mathfrak{C}$ is invertible (which has to be met or else $\mathfrak{C}$ cannot be principal), we will show that $\mathfrak{C}$ can be made coprime to $\mathfrak{F}$ if and only if $\mathfrak{C}_{\mathfrak{p}}$ is principal for all prime ideals $\mathfrak{p}$ of $\mathcal{O}$ which contain $\mathfrak{f}$. Here, $\mathfrak{C}_{\mathfrak{p}}$ denotes the localization at the set

$$S_{\mathfrak{p}} = (\mathcal{O} \smallsetminus \mathfrak{p}) \cap \boldsymbol{\mathcal{K}}^{\times},$$

which coincides with the usual localization at $\mathfrak{p}$ if $\boldsymbol{\mathcal{K}}$ is a field. If $\mathfrak{C} = \mathfrak{c}$ is an invertible ideal of $\mathcal{O}$, it can always be made coprime to $\mathfrak{f}$ because $\mathfrak{c}_{\mathfrak{p}}$ is principal for any full prime ideal $\mathfrak{p}$. Not so if $\mathfrak{C}$ is an ideal of Λ. In this case, it is indeed possible that $\mathfrak{C}_{\mathfrak{p}}$ is not principal, so $\mathfrak{C}$ cannot be made coprime to $\mathfrak{F}$. However, if this situation occurs, $\mathfrak{C}$ itself cannot be principal, leading to a negative answer to our original question. Of course, we will also explain how to decide whether $\mathfrak{C}_{\mathfrak{p}}$ is principal and how to obtain a generator, if possible.

Having dealt with the semisimple parts, we may assume $S = S'$. We then need to find an invertible matrix C such that

$$CN = N'C \quad \text{while} \quad CS = SC.$$

Since N and N' commute with S, they are uniquely related to nilpotent matrices M, $M' \in \Lambda$. As we will see, the conditions above are met if and only if M and M' are similar, that is, if there is a matrix $\mathit{\Gamma} \in \Lambda^{\times}$ such that

$$\mathit{\Gamma} M = M' \mathit{\Gamma}.$$

To treat this problem, another module theoretic approach will be discussed, which mimics the strategy known for nilpotent matrices over a field. For the modules concerned, we will introduce a new relation, the similarity of modules, which requires that certain bases are mapped onto each other. This will constitute a stronger concept than equivalence.

Unfortunately, the close connection between classes of matrices and classes of modules will break up in the nilpotent case; modules corresponding to the same matrix might not be similar. This will pose an algorithmic problem, as we will be forced to consider not just a pair but a whole family of modules. Yet even deciding similarity for two modules will be hard in general. We will circumvent this difficulty by focusing on free modules, an idea pursued in Grunewald's paper. Examining these modules more closely, we will be able to improve his strategy significantly in two ways. First, if $A \in \Lambda$ is nilpotent and $\mathfrak{S}$ is the module corresponding to the matrix S, we will show how to enumerate all free A-modules of minimal index in $\mathfrak{S}$ efficiently, that is, without repetition and without encountering any other modules. Second, we will reduce the effort for deciding similarity of modules by arguing that, essentially, we only need to consider a search area of a fairly restrictive structure. In both cases, though, the number of steps can still grow exponentially fast.

Additionally, we will examine nilpotent matrices over the integer ring (which corresponds to the situation $S = 0$). In this special case, we will establish a few necessary conditions for similarity that can be checked easily. Moreover, we will simplify the similarity test for certain matrices. For example, it will suffice to solve a system of linear equations if the kernel of the matrices has dimension 1.

The arrangement of this thesis is as follows.

In the first chapter we will introduce orders and full modules, and we will prove the theorem by Latimer and MacDuffee in the general setting outlined above. After discussing how to decide equivalence of modules over a maximal order, we will address the nonmaximal case. The problem will be reformulated as a noncommutative principal ideal test. Making use of the conductor, we will show that this is a finite problem. Also, we will explain how to benefit from the situation where the ideal in question is coprime to the conductor. At the end of the chapter, we will note some remarks about the number of module classes. Most notably, we will give an example of a module class which cannot be represented by a direct sum of ideals (a problem which does not emerge over maximal orders).

The main goal of the second chapter will be to prove that ideals can always be assumed to be coprime to the conductor (or else they cannot be principal). This will be done with the help of localizations. We will establish a necessary and sufficient condition for when an ideal can be made coprime to the conductor. This will be possible if certain local ideals are principal. We will also explain how to conduct these principal ideal tests. Additionally, we will establish a decomposition of finite quotient rings into direct sums of smaller rings, also using the concept of localization.

The third chapter will revolve around the question of how to execute the principal ideal test described in the first chapter, provided that we can perform the test over the maximal order succesfully and that the ideal is coprime to the conductor. The commutative and the noncommutative case will be discussed separately. As we will see, the commutative case can be solved mainly by standard methods for finitely presented abelian groups. In good cases, the noncommutative test can be reduced to the commutative situation. Moreover, we will briefly explain how to perform the test without the requirement that the ideal is coprime to the conductor.

In the fourth chapter we will explain how to make use of the Jordan–Chevalley decomposition and how to relate the nilpotent parts of our matrices to nilpotent elements of a suitable matrix order. It will then suffice to decide similarity for these elements. The concept of similarity will be introduced for modules, and we will show how the similarity of matrices is connected to finding a pair of similar modules. Afterwards we will explain how to decide similarity for certain free modules and how to enumerate all relevant modules of minimal index. Finally, some aspects of nilpotent integer matrices will be discussed.

At the end of each chapter, we will outline the previously developed algorithms. The thesis will be concluded with two detailed examples illustrating the strategy of our method, accompanied by a few running time examples and an outlook for further research.

Part I

Semisimple Matrices

1 Module-Theoretic Approach I

At the beginning of this chapter, we will introduce some basic objects, notations and concepts, most notably the equivalence of full modules. In the second section we will establish a one-to-one correspondence between the similarity classes of semisimple matrices and the equivalence classes of full modules. Afterwards we will briefly explain how to decide equivalence over maximal orders. To deal with the problem of equivalence in the nonmaximal case, we will need to work with matrix orders and their ideals. Primarily, we need to know how to decide whether a full right ideal is principal. The conductor of a matrix order will prove a helpful object in this context. Moreover, we will describe units of matrix orders in terms of their determinants and we will make some remarks about the number of module classes.

1.1 Full Modules over Orders

Let $\mathcal{K}$ be a finite-dimensional $\mathbb{Q}$-algebra (possibly noncommutative). An **order** of $\mathcal{K}$ is a subring $\mathcal{O}$ (with the same unit element as $\mathcal{K}$) which is finitely generated as $\mathbb{Z}$-module and which satisfies

$$\mathbb{Q}\mathcal{O} = \mathcal{K}.$$

From the definition it follows that an order has a $\mathbb{Z}$-basis of length $\dim_{\mathbb{Q}} \mathcal{K}$. As a subring of a $\mathbb{Q}$-algebra, it is torsionfree and therefore free over $\mathbb{Z}$. The fact about the dimension is a consequence of the condition $\mathbb{Q}\mathcal{O} = \mathcal{K}$.

An element ϑ of a finite-dimensional $\mathbb{Q}$-algebra is called **integral** if it is a root of a monic integer polynomial. This is equivalent to the condition that the ring

$$\mathbb{Z}[\vartheta] = \{\, f(\vartheta) \mid f \in \mathbb{Z}[X] \,\}$$

is finitely generated as a $\mathbb{Z}$-module.[1] For this reason one easily verifies that all elements of an order are integral.

The ring $\mathbb{Z}[\vartheta]$ is a first example of an order of $\mathcal{K}$, the so-called **equation order** of ϑ, provided that ϑ is integral and $\mathcal{K} = \mathbb{Q}[\vartheta]$. If $d = \dim_{\mathbb{Q}} \mathcal{K}$, a $\mathbb{Z}$-basis of $\mathbb{Z}[\vartheta]$ is given by $1, \vartheta, \ldots, \vartheta^{d-1}$.

In particular, we will be interested in the case where $\mathcal{K}$ is a number field. Then the ring of all algebraic integers, denoted by $\mathcal{O}_{\mathcal{K}}$, is an order of $\mathcal{K}$, and it contains every other order. It is therefore called the **maximal order** of $\mathcal{K}$.

More generally, we will be interested in the situation where the algebra at hand is a direct sum $\boldsymbol{\mathcal{K}} = \mathcal{K}_1 \oplus \cdots \oplus \mathcal{K}_s$ of several number fields.[2] This is a ring with

[1] Cf. Neukirch (1999), p. 6, (2.2).

[2] Throughout this work, $\boldsymbol{\mathcal{K}}$ will always have this meaning.

componentwise addition and multiplication, and it becomes a $\mathbb{Q}$-algebra via

$$ax = ax_1 \oplus \cdots \oplus ax_s \quad \text{for } a \in \mathbb{Q} \text{ and } x = x_1 \oplus \cdots \oplus x_s \text{ in } \boldsymbol{\mathcal{K}}.$$

We may regard $\mathbb{Q}$ as a subset of $\boldsymbol{\mathcal{K}}$ since we have the embedding $a \mapsto a \oplus \cdots \oplus a$. Likewise, $\mathcal{K}_\iota$ can be identified in $\boldsymbol{\mathcal{K}}$ by means of the obvious injection $\mathcal{K}_\iota \to \boldsymbol{\mathcal{K}}$.

Suppose $\vartheta = \vartheta_1 \oplus \cdots \oplus \vartheta_s$ is an element of $\boldsymbol{\mathcal{K}}$ such that $\mathcal{K}_\iota = \mathbb{Q}(\vartheta_\iota)$ for each ι. Let $\mu_1, \ldots, \mu_s$ be the minimal polynomials of $\vartheta_1, \ldots, \vartheta_s$. If the polynomials are distinct, then $\boldsymbol{\mathcal{K}} = \mathbb{Q}[\vartheta]$ because $\mu = \mu_1 \cdots \mu_s$ is the minimal polynomial of ϑ and

$$\mathbb{Q}[X]/(\mu) \simeq \mathbb{Q}[X]/(\mu_1) \oplus \cdots \oplus \mathbb{Q}[X]/(\mu_s).$$

As mentioned above, $\mathbb{Z}[\vartheta]$ is an order of $\boldsymbol{\mathcal{K}}$ precisely if ϑ is integral. In general, though,

$$\mathbb{Z}[\vartheta] \neq \mathbb{Z}[\vartheta_1] \oplus \cdots \oplus \mathbb{Z}[\vartheta_s].$$

For example, the order $\mathbb{Z}[i \oplus \sqrt{2}]$ does not contain the element $1 \oplus 0$, as one easily verifies. In section 1.7 we will give a criterion for when equality holds.

An element of $\boldsymbol{\mathcal{K}}$ is integral if and only if all of its components are integral. Hence the order

$$\mathcal{O}_{\boldsymbol{\mathcal{K}}} = \mathcal{O}_{\mathcal{K}_1} \oplus \cdots \oplus \mathcal{O}_{\mathcal{K}_s}$$

consists of all integral elements of $\boldsymbol{\mathcal{K}}$. It is the **maximal order** of $\boldsymbol{\mathcal{K}}$.

Let $\boldsymbol{n} = (n_1, \ldots, n_s)$ be a multi-index, that is, a tuple of nonnegative integers. We define

$$\boldsymbol{\mathcal{K}}^{\boldsymbol{n}} = \mathcal{K}_1^{n_1} \oplus \cdots \oplus \mathcal{K}_s^{n_s}$$

where $\mathcal{K}_\iota^0 = 0$. Like $\boldsymbol{\mathcal{K}}$, this is a vector space over $\mathbb{Q}$. It is also a $\boldsymbol{\mathcal{K}}$-module via

$$x\xi = x_1\xi_1 \oplus \cdots \oplus x_s\xi_s$$

for $x = x_1 \oplus \cdots \oplus x_s$ in $\boldsymbol{\mathcal{K}}$ and $\xi = \xi_1 \oplus \cdots \oplus \xi_s$ in $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$.

Equipped with this scalar multiplication, we can now deal with modules in $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$. A finitely generated $\mathcal{O}$-module $\mathfrak{A}$ in $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$ is called **full** if it satisfies

$$\mathbb{Q} \cdot \mathfrak{A} = \boldsymbol{\mathcal{K}}^{\boldsymbol{n}}.$$

Since every order is a finitely generated $\mathbb{Z}$-module, the same is true for full $\mathcal{O}$-modules in $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$. As for orders we may conclude that every full $\mathcal{O}$-module has a $\mathbb{Z}$-basis of length $\dim_{\mathbb{Q}} \boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$.

If $\mathcal{K}$ is a number field, the full $\mathcal{O}$-modules in $\mathcal{K}$ are the fractional ideals of $\mathcal{O}$ (except for the zero ideal, of course). The situation is quite the same if $\mathcal{O}$ is an order of $\boldsymbol{\mathcal{K}}$. In this case, the full $\mathcal{O}$-modules in $\boldsymbol{\mathcal{K}}$ are the fractional ideals of $\mathcal{O}$ which contain a nonzerodivisor.[1]

[1] Fractional ideals are of the form $\gamma\mathfrak{a}$ where $\mathfrak{a}$ is an ideal of $\mathcal{O}$ and $\gamma \in \boldsymbol{\mathcal{K}}^\times$.

As is well known, two fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ in a number field $\mathcal{K}$ are called equivalent if there is a $\gamma \in \mathcal{K}^\times$ such that $\gamma\mathfrak{a} = \mathfrak{b}$. We want to generalize this concept to the case of full modules. Let

$$\mathrm{M}(\boldsymbol{n}, \boldsymbol{\mathcal{K}}) = \bigoplus_{\iota=1}^{s} \mathrm{M}(n_\iota, \mathcal{K}_\iota).$$

This is a matrix algebra acting on $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$ via

$$\varGamma\xi = \varGamma_1\xi_1 \oplus \cdots \oplus \varGamma_s\xi_s \quad \text{for } \varGamma = \varGamma_1 \oplus \cdots \oplus \varGamma_s \text{ in } \mathrm{M}(\boldsymbol{n}, \boldsymbol{\mathcal{K}}).$$

Analogously, let

$$\mathrm{GL}(\boldsymbol{n}, \boldsymbol{\mathcal{K}}) = \bigoplus_{\iota=1}^{s} \mathrm{GL}(n_\iota, \mathcal{K}_\iota).$$

Two full $\mathcal{O}$-modules $\mathfrak{A}$ and $\mathfrak{B}$ in $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$ will be called **equivalent** if there is a $\varGamma \in \mathrm{GL}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$ such that

$$\varGamma\mathfrak{A} = \mathfrak{B}.$$

In this case we will write $\mathfrak{A} \sim \mathfrak{B}$.

Obviously, this condition defines an equivalence relation on the set of all full $\mathcal{O}$-modules in $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$. In reference to the term *ideal class*, the equivalence class of a full module will be called its **module class**, which, in fact, coincides with its isomorphy class.

(1.1) Proposition. All homomorphisms between two full $\mathcal{O}$-modules $\mathfrak{A}$ and $\mathfrak{B}$ are of the form

$$\mathfrak{A} \to \mathfrak{B}, \quad \xi \mapsto \varGamma\xi$$

where $\varGamma$ is any matrix in $\mathrm{M}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$ with the property $\varGamma\mathfrak{A} \subset \mathfrak{B}$. The modules are equivalent if and only if they are isomorphic.

Proof. Clearly, every $\varGamma$ as above defines a homomorphism $\mathfrak{A} \to \mathfrak{B}$. Suppose

$$\gamma\colon \mathfrak{A} \to \mathfrak{B}$$

is an arbitrary homomorphism. First, we observe that γ can be extended uniquely to a $\boldsymbol{\mathcal{K}}$-automorphism $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}} \to \boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$ because γ can be regarded as a homomorphism between two free $\mathbb{Z}$-modules. As such, it can be extended uniquely to a $\mathbb{Q}$-homomorphism $\mathbb{Q}\mathfrak{A} \to \mathbb{Q}\mathfrak{B}$. Since $\mathbb{Q}\mathfrak{A} = \mathbb{Q}\mathfrak{B} = \boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$ and $\mathbb{Q}\mathcal{O} = \boldsymbol{\mathcal{K}}$, our assertion follows.
Suppose $e_1, \ldots, e_{n_\iota}$ is the standard basis of $\mathcal{K}_\iota^{n_\iota}$. Write e_i^ι for the image of e_i under the natural injection $\mathcal{K}_\iota^{n_\iota} \to \boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$. For every e_i^ι there are coefficients $\gamma_{ij}^\nu \in \mathcal{K}_\nu$ such that

$$\gamma(e_i^\iota) = \sum_{\nu=1}^{s}\sum_{j=1}^{n_\nu} \gamma_{ij}^\nu e_j^\nu.$$

Let 1_ι be the unit element in $\mathcal{K}_\iota$. Then $1_\iota e_i^\nu = \delta_{\iota\nu} e_i^\nu$ where $\delta_{\iota\nu}$ is the Kronecker delta. Hence

$$\gamma(e_i^\iota) = \gamma(1_\iota e_i^\iota) = 1_\iota\gamma(e_i^\iota) = 1_\iota \sum_{\nu=1}^{s}\sum_{j=1}^{n_\nu} \gamma_{ij}^\nu e_j^\nu = \sum_{\nu=1}^{s}\sum_{j=1}^{n_\nu} \gamma_{ij}^\nu (1_\iota e_j^\nu) = \sum_{j=1}^{n_\iota} \gamma_{ij}^\iota e_j^\iota,$$

that is, $\gamma_{ij}^{\nu} = 0$ if $\nu \neq \iota$. Let $\mathit{\Gamma}_\iota = [\gamma_{ij}^{\iota}]^{\mathrm{tr}}$. Then $\mathit{\Gamma} = \mathit{\Gamma}_1 \oplus \cdots \oplus \mathit{\Gamma}_s$ belongs to $\mathrm{M}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$. It satisfies $\gamma(e_i^\iota) = \mathit{\Gamma} e_i^\iota$ and therefore

$$\mathit{\Gamma}\mathfrak{A} = \gamma(\mathfrak{A}) \subset \mathfrak{B}.$$

Hence γ is of the desired form. Consequently, $\mathfrak{A} \sim \mathfrak{B}$ if and only if $\mathfrak{A} \simeq \mathfrak{B}$. ■

In the next section we will see that the problem of deciding whether two semisimple integer matrices are similar can be translated into the problem of deciding whether certain $\mathcal{O}$-modules are equivalent. Before addressing this issue, we will introduce the notion of a **multiplier ring**. By this we understand the set

$$\mathcal{O} = \{\, x \in \boldsymbol{\mathcal{K}} \mid x\mathfrak{A} \subset \mathfrak{A} \,\}$$

where $\mathfrak{A} \subset \boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$ can be any free $\mathbb{Z}$-module of rank $\dim_{\mathbb{Q}} \boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$.

(1.2) Proposition. The multiplier ring is an order of $\boldsymbol{\mathcal{K}}$.

Proof. Clearly, $\mathcal{O}$ is a subring of $\boldsymbol{\mathcal{K}}$ containing 1. Let $m = \dim_{\mathbb{Q}} \boldsymbol{\mathcal{K}}$ and let $\pi \colon \boldsymbol{\mathcal{K}}^{\boldsymbol{n}} \to \boldsymbol{\mathcal{K}}$ be a surjective homomorphism. Then $\mathfrak{a} = \pi(\mathfrak{A})$ is a free $\mathbb{Z}$-module of rank m and it contains a nonzerodivisor a. It is also an $\mathcal{O}$-module (since $\mathfrak{A}$ obviously is), so

$$a\mathcal{O} \subset \mathfrak{a}.$$

Thereby we see that $\mathcal{O}$ is a free $\mathbb{Z}$-module of rank at most m, as it is contained in $a^{-1}\mathfrak{a}$. On the other hand, let $\alpha_1, \dots, \alpha_m$ be a $\mathbb{Z}$-basis of $\mathfrak{a}$. Let $x_{jk}^{(i)}$ denote the rational coefficients with

$$\alpha_i \alpha_j = \sum_{k=1}^{m} x_{jk}^{(i)} \alpha_k \quad (1 \leq i, j \leq m).$$

Choose a nonzero integer c such that $cx_{jk}^{(i)} \in \mathbb{Z}$ for all i, j and k. Then

$$(c\alpha_i)\alpha_j = \sum_{k=1}^{m} (cx_{jk}^{(i)})\alpha_k \in \mathfrak{a} \quad \text{for all } i \text{ and } j,$$

that is, $c\alpha_i \in \mathcal{O}$ for all i. Therefore $c\mathfrak{a} \subset \mathcal{O}$, and $\mathcal{O}$ has rank at least m. ■

As mentioned in the proof, if $\mathcal{O}$ is the multiplier ring of $\mathfrak{A}$, then $\mathfrak{A}$ is a full $\mathcal{O}$-module. In fact, $\mathcal{O}$ is the largest order of $\boldsymbol{\mathcal{K}}$ that constitutes a module structure on $\mathfrak{A}$. Since we can always think of $\mathfrak{A}$ to be defined over its multiplier ring, we may simply speak of **full modules** in $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$ without referring to a certain order. Also, if there is no danger of confusion, we will simply speak of full modules without mentioning $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$ either.

We conclude this section with a statement that is easy to prove.

(1.3) Proposition. If $\mathfrak{A} \sim \mathfrak{B}$, the modules have the same multiplier ring.

1.2 The Theorem of Latimer and MacDuffee

In this section we will establish a connection between the similarity classes of semisimple integer matrices and the equivalence classes of full modules in $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$. Recall that a matrix is semisimple if and only if its minimal polynomial is square-free. If $\boldsymbol{n} = (n_1, \dots, n_s)$ and $\boldsymbol{d} = (d_1, \dots, d_s)$ are multi-indices, we will write

$$|\boldsymbol{n}| = n_1 + \cdots + n_s \qquad \text{and} \qquad \boldsymbol{d} \cdot \boldsymbol{n} = d_1 n_1 + \cdots + d_s n_s.$$

If $d_\iota = [\mathcal{K}_\iota : \mathbb{Q}]$ for each ι, then $\boldsymbol{d} \cdot \boldsymbol{n}$ is the dimension of $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$ over $\mathbb{Q}$. We may imagine $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$ as a subset of $\mathbb{C}^{|\boldsymbol{n}|}$ and $\mathrm{M}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$ as a subset of $\mathrm{M}(|\boldsymbol{n}|, \mathbb{C})$ by identifying

$$\xi_1 \oplus \cdots \oplus \xi_n \text{ with } \begin{bmatrix} \xi_1 \\ \vdots \\ \xi_s \end{bmatrix} \quad \text{and} \quad \varGamma_1 \oplus \cdots \oplus \varGamma_s \text{ with } \begin{bmatrix} \varGamma_1 & & 0 \\ & \ddots & \\ 0 & & \varGamma_s \end{bmatrix}.$$

If $\mathfrak{A}$ is a full module in $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$, we therefore have a $|\boldsymbol{n}| \times \boldsymbol{d} \cdot \boldsymbol{n}$ matrix $\varXi$ such that

$$\mathfrak{A} = \varXi \mathbb{Z}^{\boldsymbol{d} \cdot \boldsymbol{n}},$$

that is, the columns of $\varXi$ belong to $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$ and they form a $\mathbb{Z}$-basis of $\mathfrak{A}$.

(1.4) Theorem. Suppose $\mathcal{O} = \mathbb{Z}[\vartheta]$ and $\boldsymbol{\mathcal{K}} = \mathbb{Q}[\vartheta]$ where $\vartheta = \vartheta_1 \oplus \cdots \oplus \vartheta_s$ consists of algebraic integers with distinct minimal polynomials $\mu_1, \dots, \mu_s$. Let

$$\mu = \mu_1 \cdots \mu_s, \qquad \chi = \mu_1^{n_1} \cdots \mu_s^{n_s} \qquad \text{and} \qquad \boldsymbol{n} = (n_1, \dots, n_s)$$

with $n_\iota > 0$. There is a one-to-one correspondence between

- the similarity classes of integer matrices with minimal polynomial μ and characteristic polynomial χ, and
- the module classes of full $\mathcal{O}$-modules in $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$.

This theorem is a generalization of a theorem by Latimer and MacDuffee (1933) who considered the case $\chi = \mu$ (that is, $n_\iota = 1$ for all ι). Its proof is significantly inspired by work of Taussky (1949). She dealt with the special case where χ is irreducible.

The proof is divided into six lemmata. In the following, the requirements of (1.4) will always hold. Moreover, $\mathcal{K}_\iota$ will be the field $\mathbb{Q}(\vartheta_\iota)$ of degree $d_\iota = \deg(\mu_\iota)$ (so that $\boldsymbol{\mathcal{K}} = \mathcal{K}_1 \oplus \cdots \oplus \mathcal{K}_s$), A and B will denote integer matrices with minimal polynomial μ and characteristic polynomial χ, $\mathfrak{A}$ and $\mathfrak{B}$ will be full $\mathcal{O}$-modules in $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$, and $m = d_1 n_1 + \cdots + d_s n_s$ will be the dimension of $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$ over $\mathbb{Q}$.

(1.5) Lemma. For each ι, let $x_1^\iota, \dots, x_{n_\iota}^\iota \in \mathcal{K}_\iota^m$ be a $\mathcal{K}_\iota$-Basis of $\mathrm{Eig}(A, \vartheta_\iota)$. Let

$$\varXi = [\, x_1^1 \; \dots \; x_{n_1}^1 \; \dots \; \dots \; x_1^s \; \dots \; x_{n_s}^s \,]^{\mathrm{tr}},$$

that is, the rows of $\varXi$ consist of eigenvectors. Then $\mathfrak{A} = \varXi \mathbb{Z}^m$ is a full $\mathcal{O}$-module in $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$.

Proof. Since A is a semisimple matrix and ϑ_ι an eigenvalue of multiplicity n_ι, the dimension of $\mathrm{Eig}(A, \vartheta_\iota)$ over $\mathcal{K}_\iota$ is in fact n_ι. Let $\varXi$ and $\mathfrak{A}$ be as described above. Write $x_h^\iota = [\, x_{h1}^\iota \ \dots \ x_{hm}^\iota \,]^{\mathrm{tr}}$. To show that $\mathfrak{A}$ is a module over $\mathcal{O} = \mathbb{Z}[\vartheta]$, it suffices to verify that $\vartheta\xi_i$ belongs to $\mathfrak{A}$ for each column

$$\xi_i = [\, x_{1i}^1 \ \dots \ x_{n_1 i}^1 \ \dots \ \dots \ x_{1i}^s \ \dots \ x_{n_s i}^s \,]^{\mathrm{tr}} \quad \text{of } \varXi.$$

Since x_h^ι is an eigenvector of $A = [a_{ij}]$ corresponding to ϑ_ι, we have the relation

$$\vartheta_\iota x_{hi}^\iota = \sum_{j=1}^m a_{ij} x_{hj}^\iota.$$

Therefore $\vartheta\xi_i = \sum a_{ij}\xi_j$ belongs to $\mathfrak{A}$.
It remains to show that $\mathfrak{A}$ is full. Suppose this was not the case. Then the columns of $\varXi$ are linearly dependent over $\mathbb{Z}$. Thus there is a $C \in \mathrm{GL}(m, \mathbb{Z})$ such that $\varXi C^{\mathrm{tr}} = [\, \varUpsilon \ 0 \,]$ where $\varUpsilon = [\, \upsilon_1 \ \dots \ \upsilon_k \,]$ consists of linearly independent columns. Write

$$(y_h^\iota)^{\mathrm{tr}} = [\, y_{h1}^\iota \ \dots \ y_{hk}^\iota \ 0 \ \dots \ 0 \,]$$

for the rows of $[\, \varUpsilon \ 0 \,]$ and put $B = CAC^{-1}$. The vectors $y_h^\iota = Cx_h^\iota$ then form a $\mathcal{K}_\iota$-basis of $\mathrm{Eig}(B, \vartheta_\iota)$. Write $B = [b_{ij}]$. For all ι and h and for $i > k$, we have

$$\sum_{j=1}^k b_{ij} y_{hj}^\iota = 0,$$

that is, $\sum b_{ij}\upsilon_j = 0$. Because of the linear independence, we conclude $b_{ij} = 0$ for $j \le k < i$. Hence we see that

$$B = \begin{bmatrix} B' & * \\ 0 & * \end{bmatrix} \quad \text{where } B' \in \mathrm{M}(k, \mathbb{Z}).$$

The truncated vectors $[\, y_{h1}^\iota \ \dots \ y_{hk}^\iota \,]^{\mathrm{tr}}$ are eigenvectors of B' corresponding to ϑ_ι. As the x_h^ι, they are linearly independent over $\mathcal{K}_\iota$, so ϑ_ι is an eigenvalue of B' of multiplicity at least n_ι. Therefore the characteristic polynomial of B' has degree at least $d_1 n_1 + \dots + d_s n_s = m > k$, a contradiction. ■

(1.6) Definition. A module as in (1.5) will be said to **correspond** to A.

(1.7) Lemma. The module class of $\mathfrak{A}$ does not depend on the choice of the bases for the eigenspaces $\mathrm{Eig}(A, \vartheta_\iota)$.

Proof. Let $y_1^\iota, \dots, y_{n_\iota}^\iota$ be another basis of $\mathrm{Eig}(A, \vartheta_\iota)$ for each ι. Let $\varUpsilon$ be the matrix with columns

$$\upsilon_i = [\, y_{1i}^1 \ \dots \ y_{n_1 i}^1 \ \dots \ \dots \ y_{1i}^s \ \dots \ y_{n_s i}^s \,]^{\mathrm{tr}}$$

and $\mathfrak{B} = \varUpsilon\mathbb{Z}^m$. There are matrices $\varGamma_\iota = [\gamma_{ij}^\iota]$ in $\mathrm{GL}(n_\iota, \mathcal{K}_\iota)$ such that

$$y_i^\iota = \sum_{j=1}^{n_\iota} \gamma_{ij}^\iota x_j^\iota,$$

so $y_{ik}^\iota = \sum \gamma_{ij}^\iota x_{jk}^\iota$. Thus we see that $\upsilon_k = \varGamma\xi_k$ for all k where $\varGamma = \varGamma_1 \oplus \dots \oplus \varGamma_s$. In conclusion, $\varGamma\mathfrak{A} = \mathfrak{B}$. ■

(1.8) Lemma. If A and B are similar, their corresponding modules are equivalent.

Proof. Suppose $C = [c_{ij}]$ in $\mathrm{GL}(n,\mathbb{Z})$ satisfies $B = CAC^{-1}$. Let $x_1^\iota, \ldots, x_{n_\iota}^\iota$ be a $\mathcal{K}_\iota$-basis of $\mathrm{Eig}(A, \vartheta_\iota)$. If

$$y_h^\iota = Cx_h^\iota,$$

then $y_1^\iota, \ldots, y_{n_\iota}^\iota$ forms a basis of $\mathrm{Eig}(B, \vartheta_\iota)$. Let $\varXi$ and $\varUpsilon$ be as before. We have

$$y_{hi}^\iota = \sum c_{ij} x_{hj}^\iota,$$

hence $\upsilon_i = \sum c_{ij}\xi_j$. Therefore the modules $\mathfrak{A} = \varXi\mathbb{Z}^m$ and $\mathfrak{B} = \varUpsilon\mathbb{Z}^m$ are in fact equal. Choosing other bases would result in equivalent modules by the previous lemma. ■

(1.9) Lemma. Let $\mathfrak{A} = \varXi\mathbb{Z}^m$ be a full $\mathcal{O}$-module in $\boldsymbol{\mathcal{K}^n}$ and let $A = [a_{ij}]$ be the matrix in $\mathrm{M}(m, \mathbb{Z})$ with entries satisfying

$$\vartheta\xi_i = \sum_{j=1}^{m} a_{ij}\xi_j$$

where $\xi_1, \ldots, \xi_m$ are the columns of $\varXi$. Then μ is the minimal and χ the characteristic polynomial of A.

Proof. If $(x_h^\iota)^{\mathrm{tr}} = [\, x_{h1}^\iota \; \ldots \; x_{hm}^\iota \,]$ is the hth of the $\mathcal{K}_\iota$-rows of $\varXi$, we have

$$\vartheta_\iota x_{hi}^\iota = \sum_{j=1}^{m} a_{ij} x_{hj}^\iota,$$

that is, $\vartheta_\iota x_h^\iota = Ax_h^\iota$. Thus x_h^ι is an eigenvector of A corresponding to ϑ_ι. The vectors $x_1^\iota, \ldots, x_{n_\iota}^\iota$ are linearly independent over $\mathcal{K}_\iota$ (otherwise there would be a matrix $\varGamma \in \mathrm{GL}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$ such that the first $\mathcal{K}_\iota$-row of $\varGamma\varXi$ were zero, so $\varGamma\mathfrak{A}$ would not be full). Hence the dimension of $\mathrm{Eig}(A, \vartheta_\iota)$ over $\mathcal{K}_\iota$ is at least n_ι, so

$$\chi = \mu_1^{n_1} \cdots \mu_s^{n_s}$$

divides the characteristic polynomial of A. Since both polynomials have degree

$$m = d_1 n_1 + \cdots + d_s n_s,$$

they must be equal. Therefore the geometric multiplicity of each eigenvalue is equal to its algebraic multiplicity, implying that $\mu = \mu_1 \cdots \mu_s$ is the minimal polynomial of A. ■

(1.10) Definition. A matrix as in (1.9) will be said to **correspond** to $\mathfrak{A}$.

(1.11) Lemma. The similarity class of A does not depend on the choice of a $\mathbb{Z}$-basis for $\mathfrak{A}$.

Proof. Suppose $\varUpsilon$ is another matrix satisfying $\mathfrak{A} = \varUpsilon\mathbb{Z}^m$ with columns

$$\upsilon_i = [\, y^1_{1i} \;\ldots\; y^1_{n_1 i} \;\ldots\;\ldots\; y^s_{1i} \;\ldots\; y^s_{n_s i}\,]^{\mathrm{tr}}.$$

Then there is a matrix $C = [c_{ij}]$ in $\mathrm{GL}(m, \mathbb{Z})$ such that

$$\upsilon_i = \sum_{j=1}^{m} c_{ij}\xi_j.$$

Let $B = CAC^{-1}$. The vectors $y^\iota_i = [\, y^\iota_{i1} \;\ldots\; y^\iota_{im}\,]^{\mathrm{tr}} = Cx^\iota_i$ are eigenvectors of B corresponding to ϑ_ι. Therefore $B = [b_{ij}]$ is the matrix such that

$$\vartheta\upsilon_i = \sum_{j=1}^{m} b_{ij}\upsilon_j.$$

Of course, μ is the minimal and χ the characteristic polynomial of B. In conclusion, B corresponds to $\mathfrak{A}$. ■

(1.12) Lemma. If $\mathfrak{A}$ and $\mathfrak{B}$ are equivalent, their corresponding matrices are similar.

Proof. Let $\varGamma \in \mathrm{GL}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$ satisfy $\varGamma\mathfrak{A} = \mathfrak{B}$ and let $\xi_1, \ldots, \xi_m$ and $\upsilon_1, \ldots, \upsilon_m$ be $\mathbb{Z}$-bases of $\mathfrak{A}$ and $\mathfrak{B}$. Suppose $C = [c_{ij}]$ is the integer matrix with

$$\varGamma\xi_i = \sum c_{ij}\upsilon_j$$

and let $A = [a_{ij}]$ and $B = [b_{ij}]$ be the matrices corresponding to $\mathfrak{A}$ and $\mathfrak{B}$. On the one hand, we have

$$\begin{aligned} \varGamma(\vartheta\xi_i) &= \varGamma(\sum_j a_{ij}\xi_j) = \sum_j a_{ij}(\varGamma\xi_j) \\ &= \sum_j a_{ij}\sum_k c_{jk}\upsilon_k = \sum_k(\sum_j a_{ij}c_{jk})\upsilon_k, \end{aligned}$$

and on the other hand,

$$\begin{aligned} \vartheta(\varGamma\xi_i) &= \vartheta\sum_j c_{ij}\upsilon_j = \sum_j c_{ij}(\vartheta\upsilon_j) \\ &= \sum_j c_{ij}\sum_k b_{jk}\upsilon_k = \sum_k(\sum_j c_{ij}b_{jk})\upsilon_k. \end{aligned}$$

Therefore $\sum a_{ij}c_{jk} = \sum c_{ij}b_{jk}$ for all i and k, so $AC = CB$. ■

Not only does (1.4) state a correspondence between similarity and equivalence classes, its proof also provides us with a strategy for deciding whether two matrices are similar. Given two matrices A and B, we can compute their corresponding modules $\mathfrak{A}$ and $\mathfrak{B}$ with bases $\varXi$ and $\varUpsilon$ as described in (1.5). If $\varGamma\mathfrak{A} = \mathfrak{B}$ for some $\varGamma \in \mathrm{GL}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$, then $AC = CB$, where C is the matrix of the $\mathbb{Z}$-homomorphism

$$\mathfrak{A} \to \mathfrak{B}, \quad \xi \mapsto \varGamma\xi$$

with respect to the bases $\varXi$ and $\varUpsilon$. Moreover, if $\mathfrak{A} \not\sim \mathfrak{B}$, then A and B are not similar. Hence we need to examine how to decide whether two full modules are equivalent. In the next section we will explain how this can be accomplished over a maximal order.

1.3 Equivalence over Maximal Orders

Let $\mathfrak{A}$ and $\mathfrak{B}$ be two full $\mathcal{O}_{\boldsymbol{\mathcal{K}}}$-modules in $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$. Our goal is to decide whether the modules are equivalent. Since $\mathcal{O}_{\boldsymbol{\mathcal{K}}}$ is a direct sum of maximal orders, every $\mathcal{O}_{\boldsymbol{\mathcal{K}}}$-module is of the form $\mathfrak{A}_1 \oplus \cdots \oplus \mathfrak{A}_s$. Therefore

$$\mathfrak{A} \sim \mathfrak{B} \quad \Leftrightarrow \quad \mathfrak{A}_\iota \sim \mathfrak{B}_\iota \quad \text{for all } \iota.$$

Thus it suffices to assume that $\mathfrak{A}$ and $\mathfrak{B}$ are full $\mathcal{O}_{\mathcal{K}}$-modules in $\mathcal{K}^n$ where $\mathcal{K}$ is a number field. By a well-known result, $\mathfrak{A}$ and $\mathfrak{B}$ are equivalent to modules of the form

$$\mathfrak{a} \oplus \mathcal{O}_{\mathcal{K}}^{n-1} \quad \text{and} \quad \mathfrak{b} \oplus \mathcal{O}_{\mathcal{K}}^{n-1}$$

where $\mathfrak{a}$ and $\mathfrak{b}$ are ideals of $\mathcal{O}_{\mathcal{K}}$ and

$$\mathfrak{A} \sim \mathfrak{B} \quad \Leftrightarrow \quad \mathfrak{a} \sim \mathfrak{b}.$$

In the following we will outline the main aspects for proving this theorem.[1] To begin with, an $\mathcal{O}$-module $\mathfrak{A}$ is called **projective** if it satisfies the following condition: Every exact sequence

$$0 \to \mathfrak{C} \to \mathfrak{B} \to \mathfrak{A} \to 0$$

of $\mathcal{O}$-modules is split, that is, $\mathfrak{B} \simeq \mathfrak{A} \oplus \mathfrak{C}$.

If $\mathfrak{a}$ is an ideal of $\mathcal{O}$, it is a projective module if and only if it is invertible. Hence all nonzero ideals of a maximal order are projective modules. This observation enables us to transform full $\mathcal{O}_{\mathcal{K}}$-modules into direct sums of ideals. Suppose $\mathfrak{A}$ is a full $\mathcal{O}_{\mathcal{K}}$-module in $\mathcal{K}^n$. Without restriction we may assume that $\mathfrak{A} \subset \mathcal{O}_{\mathcal{K}}^n$. Let

$$\pi_1 \colon \mathcal{K}^n \to \mathcal{K}$$

be the projection onto the first component and let $\mathfrak{a}_1 = \pi_1(\mathfrak{A})$. Then $\mathfrak{a}_1$ is a nonzero ideal of $\mathcal{O}_{\mathcal{K}}$ and there is an exact sequence

$$0 \to \mathfrak{A}' \to \mathfrak{A} \to \mathfrak{a}_1 \to 0 \qquad \text{where } \mathfrak{A}' = \ker(\pi_1).$$

Therefore

$$\mathfrak{A} \simeq \mathfrak{a}_1 \oplus \mathfrak{A}'.$$

Next, it is possible to embed $\mathfrak{A}'$ into $\mathcal{K}^{n-1}$, and by induction we may assume that $\mathfrak{A}' \simeq \mathfrak{a}_2 \oplus \cdots \oplus \mathfrak{a}_n$, hence $\mathfrak{A} \simeq \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n$. By (1.1) modules are equivalent precisely if they are isomorphic, thus we may write

$$\mathfrak{A} \sim \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n.$$

In the case of a nonmaximal order, the situation is more complicated, as not all nonzero ideals are invertible. In fact, as we will see at the end of this chapter, there are full $\mathcal{O}$-modules which cannot be transformed into direct sums of ideals. However, if the transformation is possible, we have the following result.

[1] Apart from (1.14) and (1.15), the results presented here are based on Narkiewicz (2004), section 1.3.

(1.13) Proposition. Let $\mathfrak{A} = \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n$ and $\mathfrak{B} = \mathfrak{b}_1 \oplus \cdots \oplus \mathfrak{b}_n$ be two full modules in $\mathcal{K}^n$. If $\mathit{\Gamma} \in \mathrm{GL}(n, \mathcal{K})$ satisfies $\mathit{\Gamma}\mathfrak{A} = \mathfrak{B}$, then

$$\det(\mathit{\Gamma}) \cdot \mathfrak{a}_1 \cdots \mathfrak{a}_n = \mathfrak{b}_1 \cdots \mathfrak{b}_n,$$

that is, the products of the ideals are equivalent.

Proof. Write $\mathit{\Gamma} = [\gamma_{ij}]$. From $\mathit{\Gamma}\mathfrak{A} = \mathfrak{B}$ we obtain

$$\mathfrak{b}_i = \gamma_{i1}\mathfrak{a}_1 + \cdots + \gamma_{in}\mathfrak{a}_n \quad \text{for all } i,$$

therefore

$$\mathfrak{b}_1 \cdots \mathfrak{b}_n = \prod_{i=1}^{n} (\gamma_{i1}\mathfrak{a}_1 + \cdots + \gamma_{in}\mathfrak{a}_n) = \det(\mathit{\Gamma})\, \mathfrak{a}_1 \cdots \mathfrak{a}_n + \text{further products.}$$

In particular,

$$\det(\mathit{\Gamma})\, \mathfrak{a}_1 \cdots \mathfrak{a}_n \subset \mathfrak{b}_1 \cdots \mathfrak{b}_n.$$

Conversely, we have $\mathit{\Gamma}^{-1}\mathfrak{B} = \mathfrak{A}$, implying $\det(\mathit{\Gamma})^{-1}\, \mathfrak{b}_1 \cdots \mathfrak{b}_n \subset \mathfrak{a}_1 \cdots \mathfrak{a}_n$. This establishes the proposition. ■

Next we will explain how an $\mathcal{O}_{\mathcal{K}}$-module $\mathfrak{A} = \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n$ can be simplified to the form $\mathfrak{a} \oplus \mathcal{O}_{\mathcal{K}}^{n-1}$ where $\mathfrak{a} = \mathfrak{a}_1 \cdots \mathfrak{a}_n$. To achieve this, we will apply the so-called Approximation Theorem.

(1.14) Approximation Theorem. Let $\mathfrak{P}$ be a finite set of prime ideals of $\mathcal{O}_{\mathcal{K}}$. Let $(\nu_{\mathfrak{p}})_{\mathfrak{p} \in \mathfrak{P}}$ be a collection of integers and let $v_{\mathfrak{p}}$ denote the $\mathfrak{p}$-adic valuation. Then there is an $a \in \mathcal{K}^{\times}$ such that

$$v_{\mathfrak{p}}(a) = \nu_{\mathfrak{p}} \quad \text{for } \mathfrak{p} \in \mathfrak{P} \qquad \text{and} \qquad v_{\mathfrak{p}}(a) \geq 0 \quad \text{for } \mathfrak{p} \notin \mathfrak{P}.$$

Proof. We start by choosing elements

$$y_{\mathfrak{p}} \in \mathfrak{p}^{-\nu_{\mathfrak{p}}} \smallsetminus \mathfrak{p}^{1-\nu_{\mathfrak{p}}} \quad \text{for } \mathfrak{p} \in \mathfrak{P} \text{ with } \nu_{\mathfrak{p}} < 0.$$

By the Chinese Remainder Theorem, there is a $y \in \mathcal{O}_{\mathcal{K}}$ such that, for all $\mathfrak{p} \in \mathfrak{P}$,

$$y \equiv \begin{cases} y_{\mathfrak{p}} & \bmod \mathfrak{p} \quad \text{if } \nu_{\mathfrak{p}} < 0, \\ 1 & \bmod \mathfrak{p} \quad \text{if } \nu_{\mathfrak{p}} \geq 0. \end{cases}$$

In the same fashion we can choose elements

$$x_{\mathfrak{p}} \in \mathfrak{p}^{\nu_{\mathfrak{p}}} \smallsetminus \mathfrak{p}^{1+\nu_{\mathfrak{p}}} \quad \text{for } \mathfrak{p} \in \mathfrak{P} \text{ with } \nu_{\mathfrak{p}} \geq 0$$

and

$$x_{\mathfrak{p}} \in \mathfrak{p}^{v_{\mathfrak{p}}(y)} \smallsetminus \mathfrak{p}^{1+v_{\mathfrak{p}}(y)} \quad \text{for } \mathfrak{p} \notin \mathfrak{P} \text{ with } v_{\mathfrak{p}}(y) > 0.$$

Then there is an element $x \in \mathcal{O}_{\mathcal{K}}$ such that

$$x \equiv \begin{cases} 1 & \bmod \mathfrak{p} \quad \text{if } \mathfrak{p} \in \mathfrak{P} \text{ with } \nu_{\mathfrak{p}} < 0, \\ x_{\mathfrak{p}} & \bmod \mathfrak{p} \quad \text{if } \mathfrak{p} \in \mathfrak{P} \text{ with } \nu_{\mathfrak{p}} \geq 0, \\ x_{\mathfrak{p}} & \bmod \mathfrak{p} \quad \text{if } \mathfrak{p} \notin \mathfrak{P} \text{ with } v_{\mathfrak{p}}(y) > 0. \end{cases}$$

Put $a = x/y$. Then $v_{\mathfrak{p}}(a) = v_{\mathfrak{p}}(x) - v_{\mathfrak{p}}(y)$ has the desired properties. ■

(1.15) Corollary. Let $\mathfrak{a}$ and $\mathfrak{b}$ be two nonzero ideals of $\mathcal{O}_{\mathcal{K}}$. Then there is a $\gamma \in \mathcal{K}^\times$ such that $\gamma\mathfrak{a} + \mathfrak{b} = \mathcal{O}_{\mathcal{K}}$.

Proof. Write

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{a_\mathfrak{p}} \quad \text{and} \quad \mathfrak{b} = \prod_{\mathfrak{p}} \mathfrak{p}^{b_\mathfrak{p}}$$

where $\mathfrak{p}$ ranges over all maximal ideals of $\mathcal{O}_{\mathcal{K}}$. By the Approximation Theorem we can choose a $\gamma \in \mathcal{K}^\times$ such that

$$v_\mathfrak{p}(\gamma) = -a_\mathfrak{p} \quad \text{for all } \mathfrak{p} \text{ with } b_\mathfrak{p} > 0 \qquad \text{and} \qquad v_\mathfrak{p}(\gamma) \geq 0 \quad \text{elsewhere.}$$

Then $v_\mathfrak{p}(\gamma\mathfrak{a}) \geq 0$ for all $\mathfrak{p}$, that is, $\gamma\mathfrak{a} \subset \mathcal{O}_{\mathcal{K}}$. More importantly, $\gamma\mathfrak{a}$ is not contained in any prime ideal above $\mathfrak{b}$, therefore $\gamma\mathfrak{a} + \mathfrak{b} = \mathcal{O}_{\mathcal{K}}$. ■

To prove that

$$\mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n \sim (\mathfrak{a}_1 \cdots \mathfrak{a}_n) \oplus \mathcal{O}_{\mathcal{K}}^{n-1},$$

it obviously suffices to consider the case $n = 2$. By (1.15) we may assume that

$$\mathfrak{a}_1 + \mathfrak{a}_2 = \mathcal{O}_{\mathcal{K}}.$$

Then we have an exact sequence

$$0 \to \mathfrak{a}_1 \cap \mathfrak{a}_2 \to \mathfrak{a}_1 \oplus \mathfrak{a}_2 \to \mathcal{O}_{\mathcal{K}} \to 0$$

where the second and third map are given by the rules

$$a \mapsto a \oplus (-a) \qquad \text{and} \qquad a_1 \oplus a_2 \mapsto a_1 + a_2.$$

We already know that the sequence is split, and since the ideals are coprime, we have $\mathfrak{a}_1 \cap \mathfrak{a}_2 = \mathfrak{a}_1\mathfrak{a}_2$. Therefore $\mathfrak{a}_1 \oplus \mathfrak{a}_2 \sim \mathfrak{a} \oplus \mathcal{O}_{\mathcal{K}}$.

Again, the nonmaximal situation is less clear. For example, if $\mathfrak{f}$ is the conductor of the extension $\mathcal{O} \subset \mathcal{O}_{\mathcal{K}}$ (i.e., the largest $\mathcal{O}_{\mathcal{K}}$-ideal contained in $\mathcal{O}$), then

$$\mathfrak{f} \oplus \mathfrak{f} \not\sim \mathfrak{a} \oplus \mathcal{O} \quad \text{for all } \mathcal{O}\text{-ideals } \mathfrak{a}$$

because the multiplier ring of $\mathfrak{f} \oplus \mathfrak{f}$ is $\mathcal{O}_{\mathcal{K}}$, whereas it is $\mathcal{O}$ for $\mathfrak{a} \oplus \mathcal{O}$. However, if $\mathfrak{a}_1 + \mathfrak{a}_2 = \mathcal{O}$, we can deduce $\mathfrak{a}_1 \oplus \mathfrak{a}_2 \sim \mathfrak{a} \oplus \mathcal{O}$ using the same arguments as before. Consequently, our problem is that (1.15) cannot be formulated for all ideals of a nonmaximal order.

Let us summarize our results for the case $\boldsymbol{\mathcal{K}} = \mathcal{K}_1 \oplus \cdots \oplus \mathcal{K}_s$.

(1.16) Theorem. Let $\mathfrak{A}$ and $\mathfrak{B}$ be two full $\mathcal{O}_{\boldsymbol{\mathcal{K}}}$-modules in $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$. Then there are $\mathcal{O}_{\boldsymbol{\mathcal{K}}}$-ideals $\mathfrak{a} = \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_s$ and $\mathfrak{b} = \mathfrak{b}_1 \oplus \cdots \oplus \mathfrak{b}_s$ such that

$$\mathfrak{A} \sim \bigoplus_{\iota=1}^{s} (\mathfrak{a}_\iota \oplus \mathcal{O}_{\mathcal{K}_\iota}^{n_\iota - 1}) \quad \text{and} \quad \mathfrak{B} \sim \bigoplus_{\iota=1}^{s} (\mathfrak{b}_\iota \oplus \mathcal{O}_{\mathcal{K}_\iota}^{n_\iota - 1}).$$

Moreover, $\mathfrak{A} \sim \mathfrak{B}$ if and only if $\mathfrak{a} \sim \mathfrak{b}$.

To decide whether the ideals $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent, we can apply a principal ideal test to each component of

$$\mathfrak{a}^{-1}\mathfrak{b} = (\mathfrak{a}_1^{-1}\mathfrak{b}_1) \oplus \cdots \oplus (\mathfrak{a}_s^{-1}\mathfrak{b}_s).$$

There are well-known algorithms to perform this task.[1]

Combining theorems (1.4) and (1.16), we see that deciding whether two semisimple integer matrices are similar is equivalent to a series of principal ideal tests, provided that $\mathcal{O} = \mathbb{Z}[\vartheta]$ is a maximal order. Since the best known algorithm for principal ideal testing has subexponential running time[2], testing similarity of semisimple integer matrices has to be considered a hard problem. As our earlier remarks suggest, there is little reason to be more optimistic in the nonmaximal case. The remainder of the first part of this work will deal with this situation.

1.4 Matrix Orders

In the previous section we saw how to decide whether two full modules are equivalent over a maximal order, namely by reducing the problem to a principal ideal test. We will now see that the problem is closely connected to a principal ideal test in general. For this we need to deal with orders of $\mathrm{M}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$. Such orders will be called **matrix orders**.

Let Λ be a matrix order. A subset of $\mathrm{M}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$ is called a **fractional right ideal** of Λ if it is a finitely generated right module over Λ. The term is defined accordingly for left or two-sided ideals. Fractional ideals are called **full** if they contain an element of $\mathrm{GL}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$.

Maximal matrix orders will be denoted by $\Lambda_{\boldsymbol{\mathcal{K}}}$. Unlike $\boldsymbol{\mathcal{K}}$, the algebra $\mathrm{M}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$ does not contain a unique maximal order. Instead, there are infinitely many, as we will see shortly.

If $\mathfrak{A}$ and $\mathfrak{B}$ are two full modules in $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$, the set

$$(\mathfrak{B} : \mathfrak{A}) = \{\, \varGamma \in \mathrm{M}(\boldsymbol{n}, \boldsymbol{\mathcal{K}}) \mid \varGamma\mathfrak{A} \subset \mathfrak{B} \,\}$$

is called the **multiplier ideal** of $\mathfrak{A}$ and $\mathfrak{B}$. Moreover, the set

$$\Lambda = (\mathfrak{A} : \mathfrak{A})$$

is called the **multiplier algebra** of $\mathfrak{A}$. Typically, the matrix orders we will encounter are given in this form.

(1.17) Proposition. With notations as above we observe the following.

(1) Λ is an order of $\mathrm{M}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$.

[1] For example, see Buchmann (1987).

[2] Cf. Cohen, Diaz y Diaz and Olivier (1997).

(2) $(\mathfrak{B} : \mathfrak{A})$ is a full fractional right ideal of Λ.

(3) The center of Λ is the multiplier ring of $\mathfrak{A}$.

(4) If $\mathfrak{A} \sim \mathfrak{B}$, their multiplier algebras are isomorphic.

Proof. (1) Obviously, Λ is a subalgebra of $\mathrm{M}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$ containing the identity matrix. Let

$$\pi_\iota \colon \boldsymbol{\mathcal{K}}^{\boldsymbol{n}} \to \mathcal{K}_\iota^{n_\iota} \quad \text{and} \quad \Pi_\iota \colon \mathrm{M}(\boldsymbol{n}, \boldsymbol{\mathcal{K}}) \to \mathrm{M}(n_\iota, \mathcal{K}_\iota)$$

be the canonical projections. Let $\mathfrak{A}_\iota = \pi_\iota(\mathfrak{A})$ and $\Lambda_\iota = \Pi_\iota(\Lambda)$. Then $\mathfrak{A}_\iota$ is a free $\mathbb{Z}$-module and

$$\Lambda_\iota \mathfrak{A}_\iota = \mathfrak{A}_\iota.$$

Replacing $\mathfrak{A}$ by $c\mathfrak{A}$ for some rational number c (which does not change the multiplier algebra), we may assume $\mathcal{O}_{\boldsymbol{\mathcal{K}}}^{\boldsymbol{n}} \subset \mathfrak{A}$, that is, $\mathfrak{A}_\iota$ contains the standard basis $e_1, \ldots, e_{n_\iota}$ of $\mathcal{K}_\iota^{n_\iota}$. Because of

$$\Lambda_\iota e_i \subset \Lambda_\iota \mathfrak{A}_\iota = \mathfrak{A}_\iota,$$

we see that $\Lambda_\iota e_\iota$ is a free $\mathbb{Z}$-module. Hence $\Lambda_\iota \subset \Lambda_\iota e_1 + \cdots + \Lambda_\iota e_{n_\iota}$ is free, and so is

$$\Lambda \subset \Lambda_1 \oplus \cdots \oplus \Lambda_s.$$

Let $\xi_1, \ldots, \xi_m$ be a $\mathbb{Z}$-basis of $\mathfrak{A}$ and $\mathit{\Gamma}_1, \ldots, \mathit{\Gamma}_d$ a $\mathbb{Q}$-basis of $\mathrm{M}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$. There are rational coefficients $x_{ij}^{(k)}$ such that

$$\mathit{\Gamma}_i \xi_k = \sum_j x_{ij}^{(k)} \xi_j.$$

Choose an integer λ such that $\lambda x_{ij}^{(k)} \in \mathbb{Z}$ for all i, j and k. Then

$$(\lambda \mathit{\Gamma}_i)\xi_k = \sum_j (\lambda x_{ij}^{(k)}) \xi_j \in \mathfrak{A} \quad \text{for all } i \text{ and } k,$$

that is, $\lambda \mathit{\Gamma}_1, \ldots, \lambda \mathit{\Gamma}_d \in \Lambda$. Therefore Λ is a free $\mathbb{Z}$-module of rank at least

$$d = \dim_{\mathbb{Q}} \mathrm{M}(\boldsymbol{n}, \boldsymbol{\mathcal{K}}).$$

Since Λ is a subset of $\mathrm{M}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$, its rank is exactly d, so Λ is an order of $\mathrm{M}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$.

(2) Clearly, $(\mathfrak{B} : \mathfrak{A})$ is a fractional right ideal of Λ. A slight modification of the previous arguments shows that $(\mathfrak{B} : \mathfrak{A})$ has full rank.

(3) Since Λ has full rank, its center lies in the center of $\mathrm{M}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$, so it can be identified with a subset of $\boldsymbol{\mathcal{K}}$. Therefore the center of Λ coincides with the multiplier ring of $\mathfrak{A}$.

(4) Let Λ' be the multiplier algebra of $\mathfrak{B}$ and suppose $\mathit{\Gamma} \in \mathrm{M}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$ satisfies $\mathit{\Gamma}\mathfrak{A} = \mathfrak{B}$. Then

$$\Lambda \to \Lambda', \quad X \mapsto \mathit{\Gamma} X \mathit{\Gamma}^{-1}$$

is an isomorphism. ■

Let us consider a first example of a multiplier algebra. If $\mathcal{O}$ is an order of a number field $\mathcal{K}$ and $\mathfrak{A} = \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n$ is a direct sum of ideals of $\mathcal{O}$, then its multiplier algebra is given by

$$\Lambda = \begin{bmatrix} (\mathfrak{a}_1 : \mathfrak{a}_1) & \cdots & (\mathfrak{a}_1 : \mathfrak{a}_n) \\ \vdots & \ddots & \vdots \\ (\mathfrak{a}_n : \mathfrak{a}_1) & \cdots & (\mathfrak{a}_n : \mathfrak{a}_n) \end{bmatrix},$$

that is, Λ consists of all matrices whose (i, j)-entries belong to $(\mathfrak{a}_i : \mathfrak{a}_j)$. Thus, if $\mathfrak{A}$ is an $\mathcal{O}_{\mathcal{K}}$-module of the form $\mathfrak{a} \oplus \mathcal{O}_{\mathcal{K}}^{n-1}$, the multiplier algebra is given by

$$\textbf{(1.18)} \qquad \Lambda_{\mathcal{K}} = \begin{bmatrix} \mathcal{O}_{\mathcal{K}} & \mathfrak{a} & \cdots & \mathfrak{a} \\ \mathfrak{a}^{-1} & \mathcal{O}_{\mathcal{K}} & \cdots & \mathcal{O}_{\mathcal{K}} \\ \vdots & \vdots & \ddots & \vdots \\ \mathfrak{a}^{-1} & \mathcal{O}_{\mathcal{K}} & \cdots & \mathcal{O}_{\mathcal{K}} \end{bmatrix}.$$

More generally, if

$$\mathfrak{A} = \bigoplus_{\iota=1}^{s} (\mathfrak{a}_\iota \oplus \mathcal{O}_{\mathcal{K}_\iota}^{n_\iota - 1}),$$

its multiplier algebra is a direct sum

$$\Lambda_{\boldsymbol{\mathcal{K}}} = \Lambda_{\mathcal{K}_1} \oplus \cdots \oplus \Lambda_{\mathcal{K}_s}$$

of several matrix algebras as specified above. The next theorem states that $\Lambda_{\boldsymbol{\mathcal{K}}}$ is indeed a maximal matrix order, as our notation already indicates. For the proof, see Reiner (1975), p. 189, theorem (21.6).

(1.19) Theorem. Let Λ be a matrix order. Then Λ is a maximal order if and only if it is the multiplier algebra of a full $\mathcal{O}_{\boldsymbol{\mathcal{K}}}$-module.

A maximal order as in (1.18) will be said to be of **standard form**. Notice that we obtain a different maximal order if $\mathfrak{a}$ is replaced by another ideal. Therefore $\mathrm{M}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$ contains infinitely many maximal orders.[1]

Theorem (1.19) states that every maximal matrix order is the multiplier algebra of a full $\mathcal{O}_{\boldsymbol{\mathcal{K}}}$-module $\mathfrak{A}$. Therefore, the center of $\Lambda_{\boldsymbol{\mathcal{K}}}$ is always $\mathcal{O}_{\boldsymbol{\mathcal{K}}}$. Since $\mathfrak{A}$ is equivalent to a module of the form $\bigoplus(\mathfrak{a}_\iota \oplus \mathcal{O}_{\mathcal{K}_\iota}^{n_\iota - 1})$, every maximal matrix order is isomorphic to an order $\bigoplus \Lambda_{\mathcal{K}_\iota}$ with components in standard form. Even more, as seen in the proof of (1.17), the isomorphism is given by a matrix $\Gamma \in \mathrm{GL}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$ which satisfies

$$\Gamma \mathfrak{A} = \bigoplus_{\iota=1}^{s} (\mathfrak{a}_\iota \oplus \mathcal{O}_{\mathcal{K}_\iota}^{n_\iota - 1}).$$

This observation will enable us to assume, without loss of generality, that every maximal matrix order is given in the simple form described above.

At the beginning of this section, we mentioned that our decision problem is connected to a principal ideal test. Suppose that $\mathfrak{A}$, $\mathfrak{B} \subset \boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$ are two full

[1] Unless $\boldsymbol{n} = (1, \ldots, 1)$, of course.

modules. If there is a matrix $\mathit{\Gamma} \in \mathrm{GL}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$ such that $\mathit{\Gamma}\mathfrak{A} = \mathfrak{B}$, it belongs to the multiplier ideal $\mathfrak{C} = (\mathfrak{B} : \mathfrak{A})$, and we observe that

$$\mathfrak{C}\mathfrak{A} = \mathfrak{B}$$

because $\mathfrak{B} = \mathit{\Gamma}\mathfrak{A} \subset \mathfrak{C}\mathfrak{A} \subset \mathfrak{B}$. Therefore it is reasonable to assume that $\mathfrak{C}$ satisfies the equation above. In this situation, $\mathfrak{A} \sim \mathfrak{B}$ is equivalent to $\mathfrak{C}$ being a principal ideal of $\Lambda = (\mathfrak{A} : \mathfrak{A})$.

(1.20) Proposition. Let $\mathfrak{A}$, $\mathfrak{B} \subset \boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$ be two full modules. Suppose $\mathfrak{C} = (\mathfrak{B} : \mathfrak{A})$ satisfies $\mathfrak{C}\mathfrak{A} = \mathfrak{B}$. Let $\Lambda = (\mathfrak{A} : \mathfrak{A})$ and $\mathit{\Gamma} \in \mathrm{GL}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$. Then

$$\mathit{\Gamma}\mathfrak{A} = \mathfrak{B} \quad \Leftrightarrow \quad \mathfrak{C} = \mathit{\Gamma}\Lambda.$$

Proof. Suppose $\mathit{\Gamma}\mathfrak{A} = \mathfrak{B}$. Then we have

$$\begin{aligned} C \in \mathfrak{C} \;\Leftrightarrow\; C\mathfrak{A} \subset \mathit{\Gamma}\mathfrak{A} \;\Leftrightarrow\; (\mathit{\Gamma}^{-1}C)\mathfrak{A} \subset \mathfrak{A} \\ \Leftrightarrow\; \mathit{\Gamma}^{-1}C \in \Lambda \;\Leftrightarrow\; C \in \mathit{\Gamma}\Lambda. \end{aligned}$$

Conversely, suppose $\mathfrak{C} = \mathit{\Gamma}\Lambda$. Then $\mathit{\Gamma}\mathfrak{A} = (\mathit{\Gamma}\Lambda)\mathfrak{A} = \mathfrak{C}\mathfrak{A} = \mathfrak{B}$. ∎

We are now left with the task of examining whether $\mathfrak{C}$ is a principal ideal of Λ. To decide this, we may first check if

$$\mathfrak{C}\Lambda_{\mathcal{K}} = \mathit{\Gamma}\Lambda_{\mathcal{K}}$$

where $\Lambda_{\mathcal{K}}$ is the multiplier algebra of the $\mathcal{O}_{\mathcal{K}}$-module $\mathfrak{A}_{\mathcal{K}} = \mathfrak{A}\mathcal{O}_{\mathcal{K}}$. This is a necessary condition since Λ is a subset of $\Lambda_{\mathcal{K}}$. The next proposition states that this weaker condition can be decided by checking whether $\mathfrak{A}_{\mathcal{K}} \sim \mathfrak{B}_{\mathcal{K}}$, using methods from the previous section. This is a nontrivial observation because the equality

$$\mathfrak{C}\Lambda_{\mathcal{K}} = (\mathfrak{B}_{\mathcal{K}} : \mathfrak{A}_{\mathcal{K}})$$

is not entirely obvious.

(1.21) Proposition. Let $\mathfrak{A}$, $\mathfrak{B} \subset \boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$ be two full modules. Suppose $\mathfrak{C} = (\mathfrak{B} : \mathfrak{A})$ satisfies $\mathfrak{C}\mathfrak{A} = \mathfrak{B}$. Let $\Lambda_{\mathcal{K}} = (\mathfrak{A}_{\mathcal{K}} : \mathfrak{A}_{\mathcal{K}})$ and suppose there is a $\mathit{\Gamma} \in \mathrm{GL}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$ such that $\mathit{\Gamma}\mathfrak{A}_{\mathcal{K}} = \mathfrak{B}_{\mathcal{K}}$. Then

$$\mathfrak{C}\Lambda_{\mathcal{K}} = \mathit{\Gamma}\Lambda_{\mathcal{K}}.$$

Proof. From $\mathfrak{C}\mathfrak{A} = \mathfrak{B}$ it follows that $\mathfrak{C}\mathfrak{A}_{\mathcal{K}} = \mathfrak{B}_{\mathcal{K}} = \mathit{\Gamma}\mathfrak{A}_{\mathcal{K}}$, so

$$(\mathit{\Gamma}^{-1}\mathfrak{C}\Lambda_{\mathcal{K}})\mathfrak{A}_{\mathcal{K}} = \mathit{\Gamma}^{-1}\mathfrak{C}\mathfrak{A}_{\mathcal{K}} = \mathfrak{A}_{\mathcal{K}},$$

and we may conclude $\mathit{\Gamma}^{-1}\mathfrak{C}\Lambda_{\mathcal{K}} = \Lambda_{\mathcal{K}}$ according to the following lemma. ∎

(1.22) Lemma. Let $\Lambda_{\mathcal{K}}$ be the multiplier algebra of a full $\mathcal{O}_{\mathcal{K}}$-module $\mathfrak{A}$ in $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$ and suppose $\mathfrak{C}$ is a full right ideal of $\Lambda_{\mathcal{K}}$ satisfying $\mathfrak{C}\mathfrak{A} = \mathfrak{A}$. Then $\mathfrak{C} = \Lambda_{\mathcal{K}}$.

Proof. Without loss of generality we may assume that $\boldsymbol{\mathcal{K}} = \mathcal{K}$ is a number field because, being $\mathcal{O}_{\boldsymbol{\mathcal{K}}}$-modules, $\mathfrak{A}$ and $\mathfrak{C}$ must be direct sums. Furthermore, we may assume that $\mathfrak{A}$ is given in the form

$$\mathfrak{A} = \mathfrak{a} \oplus \mathcal{O}_{\mathcal{K}}^{n-1},$$

so $\Lambda_{\mathcal{K}}$ is of the standard form (1.18). Let $e_1, \dots, e_n$ be the standard basis of $\mathcal{K}^n$ and $E_{11}, E_{12}, \dots, E_{nn}$ the standard basis of $\mathrm{M}(n, \mathcal{K})$. Since $e_2, \dots, e_n \in \mathfrak{A}$, the condition $\mathfrak{C}\mathfrak{A} = \mathfrak{A}$ implies the existence of elements $C_j \in \mathfrak{C}$ and $\xi_j \in \mathfrak{A}$ satisfying

$$\sum C_j \xi_j = e_i \quad \text{for } 2 \le i \le n.$$

Let $\varXi_{ij} = [\,0 \dots 0 \;\; \xi_j \;\; 0 \dots 0\,]$ be the matrix with ith column $(i > 1)$ equal to ξ_j. Then $\varXi_{ij}$ belongs to $\Lambda_{\mathcal{K}}$ and

$$\sum C_j \varXi_{ij} = [\,0 \dots 0 \;\; \sum C_j \xi_j \;\; 0 \dots 0\,] = [\,0 \dots 0 \;\; e_i \;\; 0 \dots 0\,] = E_{ii}.$$

Since $\mathfrak{C}$ is a right ideal of $\Lambda_{\mathcal{K}}$, we have

$$E_{ii} \in \mathfrak{C} \quad \text{for } 2 \le i \le n.$$

Moreover, we have elements $a_i \in \mathfrak{a}$ and $a_i' \in \mathfrak{a}^{-1}$ such that $\sum a_i\, a_i' = 1$, as well as elements $C_{ij} \in \mathfrak{C}$ and $\xi_{ij} \in \mathfrak{A}$ with

$$\sum_j C_{ij} \xi_{ij} = a_i e_1 \quad \text{for each } i.$$

If $\varXi_{ij} = [\,a_i' \xi_{ij} \;\; 0 \dots 0\,]$, then

$$E_{11} = \sum_i a_i a_i' E_{11} = \sum_i \sum_j C_{ij} \varXi_{ij} \in \mathfrak{C}.$$

In conclusion, $I = E_{11} + \cdots + E_{nn}$ belongs to $\mathfrak{C}$. Therefore $\mathfrak{C} = \Lambda_{\boldsymbol{\mathcal{K}}}$. ■

From now on we always may assume that our ideal $\mathfrak{C}$ satisfies $\mathfrak{C}\Lambda_{\boldsymbol{\mathcal{K}}} = \varGamma\Lambda_{\boldsymbol{\mathcal{K}}}$. The following proposition gives us a first idea why this is of advantage.

(1.23) Proposition. Let $\mathfrak{C}$ be a full right ideal of Λ such that $\mathfrak{C}\Lambda_{\boldsymbol{\mathcal{K}}} = \varGamma\Lambda_{\boldsymbol{\mathcal{K}}}$. The following statements are equivalent.

(1) $\mathfrak{C}$ is a principal ideal.

(2) There is a $U \in \Lambda_{\boldsymbol{\mathcal{K}}}^\times$ such that $\mathfrak{C} = \varGamma U \Lambda$.

If it exists, such a unit must be among any set of representatives for $\Lambda_{\boldsymbol{\mathcal{K}}}^\times / \Lambda^\times$.

Proof. Suppose $\mathfrak{C} = \varGamma' \Lambda$ for some $\varGamma' \in \Lambda$. Then

$$\varGamma' \Lambda_{\boldsymbol{\mathcal{K}}} = \mathfrak{C}\Lambda_{\boldsymbol{\mathcal{K}}} = \varGamma \Lambda_{\boldsymbol{\mathcal{K}}},$$

so $U = \varGamma^{-1}\varGamma' \in \Lambda_{\boldsymbol{\mathcal{K}}}^\times$ and $\mathfrak{C} = \varGamma'\Lambda = \varGamma U \Lambda$. The converse implication is trivial. To prove the additional statement, suppose there is another $U' \in \Lambda_{\boldsymbol{\mathcal{K}}}^\times$ which satisfies condition (2). Then

$$\begin{aligned} \varGamma U' \Lambda = \varGamma U \Lambda \quad &\Leftrightarrow \quad (U^{-1}U')\Lambda = \Lambda \\ &\Leftrightarrow \quad U^{-1}U' \in \Lambda^\times \\ &\Leftrightarrow \quad U' \in U\Lambda^\times. \end{aligned}$$

■

In general, $\Lambda_{\boldsymbol{\mathcal{K}}}^{\times}/\Lambda^{\times}$ is not a group, but, as we shall see later, it is a finite set. Therefore the question whether $\mathfrak{C}$ is principal is decidable.

1.5 Units of Matrix Orders

The main goal of this section is to prove the following statement.

(1.24) Proposition. If Λ is the multiplier algebra of a full module in $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$ and $\Lambda_{\boldsymbol{\mathcal{K}}}$ a maximal order above Λ, then

$$\Lambda^{\times} = \Lambda_{\boldsymbol{\mathcal{K}}}^{\times} \cap \Lambda.$$

While the inclusion $\Lambda^{\times} \subset \Lambda_{\boldsymbol{\mathcal{K}}}^{\times} \cap \Lambda$ is obvious, the converse direction requires a little more effort. First, we need to clarify some notations. If we regard $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$ as a vector space over $\mathbb{Q}$, the **norm** of $\mathit{\Gamma}$, denoted by $\mathrm{N}(\mathit{\Gamma})$, will be the determinant of the homomorphism

$$\boldsymbol{\mathcal{K}}^{\boldsymbol{n}} \to \boldsymbol{\mathcal{K}}^{\boldsymbol{n}}, \quad \xi \mapsto \mathit{\Gamma}\xi.$$

This defines a map

$$\mathrm{N}\colon \mathrm{M}(\boldsymbol{n}, \boldsymbol{\mathcal{K}}) \to \mathbb{Q}, \quad \mathit{\Gamma} \mapsto \mathrm{N}(\mathit{\Gamma}).$$

Moreover, we define the **determinant** of $\mathit{\Gamma} = \mathit{\Gamma}_1 \oplus \cdots \oplus \mathit{\Gamma}_s$ as its image under the map

$$\det\colon \mathrm{M}(\boldsymbol{n}, \boldsymbol{\mathcal{K}}) \to \boldsymbol{\mathcal{K}}, \quad \det(\mathit{\Gamma}) = \det(\mathit{\Gamma}_1) \oplus \cdots \oplus \det(\mathit{\Gamma}_s)$$

where each summand is the usual determinant of a matrix over a number field. If we identify a scalar $x \in \boldsymbol{\mathcal{K}}$ with a direct sum of 1×1 matrices, we can also speak of the **norm** of x and obtain the map

$$\mathrm{N}\colon \boldsymbol{\mathcal{K}} \to \mathbb{Q}, \quad x \mapsto \mathrm{N}(x).$$

Obviously, all these maps are multiplicative. Finally, a matrix $\mathit{\Gamma} \in \mathrm{M}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$ will be called **nonsingular** if each component $\mathit{\Gamma}_\iota$ has full rank.

(1.25) Proposition. If $\mathit{\Gamma} \in \mathrm{M}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$, we have $\mathrm{N}(\mathit{\Gamma}) = \mathrm{N}(\det \mathit{\Gamma})$.

Proof. The statement is clear if $\mathit{\Gamma}$ is singular. It is also verified easily if one $\mathit{\Gamma}_\iota$ is an elementary or diagonal matrix while $\mathit{\Gamma}_\nu = I$ for $\nu \neq \iota$. Since every nonsingular component $\mathit{\Gamma}_\iota$ is a product of elementary and diagonal matrices, this proves the lemma. ■

In the usual way for elements of an algebra, the characteristic polynomial of $\mathit{\Gamma}$ is defined as the characteristic polynomial of the homomorphism

$$\boldsymbol{\mathcal{K}}^{\boldsymbol{n}} \to \boldsymbol{\mathcal{K}}^{\boldsymbol{n}}, \quad \xi \mapsto \mathit{\Gamma}\xi.$$

Accordingly, $\mathit{\Gamma}$ is a root of its characteristic polynomial.

(1.26) Lemma. If $\mathit{\Gamma} \in \Lambda$, its characteristic polynomial belongs to $\mathbb{Z}[X]$.[1]

Proof. Since Λ is the multiplier algebra of a full module $\mathfrak{A}$, we have $\mathit{\Gamma}\mathfrak{A} \subset \mathfrak{A}$. If we choose a $\mathbb{Z}$-basis of $\mathfrak{A}$ as a $\mathbb{Q}$-basis of $\boldsymbol{\mathcal{K}^n}$, we see that the matrix of the homomorphism above is an integer matrix. ■

(1.27) Corollary. If $\mathit{\Gamma} \in \Lambda$, the norm of $\mathit{\Gamma}$ belongs to $\mathbb{Z}$.

Proof. Up to sign, the norm is equal to the constant term of the characteristic polynomial. ■

(1.28) Lemma. If $\mathit{\Gamma} \in \Lambda$, then $\mathit{\Gamma}$ is a unit of Λ if and only if $\mathrm{N}(\mathit{\Gamma}) = \pm 1$.

Proof. Suppose $\mathit{\Gamma}$ is nonsingular, which is necessary in either case. If $\mathit{\Gamma}$ is a unit of Λ, we observe

$$1 = \mathrm{N}(I) = \mathrm{N}(\mathit{\Gamma}\mathit{\Gamma}^{-1}) = \mathrm{N}(\mathit{\Gamma})\,\mathrm{N}(\mathit{\Gamma})^{-1},$$

so $\mathrm{N}(\mathit{\Gamma}) = \pm 1$ because the norm is an integer. For the other implication, let

$$\chi = X^n + a_1 X^{n-1} + \cdots + a_n$$

be the characteristic polynomial of $\mathit{\Gamma}$. Then each a_k is an integer and

$$\begin{aligned}\mathrm{N}(\mathit{\Gamma})\mathit{\Gamma}^{-1} = \pm a_n \mathit{\Gamma}^{-1} &= \mp(\chi(\mathit{\Gamma}) - a_n)\mathit{\Gamma}^{-1} \\ &= \mp(\mathit{\Gamma}^{n-1} + a_1\mathit{\Gamma}^{n-2} + \cdots + a_{n-1}) \in \Lambda.\end{aligned}$$

Since $\mathrm{N}(\mathit{\Gamma}) = \pm 1$, we see that $\mathit{\Gamma}^{-1} \in \Lambda$. ■

Now we can complete the proof of (1.24). If $\mathit{\Gamma} \in \Lambda_{\boldsymbol{\mathcal{K}}}^{\times} \cap \Lambda$, we have $\mathrm{N}(\mathit{\Gamma}) = \pm 1$ because it is a unit of $\Lambda_{\boldsymbol{\mathcal{K}}}$, but then it is already a unit of Λ by (1.28).

As an application we will obtain the theorem below. First notice the following: If $\mathit{\Gamma} \in \Lambda_{\boldsymbol{\mathcal{K}}}$, then

$$\det(\mathit{\Gamma}) \in \mathcal{O}_{\boldsymbol{\mathcal{K}}}.$$

Remember that $\Lambda_{\boldsymbol{\mathcal{K}}}$ is isomorphic to a matrix order where each component is of the standard form (1.18). For such an order, the assertion is clear. Since the isomorphism in the proof of (1.17) does not alter determinants, the statement is true in general.

(1.29) Theorem. Let Λ be the multiplier algebra of a full module in $\boldsymbol{\mathcal{K}^n}$ and let $\mathit{\Gamma} \in \Lambda$. Then

$$\mathit{\Gamma} \in \Lambda^{\times} \quad \Leftrightarrow \quad \det(\mathit{\Gamma}) \in \mathcal{O}_{\boldsymbol{\mathcal{K}}}^{\times}.$$

Proof. Since $\mathit{\Gamma}$ belongs to some maximal matrix order, we have $\det(\mathit{\Gamma}) \in \mathcal{O}_{\boldsymbol{\mathcal{K}}}$. The assertion now follows from (1.25) and (1.28) because the equality

$$\mathrm{N}(\mathit{\Gamma}) = \mathrm{N}(\det \mathit{\Gamma})$$

forbids that only one argument is a unit while the other is not. ■

[1] Results (1.26), (1.28) and (1.30) are based on statements by Borevich and Shafarevich (1966); cf. p. 89, lemma 2 and theorem 4, and p. 126, theorem 2.

At first glance, one might hope that the theorem could be revised to state the equivalence

$$\mathit{\Gamma} \in \Lambda^\times \;\Leftrightarrow\; \det(\mathit{\Gamma}) \in \mathcal{O}^\times$$

where $\mathcal{O}$ is the center of Λ, but in general this is not true. For example, suppose $\mathcal{O}$ is a nonmaximal order of a number field $\mathcal{K}$. Let $\mathfrak{f}$ be the conductor of $\mathcal{O} \subset \mathcal{O}_\mathcal{K}$. The multiplier algebra of the module $\mathfrak{f} \oplus \mathcal{O}$ is given by

$$\Lambda = \begin{bmatrix} \mathcal{O}_\mathcal{K} & \mathfrak{f} \\ (\mathcal{O} : \mathfrak{f}) & \mathcal{O} \end{bmatrix}.$$

Then $\mathcal{O}$ is the center of Λ and it does not contain all determinants of matrices in Λ.

The following results will be needed in chapter 4.

(1.30) Proposition. Let $\mathfrak{W}$ be a full module in $\mathcal{K}^n$ where $\mathcal{K}$ is a number field. Let $\mathfrak{A}$, $\mathfrak{B} \subset \mathfrak{W}$ be two $\mathbb{Z}$-modules with $\mathit{\Gamma}\mathfrak{A} = \mathfrak{B}$ for some $\mathit{\Gamma} \in \mathrm{GL}(n, \mathcal{K})$. Then

$$[\mathfrak{W} : \mathfrak{B}] = |\mathrm{N}(\mathit{\Gamma})| \cdot [\mathfrak{W} : \mathfrak{A}].$$

Proof. The assertion is clear if the index of $\mathfrak{A}$ and $\mathfrak{B}$ is infinite. Suppose both modules have finite index (a mixed case cannot occur since $\mathit{\Gamma}\mathfrak{A} = \mathfrak{B}$). If $\mathit{\Xi}$ is a $\mathbb{Z}$-basis of $\mathfrak{A}$, then $\mathit{\Gamma\Xi}$ is a $\mathbb{Z}$-basis of $\mathfrak{B}$. Since $\mathit{\Xi}$ and $\mathit{\Gamma\Xi}$ are both $\mathbb{Q}$-bases of $\mathcal{K}^n$, there is a rational matrix C such that

$$\mathit{\Gamma\Xi} = \mathit{\Xi} C.$$

By definition of the norm we have

$$\mathrm{N}(\mathit{\Gamma}) = \det(C).$$

Let $\mathit{\Upsilon}$ be a $\mathbb{Z}$-basis of $\mathfrak{W}$. Since $\mathfrak{W}$ contains $\mathfrak{A}$ and $\mathfrak{B}$, there are integer matrices A and B such that

$$\mathit{\Xi} = \mathit{\Upsilon} A \quad \text{and} \quad \mathit{\Gamma\Xi} = \mathit{\Upsilon} B.$$

Then we have the equalities $[\mathfrak{W} : \mathfrak{A}] = |\det A|$ and $[\mathfrak{W} : \mathfrak{B}] = |\det B|$. Because of

$$\mathit{\Upsilon} B = \mathit{\Gamma\Xi} = \mathit{\Xi} C = \mathit{\Upsilon} AC,$$

we see that $B = AC$. In conclusion,

$$[\mathfrak{W} : \mathfrak{B}] = |\det B| = |\det A| \cdot |\det C| = [\mathfrak{W} : \mathfrak{A}] \cdot |\mathrm{N}(\mathit{\Gamma})|. \qquad \blacksquare$$

(1.31) Corollary. Let $\mathfrak{W}$ be a full module in $\mathcal{K}^n$ where $\mathcal{K}$ is a number field. Let $\mathcal{O}$ be an order of $\mathcal{K}$ and suppose that $\mathfrak{A}$, $\mathfrak{B} \subset \mathfrak{W}$ are two free $\mathcal{O}$-modules. Let $X \in \mathrm{M}(n \times m, \mathcal{K})$ be a matrix of rank m and $U \in \mathrm{GL}(m, \mathcal{K})$ such that $\mathfrak{A} = X\mathcal{O}^m$ and $\mathfrak{B} = XU\mathcal{O}^m$. Then

$$[\mathfrak{W} : \mathfrak{B}] = |\mathrm{N}(U)| \cdot [\mathfrak{W} : \mathfrak{A}].$$

Proof. If $m < n$, the statement is clear, so assume $m = n$ ($m > n$ is impossible by our assumption about X). Let $\mathit{\Gamma} = XUX^{-1}$. Then

$$\mathfrak{B} = XU\mathcal{O}^n = \mathit{\Gamma} X\mathcal{O}^n = \mathit{\Gamma}\mathfrak{A}.$$

The previous proposition yields $[\mathfrak{W} : \mathfrak{B}] = |\mathrm{N}(\mathit{\Gamma})| \cdot [\mathfrak{W} : \mathfrak{A}]$ and by (1.25) we have

$$\mathrm{N}(\mathit{\Gamma}) = \mathrm{N}(\det \mathit{\Gamma}) = \mathrm{N}(\det XUX^{-1}) = \mathrm{N}(\det U) = \mathrm{N}(U). \qquad \blacksquare$$

1.6 The Conductor

As in the previous section, let $\mathfrak{C} = (\mathfrak{B} : \mathfrak{A})$ be the multiplier ideal of two full modules in $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$. This is a right ideal of the multiplier algebra $\Lambda = (\mathfrak{A} : \mathfrak{A})$. Let $\mathcal{O}$ denote the center of Λ. Our goal is to decide whether $\mathfrak{C}$ is a principal ideal and we assume that we already know that $\mathfrak{C}\Lambda_{\boldsymbol{\mathcal{K}}} = \mathit{\Gamma}\Lambda_{\boldsymbol{\mathcal{K}}}$ where $\Lambda_{\boldsymbol{\mathcal{K}}} \supset \Lambda$ is the multiplier algebra of $\mathfrak{A}_{\boldsymbol{\mathcal{K}}} = \mathfrak{A}\mathcal{O}_{\boldsymbol{\mathcal{K}}}$. In section 1.4 we saw that we need to look for a $U \in \Lambda_{\boldsymbol{\mathcal{K}}}^{\times}$ such that $\mathfrak{C} = (\mathit{\Gamma} U)\Lambda$, and we may restrict our search to a set of representatives of $\Lambda_{\boldsymbol{\mathcal{K}}}^{\times}/\Lambda^{\times}$. As mentioned before, this is a finite set, and to prove this, we will use the **conductor** $\mathfrak{F}$ of the extension $\Lambda \subset \Lambda_{\boldsymbol{\mathcal{K}}}$. It is defined, as for orders of $\boldsymbol{\mathcal{K}}$, as the largest two-sided ideal of $\Lambda_{\boldsymbol{\mathcal{K}}}$ contained in Λ, that is,

$$\mathfrak{F} = \{\, X \in \mathrm{M}(\boldsymbol{n}, \boldsymbol{\mathcal{K}}) \mid \Lambda_{\boldsymbol{\mathcal{K}}} X \Lambda_{\boldsymbol{\mathcal{K}}} \subset \Lambda \,\}.$$

The conductor is a full ideal of Λ and $\Lambda_{\boldsymbol{\mathcal{K}}}$ because $f\Lambda_{\boldsymbol{\mathcal{K}}} \subset \Lambda$ for some positive integer f. Moreover, we have the equality

$$\mathfrak{F} = \mathfrak{f}\Lambda_{\boldsymbol{\mathcal{K}}}$$

where $\mathfrak{f}$ is the conductor of $\mathcal{O} \subset \mathcal{O}_{\boldsymbol{\mathcal{K}}}$. This is, in part, a consequence of the next proposition.

(1.32) Proposition. All fractional two-sided ideals of $\Lambda_{\boldsymbol{\mathcal{K}}}$ are of the form $\mathfrak{c}\Lambda_{\boldsymbol{\mathcal{K}}}$ where $\mathfrak{c}$ is a fractional ideal of $\mathcal{O}_{\boldsymbol{\mathcal{K}}}$.

Proof. It suffices to consider the case where $\boldsymbol{\mathcal{K}} = \mathcal{K}$ is a number field and where $\Lambda_{\mathcal{K}}$ is of the standard form (1.18), that is, $\Lambda_{\mathcal{K}}$ is the multiplier algebra of $\mathfrak{a} \oplus \mathcal{O}_{\mathcal{K}}^{n-1}$ for some ideal $\mathfrak{a}$. Moreover, it suffices to examine ideals contained in $\Lambda_{\boldsymbol{\mathcal{K}}}$. Let $\mathfrak{C}$ be a two-sided ideal and let $\mathfrak{c}$ be the ideal of $\mathcal{O}_{\mathcal{K}}$ consisting of all $(1,1)$-entries of matrices in $\mathfrak{C}$, that is, $\mathfrak{c}$ is given by the equation

$$\mathfrak{c}E_{11} = E_{11}\mathfrak{C}E_{11}.$$

Here, E_{ij} denotes the matrix with 1 at position (i,j) and zeros elsewhere. For any matrix $C = [c_{ij}]$ in $\mathrm{M}(n, \mathcal{K})$ and for a, $a' \in \mathcal{K}$ we have

$$(aE_{ij})C(a'E_{k\ell}) = (aa'c_{jk})E_{i\ell}.$$

If $C \in \mathfrak{C}$ and aE_{1j}, $a'E_{k1} \in \Lambda_{\mathcal{K}}$, we therefore see that $(aa'c_{jk})E_{11} \in \mathfrak{C}$, that is,

$$aa'c_{jk} \in \mathfrak{c}.$$

Choosing a and a' to be 1 where possible and arbitrarily in $\mathfrak{a}$ and $\mathfrak{a}^{-1}$ otherwise, we obtain

$$c_{jk} \in \begin{cases} \mathfrak{c} & \text{if } j = 1,\ k = 1, \\ \mathfrak{ca} & \text{if } j = 1,\ k > 1, \\ \mathfrak{ca}^{-1} & \text{if } j > 1,\ k = 1. \end{cases}$$

Moreover, if j, $k > 1$, we may choose $a_1, \ldots, a_r \in \mathfrak{a}$ and $a'_1, \ldots, a'_r \in \mathfrak{a}^{-1}$ with $\sum a_i a'_i = 1$. Then

$$c_{jk}E_{11} = \sum (a_i a'_i c_{jk})E_{11} \in \mathfrak{C},$$

so again $c_{jk} \in \mathfrak{c}$. In conclusion, $\mathfrak{C} \subset \mathfrak{c}\Lambda_{\mathcal{K}}$. Conversely, suppose that $c \in \mathfrak{c}$ and let $C = [c_{ij}]$ be a matrix in $\mathfrak{C}$ with $c_{11} = c$. Then we observe that

$$(aa'c)E_{i\ell} = (a'E_{i1})C(aE_{1\ell}) \in \mathfrak{C}.$$

Arguing as above, we obtain

$$\mathfrak{c}E_{i\ell} \subset \mathfrak{C}, \quad \mathfrak{a}\mathfrak{c}E_{1\ell} \subset \mathfrak{C} \quad \text{and} \quad \mathfrak{a}^{-1}\mathfrak{c}E_{i1} \subset \mathfrak{C}$$

with indices chosen suitably. In summary, $\mathfrak{c}\Lambda_{\mathcal{K}} \subset \mathfrak{C}$. ■

(1.33) Corollary. Let $\mathfrak{F}$ be the conductor of $\Lambda \subset \Lambda_{\mathcal{K}}$ and $\mathfrak{f}$ the conductor of $\mathcal{O} \subset \mathcal{O}_{\mathcal{K}}$ where $\mathcal{O}$ is the center of Λ. Then

$$\mathfrak{F} = \mathfrak{f}\Lambda_{\mathcal{K}}.$$

Proof. Again, Λ is assumed to be the multiplier algebra of a full module $\mathfrak{A}$, so $\mathcal{O}$ is the multiplier ring of $\mathfrak{A}$. Because of

$$(\mathfrak{f}\Lambda_{\mathcal{K}})\mathfrak{A} = (\mathfrak{f}\Lambda_{\mathcal{K}}\mathcal{O}_{\mathcal{K}})\mathfrak{A} = (\mathfrak{f}\Lambda_{\mathcal{K}})\mathfrak{A}_{\mathcal{K}} = \mathfrak{f}\mathfrak{A}_{\mathcal{K}} = (\mathfrak{f}\mathcal{O}_{\mathcal{K}})\mathfrak{A} = \mathfrak{f}\mathfrak{A} \subset \mathcal{O}\mathfrak{A} = \mathfrak{A},$$

we have $\mathfrak{f}\Lambda_{\mathcal{K}} \subset \Lambda$. Since $\mathfrak{F}$ is the largest two-sided ideal of $\Lambda_{\mathcal{K}}$ inside Λ, we obtain $\mathfrak{f}\Lambda_{\mathcal{K}} \subset \mathfrak{F}$.
By (1.32) we know that $\mathfrak{F}$ is of the form $\mathfrak{f}'\Lambda_{\mathcal{K}}$ for some ideal $\mathfrak{f}'$ of $\mathcal{O}_{\mathcal{K}}$. Since $\mathfrak{F} \subset \Lambda$, this ideal must be contained in the center $\mathcal{O}$. This implies $\mathfrak{f}' \subset \mathfrak{f}$ because $\mathfrak{f}$ is the largest ideal of $\mathcal{O}_{\mathcal{K}}$ inside $\mathcal{O}$. In conclusion, $\mathfrak{F} \subset \mathfrak{f}\Lambda_{\mathcal{K}}$. ■

The following corollary and the subsequent lemma will be needed in the next chapter.

(1.34) Corollary. Let $C = [c_{ij}]$ be a matrix of $\mathrm{M}(n, \mathcal{K})$ where $\mathcal{K}$ is a number field. Let $\Lambda_{\mathcal{K}}$ be of the standard form (1.18). If $\mathfrak{c}$ is the fractional ideal of $\mathcal{O}_{\mathcal{K}}$ satisfying $\mathfrak{c}\Lambda_{\mathcal{K}} = \Lambda_{\mathcal{K}}C\Lambda_{\mathcal{K}}$, then

$$\mathfrak{c} = c_{11}\mathcal{O}_{\mathcal{K}} + \sum_{i,j>1} c_{ij}\mathcal{O}_{\mathcal{K}} + \sum_{i>1} c_{i1}\mathfrak{a} + \sum_{j>1} c_{1j}\mathfrak{a}^{-1}.$$

Proof. As we have seen in the proof of (1.32), $\mathfrak{c}$ consists of all $(1,1)$-entries of matrices in $\mathfrak{C} = \Lambda_{\mathcal{K}}C\Lambda_{\mathcal{K}}$. Over $\mathcal{O}_{\mathcal{K}}$, a set of generators of $\mathfrak{C}$ is given by the matrices

$$(aa'c_{jk})E_{i\ell} = (aE_{ij})C(a'E_{k\ell})$$

where a and a' are chosen suitably in $\mathfrak{a}$, $\mathfrak{a}^{-1}$ or $\mathcal{O}_{\mathcal{K}}$. Therefore $\mathfrak{c}$ is generated by the elements

$$c_{11},\ ac_{j1},\ a'c_{1k},\ aa'c_{jk} \quad (a \in \mathfrak{a},\ a' \in \mathfrak{a}^{-1},\ j, k > 1),$$

so the ideal is of the desired form. ■

(1.35) Lemma. Let C, C' be matrices in $\Lambda_{\mathcal{K}}$ and let $\mathfrak{q}$ be a full ideal of $\mathcal{O}_{\mathcal{K}}$. If $C \equiv C' \bmod \mathfrak{q}\Lambda_{\mathcal{K}}$, then

$$\det(C) \equiv \det(C') \mod \mathfrak{q}.$$

Proof. Again, it suffices to consider the situation where $\boldsymbol{\mathcal{K}} = \mathcal{K}$ is a number field and $\Lambda_{\mathcal{K}}$ is of the standard form (1.18), that is, $\Lambda_{\mathcal{K}}$ is the multiplier algebra of $\mathfrak{a} \oplus \mathcal{O}_{\mathcal{K}}^{n-1}$ for some ideal $\mathfrak{a}$. If $C = [c_{ij}]$ and $C' = [c'_{ij}]$, we have

$$c_{ij},\, c'_{ij} \in \begin{cases} \mathfrak{a} & \text{if } i = 1,\ j > 1, \\ \mathfrak{a}^{-1} & \text{if } i > 1,\ j = 1, \\ \mathcal{O}_{\mathcal{K}} & \text{otherwise.} \end{cases}$$

The assumption $C \equiv C' \bmod \mathfrak{q}\Lambda_{\boldsymbol{\mathcal{K}}}$ implies $c_{ij} = c'_{ij} + q_{ij}$ where

$$q_{ij} \in \begin{cases} \mathfrak{q}\mathfrak{a} & \text{if } i = 1,\ j > 1, \\ \mathfrak{q}\mathfrak{a}^{-1} & \text{if } i > 1,\ j = 1, \\ \mathfrak{q} & \text{otherwise.} \end{cases}$$

Let C_i and C'_i be the matrices that emerge if we remove the ith row and the first column of C and C'. The determinants of C_i and C'_i belong to $\mathcal{O}_{\mathcal{K}}$ and are subject to the following congruences:

$$\begin{aligned} \det(C_1) &\equiv \det(C'_1) && \bmod \mathfrak{q}, \\ \det(C_i) &\equiv \det(C'_i) && \bmod \mathfrak{q}\mathfrak{a} \quad \text{if } i > 1, \\ \det(C_i) &\equiv \det(C'_i) \equiv 0 && \bmod \mathfrak{a} \quad \text{if } i > 1. \end{aligned}$$

This is true for 2×2 matrices, and the inductive step uses Laplace expansion similar to the calculation below. Hence we can write

$$\det(C_i) = \det(C'_i) + q_i \qquad \text{where } q_1 \in \mathfrak{q} \text{ and } q_2, \ldots, q_n \in \mathfrak{q}\mathfrak{a}.$$

Expanding the determinant of C along the first column, we obtain

$$\begin{aligned} \det(C) &= \sum_{i=1}^{n} (-1)^{i+1} c_{i1} \det(C_i) \\ &= \sum_{i=1}^{n} (-1)^{i+1} (c'_{i1} + q_{i1})(\det(C'_i) + q_i) \\ &= \det(C') + \sum_{i=1}^{n} (-1)^{i+1} (q_i c'_{i1} + q_i q_{i1} + q_{i1} \det(C'_i)) \\ &\equiv \det(C') \quad \bmod \mathfrak{q} \end{aligned}$$

because $q_i c'_{i1}$, $q_i q_{i1}$ and $q_{i1} \det(C'_i)$ all belong to $\mathfrak{q}$. ■

We will now see that the set $\Lambda_{\boldsymbol{\mathcal{K}}}^{\times}/\Lambda^{\times}$ is finite, as there is an embedding into $(\Lambda/\mathfrak{F})^{\times}\backslash(\Lambda_{\boldsymbol{\mathcal{K}}}/\mathfrak{F})^{\times}$. In the proof of theorem (1.39) we will see why it is necessary to switch from left to right cosets (and also why to take inverses as specified below).

(1.36) Proposition. The map

$$\Lambda_{\boldsymbol{\mathcal{K}}}^{\times}/\Lambda^{\times} \to (\Lambda/\mathfrak{F})^{\times}\backslash(\Lambda_{\boldsymbol{\mathcal{K}}}/\mathfrak{F})^{\times}, \quad [U] \mapsto [U^{-1} + \mathfrak{F}]$$

is injective.

Proof. Suppose

$$[U^{-1} + \mathfrak{F}] = [V^{-1} + \mathfrak{F}] \quad \text{for } U,\, V \in \Lambda_{\mathcal{K}}^{\times}.$$

Then there is a residue class $(E + \mathfrak{F}) \in (\Lambda/\mathfrak{F})^{\times}$ such that

$$(U^{-1} + \mathfrak{F}) = (E + \mathfrak{F})(V^{-1} + \mathfrak{F}).$$

Hence $(U^{-1}V + \mathfrak{F}) = (E + \mathfrak{F})$, which implies

$$U^{-1}V \in (E + \mathfrak{F}) \subset \Lambda.$$

Therefore $U^{-1}V$ belongs to $\Lambda \cap \Lambda_{\mathcal{K}}^{\times} = \Lambda^{\times}$, where the equality is due to (1.24). This proves our assertion because

$$U^{-1}V \in \Lambda^{\times} \quad \Leftrightarrow \quad V \in U\Lambda^{\times} \quad \Leftrightarrow \quad [V] = [U]. \qquad \blacksquare$$

Theoretically, we can now search $\Lambda_{\mathcal{K}}^{\times}/\Lambda^{\times}$ in a finite number of steps to decide whether it contains a coset represented by a matrix as in (1.23). Yet in practice, it is quite likely that determining a complete set of representatives is anything but easy. First of all, $\Lambda_{\mathcal{K}}^{\times}/\Lambda^{\times}$ is not a group in general; just think of the usual matrix groups over $\mathcal{O}$ and $\mathcal{O}_{\mathcal{K}}$ where $\mathcal{K}$ is a number field. Therefore it should be no surprise if some difficulties arise. Besides, we need sufficient information about $\Lambda^{\times}$ and $\Lambda_{\mathcal{K}}^{\times}$ to begin with; sets of generators for instance. But even for $\mathrm{GL}(n, \mathcal{O})$ it is unknown in general how to determine a finite set of generators.[1] In our setting, we can at least assume that each component of $\Lambda_{\mathcal{K}}$ is given in the standard form (1.18). But no such assumption can be made about Λ. As we will see in the next section, Λ does not have to be a direct sum $\Lambda_1 \oplus \cdots \oplus \Lambda_s$. Even if it is, not much can be said about the individual components. We know that Λ_ι is the multiplier algebra of a full module $\mathfrak{A}_\iota$, yet this module does not have to be equivalent to a direct sum of ideals; again, see the next section for an example. In this unfortunate case, it is not even clear which, if any, elementary matrices belong to Λ_ι. But when it comes to matrix groups, these are the elements one typically would wish to include in a set of generators.

Given all these obstacles, we will make use of the injection (1.36) and will examine $(\Lambda/\mathfrak{F})^{\times}\backslash(\Lambda_{\mathcal{K}}/\mathfrak{F})^{\times}$ instead. This has the advantage that the individual groups are finite. In chapter 3 we will describe the group $(\Lambda_{\mathcal{K}}/\mathfrak{F})^{\times}$ as well as the image of the canonical homomorphism

$$\Lambda_{\mathcal{K}}^{\times} \to (\Lambda_{\mathcal{K}}/\mathfrak{F})^{\times}.$$

Additionally, we will explain how to compute preimages under this map. Unfortunately, just like $\Lambda^{\times}$, the group $(\Lambda/\mathfrak{F})^{\times}$ appears to elude an explicit description. So the only strategy on offer seems to be searching $(\Lambda_{\mathcal{K}}/\mathfrak{F})^{\times}$ directly.

We will conclude this section by improving the statement of (1.23), provided that the ideal $\mathfrak{C}$ is coprime to the conductor, that is, $\mathfrak{C} + \mathfrak{F} = \Lambda$. In the next chapter we will argue that this condition can always be met or else $\mathfrak{C}$ cannot be principal.

[1] Swan (1971) and Vaseršteĭn (1972) solved this problem for maximal orders and Liehl (1981) dealt with a class of nonmaximal orders.

(1.37) Lemma. If $\mathfrak{C} \subset \mathfrak{D}$ are fractional right ideals of Λ, then

$$\mathfrak{D} \cap (\mathfrak{C} + \mathfrak{F}) = \mathfrak{C} + (\mathfrak{D} \cap \mathfrak{F}).$$

Proof. If $C \in \mathfrak{C}$ and $F \in \mathfrak{F}$ with $C + F \in \mathfrak{D}$, then F belongs to $\mathfrak{D}$ because C already does. Hence $C + F \in \mathfrak{C} + (\mathfrak{D} \cap \mathfrak{F})$, that is, $\mathfrak{D} \cap (\mathfrak{C} + \mathfrak{F}) \subset \mathfrak{C} + (\mathfrak{D} \cap \mathfrak{F})$. Conversely, $\mathfrak{C}$ and $\mathfrak{D} \cap \mathfrak{F}$ both lie in $\mathfrak{D} \cap (\mathfrak{C} + \mathfrak{F})$, so the same is true for their sum. ■

(1.38) Lemma. If $\mathfrak{C} + \mathfrak{F} = \Lambda$ and $\mathfrak{C}\Lambda_{\mathcal{K}} = \mathit{\Gamma}\Lambda_{\mathcal{K}}$ for some $\mathit{\Gamma} \in \mathrm{GL}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$, then

$$\mathfrak{C} = \mathfrak{C}\Lambda_{\mathcal{K}} \cap \Lambda.$$

Proof. First we prove that

$$\mathfrak{C}\mathfrak{F} = \mathfrak{C}\Lambda_{\mathcal{K}} \cap \mathfrak{F}.$$

The inclusion $\mathfrak{C}\mathfrak{F} \subset \mathfrak{C}\Lambda_{\mathcal{K}} \cap \mathfrak{F}$ is trivial. Since $\mathfrak{C}\Lambda_{\mathcal{K}} = \mathit{\Gamma}\Lambda_{\mathcal{K}}$, any element of $\mathfrak{C}\Lambda_{\mathcal{K}}$ is of the form $\mathit{\Gamma} X$ with $X \in \Lambda_{\mathcal{K}}$. Let $\mathit{\Gamma} X$ belong to $\mathfrak{C}\Lambda_{\mathcal{K}} \cap \mathfrak{F}$. In particular, we have

$$\mathit{\Gamma} X \equiv 0 \mod \mathfrak{F}.$$

Because of

$$\mathit{\Gamma}\Lambda_{\mathcal{K}} + \mathfrak{F} = \mathfrak{C}\Lambda_{\mathcal{K}} + \mathfrak{F} = (\mathfrak{C} + \mathfrak{F})\Lambda_{\mathcal{K}} = \Lambda_{\mathcal{K}},$$

we see that $\mathit{\Gamma}$ is a unit modulo $\mathfrak{F}$. Consequently, $X \equiv 0 \bmod \mathfrak{F}$, so

$$\mathit{\Gamma} X \in \mathit{\Gamma}\mathfrak{F} = (\mathit{\Gamma}\Lambda_{\mathcal{K}})\mathfrak{F} = (\mathfrak{C}\Lambda_{\mathcal{K}})\mathfrak{F} = \mathfrak{C}\mathfrak{F}.$$

Using (1.37) and the just established equality, we obtain

$$\mathfrak{C}\Lambda_{\mathcal{K}} \cap \Lambda = \mathfrak{C}\Lambda_{\mathcal{K}} \cap (\mathfrak{C} + \mathfrak{F}) = \mathfrak{C} + (\mathfrak{C}\Lambda_{\mathcal{K}} \cap \mathfrak{F}) = \mathfrak{C} + \mathfrak{C}\mathfrak{F} = \mathfrak{C}. \qquad ■$$

(1.39) Theorem. Let $\mathfrak{C}$ be a full right ideal of Λ such that $\mathfrak{C} + \mathfrak{F} = \Lambda$ and $\mathfrak{C}\Lambda_{\mathcal{K}} = \mathit{\Gamma}\Lambda_{\mathcal{K}}$. Let $[\mathit{\Gamma} + \mathfrak{F}]$ denote the right coset of $\mathit{\Gamma} + \mathfrak{F}$ in $(\Lambda/\mathfrak{F})^\times \backslash (\Lambda_{\mathcal{K}}/\mathfrak{F})^\times$. The following statements are equivalent.

(1) $\mathfrak{C}$ is a principal ideal.

(2) There is a $U \in \Lambda_{\mathcal{K}}^\times$ such that $[\mathit{\Gamma} + \mathfrak{F}] = [U^{-1} + \mathfrak{F}]$.

If such a unit exists, then $\mathfrak{C} = \mathit{\Gamma} U \Lambda$.

Proof. Let $\mathfrak{C}$ be principal. By (1.23) there is a $U \in \Lambda_{\mathcal{K}}^\times$ such that $\mathfrak{C} = \mathit{\Gamma} U \Lambda$. Furthermore, $(\mathit{\Gamma} U + \mathfrak{F})$ belongs to $(\Lambda/\mathfrak{F})^\times$ because

$$\mathit{\Gamma} U \Lambda + \mathfrak{F} = \mathfrak{C} + \mathfrak{F} = \Lambda.$$

Hence $(\mathit{\Gamma} + \mathfrak{F}) = (\mathit{\Gamma} U + \mathfrak{F})(U^{-1} + \mathfrak{F})$, implying $[\mathit{\Gamma} + \mathfrak{F}] = [U^{-1} + \mathfrak{F}]$. Conversely, suppose $[\mathit{\Gamma} + \mathfrak{F}] = [U^{-1} + \mathfrak{F}]$, that is,

$$(\mathit{\Gamma} + \mathfrak{F}) = (E + \mathfrak{F})(U^{-1} + \mathfrak{F}) \quad \text{for some } (E + \mathfrak{F}) \in (\Lambda/\mathfrak{F})^\times.$$

Then $(\mathit{\Gamma} U + \mathfrak{F}) \in (\Lambda/\mathfrak{F})^\times$, so $\mathit{\Gamma} U \Lambda + \mathfrak{F} = \Lambda$. Applying (1.38) twice, we obtain

$$\mathfrak{C} = \mathfrak{C}\Lambda_{\mathcal{K}} \cap \Lambda = \mathit{\Gamma}\Lambda_{\mathcal{K}} \cap \Lambda = \mathit{\Gamma} U \Lambda_{\mathcal{K}} \cap \Lambda = (\mathit{\Gamma} U \Lambda)\Lambda_{\mathcal{K}} \cap \Lambda = \mathit{\Gamma} U \Lambda. \qquad ■$$

If compared to (1.23), the improvement of theorem (1.39) above may appear to be a minor one. But in chapter 3 we will see that it can have major consequences. For now, just consider the case where $\mathfrak{C} = \mathfrak{c}$ is a fractional ideal of an order $\mathcal{O}$. If $\mathfrak{c} + \mathfrak{f} = \mathcal{O}$ and $\mathfrak{c}\mathcal{O}_{\boldsymbol{\mathcal{K}}} = \gamma\mathcal{O}_{\boldsymbol{\mathcal{K}}}$, the theorem states that $\mathfrak{c}$ is principal if and only if the coset $[\gamma + \mathfrak{f}]$, which is also a left coset, belongs to the image of

$$\mathcal{O}_{\boldsymbol{\mathcal{K}}}^{\times} \to (\mathcal{O}_{\boldsymbol{\mathcal{K}}}/\mathfrak{f})^{\times}/(\mathcal{O}/\mathfrak{f})^{\times}.$$

Since all groups involved are abelian, we will be able to actually compute the image. In good cases it will also be possible to reduce the general problem to this abelian situation.

1.7 Some Remarks on the Number of Module Classes

In section 1.3 we saw that each full module over a maximal order is equivalent to a direct sum $\mathfrak{A}_1 \oplus \cdots \oplus \mathfrak{A}_s$ where $\mathfrak{A}_\iota$ is of the form $\mathfrak{a}_\iota \oplus \mathcal{O}_{\mathcal{K}_\iota}^{n_\iota - 1}$. This yields the following result.

(1.40) Proposition. Let h_ι be the class number of $\mathcal{K}_\iota$. Then $h_1 \cdots h_s$ is the number of classes of full $\mathcal{O}_{\boldsymbol{\mathcal{K}}}$-modules in $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$.

As a consequence of (1.40), there are integer matrices with the same (generalized) Jordan normal form over the rational field which are not similar over the integers. For example, suppose $\mathcal{K} = \mathbb{Q}(\vartheta)$ is a number field of class number $h > 1$ such that $\mathcal{O}_{\mathcal{K}} = \mathbb{Z}[\vartheta]$ (think of the case $\vartheta = \sqrt{-5}$). Let $\mathfrak{a}$ and $\mathfrak{b}$ be two ideals of $\mathcal{O}_{\mathcal{K}}$ which are not equivalent. Furthermore, let

$$\mu = X^d + c_{d-1}X^{d-1} + \ldots c_1 X + c_0$$

be the minimal polynomial of ϑ. If A and B are two integer matrices corresponding to $\mathfrak{a}$ and $\mathfrak{b}$, then they cannot be similar over the integers by (1.4). Moreover, μ has to be the minimal and characteristic polynomial of A and B. So over the rational numbers, A and B are both similar to the matrix

$$J = \begin{bmatrix} 0 & \cdots & 0 & -c_0 \\ 1 & & 0 & -c_1 \\ & \ddots & & \vdots \\ 0 & & 1 & -c_{d-1} \end{bmatrix},$$

the so-called companion matrix of μ.

We now want to focus on the number of module classes in the nonmaximal case.

(1.41) Proposition. Let $\mathcal{O}$ be an order of $\boldsymbol{\mathcal{K}}$. Let $\mathcal{O}_\iota$ be the image of $\mathcal{O}$ under the projection $\boldsymbol{\mathcal{K}} \to \mathcal{K}_\iota$ and let h_ι be the number of classes of full $\mathcal{O}_\iota$-modules in $\mathcal{K}_\iota^{n_\iota}$. Then the number of classes of full $\mathcal{O}$-modules in $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$ is at least $h_1 \cdots h_s$ and both values are equal if and only if $\mathcal{O} = \mathcal{O}_1 \oplus \cdots \oplus \mathcal{O}_s$.

Proof. Let $\mathfrak{A}_\iota$ be a full $\mathcal{O}_\iota$-module for each ι. Then $\mathfrak{A} = \mathfrak{A}_1 \oplus \cdots \oplus \mathfrak{A}_s$ is a full $\mathcal{O}$-module, and it can only be equivalent to another direct sum because

$$\mathit{\Gamma}\mathfrak{A} = (\mathit{\Gamma}_1\mathfrak{A}_1) \oplus \cdots \oplus (\mathit{\Gamma}_s\mathfrak{A}_s) \quad \text{for } \mathit{\Gamma} \in \mathrm{GL}(\boldsymbol{n}, \boldsymbol{\mathcal{K}}).$$

Moreover, $\mathfrak{A} \sim \mathfrak{B}$ if and only if $\mathfrak{A}_\iota \sim \mathfrak{B}_\iota$. Thus the number of module classes is at least $h_1 \cdots h_s$.

Suppose $\mathcal{O} = \mathcal{O}_1 \oplus \cdots \oplus \mathcal{O}_s$. Then each $\mathcal{O}$-module is a direct sum as described above (with $\mathfrak{A}_\iota = 1_\iota\mathfrak{A}$ where 1_ι is the unit element of $\mathcal{O}_\iota$). Hence the number of module classes is equal to $h_1 \cdots h_s$.

Now suppose $\mathcal{O} \neq \mathcal{O}_1 \oplus \cdots \oplus \mathcal{O}_s$ and let

$$\begin{bmatrix} x_{11} & & \\ \vdots & \ddots & \\ x_{s1} & \cdots & x_{ss} \end{bmatrix} \qquad (x_{\nu\iota} \text{ row vector of length } d_\iota = [\mathcal{K}_\iota : \mathbb{Q}])$$

be a matrix whose columns are a $\mathbb{Z}$-basis of $\mathcal{O}$.[1] Then at least one $x_{\nu\iota}$ is nonzero for $\nu > \iota$. We expand this matrix to the form

$$\mathit{\Xi} = \begin{bmatrix} x_{11} & & 0 & & & & \\ & \ddots & & & & & \\ 0 & & x_{11} & & & & \\ & \vdots & & \ddots & & & \\ x_{s1} & \cdots & 0 & & x_{ss} & & 0 \\ \vdots & & \vdots & \cdots & & \ddots & \\ 0 & \cdots & 0 & & 0 & & x_{ss} \end{bmatrix}$$

where $x_{\iota\iota}$ is repeated n_ι times and $x_{\nu\iota}$ is used exactly once if $\nu \neq \iota$. Then $\mathfrak{A} = \mathit{\Xi}\mathbb{Z}^{\boldsymbol{d}\cdot\boldsymbol{n}}$ is a full $\mathcal{O}$-module in $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$ which is not a direct sum of $\mathcal{O}_\iota$-modules. ■

Because of theorem (1.4), we are particularly interested in the equivalence of full modules over equation orders. The next proposition gives us a criterion for when an equation order is a direct sum of orders (which then must be equation orders themselves).[2]

(1.42) Proposition. Let $\vartheta_1, \ldots, \vartheta_s$ be algebraic integers with distinct minimal polynomials $\mu_1, \ldots, \mu_s$. Put $\vartheta = \vartheta_1 \oplus \cdots \oplus \vartheta_s$ and $\hat{\mu}_\iota = (\mu_1 \cdots \mu_s)/\mu_\iota$. Then

$$\mathbb{Z}[\vartheta] = \mathbb{Z}[\vartheta_1] \oplus \cdots \oplus \mathbb{Z}[\vartheta_s]$$

if and only if $\hat{\mu}_\iota(\vartheta_\iota)$ is a unit of $\mathbb{Z}[\vartheta_\iota]$ for each ι.

[1] It is easy to see that such a basis can be computed with methods similar to the Hermite normal form algorithm.

[2] This criterion is mentioned without proof at the end of Latimer and MacDuffee (1933).

Proof. Suppose $\mathbb{Z}[\vartheta] = \mathbb{Z}[\vartheta_1] \oplus \cdots \oplus \mathbb{Z}[\vartheta_s]$. Let 1_ι be the unit element of $\mathcal{O}_\iota$. Making use of the natural embedding $\mathcal{K}_\iota \to \boldsymbol{\mathcal{K}}$, we may regard 1_ι as an element of $\mathbb{Z}[\vartheta]$. Hence there is an integer polynomial f such that $f(\vartheta) = 1_\iota$. More precisely, since $f(\vartheta) = f(\vartheta_1) \oplus \cdots \oplus f(\vartheta_s)$, we have

$$f(\vartheta_\iota) = 1_\iota \qquad \text{and} \qquad f(\vartheta_\nu) = 0 \quad \text{for } \nu \neq \iota.$$

Therefore f is divided by $\hat{\mu}_\iota$. Let $g = f/\hat{\mu}_\iota$. Then

$$1_\iota = f(\vartheta_\iota) = g(\vartheta_\iota)\hat{\mu}_\iota(\vartheta_\iota),$$

so $\hat{\mu}_\iota(\vartheta_\iota)$ is a unit of $\mathbb{Z}[\vartheta_\iota]$.
Now suppose $\hat{\mu}_\iota(\vartheta_\iota)$ is a unit of $\mathbb{Z}[\vartheta_\iota]$ for a fixed ι. Because of $\hat{\mu}_\iota(\vartheta_\iota) = \hat{\mu}_\iota(\vartheta)$, it is contained in $\mathbb{Z}[\vartheta]$. Since the projection $\boldsymbol{\mathcal{K}} \to \mathcal{K}_\iota$ can be restricted to a surjection $\mathbb{Z}[\vartheta] \to \mathbb{Z}[\vartheta_\iota]$, there is an $x = x_1 \oplus \cdots \oplus x_s$ in $\mathbb{Z}[\vartheta]$ with $x_\iota = \hat{\mu}_\iota(\vartheta_\iota)^{-1}$. Then $x\hat{\mu}_\iota(\vartheta_\iota) = x_\iota\hat{\mu}_\iota(\vartheta_\iota) = 1_\iota$ and

$$\hat{\mu}_\iota(\vartheta_\iota)\mathbb{Z}[\vartheta] \supset x\hat{\mu}_\iota(\vartheta_\iota)\mathbb{Z}[\vartheta] = 1_\iota\mathbb{Z}[\vartheta] = \mathbb{Z}[\vartheta_\iota].$$

Hence $\mathbb{Z}[\vartheta_1] \oplus \cdots \oplus \mathbb{Z}[\vartheta_s] \subset \mathbb{Z}[\vartheta]$ if each $\hat{\mu}_\iota(\vartheta_\iota)$ is a unit. The converse inclusion is trivial. ■

Having seen that the number of module classes is at least $h_1 \cdots h_s$, we now want to examine the individual factors.[1] Let $\mathcal{O}$ be an order of a number field $\mathcal{K}$. For each ideal class of $\mathcal{O}$, we choose a representative $\mathfrak{a}_i$ (this includes classes of noninvertible ideals). According to (1.13), the modules $\mathfrak{a}_i \oplus \mathcal{O}^{n-1}$ define distinct classes of $\mathcal{O}$-modules in $\mathcal{K}^n$. Suppose that $\mathcal{O}$ is not maximal and $n > 1$. Let $\mathfrak{f}$ be the conductor of $\mathcal{O} \subset \mathcal{O}_\mathcal{K}$ and let $\mathfrak{f} \oplus \cdots \oplus \mathfrak{f}$ be the module where $\mathfrak{f}$ is repeated n times. Then

$$\mathfrak{f} \oplus \cdots \oplus \mathfrak{f} \not\sim \mathfrak{a}_i \oplus \mathcal{O}^{n-1} \quad \text{for all } i$$

because the multiplier ring of the first module is $\mathcal{O}_\mathcal{K}$, whereas it is $\mathcal{O}$ in the other cases. So in the nonmaximal context, the number of module classes always exceeds the number of ideal classes (except for $n = 1$, of course). To make matters worse, not every module class must be given by a direct sum of ideals, as the next extensive example illustrates.

Let ϑ be a root of the polynomial $X^3 - X - 1$. The maximal order of $\mathcal{K} = \mathbb{Q}(\vartheta)$ is the equation order $\mathbb{Z}[\vartheta]$. It contains the order

$$\mathcal{O} = \mathbb{Z} + 2\vartheta\mathbb{Z} + 2\vartheta^2\mathbb{Z}.$$

We want to show that there is a full $\mathcal{O}$-module in $\mathcal{K}^2$ which is not equivalent to a direct sum of two ideals. First, let us determine all ideal classes of $\mathcal{O}$. In general, there is an exact sequence[2]

$$1 \to \mathcal{O}^\times \to \mathcal{O}_\mathcal{K}^\times \to (\mathcal{O}_\mathcal{K}/\mathfrak{f})^\times/(\mathcal{O}/\mathfrak{f})^\times \to \operatorname{Pic}(\mathcal{O}) \to \operatorname{Cl}_\mathcal{K} \to 1$$

[1] So far, we have not dealt with the question whether the number of full module classes is finite. This looks very likely. Indeed, it should be possible to generalize the lattice-theoretic considerations from chapter 2 in Borevich and Shafarevich (1966), but we have not checked this rigorously.

[2] Cf. Neukirch (1999), pp. 78–80, (12.9) and (12.11).

where $\mathfrak{f}$ is the conductor of $\mathcal{O} \subset \mathcal{O}_{\mathcal{K}}$, $\mathrm{Cl}_{\mathcal{K}}$ is the class group of $\mathcal{O}_{\mathcal{K}}$, and $\mathrm{Pic}(\mathcal{O})$ is the Picard group of $\mathcal{O}$, that is, the group of invertible ideals modulo principal ideals. In our case, the class group is trivial; in fact, Minkowski's bound[1]

$$M_{\mathcal{K}} = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|D_{\mathcal{K}}|} = \frac{24}{27\pi}\sqrt{23}$$

is less than 2. Furthermore,

$$\mathfrak{f} = 2\mathcal{O}_{\mathcal{K}}$$

is a prime ideal of $\mathcal{O}_{\mathcal{K}}$ because $X^3 - X - 1$ is irreducible modulo 2.[2] Thus it is also a prime ideal of $\mathcal{O}$. For the residue class fields we obtain

$$\mathcal{O}/\mathfrak{f} \simeq \mathbb{F}_2 \quad \text{and} \quad \mathcal{O}_{\mathcal{K}}/\mathfrak{f} \simeq \mathbb{F}_8.$$

Hence $(\mathcal{O}_{\mathcal{K}}/\mathfrak{f})^\times$ is a cyclic group of order 7. Because of

$$\vartheta(\vartheta^2 - 1) = 1 \quad \text{and} \quad \vartheta \not\equiv 1 \mod \mathfrak{f},$$

we see that ϑ is a unit of $\mathcal{O}_{\mathcal{K}}$ and its residue class generates $(\mathcal{O}_{\mathcal{K}}/\mathfrak{f})^\times$. Therefore the first map in the segment

$$\mathcal{O}_{\mathcal{K}}^\times \to (\mathcal{O}_{\mathcal{K}}/\mathfrak{f})^\times/(\mathcal{O}/\mathfrak{f})^\times \to \mathrm{Pic}(\mathcal{O}) \to \mathrm{Cl}_{\mathcal{K}} \to 1$$

is an epimorphism, making the second trivial and the third injective. In conclusion, the Picard group is also trivial, so all invertible ideals of $\mathcal{O}$ are principal and it remains to determine the classes of noninvertible ideals.

Since the extension $\mathbb{F}_8/\mathbb{F}_2$ admits no intermediate fields, there are no orders between $\mathcal{O}$ and $\mathcal{O}_{\mathcal{K}}$. Therefore the multiplier ring of a noninvertible ideal can only be one of these two orders. If it is the maximal order, the ideal can be regarded as an ideal of $\mathcal{O}_{\mathcal{K}}$, thus being equivalent to $\mathcal{O}_{\mathcal{K}}$. Since $\mathcal{O}_{\mathcal{K}}$ can be seen as a fractional ideal of $\mathcal{O}$, we conclude that there is only one class of ideals with multiplier ring $\mathcal{O}_{\mathcal{K}}$. Thus we can now focus on noninvertible ideals with multiplier ring $\mathcal{O}$.

Every ideal class of $\mathcal{O}$ contains a fractional ideal $\mathfrak{a}$ above $\mathcal{O}$ such that the index $[\mathfrak{a} : \mathcal{O}]$ is subject to another Minkowski bound[3], namely

$$M = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|D|} = \frac{24}{27\pi}\sqrt{|D|}$$

where D is the discriminant of $\mathcal{O}$. In our example, $D = -368$, so $M < 6$. Hence we have to determine fractional ideals $\mathfrak{a} \supset \mathcal{O}$ with

$$(\mathfrak{a} : \mathfrak{a}) = \mathcal{O} \quad \text{and} \quad [\mathfrak{a} : \mathcal{O}] = m \quad \text{for } m = 2, 3, 4, 5.$$

For such an $\mathfrak{a}$ we have $\mathfrak{a} \supset \mathcal{O} \supset m\mathfrak{a}$ and $[\mathcal{O} : m\mathfrak{a}] = m^2$. So instead of fractional ideals, we may consider ideals $\mathfrak{a}$ satisfying

$$(\mathfrak{a} : \mathfrak{a}) = \mathcal{O} \quad \text{and} \quad [\mathcal{O} : \mathfrak{a}] = m^2 \quad \text{for } m = 2, 3, 4, 5.$$

[1] Ibid., p. 38, exercise 3. Here, n is the degree of $\mathcal{K}$, $2s$ is the number of embeddings $\mathcal{K} \to \mathbb{C}$ and $D_{\mathcal{K}}$ is the discriminant of $\mathcal{O}_{\mathcal{K}}$.

[2] Ibid., pp. 47–48, (8.3).

[3] Cf. Borevich and Shafarevich (1966), pp. 127–29, lemma 3, theorem 3 and problem 2.

If the index is 9 or 25, each prime ideal above $\mathfrak{a}$ must contain 3 or 5. Then $\mathfrak{a}$ is coprime to $\mathfrak{f} = 2\mathcal{O}_{\mathcal{K}}$ and therefore invertible by (2.30). So only the ideals of index 4 or 16 are of interest. In order to determine them, we will first enumerate all $\mathbb{Z}$-modules of index $m^2 = 4$ or $m^2 = 16$. These are given by bases of the form

$$\begin{aligned}&a_{11},\\&a_{21} + a_{22}(2\vartheta),\\&a_{31} + a_{32}(2\vartheta) + a_{33}(2\vartheta^2)\end{aligned}$$

where the a_{ij} are nonnegative integers with $a_{11}a_{22}a_{33} = m^2$ and $a_{ij} < a_{jj}$, that is, the matrices $[a_{ij}]$ run through all Hermite normal forms of determinant m^2. Moreover, a_{11}, a_{21}, a_{31} must be even so that the module is contained in $\mathfrak{f}$. These conditions give us $7 + 155 = 162$ submodules in total. But only eight of these $\mathbb{Z}$-modules are ideals of $\mathcal{O}$, one with multiplier ring $\mathcal{O}_{\mathcal{K}}$ which can be discarded.[1] The remaining seven ideals are

$$\begin{aligned}&\mathfrak{a}_1 = (2,\, 2\vartheta,\, 4\vartheta^2), && \mathfrak{a}_2 = (4,\, 2\vartheta,\, 2\vartheta^2), && \mathfrak{a}_3 = (4,\, 2+2\vartheta,\, 2\vartheta^2),\\&\mathfrak{a}_4 = (4,\, 2+2\vartheta,\, 2+2\vartheta^2), && \mathfrak{a}_5 = (2,\, 4\vartheta,\, 2\vartheta+2\vartheta^2), && \mathfrak{a}_6 = (4,\, 2\vartheta,\, 2+2\vartheta^2),\\&\mathfrak{a}_7 = (2,\, 4\vartheta,\, 2\vartheta^2).\end{aligned}$$

They are all equivalent because $\mathfrak{a}_{k+1} = \vartheta\mathfrak{a}_k$ for $1 \le k \le 6$. In summary, there are three ideal classes of $\mathcal{O}$ represented by

$$\mathcal{O}, \quad \mathcal{O}_{\mathcal{K}} \quad \text{and} \quad \mathfrak{a} = (1,\, \vartheta,\, 2\vartheta^2).$$

Now consider the module

$$\mathfrak{A} = \begin{bmatrix} 1 & 0 & \vartheta^2 \\ 0 & 1 & \vartheta \end{bmatrix} \mathcal{O}^3.$$

A $\mathbb{Z}$-basis of $\mathfrak{A}$ is given by

$$\varXi = \begin{bmatrix} 1 & 2\vartheta & \vartheta^2 & 0 & 0 & 0 \\ 0 & 0 & \vartheta & 1 & 2\vartheta & 2\vartheta^2 \end{bmatrix}.$$

Suppose this module were equivalent to a direct sum of two ideals. Then there is a $\varGamma \in \mathrm{GL}(2, \mathcal{K})$ such that

$$\varGamma\mathfrak{A} = \mathfrak{a}_1 \oplus \mathfrak{a}_2 \quad \text{with } \mathfrak{a}_i \in \{\mathcal{O},\, \mathcal{O}_{\mathcal{K}},\, \mathfrak{a}\}.$$

Because of

$$\varGamma\mathcal{O}_{\mathcal{K}}^2 = \varGamma\mathfrak{A}\mathcal{O}_{\mathcal{K}} = (\mathfrak{a}_1 \oplus \mathfrak{a}_2)\mathcal{O}_{\mathcal{K}} = \mathcal{O}_{\mathcal{K}}^2,$$

we see that $\varGamma \in \mathrm{GL}(2, \mathcal{O}_{\mathcal{K}})$. Furthermore, $\mathfrak{A}$ and $\mathfrak{a}_1 \oplus \mathfrak{a}_2$ both contain $\mathfrak{f} \oplus \mathfrak{f}$. Let

$$\bar{\mathfrak{A}} = \mathfrak{A}/(\mathfrak{f} \oplus \mathfrak{f}) \quad \text{and} \quad \bar{\mathfrak{a}}_i = \mathfrak{a}_i/\mathfrak{f}.$$

[1] Of course, this statement can be verified by a computer in no time, yet with a little effort, this can also be done by hand. Taking into account that $\mathcal{O}$ must be the multiplier ring, the number of possible ideals can be reduced further.

These are vector spaces over $\mathbb{F}_2 = \mathcal{O}/\mathfrak{f}$ which are contained in $\mathbb{F}_8^2 = (\mathcal{O}_{\mathcal{K}}/\mathfrak{f})^2$. Let $\bar{\vartheta}$ be the image of ϑ in $\mathbb{F}_8$ and $\bar{\varGamma} = [\bar{\gamma}_{ij}]$ the image of $\varGamma$ in $\mathrm{GL}(2, \mathbb{F}_8)$. Then

$$\bar{\varGamma}\bar{\mathfrak{A}} = \bar{\mathfrak{a}}_1 \oplus \bar{\mathfrak{a}}_2.$$

In particular, $\bar{\mathfrak{A}}$ and $\bar{\mathfrak{a}}_1 \oplus \bar{\mathfrak{a}}_2$ are isomorphic over $\mathbb{F}_2$. Since

$$\dim \bar{\mathfrak{A}} = 3, \quad \dim \mathbb{F}_2 = 1, \quad \dim \mathbb{F}_8 = 3, \quad \dim \bar{\mathfrak{a}} = 2 \quad (\bar{\mathfrak{a}} = \mathfrak{a}/\mathfrak{f}),$$

we may assume $\bar{\mathfrak{a}}_1 = \mathbb{F}_2$ and $\bar{\mathfrak{a}}_2 = \bar{\mathfrak{a}}$. The columns of the matrices

$$\begin{bmatrix} 1 & 0 & \bar{\vartheta}^2 \\ 0 & 1 & \bar{\vartheta} \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & \bar{\vartheta} \end{bmatrix}$$

are $\mathbb{F}_2$-bases of $\bar{\mathfrak{A}}$ and $\bar{\mathfrak{a}}_1 \oplus \bar{\mathfrak{a}}_2$. Therefore $\bar{\varGamma}\bar{\mathfrak{A}} = \bar{\mathfrak{a}}_1 \oplus \bar{\mathfrak{a}}_2$ is equivalent to

$$\bar{\varGamma} \begin{bmatrix} 1 & 0 & \bar{\vartheta}^2 \\ 0 & 1 & \bar{\vartheta} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & \bar{\vartheta} \end{bmatrix} \bar{U} \quad \text{for some } \bar{U} \in \mathrm{GL}(3, \mathbb{F}_2).$$

The first row of the right-hand product solely consists of elements of $\mathbb{F}_2$, hence the same must be true for the first row of

$$\bar{\varGamma} \begin{bmatrix} 1 & 0 & \bar{\vartheta}^2 \\ 0 & 1 & \bar{\vartheta} \end{bmatrix} = \begin{bmatrix} \bar{\gamma}_{11} & \bar{\gamma}_{12} & * \\ \bar{\gamma}_{21} & \bar{\gamma}_{22} & * \end{bmatrix}.$$

But the $(1, 3)$-entry of this product is

$$\bar{\gamma}_{11}\bar{\vartheta}^2 + \bar{\gamma}_{12}\bar{\vartheta}$$

which does not belong to $\mathbb{F}_2$ because 1, $\bar{\vartheta}$, $\bar{\vartheta}^2$ are linearly independent over $\mathbb{F}_2$. Therefore $\bar{\varGamma}\bar{\mathfrak{A}} = \bar{\mathfrak{a}}_1 \oplus \bar{\mathfrak{a}}_2$ does not hold. In conclusion, $\mathfrak{A}$ cannot be equivalent to a direct sum of ideals.

1.8 Algorithms

(1.43) Algorithm — Corresponding Module

→ A semisimple integer matrix

← $\mathfrak{A}$ full module corresponding to A

Suppose that $\mu = \mu_1 \cdots \mu_s$ is the minimal and $\chi = \mu_1^{n_1} \cdots \mu_s^{n_s}$ the characteristic polynomial of A and that ϑ_ι is a root of μ_ι. Let $\boldsymbol{\mathcal{K}} = \mathbb{Q}[\vartheta]$ where $\vartheta = \vartheta_1 \oplus \cdots \oplus \vartheta_s$. The module $\mathfrak{A}$ will be a subset of $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$ where $\boldsymbol{n} = (n_1, \dots, n_s)$. Furthermore, let $m \times m$ denote the size of A.

(1) For $\iota = 1, \dots, s$, compute a $\mathcal{K}_\iota$-basis $x_1^\iota, \dots, x_{n_\iota}^\iota \in \mathcal{K}_\iota^m$ of $\mathrm{Eig}(A, \vartheta_\iota)$.

(2) Put $\varXi := [\, x_1^1 \ \dots \ x_{n_1}^1 \ \dots \ \dots \ x_1^s \ \dots \ x_{n_s}^s \,]^{\mathrm{tr}}$.

(3) Return $\mathfrak{A} = \varXi\mathbb{Z}^m$.

(1.44) Algorithm — Corresponding Matrix

→ $\mathfrak{A}$, $\mathfrak{B}$ full modules corresp. to semisimple integer matrices A, B
Γ element of $\mathrm{GL}(\boldsymbol{n},\boldsymbol{\mathcal{K}})$ satisfying $\Gamma\mathfrak{A}=\mathfrak{B}$

← C invertible integer matrix satisfying $CA = BC$

$\mathfrak{A}$ and $\mathfrak{B}$ are given by $\mathbb{Z}$-bases $\Xi = [\,\xi_1 \ \dots \ \xi_m\,]$ and $\Upsilon = [\,\upsilon_1 \ \dots \ \upsilon_m\,]$.

(1) Compute the the matrix $C^{-1} = [c_{ij}]$ with entries given by $\Gamma\xi_i = \sum c_{ij}\upsilon_j$.

(2) Return C.

We will now describe how the multiplier ideal of two full modules $\mathfrak{A}$, $\mathfrak{B} \subset \boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$ can be computed. Let $\Xi = [\xi_1,\dots,\xi_m]$ and $\Upsilon = [\upsilon_1,\dots,\upsilon_m]$ be $\mathbb{Z}$-bases of $\mathfrak{A}$ and $\mathfrak{B}$, and let $\Gamma_1,\dots,\Gamma_\ell$ be a $\mathbb{Q}$-basis of $\mathrm{M}(\boldsymbol{n},\boldsymbol{\mathcal{K}})$. For $\Gamma \in \mathrm{M}(\boldsymbol{n},\boldsymbol{\mathcal{K}})$, we have the equivalence

$$\Gamma \in (\mathfrak{B}:\mathfrak{A}) \quad \Leftrightarrow \quad \Gamma\xi_k \in \mathfrak{B} \quad \text{for all } k.$$

Let $B^{(k)} = [b_{ij}^{(k)}]$ be the rational $\ell \times m$ matrix with

$$\Gamma_i\xi_k = \sum b_{ij}^{(k)}\upsilon_j,$$

and, for a fixed Γ, let c_i denote the rational coefficients with $\Gamma = \sum c_i\Gamma_i$. Then

$$\Gamma\xi_k = \sum_i c_i\Gamma_i\xi_k = \sum_i c_i \sum_j b_{ij}^{(k)}\upsilon_j = \sum_j (\sum_i c_i b_{ij}^{(k)})\upsilon_j,$$

that is, $\Gamma \in (\mathfrak{B}:\mathfrak{A})$ precisely if $\sum_i c_i b_{ij}^{(k)} \in \mathbb{Z}$ for all j and k. In other words,

$$\Gamma \in (\mathfrak{B}:\mathfrak{A}) \quad \Leftrightarrow \quad [\,c_1 \ \dots \ c_\ell\,][\,B^{(1)} \ \dots \ B^{(m)}\,] \in \mathbb{Z}^{m^2}.$$

Put $c = [\,c_1 \ \dots \ c_\ell\,]$ and $B = [\,B^{(1)} \ \dots \ B^{(m)}\,]$. There is an integer matrix B' and a rational diagonal matrix D such that $B = DB'$. Choose $U \in \mathrm{GL}(m^2,\mathbb{Z})$ such that

$$B'U = [\,H \ 0 \ \dots \ 0\,]$$

where H is in column Hermite normal form. Then

$$cB \in \mathbb{Z}^{m^2} \quad \Leftrightarrow \quad c(DH) \in \mathbb{Z}^\ell \quad \Leftrightarrow \quad c \in \mathbb{Z}^\ell(DH)^{-1}.$$

Put $S = (DH)^{-1}$. As we have seen, $\Gamma = \sum c_i\Gamma_i$ belongs to $(\mathfrak{B}:\mathfrak{A})$ if and only if $c = [\,c_1 \ \dots \ c_\ell\,]$ is a $\mathbb{Z}$-linear combination of the rows of $S = [s_{ij}]$. Thus the matrices

$$M_i = \sum s_{ij}\Gamma_j \quad (1 \le i \le \ell)$$

form a $\mathbb{Z}$-basis of $(\mathfrak{B}:\mathfrak{A})$.

(1.45) Algorithm — Multiplier Ideal

→ $\mathfrak{A}$, $\mathfrak{B}$ full modules in $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$

← $(\mathfrak{B} : \mathfrak{A})$ the multiplier ideal of $\mathfrak{A}$ and $\mathfrak{B}$

$\mathfrak{A}$ and $\mathfrak{B}$ are given by $\mathbb{Z}$-bases $\varXi = [\,\xi_1 \;\dots\; \xi_m\,]$ and $\varUpsilon = [\,\upsilon_1 \;\dots\; \upsilon_m\,]$. The multiplier ideal will also be given by a $\mathbb{Z}$-basis.

(1) Choose a $\mathbb{Q}$-basis $\varGamma_1, \dots, \varGamma_\ell$ of $\mathrm{M}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$.

(2) For $k = 1, \dots, m$, compute $B^{(k)} = [b_{ij}^{(k)}]$ given by $\varGamma_i \xi_k = \sum b_{ij}^{(k)} \upsilon_j$.

(3) Put $B := [\,B^{(1)} \;\dots\; B^{(m)}\,]$.

(4) Choose a diagonal matrix D of full rank such that $B' := D^{-1}B$ is an integer matrix.

(5) Compute the column Hermite normal form $[\,H \; 0 \;\dots\; 0\,]$ of B'.

(6) Put $S = (DH)^{-1}$.

(7) Return $M_1, \dots, M_\ell$ where $M_i = \sum s_{ij} \varGamma_j$.

Algorithm (1.45) can also be used to compute the conductor $\mathfrak{F}$ of an extension $\Lambda \subset \Lambda_{\boldsymbol{\mathcal{K}}}$ of matrix orders. First, the conductor $\mathfrak{f}$ of $\mathcal{O} \subset \mathcal{O}_{\boldsymbol{\mathcal{K}}}$ can be computed as the multiplier ideal $(\mathcal{O}_{\boldsymbol{\mathcal{K}}} : \mathcal{O})$ because orders of $\boldsymbol{\mathcal{K}}$ are full modules in $\boldsymbol{\mathcal{K}}$. Second, if $\mathcal{O}$ is the center of Λ, then $\mathfrak{F} = \mathfrak{f}\Lambda_{\boldsymbol{\mathcal{K}}}$.

2 Localizations of Orders

To decide whether an ideal can be made coprime to the conductor, we will need to consider localizations of the ideal in question. In the first section we will specify the sets we intend to localize. As a first application, we will establish a decomposition of finite quotient rings into direct sums. Afterwards, we will characterize the units of local matrix orders in terms of determinants. Finally, we will prove that an ideal can be made coprime to the conductor if and only if certain local versions are principal. A principal ideal test for local ideals will be provided, too.

2.1 Basic Properties

Let $\mathcal{O}$ be an order of $\boldsymbol{\mathcal{K}}$ and let S be a subset of $\mathcal{O} \cap \boldsymbol{\mathcal{K}}^\times$ which contains 1 and is closed under multiplication. The ring

$$\mathcal{O}_S = \{\, xs^{-1} \mid x \in \mathcal{O},\, s \in S \,\}$$

is called the **localization** of $\mathcal{O}$ at S. More generally, if $\mathfrak{M}$ is a finitely generated $\mathcal{O}$-module contained in a $\boldsymbol{\mathcal{K}}$-algebra, the set

$$\mathfrak{M}_S = \{\, ms^{-1} \mid m \in \mathfrak{M},\, s \in S \,\}$$

is called the **localization** of $\mathfrak{M}$ at S. Obviously, this is a module over $\mathcal{O}_S$ and we have $\mathfrak{M}_S = \mathfrak{M}\mathcal{O}_S$.

The modules we intend to localize will be matrix orders and their ideals. Moreover, we will solely examine localizations at sets of the form

$$S_\mathfrak{p} = (\mathcal{O} \smallsetminus \mathfrak{p}) \cap \boldsymbol{\mathcal{K}}^\times$$

where $\mathfrak{p}$ is a full prime ideal of $\mathcal{O}$. We will write $\mathfrak{M}_\mathfrak{p}$ for the localization at $S_\mathfrak{p}$ and will simply call this the localization of $\mathfrak{M}$ at $\mathfrak{p}$. If $\boldsymbol{\mathcal{K}}$ is a number field, this coincides with the usual notation, but if $\boldsymbol{\mathcal{K}}$ is a proper direct sum, it does not.[1] Still, we will use $\mathfrak{p}$ as index to keep notation simple.

We will now prove some statements which will be needed in this chapter. Notice that, since $\boldsymbol{\mathcal{K}}$ is the center of $\mathrm{M}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$, we can identify scalars as elements of $\mathrm{M}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$. Therefore expressions like $\mathfrak{C} \cap \mathcal{O}$ become meaningful.

(2.1) Proposition. Every full ideal of $\mathcal{O}$ is generated by its nonzerodivisors.

Proof. Let $\mathfrak{c}$ be a full ideal of $\mathcal{O}$ and suppose $\mathfrak{c}' \subset \mathfrak{c}$ is generated by the nonzerodivisors of $\mathfrak{c}$. Let c be a zero- and c' a nonzerodivisor of $\mathfrak{c}$. We have to show

[1] Usually, the set $S_\mathfrak{p} = \mathcal{O} \smallsetminus \mathfrak{p}$ is considered where zerodivisors need special treatment.

that $c \in \mathfrak{c}'$. Because of $\mathcal{K}^\times = \mathcal{K}_1^\times \oplus \cdots \oplus \mathcal{K}_s^\times$, each component of $c' = c_1' \oplus \cdots \oplus c_s'$ has to be nonzero. So for each ι, we have $c_\iota + rc_\iota' = 0$ for at most one integer r. Hence $c + rc'$ is a nonzerodivisor of $\mathfrak{c}$ for a suitable choice of r. The definition of $\mathfrak{c}'$ now implies $c = (c + rc') - rc' \in \mathfrak{c}'$. ■

(2.2) Corollary. If $\mathfrak{c}$ is a full ideal of $\mathcal{O}$ with $\mathfrak{c} \not\subset \mathfrak{p}$, then $\mathfrak{c} \cap S_\mathfrak{p}$ is not empty.

Proof. If $\mathfrak{c} \cap S_\mathfrak{p}$ were empty, all nonzerodivisors of $\mathfrak{c}$ would belong to $\mathfrak{p}$, which implies $\mathfrak{c} \subset \mathfrak{p}$ by (2.1). ■

(2.3) Proposition. Let Λ be a matrix order with center $\mathcal{O}$ and let $\mathfrak{C}$ be a full right ideal of Λ. Then $\mathfrak{c} = \mathfrak{C} \cap \mathcal{O}$ is a full ideal of $\mathcal{O}$.

Proof. As a full right ideal, $\mathfrak{C}$ has finite index in Λ. Hence there is a positive integer c such that $c\Lambda \subset \mathfrak{C}$. In particular, $c \in \mathfrak{C} \cap \mathcal{O}$, hence $\mathfrak{c}$ is full. ■

(2.4) Proposition. Every full prime ideal of $\mathcal{O}$ is a maximal ideal.

Proof. Let $\mathfrak{p}$ be a full prime ideal of $\mathcal{O}$. As a finite integral domain, $\mathcal{O}/\mathfrak{p}$ is a field, and therefore $\mathfrak{p}$ has to be maximal. ■

(2.5) Proposition. Let $\mathfrak{p}$ be a full prime ideal of $\mathcal{O}$ and let $\mathfrak{Q}$ be the set of prime ideals of $\mathcal{O}_\mathcal{K}$ containing $\mathfrak{p}$. Then

$$\mathfrak{p} = \mathfrak{q} \cap \mathcal{O} \quad \text{for all } \mathfrak{q} \in \mathfrak{Q}.$$

In particular, the prime ideals above a full $\mathcal{O}$-ideal $\mathfrak{c}$ can be determined by first factorizing $\mathfrak{c}_\mathcal{K} = \mathfrak{c}\mathcal{O}_\mathcal{K}$ and intersecting the prime factors with $\mathcal{O}$ afterwards.

Proof. Clearly, $\mathfrak{q} \cap \mathcal{O}$ is a proper ideal above $\mathfrak{p}$, hence $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}$ by (2.4). The second statement follows immediately. ■

(2.6) Proposition. Let $\mathcal{O}$ be an order of $\mathcal{K}$ and $\mathfrak{p}$ a full prime ideal of $\mathcal{O}$. Let $\mathfrak{Q}$ be the set of prime ideals of $\mathcal{O}_\mathcal{K}$ containing $\mathfrak{p}$. Then all nonzero prime ideals of $(\mathcal{O}_\mathcal{K})_\mathfrak{p}$ are of the form $\mathfrak{q}_\mathfrak{p}$ with $\mathfrak{q} \in \mathfrak{Q}$.

Proof. There is a one-to-one correspondence between the prime ideals of $(\mathcal{O}_\mathcal{K})_\mathfrak{p}$ and the prime ideals of $\mathcal{O}_\mathcal{K}$ not meeting $S_\mathfrak{p}$.[1] Clearly, the prime ideals meeting $S_\mathfrak{p}$ cannot contain $\mathfrak{p}$ because $s\mathcal{O} + \mathfrak{p} = \mathcal{O}$ for all $s \in S_\mathfrak{p}$. ■

(2.7) Proposition. Let $\mathcal{O}$ be an order of $\mathcal{K}$ and $\mathfrak{f}$ the conductor of $\mathcal{O} \subset \mathcal{O}_\mathcal{K}$. There is a one-to-one correspondence between

- the set $\mathfrak{I}$ of ideals of $\mathcal{O}$ coprime to $\mathfrak{f}$ and
- the set $\mathfrak{I}_\mathcal{K}$ of ideals of $\mathcal{O}_\mathcal{K}$ coprime to $\mathfrak{f}$.

If $\mathfrak{p}$ is a full prime ideal of $\mathcal{O}$ not containing $\mathfrak{f}$, then $\mathfrak{p}\mathcal{O}_\mathcal{K}$ is the only ideal of $\mathcal{O}_\mathcal{K}$ above $\mathfrak{p}$, and therefore prime.[2]

[1] Cf. Eisenbud (1995), p. 61, proposition 2.2.

[2] Result (2.7) is based on propositions 7.20 and 7.22 by Cox (1989).

Proof. If $\mathfrak{a} \subset \mathcal{O}$ is coprime to $\mathfrak{f}$, then so is $\mathfrak{a}\mathcal{O}_{\mathcal{K}}$ because

$$\mathfrak{a}\mathcal{O}_{\mathcal{K}} + \mathfrak{f} = \mathfrak{a}\mathcal{O}_{\mathcal{K}} + \mathfrak{f}\mathcal{O}_{\mathcal{K}} = (\mathfrak{a} + \mathfrak{f})\mathcal{O}_{\mathcal{K}} = \mathcal{O}_{\mathcal{K}}.$$

Conversely, if $\mathfrak{a}_{\mathcal{K}} \subset \mathcal{O}_{\mathcal{K}}$ is coprime to $\mathfrak{f}$, then

$$\mathfrak{a}_{\mathcal{K}} \cap \mathcal{O} + \mathfrak{f} = \mathfrak{a}_{\mathcal{K}} \cap \mathcal{O} + \mathfrak{f} \cap \mathcal{O} = (\mathfrak{a}_{\mathcal{K}} + \mathfrak{f}) \cap \mathcal{O} = \mathcal{O}.$$

Consider the maps

$$\mathfrak{I} \to \mathfrak{I}_{\mathcal{K}}, \quad \mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_{\mathcal{K}} \qquad \text{and} \qquad \mathfrak{I}_{\mathcal{K}} \to \mathfrak{I}, \quad \mathfrak{a}_{\mathcal{K}} \to \mathfrak{a}_{\mathcal{K}} \cap \mathcal{O}.$$

We will show that they are inverse to each other. Let $\mathfrak{a} \in \mathfrak{I}$. Using (1.37), we obtain

$$\mathfrak{a} \subset \mathfrak{a}\mathcal{O}_{\mathcal{K}} \cap \mathcal{O} = \mathfrak{a}\mathcal{O}_{\mathcal{K}} \cap (\mathfrak{a} + \mathfrak{f}) = (\mathfrak{a}\mathcal{O}_{\mathcal{K}} \cap \mathfrak{a}) + (\mathfrak{a}\mathcal{O}_{\mathcal{K}} \cap \mathfrak{f}) = \mathfrak{a} + (\mathfrak{a}\mathcal{O}_{\mathcal{K}} \cap \mathfrak{f}),$$

and since, in any ring, the intersection of coprime ideals is equal to their product, we have

$$\mathfrak{a} + (\mathfrak{a}\mathcal{O}_{\mathcal{K}} \cap \mathfrak{f}) = \mathfrak{a} + (\mathfrak{a}\mathcal{O}_{\mathcal{K}})\mathfrak{f} = \mathfrak{a} + \mathfrak{a}\mathfrak{f} = \mathfrak{a}.$$

Taken together, we see that $\mathfrak{a}\mathcal{O}_{\mathcal{K}} \cap \mathcal{O} = \mathfrak{a}$. Now let $\mathfrak{a}_{\mathcal{K}} \in \mathfrak{I}_{\mathcal{K}}$. Then

$$\begin{aligned}
(\mathfrak{a}_{\mathcal{K}} \cap \mathcal{O})\mathcal{O}_{\mathcal{K}} &= (\mathfrak{a}_{\mathcal{K}} \cap \mathcal{O})(\mathfrak{a}_{\mathcal{K}} + \mathfrak{f}) \\
&= (\mathfrak{a}_{\mathcal{K}} \cap \mathcal{O})\mathfrak{a}_{\mathcal{K}} + (\mathfrak{a}_{\mathcal{K}} \cap \mathcal{O})\mathfrak{f} \\
&= (\mathfrak{a}_{\mathcal{K}} \cap \mathcal{O})\mathfrak{a}_{\mathcal{K}} + (\mathfrak{a}_{\mathcal{K}} \cap \mathcal{O}) \cap \mathfrak{f} \\
&= (\mathfrak{a}_{\mathcal{K}} \cap \mathcal{O})\mathfrak{a}_{\mathcal{K}} + \mathfrak{a}_{\mathcal{K}} \cap \mathfrak{f} \\
&= (\mathfrak{a}_{\mathcal{K}} \cap \mathcal{O})\mathfrak{a}_{\mathcal{K}} + \mathfrak{a}_{\mathcal{K}}\mathfrak{f} \\
&= \mathfrak{a}_{\mathcal{K}}(\mathfrak{a}_{\mathcal{K}} \cap \mathcal{O} + \mathfrak{f}) \\
&= \mathfrak{a}_{\mathcal{K}}((\mathfrak{a}_{\mathcal{K}} + \mathfrak{f}) \cap \mathcal{O}) = \mathfrak{a}_{\mathcal{K}}(\mathcal{O}_{\mathcal{K}} \cap \mathcal{O}) = \mathfrak{a}_{\mathcal{K}},
\end{aligned}$$

again using (1.37) at the end. Applying these maps to full prime ideals, we see that the last assertion is also correct. ■

2.2 Decomposition of Quotient Rings

In section 1.6 we realized that we need to closer examine the unit group of $\Lambda/\mathfrak{F}$ where $\mathfrak{F}$ is the conductor of some extension $\Lambda \subset \Lambda_{\mathcal{K}}$. From a computational point of view, it would therefore be desirable to decompose $\Lambda/\mathfrak{F}$ into a direct sum of smaller rings using the Chinese Remainder Theorem, which also holds for noncommutative rings.

(2.8) Chinese Remainder Theorem. Let $\mathfrak{C}_1, \ldots, \mathfrak{C}_n$ be pairwise coprime two-sided ideals of Λ. Then

$$\Lambda/\bigcap_{i=1}^{n} \mathfrak{C}_i \simeq \bigoplus_{i=1}^{n} \Lambda/\mathfrak{C}_i.$$

For instance, if we regard $\mathfrak{F}$ as an ideal of $\Lambda_{\mathcal{K}}$, the Chinese Remainder Theorem yields

$$\Lambda_{\mathcal{K}}/\mathfrak{F} = \Lambda_{\mathcal{K}}/\mathfrak{f}\Lambda_{\mathcal{K}} \simeq \bigoplus_{\mathfrak{q}} \Lambda_{\mathcal{K}}/\mathfrak{q}^{e_{\mathfrak{q}}}\Lambda_{\mathcal{K}}.$$

Here, $\mathfrak{f}$ is the conductor of $\mathcal{O} \subset \mathcal{O}_{\mathcal{K}}$ with factorization $\prod_{\mathfrak{q}} \mathfrak{q}^{e_{\mathfrak{q}}}$ where $\mathfrak{q}$ runs over the full prime ideals of $\mathcal{O}_{\mathcal{K}}$. Recall that, by (1.32), the two-sided ideals of $\Lambda_{\mathcal{K}}$ correspond to the ideals of $\mathcal{O}_{\mathcal{K}}$. Therefore

$$(\prod_{\mathfrak{q}} \mathfrak{q}^{e_{\mathfrak{q}}})\Lambda_{\mathcal{K}} = \bigcap_{\mathfrak{q}} (\mathfrak{q}^{e_{\mathfrak{q}}}\Lambda_{\mathcal{K}}).$$

Unfortunately, we cannot expect $\mathfrak{F}$ to be a product of prime powers as an ideal of Λ. In general, this is already false for $\mathfrak{f}$. However, we will be able to prove the existence of sufficiently large exponents $\nu_{\mathfrak{p}}$ such that

$$\Lambda/\mathfrak{F} \simeq \bigoplus_{\mathfrak{p}} \Lambda/(\mathfrak{F} + \mathfrak{p}^{\nu_{\mathfrak{p}}}\Lambda)$$

where $\mathfrak{p}$ runs over the full prime ideals of $\mathcal{O}$. Since $\mathfrak{f}\Lambda \subset \mathfrak{f}\Lambda_{\mathcal{K}} = \mathfrak{F}$, the quotients on the right-hand side are trivial for $\mathfrak{p} \not\supset \mathfrak{f}$.

While it is obvious that the ideals $\mathfrak{F} + \mathfrak{p}^{\nu_{\mathfrak{p}}}\Lambda$ are coprime for distinct primes $\mathfrak{p}$, the equality

$$\mathfrak{F} = \bigcap_{\mathfrak{p}} (\mathfrak{F} + \mathfrak{p}^{\nu_{\mathfrak{p}}}\Lambda)$$

is less straightforward. Eventually, it will be a consequence of the following theorem, which employs the concept of localization.

(2.9) Theorem. Let $\mathfrak{C}$ be a full two-sided ideal of Λ. Then

$$\Lambda/\mathfrak{C} \simeq \bigoplus_{\mathfrak{p}} \Lambda_{\mathfrak{p}}/\mathfrak{C}_{\mathfrak{p}}$$

where $\mathfrak{p}$ runs over all full prime ideals of $\mathcal{O}$. If $\mathfrak{p}$ does not contain $\mathfrak{c} = \mathfrak{C} \cap \mathcal{O}$, then $\Lambda_{\mathfrak{p}}/\mathfrak{C}_{\mathfrak{p}}$ is trivial.[1]

This theorem is somewhat similar to the Chinese Remainder Theorem, especially if you consider the next statement.

(2.10) Proposition. Let $\mathfrak{C}$ be a right ideal of Λ. Then

$$\mathfrak{C} = \bigcap_{\mathfrak{p}} \mathfrak{C}_{\mathfrak{p}}$$

where $\mathfrak{p}$ runs over all full prime ideals of $\mathcal{O}$.

Proof. The inclusion $\mathfrak{C} \subset \bigcap_{\mathfrak{p}} \mathfrak{C}_{\mathfrak{p}}$ is clear. Let $C \in \bigcap_{\mathfrak{p}} \mathfrak{C}_{\mathfrak{p}}$. For every $\mathfrak{p}$, there is an $s_{\mathfrak{p}} \in S_{\mathfrak{p}}$ such that $s_{\mathfrak{p}}C \in \mathfrak{C}$. Therefore the set

$$\mathfrak{s} = \{\, s \in \mathcal{O} \mid sC \in \mathfrak{C} \,\}$$

is a full ideal of $\mathcal{O}$ which is not contained in any prime ideal. Hence $\mathfrak{s} = \mathcal{O}$. Taking $s = 1$, we obtain $C = sC \in \mathfrak{C}$. ■

[1] Results (2.9) and (2.10) are generalizations of statements by Neukirch (1999); cf. (12.3) on p. 74 and the proof of (11.5) on p. 68.

Before we can prove (2.9), we need to provide a few lemmata.

(2.11) Lemma. Each $s \in S_{\mathfrak{p}}$ is a unit modulo $\mathfrak{c}_{\mathfrak{p}} \cap \mathcal{O}$.

For the proof, see Eisenbud (1995), p. 61, proposition 2.2 (keep in mind that $\mathcal{O}/(\mathfrak{c}_{\mathfrak{p}} \cap \mathcal{O})$ is a finite ring, therefore each nonzerodivisor is already a unit). We want to generalize this lemma slightly.

(2.12) Lemma. Each $s \in S_{\mathfrak{p}}$ is a unit modulo $\mathfrak{C}_{\mathfrak{p}} \cap \Lambda$. Its inverse is represented by an element of $\mathcal{O}$.

Proof. Consider the composition of the canonical maps

$$\mathcal{O} \to \Lambda \to \Lambda/(\mathfrak{C}_{\mathfrak{p}} \cap \Lambda).$$

The kernel is $\mathfrak{c}_{\mathfrak{p}} \cap \mathcal{O}$, for if a belongs to $(\mathfrak{C}_{\mathfrak{p}} \cap \Lambda) \cap \mathcal{O} = \mathfrak{C}_{\mathfrak{p}} \cap \mathcal{O}$, there is an $s \in S_{\mathfrak{p}}$ such that $sa \in \mathfrak{C} \cap \mathcal{O} = \mathfrak{c}$. Hence $a \in \mathfrak{c}_{\mathfrak{p}} \cap \mathcal{O}$. Therefore we have an injection

$$\mathcal{O}/(\mathfrak{c}_{\mathfrak{p}} \cap \mathcal{O}) \to \Lambda/(\mathfrak{C}_{\mathfrak{p}} \cap \Lambda).$$

By (2.11) there is an $s' \in \mathcal{O}$ for every $s \in S_{\mathfrak{p}}$ such that $ss' \equiv 1 \bmod \mathfrak{c}_{\mathfrak{p}} \cap \mathcal{O}$. Because of the embedding above, this congruence also holds modulo $\mathfrak{C}_{\mathfrak{p}} \cap \Lambda$. ■

The next two lemmata are about prime ideals of Λ. Since Λ is noncommutative (unless $\Lambda = \mathcal{O}$, of course), a prime ideal of Λ is defined to be a proper two-sided ideal $\mathfrak{P}$ satisfying the condition

$$\mathfrak{A}\mathfrak{B} \subset \mathfrak{P} \quad \Rightarrow \quad \mathfrak{A} \subset \mathfrak{P} \text{ or } \mathfrak{B} \subset \mathfrak{P}$$

where $\mathfrak{A}$ and $\mathfrak{B}$ are two-sided ideals of Λ. Equivalently, one can require

$$A\Lambda B \subset \mathfrak{P} \;\Rightarrow\; A \in \mathfrak{P} \text{ or } B \in \mathfrak{P} \quad \text{for all } A,\, B \in \Lambda.$$[1]

Trying to define primality as in the commutative case would not prove successful, though. For example, all ideals of $\Lambda = \mathrm{M}(2, \mathcal{O})$ contain the product $\left[\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right]\left[\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right]$, but each factor generates Λ as a two-sided ideal.
Maximal two-sided ideals, however, are defined as in the commutative case, and they are always prime, for if $\mathfrak{A}$ and $\mathfrak{B}$ both are not contained in the maximal ideal $\mathfrak{M}$, the inclusion

$$\Lambda = (\mathfrak{A} + \mathfrak{M})(\mathfrak{B} + \mathfrak{M}) = \mathfrak{M}^2 + \mathfrak{A}\mathfrak{M} + \mathfrak{M}\mathfrak{B} + \mathfrak{A}\mathfrak{B} \subset \mathfrak{M} + \mathfrak{A}\mathfrak{B}$$

implies $\mathfrak{A}\mathfrak{B} \not\subset \mathfrak{M}$.

(2.13) Lemma. Let $\mathfrak{P}$ be a full prime ideal of Λ. Then $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}$ is a full prime ideal of $\mathcal{O}$.

Proof. By (2.3) we know that $\mathfrak{p}$ is a full ideal of $\mathcal{O}$. If a, $b \in \mathcal{O}$ with $ab \in \mathfrak{p}$, we have $a\Lambda b = ab\Lambda \subset \mathfrak{P}$, hence a or b belongs to $\mathfrak{P} \cap \mathcal{O} = \mathfrak{p}$. ■

[1] Cf. Lam (2001), p. 155, proposition (10.2).

(2.14) Lemma. Let $\mathfrak{P}$ be a prime ideal above $\mathfrak{C}_\mathfrak{p} \cap \Lambda$. Then $\mathfrak{P} \cap \mathcal{O} = \mathfrak{p}$.

Proof. Since $\mathfrak{P}$ lies above $\mathfrak{C}_\mathfrak{p} \cap \Lambda$, it is full. By (2.13), $\mathfrak{q} = \mathfrak{P} \cap \mathcal{O}$ is a full prime ideal of $\mathcal{O}$. Suppose $\mathfrak{q} \neq \mathfrak{p}$. Choose $s \in S_\mathfrak{p} \cap \mathfrak{q}$, which is possible by (2.2). According to (2.12), there is an $s' \in \mathcal{O}$ such that $ss' \equiv 1 \bmod \mathfrak{C}_\mathfrak{p} \cap \Lambda$. Then

$$1 = ss' + (1 - ss') \in \mathfrak{P} + (\mathfrak{C}_\mathfrak{p} \cap \Lambda)$$

and $\mathfrak{C}_\mathfrak{p} \cap \Lambda \not\subset \mathfrak{P}$, a contradiction. Therefore $\mathfrak{P} \cap \mathcal{O} = \mathfrak{p}$. ■

Proof of (2.9). First, suppose $\mathfrak{p}$ does not contain $\mathfrak{c} = \mathfrak{C} \cap \mathcal{O}$. Then $S_\mathfrak{p} \cap \mathfrak{c}$ is not empty by (2.2), so $\mathfrak{C}_\mathfrak{p}$ contains a unit of $\Lambda_\mathfrak{p}$. Therefore $\Lambda_\mathfrak{p}/\mathfrak{C}_\mathfrak{p}$ can only be nontrivial if $\mathfrak{p}$ is one of the finitely many prime ideals above $\mathfrak{c}$.
For $\mathfrak{p} \supset \mathfrak{c}$, consider the composition of the canonical homomorphisms

$$\Lambda \to \Lambda_\mathfrak{p} \to \Lambda_\mathfrak{p}/\mathfrak{C}_\mathfrak{p}.$$

It is surjective because if $X \in \Lambda_\mathfrak{p}$, we may choose an $s \in S_\mathfrak{p}$ with $sX \in \Lambda$ and, by (2.12), an $s' \in \mathcal{O}$ with $ss' \equiv 1 \bmod \mathfrak{C}_\mathfrak{p} \cap \Lambda$. The matrix $ss'X$ is mapped onto the residue class $X + \mathfrak{C}_\mathfrak{p}$, therefore we have $\Lambda/(\mathfrak{C}_\mathfrak{p} \cap \Lambda) \simeq \Lambda_\mathfrak{p}/\mathfrak{C}_\mathfrak{p}$.
Moreover, $\mathfrak{C}_\mathfrak{p} \cap \Lambda$ and $\mathfrak{C}_\mathfrak{q} \cap \Lambda$ are coprime for $\mathfrak{p} \neq \mathfrak{q}$; otherwise their sum were contained in a maximal two-sided ideal, a contradiction to (2.14). By (2.10) we have

$$\mathfrak{C} = \mathfrak{C} \cap \Lambda = (\bigcap_\mathfrak{p} \mathfrak{C}_\mathfrak{p}) \cap \Lambda = \bigcap_\mathfrak{p} (\mathfrak{C}_\mathfrak{p} \cap \Lambda).$$

Using this, the Chinese Remainder Theorem and the just established isomorphy, we obtain

$$\Lambda/\mathfrak{C} = \Lambda/\bigcap_\mathfrak{p}(\mathfrak{C}_\mathfrak{p} \cap \Lambda) \simeq \bigoplus_\mathfrak{p} \Lambda/(\mathfrak{C}_\mathfrak{p} \cap \Lambda) \simeq \bigoplus_\mathfrak{p} \Lambda_\mathfrak{p}/\mathfrak{C}_\mathfrak{p}.$$ ■

(2.15) Corollary. For every $\mathfrak{p}$, let $\nu_\mathfrak{p}$ be an integer with $\mathfrak{p}_\mathfrak{p}^{\nu_\mathfrak{p}} \subset \mathfrak{c}_\mathfrak{p}$. Then

$$\Lambda/\mathfrak{C} \simeq \bigoplus_\mathfrak{p} \Lambda/(\mathfrak{C} + \mathfrak{p}^{\nu_\mathfrak{p}}\Lambda).$$

Proof. Since $\mathfrak{p}$ is the only prime ideal above $\mathfrak{c} + \mathfrak{p}^{\nu_\mathfrak{p}} = (\mathfrak{C} + \mathfrak{p}^{\nu_\mathfrak{p}}\Lambda) \cap \mathcal{O}$, we have

$$\Lambda/\mathfrak{C} \simeq \bigoplus_\mathfrak{p} \Lambda_\mathfrak{p}/\mathfrak{C}_\mathfrak{p} = \bigoplus_\mathfrak{p} \Lambda_\mathfrak{p}/(\mathfrak{C}_\mathfrak{p} + \mathfrak{p}_\mathfrak{p}^{\nu_\mathfrak{p}}\Lambda_\mathfrak{p}) \simeq \bigoplus_\mathfrak{p} \Lambda/(\mathfrak{C} + \mathfrak{p}^{\nu_\mathfrak{p}}\Lambda)$$

where (2.9) is applied twice. ■

We are now left with the task of proving the existence of exponents as in (2.15). The next proposition and the subsequent corollary will give us two lower bounds for each $\nu_\mathfrak{p}$, the second one potentially larger but easier to compute. Afterwards, we will discuss how to obtain the smallest exponent possible.

(2.16) Proposition. Let $\mathfrak{c}$ be a full ideal and $\mathfrak{p}$ a full prime ideal of $\mathcal{O}$. Let p be the characteristic of the field $\mathcal{O}/\mathfrak{p}$ and let ν be an integer satisfying

$$\nu \geq \frac{v_p[\mathcal{O}_\mathfrak{p} : \mathfrak{c}_\mathfrak{p}]}{v_p[\mathcal{O}_\mathfrak{p} : \mathfrak{p}_\mathfrak{p}]}$$

where v_p denotes the p-adic valuation. Then $\mathfrak{p}_\mathfrak{p}^\nu \subset \mathfrak{c}_\mathfrak{p}$.[1]

[1] Result (2.16) is based on proposition 4.2 by Klüners and Pauli (2005).

Proof. First, if $\mathfrak{c} \not\subset \mathfrak{p}$, then $\mathfrak{c}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}$, and the assertion is obvious. So for the rest of the proof assume $\mathfrak{c} \subset \mathfrak{p}$.

By (2.9) the quotient ring $\mathcal{O}_\mathfrak{p}/\mathfrak{c}_\mathfrak{p}$ is finite. As an $\mathcal{O}_\mathfrak{p}$-module it is annihilated by some power of $\mathfrak{p}_\mathfrak{p}$,[1] hence $\mathfrak{p}_\mathfrak{p}^n \subset \mathfrak{c}_\mathfrak{p}$ for a suitable n. Choose n as small as possible and consider the sequence

(2.17) $$\mathcal{O}_\mathfrak{p}/\mathfrak{c}_\mathfrak{p} \supset (\mathfrak{c}_\mathfrak{p} + \mathfrak{p}_\mathfrak{p})/\mathfrak{c}_\mathfrak{p} \supset (\mathfrak{c}_\mathfrak{p} + \mathfrak{p}_\mathfrak{p}^2)/\mathfrak{c}_\mathfrak{p} \supset \cdots \supset (\mathfrak{c}_\mathfrak{p} + \mathfrak{p}_\mathfrak{p}^n)/\mathfrak{c}_\mathfrak{p} = 0.$$

We will show that each quotient

$$\frac{(\mathfrak{c}_\mathfrak{p} + \mathfrak{p}_\mathfrak{p}^{k-1})/\mathfrak{c}_\mathfrak{p}}{(\mathfrak{c}_\mathfrak{p} + \mathfrak{p}_\mathfrak{p}^{k})/\mathfrak{c}_\mathfrak{p}} \simeq \frac{\mathfrak{c}_\mathfrak{p} + \mathfrak{p}_\mathfrak{p}^{k-1}}{\mathfrak{c}_\mathfrak{p} + \mathfrak{p}_\mathfrak{p}^{k}} \quad (k \leq n)$$

is nontrivial. By our choice of n, this is clear for $k = n$. For the remaining quotients (i.e., if $n > 1$), we reduce all modules in (2.17) by $(\mathfrak{c}_\mathfrak{p} + \mathfrak{p}_\mathfrak{p}^{n-1})/\mathfrak{c}_\mathfrak{p}$, obtaining

$$\mathcal{O}_\mathfrak{p}/(\mathfrak{c}_\mathfrak{p} + \mathfrak{p}_\mathfrak{p}^{n-1}) \supset (\mathfrak{c}_\mathfrak{p} + \mathfrak{p}_\mathfrak{p})/(\mathfrak{c}_\mathfrak{p} + \mathfrak{p}_\mathfrak{p}^{n-1}) \supset \cdots \supset (\mathfrak{c}_\mathfrak{p} + \mathfrak{p}_\mathfrak{p}^{n-1})/(\mathfrak{c}_\mathfrak{p} + \mathfrak{p}_\mathfrak{p}^{n-1}) = 0.$$

This is essentially sequence (2.17) where $\mathfrak{c}_\mathfrak{p}$ is replaced by $\mathfrak{c}_\mathfrak{p} + \mathfrak{p}_\mathfrak{p}^{n-1}$ because

$$\mathfrak{c}_\mathfrak{p} + \mathfrak{p}_\mathfrak{p}^{k} = (\mathfrak{c}_\mathfrak{p} + \mathfrak{p}_\mathfrak{p}^{n-1}) + \mathfrak{p}_\mathfrak{p}^{k} \quad \text{for } k < n.$$

Notice that the new sequence contains one module less. Moreover, $n-1$ is the smallest integer such that $\mathfrak{p}_\mathfrak{p}^{n-1} \subset \mathfrak{c}_\mathfrak{p} + \mathfrak{p}_\mathfrak{p}^{n-1}$. So by induction we may assume that each quotient

$$\frac{(\mathfrak{c}_\mathfrak{p} + \mathfrak{p}_\mathfrak{p}^{k-1})/(\mathfrak{c}_\mathfrak{p} + \mathfrak{p}_\mathfrak{p}^{n-1})}{(\mathfrak{c}_\mathfrak{p} + \mathfrak{p}_\mathfrak{p}^{k})/(\mathfrak{c}_\mathfrak{p} + \mathfrak{p}_\mathfrak{p}^{n-1})} \simeq \frac{\mathfrak{c}_\mathfrak{p} + \mathfrak{p}_\mathfrak{p}^{k-1}}{\mathfrak{c}_\mathfrak{p} + \mathfrak{p}_\mathfrak{p}^{k}} \quad (k < n)$$

is nontrivial, establishing our statement.

We will now refine our original sequence to a composition series

$$\mathcal{O}_\mathfrak{p}/\mathfrak{c}_\mathfrak{p} = \mathfrak{m}_0 \supset \mathfrak{m}_1 \supset \cdots \supset \mathfrak{m}_\nu = 0,$$

that is, each module in (2.17) is equal to some $\mathfrak{m}_i$ and the quotients $\mathfrak{m}_{i-1}/\mathfrak{m}_i$ are simple nonzero $\mathcal{O}_\mathfrak{p}$-modules. Since the modules in (2.17) are all distinct, we have $\nu \geq n$ and therefore $\mathfrak{p}_\mathfrak{p}^\nu \subset \mathfrak{c}_\mathfrak{p}$.

To complete the proof, we will show that ν is equal to the stated lower bound. Since $\mathcal{O}_\mathfrak{p}$ is a local ring, the only nontrivial simple $\mathcal{O}_\mathfrak{p}$-module is $\mathcal{O}_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}$, so

$$\mathfrak{m}_{i-1}/\mathfrak{m}_i \simeq \mathcal{O}_\mathfrak{p}/\mathfrak{p}_\mathfrak{p} \quad \text{for } 1 \leq i \leq \nu.$$

Applying v_p to the left- and right-hand side of

$$[\mathcal{O}_\mathfrak{p} : \mathfrak{c}_\mathfrak{p}] = [\mathfrak{m}_0 : \mathfrak{m}_1] \cdots [\mathfrak{m}_{\nu-1} : \mathfrak{m}_\nu] = [\mathcal{O}_\mathfrak{p} : \mathfrak{p}_\mathfrak{p}]^\nu,$$

we obtain $v_p[\mathcal{O}_\mathfrak{p} : \mathfrak{c}_\mathfrak{p}] = \nu \cdot v_p[\mathcal{O}_\mathfrak{p} : \mathfrak{p}_\mathfrak{p}]$. ■

[1] Cf. Eisenbud (1995), p. 77, corollary 2.17.

(2.18) Corollary. If $\nu \geq v_p[\mathcal{O} : \mathfrak{c}]/v_p[\mathcal{O} : \mathfrak{p}]$, then $\mathfrak{p}_\mathfrak{p}^\nu \subset \mathfrak{c}_\mathfrak{p}$.[1]

Proof. Since $\mathcal{O}/\mathfrak{p} \simeq \mathcal{O}_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}$ by (2.9), we see that $v_p[\mathcal{O} : \mathfrak{p}] = v_p[\mathcal{O}_\mathfrak{p} : \mathfrak{p}_\mathfrak{p}]$. So by (2.16) it suffices to show that $v_p[\mathcal{O} : \mathfrak{c}] \geq v_p[\mathcal{O}_\mathfrak{p} : \mathfrak{c}_\mathfrak{p}]$. Let ν be any integer with $\mathfrak{p}_\mathfrak{p}^\nu \subset \mathfrak{c}_\mathfrak{p}$. As $\mathfrak{p}$ is the only prime ideal above $\mathfrak{c} + \mathfrak{p}^\nu$, (2.9) yields

$$\mathcal{O}/(\mathfrak{c} + \mathfrak{p}^\nu) \simeq \mathcal{O}_\mathfrak{p}/(\mathfrak{c}_\mathfrak{p} + \mathfrak{p}_\mathfrak{p}^\nu) = \mathcal{O}_\mathfrak{p}/\mathfrak{c}_\mathfrak{p}.$$

Therefore $[\mathcal{O}_\mathfrak{p} : \mathfrak{c}_\mathfrak{p}]$ divides $[\mathcal{O} : \mathfrak{c}] = [\mathcal{O} : \mathfrak{c} + \mathfrak{p}^\nu][\mathfrak{c} + \mathfrak{p}^\nu : \mathfrak{c}]$. ■

(2.19) Proposition. Let n be any integer with $\mathfrak{p}_\mathfrak{p}^n \subset \mathfrak{c}_\mathfrak{p}$ and let ν be the smallest integer with $\mathfrak{p}^\nu \subset \mathfrak{c} + \mathfrak{p}^n$. Then ν is the smallest integer with $\mathfrak{p}_\mathfrak{p}^\nu \subset \mathfrak{c}_\mathfrak{p}$.

Proof. First, let ν be any integer not surpassing n. If $\mathfrak{p}^\nu \subset \mathfrak{c} + \mathfrak{p}^n$, then $\mathfrak{p}_\mathfrak{p}^\nu \subset \mathfrak{c}_\mathfrak{p} + \mathfrak{p}_\mathfrak{p}^n = \mathfrak{c}_\mathfrak{p}$. Conversely, let $\mathfrak{p}_\mathfrak{p}^\nu \subset \mathfrak{c}_\mathfrak{p}$. Since $\mathfrak{p}_\mathfrak{p}^\nu$ and $\mathfrak{c}_\mathfrak{p}$ both contain $\mathfrak{p}_\mathfrak{p}^n$, we have the inclusion

$$\mathfrak{p}_\mathfrak{p}^\nu/\mathfrak{p}_\mathfrak{p}^n \subset \mathfrak{c}_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}^n = (\mathfrak{c}_\mathfrak{p} + \mathfrak{p}_\mathfrak{p}^n)/\mathfrak{p}_\mathfrak{p}^n.$$

By (2.9) we know that the canonical map $\mathcal{O}/\mathfrak{p}^n \to \mathcal{O}_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}^n$ is an isomorphism, hence

$$\mathfrak{p}^\nu/\mathfrak{p}^n \subset (\mathfrak{c} + \mathfrak{p}^n)/\mathfrak{p}^n,$$

which implies $\mathfrak{p}^\nu \subset \mathfrak{c} + \mathfrak{p}^n$.
In conclusion, if ν is the smallest integer with $\mathfrak{p}^\nu \subset \mathfrak{c} + \mathfrak{p}^n$, it is also minimal under the condition $\mathfrak{p}_\mathfrak{p}^\nu \subset \mathfrak{c}_\mathfrak{p}$, and vice versa. ■

Using (2.18) and (2.19), we can compute the smallest exponent ν satisfying $\mathfrak{p}_\mathfrak{p}^\nu \subset \mathfrak{c}_\mathfrak{p}$. The next proposition exhibits an alternative approach, provided that $\mathfrak{c}$ has the property

$$\mathfrak{c}\mathcal{O}_\mathcal{K} \cap \mathcal{O} = \mathfrak{c}.$$

Clearly, the conductor satisfies this condition, and so do all ideals coprime to $\mathfrak{f}$ by (2.7).

(2.20) Proposition. Let $\mathfrak{c}$ be a full ideal of $\mathcal{O}$ such that $\mathfrak{c}\mathcal{O}_\mathcal{K} \cap \mathcal{O} = \mathfrak{c}$. Let $\mathfrak{p}$ be a full prime ideal of $\mathcal{O}$ and let $\mathfrak{Q}$ be the set of prime ideals of $\mathcal{O}_\mathcal{K}$ containing $\mathfrak{p}$. Let

$$\mathfrak{p}\mathcal{O}_\mathcal{K} = \prod_{\mathfrak{q} \in \mathfrak{Q}} \mathfrak{q}^{e_\mathfrak{q}} \quad \text{and} \quad \mathfrak{c}\mathcal{O}_\mathcal{K} = (\prod_{\mathfrak{q} \in \mathfrak{Q}} \mathfrak{q}^{\nu_\mathfrak{q}})\mathfrak{c}'$$

where $\mathfrak{c}'$ is not divided by any $\mathfrak{q} \in \mathfrak{Q}$. Then $\nu = \max_\mathfrak{q} \lceil \nu_\mathfrak{q}/e_\mathfrak{q} \rceil$ is the smallest integer satisfying $\mathfrak{p}_\mathfrak{p}^\nu \subset \mathfrak{c}_\mathfrak{p}$.

Proof. For all $\mathfrak{q} \in \mathfrak{Q}$, we have

$$\nu e_\mathfrak{q} \geq \lceil \nu_\mathfrak{q}/e_\mathfrak{q} \rceil e_\mathfrak{q} \geq (\nu_\mathfrak{q}/e_\mathfrak{q}) e_\mathfrak{q} = \nu_\mathfrak{q},$$

and therefore

$$\mathfrak{p}^\nu \subset \mathfrak{p}^\nu \mathcal{O}_\mathcal{K} = \prod_\mathfrak{q} \mathfrak{q}^{\nu e_\mathfrak{q}} \subset \prod_\mathfrak{q} \mathfrak{q}^{\nu_\mathfrak{q}}.$$

[1] Results (2.18) and (2.20) are based on statements 4.2 and 7.4 by Klüners and Pauli (2005).

Furthermore, $\mathfrak{c}_\mathfrak{p} = (\mathfrak{c}\mathcal{O}_\mathcal{K})_\mathfrak{p} \cap \mathcal{O}_\mathfrak{p}$, for if $c \in (\mathfrak{c}\mathcal{O}_\mathcal{K})_\mathfrak{p} \cap \mathcal{O}_\mathfrak{p}$, then $sc \in (\mathfrak{c}\mathcal{O}_\mathcal{K}) \cap \mathcal{O} = \mathfrak{c}$ for a suitable $s \in S_\mathfrak{p}$, so $c \in \mathfrak{c}_\mathfrak{p}$ and $(\mathfrak{c}\mathcal{O}_\mathcal{K})_\mathfrak{p} \cap \mathcal{O}_\mathfrak{p} \subset \mathfrak{c}_\mathfrak{p}$. The converse inclusion is trivial.

Taken together, we obtain

$$\mathfrak{c}_\mathfrak{p} = (\mathfrak{c}\mathcal{O}_\mathcal{K})_\mathfrak{p} \cap \mathcal{O}_\mathfrak{p} = (\prod_\mathfrak{q} \mathfrak{q}_\mathfrak{p}^{\nu_\mathfrak{q}}) \cap \mathcal{O}_\mathfrak{p} \supset \mathfrak{p}_\mathfrak{p}^\nu.$$

It remains to show that ν is minimal. Choose $\mathfrak{q} \in \mathfrak{Q}$ such that $\nu = \lceil \nu_\mathfrak{q}/e_\mathfrak{q} \rceil$. Then

$$(\nu - 1)e_\mathfrak{q} = (\lceil \nu_\mathfrak{q}/e_\mathfrak{q} \rceil - 1)e_\mathfrak{q} < (\nu_\mathfrak{q}/e_\mathfrak{q})e_\mathfrak{q} = \nu_\mathfrak{q},$$

so

$$(\mathfrak{p}^{\nu-1}\mathcal{O}_\mathcal{K})_\mathfrak{p} = \prod_\mathfrak{q} \mathfrak{q}_\mathfrak{p}^{(\nu-1)e_\mathfrak{q}} \not\subset \prod_\mathfrak{q} \mathfrak{q}_\mathfrak{p}^{\nu_\mathfrak{q}}.$$

In conclusion, $\mathfrak{p}_\mathfrak{p}^{\nu-1}$ cannot be contained in $(\prod \mathfrak{q}_\mathfrak{p}^{\nu_\mathfrak{q}}) \cap \mathcal{O}_\mathfrak{p} = \mathfrak{c}_\mathfrak{p}$. ■

2.3 Characterization of Units

At the the end of section 1.5, we characterized the units of a multiplier algebra in terms of determinants. Our next goal is to obtain an analogous result for localizations. Recall that the determinant of a matrix in $\mathrm{M}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$ is defined as its image under the map

$$\det\colon \mathrm{M}(\boldsymbol{n}, \boldsymbol{\mathcal{K}}) \to \boldsymbol{\mathcal{K}}, \quad \det(\mathit{\Gamma}) = \det(\mathit{\Gamma}_1) \oplus \cdots \oplus \det(\mathit{\Gamma}_s)$$

where each summand is the usual determinant of a matrix over a field. Also remember that $\mathit{\Gamma}$ is called nonsingular if each component has full rank.

As usual, Λ will be the multiplier algebra of a full module $\mathfrak{A}$. In complete analogy to the definition in section 1.4, the set of all matrices $\mathit{\Gamma} \in \mathrm{M}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$ with

$$\mathit{\Gamma}\mathfrak{A}_\mathfrak{p} \subset \mathfrak{A}_\mathfrak{p}$$

will be called the **multiplier algebra** of $\mathfrak{A}_\mathfrak{p}$, which, in fact, coincides with $\Lambda_\mathfrak{p}$.

(2.21) Lemma. Let $\mathcal{O}$ be the center of Λ and let $\mathfrak{p}$ be a full prime ideal of $\mathcal{O}$. Then $\Lambda_\mathfrak{p}$ is the multiplier algebra of $\mathfrak{A}_\mathfrak{p}$. Moreover,

$$\mathit{\Gamma} \in \Lambda_\mathfrak{p}^\times \quad \Leftrightarrow \quad \mathit{\Gamma}\mathfrak{A}_\mathfrak{p} = \mathfrak{A}_\mathfrak{p}.$$

Proof. Suppose $\mathit{\Gamma} \in \mathrm{M}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$ satisfies $\mathit{\Gamma}\mathfrak{A}_\mathfrak{p} \subset \mathfrak{A}_\mathfrak{p}$. Let $\xi_1, \ldots, \xi_m$ be a set of generators of $\mathfrak{A}$. These vectors also generate $\mathfrak{A}_\mathfrak{p}$ as an $\mathcal{O}_\mathfrak{p}$-module, thus we have coefficients $\gamma_{ij} \in \mathcal{O}_\mathfrak{p}$ with $\mathit{\Gamma}\xi_i = \sum \gamma_{ij}\xi_j$. Choose $s \in S_\mathfrak{p}$ such that $s\gamma_{ij} \in \mathcal{O}$ for all i and j. Then

$$s\mathit{\Gamma}\xi_i = \sum (s\gamma_{ij})\xi_j \in \mathfrak{A} \quad \text{for all } i,$$

so $s\mathit{\Gamma} \in \Lambda$ and $\mathit{\Gamma} \in \Lambda_\mathfrak{p}$. Conversely, each $\mathit{\Gamma} \in \Lambda_\mathfrak{p}$ satisfies $\mathit{\Gamma}\mathfrak{A}_\mathfrak{p} \subset \mathfrak{A}_\mathfrak{p}$. Hence $\Lambda_\mathfrak{p}$ is the multiplier algebra of $\mathfrak{A}_\mathfrak{p}$.

Now let $\mathit{\Gamma} \in \Lambda_{\mathfrak{p}}^{\times}$. Then

$$\mathfrak{A}_{\mathfrak{p}} = \mathit{\Gamma}\mathit{\Gamma}^{-1}\mathfrak{A}_{\mathfrak{p}} \subset \mathit{\Gamma}\mathfrak{A}_{\mathfrak{p}} \subset \mathfrak{A}_{\mathfrak{p}},$$

so $\mathit{\Gamma}\mathfrak{A}_{\mathfrak{p}} = \mathfrak{A}_{\mathfrak{p}}$. On the other hand, if $\mathit{\Gamma}\mathfrak{A}_{\mathfrak{p}} = \mathfrak{A}_{\mathfrak{p}}$, then $\mathit{\Gamma}$ has to be nonsingular due to $\mathbb{Q} \cdot \mathfrak{A}_{\mathfrak{p}} = \boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$. Thus we may conclude $\mathit{\Gamma}^{-1}\mathfrak{A}_{\mathfrak{p}} = \mathfrak{A}_{\mathfrak{p}}$, so $\mathit{\Gamma}$ and $\mathit{\Gamma}^{-1}$ both belong to $\Lambda_{\mathfrak{p}}$. ∎

(2.22) Theorem. Let Λ be the multiplier algebra of a full module $\mathfrak{A}$ in $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$. Let $\mathcal{O}$ be the center of Λ and let $\mathfrak{p}$ be a full prime ideal of $\mathcal{O}$. Then

$$\mathit{\Gamma} \in \Lambda_{\mathfrak{p}}^{\times} \quad \Leftrightarrow \quad \det(\mathit{\Gamma}) \in (\mathcal{O}_{\boldsymbol{\mathcal{K}}})_{\mathfrak{p}}^{\times}.$$

Proof. We will prove that

$$\Lambda_{\mathfrak{p}}^{\times} = \Lambda_{\mathfrak{p}} \cap (\Lambda_{\boldsymbol{\mathcal{K}}})_{\mathfrak{p}}^{\times}$$

where $\Lambda_{\boldsymbol{\mathcal{K}}}$ is the multiplier algebra of $\mathfrak{A}_{\boldsymbol{\mathcal{K}}} = \mathfrak{A}\mathcal{O}_{\boldsymbol{\mathcal{K}}}$. From this the assertion will follow immediately.

Without restriction we may assume that $\mathfrak{A}_{\boldsymbol{\mathcal{K}}} = \mathfrak{A}_{\mathcal{K}_1} \oplus \cdots \oplus \mathfrak{A}_{\mathcal{K}_s}$ is a subset of $\mathcal{O}_{\boldsymbol{\mathcal{K}}}^{\boldsymbol{n}}$ and that each component of is of the form $\mathfrak{a}_{\iota} \oplus \mathcal{O}_{\mathcal{K}_{\iota}}^{n_{\iota}-1}$. Applying (1.15) to each $\mathfrak{a}_{\iota}$, we further may assume that $\mathfrak{a} = \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_s$ is coprime to the product of all prime ideals of $\mathcal{O}_{\boldsymbol{\mathcal{K}}}$ containing $\mathfrak{p}$. By (2.6), $\mathfrak{a}_{\mathfrak{p}}$ is not contained in any prime ideal of $(\mathcal{O}_{\boldsymbol{\mathcal{K}}})_{\mathfrak{p}}$. Write $\tilde{\mathcal{O}} = \mathcal{O}_{\boldsymbol{\mathcal{K}}}$. Then

$$(\mathfrak{A}_{\boldsymbol{\mathcal{K}}})_{\mathfrak{p}} = \tilde{\mathcal{O}}_{\mathfrak{p}}^{\boldsymbol{n}} \quad \text{and} \quad (\Lambda_{\boldsymbol{\mathcal{K}}})_{\mathfrak{p}} = \mathrm{M}(\boldsymbol{n}, \tilde{\mathcal{O}}_{\mathfrak{p}}).$$

Let $\mathfrak{f}$ be the conductor of $\mathcal{O} \subset \tilde{\mathcal{O}}$. Put

$$\overline{\mathfrak{A}_{\mathfrak{p}}} = \mathfrak{A}_{\mathfrak{p}}/\mathfrak{f}\mathfrak{A}_{\mathfrak{p}}.$$

Due to $\mathfrak{f}\mathfrak{A}_{\mathfrak{p}} = \mathfrak{f}\tilde{\mathcal{O}}\mathfrak{A}_{\mathfrak{p}} = \mathfrak{f}\tilde{\mathcal{O}}_{\mathfrak{p}}^{\boldsymbol{n}}$, this is a subset of

$$\tilde{\mathcal{O}}_{\mathfrak{p}}^{\boldsymbol{n}}/\mathfrak{f}\tilde{\mathcal{O}}_{\mathfrak{p}}^{\boldsymbol{n}} = (\tilde{\mathcal{O}}_{\mathfrak{p}}/\mathfrak{f}_{\mathfrak{p}})^{\boldsymbol{n}},$$

which is finite by (2.9). Obviously, $(\Lambda_{\boldsymbol{\mathcal{K}}})_{\mathfrak{p}}^{\times} = \mathrm{GL}(\boldsymbol{n}, \tilde{\mathcal{O}}_{\mathfrak{p}}/\mathfrak{f}_{\mathfrak{p}})$ acts faithfully on $(\tilde{\mathcal{O}}_{\mathfrak{p}}/\mathfrak{f}_{\mathfrak{p}})^{\boldsymbol{n}}$ via $\bar{\mathit{\Gamma}}\bar{\xi} = \overline{\mathit{\Gamma}\xi}$. Let $\mathit{\Gamma} \in \Lambda_{\mathfrak{p}} \cap (\Lambda_{\boldsymbol{\mathcal{K}}})_{\mathfrak{p}}^{\times}$. Then

$$\overline{\mathit{\Gamma}\mathfrak{A}_{\mathfrak{p}}} \subset \overline{\mathfrak{A}_{\mathfrak{p}}}.$$

Since $\bar{\mathit{\Gamma}}$ represents a bijection of $(\tilde{\mathcal{O}}_{\mathfrak{p}}/\mathfrak{f}_{\mathfrak{p}})^{\boldsymbol{n}}$, the sets $\overline{\mathit{\Gamma}\mathfrak{A}_{\mathfrak{p}}}$ and $\overline{\mathfrak{A}_{\mathfrak{p}}}$ contain the same number of elements, hence they are equal. Therefore

$$\mathit{\Gamma}\mathfrak{A}_{\mathfrak{p}} + \mathfrak{f}\tilde{\mathcal{O}}_{\mathfrak{p}}^{\boldsymbol{n}} = \mathfrak{A}_{\mathfrak{p}} + \mathfrak{f}\tilde{\mathcal{O}}_{\mathfrak{p}}^{\boldsymbol{n}} = \mathfrak{A}_{\mathfrak{p}},$$

and we conclude

$$\mathit{\Gamma}\mathfrak{A}_{\mathfrak{p}} = \mathit{\Gamma}(\mathfrak{A}_{\mathfrak{p}} + \mathfrak{f}\tilde{\mathcal{O}}_{\mathfrak{p}}^{\boldsymbol{n}}) = \mathit{\Gamma}\mathfrak{A}_{\mathfrak{p}} + \mathfrak{f}(\mathit{\Gamma}\tilde{\mathcal{O}}_{\mathfrak{p}}^{\boldsymbol{n}}) = \mathit{\Gamma}\mathfrak{A}_{\mathfrak{p}} + \mathfrak{f}\tilde{\mathcal{O}}_{\mathfrak{p}}^{\boldsymbol{n}} = \mathfrak{A}_{\mathfrak{p}}.$$

This implies $\mathit{\Gamma} \in \Lambda_{\mathfrak{p}}^{\times}$ by (2.21), so $\Lambda_{\mathfrak{p}} \cap (\Lambda_{\boldsymbol{\mathcal{K}}})_{\mathfrak{p}}^{\times} \subset \Lambda_{\mathfrak{p}}^{\times}$. The converse inclusion is trivial. ∎

2.4 Making Ideals Coprime to the Conductor

In this section we will explain how to make ideals coprime to the conductor, if possible. This is motivated by our considerations at the end of section 1.6. Again, $\mathfrak{C} = (\mathfrak{B} : \mathfrak{A})$ will be the multiplier ideal of two full modules and $\mathfrak{F}$ will be the conductor of $\Lambda \subset \Lambda_{\mathcal{K}}$ where Λ and $\Lambda_{\mathcal{K}}$ are the multiplier algebras of $\mathfrak{A}$ and $\mathfrak{A}_{\mathcal{K}} = \mathfrak{A}\mathcal{O}_{\mathcal{K}}$. Making $\mathfrak{C}$ coprime to $\mathfrak{F}$ means finding a $\Gamma \in \mathrm{GL}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$ such that

$$\Gamma\mathfrak{C} + \mathfrak{F} = \Lambda.$$

If no such Γ exists, $\mathfrak{C}$ clearly cannot be principal. However, if $\mathfrak{C} = \Gamma\Lambda$, then $\mathfrak{C}' = \Lambda\Gamma^{-1}$ is a full fractional left ideal of Λ and

$$\mathfrak{C}'\mathfrak{C} = \Lambda.$$

Hence it makes sense to say that $\mathfrak{C}'$ is an inverse of $\mathfrak{C}$. More generally, any full right ideal $\mathfrak{C}$ will be called **invertible** if there is a full fractional left ideal $\mathfrak{C}'$ such that $\mathfrak{C}'\mathfrak{C} = \Lambda$. Since we actually want to examine whether $\mathfrak{C}$ is principal, we may assume that $\mathfrak{C}$ is invertible.

Unlike for ideals of orders of $\boldsymbol{\mathcal{K}}$, the inverse of a right ideal of a matrix order has not to be unique. For example, let $\mathcal{O}$ be an order in a number field, $\mathfrak{c}$ a proper ideal of $\mathcal{O}$ and $\Lambda = \mathrm{M}(2, \mathcal{O})$. Then

$$\mathfrak{C} = \begin{bmatrix} \mathfrak{c} & \mathfrak{c} \\ \mathcal{O} & \mathcal{O} \end{bmatrix}$$

is a full right ideal of Λ and

$$\mathfrak{C}' = \begin{bmatrix} (\mathfrak{c} : \mathcal{O}) & \mathcal{O} \\ (\mathfrak{c} : \mathcal{O}) & \mathcal{O} \end{bmatrix} \quad \text{as well as} \quad \mathfrak{C}'' = \Lambda$$

are inverses of $\mathfrak{C}$ because both ideals contain $I = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$ and $J = \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right]$, and

$$I\mathfrak{C} + J\mathfrak{C} = \Lambda.$$

Nonetheless, if $\mathfrak{C}$ is an invertible right ideal, we always have a largest inverse (containing all the others), namely

$$\mathfrak{C}^{-1} = \{\, \Gamma \in \mathrm{M}(\boldsymbol{n}, \boldsymbol{\mathcal{K}}) \mid \Gamma\mathfrak{C} \subset \Lambda \,\}.$$

Therefore we can speak of *the* inverse of $\mathfrak{C}$ in reference to $\mathfrak{C}^{-1}$. In the example above, $\mathfrak{C}^{-1} = \mathfrak{C}'$.

We now come to the main result of this section. As usual, $\mathfrak{f}$ is the conductor of $\mathcal{O} \subset \mathcal{O}_{\mathcal{K}}$ where $\mathcal{O}$ is the center of Λ, so $\mathfrak{F} = \mathfrak{f}\Lambda_{\mathcal{K}}$. In addition, $\mathfrak{p}$ will always denote a full prime ideal of $\mathcal{O}$.

(2.23) Theorem. Let $\mathfrak{C}$ be an invertible right ideal of Λ. Then $\mathfrak{C}$ can be made coprime to $\mathfrak{F}$ if and only if $\mathfrak{C}_{\mathfrak{p}}$ is a principal ideal for each $\mathfrak{p} \supset \mathfrak{f}$.

To prove this theorem, we need to combine the statements (2.24), (2.26) and (2.28) below. The first statement will translate the property $\mathfrak{C} + \mathfrak{F} = \Lambda$ into local terms.

(2.24) Proposition. An ideal $\mathfrak{C} \subset \Lambda$ satisfies $\mathfrak{C} + \mathfrak{F} = \Lambda$ if and only if

$$\mathfrak{C}_\mathfrak{p} = \Lambda_\mathfrak{p} \quad \text{for all } \mathfrak{p} \supset \mathfrak{f}.$$

Proof. Let $\mathfrak{p}$ be a prime ideal above $\mathfrak{f}$ and suppose $\mathfrak{C}$ is coprime to $\mathfrak{F}$. Then we have a $C \in \mathfrak{C}$ and an $F \in \mathfrak{F}$ such that $C + F = I$, that is,

$$C \equiv I \mod \mathfrak{F}.$$

Since $\mathfrak{F} = \mathfrak{f}\Lambda_\mathcal{K}$, (1.35) yields

$$\det(C) \equiv \det(I) = 1 \mod \mathfrak{f}.$$

Therefore $\det(C)$ is not contained in any prime ideal of $\mathcal{O}_\mathcal{K}$ containing $\mathfrak{f}$. In particular, the determinant does not belong to any prime ideal above $\mathfrak{p}$. Hence $\det(C)$ is a unit of $(\mathcal{O}_\mathcal{K})_\mathfrak{p}$ by (2.6), which implies $C \in \Lambda_\mathfrak{p}^\times$ by (2.22). Therefore

$$\mathfrak{C}_\mathfrak{p} = \Lambda_\mathfrak{p} \quad \text{for all } \mathfrak{p} \supset \mathfrak{f}.$$

Conversely, suppose $\mathfrak{C}_\mathfrak{p} = \Lambda_\mathfrak{p}$ for all $\mathfrak{p} \supset \mathfrak{f}$. Then, for every $\mathfrak{p} \supset \mathfrak{f}$, we can write

$$I = C_\mathfrak{p} s_\mathfrak{p}^{-1} \quad \text{with } C_\mathfrak{p} \in \mathfrak{C} \text{ and } s_\mathfrak{p} \in S_\mathfrak{p}.$$

Let $\mathfrak{c}$ be the largest ideal of $\mathcal{O}$ with the property $\mathfrak{c}\Lambda \subset \mathfrak{C}$. Because of

$$s_\mathfrak{p}\Lambda = (s_\mathfrak{p} I)\Lambda = C_\mathfrak{p}\Lambda \subset \mathfrak{C},$$

we have $s_\mathfrak{p} \in \mathfrak{c}$. Thus $\mathfrak{c}$ cannot be contained in any prime ideal above $\mathfrak{f}$. From this we conclude

$$\mathfrak{C} + \mathfrak{F} \supset \mathfrak{c}\Lambda + \mathfrak{f}\Lambda = (\mathfrak{c} + \mathfrak{f})\Lambda = \Lambda,$$

that is, $\mathfrak{C}$ is coprime to $\mathfrak{F}$. ■

By (2.24), $\Gamma\mathfrak{C} + \mathfrak{F} = \Lambda$ implies $\mathfrak{C}_\mathfrak{p} = \Gamma^{-1}\Lambda_\mathfrak{p}$ for each $\mathfrak{p} \supset \mathfrak{f}$, so one implication of theorem (2.23) is established. The converse direction requires a little more effort.

(2.25) Proposition. Let C, $C' \in \Lambda$ be nonsingular matrices. Let $\mathfrak{p}$ be a full prime ideal of $\mathcal{O}$ and let $\mathfrak{Q}$ be the set of prime ideals of $\mathcal{O}_\mathcal{K}$ containing $\mathfrak{p}$. For $\mathfrak{q} \in \mathfrak{Q}$, let $\nu_\mathfrak{q} = v_\mathfrak{q}(\det C)$ where $v_\mathfrak{q}$ denotes the $\mathfrak{q}$-adic valuation. Choose ν large enough so that $\mathfrak{p}^\nu\Lambda_\mathfrak{p} \subset C\Lambda_\mathfrak{p}$ and $\nu > \nu_\mathfrak{q}$ for all $\mathfrak{q}$. If $C \equiv C' \bmod \mathfrak{p}^\nu\Lambda$, then

$$C\Lambda_\mathfrak{p} = C'\Lambda_\mathfrak{p}.$$

Proof. By our assumptions, there is a $P \in \mathfrak{p}^\nu\Lambda$ such that $C' = C + P$. Because of $\mathfrak{p}^\nu\Lambda_\mathfrak{p} \subset C\Lambda_\mathfrak{p}$, we have $C' \in C\Lambda_\mathfrak{p}$, so $C' = CU$ for some nonsingular $U \in \Lambda_\mathfrak{p}$. We want to show that U is a unit of $\Lambda_\mathfrak{p}$, for this will imply

$$C'\Lambda_\mathfrak{p} = CU\Lambda_\mathfrak{p} = C\Lambda_\mathfrak{p}.$$

Let $\mathfrak{q} \in \mathfrak{Q}$. Then $C' \equiv C \bmod \mathfrak{q}^\nu \Lambda_{\mathcal{K}}$. By (1.35), this implies

$$\det(C)\det(U) = \det(C') \equiv \det(C) \mod \mathfrak{q}^\nu.$$

In particular,

$$\det(C)\det(U) \not\equiv 0 \mod \mathfrak{q}^{\nu_\mathfrak{q}+1}$$

because by our assumptions $\det(C) \notin \mathfrak{q}^{\nu_\mathfrak{q}+1}$ and $\nu \geq \nu_\mathfrak{q} + 1$. We claim that $\det(U)$ does not lie in $\mathfrak{q}_\mathfrak{p}$. Suppose it did. Put $c = \det(C)$ and $u = \det(U)$. Also, choose $s \in S_\mathfrak{p}$ such that $us \in \mathfrak{q}$. Then

$$cus \in \mathfrak{q}^{\nu_\mathfrak{q}+1} \quad \text{and} \quad cu \notin \mathfrak{q}^{\nu_\mathfrak{q}+1},$$

that is, s lies in $\mathfrak{q} \cap \mathcal{O} = \mathfrak{p}$, a contradiction. In conclusion, $\det(U)$ does not belong to any $\mathfrak{q}_\mathfrak{p}$. But these are all prime ideals of $(\mathcal{O}_{\mathcal{K}})_\mathfrak{p}$ by (2.6). Therefore $\det(U)$ is a unit of $(\mathcal{O}_{\mathcal{K}})_\mathfrak{p}$. By (2.22), U is a unit of $\Lambda_\mathfrak{p}$. ■

(2.26) Corollary. If $\mathfrak{C}$ satisfies $\mathfrak{C}_\mathfrak{p} = C_\mathfrak{p}\Lambda_\mathfrak{p}$ for all $\mathfrak{p} \supset \mathfrak{f}$, there is a $C \in \Lambda$ with

$$\mathfrak{C}_\mathfrak{p} = C\Lambda_\mathfrak{p} \quad \text{for all } \mathfrak{p} \supset \mathfrak{f}.$$

Proof. Apply (2.25) and the Chinese Remainder Theorem. ■

(2.27) Lemma. Let $\tilde{\mathfrak{p}}$ be a full prime ideal of $\mathcal{O}_{\mathcal{K}}$ and $\mathfrak{p} = \tilde{\mathfrak{p}} \cap \mathcal{O}$. If $\mathfrak{p}$ does not contain $\mathfrak{f}$, then

$$\Lambda_\mathfrak{p} = (\Lambda_{\mathcal{K}})_{\tilde{\mathfrak{p}}}.$$

Proof. First we prove that $\mathcal{O}_\mathfrak{p} = (\mathcal{O}_{\mathcal{K}})_{\tilde{\mathfrak{p}}}$.[1] Choose a nonzerodivisor $f \in \mathfrak{f} \smallsetminus \mathfrak{p}$, which is possible by (2.2). If $x \in \mathcal{O}_{\mathcal{K}}$ and $s \in S_{\tilde{\mathfrak{p}}}$, then $xf \in \mathcal{O}$, $sf \in S_\mathfrak{p}$ and

$$xs^{-1} = (xf)(sf)^{-1} \in \mathcal{O}_\mathfrak{p},$$

so $(\mathcal{O}_{\mathcal{K}})_{\tilde{\mathfrak{p}}} \subset \mathcal{O}_\mathfrak{p}$. The converse inclusion is obvious.
Since $\mathfrak{f}_\mathfrak{p}$ and $\mathfrak{f}_{\tilde{\mathfrak{p}}}$ both contain $ff^{-1} = 1$, we observe that

$$\mathfrak{f}_\mathfrak{p} = \mathcal{O}_\mathfrak{p} = (\mathcal{O}_{\mathcal{K}})_{\tilde{\mathfrak{p}}} = \mathfrak{f}_{\tilde{\mathfrak{p}}}.$$

Hence

$$\mathfrak{F}_\mathfrak{p} = (\mathfrak{f}\Lambda_{\mathcal{K}})_\mathfrak{p} = \mathfrak{f}_\mathfrak{p}\Lambda_{\mathcal{K}} = \mathfrak{f}_{\tilde{\mathfrak{p}}}\Lambda_{\mathcal{K}} = (\mathfrak{f}\Lambda_{\mathcal{K}})_{\tilde{\mathfrak{p}}} = \mathfrak{F}_{\tilde{\mathfrak{p}}}.$$

Since $\mathfrak{F}_\mathfrak{p}$ contains $(\mathfrak{f}\Lambda)_\mathfrak{p} = \mathfrak{f}_\mathfrak{p}\Lambda_\mathfrak{p} = \mathcal{O}_\mathfrak{p}\Lambda_\mathfrak{p} = \Lambda_\mathfrak{p}$, the identity matrix belongs to $\mathfrak{F}_\mathfrak{p}$. Therefore

$$\Lambda_\mathfrak{p} = \mathfrak{F}_\mathfrak{p} = \mathfrak{F}_{\tilde{\mathfrak{p}}} = (\Lambda_{\mathcal{K}})_{\tilde{\mathfrak{p}}}.$$ ■

(2.28) Proposition. Let $\mathfrak{C}$ be a full right ideal of Λ and let $C \in \Lambda$ satisfy $\mathfrak{C}_\mathfrak{p} = C\Lambda_\mathfrak{p}$ for all $\mathfrak{p} \supset \mathfrak{f}$. Then $\mathfrak{C}$ can be made coprime to $\mathfrak{F}$.

[1] Cf. Neukirch (1999), p. 79, (12.10).

Proof. By our assumptions, C is nonsingular. With regard to (1.32), let $\mathfrak{c}$ be the fractional ideal of $\mathcal{O}_{\boldsymbol{\mathcal{K}}}$ satisfying

$$\mathfrak{c}\Lambda_{\boldsymbol{\mathcal{K}}} = \Lambda_{\boldsymbol{\mathcal{K}}} C^{-1} \Lambda_{\boldsymbol{\mathcal{K}}}.$$

Let

$$\mathfrak{c} = \Big(\prod_{\tilde{\mathfrak{p}} \not\supset \mathfrak{f}} \tilde{\mathfrak{p}}^{e_{\tilde{\mathfrak{p}}}}\Big)\mathfrak{c}'$$

be a partial factorization of $\mathfrak{c}$. If $\mathfrak{p}$ is a full prime ideal of $\mathcal{O}$ not containing $\mathfrak{f}$, then $\mathfrak{p}$ lies in exactly one $\tilde{\mathfrak{p}}$ by (2.7). Therefore we can choose an $s \in \mathcal{O}$ such that

$$s \equiv \begin{cases} 1 \mod \mathfrak{p} & \text{if } \mathfrak{p} \supset \mathfrak{f}, \\ 0 \mod \mathfrak{p}^{-e_{\tilde{\mathfrak{p}}}} & \text{if } \mathfrak{p} = \tilde{\mathfrak{p}} \cap \mathcal{O}. \end{cases}$$

Adding a suitable integer to s, we may assume that s is a nonzerodivisor. Put $\mathit{\Gamma} = sC^{-1}$. We claim that $\mathit{\Gamma}\mathfrak{C} + \mathfrak{F} = \Lambda$. First of all, if $\mathfrak{p} \supset \mathfrak{f}$, then $s \in S_{\mathfrak{p}}$ and

$$\mathit{\Gamma}\mathfrak{C}_{\mathfrak{p}} = \mathit{\Gamma} C \Lambda_{\mathfrak{p}} = s\Lambda_{\mathfrak{p}} = \Lambda_{\mathfrak{p}}.$$

By (2.24) it remains to show that $\mathit{\Gamma}\mathfrak{C} \subset \Lambda$ to prove our claim. For the rest of the proof, suppose $\mathfrak{p} = \tilde{\mathfrak{p}} \cap \mathcal{O}$ where $\tilde{\mathfrak{p}} \not\supset \mathfrak{f}$. To prove the stated inclusion, we will show that $\mathit{\Gamma}$ belongs to $\Lambda_{\boldsymbol{\mathcal{K}}}$. If this true, we see that

$$\mathit{\Gamma}\mathfrak{C}_{\mathfrak{p}} \subset \mathit{\Gamma}\Lambda_{\mathfrak{p}} = \mathit{\Gamma}(\Lambda_{\boldsymbol{\mathcal{K}}})_{\tilde{\mathfrak{p}}} \subset (\Lambda_{\boldsymbol{\mathcal{K}}})_{\tilde{\mathfrak{p}}} = \Lambda_{\mathfrak{p}},$$

using (2.27) for the last equality, and we may conclude that $\mathit{\Gamma}\mathfrak{C} = \bigcap_{\mathfrak{p}} \mathit{\Gamma}\mathfrak{C}_{\mathfrak{p}}$ lies in $\Lambda = \bigcap_{\mathfrak{p}} \Lambda_{\mathfrak{p}}$, where the equalities are due to (2.10).
Since $\Lambda_{\boldsymbol{\mathcal{K}}}$ is a direct sum of maximal matrix orders, it suffices to consider the case where $\boldsymbol{\mathcal{K}} = \mathcal{K}$ is a number field. Furthermore, we may assume that $\Lambda_{\mathcal{K}}$ is of the standard form (1.18), that is,

$$\Lambda_{\mathcal{K}} = \begin{bmatrix} \mathcal{O}_{\mathcal{K}} & \mathfrak{a} & \cdots & \mathfrak{a} \\ \mathfrak{a}^{-1} & \mathcal{O}_{\mathcal{K}} & \cdots & \mathcal{O}_{\mathcal{K}} \\ \vdots & \vdots & \ddots & \vdots \\ \mathfrak{a}^{-1} & \mathcal{O}_{\mathcal{K}} & \cdots & \mathcal{O}_{\mathcal{K}} \end{bmatrix}.$$

Write $C^{-1} = [c_{ij}]$. Then (1.34) yields

$$\mathfrak{c} = c_{11}\mathcal{O}_{\mathcal{K}} + \sum_{i,j>1} c_{ij}\mathcal{O}_{\mathcal{K}} + \sum_{i>1} c_{i1}\mathfrak{a} + \sum_{j>1} c_{1j}\mathfrak{a}^{-1}.$$

By our choice of s, we obtain $s\mathfrak{c} \subset s\tilde{\mathfrak{p}}^{e_{\tilde{\mathfrak{p}}}} \subset \mathcal{O}_{\mathcal{K}}$. Therefore

$$sc_{ij} \in \begin{cases} \mathfrak{a} & \text{if } i = 1,\ j > 1, \\ \mathfrak{a}^{-1} & \text{if } i > 1,\ j = 1, \\ \mathcal{O}_{\mathcal{K}} & \text{otherwise.} \end{cases}$$

In conclusion, $\mathit{\Gamma} = sC^{-1}$ is an element of $\Lambda_{\mathcal{K}}$. ■

Theorem (2.23) is now established, because if $\mathfrak{C}_\mathfrak{p} = C_\mathfrak{p}\Lambda_\mathfrak{p}$ for all $\mathfrak{p} \supset \mathfrak{f}$, we can determine a matrix C such that $\mathfrak{C}_\mathfrak{p} = C\Lambda_\mathfrak{p}$ for all $\mathfrak{p}$, and $\Gamma = sC^{-1}$, with s chosen as in the proof above, satisfies $\Gamma\mathfrak{C} + \mathfrak{F} = \Lambda$.

In the remainder of this section, we will explain how to decide whether $\mathfrak{C}_\mathfrak{p}$ is principal and, if so, how to obtain a generator. First, suppose that $\mathfrak{C} = \mathfrak{c}$ is an invertible ideal of $\mathcal{O}$. In this case, $\mathfrak{c}_\mathfrak{p}$ is always principal, that is, all invertible ideals of $\mathcal{O}$ can be made coprime to the conductor.

(2.29) Proposition. An ideal $\mathfrak{c}$ of $\mathcal{O}$ is invertible if and only if $\mathfrak{c}_\mathfrak{p}$ is principal for every full prime ideal $\mathfrak{p}$.[1]

Proof. Let $\mathfrak{c}$ be invertible. Then $\mathcal{O} = \mathfrak{c}\mathfrak{c}^{-1}$ is generated by a finite number of products cc' with $c \in \mathfrak{c}$ and $c' \in \mathfrak{c}^{-1}$. By (2.1) all factors can be chosen as nonzerodivisors. Given a prime ideal $\mathfrak{p}$, at least one product cc' does not belong to $\mathfrak{p}$. Therefore cc' is a unit of $\mathcal{O}_\mathfrak{p}$. If $x \in \mathfrak{c}_\mathfrak{p}$, then $c'x \in \mathfrak{c}^{-1}\mathfrak{c}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}$, so

$$x = c(cc')^{-1}c'x \in c\mathcal{O}_\mathfrak{p}.$$

Hence $\mathfrak{c}_\mathfrak{p} \subset c\mathcal{O}_\mathfrak{p}$. The converse inclusion is trivial.
Now suppose $\mathfrak{c}_\mathfrak{p} = c_\mathfrak{p}\mathcal{O}_\mathfrak{p}$ for each $\mathfrak{p}$. We may choose $c_\mathfrak{p}$ in $\mathfrak{c}$. Because of $\mathfrak{c} \subset \mathfrak{c}_\mathfrak{p}$, every $c \in \mathfrak{c}$ is of the form

$$c = c_\mathfrak{p}x_\mathfrak{p} \quad \text{with } x_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}.$$

Since $\mathfrak{c}$ is finitely generated, there is an $s_\mathfrak{p} \in S_\mathfrak{p}$ for every $\mathfrak{p}$ such that

$$s_\mathfrak{p}\mathfrak{c} \subset c_\mathfrak{p}\mathcal{O}.$$

Then $s_\mathfrak{p} = (s_\mathfrak{p}c_\mathfrak{p}^{-1})c_\mathfrak{p}$ is an element of $(\mathcal{O} : \mathfrak{c})\mathfrak{c}$, which means $(\mathcal{O} : \mathfrak{c})\mathfrak{c}$ cannot be contained in any $\mathfrak{p}$. Thus $(\mathcal{O} : \mathfrak{c})\mathfrak{c} = \mathcal{O}$, that is, $\mathfrak{c}$ is invertible. ■

From the proof of (2.29) we can extract a simple method for determining a principal generator of $\mathfrak{c}_\mathfrak{p}$. Among the generators of $\mathfrak{c}$ and $\mathfrak{c}^{-1}$, chosen as nonzerodivisors, we just need to find a pair c, c' such that $cc' \notin \mathfrak{p}$. Then $\mathfrak{c}_\mathfrak{p} = c\mathcal{O}_\mathfrak{p}$.

(2.30) Corollary. If $\mathfrak{c}$ is a full ideal of $\mathcal{O}$ coprime to $\mathfrak{f}$, then $\mathfrak{c}$ is invertible.

Proof. Let $\mathfrak{p}$ be a full prime ideal of $\mathcal{O}$. If $\mathfrak{p} \supset \mathfrak{f}$, then $\mathfrak{c}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}$. If $\mathfrak{p} \not\supset \mathfrak{f}$, then $\mathcal{O}_\mathfrak{p}$ is a discrete valuation ring by (2.27). In any case, $\mathfrak{c}_\mathfrak{p}$ is a principal ideal, so $\mathfrak{c}$ is invertible. ■

Unfortunately, (2.29) cannot be generalized to the case of matrix orders. In fact, there are invertible right ideals that cannot be made coprime to the conductor. For example, suppose $\mathcal{O}$ is a nonmaximal order in a number field such that the conductor $\mathfrak{f}$ of $\mathcal{O} \subset \mathcal{O}_K$ is a prime ideal of $\mathcal{O}$ (as in the case of $\mathcal{O} = \mathbb{Z}[2i]$). Let

$$\mathfrak{C} = \begin{bmatrix} \mathfrak{f} & \mathfrak{f} \\ \mathcal{O} & \mathcal{O} \end{bmatrix},$$

[1] For integral domains, result (2.29) can be found in Neukirch (1999), p. 74, (12.4).

which is the multiplier ideal of $\mathcal{O} \oplus \mathcal{O}$ and $\mathfrak{f} \oplus \mathcal{O}$. Then $\mathfrak{C}$ is an invertible right ideal of $\Lambda = \mathrm{M}(2, \mathcal{O})$. As mentioned before, the inverse is given by

$$\mathfrak{C}^{-1} = \begin{bmatrix} (\mathcal{O} : \mathfrak{f}) & \mathcal{O} \\ (\mathcal{O} : \mathfrak{f}) & \mathcal{O} \end{bmatrix}.$$

Let $\Lambda_{\mathcal{K}} = \mathrm{M}(2, \mathcal{O}_{\mathcal{K}})$. The conductor of $\Lambda \subset \Lambda_{\mathcal{K}}$ is $\mathfrak{F} = \mathrm{M}(2, \mathfrak{f})$. We claim that

$$\varGamma\mathfrak{C} + \mathfrak{F} \neq \Lambda \quad \text{for all } \varGamma \in \mathrm{GL}(2, \mathcal{K}).$$

First, let us prove that

$$\mathfrak{C}^{-1} = \begin{bmatrix} \mathcal{O}_{\mathcal{K}} & \mathcal{O} \\ \mathcal{O}_{\mathcal{K}} & \mathcal{O} \end{bmatrix}.$$

Since $\mathfrak{f}$ is assumed to be prime, the chain $\mathfrak{f} \subset (\mathcal{O} : \mathfrak{f})\mathfrak{f} \subset \mathcal{O}$ implies

$$(\mathcal{O} : \mathfrak{f})\mathfrak{f} = \mathfrak{f} \quad \text{or} \quad (\mathcal{O} : \mathfrak{f})\mathfrak{f} = \mathcal{O}.$$

In the second case, $\mathfrak{f}$ would be an invertible ideal of $\mathcal{O}$, which cannot be true because its multiplier ring is $\mathcal{O}_{\mathcal{K}}$. Hence $(\mathcal{O} : \mathfrak{f})\mathfrak{f} = \mathfrak{f}$, that is,

$$(\mathcal{O} : \mathfrak{f}) \subset (\mathfrak{f} : \mathfrak{f}) = \mathcal{O}_{\mathcal{K}}.$$

Conversely, $\mathcal{O}_{\mathcal{K}}\mathfrak{f} = \mathfrak{f} \subset \mathcal{O}$, therefore $(\mathcal{O} : \mathfrak{f}) = \mathcal{O}_{\mathcal{K}}$ is established.
Now suppose there was a matrix

$$\varGamma = \begin{bmatrix} x_1 & y_1 \\ x_2 & y_2 \end{bmatrix}$$

such that $\varGamma\mathfrak{C} + \mathfrak{F} = \Lambda$. Then, in particular, $\varGamma\mathfrak{C} \subset \Lambda$, that is, $\varGamma \in \mathfrak{C}^{-1}$. Therefore $x_i \in \mathcal{O}_{\mathcal{K}}$ and $y_i \in \mathcal{O}$. Moreover, $\varGamma\mathfrak{C} + \mathfrak{F} = \Lambda$ implies the existence of a matrix $C \in \mathfrak{C}$ such that

$$\varGamma C \equiv I \mod \mathfrak{F}.$$

But all elements of $\mathfrak{C}$ are of the form

$$\begin{bmatrix} f_1 & f_2 \\ z_1 & z_2 \end{bmatrix} \quad \text{with} \quad f_i \in \mathfrak{f} \quad \text{and} \quad z_i \in \mathcal{O}.$$

Thus we observe

$$I \equiv \varGamma C = \begin{bmatrix} x_1 f_1 + y_1 z_1 & x_1 f_2 + y_1 z_2 \\ x_2 f_1 + y_2 z_1 & x_2 f_2 + y_2 z_2 \end{bmatrix} \equiv \begin{bmatrix} y_1 z_1 & y_1 z_2 \\ y_2 z_1 & y_2 z_2 \end{bmatrix} \mod \mathfrak{F} = \begin{bmatrix} \mathfrak{f} & \mathfrak{f} \\ \mathfrak{f} & \mathfrak{f} \end{bmatrix}.$$

Therefore y_1, y_2, z_1, z_2 are a units as well as a zerodivisors modulo $\mathfrak{f}$, a contradiction. Consequently, $\varGamma\mathfrak{C} + \mathfrak{F} \neq \Lambda$ for all $\varGamma \in \mathrm{GL}(2, \mathcal{K})$.

As remarked earlier, if $\mathfrak{C}$ cannot be made coprime to $\mathfrak{F}$, we may conclude that $\mathfrak{C}$ is not principal. Hence a negative outcome poses no problem for our purposes.

What the example also illustrates is that we cannot expect $\mathfrak{c} = \mathfrak{C} \cap \mathcal{O}$ to be invertible simply because $\mathfrak{C}$ is (in the setting above we have $\mathfrak{c} = \mathfrak{f}$). This is unfortunate because below we will show that $\mathfrak{C}_\mathfrak{p}$ is principal if and only if $\mathfrak{C}$ contains a nonsingular matrix C such that

$$\mathfrak{C}^{-1}C \cap \mathcal{K}^\times \not\subset \mathfrak{p}.$$

If, however, $\mathfrak{c} = \mathfrak{C} \cap \mathcal{O}$ is invertible and $\mathfrak{c}^{-1} \subset \mathfrak{C}^{-1} \cap \mathcal{K}$, we can choose C to be a scalar c with $\mathfrak{c}_\mathfrak{p} = c\mathcal{O}_\mathfrak{p}$, which can be found easily as already explained.

(2.31) Proposition. Let $\mathfrak{C}$ be an invertible right ideal of Λ and let C be a nonsingular matrix in $\mathfrak{C}$. The following properties are equivalent.

(1) $\mathfrak{C}_\mathfrak{p} = C\Lambda_\mathfrak{p}$.

(2) $\mathfrak{C}^{-1}C \cap \mathcal{K}^\times \not\subset \mathfrak{p}$.

(3) $\mathfrak{C}^{-1}C$ contains a unit of $\Lambda_\mathfrak{p}$.

Proof. The second property implies the third because it states that $\mathfrak{C}^{-1}C$ contains an element of $S_\mathfrak{p}$. Notice that $\mathfrak{C}^{-1}C \cap \mathcal{K} \subset \Lambda \cap \mathcal{K} = \mathcal{O}$.
Suppose there is a $C' \in \mathfrak{C}^{-1}$ such that $C'C \in \Lambda_\mathfrak{p}^\times$. If $X \in \mathfrak{C}_\mathfrak{p}$, then

$$X = C(C'C)^{-1}C'X \in C\Lambda_\mathfrak{p}$$

because $C'X$ belongs to $\mathfrak{C}^{-1}\mathfrak{C}_\mathfrak{p} = \Lambda_\mathfrak{p}$ and so does $(C'C)^{-1}$. Hence $\mathfrak{C}_\mathfrak{p} \subset C\Lambda_\mathfrak{p}$, and the converse inclusion is trivial.
Now suppose $\mathfrak{C}_\mathfrak{p} = C\Lambda_\mathfrak{p}$. We will show that

$$(\mathfrak{C}^{-1})_\mathfrak{p} = (\mathfrak{C}_\mathfrak{p})^{-1} = \Lambda_\mathfrak{p}C^{-1},$$

which is not completely trivial since $\mathfrak{C}_\mathfrak{p}$ can have several inverses. If the stated equalities hold, we obtain

$$(\mathfrak{C}^{-1}C)_\mathfrak{p} = (\mathfrak{C}^{-1})_\mathfrak{p}C = \Lambda_\mathfrak{p}C^{-1}C = \Lambda_\mathfrak{p},$$

so we can write $I = C'Cs^{-1}$ with $C' \in \mathfrak{C}^{-1}$ and $s \in S_\mathfrak{p}$. Then $s = C'C$ belongs to $\mathfrak{C}^{-1}C \cap \mathcal{K}^\times$, which implies (2).
So let us prove the asserted equalities. First, $(\mathfrak{C}_\mathfrak{p})^{-1}$ contains the exterior ideals because

$$(\mathfrak{C}^{-1})_\mathfrak{p}\,\mathfrak{C}_\mathfrak{p} = (\Lambda_\mathfrak{p}\mathfrak{C}^{-1})(\mathfrak{C}\Lambda_\mathfrak{p}) = \Lambda_\mathfrak{p}$$

and

$$(\Lambda_\mathfrak{p}C^{-1})\mathfrak{C}_\mathfrak{p} = (\Lambda_\mathfrak{p}C^{-1})(C\Lambda_\mathfrak{p}) = \Lambda_\mathfrak{p}.$$

Second, $\Lambda_\mathfrak{p}C^{-1}$ is the largest inverse of $C\Lambda_\mathfrak{p}$, and it contains $(\mathfrak{C}_\mathfrak{p})^{-1}$ because

$$(\mathfrak{C}_\mathfrak{p})^{-1}(C\Lambda_\mathfrak{p}) \subset (\mathfrak{C}_\mathfrak{p})^{-1}\mathfrak{C}_\mathfrak{p} = \Lambda_\mathfrak{p}.$$

Thus it remains to show that $(\mathfrak{C}_\mathfrak{p})^{-1} \subset (\mathfrak{C}^{-1})_\mathfrak{p}$. Let $C_1, \ldots, C_n$ be generators of $\mathfrak{C}$. Since $C_j \in \mathfrak{C}_\mathfrak{p} = C\Lambda_\mathfrak{p}$, we have

$$C^{-1}C_j = X_j s_j^{-1} \quad \text{with } X_j \in \Lambda \text{ and } s_j \in S_\mathfrak{p}.$$

Put $s = s_1 \cdots s_n$. Then $sC^{-1}C_j \in \Lambda$ for all j, so $sC^{-1}\mathfrak{C} \subset \Lambda$. Therefore $sC^{-1} \in \mathfrak{C}^{-1}$ and $C^{-1} \in (\mathfrak{C}^{-1})_\mathfrak{p}$. This proves

$$(\mathfrak{C}_\mathfrak{p})^{-1} = \Lambda_\mathfrak{p}C^{-1} \subset (\mathfrak{C}^{-1})_\mathfrak{p}.$$ ■

Making use of (2.31), it is possible (at least in a finite number of steps) to decide whether $\mathfrak{C}_{\mathfrak{p}}$ is principal, as the next theorem states. Unfortunately, the method based on the theorem will come down to a search of exponential complexity. So in practice, it might be worthwhile to use a random procedure before working deterministically.

(2.32) Theorem. Let $\mathfrak{C}$ be an invertible right ideal of Λ and let $C_1, \dots, C_m$ be a set of representatives of $\mathfrak{C}/\mathfrak{p}\mathfrak{C}$. Then $\mathfrak{C}_{\mathfrak{p}}$ is principal if and only if

$$\mathfrak{C}_{\mathfrak{p}} = C_i \Lambda_{\mathfrak{p}} \quad \text{for some } C_i.$$

Proof. Suppose $\mathfrak{C}_{\mathfrak{p}} = C\Lambda_{\mathfrak{p}}$ for some matrix C. Then C can be chosen in Λ. We have to show that

$$\mathfrak{C}_{\mathfrak{p}} = (C + P)\Lambda_{\mathfrak{p}} \quad \text{for any } P \in \mathfrak{p}\mathfrak{C}.$$

By (2.31) there is a $C' \in \mathfrak{C}^{-1}$ such that $C'C = s$ is an element of $S_{\mathfrak{p}}$. Let $\mathfrak{q}$ be a prime ideal of $\mathcal{O}_{\mathcal{K}}$ containing $\mathfrak{p}$. As element of the maximal order, $s = s_1 \oplus \cdots \oplus s_r$ can be written as the product

$$s = \prod_{\iota} (1 \oplus \cdots \oplus s_\iota \oplus \cdots \oplus 1).$$

None of these factors belongs to $\mathfrak{q}$ (or else $s \in \mathfrak{q} \cap \mathcal{O} = \mathfrak{p}$), therefore

$$\begin{aligned} \det(s) = \det(s_1) \oplus \cdots \oplus \det(s_r) &= s_1^{n_1} \oplus \cdots \oplus s_r^{n_r} \\ &= \prod_{\iota} (1 \oplus \cdots \oplus s_\iota^{n_\iota} \oplus \cdots \oplus 1) \not\equiv 0 \mod \mathfrak{q}. \end{aligned}$$

If $P \in \mathfrak{p}\mathfrak{C}$, then $C'P$ belongs to $\mathfrak{C}^{-1}(\mathfrak{p}\mathfrak{C}) = \mathfrak{p}\Lambda \subset \mathfrak{q}\Lambda_{\mathcal{K}}$. By (1.35) we have

$$\det(C'(C + P)) = \det(s + C'P) \equiv \det(s) \not\equiv 0 \mod \mathfrak{q}.$$

By (2.6) this determinant cannot belong to any prime ideal of $(\mathcal{O}_{\mathcal{K}})_{\mathfrak{p}}$, hence it is a unit. Therefore $C'(C+P) \in \Lambda_{\mathfrak{p}}^{\times}$ by (2.22) and $\mathfrak{C}_{\mathfrak{p}} = (C+P)\Lambda_{\mathfrak{p}}$ by (2.31). ■

2.5 Algorithms

(2.33) Algorithm — Minimal Exponent ν

→ $\mathfrak{c}$ full ideal
$\mathfrak{p}$ prime ideal

← ν minimal integer satisfying $\mathfrak{p}_{\mathfrak{p}}^{\nu} \subset \mathfrak{c}_{\mathfrak{p}}$

The ideals $\mathfrak{c}$ and $\mathfrak{p}$ both belong to an order $\mathcal{O}$ of $\mathcal{K}$.

(1) Choose an integer n exceeding $v_p[\mathcal{O} : \mathfrak{c}]/v_p[\mathcal{O} : \mathfrak{p}]$.

(2) Determine the smallest integer ν with $\mathfrak{p}^{\nu} \subset \mathfrak{c} + \mathfrak{p}^{n}$. Return ν.

If $\mathfrak{c}$ satisfies the condition $\mathfrak{c}\mathcal{O}_{\mathcal{K}} \cap \mathcal{O} = \mathfrak{c}$, we can use the following method (which is worthwhile if the occurring factorizations have already been computed).

(1) Compute the factorization $\mathfrak{p}\mathcal{O}_{\mathcal{K}} = \prod \mathfrak{q}^{e_{\mathfrak{q}}}$.

(2) Compute a partial factorization $\mathfrak{c}\mathcal{O}_{\mathcal{K}} = (\prod \mathfrak{q}^{\nu_{\mathfrak{q}}})\mathfrak{c}'$.

(3) Put $\nu := \max_{\mathfrak{q}} \lceil \nu_{\mathfrak{q}} / e_{\mathfrak{q}} \rceil$. Return ν.

The algorithm can also be used to compute the smallest integer ν satisfying $\mathfrak{p}^{\nu}\Lambda_{\mathfrak{p}} \subset \mathfrak{C}_{\mathfrak{p}}$. Simply call it with $\mathfrak{c} = \mathfrak{C} \cap \mathcal{O}$.

(2.34) Algorithm — Is Locally Coprime

→ $\mathfrak{C}$ invertible right ideal of a matrix order Λ
$\mathfrak{p}$ full prime ideal of the center of Λ

← τ `true`/`false`
C element of $\mathrm{M}(\boldsymbol{n}, \mathcal{K})$ satisfying $\mathfrak{C}_{\mathfrak{p}} = C\Lambda_{\mathfrak{p}}$

(1) Compute the set $\mathfrak{Q}$ of all prime ideals of $\mathcal{O}_{\mathcal{K}}$ containing $\mathfrak{p}$.

(2) For every C in a set of representatives of $\mathfrak{C}/\mathfrak{p}\mathfrak{C}$, check whether

$$\det(C) \notin \mathfrak{q} \quad \text{for all } \mathfrak{q} \in \mathfrak{Q}.$$[1]

If so, return `true` and C. If no such C exists, return `false`.

If Λ is an order $\mathcal{K}$, that is, we can avoid the cumbersome search of $\mathfrak{C}/\mathfrak{p}\mathfrak{C}$. Write $\mathfrak{c} = \mathfrak{C}$ and suppose $c_1, \ldots, c_n$ are generators of $\mathfrak{c}$, all of which can be chosen to be nonzerodivisors by (2.1). By (2.29) it is already guaranteed that $\mathfrak{c}_{\mathfrak{p}}$ is principal. To obtain a generator of $\mathfrak{c}_{\mathfrak{p}}$, execute the following commands.

(1) Compute a set of nonzerodivisors $c'_1, \ldots, c'_m$ which generates $\mathfrak{c}^{-1}$.

(2) For $i = 1, \ldots, n$ and $j = 1, \ldots, m$: If $c_i\, c'_j \notin \mathfrak{p}$, return `true` and c_i.

(2.35) Algorithm — Make Coprime

→ $\mathfrak{C}$ invertible right ideal of a matrix order Λ
$\mathfrak{F}$ conductor of $\Lambda \subset \Lambda_{\mathcal{K}}$

← τ `true`/`false`
$\varGamma$ element of $\mathrm{GL}(\boldsymbol{n}, \mathcal{K})$ satisfying $\varGamma\mathfrak{C} + \mathfrak{F} = \Lambda$

Suppose $\mathcal{O} = \Lambda \cap \mathcal{K}$ and $\mathfrak{F} = \mathfrak{f}\Lambda_{\mathcal{K}}$.

(1) If $\Lambda = \Lambda_{\mathcal{K}}$ (that is, $\mathfrak{F} = \Lambda_{\mathcal{K}}$), return `true` and I.

[1] Then C is a unit of $\Lambda_{\mathfrak{p}}$ by (2.6) and (2.22). Hence it generates $\mathfrak{C}_{\mathfrak{p}}$ by (2.31).

(2) Compute all prime ideals $\mathfrak{p}$ of $\mathcal{O}$ above $\mathfrak{f}$.

(3) For each $\mathfrak{p} \supset \mathfrak{f}$, try to compute a matrix $C_\mathfrak{p}$ with $\mathfrak{C}_\mathfrak{p} = C_\mathfrak{p}\Lambda_\mathfrak{p}$ using algorithm (2.34). If not all $\mathfrak{C}_\mathfrak{p}$ are principal, return `false`.

(4) Compute a matrix C with $\mathfrak{C}_\mathfrak{p} = C\Lambda_\mathfrak{p}$ for all $\mathfrak{p} \supset \mathfrak{f}$ using (2.25) and the Chinese Remainder Theorem.

(5) Compute an element s as in the proof of (2.28).

(6) Put $\mathit{\Gamma} := sC^{-1}$. Return `true` and $\mathit{\Gamma}$.

3 Principal Ideal Testing

In this chapter we will explain how to perform a principal ideal test when dealing with ideals of nonmaximal orders, provided that we can execute the test in the maximal order successfully. Furthermore, we will assume that the ideal in question is coprime to the conductor. The commutative and the noncommutative case will be discussed separately. In good cases, the noncommutative test can be reduced to the commutative setting.

3.1 The Commutative Case

Let $\mathcal{O}$ be an order of $\mathcal{K}$ and let $\mathfrak{c}$ be a full ideal of $\mathcal{O}$ for which we want to decide whether it is principal. Suppose we already know that $\mathfrak{c}_{\mathcal{K}} = \gamma\mathcal{O}_{\mathcal{K}}$ for some $\gamma \in \mathcal{O}_{\mathcal{K}}$ and that $\mathfrak{c}$ is coprime to the conductor $\mathfrak{f}$ of $\mathcal{O} \subset \mathcal{O}_{\mathcal{K}}$. By (1.39) it then suffices to check whether the image of

$$\mathcal{O}_{\mathcal{K}}^{\times} \to (\mathcal{O}_{\mathcal{K}}/\mathfrak{f})^{\times}/(\mathcal{O}/\mathfrak{f})^{\times}$$

contains the residue class of γ. Once all groups have been determined effectively, this can be decided by solving a system of linear equations.

Let us assume that the groups $\mathcal{O}_{\mathcal{K}}^{\times}$ and $(\mathcal{O}_{\mathcal{K}}/\mathfrak{f})^{\times}$ have already been computed.[1] To compute $(\mathcal{O}/\mathfrak{f})^{\times}$ as a subgroup of $(\mathcal{O}_{\mathcal{K}}/\mathfrak{f})^{\times}$, we only have to bother about generators, not about relations. Once we possess a set of generators, we can compute the quotient of both groups—as well as preimages of residue classes—using standard methods for finitely presented abelian groups.[2]

By (2.15) we have a decomposition

$$(\mathcal{O}/\mathfrak{f})^{\times} \simeq \bigoplus_{\mathfrak{p}} (\mathcal{O}/(\mathfrak{f} + \mathfrak{p}^{\nu_{\mathfrak{p}}}))^{\times}$$

with suitable positive integers $\nu_{\mathfrak{p}}$, where the isomorphism is induced by the canonical map $\mathcal{O} \to \bigoplus(\mathcal{O}/(\mathfrak{f} + \mathfrak{p}^{\nu_{\mathfrak{p}}}))$. It therefore suffices to determine generators of $(\mathcal{O}/(\mathfrak{f} + \mathfrak{p}^{\nu_{\mathfrak{p}}}))^{\times}$ for each $\mathfrak{p} \supset \mathfrak{f}$. Afterwards, we obtain the corresponding classes in $(\mathcal{O}/\mathfrak{f})^{\times}$ using the Chinese Remainder Theorem. Another decomposition enables us to find the desired generators. Before we begin, let us remark that the set

$$(1 + \mathfrak{p})/(1 + \mathfrak{f} + \mathfrak{p}^{\nu}),$$

consisting of the classes $[1 + \pi] = (1 + \pi)(1 + \mathfrak{f} + \mathfrak{p}^{\nu})$, is a multiplicative group with multiplication inherited from $\mathcal{O}$. Notice that, since $(1 + \mathfrak{p}^{\nu}) \subset (1 + \mathfrak{f} + \mathfrak{p}^{\nu})$, the inverse of $[1 + \pi]$ is given by $[1 - \pi + \cdots + (-\pi)^{\nu-1}]$.

[1] There are well-known algorithms to compute the components of $\mathcal{O}_{\mathcal{K}}^{\times} \simeq \bigoplus \mathcal{O}_{\mathcal{K}_\iota}^{\times}$. Moreover, we can compute the components of $(\mathcal{O}_{\mathcal{K}}/\mathfrak{f})^{\times} \simeq \bigoplus(\mathcal{O}_{\mathcal{K}_\iota}/\mathfrak{f}_\iota)^{\times}$ as described by Cohen (2000), section 4.2; also see Hess, Pauli and Pohst (2003).

[2] Cf. Cohen (2000), section 4.1.

(3.1) Proposition. Let $\mathfrak{p} \supset \mathfrak{f}$ be a prime ideal of $\mathcal{O}$ and $\nu > 0$. Then

$$(\mathcal{O}/(\mathfrak{f}+\mathfrak{p}^\nu))^\times \simeq (\mathcal{O}/\mathfrak{p})^\times \oplus (1+\mathfrak{p})/(1+\mathfrak{f}+\mathfrak{p}^\nu).[1]$$

The proof of (3.1) relies on Hensel's lemma. Below, we state a special version of the lemma which is sufficient for our purposes. For the proof, in a more general setting, see Pohst and Zassenhaus (1989), pp. 301–302.

(3.2) Hensel's lemma. Let $\mathfrak{p}$ be a full prime ideal of $\mathcal{O}$. Let f be a monic polynomial over $\mathcal{O}$ and $\zeta \in \mathcal{O}$ such that

$$f(\zeta) \equiv 0 \mod \mathfrak{p} \qquad \text{and} \qquad f'(\zeta) \not\equiv 0 \mod \mathfrak{p}.$$

For each $\nu > 0$ there is an $\eta \in \mathcal{O}$ such that $f(\eta) \equiv 0 \bmod \mathfrak{p}^\nu$ and $\eta \equiv \zeta \bmod \mathfrak{p}$.

Proof of (3.1). Choose $\zeta \in \mathcal{O}$ such that its residue class generates $(\mathcal{O}/\mathfrak{p})^\times$. Let $f = X^{q-1} - 1$ where q denotes the number of elements in $\mathcal{O}/\mathfrak{p}$. Then

$$f(\zeta) \equiv 0 \mod \mathfrak{p} \qquad \text{and} \qquad f'(\zeta) \not\equiv 0 \mod \mathfrak{p},$$

so by Hensel's lemma there is an $\eta \in \mathcal{O}$ with $\eta^{q-1} \equiv 1 \bmod \mathfrak{p}^\nu$ and $\eta \equiv \zeta \bmod \mathfrak{p}$, that is, η is a unit modulo $\mathfrak{f}+\mathfrak{p}^\nu$ of order $q-1$. Therefore the canonical map

$$(\mathcal{O}/(\mathfrak{f}+\mathfrak{p}^\nu))^\times \to (\mathcal{O}/\mathfrak{p})^\times$$

is an epimorphism. Elements in the kernel are represented by elements in $1+\mathfrak{p}$, and $1+\pi$ represents the unit element precisely if it belongs to $1+\mathfrak{f}+\mathfrak{p}^\nu$. Thus we have an exact sequence

$$1 \to (1+\mathfrak{p})/(1+\mathfrak{f}+\mathfrak{p}^\nu) \to (\mathcal{O}/(\mathfrak{f}+\mathfrak{p}^\nu))^\times \to (\mathcal{O}/\mathfrak{p})^\times \to 1.$$

The sequence is split because

$$(\mathcal{O}/\mathfrak{p})^\times \to (\mathcal{O}/(\mathfrak{f}+\mathfrak{p}^\nu))^\times, \quad \zeta+\mathfrak{p} \mapsto \eta+\mathfrak{f}+\mathfrak{p}^\nu$$

defines a suitable injection. Hence $(\mathcal{O}/(\mathfrak{f}+\mathfrak{p}^\nu))^\times$ is isomorphic to the direct sum $(\mathcal{O}/\mathfrak{p})^\times \oplus (1+\mathfrak{p})/(1+\mathfrak{f}+\mathfrak{p}^\nu)$. ∎

By (3.1) we are left to compute generators of $(\mathcal{O}/\mathfrak{p})^\times$ and $(1+\mathfrak{p})/(1+\mathfrak{f}+\mathfrak{p}^\nu)$. According to the proof, generators of $(1+\mathfrak{p})/(1+\mathfrak{f}+\mathfrak{p}^\nu)$ can be used directly as part of a generating set of $(\mathcal{O}/(\mathfrak{f}+\mathfrak{p}^\nu))^\times$. Moreover, we need to compute a $(q-1)$-th root of unity modulo $\mathfrak{p}^\nu$. This second step can be simplified to computing a generator of $(\mathcal{O}/\mathfrak{p})^\times$, for if $\zeta \in \mathcal{O}$ represents such a generator, we have $\zeta^{q-1} = 1+\pi$ with $\pi \in \mathfrak{p}$. Hence ζ represents a generator of

$$\frac{(\mathcal{O}/(\mathfrak{f}+\mathfrak{p}^\nu))^\times}{(1+\mathfrak{p})/(1+\mathfrak{f}+\mathfrak{p}^\nu)} \simeq (\mathcal{O}/\mathfrak{p})^\times.$$

Now we will explain how to compute a generator of the cyclic group $(\mathcal{O}/\mathfrak{p})^\times$. Let $\mathfrak{q} = \mathfrak{q}_1 \oplus \cdots \oplus \mathfrak{q}_s$ be a prime ideal of $\mathcal{O}_{\mathcal{K}}$ above $\mathfrak{p}$ (which we need to compute

[1] Result (3.1) is stated in Klüners and Pauli (2005) for orders of number fields, cf. lemma 4.3.

in the first place to obtain $\mathfrak{p}$ as the intersection $\mathfrak{q} \cap \mathcal{O}$). There is exactly one ι such that $\mathfrak{q}_\iota$ is a prime ideal of $\mathcal{O}_{\mathcal{K}_\iota}$, while $\mathfrak{q}_\nu = \mathcal{O}_{\mathcal{K}_\nu}$ for $\nu \neq \iota$ (otherwise, $\mathfrak{q}$ would not be maximal). Hence

$$\mathcal{O}_{\mathcal{K}}/\mathfrak{q} \simeq \mathcal{O}_{\mathcal{K}_\iota}/\mathfrak{q}_\iota,$$

so the residue class field stems from a maximal order in a number field. The composition of the canonical maps

$$\mathcal{O} \to \mathcal{O}_{\mathcal{K}} \to \mathcal{O}_{\mathcal{K}}/\mathfrak{q}$$

induces an injection $\mathcal{O}/\mathfrak{p} \to \mathcal{O}_{\mathcal{K}}/\mathfrak{q}$, thus $\mathcal{O}/\mathfrak{p}$ can be realized as a subfield of $\mathcal{O}_{\mathcal{K}_\iota}/\mathfrak{q}_\iota$. By choosing elements at random, we eventually find a generator of $(\mathcal{O}/\mathfrak{p})^\times$.

Finally, we need to examine the group $(1+\mathfrak{p})/(1+\mathfrak{f}+\mathfrak{p}^\nu)$. The canonical map

$$(1+\mathfrak{p})/(1+\mathfrak{p}^\nu) \to (1+\mathfrak{p})/(1+\mathfrak{f}+\mathfrak{p}^\nu)$$

is surjective, and since we are only interested in a set of generators, it suffices to deal with the group $(1+\mathfrak{p})/(1+\mathfrak{p}^\nu)$.

(3.3) Proposition. Let $m \leq \nu$ be positive integers with $\nu \leq 2m$. The map

$$(1+\mathfrak{p}^m)/(1+\mathfrak{p}^\nu) \to \mathfrak{p}^m/\mathfrak{p}^\nu, \quad [1+\pi] \mapsto \pi + \mathfrak{p}^\nu$$

is an isomorphism.[1]

Proof. The map is well-defined, for if

$$(1+\pi)(1+\rho) = 1 + \pi + \rho + \pi\rho \qquad (\rho \in \mathfrak{p}^\nu)$$

is another representative of $[1+\pi]$, it is also mapped onto $\pi + \mathfrak{p}^\nu$. It is a homomorphism because the image of $(1+\pi)(1+\pi')$ is

$$(\pi + \pi' + \pi\pi') + \mathfrak{p}^\nu = (\pi + \mathfrak{p}^\nu) + (\pi' + \mathfrak{p}^\nu),$$

taking into account that $\pi\pi' \in \mathfrak{p}^{2m} \subset \mathfrak{p}^\nu$. Clearly, the map is surjective, and it is injective because the image of $[1+\pi]$ is trivial precisely if $\pi \in \mathfrak{p}^\nu$, that is, $(1+\pi) \in 1 + \mathfrak{p}^\nu$. ■

By (3.3) we can easily determine generators of the group $(1+\mathfrak{p}^{2^k})/(1+\mathfrak{p}^{2^{k+1}})$, simply by choosing generators of $\mathfrak{p}^{2^k}$. Furthermore, we have an exact sequence

$$1 \to (1+\mathfrak{p}^{2^k})/(1+\mathfrak{p}^{2^{k+1}}) \to (1+\mathfrak{p})/(1+\mathfrak{p}^{2^{k+1}}) \to (1+\mathfrak{p})/(1+\mathfrak{p}^{2^k}) \to 1,$$

and by induction we may assume that we are in possession of generators of $(1+\mathfrak{p})/(1+\mathfrak{p}^{2^k})$. Combining the generators of the kernel and the image, we obtain generators of $(1+\mathfrak{p})/(1+\mathfrak{p}^{2^{k+1}})$. If $2^k \geq \nu$, the map

$$(1+\mathfrak{p})/(1+\mathfrak{p}^{2^k}) \to (1+\mathfrak{p})/(1+\mathfrak{p}^\nu)$$

is surjective. So by choosing k large enough, we can also compute generators of $(1+\mathfrak{p})/(1+\mathfrak{p}^\nu)$.

[1] Again, cf. Klüners and Pauli (2005), lemma 4.3.

3.2 The Noncommutative Case

In this section we will describe two approaches for a principal ideal test in the noncommutative context. Let $\mathfrak{C} = (\mathfrak{B} : \mathfrak{A})$ be the multiplier ideal of two full modules in $\mathcal{K}^{\boldsymbol{n}}$. Let Λ be the multiplier algebra of $\mathfrak{A}$ and let $\mathcal{O}$ denote the center of Λ. Our goal is to decide whether $\mathfrak{C}$ is a principal right ideal of Λ. Suppose we already know that $\mathfrak{C}\Lambda_{\mathcal{K}} = \Gamma\Lambda_{\mathcal{K}}$ where $\Lambda_{\mathcal{K}} = (\mathfrak{A}_{\mathcal{K}} : \mathfrak{A}_{\mathcal{K}})$ and that $\mathfrak{C}$ is coprime to the conductor $\mathfrak{F} = \mathfrak{f}\Lambda_{\mathcal{K}}$ of $\Lambda \subset \Lambda_{\mathcal{K}}$. By (1.39) we then need to check whether the image of

$$\Lambda_{\mathcal{K}}^{\times} \to (\Lambda/\mathfrak{F})^{\times}\backslash(\Lambda_{\mathcal{K}}/\mathfrak{F})^{\times}$$

contains the residue class of Γ. Since the groups involved are nonabelian and the codomain has not to be a group at all, this problem is more challenging than the commutative case of the previous section. In a first approximation, we will determine the image of $\Lambda_{\mathcal{K}}^{\times} \to (\Lambda_{\mathcal{K}}/\mathfrak{F})^{\times}$. Clearly, the map above is the composition of

$$\Lambda_{\mathcal{K}}^{\times} \to (\Lambda_{\mathcal{K}}/\mathfrak{F})^{\times} \to (\Lambda/\mathfrak{F})^{\times}\backslash(\Lambda_{\mathcal{K}}/\mathfrak{F})^{\times}.$$

As usual, we may assume that each component of $\Lambda_{\mathcal{K}}$ is of the standard form (1.18). At the beginning of section 1.5, we defined the determinant as the multiplicative map

$$\det\colon \Lambda_{\mathcal{K}} \to \mathcal{O}_{\mathcal{K}}, \quad \det(\Gamma) = \det(\Gamma_1) \oplus \cdots \oplus \det(\Gamma_s).$$

This yields an epimorphism $\det\colon \Lambda_{\mathcal{K}}^{\times} \to \mathcal{O}_{\mathcal{K}}^{\times}$. Let $\mathrm{SL}(\Lambda_{\mathcal{K}})$ be the kernel of this map. Then we have a split exact sequence

$$1 \to \mathrm{SL}(\Lambda_{\mathcal{K}}) \to \Lambda_{\mathcal{K}}^{\times} \to \mathcal{O}_{\mathcal{K}}^{\times} \to 1,$$

therefore

$$\Lambda_{\mathcal{K}}^{\times} \simeq \mathrm{SL}(\Lambda_{\mathcal{K}}) \rtimes \mathcal{O}_{\mathcal{K}}^{\times}.$$

Moreover, the determinant induces an epimorphism

$$\det\colon (\Lambda_{\mathcal{K}}/\mathfrak{F})^{\times} \to (\mathcal{O}_{\mathcal{K}}/\mathfrak{f})^{\times}, \quad \det(\bar{\Gamma}) = \overline{\det(\Gamma)}$$

which is well-defined by (1.35). Let $\mathrm{SL}(\Lambda_{\mathcal{K}}/\mathfrak{F})$ denote its kernel. As above, this gives us a split exact sequence from which we deduce

$$(\Lambda_{\mathcal{K}}/\mathfrak{F})^{\times} \simeq \mathrm{SL}(\Lambda_{\mathcal{K}}/\mathfrak{F}) \rtimes (\mathcal{O}_{\mathcal{K}}/\mathfrak{f})^{\times}.$$

In the following we will show that the canonical map

$$\mathrm{SL}(\Lambda_{\mathcal{K}}) \to \mathrm{SL}(\Lambda_{\mathcal{K}}/\mathfrak{F})$$

is surjective. Once this is proved, it follows that the image of $\Lambda_{\mathcal{K}}^{\times} \to (\Lambda_{\mathcal{K}}/\mathfrak{F})^{\times}$ is isomorphic to the semidirect product

$$\mathrm{SL}(\Lambda_{\mathcal{K}}/\mathfrak{F}) \rtimes \overline{\det(\Lambda_{\mathcal{K}}^{\times})}$$

where $\overline{\det(\Lambda_{\mathcal{K}}^{\times})}$ denotes the image of $\Lambda_{\mathcal{K}}^{\times} \to \mathcal{O}_{\mathcal{K}}^{\times} \to (\mathcal{O}_{\mathcal{K}}/\mathfrak{f})^{\times}$. To simplify things, we will first show that, essentially, $\Lambda_{\mathcal{K}}/\mathfrak{F}$ is the same as $\mathrm{M}(\boldsymbol{n}, \mathcal{O}_{\mathcal{K}}/\mathfrak{f})$.

(3.4) Lemma. Let $\mathfrak{a}$ be a full fractional ideal of $\mathcal{O}_{\mathcal{K}}$. Then $\mathcal{O}_{\mathcal{K}}/\mathfrak{f}$ and $\mathfrak{a}/\mathfrak{a}\mathfrak{f}$ are isomorphic as modules over $\mathcal{O}_{\mathcal{K}}/\mathfrak{f}$.[1]

[1] Lemma (3.4) is based on lemma 4.2.9 by Cohen (2000), p. 193.

Proof. It suffices to consider the case where $\boldsymbol{\mathcal{K}} = \mathcal{K}$ is a number field and $\mathfrak{a} \subset \mathcal{O}_{\mathcal{K}}$. Let $\mathfrak{P}$ be the set of prime ideals $\mathfrak{p}$ with

$$v_{\mathfrak{p}}(\mathfrak{a}) \neq 0 \quad \text{or} \quad v_{\mathfrak{p}}(\mathfrak{f}) \neq 0$$

where $v_{\mathfrak{p}}$ denotes the $\mathfrak{p}$-adic valuation. We can choose an $a \in \mathcal{O}_{\mathcal{K}}$ such that $v_{\mathfrak{p}}(a) = v_{\mathfrak{p}}(\mathfrak{a})$ for all $\mathfrak{p} \in \mathfrak{P}$. In particular, we have $a \in \mathfrak{a}$. The homomorphism

$$\mathcal{O}_{\mathcal{K}}/\mathfrak{f} \to \mathfrak{a}/\mathfrak{a}\mathfrak{f}, \quad \overline{x} \mapsto \overline{ax}$$

is well-defined since $a\mathfrak{f} \subset \mathfrak{a}\mathfrak{f}$. Let $x \in \mathcal{O}_{\mathcal{K}}$ with $ax \equiv 0 \bmod \mathfrak{a}\mathfrak{f}$. Then, for all $\mathfrak{p} \in \mathfrak{P}$, we have

$$v_{\mathfrak{p}}(a) + v_{\mathfrak{p}}(x) = v_{\mathfrak{p}}(ax) \geq v_{\mathfrak{p}}(\mathfrak{a}\mathfrak{f}) = v_{\mathfrak{p}}(\mathfrak{a}) + v_{\mathfrak{p}}(\mathfrak{f}) = v_{\mathfrak{p}}(a) + v_{\mathfrak{p}}(\mathfrak{f}),$$

so $v_{\mathfrak{p}}(x) \geq v_{\mathfrak{p}}(\mathfrak{f})$ for all $\mathfrak{p}$. Hence $x \equiv 0 \bmod \mathfrak{f}$ and the map is injective. Since the norm of ideals is multiplicative, we have

$$|\mathcal{O}_{\mathcal{K}}/\mathfrak{a}||\mathfrak{a}/\mathfrak{a}\mathfrak{f}| = |\mathcal{O}_{\mathcal{K}}/\mathfrak{a}\mathfrak{f}| = |\mathcal{O}_{\mathcal{K}}/\mathfrak{a}||\mathcal{O}_{\mathcal{K}}/\mathfrak{f}|.$$

Therefore the map is surjective, too. ■

(3.5) Proposition. The $\mathcal{O}_{\boldsymbol{\mathcal{K}}}$-algebras $\Lambda_{\boldsymbol{\mathcal{K}}}/\mathfrak{F}$ and $\mathrm{M}(\boldsymbol{n}, \mathcal{O}_{\boldsymbol{\mathcal{K}}}/\mathfrak{f})$ are isomorphic.

Proof. As usual, it suffices to consider the case where $\boldsymbol{\mathcal{K}} = \mathcal{K}$ is a number field and where $\Lambda_{\mathcal{K}}$ is of the standard form (1.18), that is, $\Lambda_{\mathcal{K}}$ is the multiplier algebra of $\mathfrak{a} \oplus \mathcal{O}_{\mathcal{K}}^{n-1}$ for an ideal $\mathfrak{a} \subset \mathcal{O}_{\mathcal{K}}$. Let $\mathfrak{P}$ be the set of prime ideals $\mathfrak{p}$ with

$$v_{\mathfrak{p}}(\mathfrak{a}) \neq 0 \quad \text{or} \quad v_{\mathfrak{p}}(\mathfrak{f}) \neq 0.$$

Choose $a \in \mathfrak{a}$ such that $v_{\mathfrak{p}}(a) = v_{\mathfrak{p}}(\mathfrak{a})$ for all $\mathfrak{p} \in \mathfrak{P}$. As seen in the proof of (3.4), the residue class of a generates $\mathfrak{a}/\mathfrak{a}\mathfrak{f}$ as a module over $\mathcal{O}_{\mathcal{K}}/\mathfrak{f}$. Using the Approximation Theorem, we can choose an $a' \in \mathfrak{a}^{-1}$ such that

$$v_{\mathfrak{p}}(a') = -v_{\mathfrak{p}}(a) \quad \text{for all } \mathfrak{p} \in \mathfrak{P} \qquad \text{and} \qquad v_{\mathfrak{p}}(a') \geq 0 \quad \text{elsewhere.}$$

Then a' represents a generator of $\mathfrak{a}^{-1}/\mathfrak{a}^{-1}\mathfrak{f}$ and aa' is a unit modulo $\mathfrak{f}$ because

$$v_{\mathfrak{p}}(aa') = 0 \quad \text{for all } \mathfrak{p} \supset \mathfrak{f}.$$

Choose $x \in \mathcal{O}_{\mathcal{K}}$ such that $xaa' \equiv 1 \bmod \mathfrak{f}$, so $x \notin \mathfrak{p}$ for all $\mathfrak{p} \supset \mathfrak{f}$. By the Chinese Remainder Theorem, we may assume $x \notin \mathfrak{p}$ for all $\mathfrak{p} \in \mathfrak{P}$. Then

$$v_{\mathfrak{p}}(xa) = v_{\mathfrak{p}}(a) \quad \text{for all } \mathfrak{p} \in \mathfrak{P},$$

so the residue class of xa is also a generator of $\mathfrak{a}/\mathfrak{a}\mathfrak{f}$. Replacing a with xa we may assume $aa' \equiv 1 \bmod \mathfrak{f}$.

Since $\mathfrak{F} = \mathfrak{f}\Lambda_{\mathcal{K}}$, each element of $\Lambda_{\mathcal{K}}/\mathfrak{F}$ is represented by a matrix of the form

$$\varGamma = \begin{bmatrix} c_{11} & ac_{12} & \cdots & ac_{1n} \\ a'c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a'c_{n1} & c_{n2} & \cdots & c_{nn} \end{bmatrix} \qquad (c_{ij} \in \mathcal{O}_{\mathcal{K}}).$$

Put

$$C = [c_{ij}], \quad A = \begin{bmatrix} a & 0 \\ 0 & I \end{bmatrix} \quad \text{and} \quad A' = \begin{bmatrix} a' & 0 \\ 0 & I \end{bmatrix}.$$

Then $AA' \equiv I$ and $A'\Gamma A \equiv C \bmod \mathfrak{f}$. Therefore

(3.6)
$$\Lambda_{\mathcal{K}}/\mathfrak{F} \to \mathrm{M}(n, \mathcal{O}_{\mathcal{K}}/\mathfrak{f}), \quad \bar{\Gamma} \mapsto \overline{A'\Gamma A}$$

defines an isomorphism of $\mathcal{O}_{\mathcal{K}}$-algebras. ■

Next, we will show that $\mathrm{SL}(\Lambda_{\mathcal{K}}) \to \mathrm{SL}(\Lambda_{\mathcal{K}}/\mathfrak{F})$ is surjective, essentially by proving that $\mathrm{SL}(\boldsymbol{n}, \mathcal{O}_{\mathcal{K}}/\mathfrak{f})$ is generated by elementary matrices (i.e., matrices with ones on the diagonal and exactly one nonzero entry above or below the diagonal). Remember that a vector $[\,x_1 \ \ldots \ x_n\,]$ over a commutative ring R is called unimodular if

$$x_1R + \cdots + x_nR = R.$$

If A is an invertible matrix over R, all rows of A are unimodular.

(3.7) Lemma. Let $\mathcal{O}$ be an order of a number field and $\mathfrak{a}$ a full ideal of $\mathcal{O}$. Let $[\,x_1 \ \ldots \ x_n\,]$ be a unimodular vector over $\mathcal{O}/\mathfrak{a}$. Then there are coefficients $c_2, \ldots, c_n \in \mathcal{O}/\mathfrak{a}$ such that

$$x_1 + c_2x_2 + \cdots + c_nx_n \in (\mathcal{O}/\mathfrak{a})^\times.$$[1]

Proof. Suppose x_1 is not a unit or else nothing is to show. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}/\mathfrak{a}$ with $x_1 \in \mathfrak{p}$. Since $[\,x_1 \ \ldots \ x_n\,]$ is unimodular, $x_j \notin \mathfrak{p}$ for some $j > 1$. Suppose $\mathfrak{q}$ varies over all prime ideals of $\mathcal{O}/\mathfrak{a}$. By the Chinese Remainder Theorem we may choose an element $c_j \in \mathcal{O}/\mathfrak{a}$ such that

$$c_j \equiv \begin{cases} 1 & \bmod \mathfrak{q} \quad \text{if } x_1 \in \mathfrak{q} \text{ or } x_j \in \mathfrak{q}, \\ 0 & \bmod \mathfrak{q} \quad \text{otherwise.} \end{cases}$$

Then $x_1 + c_jx_j$ only belongs to the prime ideals containing both x_1 and x_j. In particular, $x_1 + c_jx_j \notin \mathfrak{p}$. Repeating the process for $x_1 + c_jx_j$, we ultimately obtain an element of the form $x_1 + c_2x_2 + \cdots + c_nx_n$ which only belongs to the prime ideals containing $x_1, \ldots, x_n$. Since no such prime ideal exists, we have found a unit. ■

From (3.7) it follows that each element of $\mathrm{SL}(n, \mathcal{O}/\mathfrak{a})$ is a product of elementary matrices. In fact, the lemma shows how to reduce a matrix $A = [a_{ij}]$ to the identity matrix using elementary operations: Once we have computed coefficients $c_2, \ldots, c_n$ such that $a_{11} + c_2a_{12} + \cdots + c_na_{1n}$ is a unit, we can replace a_{11} with this unit. Afterwards we can delete all other entries in the first row. If $a_{11} \neq 1$, we replace a_{12} and a_{11} with ones successively and delete a_{12} again. Finally, we delete all other entries in the first column. Repeating this procedure for the remaining rows will transform A into the identity matrix.

[1] Results (3.7) and (3.8) are based on statements K.11 and K.14 by Jantzen and Schwermer (2006), pp. 322–23.

(3.8) Theorem. Let $\mathcal{O}$ be an order of a number field and $\mathfrak{a}$ a full ideal of $\mathcal{O}$. Then $\mathrm{SL}(n, \mathcal{O}/\mathfrak{a})$ is generated by elementary matrices. As a consequence, the canonical map

$$\mathrm{SL}(n, \mathcal{O}) \to \mathrm{SL}(n, \mathcal{O}/\mathfrak{a})$$

is an epimorphism.

Proof. As explained above, each element of $\mathrm{SL}(n, \mathcal{O}/\mathfrak{a})$ is a product of elementary matrices. This proves the theorem because every elementary matrix over $\mathcal{O}/\mathfrak{a}$ can be lifted to an elementary matrix over $\mathcal{O}$. ■

(3.9) Corollary. The canonical map

$$\mathrm{SL}(\Lambda_{\boldsymbol{\mathcal{K}}}) \to \mathrm{SL}(\Lambda_{\boldsymbol{\mathcal{K}}}/\mathfrak{F})$$

is an epimorphism.

Proof. As usual, we may assume that $\boldsymbol{\mathcal{K}} = \mathcal{K}$ is a number field because $\mathrm{SL}(\Lambda_{\boldsymbol{\mathcal{K}}})$ and $\mathrm{SL}(\Lambda_{\boldsymbol{\mathcal{K}}}/\mathfrak{F})$ are direct sums. Furthermore, we may assume that $\Lambda_{\mathcal{K}}$ is of the standard form (1.18). By (3.5),

$$\Lambda_{\mathcal{K}}/\mathfrak{F} \simeq \mathrm{M}(n, \mathcal{O}_{\mathcal{K}}/\mathfrak{f}).$$

Consider the isomorphism (3.6). It preserves determinants, therefore it can be restricted to a group isomorphism

$$\mathrm{SL}(\Lambda_{\mathcal{K}}/\mathfrak{F}) \to \mathrm{SL}(n, \mathcal{O}_{\mathcal{K}}/\mathfrak{f}).$$

Also, it maps elementary matrices onto elementary matrices. Hence $\mathrm{SL}(\Lambda_{\mathcal{K}}/\mathfrak{F})$ is generated by elementary matrices because $\mathrm{SL}(n, \mathcal{O}_{\mathcal{K}}/\mathfrak{f})$ is by (3.8). Each of these generators has a preimage in $\mathrm{SL}(\Lambda_{\mathcal{K}})$, which establishes the corollary. ■

(3.10) Corollary. The image of $\Lambda_{\boldsymbol{\mathcal{K}}}^\times \to (\Lambda_{\boldsymbol{\mathcal{K}}}/\mathfrak{F})^\times$ is isomorphic to

$$\mathrm{SL}(\Lambda_{\boldsymbol{\mathcal{K}}}/\mathfrak{F}) \rtimes \overline{\det(\Lambda_{\boldsymbol{\mathcal{K}}}^\times)}$$

where $\overline{\det(\Lambda_{\boldsymbol{\mathcal{K}}}^\times)}$ denotes the image of $\Lambda_{\boldsymbol{\mathcal{K}}}^\times \to \mathcal{O}_{\boldsymbol{\mathcal{K}}}^\times \to (\mathcal{O}_{\boldsymbol{\mathcal{K}}}/\mathfrak{f})^\times$.

Proof. Since $\mathrm{SL}(\Lambda_{\boldsymbol{\mathcal{K}}}) \to \mathrm{SL}(\Lambda_{\boldsymbol{\mathcal{K}}}/\mathfrak{F})$ is surjective and because of

$$\Lambda_{\boldsymbol{\mathcal{K}}}^\times \simeq \mathrm{SL}(\Lambda_{\boldsymbol{\mathcal{K}}}) \rtimes \mathcal{O}_{\boldsymbol{\mathcal{K}}}^\times \qquad \text{and} \qquad (\Lambda_{\boldsymbol{\mathcal{K}}}/\mathfrak{F})^\times \simeq \mathrm{SL}(\Lambda_{\boldsymbol{\mathcal{K}}}/\mathfrak{F}) \rtimes (\mathcal{O}_{\boldsymbol{\mathcal{K}}}/\mathfrak{f})^\times,$$

an element of $(\Lambda_{\boldsymbol{\mathcal{K}}}/\mathfrak{F})^\times$ has a preimage in $\Lambda_{\boldsymbol{\mathcal{K}}}^\times$ if and only if its determinant stems from a unit in $\mathcal{O}_{\boldsymbol{\mathcal{K}}}$. ■

Let us return to the question whether a residue class $[\Gamma + \mathfrak{F}]$ belongs to the image of

$$\Lambda_{\boldsymbol{\mathcal{K}}}^\times \to (\Lambda_{\boldsymbol{\mathcal{K}}}/\mathfrak{F})^\times \to (\Lambda/\mathfrak{F})^\times \backslash (\Lambda_{\boldsymbol{\mathcal{K}}}/\mathfrak{F})^\times.$$

By our considerations so far, we can easily decide whether $\Gamma + \mathfrak{F}$ belongs to the image of $\Lambda_{\boldsymbol{\mathcal{K}}}^\times \to (\Lambda_{\boldsymbol{\mathcal{K}}}/\mathfrak{F})^\times$ (in which case $[\Gamma + \mathfrak{F}]$ certainly is hit by the composite map). We simply need to check whether

$$\det(\Gamma) \equiv u \mod \mathfrak{f} \qquad \text{for some } u \in \mathcal{O}_{\boldsymbol{\mathcal{K}}}^\times.$$

If the result is negative, one possibility remains for $[\mathit{\Gamma} + \mathfrak{F}]$ to have a preimage in $\Lambda_{\mathcal{K}}$, namely if there is a $U + \mathfrak{F} \in (\Lambda/\mathfrak{F})^{\times}$ such that

$$\det(U\mathit{\Gamma}) \equiv u \mod \mathfrak{f} \qquad \text{for some } u \in \mathcal{O}_{\mathcal{K}}^{\times}.$$

Hence our decision mainly depends on knowledge about the group $\det((\Lambda/\mathfrak{F})^{\times})$. If we are able to compute $\det((\Lambda/\mathfrak{F})^{\times})$, we can actually reduce our problem to the commutative case because we simply need to check whether $\det(\mathit{\Gamma})$ belongs to the image of

$$\mathcal{O}_{\mathcal{K}}^{\times} \to (\mathcal{O}_{\mathcal{K}}/\mathfrak{f})^{\times}/\det((\Lambda/\mathfrak{F})^{\times}).$$

Unfortunately, we cannot expect that

$$\det((\Lambda/\mathfrak{F})^{\times}) = (\mathcal{O}/\mathfrak{f})^{\times}$$

where $\mathcal{O}$ is the center of Λ. For instance, if $\mathcal{O}$ is an order of a number field, the multiplier algebra of $\mathcal{O} \oplus \mathfrak{f}$, given by

$$\Lambda = \begin{bmatrix} \mathcal{O}_{\mathcal{K}} & \mathfrak{f} \\ (\mathcal{O} : \mathfrak{f}) & \mathcal{O} \end{bmatrix},$$

is a counterexample. However, in this case we obviously have

$$\det((\Lambda/\mathfrak{F})^{\times}) = (\mathcal{O}_{\mathcal{K}}/\mathfrak{f})^{\times}.$$

The next proposition deals with situations where $\det((\Lambda/\mathfrak{F})^{\times})$ can be computed just as easily. On top of that, it will also be clear how to select a matrix U with a suitable determinant (which is important if we want to compute a preimage of $U\mathit{\Gamma} + \mathfrak{F}$).

(3.11) Proposition. Let $\mathfrak{A} = \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n$ be a full module in $\mathcal{K}^n$ where $\mathcal{K}$ is a number field. Let Λ the multiplier algebra of $\mathfrak{A}$ and let $\mathcal{O}_i$ denote the multiplier ring of $\mathfrak{a}_i$. Put $\mathcal{O} = \mathcal{O}_1$ and suppose $\mathcal{O}_i \subset \mathcal{O}$ for all i. Then

$$\det(\Lambda) = \mathcal{O}.$$

Furthermore, if $\Lambda_{\mathcal{K}}$ is the multiplier algebra of $\mathfrak{A}_{\mathcal{K}}$ and $\mathfrak{F}$ the conductor of $\Lambda \subset \Lambda_{\mathcal{K}}$, then

$$\det((\Lambda/\mathfrak{F})^{\times}) = (\mathcal{O}/\mathfrak{f})^{\times}.$$

Here, $\mathfrak{f}$ is the conductor of $\mathcal{O}_1 \cap \cdots \cap \mathcal{O}_n \subset \mathcal{O}_{\mathcal{K}}$

Proof. The multiplier algebra of $\mathfrak{A}$ is given by

$$\Lambda = \begin{bmatrix} (\mathfrak{a}_1 : \mathfrak{a}_1) & \cdots & (\mathfrak{a}_1 : \mathfrak{a}_n) \\ \vdots & \ddots & \vdots \\ (\mathfrak{a}_n : \mathfrak{a}_1) & \cdots & (\mathfrak{a}_n : \mathfrak{a}_n) \end{bmatrix},$$

and $(\mathfrak{a}_i : \mathfrak{a}_i)$ is the multiplier ring $\mathcal{O}_i$. By the Leibniz formula, the determinants of matrices in Λ belong to

$$\sum_{\sigma} \prod_{i=1}^{n} (\mathfrak{a}_i : \mathfrak{a}_{\sigma(i)})$$

where σ runs over all permutations of the set $\{1, \ldots, n\}$. If $\sigma = (i_1 \ \ldots \ i_s)$ is a cycle, then

$$\prod_{i=1}^{n} (\mathfrak{a}_i : \mathfrak{a}_{\sigma(i)}) = (\mathfrak{a}_{i_1} : \mathfrak{a}_{i_2}) \cdots (\mathfrak{a}_{i_s} : \mathfrak{a}_{i_1}) \cdot \prod_{\sigma(i)=i} \mathcal{O}_i,$$

and $(\mathfrak{a}_{i_1} : \mathfrak{a}_{i_2}) \cdots (\mathfrak{a}_{i_s} : \mathfrak{a}_{i_1}) \subset \mathcal{O}_{i_1}$ because

$$(\mathfrak{a}_{i_1} : \mathfrak{a}_{i_2}) \cdots (\mathfrak{a}_{i_s} : \mathfrak{a}_{i_1})\, \mathfrak{a}_{i_1} \subset (\mathfrak{a}_{i_1} : \mathfrak{a}_{i_2}) \cdots (\mathfrak{a}_{i_{s-1}} : \mathfrak{a}_{i_s})\, \mathfrak{a}_{i_s} \subset \cdots \subset \mathfrak{a}_{i_1}.$$

Therefore

$$\prod_{i=1}^{n} (\mathfrak{a}_i : \mathfrak{a}_{\sigma(i)}) \subset \mathcal{O}.$$

Since all permutations are products of disjoint cycles, we see that $\det(\Lambda) \subset \mathcal{O}$. Conversely, $\mathcal{O} \oplus I_{n-1}$ is a subset of Λ, so $\mathcal{O} \subset \det(\Lambda)$. The second assertion is a consequence of

$$(\Lambda/\mathfrak{F})^\times \subset (\Lambda_\mathcal{K}/\mathfrak{F})^\times \quad \text{and} \quad \det((\Lambda_\mathcal{K}/\mathfrak{F})^\times) = (\mathcal{O}_\mathcal{K}/\mathfrak{f})^\times.$$

Notice that $\mathcal{O}_1 \cap \cdots \cap \mathcal{O}_n$ is the center of Λ. ■

By the previous proposition, it is particularly easy to examine whether a full $\mathcal{O}$-module $\mathfrak{B}$ is free, provided that $\mathfrak{B}_\mathcal{K}$ is free and that $\mathfrak{C} = (\mathfrak{B} : \mathcal{O}^n)$ is coprime to the conductor of $\Lambda = \mathrm{M}(n, \mathcal{O})$ and $\Lambda_\mathcal{K} = \mathrm{M}(n, \mathcal{O}_\mathcal{K})$, because in this case we have

$$\det((\Lambda/\mathfrak{F})^\times) = (\mathcal{O}/\mathfrak{f})^\times.$$

Testing whether an $\mathcal{O}$-module is free is interesting in itself, but will also be crucial in the next chapter.

Unfortunately, the set of all determinants cannot always be determined as easily as in (3.11). In fact, $\det(\Lambda)$ and $\det(\Lambda/\mathfrak{F})$ do not have to be rings at all—not even if Λ is the multiplier algebra of a direct sum of fractional ideals. This is illustrated by the following example.

Let $\vartheta = \sqrt[6]{-2}$. The maximal order of $\mathcal{K} = \mathbb{Q}(\vartheta)$ is the equation order $\mathbb{Z}[\vartheta]$. It contains the suborders $\mathcal{O}_1$ and $\mathcal{O}_2$ generated by

$$1, 7\vartheta, 7\vartheta^2, \quad \vartheta^3, 7\vartheta^4, 7\vartheta^5 \qquad \text{and} \qquad 1, 7\vartheta, \quad \vartheta^2, 7\vartheta^3, \quad \vartheta^4, 7\vartheta^5.$$

A basis of the intersection $\mathcal{O} = \mathcal{O}_1 \cap \mathcal{O}_2$ is given by $1, 7\vartheta, \ldots, 7\vartheta^5$. Consider the $\mathcal{O}$-module $\mathcal{O}_1 \oplus \mathcal{O}_2$. Its multiplier algebra is given by

$$\Lambda = \begin{bmatrix} \mathcal{O}_1 & (\mathcal{O}_1 : \mathcal{O}_2) \\ (\mathcal{O}_2 : \mathcal{O}_1) & \mathcal{O}_2 \end{bmatrix}$$

and $\mathcal{O}$ is the center of Λ. Let $\mathfrak{f}$ be the conductor of $\mathcal{O} \subset \mathcal{O}_\mathcal{K}$. It is equal to $7\mathcal{O}_\mathcal{K}$, which is a prime ideal of $\mathcal{O}_\mathcal{K}$ because $X^6 + 2$, the minimal polynomial of ϑ, is irreducible modulo 7.[1] Thus it is also a prime ideal of $\mathcal{O}$, $\mathcal{O}_1$ and $\mathcal{O}_2$. Since

$$\mathcal{O}/\mathfrak{f} \simeq \mathbb{F}_7, \quad \mathcal{O}_1/\mathfrak{f} \simeq \mathbb{F}_{7^2}, \quad \mathcal{O}_2/\mathfrak{f} \simeq \mathbb{F}_{7^3} \quad \text{and} \quad \mathcal{O}_\mathcal{K}/\mathfrak{f} \simeq \mathbb{F}_{7^6},$$

[1] Cf. Neukirch (1999), pp. 47–48, (8.3).

we see that $\mathcal{O}_{\mathcal{K}}$ is the smallest order which contains both $\mathcal{O}_1$ and $\mathcal{O}_2$ because $\mathbb{F}_{7^6}/\mathbb{F}_{7^2}$ and $\mathbb{F}_{7^6}/\mathbb{F}_{7^3}$ admit no intermediate fields. If if $\det(\Lambda)$ were a ring, it had to be equal to $\mathcal{O}_{\mathcal{K}}$ because

$$\mathcal{O}_1,\, \mathcal{O}_2 \subset \det(\Lambda) \subset \mathcal{O}_{\mathcal{K}}.$$

In particular, the composite map

$$\Lambda \xrightarrow{\det} \mathcal{O}_{\mathcal{K}} \longrightarrow \mathcal{O}_{\mathcal{K}}/\mathfrak{f}$$

would be surjective. We will argue that this is not true. The set $(\mathcal{O}_1{:}\mathcal{O}_2)(\mathcal{O}_2{:}\mathcal{O}_1)$ is an ideal of $\mathcal{O}_1$ and $\mathcal{O}_2$, hence of $\mathcal{O}_{\mathcal{K}}$, and because of

$$(\mathcal{O}_i : \mathcal{O}_j)(\mathcal{O}_j : \mathcal{O}_i) = (\mathcal{O}_i : \mathcal{O}_j)(\mathcal{O}_j : \mathcal{O}_i)\mathcal{O}_i \subset (\mathcal{O}_i : \mathcal{O}_j)\mathcal{O}_j \subset \mathcal{O}_i,$$

it is contained in $\mathcal{O}_1 \cap \mathcal{O}_2 = \mathcal{O}$. Since $\mathfrak{f}$ is the largest ideal of $\mathcal{O}_{\mathcal{K}}$ inside $\mathcal{O}$, we conclude $(\mathcal{O}_1 : \mathcal{O}_2)(\mathcal{O}_2 : \mathcal{O}_1) \subset \mathfrak{f}$. So if

$$\mathit{\Gamma} = \begin{bmatrix} \gamma_1 & * \\ * & \gamma_2 \end{bmatrix} \in \Lambda,$$

we have

$$\det(\mathit{\Gamma}) \equiv \gamma_1\gamma_2 \bmod \mathfrak{f}.$$

This implies

$$|\overline{\det(\Lambda)}| \leq |\mathcal{O}_1/\mathfrak{f}||\mathcal{O}_2/\mathfrak{f}| = 7^5 < 7^6 = |\mathcal{O}_{\mathcal{K}}/\mathfrak{f}|.$$

Consequently, $\det(\Lambda)$ is not a ring. Furthermore, the maximal order above Λ we have to consider in our example is

$$\Lambda_{\mathcal{K}} = \mathrm{M}(2, \mathcal{O}_{\mathcal{K}})$$

because $(\mathcal{O}_1 \oplus \mathcal{O}_2)\mathcal{O}_{\mathcal{K}} = \mathcal{O}_{\mathcal{K}} \oplus \mathcal{O}_{\mathcal{K}}$. Hence the conductor of $\Lambda \subset \Lambda_{\mathcal{K}}$ is given by

$$\mathfrak{F} = \mathrm{M}(2, \mathfrak{f}).$$

Arguing as above, we see that $\det(\Lambda/\mathfrak{F})$ cannot be a ring either, because the inclusions

$$\mathcal{O}_1/\mathfrak{f},\, \mathcal{O}_2/\mathfrak{f} \subset \det(\Lambda/\mathfrak{F}) \subset \mathcal{O}_{\mathcal{K}}/\mathfrak{f}$$

would imply $\det(\Lambda/\mathfrak{F}) = \mathcal{O}_{\mathcal{K}}/\mathfrak{f}$, yet again, $|\det(\Lambda/\mathfrak{F})| \neq |\mathcal{O}_{\mathcal{K}}/\mathfrak{f}|$.

In the light of these difficulties, a reduction to the commutative situation might not always be feasible, all the more if Λ is the multiplier algebra of a module which cannot be transformed into a direct sum of ideals. Further problems emerge if we turn towards the general case of orders of $\mathrm{M}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$, for instance if

$$\Lambda \neq \Lambda_1 \oplus \cdots \oplus \Lambda_s.$$

Of course we can search $(\Lambda/\mathfrak{F})^\times$ directly for a matrix of a suitable determinant. As seen in section 2.2, we have a decomposition of the form

$$(\Lambda/\mathfrak{F})^\times \simeq \bigoplus_{\mathfrak{p} \supset \mathfrak{f}} (\Lambda/(\mathfrak{F} + \mathfrak{p}^{\nu_\mathfrak{p}}\Lambda))^\times.$$

It would be desirable to determine generators for the groups on the right. Yet an attempt to generalize the method for the commutative situation seems unlikely to succeed. One reason is that $\mathfrak{F}+\mathfrak{p}^{\nu_\mathfrak{p}}\Lambda$, in contrast to $\mathfrak{f}+\mathfrak{p}^{\nu_\mathfrak{p}}$, can be contained in several maximal two-sided ideals of Λ. For instance, if $\mathcal{O}$ is an order of a number field, the multiplier algebras of $\mathfrak{A} = \mathcal{O}_\mathcal{K} \oplus \mathcal{O}$ and $\mathfrak{A}_\mathcal{K} = \mathcal{O}_\mathcal{K} \oplus \mathcal{O}_\mathcal{K}$ are given by

$$\Lambda = \begin{bmatrix} \mathcal{O}_\mathcal{K} & \mathcal{O}_\mathcal{K} \\ \mathfrak{f} & \mathcal{O} \end{bmatrix} \quad \text{and} \quad \Lambda_\mathcal{K} = \mathrm{M}(2, \mathcal{O}_\mathcal{K}),$$

so the conductor of $\Lambda \subset \Lambda_\mathcal{K}$ is given by $\mathfrak{F} = \mathrm{M}(2, \mathfrak{f})$. Suppose that $\mathfrak{f}$ is a prime ideal of $\mathcal{O}_\mathcal{K}$ (as in the case of $\mathcal{O} = \mathbb{Z}[3i]$). Then $\mathfrak{f}$ also is a prime ideal of $\mathcal{O}$. Since $\mathfrak{F} = \mathfrak{f}\Lambda_\mathcal{K}$ contains $\mathfrak{f}\Lambda$, the decomposition above becomes trivial. The sets

$$\mathfrak{P}_1 = \begin{bmatrix} \mathcal{O}_\mathcal{K} & \mathcal{O}_\mathcal{K} \\ \mathfrak{f} & \mathfrak{f} \end{bmatrix} \quad \text{and} \quad \mathfrak{P}_2 = \begin{bmatrix} \mathfrak{f} & \mathcal{O}_\mathcal{K} \\ \mathfrak{f} & \mathcal{O} \end{bmatrix}$$

are two-sided ideals of Λ above $\mathfrak{F}$. Since $\mathfrak{P}_1 + \mathfrak{P}_2 = \Lambda$, they are contained in distinct maximal ideals. Consequently, the same holds for $\mathfrak{F}$.

What is more, the above example also illustrates that the maximal two-sided ideals above $\mathfrak{F}$ cannot be determined in the fashion familiar from the commutative situation, that is, by factorizing $\mathfrak{F}$ as an ideal of $\Lambda_\mathcal{K}$ and intersecting the prime factors with Λ. Indeed, $\mathfrak{F} = \mathfrak{f}\Lambda_\mathcal{K}$ is a maximal two-sided ideal of $\Lambda_\mathcal{K}$ by (1.32), so the only intersection we can obtain is $\mathfrak{F}$ itself. Moreover, $\mathfrak{P}_1$ and $\mathfrak{P}_2$ disappear if we lift them upwards because $\mathfrak{F} \subset \Lambda_\mathcal{K}\mathfrak{P}_i\Lambda_\mathcal{K} \subset \Lambda_\mathcal{K}$ implies $\Lambda_\mathcal{K}\mathfrak{P}_i\Lambda_\mathcal{K} = \Lambda_\mathcal{K}$.

As a last resort, we can still search the additive structure

$$\Lambda/\mathfrak{F} \simeq \bigoplus_{\mathfrak{p}} \Lambda/(\mathfrak{F} + \mathfrak{p}^{\nu_\mathfrak{p}}\Lambda)$$

with the disadvantage of encountering non-units, too. However, all methods considered so far depend on the assumption that the ideal $\mathfrak{C}$ is coprime to the conductor. Of course, this can be guaranteed with the algorithm developed in section 2.4, but this procedure already relies on a search of exponential complexity. As an alternative, we can decide whether $\mathfrak{C}$ is principal on the basis of (1.23). Then we do not have to ensure that $\mathfrak{C}$ is coprime to the conductor. Instead, we can simply search $\Lambda_\mathcal{K}^\times/\Lambda^\times$ for a unit U satisfying $\mathfrak{C} = \Gamma U\Lambda$. Since the map

$$\Lambda_\mathcal{K}^\times/\Lambda^\times \to (\Lambda/\mathfrak{F})^\times \backslash (\Lambda_\mathcal{K}/\mathfrak{F})^\times, \quad [U] \mapsto [U^{-1} + \mathfrak{F}]$$

is injective by (1.36), this can be done in finite time. Unfortunately, it is unclear how to determine the respective cosets efficiently. Still we can search $(\Lambda_\mathcal{K}/\mathfrak{F})^\times$ directly. This approach has its disadvantages, most notably that $(\Lambda_\mathcal{K}/\mathfrak{F})^\times$ is larger than $(\Lambda/\mathfrak{F})^\times$. On top of that, not every class in $(\Lambda_\mathcal{K}/\mathfrak{F})^\times$ stems from a unit in $\Lambda_\mathcal{K}^\times$. On the plus side, we know a lot more about this group than about the subgroup $(\Lambda/\mathfrak{F})^\times$. By (3.5), we have

$$(\Lambda_\mathcal{K}/\mathfrak{F})^\times \simeq \mathrm{GL}(\boldsymbol{n}, \mathcal{O}_\mathcal{K}/\mathfrak{f}) \simeq \bigoplus_{\mathfrak{q}} \mathrm{GL}(\boldsymbol{n}, \mathcal{O}_\mathcal{K}/\mathfrak{q}^{\nu_\mathfrak{q}}) \quad \text{where } \mathfrak{f} = \prod_{\mathfrak{q}} \mathfrak{q}^{\nu_\mathfrak{q}},$$

and every element of $\mathrm{GL}(\boldsymbol{n}, \mathcal{O}_{\mathcal{K}}/\mathfrak{q}^{\nu})$ can be represented by a sum

$$U = U_1 + U_2 \quad \text{with} \quad U_1 \in \mathrm{GL}(\boldsymbol{n}, \mathcal{O}_{\mathcal{K}}/\mathfrak{q}) \quad \text{and} \quad U_2 \in \mathrm{M}(\boldsymbol{n}, \mathfrak{q}/\mathfrak{q}^{\nu})$$

because U represents a unit over $\mathcal{O}_{\mathcal{K}}/\mathfrak{q}^{\nu}$ if and only if $\det(U) \not\equiv 0 \bmod \mathfrak{q}$.

3.3 Algorithms

(3.12) Algorithm — Generators of $(\mathcal{O}/\mathfrak{f})^{\times}$

```
→  $\mathfrak{f}$   conductor of $\mathcal{O} \subset \mathcal{O}_{\mathcal{K}}$
←  $G$   set of representatives generating $(\mathcal{O}/\mathfrak{f})^{\times}$

(1) Compute all prime ideals $\mathfrak{p}$ of $\mathcal{O}$ above $\mathfrak{f}$ as explained in (2.5).
(2) For each $\mathfrak{p} \supset \mathfrak{f}$:
      • determine a $\zeta_{\mathfrak{p}} \in \mathcal{O}$ generating $(\mathcal{O}/\mathfrak{p})^{\times}$ by selecting elements at random;
      • compute a minimal integer $\nu_{\mathfrak{p}}$ with $\mathfrak{p}_{\mathfrak{p}}^{\nu_{\mathfrak{p}}} \subset \mathfrak{f}_{\mathfrak{p}}$ using algorithm (2.33);
      • put $k := 1$ and $G_{\mathfrak{p}} := \{\zeta_{\mathfrak{p}}\}$;
      • while $k < \nu_{\mathfrak{p}}$,
          – compute generators $\pi_1, \dots, \pi_n$ of $\mathfrak{p}^k$;
          – put $G_{\mathfrak{p}} := G_{\mathfrak{p}} \cup \{1 + \pi_1, \dots, 1 + \pi_n\}$ and $k := 2k$.
(3) Put $G := \bigoplus_{\mathfrak{p}} G_{\mathfrak{p}}$. Then $G$ represents a generating set of $\bigoplus_{\mathfrak{p}} (\mathcal{O}/(\mathfrak{f} + \mathfrak{p}^{\nu_{\mathfrak{p}}}))^{\times}$.
(4) Apply the Chinese Remainder Theorem to the elements of $G$ to obtain the
    desired subset of $\mathcal{O}$; cf. (2.15). Return $G$.
```

(3.13) Algorithm — Is Equivalent (Ideal Case)

```
→  $\mathfrak{a}$, $\mathfrak{b}$   full ideals in $\mathcal{K}$
←  $\tau$        true/false
   $\gamma$        element of $\mathcal{K}^{\times}$ satisfying $\gamma\mathfrak{a} = \mathfrak{b}$

(1) Compute $\mathcal{O} = (\mathfrak{a} : \mathfrak{a})$ using algorithm (1.45). If $\mathcal{O} \neq (\mathfrak{b} : \mathfrak{b})$, return false.
(2) Compute an $a \in \mathcal{K}^{\times}$ with $a\mathfrak{b} \subset \mathfrak{a}$. Put $\mathfrak{b} := a\mathfrak{b}$.
(3) Compute $\mathfrak{c} = (\mathfrak{b} : \mathfrak{a})$ using algorithm (1.45). Then $\mathfrak{c} \subset \mathcal{O}$ because of (2).
(4) If $\mathfrak{c}$ is not invertible or if $\mathfrak{c}\mathfrak{a} \neq \mathfrak{b}$, return false.
(5) If $\mathfrak{c}\mathcal{O}_{\mathcal{K}}$ is not principal, return false. Otherwise, obtain $\gamma$ with $\mathfrak{c}\mathcal{O}_{\mathcal{K}} = \gamma\mathcal{O}_{\mathcal{K}}$.
(6) Compute the conductor $\mathfrak{f}$ of $\mathcal{O} \subset \mathcal{O}_{\mathcal{K}}$ using algorithm (1.45).
(7) Compute an $x \in \mathcal{K}^{\times}$ with $x\mathfrak{c} + \mathfrak{f} = \mathcal{O}$ using algorithm (2.35).
```

(8) Put $\mathfrak{c} := x\mathfrak{c}$ and $\gamma := x\gamma$.

(9) Compute the groups $\mathcal{O}_{\boldsymbol{\mathcal{K}}}^{\times}$ and $(\mathcal{O}_{\boldsymbol{\mathcal{K}}}/\mathfrak{f})^{\times}$.

(10) Compute generators of $(\mathcal{O}/\mathfrak{f})^{\times}$ using algorithm (3.12).

(11) Compute the image of $\mathcal{O}_{\boldsymbol{\mathcal{K}}}^{\times} \to (\mathcal{O}_{\boldsymbol{\mathcal{K}}}/\mathfrak{f})^{\times}/(\mathcal{O}/\mathfrak{f})^{\times}$ and check whether $[\gamma + \mathfrak{f}]$ belongs to the image. If so, compute a preimage $u \in \mathcal{O}_{\boldsymbol{\mathcal{K}}}^{\times}$. Otherwise, return `false`.

(12) Put $\gamma := \gamma(uxa)^{-1}$. Return `true` and γ.

(3.14) Algorithm — Is Equivalent (General Case)

→ $\mathfrak{A}$, $\mathfrak{B}$ full modules in $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$

← τ `true`/`false`
$\mathit{\Gamma}$ element of $\mathrm{GL}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$ satisfying $\mathit{\Gamma}\mathfrak{A} = \mathfrak{B}$

(1) Compute $\Lambda = (\mathfrak{A} : \mathfrak{A})$ using algorithm (1.45) as well as $\mathcal{O} = \Lambda \cap \boldsymbol{\mathcal{K}}$.

(2) If $\mathcal{O}$ is not the multiplier ring of $\mathfrak{B}$, return `false`.

(3) Compute E, $\mathit{\Gamma} \in \mathrm{GL}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$ with

$$E\mathfrak{A}_{\boldsymbol{\mathcal{K}}} = \bigoplus_{\iota} (\mathfrak{a}_\iota \oplus \mathcal{O}_{\mathcal{K}_\iota}^{n_\iota}) \quad \text{and} \quad \mathit{\Gamma}\mathfrak{B}_{\boldsymbol{\mathcal{K}}} = \bigoplus_{\iota} (\mathfrak{b}_\iota \oplus \mathcal{O}_{\mathcal{K}_\iota}^{n_\iota})$$

(cf. section 1.3). Put $\mathfrak{a} := \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_s$ and $\mathfrak{b} := \mathfrak{b}_1 \oplus \cdots \oplus \mathfrak{b}_s$.

(4) Check whether $\mathfrak{a}^{-1}\mathfrak{b}$ is principal. If so, obtain γ with $\mathfrak{a}^{-1}\mathfrak{b} = \gamma\mathcal{O}_{\boldsymbol{\mathcal{K}}}$. If not, return `false`.

(5) Put $\mathfrak{A} := E\mathfrak{A}$, $\Lambda := E\Lambda E^{-1}$ and $\mathit{\Gamma} := \mathit{\Gamma}^{-1}$. Multiply the first column of $\mathit{\Gamma}$ with γ (then $\mathit{\Gamma}\mathfrak{A}_{\boldsymbol{\mathcal{K}}} = \mathfrak{B}_{\boldsymbol{\mathcal{K}}}$).

(6) Compute $a \in \boldsymbol{\mathcal{K}}^{\times}$ with $a\mathfrak{B} \subset \mathfrak{A}$. Put $\mathfrak{B} := a\mathfrak{B}$ and $\mathit{\Gamma} := a\mathit{\Gamma}$.

(7) Compute $\mathfrak{C} = (\mathfrak{B} : \mathfrak{A})$ using algorithm (1.45). Then $\mathfrak{C} \subset \Lambda$ because of (6) and $\mathfrak{C}\Lambda_{\boldsymbol{\mathcal{K}}} = \mathit{\Gamma}\Lambda_{\boldsymbol{\mathcal{K}}}$.

(8) If $\mathfrak{C}$ is not an invertible right ideal of Λ or if $\mathfrak{C}\mathfrak{A} \neq \mathfrak{B}$, return `false`.

(9) Compute $\mathfrak{f} = (\mathcal{O}_{\boldsymbol{\mathcal{K}}} : \mathcal{O})$ and $\Lambda_{\boldsymbol{\mathcal{K}}} = (\mathfrak{A}_{\boldsymbol{\mathcal{K}}} : \mathfrak{A}_{\boldsymbol{\mathcal{K}}})$; then each component of $\Lambda_{\boldsymbol{\mathcal{K}}}$ is of the standard form (1.18). Put $\mathfrak{F} := \mathfrak{f}\Lambda_{\boldsymbol{\mathcal{K}}}$.

(10) Try to compute an X with $X\mathfrak{C} + \mathfrak{F} = \Lambda$ using algorithm (2.35). If no such matrix exists, return `false`.

(11) Put $\mathfrak{C} := X\mathfrak{C}$ and $\mathit{\Gamma} := X\mathit{\Gamma}$.

(12) Let G be the image of $\mathcal{O}_{\boldsymbol{\mathcal{K}}}^{\times} \to (\mathcal{O}_{\boldsymbol{\mathcal{K}}}/\mathfrak{f})^{\times}$.

(13) For each $Y \in \Lambda/\mathfrak{F}$, put $C := Y\mathit{\Gamma}$ and check whether $c := \det(C)$ represents an element of G. If so, go to the next step. If no such Y exists, return `false`.

(14) Compute $u = u_1 \oplus \cdots \oplus u_s$ in $\mathcal{O}_{\mathcal{K}}^{\times}$ with $u \equiv c \bmod \mathfrak{f}$.

(15) For $\iota = 1, \ldots, s$:

- multiply the first row of C_ι with u_ι^{-1};
- compute $U_\iota \in \mathrm{SL}(\Lambda_{\mathcal{K}_\iota})$ with $U_\iota \equiv C_\iota \bmod \mathfrak{f}_\iota$ using algorithm (3.16); pay attention to the remark following the algorithm;
- multiply the first row of U_ι with u_ι.

(16) Put $U := U_1 \oplus \cdots \oplus U_s$ and $\mathit{\Gamma} := X^{-1}\mathit{\Gamma}U^{-1}E/a$.

(17) Return `true` and $\mathit{\Gamma}$.

(3.15) Algorithm — Is Free

→ $\mathfrak{A}$ full module in $\mathcal{K}^n$
$\mathcal{O}$ order of $\mathcal{K}$

← τ `true/false`
A element of $\mathrm{GL}(n, \mathcal{K})$ satisfying $\mathfrak{A} = A\mathcal{O}^n$

(1) Put $\mathfrak{C} := (\mathfrak{A} : \mathcal{O}^n)$, $\Lambda := \mathrm{M}(n, \mathcal{O})$ and $\Lambda_{\mathcal{K}} := \mathrm{M}(n, \mathcal{O}_{\mathcal{K}})$. Without loss of generality we may suppose $\mathfrak{C} \subset \Lambda$.

(2) Compute a $\mathit{\Gamma}$ satisfying $\mathfrak{C} = \mathit{\Gamma}\Lambda_{\mathcal{K}}$ and ensure that $\mathfrak{C} + \mathfrak{F} = \Lambda$ as explained in algorithm (3.14).

(3) Put $\gamma := \det(\mathit{\Gamma})$.

(4) Check whether $[\gamma + \mathfrak{f}]$ belongs to the image of $\mathcal{O}_{\mathcal{K}}^{\times} \to (\mathcal{O}_{\mathcal{K}}/\mathfrak{f})^{\times}/(\mathcal{O}/\mathfrak{f})^{\times}$. If so, compute a preimage $\varepsilon \in \mathcal{O}_{\mathcal{K}}^{\times}$. Otherwise return `false`.

(5) Compute an $x \in \mathcal{O}$ satisfying $x(\gamma\varepsilon^{-1}) \equiv 1 \bmod \mathfrak{f}$. Put

$$X := \begin{bmatrix} x & 0 \\ 0 & I_{n-1} \end{bmatrix}.$$

Then $\det(X\mathit{\Gamma}) \equiv \varepsilon \bmod \mathfrak{f}$.

(6) Compute a matrix $U^{-1} \in \Lambda_{\mathcal{K}}^{\times}$ satisfying $U^{-1} \equiv X\mathit{\Gamma} \bmod \mathfrak{F}$, basically using algorithm (3.16); pay attention to the remark at the end.

(7) Put $A := \mathit{\Gamma}U$. Return `true` and A.

(3.16) Algorithm — Lift Matrix

→ C matrix in $\mathrm{SL}(n, \mathcal{O}/\mathfrak{m})$ where $\mathcal{O}$ is an order of a number field

← U matrix in $\mathrm{SL}(n, \mathcal{O})$ satisfying $U \equiv C \mod \mathfrak{m}$.

Suppose the entries of $C = [c_{ij}]$ are elements of $\mathcal{O}$, that is, $\det(C) \equiv 1 \bmod \mathfrak{m}$. The ith column of C will be denoted by C_i.

(1) Put $U := I_n$.

(2) Compute all prime ideals $\mathfrak{p}$ of $\mathcal{O}$ above $\mathfrak{m}$.

(3) The following loop will turn C into a lower triangular matrix modulo $\mathfrak{m}$. For $i = 1, \ldots, n-1$:

- put $\mathfrak{P} := \{\, \mathfrak{p} \supset \mathfrak{m} \mid c_{in} \in \mathfrak{p} \,\}$;
- while $\mathfrak{P}$ is not empty:
  - select $\mathfrak{p} \in \mathfrak{P}$;
  - determine an index $j \in \{i, \ldots, n-1\}$ with $c_{ij} \notin \mathfrak{p}$;
  - compute an element $x_j \in \mathcal{O}$ satisfying

    $$x_j \equiv \begin{cases} 1 \mod \mathfrak{q} & \text{if } c_{ij} \in \mathfrak{q} \text{ or } c_{in} \in \mathfrak{q}, \\ 0 \mod \mathfrak{q} & \text{otherwise} \end{cases}$$

    where $\mathfrak{q}$ runs over all prime ideals above $\mathfrak{m}$;
  - put $U_n := U_n + x_j U_j$ and $C_n := C_n + x_j C_j$ (then $c_{in} \notin \mathfrak{p}$);
  - put $\mathfrak{P} := \{\, \mathfrak{p} \in \mathfrak{P} \mid c_{in} \in \mathfrak{p} \,\}$;
- compute an $x \in \mathcal{O}$ with $x c_{in} \equiv 1 \bmod \mathfrak{m}$ and put $x_n := x(1 - c_{ii})$;
- put $U_i := U_i + x_n U_n$ and $C_i := C_i + x_n C_n$ (then $c_{ii} \equiv 1 \bmod \mathfrak{m}$);
- for $j = i+1, \ldots, n$, put $U_j := U_j - c_{ij} U_i$ and $C_j := C_j - c_{ij} C_i$.

(4) Reduce the entries of C modulo $\mathfrak{m}$. Then C is a lower triangular matrix with diagonal entries equal to 1.

(5) Put $U := CU^{-1}$ and return U.

With a slight modification, the algorithm can also compute preimages under the epimorphism

$$\mathrm{SL}(\Lambda_{\mathcal{K}}) \to \mathrm{SL}(\Lambda_{\mathcal{K}}/\mathfrak{f}\Lambda_{\mathcal{K}})$$

where $\Lambda_{\mathcal{K}}$ is a maximal matrix order of the standard form (1.18), that is,

$$\Lambda_{\mathcal{K}} = \begin{bmatrix} \mathcal{O}_{\mathcal{K}} & \mathfrak{a} & \cdots & \mathfrak{a} \\ \mathfrak{a}^{-1} & \mathcal{O}_{\mathcal{K}} & \cdots & \mathcal{O}_{\mathcal{K}} \\ \vdots & \vdots & \ddots & \vdots \\ \mathfrak{a}^{-1} & \mathcal{O}_{\mathcal{K}} & \cdots & \mathcal{O}_{\mathcal{K}} \end{bmatrix}.$$

If $C \in \Lambda_{\mathcal{K}}$ represents an element of $\mathrm{SL}(\Lambda_{\mathcal{K}}/\mathfrak{f}\Lambda_{\mathcal{K}})$, we can write

$$C = \begin{bmatrix} c_{11} & ac_{12} & \cdots & ac_{1n} \\ a'c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a'c_{n1} & c_{n2} & \cdots & c_{nn} \end{bmatrix}$$

with $c_{ij} \in \mathcal{O}_{\mathcal{K}}$, $a \in \mathfrak{a}$, $a' \in \mathfrak{a}^{-1}$ and $aa' \equiv 1 \bmod \mathfrak{f}$. This was shown in the proof of (3.5). To compute $U \in \mathrm{SL}(\Lambda_{\mathcal{K}})$ with $U \equiv C \bmod \mathfrak{f}\Lambda_{\mathcal{K}}$, we have to take into account that all column operations must stem from elementary matrices in $\Lambda_{\mathcal{K}}$. This requires a modification when dealing with the first row of C. As soon as

$$C \equiv \begin{bmatrix} 1 & 0 & \cdots & 0 \\ a'c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a'c_{n1} & c_{n2} & \cdots & c_{nn} \end{bmatrix},$$

we can obviously proceed as described before. Thus let us consider the main loop of the algorithm for $i = 1$. Again we put

$$\mathfrak{P} := \{\, \mathfrak{p} \supset \mathfrak{f} \mid a_{1n} \in \mathfrak{p} \,\}$$

and we enter the loop over $\mathfrak{P}$. If we find an index $j \geq 2$ with $c_{1j} \notin \mathfrak{p}$, we can execute all commands of the inner loop as before, but if $j = 1$, we have to change the second last line to

– put $U_n := U_n + ax_1U_1$ and $C_n := C_n + ax_1C_1$.

Having left the inner loop, we compute x and x_n as before. The last two lines of the main loop then must be changed to

- put $U_1 := U_1 + a'x_nU_n$ and $C_1 := C_1 + a'x_nC_n$;
- for $j = 2, \ldots, n$, put $U_j := U_j - ac_{1j}U_1$ and $C_j := C_j - ac_{1j}C_1$.

(3.17) Algorithm — Is Similar (Semisimple Matrices)

→	A, B	semisimple integer matrices
←	τ	`true/false`
	C	invertible integer matrix satisfying $CA = BC$

(1) Compute the minimal and the characteristic polynomial μ and χ of A.

(2) If μ is not the minimal polynomial or χ not the characteristic polynomial of B, return `false`.

(3) Compute the factorizations $\mu = \mu_1 \cdots \mu_s$ and $\chi = \mu_1^{n_1} \cdots \mu_s^{n_s}$.

(4) Put $\boldsymbol{n} := (n_1, \dots, n_s)$, $\vartheta := \vartheta_1 \oplus \cdots \oplus \vartheta_s$ where ϑ_ι is a root of μ_ι and $\boldsymbol{\mathcal{K}} := \mathbb{Q}[\vartheta]$.

(5) Compute full modules $\mathfrak{A}$ and $\mathfrak{B}$ in $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$ corresponding to A and B using algorithm (1.43).

(6) Check whether $\mathfrak{A}$ and $\mathfrak{B}$ are equivalent. If so, obtain a matrix $\mathit{\Gamma} \in \mathrm{GL}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$ with $\mathit{\Gamma}\mathfrak{A} = \mathfrak{B}$. If not, return `false`.

(7) Use algorithm (1.44) to obtain the desired matrix C. Return `true` and C.

Part II

Nilpotent Matrices

4 Module-Theoretic Approach II

To solve the problem of similarity in general, it will become necessary to deal with nilpotent elements of suitable matrix orders. For such matrices, we will present another module-theoretic approach. Our strategy will be based on ideas by Grunewald (1980), enhanced with some significant improvements. The special case of nilpotent integer matrices will be dealt with at the end of the chapter.

4.1 Nilpotent Matrices over Orders

The following theorem is the starting point of our considerations.

(4.1) Jordan–Chevalley decomposition. Suppose M is a square rational matrix. Then there are rational matrices S and N satisfying

$$M = S + N \quad \text{and} \quad SN = NS$$

where S is semisimple and N nilpotent. Both matrices are uniquely defined by these properties.

As stated in the theorem, if M and M' are integer matrices, we can decompose them into sums

$$M = S + N \quad \text{and} \quad M' = S' + N'.$$

and by multiplying M and M' with a suitable integer, we may assume that all summands are integer matrices. Suppose M and M' are similar. Then, for some invertible matrix C, we have

$$S' + N' = M' = CMC^{-1} = (CSC^{-1}) + (CNC^{-1}).$$

Since CSC^{-1} is semisimple and commutes with the nilpotent matrix CNC^{-1}, this gives us another Jordan–Chevalley decomposition of M'. But the decomposition is unique, so

$$S' = CSC^{-1} \quad \text{and} \quad N' = CNC^{-1}.$$

In particular, S and S' are similar. So if we want to decide whether M and M' are similar, we can first examine whether this is true for their semisimple parts. This can be accomplished by the methods developed in the first three chapters. Hence, without loss of generality, we may assume that

$$S = S'.$$

We are thus left to decide whether there is an invertible matrix C such that

$$CN = N'C \quad \text{while} \quad CS = SC.$$

As in the first chapter, we will translate this problem into a question about full modules. First, we will explain how to relate N and N' to nilpotent elements of a suitable matrix order.

For the remainder of this chapter, S will be a semisimple integer matrix with minimal polynomial $\mu = \mu_1 \cdots \mu_s$ and characteristic polynomial $\chi = \mu_1^{n_1} \cdots \mu_s^{n_s}$. As before, ϑ_ι will be a root of μ_ι and

$$\boldsymbol{\mathcal{K}} = \mathcal{K}_1 \oplus \cdots \oplus \mathcal{K}_s \quad \text{with } \mathcal{K}_\iota = \mathbb{Q}(\vartheta_\iota).$$

Let

$$\mathfrak{S} = \varOmega \mathbb{Z}^m$$

be a full module in $\boldsymbol{\mathcal{K}^n}$ corresponding to S, where $\varOmega = [\,\omega_1 \ \ldots \ \omega_m\,]$ is a matrix construed as in (1.5), so we have $\boldsymbol{n} = (n_1, \ldots, n_s)$ and

$$m = d_1 n_1 + \cdots + d_s n_s \quad \text{for } d_\iota = [\mathcal{K}_\iota : \mathbb{Q}].$$

Then m is the dimension of $\boldsymbol{\mathcal{K}^n}$ over $\mathbb{Q}$ and $\mathfrak{S}$ is a full module over $\mathbb{Z}[\vartheta]$ where $\vartheta = \vartheta_1 \oplus \cdots \oplus \vartheta_s$. As usual,

$$\Lambda = (\mathfrak{S} : \mathfrak{S})$$

will denote the multiplier algebra of $\mathfrak{S}$.

(4.2) Proposition. Let $M = [m_{ij}]$ be an integer matrix satisfying $SM = MS$ and let $\sigma\colon \mathfrak{S} \to \mathfrak{S}$ be the $\mathbb{Z}$-homomorphism given by

$$\sigma(\omega_i) = \sum_{j=1}^{m} m_{ij}\omega_j \quad \text{for } 1 \le i \le m.$$

Then σ is a homomorphism over $\mathbb{Z}[\vartheta]$. Conversely, if $\sigma\colon \mathfrak{S} \to \mathfrak{S}$ is a $\mathbb{Z}[\vartheta]$-homomorphism, the coefficients m_{ij} given by the equations above define a matrix $M = [m_{ij}]$ commuting with S.

Proof. Write $S = [s_{ij}]$. As shown in the proof of (1.5), we have

$$\vartheta\omega_i = \sum s_{ij}\omega_j.$$

Let σ be the $\mathbb{Z}$-homomorphism given by M. Then, on the one hand, we have

$$\begin{aligned}\sigma(\vartheta\omega_i) = \sigma(\sum_j s_{ij}\omega_j) &= \sum_j s_{ij}\sigma(\omega_j)\\ &= \sum_j s_{ij} \sum_k m_{jk}\omega_k = \sum_k (\sum_j s_{ij}m_{jk})\omega_k,\end{aligned}$$

and on the other hand, we obtain

$$\begin{aligned}\vartheta\sigma(\omega_i) = \vartheta \sum_j m_{ij}\omega_j &= \sum_j m_{ij}\vartheta\omega_j\\ &= \sum_j m_{ij} \sum_k s_{jk}\omega_k = \sum_k (\sum_j m_{ij}s_{jk})\omega_k.\end{aligned}$$

Since $SM = MS$, we see that $\sigma(\vartheta\omega_i) = \vartheta\sigma(\omega_i)$ for all basis vectors ω_i. Thus σ is a homomorphism over $\mathbb{Z}[\vartheta]$.
Conversely, every $\mathbb{Z}[\vartheta]$-homomorphism $\sigma\colon \mathfrak{G} \to \mathfrak{G}$ can be regarded as a homomorphism over $\mathbb{Z}$. Let $M = [m_{ij}]$ be the matrix of σ with respect to the basis $\omega_1, \dots, \omega_m$. Reading the chains of equations above in reverse order, we see that M commutes with S. ■

By (1.1) we know that any homomorphism $\sigma\colon \mathfrak{G} \to \mathfrak{G}$ over $\mathbb{Z}[\vartheta]$ is given by multiplication with a matrix $A \in \mathrm{M}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$, that is,

$$\sigma(\omega) = A\omega \quad \text{for all } \omega \in \mathfrak{G}.$$

As seen in the proof of (1.1), A is the matrix of σ with respect to the standard bases of $\mathcal{K}_\iota^{n_\iota}, \dots, \mathcal{K}_s^{n_s}$. Since σ is an endomorphism, A belongs to the multiplier algebra $\Lambda = (\mathfrak{G} : \mathfrak{G})$.
If M is the matrix as in (4.2), we will say that A is **related** to M. This defines a one-to-one correspondence between integer matrices commuting with S and elements of Λ. Obviously, A is invertible or nilpotent precisely if M is.

We will now prove that there is an invertible matrix C with the properties

$$N' = CNC^{-1} \quad \text{and} \quad CS = SC$$

precisely if the matrices related to N and N' are similar. As for integer matrices, two elements A, $B \in \Lambda$ will be called **similar** if there is a $\varGamma \in \Lambda^\times$ such that $\varGamma A = B\varGamma$. This is a direct generalization of the original concept for integer matrices where $\Lambda = \mathrm{M}(n, \mathbb{Z})$.

(4.3) Theorem. Let N, N' be two nilpotent integer matrices commuting with S and let A, $B \in \Lambda$ be the matrices related to N, N'. The following statements are equivalent.

(1) $S + N$ and $S + N'$ are similar.

(2) A and B are similar.

Proof. Suppose $S + N$ and $S + N'$ are similar. Choose an invertible matrix C such that

$$S + N = C(S + N')C^{-1} = CSC^{-1} + CN'C^{-1}.$$

As described at the beginning of this section, this implies

$$S = CSC^{-1} \quad \text{and} \quad N = CN'C^{-1}.$$

By (4.2), C defines an isomorphism $\mathfrak{G} \to \mathfrak{G}$ which is given by multiplication with a matrix $\varGamma \in \Lambda^\times$ according to (1.1). Write $N = [n_{ij}]$ and $N' = [n'_{ij}]$. On the one hand, we observe

$$\begin{aligned}(\varGamma A)\omega_i = \varGamma \sum_j n_{ij}\omega_j &= \sum_j n_{ij}\varGamma\omega_j \\ &= \sum_j n_{ij} \sum_k c_{jk}\omega_k = \sum_k (\sum_j n_{ij}c_{jk})\omega_k \quad \text{for all } i,\end{aligned}$$

and on the other hand, we have

$$\begin{aligned}(B\mathit{\Gamma})\omega_i = B\sum_j c_{ij}\omega_j &= \sum_j c_{ij}B\omega_j \\ &= \sum_j c_{ij}\sum_k n'_{jk}\omega_k = \sum_k(\sum_j c_{ij}n'_{jk})\omega_k.\end{aligned}$$

Since $\omega_1,\dots,\omega_n$ forms a $\mathbb{Q}$-basis of $\boldsymbol{\mathcal{K}^n}$ and $NC = CN'$, we obtain $\mathit{\Gamma}A = B\mathit{\Gamma}$, that is, A and B are similar.
Conversely, suppose there is a matrix $\mathit{\Gamma} \in \Lambda^\times$ such that $\mathit{\Gamma}A = B\mathit{\Gamma}$. Then $\mathit{\Gamma}$ is related to an invertible matrix C which commutes with S. Again, reading the chains of equations above in reverse order, we obtain $CN' = NC$, hence $S + N$ and $S + N'$ are similar ■

According to the just established theorem, we are confronted with the task of deciding whether two nilpotent matrices in Λ are similar. Below we will define modules corresponding to such matrices by imitating the strategy applied to nilpotent matrices over a field. Let us briefly recall this procedure.[1] Suppose $A \in \mathrm{M}(n,\mathcal{K})$ is nilpotent and ν is the smallest integer such that $A^\nu = 0$. First, choose a vector $v \in \mathcal{K}^n$ with the property $A^{\nu-1}v \neq 0$. Then the vectors

$$v, Av, \dots, A^{\nu-1}v$$

are linearly independent. Next, choose a vector v' with the same property such that

$$v, Av, \dots, A^{\nu-1}v, \quad v', Av', \dots, A^{\nu-1}v'$$

are linearly independent. If no such vector exists, repeat the search for v' with ν replaced by $\nu - 1$. Ultimately, we obtain a basis of the form

$$v, Av, \dots, A^{\nu-1}v, \quad v', Av', \dots, \quad v'', Av'', \dots$$

Another matrix B is similar to A if and only if there is a basis

$$w, Bw, \dots, B^{\nu-1}w, \quad w', Bw', \dots, \quad w'', Bw'', \dots$$

of the same form. The matrix C satisfying $CA = BC$ is given by the conditions

$$Cv = w, \quad CAv = Bw, \quad \dots, \quad CA^{\nu-1}v = B^{\nu-1}w, \quad \dots$$

(4.4) Definition. Let $A \in \Lambda$ be a nilpotent matrix. A full module $\mathfrak{A}$ in $\boldsymbol{\mathcal{K}^n}$ is called an ***A*-module** if there are matrices $\mathit{\Xi}_1, \dots, \mathit{\Xi}_\nu$ such that

- the columns of $\mathit{\Xi} = [\,\mathit{\Xi}_1 \ \dots \ \mathit{\Xi}_\nu\,]$ form a $\mathbb{Z}$-basis of $\mathfrak{A}$,
- the columns of $\mathit{\Xi}_k$ belong to the kernel of A^k, and
- $\mathit{\Xi}_k = [\,A\mathit{\Xi}_{k+1} \ *\,]$ for $k < \nu$.

Furthermore, a matrix $\mathit{\Xi}$ as above is called an ***A*-basis** of $\mathfrak{A}$ over $\mathbb{Z}$.

[1] For more detail, see how to compute the Jordan normal form of a nilpotent matrix.

Clearly, not every full module is an A-module, but it is easy to construct such a module following the requirements of the definition. Henceforth the notation $\mathit{\Xi} = [\,\mathit{\Xi}_1 \ \ldots \ \mathit{\Xi}_\nu\,]$ shall always indicate that the individual blocks satisfy these requirements. Usually we will drop the addition "over $\mathbb{Z}$" if it is clear that $\mathit{\Xi}$ is a $\mathbb{Z}$-basis.

From the definition it follows that the columns of $\mathit{\Xi}_k$ belong exactly to the kernel of A^k, that is, not to the kernel of A^{k-1}. Also, the definition implies that ν is the smallest integer such that $A^\nu = 0$. Otherwise $\mathfrak{A}$ would not be a full module.

To make things more clear, let us consider an example. Suppose $\Lambda = \mathrm{M}(5, \mathbb{Z})$ and

$$A = \begin{bmatrix} 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Then $\nu = 3$ and

$$\mathit{\Xi}_3 = [\,e_5\,], \qquad \mathit{\Xi}_2 = [\,A\mathit{\Xi}_3 \ e_4\,] = [\,2e_3 \ e_4\,], \qquad \mathit{\Xi}_1 = A\mathit{\Xi}_2 = [\,4e_1 \ 2e_2\,]$$

are suitable choices for an A-basis $\mathit{\Xi} = [\,\mathit{\Xi}_1 \ \mathit{\Xi}_2 \ \mathit{\Xi}_3\,]$.

Our next goal is to explain how an examination of A- and B-modules can answer the question whether the respective matrices are similar. For this we need a stronger concept than equivalence because the matrix $\mathit{\Gamma}$ we are looking for must belong to $\Lambda^\times$, not merely to $\mathrm{GL}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$. For example, suppose $\Lambda = \mathrm{M}(2, \mathbb{Z})$. If

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 0 & 2 \\ 0 & 0 \end{bmatrix},$$

then $\mathfrak{A} = \mathbb{Z}^2$ is an A-module and

$$\mathfrak{B} = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} \mathbb{Z}^2$$

a B-module. These modules are equivalent because $\mathit{\Gamma}\mathfrak{A} = \mathfrak{B}$ for $\mathit{\Gamma} = \left[\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right]$, but there is no matrix in $\Lambda^\times = \mathrm{GL}(2, \mathbb{Z})$ satisfying this equation. In fact, A and B are not similar, as one easily verifies.
Yet even the existence of a matrix $\mathit{\Gamma} \in \Lambda^\times$ with $\mathit{\Gamma}\mathfrak{A} = \mathfrak{B}$ may not be enough. For example, suppose

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} \qquad \text{and} \qquad B = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Then $\mathbb{Z}^3$ is an A- and a B-module. But again, the matrices are not similar. This time, the Jordan normal forms of A and B are different.

Of course, if the matrices are to be similar, their Jordan normal forms (over the complex numbers, say) must coincide. In terms of A- and B-bases, we can formalize this requirement in the following way. The bases

$$\varXi = [\,\varXi_1 \;\ldots\; \varXi_\nu\,] \qquad \text{and} \qquad \varUpsilon = [\,\varUpsilon_1 \;\ldots\; \varUpsilon_{\nu'}\,]$$

are said to be of the same **block structure** if $\nu = \nu'$ and if the blocks $\varXi_k$ and $\varUpsilon_k$ have the same size for all k. Indeed, finding A- and B-bases of the same block structure is equivalent to obtaining the same Jordan normal form for both matrices.

(4.5) Definition. Let $\mathfrak{A}$ be an A-module and $\mathfrak{B}$ a B-module where A, $B \in \Lambda$ are nilpotent matrices with the same Jordan normal form. The modules are called **similar** if there is

- an A-basis $\varXi$ of $\mathfrak{A}$,
- a B-basis $\varUpsilon$ of $\mathfrak{B}$, and
- a matrix $\varGamma \in \Lambda^\times$

such that $\varGamma\varXi = \varUpsilon$.

Obviously, two modules are equivalent if they are similar. This new and stronger concept is the key to solving our problem.

(4.6) Theorem. Let A, $B \in \Lambda$ be nilpotent. Let $\mathfrak{A}$ be an A- and $\mathfrak{B}$ a B-module. Then the following statements hold.

(1) If $\mathfrak{A}$ and $\mathfrak{B}$ are similar, so are A and B.

(2) If $B = \varGamma A \varGamma^{-1}$ for some $\varGamma \in \Lambda^\times$, then $\varGamma\mathfrak{A}$ is a B-module.

Proof. Suppose $\mathfrak{A}$ and $\mathfrak{B}$ are similar. Let $\varXi = [\,\varXi_1 \;\ldots\; \varXi_\nu\,]$ be an A-basis of $\mathfrak{A}$ and $\varUpsilon = [\,\varUpsilon_1 \;\ldots\; \varUpsilon_\nu\,]$ a B-basis of $\mathfrak{B}$. Then the bases must have the same structure. Let $\varGamma \in \Lambda^\times$ satisfy $\varGamma\varXi = \varUpsilon$, that is, $\varGamma\varXi_k = \varUpsilon_k$ for all k. Since $\varXi_k = [\,A\varXi_{k+1} \;*\,]$ and $\varUpsilon_k = [\,B\varUpsilon_{k+1} \;*\,]$ for $k < \nu$, this implies

$$[\,\varGamma A\varXi_{k+1} \;*\,] = [\,B\varUpsilon_{k+1} \;*\,] \quad \text{for } k < \nu.$$

Since $A\varXi_1 = B\varUpsilon_1 = 0$, we obtain

$$\varGamma A\varXi_k = B\varGamma\varXi_k \quad \text{for all } k.$$

Therefore $\varGamma A = B\varGamma$ because the columns of $\varXi_1, \ldots, \varXi_\nu$ form a $\mathbb{Q}$-bases of $\boldsymbol{\mathcal{K}^n}$. This proves the first statement.
Next suppose $B = \varGamma A\varGamma^{-1}$. Obviously, $\varGamma\varXi = [\,\varGamma\varXi_1 \;\ldots\; \varGamma\varXi_\nu\,]$ is a $\mathbb{Z}$-basis of $\varGamma\mathfrak{A}$. The columns of $\varGamma\varXi_k$ belong to the kernel of $B^k = \varGamma A^k \varGamma^{-1}$, and

$$\varGamma\varXi_k = [\,\varGamma A\varXi_{k+1} \;*\,] = [\,B\varGamma\varXi_{k+1} \;*\,] \quad \text{for } k < \nu.$$

Hence $\varGamma\varXi$ is a B-basis and thus $\varGamma\mathfrak{A}$ is a B-module. ■

Notice that the theorem explicitly does not state that $\mathfrak{A}$ and $\mathfrak{B}$ are similar if A and B are. In fact, even if $A = B$, the modules do not have to be similar. For example, suppose

$$A = \begin{bmatrix} 0 & 2 \\ 0 & 0 \end{bmatrix} \quad \text{and} \quad \Lambda = \begin{bmatrix} \mathcal{O}_{\mathcal{K}} & \mathfrak{a} \\ \mathfrak{a}^{-1} & \mathcal{O}_{\mathcal{K}} \end{bmatrix}$$

where $\mathcal{O}_{\mathcal{K}} = \mathbb{Z}[i]$ and $\mathfrak{a} = 2\mathcal{O}_{\mathcal{K}}$. Then

$$\mathfrak{A} = \begin{bmatrix} 2 & 2i & 0 & 0 \\ 0 & 0 & 1 & i \end{bmatrix} \mathbb{Z}^4 \quad \text{and} \quad \mathfrak{A}' = \begin{bmatrix} 2 & 2i & 1 & i \\ 0 & 0 & 1 & i \end{bmatrix} \mathbb{Z}^4$$

are two A-modules in $\mathcal{K}^2$. All A-bases of $\mathfrak{A}$ and $\mathfrak{A}'$ are of the form

$$\varXi = \begin{bmatrix} 2x_1 & 2x_2 & a_1 & a_2 \\ 0 & 0 & x_1 & x_2 \end{bmatrix} \quad \text{and} \quad \varXi' = \begin{bmatrix} 2x_1' & 2x_2' & c_1 & c_2 \\ 0 & 0 & x_1' & x_2' \end{bmatrix}$$

where x_1, x_2 and x_1', x_2' are bases of $\mathcal{O}_{\mathcal{K}}$ and $a_1, a_2 \in \mathfrak{a}$, but $c_1, c_2 \notin \mathfrak{a}$. If $\mathfrak{A}$ and $\mathfrak{A}'$ were similar, there would be a matrix

$$\varGamma = \begin{bmatrix} c & a \\ * & * \end{bmatrix} \in \Lambda^\times$$

and suitable A-bases $\varXi$ and $\varXi'$ such that $\varGamma\varXi = \varXi'$, that is,

$$\begin{bmatrix} * & * & ca_1 + ax_1 & ca_2 + ax_2 \\ * & * & * & * \end{bmatrix} = \begin{bmatrix} 2x_1' & 2x_2' & c_1 & c_2 \\ 0 & 0 & x_1' & x_2' \end{bmatrix}.$$

This leads to the contradiction that $c_i = ca_i + ax_i$ would belong to $\mathfrak{a}$.

Nevertheless, the theorem makes it possible to switch from matrices to modules when dealing with the problem of similarity. Remember that Λ is the multiplier algebra of a full module $\mathfrak{S}$ which was fixed at the beginning of the section. If $\mathfrak{A}$ is an A-module, we may assume that $\mathfrak{A} \subset \mathfrak{S}$. Suppose $B = \varGamma A \varGamma^{-1}$ for some $\varGamma \in \Lambda^\times$. Then $\varGamma\mathfrak{A}$ is a B-module. Moreover,

$$\varGamma\mathfrak{A} \subset \varGamma\mathfrak{S} = \mathfrak{S} \quad \text{and} \quad [\mathfrak{S} : \varGamma\mathfrak{A}] = [\mathfrak{S} : \mathfrak{A}].$$

Yet there are only finitely many submodules of the same index in $\mathfrak{S}$; in particular, only finitely many B-modules. So either $\mathfrak{A}$ is similar to one of these B-modules or the matrices are not similar. This leaves us with two tasks:

(1) Enumerate all B-modules $\mathfrak{B} \subset \mathfrak{S}$ with $[\mathfrak{S} : \mathfrak{B}] = [\mathfrak{S} : \mathfrak{A}]$;

(2) decide whether $\mathfrak{A}$ is similar to one of these modules $\mathfrak{B}$.

In the next two sections, we will solve these problems under the assumption that the modules are free. Fortunately, this simplification will mean no restriction to the matrices concerned. Furthermore, we will explain how to determine modules of minimal index in order to keep their number as low as possible.

4.2 Similarity of Free Modules

Let $\mathfrak{A}$ be an A- and $\mathfrak{B}$ a B-module where A, $B \in \Lambda$ are nilpotent matrices with the same Jordan normal form. Our goal is to decide whether $\mathfrak{A}$ and $\mathfrak{B}$ are similar, that is, if there is an A-basis $\varXi$ of $\mathfrak{A}$ and a B-basis $\varUpsilon$ of $\mathfrak{B}$ such that

$$\varGamma\varXi = \varUpsilon \quad \text{for some } \varGamma \in \Lambda^\times.$$

In this section we will explain how to decide whether $\mathfrak{A}$ and $\mathfrak{B}$ are similar if the modules are free. First, let us illustrate which problems can arise in the general case. To begin with, we should at least be able to decide whether $\mathfrak{A}$ and $\mathfrak{B}$ are equivalent, that is, whether

$$\varGamma\mathfrak{A} = \mathfrak{B} \text{ for some } \varGamma \in \mathrm{GL}(\boldsymbol{n}, \boldsymbol{\mathcal{K}}).$$

In a next step we could try to decide whether $\varGamma$ can be chosen in $\Lambda^\times$. If $\varGamma \notin \Lambda^\times$, we must find a U such that $U\varGamma \in \Lambda^\times$ and $U\varGamma\mathfrak{A} = \mathfrak{B}$. Since $\varGamma\mathfrak{A} = \mathfrak{B}$, this means U belongs to $\Delta^\times$ where $\Delta = (\mathfrak{B}\,{:}\,\mathfrak{B})$. In other words, we are looking for a matrix

$$\varGamma \in \{\, U^{-1}S \mid S \in \Lambda^\times,\ U \in \Delta^\times \,\} \quad \text{with} \quad \varGamma\mathfrak{A} = \mathfrak{B}.$$

Yet this set of products might not be contained in any matrix order (for example, if Λ and Δ are different maximal orders) and it might not be a group either. This definitely complicates the search for $\varGamma$. And even if we find such a matrix, the original question is still unanswered.

Let us briefly consider the case $\Lambda = \mathrm{M}(n, \mathbb{Z})$. In this situation, all modules are free, as they are finitely generated $\mathbb{Z}$-modules in $\mathbb{Q}^n$, so $\varXi$ and $\varUpsilon$ are square matrices. Then

$$\varGamma\varXi = \varUpsilon \quad \Leftrightarrow \quad \varGamma = \varUpsilon\varXi^{-1}.$$

We therefore have to examine whether there are A- and B-bases $\varXi$ and $\varUpsilon$ such that $\varUpsilon\varXi^{-1}$ belongs to $\Lambda^\times$. In fact, as we will see, $\varXi$ can be held constant, thus we only have to look for a suitable basis $\varUpsilon$.

In general, the matrices $\varXi$ and $\varUpsilon$ are rectangular, with more columns than rows. However, we actually want to decide whether A and B are similar, and we may choose the modules $\mathfrak{A}$ and $\mathfrak{B}$ as we desire. In particular, we can choose them to be free.

For the main part of this section, and if not stated otherwise, Λ will be an order of $\mathrm{M}(n, \mathcal{K})$ where $\mathcal{K}$ is a number field. Later on, we will see that our considerations can be transferred to the general case without much difficulty. Let $\mathcal{O}$ be an order of $\mathcal{K}$. In reference to (4.4), a full $\mathcal{O}$-module $\mathfrak{A} \subset \mathcal{K}^n$ will be called a **free *A*-module** over $\mathcal{O}$ if there are matrices $X_1, \ldots, X_\nu$ such that

- $X = [\, X_1 \ \ldots \ X_\nu \,]$ is an $\mathcal{O}$-basis of $\mathfrak{A}$,
- the columns of X_k belong to the kernel of A^k, and
- $X_k = [\, AX_{k+1} \ * \,]$ for $k < \nu$.

A matrix X as above will be called an ***A*-basis** of $\mathfrak{A}$ over $\mathcal{O}$.

Notice that we made no further assumptions about $\mathcal{O}$. In fact, we can choose the order just as we desire. This will be important later, when we will specify convenient choices for $\mathcal{O}$. For now, the order can be assumed to be arbitrary. Again, we will often drop the addition “over $\mathcal{O}$”.

(4.7) Proposition. Let $\mathfrak{A} \subset \mathcal{K}^n$ be a free A-module over $\mathcal{O}$. Then $\mathfrak{A}$ is an A-module in the sense of (4.4).

Proof. Let $X = [\, X_1 \ \dots \ X_\nu \,]$ be an A-basis of $\mathfrak{A}$ over $\mathcal{O}$ and let $\omega_1, \dots, \omega_d$ be a $\mathbb{Z}$-basis of $\mathcal{O}$. Write

$$X_k = [\, AX_{k+1} \ X_k^* \,] \quad \text{for } k < \nu \quad \text{and} \quad X_\nu = X_\nu^*.$$

Put $\varXi_k^* = [\, \omega_1 X_k^* \ \dots \ \omega_d X_k^* \,]$ for all k and

$$\varXi_k = [\, A\varXi_{k+1} \ \varXi_k^* \,] \quad \text{for } k < \nu \text{ where } \varXi_\nu = \varXi_\nu^*.$$

Then $\varXi$ is an A-basis of $\mathfrak{A}$ over $\mathbb{Z}$. ■

We also want to transfer the concept of similarity to free A-modules. Again, it will be important that A and B have the same Jordan normal form. We will ensure this by requiring that the matrices have the same **structure**. By this we understand a descending sequence

$$n_1 \geq \ldots \geq n_\nu$$

of integers with the property that $n_1 + \cdots + n_k$ is the dimension of the kernel of A^k over $\mathcal{K}$. In particular, we have

$$n = n_1 + \cdots + n_\nu.$$

If $X = [\, X_1 \ \dots \ X_\nu \,]$ is an A-basis over some order of $\mathcal{K}$ and if $n_1 \geq \ldots \geq n_\nu$ is the structure of A, then the block X_k has the size $n \times n_k$.

Let A, $B \in \Lambda$ be two nilpotent matrices of the same structure and let $\mathcal{O}$ be an order of $\mathcal{K}$. Let $\mathfrak{A}$ be a free A-module and $\mathfrak{B}$ a free B-module, both defined over $\mathcal{O}$. The modules are called **similar** if there is

- an A-basis X of $\mathfrak{A}$,
- a B-basis Y of $\mathfrak{A}$, and
- and a matrix $\varGamma \in \Lambda^\times$

such that $\varGamma X = Y$.

Just as free A-modules are A-modules in the original sense, free A- and B-modules are similar if and only if they are similar in the sense of (4.5). Moreover, theorem (4.6) can be translated in the following way (with practically the same proof).

(4.8) Theorem. Let A, $B \in \Lambda$ be nilpotent and let $\mathcal{O}$ be an order of $\mathcal{K}$. Let $\mathfrak{A}$ be a free A-module and $\mathfrak{B}$ a free B-module, both defined over $\mathcal{O}$. Then the following statements hold.

(1) If $\mathfrak{A}$ and $\mathfrak{B}$ are similar, then A and B are.

(2) If $B = \Gamma A \Gamma^{-1}$ for some $\Gamma \in \Lambda^\times$, then $\Gamma\mathfrak{A}$ is a free B-module.

According to the theorem, we can restrict ourselves to free A- and B-modules to decide whether the matrices are similar. As outlined in the case $\mathcal{O} = \mathbb{Z}$ at the beginning of this section, this comes down to the question whether $YX^{-1} \in \Lambda^\times$ for suitable A- and B-bases X and Y.

From now on, suppose all matrices have the same structure $n_1 \geq \ldots \geq n_\nu$. Furthermore, let

$$J = \begin{bmatrix} 0 & J_{12} & & 0 \\ & \ddots & \ddots & \\ & & \ddots & J_{\nu-1,\nu} \\ 0 & & & 0 \end{bmatrix}$$

be the $n \times n$ matrix with blocks

$$J_{k-1,k} = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \\ & & \\ 0 & & 0 \end{bmatrix}$$

of the size $n_{k-1} \times n_k$. Clearly, J is nilpotent with structure $n_1 \geq \ldots \geq n_\nu$ and $\mathcal{O}^n$ is a free J-module. As a first result, we will determine all J-bases of $\mathcal{O}^n$.

(4.9) Proposition. A matrix $U \in \mathrm{GL}(n, \mathcal{O})$ is a J-basis of $\mathcal{O}^n$ if and only if

$$U = \begin{bmatrix} U_{11} & \cdots & U_{1\nu} \\ & \ddots & \vdots \\ 0 & & U_{\nu\nu} \end{bmatrix}$$

where $U_{k\ell}$ is of the size $n_k \times n_\ell$ and

$$U_{k-1,\ell-1} = \begin{bmatrix} U_{k\ell} & * \\ 0 & * \end{bmatrix} \quad \text{for } \ell \geq k > 1.$$

Before proving this proposition, let us consider two examples. First, suppose $n_1 = \ldots = n_\nu$. Then

$$J = \begin{bmatrix} 0 & I & & 0 \\ & \ddots & \ddots & \\ & & \ddots & I \\ 0 & & & 0 \end{bmatrix} \quad \text{and} \quad U = \begin{bmatrix} U_1 & U_2 & \cdots & U_\nu \\ & U_1 & \ddots & \vdots \\ & & \ddots & U_2 \\ 0 & & & U_1 \end{bmatrix}.$$

where I is the identity matrix of size $n_1 \times n_1$. Second, consider the structure $3 \geq 2 \geq 1$. In this case,

$$J = \begin{bmatrix} 0 & 0 & 0 & \mathbf{1} & \mathbf{0} & 0 \\ 0 & 0 & 0 & \mathbf{0} & \mathbf{1} & 0 \\ 0 & 0 & 0 & \mathbf{0} & \mathbf{0} & 0 \\ & & & 0 & 0 & \mathbf{1} \\ & & & 0 & 0 & \mathbf{0} \\ & & & & & 0 \end{bmatrix} \quad \text{and} \quad U = \begin{bmatrix} u_{11} & u_{12} & u_{13} & \boldsymbol{u_{14}} & \boldsymbol{u_{15}} & * \\ 0 & u_{22} & u_{23} & \mathbf{0} & \boldsymbol{u_{25}} & * \\ 0 & 0 & u_{33} & \mathbf{0} & \mathbf{0} & * \\ & & & u_{11} & u_{12} & \boldsymbol{u_{14}} \\ & & & 0 & u_{22} & \mathbf{0} \\ & & & & & u_{11} \end{bmatrix}$$

(with emphasis simply to distinguish blocks).

Proof. Let U be a J-basis of $\mathcal{O}^n$. Write

$$U = \begin{bmatrix} U_{11} & \cdots & U_{1\nu} \\ \vdots & \ddots & \vdots \\ U_{\nu 1} & \cdots & U_{\nu\nu} \end{bmatrix} \quad \text{and} \quad U_k = \begin{bmatrix} U_{1k} \\ \vdots \\ U_{\nu k} \end{bmatrix}$$

with $n_k \times n_\ell$ blocks $U_{k\ell}$. By our assumptions we know that

$$U_{k-1} = [\, JU_k \; * \,] \quad \text{for } k > 1.$$

We have to show that

$$U_{k-1,\ell-1} = \begin{bmatrix} U_{k\ell} & * \\ 0 & * \end{bmatrix} \quad \text{for } \ell \geq k > 1.$$

This is true, indeed, because

$$JU_k = \begin{bmatrix} 0 & J_{12} & & 0 \\ & \ddots & \ddots & \\ & & \ddots & J_{\nu-1,\nu} \\ 0 & & & 0 \end{bmatrix} \begin{bmatrix} U_{1k} \\ \vdots \\ \vdots \\ U_{\nu k} \end{bmatrix} = \begin{bmatrix} J_{12}U_{2k} \\ \vdots \\ J_{\nu-1,\nu}U_{\nu k} \\ 0 \end{bmatrix}$$

and

$$J_{\ell-1,\ell}U_{\ell k} = \begin{bmatrix} I_\ell \\ 0 \end{bmatrix} U_{\ell k} = \begin{bmatrix} U_{\ell k} \\ 0 \end{bmatrix}.$$

Notice that the last block in the product JU_k vanishes, so k-fold multiplication with J leaves us with at most $\nu - k$ nonzero blocks of the form

$$J_{\ell-k,\ell-(k-1)} \cdots J_{\ell-1,\ell}U_{\ell k} \quad (\ell > k).$$

Yet the columns of U_k belong to the kernel of J^k, so these products have to be zero, too. As seen above, left multiplication with $J_{i-1,i}$ simply attaches zero rows to a matrix, thus we must have

$$U_{\ell k} = 0 \quad \text{for } \ell > k.$$

In conclusion, U is of the desired form. Conversely, the calculations above also serve as a proof that any matrix U of the stated form is a J-basis of $\mathcal{O}^n$. ■

(4.10) Proposition. A matrix $U \in \mathrm{GL}(n, \mathcal{O})$ is of the form as in (4.9) if and only if $JU = UJ$.

Proof. Suppose U is of the form as in (4.9). On the one hand, we have

$$JU = \begin{bmatrix} 0 & J_{12}U_{22} & J_{12}U_{23} & \cdots & J_{12}U_{2\nu} \\ & 0 & J_{23}U_{33} & \cdots & J_{23}U_{3\nu} \\ & & \ddots & \ddots & \vdots \\ & & & 0 & J_{\nu-1,\nu}U_{\nu\nu} \\ 0 & & & & 0 \end{bmatrix},$$

and on the other hand, we obtain

$$UJ = \begin{bmatrix} 0 & U_{11}J_{12} & U_{12}J_{23} & \cdots & U_{1,\nu-1}J_{\nu-1,\nu} \\ & 0 & U_{22}J_{23} & \cdots & U_{2,\nu-1}J_{\nu-1,\nu} \\ & & \ddots & \ddots & \vdots \\ & & & 0 & U_{\nu-1,\nu-1}J_{\nu-1,\nu} \\ 0 & & & & 0 \end{bmatrix}.$$

Comparing the blocks, we see that

$$J_{k-1,k}U_{k\ell} = \begin{bmatrix} I_{n_k} \\ 0 \end{bmatrix} U_{k\ell} = \begin{bmatrix} U_{k\ell} \\ 0 \end{bmatrix} = \begin{bmatrix} U_{k\ell} & * \\ 0 & * \end{bmatrix} \begin{bmatrix} I_{n_\ell} \\ 0 \end{bmatrix} = U_{k-1,\ell-1}J_{\ell-1,\ell},$$

hence $JU = UJ$. Now suppose

$$U = \begin{bmatrix} U_{11} & \cdots & U_{1\nu} \\ \vdots & \ddots & \vdots \\ U_{\nu 1} & \cdots & U_{\nu\nu} \end{bmatrix}$$

is a matrix that commutes with J. Then U also commutes with

$$J^k = \begin{bmatrix} 0 & \cdots & 0 & J_{1,k+1} & & 0 \\ & \ddots & & \ddots & \ddots & \\ & & \ddots & & \ddots & J_{\nu-k,\nu} \\ & & & \ddots & & 0 \\ & & & & \ddots & \vdots \\ 0 & & & & & 0 \end{bmatrix}$$

where $J_{\ell,\ell+k}$ is the $(\ell, \ell+k)$-block of J^k. We have

$$J_{\ell,\ell+k} = J_{\ell,\ell+1} \cdots J_{\ell+k-1,\ell+k} = \begin{bmatrix} I_{n_{\ell+k}} \\ 0 \end{bmatrix}.$$

Comparing the blocks of

$$J^kU = \begin{bmatrix} J_{1,k+1}U_{k+1,1} & \cdots & \cdots & J_{1,k+1}U_{k+1,\nu} \\ \vdots & & & \vdots \\ J_{\nu-k,\nu}U_{\nu,1} & \cdots & \cdots & J_{\nu-k,\nu}U_{\nu,\nu} \\ 0 & \cdots & \cdots & 0 \\ \vdots & & & \vdots \\ 0 & \cdots & \cdots & 0 \end{bmatrix}$$

and

$$UJ^k = \begin{bmatrix} 0 & \cdots & 0 & U_{11}J_{1,k+1} & \cdots & U_{1,\nu-k}J_{\nu-k,\nu} \\ \vdots & & \vdots & \vdots & & \vdots \\ \vdots & & \vdots & \vdots & & \vdots \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & U_{\nu 1}J_{1,k+1} & \cdots & U_{\nu,\nu-k}J_{\nu-k,\nu} \end{bmatrix},$$

we see that

$$0 = J_{\ell,\ell+k}U_{\ell+k,k} = \begin{bmatrix} U_{\ell+k,k} \\ 0 \end{bmatrix} \quad \text{for } 1 \le k < \nu \text{ and } 1 \le \ell \le \nu - k.$$

Hence $U_{\ell k} = 0$ for $\ell > k$. In particular, JU and UJ are of the form as at the beginning of the proof. Since these products are equal, we obtain

$$U_{k-1,\ell-1}J_{\ell-1,\ell} = J_{k-1,k}U_{k\ell} = \begin{bmatrix} U_{k\ell} \\ 0 \end{bmatrix} \quad \text{for } \ell \ge k > 1.$$

This implies

$$U_{k-1,\ell-1} = \begin{bmatrix} U_{k\ell} & * \\ 0 & * \end{bmatrix}$$

because right multiplication with $J_{\ell-1,\ell}$ extracts the first n_ℓ columns of a matrix. Therefore U is of the form as in (4.9). ■

(4.11) Corollary. The set $\mathcal{U}$ of all matrices as in (4.9) forms a group.

Proof. By (4.10) we have $\mathcal{U} = \{\, U \in \mathrm{GL}(n, \mathcal{O}) \mid UJ = JU \,\}$. ■

We will now describe the A-bases of an arbitrary free A-module over $\mathcal{O}$.

(4.12) Proposition. Let $\mathfrak{A}$ be a free A-module over $\mathcal{O}$ with A-basis X. Any other $\mathcal{O}$-basis of $\mathfrak{A}$ is an A-basis if and only if it is of the form XU with $U \in \mathcal{U}$.

Proof. Since right multiplication with $J_{k,k+1}$ extracts the first n_k columns of a matrix, we have

$$X_kJ_{k,k+1} = [\, AX_{k+1} \; * \,]\, J_{k,k+1} = AX_{k+1} \quad \text{for } k < \nu.$$

Therefore

$$XJ = [\, 0 \; X_1J_{12} \; \ldots \; X_{\nu-1}J_{\nu-1,\nu} \,] = [\, 0 \; AX_2 \; \ldots \; AX_\nu \,] = AX.$$

Suppose Y is another A-basis of $\mathfrak{A}$. Then $X^{-1}Y$ belongs to $\mathrm{GL}(n,\mathcal{O})$ because $X^{-1}\mathfrak{A} = \mathcal{O}^n$. Moreover, by the calculation above,

$$(X^{-1}Y)J(X^{-1}Y)^{-1} = X^{-1}(YJY^{-1})X = X^{-1}AX = J,$$

that is, $X^{-1}Y$ commutes with J. This implies $X^{-1}Y \in \mathcal{U}$, so

$$Y = XU \quad \text{for some } U \in \mathcal{U}.$$

Conversely, assume $Y = XU$ with $U \in \mathcal{U}$. Then Y is an $\mathcal{O}$-basis of $\mathfrak{A}$. Write

$$Y = [\, Y_1 \ \ldots \ Y_\nu \,]$$

with blocks of the size $n \times n_k$. Then

$$Y_k = X_1 U_{1k} + \cdots + X_k U_{kk},$$

and the columns of Y_k belong to the kernel of A^k because the columns of X_ℓ do for $\ell \leq k$. Moreover, for $\ell \leq k < \nu$, we have

$$X_\ell U_{\ell k} = [\, AX_{\ell+1} \ * \,] \begin{bmatrix} U_{\ell+1,k+1} & * \\ 0 & * \end{bmatrix} = \begin{bmatrix} AX_{\ell+1}U_{\ell+1,k+1} & * \\ 0 & * \end{bmatrix},$$

hence $Y_k = [\, AY_{k+1} \ * \,]$ for $k < \nu$. Therefore Y is an A-basis of $\mathfrak{A}$. ■

As explained before, our goal is to decide whether there are suitable A- and B-bases X and Y belonging to modules $\mathfrak{A}$ and $\mathfrak{B}$ such that

$$YX^{-1} \in \Lambda^\times.$$

If X and Y are fixed, all other A- and B-bases are of the form XU and YV with U, $V \in \mathcal{U}$ by (4.12). Hence we need to check whether

$$Y(VU^{-1})X^{-1} \in \Lambda^\times$$

for suitable choices of U and V. Since $\mathcal{U}$ is a group, this comes down to the question whether

$$YUX^{-1} \in \Lambda^\times \quad \text{for } U \in \mathcal{U}.$$

Let us explain how this can be decided in a finite number of steps. Recall that in the previous section we fixed a module $\mathfrak{S}$ with the property that

$$\Lambda = (\mathfrak{S} : \mathfrak{S}).$$

By multiplying X and Y with suitable scalars, we may assume that $\mathfrak{A}$ and $\mathfrak{B}$ are contained in $\mathfrak{S}$.

Let $\lambda \in \mathcal{O}$ be nonzero such that $\lambda\mathfrak{S} \subset \mathfrak{A}$. As we will see, it suffices to solve our problem modulo λ. If $\mathfrak{A}$ and $\mathfrak{B}$ are similar, then, in particular, $\Gamma\mathfrak{A} = \mathfrak{B}$ for some $\Gamma \in \Lambda^\times$, so

$$\lambda\mathfrak{S} = \lambda(\Gamma\mathfrak{S}) = \Gamma(\lambda\mathfrak{S}) \subset \Gamma\mathfrak{A} = \mathfrak{B}.$$

Hence $\lambda\mathfrak{S}$ is also contained $\mathfrak{B}$. Let us assume that this is the case, so we have the inclusions

$$\lambda\mathfrak{S} \subset \mathfrak{A},\ \mathfrak{B} \subset \mathfrak{S}.$$

Pay attention to the fact that $\mathfrak{S}$ does not have to be an $\mathcal{O}$-module since $\mathcal{O}$ can be any order of $\mathcal{K}$.

Our strategy will be based on the observation that any matrix $\mathit{\Gamma} \in \mathrm{M}(n, \mathcal{K})$ satisfies the equivalences

$$\mathit{\Gamma} \in \Lambda^{\times} \quad \Leftrightarrow \quad \mathit{\Gamma}\mathfrak{S} = \mathfrak{S} \quad \Leftrightarrow \quad \mathit{\Gamma}(\lambda\mathfrak{S}) = \lambda\mathfrak{S}.$$

As described above, for $\mathfrak{A}$ and $\mathfrak{B}$ to be similar, $\mathit{\Gamma}$ needs to be of the form

$$\mathit{\Gamma} = YUX^{-1} \quad \text{with } U \in \mathcal{U}.$$

Let

$$\mathfrak{C} = X^{-1}(\lambda\mathfrak{S}) \quad \text{and} \quad \mathfrak{D} = Y^{-1}(\lambda\mathfrak{S}).$$

If $\mathit{\Gamma} = YUX^{-1}$, then

$$\mathit{\Gamma}(\lambda\mathfrak{S}) = \lambda\mathfrak{S} \quad \Leftrightarrow \quad U\mathfrak{C} = \mathfrak{D}.$$

For these modules we have the inclusions

$$\lambda\mathcal{O}^n \subset \mathfrak{C},\ \mathfrak{D} \subset \mathcal{O}^n$$

because

$$\mathfrak{C} = X^{-1}(\lambda\mathfrak{S}) \subset X^{-1}\mathfrak{A} = X^{-1}X\mathcal{O}^n = \mathcal{O}^n$$

and

$$\mathfrak{C} = X^{-1}(\lambda\mathfrak{S}) \supset X^{-1}(\lambda\mathfrak{A}) = \lambda\mathcal{O}^n.$$

Consequently, we can deal with submodules of $\mathcal{O}^n$ instead of $\mathfrak{S}$.

Let $\mathcal{M}$ be the set of all matrices $M \in \mathrm{M}(n, \mathcal{O})$ of the form as in (4.9), that is,

$$M = \begin{bmatrix} M_{11} & \cdots & M_{1\nu} \\ & \ddots & \vdots \\ 0 & & M_{\nu\nu} \end{bmatrix} \quad \text{and} \quad M_{k-1,\,\ell-1} = \begin{bmatrix} M_{k\ell} & * \\ 0 & * \end{bmatrix}$$

where $M_{k\ell}$ is a block of size $n_k \times n_\ell$. Then $\mathcal{M}$ is an algebra with unit group $\mathcal{U}$. Let $\overline{\mathcal{U}}$ be the image of $\mathcal{U}$ under the homomorphism

$$\mathcal{M} \to \overline{\mathcal{M}} \quad \text{where} \quad \overline{\mathcal{M}} = \mathcal{M}/\lambda\mathcal{M}.$$

Clearly, this is a finite group acting on $\mathcal{O}^n/\lambda\mathcal{O}^n$ via $\bar{U}\bar{\xi} = \overline{U\xi}$. Moreover, let

$$\overline{\mathfrak{C}} = \mathfrak{C}/\lambda\mathcal{O}^n \quad \text{and} \quad \overline{\mathfrak{D}} = \mathfrak{D}/\lambda\mathcal{O}^n.$$

Again, $\mathfrak{C}$ and $\mathfrak{D}$ do not have to be $\mathcal{O}$-modules. Nevertheless, all modules can be considered over $\mathbb{Z}$, so the reduction above poses no problem. The next theorem summarizes the significant aspects of our considerations.

(4.13) Theorem. With notations as above, the following statements are equivalent.

(1) $\mathfrak{A}$ and $\mathfrak{B}$ are similar.

(2) There is a $\bar{U} \in \overline{\mathcal{U}}$ such that $\overline{U\mathfrak{C}} = \overline{\mathfrak{D}}$.

Proof. As explained above, if $\mathfrak{A}$ and $\mathfrak{B}$ are similar, there is a matrix $U \in \mathcal{U}$ such that $U\mathfrak{C} = \mathfrak{D}$, implying $\overline{U\mathfrak{C}} = \overline{\mathfrak{D}}$.
Conversely, suppose there is a $\bar{U} \in \overline{\mathcal{U}}$ such that $\overline{U\mathfrak{C}} = \overline{\mathfrak{D}}$. Let $U \in \mathcal{U}$ be a preimage of $\bar{U}$. For every $d \in \mathfrak{D}$ there is a $c \in \mathfrak{C}$ such that $Uc \equiv d \bmod \lambda\mathcal{O}^n$. Since $\mathfrak{C}$ and $\mathfrak{D}$ both contain $\lambda\mathcal{O}^n$, we obtain

$$U\mathfrak{C} = U(\mathfrak{C} + \lambda\mathcal{O}^n) = U\mathfrak{C} + U\lambda\mathcal{O}^n = U\mathfrak{C} + \lambda\mathcal{O}^n = \mathfrak{D}.$$

Hence $\mathfrak{A}$ and $\mathfrak{B}$ are similar for reasons given above. ∎

By the theorem we only need to search the group $\overline{\mathcal{U}}$ for a suitable element. In practice, we can search the algebra $\overline{\mathcal{M}}$ which has a considerably smaller dimension than $(\mathcal{O}/\lambda\mathcal{O})^n$.

(4.14) Proposition. The dimension of $\mathcal{M}$ over $\mathcal{O}$ is $n_1^2 + \cdots + n_\nu^2$. The same is true for $\overline{\mathcal{M}}$ over $\mathcal{O}/\lambda\mathcal{O}$.

Proof. The blocks $M_{k\nu}$ of elements in $\mathcal{M}$ contribute to the dimension of $\mathcal{M}$ by adding $n_k n_\nu$. Furthermore, the blocks

$$M_{k-1,\,\ell-1} = \begin{bmatrix} M_{k\ell} & * \\ 0 & * \end{bmatrix} \qquad (1 < k \leq \ell < \nu)$$

contribute by adding $n_{k-1}(n_{\ell-1} - n_\ell)$. All in all, $\mathcal{M}$ has dimension

$$(n_1 + \cdots + n_\nu)n_\nu + (n_1 + \cdots + n_{\nu-1})(n_{\nu-1} - n_\nu) + \cdots + n_1(n_1 - n_2)$$

which is equal to $n_1^2 + \cdots + n_\nu^2$. The proof also works modulo λ. ∎

In addition, we can reduce the number of steps in our search further because we only need to pay attention to the submodule of all matrices $\bar{M} \in \overline{\mathcal{M}}$ satisfying

$$\overline{M\mathfrak{C}} = \overline{\mathfrak{D}}.$$

Finally, two things remain to be explained. First, how to decide whether a residue class $\bar{U} \in \overline{\mathcal{M}}$ has a preimage in $\mathcal{U}$, and second, how to compute a preimage. In principle, these problems can be solved with the same strategy as described in section 3.2. Let

$$\bar{U} = \begin{bmatrix} \bar{U}_{11} & \cdots & \bar{U}_{1\nu} \\ & \ddots & \vdots \\ 0 & & \bar{U}_{\nu\nu} \end{bmatrix} \quad \text{with} \quad \bar{U}_{k\ell} = \begin{bmatrix} \bar{U}_{k+1,\,\ell+1} & * \\ 0 & \bar{U}_{k\ell}^* \end{bmatrix} \quad \text{for } 1 \leq k, \ell < \nu$$

and put $\bar{U}_{\nu\nu} = \bar{U}_{\nu\nu}^*$. Clearly, $\bar{U}$ is a unit precisely if each $\bar{U}_{kk}^*$ is invertible over $\mathcal{O}/\lambda\mathcal{O}$, and $\bar{U}$ has a preimage in $\mathcal{U}$ if and only if each $\bar{U}_{kk}^*$ can be lifted to an invertible matrix over $\mathcal{O}$. If $\bar{u}_k \in (\mathcal{O}/\lambda\mathcal{O})^\times$ is the determinant of $\bar{U}^*_{kk}$ (where the determinant of an empty block is assumed to be 1), we can write

$$\bar{U}^*_{kk} = \begin{bmatrix} \bar{u}_k & 0 \\ 0 & I \end{bmatrix} \bar{S}_k.$$

Here, I is an identity matrix of appropriate size and $\bar{S}_k$ has determinant 1. Then $\bar{S}_k$ can be lifted to a matrix with determinant 1 using algorithm (3.16), and $\bar{u}_k$ has a preimage if and only if it belongs to the image of

$$\mathcal{O}^\times \to (\mathcal{O}/\lambda\mathcal{O})^\times.$$

Both the domain and the codomain of this map can be computed using algorithms described by Klüners and Pauli (2005), so the image—as well as preimages of elements—can be determined with standard methods for finitely presented abelian groups. Thus we can lift all the crucial blocks of $\bar{U}$, if possible. For blocks above the diagonal, any preimage will do. Of course we need to make sure that identical blocks of $\bar{U}$ are lifted in the same way to ensure that the repetitive structure of elements in $\mathcal{U}$ is preserved.

—

Having explained how to decide similarity of free modules in the number field case, we will now deal with the general situation of a direct sum

$$\boldsymbol{\mathcal{K}} = \mathcal{K}_1 \oplus \cdots \oplus \mathcal{K}_s.$$

Let $\mathcal{O} = \mathcal{O}_1 \oplus \cdots \oplus \mathcal{O}_s$ be an order of $\boldsymbol{\mathcal{K}}$. Then $\mathcal{O}_\iota$ is an order of $\mathcal{K}_\iota$ for each ι. First of all, an $\mathcal{O}$-module $\mathfrak{A}$, which is always of the form

$$\mathfrak{A} = \mathfrak{A}_1 \oplus \cdots \oplus \mathfrak{A}_s,$$

will be called **free** if $\mathfrak{A}_\iota$ is a free module over $\mathcal{O}_\iota$ for each ι.

Let Λ be an order of $\mathrm{M}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$ and suppose $A = A_1 \oplus \cdots \oplus A_s$ is a nilpotent element of Λ. This is precisely the case if each A_ι is nilpotent. A full $\mathcal{O}$-module $\mathfrak{A}$ in $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$ will be called a **free $\boldsymbol{A}$-module** over $\mathcal{O}$ if $\mathfrak{A}_\iota$ is a free A_ι-module over $\mathcal{O}_\iota$ for each ι. Moreover,

$$X = X_1 \oplus \cdots \oplus X_s$$

will be called an **$\boldsymbol{A}$-basis** of $\mathfrak{A}$ over $\mathcal{O}$ if X_ι is an A_ι-basis of $\mathfrak{A}_\iota$ over $\mathcal{O}_\iota$. In this case we can write

$$\mathfrak{A} = X\mathcal{O}^{\boldsymbol{n}} \quad \text{where} \quad \mathcal{O}^{\boldsymbol{n}} = \mathcal{O}_1^{n_1} \oplus \cdots \oplus \mathcal{O}_s^{n_s}.$$

Finally, suppose that $\mathfrak{A}$ is a free A-module and $\mathfrak{B}$ a free B-module over $\mathcal{O}$ and that A_ι and B_ι are of the same structure for each ι. In this case $\mathfrak{A}$ and $\mathfrak{B}$ are called **similar** if there is an A-basis X of $\mathfrak{A}$, a B-basis Y of $\mathfrak{B}$ and a matrix $\Gamma \in \Lambda^\times$ such that $\Gamma X = Y$. Obviously, $\mathfrak{A}_\iota$ is similar to $\mathfrak{B}_\iota$ for each ι if $\mathfrak{A}$ is similar to $\mathfrak{B}$ because $\Gamma X = Y$ implies $\Gamma_\iota X_\iota = Y_\iota$ for each ι. However, this is not a sufficient condition if Λ is not a direct sum $\Lambda_1 \oplus \cdots \oplus \Lambda_s$.

As before, one easily sees that free A-modules are A-modules in the original sense and that is suffices to consider free A- and B-modules to decide whether two nilpotent matrices are similar. In fact, (4.8) can be translated to the current situation almost word by word. Making use of our option of choice, we will therefore require $\mathcal{O}$ to be a direct sum of orders if $\boldsymbol{\mathcal{K}}$ consists of several number fields. In the next section we will also specify how to choose the individual components of $\mathcal{O}$.

Continuing with our generalizations, (4.12) can be left almost unchanged as well: If $X = X_1 \oplus \cdots \oplus X_s$ is an A-basis of $\mathfrak{A}$ over $\mathcal{O}$, then any other $\mathcal{O}$-basis of $\mathfrak{A}$ is an A-basis if and only if it is of the form XU where $U = U_1 \oplus \cdots \oplus U_s$ is a direct sum of matrices as in (4.9). Let

$$\mathcal{U} = \mathcal{U}_1 \oplus \cdots \oplus \mathcal{U}_s$$

be the group of all these matrices U. The rest of our previous discussion can now be read as an instruction to solve the problem of similarity in general. We are equipped with a fixed module $\mathfrak{S}$ with multiplier algebra Λ and we may assume that

$$\lambda\mathfrak{S} \subset \mathfrak{A}, \mathfrak{B} \subset \mathfrak{S}$$

where λ is a suitable nonzerodivisor in $\mathcal{O}$. The matrix $\mathit{\Gamma}$ we are looking for has to be of the form $\mathit{\Gamma} = YUX^{-1}$ with $U \in \mathcal{U}$ and

$$\mathit{\Gamma} \in \Lambda^{\times} \quad \Leftrightarrow \quad \mathit{\Gamma}\mathfrak{S} = \mathfrak{S} \quad \Leftrightarrow \quad \mathit{\Gamma}(\lambda\mathfrak{S}) = \lambda\mathfrak{S} \quad \Leftrightarrow \quad U\mathfrak{C} = \mathfrak{D}$$

where $\mathfrak{C} = X^{-1}(\lambda\mathfrak{S})$ and $\mathfrak{D} = Y^{-1}(\lambda\mathfrak{S})$, which are subject to the inclusions

$$\lambda\mathcal{O}^{\boldsymbol{n}} \subset \mathfrak{C}, \mathfrak{D} \subset \mathcal{O}^{\boldsymbol{n}}.$$

Again, the search for U can be accomplished modulo λ, and if a suitable residue class $\bar{U} = \bar{U}_1 \oplus \cdots \oplus \bar{U}_s$ has been found, a preimage $U \in \mathcal{U}$ can be determined by lifting the individual components of $\bar{U}$ as described before.

4.3 Enumerating Free Modules of Minimal Index

As in the previous sections, let $\mathfrak{S}$ be a full module in $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$ with multiplier algebra Λ and let $A = A_1 \oplus \cdots \oplus A_s$ be a nilpotent matrix in Λ. Moreover, let

$$\mathcal{O} = \mathcal{O}_1 \oplus \cdots \oplus \mathcal{O}_s$$

be an order of $\boldsymbol{\mathcal{K}}$. Given that $\mathcal{O}$ satisfies some extra conditions specified below, we will see how to enumerate all free A-modules $\mathfrak{A}$ over $\mathcal{O}$ with minimal index in $\mathfrak{S}$. Since all modules can be considered over $\mathbb{Z}$, the index $[\mathfrak{S} : \mathfrak{A}]$ is well-defined although $\mathfrak{S}$ might not be an $\mathcal{O}$-module.

For each ι, let $\mathfrak{S}_\iota$ be the image of $\mathfrak{S}$ under the projection $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}} \to \mathcal{K}_\iota^{n_\iota}$. Put

$$\mathfrak{S}' = \mathfrak{S}_1 \oplus \cdots \oplus \mathfrak{S}_s \quad \text{and} \quad \mathfrak{S}'' = (\mathfrak{S}_1 \cap \mathfrak{S}) \oplus \cdots \oplus (\mathfrak{S}_s \cap \mathfrak{S}),$$

where we make use of the natural embedding $\mathcal{K}_\iota^{n_\iota} \to \boldsymbol{\mathcal{K}^n}$. Then we have the inclusions

$$\mathfrak{S}'' \subset \mathfrak{S} \subset \mathfrak{S}'.$$

Let $\varGamma = \varGamma_1 \oplus \cdots \oplus \varGamma_s$ be an element of Λ and let 1_ι denote the unit element of $\mathcal{K}_\iota$ (which can be identified as a subset of $\boldsymbol{\mathcal{K}}$). Then

$$\varGamma_\iota \mathfrak{S}_\iota = \varGamma_\iota(1_\iota \mathfrak{S}) = (\varGamma_\iota 1_\iota)\mathfrak{S} = (\varGamma 1_\iota)\mathfrak{S} = 1_\iota(\varGamma \mathfrak{S}) \subset 1_\iota \mathfrak{S} = \mathfrak{S}_\iota,$$

hence $\varGamma \mathfrak{S}' \subset \mathfrak{S}'$, that is, $\varGamma$ belongs to the multiplier algebra of $\mathfrak{S}'$. The same is true for the multiplier algebra of $\mathfrak{S}''$ because

$$\varGamma \mathfrak{S} \subset \mathfrak{S} \quad \text{and} \quad \varGamma_\iota \mathfrak{S}_\iota \subset \mathfrak{S}_\iota \quad \text{implies} \quad \varGamma_\iota(\mathfrak{S}_\iota \cap \mathfrak{S}) \subset \mathfrak{S}_\iota \cap \mathfrak{S}.$$

In particular, A_ι belongs to the multiplier algebra of $\mathfrak{S}_\iota \cap \mathfrak{S}$ for each ι. Let $\mathcal{O}$ be the multiplier ring of $\mathfrak{S}''$, that is, $\mathcal{O}_\iota$ is the multiplier ring of $\mathfrak{S}_\iota \cap \mathfrak{S}$. Moreover, let $\mathfrak{A} = \mathfrak{A}_1 \oplus \cdots \oplus \mathfrak{A}_s$ be a free A-module over $\mathcal{O}$, that is, $\mathfrak{A}_\iota$ is a free A_ι-module over $\mathcal{O}_\iota$ for each ι. As usual, we may assume that $\mathfrak{A}$ is contained in $\mathfrak{S}$. Since

$$\mathfrak{A}_1 \oplus \cdots \oplus \mathfrak{A}_s = \mathfrak{A} \subset \mathfrak{S} \subset \mathfrak{S}' = \mathfrak{S}_1 \oplus \cdots \oplus \mathfrak{S}_s,$$

we see that $\mathfrak{A}_\iota \subset \mathfrak{S}_\iota \cap \mathfrak{S}$ for each ι, so

$$\mathfrak{A} \subset \mathfrak{S}'' \subset \mathfrak{S}.$$

Clearly, the index $[\mathfrak{S} : \mathfrak{A}] = [\mathfrak{S} : \mathfrak{S}''][\mathfrak{S}'' : \mathfrak{A}]$ is minimal precisely if

$$[\mathfrak{S}'' : \mathfrak{A}] = \prod_{\iota=1}^{s} [\mathfrak{S}_\iota \cap \mathfrak{S} : \mathfrak{A}_\iota]$$

is minimal, and this is the case if and only if each $[\mathfrak{S}_\iota \cap \mathfrak{S} : \mathfrak{A}_\iota]$ is minimal. So henceforth we may assume the following:

- $\mathfrak{S}$ is a full module in $\mathcal{K}^n$ where $\mathcal{K}$ is a number field,
- A is a nilpotent element of $\Lambda = (\mathfrak{S} : \mathfrak{S})$, and
- $\mathcal{O}$ is the multiplier ring of $\mathfrak{S}$.

Under these assumptions we will show how to enumerate all free A-modules over $\mathcal{O}$ with minimal index in $\mathfrak{S}$. From now on we will skip the addition "over $\mathcal{O}$" and will simply speak of free A-modules.

Remember that a full module $\mathfrak{A}$ is a free A-module if it has an $\mathcal{O}$-basis

$$X = [\, X_1 \ \dots \ X_\nu \,]$$

where the columns of X_k belong to the kernel of A^k and

$$X_k = [\, AX_{k+1} \ X_k^* \,] \quad \text{for } k < \nu.$$

As a convention, we assume that X_k is an empty block for $k > \nu$ and we put $X_\nu^* = X_\nu$. The blocks X_k^* will play an important role in this section.

Before we can start, we need to define some modules and vector spaces. Let

$$V_k = \{\, x \in \mathcal{K}^n \mid A^k x = 0 \,\} \quad \text{and} \quad \mathfrak{S}_k = V_k \cap \mathfrak{S} \quad \text{for } k \geq 0.$$

This gives us an ascending chain of $\mathcal{O}$-modules

$$0 = \mathfrak{S}_0 \subset \ldots \subset \mathfrak{S}_\nu = \mathfrak{S}_{\nu+1} = \ldots = \mathfrak{S}.$$

(Do not confuse $\mathfrak{S}_k$ with the modules $\mathfrak{S}_\iota$ discussed before.) Furthermore, let

$$\mathfrak{T}_k = (V_{k-1} + AV_{k+1}) \cap \mathfrak{S} \quad \text{for } 1 \leq k \leq \nu.$$

Then $\mathfrak{T}_k$ is a submodule of $\mathfrak{S}_k$. Therefore we can define the quotient module

$$\mathfrak{W}_k = \mathfrak{S}_k / \mathfrak{T}_k.$$

Finally, let

$$W_k = V_k / (V_{k-1} + AV_{k+1}) \quad \text{for } 1 \leq k \leq \nu.$$

If X is an A-basis, the columns of X_k^* represent a $\mathcal{K}$-basis of W_k (to see this, recall how to compute the Jordan normal form of a nilpotent matrix). Throughout this section we will assume that the columns of all A-bases belong to $\mathfrak{S}$. This is equivalent to $\mathfrak{A} = X\mathcal{O}^n$ being a submodule of $\mathfrak{S}$ and implies that X_k^* generates a submodule of $\mathfrak{S}_k$.

(4.15) Proposition. There is a canonical injection $\mathfrak{W}_k \to W_k$. In particular, $\mathfrak{W}_k$ is torsionfree and can be regarded as a full $\mathcal{O}$-module in W_k.

Proof. The kernel of the composition $\mathfrak{S}_k \to V_k \to W_k$ is given by

$$\begin{aligned}(V_{k-1} + AV_{k+1}) \cap \mathfrak{S}_k &= (V_{k-1} + AV_{k+1}) \cap (V_k \cap \mathfrak{S}) \\ &= (V_{k-1} + AV_{k+1}) \cap \mathfrak{S} \\ &= \mathfrak{T}_k.\end{aligned}$$

As a result, $\mathfrak{W}_k$ can be regarded as a subset of the vector space W_k. Therefore it is torsionfree. Since $\mathfrak{S}_k$ is full in V_k, the same is true for $\mathfrak{W}_k$ in W_k. ■

(4.16) Proposition. The columns of X_k^* represent a basis of a free $\mathcal{O}$-module of finite index in $\mathfrak{W}_k$.

Proof. As mentioned before, X_k^* represent a $\mathcal{K}$-basis of W_k, hence it also represents a basis of a free submodule in $\mathfrak{W}_k$. Moreover, X_k^* is an empty block if and only if $W_k = 0$. Since the nullspace is generated by the empty set, the statement is true in this case.

So let us suppose X_k^* is a nontrivial block. By the way X is construed, the columns of

$$[\, X_1 \ \ldots \ X_k \,] = [\, X_1 \ \ldots \ X_{k-1} \ AX_{k+1} \ X_k^* \,]$$

generate an $\mathcal{O}$-module $\mathfrak{A}_k \subset \mathfrak{S}_k$ of finite index. Hence, the columns of

$$[\, AX_1 \ \ldots \ AX_{k+1} \,] = [\, 0 \ AX_2 \ \ldots \ AX_{k+1} \,]$$

generate

$$A\mathfrak{A}_{k+1} \subset A\mathfrak{S}_{k+1} \subset \mathfrak{T}_k.$$

Taken together, the columns of

$$[\, X_1 \ \ldots \ X_{k-1} \ AX_{k+1} \,] = [\, AX_2 \ X_2^* \ \ldots \ AX_k \ X_{k-1}^* \ AX_{k+1} \,]$$

generate an $\mathcal{O}$-module

$$\mathfrak{Z}_k \subset (\mathfrak{A}_{k-1} + A\mathfrak{A}_{k+1}) \subset \mathfrak{T}_k$$

of finite index in $\mathfrak{T}_k$. Furthermore, the columns of X_k^* are linearly independent of vectors in $\mathfrak{Z}_k$ and they generate a free submodule of finite rank in $\mathfrak{A}_k/\mathfrak{Z}_k$, which, in turn, has finite index in $\mathfrak{S}_k/\mathfrak{Z}_k$. Since $\mathfrak{Z}_k$ has finite index in $\mathfrak{T}_k$, the columns of X_k^* are also linearly independent of elements in $\mathfrak{T}_k$. In conclusion, they generate a free submodule of finite index in $\mathfrak{W}_k$. ■

The next theorem tells us how to construct free A-modules of minimal index.

(4.17) Theorem. Let $\mathfrak{A} \subset \mathfrak{S}$ be a free A-module with A-basis X and let $\mathfrak{X}_k \subset \mathfrak{W}_k$ be the free $\mathcal{O}$-module generated by X_k^*. The following statements are equivalent.

(1) $\mathfrak{A}$ is a free A-module of minimal index in $\mathfrak{S}$.

(2) $\mathfrak{X}_k$ is a free module of minimal index in $\mathfrak{W}_k$ for each k.

Proof. For every k, let Y_k^* represent a basis of a free $\mathcal{O}$-module $\mathfrak{Y}_k \subset \mathfrak{W}_k$ with minimal (and thus finite) index. Then the columns of Y_k^* need to belong to $\mathfrak{S}$. Let $Y = [\, Y_1 \ \ldots \ Y_\nu \,]$ be the A-basis obtained from $Y_k^*, \ldots, Y_k^*$, that is,

$$Y_\nu = Y_\nu^* \quad \text{and} \quad Y_k = [\, AY_{k+1} \ Y_k^* \,] \quad \text{for } k < \nu.$$

Since A is an element of Λ, which is the multiplier algebra of $\mathfrak{S}$, the columns of AY_k also belong to $\mathfrak{S}$. Consequently, $\mathfrak{A}' = Y\mathcal{O}^n$ is another free A-module over $\mathcal{O}$ contained in $\mathfrak{S}$.

Recall that Y_k^* represents a $\mathcal{K}$-basis of $W_k = V_k/(V_{k-1} + AV_{k+1})$. Hence we can write

$$X_k^* \equiv Y_k^* U_k^* \mod (V_{k-1} + AV_{k+1})$$

where U_k^* is a square matrix over $\mathcal{K}$. The reduction modulo $(V_{k-1} + AV_{k+1})$ works columnwise. Identifying W_k with a suitable power of $\mathcal{K}$, we may apply (1.31) to obtain

$$[\mathfrak{W}_k : \mathfrak{X}_k] = |\mathrm{N}(U_k^*)| \cdot [\mathfrak{W}_k : \mathfrak{Y}_k]$$

Here, the norm of an empty matrix is considered to be 1. Since $[\mathfrak{W}_k : \mathfrak{Y}_k]$ is minimal, we have $|\mathrm{N}(U_k^*)| \geq 1$. Let

$$U_k = \begin{bmatrix} U_\nu^* & & \\ & \ddots & \\ & & U_k^* \end{bmatrix} \qquad \text{and} \qquad U = \begin{bmatrix} U_1 & & \\ & \ddots & \\ & & U_\nu \end{bmatrix}.$$

We want to prove that $[\mathfrak{S} : \mathfrak{A}] = |\mathrm{N}(U)| \cdot [\mathfrak{S} : \mathfrak{A}']$. The congruence $X_k^* \equiv Y_k^* U_k^*$ can be translated into the equality

$$X_k^* = Y_k^* U_k^* + Z_k$$

where Z_k is a matrix with columns belonging to $V_{k-1} + AV_{k+1}$. Consider the submatrix

$$\begin{aligned}[\, X_1 \ \ldots \ X_{k-1} \ X_k \,] &= [\, X_1 \ \ldots \ X_{k-1} \ AX_{k+1} \ X_k^* \,] \\ &= [\, X_1 \ \ldots \ X_{k-1} \ AX_{k+1} \ Y_k^* U_k^* + Z_k \,].\end{aligned}$$

Since $[\, X_1 \ \ldots \ X_{k-1} \ AX_{k+1} \,]$ is a basis of the vector space $V_{k-1} + AV_{k+1}$, we can eliminate Z_k using elementary column operations over $\mathcal{K}$, that is,

$$[\, X_1 \ \ldots \ X_{k-1} \ X_k \,] \sim [\, X_1 \ \ldots \ X_{k-1} \ AX_{k+1} \ Y_k^* U_k^* \,].$$

Furthermore,

$$AX_{k+1} = [\, A^2 X_{k+2} \ AX_{k+1}^* \,] = [\, A^2 X_{k+2} \ A(Y_{k+1}^* U_{k+1}^* + Z_{k+1}) \,],$$

and the columns of AZ_{k+1} are linearly dependent of

$$A[\, X_1 \ \ldots \ X_k \ AX_{k+2} \,] = [\, 0 \ AX_2 \ \ldots \ AX_k \ A^2 X_{k+2} \,].$$

The nonzero blocks of this matrix appear in $[\, X_1 \ \ldots \ X_{k-1} \ A^2 X_{k+2} \,]$ since $X_{\ell-1} = [\, AX_\ell \ X_{\ell-1}^* \,]$. Therefore

$$\begin{aligned}&[\, X_1 \ \ldots \ X_{k-1} \ AX_{k+1} \ Y_k^* U_k^* \,] \\ &= [\, X_1 \ \ldots \ X_{k-1} \ A^2 X_{k+2} \ A(Y_{k+1}^* U_{k+1}^* + Z_{k+1}) \ Y_k^* U_k^* \,] \\ &\sim [\, X_1 \ \ldots \ X_{k-1} \ A^2 X_{k+2} \ AY_{k+1}^* U_{k+1}^* \ Y_k^* U_k^* \,].\end{aligned}$$

Continuing in this fashion, we see that

$$X = [\, X_1 \ \ldots \ X_\nu \,] \sim [\, Y_1 U_1 \ \ldots \ Y_\nu U_\nu \,] = YU.$$

More precisely, we have

$$X = YUS \quad \text{for some } S \in \mathrm{SL}(n, \mathcal{K}).$$

Applying (1.31) and (1.25), we obtain

$$[\mathfrak{S} : \mathfrak{A}] = |\mathrm{N}(US)| \cdot [\mathfrak{S} : \mathfrak{A}'] = |\mathrm{N}(U)| \cdot [\mathfrak{S} : \mathfrak{A}'].$$

Since $|\mathrm{N}(U_k^*)| \geq 1$ for all k, we see that

$$|\mathrm{N}(U)| = \prod_{k=1}^{\nu} |\mathrm{N}(U_k)| = \prod_{k=1}^{\nu} |\mathrm{N}(U_k^*)|^k \geq 1.$$

Therefore

$$[\mathfrak{S} : \mathfrak{A}] \geq [\mathfrak{S} : \mathfrak{A}'].$$

This inequality holds for any free A-module $\mathfrak{A}$, hence $\mathfrak{A}'$ is a free A-module of minimal index in $\mathfrak{S}$. We conclude

$$\begin{aligned}[\mathfrak{S} : \mathfrak{A}] \text{ is minimal } &\Leftrightarrow \ |\mathrm{N}(U)| = 1 \\ &\Leftrightarrow \ |\mathrm{N}(U_k^*)| = 1 \text{ for all } k \\ &\Leftrightarrow \ [\mathfrak{W}_k : \mathfrak{X}_k] \text{ is minimal for all } k.\end{aligned}$$

■

The just established theorem tells us that each free A-module of minimal index can be constructed from blocks X_k^* representing bases of free submodules of minimal index in $\mathfrak{W}_k$. We simply need to combine the blocks $X_1^*, \ldots, X_\nu^*$ to an A-basis in the usual way. Thus we must ponder how to determine all these free submodules.

Since $\mathfrak{S}$ is a free $\mathbb{Z}$-module, we certainly can compute $\mathbb{Z}$-bases of

$$\mathfrak{S}_k = V_k \cap \mathfrak{S} \qquad \text{and} \qquad \mathfrak{T}_k = (V_{k-1} + AV_{k+1}) \cap \mathfrak{S}$$

as well as a $\mathbb{Z}$-basis $\varXi$ of the torsionfree quotient module $\mathfrak{W}_k = \mathfrak{S}_k / \mathfrak{T}_k$. Suppose m is the number of columns of $\varXi$ and d a nonnegative integer. Let us explain how to determine all free submodules $\mathfrak{X}_k \subset \mathfrak{W}_k$ of index d. First, the $\mathbb{Z}$-modules in $\mathfrak{W}_k$ of index d are given by

$$\mathfrak{H} = (\varXi H)\mathbb{Z}^m$$

where H runs through all $m \times m$ integer matrices in Hermite normal form with determinant d, that is, all matrices of the form

$$H = \begin{bmatrix} h_{11} & & 0 \\ \vdots & \ddots & \\ h_{m1} & \cdots & h_{mm} \end{bmatrix}$$

with

$$h_{ii} > h_{ij} \geq 0 \qquad \text{and} \qquad h_{11} \cdots h_{mm} = d.$$

Clearly, the number of possibilities for H is finite. Yet not all $\mathbb{Z}$-modules must be $\mathcal{O}$-modules. We can discard all modules that are not. For the remaining ones we need to examine whether they are free over $\mathcal{O}$. A small problem arises at this point. In general, $\mathfrak{H}$ is not a full module in $\mathcal{K}^n$ (this is only the case if $\nu = 1$). However, $\mathfrak{H}$ is free if and only if $\varGamma\mathfrak{H}$ is for any $\varGamma \in \mathrm{GL}(n, \mathcal{K})$. Thus we may choose $\varGamma$ such that

$$\varGamma(\varXi H) = \begin{bmatrix} \varXi' \\ 0 \end{bmatrix}$$

where $\varXi'$ has full rank over $\mathcal{K}$. Then $\mathfrak{H}' = \varXi'\mathbb{Z}^m$ is a full module in $\mathcal{K}^\ell$ where ℓ is the number of rows of $\varXi'$, and $\mathfrak{H}$ is free precisely if $\mathfrak{H}'$ is. Therefore we can check whether $\mathfrak{H}' \sim \mathcal{O}^\ell$ as explained in the first three chapters (pay special attention to (3.11) and the subsequent remark). In doing so, we will end up with a list of all free submodules of $\mathfrak{W}_k$ with index d. Letting d run through the positive integers, we will ultimately find all free submodules of the smallest index possible.

Next, we want to obtain a list of all free A-modules of minimal index in $\mathfrak{S}$. So far, we know how to construct A-modules from the blocks X_k^*. We still need to clarify when our list is complete. To begin with, we make a rather evident observation.

(4.18) Proposition. Let $\mathfrak{A}$, $\mathfrak{A}' \subset \mathfrak{S}$ be two free A-modules with A-bases X and Y. If $\mathfrak{A} = \mathfrak{A}'$, then X_k^* and Y_k^* generate the same submodule of $\mathfrak{W}_k$.

Proof. Let

$$\mathfrak{A}_k = V_k \cap \mathfrak{A}.$$

This is a submodule of $\mathfrak{S}_k$. Suppose $v = X_1 v_1 + \cdots + X_\nu v_\nu$ is an element of $\mathfrak{A}_k$. Here, each v_k is a vector over $\mathcal{O}$ of suitable length. Then

$$0 = A^k v = (A^k X_{k+1}) v_{k+1} + \cdots + (A^k X_\nu) v_\nu.$$

Since the columns of $[\, A^k X_{k+1} \ \ldots \ A^k X_\nu \,]$ appear in the basis X, they are linearly independent over $\mathcal{O}$. We conclude $v_\ell = 0$ for $\ell > k$. Thus $\mathfrak{A}_k$ is generated by the columns of

$$[\, X_1 \ \ldots \ X_{k-1} \ X_k \,] = [\, X_1 \ \ldots \ X_{k-1} \ AX_{k+1} \ X_k^* \,].$$

The module $\mathfrak{X}_k \subset \mathfrak{W}_k$, which is generated by X_k^*, is equal to the image of the composition

$$\mathfrak{A}_k \to \mathfrak{S}_k \to \mathfrak{W}_k = \mathfrak{S}_k / \mathfrak{T}_k$$

because the columns of $[\, X_1 \ \ldots \ X_{k-1} \ AX_{k+1} \,]$ vanish modulo

$$\mathfrak{T}_k = (V_{k-1} + AV_{k+1}) \cap \mathfrak{S}.$$

Analogously, the image of

$$\mathfrak{A}'_k \to \mathfrak{S}_k \to \mathfrak{W}_k \quad \text{with } \mathfrak{A}'_k = V_k \cap \mathfrak{A}'$$

is generated by Y_k^*. So if $\mathfrak{A} = \mathfrak{A}'$, then $\mathfrak{A}_k = \mathfrak{A}'_k$, that is, X_k^* and Y_k^* generate the same submodule of $\mathfrak{W}_k$. ■

In order to compile a complete list of free A-modules of minimal index in $\mathfrak{S}$, we still need to solve one problem. Suppose $\mathfrak{A}$ is a module with A-basis X and let $\mathfrak{X}_k$ be the module with a basis represented by X_k^*. If we change the columns of X_k^* by adding elements of $\mathfrak{T}_k$, we still obtain a basis of $\mathfrak{X}_k$ modulo $\mathfrak{T}_k$. Over $\mathcal{O}$, however, the new A-basis X might generate a different module $\mathfrak{A}'$. Hence we need to examine how many modules can be obtained this way.

Let us be more exact. Suppose that $\mathfrak{A}$ and $\mathfrak{A}'$ are free A-modules with A-bases X and Y such that X_k^* and Y_k^* represent bases of the same free submodule of $\mathfrak{W}_k$ for all k. In this case we have the relation

$$Y_k^* = X_k^* U_k + Z_k$$

where U_k is invertible over $\mathcal{O}$ and the columns of Z_k belong to $\mathfrak{T}_k$. Replacing Y_k^* by $Y_k^* U_k^{-1}$ does neither change $\mathfrak{X}_k$ nor $\mathfrak{A}'$. Moreover, the columns of $Z_k U_k^{-1}$ still belong to $\mathfrak{T}_k$. Therefore we may assume

$$Y_k^* = X_k^* + Z_k.$$

The next theorem tells us precisely when $\mathfrak{A}$ and $\mathfrak{A}'$ are equal in this situation.

(4.19) Theorem. Let $\mathfrak{A}$ and $\mathfrak{A}'$ be two free A-modules of minimal index in $\mathfrak{S}$ with A-bases X and Y such that

$$Y_k^* = X_k^* + Z_k \quad \text{for all } k$$

where the columns of Z_k belong to $\mathfrak{T}_k$. Let $\mathfrak{Z}_k \subset \mathfrak{T}_k$ denote the module generated by $[\, X_1 \ \ldots \ X_{k-1} \ AX_{k+1} \,]$. The following statements are equivalent.

(1) $\mathfrak{A}$ is equal to $\mathfrak{A}'$.

(2) The columns of Z_k belong to $\mathfrak{Z}_k$ for each k.

Proof. Suppose $\mathfrak{A} = \mathfrak{A}'$. Then each column of Y is a linear combination of the columns of X, in particular each column of Y_k^*. Thus there are matrices $T_1, \ldots, T_\nu$ over $\mathcal{O}$ such that

$$X_1T_1 + \cdots + X_\nu T_\nu = Y_k^*.$$

Multiplying both sides with A^k, we see that

$$(A^kX_{k+1})T_{k+1} + \cdots + (A^kX_\nu)T_\nu = 0.$$

Since the columns of $A^kX_{k+1}, \ldots, A^kX_\nu$ appear in the basis of $\mathfrak{A}$, they are linearly independent over $\mathcal{O}$. We conclude $T_\ell = 0$ for $\ell > k$, so

$$X_1T_1 + \cdots + X_kT_k = Y_k^*.$$

Since $X_k = [\, AX_{k+1} \ X_k^* \,]$ and $Y_k^* = X_k^* + Z_k$, this equation can be written as

$$X_1T_1 + \cdots + X_{k-1}T_{k-1} + AX_{k+1}T_k' + X_k^*T_k'' = X_k^* + Z_k$$

where T_k' and T_k'' are the upper and lower rows of T_k. Reducing all columns modulo $\mathfrak{T}_k$, we obtain

$$X_k^*T_k'' \equiv X_k^* \mod \mathfrak{T}_k.$$

This implies $T_k'' = I$ because the columns of X_k^* remain linearly independent modulo $\mathfrak{T}_k$ by (4.16). Therefore

$$X_1T_1 + \cdots + X_{k-1}T_{k-1} + AX_{k+1}T_k' = Z_k,$$

that is, the columns of Z_k can be generated by $[\, X_1 \ \ldots \ X_{k-1} \ AX_{k+1} \,]$ and thus they belong to $\mathfrak{Z}_k$.

Now assume the columns of Z_k belong to $\mathfrak{Z}_k$ for each k. We want to show that we can transform Y into X using elementary column operations over $\mathcal{O}$ because this implies

$$\mathfrak{A}' = Y\mathcal{O}^n = X\mathcal{O}^n = \mathfrak{A}.$$

First we will prove that $Y_1 \sim X_1$. Since the columns of Z_ν belong to

$$\mathfrak{Z}_\nu \subset \mathfrak{T}_\nu \subset V_{\nu-1} + AV_{\nu+1} = V_{\nu-1} + AV_\nu = V_{\nu-1},$$

we know that $A^{\nu-1}Z_\nu = 0$, so

$$A^{\nu-1}Y_\nu = A^{\nu-1}Y_\nu^* = A^{\nu-1}(X_\nu^* + Z_\nu) = A^{\nu-1}X_\nu^* = A^{\nu-1}X_\nu.$$

Let us assume that $A^{k-1}Y_k \sim A^{k-1}X_k$ has already been proved for $1 < k \leq \nu$. Then

$$\begin{aligned} A^{k-2}Y_{k-1} = A^{k-2}[\,AY_k \;\; Y_{k-1}^*\,] &= [\,A^{k-1}Y_k \;\; A^{k-2}Y_{k-1}^*\,] \\ &\sim [\,A^{k-1}X_k \;\; A^{k-2}Y_{k-1}^*\,] \\ &= [\,A^{k-1}X_k \;\; A^{k-2}(X_{k-1}^* + Z_{k-1})\,]. \end{aligned}$$

By our assumptions, the columns of $A^{k-2}Z_{k-1}$ belong to $A^{k-2}\mathfrak{Z}_{k-1}$, which is generated by the columns of

$$A^{k-2}[\,X_1 \;\ldots\; X_{k-2} \; AX_k\,] = [\,0 \;\ldots\; 0 \; A^{k-1}X_k\,].$$

Performing elementary column operations over $\mathcal{O}$, we can erase $A^{k-2}Z_{k-1}$, so

$$A^{k-2}Y_{k-1} \sim [\,A^{k-1}X_k \;\; A^{k-2}X_{k-1}^*\,] = A^{k-2}[\,AX_k \; X_{k-1}^*\,] = A^{k-2}X_{k-1}.$$

By backward induction this proves $A^{k-1}Y_k \sim A^{k-1}X_k$ for $1 \leq k \leq \nu$. In particular, $Y_1 \sim X_1$.
To finish the proof, we will use forward induction. We now may assume that

$$Y = [\,X_1 \;\ldots\; X_k \; Y_{k+1} \;\ldots\; Y_\nu\,] \quad \text{for } 1 \leq k < \nu.$$

If we can show that Y_{k+1} can be transformed into X_{k+1}, we may conclude $Y \sim X$ and the theorem is established. Observe that

$$\begin{aligned} Y_{k+1} &= [\,AY_{k+2} \; Y_{k+1}^*\,] \\ &= [\,A^2Y_{k+3} \; AY_{k+2}^* \; Y_{k+1}^*\,] \\ &\;\vdots \\ &= [\,A^{\nu-k-1}Y_\nu^* \;\ldots\; AY_{k+2}^* \; Y_{k+1}^*\,] \\ &= [\,A^{\nu-k-1}(X_\nu^* + Z_\nu) \;\ldots\; A(X_{k+2}^* + Z_{k+2}) \;\; (X_{k+1}^* + Z_{k+1})\,]. \end{aligned}$$

The columns of $A^{\nu-k-1}Z_\nu$ belong to $A^{\nu-k-1}\mathfrak{Z}_\nu$ which is generated by

$$A^{\nu-k-1}[\,X_1 \;\ldots\; X_{\nu-1}\,] = [\,0 \;\ldots\; 0 \; A^{\nu-k-1}X_{\nu-k} \;\ldots\; A^{\nu-k-1}X_{\nu-1}\,].$$

The nonzero blocks of this matrix appear in $[\,X_1 \;\ldots\; X_k\,]$ because

$$X_\ell = [\,AX_{\ell+1} \; *\,] = \cdots = [\,A^{\nu-k-1}X_{\nu+\ell-k-1} \; *\,] \quad \text{for } 1 \leq \ell \leq k.$$

Hence, performing elementary column operations on Y, we can erase $A^{\nu-k-1}Z_\nu$ in Y_{k+1}. Now assume

$$Y_{k+1} = [\,A^{\nu-k-1}Y_\nu^* \;\ldots\; AY_{k+2}^* \; Y_{k+1}^*\,]$$

with

$$Y_\ell^* = X_\ell^* \quad \text{for } \nu \geq \ell > k+m \text{ for some fixed } m.$$

We have

$$A^{m-1}Y_{k+m}^* = A^{m-1}(X_{k+m}^* + Z_{k+m}).$$

The columns of $A^{m-1}Z_{k+m}$ belong to $A^{m-1}\mathfrak{Z}_{k+m}$, which is generated by

$$\begin{aligned} &A^{m-1}[\,X_1 \;\ldots\; X_{k+m-1} \; AX_{k+m+1}\,] \\ &\qquad\qquad = [\,0 \;\ldots\; 0 \; A^{m-1}X_m \;\ldots\; A^{m-1}X_{k+m-1} \;\; A^mX_{k+m+1}\,]. \end{aligned}$$

This time the nonzero blocks appear in

$$[\,X_1 \;\ldots\; X_k \; A^{\nu-k-1}X_\nu^* \;\ldots\; A^mX_{k+m+1}^*\,]$$

because

$$X_\ell = [\,AX_{\ell+1} \; *\,] = \cdots = [\,A^{m-1}X_{\ell+m-1} \; *\,] \quad \text{for } 1 \leq \ell \leq k$$

and

$$A^mX_{k+m+1} = [\,A^{\nu-k-1}X_\nu^* \;\ldots\; A^mX_{k+m+1}^*\,].$$

Hence we can erase $A^{m-1}Z_{k+m}$ in Y_{k+1}. By induction we obtain

$$Y \sim [\,X_1 \;\ldots X_{k+1} \; Y_{k+2} \;\ldots\; Y_\nu\,],$$

and ultimately this yields $Y \sim X$. ■

(4.20) Corollary. Let w_k be the number of free modules of minimal index in $\mathfrak{W}_k$. The number of free A-modules of minimal index in $\mathfrak{S}$ is equal to the product

$$\prod_{k=1}^{\nu} w_k(n_k - n_{k+1})[\mathfrak{T}_k : \mathfrak{Z}_k] \quad \text{where } n_{\nu+1} = 0.$$

Proof. Let X_k^* represent a basis of a free module $\mathfrak{X}_k \subset \mathfrak{W}_k$ of minimal index. Let X be the A-basis obtained from $X_1^*, \ldots, X_\nu^*$ and $\mathfrak{A} = X\mathcal{O}^n$. Then $\mathfrak{A}$ is an A-module of minimal index in $\mathfrak{S}$ by (4.17). Each column of X_k^* can be altered modulo $\mathfrak{T}_k$ without changing $\mathfrak{X}_k$, and by (4.19) $\mathfrak{A}$ will stay unchanged precisely if we alter each column modulo $\mathfrak{Z}_k$. Hence there are $[\mathfrak{T}_k : \mathfrak{Z}_k]$ ways of altering a column of X_k^* that will change $\mathfrak{A}$ but not $\mathfrak{X}_k$. In total, X_k^* has $n_k - n_{k+1}$ columns. Finally, if we choose X_k^* to represent a basis of another free module $\mathfrak{X}_k' \neq \mathfrak{X}_k$ of minimal index, this will also lead to a new A-module by (4.18). Since there are w_k different choices for $\mathfrak{X}_k$, this establishes the corollary. ■

4.4 Nilpotent Integer Matrices

In this section we will study some aspects of nilpotent matrices over the integers. Since we examine the similarity of integer matrices in general, nilpotent integer matrices naturally arise as a special case. Beyond that, if

$$A = S + N \quad \text{and} \quad B = S' + N'$$

are two similar matrices in Jordan–Chevalley decomposition, we saw at the beginning of the chapter that their nilpotent parts have to be similar, too. So before running the procedure for deciding whether A and B are similar, it might be worthwhile to examine N and N' in a first step.

The main goal of this section will be to develop conditions which have to be met for N and N' to be similar and which can be checked easily. Later on, we will investigate two special cases where it is rather easy to actually prove similarity.

Beforehand, let us briefly describe a major improvement of the general procedure in the case of nilpotent integer matrices. In this situation, $S = S'$ is the zero matrix, which has minimal polynomial X, so

$$\mathcal{O} = \mathbb{Z}[X]/(X) = \mathbb{Z}.$$

A full $\mathbb{Z}$-module corresponding to S is given by $\mathfrak{S} = \mathbb{Z}^n$. So if $\mathfrak{A} \subset \mathfrak{S}$ is an A-module, it is always free. Moreover, each quotient

$$\mathfrak{W}_k = \mathfrak{S}_k / \mathfrak{T}_k$$

is free and a $\mathbb{Z}$-basis can be found without difficulty. Therefore we can avoid the cumbersome search for the free submodules of minimal index in $\mathfrak{W}_k$. Still, the number of free A-modules of minimal index in $\mathbb{Z}^n$ may grow arbitrary large and so does the effort for deciding whether A- and B-modules are similar. Hence it is desirable to establish some criteria which can lead to a negative result quickly. First we will show that every nilpotent integer matrix can be transformed into a simpler form.

(4.21) Proposition. Let $n_1 \geq \ldots \geq n_\nu$ be positive integers. If $A \in \mathrm{M}(n, \mathbb{Z})$ is a nilpotent matrix with structure $n_1 \geq \ldots \geq n_\nu$, then A is similar to a matrix of the form

$$\begin{bmatrix} 0 & A_{12} & \cdots & A_{1\nu} \\ & \ddots & \ddots & \vdots \\ & & \ddots & A_{\nu-1,\nu} \\ 0 & & & 0 \end{bmatrix}$$

where $A_{k\ell}$ is a block of the size $n_k \times n_\ell$ and each $A_{k-1,k}$ has full rank n_k. Conversely, every block matrix as above is nilpotent and $n_1 \geq \ldots \geq n_\nu$ is its structure. In particular, the stated form is uniquely determined by the structure of the matrix.

Proof. Let

$$\mathfrak{A}_k = \ker(A^k) \cap \mathbb{Z}^n \quad \text{for } 0 \leq k \leq \nu.$$

Then each quotient $\mathfrak{A}_k / \mathfrak{A}_{k-1}$ is torsionfree; otherwise there would be a vector $x \in \mathfrak{A}_k \smallsetminus \mathfrak{A}_{k-1}$ such that $ax \in \mathfrak{A}_{k-1}$ for some integer $a \neq 0$, that is,

$$A^{k-1}x \neq 0 \qquad \text{and} \qquad a(A^{k-1}x) = 0.$$

Consequently, $\mathfrak{A}_k/\mathfrak{A}_{k-1}$ is a free $\mathbb{Z}$-module. Let X_{k-1} be a basis of $\mathfrak{A}_{k-1}$ and let X_k represent a basis of $\mathfrak{A}_k/\mathfrak{A}_{k-1}$. Then $[\,X_{k-1}\ X_k\,]$ is a basis of $\mathfrak{A}_k$. We can thus construct a basis

$$X = [\,X_1\ \dots\ X_\nu\,]$$

of $\mathbb{Z}^n$ where each X_k represents a basis of $\mathfrak{A}_k/\mathfrak{A}_{k-1}$. It follows that n_k is the number of columns of X_k and that $X^{-1}AX$ is of the desired form because the columns of AX_k belong to $\mathfrak{A}_{k-1}$, which means they can be expressed as linear combinations of the columns of $[\,X_1\ \dots\ X_{k-1}\,]$.
Now suppose the rank of $A_{k-1,k}$ were not full. Then the rank of

$$\begin{bmatrix} A_{12} & & * \\ & \ddots & \\ 0 & & A_{k-1,k} \end{bmatrix}$$

is not full. If $x \neq 0$ belongs to the kernel of this submatrix, then the vector $[\,0\ x^{\text{tr}}\ 0\,]^{\text{tr}}$, with n_1 leading and $n_{k+1}+\dots+n_\nu$ trailing zeros, belongs to the kernel of $X^{-1}AX$. But all elements of this kernel are of the form $[\,*\ 0\ 0\,]^{\text{tr}}$.
Finally, suppose A is of the stated block form. As one easily sees, we have $A^\nu = 0$, and if $k < \nu$, then A^k is of the form

$$\begin{bmatrix} & A'_{1,k+1} & & * \\ & & \ddots & \\ & & & A'_{\nu-k,\nu} \\ & & & \\ & & & \end{bmatrix}$$

where

$$A'_{\ell,\ell+k} = A_{\ell,\ell+1}\cdots A_{\ell+k-1,\ell+k} \neq 0.$$

Since the rank of each $A_{k-1,k}$ is full, and thus equal to n_k, the rank of $A'_{\ell,\ell+k}$ is also full and equal to $n_{\ell+k}$. In conclusion, $n_{k+1}+\dots+n_\nu$ is the rank of A^k, that is, $n_1+\dots+n_k$ is the dimension of its kernel. Hence $n_1 \geq \ldots \geq n_\nu$ is the structure of A. ■

If a matrix is given in the form as in (4.21), we say it has the **block form** $n_1 \geq \ldots \geq n_\nu$. If A and B are nilpotent integer matrices, we may assume that they are given in the same block form. Otherwise, they cannot be similar.

(4.22) Proposition. Let A and B be two nilpotent integer matrices with block form $n_1 \geq \ldots \geq n_\nu$. If $C \in \mathrm{GL}(n,\mathbb{Z})$ satisfies $CA = BC$, then

$$C = \begin{bmatrix} C_{11} & \cdots & C_{1\nu} \\ & \ddots & \vdots \\ 0 & & C_{\nu\nu} \end{bmatrix}$$

where each block $C_{k\ell}$ has the size $n_k \times n_\ell$.

Proof. Let

$$C = \begin{bmatrix} C_{11} & \cdots & C_{1\nu} \\ \vdots & \ddots & \vdots \\ C_{\nu 1} & \cdots & C_{\nu\nu} \end{bmatrix}.$$

Then

$$CA = \begin{bmatrix} 0 & C_{11}A_{12} & \cdots & \cdots & C_{11}A_{1\nu} + \cdots + C_{1,\nu-1}A_{\nu-1,\nu} \\ \vdots & \vdots & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & C_{\nu 1}A_{12} & \cdots & \cdots & C_{\nu 1}A_{1\nu} + \cdots + C_{\nu,\nu-1}A_{\nu-1,\nu} \end{bmatrix}$$

and

$$BC = \begin{bmatrix} B_{12}C_{21} + \cdots + B_{1\nu}C_{\nu 1} & \cdots & B_{12}C_{2\nu} + \cdots + B_{1\nu}C_{\nu\nu} \\ \vdots & \ddots & \vdots \\ B_{\nu-1,\nu}C_{\nu 1} & \cdots & B_{\nu-1,\nu}C_{\nu\nu} \\ 0 & \cdots & 0 \end{bmatrix}.$$

If $CA = BC$, we first observe that

$$C_{\nu 1}A_{12} = 0.$$

Since A_{12} has full rank, we conclude $C_{\nu 1} = 0$. Next we obtain

$$C_{\nu 2}A_{23} = C_{\nu 1}A_{13} + C_{\nu 2}A_{23} = 0,$$

implying $C_{\nu 2} = 0$. Proceeding like this, we see that $C_{\nu \ell} = 0$ if $\nu > \ell$. Therefore

$$C_{\nu-1,1}A_{12} = B_{\nu-1,\nu}C_{\nu 2} = 0,$$

so $C_{\nu-1,1} = 0$. Ultimately, this reasoning shows $C_{k\ell} = 0$ if $k > \ell$. ■

If C is given in the form as above, we will also say that C has the block form $n_1 \geq \ldots \geq n_\nu$. If we want to see whether two matrices are similar, making use of the the block form provides us with a first set of necessary conditions. If A and B are similar and have the block form $n_1 \geq \ldots \geq n_\nu$, the submatrices

$$\begin{bmatrix} 0 & A_{23} & \cdots & A_{2\nu} \\ & \ddots & \ddots & \vdots \\ & & \ddots & A_{\nu-1,\nu} \\ 0 & & & 0 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & B_{23} & \cdots & B_{2\nu} \\ & \ddots & \ddots & \vdots \\ & & \ddots & B_{\nu-1,\nu} \\ 0 & & & 0 \end{bmatrix}$$

(obtained by deleting the first n_1 rows and columns) are similar, too. Thus we can perform $\nu - 1$ successive tests, starting with

$$\begin{bmatrix} 0 & A_{\nu-1,\nu} \\ 0 & 0 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & B_{\nu-1,\nu} \\ 0 & 0 \end{bmatrix},$$

to decide whether A and B are similar.

We will now introduce further necessary conditions which have to be met and which can be verified easily. First of all, if A and B are similar, they are also equivalent, that is, there are invertible matrices C and D such that $CA = BD$. If A and B have the same block form, there are more conditions of this sort.

(4.23) Proposition. Let A and B be two nilpotent integer matrices with block form $n_1 \geq \ldots \geq n_\nu$. If A and B are similar, the submatrices

$$\begin{bmatrix} A_{k,k+1} & \cdots & A_{k\ell} \\ & \ddots & \vdots \\ 0 & & A_{\ell-1,\ell} \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} B_{k,k+1} & \cdots & B_{k\ell} \\ & \ddots & \vdots \\ 0 & & B_{\ell-1,\ell} \end{bmatrix}$$

are equivalent for $1 \leq k < \ell \leq \nu$.

Proof. Let $C \in \mathrm{GL}(n, \mathbb{Z})$ have the block form $n_1 \geq \ldots \geq n_\nu$. Then

$$CA = \begin{bmatrix} 0 & C_{11}A_{12} & \cdots & C_{11}A_{1\nu} + \cdots + C_{1,\nu-1}A_{\nu-1,\nu} \\ & \ddots & \ddots & \vdots \\ & & \ddots & C_{\nu-1,\nu-1}A_{\nu-1,\nu} \\ 0 & & & 0 \end{bmatrix}$$

and

$$BC = \begin{bmatrix} 0 & B_{12}C_{22} & \cdots & B_{12}C_{2\nu} + \cdots + B_{1\nu}C_{\nu\nu} \\ & \ddots & \ddots & \vdots \\ & & \ddots & B_{\nu-1,\nu}C_{\nu\nu} \\ 0 & & & 0 \end{bmatrix}.$$

A careful observation of these two matrices reveals that the products

$$\begin{bmatrix} C_{kk} & \cdots & C_{k,\ell-1} \\ & \ddots & \vdots \\ 0 & & C_{\ell-1,\ell-1} \end{bmatrix} \begin{bmatrix} A_{k,k+1} & \cdots & A_{k\ell} \\ & \ddots & \vdots \\ 0 & & A_{\ell-1,\ell} \end{bmatrix}$$

and

$$\begin{bmatrix} B_{k,k+1} & \cdots & B_{k\ell} \\ & \ddots & \vdots \\ 0 & & B_{\ell-1,\ell} \end{bmatrix} \begin{bmatrix} C_{k+1,k+1} & \cdots & C_{\ell,k+1} \\ & \ddots & \vdots \\ 0 & & C_{\ell\ell} \end{bmatrix}$$

are different expressions for the same submatrix, given that $CA = BC$. ■

The previous proposition equips us with $\nu(\nu + 1)/2$ necessary conditions for similarity, all of which can be verified by comparing the Smith normal forms of the respective submatrices. In contrast to the expensive test for similarity, this can be done considerably fast.

Unsurprisingly, there are matrices where the Smith normal forms of all submatrices coincide, yet the matrices are not similar. For example, consider

$$A = \begin{bmatrix} 0 & 3 & 1 \\ 0 & 0 & 3 \\ 0 & 0 & 0 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 0 & 3 & -1 \\ 0 & 0 & 3 \\ 0 & 0 & 0 \end{bmatrix}.$$

The Smith normal forms of the respective submatrices are

$$\begin{bmatrix}3\end{bmatrix}, \quad \begin{bmatrix}3\end{bmatrix} \quad \text{and} \quad \begin{bmatrix}1 & 0\\ 0 & 9\end{bmatrix}.$$

Suppose

$$C = \begin{bmatrix} c_{11} & c_{12} & c_{13}\\ 0 & c_{22} & c_{23}\\ 0 & 0 & c_{33}\end{bmatrix}$$

were an invertible matrix (i.e., $c_{ii} = \pm 1$) with $CA = BC$. Then we obtain

$$3c_{11} = 3c_{22}, \qquad 3c_{22} = 3c_{33}, \qquad \text{and} \qquad c_{11} + 3c_{12} = 3c_{13} - c_{33}.$$

The first two equations yield $c_{11} = c_{22} = c_{33}$ and the third one states

$$\pm 2 = c_{11} + c_{33} \equiv 0 \mod 3.$$

Hence A and B cannot be similar.

There are, however, two situations in which similarity itself can be confirmed quickly. The first one is given by the condition $\nu = 2$.

(4.24) Corollary. Let

$$A = \begin{bmatrix} 0 & A_{12}\\ 0 & 0\end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 0 & B_{12}\\ 0 & 0\end{bmatrix}$$

be two nilpotent integer matrices with block form $n_1 \geq n_2$. Then A and B are similar if and only if A_{12} and B_{12} are equivalent.

Proof. By (4.23), A_{12} and B_{12} are equivalent if A and B are similar. Conversely, suppose there are invertible matrices C_{11} and C_{22} such that

$$C_{11}A_{12} = B_{12}C_{22}.$$

Then

$$CA = \begin{bmatrix} 0 & C_{11}A_{12}\\ 0 & 0\end{bmatrix} = \begin{bmatrix} 0 & B_{12}C_{22}\\ 0 & 0\end{bmatrix} = BC$$

for $C = C_{11} \oplus C_{22}$. ■

Unfortunately, the result of the corollary cannot be generalized for higher values of ν. For example, suppose

$$A = \begin{bmatrix} 0 & A_{12} & 0\\ 0 & 0 & A_{23}\\ 0 & 0 & 0\end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 0 & B_{12} & 0\\ 0 & 0 & B_{23}\\ 0 & 0 & 0\end{bmatrix}$$

and let C be an invertible matrix of the same block form. In this situation, we have $CA = BC$ if and only if

$$C_{11}A_{12} = B_{12}C_{22} \quad \text{and} \quad C_{22}A_{23} = B_{23}C_{33}.$$

Since C_{22} appears in both equations, these requirements are not independent. Also, if $n_2 > 1$, the number of choices for C_{22} is potentially infinite.

The second rather easy situation for testing similarity is given by nilpotent matrices of the structure $n_1 = \cdots = n_\nu = 1$. In this case, the respective block form is given by an upper triangular matrix

$$\begin{bmatrix} 0 & a_{11} & \cdots & a_{1\nu} \\ & \ddots & \ddots & \vdots \\ & & \ddots & a_{\nu-1,\nu} \\ 0 & & & 0 \end{bmatrix}.$$

As we will see, similarity of such matrices can be proved by solving a system of linear equations. We will examine this situation as a special case of a more general context.

A structure $n_1 \geq \ldots \geq n_\nu$ will be called **unitarily decreasing** if the following conditions are satisfied:

- $n_\nu = 1$ and
- $n_{k+1} \geq n_k - 1$ for $k < \nu$.

In other words, the values of the structure are decremented by 0 or 1 in each step until they hit 1 eventually. For example, the structure

$$3 = 3 \geq 2 = 2 = 2 \geq 1 = 1$$

is unitarily decreasing.
Before we occupy ourselves with matrices of unitarily decreasing structure, we will show that any block form $n_1 \geq \ldots \geq n_\nu$ can be simplified further.

(4.25) Proposition. Let A be a nilpotent integer matrix given in block form $n_1 \geq \ldots \geq n_\nu$. Then each submatrix $[\,A_{k-1,k} \;\ldots\; A_{k-1,\nu}\,]$ can be chosen in row Hermite normal form.

Proof. Let $H_{\nu-1}$ be the row Hermite normal form of $A_{\nu-1,\nu}$ and let $C_{\nu-1}$ be an invertible matrix such that $H_{\nu-1} = C_{\nu-1}A_{\nu-1,\nu}$. Put

$$C = I_{n_1} \oplus \cdots \oplus I_{n_{\nu-2}} \oplus C_{\nu-1} \oplus I_{n_\nu}.$$

Then

$$CAC^{-1} = \begin{bmatrix} 0 & A_{12} & \cdots & A_{1,\nu-2} & * & A_{1\nu} \\ & \ddots & \ddots & \vdots & \vdots & \vdots \\ & & \ddots & A_{\nu-3,\nu-2} & * & A_{\nu-3,\nu} \\ & & & \ddots & * & A_{\nu-2,\nu} \\ & & & & \ddots & H_{\nu-1} \\ & & & & & 0 \end{bmatrix}.$$

Replacing A by CAC^{-1}, we thus may assume that $A_{\nu-1,\nu}$ is in row Hermite normal form. Notice that, apart from $A_{\nu-1,\nu}$, only the $(k,\, \nu-1)$-blocks of A are affected by conjugation with C.
Next, let $H_{\nu-2}$ be the row Hermite normal form of $[\, A_{\nu-2,\nu-1}\ A_{\nu-2,\nu}\,]$ and

$$C = I_{n_1} \oplus \cdots \oplus I_{n_{\nu-3}} \oplus C_{\nu-2} \oplus I_{\nu-1} \oplus I_{n_\nu}$$

where $H_{\nu-2} = C_{\nu-2}[\, A_{\nu-2,\nu-1}\ A_{\nu-2,\nu}\,]$. Switching from A to CAC^{-1} leaves $A_{\nu-1,\nu}$ unaffected and transforms $[\, A_{\nu-2,\nu-1}\ A_{\nu-2,\nu}\,]$ into row Hermite normal form. Proceeding in this manner, we will obtain the desired result. ■

(4.26) Theorem. Let A and B be two nilpotent integer matrices of unitarily decreasing structure $n_1 \geq \ldots \geq n_\nu$ given in block form as in (4.25). Then the following statements hold.

(1) If A and B are similar, the diagonals of $A_{k-1,k}$ and $B_{k-1,k}$ are equal for $1 < k \leq \nu$.

(2) If $C \in \mathrm{GL}(n, \mathbb{Z})$ satisfies $CA = BC$, then C is of the form

$$\begin{bmatrix} C_{11} & \cdots & C_{1\nu} \\ & \ddots & \vdots \\ 0 & & C_{\nu\nu} \end{bmatrix}$$

where each block C_{kk} is an upper triangular matrix of the size $n_k \times n_k$. Moreover, for $k > 1$, the first n_k diagonal entries of $C_{k-1,k-1}$ coincide with the diagonal entries of C_{kk}.

Proof. Suppose C is an invertible matrix such that $CA = BC$. By (4.22) we already know that C has the block form $n_1 \geq \ldots \geq n_\nu$. Suppose C_{kk} is an upper triangular matrix. Since $n_\nu = 1$, this is true for $k = \nu$. Write

$$C_{k-1,k-1} = \begin{bmatrix} C' & * \\ C'' & * \end{bmatrix}$$

where C' is an $n_k \times n_k$ matrix and C'' is a block of size $(n_{k-1} - n_k) \times n_k$, that is, either a row vector or nonexistent. Furthermore, we have

$$A_{k-1,k} = \begin{bmatrix} A' \\ 0 \end{bmatrix} \quad \text{and} \quad B_{k-1,k} = \begin{bmatrix} B' \\ 0 \end{bmatrix}$$

where A' and B' are square upper triangular matrices in row Hermite normal form of full rank. Again, the zero rows might be nonexistent. As seen in the proof of (4.23), we have the relation

$$C_{k-1,k-1}A_{k-1,k} = B_{k-1,k}C_{kk}$$

and in our case it reads

$$\begin{bmatrix} C'A' \\ C''A' \end{bmatrix} = \begin{bmatrix} B'C_{kk} \\ 0 \end{bmatrix}.$$

This implies $C'' = 0$ because A' has full rank. Since A', B' and C_{kk} are upper triangular matrices, the same is true for

$$C' = (A')^{-1} B' C_{kk}$$

and thus for $C_{k-1,k-1}$. With obvious notations, the ith diagonal entry of C' is of the form

$$c'_{ii} = \frac{b'_{ii}}{a'_{ii}} c_{ii} \quad \text{where } c'_{ii},\, c_{ii} = \pm 1.$$

Since A' and B' are in Hermite normal form, the entries on their diagonals are positive. Consequently, $c'_{ii} = c_{ii}$, and therefore $a'_{ii} = b'_{ii}$. This proves all statements of the theorem. ■

(4.27) Corollary. Let A and B be two nilpotent integer matrices of unitarily decreasing structure $n_1 \geq \ldots \geq n_\nu$ and let ℓ be the number of all indices $k < \nu$ with $n_k > n_{k+1}$. If the matrices are given in the form of (4.25), similarity can be decided by solving at most 2^ℓ systems of linear equations.

Proof. If C is an invertible matrix satisfying $CA = BC$, then it is an upper triangular matrix by (4.26). Therefore the entries on its diagonal are equal to ± 1. If a diagonal is fixed, the remaining entries of C can be obtained as a solution of the system $CA = BC$. If none of these systems can be solved, A and B are not similar.
Because of the repetitive structure of the diagonal of C described in (4.26), the number of possible diagonals is less than 2^n. For all k with $n_k = 1$, we have

$$C_{kk} = \cdots = C_{\nu\nu} = \pm 1,$$

giving us two possibilities for these entries. Suppose $k < \nu$ and let $[\, c_1 \ \ldots \ c_{n_{k+1}} \,]$ be the diagonal of $C_{k+1,k+1}$. If $n_k > n_{k+1}$, then

$$C_{kk} = \begin{bmatrix} c_1 & & & * \\ & \ddots & & \\ & & c_{n_{k+1}} & \\ 0 & & & * \end{bmatrix}$$

where the last diagonal entry can be chosen freely among ± 1. So every $k < \nu$ with $n_k > n_{k+1}$ increases the number of diagonals by the factor 2. If $n_k = n_{k+1}$, we have

$$C_{kk} = \begin{bmatrix} c_1 & & * \\ & \ddots & \\ 0 & & c_{n_{k+1}} \end{bmatrix},$$

leaving us no choice. Taken together, there are $2^{\ell+1}$ diagonals. But half of them can be discarded (in effect, by fixing $C_{\nu\nu} = 1$), because if C satisfies $CA = BC$, then so does $-C$. ■

As a consequence of the corollary, the case $n_1 = \cdots = n_\nu = 1$ can be handled by solving a single system of linear equations. Yet even in the case $n_1 > \ldots > n_\nu$, where $\ell = \nu - 1$, the number of systems will be considerably smaller than 2^{n-1}. In this situation, we have

$$n_k = \nu - k + 1$$

since $n_\nu = 1$ and $n_k = n_{k+1} + 1$ for $k < \nu$. Therefore

$$n = n_1 + \cdots + n_\nu = \nu + \cdots + 1 > \nu,$$

given that $\nu > 1$, of course. In practice, the case $n_1 > \ldots > n_\nu$ can actually be handled better than $n_1 = \cdots = n_\nu = 1$, if compared for a fixed $n = n_1 + \cdots + n_\nu$. This is because the systems on linear equations contain a lot more zero rows in the first case. See the next chapter for concrete running times.

Let us describe one last improvement. As mentioned before, if we want to see whether A and B are similar, we may assume that the submatrices

$$A_k = \begin{bmatrix} 0 & A_{k,k+1} & \cdots & A_{k\nu} \\ & \ddots & \ddots & \vdots \\ & & \ddots & A_{\nu-1,\nu} \\ 0 & & & 0 \end{bmatrix} \quad \text{and} \quad B_k = \begin{bmatrix} 0 & B_{k,k+1} & \cdots & B_{k\nu} \\ & \ddots & \ddots & \vdots \\ & & \ddots & B_{\nu-1,\nu} \\ 0 & & & 0 \end{bmatrix}$$

are similar. So instead of testing similarity directly, we can successively determine all possible diagonals for C_k such that the system $C_k A_k = B_k C_k$ is solvable, thereby ruling out incorrect diagonals with less effort.

4.5 Algorithms

(4.28) Algorithm — Related Matrix I

→ S semisimple integer matrix
M integer matrix commuting with S
Ω $\mathbb{Z}$-basis of a full module $\mathfrak{S}$ corresponding to S

← A the matrix in $\Lambda = (\mathfrak{S} : \mathfrak{S})$ related to M (see p. 91)

The basis Ω must have the form as in (1.5), i.e., the rows are eigenvectors of S. Suppose $M = [m_{ij}]$ and $\Omega = [\,\omega_1 \ \ldots \ \omega_s\,]$.

(1) Compute the matrix A of the homomorphism $\sigma\colon \boldsymbol{\mathcal{K}}^{\boldsymbol{n}} \to \boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$ given by

$$\sigma(\omega_i) = \sum m_{ij}\omega_j$$

with respect to the standard basis of $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$; cf. (4.2) and the proof of (1.1).

(2) Return A.

(4.29) Algorithm — Related Matrix II

→	S	semisimple integer matrix
	Ω	$\mathbb{Z}$-basis of a full module $\mathfrak{S}$ corresponding to S
	A	element of $\Lambda = (\mathfrak{S} : \mathfrak{S})$
←	M	the integer matrix related to A (see p. 91)

The basis Ω must have the form as in (1.5), i.e., the rows are eigenvectors of S. Suppose $\Omega = [\,\omega_1 \ \ldots \ \omega_s\,]$.

(1) Compute the integer matrix $M = [m_{ij}]$ given by $A\omega_i = \sum m_{ij}\omega_j$.

(2) Return M.

(4.30) Algorithm — Is Similar (Modules)

→	$\mathfrak{S}$	full module in $\mathcal{K}^n$
	$\mathfrak{A}$	free A-module over $\mathcal{O}$
	$\mathfrak{B}$	free B-module over $\mathcal{O}$
←	τ	`true`/`false`
	Γ	matrix proving the similarity of $\mathfrak{A}$ and $\mathfrak{B}$

The matrices A and B belong to $\Lambda = (\mathfrak{S} : \mathfrak{S})$, Γ will be a unit of Λ. The order $\mathcal{O}$ is a direct sum $\mathcal{O}_1 \oplus \cdots \oplus \mathcal{O}_s$. The modules $\mathfrak{A}$ and $\mathfrak{B}$ are given by A- and B-bases X and Y. The modules are contained in $\mathfrak{S}$. For each ι, the components A_ι and B_ι have the same structure.

(1) If $[\mathfrak{S} : \mathfrak{A}] \neq [\mathfrak{S} : \mathfrak{B}]$, return `false`.

(2) Compute a nonzerodivisor $\lambda \in \mathcal{O}$ with $\lambda\mathfrak{S} \subset \mathfrak{A}$. If $\lambda\mathfrak{S} \not\subset \mathfrak{B}$, return `false`.

(3) Put $\mathfrak{G} := Y^{-1}\Lambda X$. Then $\mathfrak{G}$ is the multiplier ideal $(\mathfrak{D} : \mathfrak{C})$.

(4) For $\iota = 1, \ldots, s$, compute the algebra $\mathcal{M}_\iota$ of all matrices $M \in \mathrm{M}(n_\iota, \mathcal{O}_\iota)$ of the form as in (4.9); also see p. 103. The structure referred to in (4.9) is the structure of A_ι and B_ι.

(5) Put $\mathcal{M} := \mathcal{M}_1 \oplus \cdots \oplus \mathcal{M}_s$ and $\overline{\mathcal{M}} := (\mathcal{M} \cap \mathfrak{G})/(\lambda\mathcal{M} \cap \mathfrak{G})$.

(6) For each $\overline{M} \in \overline{\mathcal{M}}$, check whether $\overline{M}$ is a unit of $\mathcal{M}/\lambda\mathcal{M}$ which stems from an element of $\mathcal{U} = \mathcal{M}^\times$. If so, go to the next step. If no such $\overline{M}$ exists, return `false`.

(7) Compute a preimage $U \in \mathcal{U}$ of $\overline{M}$, basically using algorithm (3.16); also pay attention to the remarks on p. 104.

(8) Put $\Gamma = YUX^{-1}$. Return `true` and Γ.

(4.31) Algorithm — All Free $\boldsymbol{A}$-Modules (Number Field Case)

→ $\mathfrak{S}$ full module in $\mathcal{K}^n$
A nilpotent matrix in $\Lambda = (\mathfrak{S} : \mathfrak{S})$

← $\mathcal{A}$ list of all free A-modules of minimal index in $\mathfrak{S}$

The modules in $\mathcal{A}$ will be defined over $\mathcal{O} = \Lambda \cap \mathcal{K}$, the multiplier ring of $\mathfrak{S}$. Suppose ν is the smallest integer such that $A^\nu = 0$.

(1) For $k = 1, \dots, \nu$, compute

$$\mathfrak{S}_k = V_k \cap \mathfrak{S}, \quad \mathfrak{T}_k = (V_{k-1} + AV_{k+1}) \quad \text{and} \quad \mathfrak{W}_k = \mathfrak{S}_k / \mathfrak{T}_k.$$

(2) For each $k = 1, \dots, \nu$, compute all free modules $\mathfrak{X}_k \subset \mathfrak{W}_k$ of minimal index as explained on p. 111. Let $\mathcal{X}_k^*$ be a list of matrices X_k^* with columns belonging to $\mathfrak{S}_k$ such that each $\mathfrak{X}_k$ is represented by exactly one X_k^*.

(3) Put $\mathcal{X}^* := \mathcal{X}_1^* \times \cdots \times \mathcal{X}_\nu^*$.

(4) For each $X^* = (X_1^*, \dots, X_\nu^*)$ in $\mathcal{X}^*$:

- compute the A-basis $X = [\, X_1 \ \dots \ X_\nu \,]$ constructed from X^*;
- for each $k = 1, \dots, \nu$, compute the $\mathcal{O}$-module $\mathfrak{Z}_k$ generated by the columns of $[\, X_1 \ \dots \ X_{k-1} \ AX_{k+1} \,]$;
- collect all modules $\mathfrak{A} = Y\mathcal{O}^n$ with A-bases Y constructed from blocks

  $$Y_k^* = X_k^* + Z_k$$

  where the columns of Z_k individually vary over a set of representatives of $\mathfrak{T}_k / \mathfrak{Z}_k$; cf. (4.19).

(5) Return the list of all modules $\mathfrak{A}$ collected in (4).

(4.32) Algorithm — All Free $\boldsymbol{A}$-Modules (General Case)

→ $\mathfrak{S}$ full module in $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$
A nilpotent matrix in $\Lambda = (\mathfrak{S} : \mathfrak{S})$

← $\mathcal{A}$ list of all free A-modules of minimal index in $\mathfrak{S}$

The modules in $\mathcal{A}$ will be defined over $\mathcal{O}_1 \oplus \cdots \oplus \mathcal{O}_s$ where $\mathcal{O}_\iota$ is the multiplier ring of $\mathfrak{S}_\iota \cap \mathfrak{S}$; see step (1).

(1) For $\iota = 1, \dots, s$:

- compute $\mathfrak{S}_\iota \cap \mathfrak{S}$ where $\mathfrak{S}_\iota$ is the image of $\mathfrak{S}$ under the projection $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}} \to \mathcal{K}_\iota^{n_\iota}$;
- compute a list $\mathcal{A}_\iota$ of all free A_ι-modules of minimal index in $\mathfrak{S}_\iota \cap \mathfrak{S}$ using algorithm (4.31).

(2) Return a list $\mathcal{A}$ consisting of all modules $\mathfrak{A} = \mathfrak{A}_1 \oplus \cdots \oplus \mathfrak{A}_s$ with $\mathfrak{A}_\iota \in \mathcal{A}_\iota$.

With a minor adjustment, algorithm (4.32) can also be used for computing a single free A-module of minimal index. When calling algorithm (4.31), it suffices to compute only one free module $\mathfrak{X}_k$ for each k in step (2). Afterwards, return $\mathfrak{A} = X\mathcal{O}^n$.

(4.33) Algorithm — Is Similar (Nilpotent Matrices)

→	A, B	nilpotent matrices belonging to a matrix order Λ
	$\mathfrak{S}$	full module in $\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$ with multiplier algebra Λ
←	τ	`true/false`
	Γ	unit of Λ satisfying $\Gamma A = B\Gamma$

(1) For $\iota = 1, \ldots, s$, check whether A_ι and B_ι have the same structure. If not, return `false`.

(2) Compute a free A-module $\mathfrak{A}$ of minimal index in $\mathfrak{S}$, basically using algorithm (4.32) as explained in the remark that followed.

(3) Compute a list $\mathcal{B}$ of all free B-modules $\mathfrak{B}$ of minimal index in $\mathfrak{S}$ using algorithm (4.32).

(4) For each $\mathfrak{B} \in \mathcal{B}$, check whether $\mathfrak{A}$ and $\mathfrak{B}$ are similar using algorithm (4.30). If so, a matrix Γ is being computed; return `true` and Γ. If no such module $\mathfrak{B}$ exists, return `false`.

The algorithms in this section especially work for $\Lambda = \mathrm{M}(n, \mathbb{Z})$. In this case, step (2) of algorithm (4.31) becomes trivial since each $\mathfrak{W}_k$ is a free $\mathbb{Z}$-module. Additionally, we can compute the block forms of A and B and perform the test based on (4.23) before dealing with A- and B-modules. If $\nu = 2$, this test is also sufficient by (4.24). Furthermore, if the matrices' structure is unitarily decreasing, we can dispense with A- and B-modules altogether.

(4.34) Algorithm — Block Form

→	A	nilpotent integer matrix
←	B	the block form of A
	C	invertible integer matrix with $CA = BC$

Suppose that $n_1 \geq \ldots \geq n_\nu$ is the structure of A. The matrix B will be of the form described in (4.21) together with (4.25).

(1) For $k = 1, \ldots, \nu$, compute an $n \times n_k$ matrix U_k representing a basis of $\mathfrak{A}_k/\mathfrak{A}_{k-1}$ where $\mathfrak{A}_k = \ker(A^k) \cap \mathbb{Z}^n$.

(2) Put $U := [\, U_1 \ \ldots \ U_\nu \,]$ and $A := U^{-1}AU$. Then A is of the form in (4.21).

(3) Compute a matrix $C = C_1 \oplus \cdots \oplus C_\nu$ as explained in the proof of (4.25).

(4) Put $B := CAC^{-1}$ and $C := CU^{-1}$. Return B and C.

(4.35) Algorithm — Is Similar (Unitarily Decreasing Structure)

➜	A, B	nilpotent integer matrices
⟵	τ	`true/false`
	C	invertible integer matrix satisfying $CA = BC$

Suppose that $n_1 \geq \ldots \geq n_\nu$ is the structure of A and B. Both matrices have to be given in block form as computed by algorithm (4.34).

(1) For $k = 2, \ldots, \nu$, check whether the diagonals of $A_{k-1,k}$ and $B_{k-1,k}$ coincide. If not, return `false`.

(2) For each $(c_1, \ldots, c_n) \in \{\pm 1\}^n$:

- define C to be the upper triangular matrix with diagonal $(c_1, \ldots, c_n)$ and variable entries c_{ij} for $j > i$;
- try to solve the system of linear equations $CA = BC$; if there is a solution, return `true` and C.

(3) Return `false`.

To complete things, let us outline how the individual algorithms add together to a function for general integer matrices.

(4.36) Algorithm — Is Similar (General Case)

➜	M, M'	integer matrices
⟵	τ	`true/false`
	C	invertible integer matrix satisfying $CA = BC$

(1) If M and M' do not have the Jordan normal form over $\mathbb{Q}$, return `false`.

(2) Compute the Jordan–Chevalley decompositions

$$M = S + N \quad \text{and} \quad M' = S' + N'.$$

Multiplying the matrices with a suitable positive integer, we may assume they are all defined over $\mathbb{Z}$.

(3) Check whether S and S' are similar using algorithm (3.17). If not, return `false`. Otherwise we now may assume $S = S'$.

(4) Compute the module $\mathfrak{S}$ corresponding to S using algorithm (1.43).

(5) Compute the multiplier algebra $\Lambda = (\mathfrak{S} : \mathfrak{S})$ using algorithm (1.45).

(6) Compute the matrices A, $B \in \Lambda$ related to M, M' using algorithm (4.28).

(7) Decide whether A and B are similar using algorithm (4.33). If not, return `false`. Otherwise obtain a matrix $\varGamma \in \Lambda^{\times}$ satisfying $\varGamma A = B\varGamma$.

(8) Compute the matrix C related to $\varGamma$ using algorithm (4.29).

(9) Return `true` and C.

5 Examples and Running Times

In this section we will illustrate the workings of our algorithm with two extensive examples, one for semisimple and one for nilpotent matrices.[1] Afterwards, we will examine the running time of the algorithm, partly in comparison to the current method in MAGMA for matrices of finite order.

Let us start with the semisimple matrices

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -4 & 0 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 0 & 1 & 4 & 0 \\ -4 & 0 & 0 & -4 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -4 & 0 \end{bmatrix}.$$

To decide whether these matrices are similar, we need to determine full modules corresponding to them and check whether these modules are equivalent. The minimal polynomial of both matrices is $X^2 + 4$, hence $2i$ is an eigenvalue. Let $\mathcal{O} = \mathbb{Z}[2i]$ and $\mathcal{K} = \mathbb{Q}(i)$. Over $\mathcal{K}$, the eigenspaces of A and B with respect to $2i$ are given by

$$\begin{aligned} \operatorname{Eig}(A, 2i) &= \mathcal{K}[1\ 2i\ 0\ 0]^{\mathrm{tr}} \qquad + \mathcal{K}[0\ 0\ 1\ 2i]^{\mathrm{tr}}, \\ \operatorname{Eig}(B, 2i) &= \mathcal{K}[4\ 0\ 2i\ -4]^{\mathrm{tr}} + \mathcal{K}[0\ 4\ -1\ -2i]^{\mathrm{tr}}. \end{aligned}$$

Therefore

$$\mathfrak{A} = \varXi\mathbb{Z}^4 = \begin{bmatrix} 1 & 2i & 0 & 0 \\ 0 & 0 & 1 & 2i \end{bmatrix}\mathbb{Z}^4 \quad \text{and} \quad \mathfrak{B} = \varUpsilon\mathbb{Z}^4 = \begin{bmatrix} 4 & 0 & 2i & -4 \\ 0 & 4 & -1 & -2i \end{bmatrix}\mathbb{Z}^4$$

are full $\mathcal{O}$-modules corresponding to A and B by (1.5). Our examination will start over the maximal order. Since $\mathcal{O}_{\mathcal{K}} = \mathbb{Z}[i]$ is a principal ideal domain, we can already say that $\mathfrak{A}_{\mathcal{K}}$ and $\mathfrak{B}_{\mathcal{K}}$ are equivalent. Concretely, we have

$$\mathfrak{A}_{\mathcal{K}} = \begin{bmatrix} 1 & i & 0 & 0 \\ 0 & 0 & 1 & i \end{bmatrix}\mathbb{Z}^4 \quad \text{and} \quad \mathfrak{B}_{\mathcal{K}} = \begin{bmatrix} 2 & 2i & 0 & 0 \\ 1 & i & 2 & 2i \end{bmatrix}\mathbb{Z}^4,$$

and it is easy to see that $\varGamma\mathfrak{A}_{\mathcal{K}} = \mathfrak{B}_{\mathcal{K}}$ for

$$\varGamma = \begin{bmatrix} 2 & 0 \\ i & 2 \end{bmatrix}.$$

But $\varGamma\mathfrak{A} \neq \mathfrak{B}$, so we must continue our examination. By (2.28) we need to check whether the multiplier ideal $\mathfrak{C} = (\mathfrak{B} : \mathfrak{A})$ is a principal right ideal of the multiplier algebra

$$\Lambda = (\mathfrak{A} : \mathfrak{A}) = \mathrm{M}(2, \mathcal{O}).$$

[1] Recall that, in general, it suffices to deal with semisimple matrices first and to examine nilpotent elements of a suitable matrix order afterwards.

The ideal $\mathfrak{C}$ is given by the $\mathbb{Z}$-basis

$$\begin{bmatrix}4 & 0\\ 0 & 0\end{bmatrix},\quad \begin{bmatrix}0 & 4\\ 0 & 0\end{bmatrix},\quad \begin{bmatrix}2i & 0\\ 3 & 0\end{bmatrix},\quad \begin{bmatrix}0 & 2i\\ 0 & 3\end{bmatrix},$$
$$\begin{bmatrix}0 & 0\\ 4 & 0\end{bmatrix},\quad \begin{bmatrix}0 & 0\\ 0 & 4\end{bmatrix},\quad \begin{bmatrix}0 & 0\\ 2i & 0\end{bmatrix},\quad \begin{bmatrix}0 & 0\\ 0 & 2i\end{bmatrix}.$$

Moreover, $\mathfrak{C}$ is invertible and satisfies $\mathfrak{C}\mathfrak{A} = \mathfrak{B}$. In order to apply (1.39), we need to check whether $\mathfrak{C}$ can be made coprime to the conductor $\mathfrak{F}$ of the extension $\Lambda \subset \Lambda_{\mathcal{K}}$ where

$$\Lambda_{\mathcal{K}} = (\mathfrak{A}_{\mathcal{K}} : \mathfrak{A}_{\mathcal{K}}) = \mathrm{M}(2, \mathcal{O}_{\mathcal{K}}).$$

Since $\mathfrak{F} = \mathrm{M}(2, \mathfrak{f})$ for $\mathfrak{f} = 2\mathcal{O}_{\mathcal{K}}$, we see that

$$\mathfrak{C} + \mathfrak{F} = \begin{bmatrix}\mathfrak{f} & \mathfrak{f}\\ \mathcal{O} & \mathcal{O}\end{bmatrix} \neq \Lambda.$$

To make $\mathfrak{C}$ coprime to $\mathfrak{F}$, we need to check whether $\mathfrak{C}_{\mathfrak{p}}$ is principal for each prime ideal of $\mathcal{O}$ containing $\mathfrak{f}$ according to (2.23). Since $\mathfrak{f}$ is prime, we only have to examine $\mathfrak{C}_{\mathfrak{p}}$ for $\mathfrak{p} = \mathfrak{f}$. To find a principal ideal generator, it suffices to search $\mathfrak{C}/\mathfrak{p}\mathfrak{C}$ for an element C satisfying $\mathfrak{C}^{-1}C \cap \mathcal{K} \not\subset \mathfrak{p}$ by (2.31) and (2.32). Such an element is given by

$$C = \begin{bmatrix}2i & 0\\ 3 & 2i\end{bmatrix}.$$

Moreover, $C^{-1}\mathfrak{C} + \mathfrak{F} = \Lambda$, so further adjustments are not necessary. Instead, we can now examine whether $C^{-1}\mathfrak{C}$ is principal by checking whether the residue class of

$$C^{-1}\mathit{\Gamma} = \begin{bmatrix}-i & 0\\ 2 & -i\end{bmatrix}$$

belongs to the image of

$$\Lambda_{\mathcal{K}}^{\times} \to (\Lambda/\mathfrak{F})^{\times}\backslash(\Lambda_{\mathcal{K}}/\mathfrak{F})^{\times}.$$

This is obviously true because $C^{-1}\mathit{\Gamma}$ is invertible.[1] Put $U = (C^{-1}\mathit{\Gamma})^{-1}$. By (1.39) we have

$$C^{-1}\mathfrak{C} = C^{-1}\mathit{\Gamma} U \Lambda = \Lambda,$$

so $\mathfrak{C} = C\Lambda$ and thus $C\mathfrak{A} = \mathfrak{B}$. It remains to determine the matrix of the homomorphism

$$\mathfrak{A} \to \mathfrak{B}, \quad \xi \mapsto C\xi$$

with respect to the $\mathbb{Z}$-bases $\mathit{\Xi} = [\xi_1 \ \ldots \ \xi_4]$ and $\mathit{\Upsilon} = [\upsilon_1 \ \ldots \ \upsilon_4]$ chosen at the beginning. Since

$$C\xi_1 = \upsilon_2 + \upsilon_3, \quad C\xi_2 = -4\upsilon_1 - 3\upsilon_4, \quad C\xi_3 = -\upsilon_1 - \upsilon_4, \quad C\xi_4 = -\upsilon_2,$$

[1] In a less fortunate case it would suffice to check whether there is a class $\overline{E} \in (\Lambda/\mathfrak{F})^{\times}$ such that $\overline{\det(EC^{-1}\mathit{\Gamma})}$ belongs to the image of $\mathcal{O}_{\mathcal{K}} \to (\mathcal{O}_{\mathcal{K}}/\mathfrak{f})^{\times}$. In practice, we could simply search $\Lambda/\mathfrak{F}$, which contains 16 elements.

it is given by

$$T = \begin{bmatrix} 0 & 1 & 1 & 0 \\ -4 & 0 & 0 & -3 \\ -1 & 0 & 0 & -1 \\ 0 & -1 & 0 & 0 \end{bmatrix}.$$

Indeed, $AT = TB$.

For the nilpotent case, consider the matrices

$$A = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ & & 0 & 0 & 2 & 0 \\ & & 0 & 0 & 0 & 2 \\ & & & & 0 & 0 \\ & & & & 0 & 0 \end{bmatrix} \qquad \text{and} \qquad B = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ & & 0 & 0 & 2 & 0 \\ & & 0 & 0 & 0 & 2 \\ & & & & 0 & 0 \\ & & & & 0 & 0 \end{bmatrix}.$$

To decide whether they are similar, we first need to determine a free A-module of minimal index in $\mathbb{Z}^6$ (notice that $A = 0 + A$ is the Jordan–Chevalley decomposition of A and that $\mathfrak{S} = \mathbb{Z}^6$ corresponds to $S = 0$). One such module is given by $\mathfrak{A} = X\mathbb{Z}^6$ where $X = [\, X_1 \; X_2 \; X_3 \,]$ consists of the blocks

$$X_3 = [\, e_5 \; e_6 \,], \qquad X_2 = AX_3, \qquad X_1 = AX_2,$$

that is,

$$X = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ & & 2 & 0 & 0 & 0 \\ & & 0 & 2 & 0 & 0 \\ & & & & 1 & 0 \\ & & & & 0 & 1 \end{bmatrix}.$$

Likewise, any free B-module of minimal index in $\mathbb{Z}^6$ is of the form $\mathfrak{B} = Y\mathbb{Z}^6$ where

$$Y = \begin{bmatrix} 2 & 0 & y_1 + 1 & y_2 + 1 & z_1 & z_2 \\ 0 & 2 & y_3 + 1 & y_4 + 1 & z_3 & z_4 \\ & & 2 & 0 & y_1 & y_2 \\ & & 0 & 2 & y_3 & y_4 \\ & & & & 1 & 0 \\ & & & & 0 & 1 \end{bmatrix}.$$

Performing elementary column operations on Y, which does not change the module $\mathfrak{B}$, each entry above the diagonal can be reduced modulo 2, that is, they can be chosen in $\{0, 1\}$. This gives us 256 modules in total. By (4.8) we need to decide whether $\mathfrak{A}$ is similar to one of them. If

$$y_1 = y_4 = 1 \qquad \text{and} \qquad y_2 = y_3 = z_1 = \cdots = z_4 = 0,$$

this will be the case, indeed. To verify this claim, we need to find an invertible matrix of the form $C = YUX^{-1}$ where

$$U = \begin{bmatrix} u_1 & u_2 & w_1 & w_2 & * & * \\ u_3 & u_4 & w_3 & w_4 & * & * \\ & & u_1 & u_2 & w_1 & w_2 \\ & & u_3 & u_4 & w_3 & w_4 \\ & & & & u_1 & u_2 \\ & & & & u_3 & u_4 \end{bmatrix} \in \mathrm{GL}(6, \mathbb{Z})$$

(see p. 103). Clearly, $\mathfrak{A}$ and $\mathfrak{B}$ both contain $2\mathbb{Z}^6$, so by (4.13) we can restrict our search to residue classes $\bar{U} \in \mathrm{GL}(6, \mathbb{Z}/2\mathbb{Z})$ which map

$$\overline{\mathfrak{C}} = (2X^{-1}\mathbb{Z}^6)/2\mathbb{Z}^6 \quad \text{onto} \quad \overline{\mathfrak{D}} = (2Y^{-1}\mathbb{Z}^6)/2\mathbb{Z}^6$$

and which can be lifted to $\mathrm{GL}(6, \mathbb{Z})$. In this example, $\overline{\mathfrak{C}} = \overline{\mathfrak{D}}$, so $\bar{U} = \bar{I}$ will do. Put $U = I$. Then

$$C = YUX^{-1} = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ & & 1 & 0 & 1 & 0 \\ & & 0 & 1 & 0 & 1 \\ & & & & 1 & 0 \\ & & & & 0 & 1 \end{bmatrix}$$

satisfies $CA = BC$.

Next, let us examine the running time of our algorithm. By the time of writing, we had only implemented the semisimple case for matrices with an irreducible minimal polynomial and the nilpotent case for integer matrices. Nevertheless, the advantages (and limitations) of our method can be illustrated well enough in these special cases. All functions were implemented in Magma (version 2.22-2) and were run on a computer with 3.16 GHz (Intel Core 2 Duo E8500) and 4 GB of memory.

To begin with, we will compare our algorithm to the current procedure in Magma, invoked by the function `IsGLZConjugate`. It works for matrices of finite order, that is, matrices A with the property $A^\nu = I$ for some ν. It is easy to see that such matrices are semisimple and that their complex eigenvalues are roots of unity. So in the case of an irreducible minimal polynomial, the matrices correspond to full modules over $\mathbb{Z}[\zeta]$ according to (1.4). As is well known, $\mathbb{Z}[\zeta]$ is the maximal order of the cyclotomic field $\mathbb{Q}(\zeta)$.[1] Hence, to decide similarity, we basically need to apply a principal ideal test in $\mathbb{Z}[\zeta]$ as explained in section 1.3.

Let us start with 4×4 matrices. In this case, the minimal polynomial can have degree 1, 2 or 4. Therefore

$$\zeta = \zeta_n \quad \text{for } n \in \{1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 8,\ 10,\ 12\}$$

[1] Cf. Neukirch (1999), p. 60, (10.2).

because

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n) = \prod_{p|n} p^{e_p - 1}(p-1) \quad \text{for } n = \prod_{p|n} p^{e_p}$$

where φ denotes Euler's totient function. Since $\mathbb{Q}(\zeta_n)$ has class number 1 for all the values given above,[1] all finitely generated modules over $\mathbb{Z}[\zeta_n]$ are free. Therefore any pair of 4×4 matrices of finite order has to be similar, provided the matrices share the same minimal polynomial.

To compare our method to the current algorithm, we randomly generated a few 4×4 matrices of finite order with entries in $\{0, \pm 1\}$. For each matrix A we chose a random element $C \in \mathrm{GL}(4, \mathbb{Z})$ and handed A and $B = CAC^{-1}$ over to the functions `IsSimilar` and `IsGLZConjugate`. In the case

$$A = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ -1 & 0 & 0 & 1 \\ 0 & -1 & 1 & 0 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix},$$

both functions needed 0.01 seconds to confirm the similarity of A and B. If

$$A = \begin{bmatrix} -1 & -1 & 0 & 0 \\ 1 & 1 & -1 & 1 \\ 1 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} -6 & -9 & -1 & 1 \\ 4 & 6 & 1 & -1 \\ -1 & -1 & 0 & -1 \\ -1 & -1 & 0 & 0 \end{bmatrix},$$

our method was even a bit slower (0.06 versus 0.01 seconds). Yet when calling `Random(GL(4,Z))` repeatedly, the entries of C, and thus of B, grow dramatically over time and, as it turns out, the function `IsGLZConjugate` seems to be quite sensitive towards this growth. For example, if

$$A = \begin{bmatrix} 1 & 0 & -1 & 0 \\ 0 & 0 & -1 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & -1 \end{bmatrix}$$

and

$$B = \begin{bmatrix} -390935360 & -458926807 & -73468877 & -178210853 \\ 167383377 & 196494855 & 31456483 & 76302942 \\ 423585561 & 497257356 & 79604400 & 193094258 \\ 251911603 & 295722847 & 47342306 & 114836105 \end{bmatrix},$$

our function confirmed the similarity of A and B in 0.06 seconds in contrast to 4 hours and 20 minutes needed by `IsGLZConjugate`.[2]

[1] Cf. Washington (1997), pp. 205–06, theorem 11.1. Notice that $\mathbb{Q}(\zeta_{2n}) = \mathbb{Q}(\zeta_n)$ if n is odd.

[2] In all fairness, Markus Kirschmer, who implemented `IsGLZConjugate`, told the author in March 2014 that the algorithm was only a byproduct of the results by Opgenorth, Plesken and Schulz (1998) and that no good performance should be expected of the function.

As a last example for finite order matrices, consider the case

$$A = \begin{bmatrix} 0 & 0 & 0 & -1 & -1 & 0 & 0 & 0 \\ -1 & -1 & 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & -1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & -1 & -1 \\ -1 & -1 & -1 & 0 & -1 & 0 & 0 & -1 \\ 0 & -1 & 0 & -1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

and

$$B = \begin{bmatrix} 0 & 0 & -1 & -1 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & -1 & -1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}.$$

Both matrices have minimal polynomial $X^2 + 1$, so they correspond to full modules over $\mathbb{Z}[i]$ and thus are similar. Our function finds a solution

$$C = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

in 0.03 seconds, whereas `IsGLZConjugate` worked for about 10 days until the computer ran out of memory.[1]

Now let us consider arbitrary matrices with irreducible minimal polynomial, that is, not necessarily of finite order. If the characteristic polynomial coincides with the minimal polynomial, the matrices correspond to ideals of an order in a number field. Therefore the performance of our algorithm will be as good (or as bad) as the respective principal ideal test.

If the characteristic polynomial is a proper power of the minimal polynomial, we will have to deal with modules in $\mathcal{K}^n$. For this case, consider the following example. Let $\mathcal{K} = \mathbb{Q}(\vartheta)$ where ϑ is a root of the polynomial $X^3 - X - 1$ and let

$$\mathcal{O} = \mathbb{Z} + 2\vartheta\mathbb{Z} + 2\vartheta^2\mathbb{Z}.$$

[1] This example was communicated to the author by Mathieu Dutour in May 2013.

At the end of section 1.7, we showed that

$$\mathfrak{A} = \begin{bmatrix} 1 & 2\vartheta & \vartheta^2 & 0 & 0 & 0 \\ 0 & 0 & \vartheta & 1 & 2\vartheta & 2\vartheta^2 \end{bmatrix} \mathbb{Z}^6$$

is an $\mathcal{O}$-module which cannot be transformed into a direct sum of ideals. By the proof of (1.9), $\mathfrak{A}$ corresponds to the 6×6 matrix

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 4 & 0 & -2 & 0 \\ 2 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 4 & 2 & 0 \end{bmatrix}$$

when regarded as a module over $\mathbb{Z}[2\vartheta]$, which is a suborder of $\mathcal{O}$. To test our algorithm, we randomly chose 100 matrices $\Gamma \in \mathrm{GL}(2, \mathcal{K})$ with entries of the form

$$\gamma_{ij} = c_1 + c_2\vartheta + c_3\vartheta^2 \quad \text{with } c_k \in \{0, \pm 1\}$$

and compared $\mathfrak{A}$ to $\Gamma\mathfrak{A}$ using the function `IsEquivalent`. On average, it took the computer 0.05 seconds to confirm the equivalence of both modules. All in all, the computation time ranged from 0.04 to 0.15 seconds.

In a next step, we took $\mathfrak{A} \oplus \mathfrak{A}$, which corresponds to the 12×12 matrix $A \oplus A$, and compared it to $\Gamma(\mathfrak{A} \oplus \mathfrak{A})$ for 100 matrices $\Gamma \in \mathrm{GL}(4, \mathcal{K})$ with entries chosen as above. This time, the computer worked for 2.39 seconds on average, with 0.99 seconds in the best and 11.94 seconds in the worst case.

Finally, consider $\mathfrak{A}' = \mathfrak{A} \oplus \mathfrak{A} \oplus \mathfrak{A}$. When dealing with this module, our algorithm will reach its limits because the number of potential tests will explode. Given $\mathfrak{A}'$ and $\mathfrak{B}$, the computer will first check whether $\mathfrak{A}'_{\mathcal{K}}$ and $\mathfrak{B}_{\mathcal{K}}$ are equivalent. This will pose no problem because this question can be reduced to a principal ideal test in $\mathcal{O}_{\mathcal{K}}$. Having found a matrix $\Gamma \in \mathrm{GL}(6, \mathcal{K})$ which satisfies $\Gamma\mathfrak{A}'_{\mathcal{K}} = \mathfrak{B}_{\mathcal{K}}$, we must decide whether $\mathfrak{C} = (\mathfrak{B} : \mathfrak{A}')$ is a principal ideal of $\Lambda = (\mathfrak{A}' : \mathfrak{A}')$. As explained at the beginning of this section, this comes down to searching $\Lambda/\mathfrak{F}$ for an element of a suitable determinant. In our example,

$$|\Lambda/\mathfrak{F}| = 2^{27} = 134{,}217{,}728,$$

so the search would be feasible, if need be. However, if choosing this approach, our method requires that $\mathfrak{C}$ is coprime to $\mathfrak{F}$. If it is not, we first have to make it coprime. Since $\mathfrak{f} = 2\mathcal{O}_{\mathcal{K}}$ is a prime ideal of $\mathcal{O}_{\mathcal{K}}$ and thus of $\mathcal{O}$ (again, see section 1.7), this requires searching for a suitable element in $\mathfrak{C}/\mathfrak{p}\mathfrak{C}$ for $\mathfrak{p} = \mathfrak{f}$. But

$$|\mathfrak{C}/\mathfrak{p}\mathfrak{C}| = 2^{81} \approx 2.42 \times 10^{24},$$

so we shouldn't expect a solution any time soon. Alternatively, we could adopt the approach of searching

$$(\Lambda_{\mathcal{K}}/\mathfrak{F})^{\times} = \mathrm{GL}(6, \mathcal{O}_{\mathcal{K}}/\mathfrak{f})$$

as explained at the end of section 3.2 (the equality above is due to $\mathfrak{A}'_{\mathcal{K}} = \mathcal{O}^6_{\mathcal{K}}$). Then there is no need to ensure that $\mathfrak{C}$ is coprime to $\mathfrak{F}$. Yet $\mathcal{O}_{\mathcal{K}}/\mathfrak{f}$ is a field with 8 elements, so

$$|\mathrm{GL}(6, \mathcal{O}_{\mathcal{K}}/\mathfrak{f})| = (8^6 - 1)(8^6 - 8)\cdots(8^6 - 8^5) \approx 2.79 \times 10^{32},$$

rendering this approach even more futile.

To conclude our examination, let us evaluate the running times for some nilpotent matrices, with the main focus on unitarily decreasing structures. Let us begin with the simplest unitarily decreasing structure, namely

$$n_1 = n_2 = \cdots = n_\nu = 1.$$

In this case we can find matrices of any size n because $n = n_1 + \cdots + n_\nu$. For each given n, we generated 1,000 matrices A in block form with structure $n_1 = \cdots = n_\nu = 1$ and entries randomly chosen in $\{0, 1, \ldots, 9\}$. For each A, we generated a matrix

$$C = \begin{bmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{bmatrix}$$

with entries above the diagonal randomly chosen in $\{0, \pm 1\}$. Then we compared A to CAC^{-1}. Table 1 contains the minimal, maximal and average running times.

n	avg.	min.	max.
2	0.001	0.000	0.010
3	0.001	0.000	0.010
4	0.002	0.000	0.010
5	0.003	0.000	0.010
6	0.004	0.000	0.010
7	0.006	0.000	0.010
8	0.009	0.000	0.020
9	0.013	0.010	0.020
10	0.020	0.010	0.030
11	0.033	0.020	0.050
12	0.056	0.030	0.100
13	0.106	0.050	0.190
14	0.201	0.060	0.410
15	0.394	0.110	0.880
16	0.693	0.140	1.680
17	1.811	0.280	6.490
18	4.877	0.540	15.640
19	15.323	0.800	57.680
20	37.826	2.770	149.420
21	84.869	9.330	437.650
22	185.767	13.300	815.680

Table 1

Next, consider the other extreme case in the unitarily decreasing context, that is, structures of the form

$$n_1 > n_1 - 1 > \ldots > 2 > 1,$$

The possible sizes of matrices with such a structure are given by

$$n = \frac{n_1(n_1+1)}{2} \qquad (n_1 > 1).$$

Again we generated 1,000 pairs of matrices with structure $n_1 > \ldots > 2 > 1$ as described before and handed them over to our algorithm. Table 2 contains the minimal, maximal and average running times in these cases.

n	avg.	min.	max.
3	0.001	0.000	0.010
6	0.002	0.000	0.010
10	0.007	0.000	0.010
15	0.056	0.030	0.100
21	1.671	0.570	4.010
28	119.550	21.840	1014.420

Table 2

To conclude this section, let us consider the matrices

$$A = \begin{bmatrix} 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 4 & 0 & 0 \\ & & 0 & 0 & 6 & 0 \\ & & 0 & 0 & 0 & 8 \\ & & & & 0 & 0 \\ & & & & 0 & 0 \end{bmatrix} \qquad \text{and} \qquad B = \begin{bmatrix} 0 & 0 & 2 & 2 & 6 & -6 \\ 0 & 0 & 0 & 4 & -4 & 0 \\ & & 0 & 0 & 6 & 2 \\ & & 0 & 0 & 0 & 8 \\ & & & & 0 & 0 \\ & & & & 0 & 0 \end{bmatrix}$$

whose structure is not unitarily decreasing, as they consist solely of 2×2 blocks. In this rather innocent looking example our algorithm needs more than 10 hours to find a matrix

$$C = \begin{bmatrix} 1 & 1 & 9 & 1 & -5 & 7 \\ 0 & 1 & 16 & 4 & -28 & -28 \\ & & 1 & 1 & -1 & -5 \\ & & 0 & 1 & 25 & 9 \\ & & & & 1 & 1 \\ & & & & 0 & 1 \end{bmatrix}$$

which satisfies $CA = BC$. Yet if we compare A to the matrix

$$B' = \begin{bmatrix} 0 & 0 & 2 & 2 & 4 & 2 \\ 0 & 0 & 0 & 4 & -4 & -8 \\ & & 0 & 0 & 6 & 2 \\ & & 0 & 0 & 0 & 8 \\ & & & & 0 & 0 \\ & & & & 0 & 0 \end{bmatrix},$$

it takes merely 0.01 seconds to compute a solution

$$C' = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 \\ & & 1 & 1 & 0 & 0 \\ & & 0 & 1 & 1 & 1 \\ & & & & 1 & 1 \\ & & & & 0 & 1 \end{bmatrix}.$$

Final Remarks

To conclude this work, let us address some potential starting points for future research, which could lead to an improvement of our algorithm. In the semisimple case, it would be worthwhile to solve the following problems.

- Come to a better understanding of full modules over nonmaximal orders. This should include necessary and sufficient criteria for when a module can be transformed into a direct sum of ideals.

- Find an efficient way to decide whether an invertible right ideal $\mathfrak{C}$ can be made coprime to the conductor. To accomplish this, it would suffice to find an efficient way for deciding whether $\mathfrak{C}_\mathfrak{p}$ is principal for each $\mathfrak{p} \supset \mathfrak{f}$.

- Improve the principal ideal test for multiplier ideals $\mathfrak{C}$. Given that $\mathfrak{C}$ is coprime to $\mathfrak{F}$, this can be solved by computing the group $\det((\Lambda/\mathfrak{F})^\times)$ and providing an element of a suitable determinant.

Up to now, our methods for solving the second and third problem have exponential complexity, hence it would be desirable to find a better algorithm.

In the nilpotent case, our method requires doubly exponential time in general because the number of A-modules and the number of steps in the similarity test can grow exponentially fast. The only exception are integer matrices with unitarily decreasing structure, where the algorithm lies in between polynomial and exponential time. Because of the difficulties in the general case, it might be the best to develop a completely new approach for nilpotent matrices.

Bibliography

Applegate, Harry; Onishi, Hironori: Continued fractions and the conjugacy problem in $\mathrm{SL}_2(\mathbb{Z})$. Comm. Algebra 9 (1981), no. 11, 1121–1130.

Applegate, Harry; Onishi, Hironori: The similarity problem for 3×3 integer matrices. Linear Algebra Appl. 42 (1982), 159–174.

Behn, A.; Van der Merwe, A. B.: An algorithmic version of the theorem by Latimer and MacDuffee for 2×2 integral matrices. Linear Algebra Appl. 346 (2002), 1–14.

Borevich, Zenon; Shafarevich, Igor: Number Theory. Academic Press, 1966.

Bosma, Wieb; Cannon, John (eds.): Handbook of Magma Functions. Version 2.21, 2014.

Buchmann, Johannes: On principal ideal testing in algebraic number fields. Journal of Symbolic Computation 4(1):11–19, 1987

Cohen, Henri; Diaz y Diaz, Francisco; Olivier, Michel: Subexponential algorithms for class group and unit computations. J. Symbolic Comput. 24 (1997), no. 3-4, 433–441.

Cohen, Henri: Advanced Topics in Computational Number Theory. Springer, 2000.

Cox, David: Primes of the form $x^2 + ny^2$. Wiley, 1989.

Eisenbud, David: Commutative Algebra with a View Toward Algebraic Geometry. Springer, 1995.

Grunewald, Fritz: Solution of the conjugacy problem in certain arithmetic groups. Appeared in Word Problems II, North-Holland, 1980.

Hess, Florian; Pauli, Sebastian; Pohst, Michael: Computing the multiplicative group of residue class rings. Math. Comp. 72 (2003), no. 243, 1531–1548.

Jantzen, Jens; Schwermer, Joachim: Algebra. Springer, 2006.

Klüners, Jürgen; Pauli, Sebastian: Computing Residue Class Rings and Picard Groups of Orders. J. Algebra 292 (2005), 47–64.

Lam, Y. T.: A First Course in Noncommutative Rings. Second edition, Springer, 2001.

Latimer, Claiborne; MacDuffee, C. C.: A correspondence between classes of ideals and classes of matrices. Ann. of Math. (2) 34 (1933), no. 2, 313–316.

Liehl, Bernhard: On the group SL_2 over orders of arithmetic type. J. Reine Angew. Math. 323 (1981), 153–171.

Narkiewicz, Władisław: Elementary and Analytic Theory of Algebraic Numbers. Third edition, Springer, 2004.

Neukirch, Jürgen: Algebraic Number Theory. English translation, Springer, 1999.

Opgenorth, J.; Plesken, W.; Schulz, T.: Crystallographic algorithms and tables. Acta Cryst. Sect. A 54 (1998), no. 5, 517–531.

Pohst, Michael; Zassenhaus, Hans: Algorithmic algebraic number theory. Cambridge University Press, 1989.

Reiner, Irving: Maximal Orders. Academic Press, 1975.

Sarkisjan, R. A.: The conjugacy problem for collections of integral matrices. English translation, Mat. Zametki 25 (1979), no. 6, 811–824, 956.

Swan, Richard: Generators and Relations for certain Special Linear Groups. Advances in Mathematics 6 (1971), 1–77.

Taussky, Olga: On a theorem of Latimer and MacDuffee. Canadian J. Math. 1 (1949), 300–302.

Vaseršteĭn, Leonid: On the group SL_2 over Dedekind rings of arithmetic type. English translation, Math. USSR Sbornik Vol. 18 (1972), No. 2, 321–332.

Washington, Lawrence: Introduction to Cyclotomic Fields. Second edition, Springer, 1997.

List of Symbols

$(\mathfrak{B} : \mathfrak{A})$	multiplier ideal, p. 28
$[\,\Xi_1\ \dots\ \Xi_\nu\,]$	A-basis over $\mathbb{Z}$, p. 90
$[\,X_1\ \dots\ X_\nu\,]$	A-basis of a free A-module, p. 94
$[\Gamma + \mathfrak{F}]$	right coset of $\Gamma + \mathfrak{F}$ in $(\Lambda/\mathfrak{F})^\times \backslash (\Lambda_{\boldsymbol{\mathcal{K}}}/\mathfrak{F})^\times$
$\mathfrak{a}$, $\mathfrak{b}$	full ideals
$\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{S}$	full modules
$\mathfrak{A}_{\boldsymbol{\mathcal{K}}}$	$\mathfrak{A}\mathcal{O}_{\boldsymbol{\mathcal{K}}}$
$\mathcal{M}$	algebra of all matrices as in (4.9), p. 101
$\boldsymbol{n} \cdot \boldsymbol{d}$	scalar product of multi-indices, p. 21
$\mathfrak{C}^{-1}$	largest inverse of an ideal, p. 59
χ	characteristic polynomial of a matrix
det	determinant, p. 33
$\mathfrak{F}$, $\mathfrak{f}$	conductor, p. 36
Γ	typically an element of $\mathrm{GL}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$
$\mathrm{GL}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$	$\bigoplus_{\iota=1}^{s} \mathrm{GL}(n_\iota, \mathcal{K}_\iota)$, p. 19
$\mathcal{K}$, $\mathcal{K}_\iota$	number field
$\boldsymbol{\mathcal{K}}$	direct sum of number fields, p. 17
$\boldsymbol{\mathcal{K}}^{\boldsymbol{n}}$	$\mathcal{K}_1^{n_1} \oplus \cdots \oplus \mathcal{K}_s^{n_s}$, p. 18
Λ, Λ_ι	matrix order, p. 28
$\Lambda_{\mathcal{K}}$, $\Lambda_{\boldsymbol{\mathcal{K}}}$	maximal matrix order, p. 28
N	norm, p. 33
$\mathrm{M}(\boldsymbol{n}, \boldsymbol{\mathcal{K}})$	$\bigoplus_{\iota=1}^{s} \mathrm{M}(n_\iota, \mathcal{K}_\iota)$, p. 19
μ	minimal polynomial of a matrix
$\boldsymbol{n}$, $\boldsymbol{d}$	multi-indices
$\lvert\boldsymbol{n}\rvert$	absolute value of a multi-index, p. 21

$\mathcal{O}$, $\mathcal{O}_\iota$	order, p. 17
$\mathcal{O}_\mathcal{K}$, $\mathcal{O}_{\boldsymbol{\mathcal{K}}}$	maximal order, p. 17
$\mathcal{O}_\mathfrak{p}$, $\Lambda_\mathfrak{p}$, $\mathfrak{c}_\mathfrak{p}$, $\mathfrak{C}_\mathfrak{p}$, $\ldots$	localization at $S_\mathfrak{p}$, p. 49
$\sim$	equivalence of modules, p. 19
$\simeq$	isomorphy of structures
$\mathrm{SL}(\Lambda_{\boldsymbol{\mathcal{K}}})$, $\mathrm{SL}(\Lambda_{\boldsymbol{\mathcal{K}}}/\mathfrak{F})$	group of matrices with determinant 1, p. 72
$\mathfrak{S}_k$	$V_k \cap \mathfrak{S}$, p. 106
$\mathfrak{T}_k$	$(V_{k-1} + AV_{k+1}) \cap \mathfrak{S}$, p. 106
$\mathcal{U}$	group of all matrices as in (4.9), p. 99
$\mathfrak{W}_k$	$\mathfrak{S}_k/\mathfrak{T}_k$, p. 106
$\mathit{\Xi}$, $\mathit{\Upsilon}$, $\mathit{\Omega}$	$\mathbb{Z}$-bases of full modules
$n_1 \geq \ldots \geq n_\nu$	structure of a nilpotent matrix
$S_\mathfrak{p}$	$(\mathcal{O} \smallsetminus \mathfrak{p}) \cap \boldsymbol{\mathcal{K}}^\times$, p. 49
$v_\mathfrak{p}$	$\mathfrak{p}$-adic valuation
V_k	kernel of A^k, p. 106
W_k	$V_k/(V_{k-1} + AV_{k+1})$, p. 106
X_k^*	subblock of an A-basis X, p. 105

Index