Wedge product matrices and applications

Yao Ming Brian Chan

Supervisor: Arun Ram

October 3, 2022

University of Melbourne

School of Mathematics and Statistics

A thesis submitted for the partial fulfilment of the Masters of Science (Mathematics and Statistics) degree

Contents

Acknowledgements

First and foremost, I would like to thank my family — my parents Andrew and Irene, my sister Taylor and my brother Harrison — for their constant support and for fostering a productive and comfortable environment, which was conducive to the write up of this thesis and the intense study required for the MSc degree.

I would like to thank my friends from high school — Aneesh, Ashwin, Eren, Ethan, Jono, Josh and Liam — for keeping in contact with me for the past few years and for providing encouragement with regards to my studies.

I would like to thank my friends in mathematics — Adam, Bowan, Rodney, Paul, Tom and Will — for the many interesting and stimulating mathematical discussions we had and for motivating me throughout the MSc degree.

I would like to thank Alex Ghitza, Anthony Mays and Dan Murfet for taking their time to read earlier versions of this thesis and providing useful feedback to improve the structure of the thesis.

Lastly, I would like to thank my supervisor Arun Ram for expertly guiding me throughout the long process of doing mathematical research and writing this thesis. His versatility as mathematician and integrity as a person is inspiring and has left a deep and enduring impression on me — one that I will aspire to as I progress in life.

Chapter 1

Introduction

The main goal of this thesis is to study *wedge product matrices*, a particular generalisation of the determinant over a commutative ring R. To motivate the idea behind wedge product matrices, we will begin with a brief description of the construction of the determinant in a commutative ring.

Informally, if R is a commutative ring and $A \in M_{n\times n}(R)$ (a $n \times n$ matrix with elements in R), then its determinant $\det(A)$ is computed by taking the wedge product of all n columns/rows of A. A natural question which stems from this is: what happens when one takes the wedge product of only k columns/rows of A, where $k \in \{1, \ldots, n-1\}$? By taking all possible wedge products of k columns/rows from A, one obtains the $\binom{n}{k} \times \binom{n}{k}$ wedge product matrix $\Lambda^k(A)$, a generalisation of the determinant because $\Lambda^n(A)$ is the 1×1 matrix with the single entry $\det(A)$. As such, wedge product matrices share many of the useful properties of determinants.

It should be emphasised here that wedge product matrices are commonly known as *compound matrices* (see [Mul98] for instance). I decided to call them "wedge product matrices" in order to convey the idea behind its definition.

To start the thesis, chapter 2 is dedicated to defining wedge product matrices and proving some of their properties. Our first application of wedge product matrices is the generalisation of familiar linear algebra identities, first exhibited by the extension of Laplace expansion along a single row/column to Laplace expansion along multiple rows/columns.

In chapter 3, we introduce the k^{th} adjugate matrix $\Upsilon^{n-k}(A)$ which satisfies the property $\Lambda^k(A)\Upsilon^{n-k}(A) = \Upsilon^{n-k}(A)\Lambda^k(A) = \det(A)I_{\binom{n}{k}}$ where $A \in M_{n\times n}(R)$, $k \in \{1, \ldots, n-1\}$ and $I_{\binom{n}{k}}$ is the $\binom{n}{k} \times \binom{n}{k}$ identity matrix. In this manner, we generalise the construction of the adjugate matrix, which is commonly used to compute the inverse of invertible matrices (see [Rot03, Page 766-767]). We then apply adjugate matrices to analyse quasideterminants (see [GR91, Pages 99-101]) and generalise the eigenvector-eigenvalue identity in [DPTZ20, Theorem 1].

When presented with a matrix orbit, one of the fundamental questions is to find a

representative of the matrix orbit. One way of doing this is to look for invariants — quantities which do not change across the matrix orbit. It turns out that computing wedge product matrices is an effective way of finding invariants. In this thesis, we demonstrate this idea with two different matrix orbits. In chapter 4, we analyse the two-sided orbit space $GL_m(R)\backslash M_{m\times n}(R)/GL_n(R)$, where R is a commutative ring and in chapter 5, we investigate the matrix orbit space $\Gamma_\infty(3)\backslash\Gamma(3)$, stemming from the principal congruence subgroups $\Gamma(3)$ and $\Gamma_\infty(3)$. This particular matrix orbit appeared in a minimal parabolic Eisenstein series defined in [BH86, p. 486].

Our primary method of constructing matrix representatives for the orbits in chapter 4 and chapter 5 is termed *Steinberg reduction*. Steinberg used this technique in [Ste67, §8] to provide an alternative characterisation of the Bruhat decomposition of a Chevalley group. The specific matrices we use in Steinberg reduction are similar to those in [Ste67, Lemma 43, Part (c)]. The general purpose of Steinberg reduction in this thesis is to reduce a matrix $A \in M_{m\times n}(\mathfrak{o})$ into an upper triangular form where $\mathfrak{o}$ is a PID. This is similar to what Steinberg did to prove the Bruhat decomposition in [Ste67, Theorem 15].

A particular feature of the thesis is the wealth of examples accompanying the major theorems. This was intended to make the thesis more accessible to students with a background in linear algebra. Examples also assist with understanding the main theorems of the thesis.

Chapter 2

Determinants

2.1 Definition of wedge product matrices

We will begin the thesis with Definition 2.1.3 — the definition of a wedge product matrix.

Definition 2.1.1. Let $k, n \in \mathbb{Z}_{>0}$ such that $k \leq n$. Then, we define

$$T_{\binom{n}{k}} = \{L \subseteq \{1, 2, \ldots, n\} \mid |L| = k\}.$$

where $|L|$ denotes the cardinality of the set L. The set $T_{\binom{n}{k}}$ has cardinality $|T_{\binom{n}{k}}| = \binom{n}{k} = \frac{n!}{k!(n-k)!}$.

Let R be a commutative ring. If $n \in \mathbb{Z}_{>0}$, then R^n is a free R-module, with basis $\{e_1, \ldots, e_n\}$ where $e_i \in R^n$ is a $n \times 1$ matrix with a 1 in the i^{th} entry and zeros elsewhere.

If $I = \{i_1, \ldots, i_k\} \in T_{\binom{n}{k}}$ then let $e_I = e_{i_1} \wedge \cdots \wedge e_{i_k}$ where $\wedge$ denotes the wedge product; i.e. if $x, y \in R^n$, then $x \wedge y = -(y \wedge x)$. This property of the wedge product is termed anticommutativity. The reference [Rot03, Section 9.8] provides a detailed discussion of the exterior algebra and the wedge product.

Definition 2.1.2. Let R be a commutative ring, $k \in \mathbb{Z}_{\geq 0}$ and $n \in \mathbb{Z}_{>0}$. Then, the k^{th} **exterior power** of R^n, denoted by $\bigwedge^k(R^n)$ is the free R-module with basis

$$\{e_{i_1} \wedge \cdots \wedge e_{i_k} \mid 1 \leq i_1 < \cdots < i_n \leq n\} = \{e_L \mid L \in T_{\binom{n}{k}}\}.$$

For $k = 0$, we define $\bigwedge^0(R^k) = R$.

Definition 2.1.2 is justified by [Rot03, Theorem 9.140], where it is proved that if M is a R-module of rank $n \in \mathbb{Z}_{>0}$ and $k \in \mathbb{Z}_{>0}$, then $\bigwedge^k(M)$ is a free R-module of rank $\binom{n}{k}$. When $k > n$, $\bigwedge^k(R^n) = 0$, due to the anticommutativity of the wedge product.

Definition 2.1.3. Let R be a commutative ring and $A \in M_{n\times n}(R)$ so that $A = (a_{ij})$. Then, the **determinant** of A, denoted $\det(A)$, is the unique element of R determined by

$$\Big(\sum_{i=1}^{n} a_{i1}e_i\Big) \wedge \Big(\sum_{i=1}^{n} a_{i2}e_i\Big) \wedge \cdots \wedge \Big(\sum_{i=1}^{n} a_{in}e_i\Big) = (\det(A))(e_1 \wedge \cdots \wedge e_n).$$

Let $A \in M_{m\times n}(R)$ and $k \in \mathbb{Z}_{>0}$. The k^{th} **wedge product matrix** $\Lambda^k(A)$ is the $\binom{m}{k} \times \binom{n}{k}$ matrix determined by the equations

$$\Lambda^k(A) = \Big(\Lambda^k(A)_{I,J}\Big)_{I\in T_{\binom{m}{k}}, J\in T_{\binom{n}{k}}}$$

and if $J = \{j_1, \ldots, j_k\} \in T_{\binom{n}{k}}$ then

$$Ae_J = Ae_{j_1} \wedge \cdots \wedge Ae_{j_k} = \sum_{I\in T_{\binom{m}{k}}} (\Lambda^k(A))_{I,J}e_I.$$

If $k > \min(m, n)$ then $\Lambda^k(A)$ is the 1×1 matrix (0).

The k^{th} wedge product matrix $\Lambda^k(A)$ can be thought of as a generalisation of the determinant definition in two different ways. Firstly, $\Lambda^k(A)$ is defined for non-square matrices and secondly, $\Lambda^k(A)$ is constructed from the wedge product of some (but not all) columns of the matrix A. The rows and columns of $\Lambda^k(A)$ are indexed by sets in $T_{\binom{m}{k}}$ and $T_{\binom{n}{k}}$ respectively, which are usually arranged with the **lexicographical/dictionary order**.

We have used the symbol Λ^k to refer to a wedge product matrix and the symbol $\bigwedge^k$ to refer to the exterior power of a R-module, despite the fact that definitions 2.1.2 and 2.1.3 use the same functor.

Our first endeavour is to show that the entries of $\Lambda^k(A)$ coincide with the determinants of the $k \times k$ minors of A. The result we require for this is the complete expansion of the determinant.

Definition 2.1.4. Let $n \in \mathbb{Z}_{>0}$ and $\sigma \in S_n$ be a permutation. Then, the **sign** of σ, denoted $sgn(\sigma)$, is an element of $\{-1, 1\}$ which satisfies

$$e_{\sigma(1)} \wedge \cdots \wedge e_{\sigma(n)} = sgn(\sigma)(e_1 \wedge \cdots \wedge e_n).$$

Lemma 2.1.1. *Let R be a commutative ring and $A = (a_{ij}) \in M_{n\times n}(R)$. Then,*

$$\det(A) = \sum_{\sigma\in S_n} sgn(\sigma)a_{\sigma(1),1}a_{\sigma(2),2}\ldots a_{\sigma(n),n}$$

where $sgn(\sigma)$ is the sign of the permutation $\sigma \in S_n$.

Proof. Assume that R is a commutative ring and $A = (a_{ij}) \in M_{n\times n}(R)$. From Definition 2.1.3, we have

$$\begin{aligned}\det(A) &= \sum_{j_1} a_{j_1,1}e_{j_1} \wedge \cdots \wedge \sum_{j_n} a_{j_n,n}e_{j_n} \\ &= \sum_{j_1,\ldots,j_n} a_{j_1,1}a_{j_2,2}\ldots a_{j_n,n}(e_{j_1} \wedge \cdots \wedge e_{j_n}) \\ &= \sum_{\sigma\in S_n} a_{\sigma(1),1}a_{\sigma(2),2}\ldots a_{\sigma(n),n}(e_{\sigma(1)} \wedge \cdots \wedge e_{\sigma(n)})\end{aligned}$$

where $\sigma \in S_n$ is the permutation given by $\sigma(k) = j_k$ for $k \in \{1,\ldots,n\}$. Rearranging the basis $e_{\sigma(1)} \wedge \cdots \wedge e_{\sigma(n)}$ gives

$$\det(A) = \sum_{\sigma\in S_n} sgn(\sigma)a_{\sigma(1),1}a_{\sigma(2),2}\ldots a_{\sigma(n),n}(e_1 \wedge \cdots \wedge e_n).$$

□

Theorem 2.1.2. *Let R be a commutative ring, $A = (a_{ij}) \in M_{m\times n}(R)$ and let $k \in \{1,\ldots,\min(m,n)\}$. Let $J \in T_{\binom{m}{k}}$, $K \in T_{\binom{n}{k}}$ and let $A_{J,K}$ be the $k \times k$ matrix formed from the rows indexed by J and the columns indexed by K. Then,*

$$\det(A_{J,K}) = (\Lambda^k(A))_{J,K}.$$

Proof. Assume that $A = (a_{ij}) \in M_{m\times n}(R)$ and $k \in \{1,\ldots,\min(m,n)\}$. Assume that $I = \{i_1, i_2, \ldots, i_k\} \in T_{\binom{n}{k}}$. Then, the wedge product of columns $i_1, i_2, \ldots, i_k$ of A is by Definition 2.1.3

$$\begin{aligned}\sum_{L\in T_{\binom{m}{k}}} (\Lambda^k(A))_{L,I}e_L &= Ae_{i_1} \wedge \cdots \wedge Ae_{i_k} \\ &= \sum_{j_1} a_{j_1,i_1}e_{j_1} \wedge \cdots \wedge \sum_{j_k} a_{j_k,i_k}e_{j_k} \\ &= \sum_{j_1,\ldots,j_k} a_{j_1,i_1}a_{j_2,i_2}\ldots a_{j_k,i_k}(e_{j_1} \wedge \cdots \wedge e_{j_k}).\end{aligned}$$

Let $\sigma \in S_k$ be a permutation which maps the sequence $(j_1,\ldots,j_k)$ to $(j_{\sigma(1)},\ldots,j_{\sigma(k)})$, where $j_{\sigma(1)} < \cdots < j_{\sigma(k)}$. Then, rewrite the sum over $j_1,\ldots,j_k$ as a sum over all permutations in S_k to get

$$Ae_{i_1} \wedge \cdots \wedge Ae_{i_k} = \sum_{\sigma\in S_k} a_{j_{\sigma(1)},i_1}a_{j_{\sigma(2)},i_2}\ldots a_{j_{\sigma(k)},i_k}(e_{j_1} \wedge \cdots \wedge e_{j_k}).$$

By rearranging $e_{j_1} \wedge \cdots \wedge e_{j_k}$, we find that

$$Ae_{i_1} \wedge \cdots \wedge Ae_{i_k} = \sum_{\sigma\in S_k} sgn(\sigma)a_{j_{\sigma(1)},i_1}a_{j_{\sigma(2)},i_2}\ldots a_{j_{\sigma(k)},i_k}(e_{j_{\sigma(1)}} \wedge \cdots \wedge e_{j_{\sigma(k)}}).$$

Applying Lemma 2.1.1 to the right hand side reveals that

$$\sum_{L\in T_{\binom{m}{k}}} (\Lambda^k(A))_{L,I} e_L = Ae_{i_1} \wedge \cdots \wedge Ae_{i_k} = \sum_{L\in T_{\binom{m}{k}}} \det(A_{L,I}) e_L. \tag{2.1}$$

Comparing the coefficients of e_L on both sides of equation (2.1) gives $\det(A_{L,I}) = (\Lambda^k(A))_{L,I}$. □

Example 2.1.5. Let $R = \mathbb{Z}$ and

$$A = \begin{pmatrix} 2 & -1 & 1 \\ 0 & 3 & -4 \\ 7 & 6 & -3 \end{pmatrix}.$$

We want to take the wedge product of the first two columns of A. In Definition 2.1.3,

1. I is the set $\{1, 2\}$ (Select columns 1 and 2)

2. L represents all possible selections of two rows from the available three rows: $\{1, 2\}, \{1, 3\}$ and $\{2, 3\}$.

3. The possible values of e_L are therefore: $e_{\{1,2\}} = e_1 \wedge e_2, e_{\{1,3\}} = e_1 \wedge e_3$ and $e_{\{2,3\}} = e_2 \wedge e_3$.

We find from Theorem 2.1.2 that

$$\begin{aligned} Ae_1 \wedge Ae_2 &= \sum_{L\in T_{\binom{3}{2}}} (\Lambda^2(A))_{L,I} e_L = \sum_{L\in T_{\binom{3}{2}}} (\Lambda^2(A))_{L,\{1,2\}} e_L \\ &= (\Lambda^2(A))_{\{1,2\},\{1,2\}} e_{\{1,2\}} + (\Lambda^2(A))_{\{1,3\},\{1,2\}} e_{\{1,3\}} + (\Lambda^2(A))_{\{2,3\},\{1,2\}} e_{\{2,3\}} \\ &= \det(A_{\{1,2\},\{1,2\}})(e_1 \wedge e_2) + \det(A_{\{1,3\},\{1,2\}})(e_1 \wedge e_3) + \det(A_{\{2,3\},\{1,2\}})(e_2 \wedge e_3) \\ &= \begin{vmatrix} 2 & -1 \\ 0 & 3 \end{vmatrix} (e_1 \wedge e_2) + \begin{vmatrix} 2 & -1 \\ 7 & 6 \end{vmatrix} (e_1 \wedge e_3) + \begin{vmatrix} 0 & 3 \\ 7 & 6 \end{vmatrix} (e_2 \wedge e_3) \\ &= 6(e_1 \wedge e_2) + 19(e_1 \wedge e_3) - 21(e_2 \wedge e_3). \end{aligned}$$

We can verify this calculation by doing the wedge product calculation directly:

$$\begin{aligned} Ae_1 \wedge Ae_2 &= (2e_1 + 7e_3) \wedge (-1e_1 + 3e_2 + 6e_3) \\ &= (6 - 0)(e_1 \wedge e_2) + (12 - (-7))(e_1 \wedge e_3) + (0 - 21)(e_2 \wedge e_3) \\ &= 6(e_1 \wedge e_2) + 19(e_1 \wedge e_3) - 21(e_2 \wedge e_3). \end{aligned}$$

$Ae_1 \wedge Ae_2$ comprises the first column of

$$\begin{pmatrix} 6 & -8 & 1 \\ 19 & -13 & -3 \\ -21 & 28 & 15 \end{pmatrix} = \begin{pmatrix} (\Lambda^2(A))_{\{1,2\},\{1,2\}} & (\Lambda^2(A))_{\{1,2\},\{1,3\}} & (\Lambda^2(A))_{\{1,2\},\{2,3\}} \\ (\Lambda^2(A))_{\{1,3\},\{1,2\}} & (\Lambda^2(A))_{\{1,3\},\{1,3\}} & (\Lambda^2(A))_{\{1,3\},\{2,3\}} \\ (\Lambda^2(A))_{\{2,3\},\{1,2\}} & (\Lambda^2(A))_{\{2,3\},\{1,3\}} & (\Lambda^2(A))_{\{2,3\},\{2,3\}} \end{pmatrix}.$$

2.2 Properties of wedge product matrices

As with any newly defined mathematical object, we will now analyse some of the basic properties of wedge product matrices.

Proposition 2.2.1. *Let R be a commutative ring, $A \in M_{m\times n}(R)$ and $B \in M_{n\times n}(R)$. Let $I_n \in M_{n\times n}(R)$ denote the $n \times n$ identity matrix. Then,*

(a) $\Lambda^n(B) = (\det(B))$ (a 1×1 matrix).

(b) $\Lambda^1(B) = B$ (a $n \times n$ matrix).

(c) If $k \in \{1, \dots, n\}$ then $\Lambda^k(I_n) = I_{\binom{n}{k}}$.

(d) If $k \in \{1, \dots, \min(m, n)\}$ then $\Lambda^k(A^T) = (\Lambda^k(A))^T$.

Proof. Assume that R is a commutative ring, $A \in M_{m\times n}(R)$ and $B \in M_{n\times n}(R)$.

(a): If $k = n$ in Definition 2.1.3 then the only element of $T_{\binom{n}{n}}$ is $\{1, 2, \dots, n\}$ and

$$Be_{\{1,2,\dots,n\}} = Be_1 \wedge Be_2 \wedge \cdots \wedge Be_n = \det(B)(e_1 \wedge \cdots \wedge e_n).$$

Therefore, if $B \in M_{n\times n}(R)$, then $\Lambda^n(B) = (\det(B))$.

(b): If $k = 1$ in Definition 2.1.3 then $T_{\binom{n}{1}} = \{\{i\} \mid i \in \{1, \dots, n\}\}$. We will treat each of these sets in $T_{\binom{n}{1}}$ as integers. Fix $i \in \{1, \dots, n\}$. Then,

$$Be_i = \sum_{L\in T_{\binom{n}{1}}} (\Lambda^1(B))_{L,i} e_L = \sum_{j=1}^{n} (\Lambda^1(B))_{j,i} e_j.$$

The LHS is the i^{th} column of B, whereas the RHS is the i^{th} column of $\Lambda^1(B)$. So, $\Lambda^1(B) = B$.

(c): Fix $I = \{i_1, \dots, i_k\} \in T_{\binom{n}{k}}$. Then

$$e_I = e_{i_1} \wedge \cdots \wedge e_{i_k} = \sum_{L\in T_{\binom{n}{k}}} (\Lambda^k(I_n))_{L,I} e_L.$$

Equality holds when $(\Lambda^k(I_n))_{L,I} = \delta_{L,I}$, where δ denotes the Kronecker delta. Thus, if $k \leq n$ then $\Lambda^k(I_n) = I_{\binom{n}{k}}$.

(d): Assume that $L \in T_{\binom{m}{k}}$ and $M \in T_{\binom{n}{k}}$. Using Theorem 2.1.2, we have

$$\begin{aligned}\left((\Lambda^k(A))^T\right)_{M,L} &= (\Lambda^k(A))_{L,M} \\ &= \det(A_{L,M}) \\ &= \det((A^T)_{M,L}) = (\Lambda^k(A^T))_{M,L}.\end{aligned}$$

So, $\Lambda^k(A^T) = (\Lambda^k(A))^T$. □

The most critical property of wedge product matrices is that just like the determinant, wedge product matrices are multiplicative.

Theorem 2.2.2 (Generalised Cauchy-Binet Formula)**.** *Let R be a commutative ring. Let $A \in M_{m\times n}(R)$ and $B \in M_{n\times p}(R)$. Let $k \in \{1, 2, \ldots, \min(m, n, p)\}$. Then,*

$$\Lambda^k(AB) = \Lambda^k(A)\Lambda^k(B).$$

Proof. Assume that R is a commutative ring. Assume that $A \in M_{m\times n}(R)$ and $B \in M_{n\times p}(R)$. Assume that $k \leq \min(m, n, p)$. Fix a set $I = \{i_1, \ldots, i_k\} \in T_{\binom{p}{k}}$. From Definition 2.1.3, we have

$$\begin{aligned} AB(e_I) = A(Be_I) = A(Be_{i_1} \wedge \cdots \wedge Be_{i_k}) &= A\Big(\sum_{J\in T_{\binom{n}{k}}} (\Lambda^k(B))_{J,I} e_J\Big) \\ &= \sum_{J\in T_{\binom{n}{k}}, K\in T_{\binom{m}{k}}} (\Lambda^k(A))_{K,J}(\Lambda^k(B))_{J,I} e_K. \end{aligned}$$

On the other hand,

$$AB(e_I) = \sum_{K\in T_{\binom{m}{k}}} (\Lambda^k(AB))_{K,I} e_K.$$

Comparing the two expressions, we find that

$$(\Lambda^k(AB))_{K,I} = \sum_{J\in T_{\binom{n}{k}}} (\Lambda^k(A))_{K,J}(\Lambda^k(B))_{J,I}.$$

So $\Lambda^k(AB) = \Lambda^k(A)\Lambda^k(B)$. □

Example 2.2.1. Let $R = \mathbb{Z}$,

$$A = \begin{pmatrix} 4 & 5 \\ -3 & 6 \\ 2 & 4 \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} -4 & 9 & 6 & 5 \\ 8 & -1 & -5 & 7 \end{pmatrix}.$$

Then, the product $C = AB$ is

$$C = \begin{pmatrix} 24 & 31 & -1 & 55 \\ 60 & -33 & -48 & 27 \\ 24 & 14 & -8 & 38 \end{pmatrix}.$$

Using Definition 2.1.3, we compute $\Lambda^2(A)$ and $\Lambda^2(B)$ to be

$$\Lambda^2(A) = \begin{pmatrix} 39 \\ 6 \\ -24 \end{pmatrix} \qquad \text{and} \qquad \Lambda^2(B) = \begin{pmatrix} -68 & -28 & -68 & -39 & 68 & 67 \end{pmatrix}.$$

In the above calculations, the rows and columns of $\Lambda^2(A)$ and $\Lambda^2(B)$ are indexed by sets in the lexicographical/dictionary order. From Theorem 2.2.2,

$$\Lambda^2(C) = \Lambda^2(A)\Lambda^2(B) = \begin{pmatrix} -2652 & -1092 & -2652 & -1521 & 2652 & 2613 \\ -408 & -168 & -408 & -234 & 408 & 402 \\ 1632 & 672 & 1632 & 936 & -1632 & -1608 \end{pmatrix}.$$

One can check by directly applying Definition 2.1.3 to the matrix C that this is the correct matrix for $\Lambda^2(C)$.

We called the multiplicative property in Theorem 2.2.2 the generalised Cauchy-Binet formula because it is a more general form of the standard Cauchy-Binet formula, which we will demonstrate below.

Corollary 2.2.3 (Cauchy-Binet Formula)**.** *Let R be a commutative ring, $A \in M_{m\times n}(R)$, $B \in M_{n\times m}(R)$ and $m < n$. Noting that AB is a $m \times m$ matrix, we have*

$$\det(AB) = \sum_{J\in T_{\binom{n}{m}}} \det(A_{\{1,2,\ldots,m\},J}) \det(B_{J,\{1,2,\ldots,m\}}).$$

Proof. Assume that R is a commutative ring, $m < n$, $A \in M_{m\times n}(R)$ and $B \in M_{n\times m}(R)$. Using Proposition 2.2.1 (a), Theorem 2.2.2 and Theorem 2.1.2, we have

$$\begin{aligned} \det(AB) &= \Lambda^m(AB) = \Lambda^m(A)\Lambda^m(B) \\ &= \sum_{J\in T_{\binom{n}{m}}} (\Lambda^m(A))_{\{1,2,\ldots,n\},J} (\Lambda^m(B))_{J,\{1,2,\ldots,n\}} \\ &= \sum_{J\in T_{\binom{n}{m}}} \det(A_{\{1,2,\ldots,m\},J}) \det(B_{J,\{1,2,\ldots,m\}}). \quad \square \end{aligned}$$

A major consequence of Theorem 2.2.2 and Proposition 2.2.1 is Corollary 2.2.4, which tells us how to compute the inverse of a wedge product matrix.

Corollary 2.2.4. *Let R be a commutative ring and $A \in GL_n(R)$. If $k \in \{1, \ldots, n\}$ then $\Lambda^k(A) \in GL_{\binom{n}{k}}(R)$ and*

$$\Lambda^k(A^{-1}) = (\Lambda^k(A))^{-1}.$$

Proof. Assume that R is a commutative ring and $A \in GL_n(R)$. Theorem 2.2.2 tells us that

$$\Lambda^k(A)\Lambda^k(A^{-1}) = \Lambda^k(A^{-1})\Lambda^k(A) = \Lambda^k(I_n) = I_{\binom{n}{k}} \tag{2.2}$$

where in the rightmost equality, we have used Proposition 2.2.1. Equation (2.2) demonstrates that $\Lambda^k(A)$ is invertible with inverse $(\Lambda^k(A))^{-1} = \Lambda^k(A^{-1})$. $\square$

2.3 General Laplace expansion

Our first application of wedge product matrices is to generalise known identities in linear algebra. As a first example of this, we will use wedge product matrices to prove a general form of Laplace expansion (see [Rot03, Proposition 9.160]), which is essentially Laplace expansion, but across multiple rows/columns.

For $m \in \mathbb{Z}_{>0}$, we will denote the set $\{1, 2, \ldots, m\}$ by $\mathbb{Z}_{[1,m]}$.

Definition 2.3.1. Let $k, n \in \mathbb{Z}_{>0}$, $k \leq n$ and L, M be subsets of $\mathbb{Z}_{>0}$ with $L \subseteq M$. Then, we define

$$s_{L,M} = (-1)^{\sharp\{(i,j) \mid i<j,\, i\in M\setminus L,\, j\in L\}}.$$

An important way of interpreting this definition is that if $L = \{l_1, \ldots, l_k\}$, $M\setminus L = \{j_1, \ldots, j_p\}$ and $M = \{m_1, \ldots, m_{k+p}\}$ with $m_1 < \cdots < m_{k+p}$, then s_L is the sign of the permutation $\sigma \in S_{k+p}$, which sends the sequence $(m_1, m_2, \ldots, m_{k+p})$ to $(l_1, \ldots, l_k, j_1, \ldots, j_p)$.

Proposition 2.3.1 (General Laplace Expansion)**.** *Let R be a commutative ring and $A \in M_{m\times n}(R)$. Let $p, k \in \mathbb{Z}_{>0}$ such that $p < k < \min(m, n)$. Let $K \in T_{\binom{m}{k}}$ and $M \in T_{\binom{n}{k}}$.*

(a) If $H \subseteq M \in T_{\binom{n}{k}}$ with $|H| = p$ then

$$(\Lambda^k(A))_{K,M} = \sum_{L\subsetneq K, |L|=|H|} s_{L,K} s_{H,M} (\Lambda^p(A))_{L,H} (\Lambda^{k-p}(A))_{K\setminus L,\, M\setminus H}. \tag{2.3}$$

(b) If $H \subseteq K \in T_{\binom{m}{k}}$ with $|H| = p$, then

$$(\Lambda^k(A))_{K,M} = \sum_{L\subsetneq M, |L|=|H|} s_{L,M} s_{H,K} (\Lambda^p(A))_{H,L} (\Lambda^{k-p}(A))_{K\setminus H,\, M\setminus L}. \tag{2.4}$$

Moreover, if $A \in M_{n\times n}(R)$ and $H \in T_{\binom{n}{p}}$, then

(c)

$$\det(A) = \sum_{L\in T_{\binom{n}{p}}} s_{L,\mathbb{Z}_{[1,n]}} s_{H,\mathbb{Z}_{[1,n]}} (\Lambda^p(A))_{L,H} (\Lambda^{n-p}(A))_{L^c,H^c} \tag{2.5}$$

(d)

$$\det(A) = \sum_{L\in T_{\binom{n}{p}}} s_{L,\mathbb{Z}_{[1,n]}} s_{H,\mathbb{Z}_{[1,n]}} (\Lambda^p(A))_{H,L} (\Lambda^{n-p}(A))_{H^c,L^c}. \tag{2.6}$$

Note that in parts (c) and (d) of Proposition 2.3.1, the complements H^c and L^c are done with respect to the set $\mathbb{Z}_{[1,n]}$.

Proof. (a): Assume that R is a commutative ring and $A \in M_{m\times n}(R)$. Assume that $k, p \in \mathbb{Z}_{>0}$ such that $p < k < \min(m, n)$, $K \in T_{\binom{m}{k}}$, $M \in T_{\binom{n}{k}}$ and $H \subseteq M$ with $|H| = p$. Using Definition 2.1.3, we begin with the expression

$$Ae_H \wedge Ae_{M\setminus H} = s_{H,M} Ae_M = \sum_{K\in T_{\binom{m}{k}}} s_{H,M}(\Lambda^k(A))_{K,M} e_K. \tag{2.7}$$

We can obtain another expression for $Ae_H \wedge Ae_{M\setminus H}$ by computing

$$\begin{aligned}
Ae_H \wedge Ae_{M\setminus H} &= \sum_{L\in T_{\binom{m}{p}}} (\Lambda^p(A))_{L,H} e_L \wedge \sum_{J\in T_{\binom{m}{k-p}}} (\Lambda^{k-p}(A))_{J,\, M\setminus H} e_J \\
&= \sum_{L\in T_{\binom{m}{p}}} \sum_{J\in T_{\binom{m}{k-p}}} (\Lambda^p(A))_{L,H} (\Lambda^{k-p}(A))_{J,\, M\setminus H} (e_L \wedge e_J) \\
&= \sum_{K\in T_{\binom{m}{k}}} \sum_{L\subsetneq K, |L|=|H|} (\Lambda^p(A))_{L,H} (\Lambda^{k-p}(A))_{K\setminus L,\, M\setminus H} (e_L \wedge e_{K\setminus L}) \\
&= \sum_{K\in T_{\binom{m}{k}}} \sum_{L\subsetneq K, |L|=|H|} s_{L,K} (\Lambda^p(A))_{L,H} (\Lambda^{k-p}(A))_{K\setminus L,\, M\setminus H} e_K.
\end{aligned}$$

Upon comparison with equation (2.7), we find that if $K \in T_{\binom{m}{k}}$ then

$$\sum_{L\subsetneq K, |L|=|H|} s_{L,K} (\Lambda^p(A))_{L,H} (\Lambda^{k-p}(A))_{K\setminus L,\, M\setminus H} = s_{H,M} (\Lambda^k(A))_{K,M}.$$

Multiplying both sides by $s_{H,M}$ then gives the desired result.

(b): Now assume that $H \subseteq K \in T_{\binom{m}{k}}$ with $|H| = p$. Take the expression in part (a) and apply it to the element $(\Lambda^k(A^T))_{M,K}$. We find that

$$\begin{aligned}
(\Lambda^k(A))_{K,M} &= (\Lambda^k(A^T))_{M,K} \\
&= \sum_{L\subsetneq M, |L|=|H|} s_{L,M} s_{H,K} (\Lambda^p(A^T))_{L,H} (\Lambda^{k-p}(A^T))_{M\setminus L,\, K\setminus H} \\
&= \sum_{L\subsetneq M, |L|=|H|} s_{L,M} s_{H,K} ((\Lambda^p(A))^T)_{L,H} ((\Lambda^{k-p}(A))^T)_{M\setminus L,\, K\setminus H} \\
&= \sum_{L\subsetneq M, |L|=|H|} s_{L,M} s_{H,K} (\Lambda^p(A))_{H,L} (\Lambda^{k-p}(A))_{K\setminus H,\, M\setminus L}.
\end{aligned}$$

(c): In the scenario for part (a), set $m = n = k$ and $p < k$. Then, $K = M = \mathbb{Z}_{[1,n]} \in T_{\binom{n}{n}}$, $H \in T_{\binom{n}{p}}$ and by substitution into equation (2.3), we obtain equation (2.5).

(d): Similarly to part (c), we set $m = n = k$ and $p < k$ in part (b), which fixes $K = M = \mathbb{Z}_{[1,n]} \in T_{\binom{n}{n}}$, $H \in T_{\binom{n}{p}}$ and yields equation (2.6) upon substitution into equation (2.4). □

Example 2.3.2. Let $A \in M_{4\times 4}(\mathbb{Z})$ be the matrix

$$A = \begin{pmatrix} 1 & 2 & 5 & -2 \\ 0 & 4 & 2 & 6 \\ 5 & -3 & 9 & 7 \\ -8 & -2 & -1 & 2 \end{pmatrix}.$$

The determinant of A is -3342. Let us verify this by utilising Proposition 2.3.1. We let $n = 4$ and $k = 2$. The table below depicts all possible elements L of $T_{\binom{4}{2}}$, with their associated sign s_L:

L	$s_{L,\mathbb{Z}_{[1,4]}}$
$\{1, 2\}$	+1
$\{1, 3\}$	-1
$\{1, 4\}$	+1
$\{2, 3\}$	+1
$\{2, 4\}$	-1
$\{3, 4\}$	+1

In our particular scenario, equation (2.5) reduces to

$$\det(A) = \sum_{L\in T_{\binom{4}{2}}} s_{L,\mathbb{Z}_{[1,4]}} s_{H,\mathbb{Z}_{[1,4]}} (\Lambda^2(A))_{L,H} (\Lambda^2(A))_{L^c,H^c}. \tag{2.8}$$

Computing $\Lambda^2(A)$, we find that

$$\Lambda^2(A) = \begin{array}{c} \begin{matrix} \{1,2\} & \{1,3\} & \{1,4\} & \{2,3\} & \{2,4\} & \{3,4\} \end{matrix} \\ \begin{pmatrix} 4 & 2 & 6 & -16 & 20 & 34 \\ -13 & -16 & 17 & 33 & 8 & 53 \\ 14 & 39 & -14 & 8 & 0 & 8 \\ -20 & -10 & -30 & 42 & 46 & -40 \\ 32 & 16 & 48 & 0 & 20 & 10 \\ -34 & 67 & 66 & 21 & 8 & 25 \end{pmatrix} \end{array} \begin{matrix} \{1,2\} \\ \{1,3\} \\ \{1,4\} \\ \{2,3\} \\ \{2,4\} \\ \{3,4\} \end{matrix}$$

where we have indicated the labels of the rows and columns in lexicographical order.

If $H = \{1, 2\}$, then equation (2.8) yields

$$\begin{aligned} \det(A) &= \sum_{L\in T_{\binom{4}{2}}} s_{L,\mathbb{Z}_{[1,4]}} s_{\{1,2\},\mathbb{Z}_{[1,4]}} (\Lambda^2(A))_{L,\{1,2\}} (\Lambda^2(A))_{L^c,\{3,4\}} \\ &= \sum_{L\in T_{\binom{4}{2}}} s_{L,\mathbb{Z}_{[1,4]}} (\Lambda^2(A))_{L,\{1,2\}} (\Lambda^2(A))_{L^c,\{3,4\}} \\ &= (4 \cdot 25) - (-13 \cdot 10) + (14 \cdot -40) + (-20 \cdot 8) - (32 \cdot 53) + (-34 \cdot 34) \\ &= -3342. \end{aligned}$$

Let us now test Proposition 2.3.1, but with selections of rows rather than columns. The relevant identity is

$$\det(A) = \sum_{L \in T_{\binom{4}{2}}} s_{L,\mathbb{Z}_{[1,4]}} s_{H,\mathbb{Z}_{[1,4]}} (\Lambda^2(A))_{H,L} (\Lambda^2(A))_{H^c,L^c} \tag{2.9}$$

If we set $H = \{1, 3\}$, equation (2.9) gives

$$\begin{aligned}
\det(A) &= \sum_{L \in T_{\binom{4}{2}}} s_{L,\mathbb{Z}_{[1,4]}} s_{\{1,3\},\mathbb{Z}_{[1,4]}} (\Lambda^2(A))_{\{1,3\},L} (\Lambda^2(A))_{\{2,4\},L^c} \\
&= - \sum_{L \in T_{\binom{4}{2}}} s_{L,\mathbb{Z}_{[1,4]}} (\Lambda^2(A))_{\{1,3\},L} (\Lambda^2(A))_{\{2,4\},L^c} \\
&= -\big((-13 \cdot 10) - (-16 \cdot 20) + (17 \cdot 0) + (33 \cdot 48) - (8 \cdot 16) + (53 \cdot 32)\big) \\
&= -3342.
\end{aligned}$$

This agrees with our previous computation.

Chapter 3

Adjugates, quasideterminants and eigenvectors

3.1 Adjugate matrices are almost inverses

In this section, we will explore inverses of wedge product matrices in greater detail, with Proposition 2.3.1 informing the important definition below. Recall from Definition 2.3.1 that if $L = \{l_1, \ldots, l_k\}$ and $M = \{m_1, \ldots, m_{k+p}\}$ with $m_1 < \cdots < m_{k+p}$ are two subsets of $\mathbb{Z}_{>0}$ with $L \subseteq M$ and $M \backslash L = \{j_1, \ldots, j_p\}$ then

$$s_{L,M} = (-1)^{\sharp\{(i,j) \mid i<j,\, i\in M\backslash L,\, j\in L\}}.$$

is the sign of the permutation $\sigma \in S_{k+p}$ which maps the sequence $(m_1, \ldots, m_{k+p})$ to $(l_1, \ldots, l_k, j_1, j_2, \ldots, j_p)$.

Definition 3.1.1. Let R be a commutative ring and $A \in M_{m\times n}(R)$. Let $k \in \{0, 1, \ldots, \min(m, n)\}$, $L \in T_{\binom{m}{k}}$ and $H \in T_{\binom{n}{k}}$. Then, the k^{th} **adjugate matrix** of A, denoted by $\Upsilon^{n-k}(A)$, is the $\binom{n}{k} \times \binom{m}{k}$ matrix given by

$$(\Upsilon^{n-k}(A))_{H,L} = s_{L,\mathbb{Z}_{[1,m]}} s_{H,\mathbb{Z}_{[1,n]}} (\Lambda^{n-k}(A))_{\mathbb{Z}_{[1,m]}\backslash L,\, \mathbb{Z}_{[1,n]}\backslash H} \tag{3.1}$$

where for $n \in \mathbb{Z}_{>0}$, $\mathbb{Z}_{[1,n]} = \{1, 2, \ldots, n\}$.

Theorems 3.1.1 and 3.1.3 demonstrate how Definition 3.1.1 is connected to the general Laplace expansion in Proposition 2.3.1.

Theorem 3.1.1. *Let R be a commutative ring and $A \in M_{m\times n}(R)$ with $m \leq n$. Assume that $k \in \{0, 1, \ldots, m\}$. If $I \in T_{\binom{n}{n-(m-k)}}$ and $J \in T_{\binom{n}{k}}$ then*

$$(\Upsilon^{m-k}(A)\Lambda^k(A))_{I,J} = \begin{cases} s_{I,\mathbb{Z}_{[1,n]}} s_{J,J\cup I^c} (\Lambda^m(A))_{\mathbb{Z}_{[1,m]},J\cup I^c}, & \text{if } J \subseteq I, \\ 0, & \text{otherwise.} \end{cases}$$

Proof. Assume that R is a commutative ring and $A \in M_{m\times n}(R)$ with $m \leq n$. Assume that $k \in \{0, 1, \ldots, m\}$, $I \in T_{\binom{n}{n-(m-k)}}$ and $J \in T_{\binom{n}{k}}$. There are two cases to consider.

Case 1: Assume that $J \subseteq I$. Then,

$$\begin{aligned}(\Upsilon^{m-k}(A)\Lambda^k(A))_{I,J} &= \sum_{M\in T_{\binom{m}{k}}} (\Upsilon^{m-k}(A))_{I,M}(\Lambda^k(A))_{M,J} \\ &= \sum_{M\in T_{\binom{m}{k}}} s_{M,\mathbb{Z}_{[1,m]}} s_{I,\mathbb{Z}_{[1,n]}} (\Lambda^{m-k}(A))_{M^c,I^c}(\Lambda^k(A))_{M,J} \\ &= \sum_{M\in T_{\binom{m}{k}}} s_{M,\mathbb{Z}_{[1,m]}} s_{I,\mathbb{Z}_{[1,n]}} s_{J,J\cup I^c} s_{J,J\cup I^c} (\Lambda^{m-k}(A))_{M^c,I^c}(\Lambda^k(A))_{M,J} \\ &= s_{I,\mathbb{Z}_{[1,n]}} s_{J,J\cup I^c} \sum_{M\in T_{\binom{m}{k}}} s_{M,\mathbb{Z}_{[1,m]}} s_{J,J\cup I^c} (\Lambda^{m-k}(A))_{M^c,I^c}(\Lambda^k(A))_{M,J} \\ &= s_{I,\mathbb{Z}_{[1,n]}} s_{J,J\cup I^c} (\Lambda^m(A))_{\mathbb{Z}_{[1,m]},J\cup I^c}.\end{aligned}$$

In the last line, we used Proposition 2.3.1.

Case 2: Assume that $J \cap I^c \neq \emptyset$. Then Theorem 2.1.2 gives

$$(\Lambda^m(A))_{\mathbb{Z}_{[1,m]},J\cup I^c} = \det(A_{\mathbb{Z}_{[1,m]},J\cup I^c}).$$

Since $J \cap I^c \neq \emptyset$, the $m \times m$ matrix $A_{\mathbb{Z}_{[1,m]},J\cup I^c}$ must have a repeated column. Thus, $\det(A_{\mathbb{Z}_{[1,m]},J\cup I^c}) = 0$. □

Theorem 3.1.3 is an analogue of Theorem 3.1.1 for the case where $n \leq m$. We will use the transpose to prove Theorem 3.1.3, which means that we must compute the transpose of an adjugate matrix.

Proposition 3.1.2. *Let R be a commutative ring, $B \in M_{m\times n}(R)$ and $k \in \{0, 1, \ldots, \min(m, n)\}$. Then,*

$$\Upsilon^k(B^T) = (\Upsilon^k(B))^T.$$

Proof. Assume that $B \in M_{m\times n}(R)$, $L \in T_{\binom{m}{m-k}}$ and $H \in T_{\binom{n}{n-k}}$. From equation (3.1) and part (d) of Proposition 2.2.1, we have

$$\begin{aligned}((\Upsilon^k(B))^T)_{L,H} &= (\Upsilon^k(B))_{H,L} \\ &= s_{L,\mathbb{Z}_{[1,m]}} s_{H,\mathbb{Z}_{[1,n]}} (\Lambda^k(B))_{\mathbb{Z}_{[1,m]}\setminus L,\, \mathbb{Z}_{[1,n]}\setminus H} \\ &= s_{L,\mathbb{Z}_{[1,m]}} s_{H,\mathbb{Z}_{[1,n]}} ((\Lambda^k(B))^T)_{\mathbb{Z}_{[1,n]}\setminus H,\, \mathbb{Z}_{[1,m]}\setminus L} \\ &= s_{L,\mathbb{Z}_{[1,m]}} s_{H,\mathbb{Z}_{[1,n]}} (\Lambda^k(B^T))_{\mathbb{Z}_{[1,n]}\setminus H,\, \mathbb{Z}_{[1,m]}\setminus L} = (\Upsilon^k(B^T))_{L,H}.\end{aligned}$$

So, $\Upsilon^k(B^T) = (\Upsilon^k(B))^T$. □

Theorem 3.1.3. *Let R be a commutative ring and $A \in M_{m\times n}(R)$ with $n \leq m$. Assume that $k \in \{0, 1, \ldots, n\}$. If $I \in T_{\binom{m}{k}}$ and $J \in T_{\binom{m}{m-(n-k)}}$ then*

$$(\Lambda^k(A)\Upsilon^{n-k}(A))_{I,J} = \begin{cases} s_{I,J^c\cup I}\; s_{J,\mathbb{Z}_{[1,m]}} (\Lambda^n(A))_{J^c\cup I,\mathbb{Z}_{[1,n]}}, & \text{if } I \subseteq J, \\ 0, & \text{otherwise.}\end{cases}$$

Proof. Assume that $A \in M_{m\times n}(R)$ with $n \leq m$. Assume that $k \in \{0, 1, \ldots, n\}$, $I \in T_{\binom{m}{k}}$ and $J \in T_{\binom{m}{m-n+k}}$.

Case 1: If $I \subseteq J$ then by Proposition 3.1.2 and Theorem 3.1.1,

$$\begin{aligned}(\Lambda^k(A)\Upsilon^{n-k}(A))_{I,J} &= ((\Lambda^k(A)\Upsilon^{n-k}(A))^T)_{J,I}\\ &= (\Upsilon^{n-k}(A^T)\Lambda^k(A^T))_{J,I}\\ &= s_{I,J^c\cup I}\ s_{J,\mathbb{Z}_{[1,m]}}(\Lambda^n(A^T))_{\mathbb{Z}_{[1,n]},I\cup J^c}\\ &= s_{I,J^c\cup I}\ s_{J,\mathbb{Z}_{[1,m]}}(\Lambda^n(A))_{I\cup J^c,\mathbb{Z}_{[1,n]}}.\end{aligned}$$

Case 2: If $J^c \cap I \neq 0$ then the same computation in Case 1 gives $(\Lambda^k(A)\Upsilon^{n-k}(A))_{I,J} = 0$. □

If $m = n$ in Theorems 3.1.1 and 3.1.3 and $I, J \in T_{\binom{n}{k}}$ then

$$(\Upsilon^{n-k}(A)\Lambda^k(A))_{I,J} = (\Lambda^k(A)\Upsilon^{n-k}(A))_{I,J} = \begin{cases}\det(A), \text{ if } J = I,\\ 0, \text{ otherwise.}\end{cases}$$

Thus, we obtain the corollary

Corollary 3.1.4. *Let R be a commutative ring and $n \in \mathbb{Z}_{>0}$. Let $A \in M_{n\times n}(R)$. Then,*

$$\Lambda^k(A)\Upsilon^{n-k}(A) = \Upsilon^{n-k}(A)\Lambda^k(A) = \det(A)I_{\binom{n}{k}}. \tag{3.2}$$

3.2 Properties of adjugate matrices

The properties exhibited by adjugate matrices are very similar to those of wedge product matrices. Theorem 3.2.1 and Proposition 3.2.2 are analogues of Theorem 2.2.2 and Proposition 2.2.1 respectively.

Theorem 3.2.1. *Let R be a commutative ring, $A \in M_{m\times n}(R)$ and $B \in M_{n\times p}(R)$. Let $k \in \{0, 1, \ldots, \min(m, n, p)\}$. Then,*

$$\Upsilon^k(AB) = \Upsilon^k(B)\Upsilon^k(A).$$

Proof. Assume that $A \in M_{m\times n}(R)$ and $B \in M_{n\times p}(R)$. Let $z = \min(m, n, p)$. If $k \in \{0, 1, \ldots, z\}$, $K \in T_{\binom{m}{k}}$ and $I \in T_{\binom{p}{k}}$ then

$$\begin{aligned}(\Upsilon^k(AB))_{I^c,K^c} &= s_{K^c,\mathbb{Z}_{[1,m]}}s_{I^c,\mathbb{Z}_{[1,p]}}(\Lambda^k(AB))_{K,I}\\ &= s_{K^c,\mathbb{Z}_{[1,m]}}s_{I^c,\mathbb{Z}_{[1,p]}}\sum_{J\in T_{\binom{n}{k}}}(\Lambda^k(A))_{K,J}(\Lambda^k(B))_{J,I}\\ &= \sum_{J\in T_{\binom{n}{k}}} s_{K^c,\mathbb{Z}_{[1,m]}}s_{J^c,\mathbb{Z}_{[1,n]}}(\Lambda^k(A))_{K,J}\ s_{I^c,\mathbb{Z}_{[1,p]}}s_{J^c,\mathbb{Z}_{[1,n]}}(\Lambda^k(B))_{J,I}\\ &= \sum_{J\in T_{\binom{n}{k}}}(\Upsilon^k(A))_{J^c,K^c}(\Upsilon^k(B))_{I^c,J^c}\\ &= \sum_{J\in T_{\binom{n}{k}}}(\Upsilon^k(B))_{I^c,J^c}(\Upsilon^k(A))_{J^c,K^c} = (\Upsilon^k(B)\Upsilon^k(A))_{I^c,K^c}.\end{aligned}$$

Thus, $\Upsilon^k(AB) = \Upsilon^k(B)\Upsilon^k(A)$. □

Proposition 3.2.2. *Let R be a commutative ring, $A \in M_{n\times n}(R)$ and $B \in M_{m\times n}(R)$. Let $k \in \{0, 1, \ldots, n-1\}$ and $I_n \in M_{n\times n}(R)$ denote the identity matrix. Then,*

(a) $\Upsilon^0(A)$ is the 1×1 matrix I_1.

(b) If A is invertible then $\Upsilon^{n-1}(A) = \det(A)A^{-1}$.

(c) $\Upsilon^k(I_n) = I_{\binom{n}{k}}$.

Proof. Assume that R is a commutative ring, $A \in M_{n\times n}(R)$, $B \in M_{m\times n}(R)$ and $k \in \{0, \ldots, n-1\}$.

(a): By equation (3.2), we note that $\Lambda^n(A)\Upsilon^0(A) = \det(A)I_1 = (\det(A))$ (a 1×1 matrix). Since $\Lambda^n(A) = (\det(A))$, $\Upsilon^0(A) = (1) = I_1$.

(b): Assume that A is invertible. From equation (3.2), $\Lambda^1(A)\Upsilon^{n-1}(A) = \det(A)I_n$. Since $\Lambda^1(A) = A$, we have $\Upsilon^{n-1}(A) = \det(A)A^{-1}$.

(c): By equation (3.2), $\Lambda^{n-k}(I_n)\Upsilon^k(I_n) = I_{\binom{n}{k}}$. Since $\Lambda^{n-k}(I_n) = I_{\binom{n}{k}}$, we have $\Upsilon^k(I_n) = I_{\binom{n}{k}}$. □

It is worth noting that in part (b) of Proposition 3.2.2, the matrix $\Upsilon^{n-1}(A)$ is commonly called the adjugate matrix of A, i.e. the transpose of the cofactors matrix of A. The adjugate matrix is commonly used to compute the inverse of an invertible matrix (see [Rot03, Page 766-767]).

Example 3.2.1. Continuing from Example 2.3.2, we have

$$A = \begin{pmatrix} 1 & 2 & 5 & -2 \\ 0 & 4 & 2 & 6 \\ 5 & -3 & 9 & 7 \\ -8 & -2 & -1 & 2 \end{pmatrix} \quad \text{and} \quad \Lambda^2(A) = \begin{pmatrix} 4 & 2 & 6 & -16 & 20 & 34 \\ -13 & -16 & 17 & 33 & 8 & 53 \\ 14 & 39 & -14 & 8 & 0 & 8 \\ -20 & -10 & -30 & 42 & 46 & -40 \\ 32 & 16 & 48 & 0 & 20 & 10 \\ -34 & 67 & 66 & 21 & 8 & 25 \end{pmatrix}.$$

From equation (3.1), we compute the 2^{nd} adjugate matrix $\Upsilon^2(A)$ as

$$\Upsilon^2(A) = \begin{pmatrix} 25 & -10 & -40 & 8 & -53 & 34 \\ -8 & 20 & -46 & 0 & 8 & -20 \\ 21 & 0 & 42 & 8 & -33 & -16 \\ 66 & -48 & -30 & -14 & -17 & 6 \\ -67 & 16 & 10 & -39 & -16 & -2 \\ -34 & -32 & -20 & 14 & 13 & 4 \end{pmatrix}.$$

One can then verify by direct calculation that $\Lambda^2(A)\Upsilon^2(A) = \det(A)I_6$ with I_6 being the 6×6 identity matrix. This is consistent with equation (3.2).

We will now improve on Corollary 2.2.4 by computing the determinant of wedge product and adjugate matrices.

Theorem 3.2.3 (Sylvester-Franke)**.** *Let R be a commutative ring and $A \in M_{n\times n}(R)$. If $k \in \{1, \ldots, n\}$, then*

$$\det(\Lambda^k(A)) = \det(\Upsilon^k(A)) = (\det(A))^{\binom{n-1}{k-1}}.$$

Our proof of Theorem 3.2.3 will follow the reference [Con]. In particular, we will prove two preliminary results first. The method we use is referred to as the *principle of permanence of identities* in [Art91, Chapter 12, Section 3].

Lemma 3.2.4. *Let R be a commutative ring and $a_1, \ldots, a_n \in R$. Define $ev_{a_1,\ldots,a_n} : \mathbb{Z}[x_1, \ldots, x_n] \to R$ by*

$$ev_{a_1,\ldots,a_n}(f(x_1, \ldots, x_n)) = f(a_1, \ldots, a_n) \qquad \text{for} \qquad f \in \mathbb{Z}[x_1, \ldots, x_n].$$

Then, $ev_{a_1,\ldots,a_n}$ is a ring homomorphism.

Proof. Assume that R is a commutative ring and $a_1, \ldots, a_n \in R$. Assume that $f, g \in \mathbb{Z}[x_1, \ldots, x_n]$. If $i = (i_1, \ldots, i_n) \in (\mathbb{Z}_{\geq 0})^n$ is a n-tuple, let $x^i = x_1^{i_1} \ldots x_n^{i_n}$ and $a^i = a_1^{i_1} \ldots a_n^{i_n}$. Write f and g as

$$f(x_1, \ldots, x_n) = \sum_{i\in(\mathbb{Z}_{\geq 0})^n} c_i x^i \qquad \text{and} \qquad g(x_1, \ldots, x_n) = \sum_{j\in(\mathbb{Z}_{\geq 0})^n} d_j x^j.$$

Then,

$$\begin{aligned} ev_{a_1,\ldots,a_n}(f+g) &= ev_{a_1,\ldots,a_n}\Big(\sum_{i\in(\mathbb{Z}_{\geq 0})^n} c_i x^i + \sum_{j\in(\mathbb{Z}_{\geq 0})^n} d_j x^j\Big) \\ &= \sum_{i\in(\mathbb{Z}_{\geq 0})^n} c_i a^i + \sum_{j\in(\mathbb{Z}_{\geq 0})^n} d_j a^j = ev_{a_1,\ldots,a_n}(f) + ev_{a_1,\ldots,a_n}(g) \end{aligned}$$

and

$$\begin{aligned} ev_{a_1,\ldots,a_n}(fg) &= ev_{a_1,\ldots,a_n}\Big(\sum_{i,j\in(\mathbb{Z}_{\geq 0})^n} c_i d_j x^{i+j}\Big) = \sum_{i,j\in(\mathbb{Z}_{\geq 0})^n} c_i d_j a^{i+j} \\ &= \Big(\sum_{i\in(\mathbb{Z}_{\geq 0})^n} c_i a^i\Big)\Big(\sum_{j\in(\mathbb{Z}_{\geq 0})^n} d_j a^j\Big) = ev_{a_1,\ldots,a_n}(f) ev_{a_1,\ldots,a_n}(g). \end{aligned}$$

So, the evaluation map $ev_{a_1,\ldots,a_n}$ is a ring homomorphism from $\mathbb{Z}[x_1, \ldots, x_n]$ to R. □

Lemma 3.2.5. *Let $f, g \in \mathbb{C}[x_1, \ldots, x_n]$ and U be a non-empty open set in $\mathbb{C}^n$. If f and g satisfy the statement*

$$\text{If } a_1, \ldots, a_n \in U \text{ then } ev_{a_1,\ldots,a_n}(f) = ev_{a_1,\ldots,a_n}(g)$$

then $f = g$ in $\mathbb{C}[x_1, \ldots, x_n]$.

Proof. Assume that U is a non-empty open subset of $\mathbb{C}^n$. Assume that $a_1, \ldots, a_n \in U$ and $ev_{a_1,\ldots,a_n}(f) = ev_{a_1,\ldots,a_n}(g)$. Then, f and g are equal holomorphic functions in $\mathbb{C}^n$ and by the identity theorem (see [FG02, p. 156]), $f = g$. □

By combining Lemma 3.2.4 and Lemma 3.2.5, we will use the powerful technique developed in [Con] in order to supply a proof of Theorem 3.2.3.

Proof of Theorem 3.2.3. Assume that R is a commutative ring, $k \in \{1, 2, \ldots, n\}$ and $A = (a_{ij}) \in M_{n\times n}(R)$. We will first prove Theorem 3.2.3 in the case where $R = \mathbb{C}$.

Assume that $A \in M_{n\times n}(\mathbb{C})$. Since $\mathbb{C}$ is an algebraically closed field, Jordan normal form (see [DF04, Section 12.3]) tells us that there exists $P \in GL_n(\mathbb{C})$ such that $A = PJP^{-1}$, where

$$J = \begin{pmatrix} \lambda_1 & * & * \\ & \ddots & * \\ & & \lambda_n \end{pmatrix}$$

and $\lambda_1, \ldots, \lambda_n$ are the eigenvalues of A.

If J is upper triangular with diagonal entries $\lambda_1, \ldots, \lambda_n$ then $\Lambda^k(J)$ is upper triangular with diagonal entries λ_L, where if $L = \{i_1, \ldots, i_k\} \in T_{\binom{n}{k}}$ then λ_L is the product

$$\lambda_L = \lambda_{i_1}\lambda_{i_2}\ldots\lambda_{i_k}.$$

Since $A = PJP^{-1}$ then $\Lambda^k(A) = \Lambda^k(P)\Lambda^k(J)\Lambda^k(P)^{-1}$. By taking determinants of both sides,

$$\det(\Lambda^k(A)) = \prod_{L\in T_{\binom{n}{k}}} \lambda_L = \lambda_1^{\binom{n-1}{k-1}} \ldots \lambda_n^{\binom{n-1}{k-1}} = (\prod_{i=1}^{n} \lambda_i)^{\binom{n-1}{k-1}} = (\det(A))^{\binom{n-1}{k-1}},$$

since every eigenvalue λ_l is contained in the product $\prod_{L\in T_{\binom{n}{k}}} \lambda_L$ exactly $\binom{n-1}{k-1}$ times.

Hence, if $A \in M_{n\times n}(\mathbb{C})$, then $\det(\Lambda^k(A)) = (\det(A))^{\binom{n-1}{k-1}}$. Both sides of the equation are polynomials in the polynomial ring $\mathbb{C}[a_{11}, \ldots, a_{nn}]$. So, let

$$f(a_{11}, \ldots, a_{nn}) = \det(\Lambda^k(A)) \qquad \text{and} \qquad g(a_{11}, \ldots, a_{nn}) = (\det(A))^{\binom{n-1}{k-1}}$$

as polynomials in $\mathbb{C}[a_{11}, \ldots, a_{nn}]$. By identifying $M_{n\times n}(\mathbb{C})$ with $\mathbb{C}^{n^2}$, we deduce that $ev_{x_1,\ldots,x_{n^2}}(f) = ev_{x_1,\ldots,x_{n^2}}(g)$ on $\mathbb{C}^{n^2}$. Hence, from Lemma 3.2.5, $f(a_{11}, \ldots, a_{nn}) = g(a_{11}, \ldots, a_{nn})$ in $\mathbb{C}[a_{11}, \ldots, a_{nn}]$ and consequently, in $\mathbb{Z}[a_{11}, \ldots, a_{nn}]$ as well. Finally, by an application of Lemma 3.2.4, we deduce that if $i \in \{1, \ldots, n^2\}$ and $z_i \in R$ then $f(z_1, \ldots, z_{n^2}) = g(z_1, \ldots, z_{n^2})$. From the definitions of f and g, we deduce that if $A \in M_{n\times n}(R)$ then $\det(\Lambda^k(A)) = (\det(A))^{\binom{n-1}{k-1}}$.

Finally, from equation (3.2), $\Lambda^{n-k}(A)\Upsilon^k(A) = \det(A)I_{\binom{n}{k}}$. Taking the determinant of both sides, we obtain

$$\det(\Upsilon^k(A)) = \det(A)^{\binom{n}{k}-\binom{n-1}{n-k-1}} = \det(A)^{\binom{n}{k}-\binom{n-1}{k}} = \det(A)^{\binom{n-1}{k-1}} = \det(\Lambda^k(A)).$$

□

3.3 Quasideterminants in a commutative ring

Quasideterminants are an analogue of determinants used for square matrices with entries in a *non-commutative ring*. In [Mol07, Section 1.10] and [GR91, Pages 99-101], quasideterminants were used to provide a factorisation of the quantum determinant — another variant of the determinant used for non-commutative rings.

In this section, we will consider a more general analogue of the quasideterminant and demonstrate, by following [Mol07, Section 1.10], that in a commutative ring, they are linked to the elements of adjugate matrices.

Let R be a possibly non-commutative ring and $J = \{j_1, \ldots, j_k\}$ and $L = \{l_1, \ldots, l_k\}$ be elements of $T_{\binom{n}{k}}$ (see Definition 2.1.1), where $k \in \{1, 2, \ldots, n-1\}$. Denote by $A_{J,L}$ the $k \times k$ matrix of A formed from rows $j_1, j_2, \ldots, j_k$ of A and columns $l_1, l_2, \ldots, l_k$ of A.

Definition 3.3.1. Let R be a possibly non-commutative ring and $A = (a_{ij}) \in M_{n\times n}(R)$. Let $J = \{j_1, \ldots, j_k\}$ and $L = \{l_1, \ldots, l_k\}$ be elements of $T_{\binom{n}{k}}$, where $k \in \{1, \ldots, n-1\}$. Suppose that the $(n-k)\times(n-k)$ matrix A_{J^c,L^c} has a two-sided inverse. Then, the J, L **quasideterminant** of A is the matrix

$$|A|_{J,L} \in M_{k\times k}(R) \quad \text{given by} \quad |A|_{J,L} = A_{J,L} - A_{J,L^c}(A_{J^c,L^c})^{-1}A_{J^c,L}. \tag{3.3}$$

The complements J^c and L^c are taken with respect to the set $\mathbb{Z}_{[1,n]} = \{1, 2, \ldots, n\}$.

Setting $k = 1$ gives the definition of a quasideterminant in [GR91, Equation 1.1]. We will now build up to the main result of this section, following the exposition of [Mol07, Section 1.10] for the $k = 1$ case.

Lemma 3.3.1. *Let R be a possibly non-commutative ring. Let $k \in \{1, \ldots, n-1\}$, $A = (a_{ij}) \in M_{n\times n}(R)$ and $X = (x_{ij}) \in M_{n\times k}(R)$. Let $J = \{j_1, \ldots, j_k\} \in T_{\binom{n}{k}}$ and $L = \{l_1, \ldots, l_k\} \in T_{\binom{n}{k}}$. Suppose that if $p \in \{1, 2, \ldots, n\}$ and $r \in \{1, 2, \ldots, k\}$ then A and X satisfy*

$$\sum_{\ell=1}^{n} a_{p,\ell}x_{\ell,r} = 0 \tag{3.4}$$

for $p \neq j_r$. Define $y_{j_r} = \sum_{\ell=1}^{n} a_{j_r,\ell}x_{\ell,r} \in R$. If A_{J^c,L^c} has a two-sided inverse then

$$|A|_{J,L}X_{L,\mathbb{Z}_{[1,k]}} = diag[y_{j_1}, y_{j_2}, \ldots, y_{j_k}] \in M_{k\times k}(R).$$

Proof. Assume that R is a (possibly non-commutative) ring and $A \in M_{n\times n}(R)$. Assume that $k \in \{1, \ldots, n-1\}$ and $J = \{j_1, \ldots, j_k\}$ and $L = \{l_1, \ldots, l_k\}$ are elements of $T_{\binom{n}{k}}$. Assume that equation (3.4) holds, $y_{j_r} \in R$ is defined as above and A_{J^c,L^c} has a two-sided inverse. Then,

$$A_{J,L}X_{L,\mathbb{Z}_{[1,k]}} + A_{J,L^c}X_{L^c,\mathbb{Z}_{[1,k]}} = diag[y_{j_1}, y_{j_2}, \ldots, y_{j_k}] \in M_{k\times k}(R) \tag{3.5}$$

and

$$A_{J^c,L^c}X_{L^c,\mathbb{Z}_{[1,k]}} = -A_{J^c,L}X_{L,\mathbb{Z}_{[1,k]}} \in M_{(n-k)\times k}(R).$$

Since A_{J^c,L^c} has a two-sided inverse by assumption, then

$$X_{L^c,\mathbb{Z}_{[1,k]}} = -(A_{J^c,L^c})^{-1}A_{J^c,L}X_{L,\mathbb{Z}_{[1,k]}}. \tag{3.6}$$

Now substitute equation (3.6) into equation (3.5) to get

$$(A_{J,L} - A_{J,L^c}(A_{J^c,L^c})^{-1}A_{J^c,L})X_{L,\mathbb{Z}_{[1,k]}} = |A|_{J,L}X_{L,\mathbb{Z}_{[1,k]}} = diag[y_{j_1}, y_{j_2}, \ldots, y_{j_k}].$$

□

Lemma 3.3.2. *Let R be a possibly non-commutative ring and $A = (a_{ij}) \in M_{n\times n}(R)$ be an invertible matrix with two-sided inverse $B = (b_{ij})$. Let $k \in \{1, \ldots, n-1\}$, $J = \{j_1, \ldots, j_k\} \in T_{\binom{n}{k}}$ and $L = \{l_1, \ldots, l_k\} \in T_{\binom{n}{k}}$. Suppose that the matrix $(B_{L,J})^{-1}$ is a two-sided inverse for $B_{L,J}$. Then,*

$$|A|_{J,L}B_{L,J} = I_k.$$

Proof. Assume that R is a possibly non-commutative ring and $A = (a_{ij}) \in M_{n\times n}(R)$ has the two-sided inverse $B = (b_{ij})$. Assume that $k \in \{1, \ldots, n-1\}$ and $J, L \in T_{\binom{n}{k}}$ as defined above. Assume that the matrix$(B_{L,J})^{-1}$ is a two-sided inverse for $B_{L,J}$. Then,

$$AB = \begin{pmatrix} A_{J,L} & A_{J,L^c} \\ A_{J^c,L} & A_{J^c,L^c} \end{pmatrix} \begin{pmatrix} B_{L,J} & B_{L,J^c} \\ B_{L^c,J} & B_{L^c,J^c} \end{pmatrix} = \begin{pmatrix} I_k & 0 \\ 0 & I_{n-k} \end{pmatrix}.$$

From the block multiplication above, we have the following two equations:

$$A_{J^c,L}B_{L,J^c} + A_{J^c,L^c}B_{L^c,J^c} = I_{n-k}. \tag{3.7}$$

$$A_{J^c,L}B_{L,J} + A_{J^c,L^c}B_{L^c,J} = 0. \tag{3.8}$$

Rearranging equation (3.8) we find that $A_{J^c,L} = -A_{J^c,L^c}B_{L^c,J}(B_{L,J})^{-1}$ and upon substitution into equation (3.7), we obtain

$$A_{J^c,L^c}(B_{L^c,J^c} - B_{L^c,J}(B_{L,J})^{-1}B_{L,J^c}) = A_{J^c,L^c}|B|_{L^c,J^c} = I_{n-k}.$$

This shows that A_{J^c,L^c} is invertible. Hence, the quasideterminant $|A|_{J,L}$ is well-defined.

Define $C = (c_{ij}) = B_{\{1,\ldots,n\},J} \in M_{n\times k}(R)$. Since $AB = I_n$, if $p \in \{1, 2, \ldots, n\}$ and $q, r \in \{1, 2, \ldots, k\}$ then

$$\sum_{\ell=1}^{n} a_{p,\ell}c_{\ell,q} = \begin{cases} 1, \text{ if } (p,q) = (j_r, r), \\ 0, \text{ otherwise.} \end{cases}$$

By Lemma 3.3.1, we deduce that

$$|A|_{J,L}B_{L,J} = |A|_{J,L}C_{L,\{1,\ldots,k\}} = I_k.$$

Hence, $|A|_{J,L} = (B_{L,J})^{-1}$. □

Now, we will use Lemma 3.3.2 to prove our characterisation of quasideterminants for matrices whose entries are in a *commutative* ring.

Theorem 3.3.3. *Let R be a commutative ring and $A \in GL_n(R)$. Let $J, L \in T_{\binom{n}{k}}$ where $k \in \{1, \ldots, n-1\}$. Then,* $\det(|A|_{L,J}), \det(A)$ *and* $(\Upsilon^{n-k}(A))_{J,L}$ *are elements of R which satisfy*

$$\det(|A|_{L,J})(\Upsilon^{n-k}(A))_{J,L} = \det(A).$$

Proof. Assume that R is a commutative ring and $A \in M_{n\times n}(R)$ is an invertible matrix. Assume that $J, L \in T_{\binom{n}{k}}$, where $k \in \{1, \ldots, n-1\}$. Assume that $B = A^{-1}$. The k^{th} wedge product matrix $\Lambda^k(B)$ is well-defined for a commutative ring (see Definition 2.1.3). By Lemma 3.3.2, $|A|_{L,J} = (B_{J,L})^{-1}$ and by Theorem 2.1.2,

$$\begin{aligned}
\det(|A|_{L,J})(\Upsilon^{n-k}(A))_{J,L} &= (\det(B_{J,L}))^{-1}(\Upsilon^{n-k}(A))_{J,L} \\
&= ((\Lambda^k(B))_{J,L})^{-1}(\Upsilon^{n-k}(A))_{J,L} \\
&= ((\Lambda^k(A^{-1}))_{J,L})^{-1}(\Upsilon^{n-k}(A))_{J,L} \\
&= \big(\frac{1}{\det(A)}(\Upsilon^{n-k}(A))_{J,L}\big)^{-1}(\Upsilon^{n-k}(A))_{J,L} \\
&= \det(A)\frac{1}{(\Upsilon^{n-k}(A))_{J,L}}(\Upsilon^{n-k}(A))_{J,L} = \det(A).
\end{aligned}$$

□

Example 3.3.2. Let $R = \mathbb{Q}$ and

$$A = \begin{pmatrix} 1 & -2 & 5 & 23 \\ 3 & 4 & 3 & -12 \\ 0 & -3 & 4 & 15 \\ -2 & -6 & 3 & 13 \end{pmatrix} \in GL_4(\mathbb{Q}).$$

Note that $\det(A) = 5$. In the context of Theorem 3.3.3, set $k = 2$. Then,

$$\Lambda^2(A) = \begin{pmatrix} 10 & -12 & -81 & -26 & -68 & -129 \\ -3 & 4 & 15 & 7 & 39 & -17 \\ -10 & 13 & 59 & 24 & 112 & -4 \\ -9 & 12 & 45 & 25 & 24 & 93 \\ -10 & 15 & 15 & 30 & -20 & 75 \\ -6 & 8 & 30 & 15 & 51 & 7 \end{pmatrix}$$

and

$$\Upsilon^2(A) = \begin{array}{c} \begin{matrix} \{1,2\} & \{1,3\} & \{1,4\} & \{2,3\} & \{2,4\} & \{3,4\} \end{matrix} \\ \begin{pmatrix} 7 & -75 & 93 & -4 & 17 & -129 \\ -51 & -20 & -24 & -112 & 39 & 68 \\ 15 & -30 & 25 & 24 & -7 & -26 \\ 30 & -15 & 45 & 59 & -15 & -81 \\ -8 & 15 & -12 & -13 & 4 & 12 \\ -6 & 10 & -9 & -10 & 3 & 10 \end{pmatrix} \end{array} \begin{matrix} \{1,2\} \\ \{1,3\} \\ \{1,4\} \\ \{2,3\} \\ \{2,4\} \\ \{3,4\} \end{matrix}$$

Let $J = \{2,4\}$ and $L = \{1,4\}$. Then, $(\Upsilon^2(A))_{\{2,4\},\{1,4\}} = -12$. The quasideterminant $|A|_{\{1,4\},\{2,4\}}$ is

$$|A|_{\{1,4\},\{2,4\}} = \begin{pmatrix} -2 & 23 \\ -6 & 13 \end{pmatrix} - \begin{pmatrix} 1 & 5 \\ -2 & 3 \end{pmatrix} \begin{pmatrix} 3 & 3 \\ 0 & 4 \end{pmatrix}^{-1} \begin{pmatrix} 4 & -12 \\ -3 & 15 \end{pmatrix} = \begin{pmatrix} -1/3 & 12 \\ 5/12 & -55/4 \end{pmatrix}.$$

Let $B = A^{-1}$. Then,

$$B_{\{2,4\},\{1,4\}} = \begin{pmatrix} 33 & 144/5 \\ 1 & 4/5 \end{pmatrix} = \begin{pmatrix} -1/3 & 12 \\ 5/12 & -55/4 \end{pmatrix}^{-1} = |A|^{-1}_{\{1,4\},\{2,4\}}.$$

as in Lemma 3.3.2. Moreover,

$$\det(|A|_{\{1,4\},\{2,4\}}) = \begin{vmatrix} -1/3 & 12 \\ 5/12 & -55/4 \end{vmatrix} = -\frac{5}{12} = \frac{\det(A)}{(\Upsilon^2(A))_{\{2,4\},\{1,4\}}}$$

as in Theorem 3.3.3.

3.4 The eigenvector-eigenvalue identity

As the final application of wedge product matrices in this chapter, we will investigate a technique outlined in [DPTZ20, Page 6, Section 2.1]. The authors use this technique to prove the eigenvector-eigenvalue identity ([DPTZ20, Theorem 1]), which links the eigenvalues of a Hermitian matrix $A \in M_{n\times n}(\mathbb{C})$ to the elements of the eigenvectors of A and the eigenvalues of the $(n-1)\times(n-1)$ minors of A.

Theorem 3.4.1 (Eigenvector-eigenvalue identity)**.** *Let $A \in M_{n\times n}(\mathbb{C})$ such that $AA^* = A^*A$ and let $\lambda_1, \ldots, \lambda_n$ be distinct eigenvalues of A, with corresponding eigenvectors $v_1, v_2, \ldots, v_n \in M_{n\times 1}(\mathbb{C})$. For $i, j \in \{1, 2, \ldots, n\}$, let $v_{i,j}$ be the j^{th} entry of v_i, $j^c = \mathbb{Z}_{[1,n]}\backslash\{j\} \in T_{\binom{n}{n-1}}$ and $\mu_1^{(j)}, \ldots, \mu_{n-1}^{(j)}$ be the eigenvalues of the matrix $A_{j^c,j^c} \in M_{(n-1)\times(n-1)}(\mathbb{C})$. Then,*

$$|v_{i,j}|^2 = \frac{\prod_{k=1}^{n-1}(\lambda_i - \mu_k^{(j)})}{\prod_{k=1,\, k\neq i}^{n}(\lambda_i - \lambda_k)}.$$

We will give an independent proof of Theorem 3.4.1 at the end of this section. One of the proofs of the eigenvector-eigenvalue identity given in [DPTZ20, Page 6, Section 2.1] revolves around the adjugate matrix of A, which is $\Upsilon^{n-1}(A)$ from

Definition 3.1.1. Thus, it is expected that the same proof technique can be adapted to use $\Upsilon^{n-k}(A)$ for $k \in \{1, \ldots, n-1\}$.

Let R be a commutative ring. An important calculation we will use in what follows is that if $D = diag[\lambda_1, \ldots, \lambda_n] \in M_{n\times n}(R)$ then for $k \in \{1, 2, \ldots, n\}$,

$$\Lambda^k(D) = diag[\lambda_L \mid L \in T_{\binom{n}{k}}] \tag{3.9}$$

where if $L = \{l_1, \ldots, l_k\} \in T_{\binom{n}{k}}$ then $\lambda_L = \lambda_{l_1}\lambda_{l_2}\ldots\lambda_{l_k}$.

Definition 3.4.1. Let $L = \{l_1, \ldots, l_k\} \in T_{\binom{n}{k}}$. Define $D_L = (d_{ij}) \in M_{n\times n}(R)$ to be a diagonal matrix such that $d_{l_i l_i} = 1$ for all $i \in \{1, 2, \ldots, k\}$ and the rest of the entries are zero. We also define $p_L = \Lambda^k(D_L) \in M_{\binom{n}{k}\times\binom{n}{k}}(R)$. In particular, the matrix p_L is the diagonal matrix whose LL entry is 1 and every other entry is zero.

Theorem 3.4.2. *Let R be a commutative ring, $A \in M_{n\times n}(R)$ and $k \in \{1, \ldots, n-1\}$. Let $P, Q \in GL_n(R)$, $A = PUQ$ and $A' = PUP^{-1}$, where $U = diag[u_1, \ldots, u_n] \in M_{n\times n}(R)$ and $u_r \neq u_s$ whenever $r \neq s$. Let $L \in T_{\binom{n}{k}}$. Then,*

$$\big(\prod_{l\in L}\prod_{a\in L^c}(u_a - u_l)\big)\Lambda^k(P)p_L\Lambda^k(Q) = \Lambda^k\big(\prod_{a\in L^c}(u_a I_n - A')PQ\big). \tag{3.10}$$

Proof. Assume that $A \in M_{n\times n}(R)$ and $L \in T_{\binom{n}{k}}$. Let $\beta_b \in R$ for $b \in \{1, \ldots, n-k\}$. Then,

$$\beta_b I_n - A' = P(\beta_b I_n)P^{-1} - PUP^{-1} = P(\beta_b I_n - U)P^{-1}. \tag{3.11}$$

By taking the product over the variable b from 1 to $n-k$ on both sides of (3.11) and then multiplying by PQ, we obtain

$$\Big(\prod_{b=1}^{n-k}(\beta_b I_n - A')\Big)PQ = P\big(\prod_{b=1}^{n-k}(\beta_b I_n - U)\big)Q = P\ diag[\lambda_1, \ldots, \lambda_n]\ Q$$

where, for $m \in \{1, 2, \ldots, n\}$, $\lambda_m = \prod_{b=1}^{n-k}(\beta_b - u_m)$. Taking Λ^k of both sides of the above equation, we obtain from equation (3.9),

$$\Lambda^k\big(\prod_{a=1}^{n-k}(\beta_a I_n - A')PQ\big) = \Lambda^k(P)\ diag[\lambda_K \mid K \in T_{\binom{n}{k}}]\ \Lambda^k(Q).$$

Now let $L^c = \{i_1, i_2, \ldots, i_{n-k}\} \in T_{\binom{n}{n-k}}$. If we set $\beta_b = u_{i_b}$ for $b \in \{1, 2, \ldots, n-k\}$, the above equation simplifies immensely, yielding

$$\Lambda^k\big(\prod_{b=1}^{n-k}(u_{i_b}I_n - A')\ PQ\big) = \Lambda^k\big(\prod_{a\in L^c}(u_a I_n - A')\ PQ\big) = \big(\prod_{l\in L}\prod_{a\in L^c}(u_a - u_l)\big)\Lambda^k(P)p_L\Lambda^k(Q)$$

where p_L is from Definition 3.4.1 □

Next, we will prove an analogue of Theorem 3.4.2, where the LHS of equation (3.10) is replaced with an adjugate matrix.

Theorem 3.4.3. *Let R be a commutative ring, $A \in M_{n\times n}(R)$ and $k \in \{1,\dots,n-1\}$. Let $P, Q \in GL_n(R)$, $A = PUQ$ and $A' = PUP^{-1}$, where $U = diag[u_1,\dots,u_n] \in M_{n\times n}(R)$ and $u_r \neq u_s$ whenever $r \neq s$. Let $L \in T_{\binom{n}{k}}$. Then,*

$$\Big(\prod_{l\in L^c}\prod_{a\in L}(u_a - u_l)\Big)\ \Lambda^k(P)p_L\Lambda^k(Q) = \det(PQ)\ \Upsilon^{n-k}(Q^{-1}P^{-1}(\prod_{a\in L}(u_aI_n - A'))). \tag{3.12}$$

Proof. Assume that $A \in M_{n\times n}(R)$ and $L = \{i_1,\dots,i_k\} \in T_{\binom{n}{k}}$. Let $\beta_b \in R$ for $b \in \{1,\dots,k\}$. Then, equation (3.11) holds and by taking the product over the variable b from 1 to k on both sides of equation (3.11), we have

$$\prod_{b=1}^{k}(\beta_bI_n - A') = P\Big(\prod_{b=1}^{k}(\beta_bI_n - U)\Big)P^{-1} = P\ diag[\lambda_1,\dots,\lambda_n]\ P^{-1}$$

where for $m \in \{1,2,\dots,n\}$, $\lambda_m = \prod_{b=1}^{k}(\beta_b - u_m)$. Taking Λ^k of both sides, we obtain from equation (3.9)

$$\Lambda^k(\prod_{b=1}^{k}(\beta_bI_n - A')) = \Lambda^k(P)\ diag[\lambda_K \mid K \in T_{\binom{n}{k}}]\ (\Lambda^k(P))^{-1}.$$

We know from equation (3.2) that the product

$$\Lambda^k(\prod_{b=1}^{k}(\beta_bI_n - A'))\Upsilon^{n-k}(\prod_{b=1}^{k}(\beta_bI_n - A')) = \prod_{m=1}^{n}\prod_{b=1}^{k}(\beta_b - u_m)I_{\binom{n}{k}}.$$

So,

$$\Upsilon^{n-k}(\prod_{b=1}^{k}(\beta_bI_n - A')) = \Lambda^k(P)\ diag[\lambda_{K^c} \mid K \in T_{\binom{n}{k}}]\ (\Lambda^k(P))^{-1}.$$

Multiplying both sides by $\det(PQ)\Upsilon^{n-k}(P^{-1})\Upsilon^{n-k}(Q^{-1})$, we find that

$$\det(PQ)\Upsilon^{n-k}(Q^{-1}P^{-1}\prod_{b=1}^{k}(\beta_bI_n - A')) = \Lambda^k(P)\ diag[\lambda_{K^c} \mid K \in T_{\binom{n}{k}}]\ \Lambda^k(Q).$$

Recalling that $L = \{i_1, i_2, \dots, i_k\}$, if we set $\beta_b = u_{i_b}$ for $b \in \{1,2,\dots,k\}$ in the above equation then we obtain equation (3.12). □

Example 3.4.2. Let $R = \mathbb{C}$,

$$A = P\begin{pmatrix}1 & & & \\ & 1 & & \\ & & 2 & \\ & & & 6\end{pmatrix}P^{-1} \qquad \text{and} \qquad B = P\begin{pmatrix}0 & & & \\ & 1 & & \\ & & 2 & \\ & & & 6\end{pmatrix}P^{-1}$$

where

$$P = \begin{pmatrix} 1 & -2 & 5 & -3 \\ 2 & -1 & 4 & 2 \\ -2 & 3 & -2 & 5 \\ 4 & -1 & 0 & 4 \end{pmatrix} \in GL_4(\mathbb{C}).$$

By applying Theorem 3.4.2 to the matrix B with $n = 4$ and $k = 2$, we obtain

1. $\Lambda^2((2I_4 - B)(6I_4 - B)) = 60\ \Lambda^2(P)p_{\{1,2\}}\Lambda^2(P^{-1})$.

2. $\Lambda^2((I_4 - B)(6I_4 - B)) = -24\ \Lambda^2(P)p_{\{1,3\}}\Lambda^2(P^{-1})$.

3. $\Lambda^2((I_4 - B)(2I_4 - B)) = 40\ \Lambda^2(P)p_{\{1,4\}}\Lambda^2(P^{-1})$.

4. $\Lambda^2(-B(6I_4 - B)) = 40\ \Lambda^2(P)p_{\{2,3\}}\Lambda^2(P^{-1})$.

5. $\Lambda^2(-B(2I_4 - B)) = -24\ \Lambda^2(P)p_{\{2,4\}}\Lambda^2(P^{-1})$.

6. $\Lambda^2(-B(I_4 - B)) = 60\ \Lambda^2(P)p_{\{3,4\}}\Lambda^2(P^{-1})$.

From equation (3.9), we compute that $\Lambda^2(A) = \Lambda^2(P)\ diag[1, 2, 6, 2, 6, 12]\ \Lambda^2(P)^{-1}$, which is explicitly from Definition 3.4.1

$$\Lambda^2(A) = \Lambda^2(P)(p_{\{1,2\}} + 2p_{\{1,3\}} + 6p_{\{1,4\}} + 2p_{\{2,3\}} + 6p_{\{2,4\}} + 12p_{\{3,4\}})\Lambda^2(P^{-1}).$$

Consequently, we can use the above computations from Theorem 3.4.2 to express $\Lambda^2(A)$ as the following $\mathbb{Q}$-linear combination:

$$\begin{aligned} \Lambda^2(A) = &\frac{1}{60}\Lambda^2((2I_4 - B)(6I_4 - B)) - \frac{1}{12}\Lambda^2((I_4 - B)(6I_4 - B)) \\ &+\frac{3}{20}\Lambda^2((I_4 - B)(2I_4 - B)) + \frac{1}{20}\Lambda^2(-B(6I_4 - B)) \\ &-\frac{1}{4}\Lambda^2(-B(2I_4 - B)) + \frac{1}{5}\Lambda^2(-B(I_4 - B)). \end{aligned}$$

By Theorem 2.1.2, the elements of $\Lambda^2(A)$ are the 2×2 minors of A. So, the decomposition above provides a decomposition of the 2×2 minors of A as the sum of other 2×2 minors. For example, if we take the $\{1, 2\}, \{1, 2\}$ element of both sides, we obtain the equation

$$\begin{aligned} \begin{vmatrix} 314/9 & -65/2 \\ -152/9 & 19 \end{vmatrix} = &\frac{1}{60}\begin{vmatrix} -176/9 & 18 \\ 488/9 & -54 \end{vmatrix} - \frac{1}{12}\begin{vmatrix} 52/9 & -11 \\ 272/9 & -34 \end{vmatrix} + \frac{3}{20}\begin{vmatrix} 1144/9 & -127 \\ -592/9 & 66 \end{vmatrix} \\ &+\frac{1}{20}\begin{vmatrix} 280/9 & -40 \\ 56/9 & -14 \end{vmatrix} - \frac{1}{4}\begin{vmatrix} 1408/9 & -156 \\ -808/9 & 90 \end{vmatrix} + \frac{1}{5}\begin{vmatrix} 1690/9 & -185 \\ -1024/9 & 116 \end{vmatrix} \end{aligned}$$

which can be checked by direct computation to be true.

Our main goal now is to use Theorem 3.4.2 to generalise Theorem 3.4.1. To this end, we will now work in $\mathbb{C}$. For $A \in M_{n\times n}(\mathbb{C})$, we will denote the complex conjugate transpose of A as A^*.

Theorem 3.4.4. *Let $A \in M_{n\times n}(\mathbb{C})$ and $\lambda_1, \ldots, \lambda_n$ be distinct eigenvalues of A with corresponding eigenvectors $v_1, \ldots, v_n$. Suppose that there exists a unitary matrix U such that $A = U diag[\lambda_1, \ldots, \lambda_n]U^*$. If $L = \{i_1, \ldots, i_k\} \in T_{\binom{n}{k}}$ with $k \in \{1, \ldots, n-1\}$, define $v_L = v_{i_1} \wedge \cdots \wedge v_{i_k}$. If $M, P \in T_{\binom{n}{k}}$ and $v_{L,M}$ is the M element of v_L then*

$$v_{L,M}\overline{v_{L,P}} = \frac{1}{\Big(\prod_{l\in L,\, a\in L^c}(\lambda_a - \lambda_l)\Big)}\big(\Lambda^k(\prod_{a\in L^c}(\lambda_a I_n - A))\big)_{M,P} \tag{3.13}$$

and

$$v_{L,M}\overline{v_{L,P}} = \frac{s_{M,\mathbb{Z}_{[1,n]}}s_{P,\mathbb{Z}_{[1,n]}}}{\Big(\prod_{l\in L,\, a\in L^c}(\lambda_l - \lambda_a)\Big)}\big(\Lambda^{n-k}(\prod_{a\in L}(\lambda_a I_n - A))\big)_{P^c,M^c}. \tag{3.14}$$

where $s_{M,\mathbb{Z}_{[1,n]}}$ and $s_{P,\mathbb{Z}_{[1,n]}}$ are the signs from Definition 2.3.1.

Proof. Assume that $A \in M_{n\times n}(\mathbb{C})$ satisfies $A = U\ diag[\lambda_1, \ldots, \lambda_n]\ U^*$ for some unitary matrix U. Assume that $k \in \{1, \ldots, n-1\}$ and $M, P \in T_{\binom{n}{k}}$. An application of Theorem 3.4.2 gives

$$\Lambda^k(\prod_{a\in L^c}(\lambda_a I_n - A)) = \Big(\prod_{l\in L,\, a\in L^c}(\lambda_a - \lambda_l)\Big)\ \Lambda^k(U)p_L\Lambda^k(U^*).$$

Taking the M, P entry of both sides then yields equation (3.13). Similarly, if we apply Theorem 3.4.3 then we obtain

$$\Upsilon^{n-k}(\prod_{a\in L}(\lambda_a I_n - A)) = \Big(\prod_{l\in L,\, a\in L^c}(\lambda_l - \lambda_a)\Big)\ \Lambda^k(U)p_L\Lambda^k(U^*).$$

Taking the M, P entry of both sides and using equation (3.1) on the LHS gives equation (3.14). □

Theorem 3.4.1 allows one to compute eigenvectors of a matrix $A \in M_{n\times n}(\mathbb{C})$ satisfying $AA^* = A^*A$ from its eigenvalues. As we will see in the example below, Theorem 3.4.4 tells us that knowledge of the eigenvalues λ_i allows us to compute wedge products of eigenvectors, even without knowing the eigenvectors of A themselves.

Example 3.4.3. Let

$$A = \begin{pmatrix} -1 & 1 & 2 & -3 \\ 1 & 3 & -4 & 1 \\ 2 & -4 & -3 & -2 \\ -3 & 1 & -2 & 1 \end{pmatrix}.$$

The eigenvalues of A are $\lambda_1 = -6$, $\lambda_2 = -3$, $\lambda_3 = 3$ and $\lambda_4 = 6$. We will compute the wedge product $v_2 \wedge v_4 = v_{\{2,4\}}$. With $L = \{2,4\}$, the LHS of equation (3.13) is

$$\begin{aligned}\Lambda^k(\prod_{l\in L^c}(\lambda_l I_n - A)) &= \Lambda^2(\prod_{l\in\{1,3\}}(\lambda_l I_3 - A)) \\ &= \Lambda^2((-6I_4 - A)(3I_4 - A)) \\ &= \Lambda^2\begin{pmatrix} -6 & -6 & 0 & -12 \\ -6 & 18 & -12 & 12 \\ 0 & -12 & 6 & -12 \\ -12 & 12 & -12 & 0 \end{pmatrix}.\end{aligned}$$

By direct computation, the first column of $\Lambda^2((-6I - A)(3I - A))$ (indexed by the set $\{1,2\}$) is $[-144, 72, -144, 72, 144, -144]^T$. On the RHS of equation (3.13), we have

$$\prod_{l\in L,\, a\in L^c}(\lambda_a - \lambda_l) = -648.$$

By taking $M = P = \{1,2\}$ in equation (3.13), $-144 = -648(v_{\{2,4\},\{1,2\}})^2$. So, $v_{\{2,4\},\{1,2\}} = \sqrt{2}/3$, where we chose the positive square root. Now, we take $M = \{1,3\}$ and $P = \{1,2\}$ so that,

$$-648\; v_{\{2,4\},\{1,3\}}\overline{v_{\{2,4\},\{1,2\}}} = \left(\Lambda^2((-6I - A)(3I - A))\right)_{\{1,3\},\{1,2\}} = 72.$$

Thus, $v_{\{2,4\},\{1,3\}} = -1/9 \times 3/\sqrt{2} = -\sqrt{2}/6$. By fixing $P = \{1,2\}$, varying $M \in T_{\binom{n}{k}}$ and using equation (3.13), we find that $v_{\{2,4\},\{2,3\}} = -\sqrt{2}/6$, $v_{\{2,4\},\{2,4\}} = -\sqrt{2}/3$ and $v_{\{2,4\},\{1,4\}} = v_{\{2,4\},\{3,4\}} = \sqrt{2}/3$. Therefore,

$$v_{\{2,4\}} = \begin{pmatrix} \sqrt{2}/3 \\ -\sqrt{2}/6 \\ \sqrt{2}/3 \\ -\sqrt{2}/6 \\ -\sqrt{2}/3 \\ \sqrt{2}/3 \end{pmatrix} \begin{matrix} \{1,2\} \\ \{1,3\} \\ \{1,4\} \\ \{2,3\} \\ \{2,4\} \\ \{3,4\} \end{matrix} \tag{3.15}$$

The constituent eigenvectors of the wedge product in equation (3.15) are

$$v_2 = \begin{pmatrix} 2/3 \\ 0 \\ 1/3 \\ 2/3 \end{pmatrix} \text{ and } v_4 = \begin{pmatrix} \sqrt{2}/6 \\ -1/\sqrt{2} \\ \sqrt{2}/3 \\ -\sqrt{2}/3 \end{pmatrix}.$$

By computing the wedge product $v_2 \wedge v_4$ directly, we obtain equation (3.15) scaled by a factor of -1.

We will finish this section with a proof of Theorem 3.4.1 for matrices $A \in M_{n\times n}(\mathbb{C})$ $AA^* = A^*A$. Recall that if $AA^* = A^*A$ then there exists a unitary matrix $U \in GL_n(\mathbb{C})$ such that $A = Udiag[\lambda_1, \ldots, \lambda_n]U^*$.

Proof of Theorem 3.4.1. Assume that $A \in M_{n\times n}(\mathbb{C})$ satisfies $AA^* = A^*A$. Let $\lambda_1, \ldots, \lambda_n$ denote the distinct eigenvalues of A and $v_1, \ldots, v_n$ be the corresponding eigenvectors. Let $\mu_1^{(j)}, \ldots, \mu_{n-1}^{(j)}$ be the eigenvalues of A_{j^c,j^c}.

From equation (3.14), we have

$$\left(\Lambda^{n-k}(\prod_{a\in L}(\lambda_a I_n - A))\right)_{M^c,M^c} = \prod_{a\in L,\, l\in L^c} (\lambda_a - \lambda_l)\, |v_{L,M}|^2$$

where $L, M \in T_{\binom{n}{k}}$. Specialising to the case $k = 1$, let $i, j \in \{1, 2, \ldots, n\}$ and $M = \{j\} \in T_{\binom{n}{1}}$ and $L = \{i\} \in T_{\binom{n}{1}}$ so that

$$\left(\Lambda^{n-1}(\lambda_i I_n - A)\right)_{M^c,M^c} = \prod_{l=1,\, l\neq i}^{n} (\lambda_i - \lambda_l)\, |v_{i,j}|^2. \tag{3.16}$$

From Theorem 2.1.2,

$$\left(\Lambda^{n-1}(\lambda_i I_n - A)\right)_{M^c,M^c} = \det((\lambda_i I_n - A)_{M^c,M^c}) = \det(\lambda_i I_{n-1} - A_{j^c,j^c}).$$

By diagonalising $A_{j^c,j^c} \in M_{(n-1)\times(n-1)}(\mathbb{C})$, we find that

$$\det(\lambda_i I_{n-1} - A_{j^c,j^c}) = \prod_{k=1}^{n-1}(\lambda_i - \mu_k^{(j)}).$$

Substituting the above equality into the LHS of equation (3.16), we find that if $i \in \{1, 2, \ldots, n\}$ then

$$|v_{i,j}|^2 \prod_{l=1,\, l\neq i}^{n} (\lambda_i - \lambda_l) = \prod_{k=1}^{n-1}(\lambda_i - \mu_k^{(j)})$$

as required. □

Chapter 4

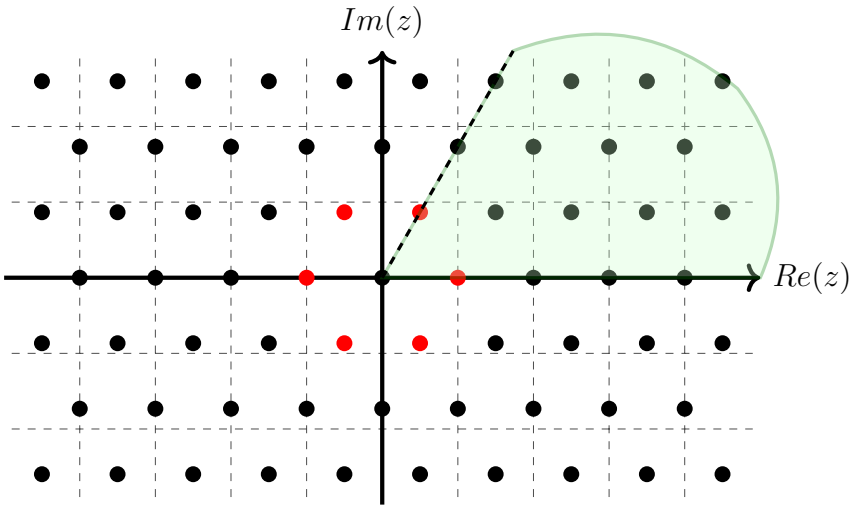
Smith normal form

4.1 Steinberg reduction

In the next two chapters, wedge product matrices are used to obtain invariants of a matrix orbit — quantities which remain unchanged throughout the entire orbit — and to construct a particular representative of the matrix orbit. The flagship method we will employ for constructing representatives originates from [Ste67, §8], where it was used to prove multiple variants of the Bruhat decomposition of a Chevalley group (see [Ste67, Theorem 4]). Our variant of the method will be called *Steinberg reduction*. The goal of this section is to provide an explicit description of Steinberg reduction suitable for the construction of matrix representatives in this chapter and the next.

Let R be a principal ideal domain and $R^\times$ be the group of units of R, which acts on R via multiplication. The set of $R^\times$-orbits $R/R^\times$ consists of representatives of the ideals of R.

Example 4.1.1. Let $\omega = e^{2\pi i/3}$ and $R = \mathbb{Z}[\omega]$ denote the ring of Eisenstein integers. Then, $R^\times = \{\pm 1, \pm\omega, \pm\omega^2\}$. The representatives of the $R^\times$-orbits in $R/R^\times$ are depicted pictorially by the sector $0 \leq \arg(z) < \pi/3$:



Each black point corresponds to an element of R and the six red points are the units of R. The shaded green sector without the dashed black line contains the elements of $R/R^\times$. For example, the point $-\omega^2 = 1 + \omega$ lies on the dashed black line, but $-\omega^2 R = R$ as ideals in R.

Definition 4.1.2. Let R be a PID and $g_1, g_2, \ldots, g_n \in R$. The greatest common divisor $\gcd(g_1, g_2, \ldots, g_n)$ is an element of $R/R^\times$ satisfying

$$\gcd(g_1, g_2, \ldots, g_n)R = g_1R + g_2R + \cdots + g_nR.$$

Let $A = (a_{ij}) \in M_{m\times n}(R)$. We define $\gcd(A)$ to be

$$\gcd(A) = \gcd(a_{11}, a_{12}, \ldots, a_{mn}).$$

In an abuse of notation, we will refer to the gcd as both a representative of an ideal in $R/R^\times$ and as an element of R, up to multiplication by a unit.

In [Ste67, Theorem 15], the Bruhat decomposition provided by Steinberg relies on a particular subset of $SL_2(R)$. For our purposes, we will follow this approach and define

$$Y(R) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(R) \;\middle|\; \begin{matrix} c \in (R - \{0\})/R^\times, \\ d \in R/cR \end{matrix} \right\} \cup \{\pm I_2\} \tag{4.1}$$

where I_2 denotes the 2×2 identity matrix.

4.1.1 Steinberg reduction on a 2×1 matrix

Assume that $(a, b)^T \in M_{2\times 1}(R)$. We will construct a matrix

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in Y(R) \qquad \text{such that} \qquad \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \gcd(a, b) \\ 0 \end{pmatrix}. \tag{4.2}$$

There are three separate cases to consider.

Case 1: $a \neq 0$ and $b \neq 0$

Step 1: Since R is a unique factorisation domain, select $r, s \in R$ such that $ra+sb = 0$, $r \in R-\{0\}/R^\times$ and $\gcd(r, s) = 1$. This is accomplished by selecting $r \in R-\{0\}/R^\times$ and $s \in R$ such that $a = \gcd(a, b)s$ and $b = -\gcd(a, b)r$.

Step 2: Since $\gcd(r, s) = 1$ from step 1, choose $p, q \in R$ such that $ps - qr = 1$. For all $t \in \mathbb{Z}$, define $p_t = p - rt$ and $q_t = q - st$ so that $p_t s - q_t r = 1$. Then, select $v \in \mathbb{Z}$ such that $p_v \in R/rR$.

Step 3: The result of Steinberg reduction is a matrix

$$\begin{pmatrix} p_v & q_v \\ r & s \end{pmatrix} \in Y(R) \qquad \text{satisfying} \qquad \begin{pmatrix} p_v & q_v \\ r & s \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \gcd(a, b) \\ 0 \end{pmatrix}$$

because $p_v a + q_v b = (p_v s - q_v r)\gcd(a,b) = \gcd(a,b)$.

Case 2: $a = 0$ and $b \neq 0$

Assume that $(0,b)^T \in M_{2\times 1}(R)$. Then, the matrix

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in Y(R) \qquad \text{satisfies} \qquad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ b \end{pmatrix} = \begin{pmatrix} -b \\ 0 \end{pmatrix}.$$

Case 3: $b = 0$

In this vacuous case, the matrix $(a,0)^T \in M_{2\times 1}(R)$ is already in the form required by equation (4.2).

4.1.2 Steinberg reduction on a $n \times 1$ matrix

Assume that $n \in \mathbb{Z}_{>1}$. For $i,j \in \{1,2,\ldots,n\}$, define the map $\varphi_{i,j} : GL_2(R) \to GL_n(R)$ by

$$\begin{aligned} \varphi_{i,j} : \ GL_2(R) \ &\to \quad GL_n(R) \\ \begin{pmatrix} p & q \\ r & s \end{pmatrix} \ &\mapsto \ \varphi_{i,j}(p,q,r,s) \end{aligned}$$

where the 2×2 block formed from the i^{th} and j^{th} rows and columns of $\varphi_{i,j}(p,q,r,s)$ is

$$(\varphi_{i,j}(p,q,r,s))_{\{i,j\},\{i,j\}} = \begin{pmatrix} p & q \\ r & s \end{pmatrix}.$$

The remaining diagonal entries of $\varphi_{i,j}(p,q,r,s)$ are 1 and the remaining non-diagonal entries are 0.

Assume that $(a_1,\ldots,a_n)^T \in M_{n\times 1}(R)$. The goal of Steinberg reduction in this case is to construct a matrix $A \in GL_n(R)$ such that

$$A \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} g \\ 0 \\ \vdots \\ 0 \end{pmatrix} \qquad \text{where} \qquad g = \gcd(a_1,a_2,\ldots,a_n).$$

Step 1: Using Steinberg reduction for the 2×1 case, obtain $p_{n-1}, q_{n-1}, r_{n-1}, s_{n-1} \in R$ such that

$$\begin{pmatrix} p_{n-1} & q_{n-1} \\ r_{n-1} & s_{n-1} \end{pmatrix} \in Y(R) \qquad \text{and} \qquad \begin{pmatrix} p_{n-1} & q_{n-1} \\ r_{n-1} & s_{n-1} \end{pmatrix} \begin{pmatrix} a_{n-1} \\ a_n \end{pmatrix} = \begin{pmatrix} \gcd(a_{n-1},a_n) \\ 0 \end{pmatrix}.$$

In the case where $a_n = 0$, we select $p_n = s_n = 1$ and $q_n = r_n = 0$, which yields the identity matrix $I_2 \in Y(R)$. Consequently, we have

$$\varphi_{n-1,n}(p_{n-1}, q_{n-1}, r_{n-1}, s_{n-1}) \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_{n-1} \\ a_n \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ \gcd(a_{n-1}, a_n) \\ 0 \end{pmatrix}.$$

Step 2: For $i \in \{1, \ldots, n-2\}$, repeat Step 1 for each matrix $(a_{n-i-1}, g_{n-i})^T \in M_{2\times 1}(R)$, where $g_i = \gcd(a_i, a_{i+1}, \ldots, a_n)$. This ensures that

$$\varphi_{1,2}(p_1, q_1, r_1, s_1)\varphi_{2,3}(p_2, q_2, r_2, s_2) \ldots \varphi_{n-1,n}(p_{n-1}, q_{n-1}, r_{n-1}, s_{n-1}) \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} g_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

where

$$\varphi_{1,2}(p_1, q_1, r_1, s_1)\varphi_{2,3}(p_2, q_2, r_2, s_2) \ldots \varphi_{n-1,n}(p_{n-1}, q_{n-1}, r_{n-1}, s_{n-1}) \in GL_n(R).$$

4.2 Smith normal form algorithm

4.2.1 The case of $n \times 1$ matrices

The matrix orbit space we are interested in is $GL_m(R)\backslash M_{m\times n}(R)/GL_n(R)$, where R is a PID. It is proved in [Art91, Chapter 12, Section 5] and [Rot03, Section 9.4] that if $A \in M_{m\times n}(R)$, then a representative of the matrix orbit $GL_m(R) \cdot A \cdot GL_n(R)$ is given by its *Smith normal form* — a diagonal matrix $D = (d_{ij}) \in M_{m\times n}(R)$ satisfying $d_{11}|d_{22}|\ldots|d_{kk}$, where $k = \min(m, n)$. To be clear, $d_{11}|d_{22}$ means d_{11} divides d_{22}.

Theorem 4.2.1 is a consequence of Steinberg reduction and can be thought of as computing the Smith normal form of a $n \times 1$ matrix.

Theorem 4.2.1. *Let R be a PID. Then, the following map is a bijection:*

$$\begin{aligned} \phi : \quad R/R^\times \quad &\to \quad GL_n(R) \cdot M_{n\times 1}(R) \\ g \quad &\mapsto \quad GL_n(R) \cdot \begin{pmatrix} g \\ 0 \\ \vdots \\ 0 \end{pmatrix} \end{aligned}$$

with inverse given by

$$\phi^{-1}: \quad GL_n(R) \cdot M_{n\times 1}(R) \quad \to \qquad R/R^\times$$

$$GL_n(R) \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \quad \mapsto \quad \gcd(a_1, a_2, \ldots, a_n).$$

Proof. Assume that R is a PID. Assume that $(a_1, a_2, \ldots, a_n)^T \in M_{n\times 1}(R)$. By following the steps of Steinberg reduction in subsection 4.1.2, we obtain a matrix $A \in GL_n(R)$ which satisfies

$$A \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} \gcd(a_1, \ldots, a_n) \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{4.3}$$

Thus, the map ϕ^{-1} is a well-defined map from the orbit space $GL_n(R) \cdot M_{n\times 1}(R)$ to $R/R^\times$. Moreover, the maps ϕ and ϕ^{-1} are inverses of each other because from equation (4.3), we have the equality of matrix orbits

$$GL_n(R) \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = GL_n(R) \cdot \begin{pmatrix} \gcd(a_1, \ldots, a_n) \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

□

Corollary 4.2.2 is obtained by taking the transpose of the RHS of the bijection ϕ in Theorem 4.2.1. It forms an important part of the Smith normal form algorithm we describe in the next section.

Corollary 4.2.2. *Let R be a PID. Then, the following map is a bijection:*

$$\psi: \quad R/R^\times \quad \to \qquad M_{1\times n}(R) \cdot GL_n(R)$$

$$g \qquad \mapsto \quad \begin{pmatrix} g & 0 & \ldots & 0 \end{pmatrix} \cdot GL_n(R)$$

4.2.2 Reduction to a diagonal form

We will now describe in detail an algorithm for computing the Smith Normal form of a matrix $A = (a_{ij}) \in M_{m\times n}(R)$, which uses Theorem 4.2.1 and Corollary 4.2.2 extensively. The first part of the algorithm converts A to a form where at the very least, all the non-main diagonal elements of A are zero. Suppose that

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}.$$

Step 1: (First column of A) Use Theorem 4.2.1 to construct a matrix $B \in GL_m(R)$ such that

$$BA = \begin{pmatrix} g_1 & a_{12} & \dots & a_{1n} \\ 0 & a'_{22} & \dots & a'_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a'_{m2} & \dots & a'_{mn} \end{pmatrix} \qquad \text{where} \qquad g_1 = \gcd(a_{11}, a_{21}, \dots, a_{m1}).$$

Step 2: (First row of A) Next, Corollary 4.2.2 tells us that there exists a matrix $B_2 \in GL_n(R)$ such that

$$\begin{pmatrix} g_1 & a_{12} & \dots & a_{1n} \\ 0 & a'_{22} & \dots & a'_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a'_{m2} & \dots & a'_{mn} \end{pmatrix} B_2 = \begin{pmatrix} g_2 & 0 & \dots & 0 \\ * & a''_{22} & \dots & a''_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ * & a''_{m2} & \dots & a''_{mn} \end{pmatrix}$$

Here g_2 is the gcd of all of the elements in the first row and first column of A and $*$ represents some unknown elements.

Step 3: (First row and first column of A) If there exists a non-zero element below g_2 in the current matrix we have, then repeat steps 1 and 2 until the matrix takes the form

$$\begin{pmatrix} h_1 & 0 & \dots & 0 \\ 0 & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & b_{m2} & \dots & b_{mn} \end{pmatrix}.$$

This process creates a chain of ideals

$$g_1R \subseteq g_2R \subseteq g_3R \subseteq \dots$$

Since R is a PID, it satisfies the ascending chain condition. Hence, there exists an ideal h_1R within the chain, which contains all of the ideals in the chain above. Consequently, h_1 will divide every non-zero element remaining in either the first row or first column of the matrix, allowing it to take the form above.

Step 4: Repeat the first three steps for the ℓ^{th} row and ℓ^{th} column of the matrix, where $\ell \in \{2, \dots, k = \min(m, n)\}$ to obtain a sequence of elements h_1, $\dots$, h_k on the main diagonal of the matrix

$$\begin{pmatrix} h_1 & & & \\ & h_2 & & \\ & & \ddots & \\ & & & h_k \end{pmatrix}.$$

4.2.3 Organising the main diagonal

So far, it is not necessarily the case that $h_1|h_2|\dots|h_k$. The point of the second part of the algorithm is to rectify this issue and obtain the Smith normal form of A. From here, we will treat the case where $m = n$ and the current matrix is the diagonal square matrix $diag[h_1, \dots, h_n]$, since the other cases ($m > n$ and $m < n$) are very similar.

Definition 4.2.1. Let R be a PID and $c \in R$. Define $x_{m,ij}(c) \in GL_m(R)$ to be a triangular matrix such that each diagonal entry of $x_{m,ij}(c)$ is 1, $(x_{m,ij}(c))_{ij} = c$ and every other entry is zero.

We now describe the second part of the Smith normal form algorithm, continuing from step 4 and beginning with step 5.

Step 5: Assume that there exists $r \in \{2, \dots, k\}$ such that $h_1 \nmid h_r$. To rectify this, we do the matrix multiplication below.

$$\begin{pmatrix} h_1 & 0 & \dots & 0 & \dots & 0 \\ 0 & h_2 & \dots & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & h_r & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & \dots & h_n \end{pmatrix} x_{n,r1}(1) = \begin{pmatrix} h_1 & 0 & \dots & 0 & \dots & 0 \\ 0 & h_2 & \dots & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ h_r & 0 & \dots & h_r & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & \dots & h_n \end{pmatrix}$$

where the matrix $x_{n,r1}(1) \in GL_n(R)$ is from Definition 4.2.1. This leaves h_1 and h_r as the only two non-zero elements in the first column of the matrix. Now we use Steinberg reduction in subsection 4.1.1 to construct the matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(R) \qquad \text{such that} \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} h_1 \\ h_r \end{pmatrix} = \begin{pmatrix} \gcd(h_1, h_r) \\ 0 \end{pmatrix}$$

and consequently,

$$\varphi_{1,r}(a,b,c,d) \begin{pmatrix} h_1 & 0 & \dots & 0 & \dots & 0 \\ 0 & h_2 & \dots & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ h_r & 0 & \dots & h_r & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & \dots & h_n \end{pmatrix} = \begin{pmatrix} i_1 & 0 & \dots & \alpha h_r & \dots & 0 \\ 0 & h_2 & \dots & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & \beta h_r & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & \dots & h_n \end{pmatrix}$$

where $\alpha, \beta \in R$ and $i_1 = \gcd(h_1, h_r)$. So, there exists $p \in R$ such that $pi_1 = h_r$. Hence, the final matrix multiplication in this step is

$$\begin{pmatrix} i_1 & 0 & \dots & \alpha h_r & \dots & 0 \\ 0 & h_2 & \dots & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & \beta h_r & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & \dots & h_n \end{pmatrix} x_{n,1r}(-p\alpha) = \begin{pmatrix} i_1 & 0 & \dots & 0 & \dots & 0 \\ 0 & h_2 & \dots & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & \beta h_r & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & \dots & h_n \end{pmatrix}$$

which renders the matrix diagonal.

Step 6: Repeat step 5 for all $s \in \{2, \dots, k\}$ satisfying $i_1 \nmid h_s$, until the a_{11} element of the matrix divides all of the other diagonal elements. After this is done, the matrix we obtain is

$$\begin{pmatrix} d_1 & 0 & \dots & 0 & \dots & 0 \\ 0 & x_2 & \dots & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & x_r & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & \dots & x_n \end{pmatrix} \qquad \text{where} \qquad d_1 = \gcd(h_1, h_2, \dots, h_n).$$

Step 7: Repeat steps 5 and 6 for each of the other diagonal elements in succession, systematically beginning with the a_{22} element of the matrix and ending with the a_{nn} element. After this is done, the matrix becomes

$$\begin{pmatrix} d_1 & 0 & \dots & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & d_r & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & \dots & d_n \end{pmatrix} \qquad \text{with} \qquad d_1 | d_2 | \dots | d_n.$$

The above algorithm constitutes a proof of Smith normal form.

Theorem 4.2.3 (Smith Normal Form)**.** *Let R be a PID, $A \in M_{m\times n}(R)$, $P \in GL_m(R)$ be the product of the matrices multiplied on the LHS in the algorithm and $Q \in GL_n(R)$ be the product of all the matrices multiplied on the RHS in the algorithm. Then, $A = PDQ$ where $D = (d_{ij})$ consists of the elements $d_{jj} = d_j$ for all $j \in \{1, \dots, \min(m, n)\}$ and zeros elsewhere. Furthermore, $d_1 | d_2 | \dots | d_k$ with $k = \min(m, n)$.*

Example 4.2.2. Let $R = \mathbb{Z}$ and

$$A = \begin{pmatrix} 2 & 3 & -5 \\ -4 & 1 & -9 \\ 7 & 8 & -3 \end{pmatrix}.$$

Step 1 of the algorithm reveals that, after applying Theorem 4.2.1 twice

$$\begin{pmatrix} 1 & -1 & \\ -1 & 2 & \\ & & 1 \end{pmatrix} \begin{pmatrix} 1 & & \\ & -2 & -1 \\ & -7 & -4 \end{pmatrix} \begin{pmatrix} 2 & 3 & -5 \\ -4 & 1 & -9 \\ 7 & 8 & -3 \end{pmatrix} = \begin{pmatrix} 1 & 13 & -26 \\ 0 & -23 & 47 \\ 0 & -39 & 75 \end{pmatrix}.$$

In the second step, we focus on the first row of the matrix. Fortunately, 1 divides both 13 and -26 and the next calculation is

$$\begin{pmatrix} 1 & 13 & -26 \\ 0 & -23 & 47 \\ 0 & -39 & 75 \end{pmatrix} \begin{pmatrix} 1 & -13 & \\ & 1 & \\ & & 1 \end{pmatrix} \begin{pmatrix} 1 & & 26 \\ & 1 & \\ & & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -23 & 47 \\ 0 & -39 & 75 \end{pmatrix}.$$

The third step of the algorithm is simply reapplying the first two steps to bottom right 2×2 minor of our current matrix. Applying the first step again, we have the computation

$$\begin{pmatrix} 1 & & \\ & 17 & -10 \\ & -39 & 23 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -23 & 47 \\ 0 & -39 & 75 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 49 \\ 0 & 0 & -108 \end{pmatrix}.$$

Finally, applying the second step to the bottom right 2×2 minor renders the matrix diagonal.

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 49 \\ 0 & 0 & -108 \end{pmatrix} \begin{pmatrix} 1 & & \\ & 1 & 49 \\ & & 1 \end{pmatrix} = \begin{pmatrix} 1 & & \\ & -1 & \\ & & -108 \end{pmatrix}.$$

We do not need to proceed further with the algorithm because the diagonal matrix above is in Smith Normal form, as $1|-1|-108$. In this case, $d_1 = 1$, $d_2 = -1$ and $d_3 = -108$.

4.3 Smith normal form invariants

In Theorem 4.2.3, $D \in M_{m\times n}(R)$ is a representative of the matrix orbit $GL_m(R) \cdot A \cdot GL_n(R)$. Wedge product matrices provide us with a method for finding invariants of the orbit $GL_m(R) \cdot A \cdot GL_n(R)$, which helps us to understand Smith normal form better. First, Lemma 4.3.1 is pertinent to our analysis of these invariants. Recall from Definition 4.1.2 that if $A = (a_{ij}) \in M_{m\times n}(R)$ then we define

$$\gcd(A) = \gcd(a_{11}, a_{12}, \ldots, a_{nn}).$$

Lemma 4.3.1. *Let R be a PID and $A = (a_{ij}) \in M_{m\times n}(R)$. Let $B = (b_{ij}) \in GL_m(R)$ and $C = (c_{ij}) \in GL_n(R)$. Then,* $\gcd(A) = \gcd(BAC)$.

Proof. Assume that R is a PID. Assume that A, B and C are the matrices defined as in the statement of the lemma.

To show: (a) $\gcd(A) = \gcd(BA)$.

(b) $\gcd(A) = \gcd(AC)$.

(a) The elements of BA are of the form $\sum_{i=1}^{m} b_{ji}a_{ik}$ where $j \in \{1, \ldots, m\}$ and $k \in \{1, \ldots, n\}$. Since B is invertible, Laplace expansion on the k^{th} column of B yields the equality of ideals

$$b_{1k}R + b_{2k}R + \cdots + b_{mk}R = R.$$

So, $\gcd(b_{1k}, \ldots, b_{mk}) = 1$ for all $k \in \{1, \ldots, n\}$. To see that $\gcd(A) = \gcd(BA)$, we compute directly from the elements of BA that

$$\begin{aligned}
\gcd(BA)R &= \sum_{k=1}^{n}\sum_{j=1}^{m}\Big(\sum_{l=1}^{m} b_{jl}a_{lk}R\Big) \\
&= \sum_{k=1}^{n}\sum_{l=1}^{m}(b_{1l} + b_{2l} + \cdots + b_{ml})a_{lk}R \\
&= \sum_{l=1}^{m}\big((b_{1l} + b_{2l} + \cdots + b_{ml})R\big)(a_{l1} + a_{l2} + \cdots + a_{ln}) \\
&= \sum_{l=1}^{m} R(a_{l1} + a_{l2} + \cdots + a_{ln}) \\
&= \gcd(A)R.
\end{aligned}$$

(b) Since $\gcd(X) = \gcd(X^T)$ for all $X \in M_{m\times n}(R)$, we can use part (a) to deduce that $\gcd(AC) = \gcd(C^TA^T) = \gcd(A^T) = \gcd(A)$.

Therefore, $\gcd(A) = \gcd(BAC)$ as required. □

Proposition 4.3.2. *Let R be a PID. Let $A \in M_{m\times n}(R)$ and d_i be the diagonal entries of the Smith normal form of A produced by the algorithm resulting in Theorem 4.2.3, where $i \in \{1, \ldots, k\}$, $k = \min(m, n)$ and $d_1|\ldots|d_k$. Then,*

(a) $\prod_{j=1}^{i} d_j = \gcd(\Lambda^i(A))$.

(b) The quantity $\gcd(\Lambda^i(A))$ is an invariant of the orbit $GL_m(R) \cdot A \cdot GL_n(R)$.

Proof. Assume that R is a PID and $A \in M_{m\times n}(R)$. Assume that d_i are the diagonal entries of the Smith normal form of A for $i \in \{1, \ldots, k\}$, where $k = \min(m, n)$.

Part (a): By Theorem 4.2.3, there exists $P \in GL_m(R)$ and $Q \in GL_n(R)$ such that $A = PDQ$, where D is the Smith normal form of A. So $\Lambda^i(A) = \Lambda^i(P)\Lambda^i(D)\Lambda^i(Q)$, and since P and Q are invertible, $\Lambda^i(P)$ and $\Lambda^i(Q)$ must also be invertible by Corollary 2.2.4. From Lemma 4.3.1, we conclude that

$$\gcd(\Lambda^i(A)) = \gcd(\Lambda^i(D)) = \gcd(\{\prod_{j\in L} d_j \mid L \in T_{\binom{k}{i}}\}) = \prod_{j\in\{1,2,\ldots,i\}} d_j = d_1d_2\ldots d_i,$$

since $d_1|d_2|\ldots|d_k$.

Part (b): From part (a), we found that if $i \in \{1, 2, \ldots, k\}$ then $\gcd(\Lambda^i(A)) = \gcd(\Lambda^i(D))$. Thus, $\gcd(\Lambda^i(A))$ is an invariant of the matrix orbit $GL_m(R) \cdot A \cdot GL_n(R)$. □

We observe that the gcd of the $i \times i$ minors of A is equal to $\gcd(\Lambda^i(A))$ by Theorem 2.1.2. Thus, Proposition 4.3.2 tells us that the gcd of the $i \times i$ minors of $A \in M_{m\times n}(R)$ for $i \in \{1, \ldots, \min(m, n)\}$ is invariant under the matrix orbit $GL_m(R) \cdot A \cdot GL_n(R)$. We will call these *Smith normal form invariants.*

Theorem 4.3.3 demonstrates the connection between the Smith normal form invariants and the orbit space $GL_m(R)\backslash M_{m\times n}(R)/GL_n(R)$.

Theorem 4.3.3. *Let R be a PID. Let $A, B \in M_{m\times n}(R)$. Then*

$$GL_m(R) \cdot A \cdot GL_n(R) = GL_m(R) \cdot B \cdot GL_n(R)$$

if and only if A and B have the same Smith normal form invariants.

Proof. Assume that R is a PID. Assume that $A, B \in M_{m\times n}(R)$.

To show: (a) If $GL_m(R) \cdot A \cdot GL_n(R) = GL_m(R) \cdot B \cdot GL_n(R)$, then A and B have the same Smith normal form invariants.

(b) If A and B have the same Smith normal form invariants, then

$$GL_m(R) \cdot A \cdot GL_n(R) = GL_m(R) \cdot B \cdot GL_n(R).$$

Proof of (a): Assume that $GL_m(R)\cdot A\cdot GL_n(R) = GL_m(R)\cdot B\cdot GL_n(R)$. Then, there exists $X \in GL_m(R)$ and $Y \in GL_n(R)$ such that $XAY = B$. If $i \in \{1, \ldots, \min(m, n)\}$ then $\Lambda^i(X)\Lambda^i(A)\Lambda^i(Y) = \Lambda^i(B)$. Since $\Lambda^i(X) \in GL_{\binom{m}{i}}(R)$ and $\Lambda^i(Y) \in GL_{\binom{n}{i}}(R)$, we can apply Lemma 4.3.1 once again to deduce that $\gcd(\Lambda^i(A)) = \gcd(\Lambda^i(B))$. So, A has the same Smith normal form invariants as B.

Proof of (b): Assume that A and B have the same Smith normal form invariants. Suppose that D is the Smith normal form of A produced from the algorithm resulting in Theorem 4.2.3, with diagonal entries d_i for all $i \in \{1, \ldots, k\}$ where $k = \min(m, n)$, such that $d_1|d_2|\ldots|d_k$. Similarly, suppose that E is the Smith normal form of B produced from the algorithm resulting in Theorem 4.2.3, with diagonal entries e_i for all $i \in \{1, \ldots, k\}$, such that $e_1|e_2|\ldots|e_k$.

To show: (ba) If $i \in \{1, 2, \ldots, k\}$ then $d_i = e_i$.

(ba) We will prove this by induction on i. For the base case, suppose that $i = 1$. Then, $d_1 = \gcd(A)$ and $e_1 = \gcd(B)$ from Theorem 4.3.3. Since $\gcd(A) = \gcd(B)$ by assumption, we deduce that $d_1 = e_1$.

For the inductive hypothesis, suppose that $d_j = e_j$ for some $j \in \{1, \ldots, k\}$. Suppose that $d_l = e_l$ for all $l \leq j$. We must show that $d_{j+1} = e_{j+1}$. Since A and B have the same Smith normal form invariants, $\prod_{p=1}^{j+1} d_p = \prod_{p=1}^{j+1} e_p$. From the inductive hypothesis, $d_l = e_l$ for all $l \leq j$. So, we can simplify this as

$$d_{j+1} \prod_{p=1}^{j} d_p = e_{j+1} \prod_{p=1}^{j} d_p.$$

If $\prod_{p=1}^{j} d_p \neq 0$, then $d_{j+1} = e_{j+1}$ since R is an integral domain. On the other hand, if $\prod_{p=1}^{j} d_p = 0$, then there exists $a \in \{1, \ldots, j\}$ such that $d_a = 0$. Since $d_a | d_{j+1}$, $e_a | e_{j+1}$ and $d_a = e_a$, $d_{j+1} = e_{j+1} = 0$. This completes the induction. Hence, if $i \in \{1, 2, \ldots, k\}$, $d_i = e_i$.

(b) Part (ba) reveals that the matrices A and B must have the same Smith normal form so that $D = E$. From Theorem 4.2.3, there exists $P_1, P_2 \in GL_m(R)$ and $Q_1, Q_2 \in GL_n(R)$ such that $P_1 D Q_1 = A$ and $P_2 D Q_2 = B$. We note that

$$A = P_1 P_2^{-1} (P_2 D Q_2) Q_2^{-1} Q_1 = (P_1 P_2^{-1}) B (Q_2^{-1} Q_1).$$

Since $P_1 P_2^{-1} \in GL_m(R)$ and $Q_2^{-1} Q_1 \in GL_n(R)$, A and B must lie in the same orbit. □

4.4 The structure theorem

A useful application of Smith normal form is the structure theorem for finitely generated R-modules, where R is a PID, which we will prove as a consequence of Smith normal form.

Before we dive into the statement of the structure theorem, we need to show that if R is a PID then every submodule of a free R-module of rank n must be free with rank at most n. We will give a constructive proof of this fact using Theorem 4.2.3.

Lemma 4.4.1. *Let R be a PID, M be a free R-module of rank $n \in \mathbb{Z}_{>0}$ and $N \subseteq M$ be a submodule of M. Then N is a finitely generated R-module with at most n generators.*

Proof. Assume that R is a PID and M is a free R-module of rank $n \in \mathbb{Z}_{>0}$. Assume that N is a submodule of M. Since M is free of rank n, it is isomorphic to R^n. Hence, it suffices to prove the lemma for $M = R^n$, where $n \in \mathbb{Z}_{>0}$.

For the base case, let $n = 1$ and suppose that N is a submodule of $M = R$. Then, N is an ideal of R and since R is a PID, there exists $r_N \in R$ such that $N = r_N R$. So, N is generated by 1 element, which proves the base case.

For the inductive hypothesis, assume that the statement of the lemma holds for $n = k \in \mathbb{Z}_{>0}$ and let N be a submodule of $M = R^{k+1}$. Let $\pi|_N : N \to R^k$ denote the following composite:

$$N \hookrightarrow M = R^{k+1} \xrightarrow{\pi} R^k$$

where $\pi : R^{k+1} \to R^k$ is the surjective R-module homomorphism

$$\begin{array}{ccccc} \pi : & R^{k+1} & \to & R^k \\ & (r_1, r_2, \ldots, r_{k+1}) & \mapsto & (r_2, \ldots, r_{k+1}). \end{array}$$

The kernel of $\pi|_N$ is

$$\ker \pi|_N = N \cap \{(r, 0, \ldots, 0) \in R^{k+1} \mid r \in R\}.$$

Since $\{(r, 0, \ldots, 0) \in R^{k+1} \mid r \in R\} \cong R$, then $\ker \pi|_N$ is isomorphic to a submodule of R. From the base case, there exists $x_0 \in N$ such that $\ker \pi|_N = Rx_0$. The image $\pi|_N(N) = \pi(N)$ is a submodule of R^k. By the inductive hypothesis, $\pi(N)$ is finitely generated with at most k generators. Let $\{y_1, \ldots, y_\ell\} \subseteq R^k$ be a generating set for $\pi(N)$, where $\ell \leq k$.

For $j \in \{1, \ldots, \ell\}$, we can write $\pi(x_j) = y_j$, where $x_j \in N$. We claim that $\{x_0, x_1, \ldots, x_\ell\}$ is a generating set for N. Assume that $n \in N$. Then, $\pi(n) \in \pi(N)$ and

$$\pi(n) = \sum_{i=1}^{\ell} n_i y_i = \sum_{i=1}^{\ell} n_i \pi(x_i) = \pi(\sum_{i=1}^{\ell} n_i x_i)$$

where $n_i \in R$. So, $\pi(n - \sum_{i=1}^{\ell} n_i x_i) \in \ker \pi|_N$ and subsequently, $n - \sum_{i=1}^{\ell} n_i x_i = n_0 x_0$ for some $n_0 \in R$. Thus,

$$n = \sum_{i=0}^{\ell} n_i x_i$$

and N must be finitely generated with $\ell + 1 \leq k + 1$ generators. This completes the induction. □

Theorem 4.4.2. *Let R be a PID and M be a free R-module of rank n. Let $N \subseteq M$ be a submodule of M. Then N itself is free R-module, with rank $\leq n$.*

Proof. Assume that R is a PID and M is a free R-module of rank n. Then, M has a basis $B = \{m_1, \ldots, m_n\}$. Assume that $N \subseteq M$ is a submodule of M.

To show: (a) N is a free R-module.

(a) Since M is free, we have an isomorphism $\varphi : M \to R^n$ defined by

$$\varphi(r_1 m_1 + \cdots + r_n m_n) = (r_1, r_2, \ldots, r_n).$$

Since N is a submodule of M, we can apply Lemma 4.4.1 so that $N = span\{n_1, \ldots, n_s\}$, where $s \leq n$. Then, we define the matrix $A \in M_{n \times s}(R)$ as

$$A = (\varphi(n_1), \ldots, \varphi(n_s)) = \begin{pmatrix} n_{11} & n_{12} & \ldots & n_{1s} \\ n_{21} & n_{22} & \ldots & n_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ n_{k1} & n_{k2} & \ldots & n_{ks} \end{pmatrix}.$$

Here, the i^{th} column of A is $\varphi(n_i)$. By Smith normal form (Theorem 4.2.3), there exists $P \in GL_n(R)$ and $Q \in GL_s(R)$ such that

$$PAQ = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_s \\ 0 & \ldots & 0 \\ \vdots & \vdots & \vdots \\ 0 & \ldots & 0 \end{pmatrix}$$

where $d_1|d_2|\ldots|d_s$. Since $Q \in GL_s(R)$, $\{Qm_1, \ldots, Qm_n\}$ is another basis for M. Furthermore, the Smith normal form decomposition above tells us that if $i \in \{1, \ldots, s\}$, then $Pn_i = d_i Qm_i$, where Pn_i is a linear combination of the elements in the set $\{n_1, \ldots, n_s\}$.

We finally claim that the set $\{Pn_1, \ldots, Pn_s\}$ forms a basis for N. Firstly, since each Pn_i is a linear combination of elements in the set $\{n_1, \ldots, n_2\}$ then the set $\{Pn_1, \ldots, Pn_s\}$ spans N. Secondly, $\{Pn_1, \ldots, Pn_s\}$ is linearly independent in N because it is linearly independent in M, as $Pn_i = d_i Qm_i$ for $i \in \{1, \ldots, s\}$. Therefore, $\{Pn_1, \ldots, Pn_s\}$ is a basis for N and so, N is a free R-module with rank $s \leq n$. □

Our proof of the structure theorem will closely follow the proof given in the reference [Ghi18, Page 2].

Theorem 4.4.3 (Structure Theorem)**.** *Let R be a PID and M be a finitely generated R-module over a PID. Then, there exists $d_1, \ldots, d_k \in R$ such that $k \in \{1, 2, \ldots, n\}$, $d_1|d_2|\ldots|d_k$ and*

$$M \cong R/d_1R \oplus R/d_2R \oplus \cdots \oplus R/d_kR. \tag{4.4}$$

Proof. Assume that R is a PID and M is a finitely generated R-module, which is generated by k elements. Assume that $i \in \{1, \ldots, k\}$. By applying Theorem 4.4.2 to the surjective homomorphism $\varphi : R^k \to M$, we deduce that $\ker \varphi$ is a submodule of R^k, which is free with rank $s \leq k$.

Choose a basis for $\ker \varphi$ and let $A \in M_{k \times s}(R)$ be the matrix associated to the inclusion map $\iota : \ker \varphi \to R^k$. By Theorem 4.2.3, A has Smith normal form

$$\begin{pmatrix} d_1 & & & \\ & d_2 & & \\ & & \ddots & \\ & & & d_s \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}$$

where $d_1|d_2|\dots|d_s$. So, there exists a basis $\{f_1, f_2, \dots, f_k\}$ of R^k such that

$$\{d_1 f_1, d_2 f_2, \dots, d_k f_k\}$$

is a basis for $\ker\varphi$. Note that $d_j = 0$ for $j > s$. We now define the R-module homomorphism $\psi : R^k \to R/d_1R \oplus \cdots \oplus R/d_kR$ by

$$\psi(\sum_{i=1}^{k} r_i f_i) = (r_1 + d_1R, \dots, r_k + d_kR).$$

Observe that ψ is a surjective R-module homomorphism and $\ker\psi = \ker\varphi$. By the first isomorphism theorem,

$$M \cong R^k/\ker\varphi = R^k/\ker\psi \cong R/d_1R \oplus R/d_2R \oplus \cdots \oplus R/d_kR.$$

□

The factors $d_i \in R$ in equation (4.4) are called the **invariant factors** of M.

Example 4.4.1. This example was taken from [Ghi18, Page 5]. Let

$$M = \mathbb{Z}^2/N \qquad \text{where} \qquad N = span\{(6,4),(4,8),(4,0)\}.$$

Define a surjective map $\varphi : \mathbb{Z}^3 \to \mathbb{Z}^2$ by

$$\varphi(a,b,c) = a(6,4) + b(4,8) + c(4,0).$$

Each basis element of $\mathbb{Z}^3$ gets sent to a generator in N. The matrix of φ with respect to the standard bases of $\mathbb{Z}^3$ and $\mathbb{Z}^2$ is now

$$\begin{pmatrix} 6 & 4 & 4 \\ 4 & 8 & 0 \end{pmatrix}.$$

whose Smith normal form decomposition is

$$\begin{pmatrix} 1 & -1 \\ -2 & 3 \end{pmatrix} \begin{pmatrix} 6 & 4 & 4 \\ 4 & 8 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & -2 \\ 0 & 1 & 1 \\ 0 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 8 & 0 \end{pmatrix}.$$

Theorem 4.4.3 (the structure theorem) then tells us that

$$M = \mathbb{Z}^2/N \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}.$$

Explicitly, consider the bases

$$B = \{(1,0,0),(0,1,1),(-2,1,2)\} \text{ of } \mathbb{Z}^3 \qquad \text{and} \qquad C = \{(3,2),(1,1)\} \text{ of } \mathbb{Z}^2.$$

Then,

$$\varphi((1,0,0)) = 2(3,2), \varphi((0,1,1)) = 8(1,1) \text{ and } \varphi((-2,1,2)) = (0,0)$$

and $N = span\{(6,4),(4,8),(4,0)\} = 2(3,2)\mathbb{Z} \oplus 8(1,1)\mathbb{Z}$.

Chapter 5

Orbits of principal congruence subgroups

5.1 Basic definitions

In this section, we will define the matrix orbit space $\Gamma_\infty(3)\backslash\Gamma(3)$, which appears in [BH86, Page 489] in the context a minimal parabolic Eisenstein series. Let $\omega = e^{2\pi i/3}$ and $\mathbb{Z}[\omega] = \mathfrak{o}$ be the ring of Eisenstein integers. Note that $\mathfrak{o}$ is a Euclidean domain and hence, a PID.

Definition 5.1.1. Define

$$\begin{aligned} \Gamma(3) &= \{A \in SL_3(\mathfrak{o}) \mid A \equiv I_3 \bmod 3\mathfrak{o}\}, \\ \Gamma_\infty(3) &= \Gamma(3) \cap U, \\ \Gamma_\infty(3)\backslash\Gamma(3) &= \{\Gamma_\infty(3) \cdot A \mid A \in \Gamma(3)\}. \end{aligned}$$

where the congruence $A \equiv I_3 \bmod 3\mathfrak{o}$ is computed entry by entry and U denotes the subgroup of upper triangular matrices in $SL_3(\mathfrak{o})$.

Equivalently, $\Gamma_\infty(3)$ is the subgroup of upper triangular unipotent matrices in $\Gamma(3)$. This is because if $A \in \Gamma_\infty(3)$ then its diagonal entries must be congruent to 1 mod $3\mathfrak{o}$. Since 1 is the only element of $\mathfrak{o}^\times = \{\pm 1, \pm\omega, \pm\omega^2\}$ which is congruent to 1 mod $3\mathfrak{o}$, the diagonal entries of A are all 1 and consequently, A is an upper triangular, unipotent matrix in $\Gamma(3)$.

The question we will focus on is: If $A \in \Gamma(3)$, then what is a matrix representative for the orbit $\Gamma_\infty(3) \cdot A$? Analogously to Smith normal form, one of the most useful ways of understanding matrix orbits is to look for **invariants** — elements in $\mathfrak{o}$ which remain the same when A is multiplied on the left by an element of the group $\Gamma_\infty(3)$.

Definition 5.1.2. Let

$$A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \in \Gamma(3).$$

Define

$$Inv(A) = (A_1, B_1, C_1, A_2, B_2, C_2) \in \mathfrak{o}^6$$

where

$$\begin{array}{ccc} A_1 = g, & B_1 = h, & C_1 = i, \\ A_2 = dh - eg, & B_2 = di - fg, & C_2 = ei - fh. \end{array} \tag{5.1}$$

We call A_1, B_1, C_1 the Λ^1 **invariants** of A and A_2, B_2, C_2 the Λ^2 **invariants** of A.

The notations A_1, B_1, C_1, A_2, B_2 and C_2 used for each invariant are adopted from [BH86, Page 485]. The Λ^1 invariants form the bottom row of $A = \Lambda^1(A)$ and the Λ^2 invariants form the bottom row of $\Lambda^2(A)$.

Let $\varphi_1, \varphi_2 : SL_2(\mathfrak{o}) \to SL_3(\mathfrak{o})$ denote the group homomorphisms

$$\varphi_1 \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b & \\ c & d & \\ & & 1 \end{pmatrix} \qquad \text{and} \qquad \varphi_2 \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & & \\ & a & b \\ & c & d \end{pmatrix}.$$

Then with $ijk = 1$,

$$\Lambda^2 \begin{pmatrix} 1 & x & y \\ & 1 & z \\ & & 1 \end{pmatrix} = \begin{pmatrix} 1 & z & xz - y \\ & 1 & x \\ & & 1 \end{pmatrix}, \tag{5.2}$$

$$\Lambda^2(diag[i, j, k]) = diag[ij, ik, jk] = diag[k^{-1}, j^{-1}, i^{-1}], \tag{5.3}$$

$$\begin{aligned} \Lambda^2(\varphi_1(a, b, c, d)) &= \varphi_2(a, b, c, d), \\ \Lambda^2(\varphi_2(a, b, c, d)) &= \varphi_1(a, b, c, d). \end{aligned} \tag{5.4}$$

Equation (5.2) demonstrates that $\Lambda^2(\Gamma_\infty(3)) \subseteq \Gamma_\infty(3)$. Since $\Lambda^2(I_3) = I_3$, where $I_3 \in SL_3(\mathfrak{o})$ is the identity matrix, $\Lambda^2(\Gamma(3)) \subseteq \Gamma(3)$.

5.2 Properties of Λ^1 and Λ^2 invariants

The main point of this section is that the invariants as defined in Definition 5.1.2 satisfy very similar properties to the Smith normal form invariants investigated in section 4.3. The main properties we want $(A_1, B_1, C_1, A_2, B_2, C_2) \in \mathfrak{o}^6$ in Definition 5.1.2 to satisfy are

$$A_1 \equiv A_2 \equiv B_1 \equiv B_2 \equiv 0 \bmod 3\mathfrak{o}, \tag{I1}$$

$$C_1 \equiv C_2 \equiv 1 \bmod 3\mathfrak{o}, \tag{I2}$$

$$\gcd(A_1, B_1, C_1) = \gcd(A_2, B_2, C_2) = 1, \tag{I3}$$

$$A_1C_2 - B_1B_2 + C_1A_2 = 0. \tag{I4}$$

Equations (I1), (I2), (I3) and (I4) together form the **invariant conditions**.

Proposition 5.2.1. *Let $A \in \Gamma(3)$. Then, $Inv(A) \in \mathfrak{o}^6$ satisfies the invariant conditions* (I1), (I2), (I3) *and* (I4).

Proof. Assume that

$$A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \in \Gamma(3) \qquad \text{and} \qquad Inv(A) = (A_1, B_1, C_1, A_2, B_2, C_2).$$

By using the definition of $\Gamma(3)$ in Definition 5.1.1 and equation (5.1), a direct computation yields the conditions (I1) and (I2).

Since $A \in SL_3(\mathfrak{o})$ then $\det(A) = 1$ and Laplace expansion along the bottom row of A yields

$$1 = g(bf - ec) - h(af - cd) + i(ae - bd) \in g\mathfrak{o} + h\mathfrak{o} + i\mathfrak{o}.$$

Hence, $\gcd(A_1, B_1, C_1) = \gcd(g, h, i) = 1$. Similarly, Laplace expansion along the top row of A yields

$$1 = a(ei - fh) - b(di - fg) + c(dh - eg) \in C_2\mathfrak{o} + B_2\mathfrak{o} + A_2\mathfrak{o}.$$

So, $\gcd(A_2, B_2, C_2) = 1$. Equation (I4) follows from the direct computation

$$A_1C_2 - B_1B_2 + C_1A_2 = g(ei - fh) - h(di - fg) + i(dh - eg) = 0.$$

□

The next theorem establishes a bijection between sets of invariants satisfying the invariant conditions and orbits in $\Gamma_\infty(3)\backslash\Gamma(3)$. Observe the similarity to Theorem 4.3.3 in the previous chapter.

Theorem 5.2.2. *Let $A, B \in \Gamma(3)$. Then, $\Gamma_\infty(3) \cdot A = \Gamma_\infty(3) \cdot B$ if and only if $Inv(A) = Inv(B)$.*

Proof. Assume that $A, B \in \Gamma(3)$.

To show: (a) If $\Gamma_\infty(3) \cdot A = \Gamma_\infty(3) \cdot B$, then $Inv(A) = Inv(B)$.

(b) If A and B have the same set of invariants, then $\Gamma_\infty(3) \cdot A = \Gamma_\infty(3) \cdot B$.

Proof of (a): Suppose that $\Gamma_\infty(3) \cdot A = \Gamma_\infty(3) \cdot B$. Then there exists $C \in \Gamma_\infty(3)$ such that $CA = B$. Since the bottom rows of C and $\Lambda^2(C)$ are both $[0, 0, 1]$, a quick computation of the bottom rows of CA and $\Lambda^2(CA)$ gives $Inv(A) = Inv(CA) = Inv(B)$.

Proof of (b): Now assume that $Inv(A) = Inv(B) = (A_1, B_1, C_1, A_2, B_2, C_2)$.

To show: (ba) There exists a $C \in \Gamma_\infty(3)$ such that $CA = B$.

(ba) Since $A, B \in \Gamma(3)$ are invertible, we define $C = BA^{-1}$.

To show: (baa) $BA^{-1} \in \Gamma_\infty(3)$.

(baa) We first write A and B as

$$A = \begin{pmatrix} a_1 & b_1 & c_1 \\ d_1 & e_1 & f_1 \\ A_1 & B_1 & C_1 \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} a_2 & b_2 & c_2 \\ d_2 & e_2 & f_2 \\ A_1 & B_1 & C_1 \end{pmatrix}.$$

Since $\det(A) = 1$, we can apply Proposition 3.2.2 to find that $A^{-1} = \Upsilon^2(A)$. Consequently,

$$BA^{-1} = B\Upsilon^2(A) = \begin{pmatrix} a_2 & b_2 & c_2 \\ d_2 & e_2 & f_2 \\ A_1 & B_1 & C_1 \end{pmatrix} \begin{pmatrix} C_2 & c_1B_1 - b_1C_1 & b_1f_1 - e_1c_1 \\ -B_2 & a_1C_1 - c_1A_1 & c_1d_1 - a_1f_1 \\ A_2 & b_1A_1 - a_1B_1 & a_1e_1 - b_1d_1 \end{pmatrix}. \quad (5.5)$$

It remains to show that BA^{-1} is upper triangular and unipotent. Let d_{ij} denote the i, j element of BA^{-1}. By equation (5.5) and the invariant condition in equation (I4), $d_{31} = A_1C_2 - B_1B_2 + A_2C_1 = 0$.

The entry $d_{32} = A_1(c_1B_1 - b_1C_1) + B_1(a_1C_1 - c_1A_1) + C_1(b_1A_1 - a_1B_1) = 0$.

The entry

$$d_{33} = \begin{vmatrix} a_1 & b_1 & c_1 \\ d_1 & e_1 & f_1 \\ A_1 & B_1 & C_1 \end{vmatrix} = \det(A) = 1.$$

The entry

$$d_{21} = \begin{vmatrix} d_2 & e_2 & f_2 \\ d_2 & e_2 & f_2 \\ A_1 & B_1 & C_1 \end{vmatrix} = 0.$$

Since $Inv(A) = Inv(B)$,

$$d_{22} = \begin{vmatrix} a_1 & b_1 & c_1 \\ d_2 & e_2 & f_2 \\ A_1 & B_1 & C_1 \end{vmatrix} = \begin{vmatrix} a_1 & b_1 & c_1 \\ d_1 & e_1 & f_1 \\ A_1 & B_1 & C_1 \end{vmatrix} = 1.$$

Finally, since $\det(BA^{-1}) = 1$ and $d_{22} = d_{33} = 1$ then $d_{11} = 1$.

So BA^{-1} is an upper triangular unipotent matrix in $\Gamma(3)$. Hence, $BA^{-1} \in \Gamma_\infty(3)$. □

In [BH86, Page 484], Bump and Hoffstein define the involution $\iota : GL_3(\mathbb{C}) \to GL_3(\mathbb{C})$ by

$$ {}^{\iota}A = \begin{pmatrix} & & 1 \\ & 1 & \\ 1 & & \end{pmatrix} (A^{-1})^T \begin{pmatrix} & & 1 \\ & 1 & \\ 1 & & \end{pmatrix}. $$

The invariants of $A \in \Gamma(3)$ in [BH86] are defined as the elements of $\mathfrak{o}$ which comprise the bottom rows of A and ${}^{\iota}A$, denoted by $[A_1, B_1, C_1]$ and $[A_2, B_2, C_2]$ respectively. To see how this is related to Definition 5.1.2, we compute directly that

$$ \Lambda^2(A) = \begin{pmatrix} 1 & & \\ & -1 & \\ & & 1 \end{pmatrix} \begin{pmatrix} & & 1 \\ & 1 & \\ 1 & & \end{pmatrix} (\Upsilon^2(A))^T \begin{pmatrix} & & 1 \\ & 1 & \\ 1 & & \end{pmatrix} \begin{pmatrix} 1 & & \\ & -1 & \\ & & 1 \end{pmatrix}. $$

Since $\det(A) = 1$, then by Proposition 3.2.2, $\Upsilon^2(A) = A^{-1}$. So,

$$ \Lambda^2(A) = \begin{pmatrix} 1 & & \\ & -1 & \\ & & 1 \end{pmatrix} ({}^{\iota}A) \begin{pmatrix} 1 & & \\ & -1 & \\ & & 1 \end{pmatrix}. \tag{5.6} $$

Equation (5.6) provides the crucial link between the bottom row $[A_2, B_2, C_2]$ of ${}^{\iota}A$ in [BH86, p. 486] and $Inv(A)$. In particular, the only difference between A_2, B_2, C_2 as in [BH86, p. 486] and the Λ^2 invariants in Definition 5.1.2 is the sign of B_2. Thus, we have connected our approach to the invariants of $\Gamma_\infty(3)\backslash\Gamma(3)$ with that of Bump and Hoffstein.

5.3 The form of a representative of $\Gamma_\infty(3)\backslash\Gamma(3)$

Suppose that we are given $(A_1, B_1, C_1, A_2, B_2, C_2) \in \mathfrak{o}^6$ which satisfy the invariant conditions. We would like to construct a matrix $A \in \Gamma(3)$ such that $Inv(A) = (A_1, B_1, C_1, A_2, B_2, C_2)$. Similarly to Smith normal form, Steinberg reduction in subsection 4.1.2 will be the main tool for achieving this construction. Define

$$ D(3) = \Big\{ \begin{pmatrix} i & & \\ & j & \\ & & k \end{pmatrix} \in SL_3(\mathfrak{o}) \mid i, j, k \in \mathfrak{o}^\times \text{ and } ijk = 1 \Big\}. \tag{5.7} $$

$$ U(3) = \Big\{ \begin{pmatrix} 1 & \alpha & \beta \\ & 1 & \gamma \\ & & 1 \end{pmatrix} \in SL_3(\mathfrak{o}) \mid \alpha, \beta, \gamma \in \mathfrak{o}/3\mathfrak{o} \Big\}. \tag{5.8} $$

Theorem 5.3.1. *We have the following equality:*

$$ SL_3(\mathfrak{o}) = \bigcup_{y_1, y_2, y_3 \in Y(\mathfrak{o})} \bigcup_{d \in D(3)} \bigcup_{u \in U(3)} \varphi_2(y_1^{-1})\varphi_1(y_2^{-1})\varphi_2(y_3^{-1}) du \Gamma_\infty(3). \tag{5.9} $$

Proof. To show: (a) RHS of equation (5.9) $\subseteq$ LHS of equation (5.9).

Proof of (a): Suppose that $B = \varphi_2(y_1^{-1})\varphi_1(y_2^{-1})\varphi_2(y_3^{-1})duC$ where $y_1, y_2, y_3 \in Y(\mathfrak{o})$, $d \in D(3)$, $u \in U(3)$ and $C \in \Gamma_\infty(3)$. Since B is a product of matrices whose determinants are all 1, $\det(B) = 1$. So, $B \in SL_3(\mathfrak{o})$. This proves equation (5.9).

To show: (b) LHS of equation (5.9) $\subseteq$ RHS of equation (5.9).

Proof of (b): Assume that

$$A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \in SL_3(\mathfrak{o}).$$

Step 1: (First column of A) Use Steinberg reduction (see subsection 4.1.2) on the first column to construct matrices $y_1, y_2 \in Y(\mathfrak{o})$, with $Y(\mathfrak{o})$ being the set in equation (4.1), which satisfy

$$y_1 \begin{pmatrix} d \\ g \end{pmatrix} = \begin{pmatrix} \gcd(d,g) \\ 0 \end{pmatrix} \qquad \text{and} \qquad y_2 \begin{pmatrix} a \\ \gcd(d,g) \end{pmatrix} = \begin{pmatrix} p \\ 0 \end{pmatrix}.$$

Here, $p = \gcd(a,d,g) \in \mathfrak{o}^\times$. Consequently,

$$\varphi_1(y_2)\varphi_2(y_1)A = \begin{pmatrix} p & b' & c' \\ 0 & e' & f' \\ 0 & h' & i' \end{pmatrix}.$$

Step 2: (Second column of A) Using Steinberg reduction on the second column of $\varphi_1(y_2)\varphi_2(y_1)A$, we construct another matrix $y_3 \in Y(\mathfrak{o})$ satisfying

$$y_3 \begin{pmatrix} e' \\ h' \end{pmatrix} = \begin{pmatrix} q \\ 0 \end{pmatrix} \qquad \text{where} \qquad q = \gcd(e', h') \in \mathfrak{o}^\times.$$

Thus,

$$\varphi_2(y_3)\varphi_1(y_2)\varphi_2(y_1)A = \begin{pmatrix} p & x & y \\ 0 & q & z \\ 0 & 0 & r \end{pmatrix}.$$

Step 3: (Decomposing the upper triangular matrix) On the RHS, we have

$$\begin{pmatrix} p & x & y \\ 0 & q & z \\ 0 & 0 & r \end{pmatrix} = \begin{pmatrix} p & & \\ & q & \\ & & r \end{pmatrix} \begin{pmatrix} 1 & qrx & qry \\ & 1 & prz \\ & & 1 \end{pmatrix}.$$

because $pqr = 1$. Furthermore,

$$\begin{pmatrix} 1 & qrx & qry \\ & 1 & prz \\ & & 1 \end{pmatrix} = \begin{pmatrix} 1 & \alpha & \beta \\ & 1 & \gamma \\ & & 1 \end{pmatrix} \begin{pmatrix} 1 & qrx - \alpha & qry - \alpha(prz - \gamma) - \beta \\ & 1 & prz - \gamma \\ & & 1 \end{pmatrix}$$

where $\alpha, \beta, \gamma \in \mathfrak{o}/3\mathfrak{o}$ are chosen so that the elements

$$qrx - \alpha,\ prz - \gamma,\ qry - \alpha(prz - \gamma) - \beta \in 3\mathfrak{o}. \tag{5.10}$$

Equation (5.10) ensures that the matrix

$$U = \begin{pmatrix} 1 & qrx - \alpha & qry - \alpha(prz - \gamma) - \beta \\ & 1 & prz - \gamma \\ & & 1 \end{pmatrix} \in \Gamma_\infty(3).$$

Putting all of the computations together, we obtain the decomposition

$$A = \varphi_2(y_1^{-1})\varphi_1(y_2^{-1})\varphi_2(y_3^{-1}) \begin{pmatrix} p & & \\ & q & \\ & & r \end{pmatrix} \begin{pmatrix} 1 & \alpha & \beta \\ & 1 & \gamma \\ & & 1 \end{pmatrix} U$$

so that

$$SL_3(\mathfrak{o}) \subseteq \bigcup_{y_1,y_2,y_3 \in Y(\mathfrak{o})} \bigcup_{d \in D(3)} \bigcup_{u \in U(3)} \varphi_2(y_1^{-1})\varphi_1(y_2^{-1})\varphi_2(y_3^{-1}) du \Gamma_\infty(3).$$

□

Example 5.3.1. Let

$$A = \begin{pmatrix} 4 & -3 & -12 \\ -3 & 4 & 15 \\ -6 & 3 & 13 \end{pmatrix} \in \Gamma(3).$$

Following the steps in Theorem 5.3.1, $A = \varphi_2(y_1^{-1})\varphi_1(y_2^{-1})\varphi_2(y_3^{-1}) du C$, where

$$y_1 = \begin{pmatrix} 1 & -1 \\ 2 & -1 \end{pmatrix}, \qquad y_2 = \begin{pmatrix} 2 & -3 \\ 3 & -4 \end{pmatrix}, \qquad y_3 = \begin{pmatrix} 2 & 5 \\ 5 & 13 \end{pmatrix} \in Y(\mathfrak{o}),$$

$$d = \begin{pmatrix} -1 & & \\ & -1 & \\ & & 1 \end{pmatrix} \in D(3), \qquad u = \begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix} \in U(3)$$

$$\text{and} \qquad C = \begin{pmatrix} 1 & 9 & 30 \\ & 1 & 3 \\ & & 1 \end{pmatrix} \in \Gamma_\infty(3).$$

Consequently, $\varphi_2(y_1^{-1})\varphi_1(y_2^{-1})\varphi_2(y_3^{-1}) du$ is a representative of the orbit $A \cdot \Gamma_\infty(3)$.

For $A \in \Gamma(3)$, Theorem 5.3.1 gives a representative of the right orbit $A \cdot \Gamma_\infty(3) \in \Gamma(3)/\Gamma_\infty(3)$. The main motivation behind Theorem 5.3.2 is that we can obtain a representative of the left orbit $\Gamma_\infty(3) \cdot A$ by using Υ^1 from Definition 3.1.1.

Theorem 5.3.2. *We have the following equality:*

$$SL_3(\mathfrak{o}) = \bigcup_{y_1,y_2,y_3 \in Y(\mathfrak{o})} \bigcup_{d \in D(3)} \bigcup_{u \in U(3)} \Gamma_\infty(3) u d \varphi_1(y_3)\varphi_2(y_2)\varphi_1(y_1). \tag{5.11}$$

Proof. Assume that

$$A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \in \Gamma(3)$$

so that

$$\Lambda^2(A) = \begin{pmatrix} ae - bd & af - cd & bf - ec \\ ah - bg & ai - cg & bi - ch \\ dh - eg & di - fg & ei - fh \end{pmatrix} \in \Gamma(3).$$

Since $\det(\Lambda^2(A)) = 1$, equation (3.2) gives

$$\Upsilon^1(A) = (\Lambda^2(A))^{-1} = \begin{pmatrix} i & -f & c \\ -h & e & -b \\ g & -d & a \end{pmatrix} \in \Gamma(3) \tag{5.12}$$

and subsequently, $A = \Upsilon^1(\Upsilon^1(A))$. By Theorem 5.3.1,

$$\Upsilon^1(A) = \varphi_2(y_1^{-1})\varphi_1(y_2^{-1})\varphi_2(y_3^{-1})duC$$

where $y_1, y_2, y_3 \in Y(\mathfrak{o})$, $d \in D(3)$, $u \in U(3)$ and $C \in \Gamma_\infty(3)$. Applying Υ^1 to both sides and using equation (5.4) yields

$$A = \Upsilon^1(\Upsilon^1(A)) = \Upsilon^1(C)\Upsilon^1(u)\Upsilon^1(d)\varphi_1(y_3)\varphi_2(y_2)\varphi_1(y_1)$$

with $\Upsilon^1(C) \in \Gamma_\infty(3)$ and $\Upsilon^1(d) \in D(3)$. Assume that

$$u = \begin{pmatrix} 1 & x & y \\ & 1 & z \\ & & 1 \end{pmatrix} \in U(3) \qquad \text{so that} \qquad \Upsilon^1(u) = \begin{pmatrix} 1 & -z & y \\ & 1 & -x \\ & & 1 \end{pmatrix}.$$

Then, $\Upsilon^1(u) = KL$, where

$$K = \begin{pmatrix} 1 & 3m & 3mx + 9mp + 3n \\ & 1 & 3p \\ & & 1 \end{pmatrix} \qquad \text{and} \qquad L = \begin{pmatrix} 1 & -z - 3m & y - 3n \\ & 1 & -x - 3p \\ & & 1 \end{pmatrix}.$$

The elements $m, n, p \in \mathfrak{o}$ are chosen such that $-z - 3m, y - 3n, -x - 3p \in \mathfrak{o}/3\mathfrak{o}$. This ensures that $K \in \Gamma_\infty(3)$ and $L \in U(3)$. Hence,

$$A = \Upsilon^1(\Upsilon^1(A)) = (\Upsilon^1(C)K)L\Upsilon^1(d)\varphi_1(y_3)\varphi_2(y_2)\varphi_1(y_1).$$

which gives equation (5.11). □

We remark that we can use the inverse A^{-1} in place of $\Upsilon^1(A)$ to prove an analogous result to Theorem 5.3.2. We used $\Upsilon^1(A)$ in the above proof because by equation (5.12), $\Upsilon^1(A)$ is easier to compute than A^{-1}.

Example 5.3.2. Let

$$A = \begin{pmatrix} 4 & -3 & -12 \\ -3 & 4 & 15 \\ -6 & 3 & 13 \end{pmatrix} \in \Gamma(3).$$

By following the steps outlined in the proof of Theorem 5.3.2, $A = Cud\varphi_1(y_3)\varphi_2(y_2)\varphi_1(y_1)$, where

$$y_1 = \begin{pmatrix} 1 & -1 \\ 2 & -1 \end{pmatrix}, \qquad y_2 = \begin{pmatrix} 2 & -9 \\ 3 & -13 \end{pmatrix}, \qquad y_3 = \begin{pmatrix} 2 & 23 \\ 5 & 58 \end{pmatrix} \in Y(\mathfrak{o}),$$

$$d = \begin{pmatrix} 1 & & \\ & -1 & \\ & & -1 \end{pmatrix} \in D(3), \qquad u = \begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix} \in U(3)$$

$$\text{and} \qquad C = \begin{pmatrix} 1 & 0 & 15 \\ & 1 & -39 \\ & & 1 \end{pmatrix} \in \Gamma_\infty(3).$$

Consequently, $ud\varphi_1(y_3)\varphi_2(y_2)\varphi_1(y_1)$ is a representative of the left orbit $\Gamma_\infty(3) \cdot A$.

5.4 Constructing a representative from a set of invariants

Theorem 5.4.1 forms the crucial link between Theorem 5.3.2 and the Λ^1 and Λ^2 invariants, as defined in Definition 5.1.2. Before we proceed, we recall the invariant conditions (I1), (I2), (I3) and (I4).

Theorem 5.4.1. *Let $(A_1, B_1, C_1, A_2, B_2, C_2) \in \mathfrak{o}^6$ be a sequence satisfying the invariant conditions* (I1), (I2), (I3) *and* (I4) *with at least one of $A_1, B_1 \neq 0$. Let $r_1, r_2, r_3 \in \mathfrak{o} - \{0\}/\mathfrak{o}^\times$ and $\alpha, \beta \in \mathfrak{o}^\times$ be such that*

$$\begin{array}{rcl} \gcd(A_1, B_1) & = & \alpha r_2, \\ A_1 & = & \gcd(A_1, B_1) r_1, \\ A_2 & = & \gcd(A_1, B_1)\beta r_3. \end{array} \tag{5.13}$$

Define $p_1, q_1, s_1 \in \mathfrak{o}$ such that

$$p_1 \in \mathfrak{o}/r_1\mathfrak{o}, \qquad \gcd(A_1, B_1)s_1 = B_1 \qquad \textit{and} \qquad p_1 s_1 - q_1 r_1 = 1.$$

Define $p_2, q_2, s_2 \in \mathfrak{o}$ such that

$$p_2 \in \mathfrak{o}/r_2\mathfrak{o}, \qquad s_2 = \alpha^{-1} C_1 \qquad \textit{and} \qquad p_2 s_2 - q_2 r_2 = 1.$$

Define $p_3, q_3, s_3 \in \mathfrak{o}$ such that

$$p_3 \in \mathfrak{o}/r_3\mathfrak{o}, \qquad s_3 = \alpha^{-1}\beta^{-1}(p_1 C_2 - q_1 B_2) \qquad \textit{and} \qquad p_3 s_3 - q_3 r_3 = 1.$$

For $i \in \{1, 2, 3\}$, let

$$d = \begin{pmatrix} \alpha^{-1}\beta^{-1} & & \\ & \beta & \\ & & \alpha \end{pmatrix} \qquad \textit{and} \qquad y_i = \begin{pmatrix} p_i & q_i \\ r_i & s_i \end{pmatrix}$$

Then, define the matrix

$$X = VW \in M_{3\times 3}(\mathfrak{o})$$

where

$$W = d\varphi_1(y_1)\varphi_2(y_2)\varphi_1(y_3) \qquad \textit{and} \qquad V = W^{-1} \mod 3\mathfrak{o}.$$

Then,

$$X \in \Gamma(3) \qquad \textit{and} \qquad Inv(X) = (A_1, B_1, C_1, A_2, B_2, C_2).$$

Moreover, the decomposition $X = I_3 V d\varphi_1(y_1)\varphi_2(y_2)\varphi_1(y_3)$ with the identity matrix $I_3 \in \Gamma_\infty(3)$ is the decomposition from equation (5.11)*.*

Proof. Assume that $(A_1, B_1, C_1, A_2, B_2, C_2) \in \mathfrak{o}^6$ satisfies the invariant conditions (I1), (I2), (I3) and (I4). Assume that we have $r_1, r_2, r_3 \in \mathfrak{o} - \{0\}/\mathfrak{o}^\times$ and $\alpha, \beta \in \mathfrak{o}^\times$ satisfying equation (5.13). We will show that the matrix X is an element of $\Gamma(3)$ with $Inv(X) = (A_1, B_1, C_1, A_2, B_2, C_2)$ and that the decomposition $X = I_3 V d\varphi_1(y_1)\varphi_2(y_2)\varphi_1(y_3)$ is the one in Theorem 5.3.2.

To show: (a) The matrices $y_1, y_2, y_3 \in Y(\mathfrak{o})$.

(b) The matrices $d \in D(3)$ and $V \in U(3)$.

(c) The matrix $X \in \Gamma(3)$ and $Inv(X) = (A_1, B_1, C_1, A_2, B_2, C_2)$.

(a) From equation (4.1), the assertion is equivalent to showing that if $i \in \{1, 2, 3\}$ then $r_i \in \mathfrak{o} - \{0\}/\mathfrak{o}^\times$ and $p_i \in \mathfrak{o}/r_i\mathfrak{o}$. We already have by assumption $r_1, r_2, r_3 \in \mathfrak{o} - \{0\}/\mathfrak{o}^\times$.

To show: (aa) If $i \in \{1, 2, 3\}$ then $\gcd(r_i, s_i) = 1$.

(aa) To see that $\gcd(r_1, s_1) = 1$, note that

$$\gcd(\gcd(A_1, B_1)r_1, \gcd(A_1, B_1)s_1) = \gcd(A_1, B_1)\gcd(r_1, s_1) = \gcd(A_1, B_1).$$

Since $\gcd(A_1, B_1) \neq 0$, then $\gcd(r_1, s_1) = 1$. Next, to see that $\gcd(r_2, s_2) = 1$, the invariant condition equation (I3) gives $\gcd(A_1, B_1, C_1) = 1$ and subsequently,

$$\gcd(r_2, s_2) = \gcd(\gcd(A_1, B_1), C_1) = \gcd(A_1, B_1, C_1) = 1.$$

Finally, to see that $\gcd(r_3, s_3) = 1$, we first observe that since $\gcd(r_1, s_1) = 1$, then there exists $p_{1,0}, q_{1,0} \in \mathfrak{o}$ such that $p_{1,0}s_1 - q_{1,0}r_1 = 1$. If $n \in \mathfrak{o}$ then define

$$p_{1,n} = p_{1,0} - nr_1 \qquad \text{and} \qquad q_{1,n} = q_{1,0} - ns_1.$$

A quick computation reveals that if $n \in \mathfrak{o}$ then $p_{1,n}s_1 - q_{1,n}r_1 = 1$. Thus, there exists $\ell \in \mathfrak{o}$ such that $p_{1,\ell} \in \mathfrak{o}/r_1\mathfrak{o}$. Let $p_1 = p_{1,\ell}$ and $q_1 = q_{1,\ell}$ so that $s_3 = \alpha^{-1}\beta^{-1}(p_1C_2 - q_1B_2)$.

To see that $\gcd(r_3, s_3) = 1$, we will find constants $u, v \in \mathfrak{o}$ such that $ur_3 + vs_3 = 1$. Since $\gcd(A_2, B_2, C_2) = 1$ by invariant condition (I3), there exists $\gamma_1, \gamma_2, \gamma_3 \in \mathfrak{o}$ such that $\gamma_1A_2 + \gamma_2B_2 + \gamma_3C_2 = 1$.

We will now derive expressions for B_2 and C_2. Since $p_1s_1 - q_1r_1 = 1$, then

$$p_1B_1 - q_1A_1 = \gcd(A_1, B_1) = \alpha r_2. \tag{5.14}$$

Since $s_3 = \alpha^{-1}\beta^{-1}(p_1C_2 - q_1B_2)$, then

$$p_1C_2 - q_1B_2 = \alpha\beta s_3. \tag{5.15}$$

If we multiply equation (5.14) by C_2 and then subtract equation (5.15) multiplied by B_1 from it, we find that since $A_1C_2 - B_1B_2 + A_2C_1 = 0$,

$$q_1A_2C_1 = q_1(B_1B_2 - A_1C_2) = \alpha r_2(C_2 - \alpha\beta s_1 s_3).$$

Substituting the expressions $A_2 = \alpha\beta r_2 r_3$ and $C_1 = \alpha s_2$ into the LHS and then solving for C_2, we arrive at

$$C_2 = \alpha\beta(q_1r_3s_2 + s_1s_3). \tag{5.16}$$

Similarly, if we multiply equation (5.14) by B_2 and then subtract equation (5.15) multiplied by A_1 from it, we obtain the equation

$$p_1A_2C_1 = p_1(B_1B_2 - A_1C_2) = \alpha r_2B_2 - \alpha\beta s_3A_1.$$

Using the fact that $A_2 = \alpha\beta r_2 r_3$ and $C_1 = \alpha s_2$, we solve for B_2 to obtain

$$B_2 = \alpha\beta(p_1r_3s_2 + r_1s_3). \tag{5.17}$$

Therefore, if we substitute equations (5.17), (5.16) and $A_2 = \alpha\beta r_2 r_3$ into the equation $\gamma_1A_2 + \gamma_2B_2 + \gamma_3C_2 = 1$, we deduce that

$$1 = r_3(\gamma_1\alpha\beta r_2 + \alpha\beta\gamma_2 p_1 s_2 + \gamma_3\alpha\beta q_1 s_2) + s_3(\alpha\beta\gamma_2 r_1 + \alpha\beta\gamma_3 s_1).$$

Hence, $r_3\mathfrak{o} + s_3\mathfrak{o} = \mathfrak{o}$ and so, $\gcd(r_3, s_3) = 1$, thereby showing that if $i \in \{1, 2, 3\}$ then $\gcd(r_i, s_i) = 1$.

(a) Since $\gcd(r_2, s_2) = \gcd(r_3, s_3) = 1$, we can construct p_2, q_2, p_3, q_3 in a similar manner to $p_1 = p_{1,\ell}$ and $q_1 = q_{1,\ell}$ previously. This gives $p_2 \in \mathfrak{o}/r_2\mathfrak{o}$, $p_3 \in \mathfrak{o}/r_3\mathfrak{o}$ and $q_2, q_3 \in \mathfrak{o}$ which satisfy $p_2s_2 - q_2r_2 = 1$ and $p_3s_3 - q_3r_3 = 1$. So, $y_1, y_2, y_3 \in Y(\mathfrak{o})$.

(b) The matrix $d \in D(3)$ because $(\alpha^{-1}\beta^{-1})\beta\alpha = 1$. To see that the matrix $V \in U(3)$, we will first show that

$$W = \begin{pmatrix} \alpha^{-1}\beta^{-1}(p_1p_3 + p_2q_3r_1) & \alpha^{-1}\beta^{-1}(p_2q_3s_1 + p_3q_1) & \alpha^{-1}\beta^{-1}q_2q_3 \\ \beta(p_1r_3 + p_2r_1s_3) & \beta(p_2s_1s_3 + q_1r_3) & \beta q_2s_3 \\ \alpha r_1r_2 & \alpha r_2s_1 & \alpha s_2 \end{pmatrix} \tag{5.18}$$

is congruent to an upper triangular, unipotent matrix mod $3\mathfrak{o}$. Let w_{ij} denote the i, j entry of W. For the bottom row of W, we note that $w_{31} = \alpha r_1 r_2 = A_1 \equiv 0 \bmod 3\mathfrak{o}$, $w_{32} = \alpha r_2 s_1 = B_1 \equiv 0 \bmod 3\mathfrak{o}$ and $w_{33} = \alpha s_2 \equiv C_1 \equiv 1 \bmod 3\mathfrak{o}$ by invariant condition (I2).

Before we compute w_{11}, w_{21} and w_{22} modulo $3\mathfrak{o}$, we must establish several other relations first. We begin with the fact that $A_1 \equiv B_1 \equiv 0 \bmod 3\mathfrak{o}$ from invariant condition (I1). This reveals that $\gcd(A_1, B_1) \equiv 0 \bmod 3\mathfrak{o}$ and thus,

$$r_2 = \alpha^{-1}\gcd(A_1, B_1) \equiv 0 \bmod 3\mathfrak{o}. \tag{5.19}$$

Since $C_1 \equiv 1 \bmod 3\mathfrak{o}$, $s_2 \equiv ij \bmod 3\mathfrak{o}$ and

$$s_2 = \alpha^{-1}C_1 \equiv \alpha^{-1} \bmod 3\mathfrak{o}. \tag{5.20}$$

Next, we reduce the equation $s_3 = \alpha^{-1}\beta^{-1}(p_1C_2 - q_1B_2)$ modulo $3\mathfrak{o}$ to obtain

$$s_3 \equiv \alpha^{-1}\beta^{-1}(p_1(1) - q_1(0)) \equiv \alpha^{-1}\beta^{-1}p_1 \bmod 3\mathfrak{o} \tag{5.21}$$

where we used the congruence $C_2 \equiv 1 \bmod 3\mathfrak{o}$ from invariant condition (I2). Since $p_2s_2 - q_2r_2 = 1$ by construction then

$$p_2s_2 \equiv 1 + q_2r_2 \bmod 3 \equiv 1 \bmod 3\mathfrak{o},$$

due to equation (5.19). By using equation (5.20), we find that $p_2s_2 \equiv p_2\alpha^{-1} \bmod 3\mathfrak{o}$ and

$$p_2 \equiv \alpha \bmod 3\mathfrak{o}. \tag{5.22}$$

Since $A_1C_2 - B_1B_2 + A_2C_1 = 0$ from invariant condition (I4), then equation (5.13) yields $r_1C_2 - s_1B_2 + \beta r_3C_1 = 0$. Reducing modulo $3\mathfrak{o}$, we find that

$$0 = r_1C_2 - s_1B_2 + \beta r_3C_1 \equiv r_1(1) - s_1(0) + \beta r_3(1) \equiv r_1 + \beta r_3 \bmod 3\mathfrak{o},$$

where $B_2 \equiv 0 \bmod 3\mathfrak{o}$ by invariant condition (I1). So,

$$r_1 \equiv -\beta r_3 \bmod 3\mathfrak{o}. \tag{5.23}$$

Reducing the matrix elements w_{11}, w_{21} and w_{22} modulo $3\mathfrak{o}$, we obtain

$$\begin{aligned} w_{21} &= \beta(r_3p_1 + p_2r_1s_3) \\ &= \beta r_3p_1 + \beta p_2r_1s_3 \\ &\equiv (-r_1)p_1 + \beta p_2r_1s_3 \bmod 3\mathfrak{o} \quad (5.23) \\ &\equiv -p_1r_1 + \beta\alpha r_1s_3 \bmod 3\mathfrak{o} \quad (5.22) \\ &\equiv -p_1r_1 + \beta\alpha r_1(\alpha^{-1}\beta^{-1}p_1) \bmod 3\mathfrak{o} \quad (5.21) \\ &\equiv 0 \bmod 3\mathfrak{o}. \end{aligned}$$

$$\begin{aligned} w_{22} &= \beta(p_2s_1s_3 + q_1r_3) \\ &= \beta p_2s_1s_3 + \beta q_1r_3 \\ &\equiv \beta p_2s_1s_3 + q_1(-r_1) \bmod 3\mathfrak{o} \quad (5.23) \\ &\equiv \beta\alpha s_1s_3 - q_1r_1 \bmod 3\mathfrak{o} \quad (5.22) \\ &\equiv \beta\alpha s_1(\alpha^{-1}\beta^{-1}p_1) - q_1r_1 \bmod 3\mathfrak{o} \quad (5.21) \\ &\equiv p_1s_1 - q_1r_1 \equiv 1 \bmod 3\mathfrak{o}. \end{aligned}$$

$$\begin{aligned} w_{11} &= \alpha^{-1}\beta^{-1}(p_1p_3 + p_2q_3r_1) \\ &= \alpha^{-1}\beta^{-1}p_1p_3 + \alpha^{-1}\beta^{-1}p_2q_3r_1 \\ &\equiv s_3p_3 + \alpha^{-1}\beta^{-1}p_2q_3r_1 \bmod 3\mathfrak{o} \quad (5.21) \\ &\equiv s_3p_3 + \alpha^{-1}\beta^{-1}p_2q_3(-\beta r_3) \bmod 3\mathfrak{o} \quad (5.23) \\ &\equiv p_3s_3 - q_3r_3 \bmod 3\mathfrak{o} \quad (5.22) \\ &\equiv 1 \bmod 3\mathfrak{o}. \end{aligned}$$

Hence,

$$W \equiv \begin{pmatrix} 1 & \alpha^{-1}\beta^{-1}(p_2q_3s_1 + p_3q_1) & \alpha^{-1}\beta^{-1}q_2q_3 \\ & 1 & \beta q_2s_3 \\ & & 1 \end{pmatrix} \mod 3\mathfrak{o}.$$

and so the matrix $V = W^{-1} \mod 3\mathfrak{o}$ must also be upper triangular and unipotent. Since $V \in M_{3\times3}(\mathfrak{o}/3\mathfrak{o})$ by construction, we conclude that $V \in U(3)$.

(c) From parts (a) and (b), we find that the decomposition $X = I_3Vd\varphi_1(y_1)\varphi_2(y_2)\varphi_1(y_3)$ is the same one in Theorem 5.3.2. The matrix $X \in \Gamma(3)$ because $X = VW \equiv W^{-1}W \equiv I_3 \bmod 3$ and $\det(X) = 1$ by Theorem 5.3.2.

To check that $Inv(X) = (A_1, B_1, C_1, A_2, B_2, C_2)$, it suffices to compute $Inv(W)$ because since $V \in U(3)$, $Inv(W) = Inv(VW) = Inv(X)$. Recalling the definition of W from equation (5.18), the Λ^1 invariants of this matrix are $\alpha r_1r_2 = A_1$, $\alpha r_2s_1 = B_1$ and $\alpha s_2 = C_1$. In order to compute the bottom row of $\Lambda^2(W)$, which is comprised of the Λ^2 invariants of W, we calculate that

$$\begin{aligned} \alpha\beta r_2s_1(p_1r_3 + p_2r_1s_3) - \alpha\beta r_1r_2(p_2s_1s_3 + q_1r_3) &= \alpha\beta p_1r_2r_3s_1 - \alpha\beta r_1r_2r_3q_1 \\ &= \alpha\beta r_2r_3(p_1s_1 - q_1r_1) \\ &= \alpha\beta r_2r_3 = A_2, \end{aligned}$$

$$\begin{aligned}\gcd(A_1,B_1)(\alpha\beta s_2(p_1r_3+p_2r_1s_3)-\alpha\beta q_2s_3r_1r_2) &= \gcd(A_1,B_1)(\alpha\beta p_1r_3s_2+\alpha\beta r_1s_3)\\ &= p_1A_2C_1+p_1A_1C_2-q_1A_1B_2\\ &= p_1B_1B_2-q_1A_1B_2 \quad \text{(by invariant condition (I4))}\\ &= \gcd(A_1,B_1)(p_1s_1B_2-q_1r_1B_2) = \gcd(A_1,B_1)B_2,\end{aligned}$$

and

$$\begin{aligned}\gcd(A_1,B_1)(\alpha\beta s_2(p_2s_1s_3+q_1r_3)-\alpha\beta q_2r_2s_1s_3) &= \gcd(A_1,B_1)(\alpha\beta s_1s_3+\alpha\beta q_1r_3s_2)\\ &= p_1B_1C_2-q_1B_1B_2+q_1A_2C_1\\ &= p_1B_1C_2-q_1A_1C_2 \quad \text{(by invariant condition (I4))}\\ &= \gcd(A_1,B_1)(p_1s_1C_2-q_1r_1C_2) = \gcd(A_1,B_1)C_2.\end{aligned}$$

Since $\gcd(A_1,B_1)\neq 0$, the Λ^2 invariants of W are A_2, B_2 and C_2. Hence,

$$(A_1,B_1,C_1,A_2,B_2,C_2) = Inv(W) = Inv(X).$$

□

Example 5.4.1. Suppose that we have the following elements of $\mathfrak{o}$ which satisfy the invariant conditions:

$$\begin{array}{lll} A_1=-3+6\omega, & B_1=-3, & C_1=-2-3\omega,\\ A_2=-6+3\omega, & B_2=3-6\omega, & C_2=4+3\omega.\end{array}$$

We want to construct a matrix $A\in\Gamma(3)$ such that $Inv(A)=(A_1,B_1,C_1,A_2,B_2,C_2)$ using Theorem 5.4.1. First, we select $r_1,r_2,r_3\in\mathfrak{o}-\{0\}/\mathfrak{o}^\times$ and $\alpha,\beta\in\mathfrak{o}^\times$ such that equations in (5.13) are satisfied. Recalling the definition of $\mathfrak{o}-\{0\}/\mathfrak{o}^\times$ from example 4.1.1, we find that the correct choices are

$$r_1=2+3\omega, \qquad r_2=3, \qquad r_3=3+2\omega \qquad \text{and} \qquad \alpha=\beta=1+\omega.$$

Additionally, from Theorem 5.4.1,

$$\alpha^{-1}\beta^{-1}=-1-\omega, \qquad s_1=\omega, \qquad \text{and} \qquad s_2=\alpha^{-1}C_1=-\omega(-2-3\omega)=-3-\omega.$$

Before we compute s_3, we must find $p_1,q_1\in\mathfrak{o}$ such that $p_1s_1-q_1r_1=1$ and $p_1\in\mathfrak{o}/r_1\mathfrak{o}$. This is accomplished by setting $p_1=1+2\omega$ and $q_1=\omega$. Now, we are able to compute s_3 as

$$s_3=\alpha^{-1}\beta^{-1}(p_1C_2-q_1B_2)=4+8\omega.$$

By using the Euclidean algorithm in $\mathfrak{o}$, we also find that $p_2=1+\omega, q_2=-1-\omega, p_3=2+2\omega$ and $q_3=1+6\omega$. It remains to find the matrix $V\in U(3)$ from Theorem 5.4.1. Since the product

$$\begin{pmatrix}-1-\omega & & \\ & 1+\omega & \\ & & 1+\omega\end{pmatrix}\varphi_1\begin{pmatrix}2+2\omega & 1+6\omega\\ 3+2\omega & 4+8\omega\end{pmatrix}\varphi_2\begin{pmatrix}1+\omega & -1-\omega\\ 3 & -3-\omega\end{pmatrix}\varphi_1\begin{pmatrix}1+2\omega & \omega\\ 2+3\omega & \omega\end{pmatrix}$$

$$\equiv \begin{pmatrix} 1 & 0 & \omega \\ & 1 & 2+\omega \\ & & 1 \end{pmatrix} \mod 3\mathfrak{o},$$

$$V = \begin{pmatrix} 1 & 0 & \omega \\ & 1 & 2+\omega \\ & & 1 \end{pmatrix}^{-1} \mod 3\mathfrak{o} = \begin{pmatrix} 1 & 0 & 2\omega \\ & 1 & 1+2\omega \\ & & 1 \end{pmatrix} \in U(3).$$

Consequently, our final representative of the orbit in $\Gamma_\infty(3)\backslash\Gamma(3)$ with the original invariants is given by the matrix X in Theorem 5.4.1, where

$$X = \begin{pmatrix} -11-3\omega & -3-3\omega & -3\omega \\ -24-33\omega & -2-12\omega & 12+3\omega \\ -3+6\omega & -3 & -2-3\omega \end{pmatrix} \in \Gamma(3).$$

One can check that $Inv(X) = (A_1, B_1, C_1, A_2, B_2, C_2)$. Thus, the matrix X is a representative of the matrix orbit $\Gamma_\infty(3) \cdot A$, where $A \in \Gamma(3)$ and $Inv(A) = (A_1, B_1, C_1, A_2, B_2, C_2)$.

In Theorem 5.4.1, we excluded the case where $A_1 = B_1 = 0$. In this case, a direct computation reveals the following corollary.

Corollary 5.4.2. *Let* $(0, 0, C_1, A_2, B_2, C_2) \in \mathfrak{o}^6$ *satisfying the invariant conditions* (I1), (I2), (I3) *and* (I4). *Then, the matrix*

$$X = \varphi_1 \begin{pmatrix} a - bB_2 + B_2 & b - bC_2 + C_2 \\ B_2 & C_2 \end{pmatrix} \qquad \textit{with} \qquad aC_2 - bB_2 = 1 \tag{5.24}$$

is an element of $\Gamma(3)$ *which satisfies* $Inv(X) = (0, 0, C_1, A_2, B_2, C_2)$.

Proof. Assume that $(0, 0, C_1, A_2, B_2, C_2) \in \mathfrak{o}^6$ is a sequence which satisfies Proposition 5.2.1. By equation (5.1), $A_2 = 0$ because $A_1 = B_1 = 0$. Also, $\gcd(0, 0, C_1) = 1$ and $\gcd(0, B_2, C_2) = \gcd(B_2, C_2) = 1$ from invariant condition (I3). Since $C_1 \equiv 1 \mod 3\mathfrak{o}$ from invariant condition (I2) and 1 is the only element of $\mathfrak{o}^\times$ which satisfies the congruence 1 mod $3\mathfrak{o}$, $C_1 = 1$ and there exists $a, b \in \mathfrak{o}$ such that $aC_2 - bB_2 = 1$.

For all $m \in \mathfrak{o}$, define $a_m = a - mB_2$ and $b_m = b - mC_2$. Then, $a_mC_2 - b_mB_2 = 1$. By setting $m = b - 1$, we obtain

$$a_{b-1} = a - bB_2 + B_2 \qquad \text{and} \qquad b_{b-1} = b - bC_2 + C_2.$$

Since $B_2 \equiv 0 \mod 3\mathfrak{o}$ and $C_2 \equiv 1 \mod 3\mathfrak{o}$ from invariant conditions (I1) and (I2), $b_{b-1} \equiv 0 \mod 3\mathfrak{o}$. Since $a_{b-1}C_2 - b_{b-1}B_2 = 1$, reducing both sides of the equation modulo $3\mathfrak{o}$ gives $a_{b-1}C_2 \equiv 1 \mod 3\mathfrak{o}$ and $a_{b-1} \equiv 1 \mod 3\mathfrak{o}$ as a result.

By defining the matrix X as in equation (5.24), we find that $X \in \Gamma(3)$ and by direct computation, $Inv(X) = (0, 0, C_1, A_2, B_2, C_2)$ as required. □

Suppose that $X \in \Gamma(3)$. Theorem 5.4.1 tells us how to construct a representative of the orbit $\Gamma_\infty(3) \cdot X$. One computes $Inv(X)$ and then constructs a representative according to Theorem 5.4.1. The main point we emphasise here is that the representative in $\Gamma(3)$ decomposes according to equation (5.11). By constructing a representative for all the orbits in orbit space $\Gamma_\infty(3)\backslash\Gamma(3)$, and then decomposing them according to Theorem 5.4.1, we obtain the following Bruhat decomposition of $\Gamma(3)$:

Corollary 5.4.3. *Define the map*

$$\begin{array}{rccc} \rho: & SL_3(\mathfrak{o}) & \to & SL_3(\mathfrak{o}/3\mathfrak{o}) \\ & A & \mapsto & A^{-1} \ mod\ 3\mathfrak{o}. \end{array}$$

where A^{-1} mod $3\mathfrak{o}$ is computed entrywise. Then, we have the following equality:

$$\Gamma(3) = \bigsqcup_{y_1,y_2,y_3 \in Y(\mathfrak{o})} \bigsqcup_{d \in D(3)} \Gamma_\infty(3)\ \rho(d\varphi_1(y_3)\varphi_2(y_2)\varphi_1(y_1))\ d\varphi_1(y_3)\varphi_2(y_2)\varphi_1(y_1). \quad (5.25)$$

Proof. Assume that $\rho : SL_3(\mathfrak{o}) \to SL_3(\mathfrak{o}/3\mathfrak{o})$ is the map defined in the statement of the corollary.

To show: (a) LHS of equation (5.25) $\subseteq$ RHS of equation (5.25).

(a) Assume that $X \in \Gamma(3)$. By Proposition 5.2.1, $Inv(X)$ satisfies the invariant conditions. Applying Theorem 5.4.1, we construct the matrix

$$A = \rho(d\varphi_1(y_3)\varphi_2(y_2)\varphi_1(y_1))d\varphi_1(y_3)\varphi_2(y_2)\varphi_1(y_1)$$

where $y_1, y_2, y_3 \in Y(\mathfrak{o})$ and $d \in D(3)$. Moreover, $A \in \Gamma(3)$ with $Inv(A) = Inv(X)$. By Theorem 5.2.2, $\Gamma_\infty(3) \cdot A = \Gamma_\infty(3) \cdot X$. So, there exists $C \in \Gamma_\infty(3)$ such that

$$X = C\rho(d\varphi_1(y_3)\varphi_2(y_2)\varphi_1(y_1))d\varphi_1(y_3)\varphi_2(y_2)\varphi_1(y_1).$$

So, X is an element of the RHS of equation (5.25) and subsequently,

$$\Gamma(3) \subseteq \bigsqcup_{y_1,y_2,y_3 \in Y(\mathfrak{o})} \bigsqcup_{d \in D(3)} \Gamma_\infty(3)\ \rho(d\varphi_1(y_3)\varphi_2(y_2)\varphi_1(y_1))\ d\varphi_1(y_3)\varphi_2(y_2)\varphi_1(y_1).$$

To show: (b) RHS of equation (5.25) $\subseteq$ LHS of equation (5.25)

(b) Assume that

$$P = K\ \rho(e\varphi_1(x_3)\varphi_2(x_2)\varphi_1(x_1))\ e\varphi_1(x_3)\varphi_2(x_2)\varphi_1(x_1)$$

where $x_1, x_2, x_3 \in Y(\mathfrak{o})$, $e \in D(3)$ and $K \in \Gamma_\infty(3)$. Define $W = e\varphi_1(x_3)\varphi_2(x_2)\varphi_1(x_1)$. Since $W \in SL_3(\mathfrak{o})$, the matrix $\rho(W^{-1}) = W \bmod 3\mathfrak{o}$ is well-defined with inverse $\rho(W)$. So, $\det(\rho(W^{-1})) \equiv \det(W) \equiv 1 \bmod 3\mathfrak{o}$. Since $\det(\rho(W^{-1})) \in \mathfrak{o}^\times$ and $\det(\rho(W^{-1})) \equiv 1 \bmod 3\mathfrak{o}$, $\det(\rho(W)) = \det(\rho(W^{-1})) = 1$.

Now, the matrix $\rho(W)W$ is a product of matrices with determinant 1. So, $\rho(W)W \in SL_3(\mathfrak{o})$. Moreover, $\rho(W)W \equiv (W^{-1})W \equiv I_3 \bmod 3\mathfrak{o}$. So, $\rho(W)W \in \Gamma(3)$. Since $K \in \Gamma_\infty(3) \subseteq \Gamma(3)$, then $P = K\rho(W)W \in \Gamma(3)$, which yields equation (5.25). $\square$

Bibliography

[Art91] M. Artin, *Algebra*, Prentice Hall Inc, 1991. ISBN: 0-13-004763-5. MR1129886

[BH86] D. Bump, J. Hoffstein, *Cubic metaplectic forms on GL(3)*, Inv. Math. **84** (1986) 481-505, MR0837524

[Con] K. Conrad, *Exterior Powers*, Available at: https://kconrad.math.uconn.edu/blurbs/linmultialg/univid.pdf.

[DF04] D. Dummit, R. Foote. *Abstract Algebra*, John Wiley and Sons Inc, 3rd Edition, 2004. ISBN 0-471-43334-9. MR2286236

[DPTZ20] P. Denton, S. Parke, T. Tao, and X. Zhang. *Eigenvectors from Eigenvalues*, 2020, https://arxiv.org/pdf/1908.03795.pdf.

[FG02] K. Fritzsche, H. Grauert, *From Holomorphic Functions to Complex Manifolds*, Springer-Verlag, 2002. ISBN: 0-387-95395-7. MR1893803

[Ghi18] A. Ghitza. *Lecture 16 of MAST30005*, 11/04/2018.

[GR91] I. Gel'fand, V. Retakh, *Determinants of matrices over noncommutative rings*, Functional Analysis and Its Applications, **25** (1991) 91-102, MR1142205

[Mol07] A. Molev, *Yangians and Classical Lie Algebras*, American Mathematical Society, Volume 143, 2007. ISBN: 978-0-8218-4374-1. MR2355506

[Mul98] J. Muldowney. *Compound Matrices and Applications*, Universidad de los Andes, 1998, https://sites.ualberta.ca/∼mathirl/IUSEP/IUSEP_2019/lecture_notes/compound_ula.pdf.

[Rot03] J. J Rotman, *Advanced Modern Algebra*, Pearson Prentice Hall, 2nd edition, 2003. ISBN: 0130878685. MR2043445

[Ste67] R. Steinberg, *Lectures on Chevalley groups*, Notes prepared by John Faulkner and Robert Wilson. Revised and corrected edition of the 1968 original, University Lecture Series **66** American Mathematical Society, Providence, RI, 2016. ISBN: 978-1-4704-3105-1. MR0466335