UNIVERZA NA PRIMORSKEM
FAKULTETA ZA MATEMATIKO, NARAVOSLOVJE IN
INFORMACIJSKE TEHNOLOGIJE

Zaključna naloga
(Final project paper)

# Wittov izrek

(Witt's theorem)

Ime in priimek: Narmina Baghirova
Študijski program: Matematika
Mentor: izr. prof. dr. Marko Orel

**Koper, avgust 2018**

# Ključna dokumentacijska informacija

Ime in PRIIMEK: Narmina BAGHIROVA

Naslov zaključne naloge: Wittov izrek

Kraj: Koper

Leto: 2018

Število listov: 54 Število referenc: 9

Mentor: izr. prof. dr. Marko Orel

Ključne besede: Wittov izrek, linearna algebra, bilinearne forme

Math. Subj. Class. (2010):15A63

**Izvleček:**
Cilj naloge je preučiti in predstaviti vsebino petega poglavja knjige [3], ki vsebuje teorijo o bilinearnih formah, vključno z Wittovim izrekom. Ker je knjiga precej stara, je en izmed ciljev naloge napisati vsebino na bolj moderen in bralcu dostopen način. Vsebina zaključne naloge je razdeljena na 9 poglavij. Uvodu v prvem poglavju sledita poglavji 2 in 3, ki vsebujeta osnovne lastnosti bilinearnih form. Poglavje 4 opiše lastnosti skalarnih produktov. Slednji predstavljajo posebno vrsto bilinearnih form. Pomemebne vrste skalarnih produktov predstavljajo hermitiski, simetrični in alternirajoči skalarni produkti, ki so natančneje preučevani v poglavjih 5-7. Osmo poglavje vsebuje Wittov izrek in njegove posledice. V zadnjem poglavju je razloženo, zakaj Wittov izrek v splošnem ne velja, če je karakteristika obsega enaka dva.

# Key words documentation

Name and SURNAME: Narmina BAGHIROVA

Title of final project paper: Witt's theorem

Place: Koper

Year: 2018

Number of pages: 54 Number of references: 9

Mentor: Assoc. Prof. Marko Orel, PhD

Keywords: Witt's theorem, linear algebra, bilinear forms

Math. Subj. Class. (2010):15A63

**Abstract:** The aim of the final project paper is to learn, understand, and present the content of Chapter 5 in the book [3], which contains a theory about bilinear forms, including the Witt's Theorem. Since the book is quite old, some parts of it are not written in modern mathematical style and hence one of the goals of the thesis is to rewrite the content of this chapter in a more accessible and modern way. The content of the final project paper is divided into 9 chapters. The introduction in Chapter 1 is followed by Chapters 2 and 3, which contain the basic properties of bilinear forms. Chapter 4 introduces scalar products, which are special kind of bilinear forms. Particular types of scalar products, namely hermitian, symmetric and alternate scalar products are studied in Chapters 5-7. Chapter 8 contains the Witt's theorem and its corollaries. In Chapter 9 it is explained why the Witt's theorem is not necessarily true in characteristic two.

# Acknowledgement

I would like to express my gratitude to my mentor, dr. Marko Orel, for his guidance, help, explanations and advices for my final project paper.
I would also like to thank Faculty of Mathematics, Natural Sciences and Information Technologies for their support through scholarship.
Finally, I wish to thank my mother for support and encouragement throughout my study.

# Contents

# List of Abbreviations

| | |
|---|---|
| *i.e.* | that is |
| *e.g.* | for example |
| *w.l.o.g.* | without loss of generality |

# 1 Introduction

The final project paper is mostly based on Chapter 5 in the Jacobson's book [3]. The aim of the final project paper is to understand the preliminary theory for Witt's theorem and ultimately understand the theorem and the proof. This theorem is of particular interested, since it can be applied to prove certain 'symmetric' properties of various graphs that are constructed from certain vector spaces [4–6]. Strangely, the Witt's theorem is excluded from several textbooks about linear algebra. We were also unable to find this theorem in the handbook [2]. On the other hand, some old masterpieces [1,3] contain this result as one of the essential ingredients. Witt's theorem is named after Ernst Witt. There are several different versions of the Witt's theorem. If $\mathbb{F}$ is a field of odd characteristic and $\mathbb{F}^n$ is a vector space that is formed by all $n$-dimensional column vectors over $\mathbb{F}$, then one version of Witt's theorem says the following.

*Let $V \subseteq \mathbb{F}^n$ be a vector subspace and let $u : V \to \mathbb{F}^n$ be an injective linear map. If $A$ is an $n \times n$ symmetric invertible matrix and*

$$u(x)^T A u(y) = x^T A y \tag{1.1}$$

*holds for all $x, y \in V$, then $u$ can be extended on whole $\mathbb{F}^n$ in such way that* (1.1) *holds for all $x, y \in \mathbb{F}^n$.*

A similar kind of version of Witt's theorem was applied in the results [4–6] mentioned above. Moreover, the version of the Witt's theorem in this thesis, together with its corollary, i.e. Theorem 8.4, can be applied to deduce similar versions of the Witt's theorem for hermitian matrices, alternate matrices, etc.

In the final project paper we study maps that are called bilinear forms, and our particular interest is in non-degenerate bilinear forms. We study the notion of symmetric, hermitian, alternate scalar products. Moreover we will have a look on canonical matrices for such forms that are of interest in various context of geometry. We prove the Witt's theorem for hermitian forms in Chapter 8. Ernst Witt proved Witt's theorem for symmetric scalar products over a field of characteristic $\neq 2$ [9]. Later the theorem was generalized by Pall [7] to obtain a result for hermitian scalar products over a division ring of characteristic $\neq 2$. In the last chapter of the thesis, it will be explained why Witt's theorem does not necessarily hold for symmetric scalar products over a field of characteristic 2.

# 2 Bilinear forms

First we will define what is left abstract vector space and right abstract vector space for a given division ring $\mathbb{D}$.

**Definition 2.1.** A left vector space $\Re$ over a division ring $\mathbb{D}$ is a set $\Re$ equipped with two operations. The addition

$$\Re \times \Re \mapsto \Re,$$

$$(x, y) \mapsto x + y$$

satisfies

$$(x + y) + z = x + (y + z)$$

and

$$x + y = y + x$$

for all $x, y, z \in \Re$. There exist an element $0 \in \Re$ such that

$$x + 0 = 0$$

for all $x \in \Re$.
For each $x \in \Re$ there exist an element $-x \in \Re$ such that

$$x + (-x) = 0.$$

The multiplication by scalars

$$\mathbb{D} \times \Re \to \Re,$$

$$(\alpha, x) \mapsto \alpha x$$

satisfies

$$\alpha(x + y) = \alpha x + \alpha y,$$

$$(\alpha + \beta)x = \alpha x + \beta x,$$

$$(\alpha\beta)x = \alpha(\beta x)$$

for all $\alpha, \beta \in \mathbb{D}$ and for all $x, y \in \Re$. There exist an element $1 \in \mathbb{D}$ such that

$$1x = x$$

for all $x \in \Re$.

If in addition there exist finite number of vectors $e_1, \dots, e_n \in \Re$ such that every vector can be written in a unique way in the form $\phi_1 e_1 + \cdots + \phi_n e_n$, where $\phi_1, \dots, \phi_n \in \mathbb{D}$ then we say that $\Re$ is finite dimensional and $n$ is the dimension, dim$\Re$, of $\Re$.
Right abstract vector space is defined in a similar way, however while for defining left vector space we were using the multiplication from the left hand-side, for defining right vector space we will use multiplication from right hand-side.

**Definition 2.2.** A right vector space $\Re'$ over a division ring $\mathbb{D}$ is a set $\Re'$ equipped with two operations. The addition

$$\Re' \times \Re' \to \Re',$$
$$(x', y') \mapsto x' + y'$$

satisfies

$$(x' + y') + z' = x' + (y' + z')$$

and

$$x' + y' = y' + x'$$

for all $x', y', z' \in \Re'$. There exist an element $0 \in \Re$ such that

$$x' + 0 = 0$$

for all $x' \in \Re'$. For all $x' \in \Re$ there exist an element $-x' \in \Re'$ such that

$$x' + (-x') = 0.$$

The multiplication by scalars

$$\Re' \times \mathbb{D} \to \Re',$$
$$(x', \alpha) \mapsto x'\alpha$$

satisfies

$$(x' + y')\alpha = x'\alpha + y'\alpha,$$
$$x'(\alpha + \beta) = x'\alpha + y'\beta,$$
$$x'(\alpha\beta) = (x'\alpha)\beta$$

for all $\alpha, \beta \in \mathbb{D}$ and for all $x', y' \in \Re'$. There exist an element $1 \in \mathbb{D}$ such that

$$x'1 = x'$$

for all $x' \in \Re'$.

**Definition 2.3.** Let $\Re_1$,$\Re_2$ be left vector spaces over a division ring $\mathbb{D}$. A map $A : \Re_1 \to \Re_2$ is *left linear*, or simply *linear* if

$$(x+y)A = xA + yA, \quad (\alpha x)A = \alpha(xA)$$

hold for all $x, y \in \Re_1$ and for all $\alpha \in \mathbb{D}$.

In the case of a left linear map, we often denote the image $A(x)$ by $xA$, if there is no risk of confusion.

**Definition 2.4.** Let $\Re'_1$,$\Re'_2$ be right vector spaces over a division ring $\mathbb{D}$. A map $A : \Re'_1 \to \Re'_2$ is *right linear*, or simply *linear* if

$$A(x' + y') = Ax' + Ay', \quad A(x'\alpha) = Ax'\alpha$$

hold for all $x', y' \in \Re'_1$ and for all $\alpha \in \mathbb{D}$.

**Definition 2.5.** Conjugate space $\Re^*$ of a left vector space $\Re$ is a set of all (left) linear functionals $f : \Re \to \mathbb{D}$ which is equipped with the following two operations.
The addition of the two linear functionals f and g is defined by

$$(f+g)(x) = f(x) + g(x)$$

for all $x \in \Re$. The multiplication of a linear functional f and a scalar $\phi \in \mathbb{D}$ is defined by

$$(f\phi)(x) = f(x)\phi$$

for all $x \in \Re$. With these two operations $\Re^*$ form a right vector space.

**Definition 2.6.** The conjugate space $(\Re')^*$ of a right vector space $\Re'$ is a set of all (right) linear functionals $f : \Re' \to \mathbb{D}$, which is equipped with the following operations.
The addition of the two linear functionals f and g is defined by

$$(f+g)(y') = f(y') + g(y')$$

for all $y' \in \Re'$. The multiplication of a linear functional f and a scalar $\phi \in \mathbb{D}$ is defined by

$$(\phi f)(y') = \phi f(y')$$

for all $y' \in \Re'$. With these two operations $(\Re')^*$ form a left vector space.

## 2.1 Definition of a bilinear form

In this section we study functions, called bilinear that are defined for pairs of vectors $(x, y')$, where $x$ is from a left vector space $\Re$ and $y'$ is from a right vector space $\Re'$. Of a particular interest are non-degenerate bilinear forms, since they determine a linear bijective transformation of $\Re'$ onto $\Re^*$

**Definition 2.7.** Let $\Re'$ be a right vector space over $\mathbb{D}$ and let $\Re$ be a left vector space over $\mathbb{D}$. Then a map: $\Re \times \Re' \to \mathbb{D}$ is a bilinear form if it satisfies the following properties

$$g(x_1 + x_2, y') = g(x_1, y') + g(x_2, y'), \tag{2.1}$$

$$g(\alpha x, y') = \alpha g(x, y'), \tag{2.2}$$

$$g(x, y'_1 + y'_2) = g(x, y'_1) + g(x, y'_2), \tag{2.3}$$

$$g(x, y'\alpha) = g(x, y')\alpha \tag{2.4}$$

for all $x, x_1, x_2 \in \Re$, for all $y', y_1, y_2 \in \Re'$, and for all $\alpha \in \mathbb{D}$.

Let $y : \Re \times \Re' \to \mathbb{D}$ be a bilinear form connecting a left vector space $\Re$ over $\mathbb{D}$ with a right vector space $\Re'$ over $\mathbb{D}$. In the sequel we use $x$ to denote an element from $\Re$ and $y'$ for an element in $\Re'$. In this way $g(x, y') \in \mathbb{D}$.
Given a fixed $y' \in \Re'$, define the function $g_{y'} : \Re \to \mathbb{D}$ by $g_{y'} = g(x, y')$ for all $x \in \Re$. By properties (2.1) and (2.2) of the bilinear form $g$ it follows that $g_{y'} \in \Re^*$. Moreover, the map $R : \Re' \to \Re^*$, defined by

$$R(y') = g_{y'}, \tag{2.5}$$

is (right) linear.
Similarly, given a fixed $x \in \Re$, define the function $g_x : \Re' \to \mathbb{D}$ by $g_x(y') = g(x, y')$ for all $y' \in \Re'$. By properties (2.3) and (2.4) of the bilinear form g it follows that $g_x \in (\Re')^*$. Moreover, the map $L : \Re \to (\Re')^*$, defined by

$$L(x) = g_x, \tag{2.6}$$

is (left) linear.

## 2.2 Matrices of bilinear forms

**Definition 2.8.** The matrix of the bilinear form g relative to a given basis $(e_1, e_2, \dots, e_n)$ of a finite dimensional $\Re$ , and a basis $(f'_1, f'_2, \dots, f'_{n'})$ of a finite dimensional $\Re'$ is

$$G := \begin{bmatrix} g(e_1, f'_1) & g(e_1, f'_2) & \dots & g(e_1, f'_{n'}) \\ g(e_2, f'_1) & g(e_2, f'_2) & \dots & g(e_2, f'_{n'}) \\ \vdots & \vdots & \ddots & \vdots \\ g(e_n, f'_1) & g(e_n, f'_2) & \dots & g(e_n, f'_{n'}) \end{bmatrix}. \tag{2.7}$$

The value $g(x, y')$ can be deduced from the representations of x and y and from the entries of the matrix (2.7). Namely, for arbitrary $x \in \Re$, $y \in \Re'$ we can write

$$x = \sum_{i=1}^{n} \alpha_i e_i, \quad y' = \sum_{j=1}^{n'} f_j \beta_j.$$

Consequently

$$g(x, y') = g\left(\sum_{i=1}^{n} \alpha_i e_i, \sum_{j=1}^{n'} f_j \beta_j\right) = \sum_{i,j} \alpha_i g(e_i, f_j)\beta_j.$$

Moreover, if $G$ is any $n \times n'$ matrix whose entries are from a division ring $\mathbb{D}$, then there exists some bilinear form $h$ which has matrix $G$ as its matrix relative to basis $(e_1, e_2, \dots, e_n)$ of a finite dimensional left vector space $\Re$ , and basis $(f'_1, f'_2, \dots, f'_{n'})$ of a finite dimensional right vector space $\Re'$.

We can also choose other basis vectors instead of $(e_1, e_2, \dots, e_n)$ and $(f'_1, f'_2, \dots, f'_{n'})$ of a vector space$\Re$ and $\Re'$, respectively. We will now consider the effect of changes of bases in the two spaces, on the matrix $G$ of $g(x, y')$.

Let $(u_1, u_2, .., u_n)$ be another basis of $\Re$ and $(v'_1, v'_2, \dots, v'_{n'})$ another basis of $\Re'$. Then $u_i = \sum \mu_{ij} e_j$ and $v'_k = \sum f'_l v_{lk}$ for some scalars $\mu_{ij}, v_{lk} \in \mathbb{D}$. Hence

$$g(u_i, v'_k) = g\left(\sum_j \mu_{ij} e_j, \sum_l f'_l v_{lk}\right) = \sum_{j,l} \mu_{ij} g(e_j, f'_l) v_{lk}.$$

If $M$ is a matrix with entries $\mu_{ij}$ and $V$ is a matrix with entries $v_{lk}$, then $P := MGV$ is the matrix of $g$ relative to basis $(\mu_1, \dots, \mu_n)$ of a left vector space $\Re$ and basis $(v'_1, \dots, v'_{n'})$ of a right vector space $\Re'$. We say that matrices $P$ and $G$ are equivalent.

*Remark* 2.9. In the commutative case, where $\mathbb{D} = \mathbb{F}$ is a field, this relation is often written in a slightly different form. Namely, in the commutative case the vector spaces are usually treated as left vector spaces. Therefore, $v'_k \in \Re'$ is represented as $v'_k = \sum_l v_{kl} f'_l$ and consequently the matrix $P$ of $g$ relative to basis $(\mu_1, \dots, \mu_n)$ and basis $(v'_1, \dots, v'_{n'})$ equals $MGV^T$.

**Definition 2.10.** Define $M_{n\times n'}(\mathbb{D})$ as the set of all $n \times n'$ matrices with coefficients in $\mathbb{D}$. Similarly, define $GL_n(\mathbb{D})$ as the set of all invertible $n \times n'$ matrices with coefficients in $\mathbb{D}$.

Let $\mathbb{D}^n$ denote the n-dimensional left vector space over $\mathbb{D}$,which is spanned by all the vectors $e_1, e_2, \ldots, e_n$, where $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$, where 1 is the $i-th$ entry. Let $(\mathbb{D}^{n'})'$ denote the n'-dimensional right vector space over $\mathbb{D}$, which is spanned by all vectors $f_1', f_2', \ldots, f_n'$, where $f_i' = (0, \ldots, 0, 1, 0, \ldots, 0)^T$, where 1 is $i-th$ entry.
Given a matrix $G \in M_{n\times n'}(\mathbb{D})$ with coefficients $g_{ij}$, let the *row-rank* of $G$ be the dimension of the subspace in $\mathbb{D}^n$, which is spanned by vectors

$$\sum_{j=1}^{n} g_{1j}e_j, \sum_{j=1}^{n} g_{2j}e_j, \ldots, \sum_{j=1}^{n} g_{nj}e_j.$$

Similarly, let the *column-rank* of $G$ be the dimension of the subspace in $(\mathbb{D}^{n'})'$, which is spanned by vectors

$$\sum_{i=1}^{n'} f_i'g_{i1}, \sum_{i=1}^{n'} f_i'g_{i2}, \ldots, \sum_{i=1}^{n'} f_i'g_{in'}.$$

It is well-known that the row-rank of a matrix is the same as its column-rank(cf. [Theorem 9 on page 51 in [3]). We say that the *rank* of $A$ is $r$ and write $rank(A) = r$ if the column-rank/row-rank of A equals $r$.

**Theorem 2.11.** *(cf. Theorem 4 on page 45 in [3])*
*Let $G \in M_{n\times n'}(\mathbb{D})$. Then there exist $M \in GL_n(\mathbb{D})$ and $V \in GL_{n'}(\mathbb{D})$ such that*

$$MGV = \begin{bmatrix} I_r & 0_{r,n'-r} \\ 0_{n-r,r} & 0_{n-r,n'-r} \end{bmatrix} \tag{2.8}$$

*where $r = rank(G)$, $I_r$ is the identity matrix of size $r$, and $0_{r,n'-r}, 0_{n-r,r}, 0_{n-r,n'-r}$ are zero matrices of appropriate forms.*

This yields to the result on bilinear forms.

**Theorem 2.12.** *Let $g(x, y')$ be a bilinear form connecting a left vector space $\Re$ of dimension $n$ and a right vector space $\Re'$ of dimension $n'$. Then there exist bases $(u_1, u_2, .., u_n), (v_1', v_2', .., v_n')$ for these spaces such that*

$$g(u_i, v_j') = \mathbb{D}_{ij} \quad if \quad i, j = 1, 2, \ldots, r,$$

$$g(u_i, v_j') = 0 \quad if \quad i > r \quad or \quad j > r.$$

*Proof.* Let $G$ be the matrix of $g$ with respect to some basis $(e_1, \dots, e_n)$ of $\Re$ and some basis $(f'_1, \dots, f'_n)$ of $\Re'$. By Theorem 2.11 there exist $M = [\mu_{ij}] \in GL_n(\mathbb{D})$ and $V = [v'_{ij}] \in GL_{n'}(\mathbb{D})$ such that

$$MGV = \begin{bmatrix} I_r & 0_{r,n'-r} \\ 0_{n-r,r} & 0_{n-r,n'-r} \end{bmatrix} \tag{2.9}$$

Moreover, matrix $MGV$ is the matrix of $g$, with respect to the basis $(\mu_1, \dots, \mu_n)$ of $\Re$ and the basis $(v'_1, \dots, v'_{n'})$ of $\Re'$, where $\mu_i = \sum_{j=1}^{n} \mu_{ij} e_j$ and $v_i = \sum_{i=1}^{n'} f'_i v'_{ij}$. The result follows. □

## 2.3 Non-degenerate forms

**Definition 2.13.** Let $g : \Re \times \Re' \to \mathbb{D}$ be a bilinear form. Then the subspace

$$J := \{z \in \Re; g(z, y') = 0 \text{ for all } y' \in \Re'\}$$

is the *left radical* of $g$.

**Definition 2.14.** Let $g : \Re \times \Re' \to \mathbb{D}$ be a bilinear form. Then the subspace

$$J' := \{y' \in \Re'; g(z, y') = 0 \text{ for all } z \in \Re\}$$

is the *right radical* of $g$.

The left radical is obviously the null space of the transformation $L$, defined in (2.5). Similarly the right radical is the null space of the linear transformation $R$, defined in (2.6).

**Definition 2.15.** A bilinear form $y : \Re \times \Re' \to \mathbb{D}$ is non-degenerate, if its left and right radicals are trivial, that is $J = \{0\}$ and $J' = \{0\}$.

**Theorem 2.16.** *Let $g : \Re \times \Re' \to \mathbb{D}$ be a bilinear form connecting a finite dimensional left vector space $\Re$ and a finite dimensional right vector space $\Re'$. Then $g$ is non-degenerate if and only if the following two conditions are satisfied.*

*a) Vector spaces $\Re$ and $\Re'$ have the same dimension.*

*b) The matrix of the bilinear form $g$ relative to any pair of bases is invertible.*

*If $g$ is non-degenerate, then the linear maps $L : \Re \to (\Re')^*$ and $R : \Re' \to \Re^*$ are bijective.*

*Proof.* Let $n := dim\Re$ and $n' := dim\Re'$.
Assume that g is non-degenerate. Then by definition its left and right radicals are trivial, that is, the null spaces of the maps $L : \Re \to (\Re')^*$ and $R : \Re' \to \Re^*$ are trivial. Hence, the maps $L$ and $R$ are injective. Since both radicals are trivial, it follows from Theorem 2.12 that $n = r = n'$, where $r$ is the rank of the matrix of $g$ relative to any pair of basis of $\Re$ and $\Re'$. This proves $a$) and $b$). Moreover, since

$$dim\Re = n = n' = dim\Re' = dim(\Re')^*$$

and $L$ is linear and injective, it follows that $L$ is also surjective, hence a bijective map. Since $dim\Re' = n' = n = dim\Re = dim\Re^*$, we similarly deduce that $\Re$ is bijective as well.
Assume now that the conditions $a), b)$ hold. By Theorem 2.12 we know that $n = r = n'$. Let $z \in J$ and let $\mu_1, \dots, \mu_r$ and $v'_1, \dots, v'_r$ be as in Theorem 2.12. Write $z = \sum_{i=1}^{r} \alpha_i \mu_i$ for some $\alpha_i \in \mathbb{D}$. Then

$$0 = g(z, v'_j) = \sum_{i=1}^{r} \alpha_i g(\mu_i, v'_j) = \alpha_j$$

for all $j$. Hence, $z = 0$, that is $J$ is trivial. Similarly we see that the right radical $J'$ is trivial. Hence, g is non-degenerate. □

**Definition 2.17.** Let $\Re$ and $\Re'$ be left and right vector spaces, respectively. If a left vector space $\Re$ and a right vector space $\Re'$ are connected by a non-degenerate bilinear form g, then we say that $\Re$ and $\Re$ are *dual* relative to g.

Let two vector spaces $\Re$ and $\Re'$ be connected by a non-degenerate bilinear form g. In particular, $dim\Re = dim\Re' = n$. We say that bases $(e_1, \dots, e_n)$ and $(e'_1, \dots, e'_n)$ of $\Re$ and $\Re'$, respectively, are *complementary* if

$$g(e_i, e_j) = \delta_{ij}$$

for all $i, j \in \{1, \dots, n\}$. That is, the matrix of g relative to these two bases is the identity matrix $I_n$.

**Proposition 2.18.** *Let two vector spaces $\Re$ and $\Re'$ be connected by a non-degenerate bilinear form g.*

*a) If $(e_1, \dots, e_n)$ is a basis of $\Re$, then there exists a unique basis $(e'_1, \dots, e'_n)$ of $\Re'$ such that these two bases are complementary.*

*b) If $(e'_1, \dots, e'_n)$ is a basis of $\Re'$, then there exists a unique basis $(e_1, \dots, e_n)$ of $\Re$ such that these two bases are complementary.*

*Proof.* First we prove the uniqueness in part $a$). Suppose that $(e_1, \dots, e_n)$, $(e'_1, \dots, e'_n)$ and $(e_1, \dots, e_n)$, $(e''_1, \dots, e''_n)$ are both pairs of complementary bases. For each $j$ write $e''_j = \sum_{i=1}^{n} e'_i v_{ij}$ for suitable $v_{ij} \in \mathbb{D}$. If $G$ is the matrix of $g$ relative to bases $(e_1, \dots, e_n)$ and $(e'_1, \dots, e'_n)$, then $GV$, where $V = (v_{ij})$, is the matrix of $g$ relative to bases $(e_1, \dots, e_n)$ and $(e''_1, \dots, e''_n)$. Since both $G$ and $GV$ are identity matrices, it follows that $V = I_n$ as well. That is $v_{ij} = \delta_{ij}$, hence $e''_j = e'_j$ for all $j$.
Next we prove the existence. Choose an arbitrary basis $(f'_1, \dots, f'_n)$ of $\mathfrak{R}'$. Let $G$ be the matrix of $g$ relative to bases $(e_1, \dots, e_n)$ and $(f'_1, \dots, f'_n)$. Let $v_{ij}$ be the $(i, j)$-th entry of the inverse of $G$, that is, $G^{-1} = (v_{ij})$. If we define the basis $(e'_1, \dots, e'_n)$ of $\mathfrak{R}'$ by $e'_j = \sum_{i=1}^{n} f'_i v_{ij}$ for all $j \in \{1, \dots, n\}$, then the matrix of $g$ relative to bases $(e_1, \dots, e_n)$ and $(e'_1, \dots, e'_n)$ equals $GG^{-1} = I_n$. Hence, they are complementary.
Statement $b$) is proved in a similar way. □

**Definition 2.19.** Let $\mathfrak{R}$ and $\mathfrak{R}'$ be left and right vector spaces respectively. Assume that $\mathfrak{R}$ and $\mathfrak{R}'$ are connected by non-degenerate bilinear form g, that is they are dual relative to $g(x, y')$. Let $\mathfrak{S}$ be a subspace of $\mathfrak{R}$. We define $j(\mathfrak{S}) = \{y' \in \mathfrak{R}' : g(x, y') = 0$ for all $x \in \mathfrak{S}\}$. Then $j(\mathfrak{S})$ is a vector subspace in $\mathfrak{R}'$. We say that it is *incident* to $\mathfrak{S}$.

**Definition 2.20.** Let $\mathfrak{R}$ and $\mathfrak{R}'$ be left and right abstract space respectively. Assume that $\mathfrak{R}$ and $\mathfrak{R}'$ are connected by non-degenerate bilinear form g, that is they are dual relative to $g(x, y')$. Let $\mathfrak{S}'$ be a subspace of $\mathfrak{R}'$. We define $j(\mathfrak{S}') = \{x \in \mathfrak{R} : g(x, y') = 0$ for all $y' \in \mathfrak{S}'\}$. Then $j(\mathfrak{S}')$ is a vector subspace in $\mathfrak{R}$. We say that it is *incident* to $\mathfrak{S}'$.

**Proposition 2.21.** *Let $n$-dimensional vector spaces $\mathfrak{R}$ and $\mathfrak{R}'$ be dual relative to a non-degenerate bilinear form $g : \mathfrak{R} \times \mathfrak{R}' \to \mathbb{D}$. Let $\mathfrak{S}$ and $\mathfrak{S}'$ be two vector subspaces in $\mathfrak{R}$ and $\mathfrak{R}'$, respectively. Then*

$$dim j(\mathfrak{S}) = n - dim \mathfrak{S}$$

*and*

$$dim j(\mathfrak{S}') = n - dim \mathfrak{S}'.$$

*Moreover,*

$$j(j(\mathfrak{S})) = \mathfrak{S} \quad \textit{and} \quad j(j(\mathfrak{S}')) = \mathfrak{S}'.$$

*Proof.* Let $r := dim \mathfrak{S}$.
Choose a basis $(\mu_1, \dots, \mu_r)$ for the subspace $\mathfrak{S}$ and extend it to a basis $(\mu_1, \dots, \mu_n)$ for $\mathfrak{R}$. Let $(\mu'_1, \dots, \mu'_n)$ be the basis of $\mathfrak{R}'$, which is complementary to $(\mu_1, \dots, \mu_n)$.

In order to prove that $j(\mathfrak{S}) = n - dim\mathfrak{S}$ is suffices to show that $j(\mathfrak{S})$ is spanned by vectors $\mu'_{r+1}, \ldots, \mu'_n$.

Let $y' = \sum_{j=r+1}^{n} \mu'_j \beta_j$ for some $\beta_{r+1}, \ldots, \beta_n \in \mathbb{D}$. Then

$$g(\mu_i, y') = \sum_{j=r+1}^{n} g(\mu_i, \mu'_j)\beta_j = \sum_{j=r+1}^{n} \delta_{ij}\beta_j = 0$$

for all $i \in \{1, \ldots, r\}$. Hence $g(x, y') = 0$ for all $x \in \mathfrak{S}$. That is $y' \in j(\mathfrak{S})$. Conversely, let $z' \in j(\mathfrak{S})$. Then

$$g(\mu_i, z') = 0$$

for all $i \in \{1, \ldots, r\}$. Choose $\gamma_1, \ldots, \gamma_n \in \mathbb{D}$ such that $z' = \sum_{j=1}^{n} \mu'_j \gamma_j$. From the equations $g(\mu_i, z') = 0$ for all $i \in \{1, \ldots, r\}$ we deduce that

$$0 = g(\mu_i, z') = \sum_{j=1}^{n} \delta_{ij}\gamma_j = \gamma_i$$

for $i \in \{1, \ldots, r\}$. Hence, $z'$ is in the span of $\mu'_{r+1}, \ldots, \mu'_n$. Therefore, this span equals $j(\mathfrak{S})$. Consequently,

$$dimj(\mathfrak{S}) = n - r = n - dim\mathfrak{S}.$$

Symmetrically we prove that

$$dimj(\mathfrak{S}') = n - dim\mathfrak{S}'.$$

Consequently,

$$dimj(j(\mathfrak{S})) = n - dim(j(\mathfrak{S})) = n - (n - dim\mathfrak{S}) = dim\mathfrak{S}.$$

If $\mu \in \mathfrak{S}$, then $g(\mu, y') = 0$ for all $y' \in j(\mathfrak{S})$. Therefore $\mu \in j(j(\mathfrak{S}))$, that is, $\mathfrak{S} \subseteq j(j(\mathfrak{S}))$. Since $\mathfrak{S}$ and $j(j(\mathfrak{S}))$ are of the same dimension it follows that $\mathfrak{S} = j(j(\mathfrak{S}))$. Similarly we prove that $j(j(\mathfrak{S}')) = \mathfrak{S}'$ □

# 3 Transpose of a linear transformation relative to a pair of bilinear forms

Let $A : \Re_1 \to \Re_2$ be a left linear transformation and assume that $f \in \Re_2^*$. Then we define a map $A^T : \Re_2^* \to \Re_1^*$ by

$$(A^T f)x_1 = f(x_1 A)$$

for all $x_1 \in \Re_1$.

**Proposition 3.1.** *The map $A^T : \Re_2^* \to \Re_1^*$ is right linear.*

*Proof.* Let $f, g \in \Re_2^*$ and $x \in \Re_1$. Then

$$(A^T(f+g))x = (f+g)(xA) = f(xA) + g(xA) = (A^T f)x + (A^T g)x = (A^T f + A^T g)x.$$

Hence,

$$A^T(f+g) = A^T f + A^T g.$$

If $\alpha \in \mathbb{D}$, then

$$(A^T(f\alpha))x = (f\alpha)(xA) = f(xA)\alpha = (A^T f)x\alpha = (A^T f\alpha)x.$$

Hence,

$$A^T(f\alpha) = A^T f\alpha.$$

□

**Definition 3.2.** The linear transformation $A^T : \Re_2^* \to \Re_1^*$ is the *transpose* of $A$.

Let $\Re_1$ be a left vector space and $\Re_1'$ be the dual to $\Re_1$ relative to a non-degenerate bilinear form $g_1(x_1, y_1')$. Let $\Re_2$ be a left vector space as well and let $\Re_2'$ be the dual to $\Re_2$ relative to a non-degenerate bilinear form $g_2(x_2, y_2')$.

We now define the linear map $A' : \Re_2' \to \Re_1'$ as a composition of maps

$$R_2 : \Re_2' \to \Re_2^*,$$
$$A^T : \Re_2^* \to \Re_1^*,$$
$$R_1^{-1} : \Re_1^* \to \Re_1'$$

where $A^T$ is the transpose of $A$ and $R_1, R_2$ are defined analogously as the map $R(y') = g_{y'}$ in (2.5). That is $A' = R_1^{-1}A^T R_2$. The map $A'$ defined above is the *transpose* of $A$ relative to non-degenerate bilinear forms $g_1, g_2$.

Now we will determine the form of a linear map $A'$. Let $y_2' \in \Re_2'$, since $R_2 : \Re_2' \to \Re_2^*$, the image of an element $y_2' \in \Re'$ under the map $R_2$ is the linear function $x \mapsto g_2(x, y_2') \in \Re_2^*$. Now let's see what happens when we apply $A^T R_2$ on an element $y_2' \in \Re_2'$. We already know what is $R_2 y_2'$, now since $A^T : \Re_2^* \to \Re_1^*$, the image of $A^T R_2 y_2'$ is a linear function $f_1 \in \Re_1^*$ such that

$$(A^T R_2 y_2')(x_1) = f_1(x_1) = g_2(x_1 A, y_2').$$

And finally if we apply the linear map $A'$ on an element $y_2' \in \Re_2'$ we will get the vector $y_1' \in \Re_1'$ such that

$$f_1(x_1) = g_2(Ax_1, y_2') = g_1(x_1, y_1')$$

Moreover we see from the equation above that $y_1' = A'y_2'$ is unique vector of $\Re_1$ such that

$$g_1(x_1, A'y_2') = g_2(x_1 A, y_2')$$

for all $x_1 \in \Re_1$. Recall that if a vector space $\Re$ and a vector space $\Re'$ are connected by a non-degenerate bilinear form then we say that they are dual. Duality is a symmetric relation. So if $A'$ is linear transformation from $\Re_2'$ to $\Re_1'$, then what is the transpose? Similarly as before we define a left linear transformation $A''$ as a composition of maps

$$\begin{aligned} L_1 : \Re_1 &\to (\Re_1')^*, \\ A'^T : (\Re_1')^* &\to (\Re_2')^*, \\ L_2^{-1} : (\Re_2')^* &\to \Re_2 \end{aligned}$$

where $A'^T$ is the transpose of $A'$ and $L_1, L_2$ are defined analogously as the map $L(x) = g_x$ in (2.6). That is $A'' = L_1 A'^T L_2^{-1}$.

Let $x_1 \in \Re_1$. If we apply the map $L_1$ to an element $x_1$, then the image is a linear function $y_1' \mapsto g_1(x_1, y_1') \in (\Re_1')^*$. Further if we apply $A'^T$ we get a linear function $f_2 \in (\Re_2')^*$ such that $f_2(y_2') = g_1(x_1, A'y_2')$.

Finally if we apply $L_2^{-1}$, we get some vector $x_2 \in \Re_2$ such that $f_2(y_2') = g_1(x_1, A'y_2') = g_2(x_2, y_2')$. Hence we see that $x_2 = x_1 A''$. By substituting we get

$$g_1(x_1, A'y_2') = g_2(x_1 A'', y_2')$$

for all $y_2' \in \Re_2'$. Hence we can see from the equations

$$g_2(x_1 A, y_2') = g_1(x_1, A'y_2')$$

for all $x_1 \in \Re_1$ and

$$g_1(x_1, A'y_2') = g_2(x_1A'', y_2')$$

for all $y_2' \in \Re_2'$, that if $A'$ is the transpose of $A$ then $A$ is the transpose of $A'$. In other words, $A'' = A$. Moreover, $A \mapsto A'$ is a bijective map from $L(\Re_1, \Re_2)$ to $L(\Re_2', \Re_1')$, where $L(\Re_1, \Re_2)$ is the set of left linear transformations from $\Re_1$ to $\Re_2$ and $L(\Re_2', \Re_1')$ is the set of right linear transformations from $\Re_2'$ into $\Re_1'$.
Now we list the algebraic properties of the map $A \mapsto A'$.

**Proposition 3.3.** *For $i \in \{1, 2, 3\}$ assume that $\Re_i$ and $\Re_i'$ are dual vector spaces relative a non-degenerate form $g_i : \Re_i \times \Re_i' \to \mathbb{D}$.*

*(a) If $A, B : \Re_1 \to \Re_2$ are linear, then*

$$(A + B)' = B' + A',$$

*where $X'$ denotes the transpose of $X$ relative to the pair $g_1, g_2$.*

*(b) If $A : \Re_1 \to \Re_2$ and $B : \Re_2 \to \Re_3$ are linear, then*

$$(B \circ A)' = A' \circ B',$$

*where $X'$ denotes the transpose of $X$ relative to the appropriate pair of bilinear forms.*

*(c) If $\Re_1 = \Re_2$, $\Re_1' = \Re_2'$, $g_1 = g_2$, then the map $A \mapsto A'$ is an anti-isomorphism between rings $L(\Re_1, \Re_1)$ and $L(\Re_1', \Re_1')$.*

*Proof.* (a) Obviously, $(A + B)^T = A^T + B^T$. Therefore

$$(A+B)' = R_1^{-1}(A+B)^T R_2 = R_1^{-1}(A^T+B^T)R_2 = R_1^{-1}A^T R_2+R_1^{-1}B^T R_2 = A'+B'.$$

(b) Since $(B \circ A)^T = A^T \circ B^T$ it follows that

$$(B \circ A)' = R_1^{-1} \circ (B \circ A)^T \circ R_3 = R_1^{-1} \circ A^T \circ B^T R_3 =$$
$$= R_1^{-1} \circ A^T \circ R_2 \circ R_2^{-1} B^T R_3 = A' \circ B'.$$

(c) Follows immediately from $(a), (b)$ and the fact that $A \mapsto A'$ is a bijective map.

□

We will now determine relation between matrix of a linear transformation and a matrix of its transpose.
Let $\Re_1$ and $\Re_1'$ be dual spaces relative to a non-degenerate bilinear form $g_1$. Similarly let

$\Re_2$ and $\Re'_2$ be dual spaces relative to a non-degenerate bilinear form $g_2$. Let $A : \Re_1 \to \Re_2$ be linear map. Let $(e_1, e_2, \dots, e_{n_1})$ be a basis for $\Re_1$ and let $(e'_1, e'_2, \dots, e'_n)$ be the complementary basis in $\Re'_1$. Let $(f_1, f_2, \dots, f_{n_2})$ be a basis for $\Re_2$ and let $(f'_1, f'_2, \dots, f'_{n_2})$ be the complementary basis. Suppose

$$e_iA = \sum_{k=1}^{n_2} \alpha_{ik} f_k, \quad i = 1, 2, \dots, n_1,$$
$$A'f'_l = \sum_{j=1}^{n_1} e'_j \alpha'_{jl}, \quad l = 1, 2, \dots, n_2.$$

Then the condition

$$g_2(e_iA, f'_l) = g_1(e_i, A'f'_l)$$

yields the relations $\alpha_{il} = \alpha'_{il}$ for the matrices. Thus if complementary bases are used in the dual spaces, then the matrices of the transformation and of its transpose are equal. In particular, rank$A'$=rank$A$.

## 3.1 Another relation between bilinear forms and linear transformations

Assume that $\Re_1$ and $\Re'_1$ are dual spaces relative to a non-degenerate bilinear form $g_1$ and $\Re_2$ and $\Re'_2$ are dual spaces relative to a non-degenerate bilinear form $g_2$. Fix a vector $u' \in \Re'_1$ and $v \in \Re_2$.
Define a map $u' \times v : \Re_1 \to \Re_2$ by

$$u' \times v : x \mapsto g_1(x, u')v$$

In more general case, let $u'_1, u'_2, .., u'_m \in \Re'_1$ and $v_1, v_2, .., v_m \in \Re_2$, then we define the mapping

$$u'_1 \times v_1 + u'_2 \times v_2 + \cdots + u'_m \times v_m : x \mapsto g_1(x, u'_1)v_1 + g_1(x, u'_2)v_2 + \cdots + g_1(x, u'_m)v_m$$

**Theorem 3.4.** *Any linear transformation $A \in L(\Re_1, \Re_2)$ is of the form*

$$A = u'_1 \times v_1 + u'_2 \times v_2 + \ldots + u'_r \times v_r$$

*for some $r \leq min\{dim\Re_1,\ dim\Re_2\}$.*

*Remark* 3.5. We will denote the range of linear transformation $A$ by $A\Re_1$.

*Proof.* Let $(v_1, \dots, v_r)$ be a basis for the space $A\Re_1$. Let $x \in \Re_1$. Then $xA = \phi_1 v_1 + \phi_2 v_2 + \cdots + \phi_r v_r$, where $\phi_1, \phi_2, \dots, \phi_r$ are unique coefficients from the division ring $\mathbb{D}$.

Since coefficients are uniquely determined by $x$ we may consider $\phi_i$ as a function of $x$. Hence we rewrite $xA$ in the following way

$$xA = \phi_1(x)v_1 + \phi_2(x)v_2 + \cdots + \phi_r(x)v_r.$$

Let $y \in \Re_1$. Then

$$\sum_{i=1}^{r} \phi_i(x)v_i + \sum_{i=1}^{r} \phi_i(y)v_i = xA + yA = (x+y)A = \sum_{i=1}^{r} \phi_i(x+y)v_i.$$

Also take $\alpha \in \mathbb{D}$, then

$$\phi_1(\alpha x)v_1 + \cdots + \phi_r(\alpha x)v_r = (\alpha x)A = \alpha(xA) = \alpha\phi_1(x)v_1 + \alpha\phi_2(x)v_2 + \cdots + \alpha\phi_r(x)v_r.$$

Thus we have shown that $\phi_i(x+y) = \phi_i(x) + \phi_i(y)$ and that $\phi_i(\alpha x) = \alpha\phi_i(x)$. Hence $\phi_i$ are linear.

Since $g_1(x, y')$ is non-degenerate by the assumption, there exist some $u'_i \in \Re'_1$, such that

$$\phi_i(x) = g_1(x, u'_i)$$

for all $x \in \Re_1$. Hence

$$xA = g_1(x, u'_1)v_1 + g_1(x, u'_2)v_2 + \ldots. + g_1(x, u'_m)v_r$$

and consequently

$$A = u'_1 \times v_1 + u'_2 \times v_2 + \ldots + u'_r \times v_r.$$

□

For $u'_1, \ldots, u'_m \in \Re'_1$ and $v'_1, \ldots, v_n \in \Re_2$ we define linear transformation $A' = u'_1 \times' v_1 + \ldots + u'_m \times' v_m : \Re'_2 \to \Re'_1$ by

$$A'x' = u'_1 g_2(v_1, x') + u'_2 g_2(v_2, x') + .. + u'_m g_2(v_m, x')$$

for all $x' \in \Re'_2$.

**Theorem 3.6.** *The linear transformation $A' = u'_1 \times' v_1 + \ldots + u'_m \times' v_m$ is the transpose of $A = u'_1 \times v_1 + u'_2 \times v_2 + \ldots + u'_m \times v_m$ relative to the pair $g_1, g_2$.*

*Proof.* Take $x \in \Re_1$ and $x' \in \Re'_2$, then

$$g_1(x, A'x') = g_1\left(x, \sum_{i=1}^{m} u'_i g_2(v_i, x')\right) = \sum_{i=1}^{m} g_1(x, u'_i) g_2(v_i, x')$$

$$g_2(xA, x') = g_2\left(\sum_{i=1}^{m} g_1(x, u_i)v_i, x'\right) = \sum_{i=1}^{m} g_1(x, u'_i) g_2(v_i, x')$$

Hence $g_1(x, A'x') = g_2(xA, x')$, as we wanted to show. □

**Theorem 3.7.** *The product* $\times : \Re_1' \times \Re_2 \to L(\Re_1, \Re_2)$ *satisfies*

$$\begin{aligned}(u_1' + u_2') \times v &= u_1' \times v + u_2' \times v,\\ u' \times (v_1 + v_2) &= u' \times v_1 + u' \times v_2,\\ (u'\alpha) \times v &= u' \times (\alpha v)\end{aligned}$$

*for all* $u', u_1', u_2' \in \Re_1'$, $v, v_1, v_2 \in \Re_2$ *and* $\alpha \in \mathbb{D}$.

*Proof.* The bilinearity of $g_1$ imply that

$$\begin{aligned}(u_1 + u_2) \times v = g_1(x, (u_1' + u_2'))v &= g_1(x, u_1')v + g_1(x, u_2')v = u_1 \times v + u_2 \times v,\\ u' \times (v_1 + v_2) = g_1(x, u')(v_1 + v_2) &= g_1(x, u')v_1 + g_1(x, u')v_2 = u' \times v_1 + u' \times v_2,\\ u'\alpha \times v = g_1(x, u'\alpha)v &= g_1(x, u')\alpha v = u' \times \alpha v.\end{aligned}$$

□

# 4 Scalar products

**Definition 4.1.** A bijective map $f : \mathbb{D} \to \mathbb{D}$ such that

$$f(\alpha + \beta) = f(\alpha) + f(\beta)$$

for all $\alpha, \beta \in \mathbb{D}$ and

$$f(\alpha\beta) = f(\beta)f(\alpha)$$

for all $\alpha, \beta \in \mathbb{D}$ is an *anti-automorphism* of the division ring $\mathbb{D}$.

*Remark* 4.2. If $\mathbb{D} = \mathbb{F}$ is a field, then an anti-automorphism is just an automorphism $f : \mathbb{F} \to \mathbb{F}$ of the field.

Let $\Re$ be a left vector space over a division ring $\mathbb{D}$ and $\Re'$ be a right vector space over a division ring $\mathbb{D}$. If a division ring $\mathbb{D}$ possesses an anti-automorphism, we have a possibility of defining a non-degenerate bilinear form connecting a left vector space $\Re$ with itself and regarding $\Re$ as the dual of itself.
Let $\Re$ be a left vector space over a division ring $\mathbb{D}$ and $\Re'$ be a right vector space over a division ring $\mathbb{D}$. Let $f$ be an anti-automorphism and let $f^{-1}$ be its inverse. Then we can easily turn a left vector space $\Re$ into a right vector space if we set

$$xf(\alpha) = \alpha x$$

for all $x \in \Re$ and for all $\alpha \in \mathbb{D}$. Or in other words $x\alpha = f^{-1}(\alpha)x$. In the same way we may also turn a right vector space into a left vector space.

**Proposition 4.3.** *A left vector space $\Re$ over a division ring $\mathbb{D}$ becomes a right vector space over $\mathbb{D}$ if we set*

$$x\alpha = f^{-1}(\alpha)x$$

*for all $x \in \Re$ and for all $\alpha \in \mathbb{D}$.*

*Proof.* If $x, y \in \Re$ and $\alpha, \beta \in \mathbb{D}$ are arbitrary, then

$$(x + y)\alpha = f^{-1}(\alpha)(x + y) = f^{-1}(\alpha)x + f^{-1}(\alpha)y = x\alpha + y\alpha,$$

$$x(\alpha + \beta) = f^{-1}(\alpha + \beta)x = (f^{-1}(\alpha) + f^{-1}(\beta))x = f^{-1}(\alpha)x + f^{-1}(\beta)x = x\alpha + x\beta,$$

and

$$x(\alpha\beta) = f^{-1}(\alpha\beta)x = f^{-1}(\beta)(f^{-1}(\alpha)x) = f^{-1}(\beta)(x\alpha) = (x\alpha)\beta.$$

Moreover, $x1 = f^{-1}(1)x = 1x = x$ for all $x \in \Re$ □

**Proposition 4.4.** *If $(e_1, \dots, e_n)$ is a left basis for a vector space $\mathfrak{R}$ then it is also a right basis for $\mathfrak{R}$.*

*Proof.* Since $(e_1, \dots, e_n)$ is a left basis of $\mathfrak{R}$, each element $x \in \mathfrak{R}$ can be written as

$$x = \sum_{i=1}^{n} \xi_i e_i$$

for some $\xi_i \in \mathbb{D}$. By using the anti-automorphism we deduce that

$$x = \sum_{i=1}^{n} e_i f(\xi_i).$$

Moreover, if $\sum_{i=1}^{n} e_i \delta_i = 0$, then $\sum_{i=1}^{n} f^{-1}(\delta_i) e_i = 0$. Hence, we deduce that $f^{-1}(\delta_i) = 0$ and $\delta_i = 0$. □

**Definition 4.5.** A *scalar product* is a map $g : \mathfrak{R} \times \mathfrak{R} \to \mathbb{D}$ such that

$$g(x_1 + x_2, y) = g(x_1, y) + g(x_2, y),$$

$$g(\alpha x, y) = \alpha g(x, y),$$

$$g(x, y_1 + y_2) = g(x, y_1) + g(x, y_2),$$

and

$$g(x, \alpha y) = g(x, y) f(\alpha)$$

for all $x, y, x_1, y_1, x_1, y_2 \in \mathfrak{R}$ and for all $\alpha \in \mathbb{D}$.

**Definition 4.6.** Let $(e_1, \dots, e_n)$ be a basis for a vector space $\mathfrak{R}$ over a division ring $\mathbb{D}$. The matrix of the scalar product $g$ relative to $(e_1, \dots, e_n)$ is

$$G := \begin{bmatrix} g(e_1, e_1) & g(e_1, e_2) & \dots & g(e_1, e_n) \\ g(e_2, e_1) & g(e_2, e_2) & \dots & g(e_2, e_n) \\ \vdots & \vdots & \ddots & \vdots \\ g(e_n, e_1) & g(e_n, e_2) & \dots & g(e_n, e_n) \end{bmatrix}. \tag{4.1}$$

Similarly as before, the value of $g(x, y)$ can be deduced from representation of $x$ and $y$ and from the entries of a matrix (4.1) defined above. Namely assume that $x = \sum_{i=1}^{n} \xi_i e_i$ for some $\xi_i \in \mathbb{D}$ and $y = \sum_{i=1}^{n} \beta_i e_i$ for some $\beta_i \in \mathbb{D}$. Then

$$g(x, y) = \sum_{i,j} \xi_i g(e_i, e_j) f(\beta_j).$$

Conversely, if a basis $(e_1, \dots, e_n)$ for a vector space $\mathfrak{R}$ is given and a matrix of the scalar product relative to a given basis is given, we can define a scalar product in $\mathfrak{R}$.

**Definition 4.7.** Let $(f_1, \dots, f_n)$ be another basis for a vector space $\mathfrak{R}$ and suppose that $f_i = \sum_{i=1}^{n} \mu_{ij} e_j$ for some $\mu_{ij} \in \mathbb{D}$. Denote $M := (\mu_{ij}) \in M_n(\mathbb{D})$. Now if we regard a vector space $\mathfrak{R}$ as a right vector space by using an anti-automorphism $f$ then $f_i = \sum_{i=1}^{n} e_j v_{ji}$, where $v_{ji} = f(\mu_{ij})$.

Thus the matrix connecting the right bases is $V = [f(\mu_{ij})]^T$. The matrix $V$ is the *conjugate transpose* of a matrix $M$.

We have seen before that the new matrix of $g(x, y)$ is $P := MGV$. We say that matrices $P$ and $G$ are *cogredient* relative to a given anti-automorphism.
Let $\mathfrak{R}$ be a vector space. Let $\mathfrak{S}$ be a subspace of a vector space $\mathfrak{R}$. Obviously, the restriction of the function $g : \mathfrak{R} \times \mathfrak{R} \to \mathfrak{R}$ to the pairs of vectors of a subspace $\mathfrak{S}$ is a scalar product for $\mathfrak{S}$.

**Definition 4.8.** Let $\mathfrak{R}$ be a vector space, let $\mathfrak{S}_1$ and $\mathfrak{S}_2$ be its subspaces. Then subspaces $\mathfrak{S}_1$ and $\mathfrak{S}_2$ are *g-equivalent* if there exist a bijective linear map $U : \mathfrak{S}_1 \to \mathfrak{S}_2$ such that

$$g(x_1, y_1) = g(U(x_1), U(y_1))$$

for all $x_1, y_1 \in \mathfrak{S}_1$.

**Theorem 4.9.** *Let $\mathfrak{R}$ be a vector subspace and let $\mathfrak{S}_1$ and $\mathfrak{S}_2$ be subspaces of a vector space $\mathfrak{R}$. Then subspaces $\mathfrak{S}_1$ and $\mathfrak{S}_2$ are g-equivalent if and only if matrices of scalar products $g : \mathfrak{S}_1 \times \mathfrak{S}_1 \to \mathbb{D}$ and $g : \mathfrak{S}_2 \times \mathfrak{S}_2 \to \mathbb{D}$ determined by arbitrary bases in $\mathfrak{S}_1$ and $\mathfrak{S}_2$ are cogredient.*

*Proof.* Let $\mathfrak{R}$ be a vector subspace and let $\mathfrak{S}_1$ and $\mathfrak{S}_2$ be subspaces of a vector space $\mathfrak{R}$. Assume that subspaces $\mathfrak{S}_1$ and $\mathfrak{S}_2$ are $g$-equivalent. Let $(e_1, \dots, e_n)$ be a basis for $\mathfrak{S}_1$, then by the definition

$$g(e_i, e_i) = g(U(e_i), U(e_j)).$$

Moreover $(U(e_1), \dots, U(e_n))$ is a basis for a subspace $\mathfrak{S}_2$. Hence the matrices of the restriction of g relative to these bases are identity matrices. Hence, if we choose arbitrary bases in $g$-equivalent subspaces, matrices determined by these bases are cogredient.
Conversely, assume that subspaces $\mathfrak{S}_1$ and $\mathfrak{S}_2$ are subspaces such that any matrices relative to g determined by arbitrary bases are cogredient.
Choose a basis $(e_1, \dots, e_n)$ for a subspace $\mathfrak{S}_1$ and a basis $(f_1, \dots, f_n)$ for a subspace $\mathfrak{S}_2$ such that

$$g(e_i, e_j) = g(f_i, f_j)$$

Let $x_1, y_1 \in \mathfrak{S}_1$. Then we know that $x_1 = \sum_{i=1}^{n} \xi_i e_i$ for some $\xi_i \in \mathbb{D}$ and $y_1 = \sum_{j=1}^{n} \gamma_j e_j$ for some $\gamma_j \in \mathbb{D}$. We have that,

$$g(x_1, y_1) = \sum_{i,j} \xi_i g(e_i, e_j)\overline{\gamma_i} = \sum_{i,j} \xi_i g(f_i, f_j) f(\gamma_i) = g\left(\sum_{i=1}^{n} \xi_i f_i, \sum_{j=1}^{n} \gamma_j f_j\right).$$

Define a linear map $U : \sum_{i=1}^{n} \xi_i e_i \to \sum_{j=1}^{n} \gamma_j f_j$. Clearly it is a bijective map of $\mathfrak{S}_1$ onto $\mathfrak{S}_2$ which satisfies the required properties. Hence subspaces $\mathfrak{S}_1$ and $\mathfrak{S}$ are $g$-equivalent. □

# 5 Hermitian scalar products

**Definition 5.1.** An anti-automorphism is *involutorial* if

$$f(f(\alpha)) = \alpha$$

for all $\alpha \in \mathbb{D}$. In this case we denote $f(\alpha)$ by $\overline{\alpha}$.

**Definition 5.2.** Let $\Re$ be a vector space. A scalar product $g$ is *hermitian* if

$$g(x, y) = \overline{g(x, y)}$$

for all $x, y \in \Re$.

**Definition 5.3.** In the case when $\Re$ is a vector space over a field $\mathbb{F}$ and $f(\alpha) = \alpha$ is the identity map, then a scalar product is *symmetric* if

$$g(y, x) = g(x, y).$$

**Theorem 5.4.** *A scalar product $g(x, y)$ is hermitian if and only if matrices $G$ of a scalar product are hermitian, that is $G = \overline{G}^T$.*

*Proof.* Let $\Re$ be a vector space over a division ring $\mathbb{D}$. Let $(e_1, \ldots, e_n)$ be a basis for a vector space $\Re$, and let $G$ be a matrix of the scalar product $g$ relative to a given basis. If the scalar product is hermitian, then

$$\beta_{ij} = g(e_i, e_j) = \overline{g(e_j, e_i)} = \overline{\beta_{ji}}$$

for all $i, j$, which implies that $G = \overline{G}^T$.

Conversely, we know that $x, y \in \Re$ can be written as $x = \sum_{i=1}^{n} \xi_i e_i$ for some $\xi_i \in \mathbb{D}$ and $y = \sum_{i=1}^{n} \gamma_i e_i$ for some $\gamma_i \in \mathbb{D}$. Then

$$g(y, x) = \sum_{i,j} \gamma_i g(e_i, e_j)\overline{\xi_j} = \sum_{i,j} \gamma_i g(e_i, e_j)\overline{\xi_j}$$

and

$$\overline{g(x, y)} = \overline{\sum_{i,j} \xi_i g(e_i, e_j)\overline{\gamma_j}} = \sum_{i,j} \gamma_j g(e_j, e_i)\overline{\xi_i} = \sum_{i,j} \gamma_i g(e_i, e_j)\overline{\xi_j}$$

Hence, $g(y, x) = \overline{g(x, y)}$. □

*Remark* 5.5. In a case of a vector space over a field, which is equipped with the identity map, the scalar product $g(x, y)$ is symmetric if and only if its matricex is symmetric, that is $G^T = G$.

**Definition 5.6.** Let $g(x, y)$ be a hermitian product. If $g(u, v) = 0$ for particular vectors $v, u$, then $g(v, u) = \overline{g(u, v)} = 0$ and vectors $u$ and $v$ are *orthogonal* relative to g.

**Definition 5.7.** Let $\mathfrak{R}$ be a vector space and let $\mathfrak{S}$ be its subspace. Then the subspace

$$\mathfrak{S}^{\perp} := \{v \in \mathfrak{R} : g(v, u) = 0 \text{ for all } u \in \mathfrak{S}\}$$

is the *orthogonal complement* of $\mathfrak{S}$.

*Remark* 5.8. The subspace $\mathfrak{S}^{\perp}$ is not in general a complement of $\mathfrak{S}$ in the lattice of all subspaces.

**Definition 5.9.** Let $\mathfrak{R}$ be a vector space over a division ring $\mathbb{D}$. Then the subspace

$$\mathfrak{R}^{\perp} = \{z \in \mathfrak{R} : g(z, x) = 0 \text{ for all } x \in \mathfrak{R}\}$$

is the *radical* of the scalar product $g(x, y)$. The scalar product is *non-degenerate* if $\mathfrak{R}^{\perp} = \{0\}$.

*Remark* 5.10. In the case of a non-degenerate scalar product, the orthogonal complement $\mathfrak{S}^{\perp}$ of $\mathfrak{S}$ coincides with the space $j(\mathfrak{S})$ that was defined for more general non-degenerate bilinear forms.

**Definition 5.11.** Let $\mathfrak{R}$ be a vector space and let $\mathfrak{S}$ be its subspace. Then $\mathfrak{S}$ is *isotropic* if

$$\mathfrak{S} \cap \mathfrak{S}^{\perp} \neq \{0\}.$$

*Remark* 5.12. The condition $\mathfrak{S} \cap \mathfrak{S}^{\perp} \neq \{0\}$ implies that $\mathfrak{S}$ contains a non-zero vector $u$ which is *isotropic*, that is

$$g(u, u) = 0.$$

**Definition 5.13.** Let $\mathfrak{R}$ be a vector space over a division ring $\mathbb{D}$ and let $\mathfrak{S}$ be its subspace. A subspace $\mathfrak{S}$ is *totally isotropic* if $\mathfrak{S} \subseteq \mathfrak{S}^{\perp}$.

*Remark* 5.14. If g is non-degenerate and $\mathfrak{S}$ is non-isotropic subspace, then $\mathfrak{S} \cap \mathfrak{S}^{\perp} = \{0\}$ and $dim\mathfrak{S}^{\perp} = n - dim\mathfrak{S}$. Hence in this case we have a decomposition $\mathfrak{R} = \mathfrak{S} \oplus \mathfrak{S}^{\perp}$.

## 5.1 Matrices of hermitian scalar products

**Definition 5.15.** Let $\mathbb{F}$ be a field. If

$$0 = n = 1 + 1 + \cdots + 1$$

then the smallest such $n$ is the characteristic of a field $\mathbb{F}$. We denote it by $Char(\mathbb{F})$.

**Definition 5.16.** Let $g$ be a symmetric scalar product on a vector space over a field. The function $Q(x) = g(x,x)$ of a single vector $x \in \Re$ determined by the scalar product is the *quadratic form* determined by $g$.

If a hermitian scalar product is symmetric, that is, $\mathbb{D} = \mathbb{F}$ is a field and $\overline{\alpha} = \alpha$ is the identity map, then in the rest of the chapter we assume that $char(\mathbb{F}) \neq 2$.

**Definition 5.17.** Let $g$ be a hermitian scalar product. If for an element $\beta \in \mathbb{D}$ there exist a vector $u \neq 0 \in \Re$ such that

$$g(u,u) = \beta,$$

then $\beta \in \mathbb{D}$ is *represented* by the scalar product.

**Proposition 5.18.** *Elements represented by a scalar product are invariant under an anti-automorphism $f$.*

*Proof.* If $\beta \in \mathbb{D}$ is represented by a scalar product $g$, then

$$\beta = g(u,u) = \overline{g(u,u)} = \overline{\beta}.$$

□

**Proposition 5.19.** *Let $\Re$ be a vector space. If $\Re$ is not totally isotropic, then there exist a vector $u \in \Re$ such that $u$ is non-isotropic.*

*Remark* 5.20. The proposition above says that if $g(x,y) \neq 0$ is a hermitian scalar product, then there exists an element not equal to 0, which is represented by the scalar product $g(x,y)$.

*Proof.* Assume that there does not exist non-zero elements which are represented by the scalar product, that is

$$g(u,u) = 0$$

for all $u \in \Re$. Then

$$g(x,y) + g(y,x) = g(x+y, x+y) - g(x,x) - g(y,y) = 0$$

for all $x, y \in \mathfrak{R}$. By the assumption $g(x, y)$ is a hermitian scalar product, that is $g(x, y) = \overline{g(y, x)}$. Since

$$g(x, y) + g(y, x) = 0$$

it follows that $g(x, y) = -\overline{g(x, y)}$. Now since $g(x, y) \neq 0$, then there exist vectors $u, v \in \mathfrak{R}$ such that $g(u, v) = \rho \neq 0$. If we replace $u$ by $\rho^{-1}u$ and change the notation, we can suppose that $g(u, v) = 1$. Consequently,

$$\overline{\alpha} = \overline{g(u, v)}\overline{\alpha} = \overline{\alpha g(u, v)} = \overline{g(\alpha u, v)} = -g(\alpha u, v) = -\alpha g(u, v) = -\alpha.$$

Since $\overline{1} = 1$, this implies that the characteristic is two and $\overline{\alpha} = \alpha$ for all $\alpha \in \mathbb{D}$. Hence an anti-automorphism is the identity mapping and $\mathbb{D} = \mathbb{F}$ is commutative. However due to our assumptions we do not consider this case.

□

**Theorem 5.21.** *Let $\mathfrak{R}$ be a vector space of dimension n. Let $g(x, y)$ be a hermitian scalar product, then there exist a basis $(u_1, \ldots, u_r, z_1, \ldots, z_{n-r})$ of $\mathfrak{R}$ such that*

$$g(u_i, u_i) = \beta_i \neq 0$$

*for $i = 1, 2, \ldots, r$ and all other products of pairs of the basis elements equal 0.*

*Proof.* In the case when the hermitian product $g = 0$ we can take $r = 0$ and any basis to be a set of $z$'s. From now on we will assume $g \neq 0$. We know from Proposition 5.19 that there exists some vector $u_1 \in \mathfrak{R}$ such that $g(u_1, u_1) = \beta_1 \neq 0$.
Assume that $(u_1, u_2, \ldots, u_k)$ are linearly independent vectors such that

$$g(u_i, u_i) = \beta_i \neq 0$$

and $g(u_i, u_u) = 0$ whenever $i \neq j$.
Let $\mathfrak{S}_k$ be the subspace in $\mathfrak{R}$ that is spanned by vectors $u_1, \ldots, u_k$.
Define a linear map $E_k : \mathfrak{R} \to \mathfrak{S}_k$ by

$$x \mapsto \sum_{i=1}^{k} g(x, u_i)\beta_i^{-1}u_i.$$

The map $E_k$ is the identity map on $\mathfrak{S}_k$, since $E_k(u_j) = \sum_{i=1}^{k} g(u_j, u_i)\beta_i^{-1}u_i = u_j$. Consequently, $E_k^2 = E_k$ on $\mathfrak{S}_k$. Hence, $\mathfrak{R} = \mathfrak{S}_k \oplus F_k(\mathfrak{R})$ for the map $F_K := I - E_k$. Moreover

$$g(E_k(x), u_j) = g\left(\sum_1^k g(x, u_i)\beta_i^{-1}u_i, u_j\right) =$$

$$= \sum_1^k g(x, u_i)\beta_i^{-1}g(u_i, u_j) = g(x, u_j).$$

Therefore

$$g(F_k(x), u_j) = g((I - E_k)(x_k), u_j) = g(x, u_j) - g(E_k(x), u_j) = 0,$$

which means that the vectors in $F_k(\mathfrak{R})$ are orthogonal to each vector in $\mathfrak{S}_k$. Consequently $F_k(\mathfrak{R}) \subseteq \mathfrak{S}_k^{\perp}$.

Assume firstly that the scalar product $g = 0$ for all vectors $u \in F_k(\mathfrak{R})$. Then choose a basis $(z_1, \ldots, z_m)$ for a subspace $F_k(\mathfrak{R})$. Since $\mathfrak{R} = \mathfrak{S}_k \oplus F_k(\mathfrak{R})$, then $(u_1, u_2, \ldots, u_k, z_1, \ldots, z_m)$ is a basis for $\mathfrak{R}$. And hence this is a basis that we wanted to find, as $F_k(\mathfrak{R}) \subseteq \mathfrak{S}_k$.

If the scalar product $g \neq 0$ in $F_k(\mathfrak{R})$, then we can find a vector $u_{k+1} \in F_k(\mathfrak{R})$ such that $g(u_{k+1}, u_{k+1}) = \beta_{k+1} \neq 0$. This implies that $(u_1, \ldots, u_{k+1})$ are linearly independent vectors and since $u_{k+1} \in F_k(\mathfrak{R})$ and vectors in $F_k(\mathfrak{R})$ are orthogonal to $u_i$, $i \in (1, \ldots, k)$, the new set $(u_1, \ldots, u_{k+1})$ satisfies the same conditions as $(u_1, \ldots, u_k)$. The process can be repeated to find a required basis for a vector space $\mathfrak{R}$. □

*Remark* 5.22. In Theorem 5.21, any vector $u_i$ can be replaced by $\gamma_i u_i$, where $\gamma_i \neq 0$. Namely, if $\beta_i' := \gamma_i \beta_i \overline{\gamma_i}$, then we get $g(\gamma_i u_i, \gamma_i u_i) = \gamma_i \beta_i f(\gamma_i) = \beta_i'$.

# 6 Symmetric and hermitian scalar products over special division rings

In this chapter we will consider the special case of the cogredience problem. In particular we will discuss conditions for cogredience of diagonal matrices. First we will specialize the result from the preceding section to the case when a vector space $\Re$ is over a field $\mathbb{F}$ and $\overline{\alpha} = \alpha$ is the identity map.
Recall that $M_{n\times n}(\mathbb{F})$ denotes the set of all $n \times n$ matrices with coefficients in $\mathbb{F}$.

**Definition 6.1.** Let $\mathbb{F}$ be a field. Denote $\mathbb{F}[x]$ is the ring of polynomials in the variable x with coefficients in $\mathbb{F}$. If $\mathbb{F}$ contains a root for every non-constant polynomial in $\mathbb{F}[x]$, then a field $\mathbb{F}$ is algebraically closed.

**Theorem 6.2.** *Let $\mathbb{F}$ be algebraically closed field such that $Char(\mathbb{F}) \neq 2$. Then any two symmetric matrices in $M_{n\times n}(\mathbb{F})$ are cogredient if and only if they have the same rank.*

*Proof.* Let $g(x, y)$ be a symmetric scalar product. Let $(u_1, \dots, u_n)$ be a basis such that

$$g(u_i, u_j) = \delta_{ij}\beta_i$$

where $\beta_i \neq 0$ for $i \in \{1, \dots, r\}$. Hence $r$ is the rank of the matrix

$$\begin{bmatrix} \beta_1 & 0 & \dots & 0 \\ 0 & \beta_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \beta_n \end{bmatrix} \tag{6.1}$$

of the symmetric scalar product $g(x, y)$. Since we can take any element $\beta_i \neq 0$ that is represented by a scalar product, $r$ is is the rank of any matrix of the symmetric scalar product. Denote $v_i := \gamma_i u_i$. As we have seen in the last Remark of the preceding chapter we can substitute each vector $u_i$ by $v_i = \gamma_i u_i$, where $\gamma_i \neq 0$. Hence $(v_1, \dots, v_n)$ form another basis and the matrix determined by this basis is

$$\begin{bmatrix} \beta_1' & 0 & \dots & 0 \\ 0 & \beta_2' & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \beta_n' \end{bmatrix} \tag{6.2}$$

where $\beta_i = \gamma_i \beta_i \overline{\gamma_i}$. However now $\mathfrak{R}$ is a vector space over a field $\mathbb{F}$, and $\overline{\alpha} = \alpha$ is the identity map. Hence $\beta_i' = \gamma_i^2 \beta_i$. Since $\mathbb{F}$ is algebraically closed, every element in $\mathbb{F}$ is a square. Hence, for each $i \leq r$ there exists $\gamma_i \in \mathbb{F}$ such that $\gamma_i^2 = \frac{1}{\beta_i}$. Hence our matrix in Equation (6.2) becomes a matrix which looks as follows

$$\begin{bmatrix} I_r & 0_{r,n-r} \\ 0_{n-r,r} & 0_{n-r,n-r} \end{bmatrix}. \tag{6.3}$$

Let $G$ is any symmetric matrix, then $G$ can be used to define a symmetric scalar product in $\mathfrak{R}$ over the field $\mathbb{F}$. The matrices of this scalar product constitute the cogredience class determined by the matrix $G$. Hence any symmetric matrix $G \in M_{n\times n}(\mathbb{F})$ is cogrediente to a matrix of the form (6.3). And obviously matrix in Eq 6.3 is completely determined by the rank of $G$. □

## 6.1 Case $\mathbb{F} = \mathbb{R}$

Let a field $\mathbb{F}$ be the field of real numbers, that is $\mathbb{F} = \mathbb{R}$. Let $(u_1, \ldots, u_n)$ be vectors such that

$$\beta_i > 0$$

for $i = 1, \ldots, p$ and

$$\beta_j < 0$$

for $j = p+1, \ldots, r$, here, $p \in \{0, 1, \ldots, r\}$. Define $\gamma_i = \frac{1}{\sqrt{\beta_i}}$ for $i \leq p$ and $\gamma_j = \frac{1}{\sqrt{-\beta_j}}$ for $p < j \leq r$.

The matrix of $g$ with respect to the basis $(v_1, \ldots, v_r, u_{r+1}, \ldots, u_n)$, where $v_i = \gamma_i \mu_i$, equals

$$\begin{bmatrix} I_p & 0_{r-p} & 0_{n-r} \\ 0_p & I_{r-p} & 0_{n-r} \\ 0_p & 0_{r-p} & 0_{n-r} \end{bmatrix} \tag{6.4}$$

Hence any real symmetric matrix is cogredint to a matrix of the form (6.4).

**Definition 6.3.** The *signature* of a diagonal matrix is the difference $2p - r$ between the number of positive elements and the number of negative elements on the diagonal of matrix (6.1).

**Proposition 6.4.** *Recall that if $\mathfrak{R}$ is a vector space and $\mathfrak{S}_1, \mathfrak{S}_2$ are its vector subspaces, then*

$$dim(\mathfrak{S}_1 \cap \mathfrak{S}_2) = dim\mathfrak{S}_1 + dim\mathfrak{S}_2 - dim(\mathfrak{S}_1 + \mathfrak{S}_2).$$

**Theorem 6.5** (Sylvester)**.** *Let $\mathfrak{R}$ be a vector space over $\mathbb{F} = \mathbb{R}$ and let $\overline{\alpha} = \alpha$ be the identity map. Let*

$$\begin{bmatrix} \beta_1 & 0 & \dots & 0 \\ 0 & \beta_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \beta_n \end{bmatrix} \tag{6.5}$$

*and*

$$\begin{bmatrix} \beta'_1 & 0 & \dots & 0 \\ 0 & \beta'_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \beta'_n \end{bmatrix} \tag{6.6}$$

*be matrices that are cogredient in $M_{n\times n}(\mathbb{F})$. Let $p$ be the number of positive $\beta_i$ in the matrix (6.5) and let $p'$ be the numbet of positive $\beta'_i$ in the matrix (6.6). Then $p = p'$.*

*Proof.* Let $(u_1, \dots, u_n)$ be a basis relative to which the matrix of $g(x, y)$ is the matrix (6.5) and let $(v_1, \dots, v_n)$ be a basis relative to which the matrix of $g(x, y)$ is the matrix (6.6). We may assume that

$$\begin{aligned} \beta_1, \dots, \beta_p &> 0, \\ \beta_{p+1}, \dots, \beta_r &< 0, \\ \beta_{r+1}, \dots, \beta_n &= 0. \end{aligned}$$

And similarly

$$\begin{aligned} \beta'_1, \dots, \beta'_{p'} &> 0, \\ \beta'_{p'+1}, \dots, \beta'_r &< 0, \\ \beta'_{r+1}, \dots, \beta'_n &= 0. \end{aligned}$$

Hence the radical of the vector space $\mathfrak{R}$ is the set $\mathfrak{R}^\perp = [u_{r+1}, \dots, u_n] = [v_{r+1}, \dots, v_n]$, where $[x_1, \dots, x_k]$ denotes the subspace that is spanned by vectors $x_1, \dots, x_k$. Define

$$\begin{aligned} \mathfrak{R}_+ &= [u_1, \dots, u_p], \\ \mathfrak{R}_- &= [u_{p+1}, \dots, u_r], \\ \mathfrak{S}_+ &= [v_1, \dots, v_{p'}], \\ \mathfrak{S}_- &= [v_{p'+1}, \dots, v_r]. \end{aligned}$$

Let $y \in \mathfrak{R}_+ + \mathfrak{R}^\perp$. Then $y = \sum_{i=1}^{p} \eta_i u_i + \sum_{j=r+1}^{n} \eta_j u_j$ for some $\eta_1, \dots, \eta_n \in \mathbb{R}$. Consequntly,

$$g(y, y) = g\left(\sum_{i=1}^{p} \eta_i u_i + \sum_{j=r+1}^{n} \eta_j u_j, \sum_{i=1}^{p} \eta_i u_i + \sum_{j=r+1}^{n} \eta_j u_j\right) = \sum_{i=1}^{p} \eta_i^2 \beta_i.$$

By the assumption $\beta_i > 0$ for $i \in \{1, \dots, p\}$. Hence $g(y,y) \geq 0$ and $g(y,y) = \sum_{i=1}^{p} \eta_i^2 \beta_i =$ 0 if and only if $\eta_i = 0$ for $i \in \{1, \dots, p\}$. Hence $g(y,y) \geq 0$ and $g(y,y) = \sum_{1}^{p} \eta^2 \beta_i = 0$ only if $y \in \mathfrak{R}^{\perp}$. A similar observation holds for vectors in $\mathfrak{S}_+ + \mathfrak{R}^{\perp}$.
On the other side, the same argument shows that if $y \in \mathfrak{S}_- + \mathfrak{R}^{\perp}$ or $y \in \mathfrak{R}_- + \mathfrak{R}^{\perp}$, then $g(y,y) \leq 0$ and $g(y,y) = 0$ only if $y \in \mathfrak{R}^{\perp}$.
Now let $y \in (\mathfrak{R}_+ + \mathfrak{R}^{\perp}) \cap (\mathfrak{S}_- + \mathfrak{R}^{\perp})$. Then $g(y,y) \geq 0$ and $g(y,y) \leq 0$, which implies that $g(y,y) = 0$ and hence $y \in \mathfrak{R}^{\perp}$. Consequntly,

$$(\mathfrak{R}_+ + \mathfrak{R}^{\perp}) \cap (\mathfrak{S}_- + \mathfrak{R}^{\perp}) = \mathfrak{R}^{\perp}. \tag{6.7}$$

By Proposition 6.4.

$$dim(\mathfrak{S}_1 \cap \mathfrak{S}_2) = dim\mathfrak{S}_1 + dim\mathfrak{S}_2 - dim(\mathfrak{S}_1 + \mathfrak{S}_2) \geq dim\mathfrak{S}_1 + dim\mathfrak{S}_2 - n.$$

By (6.7) we get that

$$n - r \geq p + (n-r) + (r - p') + (n - r) - n.$$

Hence we get that $p - p' \leq 0$, so $p \leq p'$.
Similarly, by

$$(\mathfrak{R}_- + \mathfrak{R}^{\perp}) \cap (\mathfrak{S}_+ + \mathfrak{R}^{\perp}) = \mathfrak{R}^{\perp}$$

we get $p' \leq p$ and hence $p = p'$. □

The content of Section 6.1 is summarized in Thereom 6.6.

**Theorem 6.6.** *Two real symmetric matrices of the same size are cogredient if and only if they have the same rank and the same signature.*

## 6.2 Case $\mathbb{F} = \mathbb{C}$

We will assume in this subsection that a vector space $\mathfrak{R}$ is over a field $\mathbb{C}$. We will also assume that an anti-automorphism $f : \mathbb{C} \to \mathbb{C}$ the a map

$$\alpha \mapsto \overline{\alpha}$$

for all $\alpha \in \mathbb{C}$, where $\overline{\alpha}$ is the complex conjugate. Let $g(x,y)$ be a hermitian scalar product in a vector space $\mathfrak{R}$ over a field of complex numbers. Then

$$\overline{g(u,u)} = g(u,u) \in \mathbb{R}$$

for any $u \in \Re$.
Let $(u_1, \dots, u_n)$ be a basis such that

$$g(u_i, u_i) = \beta_i \neq 0$$

for $i = 1, 2, \dots, r$ and all other products equals 0. Then $\beta_i \in \mathbb{R}$ for all $i$. If we replace $u_i$ by $v := \gamma_i u_i$, where $\gamma_i \neq 0$, then $g(\gamma_i u_i, \gamma_i u_i) = \gamma_i \beta_i \overline{\gamma_i} = |\gamma_i|^2 \beta_i$. Hence a vector space $\Re$ has a basis relative to which the matrix of $g$ has the form

$$\begin{bmatrix} I_p & 0_{r-p} & 0_{n-r} \\ 0_p & I_{r-p} & 0_{n-r} \\ 0_p & 0_{r-p} & 0_{n-r} \end{bmatrix}$$

Theorems 6.7. and 6.8. are proved essentially in the same way as Theorem 6.5 and 6.6., respectively.

**Theorem 6.7.** *Let $\Re$ be a vector space over $\mathbb{F} = \mathbb{C}$ and let $\overline{\alpha} = \alpha$ be the complex conjugation. Let*

$$B = \begin{bmatrix} \beta_1 & 0 & \dots & 0 \\ 0 & \beta_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \beta_n \end{bmatrix} \tag{6.8}$$

*and*

$$B' = \begin{bmatrix} \beta'_1 & 0 & \dots & 0 \\ 0 & \beta'_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \beta'_n \end{bmatrix} \tag{6.9}$$

*be matrices that are cogredient in $M_{n\times n}(\mathbb{C})$,that is there exist an invertible matrix $M \in M_{n\times n}(\mathbb{C})$ such that*

$$B' = MB\overline{M^T}$$

*Let p be the number of positive $\beta_i$ in the matrix (6.8) and let p′ be the numbet of positive $\beta'_i$ in the matrix (6.9). Then $p = p'$.*

**Theorem 6.8.** *Two complex hermitian matrices of the same size are cogredient relative to the complex conjugation if and only if they have the same rank and the same signature.*

# 7 Alternate scalar products

**Definition 7.1.** Let $\Re$ be a vector space. Let $g(x, y)$ be a scalar product. Then $g(x, y)$ is a *skew-symmetric* scalar product if

$$g(x, y) = -g(y, x)$$

for all $x, y \in \Re$.

**Proposition 7.2.** *Let $\Re$ be a vector space. Assume that $g \neq 0$ is a skew symmetric scalar product. Then $\overline{\alpha} = \alpha$ is the identity map and vector space $\Re$ is over a field $\mathbb{D} = \mathbb{F}$.*

*Proof.* Assume that $g \neq 0$ is a skew symmetric scalar product then we know that

$$g(x, y) = -g(y, x)$$

For all $x, y \in \Re$. Since $g \neq 0$ there exist vectors $u, v \in \Re$ such that $g(u, v) = \beta \neq 0$. If we replace $u$ by $\beta^{-1}u$ and change the notation, then we can suppose that $g(u, v) = 1$. Then for any $\alpha \in \mathbb{D}$ we have that

$$\alpha = \alpha g(u, v) = g(\alpha u, v) = -g(v, \alpha u) = -g(v, u)\overline{\alpha} = \overline{\alpha}.$$

Consequently, $\alpha\beta = \overline{\alpha\beta} = \overline{\beta}\overline{\alpha} = \beta\alpha$. Hence, $\mathbb{D}$ is a field. □

If a scalar product $g(x, y)$ is skew-symmetric then $g(x, x) = -g(x, x)$ for all $x \in \Re$. If $Char(\mathbb{F}) \neq 2$, then we deduce that $g(x, x) = 0$ for all $x \in \Re$

**Definition 7.3.** Let $\Re$ be a vector space. A scalar product $g(x, y)$ *alternate* if

$$g(x, x) = 0$$

for all $x \in \Re$.

**Proposition 7.4.** *Let $\Re$ be a vector space. Let $g(x, y)$ be alternate then $g(x, y)$ is skew symmetric.*

*Proof.* Assume that $g(x, y)$ is alternate scalar product, then we know that

$$g(u, u) = 0$$

for all $u \in \mathfrak{R}$. Consequently,

$$g(x,y)+g(y,x)=g(x+y,x+y)-g(x,x)-g(y,y)=0.$$

Hence $g(x,y)+g(y,x)=0$, which implies that $g(x,y)=-g(y,x)$. □

**Theorem 7.5.** *Let $\mathfrak{R}$ be a vector space. Let $g(x,y)$ be an alternate scalar product, then there exist a basis for $\mathfrak{R}$ such that the matrix relative to this basis has the form*

$$S=\begin{bmatrix} J_1 & \dots & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \\ 0 & \dots & J_r & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \\ 0 & \dots & 0 & \dots & 0 \end{bmatrix}$$

*where $J_1,\dots,J_r$ are $r$ blocks of the form*

$$J_i=\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

*Proof.* Let $g(x,y)$ be an alternate scalar product such that $g(x,y)$ is not identically 0. That is, there exist $u,v\in\mathfrak{R}$ such that

$$g(u,v)\neq 0.$$

Replace $v$ by a suitable multiple of $v$, say $v_1:=g(u,v)^{-1}v$. Then we obtain $u_1=u$ and $v_1$ such that $g(u_1,v_1)=1$. Since by Proposition 7.4 we know that $g(x,y)$ is skew symmetric, it follows that $g(v_1,u_1)=-1$. Hence $u_1,v_1$ are linearly independent.
Assume that $u_1,v_1,\dots,u_k,v_k$ are k pairs of linearly independent vectors such that

$$g(u_i,v_i)=1, g(v_i,u_i)=-1$$

and all other products among these $2k$ vectors are equal to 0.
Denote $\mathfrak{S}_k=[u_1,v_1,\dots,u_k,v_k]$. Define a linear map $E_k:\mathfrak{R}\to\mathfrak{S}_k$ such that

$$x\mapsto\sum_{i=1}^{k}g(x,v_i)u_i-\sum_{i=1}^{k}g(x,u_i)v_i$$

for all $x\in\mathfrak{R}$. Then

$$E_k(u_j)=\sum_{i=1}^{k}g(u_j,v_i)u_i-\sum_{i=1}^{k}g(u_j,u_i)v_i=u_j$$

and

$$E_k(v_j)=\sum_{i=1}^{k}g(v_j,v_i)u_i-\sum_{i=1}^{k}g(v_j,u_i)v_i=-v_j$$

for all $j \in \{1, \dots, k\}$. Hence $E_k$ maps as the identity on $\mathfrak{S}_k$ and $E_k^2 = E_k$.
Define $F_k = 1 - E_k$. Then $\mathfrak{R} = \mathfrak{S}_k \oplus F_k(\mathfrak{R})$.
Also we have that

$$(E_k(x), u_j) = g\left(\sum_{i=1}^{k} g(x, v_i)u_i - \sum_{i=1}^{k} g(x, u_i)v_i, u_j\right)$$
$$= g\left(\sum_{i=1}^{k} g(x, v_i)u_i, u_j\right) - g\left(\sum_{i=1}^{k} g(x, u_i)v_i, u_j\right) =$$
$$= \sum_{i=1}^{k} g(x, v_i)g(u_i, u_j) - \sum_{i=1}^{k} g(x, u_i)g(v_i, u_j) = g(x, u_j).$$

Similarly we get that

$$g(E_k(x), v_i) = g(x, v_i).$$

Consequently,

$$g(F_k(x), u_i) = g((I - E_k)(x), u_i) = g(x, u_i) - g(x, u_i) = 0$$

And similarly

$$g(F_k(x), v_i) = 0.$$

Hence we see that $F_k(\mathfrak{R}) \subseteq \mathfrak{S}_k^{\perp}$.
The alternate scalar product $g(x, y)$ is either equal to 0 in the space $F_k(\mathfrak{R})$ or we can choose a pair of vectors $u_{k+1}, v_{k+1}$ such that

$$g(u_{k+1}, v_{k+1}) = 1 = -g(u_{k+1}, v_{k+1})$$

Since $\mathfrak{S}_k \cap F_k(\mathfrak{R}) = \{0\}$, then $(u_1, v_1, \dots, u_{k+1}, v_{k+1})$ is a linearly independent set and since last two vectors $u_{k+1}, v_{k+1}$ are in $F_k(\mathfrak{R})$, it follows that they are orthogonal to the preceding ones. Hence this set of $2(k+1)$ vectors satisfies the same conditions as the set $(u_1, v_1, \dots, u_k, v_k)$. Hence we either span the whole space or obtain the space $F_r(\mathfrak{R})$ in which $g = 0$.
In the latter case we choose any basis, say $(z_{2r+1}, \dots, z_n)$, for the space $F_r(\mathfrak{R})$. Clearly the matrix of the alternate scalar product $g(x, y)$ relative to the basis

$$(u_1, v_1, \dots, u_r, v_r, z_{2r+1}, z_{2r+2}, \dots, z_n)$$

is matrix of the form

$$S = \begin{bmatrix} J_1 & \dots & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \\ 0 & \dots & J_r & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \\ 0 & \dots & 0 & \dots & 0 \end{bmatrix},$$

□

Let $g(x, y)$ be an alternate scalar product. The matrices $A = [a_{ij}]$ of an alternate scalar product $g(x, y)$ are *alternate*, that is

$$A^T = -A$$

and $a_{ii} = 0$ for $i \in \{1, \ldots, n\}$.
From Theorem 7.5 we immediately deduce Propositions 7.6 and 7.7.

**Proposition 7.6.** *The rank of an alternate matrix with elements in a field is even.*

**Proposition 7.7.** *Two alternate matrices $A_1, A_2 \in M_{n \times n}(\mathbb{F})$ are cogredient if and only if their ranks are equal.*

# 8 Witt's theorem

If $\beta \in \mathbb{D}$ satisfies $\overline{\beta} = \beta$, then we say that $\beta$ is a hermitian element. In this section we will assume that the anti-automorphism $\alpha \to \overline{\alpha}$ satisfies the following condition.

**Axiom.** *The equation $\xi + \overline{\xi} = \beta$ has a solution for every hermitian element $\beta \in \mathbb{D}$.*

In the case $Char(\mathbb{D}) \neq 2$ we can take $\xi = \frac{\beta}{2}$ and the Axiom is automatically satisfied.

In the case $Char(\mathbb{D}) = 2$ the axiom is satisfied if, for example, there exist an element $\gamma \in C(\mathbb{D})$ such that $\overline{\gamma} \neq \gamma$, where $C(\mathbb{D})$ is the center of a division ring $\mathbb{D}$. Then $\delta = \gamma + \overline{\gamma} \neq 0 \in C(\mathbb{D})$. Hence if $\xi = \beta\gamma\delta^{-1}$, then

$$\xi + \overline{\xi} = \beta\gamma\delta^{-1} + \beta\overline{\gamma}\delta^{-1} = \beta\delta^{-1}(\gamma + \overline{\gamma}) = \beta.$$

The case when $\mathbb{D} = \mathbb{F}$ is a field and $Char(\mathbb{F}) = 2$, $\overline{\alpha} = \alpha$ is ruled out by the axiom, since in that case $\xi + \overline{\xi} = 0$, while $\beta$ need not to be equal to 0.

Let $\mathfrak{R}$ be a vector space over a division ring $\mathbb{D}$. Let $g(x, y)$ be a non-degenerate hermitian scalar product relative to the anti-automorphism $\alpha \to \overline{\alpha}$.

**Theorem 8.1** (Witt's theorem)**.** *Let $\mathfrak{R}$ be a vector space and let $\mathfrak{S}_1, \mathfrak{S}_2$ be its subspaces. If $\mathfrak{S}_1$ and $\mathfrak{S}$ are non-isotropic and g-equivalent,then $\mathfrak{S}_1^{\perp}$ and $\mathfrak{S}_2^{\perp}$ are g-equivalent.*

*Proof.* The claim is trivial if $g(x, y) = 0$ for all $x, y$. Hence, we may assume that $g \neq 0$.

Step 1 First we show that the claim in Witt's theorem is true if $\dim\mathfrak{S}_1 = 1$ and $\dim\mathfrak{R} = 2$.

Since $\mathfrak{S}_1$ is non-isotropic it follows that $\mathfrak{S}_1 = [u_1]$ for some vector $u_1$ such that $g(u_1, u_1) =: \alpha \neq 0$.

Moreover,

$$\mathfrak{R} = [u_1] \oplus [u_1]^{\perp}.$$

Since $\dim\mathfrak{R} = 2$, it follows that $dim[u_1]^{\perp} = 1$, that is, $[u_1]^{\perp} = [v_1]$ for some vector $v_1$. Denote $g(v_1, v_1) =: \beta_1$. Clearly $g(u_1, v_1) = 0 = g(v_1, u_1)$.

By the assumption, $\mathfrak{S}_1$ and $\mathfrak{S}_2$ are g-equivalent, that is, there is a linear bijection

$$U : \mathfrak{S}_1 \to \mathfrak{S}_2$$

such that

$$g(U(u_1), U(u_1)) = g(u_1, u_1).$$

Now ,

$$\mathfrak{S}_2 = U(\mathfrak{S}_1) = U([u_1]) = [U(u_1)].$$

As above we see that

$$\mathfrak{R} = [U(u_1)] \oplus [U(u_1)]^\perp \text{ and } [U(u_1)]^\perp = [v_2]$$

for some vector $v_2$. Let $u_2 := U(u_1)$ then

$$g(u_2, u_2) = g(U(u_1), U(u_1)) = g(u_1, u_1) = \alpha.$$

Obviously $g(u_2, v_2) = 0 = g(v_2, u_2)$. Denote $\beta_2 := g(v_2, v_2)$. The matrix of $g$ in basis $(u_1, v_1)$ equals

$$\begin{bmatrix} g(u_1, u_1) & g(u_1, v_1) \\ g(v_1, u_1) & g(v_1, v_1) \end{bmatrix} = \begin{bmatrix} \alpha & 0 \\ 0 & \beta_1 \end{bmatrix}.$$

The matrix of $g$ in basis $(u_2, v_2)$ equals

$$\begin{bmatrix} g(u_2, u_2) & g(u_2, v_2) \\ g(v_2, u_2) & g(v_2, v_2) \end{bmatrix} = \begin{bmatrix} \alpha & 0 \\ 0 & \beta_2 \end{bmatrix}.$$

By the change of basis described in Chapter 4, we know that there exist an invertible matrix

$$\begin{bmatrix} \mu_{11} & \mu_{12} \\ \mu_{21} & \mu_{22} \end{bmatrix}$$

such that

$$\begin{bmatrix} \alpha & 0 \\ 0 & \beta_1 \end{bmatrix} = \begin{bmatrix} \mu_{11} & \mu_{12} \\ \mu_{21} & \mu_{22} \end{bmatrix} \begin{bmatrix} \alpha & 0 \\ 0 & \beta_2 \end{bmatrix} \begin{bmatrix} \overline{\mu_{11}} & \overline{\mu_{12}} \\ \overline{\mu_{21}} & \overline{\mu_{22}} \end{bmatrix}.$$

We want to prove that

$$\mathfrak{S}_1^\perp = [v_1] \text{ and } \mathfrak{S}_2^\perp = [v_2]$$

are g-equivalent. That is, we want to find a linear bijection

$$V : [v_1] \to [v_2]$$

such that

$$g(V(v_1), V(v_1)) = g(v_1, v_1). \tag{8.1}$$

Clearly, any linear map $V : [v_1] \to [v_2]$ is of the form $V(v_1) = \epsilon v_2$ for some scalar $\epsilon$. It is bijective if and only if $\epsilon \neq 0$. The condition (8.1) tansforms into

$$\epsilon\beta_2\bar{\epsilon} = \epsilon g(v_2, v_2)\bar{\epsilon} = g(\epsilon v_2, \epsilon v_2) = g(V(v_1), V(v_1)) = g(v_1, v_1) = \beta_1.$$

Therefore we want to find $\epsilon \in \mathbb{D}$ such that

$$\epsilon\beta_2\bar{\epsilon} = \beta_1$$

or equivalently, we want to find $\eta \in \mathbb{D}$ such that

$$\beta_2 = \eta\beta_1\overline{\eta}.$$

In the case when $\mathbb{D} = \mathbb{F}$ is commutative $\beta_2 = det(M)\beta_1 det(M^T)$ and hence elements $\beta_1$ and $\beta_2$ are cogredient.
In the case when $\mathbb{D}$ is not commutative we have the conditions

$$\mu_{11}\alpha\overline{\mu}_{11} + \mu_{12}\beta_1\overline{\mu}_{12} = \alpha \tag{8.2}$$

$$\mu_{11}\alpha\overline{\mu}_{21} + \mu_{12}\beta_1\overline{\mu}_{22} = 0 = \mu_{21}\alpha\overline{\mu}_{11} + \mu_{22}\beta_1\overline{\mu}_{12} \tag{8.3}$$

$$\mu_{21}\alpha\overline{\mu}_{21} + \mu_{22}\beta_1\overline{\mu}_{22} = \beta_2 \tag{8.4}$$

Assume that $\mu_{11} = 0$. Since $M$ is invertible, it follows that $\mu_{12} \neq 0$. Consequently, (8.3) implies that $\mu_{22} = 0$. Hence by (8.4) we get that

$$\beta_2 = \mu_{21}\alpha\overline{\mu}_{21}.$$

By (8.2) we get that

$$\mu_{12}\beta_1\overline{\mu}_{12} = \alpha.$$

This implies that $\beta_1$ and $\beta_2$ are cogredient.
Now assume that $\mu_{11} \neq 0$ then by (8.3) we get that

$$\begin{aligned} \alpha\overline{\mu}_{21} &= -\mu_{11}^{-1}\mu_{12}\beta_1\overline{\mu}_{22}, \\ \mu_{21} &= -\mu_{22}\beta_1\overline{\mu}_{12}\overline{\mu}_{11}^{-1}\alpha^{-1}. \end{aligned}$$

Consequently, by (8.4) we get that

$$\mu_{22}(\beta_1\overline{\mu}_{12}\overline{\mu}_{11}^{-1}\alpha^{-1}\mu_{11}^{-1}\mu_{12}\beta_1 + \beta_1)\overline{\mu}_{22} = \beta_2.$$

Thus $\beta_2$ is cogredient to $(\beta_1\overline{\mu}_{12}\overline{\mu}_{11}^{-1}\alpha^{-1}\mu_{11}^{-1}\mu_{12}\beta_1 + \beta_1)$. Now we want to show that $\beta_1$ is cogredient to $(\beta_1\overline{\mu}_{12}\overline{\mu}_{11}^{-1}\alpha^{-1}\mu_{11}^{-1}\mu_{12}\beta_1 + \beta_1)$. We want to find $\xi$ such that

$$(1 + \beta_1\overline{\mu}_{12}\xi\mu_{12})\beta_1(1 + \overline{\mu}_{12}\overline{\xi}\mu_{12}\beta_1) = (\beta_1\overline{\mu}_{12}\overline{\mu}_{11}^{-1}\alpha^{-1}\mu_{11}^{-1}\mu_{12}\beta_1 + \beta_1),$$

which will be satisfied if $\xi + \overline{\xi} + \xi\mu_{12}\beta_1\overline{\mu}_{12}\overline{\xi} = (\mu_{11}\alpha\overline{\mu}_{11})^{-1}$. From (8.2) we deduce that $\alpha - \mu_{11}\alpha\overline{\mu}_{11} = \mu_{12}\beta_1\overline{\mu}_{12}$, and therefore

$$\xi + \overline{\xi} + \xi(\alpha - \mu_{11}\alpha\overline{\mu}_{11})\overline{\xi} = (\mu_{11}\alpha\overline{\mu}_{11})^{-1}. \tag{8.5}$$

Assume firstly that $\mu_{11} = 1$. Then (8.5) transforms into

$$\xi + \overline{\xi} = (\mu_{11}\alpha\overline{\mu}_{11})^{-1},$$

which is solvable by the Axiom.
If $\mu_{11} \neq 1$ then substitute $\xi$ by $\eta^{-1}$ and multiply on the left by $\eta$ and on the right by $\overline{\eta}$ to get

$$\eta + \overline{\eta} + (\alpha - \mu_{11}\alpha\overline{\mu}_{11}) = \eta(\mu_{11}\alpha\overline{\mu}_{11})^{-1}\overline{\eta}. \tag{8.6}$$

Next we substite $\eta = \zeta + \mu_{11}\alpha\overline{\mu}_{11}$ and obtain

$$\zeta(\mu_{11}\alpha\overline{\mu}_{11})^{-1}\overline{\zeta} = \alpha.$$

We see that the equation above is satisfied by $\zeta = -\alpha\overline{\mu}_{11}$. Hence since we made a substitution $\eta = \zeta + \mu_{11}\alpha\overline{\mu}_{11}$ implies that (8.6) is satisfied by $\eta = \alpha\overline{\mu}_{11}(\mu_{11} - 1)$. Then $\xi = \eta^{-1}$ satisfies (8.5). Hence this shows that $\beta_1$ and $\beta_2$ are cogredient.
Step 2 We show that the claim in Witt's theorem is true if dim$\mathfrak{S}_1 = 1$ and dim$\Re < \infty$ is arbitrary.
As in Step 1 we have

$$\Re = [u_1] \oplus [u_1]^{\perp} \text{ with } g(u_1, u_1) \neq 0$$

and

$$\Re = [u_2] \oplus [u_2]^{\perp},$$

where $u_2 := U(u_1)$ and $U : [u_1] \to [u_2]$ is the linear bijection such that

$$g(U(u_1), U(u_1)) = g(u_1, u_1)$$

that is

$$g(u_2, u_2) = g(u_1, u_1).$$

In the notation above, we have $\mathfrak{S}_1 = [u_1]$ and $\mathfrak{S}_2 = [u_2]$.
We split the proof of step 2 into 3 cases.
*Case 1.* Let dim$[u_1, u_2] = 1$.
Then $u_2 = \lambda u_1$ for some $\lambda \in \mathbb{D}$. Consequently $[u_1]^{\perp} = [u_2]^{\perp}$. Hence, the identity map

$$I : \mathfrak{S}_1^{\perp} = [u_1]^{\perp} \to \mathfrak{S}_2^{\perp} = [u_2]^{\perp}$$

is the required map that induces the g-equivalence between $\mathfrak{S}_1^{\perp}$ and $\mathfrak{S}_2^{\perp}$.
*Case 2.* Let dim$[u_1, u_2] = 2$ and assume that $[u_1, u_2]$ is non isotropic. Then

$$\Re = [u_1, u_2] \oplus [u_1, u_2]^{\perp}.$$

We claim that

$$[u_1, u_2] = [u_1] \oplus \left([u_1, u_2] \cap [u_1]^{\perp}\right).$$

Since $[u_1] \cap [u_1]^{\perp} = \{0\}$ it follows that $[u_1] \cap \left([u_1, u_2] \cap [u_1]^{\perp}\right) = \{0\}$. Obviously, $[u_1] \subseteq [u_1, u_2]$ and

$$[u_1, u_2] \cap [u_1]^{\perp} \subseteq [u_1, u_2].$$

Consequently,

$$[u_1] \oplus \left([u_1, u_2] \cap [u_1]^{\perp}\right) \subseteq [u_1, u_2].$$

Let $x \in [u_1, u_2] \subseteq \Re$ be arbitrary. Since $\Re = [u_1] \oplus [u_1]^{\perp}$, x can be written in a unique way as $x = w + z$, where $w \in [u_1]$ and $z \in [u_1]^{\perp}$. Clearly, $z = x - w \in [u_1, u_2]$. Therefore $z \in [u_1]^{\perp} \cap [u_1, u_2]$ and $x \in [u_1] \oplus \left([u_1, u_2] \cap [u_1]^{\perp}\right)$.
Therefore

$$[u_1, u_2] \subseteq [u_1] \oplus \left([u_1, u_2] \cap [u_1]^{\perp}\right)$$

that is

$$[u_1, u_2] = [u_1] \oplus \left([u_1, u_2] \cap [u_1]^{\perp}\right),$$

as claimed.
Similarly we see that

$$[u_1, u_2] = [u_2] \oplus \left([u_1, u_2] \cap [u_2]^{\perp}\right).$$

Since $\mathfrak{S}_1 = [u_1]$ and $\mathfrak{S}_2 = [u_2]$ are g-equivalent and $\dim[u_1, u_2] = 2$, it follows that their orthogonal complements in $[u_1, u_2]$, that is $[u_1, u_2] \cap [u_1]^{\perp}$ and $[u_1, u_2] \cap [u_2]^{\perp}$ are g-equivalent. Hence, there exist a linear bijective map $U : [u_1, u_2] \cap [u_1]^{\perp} \to [u_1, u_2] \cap [u_2]^{\perp}$ such that

$$g(U(x), U(y)) = g(x, y) \text{ for all } x, y \in [u_1, u_2] \cap [u_1]^{\perp}.$$

Next we claim that

$$[u_1]^{\perp} = \left([u_1, u_2] \cap [u_1]^{\perp}\right) \oplus [u_1, u_2]^{\perp}$$

Obviously,

$$[u_1, u_2] \cap [u_1]^{\perp} \subseteq [u_1]^{\perp}$$

and

$$[u_1, u_2]^{\perp} \subseteq [u_1]^{\perp}$$

Hence,

$$\left([u_1, u_2] \cap [u_1]^{\perp}\right) \oplus [u_1, u_2]^{\perp} \subseteq [u_1]^{\perp}$$

Let $x \in [u_1]^{\perp} \subseteq \Re = [u_1, u_2] \oplus [u_1, u_2]^{\perp}$. Then there are $y \in [u_1, u_2]$ and $t \in [u_1, u_2]^{\perp}$ such that $x = y + t$. Since $x \in [u_1]^{\perp}$, we have

$$0 = g(u_1, x) = g(u_1, y) + g(u_1, t) = g(u_1, y).$$

Therefore

$$y \in [u_1]^{\perp}, \text{ that is } y \in [u_1, u_2] \cap [u_1]^{\perp}.$$

Consequently,

$$x = y + t \in \big([u_1, u_2] \cap [u_1]^{\perp}\big) \oplus [u_1, u_2]^{\perp},$$

that is,

$$[u_1]^{\perp} \subseteq \big([u_1, u_2] \cap [u_1]^{\perp}\big) \oplus [u_1, u_2]^{\perp}$$

which yields the equality

$$[u_1]^{\perp} = \big([u_1, u_2] \cap [u_1]^{\perp}\big) \oplus [u_1, u_2]^{\perp}.$$

Similarly we see that

$$[u_2]^{\perp} = \big([u_1, u_2] \cap [u_2]^{\perp}\big) \oplus [u_1, u_2]^{\perp}.$$

Finally, we construct a map

$$V : [u_1]^{\perp} \to [u_2]^{\perp}$$

with the required properties. Each $x \in [u_1]^{\perp}$ can be uniquely written as $x = y + t$, where $y \in \big([u_1, u_2] \cap [u_1]^{\perp}\big)$ and $t \in [u_1, u_2]^{\perp}$. We define $V(x) := U(y) + t$. Obviously, $V$ is linear and bijective.
Moreover, if $x' \in [u_1]^{\perp}$ and $x' = y' + t'$ is its unique decomposition, then

$$\begin{aligned} g(V(x), V(x')) = g(U(y) + t, U(y') + t') = g(U(y), U(y')) + g(U(y), t')+ \\ g(t, U(y')) + g(t, t') = g(y, y') + g(t, t') = g(y, t') + g(t, y')+ \\ g(y, y) + g(t, t') = g(y + t, y' + t') = g(x, x'). \end{aligned}$$

Consequently, the map $V$ is the g-equivalence between $[u_1]^{\perp}$ and $[u_2]^{\perp}$, which ends the proof of case 2.
*Case 3.* Let $\dim[u_1, u_2] = 2$ and assume that $[u_1, u_2]$ is isotropic.
Since $[u_1, u_2]$ is isotropic, then exists

$$0 \neq w \in [u_1, u_2] \cap [u_1, u_2]^{\perp}.$$

In particular, $g(w, u_1) = 0 = g(w, u_2)$ and $g(w, w) = 0$. Since $g(u_1, u_1) \neq 0$, it follow that $u_1$ and $w$ are linearly independent. Since $g \neq 0$ then exists $t \in \Re$ such that $g(w, t) \neq 0$. Consequntly, $[u_1, u_2, t]$ is a 3-dimensional space and $(w, u_1, t)$ is its basis. We claim that

$$[u_1, u_2, t] = [w, u_1, t]$$

is not isotropic. Suppose that

$$x \in [w, u_1, t] \cap [w, u_1, t]^{\perp}.$$

Then $x = \alpha w + \beta u_1 + \gamma t$ for some $\alpha, \beta, \gamma \in \mathbb{D}$ and

$$0 = g(x, w) = \alpha g(w, w) + \beta g(u_1, w) + \gamma g(t, w) = \gamma g(t, w)$$

$$0 = g(x,u_1) = \alpha g(w,u_1) + \beta g(u_1,u_1) + \gamma g(t,u_1) = \beta g(u_1,u_1) + \gamma g(t,u_1)$$

$$0 = g(x,t) = \alpha g(w,t) + \beta g(u_1,t) + \gamma g(t,t)$$

Since $g(t,w)$,$g(u_1,u_1)$,$g(w,t)$ are all nonzero, we deduce that $\alpha, \beta, \gamma$ are all zero, that is $x = 0$. Hence $[u_1,u_2,t]$ is not isotropic.
Consequently,

$$\Re = [u_1,u_2,t] \oplus [u_1,u_2,t]^{\perp}.$$

We can now prove that

$$[u_1,u_2,t] = [u_1] \oplus \big([u_1,u_2,t] \cap [u_1]^{\perp}\big) \tag{8.7}$$

$$[u_1,u_2,t] = [u_2] \oplus \big([u_1,u_2,t] \cap [u_2]^{\perp}\big) \tag{8.8}$$

$$[u_1]^{\perp} = \big([u_1,u_2,t] \cap [u_1]^{\perp}\big) \oplus [u_1,u_2,t]^{\perp} \tag{8.9}$$

$$[u_2]^{\perp} = \big([u_1,u_2,t] \cap [u_2]^{\perp}\big) \oplus [u_1,u_2,t]^{\perp} \tag{8.10}$$

In an analagous way as the the corresponding statements in Case 2. Moreover, from (8.7) and (8.8) it follows that $dim([u_1,u_2,t] \cap [u_1]^{\perp}) = 2 = dim([u_1,u_2,t] \cap [u_2]^{\perp})$. Hence if we find a g-equivalence

$$U : [u_1,u_2,t] \cap [u_1]^{\perp} \to [u_1,u_2,t] \cap [u_2]^{\perp},$$

then the map $V : [u_1]^{\perp} \to [u_2]^{\perp}$, defined by, $V(x) := U(y) + z$, where $x = y + z$ is the decomposition with respect to (8.9) is the required g-equivalence, similarly as in Case 2.
Recall that $w \in [u_1,u_2,t] \cap [u_1]^{\perp}$ and $w \in [u_1,u_2,t] \cap [u_2]^{\perp}$. Define

$$\alpha_1 := -g(t,w)^{-1} g(t,u_1) g(u_1,u_1)^{-1},$$

$$\beta_1 := g(t,w)^{-1},$$

$$q_1 := \alpha_1 u_1 + \beta_1 t \in [u_1,u_2,t].$$

Then

$$g(q_1,u_1) = \alpha_1 g(u_1,u_1) + \beta_1 g(t,u_1) =$$
$$-g(t,w)^{-1} g(t,u_1) g(u_1,u_1)^{-1} g(u_1,u_1) + g(t,w)^{-1} g(t,u_1) = 0$$

Consequntly,

$$q_1 \in [u_1,u_2,t] \cap [u_1]^{\perp}.$$

Moreover, $g(q_1,w) = \alpha_1 g(u_1,w) = \beta_1 g(t,w) = \beta_1 g(t,w) = 1$ and therefore $g(w,q_1) = 1$. By Axiom there exists $\lambda_1 \in \mathbb{D}$ such that $\lambda + \overline{\lambda} = -g(q_1,q_1)$.

Define $z_1 := q_1 + \lambda_1 w$. Then $z_1 \in [u_1, u_2, t] \cap [u_1]^\perp$. Moreover,

$$\begin{aligned} g(z_1, w) = g(q_1, w) + \lambda_1 g(w, w) = g(q_1, w) = 1, \\ g(w, z_1) = \overline{g(z_1, w)} = 1, \\ g(z_1, z_1) = g(q_1, q_1) + g(q_1, w)\overline{\lambda_1} + \lambda_1 g(w, q_1) + \lambda_1 g(w, w)\overline{\lambda_1} = \\ g(q_1, q_1) + \overline{\lambda_1} + \lambda_1 = 0. \end{aligned}$$

In particular, we see that $w$ and $z_1$ are linearly independent. Hence $(w, z_1)$ is a basis of $[u_1, u_2, t] \cap [u_1]^\perp$ such that the matrix of $g$ in $[u_1, u_2, t] \cap [u_1] \perp$ equals

$$\begin{bmatrix} g(w,w) & g(w,z_1) \\ g(z_1,w) & g(z_1,z_1) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

In the same way we construct vector $z_2$ such that $(w, z_2)$ is a basis of $[u_1, u_2, t] \cap [u_2]^\perp$ with the property that $g$ in $[u_1, u_2, t] \cap [u_2]^\perp$ has matrix

$$\begin{bmatrix} g(w,w) & g(w,z_2) \\ g(z_2,w) & g(z_2,z_2) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Define the map

$$U : [u_1, u_2, t] \cap [u_1]^\perp = [w, z_1] \to [u_1, u_2, t] \cap [u_2]^\perp = [w, z_2]$$

by

$$U(\alpha w + \beta z_1) := \alpha w + \beta z_2.$$

Obviously, it is linear and bijective. Moreover,

$$\begin{aligned} g(U(\alpha w + \beta z_1), U(\alpha' w + \beta' z_1) = g(\alpha w + \beta z_2, \alpha' w + \beta' z_1)) = \\ \alpha g(w,w)\overline{\alpha'} + \alpha g(w, z_2)\overline{\beta'} + \beta g(z_2, w)\overline{\alpha'} + \beta g(z_2, z_2)\overline{\beta'} = \\ \alpha g(w,w)\overline{\alpha'} + \alpha g(w, z_1)\overline{\beta'} + \beta g(z_1, w)\overline{\alpha'} + \beta g(z_1, z_1)\overline{\beta'} \\ = g(\alpha w + \beta z_1, \alpha' w + \beta' z_1). \end{aligned}$$

Hence, U is g-equivalence. This end the proof of Case 3 and the proof of Step 2.
Step 3 In this step we show that, the claim in Witt's theorem is true in general case. We prove Step 3 by applying the induction on dim$\mathfrak{S}_1$. If dim$\mathfrak{S}_1 = 1$, then the claim of Witt's theorem is true by Step 2. Suppose that the claim is true for spaces of dimension $\leq k$. Let dim$\mathfrak{S}_1 = k + 1$. By proposition 5.19 there exist $u_1 \in \mathfrak{S}_1$ such that $g(u_1, u_1) \neq 0$. That is, $[u_1]$ is not isotropic. Hence

$$\Re = [u_1] \oplus [u_1]^\perp. \tag{8.11}$$

Consecuently,

$$\mathfrak{S}_1 = [u_1] \oplus \mathfrak{U}_1, \tag{8.12}$$

where $\mathfrak{U}_1 \subseteq [u_1]^\perp$. Moreover, (8.11), (8.12) and the fact that $\mathfrak{R} = \mathfrak{S}_1 \oplus \mathfrak{S}_1^\perp$ imply that

$$[u_1]^\perp = \mathfrak{U}_1 \oplus \mathfrak{S}_1^\perp.$$

Let $V : \mathfrak{S}_1 \to \mathfrak{S}_2$ be the g-equivalence that exists by the assumption. Define $u_2 := V(u_1)$ and $\mathfrak{U}_2 := V(\mathfrak{U}_1)$. Then $\mathfrak{S}_2 = [u_2] \oplus \mathfrak{U}_2$. Clearly, $\mathfrak{U}_1$ and $\mathfrak{U}_2$ are g-equivalent by V. As above we see that $\mathfrak{R} = [u_2] \oplus [u_2]^\perp$, $\mathfrak{U}_2 \subseteq [u_2]^\perp$ and $[u_2]^\perp = \mathfrak{U}_2 \oplus \mathfrak{S}^\perp$. Since $\dim[u_1] = 1$, it follows from step 2 that there exists a g-equivalence.

$$U : [u_1]^\perp = \mathfrak{U}_1 \oplus \mathfrak{S}_1^\perp \to [u_2]^\perp = \mathfrak{U}_2 \oplus \mathfrak{S}_2^\perp.$$

In particular,

$$[u_2]^\perp = \mathfrak{U}_2 \oplus \mathfrak{S}_2^\perp = U(\mathfrak{U}_1) \oplus U(\mathfrak{S}_1^\perp).$$

Above we saw that $\mathfrak{U}_1$ and $\mathfrak{U}_2$ are g-equivalent. Hence, $\mathfrak{U}_2$ and $U(\mathfrak{U}_1)$ are g-equivalent. Now, since

$$\mathfrak{R} = [u_2] \oplus [u_2]^\perp$$

and

$$[u_2]^\perp = \mathfrak{U}_2 \oplus \mathfrak{S}_2^\perp$$

If follows that the orthogonal complement of $\mathfrak{U}_2$ in the space $[u_2]^\perp$ equals $\mathfrak{S}_2^\perp$. Similarly, the orthogonal complement of $\mathfrak{U}_1$ in the space $[u_1]^\perp$ equals $\mathfrak{S}_1^\perp$. Since $U$ is a g-equivalence, it follows that $U(\mathfrak{U}_1)$ and $U(\mathfrak{S}_1^\perp)$ are orthogonal. That is, the orthogonal complement of $U(\mathfrak{U}_1)$ in the space $[u_2]^\perp$ equals $U(\mathfrak{S}_1^\perp)$. Since $dim(U(\mathfrak{U}_1)) = dim\mathfrak{U}_1 = dim\mathfrak{S}_1 - 1 = k$. It follows from the induction assumption that $U(\mathfrak{S}_1^\perp)$ and $\mathfrak{S}_2^\perp$ are g-equivalent. Hence $\mathfrak{S}_1^\perp$ and $\mathfrak{S}_2^\perp$ are g-equivalent. This ends the proof.

□

**Definition 8.2.** Let $\mathfrak{R}$ be a vector space and $g$ a non-degenerate hermitian scalar product on it. Let $U : \mathfrak{R} \to \mathfrak{R}$ be a bijective linear map such that

$$g(Ux, Uy) = g(x, y)$$

for all $x, y \in \mathfrak{R}$. Then $g$ is a *g-unitary* transformation.

**Proposition 8.3.** *Let $\mathfrak{R}$ be a vector space. Let $\mathfrak{S}_1$ and $\mathfrak{S}_2$ be two non-isotropic subspaces of $\mathfrak{R}$. Any g-equivalence $U : \mathfrak{S}_1 \to \mathfrak{S}_2$ can be extended to a g-unitary transformation defined on $\mathfrak{R}$.*

*Proof.* Suppose that $\mathfrak{S}_1$ and $\mathfrak{S}_2$ are two non-isotropic spaces. Assume that they are g-equivalent. Let $M : \mathfrak{S}_1 \to \mathfrak{S}_2$ be a g-equivalence. By Witt's theorem we know that $\mathfrak{S}_1^\perp$ and $\mathfrak{S}_2^\perp$ are g-equivalent. Let $N : \mathfrak{S}_1^\perp \to \mathfrak{S}_2^\perp$ be a g-equivalence. Since $\mathfrak{S}_1$ is non-isotropic, then $\mathfrak{R} = \mathfrak{S}_1 \oplus \mathfrak{S}_1^\perp$. Hence any vector $x \in \mathfrak{R}$ can be written in the form $x = u + v$, where $u \in \mathfrak{S}_1$ and $v \in \mathfrak{S}_1^\perp$. Similarly, $\mathfrak{R} = \mathfrak{S}_2 \oplus \mathfrak{S}_2^\perp$. Moreover, we know that $Mu \in \mathfrak{S}_2$ and $Nv \in \mathfrak{S}_2^\perp$. Define a bijective linear map

$$U : \mathfrak{R} \to \mathfrak{R}$$

by

$$x \mapsto Mu + Nv.$$

Obviously, $U$ is bijective. Let $y = u' + v' \in \mathfrak{R}$. The linear map $U$ is g-unitary, since

$$g(Ux, Uy) = g(Mu + Nv, Mu' + Nv') = g(u + v, u' + v') = g(x, y).$$

This completes the proof.

□

**Theorem 8.4.** *Let $\mathfrak{R}$ be a vector space. Any g-equivalence of a subspace of $\mathfrak{R}$ can be extended to a g-unitary transformation in $\mathfrak{R}$.*

*Proof.* Let $\mathfrak{S}$ be a subspace of $\mathfrak{R}$. For $x \in \mathfrak{R}$ define a map $K : \mathfrak{S} \to \mathbb{D}$ by

$$y \mapsto g_x(y) = g(y, x).$$

Linear functions of this type fill up the conjugate space $\mathfrak{S}^*$ of $\mathfrak{S}$. Let $(y_1, y_2, \dots, y_m)$ be a basis for a vector subspace $\mathfrak{S}$. Let $v_1$ be a vector such that

$$g(y_1, v_1) = 1, \quad g(y_i, v_1) = 0$$

for $i > 1$. In the sequel we assume that $\mathfrak{S}$ is isotropic, since Proposition 8.3 ends the proof in the non-isotropic case. Let $(y_1, \dots, y_v)$ be a basis for the radical of $\mathfrak{S}$. Then we can choose a vector $v_1$ so that

$$g(y_1, v_1) = 1, \quad g(y_i, v_1) = 0$$

and in addition

$$g(v_1, v_1) = 0.$$

Namely, if $g(v_1, v_1) \neq 0$, then we can find $\lambda$ such that $\lambda + \overline{\lambda} + g(v_1, v_1) = 0$ and we can replace vector $v_1$ by $v_1 + \lambda y_1$. Now the space $[y_1, v_1]$ is a two-dimensional non-isotropic subspace of a vector space $\mathfrak{R}$. Since it is non-isotropic, we know that we can write $\mathfrak{R} = [y_1, v_1] \oplus [y_1, v_1]^\perp$. Then $[y_2, \dots, y_v]$ is the radical of $[y_2, \dots, y_m]$ and

$[y_2, \ldots, y_m] \subseteq [y_1, v_1]^{\perp}$. By induction on $v$ there exist a linearly independent set of vectors $(v_1, \ldots, v_v)$ such that such that

$$g(y_j, v_j) = 1$$

for $j = 1, \ldots, v$,

$$g(y_i, v_j) = 0$$

otherwise, and

$$g(v_j, v_k) = 0$$

for $j, k = 1, \ldots, v$. Let $\mathfrak{B} = [v_1, \ldots, v_v]$. Then $\mathfrak{B}$ is totally isotropic and $\mathfrak{B} \cap \mathfrak{S} = 0$. Let $B$ be the matrix of $g$ restricted to $[y_{v+1}, \ldots, y_m]$. Since $[y_1, \ldots, y_v]$ is the radical of $\mathfrak{S}$, $B$ is non-singular. Then the matrix of $g$ relative to the basis $(y_1, \ldots, y_m, v_1, \ldots, v_v)$ in $\mathfrak{S} + \mathfrak{B}$ is of the form

$$\begin{bmatrix} 0 & 0 & I \\ 0 & B & 0 \\ I & 0 & 0 \end{bmatrix}, \tag{8.13}$$

where $I$ is the identity matrix of appropriate size. Since the matrix $B$ is non-singular matrix, the matrix (8.13) is non-singular. Hence $\mathfrak{S} + \mathfrak{B}$ is not isotropic. Now we need to find a g-equivalence of $\mathfrak{S} + \mathfrak{B}$ that extends a given g-equivalence on $\mathfrak{S}$, since by Proposition 8.3 we know that a g-equivalence between non-isotropic subspaces can be extended to a g-unitary transformation.

Let $U$ be an equivalence of $\mathfrak{S}$. A subspace $[Uy_1, \ldots, Uy_v]$ is the radical of $U(\mathfrak{S})$. Hence we can find a set of vectors $(\overline{v}_1, \ldots, \overline{v}_v)$ such that

$$g(Uy_j, \overline{v}_j) = 1$$

for $j = 1 \ldots, v$,

$$g(Uy_i, \overline{v}_j)$$

otherwise, and

$$g(\overline{v}_i, \overline{v}_j) = 0$$

for $i, j = 1, \ldots, v$. Now define a linear map $U'$ on $\mathfrak{S} + \mathfrak{B}$ such that $U'(v_j) = \overline{v_j}$ for $j = 1, \ldots, v$ and $U'$ coincides with $U$ on $\mathfrak{S}$. Clearly $U'$ is a g-equivalence of $\mathfrak{S} + \mathfrak{B}$. The result follows.

□

**Definition 8.5.** Let $g(x, y)$ be a hermitian scalar product. Then $g$ is *totally regular* if

$$g(x, x) \neq 0$$

for every $x \neq 0 \in \mathfrak{R}$.

*Remark* 8.6. The definition above is equivalent to saying that every non-zero subspace of $\mathfrak{R}$ is not isotropic.

**Definition 8.7.** Let $\mathfrak{R}$ be a vector space and let $\mathfrak{S}$ be its totally isotropic subspace. Then $\mathfrak{S}$ is a maximal totally isotropic subspace of $\mathfrak{R}$ if whenever $\mathfrak{S}'$ is a totally isotropic subspace in $\mathfrak{R}$ and $\mathfrak{S} \subseteq \mathfrak{S}'$, we can conclude that $\mathfrak{S} = \mathfrak{S}'$.

**Proposition 8.8.** *Any two maximal totally isotropic subspaces have the same dimension.*

*Proof.* Let $\mathfrak{S}_1$ and $\mathfrak{S}_2$ be two maximal totally isotropic subspaces. Assume w.l.o.g. that $dim\mathfrak{S}_1 \geq dim\mathfrak{S}_2$. Then there exists a totally isotropic subspace $\mathfrak{U}_1 \subset \mathfrak{S}_1$, such that $dim\mathfrak{U}_1 = dim\mathfrak{S}_2$. Since $\mathfrak{U}_1$ and $\mathfrak{S}_2$ are totally isotropic any bijective linear map $U : \mathfrak{U}_1 \to \mathfrak{S}_2$ is a g-equivalence, by Theorem 8.4 it can be extended to a g-unitary map $U'$. Then $U'(\mathfrak{S}_1)$ is totally isotropic and contains $U'(\mathfrak{U}_1) = \mathfrak{S}_2$. Since $\mathfrak{S}_2$ is a maximal totally isotropic subspace, then $\mathfrak{U}_1 = \mathfrak{S}_1$ and hence $dim\mathfrak{S}_1 = dim\mathfrak{S}_2$. □

**Theorem 8.9.** *Any non-singular hermitian matrix is cogredient to the matrix of the form*

$$\begin{bmatrix} 0 & I & 0 \\ I & 0 & 0 \\ 0 & 0 & B \end{bmatrix} \tag{8.14}$$

*where $I$ is the identity matrix and $B$ is totally regular. Two matrices of the form above are cogredient if and only if the submatrices $B$ are cogredient.*

*Proof.* Let $\mathfrak{S}$ be a maximal totally isotropic subspace of a vector space $\mathfrak{R}$. Let $(y_1, \ldots, y_v)$ be linearly independent vectors such that $\mathfrak{S} = [y_1, \ldots, y_v]$. In the proof of the Theorem 8.4 we have seen that we can find a totally isotropic space $\mathfrak{V} = [v_1, \ldots, v_v]$ such that the matrix of $g$ relative to the basis $(y_1, \ldots, y_v, v_1, \ldots, v_v)$ is of the form

$$\begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix}, \tag{8.15}$$

where $I$ is an identity matrix of an appropriate size. Denote $\mathfrak{D} := \mathfrak{S} \oplus \mathfrak{V}$. Since $\mathfrak{S}$ is a maximal totally isotropic subspace and $\mathfrak{S} + \mathfrak{V}$ is not isotropic, then $\mathfrak{R} = \mathfrak{D} \oplus \mathfrak{D}^{\perp}$ and $g$ is totally regular in $\mathfrak{D}^{\perp}$. We can choose a basis for $\mathfrak{R}$ so that the matrix of $g$ has the form

$$\begin{bmatrix} 0 & I & 0 \\ I & 0 & 0 \\ 0 & 0 & B \end{bmatrix}, \tag{8.16}$$

where $I$ is an identity matrix of appropriate size and the matrix $B$ is a matrix of $g$ in $\mathfrak{D}^{\perp}$. Hence, any non-singular hermitian matrix is cogredient to the matrix of the form above in which $B$ is totally regular.

Now we want to show that two matrices of the form

$$\begin{bmatrix} 0 & I_a & 0 \\ I_a & 0 & 0 \\ 0 & 0 & B_a \end{bmatrix}, \begin{bmatrix} 0 & I_b & 0 \\ I_b & 0 & 0 \\ 0 & 0 & B_b \end{bmatrix} \tag{8.17}$$

where $B_a$ and $B_b$ are totally regular, are cogredient if and only if $a = b$ and submatrices $B_b$ and $B_a$ are cogredient. Firstly, observe that if we have a basis $(y_1, \ldots, y_v, v_1, \ldots, v_v)$ and the matrix of g relative to the basis is of the form (8.17), then $\mathfrak{S} = [y_1, \ldots, y_v]$ is maximal totally isotropic subspace. Namely, if it is not maximal, then there exists a totally isotropic subspace $\mathfrak{S}'$ of a vector space $\mathfrak{R}$ such that $\mathfrak{S} \subsetneqq \mathfrak{S}'$. Then a subspace $\mathfrak{S}'$ contains a vector $v + z \neq 0$, where $v \in [v_1, \ldots, v_v]$ and $z \in [z_1, \ldots, z_{n-2v}]$ where $(y_1, \ldots, y_v, v_1, \ldots, v_v, z_1, \ldots, z_{n-2v})$ is a basis of $\mathfrak{R}$. Then

$$g(v + z, v + z) = g(z, z) = 0.$$

Hence $z = 0$, since by the assumsption $g$ is totally regular. On the other hand $v = 0$, since $v = \sum \phi_i v_i$ for some $\phi_i \in \mathbb{D}$ and $g(v, y_i) = \sum \phi_i g(v_i, y_j) = 0$. Hence $v + z = 0 + 0 = 0$, which is a contradiction. Hence, by Proposition 8.8, the condition $a = b$ is a necessary condition for matrices in (8.17) to be cogredient.

Clearly, if matrices $B_a$ and $B_b$ are cogredient, then both matrices in (8.17) are also cogredient. Hence we only need to show the other direction. Let $\mathfrak{S}_1$ and $\mathfrak{S}_2$ be two maximal totally isotropic subspaces. Let $\mathfrak{S}_1 = [y_1^{(1)}, \ldots, y_v^{(1)}]$ and $\mathfrak{S}_2 = [y_1^{(2)}, \ldots, y_v^{(2)}]$. Now determine $\mathfrak{B}_1 = [v_1^{(1)}, \ldots, v_v^{(1)}]$ and $\mathfrak{B}_2 = [v_1^{(2)}, \ldots, v_v^{(2)}]$ such that the matrix of $g$ relative to $\mathfrak{D}_1 = \mathfrak{S}_1 + \mathfrak{B}_1$ and $\mathfrak{D}_2 = \mathfrak{S}_2 + \mathfrak{B}_2$ are of the form

$$\begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix}, \tag{8.18}$$

and $\mathfrak{D}_1$ and $\mathfrak{D}_2$ are non-isotropic as above. Then $\mathfrak{D}_1$ and $\mathfrak{D}_2$ are g-equivalent. Then also $\mathfrak{D}_1^{\perp}$ and $\mathfrak{D}_2^{\perp}$ are g-equivalent by the Witt's theorem. It follows that the cogredience of matrices in (8.17) imply the cogredience of matrices $B_a$ and $B_b$.

□

**Definition 8.10.** Let $\mathfrak{R}$ be a vector space of dimension $n$. Let $v$ be the maximum dimensionality of a totally isotropic subspaces relative to a scalar product $g(x, y)$. Then the *Witt's signature* is $n - 2v$.

# 9 Non-alternate skew-symmetric forms

In this chapter we assume that $g(x, y)$ is a skew symmetric scalar product that is not alternate. Recall that this means that $\mathfrak{D} = \mathfrak{S}$ is a field of characteristic two and $\overline{\alpha} = \alpha$ is the identity map. In particular, g is symmetric.

**Theorem 9.1.** *Let $\mathfrak{R}$ be a vector space over a field $\mathbb{F}$ of characteristic two and let $g(x, y)$ be a non-alternate symmetric scalar product in $\mathfrak{R}$. Then there exist a basis $(u_1, \ldots, u_r, z_1, \ldots, z_{n-r})$ such that the matrix of $g(x, y)$ relative to this basis equals*

$$\begin{bmatrix} \beta_1 & \ldots & 0 & \ldots & 0 \\ \vdots & \ddots & \vdots & \ddots & \\ 0 & \ldots & \beta_r & \ldots & 0 \\ \vdots & \ddots & \vdots & \ddots & \\ 0 & \ldots & 0 & \ldots & 0 \end{bmatrix} \tag{9.1}$$

*where $\beta_i \neq 0$.*

*Proof.* By Lemma 5.19, there exists a vector $u_1$ such that $g(u_1, u_1) = \beta_1 \neq 0$. Now suppose that we have already found $k$ vectors $u_1, \ldots, u_k$ such that $g(u_i, u_j) = \delta_{ij}\beta_i$, where $\beta_i \neq 0$. As in the proof of Theorem 5.21 we can write $\mathfrak{R} = \mathfrak{S}_k \oplus F_k(\mathfrak{R})$, where $\mathfrak{S}_k = [u_1, \ldots, u_k]$ and $F_k(\mathfrak{R}) \subseteq \mathfrak{S}_k^{\perp}$.
Now we separate these cases. If $g = 0$ for all $u \in F_k(\mathfrak{R})$, then $k = r$ and we choose any basis $(z_1, \ldots, z_{n-r})$ of the space $F_k(\mathfrak{R})$. If $g$ is not alternate in $F_k(\mathfrak{R})$, then we can choose a vector $u_{k+1} \in F_k(\mathfrak{R})$ such that $g(u_{k+1}, u_{k+1}) = \beta_{k+1} \neq 0$ and then repeat the process with $k + 1$ vectors.
Now consider the case when $g$ is not identically zero and is alternate in $F_k(\mathfrak{R})$. In this case we can find two linearly independent vectors $w, v$ in $F_k(\mathfrak{R})$ such that

$$g(v, v) = 0 = g(w, w)$$

and

$$g(v, w) = 1 = g(w, v).$$

Let $u = u_k$, $\beta = \beta_k$ and consider a scalar product $g$ in the three-dimensional space $[u, v, w]$. Matrix of $g$ relative to the basis $(u, v, w)$ is of the following form

$$\begin{bmatrix} \beta & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}. \tag{9.2}$$

Let $y = \xi u + \eta v + \gamma w$ and $y' = \xi' u + \eta' v + \gamma' w$ for some $\xi, \xi' \eta, \eta', \gamma, \gamma' \in \mathbb{F}$. Then

$$g(y, y') = \beta\xi\xi' + \eta\gamma' + \eta'\gamma$$

Hence

$$\begin{aligned} y_1 &= u + v \\ y_2 &= u + \beta w \\ y_3 &= u + v + \beta w \end{aligned}$$

are pairwise orthogonal and $g(y_i, y_i) = \beta$. Hence if we replace vector $u_k$ by $y_1$, change the notation and call this vector $u_k$ again, then $u_1, \ldots, u_k, u_{k+1} = y_2, u_{k+2} = y_3$ satisfy $g(u_i, u_j) = \delta_{ij}\beta_i$, where $\beta_i \neq 0$. This completes the proof. □

The argument used in the proof above shows that the matrices

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \tag{9.3}$$

and

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{9.4}$$

are cogredient. On the other hand submatrices

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{9.5}$$

and

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{9.6}$$

are not cogredient, which shows why Witt's theorem does not hold in a field of characterictic two.

# 10 Conclusion

To conclude, Witt's theorem and its corollary, i.e. Theorem 8.4, are important results that can be useful in various matrix analysis as well as to prove vertex-transitivity, arc-transitivity, and related properties of several graphs, which are induced by certain vector space structures (see [4–6]). We have presented the preliminary theory, stated Witt's theorem, presented a proof and illustrated why this theorem is no longer true in a field of characteristic two. However, there exist a version of Witt's theorem, with some additional assumptions, also for fields of characteristic two [8]. Witt's theorem, or more precisely Theorem 8.4, can be stated in a purely matrix theoretical way as well.

Preliminary theory contains firstly the theory about certain types of maps, called bilinear. Of particular interest are non-degenerate bilinear forms, since they determine a bijective linear map $R : \mathfrak{R}' \to \mathfrak{R}^*$, between the right vector space $\mathfrak{R}'$ of the bilinear form and the space $\mathfrak{R}^*$ of all linear functionals on the left vector space $\mathfrak{R}$ of the bilinear form. We have also seen that if a division ring $\mathbb{D}$ possesses an anti-automorphism, then any left vector space over division ring $\mathbb{D}$ can be also regarded as a right vector space over $\mathbb{D}$. Hence in this case there is a possibility of connecting the space with itself. Such forms are called scalar products. Then we moved on to the study of an equivalence relation on the set of of matrices, called cogredience relation, which is closely related to the study of scalar products. The most important types of scalar products are the hermitian, symmetric, and alternate scalar products. Moreover complete solutions of the cogredience of hermitian matrices were presented in the final project paper.

# 11 Povzetek naloge v slovenskem jeziku

Poglavitni cilj naloge je preučiti in povzeti peto poglavje v knjigi [1]. Ker je knjiga precej stara, slog pisanja v njej ne ustreza povsem modernim standardom. Posledično bralec, ki ga zanima določen izrek v njej, potrebuje precej časa, da ugotovi, kaj natančno so predpostavke izreka. Razumevanje dokazov je še bolj zamudno, saj so ti pogosto zapisani pred samim izrekom, brez znaka, ki bi označeval konec dokaza. Zaključna naloga tako izboljša ta vidik knjige.
V nalogi so preučevane bilinearne forme, ki so definirane nad parom, sestavljenim iz končno-razsežnega levega vektorskega prostora in iz končno-razsežnega desnega vektorskega prostora. Pri tem sta oba vektorska prostora nad obsegom, ki ni nujno komutativen, in predstavlja tudi sliko bilinearne forme. Za dano bilinearno formo in za par baz obeh prostorov smo definirali matriko, ki pripada tej formi. Ogledali smo si, kako se matrika spreminja, če spreminjamo bazi. Spoznali smo pojem levega in desnega radikala bilinearne forme. Med bilinearnimi formami so še posebej pomembne tiste, ki so nedegenerirane. V nalogi smo spoznali potrebne in zadostne pogoje za nedegeneriranost. Za tovrstne bilinearne forme smo spoznali dual vektorskega prostora glede na dano nedegenerirano formo ter pojem komplementarnih baz v prostoru in v njegovem dualu. Za linearno preslikavo med dvema vektorskima prostoroma, ki sta opremljena vsak s svojo nedegenerirano bilinearno formo, smo definirali njeno transponiranko glede na omenjeni formi ter spoznali njene lastnosti. Preučili smo, kako linearno preslikavo zapišemo kot vsoto preslikav ranga ena, ter kako se tovrstni zapis pozna na njeni transponiranki. Za obsege, ki so opremljeni z antiavtomorfizmom, smo definirali t.i. skalaren produkt, pri čemer je potrebno povdariti, da gre v splošnem za posebne vrste bilinearnih preslikav, ki lahko zavzamejo vrednost nič na paru $(x, x)$, kjer je $x$ neničelen vektor. Za vektorski prostor, ki je opremljen s skalarnim produktom $g$ in za par njegovih podprostorov smo definirali pojem $g$-ekvivalence. To je linearna bijekcija med prostoroma, ki ohranja skalarni produkt. Če je antiavtomorfizem obsega involucija, potem pravimo, da je skalaren produkt hermitski. V primeru komutativnega obsega in involucije, ki je identična preslikava, pravimo, da gre za simetričen skalaren produkt. Za hermitske skalarne produkte smo spoznali obliko matrike, ki pripada tovrstni

bilinearni formi. Nato smo spoznali še posebne primere, če gre za algebraično zaprt obseg, ki ni karakteristike dva, ter simetričen produkt nad realnim obsegom in hermitski produkt nad kompleksnim obsegom, kjer je involucija kompleksno konjugiranje. Prav tako smo v nalogi preučili alternirajoče skalarne produkte, tj. produkte, ki uničijo vsak par oblike $(x, x)$. V primeru neničelnega tovrstnega produkta je obseg avtomatsko komutativen, involucija pa je identična preslikava. Spoznali smo obliko matrike alternirajočega skalarnega produkta, ki je vedno sodega ranga. Za podprostor vektorskega prostora, ki je opremljen z nedegeneriranim hermitskim skalarnim produktom $g$, smo spoznali pojem ortogonalnega komplementa. Prav tako smo spoznali, kaj pomeni, če je podprostor izotropičen, totalno izotropičen ali neizotropičen. Poglavitni cilj naloge je preučiti in zapisati dokaz Wittovega izreka. Slednji v eni izmed oblik pove, da $g$-ekvivalenca med dvema neizotropičnega podprostoroma implicira obstoj $g$-ekvivalence med njunima ortogonalnima komplementoma. Pri tem je privzeta predpostavka, da ima enačba $x + \overline{x} = \beta$ rešitev $x$ v obsegu, za vsak hermitski element $\beta$. To izloči primer komutativnega obsega karakteristike dva, kjer je involucija identična preslikava. Zelo pomembna posledica Wittovega izreka, ki se tudi sama pogosto imenuje Wittov izrek, pravi, da lahko vsako $g$-ekvivalenco med dvema podprostoroma, ki nista nujno neizotropična, lahko razširimo do $g$-unitarne preslikave na celotnem prostoru. V nalogi je prikazan tudi dokaz tega rezultata. Prav tako je razloženo, da Wittov izrek v splošnem ne drži, če je karakteristika obsega enaka dva.

# 12 Bibliography

[1] E. Artin, *Geometric algebra*, Interscience Publishers, Inc., New York-London, 1957. *(Cited on page 1.)*

[2] L. Hogben (Ed.), *Handbook of linear algebra. 2nd ed.*, Boca Raton (FL): CRC Press; 2014. *(Cited on page 1.)*

[3] N. Jacobson, *Lectures in abstract algebra. Volume II: Linear algebra*, Van Nostrand Reinhold, 1953. *(Cited on pages II, III, 1, and 7.)*

[4] M. Orel, Adjacency preservers on invertible hermitian matrices I. *Linear Algebra Appl.* 499 (2016) 99–128. *(Cited on pages 1 and 51.)*

[5] M. Orel, On generalizations of the Petersen and the Coxeter graph. *Electron. J. Combin.* 22 (2015) P.4.27. *(Cited on pages 1 and 51.)*

[6] M. Orel, On Minkowski space and finite geomtery. *J. Combin. Theory Ser. A* 148 (2017) 145–182. *(Cited on pages 1 and 51.)*

[7] G. Pall, Hermitian quadratic forms in a quasi-field. *Bulletin Amer. Math. Soc.* 51 (1945) 889–893. *(Cited on page 1.)*

[8] V. Pless, On Witt's theorem for nonalternating symmetric bilinear forms over a field of characteristic 2. *Proc. Amer. Math. Soc.* 15 (1945) 979–983. *(Cited on page 51.)*

[9] E. Witt, Theorie der quadratischen Formen in beliebigen Körper. *Journal für Mathematik* 176 (1937) 31–44. *(Cited on page 1.)*