The Dissertation Committee for Silvia María Adduci
certifies that this is the approved version of the following dissertation:

On real and p-adic Bezoutians

Committee:

Fernando Rodriguez Villegas, Supervisor

David Helm

Jeff Vaaler

Felipe Voloch

Bernd Sturmfels

On real and p-adic Bezoutians

by

Silvia María Adduci, Lic.

DISSERTATION

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

DOCTOR OF PHILOSOPHY

THE UNIVERSITY OF TEXAS AT AUSTIN

May 2010

Dedicated to my friends.

Acknowledgments

Over the years I have been very fortunate to find the friendship and guidance from many people. To begin with, I would like to thank my advisor Fernando Rodriguez Villegas and his wife Adriana Sofer, for the orientation they gave me during the past years in Austin and for helping me when I decided to apply here in the first place.

Jeff Vaaler, Felipe Voloch, David Helm, Bernd Sturmfels, John Tate: thanks for agreeing to be in my committee and for your useful comments and support over the years.

The students, professors, and staff of the Department of Mathematics of The University of Texas at Austin create a warm and friendly atmosphere. It is a pleasure and an honor to work with you guys. Nancy Lamm, second mom: you are awesome! To the people in the Actuarial Program, specially Jim Daniel and Leslie Vaaler: thank you so much for your support and advice.

For their comments and availability via email I wish to thank my undergraduate advisor Alicia Dickenstein and my friends Carlos D'Andrea and Matilde Lalin. The later gave me invaluable help when applying to graduate school and in my first months here in Texas.

My parents and my siblings Alejandro and Patricia have offered support and laugh in the distance. This dissertations is what I was doing while I was

missing you so much during all these years.

My life in Austin would not have been so full and rich without my friends. Martin Mereb, whose constant companionship has become an invaluable gift of everyday life; Eva Dardati, with whom we share afternoons of work and matté; Cody and Nicolas, who were there for me when I most needed them. Renato, Mar, Nacho, Miguel, Fred, Tim, Mariela, and specially my spiritual friend Hernán ... it is impossible to write all your names on paper, but they are written in my heart. You guys have been my family here, you have made it possible for me to call Austin my third home (after Buenos Aires and Mar del Plata). You have brought comfort and fullness to my life. I have no words to thank you for so much kindness and friendship. I am happy to have you all in my life, you guys are fantastic!

On real and p-adic Bezoutians

Publication No. _____

Silvia María Adduci, Ph.D.
The University of Texas at Austin, 2010

Supervisor: Fernando Rodriguez Villegas

We study the quadratic form induced by the Bezoutian of two polynomials $\mathfrak{p}$ and $\mathfrak{q}$, considering four problems. First, over $\mathbb{R}$, in the separable case we count the number of configurations of real roots of $\mathfrak{p}$ and $\mathfrak{q}$ for which the Bezoutian has a fixed signature. Second, over $\mathbb{Q}_p$ we develop a formula for the Hasse invariant of the Bezoutian. Third, we formulate a conjecture for the behavior of the Bezoutian in the non separable case, and offer a proof over $\mathbb{R}$. We wrote a `Pari` code to test it over $\mathbb{Q}_p$ and $\mathbb{Q}$ and found no counterexamples. Fourth, we state and prove a theorem that we hope will help prove the conjecture in the near future.

Table of Contents

List of Notation

Chapter 1

Introduction

In this dissertation we study the quadratic form induced by the Bezoutian of two polynomials $\mathfrak{p}$ and $\mathfrak{q}$ in some field K with characteristic other than two.

The first chapter is introductory, to fix notation and to avoid some common misunderstandings.

In the second chapter we consider Bezoutians over $\mathbb{R}$. A classical result says that the Bezoutian is definite if and only if the roots of $\mathfrak{p}$ and $\mathfrak{q}$ interlace over the real line, i.e., if we identify $\mathbb{P}^1(\mathbb{R})$ with a circle, between any two roots of $\mathfrak{p}$ there is a unique root of $\mathfrak{q}$ and vice versa. That is to say that, for a given maximal or minimal signature, there is a unique configuration of the roots of $\mathfrak{p}$ and $\mathfrak{q}$, namely interlacing, the first root being of $\mathfrak{p}$ or $\mathfrak{q}$ depending on the signature being maximal or minimal. Here we obtain and prove a formula for the number of configurations of roots of $\mathfrak{p}$ and $\mathfrak{q}$ with any given signature.

The third chapter is dedicated to the study of Bezoutians over the p-adic fields $\mathbb{Q}_p$. We obtain and prove a formula for the Hasse invariant depending only on $\mathfrak{p}$ and $\mathfrak{q}$.

In the fourth and last chapter we address the issue that all the previous, as well as most of the existing literature, do not cover the case when the polynomials are not separable. We conjecture what should happen, prove it for the real case and offer a computational approach over $\mathbb{Q}$ and $\mathbb{Q}_p$, that is, a code in `Pari` that checks the conjecture and has found no counterexamples whatsoever. Finally we offer a theorem that not only is appealing on its own but also, we hope, might help prove the general case of the conjecture in the future.

1.1 Quadratic Forms and Quadratic Spaces

Let

- K be a field with $\mathrm{ch}(K) \neq 2$
- V be a vector space over K of finite dimension n.
- b be a *symmetric* bilinear form over V

$$b: \quad \begin{array}{ccc} V \times V & \stackrel{b}{\longrightarrow} & K \\ (x,y) & \mapsto & b(x,y) \end{array}$$

Definition: the map $\mathcal{Q} : V \to K,\ \mathcal{Q}(x) := b(x,x)$ is a **quadratic form** and the pair (V,b) $\big($or $(V,\mathcal{Q})\big)$ is a **quadratic space**.

1.1.1 Matrix notation & Bases

We can write b in matrix notation as follows. Let $x \in V$ as a column vector $x = (x_1, ..., x_n)^t$ where $x_i \in K$ for all i. Therefore $b(x, y) = x^t by$:

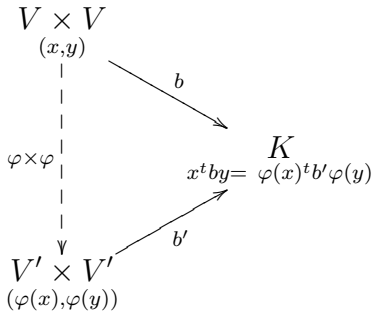
$$b(x,y) = (x_1, ..., x_n) \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & & b_{2n} \\ \vdots & & \ddots & \vdots \\ b_{n1} & b_{n2} & & b_{nn} \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}$$

Abusing notation we call b both the matrix and the bilinear form. The matrix $b := (b_{ij})$ is symmetric, and it is the matrix of the symmetric bilinear form b in the **standard basis** $\mathcal{S}_{td} := \{e_1, ..., e_n\}$ where

$$\begin{cases} e_1 := \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \\ \qquad \vdots \\ e_n := \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \end{cases}$$

1.1.2 Isometry

Two quadratic spaces (V, b) and (V', b') over the same field K are said to be **isometric** (denoted $V \simeq V'$) if there exists a linear isomorphism $\varphi : V \to V'$ such that $b' \circ (\varphi \times \varphi) = b$. That is, if there exist φ such that the following diagram is commutative:



(1.1)

In matrix notation, isometry of quadratic forms corresponds bijectively to congruence of symmetric matrices: two $n \times n$ matrices B, B' are **congruent** (also denoted $B \simeq B'$) if there exists an invertible matrix M such that $B' = M^t B M$. Note that $\det(B') = \det(B) \det(M)^2$. This shows that the determinant of a quadratic form is unique up to squares. This number, the class of the determinant modulo squares, is an element of K^*/K^{*2} and its called the **discriminant** of V, denoted $\Delta(V)$ or just Δ.

1.1.3 Orthogonality

Some definitions

1. Two elements $x, y \in V$ are called **orthogonal** if $b(x, y) = 0$.

2. For a subspace $W \subset V$, the **orthogonal complement** of W is $W^{\perp} = \{x \in V |\ b(x, y) = 0\ \forall\ y \in W\}$

3. The **rank** of V is $\text{rank}(V) = \text{codim}(V^{\perp})$.

4. V is called **regular** or **non-degenerate** or **nonsingular** if $\text{rank}(V) = \dim_K(V)$, that is, if $V^{\perp} = 0$.

5. Given two quadratic spaces (V_1, b_1) and (V_2, b_2) their (external) **orthogonal sum**, denoted by $(V_1, b_1) \perp (V_2, b_2)$, (or just $V_1 \perp V_2$) is a new quadratic space (V, b) with

$$\begin{cases} (i)\ V \ = \ V_1 \oplus V_2 \\ (ii)\ b((x_1, x_2), (y_1, y_2)) \ = \ b_1(x_1, y_1) \ + \ b_2(x_2, y_2) \end{cases}$$

6. A quadratic form is said to be **diagonalized** when it is expressed as the orthogonal sum of spaces of dimension one, i.e., when it has the form $\lambda_1 x_1^2 + \cdots + \lambda_n x_n^2$ for constants $\lambda_1,\ \cdots,\ \lambda_n$.

7. The **Witt-Grothendieck ring** of K, denoted by $\widehat{W}(K)$ is the ring of isometry classes of regular quadratic forms over K. The addition is given by the orthogonal sum and the product is given by the tensor product $\otimes$, defined next.

8. Given two quadratic spaces $(V_1, \mathcal{Q}_1)$ and $(V_2, \mathcal{Q}_2)$ their **tensor product**, denoted by $(V_1, \mathcal{Q}_1) \otimes (V_2, \mathcal{Q}_2)$, is a new quadratic space $(V, \mathcal{Q})$ with

$$\begin{cases} (i) & V & = & V_1 \otimes V_2 \\ (ii) & \mathcal{Q}(x) & = & \mathcal{Q}_1(x_1) \cdot \mathcal{Q}_2(x_2) \end{cases}$$

The following theorem is fundamental. For a proof see the work of Lam or Scharlau: [16], [22].

Theorem 1.1.1. *(Witt's Cancellation Theorem)*

Let V and V' be isometric quadratic spaces with orthogonal decompositions

$$\begin{cases} V & = & U \perp W \\ V' & = & U' \perp W' \end{cases}$$

with U, U' both regular. Then $U \simeq U' \Rightarrow W \simeq W'$.

1.1.4 Hyperbolic spaces

Some definitions

1. An element $0 \neq x \in V$ is called **isotropic** if $\mathcal{Q}(x) = 0$.

2. The space $(V, \mathcal{Q})$ is called $\begin{cases} \textbf{isotropic} \text{ if it contains an isotropic element.} \\ \textbf{anisotropic} \text{ otherwise.} \\ \textbf{totally isotropic} \text{ if } \mathcal{Q} = 0. \end{cases}$

3. A $2-$dimensional space (V, b) is called a **hyperbolic plane** (denoted $\mathbb{H}$) if it contains two isotropic elements x, y such that $b(x, y) \neq 0$.

4. A $2m-$dimensional space (V, b) is called a **hyperbolic space** if it is the orthogonal sum of m hyperbolic planes. Denoted $\mathbb{H}(K^m)$.

5. The **Witt decomposition** of a space V is

$$V = V_T \perp \mathbb{H}_1 \perp ... \perp \mathbb{H}_m \perp V_A$$

where $\begin{cases} V_T \text{ is a totally isotropic space} \\ \mathbb{H}_i \text{ are hyperbolic planes} \\ V_A \text{ is anisotropic} \end{cases}$

6. The **anisotropic part** of V is the subspace V_A in the Witt decomposition of V, and it is unique up to isometry.

7. Two quadratic spaces (V_1, b_1) and (V_2, b_2) are called **Witt equivalent**, denoted $V_1 \underset{W}{\equiv} V_2$ if their anisotropic parts are isometric.

8. The **Witt ring** of K, denoted $W(K)$, is the factor ring $\widehat{W}(K)/\mathbb{Z}.\mathbb{H}$. It can be thought of as the ring of Witt equivalence classes of regular anisotropic quadratic forms.

1.1.5 The Spectral Theorem

When we talk about diagonalization of a bilinear form B we are thinking of an invertible matrix C such that C^tBC is diagonal. When we talk about diagonalization of a *linear* transformation, the diagonal matrix is $C^{-1}BC$.

There is a special case though, that one of $K = \mathbb{R}$, where the Spectral Theorem says that *symmetric* linear transformations over $\mathbb{R}$ are always diagonalizable with real eigenvalues and an orthogonal change of basis. That is, the matrix C satisfies that $C^{-1} = C^t$, therefore this change of basis is also bilinearly admissible.

Theorem 1.1.2. Spectral theorem (real symmetric case)
Let $K = \mathbb{R}$, $n \geq 1$ and let $\varphi : V \to V$ be a symmetric linear map. Then there exists an orthogonal basis of V consisting of eigenvectors of φ.

For a proof of this theorem see [17].

It is worth mentioning here the complex case as well. In the case of $K = \mathbb{C}$ we are interested in *hermitian* forms rather than bilinear forms. A **hermitian form** over a complex linear space V is a function

$$g : \begin{array}{ccc} V \times V & \xrightarrow{b} & \mathbb{C} \\ (x, y) & \mapsto & g(x, y) = \overline{x}^t[g]y \end{array}$$

such that:

$$\begin{cases} 1. g(ax_1 + bx_2, y) = ag(x_1, y) + bg(x_2, y). \\ 2. g(x, y) = \overline{g(y, x)} \end{cases}$$

where $a, b \in \mathbb{C}$ and the overline indicates complex conjugation. Note that $g(x, x) \in \mathbb{R}$ for all $x \in V$. So it makes sense to define the following: a hermitian form g is said to be **positive definite (negative)** if $g(x, x) > 0$ $(g(x, x) < 0)$ for all $x \neq 0$. Recall that in this context, a *linear* form $\varphi : V \to V$ is said to be **hermitian** if $g(\varphi(x), x)) \in \mathbb{R}$ for all $x \in V$. We can now state the complex case of the Theorem.

Theorem 1.1.3. Spectral theorem: complex hermitian case
Let $K = \mathbb{C}$ and let $V \neq 0$ be a complex vector space with a positive definite hermitian form f. Let $\varphi : V \to V$ be a hermitian linear map. Then there exists an orthogonal basis of V consisting of eigenvectors of φ.

For a proof of this theorem see [17].

Next we focus on some particular examples of quadratic forms.

1.2 Bezoutians

Let $\mathfrak{p},\ \mathfrak{q}$, in $K[x]$ and let $n := deg\ \mathfrak{p} \geq deg\ \mathfrak{q}$. It is not necessary but it is convenient to ask $\mathfrak{p}$ and $\mathfrak{q}$ to be monic, and we do so.

1.2.1 Bezoutians

The **Bezoutian** of $\mathfrak{p}$ and $\mathfrak{q}$ is:

$$\begin{aligned} \mathcal{B}[\mathfrak{p},\mathfrak{q}](x,y) &= \frac{\mathfrak{p}(x)\mathfrak{q}(y)-\mathfrak{p}(y)\mathfrak{q}(x)}{x-y} \\ &= \sum_{i,j=1}^{n} b_{ij}x^{i-1}y^{j-1} \end{aligned} \tag{1.2}$$

It induces a symmetric bilinear form on V, called the **Bezoutian form**:

$$\begin{array}{ccc} V\times V & \xrightarrow{\mathcal{B}} & K \\ (\alpha,\beta) & \mapsto & \langle\alpha,\beta\rangle \end{array}$$

given by

$$\langle\alpha,\beta\rangle := (\alpha_0,...,\alpha_{n-1}) \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \vdots & & \vdots \\ b_{n1} & \dots & b_{nn} \end{pmatrix} \begin{pmatrix} \beta_0 \\ \vdots \\ \beta_{n-1} \end{pmatrix}$$

where we are thinking $\begin{cases} \alpha = \alpha_0+\alpha_1x+...+\alpha_{n-1}x^{n-1} \\ \beta = \beta_0+\beta_1x+...+\beta_{n-1}x^{n-1} \end{cases}$

Some properties of the Bezoutian

1. Symmetric on x and y : $\mathcal{B}[\mathfrak{p},\mathfrak{q}](x,y) = \mathcal{B}[\mathfrak{p},\mathfrak{q}](y,x)$.
2. Anti-symmetric on $\mathfrak{p}$ and $\mathfrak{q}$: $\mathcal{B}[\mathfrak{p},\mathfrak{q}](x,y) = -\mathcal{B}[\mathfrak{q},\mathfrak{p}](x,y)$.
3. Linear in $\mathfrak{p}$ and linear in $\mathfrak{q}$.
4. $\dim(\mathcal{B}) = \max\{ \deg \mathfrak{p}, \deg \mathfrak{q} \} =: n$
5. $\dim(\ker(\mathcal{B})) = \deg(\gcd(\mathfrak{p} : \mathfrak{q}))$ (see [7]).
6. $\det(\mathcal{B}) = (-1)^{n(n+1)/2} \operatorname{Res}(\mathfrak{p},\mathfrak{q})$ where Res denotes the resultant. For a proof of this see [7].

1.2.1.1 Generating function: diagonalization

The function defined by (1.2) is called the **generating function** of the Bezoutian. Every Bezoutian has associated a rational function $w := \mathfrak{q}/\mathfrak{p}$. In the particular case when $\mathfrak{p}$ is separable and its roots belong to the base field K, say $\mathfrak{p}(x) = \prod_{j=1}^{n}(x - \xi_j)$ with $\xi_i \neq \xi_j$ for $i \neq j$, w has a very simple partial fractions decomposition:

$$w(x) = \sum_{j=1}^{n} \frac{\mathfrak{q}(\xi_j)/\mathfrak{p}'(\xi_j)}{x - \xi_j}$$

The generating function of the Bezoutian can be written using this decomposition:

$$\begin{aligned}
\mathcal{B}[\mathfrak{p},\mathfrak{q}](x,y) &= \mathfrak{p}(x)\mathfrak{p}(y)\frac{w(y)-w(x)}{x-y} \\
&= \frac{\mathfrak{p}(x)\mathfrak{p}(y)}{x-y}\ \sum_{j=1}^{n}\frac{\mathfrak{q}(\xi_j)}{\mathfrak{p}'(\xi_j)}\left(\frac{1}{y-\xi_j}-\frac{1}{x-\xi_j}\right) \\
&= \sum_{j=1}^{n}\frac{\mathfrak{q}(\xi_j)}{\mathfrak{p}'(\xi_j)}\ \frac{\mathfrak{p}(x)}{(x-\xi_j)}\ \frac{\mathfrak{p}(y)}{(y-\xi_j)}
\end{aligned}$$

Here it will be useful to introduce a couple of bases of V. Only for the particular case when the roots of $\mathfrak{p}$ are all simple, the following polynomials are linearly independent over K:

$$\left\{\begin{array}{rcl} u_1(x) &:=& \displaystyle\prod_{j\neq 1}(x-\xi_j) \\ &\vdots& \\ u_n(x) &:=& \displaystyle\prod_{j\neq n}(x-\xi_j) \end{array}\right.$$

These polynomials form a basis of V, known as the **spectral basis** and denoted by $\mathcal{S}_p$. The generating function of the Bezoutian in the spectral basis is then

$$\sum_{j=1}^{n}\frac{\mathfrak{q}(\xi_j)}{\mathfrak{p}'(\xi_j)}\ u_j(x)u_j(y).$$

Still in the separable case and still assuming all the roots of $\mathfrak{p}$ belong to K, the spectral basis gives rise to the **Lagrange basis**, denoted by $\mathcal{L}$ and defined by the interpolators:

$$\left\{\begin{array}{rcccc} l_1(x) & := & \dfrac{u_1(x)}{u_1(\xi_1)} & = & \dfrac{u_1(x)}{\mathfrak{p}'(\xi_1)} \\ & \vdots & & & \\ l_n(x) & := & \dfrac{u_n(x)}{u_n(\xi_n)} & = & \dfrac{u_n(x)}{\mathfrak{p}'(\xi_n)} \end{array}\right.$$

The generating function of the Bezoutian in the Lagrange basis is then

$$\sum_{j=1}^{n} \mathfrak{p}'(\xi_j)\mathfrak{q}(\xi_j) l_j(x) l_j(y).$$

The coefficients of this function are those of the Bezoutian matrix in the Lagrange basis. Isolating them, we see that for $i \neq j$ all the ij coefficients are zero, and for $i = j$ all the jj coefficients are $\mathfrak{p}'(\xi_j)\mathfrak{q}(\xi_j)$. Hence the matrix of the Bezoutian in the Lagrange basis is the following diagonal matrix:

$$[\mathcal{B}]_{\mathcal{L}} = \begin{pmatrix} \mathfrak{p}'(\xi_1)\mathfrak{q}(\xi_1) & \ldots & 0 \\ \vdots & & \vdots \\ 0 & \ldots & \mathfrak{p}'(\xi_n)\mathfrak{q}(\xi_n) \end{pmatrix}$$

This means that the quadratic form given by the Bezoutian is isometric to that one given by

$$\mathfrak{p}'(\xi_1)\mathfrak{q}(\xi_1)x_1^2 + \ldots + \mathfrak{p}'(\xi_n)\mathfrak{q}(\xi_n)x_n^2.$$

1.2.1.2 Change of basis

We might as well compute the matrix of the change of basis. As it is well known, the Lagrange basis has the following interpolating property

$$\begin{cases} l_i(\xi_i) &= 1 \\ l_i(\xi_j) &= 0 \ (i \neq j) \end{cases}$$

But the really lovely property the Lagrange polynomials have is the following: every polynomial f in V (that is, deg $f < n$) can be written in the following way:

$$f(x) = \sum_{i=1}^{n} l_i(x) f(\xi_i) \tag{1.3}$$

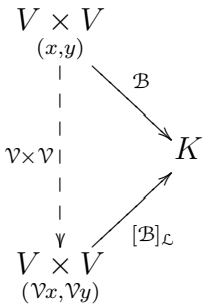
In particular, the standard basis vectors:

$$\begin{aligned} 1 &= \sum l_i(x) \\ x &= \sum l_i(x)\xi_i \\ x^2 &= \sum l_i(x)\xi_i^2 \\ &\vdots \\ x^{n-1} &= \sum l_i(x)\xi_i^{n-1} \end{aligned}$$

This gives us the coefficients of the standard vectors in the Lagrange basis. So we have the matrix of the (linear) change of basis from $\mathcal{S}_{td}$ to $\mathcal{L}$. This matrix will be denoted $\mathcal{V}$ for Vandermonde:

$$\mathcal{V} \;=\; \begin{pmatrix} 1 & \xi_1 & \xi_1^2 & \ldots & \xi_1^{n-1} \\ 1 & \xi_2 & \xi_2^2 & & \xi_2^{n-1} \\ \vdots & & & \ddots & \vdots \\ 1 & \xi_n & \xi_n^2 & \ldots & \xi_n^{n-1} \end{pmatrix}$$

Note that since this is the matrix of the *linear* map that changes basis, the result is that, for a vector x in standard basis, the vector $\mathcal{V}x$ is in Lagrange basis. Of course $\mathcal{V}$ is invertible every time the ξ_j are all different, so we have our isometry, that is:



(1.4)

This diagram is commutative, therefore

$$\begin{aligned} x^t \mathcal{B} y &= (\mathcal{V}x)^t [\mathcal{B}]_{\mathcal{L}} (\mathcal{V}y) \\ &= x^t \; \mathcal{V}^t [\mathcal{B}]_{\mathcal{L}} \mathcal{V} \; y \end{aligned}$$

This holds for every x and every y, therefore $\mathcal{B} = \mathcal{V}^t [\mathcal{B}]_{\mathcal{L}} \mathcal{V}$, that is:

$$\mathcal{B} = \begin{pmatrix} 1 & \dots & 1 \\ \xi_1 & & \xi_n \\ \vdots & & \vdots \\ \xi_n^{n-1} & \dots & \xi_n^{n-1} \end{pmatrix} \begin{pmatrix} p'(\xi_1)\mathfrak{q}(\xi_1) & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & \mathfrak{p}'(\xi_n)\mathfrak{q}(\xi_n) \end{pmatrix} \begin{pmatrix} 1 & \xi_1 & \dots & \xi_1^{n-1} \\ 1 & \xi_2 & & \xi_2^{n-1} \\ \vdots & & & \\ 1 & \xi_n & & \xi_n^{n-1} \end{pmatrix}$$

1.2.2 Traces

For this part we refer specially to an article by Serre found in [24]. For each $\gamma \in V$ the **Trace form** associated to γ is

$$\begin{array}{ccc} V \times V & \xrightarrow{Tr_\gamma} & K \\ (\alpha, \beta) & \mapsto & Tr(\alpha\beta\gamma) = \sum_{\xi \in Z_\mathfrak{p}} \alpha(\xi)\beta(\xi)\gamma(\xi) \end{array}$$

where $Z_\mathfrak{p}$ denotes the distinct zeros of $\mathfrak{p}$. We will be interested in the case when $\mathfrak{p}$ is separable, in which we choose $\gamma = \mathfrak{p}'\mathfrak{q}$.

The trace form has a matrix in the standard basis with coefficients defined by $t_{ij} := \langle e_i, e_j \rangle$. The generating function of the trace is therefore

$$\mathcal{T}(x, y) := \sum_{ij=1}^{n} t_{ij} x^{i-1} y^{j-1}$$

The coefficients t_{ij} can be computed explicitly as follows:

$$\begin{aligned} t_{ij} &= \langle x^{i-1}, x^{j-1} \rangle \\ &= Tr(x^{i+j-2}\gamma) \\ &= \sum_{\xi \in Z_{\mathfrak{p}}} \xi^{i+j-2} \mathfrak{p}'(\xi)\mathfrak{q}(\xi) \end{aligned}$$

Of much more interest however are the coefficients of this matrix in the Lagrange basis. These are easily computed as follows:

$$\begin{aligned} \langle l_i, l_j \rangle &= Tr(l_i l_j \gamma) \\ &= \sum_{k=1}^{n} l_i(\xi_k) l_j(\xi_k) \gamma(\xi_k) \\ &= \begin{cases} 0 & i \neq j \\ \gamma(\xi_i) & i = j \end{cases} \end{aligned}$$

Therefore, the matrix of the Trace in the Lagrange basis is diagonal:

$$[\mathcal{T}]_{\mathcal{L}} = \begin{pmatrix} \mathfrak{p}'(\xi_1)\mathfrak{q}(\xi_1) & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & \mathfrak{p}'(\xi_n)\mathfrak{q}(\xi_n) \end{pmatrix}$$

This shows that, in the separable case, both the Trace and the Bezoutian have the same diagonalization on the Lagrange basis.

1.2.3 Residues

For this part we refer to [25] and to the work of Cattani and Dickenstein in [4].

Let us consider the rational function $w := \mathfrak{q}/\mathfrak{p}$. The quadratic form induced by the residue, called the **Residue form** is:

$$\begin{array}{ccc} V \times V & \xrightarrow{\mathcal{R}_w} & K \\ (\alpha, \beta) & \mapsto & \mathcal{R}es_w(\alpha\beta) = \sum_{\xi \in Z_{\mathfrak{p}}} \mathcal{R}es_\xi(\alpha\beta w \; dz) \end{array}$$

Note that $\mathcal{R}es_w$ refers to the global residue of the rational function w whereas $\mathcal{R}es_\xi$ is the local residue of the product $\alpha\beta w$ at ξ, that is, if w has Laurent series expansion at ξ given by

$$w(z) \; = \; \sum_{k \in \mathbb{Z}} w_k (z - \xi)^k$$

then

$$\mathcal{R}es_\xi(w) = w_{-1}$$

The matrix in the standard basis will be denoted with coefficients r_{ij} and the generating function will be $\mathcal{R}(x, y) = \sum_{ij=1}^{n} r_{ij} x^{i-1} y^{j-1}$.

In the case when $\mathfrak{p}$ is separable, the Residue is the Trace. This rests on the fact that when $\mathfrak{p}$ is separable and ξ is a root of $\mathfrak{p}$ and $\gcd(\mathfrak{p}, h) = 1$ then $\mathcal{R}es_\xi(h/\mathfrak{p}) = h(\xi)/\mathfrak{p}'(\xi)$. We have already used this in the partial fraction

decomposition of w. The coefficients of the Residue matrix in the standard basis are computed as follows:

$$\begin{aligned}
\langle 1,1\rangle &= \sum_{\xi\in Z_{\mathfrak{p}}} \mathcal{R}es_{\xi}(1.1.\mathfrak{q}/\mathfrak{p}) \\
\langle 1,x\rangle &= \sum_{\xi\in Z_{\mathfrak{p}}} \mathcal{R}es_{\xi}(1.x.\mathfrak{q}/\mathfrak{p}) \\
&\vdots \\
\langle x^{n-1},x^{n-1}\rangle &= \sum_{\xi\in Z_{\mathfrak{p}}} \mathcal{R}es_{\xi}(x^{2n-2}\mathfrak{q}/\mathfrak{p})
\end{aligned}$$

So if $\mathfrak{p}(0)\neq 0$ these coefficients are:

$$\begin{aligned}
r_{11} &= \sum_{\xi\in Z_{\mathfrak{p}}} \mathfrak{p}'(\xi)\mathfrak{q}(\xi) \\
r_{12} &= \sum_{\xi\in Z_{\mathfrak{p}}} \xi\mathfrak{p}'(\xi)\mathfrak{q}(\xi) \\
&\vdots \\
r_{nn} &= \sum_{\xi\in Z_{\mathfrak{p}}} \xi^{2n-2}\mathfrak{p}'(\xi)\mathfrak{q}(\xi)
\end{aligned}$$

That is, $r_{ij}=t_{ij}$.

1.3 Hankel matrices and Rational functions

1.3.1 Hankel matrices

A **Hankel matrix** is a matrix $(a_{ij})_{ij}$ where the coefficients only depend on $i+j$, i.e., there exist a sequence $(s_k)_k$ such that $a_{ij} = s_{i+j}$.

On the other hand, any given sequence $(s_k)_{k\in\mathbb{N}}$ determines an infinite Hankel matrix $\mathcal{H}$:

$$\mathcal{H} := \begin{pmatrix} s_1 & s_2 & s_3 & \dots \\ s_2 & s_3 & s_4 & \dots \\ s_3 & s_4 & s_5 & \dots \\ \vdots & & & \ddots \end{pmatrix} \tag{1.5}$$

Let $\mathcal{H}_n$ denote the truncated $n \times n$ Hankel matrix $\mathcal{H}$, that is:

$$\mathcal{H}_n := \begin{pmatrix} s_1 & s_2 & \dots & s_n \\ s_2 & s_3 & & s_{n+1} \\ \vdots & & & \vdots \\ s_n & s_{n+1} & \dots & s_{2n-1} \end{pmatrix}$$

Every rational function has associated an infinite Hankel matrix. We see this next.

1.3.2 Rational functions

Partial fractions. Let w be a rational function and let $\xi_1, ..., \xi_r$ be the different poles of w with corresponding multiplicities $n_1, ..., n_r$ and let $n = n_1 + ... + n_r$. Then w has a partial fraction expansion:

$$w(x) = P(x) + \sum_{j=1}^{r} \left[\frac{A_1^{(j)}}{(x-\xi_j)} + \frac{A_2^{(j)}}{(x-\xi_j)^2} + ... + \frac{A_{n_j}^{(j)}}{(x-\xi_j)^{n_j}} \right] \tag{1.6}$$

where $A_i^{(j)}$ are constants and P is some polynomial. Let us recall a few generating functions:

$$\begin{aligned}
\frac{1}{1-X} &= \sum_{k\geq 0} X^k \\
\frac{1}{X-\xi} &= \sum_{k\geq 1} \frac{\xi^{k-1}}{X^k} \\
\frac{1}{(1-X)^n} &= \sum_{k\geq 0} \binom{k+n-1}{k} X^k \\
\frac{1}{(X-\xi)^n} &= \sum_{k\geq n} \frac{\binom{k+n-1}{k}\ \xi^{k-n}}{X^k}
\end{aligned}$$

Using these and substituting in (1.6) we obtain an expansion of the form

$$w(x) \;=\; P(x) + \sum_{k\geq 1} \frac{s_k}{x^k} \tag{1.7}$$

In particular the sequence $(s_k)_k$ of coefficients of negative powers of x determines an infinite Hankel matrix $\mathcal{H}(w)$:

$$\mathcal{H}(w) := \begin{pmatrix} s_1 & s_2 & s_3 & \dots \\ s_2 & s_3 & s_4 & \dots \\ s_3 & s_4 & s_5 & \dots \\ \vdots & & & \ddots \end{pmatrix} \tag{1.8}$$

Some observations

1. Let w_1, w_2 be two rational functions differing only on a polynomial, then their Hankel matrices are equal: $w_1 - w_2 \in K[x] \Rightarrow \mathcal{H}(w_1) = \mathcal{H}(w_2)$
2. Let $\lambda_1, \lambda_2 \in K$, then $\mathcal{H}(\lambda_1 w_1 + \lambda_2 w_2) \;=\; \lambda_1 \mathcal{H}(w_1) + \lambda_2 \mathcal{H}(w_2)$

1.3.3 Connection between Hankel Matrices and Rational Functions

Theorem 1.3.1. *The infinite matrix $\mathcal{H}$ is of finite rank if and only if the series $w(z) = \sum_{j\geq 1} \frac{s_j}{z^j}$ is a rational function of z. Furthermore, if $w = \frac{\mathfrak{q}}{\mathfrak{p}}$ with $\mathfrak{q}$ and $\mathfrak{p}$ coprime, then rank($\mathcal{H}$) = deg ($\mathfrak{p}$).*

A proof of this theorem can be found in [8] Vol. II 10.2.

1.3.4 Connection between Bezoutian Forms and Hankel Matrices of Rational Functions

It will be convenient here to introduce yet one more basis of V. The **Horner** basis of V, denoted by H, is the basis of V given by the **Horner polynomials** associated to $\mathfrak{p}(x) = p_0+p_1x+p_2x^2+...+p_{n-1}x^{n-1}+x^n$, which are defined as follows.

$$\begin{cases} h_1 &= p_1 + p_2x + ... + p_{n-1}x^{n-2} + x^{n-1} \\ h_2 &= p_2 + ... + p_{n-1}x^{n-3} + x^{n-2} \\ h_k &= p_k + ... + x^{n-k} \\ \vdots & \\ h_n &= 1 \end{cases}$$

The recursive relations that classically define the Horner polynomials are:

$$\begin{cases} xh_k(x) &= h_{k-1}(x) - p_k \\ xh_0 &= \mathfrak{p}(x) - p_0 \end{cases}$$

Let C be the matrix of change of basis from Horner to Standard:

$$C = \begin{pmatrix} p_1 & p_2 & p_3 & \cdots & p_{n-1} & 1 \\ p_2 & p_3 & p_4 & & 1 & 0 \\ p_3 & p_4 & p_5 & & 0 & 0 \\ \vdots & & & & & \\ p_{n-1} & 1 & 0 & & 0 & 0 \\ 1 & 0 & 0 & & 0 & 0 \end{pmatrix}$$

This matrix has some interesting properties, for instance:

- C is a Hankel matrix, in particular $C^t = C$.
- C is a Bezoutian: $C = \mathcal{B}(\mathfrak{p}, 1)$.

Now we can state a theorem that relates the Bezoutian of $\mathfrak{p}$ and $\mathfrak{q}$ to the Hankel matrix of $\mathfrak{q}/\mathfrak{p}$. Recall that $n = \deg \mathfrak{p} \geq \deg \mathfrak{q}$.

Theorem 1.3.2.

$$\mathcal{B}(\mathfrak{p}, \mathfrak{q}) \;=\; C^t \mathcal{H}(\mathfrak{q}/\mathfrak{p})_n C$$

Proof: in [7] (Theorem 8.7.2, page 217).

Note that since $\det(C) = \pm 1$, both $\mathcal{B}(\mathfrak{p}, \mathfrak{q})$ and $\mathcal{H}(\mathfrak{q}/\mathfrak{p})_n$ have the same determinant.

Chapter 2

Real Bezoutians

In this chapter we consider Bezoutians in the case when the base field is $K = \mathbb{R}$. As usual, the polynomials $\mathfrak{p},\ \mathfrak{q}\ \in \mathbb{R}[x]$ are monic.

Two regular quadratic forms are isometric over $\mathbb{R}$ if and only if they share the three invariants: rank, discriminant, signature. Let us recall here what the signature is.

2.1 Signature

Theorem 2.1.1. Sylvester Law of Inertia
Let $(V, \mathcal{Q})$ be a regular quadratic space over $K = \mathbb{R}$ of dimension n. Then there exists a decomposition $n = n_+ + n_-$ with $0 \leq n_+, n_- \leq n$ such that, for every diagonalization $\mathcal{Q}(x) \simeq a_1x_1^2 + ... + a_nx_n^2$ exactly n_+ among the n coefficients $a_1, ..., a_n$ are positive and n_- are negative.

For a proof of this theorem see [17] XV.4.

Definition 2.1.1. Using the notation of the previous theorem, the **signature** of V, denoted $\sigma(V)$ or just σ is the difference between the number of positive coefficients and the number of negative ones, that is $\sigma = n_+ - n_- = 2n_+ - n$.

Note that $-n \leq \sigma \leq n$. As with hermitian forms, a regular quadratic form $\mathcal{Q}$ is said to be **definite** if its signature has maximum absolute value, that is, $\sigma = \pm n$. It is said to be **positive definite** if $\sigma = +n$ or equivalently if $\mathcal{Q}(x) > 0$ for every $x \neq 0$. Analogously, a regular quadratic form $\mathcal{Q}$ is said to be **negative definite** if $\sigma = -n$ or equivalently if $\mathcal{Q}(x) < 0$ for every $x \neq 0$.

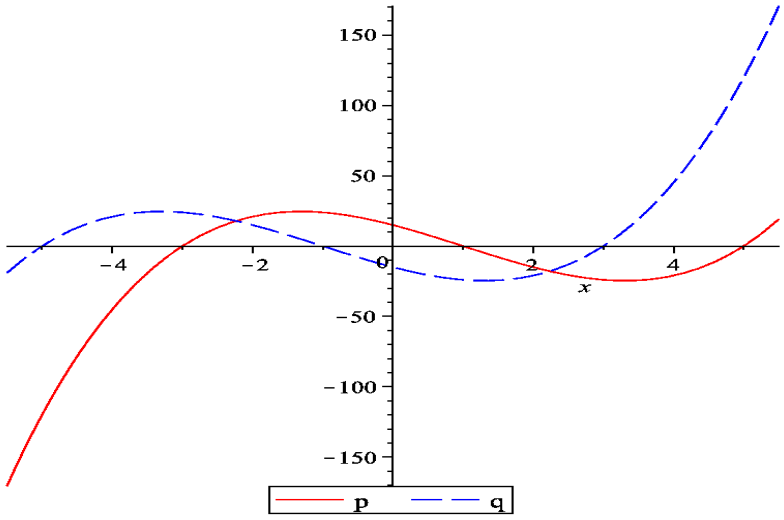
2.2 Interlacing

We begin this key section in the understanding of Bezoutians with a definition.

Definition 2.2.1. Two polynomials $\mathfrak{p},\ \mathfrak{q}\ \in\ \mathbb{R}[x]$ of the same degree n are said to *interlace* if the following three conditions are satisfied:

1. The roots of $\mathfrak{p}$ and $\mathfrak{q}$ are all real.
2. The roots of $\mathfrak{p}$ and $\mathfrak{q}$ are all different.
3. The roots of $\mathfrak{p}$ interlace with the roots of $\mathfrak{q}$ on the real line.

For example, let $\begin{cases} \mathfrak{p} &= (x+3)(x-1)(x-5) \\ \mathfrak{q} &= (x+5)(x+1)(x-3) \end{cases}$



For the following classical theorem we refer to the work of Olshevsky and Olshevsky in [19].

Theorem 2.2.1. (Interlacing)

Let $\mathfrak{p}, \mathfrak{q} \in \mathbb{R}[x]$ *be both of the same degree* n *and let* $K = \mathbb{R}$. *Then the Bezoutian* $\mathcal{B}_{\mathfrak{p},\mathfrak{q}}$ *is definite if and only if* $\mathfrak{p}$ *and* $\mathfrak{q}$ *interlace.*

Proof. ($\Rightarrow$)

1. Being a definite symmetric matrix, $\mathcal{B}$ induces a hermitian form on $\mathbb{C}^n$, which has matrix notation $\langle x, y\rangle = \overline{x^t}\mathcal{B}y$.

Now suppose there is a root of $\mathfrak{p}$ or $\mathfrak{q}$ in $\mathbb{C} \setminus \mathbb{R}$, call it ξ and let us consider the Vandermonde vector $\boldsymbol{\xi} := (1,\ \xi,\ \xi^2,\ \ldots\ ,\ \xi^{n-1})^t$. Then:

$$\overline{\boldsymbol{\xi}}^{\boldsymbol{t}}\ \mathcal{B}\ \boldsymbol{\xi}\ =\ \sum_{i,j=1}^{n-1} b_{ij}\overline{\xi}^{i-1}\xi^{j-1}\ =\ \frac{\mathfrak{p}(\overline{\xi})\mathfrak{q}(\xi)\ -\ \mathfrak{p}(\xi)\mathfrak{q}(\overline{\xi})}{\overline{\xi}-\xi}$$

And here is the contradiction: the left hand side is not zero for $\mathcal{B}$ is definite and $\boldsymbol{\xi} \neq 0$, but the right hand side is zero for ξ is a root of a real polynomial, so $\overline{\xi}$ is a root as well.

2. Now let us consider the symmetric quadratic form $x^t\mathcal{B}y$ over $\mathbb{R}^n$ and suppose not all the roots of $\mathfrak{p}$ and $\mathfrak{q}$ are different. Then either they have a root in common or at least one of them has a multiple root. We see each of these cases separately, but in each one the conclusion is the same: we start with $\boldsymbol{\xi}^{\boldsymbol{t}}\mathcal{B}\boldsymbol{\xi}$, which cannot be zero, and we arrive to something that must be zero, obtaining a contradiction.

(i) Suppose that $\xi \in \mathbb{R}$ is a common root of $\mathfrak{p}$ and $\mathfrak{q}$, then:

$$\boldsymbol{\xi}^{\boldsymbol{t}}\mathcal{B}\boldsymbol{\xi}\ =\ \lim_{x\to\xi}\ \frac{\mathfrak{p}(x)\mathfrak{q}(\xi)\ -\ \mathfrak{p}(\xi)\mathfrak{q}(x)}{x-\xi}\ =\ 0$$

(ii) If ξ is a multiple root of $\mathfrak{p}$:

$$\begin{aligned}\boldsymbol{\xi}^{\boldsymbol{t}}\mathcal{B}\boldsymbol{\xi}\ &=\ \mathfrak{q}(\xi)\lim_{x\to\xi}\ \frac{\mathfrak{p}(x)\ -\ \mathfrak{p}(\xi)}{x-\xi}\\ &=\ \mathfrak{p}'(\xi)\ \mathfrak{q}(\xi) = 0\end{aligned}$$

(iii) If ξ is a multiple root of $\mathfrak{q}$:

$$\begin{aligned} \boldsymbol{\xi}^{\boldsymbol{t}}\mathcal{B}\boldsymbol{\xi} &= -\mathfrak{p}(\xi)\lim_{x\to\xi}\frac{\mathfrak{q}(x)-\mathfrak{q}(\xi)}{x-\xi} \\ &= -\mathfrak{p}(\xi)\ \mathfrak{q}'(\xi) = 0 \end{aligned}$$

3. Let $\xi_1 < ... < \xi_n \ \in \mathbb{R}$ be all the roots of $\mathfrak{p}$. Because $\mathfrak{p}$ is separable, the Vandermonde matrix $\mathcal{V}$ of the $\xi_j's$ is invertible, therefore it is a valid change of basis, hence the diagonalization from chapter one holds:

$$\mathcal{B} \ = \ \mathcal{V}^t \begin{pmatrix} \mathfrak{p}'(\xi_1)\ \mathfrak{q}(\xi_1) & 0 & & \\ 0 & \mathfrak{p}'(\xi_2)\ \mathfrak{q}(\xi_2) & & \\ & & \ddots & \\ & & & \mathfrak{p}'(\xi_n)\ \mathfrak{q}(\xi_n) \end{pmatrix} \mathcal{V}$$

Now $\mathcal{B}$ is definite and this is a (bilinear) diagonalization of $\mathcal{B}$, therefore all the elements in the diagonal must have the same sign. But $\mathfrak{p}$ being separable implies that $\{\mathfrak{p}'(\xi_i)\}$ is sign-alternating, therefore $\{\mathfrak{q}(\xi_i)\}$ must be so as well, giving us interlacing: $\mathfrak{q}$ is changing sign at each one of the roots of $\mathfrak{p}$. This implies, by Bolzano's theorem, that $\mathfrak{q}$ must have at least one root in between each root of $\mathfrak{p}$. This accounts for $n-1$ of the roots of $\mathfrak{q}$. There is just one more to take care of.

This lone root cannot be in any one of the bounded intervals determined by the roots of $\mathfrak{p}$, since all of those already contain a root of $\mathfrak{q}$ and it can only contain an odd number of roots of $\mathfrak{q}$: if there were an even number of roots of

$\mathfrak{q}$ between ξ_i and ξ_{i+1} then $\mathfrak{q}$ would have the same sign on both ξ_i and ξ_{i+1}, a contradiction.

Therefore this root of $\mathfrak{q}$ must be either before all of those of $\mathfrak{p}$ or after them, and either case gives rise to an interlacing pattern.

($\Leftarrow$)

This direction should be clear considering the diagonalization of the Bezoutian in the separable case.

□

2.3 Forms with a given signature

The previous section can be rephrased by saying that if the roots of $\mathfrak{p}$ and $\mathfrak{q}$ are set or configured so that they interlace, then the signature of the Bezoutian is either n or $-n$, depending on the first root being one of $\mathfrak{p}$ or one of $\mathfrak{q}$. It would also depend on the sign of the leading terms of $\mathfrak{p}$ and $\mathfrak{q}$, but our polynomials are monic, so that is not a variable here.

It is indeed clear that given any configuration of the roots of $\mathfrak{p}$ and $\mathfrak{q}$ (when all real and different) the signature is immediately determined: in such case the diagonalization given by $\{\mathfrak{p}'(\xi_i)\mathfrak{q}(\xi_i)\}$ still holds, making it easy to count the number of positive and negative signs.

This raises the question of what happens in the opposite direction, that is: if we are given a signature $\sigma = k$, is there a way to effectively count

how many configurations of the roots of $\mathfrak{p}$ and $\mathfrak{q}$ will give us that particular signature? The answer is yes, and we study this in this section.

Always assuming the roots of $\mathfrak{p}$ and $\mathfrak{q}$ are all real and distinct, it will be useful to think of each string of roots of $\mathfrak{p}$ and $\mathfrak{q}$ as a word on letters A and B, A representing the roots of $\mathfrak{p}$ and B representing the roots of $\mathfrak{q}$. So for example the polynomials $\begin{cases} \mathfrak{p}(x) = (x-1)(x-4) \\ \mathfrak{q}(x) = (x-2)(x-3) \end{cases}$ would be represented by the word $ABBA$.

2.3.1 The words

Let P_n be the set of words representing two separable polynomials of n roots each, that is, words on $2n$ symbols A and B, n $A's$ and n $B's$, that is:

$$P_n := \{\text{words in } \langle A, B\rangle : \#A's = \#B's = n\}, \quad \#P_n = \binom{2n}{n}$$

The analysis in the previous section shows that no consecutive occurrences of $A's$ or $B's$ (i.e., interlacing) happens exactly when the signature is max or min. That implies that when consecutive occurrences of $A's$ or $B's$ do happen, the signature experiments a drop in absolute value. Indeed, this seems to suggest that each occurrence of a consecutive pair AA or BB might cause a drop in the absolute value of the signature.

In order to analyze this, let us denote by P the union of all the $P_i's$ with $0 \leq i \leq n$ and let π be the projection from a word to its reduced version,

where by **reduced** we mean that we mod out by the relation $AA = BB = \emptyset$. If χ denotes a word in P_n, let $\overline{\chi}$ denote its reduced version:

$$P = \bigcup_{i=0}^{n} P_i \qquad\qquad \begin{array}{ccc} P_n & \xrightarrow{\pi} & P \\ \chi & \mapsto & \overline{\chi} \end{array}$$

Observation. When canceling out pairs AA and BB in a word χ, the number of letters in that word decreases by an even number. Therefore, the projection $\pi(\chi)$ belongs to a subset of P, namely that one formed by the union of the $P_i's$ with i having the same parity as n. Also, each drop of the kind AA causes a drop of the kind BB and vice-versa, by the pigeons principle. Therefore:

$$\pi(P_n) \quad \subset \quad \bigcup_{\substack{i=0 \\ i \equiv n \pmod 2}}^{n} P_i$$

Definition 2.3.1. For $\chi \in P_n$ we define the **length** of χ (denoted $\mathrm{l}(\chi)$) to be the index i for which $\pi(\chi) \in P_i$.

Note that $0 \leq \mathrm{l}(\chi) \leq n$ and that $\mathrm{l}(\chi)$ has the same parity of n. Hence, for some $0 \leq j \leq [n/2]$,

$$\mathrm{l}(\chi) = n - 2j.$$

2.3.2 A corollary of the Interlacing theorem

The following theorem was stated without proof by Sylvester.

Theorem 2.3.1. *Let* $\mathfrak{p}$ *and* $\mathfrak{q}$ *be as before, let* $\mathcal{B}$ *be the Bezoutian of* $\mathfrak{p}$ *and* $\mathfrak{q}$ *and let* χ *be the word in* P_n *corresponding to the configuration of the roots of* $\mathfrak{p}$ *and* $\mathfrak{q}$*. Then the length of* χ *equals the absolute value of the signature of* $\mathcal{B}$*:*

$$\mathrm{l}(\chi) \;=\; |\sigma(\mathcal{B})|$$

Proof.

Because we are in the separable case, the diagonalization of the Bezoutian in the Lagrange basis is:

$$\mathcal{B} \;\simeq\; \begin{pmatrix} \mathfrak{p}'(\xi_1)\mathfrak{q}(\xi_1) & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & \mathfrak{p}'(\xi_n)\mathfrak{q}(\xi_n) \end{pmatrix}$$

hence the signature of $\mathcal{B}$ is

$$\begin{aligned} \sigma(\mathcal{B}) \;&=\; \#\{k:\ \mathfrak{p}'(\xi_k)\mathfrak{q}(\xi_k) > 0\} \;-\; \#\{k:\ \mathfrak{p}'(\xi_k)\mathfrak{q}(\xi_k) < 0\} \\ &=\; \#\{k:\ \mathsf{sign}(\mathfrak{p}'(\xi_k)) = \mathsf{sign}(\mathfrak{q}(\xi_k))\} \;-\; \#\{k:\ \mathsf{sign}(\mathfrak{p}'(\xi_k)) \neq \mathsf{sign}(\mathfrak{q}(\xi_k))\} \end{aligned}$$

Every real number $a \neq 0$ can be expressed in one of the forms $a = b^2$ or $a = -1.b^2$ for some other real number b. Therefore, in the real case, we can take the diagonalization one step further and end up with a string of ones and

minus ones. Indeed, a set of representatives for the classes of regular quadratic forms over $\mathbb{R}$ is given by the forms $\pm x_1^2 \pm ... \pm x_n^2$.

So from now on we will think of the diagonal of $\mathcal{B}$ as a string of ones and minus ones, i.e., a word of n letters on two symbols, $+$ and $-$. In order to compute the signature of a given word, we add the relation $+- = -+ = \emptyset$. This way it is obvious that the signature of $\mathcal{B}$ is the length of the reduced word induced by the diagonal of $\mathcal{B}$. For example, if the signs in $\mathcal{B}$ are $++-+$ then the signature of $\mathcal{B}$ is

$$+\not{+}\not{-}+ \;=\; 2.$$

Note that if we reduce $\mathcal{B}$ to a diagonal matrix with ones and minus ones, the signature is nothing but the trace. We mention this as a curiosity in this case, but it is is not an invariant of isometry in general.

Now $\mathfrak{p}$ has all real simple roots, which means its graph intersects with the real line exactly n times, and in each one of the $n-1$ (bounded) intervals determined by the roots, $\mathfrak{p}$ has exactly one critical point (which is indeed a local maximum or a local minimum).

The parity of n determines the sign of $\mathfrak{p}'(\xi_1)$:

$$\mathfrak{p}'(\xi_1) = \prod_{i=2}^{n}(\xi_1 - \xi_i) \qquad \Rightarrow \qquad \mathsf{sign}(\mathfrak{p}'(\xi_1)) = (-1)^{n-1}$$

while the sign of $\mathfrak{p}'(a_n)$ is always positive, regardless of the of n because $\mathfrak{p}$ is monic. Indeed:

$$\begin{cases} \mathfrak{p}'(\xi_n) & > & 0 \\ \mathfrak{p}'(\xi_{n-1}) & < & 0 \\ \vdots & & \\ \mathfrak{p}'(\xi_{n-2j}) & > & 0 \\ \mathfrak{p}'(\xi_{n-(2j+1)}) & < & 0 \\ \vdots & & \end{cases}$$

that is to say,

$$\mathfrak{p}'(\xi_k) > 0 \qquad \Leftrightarrow \qquad k \equiv n(\mathsf{mod}\ 2)$$

Now to use this on the signature, let us first start with the simplest case, that is when the signature is maximum or minimum, that is $\sigma = \pm n$. The following lemma is a particular case of the theorem we are trying to prove.

Lemma 2.3.2. $\sigma = \pm n \ \Leftrightarrow l\,(\chi) = n.$

Proof. Suppose first that the signature is maximum. Then for every $1 \leq i \leq n$,

$$\mathsf{sign}(\mathfrak{q}(\xi_i)) \;=\; \mathsf{sign}(\mathfrak{p}'(\xi_i)).$$

We have seen in the Interlacing theorem that this implies that the roots of $\mathfrak{p}$ and $\mathfrak{q}$ interlace. Now we want to prove that the first root of the sequence is one of $\mathfrak{q}$. Because of the interlacing pattern and the fact that both polynomials have n roots, if the first root is not one of $\mathfrak{q}$ then the last one must be. It cannot be the last one for the following reason. We know that $\mathfrak{q}$ has the same sign as $\mathfrak{p}'$ at each of the $\xi_k' s$, in particular, $\mathfrak{q}(\xi_n) > 0$.

Now if $\mathfrak{q}$ had one more root $\zeta_n > \xi_n$, that would mean that $\mathfrak{q}$ is decreasing on ζ_n. But $\mathfrak{q}$ does not have any more roots after ζ_n, so it would be negative at ∞. This is a contradiction, since $\mathfrak{q}$ is monic.

Therefore, the lone root of $\mathfrak{q}$ must be before all of those of $\mathfrak{p}$: $\zeta_1 < \xi_1$, which lead us to

$$\sigma = n \qquad \Rightarrow \qquad \chi = BABA...BA.$$

The same reasoning shows that when the signature is minimum then there is interlacing of the opposite kind, namely:

$$\sigma = -n \qquad \Rightarrow \qquad \chi = ABAB...AB.$$

Now $\chi = BABA...BA$ or $\chi = ABAB...AB$ (with n repetition of BA or AB in each case) exactly when $\mathrm{ord}(\chi) = n$. This shows that $\sigma = \pm n \;\Rightarrow \mathrm{l}\,(\chi) = n$.

The reciprocal implication follows clearly with the same reasoning, so this concludes the proof of the lemma. □

Note here that there was no cancellation AA nor BB on χ the same way that there was no cancellation $+-$ nor $-+$ on the reduce diagonal of $\mathcal{B}$.

This seems to suggest a correspondence between these different kind of cancellations. Indeed, suppose there is an occurrence of AA in the configurations of the roots. Say there are no roots of $\mathfrak{q}$ between ξ_i and ξ_{i+1}. Then $\mathfrak{q}$ cannot change sign from ξ_i to ξ_{i+1}:

$$\mathsf{sign}(\mathfrak{q}(\xi_i)) \;=\; \mathsf{sign}(\mathfrak{q}(\xi_{i+1})).$$

But $\mathfrak{p}'$ always changes signs (because all of the roots are simple), hence:

$$\mathsf{sign}(\mathfrak{p}'(\xi_i)) \;\neq\; \mathsf{sign}(\mathfrak{p}'(\xi_{i+1})).$$

Therefore their product must change signs:

$$\mathsf{sign}(\mathfrak{p}'(\xi_i)\mathfrak{q}(\xi_i)) \;\neq\; \mathsf{sign}(\mathfrak{p}'(\xi_{i+1})\mathfrak{q}(\xi_{i+1}))$$

which is to say that there is an occurrence of $+-$ or $-+$ in the reduced diagonal of $\mathcal{B}$.

This shows that every cancellation on χ of the type AA induces a cancellation of type $+-$ or $-+$ on the signature.

Now every cancellation of the type AA comes with a twin one of the type BB (and vice versa), since the original number of $A's$ equals that one of $B's$, so if we take out 2 of the original n $A'2$ we are left with $(n-2)$ $A's$ distributed among n $B's$. By the pigeon hole principle, there must be at least two $B's$ together.

This implies that after canceling out AA and BB from χ, we are left with a word on P_{n-1}, and inductively everything starts again.

Now we need to show that reciprocally, every cancellation of the type $+-$ or $-+$ on the reduced diagonal induces one of the type AA or BB on χ. So let there be an occurrence of $+-$ or of $-+$, say for instance

$$\mathsf{sign}(\mathfrak{p}'(\xi_i)\mathfrak{q}(\xi_i)) \;\neq\; \mathsf{sign}(\mathfrak{p}'(\xi_{i+1})\mathfrak{q}(\xi_{i+1})).$$

Let us see up to what point we can go backwards in the previous argument. Since $\mathfrak{p}'$ always changes sign on the $\xi_i's$, it must be that $\mathfrak{q}$ did not change sign this time:

$$\mathsf{sign}(\mathfrak{q}(\xi_i)) \;=\; \mathsf{sign}(\mathfrak{q}(\xi_{i+1})).$$

Now in order for this to happen it must be that the number of roots of $\mathfrak{q}$ in between ξ_i and ξ_{i+1} must be even.

• If this number is zero, then there are no $\zeta_j's$ between ξ_i and ξ_{i+1}, giving us an occurrence of AA (which comes with a twin one of BB).

• If this number is not zero, it must be at least 2 (since it is even), giving us an occurrence of BB (which comes with a twin one of AA).

In any case, after cancellations we are reduced to a word in P_{n-1} and a reduced diagonal of dimension $n-2$, and we use induction. This concludes the proof of the theorem.

□

2.3.3 Number of words with a given signature

Recall that

$$\pi(P_n) \subseteq \bigcup_{\substack{0 \leq k \leq n \\ k \equiv n \pmod 2}} P_k.$$

Furthermore, for $\chi \in P_n$, $\pi(\chi) \in P_k$ if and only if $\pi(\chi) = ABAB...AB$ or $\pi(\chi) = BABA...BA$ with exactly k occurrences of AB or BA respectively.

In the first case the signature is negative and in the second it is positive (the absolute value is k in both cases). Let us define $\mathcal{O}_k$ to be the set of words with signature $\sigma = k$, that is, for each $0 \leq k \leq n$:

$$\mathcal{O}_k := \{\chi \in P_n : \sigma(\chi) = k\} = \{\chi \in P_n : \pi(\chi) = BA...BA \in P_k\}$$

$$\mathcal{O}_{-k} := \{\chi \in P_n : \sigma(\chi) = -k\} = \{\chi \in P_n : \pi(\chi) = AB...AB \in P_k\}$$

We wish to study the cardinality of $\mathcal{O}_k$ for every $-n \leq k \leq n$. Let us first get some simple remarks out of the way.

1. $P_n = \bigsqcup_{-n \leq k \leq n} \mathcal{O}_k$. (The symbol $\sqcup$ stands for disjoint union).

2. $\mathcal{O}_k = \emptyset$ every time that k and n have different parities. So it is only interesting to study those $\mathcal{O}_k$ with $k \equiv n \pmod 2$.

3. $\#\mathcal{O}_k = \#\mathcal{O}_{-k}$

4. $\#P_n = \sum_{i=-n}^{n} \#\mathcal{O}_k$, therefore $\binom{2n}{n} = \#\mathcal{O}_0 + 2\sum_{i=1}^{n} \#\mathcal{O}_k$.

5. $\#\mathcal{O}_n = 1$ since $\mathcal{O}_n = \{BABA...BA\}$.

Because of the second remark above, we will only care to study the cardinality of $\mathcal{O}_k$ for $k \equiv n \pmod 2$. Therefore from now on instead of $\mathcal{O}_k$ we will write $\mathcal{O}_{n-2j}$, so instead of $-n \leq k \leq n$ our index will now be $0 \leq j \leq n$.

When counting the cardinality of $\mathcal{O}_{n-2j}$ we see that for each given word $\chi \in \mathcal{O}_{n-2j}$ it does not really matter the distribution of the $A's$ and the $B's$, but the number of double blocks AB, BA, and so on. This suggests a new way to look at P_n, which we introduce next.

2.3.4 P_n as words on four letters

As we said above, we want to focus on double blocks instead of on isolated letters. There are four kind of such blocks, namely:

$$\begin{cases} X & := & BA \\ Y & := & AB \\ Z & := & AA \\ W & := & BB \end{cases}$$

There is an immediate benefit on changing into this language, and that is that each letter X, Y, Z, W has an obvious contribution to the signature, as we can see:

$$\begin{cases} X & \to & +1 \\ Y & \to & -1 \\ Z & \to & 0 \\ W & \to & 0 \end{cases}$$

In this new context what used to be words in A and B with $\#A = \#B = n$ is now words in X, Y, W, Z where $\#Z = \#W$, that is:

$$P_n := \{\text{words in } \langle X, Y, W, Z\rangle : \ \#X + \#Y + \#W + \#Z = n \text{ and } \#W = \#Z\}$$

2.3.5 The signature in this context

Given a word χ on the four letters X, Y, Z, W; the signature of χ can be easily obtained looking only at the occurrences of X and Y. Namely, let us define the **degree** of χ on a given letter as the number of times that letter appears in χ:

$$\mathsf{deg}_\chi(X) = \#\{X \text{ appearing on } \chi\}$$

and so on. Note that for $\chi \in P_n$, $\mathsf{deg}_\chi(Z) = \mathsf{deg}_\chi(W)$ and

$$\mathsf{deg}_\chi(X) + \mathsf{deg}_\chi(Y) + 2\mathsf{deg}_\chi(Z) \;=\; n \tag{2.1}$$

Each appearance of X that is not canceled out by one of Y, counts as a plus one in the signature. Symmetrically, each appearance of Y that is not canceled out by one of X, contributes a minus one to the signature. The appearances of Z and W do not matter for the signature. It is therefore clear that:

$$\sigma(\chi) \;=\; \mathsf{deg}_\chi(X) - \mathsf{deg}_\chi(Y)$$

Hence:

$$\mathcal{O}_{n-2j} = \; \{\chi \in \mathcal{P}_n |\; \mathsf{deg}_\chi(X) - \mathsf{deg}_\chi(Y) = n - 2j\}$$

Note that for a word χ to have $\sigma = n - 2j$ it is necessary that

$$\mathsf{deg}_\chi(X) \geq n - 2j$$

hence because of (2.1) it must be that

$$0 \leq \mathsf{deg}_{\chi}(Z) \leq j.$$

So we may count the number of elements in $\mathcal{O}_{n-2j}$ depending on $\mathsf{deg}_{\chi}(Z)$, thanks to the fact that:

$$\mathcal{O}_{n-2j} \;=\; \bigsqcup_{0\leq k\leq j} \{\chi \in \mathcal{O}_{n-2j} |\ \mathsf{deg}_{\chi}(Z) = k\}$$

Let us do that then.

1. $\underline{\mathsf{deg}_{\chi}(Z) = j}$

   There are exactly j occurrences of Z on χ, hence another j ones of W, therefore the reminder $n-2j$ letters must be all X in order to have $\sigma = n-2j$. We must count how many of these words can there be.
   We choose the j positions for the $Z's$ out of the n available. For each one of these configurations we choose j positions for the $W's$ from the $n-j$ reminders. The reminder positions are all $X's$, so the total number is

$$\binom{n}{j}\binom{n-j}{j}.$$

2. $\underline{\mathsf{deg}_\chi(Z) = j - 1}$

Following the previous idea, we choose the $j-1$ positions for Z and the $j-1$ ones for W. There are now $n - 2(j-1) \;=\; (n-2j)+2$ leftover positions, $n-2j$ of which must be $X's$. There are still 2 leftover positions, which must add up to a signature of 0. Since we already chose all the $Z's$ and $W's$ for this word, the two reminder positions can only be filled in with an X and a Y. Which amounts to choosing the place for that one Y out of the $(n-2j)+2$ available after choosing the $Z's$ and the $W's$ and let the leftover be all $X's$. The total number then is:

$$\binom{n}{j-1}\binom{n-(j-1)}{j-1}\binom{n-2(j-1)}{1}.$$

We start to see a pattern here. Let $0 \leq k \leq j$.

3. $\underline{\mathsf{deg}_\chi(Z) = k}$

If $\mathsf{deg}_\chi(Z) = k$ (for any $0 \leq k \leq j$) we'll need to choose k positions for Z out of the n initial ones. For each one of those configurations we choose now k more positions for W out of the $n-k$ available.

Now to the reminder $n-2k$ positions: $n-2j$ of those will be X so that $\sigma = n-2j$. There are now $(n-2k)-(n-2j) = 2(j-k)$ leftover positions adding up to a signature of zero and with neither Z nor W. Therefore

they can only be filled in with $(j-k)$ $X's$ and $(j-k)$ $Y's$. So this last step is reduced to choosing the $j-k$ positions for the $Y's$ out of the $n-2k$ leftover after positioning the $Z's$ and the $W's$. The total number then is:

$$\binom{n}{k}\binom{n-k}{k}\binom{n-2k}{j-k}.$$

Therefore, the number of words giving signature $n-2j$ is

$$\#\mathcal{O}_{n-2j} = \sum_{k=0}^{j}\binom{n}{k}\binom{n-k}{k}\binom{n-2k}{j-k} \tag{2.2}$$

2.3.6 Last details

Let us work out this last expression.

$$\begin{aligned}
\binom{n}{k}\binom{n-k}{k}\binom{n-2k}{j-k} &= \frac{n!}{k!(n-k)!}\,\frac{(n-k)!}{k!(n-2k)!}\,\frac{(n-2k)!}{(j-k)!(n-j-k)!} \\
&= \frac{n!}{k!k!(j-k)!(n-j-k)!} \\
&= \frac{n!}{k!\;(n-j-k)!\;j!}\binom{j}{k} \\
&= \binom{n}{j}\binom{n-j}{k}\binom{j}{k}
\end{aligned}$$

Adding up both sides over k we obtain:

$$\begin{aligned}\sum_{k=0}^{j}\binom{n}{k}\binom{n-k}{k}\binom{n-2k}{j-k} &= \binom{n}{j}\sum_{k=0}^{j}\binom{n-j}{k}\binom{j}{k} \\ &= \binom{n}{j}\sum_{k=0}^{j}\binom{n-j}{k}\binom{j}{j-k}\end{aligned}$$

Note that the sum on the right hand side equals the coefficient of x^j in the product $(1+x)^{n-j}(1+x)^j$: we are choosing j possibilities for x, k from $(1+x)^{n-j}$ and the leftover $j-k$ from $(1+x)^j$, this for all possible choices of k, that is $0 \leq k \leq j$. But this is of course the coefficient of x^j in $(1+x)^n$, therefore:

$$\sum_{k=0}^{j}\binom{n-j}{k}\binom{j}{j-k} = \binom{n}{j}$$

Therefore:

$$\sum_{k=0}^{j}\binom{n}{k}\binom{n-k}{k}\binom{n-2k}{j-k} = \binom{n}{j}^2$$

and we can finally conclude that

$$\#\mathcal{O}_{n-2j} = \binom{n}{j}^2$$

We have just proved the following proposition.

Proposition 2.3.3. *Let* $\mathfrak{p}$ *and* $\mathfrak{q} \in \mathbb{R}[x]$ *be monic, coprime and separable of degree* n *with all real roots. For* $-n \leq k \leq n$ *and* $k \equiv n \pmod 2$*, the number of root configurations of* $\mathfrak{p}$ *and* $\mathfrak{q}$ *over the real line that induce a Bezoutian with signature* $\sigma = k$ *is*

$$\binom{n}{\frac{n-k}{2}}^2$$

□

2.4 Hermite-Hurwitz Theorem

The theorem we present in this section is a classical result, proved by Hermite in 1856 only for the case of simple roots, then by Hurwitz for the general case. We first need to define the Cauchy index of a rational function.

2.4.1 Cauchy Index

Recall from (1.6) the partial fraction decomposition of a rational function and let $\xi_1, ..., \xi_r$ be the different real poles of R and $\xi_{r+1}, \overline{\xi}_{r+1}, ..., \xi_{r+s}, \overline{\xi}_{r+s}$ be the complex (not real) ones, counted without multiplicity, so that the total number of different poles of R is $r + 2s$. For each $1 \leq j \leq r + 2s$ let ν_j be the order of ξ_j as a pole of R. Then R has partial fraction expansion:

$$
\begin{aligned}
R(x) \;&=\; P(x) + \sum_{j=1}^{r} \left[\frac{A_1^{(j)}}{x-\xi_j} + ... + \frac{A_{\nu_j}^{(j)}}{(x-\xi_j)^{\nu_j}} \right] + \\
&+ \sum_{j=r+1}^{s} \left[\frac{A_1^{(j)}}{x-\xi_j} + ... + \frac{A_{\nu_j}^{(j)}}{(x-\xi_j)^{\nu_j}} \right] + \left[\frac{B_1^{(j)}}{x-\overline{\xi}_j} + ... + \frac{B_{\nu_j}^{(j)}}{(x-\overline{\xi}_j)^{\nu_j}} \right]
\end{aligned}
\tag{2.3}
$$

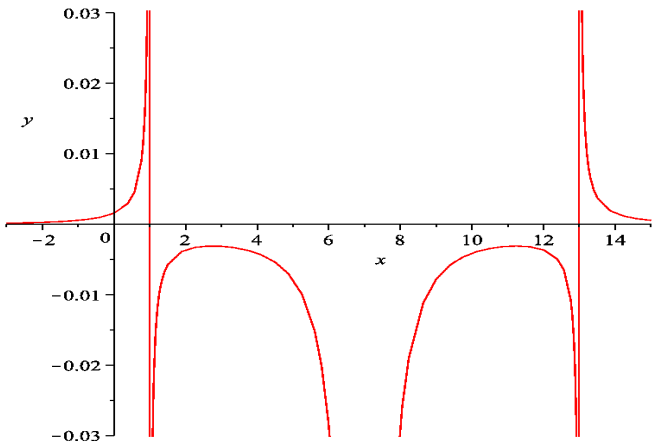
where P is some real polynomial and $A_i^{(j)}$ and $B_i^{(j)}$ are constants. We define the **local Cauchy index** of R at a pole ξ_j as:

$$
I_R(\xi_j) := \begin{cases} \operatorname{sign}(A_{\nu_j}^{(j)}) & 1 \leq j \leq r \\ 0 & \text{otherwise} \end{cases} \tag{2.4}
$$

That is, the Cauchy index is zero at the complex (not real) poles, and at the real poles, it depends on the local behavior of R around ξ_i: if R mimics the behavior of $1/x$ around zero (i.e., goes to $-\infty$ in the left and to $+\infty$ in the right) then the index is $+1$. If it mimics the behavior of $-1/x$ then the index is -1. If it does neither of the previous, then the index is zero. The global Cauchy index, or simply the **Cauchy index** of R is the sum over the local indices, that is:

$$
I_R \;=\; \sum_{j=1}^{r+2s} I_R(\xi_j) \;=\; \sum_{\substack{1 \leq j \leq r \\ \nu_j \text{ odd}}} \operatorname{sign}(A_{\nu_j}^{(j)}) \tag{2.5}
$$

For example, the Cauchy Index of $\dfrac{1}{(x-1)(x-7)^2(x-13)}$ is zero:



2.4.2 Hermite-Hurwitz Theorem

Theorem 2.4.1. Hermite-Hurwitz

Let R be a real rational function: $R(z) = s_{-u}z^u + ... + s_0 + \dfrac{s_1}{z} + \dfrac{s_2}{z^2} + ...$ and let $\mathcal{H}(R)$ be its associated infinite Hankel matrix: $\mathcal{H}(R) = \begin{pmatrix} s_1 & s_2 & ... \\ s_2 & \ddots & \\ \vdots & & \end{pmatrix}$

Then the Cauchy Index of R equals the signature of $\mathcal{H}(R)_N$, for all N greater than or equal than rank $\mathcal{H}(R)$:

$$I_R = \sigma(\mathcal{H}(R)_N) \qquad (\forall\ N \geq \text{rank } \mathcal{H}) \tag{2.6}$$

Proof. Outline, in three steps: (from [8])

1. Use partial fractions on R to decompose $\mathcal{H}(R)$ between real and not-real poles.

2. Show that the signature of $\mathcal{H}(R)$ equals the sum of the signature of its components.

3. Show that sum of the signature of those components is the Cauchy Index of R.

Let us first recall from theorem (1.3.3) that the rank of $\mathcal{H}(R)$ equals the number of poles of R, counted with multiplicity. That is, if $\mathfrak{p}$ and $\mathfrak{q}$ are coprime polynomials with $n = deg\ \mathfrak{p}$ such that $\mathfrak{q}/\mathfrak{p} = R$, then rank $\mathcal{H}(R) = n$. So the theorem claims that $I_R = \sigma(\mathcal{H}(R)_N)$ for all $N \geq n$. Because of the particular use we want to give to this theorem later on, it will suffice to show that $I_R = \sigma(\mathcal{H}(R)_n)$. For a more general proof see [8](II.11).

Step 1: partial fractions decomposition. In the partial fraction expansion of R (2.3) let us denote R_{ξ_j} the component of R that has a unique pole at ξ_j, so that

$$R(x) = \sum_{j=1}^{r+2s} R_{\xi_j}(x). \tag{2.7}$$

For constants λ_1, λ_2 and rational functions w_1, w_2 we have $\mathcal{H}(\lambda_1 w_1 + \lambda_2 w_2) =$

$\lambda_1\mathcal{H}(w_1)+\lambda_2\mathcal{H}(w_2)$ so the corresponding infinite Hankel form of R is the sum of the infinite Hankel forms of the $R'_{\xi_j}s$.

$$\mathcal{H}(R) \;=\; \sum_{j=1}^{r}\mathcal{H}(R_{\xi_j}) \;+\; \sum_{j=1}^{s}\Big[\mathcal{H}(R_{\xi_{r+j}})+\mathcal{H}(R_{\overline{\xi}_{r+j}})\Big] \tag{2.8}$$

This equality is on infinite matrices, so in particular it holds true if we truncate them at any point.

$$\mathcal{H}(R)_n \;=\; \sum_{j=1}^{r}\mathcal{H}(R_{\xi_j})_n \;+\; \sum_{j=1}^{s}\Big[\mathcal{H}(R_{\xi_{r+j}})_n+\mathcal{H}(R_{\overline{\xi}_{r+j}})_n\Big] \tag{2.9}$$

Step 2: signature stable by decomposition. Let us first note that the *rank* is stable by the previous decomposition. Theorem (1.3.3) applied to the right hand side of (2.9) says that each $\mathcal{H}(R_{\xi_j})_n$ has rank ν_j, and since the rank of $\mathcal{H}(R)_n$ is n, which is the sum of all the $\nu'_j s$, for that is the number of poles of R counted with multiplicity; we conclude that in this case, the rank of the sum of the quadratic forms equals the sum of the ranks of the component forms. We assert that when this is the case, the same relation holds for the signature. A proof of this can be found, for instance on [8](I 5.2) or [7](8.2). We therefore conclude that:

$$\sigma(\mathcal{H}(R)_n) \;=\; \sum_{j=1}^{r} \sigma(\mathcal{H}(R_{\xi_j})_n) \;+\; \sum_{j=1}^{s} \sigma\left(\mathcal{H}(R_{\xi_{r+j}})_n + \mathcal{H}(R_{\overline{\xi}_{r+j}})_n\right) \qquad (2.10)$$

Step 3: the sum of the signatures is the Cauchy index. In the real case, $R_{\xi_j} = \frac{A_1^{(j)}}{x-\xi_j} + \frac{A_2^{(j)}}{(x-\xi_j)^2} + ... + \frac{A_{\nu_j}^{(j)}}{(x-\xi_j)^{\nu_j}}$ has rank ν_j. In fact, the rank remains unchanged under any variation of the parameters $A_1^{(j)},\ A_2^{(j)},\ ...\ ,\ A_{\nu_j-1}^{(j)},\ \xi_j$, therefore so does the signature. In particular we may take $A_1^{(j)} = A_2^{(j)} = ... = A_{\nu_j-1}^{(j)} = \xi_j = 0$. Now the Hankel matrix $\mathcal{H}(R_{\xi_j})_n$ has zeros everywhere except in the positions where $i + j - 1 = \nu_j$. After diagonalization we see that this matrix has signature zero when ν_j is even and $\text{sign}(A_j^{\nu_j})$ when ν_j is odd.

In the complex case, after doing some algebra with complex forms we obtain that $\sigma\left(\mathcal{H}(R_{\xi_{r+j}})_n + \mathcal{H}(R_{\overline{\xi}_{r+j}})_n\right) = 0$.

Hence:

(i) Real case: $\sigma(\mathcal{H}(R_{\xi_j})_n) = \begin{cases} \text{sign}A_{\nu_j}^{(j)} & \nu_j \text{ odd} \\ 0 & \nu_j \text{ even} \end{cases}$

(ii) Complex case: $\sigma\left(\mathcal{H}(R_{\xi_{r+j}})_n + \mathcal{H}(R_{\overline{\xi}_{r+j}})_n\right) = 0$

Therefore, the signature of $\mathcal{H}(R)_n$ is

$$\sigma(\mathcal{H}(R)_n) = \sum_{\substack{1 \le j \le r \\ \nu_j \text{ odd}}} \text{sign}(A_{\nu_j}^{(j)})$$

which is the Cauchy index of R.

Chapter 3

p-adic Bezoutians

3.1 Quadratic forms over $\mathbb{Q}_p$

In this chapter we study quadratic forms over the p-adic field $K = \mathbb{Q}_p$ with special considerations of Bezoutians. For this part we refer to [1], [5], [9], [14], [18], and [21].

Two regular quadratic forms over $\mathbb{Q}_p$ are isometric if and only if they share the three invariants: rank, discriminant, and Hasse invariant, which we define next.

Let $\mathbb{Q}_p^*$ denote $\mathbb{Q}_p \setminus \{0\}$. For $a, b \in \mathbb{Q}_p^*$ the **Hilbert symbol** of a and b is

$$(a,b)_p := \begin{cases} 1 & \text{if } ax^2 + by^2 = z^2 \text{ has a nontrivial solution in } \mathbb{Q}_p \\ -1 & \text{otherwise} \end{cases} \tag{3.1}$$

It satisfies that if u and v are units in $\mathbb{Q}_p^*$ then

$$\begin{cases} (u,v)_p &= 1 \\ (pu,v)_p &= \left(\dfrac{v}{p}\right) \\ (pu,pv)_p &= (-1)^{\frac{p-1}{2}} \left(\dfrac{u}{p}\right)\left(\dfrac{v}{p}\right) \end{cases} \tag{3.2}$$

where $\left(\frac{\cdot}{p}\right)$ denotes the **Legendre symbol** of v. Let us briefly recall how the Legendre symbol works on $\mathbb{Z}_p^*$: if $v \in \mathbb{Z}_p^*$ and if $\pi : \mathbb{Z}_p^* \to \mathbb{F}_p^*$ is the usual projection from $\mathbb{Z}_p^*$ to $\mathbb{F}_p^*$, then the Legendre symbol of v is

$$\left(\frac{v}{p}\right) \;=\; \pi(v)^{\frac{p-1}{2}}.$$

Let V be a quadratic space with a representation $V \simeq \langle \lambda_1,\ ...,\ \lambda_n \rangle$. Then we define the **Hasse invariant** of V, denoted by $\sigma_p(V)$ or just σ_p to be:

$$\sigma_p := \prod_{i<j} (\lambda_i, \lambda_j)_p \tag{3.3}$$

It is not trivial that this number does not depend on the choice of diagonalization. For a proof see [23] (I.4.2).

We saw in the previous chapter that there are only two classes of isometry of regular quadratic forms of dimension one over $\mathbb{R}$, namely $\langle +1 \rangle$ and $\langle -1 \rangle$. The forms are given by the classes modulo square in $\mathbb{R}$. In $\mathbb{Q}_p$ there are four such classes: $1,\ \varepsilon,\ p,\ p\varepsilon$, where ε is some non-square unit in $\mathbb{Q}_p^*$. With a similar reasoning, the regular quadratic forms in $\mathbb{Q}_p$ will be represented by matrices of the form:

$$V \simeq \begin{pmatrix} 1 & & & & & & & & & & \\ & \ddots & & & & & & & & & \\ & & 1 & & & & & & & & \\ & & & \varepsilon & & & & & & & \\ & & & & \ddots & & & & & & \\ & & & & & \varepsilon & & & & & \\ & & & & & & p & & & & \\ & & & & & & & \ddots & & & \\ & & & & & & & & p & & \\ & & & & & & & & & p\varepsilon & \\ & & & & & & & & & & \ddots \\ & & & & & & & & & & & p\varepsilon \end{pmatrix}$$

In fact, for any given rank, there are only finitely many such forms.

3.2 Hasse Invariant

Let $u_1,\ ...,\ u_n$ be p-adic units and let V be the quadratic form given by

$$V \simeq p\langle u_1,\ ...,\ u_h\rangle \perp \langle u_{h+1},\ ...,\ u_n\rangle \tag{3.4}$$

We want to compute the Hasse invariant of V.

3.2.1 Some observations

1. For Hasse invariant matters we only care about the case when $n \geq 2$.
2. If $h = 0$ then $V = \langle u_1, u_2, ..., u_n\rangle$ and $\sigma_p = \prod_{1\leq i<j\leq n} (u_i, u_j) \ = \ 1$.
3. If $h = 1$ then $n - h \geq 1$ and $V = p\langle u_1\rangle \ \perp \ \langle u_2, ..., u_n\rangle$ and

$$\begin{aligned}
\sigma_p &= \prod_{j=2}^{n}(pu_1, u_j) \\
&= \prod_{j=2}^{n}\left(\frac{u_j}{p}\right) \\
&= \left(\frac{\prod_{j=2}^{n} u_j}{p}\right)
\end{aligned}$$

4. If $h = n$ then $V = p\langle u_1, ..., u_n\rangle$ and

$$\begin{aligned}
\sigma_p &= \prod_{1\le i<j\le n}(pu_i, pu_j) \\
&= \prod_{1\le i<j\le n}(-1)^{\frac{p-1}{2}}\left(\frac{u_i}{p}\right)\left(\frac{u_j}{p}\right) \\
&= (-1)^{\binom{n}{2}\frac{p-1}{2}}\left[\prod_{j=1}^{n}\left(\frac{u_j}{p}\right)\right]^{n-1} \\
&= (-1)^{\binom{n}{2}\frac{p-1}{2}}\left(\frac{\prod_{j=1}^{n} u_j}{p}\right)^{n-1}
\end{aligned}$$

Note that the power of $n-1$ in the last product comes from the fact that each of the $u_j s$ appears exactly $n-1$ times in the product, multiplying against each one of the other $n-1$ $u_j s$.

5. If $h = n-1$, $V = p\langle u_1, ..., u_{n-1}\rangle \perp \langle u_n\rangle$ and the Hasse invariant of V is

$$\begin{aligned}
\sigma_p &= \prod_{1\le i<j\le n-1}(pu_i, pu_j)\prod_{i=1}^{n-1}(pu_i, u_n) \\
&= (-1)^{\binom{n-1}{2}\frac{p-1}{2}}\left(\frac{\prod_{j=1}^{n-1}u_j}{p}\right)^{n-2}\prod_{i=1}^{n-1}\left(\frac{u_n}{p}\right) \\
&= (-1)^{\binom{n-1}{2}\frac{p-1}{2}}\left(\frac{\prod_{j=1}^{n-1}u_j}{p}\right)^{n-2}\left(\frac{u_n}{p}\right)^{n-1} \\
&= (-1)^{\binom{n-1}{2}\frac{p-1}{2}}\left(\frac{\prod_{j=1}^{n}u_j}{p}\right)^{n-2}\left(\frac{u_n}{p}\right)
\end{aligned}$$

3.2.2 Computation of the Hasse invariant of V

Having considered the cases above, now we assume $2 \leq h \leq n-2$: then $V = p\langle u_1,\ u_2,\ ...,\ u_h\rangle\ \perp\ \langle u_{h+1},\ u_{h+2},\ ...,\ u_n\rangle$ and lets call

$$\begin{cases} W := p\langle u_1,\ u_2,\ ...,\ u_h\rangle \\ U := \langle u_{h+1},\ u_{h+2},\ ...,\ u_n\rangle \end{cases}$$

so that the Hasse invariant of V is:

$$\sigma_p(V) \ = \ \sigma_p(W)\ \sigma_p(U) \prod_{\substack{1\leq i\leq h \\ h+1\leq j\leq n}} (pu_i, u_j)_p \tag{3.5}$$

The previous considerations apply here as well, therefore:

1. $\sigma_p(U) = 1$
2. $\sigma_p(W) = (-1)^{\binom{h}{2}\frac{p-1}{2}} \left(\dfrac{\prod_{j=1}^{h} u_j}{p} \right)^{h-1}$

$$3. \prod_{\substack{1\le i\le h\\ h+1\le j\le n}} (pu_i, u_j)_p = \prod_{i=1}^{h}\prod_{j=h+1}^{n} (pu_i, u_j)_p$$

$$= \prod_{i=1}^{h}\prod_{j=h+1}^{n} \left(\frac{u_j}{p}\right)$$

$$= \left[\prod_{j=h+1}^{n} \left(\frac{u_j}{p}\right)\right]^h$$

$$= \left(\frac{\prod_{j=h+1}^{n} u_j}{p}\right)^h$$

Therefore, the Hasse invariant of V is

$$\sigma_p(V) = \sigma_p(W) \prod_{i=1}^{h}\prod_{j=h+1}^{n} \sigma_p(\langle pu_i, u_j\rangle)$$

$$= (-1)^{\binom{h}{2}\frac{p-1}{2}} \left(\frac{\prod_{j=1}^{h} u_j}{p}\right)^{r-1} \left(\frac{\prod_{j=h+1}^{n} u_j}{p}\right)^h \tag{3.6}$$

i.e.:

$$\sigma_p \;=\; \begin{cases} (-1)^{\binom{h}{2}\frac{p-1}{2}} \left(\dfrac{\prod_{j=1}^{h} u_j}{p} \right) & h \text{ even} \\ (-1)^{\binom{h}{2}\frac{p-1}{2}} \left(\dfrac{\prod_{j=h+1}^{n} u_j}{p} \right) & h \text{ odd} \end{cases} \tag{3.7}$$

3.3 Bezoutian: separable case

In the case when $V = \mathcal{B}$ with $\mathfrak{p}$ and $\mathfrak{q}$ separable and with all their roots in $\mathbb{Q}_p$, we have the diagonalization $\mathcal{B} \simeq \langle \mathfrak{p}'(\xi_1)\mathfrak{q}(\xi_1),\ \ldots\ ,\ \mathfrak{p}'(\xi_n)\mathfrak{q}(\xi_n)\rangle$. Now for each $1 \leq i \leq n$ let ν_i be the p-adic valuation of $\mathfrak{p}'(\xi_i)\mathfrak{q}(\xi_i)$, i.e., write

$$\mathfrak{p}'(\xi_i)\mathfrak{q}(\xi_i) = p^{\nu_i} u_i \tag{3.8}$$

with u_i units. Let $h := \#\{i : \nu_i \text{ is odd}\}$ and lets reorder the roots of $\mathfrak{p}$ so that ν_i is odd for every $1 \leq i \leq h$. Now we brake $\mathfrak{p}$ into $\mathfrak{p}_1$ and $\mathfrak{p}_2$ as follows:

$$\mathfrak{p}_1(x) := \prod_{i=1}^{h}(x - \xi_i) \qquad \mathfrak{p}_1(x) := \prod_{i=h+1}^{n}(x - \xi_i)$$

In order to compute the Hasse invariant of $\mathcal{B}$, lets substitute $u_i = \mathfrak{p}'(\xi_i)\mathfrak{q}(\xi_i)p^{-\nu_i}$ in (3.7):

1. For h even:

$$\begin{aligned} \prod_{j=1}^{h} u_j &= \prod_{j=1}^{h} \mathfrak{p}'(\xi_j)\mathfrak{q}(\xi_j)p^{-\nu_j} \\ &= p^{-S_h} \prod_{j=1}^{h} \mathfrak{p}'(\xi_j)\ \mathfrak{q}(\xi_j) \\ &= p^{-S_h}\ Res(\mathfrak{p}_1, \mathfrak{p}'\mathfrak{q}) \end{aligned} \tag{3.9}$$

where $S_h = \sum_{j=1}^{h} \nu_j$

Remember that for $1 \leq j \leq h$ the $\nu_j' s$ are odd. So the parity of S_h will be that one of h. But we are in the case when h is even, hence S_h is even. Therefore, substituting everything back in (3.7) the Hasse invariant is:

$$\begin{aligned} \sigma_p &= (-1)^{\binom{h}{2}\frac{p-1}{2}} \left(\frac{p^{-S_h}\ Res(\mathfrak{p}_1, \mathfrak{p}'\mathfrak{q})}{p} \right) \\ &= (-1)^{\binom{h}{2}\frac{p-1}{2}} \left(\frac{Res(\mathfrak{p}_1, \mathfrak{p}'\mathfrak{q})}{p} \right) \end{aligned} \tag{3.10}$$

2. For h odd, a similar analysis leads to a similar formula.

$$\begin{aligned}\prod_{j=h+1}^{n} u_j &= \prod_{j=h+1}^{n} \mathfrak{p}'(\xi_j)\mathfrak{q}(\xi_j)p^{-\nu_j} \\ &= p^{-(S_n-S_h)} \prod_{j=h+1}^{n} \mathfrak{p}'(\xi_j)\ \mathfrak{q}(\xi_j) \\ &= p^{-(S_n-S_h)}\ Res(\mathfrak{p}_2, \mathfrak{p}'\mathfrak{q})\end{aligned} \tag{3.11}$$

Note that in this case, the exponent of p is $-(S_n - S_h)$ but it does not matter, because we are adding up the $\nu_j's$ with $h+1 \leq j \leq n$, that is, the even ones. Hence the exponent of p is even and the Hasse invariant is:

$$\begin{aligned}\sigma_p &= (-1)^{\binom{h}{2}\frac{p-1}{2}} \left(\frac{p^{-(S_n-S_h)}\ Res(\mathfrak{p}_2, \mathfrak{p}'\mathfrak{q})}{p}\right) \\ &= (-1)^{\binom{h}{2}\frac{p-1}{2}} \left(\frac{Res(\mathfrak{p}_2, \mathfrak{p}'\mathfrak{q})}{p}\right)\end{aligned} \tag{3.12}$$

so that for arbitrary h we have

$$\sigma_p = (-1)^{\binom{h}{2}\frac{p-1}{2}} \left(\frac{Res(\mathfrak{p}_1, \mathfrak{p}'\mathfrak{q})}{p}\right)^{h+1} \left(\frac{Res(\mathfrak{p}_2, \mathfrak{p}'\mathfrak{q})}{p}\right)^{h} \tag{3.13}$$

In this section we have proven the following theorem.

Theorem 3.3.1. *Let $\mathfrak{p}, \mathfrak{q} \in \mathbb{Q}_p[x]$ be coprime and separable, all their roots in $\mathbb{Q}_p$. Let $\xi_1, \cdots, \xi_n$ be the roots of $\mathfrak{p}$, and as usual $\mathcal{B} \simeq \langle \mathfrak{p}'(\xi_1)\mathfrak{q}(\xi_1), \cdots, \mathfrak{p}'(\xi_n)\mathfrak{q}(\xi_n)\rangle$. Let ν_i be the p-adic valuation of $\mathfrak{p}'(\xi_i)\mathfrak{q}(\xi_i)$, that is, we can write $\mathfrak{p}'(\xi_i)\mathfrak{q}(\xi_i) = p^{\nu_i}u_i$ with u_i units. Let $h := \#\{i : \nu_i \text{ is odd}\}$ & let us reorder if necessary so that ν_i is odd for every $1 \leq i \leq r$. Finally, let $\mathfrak{p}_1 := \prod_{i \leq h}(x - \xi_i)$ & $\mathfrak{p}_2 := \prod_{i>h}(x - \xi_i)$, so that $\mathfrak{p} = \mathfrak{p}_1\mathfrak{p}_2$. Then:*

$$\sigma_p \;=\; (-1)^{\binom{h}{2}\frac{p-1}{2}} \left(\frac{Res(\mathfrak{p}_1, \mathfrak{p}'\mathfrak{q})}{p}\right)^{h+1} \left(\frac{Res(\mathfrak{p}_2, \mathfrak{p}'\mathfrak{q})}{p}\right)^{h}$$

3.3.1 An Example

To see how this proposition is useful in practice, let us see an example an compare computing the Hasse invariant by definition and by this last formula.

$$\text{Let } \begin{cases} \mathfrak{p} &= (x+4)(x+2)\ x\ (x-2)(x-4) \\ \mathfrak{q} &= (x+5)(x+3)(x+1)(x-1)(x-3) \end{cases}$$

We need the diagonal of the Bezoutian. Both polynomials are separable, so we compute the trace:

$$\begin{cases} \mathfrak{p}'\mathfrak{q}(-4) &= 2^7 \times 3^2 \times 5 \times 7 &\equiv& 2 \times 5 \times 7 \\ \mathfrak{p}'\mathfrak{q}(-2) &= 2^5 \times 3^3 \times 5 &\equiv& 2 \times 3 \times 5 \\ \mathfrak{p}'\mathfrak{q}(0) &= 2^6 \times 3^2 \times 5 &\equiv& 5 \\ \mathfrak{p}'\mathfrak{q}(2) &= 2^5 \times 3^2 \times 5 \times 7 &\equiv& 2 \times 5 \times 7 \\ \mathfrak{p}'\mathfrak{q}(4) &= 2^7 \times 3^4 \times 5 \times 7 &\equiv& 2 \times 5 \times 7 \end{cases}$$

Cleaning up squares we obtain a diagonalization and the discriminant:

$$\mathcal{B} \simeq \langle 70,\ 30,\ 5,\ 70,\ 70\rangle \qquad \Delta = 3\times 5\times 7$$

Now for any prime p other than 3, 5, or 7, all the elements in the diagonal are units with respect to p, therefore the Hilbert symbols will be all one and the Hasse invariant with respect to p will be one. So we only care about 3, 5, and 7. Let us compute the Hasse invariant for $p = 7$.

Using the definition of the Hasse invariant:

$$\begin{aligned}
\sigma_7 &= (70,30)_7(70,5)_7(70,70)_7^2(30,5)_7(30,70)_7^2(5,70)_7^2(70,70)_7 \\
&= (70,30)_7(70,5)_7(30,5)_7(70,70)_7 \\
&= \left(\frac{30}{7}\right)\left(\frac{5}{7}\right)(-1)^{\frac{7-1}{2}}\left(\frac{10}{7}\right)\left(\frac{10}{7}\right) \\
&= \left(\frac{2}{7}\right)\left(\frac{5}{7}\right)(-1)^3 \\
&= 1\times(-1)\times(-1) \quad = \quad 1.
\end{aligned}$$

Using Theorem 3.3.1:

$$\mathcal{B} \simeq \langle \underbrace{70,\ 70,\ 70}_{h=3\ (\text{odd})},\ 30,\ 5\rangle \ \Rightarrow\ \sigma_p = (-1)^{\binom{3}{2}\frac{7-1}{2}}\left(\frac{30}{7}\right)\left(\frac{5}{7}\right)$$

So we clearly made an improvement in time, resources, and beauty.

3.4 The non-separable case

The previous section applies only when $\mathfrak{p}$ and $\mathfrak{q}$ are separable. Now what if that is not the case? Let $\mathfrak{p}$ and $\mathfrak{q}$ be two arbitrary monic polynomials,

$$\begin{aligned} \mathfrak{p}(x) &= \prod_{j=1}^{N}(x-\xi_j) \\ \mathfrak{q}(x) &= \prod_{j=1}^{M}(x-\zeta_j) \end{aligned} \tag{3.14}$$

and let us factor out their separable parts and their square parts. After re-ordering the indices:

$$\begin{aligned} \mathfrak{p}(x) &= \prod_{j=1}^{n}(x-\xi_j)\ \prod(x-\xi_j)^{2t_j} \\ \mathfrak{q}(x) &= \prod_{j=1}^{m}(x-\zeta_j)\ \prod(x-\zeta_j)^{2s_j} \end{aligned} \tag{3.15}$$

From this factorization, we want to isolate the separable parts. Say

$$\begin{aligned} \tilde{\mathfrak{p}}(x) &= \prod_{j=1}^{n}(x-\xi_j) \\ \tilde{\mathfrak{q}}(x) &= \prod_{j=1}^{m}(x-\zeta_j) \end{aligned} \tag{3.16}$$

and let us denote by $\mathcal{B}$ the Bezoutian induced by $\mathfrak{p}$ and $\mathfrak{q}$ and by $\tilde{\mathcal{B}}$ that one induced by $\tilde{\mathfrak{p}}$ and $\tilde{\mathfrak{q}}$.

The dimension of $\mathcal{B}$ depends on $\max\{N,\ M\}$ whereas the dimension of $\tilde{\mathcal{B}}$ depends on $\max\{n,\ m\}$. Since these two maximum need not be the same, there is no reason to expect for these two quadratic forms to be isometric. Even if the dimension were the same, that is not our point. We claim that, even though $\mathcal{B}$ and $\tilde{\mathcal{B}}$ might not be isometric, they are in fact Witt equivalent, that is, they are isometric except for hyperbolic planes. More precisely, we formulate the following conjecture.

Conjecture. Let $\mathfrak{p}, \mathfrak{q}, \mathfrak{r} \in \mathbb{Q}_p[x]$ be such that:

- $\mathfrak{p}$ and $\mathfrak{q}$ are separable with all their roots in $\mathbb{Q}_p$.
- $\gcd(\mathfrak{p} : \mathfrak{q}) = \gcd(\mathfrak{p} : \mathfrak{r}) = \gcd(\mathfrak{q} : \mathfrak{r}) = 1$
- $n := \deg \mathfrak{p} \geq \deg \mathfrak{q}$
- $r := \deg \mathfrak{r}$

Then the Bezoutian of $\mathfrak{p}$ and $\mathfrak{q}$ is Witt equivalent to that one of $\mathfrak{p}\mathfrak{r}^2$ and $\mathfrak{q}$, more precisely:

$$\mathcal{B}(\mathfrak{p}\mathfrak{r}^2, \mathfrak{q}) \ \simeq \ \mathcal{B}(\mathfrak{p}, \mathfrak{q}) \perp \mathbb{H}^h \tag{3.17}$$

Furthermore, we conjecture that this is indeed the case for any field K, not just $\mathbb{Q}_p$. That is the subject of the next and last chapter.

Chapter 4

A Conjecture and a Theorem

We now consider the question brought up at the end of last chapter: what happens with the Bezoutian when $\mathfrak{p}$ or $\mathfrak{q}$ is not separable? Of special interest is the case when $\mathfrak{p}$, the leading polynomial, is not separable. A first approach to the problem is to assume that the separable part of $\mathfrak{p}$ is still of degree higher or equal than $\mathfrak{q}$ and see what happens then. We conjecture that in that case we can forget about the squares that make $\mathfrak{p}$ not separable, modulo Witt equivalence.

Conjecture.

Let $\mathfrak{p}, \mathfrak{q}, \mathfrak{r} \in K[x]$ be such that:

- $\mathfrak{p}$ and $\mathfrak{q}$ are separable with all their roots in K.
- $\gcd(\mathfrak{p} : \mathfrak{q}) = \gcd(\mathfrak{p} : \mathfrak{r}) = \gcd(\mathfrak{q} : \mathfrak{r}) = 1$.
- $n := \deg \mathfrak{p} \geq \deg \mathfrak{q}$.
- $r := \deg \mathfrak{r}$.

Then the Bezoutian of $\mathfrak{p}$ and $\mathfrak{q}$ is Witt-equivalent to that one of $\mathfrak{p}\mathfrak{r}^2$ and $\mathfrak{q}$, furthermore:

$$\mathcal{B}(\mathfrak{p}\mathfrak{r}^2, \mathfrak{q}) \simeq \mathcal{B}(\mathfrak{p}, \mathfrak{q}) \perp \mathbb{H}^r \tag{4.1}$$

There is no one unique set of invariants that classify the *isometry* classes of quadratic forms for all fields K (with $\mathrm{ch}(K) \neq 2$). [6] There are however a few invariants of most fields, such as dimension and discriminant, that we can easily check.

Dimension

The dimension is clearly the same in both sides of (4.1) since we chose r exactly for this purpose.

Discriminant

Let us first compute the determinants.

(i)Determinant of $\mathcal{B}(\mathfrak{p}\mathfrak{r}^2, \mathfrak{q})$

$$\begin{aligned} \det(\mathcal{B}[\mathfrak{p}\mathfrak{r}^2, \mathfrak{q}]) &= (-1)^{[(n+2r)(n+2r+1)]/2}\, Res(\mathfrak{p}\mathfrak{r}^2, \mathfrak{q}) \\ &= (-1)^{(n^2+n+2r)/2}\, Res(\mathfrak{p}, \mathfrak{q}) Res(\mathfrak{r}, \mathfrak{q})^2 \end{aligned}$$

(Ii) Determinant of $\mathcal{B}(\mathfrak{p}, \mathfrak{q}) \perp \mathbb{H}^r$

$$\begin{aligned} \det(\mathcal{B}[\mathfrak{p}, \mathfrak{q}] \perp \mathbb{H}^r) &= (-1)^{[n(n+1)]/2}\, Res(\mathfrak{p}, \mathfrak{q})(-1)^r \\ &= (-1)^{(n^2+n+2r)/2}\, Res(\mathfrak{p}, \mathfrak{q}) \end{aligned}$$

Since both determinants only differ by a square, the discriminants are the same, regardless of the field K.

In this chapter we offer a proof of the conjecture for the case $K = \mathbb{R}$, a code that has found no counterexample in the case $K = \mathbb{Q}$, and a theorem that we think will help prove this conjecture for the general case in the future.

4.1 Proof for $K = \mathbb{R}$

The only invariant still to check is the signature. Here we use the Hermite-Hurwitz theorem and the fact that hyperbolic planes have zero signature:

1) $\sigma(\mathcal{B}(\mathfrak{p}\mathfrak{r}^2, \mathfrak{q}) = I(\mathfrak{q}/(\mathfrak{p}\mathfrak{r}^2))$

2) $\sigma(\mathcal{B}(\mathfrak{p}, \mathfrak{q}) \perp \mathbb{H}^r) = \sigma(\mathcal{B}(\mathfrak{p}, \mathfrak{q})) + \sigma(\mathbb{H}^r) = I(\mathfrak{q}/\mathfrak{p})$

So all we have to prove is that $I(\mathfrak{q}/(\mathfrak{p}\mathfrak{r}^2)) = I(\mathfrak{q}/\mathfrak{p})$. Recall from (2.3.1) that the local Cauchy index of a rational function $\mathfrak{q}/\mathfrak{p}$ is zero at the complex (not real) poles, and at any real pole ξ it satisfies that:

$$I_{\mathfrak{q}/\mathfrak{p}}(\xi) = \begin{cases} +1 & \text{if} \quad \lim\limits_{x\to\xi^-} \dfrac{\mathfrak{q}}{\mathfrak{p}}(x) = -\infty \quad \& \quad \lim\limits_{x\to\xi^+} \dfrac{\mathfrak{q}}{\mathfrak{p}}(x) = +\infty \\ -1 & \text{if} \quad \lim\limits_{x\to\xi^-} \dfrac{\mathfrak{q}}{\mathfrak{p}}(x) = +\infty \quad \& \quad \lim\limits_{x\to\xi^+} \dfrac{\mathfrak{q}}{\mathfrak{p}}(x) = -\infty \\ 0 & \text{otherwise} \end{cases}$$

Note that none of these limits change if we modify our function by multiplication with a square, namely $1/\mathfrak{r}^2(x)$. Therefore:

$$I_{\mathfrak{q}/(\mathfrak{p}\mathfrak{r}^2)} \;=\; I_{\mathfrak{q}/\mathfrak{p}}(\xi) \qquad (\forall\ \xi \in Z_{\mathfrak{p}} \cap \mathbb{R}) \tag{4.2}$$

Now for the rest of the real poles of $\mathfrak{q}/(\mathfrak{p}\mathfrak{r}^2)$, that is, the real zeros of $\mathfrak{r}$, the following holds:

$$\begin{aligned}
\lim_{x\to\xi} \frac{\mathfrak{q}}{\mathfrak{p}\mathfrak{r}^2}(x) &= \frac{\mathfrak{q}(\xi)}{\mathfrak{p}(\xi)} \lim_{x\to\xi} \frac{1}{\mathfrak{r}^2}(x) \\
&= \begin{cases} +\infty & \text{if } \dfrac{\mathfrak{q}(\xi)}{\mathfrak{p}(\xi)} > 0 \\ -\infty & \text{if } \dfrac{\mathfrak{q}(\xi)}{\mathfrak{p}(\xi)} < 0 \end{cases}
\end{aligned}$$

and this limit is the same at both sides of ξ, therefore:

$$I_{\mathfrak{q}/(\mathfrak{p}\mathfrak{r}^2)}(\xi) \;=\; 0 \qquad (\forall\ \xi \in Z_{\mathfrak{r}} \cap \mathbb{R}) \tag{4.3}$$

Since the Cauchy index of $\mathfrak{q}/(\mathfrak{p}\mathfrak{r}^2)$ is the sum of the local Cauchy indexes over the real zeros of $\mathfrak{p}$ and those of $\mathfrak{r}$, we have just proven that

$$I(\mathfrak{q}/(\mathfrak{p}\mathfrak{r}^2)) = I(\mathfrak{q}/\mathfrak{p})$$

as we wished. □

4.2 Code for $K = \mathbb{Q}$

In the case $K = \mathbb{Q}$, Hasse-Minkowski's theorem tells us that it is necessary and sufficient that isometry holds in $\mathbb{Q}_p$ for every prime p and in $\mathbb{R}$. The

case $K = \mathbb{R}$ has just been proven, so we now need to focus on the p-adic fields $K = \mathbb{Q}_p$. Here the invariants are rank, discriminant, and Hasse invariant. Again, the only invariant we still need to check is the Hasse invariant.

Next we offer a code in Pari that checks the p-adic invariants, for each p dividing the discriminant, in random examples. The idea is that if we find a *counterexample* to (4.1) then the conjecture would be false. But there is none so far. About codes in Pari see [20].

The way this code works is as follows.

1. First we compute the Hasse invariant of a *diagonal* quadratic form `Q` for a prime p.

2. Next we compute the Bezoutian of two polynomials f and g.

3. Now we need to diagonalize the previous Bezoutian. Here we output the diagonal as a vector.

4. We create a vector of ones and minus ones that is the diagonal of the hyperbolic matrix of dimension twice the degree of $\mathfrak{r}$. (For technical reasons that dimension is m in the code and not r).

5. We only need to compute the Hasse invariant for the primes dividing the discriminant of the Bezoutian. Here we define three local variables:

   (a) w is the determinant of the Bezoutian, factored, and with negative sign. We include the negative sign to make sure that we check the

prime at infinity together with the finite primes. The format of w is that of a 2-column matrix, the first column having the primes that divide the determinant of $\mathcal{B}$, the second column having the power of those primes in $\mathcal{B}$. It would suffice to check for the primes with odd powers, but we check them all.

(b) B is the diagonal of $\mathcal{B}(f, g) \perp \mathbb{H}^r$.

(c) C is the diagonal of $\mathcal{B}(fr^2, g)$.

Next we produce a matrix showing in each row the Hasse invariant of B and of C for a particular prime, for example:

$$\begin{pmatrix} \sigma(B) & \sigma(C) & -1 \\ \sigma_2(B) & \sigma_2(C) & 2 \\ \sigma_5(B) & \sigma_5(C) & 5 \\ \sigma_{11}(B) & \sigma_{11}(C) & 11 \\ \sigma_{19}(B) & \sigma_{19}(C) & 19 \end{pmatrix}$$

which in practice looks like something of the form:

```
1   1   -1
-1  -1   2
1   1    5
1   1    11
-1  -1   19
```

The purpose of this code is that if you ever find a matrix where in the same row the first two entries are not the same, then if the conditions

for the polynomials are satisfied, you have found a counterexample to the conjecture. Such counterexample has not been found yet.

6. Now we need to generate random polynomials to test as many examples as possible.

7. Finally we do the testing. The output is a matrix as showed in (5) and the random polynomials generated in (6) that were used, so that if there is the appearance of a counterexample, we can check the conditions on the polynomials. Here is the code.

```
\\-------------------------------------------------------------
\\ Given three polynomials f,g,r; check if the Bezoutians
\\ bez(f,g) and  bez(f*r^2,g) are Witt equivalent.
\\-------------------------------------------------------------
\\
\\ 1. Hasse invariant of a quadratic form Q of dimension n for
\\ a prime p.

s(Q,p)=
{
      local(l);

      l=#Q;  \\  dimension of Q
```

```
      prod(i=1,l-1,
          prod(j=i+1,l,
      hilbert(Q[i],Q[j],p)));
}
\\-----------------------------------------------------------------
\\ 2. Bezoutian of two polynomials f, g.

bez(f,g)=
{
       local(h,n);

       h=(f*subst(g,x,y)-g*subst(f,x,y))/(y-x);
       n=max(poldegree(f),poldegree(g));
       matrix(n,n,j,k,polcoeff(polcoeff(h,j-1,x),k-1,y))
}
\\-----------------------------------------------------------------
\\ 3. Diagonal of the reduced form of the Bezoutian.

dbez(f,g)=
{
      vector(#bez(f,g),i,qfgaussred(bez(f,g))[i,i]);
}
\\-----------------------------------------------------------------
```

```
\\ 4. Diagonal of the hyperbolic matrix as a function
\\ of the  dimension 2m.

dhyperb(m)=
{
      vector(2*m,i,(-1)^(i+1));
}
\\----------------------------------------------------------------
\\ 5.  Primes dividing the discriminant of bez(f,g).

check(f,g,r)=
{
      local(w,B,C);

      w = factor(-abs(matdet(bez(f,g))));
      B = concat(dbez(f,g),dhyperb(poldegree(r)));
      C = dbez(f,g*r^2);

      print(issquare(prod(i=1,length(B),B[i]/C[i])));

      for(i=1,matsize(w)[1],w[i,1];print(s(B,w[i,1])," ",
           s(C,w[i,1])," ",w[i,1]));
}
```

```
\\-----------------------------------------------------------------
\\ 6. Random polynomials.

fu(d,c)=
{
      vector(d,i,random(c)-c\2); \\ d=degree, c=coefficients
}
\\-----------------------------------------------------------------
\\ 7. Testing with random polynomials, as function of the
\\ degree and the range of the coefficients.

test(d,c)=
{
      local(p,q,r);

      p=Pol(fu(d,c),x);
      q=Pol(fu(d,c),x);
      r=Pol(fu(d,c),x);

print(p);print(q);print(r);
check(p,q,r)
}
\\-----------------------------------------------------------------
```

4.3 The Theorem

Theorem 4.3.1. *Let* $\mathfrak{p},\ \mathfrak{q}$, *in* $K[x]$ *be two polynomials such that*

- $n := deg\ \mathfrak{p}\ \geq deg\ \mathfrak{q}$.
- $(\mathfrak{p} : \mathfrak{q}) = 1$.
- $\mathfrak{p} = \mathfrak{p}_1 ... \mathfrak{p}_m$ *with* $\mathfrak{p}_i$ *pairwise coprime.*
- $\dfrac{\mathfrak{q}}{\mathfrak{p}} = \dfrac{\mathfrak{q}_1}{\mathfrak{p}_1} + ... + \dfrac{\mathfrak{q}_m}{\mathfrak{p}_m}$ *(partial fractions).*

Let $V_{\mathfrak{q}/\mathfrak{p}}$ *be the quadratic space induced by the residue map associated to the rational function* $\mathfrak{q}/\mathfrak{p}$, *that is* $V_{\mathfrak{q}/\mathfrak{p}} = (K[x]/\mathfrak{p},\ \mathcal{R}_{\mathfrak{q}/\mathfrak{p}})$. *Then:*

$$V_{\mathfrak{q}/\mathfrak{p}}\ \simeq\ V_{\mathfrak{q}_1/\mathfrak{p}_1} \perp ... \perp V_{\mathfrak{q}_m/\mathfrak{p}_m}. \tag{4.4}$$

where $V_{\mathfrak{q}_i/\mathfrak{p}_i} = (K[x]/\mathfrak{p}_i,\ \mathcal{R}_{\mathfrak{q}_i/\mathfrak{p}_i})$ *are the subspaces correspondent from the partial fraction decomposition with the quadratic form being the one induced by the residue form associated to the rational function* $\mathfrak{q}_i/\mathfrak{p}_i$.

Lemma 4.3.2. *If* $\mathfrak{q}(\xi) \neq 0$ *and deg* $\mathfrak{q} \leq 2r$ *then*

$$V_{\mathfrak{q}/(x-\xi)^{2r}} \simeq \mathbb{H}^r \tag{4.5}$$

Lemma 4.3.3. *If* $\mathfrak{q}(\xi) \neq 0$ *and deg* $\mathfrak{q} \leq 2r+1$ *then there exists* λ *in* K^* *such that*

$$V_{\mathfrak{q}/(x-\xi)^{2r+1}} \simeq \mathbb{H}^r \perp \langle \lambda \rangle \tag{4.6}$$

Proof of the theorem.

In order to prove this we need to check two things: (1) the right hand side is well defined, i.e. the subspaces are orthogonal; (2) both sides are indeed isometric.

1. Orthogonality: we want to see that given $\alpha, \beta \in K[x]/\mathfrak{p}$ such that $\alpha \in K[x]/\mathfrak{p}_i$ and $\beta \in K[x]/\mathfrak{p}_j$ their inner product (in V) is zero. $(i \neq j)$

Assume $\mathfrak{p} = \mathfrak{p}_1 \ldots \mathfrak{p}_m$ with $(\mathfrak{p}_i : \mathfrak{p}_j) = 1$ for $i \neq j$ and define the polynomials

$$\check{\mathfrak{p}}_i := \prod_{j \neq i} \mathfrak{p}_j$$

Then $\check{\mathfrak{p}}_i' s$ are coprime as well, with Bezout coefficients μ_i, that is:

$$1 = \mu_1 \check{\mathfrak{p}}_1 + \ldots + \mu_m \check{\mathfrak{p}}_m \tag{4.7}$$

therefore every element $\alpha \in K[x]/\mathfrak{p}$ has an expression of the form

$$\alpha = \alpha_1 \check{\mathfrak{p}}_1 + \ldots + \alpha_m \check{\mathfrak{p}}_m \tag{4.8}$$

Now let us focus on $\mathfrak{p}_1$ for clarity: the only $\check{q}_i$ not divisible by $\mathfrak{p}_1$ is $\check{q}_1$. So if α were an element of the *subspace* $K[x]/\mathfrak{p}_1$, it would necessarily be $\alpha_2 = \cdots = \alpha_m = 0$, that is, in general:

$$K[x]/\mathfrak{p}_i \ \subseteq \ \langle \check{\mathfrak{p}}_i \rangle \tag{4.9}$$

Now in order to establish that $V_i \perp V_j$ for $i \neq j$ let us take $\alpha, \beta \in K[x]$ such that

$$\begin{cases} \alpha \in K[x]/\mathfrak{p}_i & \text{i.e.} \quad \alpha \in \langle \check{\mathfrak{p}}_i \rangle \\ \beta \in K[x]/\mathfrak{p}_j & \text{i.e.} \quad \beta \in \langle \check{\mathfrak{p}}_j \rangle. \end{cases}$$

We want to see that their inner product in $K[x]/\mathfrak{p}$ is zero, but this is now rather clear, since:

$$\begin{aligned} \langle \alpha, \beta \rangle_V &:= \sum_{\xi \in Z(\mathfrak{p})} \mathcal{R}es_\xi(\alpha\beta w \ dt) \\ &= \sum_{\xi \in Z(\mathfrak{p})} \mathcal{R}es_\xi \left(\frac{(\tilde{\alpha}\check{\mathfrak{p}}_i)(\tilde{\beta}\check{\mathfrak{p}}_j)\mathfrak{q}}{\mathfrak{p}} \ dt \right) \\ &= \sum_{\xi \in Z(\mathfrak{p})} \mathcal{R}es_\xi \left((\tilde{\alpha}\tilde{\beta})\mathfrak{q}\frac{\check{\mathfrak{p}}_i\check{\mathfrak{p}}_j}{\mathfrak{p}} \ dt \right) \end{aligned}$$

and each of the terms in this sum is zero, since the product $\check{\mathfrak{p}}_i\check{\mathfrak{p}}_j$ is divisible by $\mathfrak{p}$.

2. Isometry: now that we know that $\perp_{1 \leq i \leq m} V_i$ is well defined, we want to see that it is isometric to V. That the underlying vector spaces are isomorphic is given by the Chinese Reminder Theorem. We still need to check that this

isometry respects the bilinear form of the spaces. That is, we need to see that for any $\alpha, \beta \in K[x]/\mathfrak{p}$ the following holds:

$$\langle \alpha, \beta \rangle_V \;=\; \langle \sigma(\alpha), \sigma(\beta) \rangle_{\perp V_i} \tag{4.10}$$

$$\text{where} \begin{cases} \sigma(\alpha) := \sigma_1(\alpha) \times ... \times \sigma_m(\alpha) \\ \quad \text{is the isometry given by the Chinese Reminder Theorem.} \\ \\ \langle \sigma(\alpha), \sigma(\beta) \rangle_{\perp V_i} := \sum_i \langle \sigma_i(\alpha), \sigma_i(\beta) \rangle_{V_i} \end{cases}$$

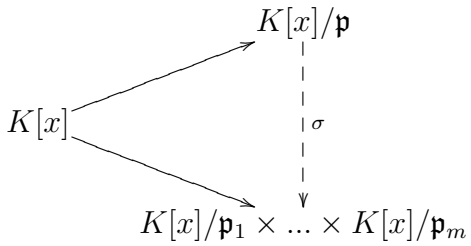
For $f, g \in K[x]/\mathfrak{p}_i$ the inner product on V_i is

$$\langle f, g \rangle_{V_i} \;=\; \sum_{\xi \in Z(\mathfrak{p}_i)} \mathcal{R}es_\xi(fgw_i \; dt) \tag{4.11}$$

where $w_i = \dfrac{\mathfrak{q}_i}{\mathfrak{p}_i}$ and $\mathfrak{q}_i$ is defined as the reminder of dividing $\mathfrak{q}\check{\mathfrak{p}}_i\mu_i^2$ by $\mathfrak{p}_i$, that is,

$$\mathfrak{q}_i \equiv \mathfrak{q}\check{\mathfrak{p}}_i\mu_i^2 \pmod{\mathfrak{p}_i}$$

By the Chinese Reminder Theorem (modulo quotients) the following diagram is commutative:



where σ and its inverse τ are constructed as follows. Let us start with τ:

$$\begin{array}{ccc} K[x]/\mathfrak{p}_1 \times ... \times K[x]/\mathfrak{p}_m & \xrightarrow{\tau} & K[x]/\mathfrak{p} \\ (\alpha_1, ..., \alpha_m) & \mapsto & \alpha \end{array}$$

so α must be a simultaneous solution to the system of equations $x \equiv \alpha_i \pmod{\mathfrak{p}_i}$. Let us construct this solution: $(\mathfrak{p}_i : \check{\mathfrak{p}}_i) = 1 \Rightarrow \exists$ Bezout coefficients λ_i, μ_i such that

$$\lambda_i \mathfrak{p}_i \ + \mu_i \check{\mathfrak{p}}_i \ = \ 1 \tag{4.12}$$

Define $e_i := \mu_i \check{\mathfrak{p}}_i$, then by (4.12) e_i satisfies

$$\begin{cases} e_i \ \equiv \ 1 \pmod{q_i} \\ e_i \ \equiv \ 0 \pmod{q_j} \quad (\forall \ j \neq i) \end{cases}$$

Now define

$$\alpha := \sum_i \alpha_i e_i$$

Clearly α satisfies that $\mathfrak{q}_i(\alpha) = \alpha_i$ for each i.

Note also that $\sum_i e_i \equiv 1 \pmod{\mathfrak{p}_j}$ for all j, therefore $\pmod{\mathfrak{p}}$, that is to say that in $K[x]/\mathfrak{p}$ the following holds:

$$1 = \mu_1 \check{\mathfrak{p}}_1 + ... + \mu_m \check{\mathfrak{p}}_m$$

and therefore, every $\alpha \in K[x]/\mathfrak{p}$ can be written as

$$\alpha = \alpha_1 \check{\mathfrak{p}}_1 + ... + \alpha_m \check{\mathfrak{p}}_m$$

with $\alpha_i = \alpha\mu_i$.

To summarize, the isomorphism is:

$$\begin{array}{ccc} K[x]/\mathfrak{p} & \longleftrightarrow & K[x]/\mathfrak{p}_1 \times ... \times K[x]/\mathfrak{p}_m \\ \\ \alpha & \overset{\sigma}{\rightarrowtail} & (\alpha \bmod \mathfrak{p}_1,\ ...\ , \alpha \bmod \mathfrak{p}_m) \\ \sum_i \alpha_i e_i & \overset{\tau}{\leftarrowtail} & (\alpha_1,\ ...\ \alpha_m) \end{array}$$

Now we are ready to check (4.10). Let $\alpha, \beta \in \perp_i V_i$, so that

$$\begin{cases} \alpha = (\alpha_1, ..., \alpha_m) \\ \\ \beta = (\beta_1, ..., \beta_m) \end{cases}$$

$$\begin{aligned}
\langle \alpha, \beta \rangle_{\perp_{V_i}} &= \sum_i \sum_{\xi \in Z(\mathfrak{p}_i)} \langle \alpha_i, \beta_i \rangle_{V_i} \\
&= \sum_i \sum_{\xi \in Z(\mathfrak{p}_i)} \mathcal{R}es_\xi \left(\alpha_i \beta_i w_i \ dt \right) \\
&= \sum_{\xi \in Z(\mathfrak{p})} \mathcal{R}es_\xi \left(\sum_i \alpha_i \beta_i \frac{\mathfrak{q}_i}{\mathfrak{p}_i} \ dt \right) \\
&= \sum_{\xi \in Z(\mathfrak{p})} \mathcal{R}es_\xi \left(\frac{\alpha_1 \beta_1 \mathfrak{q}_1 \check{\mathfrak{p}}_1 + ... + \alpha_m \beta_m \mathfrak{q}_m \check{\mathfrak{p}}_m}{\mathfrak{p}} \ dt \right) \\
&= \sum_{\xi \in Z(\mathfrak{p})} \mathcal{R}es_\xi \left(\mathfrak{q} \ \frac{\alpha_1 \beta_1 \mu_1^2 \check{\mathfrak{p}}_1^2 + ... + \alpha_m \beta_m \mu_m^2 \check{\mathfrak{p}}_m^2}{\mathfrak{p}} \ dt \right) \\
&= \sum_{\xi \in Z(\mathfrak{p})} \mathcal{R}es_\xi \left(\mathfrak{q} \ \frac{(\alpha_1 e_1)(\beta_1 e_1) + ... + (\alpha_m e_m)(\beta_m e_m)}{\mathfrak{p}} dt \right) \\
&= \sum_{\xi \in Z(\mathfrak{p})} \mathcal{R}es_\xi \left(\sum_i (\alpha_i e_i)(\beta_i e_i) \frac{\mathfrak{q}}{\mathfrak{p}} \ dt \right) \\
&= \sum_{\xi \in Z(\mathfrak{p})} \mathcal{R}es_\xi \left(\alpha \beta \frac{\mathfrak{q}}{\mathfrak{p}} \ dt \right)
\end{aligned}$$

Note that the last equality holds because all the terms that are missing in the sum are multiples of $\mathfrak{p}$, that is:

$$\begin{aligned}\alpha\beta &= \sum_i \alpha_i e_i \sum_i \beta_i e_i \\ &= \sum_i (\alpha_i e_i)(\beta_i e_i) \; + \; \sum_{i\neq j} (\alpha_i e_i)(\beta_j e_j)\end{aligned}$$

and $e_i e_j = \mu_i \mu_j \check{\mathfrak{p}}_i \check{\mathfrak{p}}_j$ is divisible by $\mathfrak{p}$ (when $i \neq j$).

This proves isometry and concludes the proof of the theorem. □

Proof of Lemma 1.

Here we are in the case when $\mathfrak{p} = (x-\xi)^n$ with $n = 2r$. Without loss of generality we may assume $\xi = 0$

and let $\mathfrak{q} = a_0 + a_1 x + ... + a_{n-1} x^{n-1}$, so that

$$w = \frac{a_0 + a_1 x + ... + a_{n-1} x^{n-1}}{x^n}$$

We need the residue form correspondent to this rational function. For this we choose the standard basis $\{1, x, \cdots, x^{n-1}\}$ and compute the inner products $\langle x^i, x^j \rangle_w$ for $0 \leq i, j \leq n-1$. There is only one zero ($\xi = 0$) so the global residue is the same as the local one:

$$\begin{aligned}\langle x^i, x^j \rangle_w &= \mathcal{R}es_{x=0} \left(x^{i+j} \; w(x) \; dx \right) \\ &= \mathcal{R}es_{x=0} \left(\tfrac{a_0 + a_1 x + ... + a_{n-1} x^{n-1}}{x^{n-(i+j)}} \; dx \right) \\ &= \begin{cases} a_{n-(i+j)-1} & i+j < n \\ 0 & i+j \geq n \end{cases}\end{aligned}$$

So the matrix of the inner product in this basis is the following Hankel matrix:

$$\begin{pmatrix} a_{n-1} & a_{n-2} & a_{n-3} & \dots & a_0 \\ a_{n-2} & a_{n-3} & a_{n-4} & & 0 \\ a_{n-3} & a_{n-4} & & & \\ \vdots & & & & \\ a_0 & 0 & & & 0 \end{pmatrix}$$

This matrix has the shape $\begin{pmatrix} D & C \\ C^t & 0 \end{pmatrix}$ with $\det(C) = \mathfrak{q}_m a_0^{n/2} \neq 0$, therefore the correspondent quadratic space is hyperbolic ([22]1.4 Thm 4.5)

We include an explicit diagonalization of this quadratic form. Special thanks to professor John H. Conway for sharing the following simple diagonalization technique at the Arizona Winter School 2009.

Start with $n = 2$:

$$\begin{array}{c|c|c} & \begin{pmatrix} a_1 & a_0 \\ a_0 & 0 \end{pmatrix} & \\ \hline R_1 - R_2 \frac{a_1}{2a_0} & \begin{pmatrix} \frac{a_1}{2} & a_0 \\ a_0 & 0 \end{pmatrix} & C_1 - C_2 \frac{a_1}{2a_0} \\ \hline & & \begin{pmatrix} 0 & a_0 \\ a_0 & 0 \end{pmatrix} \end{array}$$

Finally:

$$\begin{pmatrix} -1/(2a_0) & -1 \\ -1/(2a_0) & 1 \end{pmatrix} \begin{pmatrix} 0 & a_0 \\ a_0 & 0 \end{pmatrix} \begin{pmatrix} -1/(2a_0) & -1/(2a_0) \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

For $n = 4$:

	$\begin{pmatrix} a_3 & a_2 & a_1 & a_0 \\ a_2 & a_1 & a_0 & 0 \\ a_1 & a_0 & 0 & 0 \\ a_0 & 0 & 0 & 0 \end{pmatrix}$	
$R_1 - R_4 \frac{a_3}{2a_0}$	$\begin{pmatrix} a_3/2 & a_2 & a_1 & a_0 \\ a_2 & a_1 & a_0 & 0 \\ a_1 & a_0 & 0 & 0 \\ a_0 & 0 & 0 & 0 \end{pmatrix}$	$C_1 - C_4 \frac{a_3}{2a_0}$
		$\begin{pmatrix} 0 & a_2 & a_1 & a_0 \\ a_2 & a_1 & a_0 & 0 \\ a_1 & a_0 & 0 & 0 \\ a_0 & 0 & 0 & 0 \end{pmatrix}$

Next:

	$\begin{pmatrix} 0 & a_2 & a_1 & a_0 \\ a_2 & a_1 & a_0 & 0 \\ a_1 & a_0 & 0 & 0 \\ a_0 & 0 & 0 & 0 \end{pmatrix}$	
$R_2 - R_4 \frac{a_2}{a_0}$ $R_3 - R_4 \frac{a_1}{a_0}$	$\begin{pmatrix} 0 & a_2 & a_1 & a_0 \\ 0 & a_1 & a_0 & 0 \\ 0 & a_0 & 0 & 0 \\ a_0 & 0 & 0 & 0 \end{pmatrix}$	$C_2 - C_4 \frac{a_2}{a_0}$ $C_3 - C_4 \frac{a_1}{a_0}$
		$\begin{pmatrix} 0 & 0 & 0 & a_0 \\ 0 & a_1 & a_0 & 0 \\ 0 & a_0 & 0 & 0 \\ a_0 & 0 & 0 & 0 \end{pmatrix}$

Which brings us back to the case $n = 2$. Again finally:

$$\begin{pmatrix} \frac{-1}{2a_0} & 0 & -1 & 0 \\ 0 & \frac{-1}{2a_0} & 0 & -1 \\ \frac{-1}{2a_0} & 0 & 1 & 0 \\ 0 & \frac{-1}{2a_0} & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & a_0 \\ 0 & 0 & a_0 & 0 \\ 0 & a_0 & 0 & 0 \\ a_0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} \frac{-1}{2a_0} & 0 & \frac{-1}{2a_0} & 0 \\ 0 & \frac{-1}{2a_0} & 0 & \frac{-1}{2a_0} \\ -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix}$$

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

In general, if I is the $r \times r$ identity matrix and C is the $r \times r$ matrix of the shape $\begin{pmatrix} 0 & \dots & a_0 \\ \vdots & & \vdots \\ a_0 & \dots & 0 \end{pmatrix}$, then:

$$\begin{pmatrix} -1/(2a_0)\ I & -I \\ -1/(2a_0)\ I & I \end{pmatrix} \begin{pmatrix} 0 & C \\ C & 0 \end{pmatrix} \begin{pmatrix} -1/(2a_0)\ I & -1/(2a_0)\ I \\ -I & I \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & -I \end{pmatrix}$$

Which concludes the proof of Lemma 1. □

Proof of Lemma 2.

Using the same diagonalization method as before, (except for the final step), gives us the following quadratic form:

$$(x_1, ..., x_n) \begin{pmatrix} 0 & \dots & a_0 \\ \vdots & & \vdots \\ a_0 & \dots & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = a_0(x_1x_n + ... + x^2_{\frac{n+1}{2}} + ... + x_nx_1)$$

$$= 2a_0 \sum_{i=1}^{n-1/2} x_i x_{n+1-i} + 2a_0 x^2_{\frac{n+1}{2}}$$

Now the sum $\sum_i x_i x_{n+1-i}$ is a hyperbolic quadratic form, therefore our original quadratic space is Witt equivalent to $\langle 2a_0 \rangle$. $\square$

Bibliography

[1] Yvette Amice. *Les nombres p-adiques.* Presses Universitaires de France, 1975.

[2] Brian D.O. Anderson. On the computation of the Cauchy Index. *Quarterly of Applied Mathematics*, pages 577–582, 1972.

[3] Christopher I. Byrnes. On a Theorem of Hermite and Hurwitz. *Linear algebra and its applications*, (50):61–101, 1983.

[4] Eduardo Cattani and Alicia Dickenstein. Introduction to Residues and Resultants. In Alicia Dickenstein and I.Z. Emiris, editors, *Solving Polynomial Equations: Foundations, Algorithms, and Applications*, volume 14, pages 1–61. Springer-Verlag, 2005.

[5] David S. Dummit and Richard M. Foote. *Abstract Algebra.* John Wiley & Sons, 1999.

[6] Richard Elman and T.Y. Lam. Classification Theorems for quadratic forms over fields. *Commentarii Mathematici Helvetici*, 49(1):373–381, 1974.

[7] Paul A. Fuhrmann. *A polynomial approach to linear algebra.* Springer, 1996.

[8] F.R. Gantmacher. *The Theory of Matrices.* Chelsea Publishing Company, 1964.

[9] Fernando Gouvea. *p-adic Numbers.* Springer-Verlag, 2003.

[10] N. Hamada and B.D.O. Anderson. The unit circle Cauchy Index: definition, characterization and polynomial zero distribution. *SIAM Journal on Applied Mathematics*, 44(4):803–818, 1984.

[11] Peter Henrici. *Applied and computational complex analysis.* John Wiley & Sons, 1974.

[12] Ch. Hermite. Extrait d'une lettre de Mr. Ch. Hermite de Paris a Mr. Borchardt de Berlin sur le nombre des racines d'une equation algebrique comprises entre des limites donnees. 1856.

[13] A. Hurwitz. Ueber die Bedingungen, unter welchen eine Gleichung nur Wurzeln mit negativen reellen Theilen besitzt. 1895.

[14] Neal Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-Functions.* Springer-Verlag, 1984.

[15] M.G. Krein and M.A. Naimark. The method of symmetric and hermitian forms in the theory of the separation of the roots of algebraic equations. *Linear and Multilinear Algebra*, 10:265–308, 1981.

[16] T.Y. Lam. *Introduction to quadratic forms over fields.* American Mathematical Society, 2004.

[17] Serge Lang. *Algebra.* Springer-Verlag, 2002.

[18] Franz Lemmermeyer. *Reciprocity Laws: from Euler to Eisenstein.* Springer-Verlag, 2000.

[19] Alexander Olshevsky and Vadim Olshevsky. The Kharitonov Theorem and Bezoutians. *Linear Algebra and its Applications*, (399):285–297, 2005.

[20] Fernando Rodriguez-Villegas. *Experimental Number Theory.* Oxford University Press, 2007.

[21] J. Maurice Rojas. Arithmetic multivariate Descartes' rule. *American Journal of Mathematics*, 126(1):1–30, 2004.

[22] W. Scharlau. *Quadratic and Hermitian Forms.* Springer-Verlag, 1985.

[23] Jean-Pierre Serre. *A Course in Arithmetic.* Springer-Verlag, 1973.

[24] Jean-Pierre Serre. L'invariant de Witt de la forme $Tr(x^2)$. *Commentarii Mathematici Helvetici*, 59:651–676, 1984.

[25] John Tate. Residues of differentials on curves. *Annales scientifiques de l' E.N.S.*, 1 serie 4(1):149–159, 1968.

Index

Vita

Silvia María Adduci was born in Buenos Aires, Argentina, the daughter of Vicente Adduci and Lidia Romero.

In 1999 she started undergraduate studies in Mathematics at the University of Buenos Aires, obtaining a degree of Licenciatura en Matemática in July 2004.

In August 2004 she started graduate studies at the Department of Mathematics of The University of Texas at Austin in Number Theory, and in 2009 she took and passed her two first exams of the Society of Actuaries. She received her Ph.D. in Mathematics in May 2010.

Permanent address: 2515 Speedway # 8.100
Austin, Texas 78712
silvia.adduci@gmail.com

This dissertation was typeset with LaTeX[†] by the author.

[†]LaTeX is a document preparation system developed by Leslie Lamport as a special version of Donald Knuth's TeX Program.