UNIVERSIDAD DE CANTABRIA
Dpto. Matemáticas, Estadística y Computación

TESIS DOCTORAL

Two Tools in Algebraic Geometry: Construction of Configurations in Tropical Geometry and Hypercircles for the Simplification of Parametric Curves

---

Luis Felipe Tabera Alonso

Dirigida por Michel Coste y Tomás Jesús Recio Muñiz

Santander, 2007

THÈSE

Présentée

DEVANT L'UNIVERSITÉ DE RENNES I

pour obtenir

le grade de DOCTEUR DE L'UNIVERSITÉ DE RENNES I

Mention Mathématiques et Applications

par

Luis Felipe Tabera Alonso

Institut de Recherche Mathématique de Rennes
École Doctorale MATISSE
U.F.R. Mathématiques

TITRE DE LA THÈSE:

Two Tools in Algebraic Geometry: Construction of Configurations in Tropical Geometry and Hypercircles for the Simplification of Parametric Curves

Directeurs de thèse: Michel Coste, Tomás Recio

Agradecimientos

En ocasiones se dice que desarrollar, escribir y publicar una tesis es como una carrera de obstáculos... donde no siempre los que parecen más grandes son los científicos diría yo. Por suerte, me he encontrado a lo largo de estos años con una gran cantidad de gente que ha celebrado conmigo mis éxitos y me ha echado una mano en los momentos difíciles. Con estas líneas quiero expresarles mi gratitud.

Primeramente quisiera agradecer a mis directores, Michel y Tomás que tanto me han enseñado. Quisiera agradecerles toda su ayuda y apoyo, así como la confianza que me han mostrado. Por supuesto también al *director on-line* por responder a las más variopintas preguntas a las horas más intempestivas desde cualquier sitio.

Quisiera agradecer al profesor Rafael Sendra y a Carlos Villarino de la Universidad de Alcalá por hacerme sentir como en casa y por el estupendo ambiente de trabajo que se respira con ellos. A Ilia Itenberg y Etienne de la universidad de Estrasburgo por sus acertados comentarios y críticas. Al profesor Sottile por sus enseñanzas sobre como escribir matemáticas. A Lalo, Carlos Andradas y Luis Miguel Pardo. A la paciencia y eficacia de Araceli, Asún, Claude Boschet, Karine Falc'hon, Chantal Halet y Danielle Lanneau.

A todos los compañeros que me he encontrado en Santander, Rennes y Kaiserslautern, a colegas y amigos de toda la vida, que veo mucho menos de lo que quisiera, pero que siempre me echan una mano para desconectar: Albán, Alicia, Alfredo, Alvar, Arancha, Asia, Benoit, Carmen, Claudiu, Choss, Cruz, Damien, Emmanuel, Erwan, Fabrizio, Fernando, Fred, Glenn, Germán, JM, Jorge, María, María vgj :) Michael, Olivier, Pilar, Ruben, Savvas (Rennes pierde sin las escapadas), Saida, Sara, Sergio, Sysadmin :P, Solen, Tonino, Victor, Zaida...

A los diseñadores, testeadores, traductores y usuarios de software libre por proporcionarme las herramientas técnicas para escribir esta tesis.

Por último no podría faltar mi familia, a ellos les quiero dedicar este trabajo: a mis padres, a mis hermanas, tíos y primos, a *güelito*. Sin vuestro cariño y apoyo constante nada de esto habría sido posible.

"If you have an apple and I have an apple and we exchange these apples then you and I will still each have one apple. But if you have an idea and I have an idea and we exchange these ideas, then each of us will have two ideas."

George Bernard Shaw

Contents

List of Figures

Introducción

Esta memoria trata sobre el estudio de dos herramientas novedosas en el contexto de la Geometría Algebraica. La primera de ellas es la introducción del concepto de construcción geométrica para la comparación de las realizaciones de configuraciones en Geometría Algebraica y Geometría Tropical. La segunda consiste en el estudio de la geometría de las curvas Hipercírculos y su aplicación al problema de reparametrización y simplificación algebraica de curvas racionales.

Construcciones en Geometría Tropical

La Geometría Tropical es un área de las Matemáticas de reciente creación. Su característica más destacable es la sustitución de las variedades algebraicas clásicas por complejos poliedrales. Los complejos poliedrales asociados comparten muchas de las propiedades geométricas de las variedades algebraicas, aunque tal vez requiera realizar un *"cambio de mentalidad"* para redefinir estas propiedades geométricas en el contexto tropical. El interés que tiene esta sustitución es que, en bastantes ocasiones, estas propiedades de las variedades algebraicas son más sencillas de calcular o acotar en el contexto tropical, obteniendo, de esta forma, información adicional de las variedades algebraicas que de otra forma sería complicada de hallar.

La redefinición de los conceptos geométricos en un contexto tropical ha despertado un creciente interés en los últimos años. En [Mik05], Mikhalkin proporciona los conceptos de grado y género de curvas planas tropicales, así como las nociones básicas de Geometría Enumerativa Tropical. A partir de estas nociones, se prueba el teorema de correspondencia de Mikhalkin, que relaciona el número de curvas tropicales de género y grado fijado que pasan por una familia adecuada de puntos con el número correspondiente de curvas algebraicas planas de grado y género fijado que pasan por un conjunto de puntos. También demuestra un teorema de correspondencia análogo para curvas reales, pero en este contexto la correspondencia no se refiere al número de curvas, que no es un invariante de la familia de puntos ni siquiera en el plano complejo, sino con el llamado invariante de Welschinger. Estas técnicas han revolucionado la Geometría Enumerativa: en [IKS03], los autores proporcionan una equivalencia asintótica logarítmica de los invariantes de Gromov-Witten y Welschinger en el plano. En [GMar] los autores relacionan los invariantes de Gromov-Witten relativos y demuestran la validez de la fórmula de Caporaso-Harris en el contexto tropical. Estos éxitos han animado a diversos autores a desarrollar aún más diversos conceptos de geometría algebraica

tropical. Así, en [RGST05] se proporcionan unas nociones elementales de teoría de la intersección, con unas pruebas de los teoremas de Bezout y Bernstein en el contexto tropical. En [SS04a] se estudia la grasmaniana tropical, prestando especial atención a sus propiedades combinatorias. En [Vig04], se proporciona una noción de operación sobre las curvas elípticas tropicales. Una teoría completa de geometría tropical en términos de esquemas y morfismos está aún en fase embrionaria.

Sin embargo, a pesar del éxito de este diccionario algebraico tropical, esta correspondencia no es completa. Para ver esto, definimos las variedades tropicales como sigue:

Definición 1.11 Sea $\mathbb{K}$ un cuerpo algebraicamente cerrado provisto de una valuación v no trivial $v : \mathbb{K}^* \to \mathbb{R}$. Sea $\mathcal{V}$ una variedad algebraica en $(\mathbb{K}^*)^n$. La imagen $-v(\mathcal{V}) \subseteq \mathbb{R}^n$ resultante de aplicar el opuesto de la valuación sobre cada componente es la *variedad tropical* asociada a $\mathcal{V}$.

De esta forma, las variedades tropicales son proyecciones de variedades algebraicas a través de una valuación fijada en un cuerpo algebraicamente cerrado. A través de esta definición, se puede entender la Geometría Tropical como el intento de dar un sentido geométrico a estos objetos $v(\mathcal{V})$. Pero, inevitablemente, esta proyección de las variedades a través de la valuación conlleva una pérdida de información. Tal vez el caso más llamativo por la inmediatez de esta pérdida de información es el hecho de que dos rectas tropicales distintas en el plano pueden tener infinitos puntos en común. Este simple hecho demuestra que no se puede dar una axiomática proyectiva en el conjunto de rectas tropicales. La memoria que presentamos trata de cuantificar esta pérdida de información mediante la comparación de las realizaciones algebraicas y tropicales de una configuración de incidencia.

Para poder estudiar las relaciones entre las configuraciones de incidencia algebraicas y tropicales, una noción fundamental es la de estabilidad. Dadas dos curvas planas tropicales C_1, C_2 sin ninguna componente común, estas pueden tener infinitos puntos de intersección. Si queremos comparar la Geometría Algebraica con la Geometría Tropical, es deseable una nueva noción de *intersección* tal que dos curvas diferentes posean solamente una cantidad finita de puntos de intersección. Una respuesta a esta pregunta es la noción de intersección estable (cf. [RGST05]). Se puede definir la intersección estable como el conjunto de puntos de intersección que es continuo por pequeñas perturbaciones de una de las curvas. Esta intersección estable es siempre un conjunto finito, aunque las curvas C_1 y C_2 tengan componentes comunes, o incluso en el caso de que $C_1 = C_2$. Además, esta noción de intersección verifica teoremas elementales de intersección como el teorema de Bernstein-Koushnirenko (cf. [RGST05]). Análogamente, podemos definir la curva tropical estable que pasa por un conjunto de puntos dados. Sea I el soporte de un polinomio bivariado, $\delta = \#(I)$ y $\delta - 1$ puntos en el plano tropical $P = \{q_1, \ldots, q_{\delta-1}\}$. Es posible que haya infinitas curvas distintas de soporte I que pasen por los puntos. Sin embargo, existe una única curva tropical de soporte I que pasa por P y tal que se puede deformar de manera continua para que pase por pequeñas perturbaciones (translaciones) $\{q'_1, \ldots, q'_{n-1}\}$ de los puntos. A la curva que tiene esta propiedad de continuidad se la denomina la curva tropical estable que pasa

por P.

A continuación presentamos un breve sumario de los problemas tratados en la memoria y las principales aportaciones originales.

Capítulo 1

En este Capítulo presentamos las nociones básicas de cuerpos valuados y las definiciones básicas de variedades tropicales e introducimos el concepto de configuración de incidencia. Las configuraciones de incidencia son una herramienta clásica en el estudio de geometrías finitas, véase por ejemplo [Dem68], cuya definición reproducimos aquí.

Definición 1.27 Una *estructura de incidencia* es un triple $G = (\mathfrak{p}, \mathfrak{B}, \mathfrak{I})$, tal que

$$\mathfrak{p} \cap \mathfrak{B} = \emptyset, \qquad \mathfrak{I} \subseteq \mathfrak{p} \times \mathfrak{B}$$

los elementos de $\mathfrak{p}$ se llaman *puntos*, los elementos de $\mathfrak{B}$ son *curvas* y los elementos de I son *relaciones de incidencia*. Además, suponemos que cada elemento $x \in \mathfrak{B}$ está etiquetado con un *soporte* I_x, es decir, un subconjunto finito de $\mathbb{Z}^2$.

Se sigue de la definición que una estructura de incidencia se puede interpretar como un grafo bipartito G con dos colores $\mathfrak{p}$ y $\mathfrak{B}$ y aristas $\mathfrak{I}$ en el que los elementos de tipo $\mathfrak{B}$ están etiquetados con un soporte.

Una realización algebraica (respectivamente tropical) de una estructura de incidencia es una asignación de un punto en el plano (tropical) para cada elemento $x \in \mathfrak{p}$ y de una curva plana (tropical) definida por un polinomio de soporte I_y para cada elemento $y \in \mathfrak{B}$. Se exige además que, para cada relación de incidencia $(x, y) \in \mathfrak{I}$, el punto representado por x esté contenido en la curva representada por y.

Las curvas tropicales son más flexibles que las algebraicas, en el sentido de que, fijada una estructura de incidencia G, pueden existir realizaciones tropicales que no son nunca la proyección de una realización algebraica de G. Sin embargo, toda realización algebraica de G se proyecta sobre una realización tropical de G.

Nuestro primer resultado original es:

Teorema 1.30 *Sea G una estructura de incidencia tal que, si se interpreta como grafo, éste es acíclico. Entonces hay una correspondencia entre las realizaciones tropicales y algebraicas. Es decir, para cada realización tropical x de G existe una realización algebraica $\widetilde{x}$ de G que se proyecta sobre x.*

Capítulo 2

En el siguiente Capítulo estudiamos la regla de Cramer tropical presentada en [RGST05] y su relación con la regla de Cramer algebraica. Para ello, sea k el cuerpo residual de $\mathbb{K}$ por la valuación. Sea $t^\Gamma = \{t^\gamma \mid \gamma \in \Gamma\}$ una sección de la valuación de $\mathbb{K}^*$ sobre Γ, es decir $v : t^\Gamma \to \Gamma$ es un isomorfismo de grupos. La projección natural del anillo de valuación de $\mathbb{K}$ sobrer k se puede extender a un homomorfismo de grupos multiplicativos $\pi : \mathbb{K}^* \to k^*$. Si $\widetilde{x} \in \mathbb{K}^*$, $v(\widetilde{x}) = \gamma$, entonces $\pi(\widetilde{x})$ es la proyección de $\widetilde{x}t^{-\gamma}$ sobre k^*. Este elemento se le denominará *el coeficiente principal de $\widetilde{x}$* o el *coeficiente residual* de

$\widetilde{x}$. Esta noción está inspirada en el caso de las series de Puiseux. Todos los resultados de genericidad que exijamos serán resultados de genericidad residual, es decir, que la imagen por π sea un elemento genérico de k. De esta forma, estudiamos la proyección de la solución de un sistema de ecuaciones lineales cuando sus coeficientes residuales son genéricos y su aplicación al cálculo de la curva de soporte fijo I que pasa por $\#(I)-1$ puntos. El resultado original que relaciona los sistemas lineales en el contexto algebraico y tropical es el siguiente:

Teorema 2.10 *Sea I un soporte, $\delta = \#(I)$, $P = \{q_1, \ldots, q_{\delta-1}\}$, $q_j = (q_j^1, q_j^2)$ un conjunto de puntos tropicales, $\widetilde{P} = \{\widetilde{q}_1, \ldots, \widetilde{q}_{\delta-1}\}$ un conjunto de puntos algebraicos tales que su proyección es P. Entonces, si los puntos residuales $\pi(\widetilde{q}_i) = \gamma_i \in k^2$ son genéricos, sólo hay una curva algebraica $\widetilde{C}$ pasando por $\widetilde{P}$ y ésta se proyecta sobre la curva tropical estable de soporte I pasando por P. Además, podemos calcular explícitamente condiciones de genericidad suficientes en las coordenadas de γ_i para tener esta correspondencia.*

En esta caso, además, la curva calculada también es genérica entre las curvas de soporte I.

Teorema 2.11 *En las condiciones anteriores, si los puntos residuales γ_i son genéricos y $\widetilde{C}$ es la curva algebraica de soporte I pasando por $\widetilde{P}$, entonces los coeficientes residuales en k de un polinomio definiendo $\widetilde{C}$ también son genéricos.*

Capítulo 3

Con una aproximación análoga al Capítulo 2, en este Capítulo estudiamos la intersección de curvas algebraicas y su relación con la intersección de curvas tropicales. Para poder estudiar esta relación proponemos una definición de resultante tropical como la proyección de la resultante algebraica para polinomios de soporte fijado. Probamos que esta noción tiene un significado geométrico análogo a la resultante algebraica y permite biyectar los puntos de intersección de dos curvas genéricas $\widetilde{f}$, $\widetilde{g}$ de soporte dado I_1, I_2 con la intersección estable de dos curvas tropicales $f = T(\widetilde{f})$, $g = T(\widetilde{g})$, contando multiplicidades. La aportación principal es un resultado análogo al presentado en el capítulo anterior, y que detallamos a continuación.

Teorema 3.10 *Sean $\widetilde{f}$, $\widetilde{g} \in \mathbb{K}[x,y]$. Entonces podemos calcular condiciones suficientes en los coeficientes principales de los polinomios $\widetilde{f}$, $\widetilde{g}$, que dependen solamente de la proyección f, g de dichos polinomios, tales que si estas condiciones se cumplen, entonces la proyección de la intersección de $\widetilde{f}$, $\widetilde{g}$ es exactamente la intersección estable de f y g. Además, las multiplicidades de intersección se conservan.*

$$\sum_{\substack{\widetilde{q}\in\widetilde{f}\cap\widetilde{g}\\ T(\widetilde{q})=q}} mult(\widetilde{q}) = mult_t(q)$$

Además, en este caso, si las curvas tienen coeficientes residuales genéricos, también los tiene genéricos cualquier punto de intersección de las mismas. Este teorema es

imprescindible para los resultados del siguiente Capítulo:

Teorema 3.14 *Sean $\widetilde{f}$, $\widetilde{g} \in \mathbb{K}[x,y]$ dos polinomios representando dos curvas. Si los coeficientes principales de estos polinomios son genéricos en k entonces, cualquier punto intersección de $\widetilde{f}$, $\widetilde{g}$ también tiene coeficientes principales genéricos.*

Capítulo 4

En este Capítulo proponemos y exploramos las posibilidades de una sencilla herramienta para el estudio de las configuraciones de incidencia: la noción de construcción geométrica. Intuitivamente, una construcción es un procedimiento que toma como elementos de entrada un conjunto de puntos y curvas y da como resultado una configuración de incidencia que contiene a estos puntos y curvas de entrada entre sus elementos.

Definición 4.1 Una *construcción geométrica* es un procedimiento abstracto consistente en:

- Elementos de entrada: dos conjuntos finitos $\mathfrak{p}_0$, $\mathfrak{B}_0$ tales que $\mathfrak{p}_0 \cap \mathfrak{B}_0 = \emptyset$ y cada elemento $x \in \mathfrak{B}_0$ tiene asociado un soporte I_x. El conjunto de relaciones de incidencia inicial es el conjunto vacío $\mathfrak{I} = \emptyset$.

- Pasos de una construcción: una sucesión finita de pasos tales como los siguientes

  - Dado un soporte I con $\#\delta(I) = n \geq 2$ y $n-1$ puntos $\{q_1, \ldots, q_{n-1}\}$, añadimos una nueva curva C de soporte I a $\mathfrak{B}$, también añadimos condiciones de incidencia orientadas $q_i \to C$, $1 \leq i \leq n-1$.
  - Dadas dos curvas C_1, C_2 de soporte I_1, I_2 y polígonos de Newton (clausuras convexas) $\Delta(I_1)$, $\Delta(I_2)$ respectivamente, añadimos $\mathcal{M}(\Delta(I_1), \Delta(I_2))$ puntos nuevos a $\mathfrak{p}$, donde

    $$\mathcal{M}(\Delta(I_1), \Delta(I_2)) = vol(\Delta(I_1) + \Delta(I_2)) - vol(\Delta(I_1)) - vol(\Delta(I_2)).$$

    También añadimos condiciones de incidencia orientadas $C_1 \to q_i$, $C_2 \to q_i$, $1 \leq i \leq \mathcal{M}(\Delta(I_1), \Delta(I_2))$.

- Salida: una estructura de incidencia G en la que las relaciones de incidencia están provistas de una orientación.

Una realización (tropical) de una construcción algebraica es una realización del grafo de incidencia de salida G tal que

- Si $x \in \mathfrak{B} \setminus \mathfrak{B}_0$ de soporte I y $\{y_1, \ldots, y_{\delta(I)-1}\}$ son sus predecesores inmediatos entonces x es la curva (tropical estable) que pasa por el conjunto de puntos $\{y_1, \ldots, y_n\}$.

- Si $x \in \mathfrak{p}$ y no es un elemento de entrada, sean y_1, y_2 sus predecesores inmediatos, y sean $\{x_1, \ldots, x_n\}$ los sucesores inmediatos comunes de y_1 e y_2. Entonces $\{x_1, \ldots, x_n\}$ es exactamente la intersección (tropical estable) de y_1 e y_2, contadas con multiplicidad.

Notemos que, en el contexto tropical, la curva que pasa por un conjunto de puntos se interpreta siempre como la curva estable que pasa por ellos y la intersección de dos curvas como la intersección estable. Estas nociones se comportan razonablemente bien con la proyección del contexto algebraico al tropical.

Con el concepto que hemos introducido de construcción como herramienta, podemos estudiar las realizaciones tropicales de una configuración de incidencia obtenidas a través de una construcción con las realizaciones de algebraicas de esta misma construcción. Para ello introducimos la noción de admisibilidad.

Definición 4.5 Sea $\mathfrak{C}$ una construcción geométrica. Sea G el grafo de incidencia orientado inducido por la construcción. La construcción $\mathfrak{C}$ es *admisible* si, para cada par de nodos A, B de G, existe a lo más un camino orientado de A a B.

Esta noción es clave en nuestro contexto. Nuestro resultado original principal es el siguiente:

Teorema 4.6 *Sea $\mathfrak{C}$ una construcción admisible. Entonces, para cada realización x tropical de $\mathfrak{C}$, existe una realización algebraica $\widetilde{x}$ de la construcción $\mathfrak{C}$ tal que se proyecta sobre x.*

En este Capítulo también estudiamos diversas situaciones en las que se puede obtener información de una construcción geométrica aun cuando esta no sea admisible. También discutimos los distintos casos que pueden aparecer al estudiar las construcciones.

Capítulo 5

La principal aplicación que tienen las técnicas desarrolladas en los capítulos anteriores es un teorema de transferencia del contexto algebraico al tropical. Ahora bien, teoremas equivalentes en Geometría Proyectiva pueden no serlo en Geometría Tropical. En este Capítulo presentamos un resultado de transferencia cuando el teorema a transferir está enunciado de una manera muy explícita. Para poder formalizar cómo debe estar enunciado un teorema para poder aplicar nuestros resultados, introducimos la noción de teorema construible admisible.

Definición 5.1 Un *enunciado de incidencia construible* es un triple (G, H, x) tal que G es una estructura de incidencia, H es una construcción geométrica, llamada las *hipótesis*, tal que, considerado como estructura de incidencia, H es una subestructura completa de G, $H \subseteq G$. Además,

$$\{\mathfrak{p}_G \cup \mathfrak{B}_G\} \setminus \{\mathfrak{p}_H \cup \mathfrak{B}_H\} = \{x\},$$

se requiere que sólo hay un vértice x de G que no es un vértice de H, este vértice es llamado el *nodo tesis*.

Sean H_0 los elementos de entrada de H. Sea $\mathbb{K}$ un cuerpo algebraicamente cerrado. Diremos que un enunciado de incidencia *se cumple* en $\mathbb{K}$ o que es *un teorema* en $\mathbb{K}$ si se cumple una realization genérica de H_0. Es decir, si existe un conjunto denso L en el espacio de realizaciones de H_0 tal que:

- Para cada $\widetilde{h} \in L$, la construcción H está bien definida.
- Si $\widetilde{p} \in R_H$ es una realización de H construida a partir de $\widetilde{h} \in L$, entonces existe un elemento $\widetilde{x}$ tal que $(\widetilde{p}, \widetilde{x})$ es una realización de G.

En el contexto tropical, la construcción H está siempre bien definida para toda entrada gracias a la noción de estabilidad. Por lo que un teorema *se cumple* en el plano tropical si, para cada realización p de H obtenida por la construcción, existe un elemento x tal que (p, x) es una realización tropical de G.

Un enunciado de incidencia construible es *admisible* si la construcción asociada a las hipótesis es una construcción admisible. Con este lenguaje, podemos probar que:

Teorema 5.3 *Sea $\mathcal{Z} = (G, H, x)$ un enunciado de incidencia construible que sea admisible. Si $\mathcal{Z}$ se cumple en un cuerpo algebraicamente cerrado $\mathbb{K}$, entonces se cumple para el plano tropical sobre cualquier cuerpo.*

Utilizando esta técnica hemos demostrado con éxito versiones tropicales del Teorema de la configuración del plano de Fano (5.4), el Teorema de Pappus (5.5), el recíproco del Teorema de Pascal (5.6), el Teorema de Chasles (5.7) y su generalización el Teorema de Cayley-Bacharach (5.8), así como una versión no universal del Teorema de Pascal (5.9).

En particular, con la prueba del Teorema de Pappus, damos una respuesta positiva a una conjetura aparecida en [RGST05]. En este artículo, los autores muestran dos enunciados del Teorema de Pappus equivalentes en el contexto algebraico, pero que no lo son en el contexto tropical. Los autores proporcionan un contraejemplo al primero de estos enunciados, conjeturando que el otro enunciado siempre se cumple. Resulta que este enunciado alternativo es un enunciado de incidencia construible cuyas hipótesis forman una construcción admisible. Por tanto, aplicando las técnicas que hemos aportado, se demuestra que este enunciado se verifica siempre.

Hipercírculos y Simplificación de Curvas Paramétricas

En esta segunda parte de la memoria nos dedicamos a estudiar un problema diferente, en el que también aportamos una herramienta original para su análisis y resolución. Para presentar el contexto del problema, introduzcamos el siguiente ejemplo:

Ejemplo Consideremos el círculo $x^2 + y^2 - 1 = 0 \subseteq \mathbb{C}^2$. Tomemos las siguientes parametrizaciones del mismo:

$$\phi(t) = \left(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1} \right)$$

$$\psi(t) = \left(\frac{2 + 2t^2 + 2t^4}{2 + 2t^2 + 3t^4 + 2t^6 + t^8}, \frac{2t^2 + 3t^4 + 2t^6 + t^8}{2 + 2t^2 + 3t^4 + 2t^6 + t^8} \right)$$

$$\eta(t) = \left(\frac{2\sqrt{2}t^2 - 6t - 4\sqrt{2}}{3t^2 - 2t\sqrt{2} + 9}, \frac{t^2 + 6\sqrt{2}t - 7}{3t^2 - 2\sqrt{2}t + 9} \right)$$

La primera parametrización es la clásica que se calcula a partir del haz de rectas que pasan por el punto $(0, 1)$. La segunda parametrización es más *complicada*, puesto que el grado de las funciones racionales involucradas es mayor que el grado de la curva que están parametrizando. El problema de la tercera parametrización es que sus coeficientes no son racionales, sino que pertenecen al cuerpo $\mathbb{Q}(\sqrt{2})$.

La simplificación de la segunda parametrización $\psi(t)$ se puede efectuar mediante (una versión constructiva de) el Teorema de Lüroth. Este teorema afirma que toda reparametrización de una curva puede reemplazarse por una parametrización fiel, es decir, que sea uno a uno en casi todo su dominio. En nuestro ejemplo se puede obtener una parametrización fiel mediante el cambio $1 + t^2 + t^4 = s$.

La tercera parametrización plantea otro tipo de problemas. ¿Es posible, a partir de $\eta(t)$ obtener una parametrización similar a $\phi(t)$? En este caso nos preguntamos si existen algoritmos que nos permitan pasar de una parametrización con coeficientes algebraicos a una representación con coeficientes racionales, o más generalmente, dada una curva a través de una parametrización $\eta(t) \in \mathbb{K}(\alpha)(t)$, donde $\mathbb{K}$ es un cuerpo de característica cero y α es un elemento algebraico sobre $\mathbb{K}$, buscamos métodos para calcular, si es posible una parametrización $\phi(t)$ de la misma curva, pero esta vez con coeficientes en el cuerpo $\mathbb{K}$.

En un contexto computacional, dependiendo del problema que pretendamos resolver, puede ser más interesante tener una representación implícita o paramétrica de una curva racional. Si bien ambas representaciones son equivalentes y se conocen algoritmos para pasar de una representación a la otra, estos algoritmos pueden ser costosos. Por tanto, en nuestro problema de reparametrización, buscamos además algoritmos que permitan calcular dicha reparametrización sin recurrir a técnicas de implicitación. Esto es, sin calcular las ecuaciones implícitas de la curva a tratar.

Una respuesta a esta pregunta es la utilización de una curva auxiliar, introducida por Andradas, Recio y Sendra en [ARS99]. Esta es una curva auxiliar que codifica, geométricamente, el cambio de parámetro necesario para resolver el problema propuesto. En nuestro ejemplo, el cambio de parámetro necesario para pasar de la parametrización $\eta(t)$ a $\phi(t)$ es

$$t \to \frac{2\sqrt{2}t + 1}{t - \sqrt{2}}$$

Esta fracción lineal puede escribirse como

$$\frac{2\sqrt{2}t + 1}{t - \sqrt{2}} = \frac{5t}{t^2 - 2} + \sqrt{2}\frac{1 + 2t^2}{t^2 - 2}$$

La hipérbola definida por la parametrización $\left(\frac{5t}{t^2-2}, \frac{1+2t^2}{t^2-2}\right)$ codifica la información necesaria para obtener la reparametrización deseada del círculo en nuestro ejemplo. Esta

curva obtenida por la reescritura de una fracción lineal en la base $(1, \sqrt{2})$ recibe el nombre de hipercírculo en [ARS99].

Definición 8.1 Sea $u(t) = \frac{at+b}{ct+d} \in \mathbb{K}(\alpha)(t)$ una fracción lineal, $ad-bc \neq 0$. Supongamos que $[\mathbb{K}(\alpha) : \mathbb{K}] = n$ y escribamos

$$u(t) = \sum_{i=0}^{n-1} \phi_i(t)\alpha^i, \ \phi_i(t) \in \mathbb{K}(t)$$

dicha fracción lineal en la base $\{1, \alpha, \ldots, \alpha^{n-1}\}$. El *hipercírculo* asociado a $u(t)$ es la curva parametrizada por $(\phi_0, \ldots, \phi_{n-1})$ sobre la clausura algebraica de $\mathbb{K}$.

Capítulo 6

En este Capítulo presentamos el contexto algebraico en el que desarrollaremos la teoría de hipercírculo. Si $\mathbb{F}$ es un cuerpo algebraicamente cerrado de característica cero y $\mathbb{K} \subseteq \mathbb{F}$ es un subcuerpo, estamos interesados en el estudio de las $\mathbb{K}$-variedades, es decir, las variedades algebraicas que pueden expresarse como el conjunto de soluciones comunes a una familia de polinomios con coeficientes en $\mathbb{K}$. Se presentan algunas caracterizaciones clásicas de las $\mathbb{K}$-variedades y algunas de las propiedades geométricas que se pueden definir de manera racional, es decir, a partir del ideal de polinomios con coeficientes en $\mathbb{K}$ y con operaciones en el cuerpo $\mathbb{K}$ solamente. Adaptamos a este contexto nociones clásicas como la irreducibilidad de un variedad con respecto a un cuerpo $\mathbb{K}$, la $\mathbb{K}$-birracionalidad de variedades así como la posibilidad que tiene una curva para ser parametrizable sobre $\mathbb{K}$. También estudiaremos la relación existente entre las topologías Zariski de $\mathbb{F}^n$ para distintos subcuerpos $\mathbb{K}$ de $\mathbb{F}$, donde la topología $\tau_{\mathbb{K}}$ de $\mathbb{F}^n$ es la topología de variedades $\mathbb{K}$-definibles de $\mathbb{F}^n$.

Esta recopilación de resultados clásicos se incluye en la memoria por dos razones. En primer lugar para que la memoria sea autocontenida. En segundo lugar porque no conocemos ninguna referencia estándar donde aparezcan recogidos a la vez todos estos resultados, o donde aparezcan en un lenguaje afín a nuestros intereses. La referencia básica de este Capítulo es [ZS75b].

Capítulo 7

En este Capítulo abordamos la definición de la variedad de Weil en el caso implícito y presentamos una construcción análoga al caso paramétrico.

Definición 7.1 Sea $\mathbb{K}$ un cuerpo de característica cero, $\mathbb{F}$ su clausura algebraica y α un elemento algebraico sobre $\mathbb{K}$ de grado d. Sea

$$\mathcal{V} = \{f_1(x_1, \ldots, x_n) = \ldots = f_r(x_1, \ldots, x_n) = 0\} \subseteq \mathbb{F}^n$$

una variedad algebraica de dimensión m, donde $f_j \in \mathbb{K}(\alpha)[x_1, \ldots, x_n]$, $1 \leq j \leq r$.

Definimos la variedad de Weil asociada a $\mathcal{V}$ como en [Wei95], reemplacemos cada variable x_j por $x_{j0} + \alpha x_{j1} + \cdots + \alpha^{d-1} x_{j,d-1}$, donde hemos introducido las nuevas

variables x_{ji} y escribamos f_k en este nuevo conjunto de variables:

$$f_k(x_{(1)};\ldots;x_{(n)}) \in \mathbb{K}(\alpha)[x_{(1)};\ldots;x_{(n)}],$$

donde $x_{(j)}$ denota el vector de variables $(x_{j0},\ldots,x_{j,d-1})$. Expresemos las polinomios $f_k(x_{(1)};\ldots;x_{(n)})$ como

$$f_{k0}(x_{(1)};\ldots;x_{(n)}) + \alpha f_{k1}(x_{(1)};\ldots;x_{(n)}) + \cdots + \alpha^{d-1} f_{k,d-1}(x_{(1)};\ldots;x_{(n)})$$

con $f_{ki} \in \mathbb{K}[x_{(1)};\ldots;x_{(n)}]$ unívocamente determinados. La variedad $\mathcal{W}$ definida por los polinomios f_{ki} es la *variedad de Weil* asociada a $\mathcal{V}$.

$$W = \{f_{ki}(x_{(1)};\ldots;x_{(n)}) = 0 \mid k = 1,\ldots,r, i = 0,\ldots,d-1\} \subseteq \mathbb{F}^{nd}$$

Por definición, esta variedad siempre está definida sobre el cuerpo $\mathbb{K}$. Es conocido (véase [Wei95]) que la variedad $\mathcal{V}$ puede definirse sobre $\mathbb{K}$ si y sólo si $\widetilde{W} = W \cap \{x_{ji} = 0 \mid j = 1,\ldots,n, i \geq 1\}$ tiene la misma dimensión que $\mathcal{V}$. Este método funciona para una representación implícita de la variedad. Puesto que nosotros estamos interesados en trabajar con una curva paramétrica, proporcionamos una construcción análoga para el caso paramétrico inspirado en el caso de curvas de [ARS99].

Para ello, sea $\mathcal{V}$ una variedad dada por la parametrización unirracional

$$\begin{array}{rccc} \phi(t): & \mathbb{F}^m & \to & \mathbb{F}^n \\ & (t_1,\ldots,t_m) & \to & (\phi_1(t_1,\ldots,t_m),\ldots,\phi_n(t_1,\ldots,t_m)) \end{array}$$

donde $\phi_k \in \mathbb{K}(\alpha)(x_1,\ldots,x_n)$. Por lo que cada función coordenada ϕ_k tiene una representación como un cociente

$$\phi_k(t_1,\ldots,t_m) = \frac{h_k(t_1,\ldots,t_m)}{g_k(t_1,\ldots,t_m)}, \quad h_k, g_k \in \mathbb{K}[x_1,\ldots,x_n].$$

Además, sustituyendo g_k por el mínimo común múltiplo de los denominadores g_k, podemos suponer que el denominador g es común y que la representación de las funciones racionales no tiene componentes comunes $\gcd(h_1(t),\ldots,h_n(t),g(t)) = 1$.

Definición 7.6 Sea $\phi = (\phi_1,\ldots,\phi_n)$ como arriba, escribamos $t_j = t_{j0} + t_{j1}\alpha + \cdots + t_{j,d-1}\alpha^{d-1}$, donde t_{ji} son nuevas variables. La sustitución de estas variables en ϕ define funciones racionales en $\mathbb{K}(\alpha)(t_{(1)};\ldots;t_{(m)})$, donde $t_{(j)}$ denota el vector de variables $(t_{j0},\ldots,t_{j,d-1})$.

Estas funciones racionales tienen una expresión única como:

$$\phi_k = \phi_{k0}(t_{(1)};\ldots;t_{(m)}) + \alpha\phi_{k1}(t_{(1)};\ldots;t_{(m)}) + \cdots + \phi_{k,d-1}\alpha^{d-1}(t_{(1)};\ldots;t_{(m)})$$

donde $\phi_{ki} \in \mathbb{K}(t_{(1)};\ldots;t_{(m)})$. La aplicación unirracional $\Phi : \mathbb{F}^{md} \to \mathbb{F}^{nd}$ definida por

$$\begin{array}{ccc} \big(t_{10} & \ldots & t_{1d-1}; \\ t_{20} & \ldots & t_{2d-1}; \\ \multicolumn{3}{c}{\ldots\ldots\ldots} \\ t_{m0} & \ldots & t_{md-1}\big) \end{array} \to \begin{array}{ccc} \big(\phi_{10}(t_{(1)};\ldots;t_{(m)}) & \ldots & \phi_{1d-1}(t_{(1)};\ldots;t_{(m)}); \\ \phi_{20}(t_{(1)};\ldots;t_{(m)}) & \ldots & \phi_{2d-1}(t_{(1)};\ldots;t_{(m)}); \\ \multicolumn{3}{c}{\ldots\ldots\ldots} \\ \phi_{n0}(t_{(1)};\ldots;t_{(m)}) & \ldots & \phi_{nd-1}(t_{(1)};\ldots;t_{(m)})\big) \end{array}$$

se llama la parametrización obtenida por desarrollo de ϕ.

Se tiene que Φ parametriza la variedad de Weil $\mathcal{W}$ y que ϕ es birracional si y sólo si Φ es birracional. Definimos la *variedad testigo* como

Definición 7.12 Sea $Y = \{t \in \mathbb{F}^{md} \mid \phi_{ki}(t) = 0, i > 0\}$. Sean $\phi_{ki} = h_{ki}(t)/\delta(t)$ las funciones racionales escritas con un denominador común. Sea D_δ el conjunto de puntos donde $\delta(t) \neq 0$. Definimos la *variedad testigo* de $\mathcal{V}$ como la clausura Zariski de $Y \cap D_\delta$.

Con estas definiciones, el principal resultado original de este Capítulo es:

Teorema 7.11 *Sea U el conjunto de puntos donde $\Phi(t)$ es una aplicación finito a uno. Entonces $\mathcal{V}$ está definida sobre $\mathbb{K}$ si y sólamente si* $\dim(Y \cap D_\delta \cap U) = \dim(\mathcal{V})$. *Además, en este caso, si $\tau : \mathbb{F}^m \to Y \cap D_\delta \cap U$ es una parametrización unirracional una componente de $Y \cap D_\delta \cap U$ de dimensión* $\dim(\mathcal{V})$, *entonces* $\big(\phi_{10}(\tau), \ldots, \phi_{n0}(\tau)\big)$ *es una parametrización de $\mathcal{V}$ sobre $\mathbb{K}$.*

Además, en el caso birracional, podemos determinar cómo es la estructura geométrica de esta componente parametrizable. Para ello introducimos la noción de hipercuádrica.

Definición 7.15 Sea θ un $\mathbb{F}$-automorfismo del cuerpo de funciones racionales en m variables

$$\theta : \mathbb{F}(t_1, \ldots, t_m) \to \mathbb{F}(t_1, \ldots, t_m)$$

dado por la sustitución

$$t_1 = \theta_1(t_1, \ldots, t_m), \ldots, t_m = \theta_m(t_1, \ldots, t_m).$$

Supongamos que los coeficientes de θ_j pertenecen a $\mathbb{K}(\alpha)$ y desarrollemos cada función racional como

$$\theta_j(t_1, \ldots, t_m) = \sum_{i=0}^{d-1} \theta_{ji}(t_1, \ldots, t_m)\alpha^i, \theta_{ji} \in \mathbb{K}(t_1, \ldots, t_m).$$

Una *hipercuádrica* es la variedad de $\mathbb{F}^{md}$ parametrizada por las componentes $\theta_{ji}, j = 1, \ldots, m$, $i = 0, \ldots, d-1$ de un automorfismos θ en base $1, \alpha, \ldots, \alpha^{d-1}$

Con esta notación tenemos que:

Teorema 7.16 *Supongamos que ϕ es birracional. Entonces $\mathcal{V}$ es parametrizable sobre $\mathbb{K}$ y θ es un automorfismo de $\mathbb{F}^{md}$ con coeficientes en $\mathbb{K}(\alpha)$ tal que $\phi(\theta) \in \mathbb{K}(t_1, \ldots, t_m)$ si y sólo si $Y \cap D_\delta \cap U$ tiene una componente que es la hipercuádrica asociada a θ.*

A continuación presentamos una serie de ejemplos y contraejemplos que muestran cómo funciona el método y cómo son necesarias las hipótesis de los teoremas, especialmente la inclusión de los conjuntos D_δ y U en los enunciados de los teoremas.

Capítulo 8

En este Capítulo nos centramos en el estudio de las propiedades de los hipercírculos, esto es, las hipercuádricas de dimensión 1. Los resultados de este Capítulo son el

resultado de un trabajo conjunto con los profesores Recio, Sendra y Villarino. La principal aportación es un teorema de estructura de los hipercírculos:

Teorema 8.7 *Sea $\mathcal{U}$ un hipercírculo asociado al isomorfismo $u(t) = \frac{at+b}{t+d} \in \mathbb{K}(\alpha)(t)$, sea $r = [\mathbb{K}(-d) : \mathbb{K}]$. Entonces, existe una transformación proyectiva $\rho : \mathbb{P}(\mathbb{F})^n \longrightarrow \mathbb{P}(\mathbb{F})^n$, definida sobre $\mathbb{K}$ tal que la curva $\rho(\mathcal{U})$ es la curva racional normal de grado r en $\mathbb{P}(\mathbb{F})^n$ parametrizada por*

$$\widetilde{\rho}(t : s) = [s^r : s^{r-1}t : \cdots : st^{r-1} : t^r : 0 : \cdots : 0].$$

De aquí deducimos las propiedades más importantes de los hipercírculos:

Corolario 8.8 *En las condiciones anteriores:*

1. *$\mathcal{U}$ es una curva de grado r.*
2. *$\mathcal{U}$ está contenido en una variedad lineal de dimensión r y no está contenido en ninguna variedad lineal de dimensión $r-1$.*
3. *$\mathcal{U}$ es regular en $\mathbb{P}(\mathbb{F})^n$.*
4. *La función de Hilbert de $\mathcal{U}$ es igual a su polinomio de Hilbert, $h_{\mathcal{U}}(m) = mn + 1$.*

Una manera de distinguir un hipercírculo de una curva racional normal es mediante los puntos del infinito. Si la extensión algebraica $[\mathbb{K}(\alpha) : \mathbb{K}] = n$ y $\mathcal{U}$ es un hipercírculo cualquiera de grado n, entonces los puntos del infinito de $\mathcal{U}$ sólo depende de la extensión $\mathbb{K} \subseteq \mathbb{K}(\alpha)$. Si $P = \{P_1, \ldots, P_n\}$ son los puntos del infinito de $\mathcal{U}$, entonces

$$\{x_0 + \alpha_j x_1 + \cdots + \alpha_j^{n-1} x_{n-1} = 0\} \cap \overline{\mathcal{U}} = P \setminus \{P_j\},$$

donde $\alpha_j = \sigma_j(\alpha)$ son los conjugados de α en $\mathbb{F}$, $1 \leq j \leq n$ y $\overline{\mathcal{U}}$ es la clausura proyectiva de $\mathcal{U}$.

La caracterización proyectiva de los hipercírculos y el conocimiento de los puntos del infinito proporcionan algoritmos de parametrización e implicitación adaptados a los hipercírculos. La aportación original más relevante en este aspecto es el siguiente algoritmo de implicitación. Recordemos que, dada la curva racional normal de grado n, un sistema de generadores de su ideal homogéneo es $\{y_i y_{j-1} - y_{i-1} y_j \mid 1 \leq i, j \leq n\}$ (cf. [Har92]).

Teorema 8.21 *Sea $\varphi(t) = (\frac{q_0(t)}{N(t)}, \ldots, \frac{q_{n-1}(t)}{N(t)})$ una parametrización propia de un hipercírculo $\mathcal{U}$ de grado n con coeficientes en $\mathbb{F}$. Sea I el ideal homogéneo de la curva racional normal de grado n en $\mathbb{P}(\mathbb{F})^n$ dado por polinomios homogéneos $h_1(\bar{y}), \ldots, h_r(\bar{y})$, $\bar{y} = (y_0, \ldots, y_n)$. Sea $\mathcal{Q} \in \mathcal{M}_{n+1\times n+1}(\mathbb{F})$ la matriz de cambio de base de $\{q_0(t), \ldots, q_{n-1}(t), N(t)\}$ a $\{1, t, \ldots, t^n\}$. Sea*

$$f_i(\bar{x}) = h_i\left(\sum_{j=0}^{n} \mathcal{Q}_{0j} x_j, \ldots, \sum_{j=0}^{n} \mathcal{Q}_{nj} x_j\right), \ 1 \leq i \leq r.$$

Entonces, $\{f_1, \ldots, f_r\}$ *es un conjunto de generadores del ideal homogéneo de* $\mathcal{U}$*.*

Además, las propiedades de los hipercírculos nos proporcionan el siguiente teorema de caracterización de hipercírculos de grado máximo.

Teorema 8.24 *Sea* $\mathcal{U} \subseteq \mathbb{F}^n$ *un conjunto algebraico de grado* n *tal que todas sus componentes son de dimensión 1. Entonces,* $\mathcal{U}$ *es un hipercírculo si y sólo si tiene infinitos puntos con coordenadas en* $\mathbb{K}$ *y pasa por los puntos del infinito propios de un hipercírculo.*

Capítulo 9

En este Capítulo presentamos la relación de los hipercírculos con la variedad testigo definida en el Capítulo 7. En este caso, podemos refinar sensiblemente los resultados presentados en el Capítulo 7. Primeramente, no es necesaria la inclusión del conjunto U en el que la aplicación es finito a uno en las hipótesis de los teoremas porque se puede probar, en el caso de curvas, que la parametrización Φ obtenida por desarrollo siempre es finito a uno en su dominio de definición D_δ. Por otro lado, la variedad testigo tiene a lo más una componente de dimensión 1. Estos resultados simplifican enormemente los cálculos en el caso de curvas. Si $\mathcal{Z}$ es la variedad testigo asociada a una curva $\mathcal{V}$, entonces se cumple una de estas posibilidades:

- $\mathcal{Z}$ es un conjunto finito y $\mathcal{V}$ no es $\mathbb{K}$-definible.
- $\dim(\mathcal{Z}) = 1$, entonces $\mathcal{V}$ es $\mathbb{K}$-definible, además, $\mathcal{V}$ es $\mathbb{K}$-parametrizable si y sólo si la única componente 1-dimensional de $\mathcal{Z}$ es un hipercírculo.

En particular, podemos utilizar todos los resultados presentados en el Capítulo 8 para estudiar esta componente unidimensional de $\mathcal{Z}$.

Además, en el caso en el que el cuerpo base sean los racionales $\mathbb{K} = \mathbb{Q}$, tenemos la siguiente observación. Si una curva definida sobre $\mathbb{Q}$ no es $\mathbb{Q}$ parametrizable, entonces existen cuerpos cuadráticos $\mathbb{Q}(\beta)$ que parametrizan la curva. Como corolario de estas afirmaciones tenemos la siguiente propiedad:

Corolario 9.9 *Sea* $\mathcal{V}$ *una curva definida sobre* $\mathbb{Q}$*, parametrizada sobre* $\mathbb{Q}(\alpha)$ *y tal que no sea parametrizable sobre* $\mathbb{Q}$*. Sea* $\mathcal{U}$ *la componente 1-dimensional de la variedad testigo asociada a* $\mathcal{V}$*. Entonces, existen infinitos cuerpos cuadráticos distintos* $\mathbb{Q}(\beta)$ *tales que* $\mathcal{U}$ *es un hipercírculo para la extensión* $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\beta, \alpha)$*.*

A partir de aquí, podemos obtener una aplicación a la reparametrización de $\mathcal{V}$. Tenemos un resultado sobre reparametrizaciones óptimas de $\mathcal{V}$ mediante un cambio afín de parámetro $t \mapsto e_1 t + e_2$. La principal aportación original en este sentido es la siguiente:

Teorema 9.12 *Sea* $\mathcal{V}$ *una curva definida sobre* $\mathbb{Q}$ *dada por una parametrización* ϕ *con coeficientes en* $\mathbb{Q}(\alpha)$*. Entonces, siempre existe* $[a_0 : \ldots : a_{n-1} : 0]$*, un punto del infinito de la variedad testigo* $\mathcal{U}$ *que es representable sobre* $\mathbb{Q}(\alpha)$ *y que supondremos deshomogeneizado respecto a una coordenada* i*. Supongamos que el grado de* $\mathcal{U}$ *es* $r < n$*.*

Entonces, $\mathcal{V}$ *admite una reparametrización sobre* $\mathbb{Q}(\gamma) = \mathbb{Q}(a_0, \ldots, a_{n-1}) \subseteq \mathbb{Q}(\alpha)$*, donde* $[\mathbb{Q}(\gamma) : \mathbb{Q}] = r$*.*

Además, si $e_1, e_2 \in \mathbb{C}$*,* $e_1 \neq 0$ *son números algebraicos, sea* $\phi(e_1 t + e_2)$ *otra parametrización de* $\mathcal{V}$ *y sea* $\mathbb{L}$ *el cuerpo generado sobre* $\mathbb{Q}$ *por los coeficientes de* $\phi(e_1 t + e_2)$*, entonces*

1. $\mathbb{L}$ *contiene un cuerpo (isomorfo a)* $\mathbb{Q}(\gamma)$*.*
2. $[\mathbb{L} : \mathbb{Q}] \geq r$*.*
3. *Si* $[\mathbb{L} : \mathbb{Q}] = r$ *entonces* $\mathbb{L}$ *es isomorfo a* $\mathbb{Q}(\gamma)$*.*
4. *Existen* $e_1', e_2' \in \mathbb{L}$ *tales que* $e_1' t + e_2'$ *reparametriza* ϕ *sobre (un cuerpo isomorfo a)* $\mathbb{Q}(\gamma)$*.*

Résumé

Cette thèse traite de l'étude de deux outils nouveaux dans le contexte de la Géométrie Algébrique. Le premier est l'introduction du concept de construction géométrique pour la comparaison des réalisations des configurations en Géométrie Algébrique et Géométrie Tropicale. Le deuxième est l'étude de la géométrie des hypercercles et son application au problème de reparamétrisation et simplification algébrique des courbes rationnelles.

Constructions en Géométrie Tropicale

La Géométrie Tropicale est une branche des mathématiques de création récente. Sa caractéristique la plus remarquable est la substitution des variétés algébriques classiques par des complexes polyédraux. Les complexes polyédraux associés partagent beaucoup des propriétés géométriques des variétés algébriques, même s'il faut, peut-être, un *"changement de mentalité"* pour redéfinir des propriétés géométriques dans le contexte tropical. L'intérêt de cette substitution est qu'il y a de nombreuses occasions dans les quelles les propriétés des variétés algébriques sont plus simples à calculer ou à borner dans le contexte tropical. On obtient, de cette manière, de nouvelles informations sur les variétés algébriques qui seraient plus compliquées à trouver d'une autre manière.

La redéfinition des concepts géométriques dans un contexte tropical a suscité un intérêt croissant pendant les dernières années. Dans [Mik05], Mikhalkin fournit les concepts de genre des courbes tropicales planes ainsi que les notions de base de la Géométrie Énumérative Tropicale. À partir de ces notions, il prouve son théorème de correspondance, qui donne l'égalité du nombre de courbes tropicales de genre et degré fixés (comptées avec multiplicité) qui passent par une famille de points de cardinal convenable avec le nombre correspondant pour les courbes algébriques. Il démontre aussi un théorème analogue de correspondance pour les courbes réelles. Cette fois la correspondance n'est pas avec le nombre de courbes algébriques, qui n'est pas un invariant de la famille de points, mais avec l'invariant de Welschinger. Ces techniques ont révolutionné la Géométrie Énumérative: dans [IKS03], les auteurs fournissent une équivalence asymptotique logarithmique des invariants de Gromov-Witten et de Welschinger pour le plan. Dans [GMar] les auteurs démontrent la validité de la formule de Caporaso-Harris dans le contexte tropical.

Ces succès ont encouragé divers auteurs à développer d'autres concepts de la géo-

métrie algébrique tropicale. Ainsi, dans [RGST05] les notions élémentaires de théorie de l'intersection, avec les théorèmes de Bezout et de Bernstein dans le contexte tropical sont montrés. Dans [SS04a] la grassmannienne tropicale est étudiée, surtout ses propriétés combinatoires. Dans [Vig04], l'auteur fournit une notion d'opération sur les courbes elliptiques tropicales. Une théorie complète de la géométrie tropicale en termes de schémas et morphismes est encore dans une phase embryonnaire.

Toutefois, malgré le succès de ce dictionnaire algébrico-tropical, cette correspondance n'est pas complète. Pour voir ceci, on définit les variétés tropicales de la manière suivante:

Définition 1.11 Soit $\mathbb{K}$ un corps algébriquement clos avec une valuation non triviale, $v : \mathbb{K}^* \to \mathbb{R}$. Soit $\mathcal{V}$ une variété algébrique dans $(\mathbb{K}^*)^n$. L'image $-v(\mathcal{V}) \subseteq \mathbb{R}^n$ obtenue en appliquant l'opposé de la valuation sur chaque coordonnée est la *variété tropicale* associée à $\mathcal{V}$.

De cette manière, les variétés tropicales sont des projections de variétés algébriques par une valuation fixée sur un corps algébriquement clos. Donc, on peut entendre la Géométrie Tropicale comme la tentative de donner un sens géométrique à ces objets $v(\mathcal{V})$. Mais, inévitablement, cette projection des variétés par la valuation entraîne une perte d'information. Peut-être le cas le plus immédiat de cette perte d'information est le fait que deux droites tropicales différentes dans le plan peuvent avoir une infinité de points dans leur intersection. Ce simple fait démontre qu'on ne peut pas donner une axiomatique projective dans l'ensemble de droites tropicales. La thèse qu'on présente essaye de quantifier cette perte d'information par la comparaison des réalisations algébriques et tropicales d'une configuration d'incidence.

Pour étudier les relations entre les configurations d'incidence algébriques et tropicales, une notion fondamentale est la stabilité. Soient C_1, C_2 deux courbes planes tropicales sans aucune composante commune. Les courbes peuvent avoir une infinité de points d'intersection. Si on veut comparer la Géométrie Algébrique avec la Géométrie Tropicale, une nouvelle notion *d'intersection* est désirable telle que deux courbes différentes possèdent seulement un nombre fini de points d'intersection. Une réponse à cette question est la notion d'intersection stable (cf. [RGST05]). On peut définir l'intersection stable comme l'ensemble des points d'intersection qui sont limites de points d'intersection de C_1 avec une petite perturbation générique de C_2. Cette intersection stable est toujours un ensemble fini, même si les courbes C_1 et C_2 ont des composantes communes, ou même dans le cas $C_1 = C_2$. De plus, cette notion d'intersection vérifie des théorèmes élémentaires d'intersection comme le théorème de Bernstein-Koushnirenko (cf. [RGST05]). De façon analogue, on peut définir la courbe tropicale stable qui passe par un ensemble de points donné. Soit I un ensemble fini de $\mathbb{Z}^2$ qui représente le support d'un polynôme à deux variables, $\delta = \#(I)$ et $\delta - 1$ points dans le plan tropical $P = \{q_1, \ldots, q_{\delta-1}\}$. Il est possible qu'il y ait une infinité de courbes différentes de support I qui passent par les points. Toutefois, il existe une seule courbe tropicale de support I qui passe par P et telle que toute perturbation continue de P puisse être suivie par une perturbation continue de la courbe. Cette courbe qui a cette propriété de continuité est appelée la courbe tropicale stable qui passe par P.

Nous présentons maintenant un bref résumé des problèmes traités dans la thèse et les principales contributions originales.

Chapitre 1

Dans ce Chapitre on présente les notions élémentaires de corps valués et les définitions de base de variétés tropicales et on introduit le concept de configuration d'incidence. Les configurations d'incidence sont un outil classique dans l'étude des géométries finies, par exemple [Dem68], dont son définition est reproduite ici.

Définition 1.27 Une *structure d'incidence* est un triplet $G = (\mathfrak{p}, \mathfrak{B}, \mathfrak{I})$, tel que

$$\mathfrak{p} \cap \mathfrak{B} = \emptyset, \quad \mathfrak{I} \subseteq \mathfrak{p} \times \mathfrak{B}.$$

Les éléments de $\mathfrak{p}$ sont appelés *points*, les éléments de $\mathfrak{B}$ sont les *courbes* et les éléments de I sont les *relations d'incidence*. En plus, on suppose que chaque élément $x \in \mathfrak{B}$ est étiqueté avec un *support* I_x, c'est-à-dire, un sous-ensemble fini de $\mathbb{Z}^2$.

Il suit de la définition qu'une structure d'incidence peut être interprétée comme un graphe biparti G avec deux couleurs $\mathfrak{p}$ et $\mathfrak{B}$ et les arêtes $\mathfrak{I}$, dans lequel les éléments de type $\mathfrak{B}$ sont étiquetés avec un support.

Une réalisation algébrique (respectivement tropicale) d'une structure d'incidence est une assignation, d'un point sur le plan (tropical) pour chaque élément $x \in \mathfrak{p}$ et d'une courbe plane (tropicale) définie par un polynôme de support I_y pour chaque élément $y \in \mathfrak{B}$. On demande en plus que, pour chaque relation d'incidence $(x, y) \in \mathfrak{I}$, le point représenté par x soit contenu dans la courbe représentée par y.

Les courbes tropicales sont plus flexibles que les courbes algébriques, dans le sens que, étant donné une structure d'incidence G, on peut trouver (dans quelques cas) des réalisations tropicales qui ne sont jamais la projection d'une réalisation algébrique de G. Mais tout réalisation algébrique de G est projété sur une réalisation tropicale de G.

Le premier résultat original est:

Théorème 1.30 *Soit G une structure d'incidence dont le graphe sous-jacent est acyclique. Alors, il y a une correspondance entre les réalisations tropicales et algébriques. C'est-à-dire, pour chaque réalisation tropicale x de G il existe une réalisation algébrique $\widetilde{x}$ de G qui est projetée sur x.*

Chapitre 2

Dans ce Chapitre on étudie la règle de Cramer tropicale présentée dans [RGST05] et sa relation avec la règle de Cramer algébrique. À cet effet, soit k le corps résiduel de $\mathbb{K}$ par la valuation et Γ le group de valuation. Soit $t^\Gamma = \{t^\gamma \mid \gamma \in \Gamma\}$ une section de la valuation de $\mathbb{K}^*$ à Γ, c'est-à-dire $v : t^\Gamma \to \Gamma$ est un isomorphisme de groups. La projection naturelle de l'anneau de valuation de $\mathbb{K}$ dans k peut s'étendre en un homomorphisme de groupes multiplicatifs $\pi : \mathbb{K}^* \to k^*$. Si $\widetilde{x} \in \mathbb{K}^*$, $v(\widetilde{x}) = \gamma$, alors $\pi(\widetilde{x})$ est la projection de $\widetilde{x}t^{-\gamma}$ sur k^*. Cette élément est appellé *le coefficient principale de* $\widetilde{x}$ où le *coefficient résiduel* de $\widetilde{x}$. Cette notion est inspirée par le cas des séries de Puiseux. Tous les

résultats de généricité qu'on montre seront des résultats de généricité résiduelle, c'est-à-dire, que l'image par π soit un élément générique de k. De cette manière, on étudie la projection de la solution d'un système d'équations linéaires quand ses coefficients résiduels sont génériques et son application au calcul de la courbe de support fixé I qui passe par $\#(I)-1$ points. Le résultat original qui met en rapport les systèmes linéaires dans le contexte algébrique et tropical est le suivant:

Théorème 2.10 *Soit I un support, $\delta = \#(I)$, $P = \{q_1, \ldots, q_{\delta-1}\}$, $q_j = (q_j^1, q_j^2)$ un ensemble de points tropicaux, $\widetilde{P} = \{\widetilde{q}_1, \ldots, \widetilde{q}_{\delta-1}\}$ un ensemble de points algébriques dont la projection est P. Alors, si les points résiduels $\pi(\widetilde{q}_i) = \gamma_i \in k^2$ sont génériques, il y a seulement une courbe algébrique $\widetilde{C}$ en passant par $\widetilde{P}$ et elle est projetée sur la courbe tropicale stable de support I en passant par P. De plus, on peut calculer explicitement des conditions de généricité suffisantes dans les coordonnées de γ_i pour avoir cette correspondance.*

Dans ce cas, la courbe calculée est aussi générique parmi les courbes de support I.

Théorème 2.11 *Dans les conditions du Théorème précédent, si les points résiduels γ_i sont génériques et $\widetilde{C}$ est la courbe algébrique de support I en passant par $\widetilde{P}$, alors, les coefficients résiduels dans k d'un polynôme définissant $\widetilde{C}$ sont aussi génériques.*

Chapitre 3

Avec une approche semblable à celle du Chapitre 2, on étudie ici l'intersection de courbes algébriques et leur relation avec l'intersection de courbes tropicales. Pour pouvoir étudier cette relation on propose une définition du résultant tropical comme la projection du résultant algébrique pour des polynômes de support fixé. On prouve que cette notion a une signification géométrique analogue à celle du résultant algébrique et permet faire une bijection (en comptant les multiplicités) des points d'intersection de deux courbes génériques $\widetilde{f}$, $\widetilde{g}$ de support donné I_1, I_2 avec l'intersection stable des deux courbes tropicales $f = T(\widetilde{f})$, $g = T(\widetilde{g})$. La contribution principale est le résultat analogue à celui présenté dans le chapitre précédent.

Théorème 3.10 *Soient $\widetilde{f}$, $\widetilde{g} \in \mathbb{K}[x, y]$. On peut calculer des conditions suffisantes sur les coefficients résiduels des polynômes $\widetilde{f}$, $\widetilde{g}$, qui dépendent seulement de la projection f, g de ces polynômes, tels que si ces conditions sont remplies, la projection de l'intersection de $\widetilde{f}$, $\widetilde{g}$ est précisément l'intersection stable de f et g. De plus, les multiplicités d'intersection sont conservées.*

$$\sum_{\substack{\widetilde{q} \in \widetilde{f} \cap \widetilde{g} \\ T(\widetilde{q}) = q}} mult(\widetilde{q}) = mult_t(q)$$

Dans ce cas, si les polynômes définissant les courbes ont des coefficients résiduels génériques, alors un point d'intersection a aussi des coefficients résiduels génériques. Ce théorème est indispensable pour les résultats du Chapitre suivant:

Théorème 3.14 *Soient $\widetilde{f}, \widetilde{g} \in \mathbb{K}[x, y]$ deux polynômes représentant deux courbes. Si les coefficients résiduels de ces polynômes sont génériques dans k alors, tout point d'intersection de $\widetilde{f}$, $\widetilde{g}$ a aussi des coefficients résiduels génériques.*

Chapitre 4

Dans ce Chapitre on propose et explore les possibilités d'un outil simple pour l'étude des configurations d'incidence: la notion de construction géométrique. Intuitivement, une construction est un procédé qui prend comme éléments d'entrée un ensemble de points et de courbes et donne comme résultat une configuration d'incidence qui contient les points et les courbes d'entrée parmi ses éléments.

Définition 4.1 Une *construction géométrique* est une procédure abstraite consistant en:

- Éléments d'entrée: deux ensembles finis $\mathfrak{p}_0$, $\mathfrak{B}_0$ tels que $\mathfrak{p}_0 \cap \mathfrak{B}_0 = \emptyset$ et chaque élément $x \in \mathfrak{B}_0$ a un support I_x associé. L'ensemble des relations d'incidence initiale est l'ensemble vide $\mathfrak{I} = \emptyset$.
- Étapes de la construction: une succession finie de pas comme les suivants:
  - Soit I un support avec $\#\delta(I) = n \geq 2$ et $n-1$ points $\{q_1, \ldots, q_{n-1}\}$; on ajoute une nouvelle courbe C de support I à $\mathfrak{B}$, on ajoute aussi des conditions d'incidence orientées $q_i \to C$, $1 \leq i \leq n-1$.
  - Soient deux courbes C_1, C_2 de support I_1, I_2 respectivement et polygones de Newton (enveloppe convexe des supports) $\Delta(I_1)$, $\Delta(I_2)$ respectivement; on ajoute $\mathcal{M}(\delta(I_1), \Delta(I_2))$ nouveaux points à $\mathfrak{p}$, où

    $$\mathcal{M}(\Delta(I_1), \Delta(I_2)) = vol(\Delta(I_1) + \Delta(I_2)) - vol(\Delta(I_1)) - vol(\Delta(I_2))$$

    et aussi des conditions d'incidence orientées $C_1 \to q_i$, $C_2 \to q_i$, $1 \leq i \leq \mathcal{M}(\Delta(I_1), \Delta(I_2))$.
- Sortie: une structure d'incidence G dans laquelle les relations d'incidence ont une orientation.

Une réalisation (respectivement réalisation tropicale) d'une construction algébrique est une réalisation du graphe d'incidence G tel que

- Si $x \in \mathfrak{B} \backslash \mathfrak{B}_0$ et une courbe de support I et $\{y_1, \ldots, y_{\delta(I)-1}\}$ sont ses prédécesseurs immédiats alors x est la courbe (tropicale stable) qui passe par l'ensemble de points $\{y_1, \ldots, y_n\}$.
- Si $x \in \mathfrak{p}$ n'est pas un élément d'entrée, soient y_1, y_2 ses prédécesseurs immédiats, et soient $\{x_1, \ldots, x_n\}$ les successeurs immédiats communs de y_1 e y_2. Alors $\{x_1, \ldots, x_n\}$ est précisément l'intersection (tropicale stable) de y_1 et y_2 en comptant les multiplicités.

Remarquez que, dans le contexte tropical, la courbe qui passe par un ensemble de points est toujours interprétée comme la courbe stable passant par ceux-ci et l'intersection de deux courbes tropicales comme l'intersection stable.

Avec le concept qu'on a introduit de construction comme outil, on peut étudier les réalisations d'une configuration d'incidence exprimée comme une construction avec les réalisations de la même construction dans le contexte algébrique. Pour cela on introduit la notion d'admissibilité.

Définition 4.5 Soit $\mathfrak{C}$ une construction géométrique. Soit G le graphe d'incidence orienté induit par la construction. La construction $\mathfrak{C}$ est *admissible* si, pour chaque paire de sommets A, B de G, il existe au plus un chemin orienté de A à B.

Cette notion est très importante dans notre contexte. Notre résultat original principal est le suivant:

Théorème 4.6 *Soit $\mathfrak{C}$ une construction admissible. Alors, pour chaque réalisation tropicale x de $\mathfrak{C}$, il existe une réalisation algébrique $\widetilde{x}$ de la construction $\mathfrak{C}$ qui se projette sur x.*

Dans ce Chapitre on étudie aussi diverses situations où on peut encore obtenir des informations pour une construction géométrique même si elle n'est pas admissible. On regarde aussi les différents cas qui peuvent apparaître en étudiant les constructions.

Chapitre 5

La principale application des techniques développées dans les Chapitres précédents est un théorème de transfert du contexte algébrique au contexte tropical. Mais des formulations équivalentes de théorèmes de Géométrie Projective peuvent ne plus être équivalentes dans le cadre tropical. Dans ce Chapitre on présente un résultat de transfert quand le théorème à transférer est énoncé d'une manière très explicite. Pour pouvoir formaliser comment doit être énoncé un théorème et appliquer les résultats, on introduit la notion de théorème constructible admissible.

Définition 5.1 Un *énoncé d'incidence constructible* est un triple (G, H, x) où G est une structure d'incidence, H est une construction géométrique, appelée *l'hypothèse*, telle que, considérée comme structure d'incidence, H est une sous-structure complète de G, $H \subseteq G$. En outre, on demande qu'il y ait seulement un sommet x de G qui ne soit pas un sommet de H:

$$\{\mathfrak{p}_G \cup \mathfrak{B}_G\} \setminus \{\mathfrak{p}_H \cup \mathfrak{B}_H\} = \{x\};$$

ce sommet x est appelé *sommet de thèse*.

Soient H_0 les éléments d'entrée de H. Soit $\mathbb{K}$ un corps algébriquement clos. On dit qu'un énoncé d'incidence *est vrai* dans $\mathbb{K}$ où qu'il est un *théorème* en $\mathbb{K}$ s'il est vrai pour des réalisations génériques de H_0, c'est-à-dire, s'il existe un ensemble dense L dans l'espace de réalisations de H_0 tel que:

- Pour chaque $\widetilde{h} \in L$, la construction H est bien défini.

- Si $\widetilde{p} \in R_H$ est une réalisation de H construite à partir de $\widetilde{h} \in L$, alors il y a un élément $\widetilde{x}$ tel que $(\widetilde{p}, \widetilde{x})$ soit une réalisation de G.

Dans le contexte tropical, la construction H est bien définie pour toute entrée gràce à la notion de stabilité. Un énoncé *est vrai* ou il est un *théorème* sur le plan tropical si, pour chaque réalisation p de H obtenue par la construction, il existe un élément x tel que (p, x) soit une réalisation tropicale de G.

Un énoncé d'incidence constructible est *admissible* si la construction associée aux hypothèses est une construction admissible. Avec ce langage, on peut prouver que:

Théorème 5.3 *Soit $\mathcal{Z} = (G, H, x)$ un énoncé d'incidence constructible admissible. Si $\mathcal{Z}$ est vrai dans un corps algébriquement clos $\mathbb{K}$, alors il est vrai pour tout plan tropical.*

En utilisant cette technique on a démontré avec succès des versions tropicales du Théorème de la configuration du plan de Fano (5.4), du Théorème de Pappus (5.5), de la réciproque du Théorème de Pascal (5.6), du Théorème de Chasles (5.7) et de sa généralisation le Théorème de Cayley-Bacharach (5.8), ainsi qu'une version non universelle du Théorème de Pascal (5.9).

En particulier, avec la preuve du Théorème du Pappus, on donne une réponse positive à une conjecture formulée dans [RGST05]. Dans cet article, les auteurs donnent deux énoncés du Théorème de Pappus équivalents dans le contexte algébrique, mais qui ne le sont pas dans le contexte tropical. Les auteurs fournissent un contrexemple au premier de ces énoncés, et conjecturent que l'autre énoncé est toujours vrai. Mais ce deuxième énoncé est un énoncé d'incidence constructible dont l'hypothèse est une construction admissible. Par conséquent, en appliquant les techniques qu'on a développées, on démontre que cette énoncé est toujours vrai.

Hypercercles et Simplification de Courbes Paramétriques

Dans cette deuxième partie de la thèse on étudie un problème différent, dans lequel on apporte aussi un outil original pour son analyse et sa résolution. Pour présenter le contexte du problème, on introduit l'exemple suivant:

Exemple Considérons les paramétrisations du cercle unité $x^2 + y^2 - 1 = 0 \subseteq \mathbb{C}^2$ suivantes:

$$\phi(t) = \left(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1} \right)$$

$$\psi(t) = \left(\frac{2+2t^2+2t^4}{2+2t^2+3t^4+2t^6+t^8}, \frac{2t^2+3t^4+2t^6+t^8}{2+2t^2+3t^4+2t^6+t^8} \right)$$

$$\eta(t) = \left(\frac{2\sqrt{2}t^2-6t-4\sqrt{2}}{3t^2-2t\sqrt{2}+9}, \frac{t^2+6\sqrt{2}t-7}{3t^2-2\sqrt{2}t+9} \right)$$

La première paramétrisation est une paramétrisation classique qui est calculée à partir du faisceau de droites passent par le point $(0, 1)$. La seconde paramétrisation est *plus compliquée*, puisque le degré des fonctions rationnelles ψ est plus grand que le

degré du cercle. Le problème avec la troisième paramétrisation est que ses coefficients ne sont pas rationnels, mais appartiennent au corps $\mathbb{Q}(\sqrt{2})$.

La simplification de la seconde paramétrisation $\psi(t)$ peut être effectuée par (une version constructive de) le Théorème de Lüroth. Ce théorème affirme que toute paramétrisation rationnelle d'une courbe peut être remplacée par une paramétrisation birationelle. Dans notre exemple on peut obtenir une paramétrisation birationelle par le changement $1 + t^2 + t^4 = s$.

La troisième paramétrisation pose un autre type de problème. Est-ce qu'il est possible d'obtenir à partir de $\eta(t)$ une paramétrisation semblable à $\phi(t)$? Dans ce cas on demande s'il existe des algorithmes qui permettent de passer d'une paramétrisation avec des coefficients algébriques à une représentation avec des coefficients rationnels, ou plus généralement: Soit C une courbe donnée au moyen d'une paramétrisation $\eta(t)$, avec des coordonnées dans $\mathbb{K}(\alpha)(t)$ où $\mathbb{K}$ est un corps de caractéristique zéro et α est un élément algébrique sur $\mathbb{K}$; on cherche des méthodes pour calculer si une paramétrisation $\phi(t)$ de C est possible, mais cette fois avec des coefficients dans le corps $\mathbb{K}$.

Dans un contexte de calcul formel, par rapport au problème qu'on veut résoudre, il peut être plus intéressant d'avoir une représentation implicite ou paramétrique d'une courbe rationnelle. Bien que les deux représentations soient équivalentes et qu'on connaisse des algorithmes pour passer d'une représentation à l'autre, ces algorithmes peuvent être trop coûteux. Par conséquent, dans notre problème de reparamétrisation, on cherche des méthodes qui permettent de calculer cette reparamétrisation sans utiliser des techniques d'implicitation, c'est-à-dire sans calculer les équations implicites de la courbe à traiter.

Une réponse à cette question est l'utilisation d'une courbe auxiliaire, introduite par Andradas, Recio et Sendra dans [ARS99]. Cette courbe auxiliaire codifie, géométriquement, le changement de paramètre nécessaire pour résoudre le problème proposé. Dans l'exemple, le changement de paramètre nécessaire pour passer de la paramétrisation $\eta(t)$ à $\phi(t)$ est

$$t \to \frac{2\sqrt{2}t + 1}{t - \sqrt{2}}$$

Cette homographie peut être écrite comme

$$\frac{2\sqrt{2}t + 1}{t - \sqrt{2}} = \frac{5t}{t^2 - 2} + \sqrt{2}\frac{1 + 2t^2}{t^2 - 2}.$$

L'hyperbole définie par la paramétrisation $\left(\frac{5t}{t^2-2}, \frac{1+2t^2}{t^2-2}\right)$ codifie l'information nécessaire pour obtenir la reparamétrisation souhaitée du cercle dans l'exemple. Cette courbe obtenue par l'écriture d'une homografie dans la base $(1, \sqrt{2})$ est appelée hypercercle dans [ARS99].

Définition 8.1 Soit $u(t) = \frac{at+b}{ct+d} \in \mathbb{K}(\alpha)(t)$ une homographie, $ad - bc \neq 0$. On suppose que $[\mathbb{K}(\alpha) : \mathbb{K}] = n$ et soit

$$u(t) = \sum_{i=0}^{n-1} \phi_i(t)\alpha^i, \ \phi_i(t) \in \mathbb{K}(t)$$

l'expression de cette homographie dans la base $\{1, \alpha, \ldots, \alpha^{n-1}\}$. *L'hypercercle* associé a $u(t)$ est la courbe paramétrée par $(\phi_0, \ldots, \phi_{n-1})$ sur la clôture algébrique de $\mathbb{K}$.

Chapitre 6

Dans ce Chapitre on présente le contexte algébrique dans lequel on travaillera. Si $\mathbb{F}$ est un corps algébriquement clos de caractéristique zéro et $\mathbb{K} \subseteq \mathbb{F}$ est un sous-corps, on est intéressé dans l'étude des $\mathbb{K}$-variétés, c'est-à-dire, les variétés algébriques qui peuvent être exprimée comme l'ensemble des solutions communes à une famille de polynômes à coefficients dans $\mathbb{K}$. On présente quelques caractérisations classiques des $\mathbb{K}$-variétés et quelques-unes des propriétés géométriques qui peuvent être définies de manière rationnelle, c'est-à-dire à partir de l'idéal de polynômes à coefficients en $\mathbb{K}$ et avec des opérations dans le corps $\mathbb{K}$ seulement. On adapte à ce contexte des notions classiques comme l'irréductibilité d'une variété sur $\mathbb{K}$, la birationalité des variétés sur $\mathbb{K}$ ainsi que la possibilité de paramétriser une courbe sur le corps $\mathbb{K}$. On étudie aussi la relation existant entre les topologies de Zariski de $\mathbb{F}^n$ pour différents sous-corps $\mathbb{K}$ de $\mathbb{F}$, où la topologie $\tau_{\mathbb{K}}$ de $\mathbb{F}^n$ est la topologie dont les fermés sont les sous-variétés de $\mathbb{F}^n$ définissables sur $\mathbb{K}$.

Ce résumé de résultats classiques est inclus dans la thèse pour deux raisons. D'abord pour que la thèse soit autocontenue. Ensuite, parce qu'on ne connait aucune référence standard où tous ces résultats soient rassemblés et formulés dans un langage proche de nos intérêts. La référence de base de ce Chapitre est [ZS75b].

Chapitre 7

Dans ce Chapitre on rappelle la définition de la variété de Weil dans le cas implicite et on présente une construction analogue dans le cas paramétrique.

Définition 7.1 Soit $\mathbb{K}$ un corps de caractéristique zéro, $\mathbb{F}$ sa clôture algébrique et $\alpha \in \mathbb{F}$ un élément algébrique de degré d sur le corps $\mathbb{K}$. Soit

$$\mathcal{V} = \{f_1(x_1, \ldots, x_n) = \ldots = f_r(x_1, \ldots, x_n) = 0\} \subseteq \mathbb{F}^n$$

une variété algébrique de dimension m, où $f_j \in \mathbb{K}(\alpha)[x_1, \ldots, x_n]$, $1 \leq j \leq r$.

On définit la variété de Weil associée à $\mathcal{V}$ comme dans [Wei95]: on remplace chaque variable x_j par $x_{j0} + \alpha x_{j1} + \cdots + \alpha^{d-1} x_{j,d-1}$, où on a introduit de nouvelles variables x_{ji}. On peut réécrire f_k dans ce nouvel ensemble de variables:

$$f_k(x_{(1)}; \ldots; x_{(n)}) \in \mathbb{K}(\alpha)[x_{(1)}; \ldots; x_{(n)}],$$

où $x_{(j)}$ dénote le vecteur de variables $(x_{j0}, \ldots, x_{j,d-1})$. Le polynôme $f_k(x_{(1)}; \ldots; x_{(n)})$ peut être écrit comme

$$f_{k0}(x_{(1)}; \ldots; x_{(n)}) + \alpha f_{k1}(x_{(1)}; \ldots; x_{(n)}) + \cdots + \alpha^{d-1} f_{k,d-1}(x_{(1)}; \ldots; x_{(n)})$$

avec $f_{ki} \in \mathbb{K}[x_{(1)}; \ldots; x_{(n)}]$ univoquement déterminés. La variété $\mathcal{W}$ définie par les polynômes f_{ki} est la *variété de Weil* associée à $\mathcal{V}$.

$$W = \{f_{ki}(x_{(1)}; \ldots; x_{(n)}) = 0 \mid k = 1, \ldots, r, i = 0, \ldots, d-1\} \subseteq \mathbb{F}^{nd}$$

Par définition, cette variété est toujours définie sur le corps $\mathbb{K}$. Il est connu (cf. [Wei95]) que la variété $\mathcal{V}$ peut être définie sur $\mathbb{K}$ si et seulement si la variété $\widetilde{W} = W \cap \{x_{ji} = 0 \mid j = 1, \ldots, n, i \geq 1\}$ a la même dimension que $\mathcal{V}$. Cette méthode fonctionne pour une représentation implicite de la variété. Puisqu'on souhaite travailler avec une courbe paramétrique, on introduit une construction analogue pour le cas paramétrique qui s'inspires de [ARS99] dans le cas des courbes.

À cet effet, soit $\mathcal{V}$ une variété donnée par la paramétrisation unirationnelle

$$\begin{array}{rccc} \phi(t): & \mathbb{F}^m & \rightarrow & \mathbb{F}^n \\ & (t_1, \ldots, t_m) & \rightarrow & (\phi_1(t_1, \ldots, t_m), \ldots, \phi_n(t_1, \ldots, t_m)) \end{array}$$

où $\phi_k \in \mathbb{K}(\alpha)(x_1, \ldots, x_n)$. Chaque fonction coordonnée ϕ_k a une représentation comme un quotient

$$\phi_k(t_1, \ldots, t_m) = \frac{h_k(t_1, \ldots, t_m)}{g_k(t_1, \ldots, t_m)}, \quad h_k, g_k \in \mathbb{K}[x_1, \ldots, x_n].$$

En outre, en remplaçant g_k par le plus petit commun multiple des dénominateurs g_k, on peut supposer que le dénominateur g est commun et que la représentation des fonctions rationnelles n'a pas de composante commune: $\gcd(h_1(t), \ldots, h_n(t), g(t)) = 1$.

Définition 7.6 Soit $\phi = (\phi_1, \ldots, \phi_n)$ comme ci-dessus, écrivons $t_j = t_{j0} + t_{j1}\alpha + \cdots + t_{j,d-1}\alpha^{d-1}$, où t_{ji} sont de nouvelles variables. La substitution de ces variables dans ϕ définit des fonctions rationnelles dans $\mathbb{K}(\alpha)(t_{(1)}; \ldots; t_{(m)})$, où $t_{(j)}$ dénote le vecteur de variables $(t_{j0}, \ldots, t_{j,d-1})$.

Ces fonctions rationnelles ont une expression unique comme:

$$\phi_k = \phi_{k0}(t_{(1)}; \ldots; t_{(m)}) + \alpha\phi_{k1}(t_{(1)}; \ldots; t_{(m)}) + \cdots + \phi_{k,d-1}\alpha^{d-1}(t_{(1)}; \ldots; t_{(m)}),$$

$\phi_{ki} \in \mathbb{K}(t_{(1)}; \ldots; t_{(m)})$. L'application unirationnelle $\phi : \mathbb{F}^{md} \rightarrow \mathbb{F}^{nd}$ définie par

$$\begin{array}{ccc} \begin{pmatrix} t_{10} & \ldots & t_{1d-1}; \\ t_{20} & \ldots & t_{2d-1}; \\ \ldots\ldots\ldots & & \\ t_{m0} & \ldots & t_{md-1} \end{pmatrix} & \rightarrow & \begin{pmatrix} \phi_{10}(t_{(1)}; \ldots; t_{(m)}) & \ldots & \phi_{1d-1}(t_{(1)}; \ldots; t_{(m)}); \\ \phi_{20}(t_{(1)}; \ldots; t_{(m)}) & \ldots & \phi_{2d-1}(t_{(1)}; \ldots; t_{(m)}); \\ \ldots\ldots\ldots & & \\ \phi_{n0}(t_{(1)}; \ldots; t_{(m)}) & \ldots & \phi_{nd-1}(t_{(1)}; \ldots; t_{(m)}) \end{pmatrix} \end{array}$$

est appelée la paramétrisation obtenue par expansion de ϕ.

On a que Φ paramétrise la variété de Weil $\mathcal{W}$ et que Φ est birationnel si et seulement si ϕ est birationnel. On définit la *variété témoin* comme

Définition 7.12 Soit $Y = \{t \in \mathbb{F}^{md} \mid \phi_{ki}(t) = 0, i > 0\}$. Soient $\phi_{ki} = h_{ki}(t)/\delta(t)$ écris avec un dénominateur commun. Soit D_δ l'ensemble des points où $\delta \neq 0$. On définit la *variété témoin* de $\mathcal{V}$ comme la clôture de Zariski de $Y \cap D_\delta$.

Avec ces définitions, le principal résultat original de ce Chapitre est:

Théorème 7.11 *Soit U l'ensemble des points $t \in D_\delta$ tels que $\Phi^{-1}(\Phi(t))$ soit fini. Alors, $\mathcal{V}$ est définie sur $\mathbb{K}$ si et seulement si* $\dim(Y \cap D_\delta \cap U) = \dim(\mathcal{V})$. *En outre,*

dans ce cas, si $\tau : \mathbb{F}^m \to Y \cap D_\delta \cap U$ *est une paramétrisation unirationnelle d'une composante de* $Y \cap D_\delta \cap U$ *de dimension* $\dim(\mathcal{V})$*, alors* $\big(\phi_{10}(\tau), \ldots, \phi_{n0}(\tau)\big)$ *est une paramétrisation de* $\mathcal{V}$ *sur* $\mathbb{K}$*.*

Dans le cas birationnel, on peut déterminer quelle est la structure géométrique de la composante paramétrisable. Pour cela on introduit la notion d'hyperquadrique.

Définition 7.15 Soit θ un $\mathbb{F}$-automorphisme du corps de fonctions rationnelles à m variables

$$\theta : \mathbb{F}(t_1, \ldots, t_m) \to \mathbb{F}(t_1, \ldots, t_m)$$

défini par la substitution

$$t_1 = \theta_1(t_1, \ldots, t_m), \ldots, t_m = \theta_m(t_1, \ldots, t_m).$$

On suppose que les coefficients de θ_j appartiennent à $\mathbb{K}(\alpha)$ et on développe chaque fonction rationnelle comme

$$\theta_j(t_1, \ldots, t_m) = \sum_{i=0}^{d-1} \theta_{ji}(t_1, \ldots, t_m)\alpha^i, \theta_{ji} \in \mathbb{K}(t_1, \ldots, t_m).$$

Une *hyperquadrique* est la variété de $\mathbb{F}^{md}$ paramétrisée par les composantes $\theta_{ji}, j = 1, \ldots, m$, $i = 0, \ldots, d-1$ des automorphismes θ dans la base $1, \alpha, \ldots, \alpha^{d-1}$.

Avec cette notation on a:

Théorème 7.16 *Supposons que* ϕ *est birationnel. Alors* $\mathcal{V}$ *est paramétrisable sur* $\mathbb{K}$ *et* θ *est un automorphisme de* $\mathbb{F}^{md}$ *à coefficients dans* $\mathbb{K}(\alpha)$ *tel que* $\phi(\theta) \in \mathbb{K}(t_1, \ldots, t_m)$ *si et seulement si* $Y \cap D_\delta \cap U$ *a une composante qui est l'hyperquadrique associée à* θ*.*

On présente finalement une série d'exemples et contrexemples qui montrent comment fonctionne la méthode et comment les hypothèses des théorèmes sont nécessaires, spécialement la présence des ensembles D_δ et U dans les énoncés des théorèmes.

Chapitre 8

Dans ce Chapitre on étudie les propriétés des hypercercles, c'est-à-dire des hyperquadriques de dimension 1. Les résultats de ce Chapitre sont le résultat d'un travail commun avec les professeurs Recio, Sendra et Villarino. La principale contribution est un théorème de structure des hypercercles:

Théorème 8.7 *Soit* $\mathcal{U}$ *l'hypercercle associé à l'isomorphisme* $u(t) = \frac{at+b}{t+d} \in \mathbb{K}(\alpha)(t)$*, soit* $r = [\mathbb{K}(-d) : \mathbb{K}]$*. Alors, il existe une transformation projective* $\rho : \mathbb{P}(\mathbb{F})^n \longrightarrow \mathbb{P}(\mathbb{F})^n$*, définie sur* $\mathbb{K}$ *tel que la courbe* $\rho(\mathcal{U})$ *soit la courbe rationnelle normale de degré* r *dans* $\mathbb{P}(\mathbb{F})^n$ *paramétrisée par*

$$\widetilde{\rho}(t : s) = [s^r : s^{r-1}t : \cdots : st^{r-1} : t^r : 0 : \cdots : 0].$$

On déduit de ce théorème les propriétés plus importantes des hypercercles:

Corollaire 8.8 *Dans les conditions précédentes:*

1. *$\mathcal{U}$ est une courbe de degré r.*

2. *$\mathcal{U}$ est contenu dans une variété linéaire de dimension r et n'est contenu dans aucune variété linéaire de dimension $r-1$.*

3. *$\mathcal{U}$ est non-singulière dans $\mathbb{P}(\mathbb{F})^n$.*

4. *La fonction de Hilbert de $\mathcal{U}$ est égale à son polynôme de Hilbert, $h_{\mathcal{U}}(m) = mn+1$.*

Une manière de distinguer un hypercercle d'une courbe rationnelle normale arbitraire est au moyen de ses points à l'infini. Si $\mathbb{K}(\alpha)$ est de degré n sur $\mathbb{K}$ et $\mathcal{U}$ est un hypercercle de degré n, alors les points à l'infini de $\mathcal{U}$ ne dépendent que de l'extension $\mathbb{K} \subseteq \mathbb{K}(\alpha)$. Si $P = \{P_1, \ldots, p_n\}$ sont les points à l'infini de $\mathcal{U}$, alors

$$\{x_0 + \alpha_j x_1 + \cdots + \alpha_j^{n-1} x_{n-1} = 0\} \cap \overline{\mathcal{U}} = P \setminus \{P_j\},$$

où $\alpha_j = \sigma_j(\alpha)$ sont les conjugués de α dans $\mathbb{F}$, $1 \leq j \leq n$ et $\overline{\mathcal{U}}$ est la clôture projective de $\mathcal{U}$.

La caractérisation projective des hypercercles et la connaissance des points à l'infini fournissent des méthodes de paramétrisation et d'implicitation adaptés aux hypercercles. La contribution originale la plus significative de ce point de vue est la méthode suivante d'implicitation. Rappelons qu'un système de générateurs de l'idéal homogène de la courbe rationnelle normale de degré n est $\{y_i y_{j-1} - y_{i-1} y_j \mid 1 \leq i, j \leq n\}$ (cf. [Har92]).

Théorème 8.21 *Soit $\varphi(t) = (\frac{q_0(t)}{n(t)}, \ldots, \frac{q_{n-1}(t)}{n(t)})$ une paramétrisation propre d'un hypercercle $\mathcal{U}$ de degré n avec des coefficients dans $\mathbb{F}$. Soit I l'idéal homogène de la courbe rationnelle normale de degré n dans $\mathbb{P}(\mathbb{F})^n$ exprimée par des polynômes homogènes $h_1(\bar{y}), \ldots, h_r(\bar{y})$, $\bar{y} = (y_0, \ldots, y_n)$ (par exemple, les génerateurs décrits avant). Soit $\mathcal{Q} \in \mathcal{M}_{n+1 \times n+1}(\mathbb{F})$ la matrice de changement de base de $\{q_0(t), \ldots, q_{n-1}(t), N(t)\}$ à $\{1, t, \ldots, t^n\}$. Soit*

$$f_i(\bar{x}) = h_i\left(\sum_{j=0}^{n} \mathcal{Q}_{0j} x_j, \ldots, \sum_{j=0}^{n} \mathcal{Q}_{nj} x_j\right), \ 1 \leq i \leq r$$

Alors, $\{f_1, \ldots, f_r\}$ est un ensemble de générateurs de l'idéal homogène de $\mathcal{U}$.

En outre, les propriétés des hypercercles fournissent la caractérisation suivante des hypercercles de degré maximal.

Théorème 8.24 *Soit $\mathcal{U} \subseteq \mathbb{F}^n$ un ensemble algébrique de degré n tel que toutes ses composantes sont de dimension 1. Alors, $\mathcal{U}$ est un hypercercle si et seulement s'il a une infinité de points à coordonnées dans $\mathbb{K}$ et passe par les points à l'infini propres à un hypercercle.*

Chapitre 9

Dans ce Chapitre on présente la relation entre les hypercercles et la variété témoin définie dans le Chapitre 7. Dans ce cas, on peut raffiner les résultats présentés dans le Chapitre 7. Premièrement, l'introduction de l'ensemble U où la paramétrisation Φ est à fibres finies n'est pas nécessaire dans les hypothèses des théorèmes parce qu'on peut démontrer que, dans le cas des courbes, l'application Φ obtenue par développement est toujours à fibres finies dans l'ensemble D_δ. D'autre part, la variété témoin a au plus une composante de dimension 1. Ces résultats simplifient énormément les calculs dans le cas de courbes. Si $\mathcal{Z}$ est la variété témoin associé à une courbe $\mathcal{V}$, alors on a les possibilités suivantes:

- ou bien $\mathcal{Z}$ est un ensemble fini et $\mathcal{V}$ n'est pas $\mathbb{K}$-definissable.
- ou bien $\dim(\mathcal{Z}) = 1$, alors $\mathcal{V}$ est $\mathbb{K}$-définissable; $\mathcal{V}$ est $\mathbb{K}$-paramétrisable si et seulement si la seule composante de dimension 1 de $\mathcal{Z}$ est un hypercercle.

En particulier, on peut utiliser tous les résultats présentés dans le Chapitre 8 pour étudier la composante de dimension 1 de $\mathcal{Z}$.

En plus, dans le cas où le corps de base est $\mathbb{K} = \mathbb{Q}$ le corps des rationnels, on fait l'observation suivante. Si une courbe définie sur $\mathbb{Q}$ n'est pas $\mathbb{Q}$ paramétrisable, il existe des corps quadratiques $\mathbb{Q}(\beta)$ qui paramétrisent la courbe. Comme corollaire de ces affirmations on a la propriété suivante:

Corollaire 9.9 *Soit $\mathcal{V}$ une courbe définie sur $\mathbb{Q}$, paramétrisée sur $\mathbb{Q}(\alpha)$ et tel qu'elle n'est pas paramétrisable sur $\mathbb{Q}$. Soit $\mathcal{U}$ la composante de dimension 1 de la variété témoin associée à $\mathcal{V}$. Alors, il existe une infinité de corps quadratiques différents $\mathbb{Q}(\beta)$ tels que $\mathcal{U}$ soit un hypercercle pour l'extension $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\beta, \alpha)$.*

À partir d'ici, on peut obtenir une application à la reparamétrisation de $\mathcal{V}$. On donne un résultat sur les reparamétrisations optimales de $\mathcal{V}$ par un changement affine de paramètre $t \mapsto e_1 t + e_2$. La principale contribution originale dans cette direction est la suivante:

Théorème 9.12 *Soit $\mathcal{V}$ une courbe définie sur $\mathbb{Q}$ donnée par une paramétrisation ϕ à coefficients dans $\mathbb{Q}(\alpha)$. Alors, il existe toujours un point $[a_0 : \ldots : a_{n-1} : 0]$ à l'infini de la variété témoin $\mathcal{U}$ qui est représentable sur le corps $\mathbb{Q}(\alpha)$ et qu'on suppose deshomogénéisé à l'indice i ($a_i = 1$). Soit $r < n$ le degré de $\mathcal{U}$. Dans ces conditions $\mathcal{V}$ peut être paramétrisée sur $\mathbb{Q}(\gamma) = \mathbb{Q}(a_0, \ldots, a_{n-1}) \subseteq \mathbb{Q}(\alpha)$, où $[\mathbb{Q}(\gamma) : \mathbb{Q}] = r$.*

En outre, si $e_1, e_2 \in \mathbb{C}$, $e_1 \neq 0$ sont des nombres algébriques, soit $\phi(e_1 t + e_2)$ une autre paramétrisation de $\mathcal{V}$ et soit $\mathbb{L}$ le corps engendré sur $\mathbb{Q}$ par les coefficients de $\phi(e_1 t + e_2)$, alors

1. *$\mathbb{L}$ contient un corps (isomorphe à) $\mathbb{Q}(\gamma)$.*
2. *$[\mathbb{L} : \mathbb{Q}] \geq r$.*
3. *Si $[\mathbb{L} : \mathbb{Q}] = r$ alors $\mathbb{L}$ est isomorphe à $\mathbb{Q}(\gamma)$.*

4. Il y a $e'_1, e'_2 \in \mathbb{L}$ *tel que* $e'_1 t + e'_2$ *paramétrise* ϕ *sur (un corps isomorphe à)* $\mathbb{Q}(\gamma)$.

Notation

Part I.

- $\mathbb{K}$ is an algebraically closed field provided with a rank 1 valuation.
- k is the residual field of $\mathbb{K}$
- The valuation group is denoted by Γ. This set, once we define the tropical addition and product is denoted by $\mathbb{T}$.
- The tropical operations in $\mathbb{T}$ are the tropical addition "$a + b$" $= max(a, b)$ and tropical product "$a \cdot b$" = "ab" $= a + b$.
- T is the tropicalization or projection map.
- $\mathcal{T}(f)$ is the tropical hypersurface associated to the polynomial f.
- $\mathcal{I}$, $\mathcal{J}$ will denote Ideals.
- $V(\mathcal{I})$ is the algebraic variety defined by $\mathcal{I}$.
- The tropical objects will be denoted by latin letters: q, C for points and curves, a, b, c for elements in the semifield $\mathbb{T}$ etc.
- x, y, z we will denote variables.
- The lift or preimage of an element X is denoted by $\widetilde{X}$.
- I, J will denote the support of a curve C, if it is needed to avoid confusions we will use $I(C)$, $\delta = \delta(I)$ is its cardinal and $\Delta = \Delta(I)$ is its convex hull in $\mathbb{R}^2$.
- $Subdiv(\Delta)$ is the subdivision of the Newton polygon Δ dual to a tropical curve.
- Δ_q is the cell in $Subdiv(\Delta)$ dual to the one containing the point q.
- α, β, γ will denote elements in the residual field k.
- We will write $\alpha t^{-a} + \ldots$ or $\alpha t^{-a} + o(t^{-a})$ to denote an element of tropicalization a and principal coefficient α.
- $\mathcal{M}(\Delta_1, \Delta_2)$ is the mixed volume of two polygons Δ_1, Δ_2.

- $R(I, J, \mathbb{K})$ is the resultant of two generic polynomials of supports I, J with coefficients in $\mathbb{K}$.
- $R(I, J, \mathbb{K})_t$ is the tropicalization of $R(I, J, \mathbb{K})$.
- Given a tropical matrix A and a matrix B over an arbitrary ring, $\Delta_A(B)$ denotes the pseudodeterminant of B with respect to weight A.
- G is a finite incidence structure.
- $\mathfrak{p}$ denotes the points of G.
- $\mathfrak{B}$ is the set of blocks or curves of G.
- $\mathfrak{I}$ is the set of flags or incidence conditions of G.
- S_G is the algebraic support of G.
- S_G^t, the tropical support of G.
- R_G, the space of algebraic realizations of G.
- R_G^t the space of tropical configurations of G.
- *Sup* The support map that associates every curve C with its support $I(C)$.
- $\mathfrak{C}$ an abstract geometric construction.
- S_n the group of permutations of n elements.
- σ, a permutation of S_n.
- $|A|_t$ the tropical determinant of A.
- $\mathfrak{S}$ the definable set in k^N associated to a tropical instance of a construction.

Part II.

- $\mathbb{K}$ will be a field of characteristic zero, $\mathbb{K} \subseteq \mathbb{L}$ a finite algebraic extension of degree n and $\mathbb{F}$ the algebraic closure of $\mathbb{K}$.
- α will be a primitive element of $\mathbb{L}$ over $\mathbb{K}$.
- $u(t)$ will be a unit under composition of $\mathbb{L}(t)$. That is, $u(t) = \frac{at+b}{ct+d}$ with $ad-bc \neq 0$. Its inverse $\frac{-dt+b}{ct-a}$ is denoted by $v(t)$.
- For $u(t) = \frac{at+b}{ct+d}$ and $c \neq 0$, $M(t) = t^r + k_{r-1}t^{r-1} + \cdots + k_0 \in \mathbb{K}[t]$ denotes the minimal polynomial of $-d/c$ over $\mathbb{K}$.

- We will denote as $m(t)$ the polynomial obtained by dividing $M(t)$ by $ct+d$. That is, $m(t) = \dfrac{M(t)}{ct+d} = l_{r-1}t^{r-1} + l_{r-2}t^{r-2} + \cdots + l_0 \in \mathbb{L}[t]$.
- Sometimes we will represent $u(t)$ as

$$u(t) = \frac{(at+b)m(t)}{M(t)} = \frac{p_0(t) + p_1(t)\alpha + \cdots + p_{n-1}(t)\alpha^{n-1}}{M(t)},$$

  where $p_i(t) \in \mathbb{K}[t]$.
- By $\{\sigma_1 = Id, \sigma_2, \ldots, \sigma_s\}$, $s \geq n$ we will denote the group of $\mathbb{K}$ - automorphisms of the normal closure of $\mathbb{K} \subseteq \mathbb{L}$.
- We will represent by $\{\alpha_1 = \alpha, \ldots, \alpha_n\}$ the conjugates of α. We assume without loss of generality that $\sigma_i(\alpha) = \alpha_i$ for $i = 1, \ldots, n$.

Part I

Construction of Configurations in Tropical Geometry

Chapter 1

Preliminaries

Tropical Geometry is a rather new topic in Mathematics. Its main characteristic is the substitution of algebraic varieties by suitable polyhedral complexes. Many geometric concepts can be translated to this context. However, this translation sometimes contradicts our geometric intuition.

The approach to Tropical Geometry chosen is defining tropical varieties as non archimedean amoebas, see [EKL04]. Fixed an algebraically closed field and a valuation on it, a tropical variety is the set of valuations of the points in an algebraic variety. Determining these valuations already appear in the classical method of Newton Puiseux to compute solutions of a bivariate polynomial as fractional power series [Wal50]. A generalization to planar curves is presented in [Tha64], where some components of tropical curves are described and it is proved their relationship with the bivariate Newton polytope. We will not restrict our interest to working with just one variety.

Our objective in this Chapter is to study the relationship of algebraic and tropical realizations of incidence configurations of curves and points. In order to achieve this, we start with an introduction of tropical varieties and the statement of some problems that appear when trying to give geometric significance to these objects.

1.1 Basic Notions of Valued Fields

In this Section we recall the basic notions and properties of valued fields (cf [ZS75b]) that will be used later.

Definition 1.1. Let $\mathbb{K}$ be a field, Γ a totally ordered abelian group, a *valuation* is a map:

$$v: \quad \mathbb{K}^* \quad \longrightarrow \quad \Gamma$$

such that

- $v(ab) = v(a) + v(b)$ (it is a group homomorphism)
- If $a + b \neq 0$, $v(a + b) \geq \min\{v(a), v(b)\}$

In this case, $\mathbb{K}$ is a *valued field* and Γ is its *valuation group*.

From the definition, it follows that $v(a^{-1}) = -v(a)$, $v(-a) = v(a)$ and, if $v(a) \neq v(b)$ then $v(a+b) = \min\{v(a), v(b)\}$. It is sometimes useful to extend the valuation to the whole field, defining $\overline{\Gamma} = \Gamma \cup \{\infty\}$, $v(0) = \infty$ with the usual extended operations, for $g \in \Gamma$, $g + \infty = \infty + \infty = \infty$, $g < \infty$. We will also suppose that the valuation is always onto Γ.

Definition 1.2. Let $\mathbb{K}$ be a valued field. Let $V = \{x \in \mathbb{K} \mid v(x) \geq 0\}$. This set is the *valuation ring* of $\mathbb{K}$. It is a local integral domain whose maximal ideal is $m = \{x \in \mathbb{K} \mid v(x) > 0\}$. The field $k = V/m$ is the *residual field* of $\mathbb{K}$. It follows from the definition that $V^* = \{x \in \mathbb{K} \mid v(x) = 0\}$.

Valued fields can be classified at a first step by their characteristic. This classification will be relevant in Chapter 3. If $\mathbb{K}$ is a field of characteristic $p > 0$, then V is an integral domain of characteristic p that projects onto k. Thus, in this case, k must be a field of characteristic p. If $\mathbb{K}$ is a characteristic 0 field, we have that $\mathbb{Z} \subseteq V$. Hence, $\mathbb{Z} \cap m$ is an ideal of $\mathbb{Z}$. There are two possibilities, if $\mathbb{Z} \cap m = (0)$, then k is also a characteristic zero field and $\mathbb{Q} \subseteq V$. If $\mathbb{Z} \cap m = (p)$, then k is a characteristic p field and the local ring $\mathbb{Z}_{(p)} \subseteq V$. This is called the p-adic case.

The case when $\mathrm{char}(k)$=$\mathrm{char}(\mathbb{K})$ is called the *equicharacteristic case*. In this case the prime field of k may be identified with the prime field of $\mathbb{K}$. One would like to identify k with a subfield of $\mathbb{K}$, but this is not always possible. For example, let $\mathbb{K} = \mathbb{Q}(\sqrt{2}+\sqrt{3}t) \subseteq \mathbb{C}((t))$, where $\mathbb{C}((t))$ is the field of complex Laurent series, equipped with the valuation of the order. $\mathbb{K}$ is a valued field with the restriction of the valuation of $\mathbb{C}((t))$ to $\mathbb{K}$. $\sqrt{2} = \overline{\sqrt{2} + \sqrt{3}t} \in k$, but $\sqrt{2} \notin \mathbb{Q}(\sqrt{2} + \sqrt{3}t)$, because $\sqrt{2} + \sqrt{3}t$ is transcendent over $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2} + \sqrt{3}t) \cong \mathbb{Q}(t)$. However, we are showing in the next Proposition that if $\mathbb{K}$ is algebraically closed this problem never arise.

Proposition 1.3. *Let $\mathbb{K}$ be an algebraically closed equicharacteristic field with residual field k. Then, $\mathbb{K}$ contains a subfield isomorphic to k via the canonical projection. $\pi : V \to k$. Moreover, k is also an algebraically closed field.*

Proof. The prime field F of $\mathbb{K}$ can be identified with the prime field of k. Let L be a transcendence basis of k over F. Let $\widetilde{L}$ be any system of representatives of L in V, then $\widetilde{L}$ is algebraically independent over F. Namely, if a nonzero polynomial f with coefficients in F is such that $f(\widetilde{l}_1, \ldots, \widetilde{l}_n) = 0$, using the projection, we obtain that $f(l_1, \ldots, l_n) = 0$, which is a contradiction with the algebraic independence of L in k. So, these two fields may be identified.

$$\begin{array}{ccc} V & \xrightarrow{\pi} & k \\ F(\widetilde{L}) & \mapsto & F(L) \end{array}$$

Let $\widetilde{k}$ be the algebraic closure of $F(\widetilde{L})$ in $\mathbb{K}$. Then, $\widetilde{k}^*$ is contained in V^*. Let $x \in \widetilde{k}^*$ and $f = \sum_{i=0}^{n} a_i x^i$ be its minimal polynomial over $F(\widetilde{L})$. In particular, the coefficients a_i different from zero are always of valuation zero. Note that a_0 and a_n are always different from zero. If x were not a valuation zero element, then $v(x^i) \neq v(x^j)$ whenever $i \neq j$ and $v(f(x)) = \min\{0, v(x^n)\}$. It follows that $f(x) \neq 0$ and x cannot be a root of

f. On the other hand, π is injective on $\widetilde{k}$ because if $\pi(x) = 0$, then $x = 0$ or $x \notin V^*$. We have that $\widetilde{k} \cong \pi(\widetilde{k}) \subseteq k$ is an algebraically closed field containing $F(L)$. Thus, $k = \pi(\widetilde{k})$ and k is algebraically closed. □

We have seen that, in certain cases, we may suppose that $k \subseteq \mathbb{K}$. Now, we are proving that we can also suppose that the valuation group is isomorphic to a subgroup of the multiplicative group of $\mathbb{K}^*$.

Proposition 1.4. *Let $\mathbb{K}$ be a not necessarily equicharacteristic algebraically closed valued field. Then $\mathbb{K}^*$ contains a subgroup isomorphic to Γ by the map*

$$\phi : \mathbb{K}^* \to \Gamma \cong \mathbb{K}^*/V^*.$$

Proof. The reasoning uses Zorn's Lemma. Take the family of all subgroups of $\mathbb{K}$ such that the projection into Γ is injective. This is not an empty family, because it contains the trivial subgroup $\{1\}$. Furthermore, it is an inductive family by the inclusion. Let G be a maximal element. Then G projects into a subgroup of Γ. In this case, the projection is also onto. If this were not the case, there would be an element u of Γ not belonging to the image. Take the group $< \phi(G), u >$, this is the image of $\phi(G) \oplus \mathbb{Z}$ by the map $(g, n) \mapsto g + nu$. If this map is injective, then $< \phi(G), u >= \phi(G) \oplus < u >$ is a direct sum. Let v be any element of $\mathbb{K}^*$ such that $\phi(v) = u$. Then $G \oplus < v >$ is a group isomorphic to $\phi(G) \oplus u$. This is a contradiction with the maximality of G. If the projection of $G \oplus \mathbb{Z}$ is non injective, let n be the minimum element of $\mathbb{N}^*$ such that there is a $g \in G$ with $\phi(g) = nu$. If $w \in G$ and $\phi(w) = mu$, then $m = rn$, $r \in \mathbb{Z}$ and $w = g^r$. Let v be any root of the polynomial $x^n - g$ in $\mathbb{K}^*$. It follows that the projection is injective in the group $< G, v >$ and its image is isomorphic to $< \phi(G), u >$, which contradicts again the maximality of G. □

If G is a subgroup of $\mathbb{K}^*$ isomorphic to Γ by ϕ, we denote $G = t^\Gamma$. $t^\gamma \in t^\Gamma$ denotes the unique element of G such that $\phi(t^\gamma) = \gamma$. By the isomorphism, we have that $t^u t^v = t^{u+v}$, $t^0 = 1$, $t^{-u} = (t^u)^{-1}$. From now on, we will always suppose that we are given a fixed subgroup $t^\Gamma \subseteq \mathbb{K}^*$ with these characteristics.

In the Puiseux series case $\mathbb{K} = \mathbb{C}[[t^{\mathbb{Q}}]]$, every element is a power series of the form

$$x = \sum_{z=z_0}^{\infty} a_{z/n} t^{z/n}, z_0, n \in \mathbb{Z}, n > 0.$$

The valuation is $v(x) = \min\{z/n | a_{z/n} \neq 0\}$. In this case, the valuation group is isomorphic to the subgroup G of $\mathbb{K}$ consisting in the elements $\{t^q, q \in \mathbb{Q}\}$. Without loss of generality, if an element $x \neq 0$, we may suppose that $a_{z_0/n} \neq 0$ (equivalently $v(x) = z_0/n$). The term $a_{z_0/n} \in \mathbb{C}$ is usually called the principal coefficient of the series and the element $a_{z_0/n} t^{z_0/n} \in \mathbb{K}$ is called the principal term. This concepts can be extended to a general field.

Definition 1.5. Suppose fixed the subgroup G defined in Proposition 1.4. Let $x \in \mathbb{K}^*$, $u = v(x)$, then $xt^{-u} \in V^*$. We write

$$Pc(x) = \pi(xt^{-u}) = y \in k$$

the *principal coefficient* of x. The *principal term* of x is denoted by $Pt(x) = yt^u$. This principal element is only a notation, it is not an element of $\mathbb{K}$ nor k. It happens that $v(z) = v(x) < v(x-z)$ if and only if $Pt(z) = Pt(x)$. Usually we will write

$$x = yt^u + \dots \quad \text{or} \quad yt^u + o(t^u)$$

in order to emphasize the principal term of an element x.

This notion of principal coefficient is essential in our context. Our geometric objects in $\mathbb{K}^n$ will be supposed to be generic. But the genericity conditions will be stated in terms of the principal coefficients of elements defining our objects. So, we introduce the notion of residually genericity.

Definition 1.6. Let $x \in \mathbb{K}^n$ be a point, we say that x is *residually generic* if $Pc(x) \in k^n$ is generic.

Proposition 1.3 proves that if a polynomial has every nonzero coefficient of valuation zero, then all its non zero roots have valuation zero. This is a particular case of a well known phenomenon. Given a polynomial, we can compute the valuations of its roots from the valuations of its coefficients. This is a precursor of the facts about tropical varieties we will face later. Because of its importance, we provide a complete proof here. For the notation used and the approach itself we refer to [KLP03].

Definition 1.7. Let Γ be the valuation group of $\mathbb{K}$. If Γ is isomorphic to an ordered subgroup of $\mathbb{R}$. Then we say that the valuation is of *rank one*. In this case, we will always suppose that $v : \mathbb{K}^* \to \Gamma \subseteq \mathbb{R}$.

Let $f = \sum_{i=0}^{n-1} a_i x^i \in \mathbb{K}[x]$, the *Newton diagram* of f is the set $\{(i, v(a_i)) \mid 0 \leq i \leq n\} \subseteq \mathbb{N} \times \overline{\Gamma}$. If the valuation is of rank one, $\Gamma \subseteq \mathbb{R}$, we may define the Newton polygon as the convex hull of $\{(i, x) \mid 0 \leq i \leq n, x \geq v(a_i)\} \subseteq \mathbb{R}^2$. Given two different vertices $(i, v(a_i))$, $(j, v(a_j))$ of the Newton diagram of f such that $a_i, a_j \neq 0$, we define the *slope between the vertices* $(i, v(a_i))$ and $(j, v(a_j))$ as the quantity $(v(a_j) - v(a_i))/(j - i)$. The slope of two such vertices is always well defined, since it can be easily checked that if $\mathbb{K}$ is algebraically closed then Γ is always a division group.

The next goal is the classical study of the valuations of the roots of f. So, we may suppose that $a_n = 1$ and that $a_0 \neq 0$. In the case where $\Gamma \subseteq \mathbb{R}$, it is usually proved that the valuations of the roots are the opposite of the slopes of the lower convex hull of the Newton polygon (See, [Wal50]). To provide a similar result in the general case, in [KLP03] two *consecutive points of the Newton diagram* are defined as two points $(i, v(a_i))$, $(j, v(a_j))$, $j > i$ such that:

- If $k < i$, $$\frac{v(a_i) - v(a_k)}{i - k} < \frac{v(a_j) - v(a_i)}{j - i}$$
- If $i < k < j$, $$\frac{v(a_k) - v(a_i)}{k - i} \geq \frac{v(a_j) - v(a_i)}{j - i}$$
- If $k > j$, $$\frac{v(a_k) - v(a_j)}{k - j} > \frac{v(a_j) - v(a_i)}{j - i}$$

Note that is $a_i = 0$ or $a_j = 0$ then $(i, v(a_i)), (j, v(a_j))$ are not two consecutive points of the Newton diagram.

Proposition 1.8. *Let $\widetilde{f} = \sum_{i=0}^{n} a_i x^i$. Let $[x_1, \ldots, x_n]$ be the list of roots of $\widetilde{f}$ ordered by the valuation, $v(x_i) \leq v(x_{i+1})$. Let $0 \leq i < j \leq n$ be two elements such that*

$$v(x_1) \leq \ldots \leq v(x_{n-j}) < v(x_{n-j+1}) = \cdots = v(x_{n-i}) < v(x_{n-i+1}) \leq \ldots \leq v(x_n).$$

Then, $(i, v(a_i))$, $(j, v(a_j)) \in \mathbb{N} \times \Gamma$ are two consecutive points on the Newton diagram of $\widetilde{f}$ and the slope between (i, a_i) and (j, a_j) is $-v(x_{n-i}) = -v(x_{n-j+1})$.

Proof. We write the coefficients of f as symmetric functions of the roots:

$$a_i = (-1)^{n-i} \sum_{\substack{J \subset \{1,\ldots,n\} \\ \#J = n-i}} \prod_{l \in J} x_l.$$

If $v(x_k) < v(x_{k+1})$, we have that $v(x_1 \cdots x_k) < v(x_{i_1} \cdots x_{i_k})$ for every subset $\{i_1, \ldots i_k\}$ of k elements different from $\{1, \ldots, k\}$. Thus, we have that $v(a_{n-k}) = v(x_1 \cdots x_k)$. On the other hand, if $v(x_k) = v(x_{k+1})$, we can only affirm that $v(x_1 \cdots x_k) \leq v(x_{i_1} \cdots x_{i_k})$ and the equality hold, for example, for the set $\{1, \ldots, k-1, k+1\}$. In this case $v(a_{n-k}) \geq v(x_1 \cdots x_k)$.

As $v(x_{n-i}) < v(x_{n-i+1})$ and $v(x_{n-j}) < v(x_{n-j+1})$, then $v(a_j) = v(x_1 \cdots x_{n-j})$ and

$$v(a_i) = v(x_1 \cdots x_{n-i}) = v(x_1 \cdots x_{n-j}) + (j-i)v(x_{n-i}),$$

from this,

$$\frac{v(a_j) - v(a_i)}{j - i} = -v(x_{n-i}).$$

If $i < k < j$, then $v(a_k) \geq v(x_1 \cdots x_{n-k}) = v(a_i) - (k-i)v(x_i)$, hence

$$\frac{v(a_k) - v(a_i)}{k - i} \geq -v(x_{n-i}) = \frac{v(a_j) - v(a_i)}{j - i}.$$

If $k < i$, $v(a_k) \geq v(x_1 \cdots x_{n-k}) = v(x_1 \cdots x_{n-i}) + v(x_{n-i+1} \cdots x_{n-k}) > v(a_i) + (i-k)v(x_{n-i})$ it happens that

$$\frac{v(a_i) - v(a_k)}{i - k} < -v(x_{n-i}) = \frac{v(a_j) - v(a_i)}{j - i}$$

Finally, if $k > j$, $v(a_j) = v(x_1 \cdots x_{n-j}) = v(x_1 \cdots x_{n-k}) + v(x_{n-k+1} \cdots x_{n-j}) < v(a_k) + (k-j)v(x_{n-j+1})$, so

$$\frac{v(a_k) - v(a_j)}{k - j} > -v(x_{n-j+1}) = \frac{v(a_j) - v(a_i)}{j - i}$$

□

Thus, every block of roots of the polynomial corresponds with a segment whose vertices are consecutive points of the Newton diagram of f. Furthermore, the valuation of these roots is the opposite of the slope of the segment and the number of roots with this valuation is exactly the integer length of the segment, $(j-i)$. As f has n roots and the Newton diagram has length n, there is a bijection between the valuation of the roots and the slopes of the Newton diagram. Once we know the valuation of the roots, the next step is to determine the principal terms of the roots.

Proposition 1.9. *Let $\widetilde{f} = \sum_{l=0}^{n} a_l x^l$ be a monic polynomial such that $a_0 \neq 0$. Let $(i, v(a_i))$, $(j, v(a_j))$, $j > i$ be two consecutive points of the Newton diagram of $\widetilde{f}$. Let $v = -\frac{v(a_j)-v(a_i)}{j-i}$, $\widetilde{g} = \widetilde{f}(xt^v)$. Let w be the minimal valuation of the coefficients of $\widetilde{g}$ and let g be the residual polynomial of $t^{-w}\widetilde{g}$ mod m. Then, the degree of g is j and its order is i. Let $[b_{n-j+1}t^v, \ldots, b_{n-i}t^v]$ be the list of principal terms of the roots of $\widetilde{f}$ of valuation v counted with multiplicity. Then, the list of nonzero roots of g counted with multiplicities is $[b_{n-j+1}, \ldots, b_{n-i}]$.*

Proof. $\widetilde{f} = \prod(x - x_k)$, where $v(x_k) \leq v(x_{k+1})$. Let $Pc(x_k) = b_k t^{v_k}$.

$$\widetilde{f}(xt^v) = \prod_{l=1}^{n}(xt^v - x_l) = \prod_{l=1}^{n-j}(xt^v - x_l) \times \prod_{l=n-j+1}^{n-i}(xt^v - x_l) \times \prod_{l=n-i+1}^{n}(xt^v - x_l)$$

$$= t^{nv} \times \prod_{l=1}^{n-j}(x - x_l t^{-v}) \times \prod_{l=n-j+1}^{n-i}(x - x_l t^{-v}) \times \prod_{l=n-i+1}^{n}(x - x_l t^{-v})$$

Once normalized by t^{-w}, the minimum of the valuations of the coefficients is zero. so we can compute the residual polynomial.

$$g(x) = Pc(t^{-w}\widetilde{f}(xt^v)) = \prod_{l=1}^{n-j} Pc(-x_l) \times \prod_{l=n-j+1}^{n-i}(x - Pc(x_l)) \times \prod_{l=n-i+1}^{n} x$$

From this expression, it is deduced that the degree of g is j, its order is i and its roots, counted with multiplicities are $Pc(x_l)$, $n - j + 1 \leq l \leq n - i$. That is, the principal coefficients of the roots of $\widetilde{f}$ of valuation v. □

1.2 Tropical Varieties

Definition 1.10. Let $\mathbb{K}$ be an algebraically closed field with a rank one valuation $v : \mathbb{K} \to \Gamma$. Without loss of generality, we may suppose that $\mathbb{Q} \subseteq \Gamma \subseteq \mathbb{R}$. The *tropicalization map* is the opposite of the valuation

$$\begin{array}{rccc} T: & \mathbb{K}^* & \to & \mathbb{T} = \Gamma \\ & x & \mapsto & T(x) = -v(x), \end{array}$$

Clearly $T(xy) = T(x) + T(y)$, and $T(x + y) = \max\{T(x), T(y)\}$ whenever $T(x) \neq T(y)$. This provides the set $\mathbb{T}$ with the algebraic structure of idempotent semifield with

the operations of *tropical addition* "$a+b$" $= \max\{a, b\}$ and *tropical product* "ab" $= a+b$. These operations are associative, commutative and distributive, "$a(b+c)$" = "$ab+ac$". Furthermore, every element a has a multiplicative inverse (the additive inverse $-a$ as an element of the group Γ and 0 is the neutral element for tropical multiplication.).

As in the valuation case, we may define a value $T(0) = -\infty$. This will be the identity element of the tropical addition. However, we will mainly work with finite elements of $\mathbb{T}$.

The *affine tropical space* is the set $\mathbb{T}^n$, each element of it is represented by a tuple $(a_1, \ldots, a_n)$. Every element can also be represented by a projective tuple, that is a $(n+1)-$tuple $[b_1 : \ldots : b_{n+1}]$ with the identification

$$[b_1 : \ldots : b_{n+1}] \sim [a_1 : \ldots : a_{n+1}]$$

if and only if there is an element $c \in \mathbb{T}$ such that $b_i =$ "ca_i", $1 \leq i \leq n+1$. The *tropical homogenization* and *dehomogenization* with respect to the $i-th$ coordinate is made by:

$$(b_1 - b_i, b_2 - b_i, \ldots, b_{i-1} - b_i, b_{i+1} - b_i, \ldots, b_{n+1} - b_i) \leftrightarrow [b_1 : \ldots : b_{i-1} : b_i : b_{i+1} : \ldots : b_n]$$

where the minus sign on the left denotes the subtraction in the group Γ that correspond with tropical division. Note that, as long as we are working in $\mathbb{T}^n$, $-\infty$ is never a valid coordinate, so there is a bijection between the affine and projective representations. We refer to [RGST05] for this projective notation of points.

Definition 1.11. Let $\widetilde{\mathcal{V}}$ be the variety in the algebraic torus $(\mathbb{K}^*)^n$ defined by a finite set of Laurent polynomials

$$\widetilde{f}_1, \ldots, \widetilde{f}_m \in \mathbb{K}[x_1, \ldots, x_n, x_1^{-1}, \ldots, x_n^{-1}],$$

$$\widetilde{\mathcal{V}} = \{x \in (\mathbb{K}^*)^n \mid \widetilde{f}_1(x) = \cdots = \widetilde{f}_m(x) = 0\}.$$

The *affine tropical variety* $T(\widetilde{\mathcal{V}}) \subseteq \mathbb{T}^n$ is the image of $\widetilde{\mathcal{V}}$ applying T componentwise.

$$\begin{array}{rccc} T: & (\mathbb{K}^*)^n & \longrightarrow & \mathbb{T}^n \\ & (x_1, \ldots, x_n) & \mapsto & \big(T(x_1), \ldots, T(x_n)\big) \\ & \widetilde{\mathcal{V}} & \mapsto & T(\widetilde{\mathcal{V}}) = \mathcal{V} \end{array}$$

That is, our geometric objects are the images of algebraic varieties in the torus. They are essentially the possible valuations of the points in $\widetilde{\mathcal{V}}$

The map T will be called *projection* or *tropicalization*. Given a tropical variety U, every algebraic variety projecting onto U (that always exists by definition) will be called a *lift* of U and will be denoted by $\widetilde{U}$. This lift is not unique.

The definition uses Laurent polynomials to define the varieties. But $\widetilde{\mathcal{V}}$ is invariant under multiplication of the polynomials $\widetilde{f}_i$ by a monomial. So, if necessary, we may always suppose that $\widetilde{f}_i$ is always a polynomial and that, for each variable x_j, the order of $\widetilde{f}_i$ with respect to x_j is zero.

1.2.1 Tropical Hypersurfaces

In this Section we provide a self contained notion of tropical hypersurface that does not need a specific projection T from a valued field. This definition is somehow necessary if we want to work with tropical objects on their own.

A Laurent *tropical polynomial* in n variables is a formal sum of monomials

$$\text{“}\sum_{i\in I} a_i x_1^{i_1}\dots x_n^{i_n}\text{”},\quad a_i\in\mathbb{T}$$

where I is the support of the polynomial, that is a finite subset in $\mathbb{Z}^n$. We may provide the set $\mathbb{T}[x_1,\dots,x_n]$ of polynomials with the structure of idempotent semiring, using tropical addition and product. The evaluation of the polynomial in a point $(b_1,\dots,b_n)$ is the element

$$\text{“}\sum_{i\in I} a_i b_1^{i_1}\dots b_n^{i_n}\text{”} = \max_{i\in I}\{a_i + i_1 b_1 + \dots + i_n b_n\}\in\mathbb{T}.$$

So every tropical polynomial is a convex piecewise affine function. Note that 0 is the multiplicative identity, so the monomials whose coefficient is 0 cannot be erased. The coefficient of a polynomial necessary in order to allow erasing should be $-\infty$ which does not belong to $\mathbb{T}$.

Definition 1.12. Let $f\in\mathbb{T}[x_1,\dots,x_n]$ be a tropical polynomial. The set of zeroes of f is the set of points b where the value $f(b)$ is attained for at least two different indices $i,j\in I$

$$V(f) = \bigcup_{i\neq j\in I}\{b\in\mathbb{T}^n | a_i + i_1 b_1 + \dots + i_n b_n = a_j + j_1 b_1 + \dots + j_n b_n = f(b)\}$$

$$\bigcup_{i\neq j\in I}\{b\in\mathbb{T}^n | \forall\, k\ \ a_i + i_1 b_1 + \dots + i_n b_n = a_j + j_1 b_1 + \dots + j_n b_n \geq a_k + k_1 b_1 + \dots + k_n b_n\}$$

Equivalently, if we consider the piecewise affine function $f:\mathbb{R}^n\to\mathbb{R}$ and W is the corner locus of this function (the set of points where f is not differentiable), then $V(f) = W\cap\mathbb{T}^n$.

The set of zeroes of a tropical polynomial is a polyhedral complex of pure dimension $n-1$. The relevant fact is that it coincides with the notion of tropical hypersurface.

Theorem 1.13 (Kapranov's Theorem)**.** *Let $\widetilde{f} = \sum_{i\in I}\widetilde{a}_i x_1^{i_1}\dots x_n^{i_n}$ be a polynomial in $\mathbb{K}[x_1,\dots,x_n]$. Let $f = \text{“}\sum_{i\in I} T(\widetilde{a}_i) x_1^{i_1}\dots x_n^{i_n}\text{”}$ be the tropical polynomial whose coefficients are the projection of the coefficients of $\widetilde{f}$. Then $T(\{\widetilde{f}=0\})$ is exactly the set of zeroes of f.*

Proof. See for example [EKL04]. □

This Theorem only describes the possible projections of the points belonging to an algebraic hypersurface. For the applications, we will need more information. Namely, we will need the possible principal terms of the points in a hypersurface. We introduce the following notions.

Definition 1.14. Let $\widetilde{f} = \sum_{i\in I} \widetilde{a}_i x^i \in \mathbb{K}[x]$ be a polynomial of support I in n variables $x = x_1, \ldots, x_n$, $i = i_1, \ldots, i_n$, $Pc(\widetilde{a}_i) = \alpha_i$, $T(\widetilde{a}_i) = a_i$, $f(x) = \text{“}\sum_{i\in I} a_i x^i$. Let $b = (b_1, \ldots, b_n) \in \mathbb{T}^n$ be a tropical point. Let

$$\widetilde{f}_b(x_1, \ldots, x_n) = \sum_{\substack{i\in I \\ a_i + i_1 b_1 + \cdots + i_n b_n = f(b_1,\ldots,b_n)}} \alpha_i x^i = Pc(\widetilde{f}(x_1 t^{-b_1}, \ldots, x_n t^{-b_n}))$$

be the *residual polynomial over b*. This is a non zero polynomial in $k[x_1, \ldots, x_n]$.

That is, we rewrite the polynomial as $\widetilde{f}(x_1 t^{-b_1}, \ldots, x_n t^{-b_n})$ as

$$\widetilde{f}(xt^{-b}) = \widetilde{f}_b(x) t^{-f(b)} + o(t^{-f(b)}).$$

Remark 1.15. By construction, the monomials of $\widetilde{f}_b$ correspond with the indices i where $f(b)$ is attained. Hence, the following assertions are equivalent:

- $b \in \mathcal{T}(f)$.
- $\widetilde{f}_b$ contains at least two monomials.
- There is a root of $\widetilde{f}_b$ in $(k^*)^n$.

With the notion of residual polynomial, we can derive what the possible principal terms of the points in a given hypersurface are.

Theorem 1.16. *Let $\widetilde{f} = \sum_{i\in I} \widetilde{a}_i x^i \in \mathbb{K}[x_1, \ldots, x_n]$ be a polynomial. Then, given*

$$(\gamma_1, \ldots, \gamma_n) \in (k^*)^n, \quad (b_1, \ldots, b_n) \in \mathbb{T}^n,$$

there is a point $\widetilde{b} = (\widetilde{b}_1, \ldots, \widetilde{b}_n) \in V(\widetilde{f})$ with $Pc(\widetilde{b}_j) = \gamma_j, T(\widetilde{b}_j) = b_j$ if and only if $(b_1, \ldots, b_n) \in \mathcal{T}(f)$ and $\widetilde{f}_b(\gamma_1, \ldots, \gamma_n) = 0$.

Proof. The only if condition is trivial. The if condition is done by induction on n, for $n = 1$ this is the result proved in Proposition 1.9. Now assume $n > 1$ and that the result holds for less than n variables. Fix a system of representatives $(\widetilde{b}_1, \ldots, \widetilde{b}_n)$ of $(\gamma_1, \ldots, \gamma_n)$, that is take $\widetilde{b}_i$ any element of valuation 0 whose residual class is γ_i. If $\widetilde{f}(bt^{-b}) = 0$, we are done. If there is a variable x_j that does not appear in $\widetilde{f}_b$, we evaluate the variable x_j of $\widetilde{f}$ in $\widetilde{b}_i t^{-b_i}$ without changing the hypothesis. So, without loss of generality, all the variables $x_1, \ldots, x_n$ appear in $\widetilde{f}_b$. Here, we distinguish two cases:

• If there is an index j, $1 \leq j \leq n$, such that $\widetilde{f}_b(x_1, \ldots, \gamma_j, \ldots, x_n) \neq 0$ then, reordering the variables if necessary, we may take $j = 1$. Let us write $b = (b_1, b')$, $x = (x_1, x')$, $\gamma = (\gamma_1, \gamma')$. The conditions needed to apply induction over $\widetilde{g}(x') = \widetilde{f}(\widetilde{b}_1 t^{-b_1}, x')$ are:

$$b' = (b_2, \ldots, b_n) \in \mathcal{T}(g); \quad \widetilde{g}_{b'}(\gamma_2, \ldots, \gamma_n) = 0.$$

It is possible that $g \neq f(b_1, x)$, as showed in the Example 1.17. However, as $\widetilde{g}(x') = \widetilde{f}(\widetilde{b}_1 t^{-b_1}, x')$, it is verified that

$$\widetilde{g}(x't^{-b'}) = \widetilde{f}(\widetilde{b}_1 t^{-b_1}, x't^{-b'}) = \widetilde{f}_b(\gamma_1, x')t^{-f(b)} + o(t^{-f(b)}).$$

So $\widetilde{g}_{(b')}(\gamma') = \widetilde{f}_b(\gamma_1, \gamma') = 0$ and it is verified the second condition of Remark 1.15. By the equivalence there, $\gamma' \in (k^*)^{n-1}$ implies that $(b_2, \ldots, b_n) \in \mathcal{T}(g)$ as wanted. That is, with this substitution we can apply induction hypothesis and find the desired root.

• Suppose now that, for each i, $1 \leq i \leq n$, $\widetilde{f}_b(x_1, \ldots, \gamma_i, \ldots, x_n) = 0$. In order to follow with the induction step, recall that $\widetilde{f}(xt^{-b}) = \widetilde{f}_b t^{-f(b)} + o(t^{-f(b)})$. Write

$$\widetilde{f}_b = (x_1 - \gamma_1)^k (x_2 - \gamma_2) \cdots (x_n - \gamma_n) q(x_1, \ldots, x_n); q(\gamma_1, x') \neq 0.$$

Making here the same substitution $x_1 = \widetilde{b}_1$ as in the previous case would destroy the structure needed to ensure induction. To avoid this, let $\widetilde{h} = (x_1 - \widetilde{b}_1 t^{-b_1})^k (x_2 - \widetilde{b}_2 t^{-b_2}) \cdots (x_n - \widetilde{b}_n t^{-b_n}) \widetilde{q}(x_2 t^{b_2}, \ldots, x_n t^{b_n}) \neq 0$, where $\widetilde{q}(x_2, \ldots, x_n)$ is any polynomial such that $\widetilde{q} = q(x_2, \ldots, x_n)t^0 + o(t^0)$. Note that $\widetilde{h}_b = \widetilde{f}_b$ and that $\widetilde{h}(\widetilde{b}_1 t^{-b_1}, x') = 0$. Hence $\widetilde{f}(xt^{-b}) - \widetilde{h}(xt^{-b}) = ht^{-f(b)+\epsilon} + o(t^{f(b)+\epsilon})$, $0 < \epsilon \in \Gamma$, $h \in k[x_1, \ldots, x_n]$. We substitute x_1 by $\widetilde{b}_1 + t^{\frac{\epsilon}{2k}}$ instead. In this way

$$\widetilde{f}(\widetilde{b}_1 t^{-b_1}, x't^{-b'}) - \widetilde{h}(\widetilde{b}_1 t^{-b_1}, x't^{-b'}) = h(\gamma_1, x')t^{-f(b)+\epsilon} + o(t^{-f(b)+\epsilon})$$

but, as

$$\widetilde{h}((\widetilde{b}_1 + t^{\frac{\epsilon}{2k}})t^{-b_1}, x't^{-b'}) = t^{\frac{\epsilon}{2}}(x_2 - \widetilde{b}_2 t^{-b_2}) \cdots (x_n - \widetilde{b}_n t^{-b_n}) \widetilde{q}((\widetilde{b}_1 + t^{\frac{\epsilon}{2k}}), x_2, \ldots, x_n),$$

moreover $\widetilde{q}((\widetilde{b}_1 + t^{\frac{\epsilon}{2k}}), x') = q(\gamma_1, x')t^0 + o(t^0)$, so $\widetilde{h}(\widetilde{b}_1 t^{-b_1}, x't^{-b'})_{b'} =$

$$= \widetilde{f}(\widetilde{b}_1 t^{-b_1}, x't^{-b'})_{b'} = t^{-f(b)+\frac{\epsilon}{2}}(x_2 - \gamma_2) \cdots (x_n - \gamma_n) q(\gamma_1, x') + o(t^{-f(b)+\frac{\epsilon}{2}}).$$

Thus, let $\widetilde{g}(x') = \widetilde{f}((\widetilde{b}_1 + t^{\frac{\epsilon}{2k}})t^{-b_1}, x')$ and let us write as before $b' = (b_2, \ldots, b_n)$, $\gamma' = (\gamma_2, \ldots, \gamma_n)$. From the previous computations, $\widetilde{g}_{b'}(\gamma') = 0$. Hence, $(b_2, \ldots, b_n) \in \mathcal{T}(g)$ and we can apply induction. □

Example 1.17. Take the polynomial

$$\widetilde{f} = -3t^2 + 3tx - t^2 y + txy - t^3 xy^4 + (t^4 + t^5)y^4 + x^5$$

over the field of Puiseux series,

$$f = \text{“}(-2) + (-1)x + (-2)y + (-1)xy + (-3)xy^4 + (-4)y^4 + x^5\text{”} =$$

$$= \max\{-2, -1 + x, -2 + y, -1 + x + y, -3 + x + 4y, -4 + 4y, 0 + 5x\}$$

Let $b = (-1, 0) \in \mathcal{T}(f)$, $\widetilde{f}(tx, y) = (-3 + 3x - y + xy)t^2 + o(t^4)$. Thus, $\widetilde{f}_b = -3 + 3x - y + xy$, $\widetilde{f}_b(1, -3) = 0$. By Theorem 1.16, there is a root in $(\mathbb{K}^*)^2$ whose principal term is $(t, -3)$.

It happens that $\widetilde{f}_b(1,y) = \widetilde{f}_b(x,-3) = 0$, so we are in the second case of the Theorem. Perform the substitution $x = t + t^2$ in $\widetilde{f}$.

$$\widetilde{f}(t+t^2,y) = \widetilde{g}(y) = 3t^3 + t^5 + 5t^6 + 10t^7 + 10t^8 + 5t^9 + t^{10} + t^3 y,$$

$g(y) = (-3) + (-3)y$. In this case $g(y) \neq f(-1,y) = (-2) + (-2)y + (-4)y^4$, but even now, as proved in the Theorem, $0 \in \mathcal{T}(g)$. Now we are in the conditions of classical Newton-Puiseux method to compute a root of $\widetilde{g}(y)$ whose principal term is -3, this point is:

$$(x,y) = (t+t^2, -3 - t^2 - 5t^3 - 10t^4 - 10t^5 - 5t^6 - t^7)$$

Using these concepts, we can make abstraction and work with tropical hypersurfaces without having a concrete lift. For general varieties, this is not so easy. Even if abstract tropical varieties can be defined without the need of an ambient space, our objective is to work in the plane. So we are always working in a context of hypersurfaces and points and we may define a planar tropical curve as the set of zeroes of a bivariate tropical polynomial.

As in the algebraic torus case, multiplying a tropical polynomial by a monomial does not change the set of zeroes of $f = \text{“}\sum_{i\in I} a_i x^i\text{”}$. Thus, multiplying by an appropriate monomial, we can always assume that our polynomials are not Laurent polynomials, that is, every exponent in the variables is non negative. Moreover, we can suppose that for each variable x_j there is an index i such that x_j appear with exponent 0 in the monomial $a_i x^i$.

Another aspect we have to take into account is that different tropical polynomials may yield the same tropical hypersurface. For example, take the support $I = \{(0,0),(2,0),(0,2),(1,0)\}$ and the set of polynomials “$0 + ax + 0x^2 + 0y^2$” where $a \leq 0$. All of them define the same tropical curve in the plane, this is the set of three rays emerging from the point $(0,0)$ and directions $(-1,0),(0,-1),(1,1)$. So, in contrast with the algebraic case, it is not true that different Laurent polynomials define the same hypersurface if and only if they differ by the multiplication of a monomial. The previous variety is also defined by the polynomial “$0 + 0x^2 + 0y^2$”. So, tropical polynomials with different support can also define the same hypersurface. Next, we define a notion of a canonical polynomial of given support defining a tropical hypersurface $\mathcal{V}$. The approach chosen is using *concave polynomials*as in [Mik05].

Definition 1.18. To a given tropical polynomial $f = \text{“}\sum_{i\in I} a_i x^i\text{”}$, we may associate the function $\varphi : I \subseteq \mathbb{Z}^n \to \Gamma$, given by $\varphi(i) = a_i$. We say that φ is concave if for any (possibly non distinct) $i_0,\ldots,i_n \in I \subseteq \mathbb{Z}^n$ and any $t_0,\ldots,t_n \geq 0$ with $\sum_{k=0}^n t_k = 1$ and $\sum_{k=0}^n t_k i_k \in I$ we have

$$\varphi\Big(\sum_{k=0}^n t_k i_k\Big) \geq \sum_{k=0}^n t_k \varphi(b_k),$$

note that necessarily $t_k \in \mathbb{Q} \subseteq \Gamma$, so the sum on the right-hand side is well defined. In this case, we say that f is a *concave polynomial*.

Fixed the support I and a tropical hypersurface $\mathcal{V}$ defined by a polynomial g of support I, there is (up to a multiplicative constant) a unique concave tropical polynomial f of support I such that $\mathcal{T}(f) = \mathcal{V}$. Sometimes, it will be convenient to take precisely, the concave polynomial defining a hypersurface.

1.2.2 The Newton Polytope

Let I be the support of a tropical polynomial f, the convex hull $\Delta = \Delta(I)$ of I in $\mathbb{R}^n$ is the *Newton Polytope* of f. This object is strongly connected with the set of zeroes of f. Every tropical polynomial f defines a regular subdivision of its Newton polytope Δ. The topological closure of $\mathcal{T}(f)$ in $\mathbb{R}^n$ has naturally a structure of piecewise affine polyhedral complex. This complex is dual to the subdivision induced to Δ. To achieve this duality we have first to define the subdivision of Δ.

Let Δ' be the convex hull of the set $\{(i,t)|i \in I, t \leq a_i\} \subseteq \mathbb{R}^{n+1}$. The upper convex hull of Δ', that is, the set of boundary maximal cells whose outgoing normal vector has its last coordinate positive, projects onto Δ by deleting the last coordinate. This projection defines the regular subdivision of Δ associated to f (cf. [Mik05]).

Proposition 1.19. *The subdivision of Δ associated to f is dual to the set of zeroes of f. There is a bijection between the cells of $Subdiv(\Delta)$ and the cells of $\mathcal{T}(f)$ such that:*

- *Every k-dimensional cell Λ of Δ corresponds to a cell V^Λ of $\mathcal{T}(f)$ of dimension $n-k$ such that the affine linear space generated by V^Λ is orthogonal to Λ. (In the case where $k = 0$, the corresponding dual cell is a connected component of $\mathbb{R}^n \setminus \overline{\mathcal{T}(f)}$)*
- *If $\Lambda_1 \neq \Lambda_2$, then $V^{\Lambda_1} \cap V^{\Lambda_2} = \emptyset$*
- *If $\Lambda_1 \subset \overline{\Lambda}_2$, then $V^{\Lambda_2} \subset \overline{V^{\Lambda_1}}$*
- $\mathcal{T}(f) = \bigcup_{0 \neq \dim(\Lambda)} V^\Lambda$ *where the union is disjoint.*
- V^Λ *is not bounded if and only if* $\Lambda \subseteq \partial\Delta$.

From this, we deduce that, given a fixed support I, there are finitely many combinatorial types of tropical curves with support I. These different types are in bijection with the different regular subdivisions of Δ.

One of the first problems encountered in Tropical Geometry is that the Projective Geometry intuition is no longer valid. If we define a tropical line as the set of zeroes of a polynomial "$ax + by + c$", then two different lines always intersect at least in a point. The problem is that sometimes they intersect in more than one point. The usual answer to deal with this problem is using the notion of stable intersection.

Let C_f, C_g be the set of zeroes of two tropical polynomials f and g respectively. Let P be the intersection of the curves, $P = C_f \cap C_g$. It is possible that P can not be lifted to an algebraic variety $\widetilde{P}$. We want to associate, to each $q \in P$ an intersection multiplicity. We will follow the notions of [RGST05] and we will compare

them with the subdivisions of the associated Newton polygons of the curves in terms of mixed volumes. See [Stu02] to precise the comparison between mixed volumes and intersection of algebraic curves.

Let $C_{fg} = C_f \cup C_g$. It is easy to check that the union of the two tropical curves is the set of zeroes of the product "fg". The Newton polygon Δ_{fg} of $C_f \cup C_g$ is the Minkowski sum of Δ_f and Δ_g. That is:

$$\Delta_{fg} = \{x + y \mid x \in \Delta_f, y \in \Delta_g\}$$

The subdivision of Δ_{fg} dual to C_{fg} is a subdivision induced by the subdivisions of Δ_f, Δ_g. More concretely, let q be a point in C_{fg}, let $\{i_1, \ldots, i_n\}$ be the monomials of f where $f(q)$ is attained and let $\{j_1, \ldots, j_m\}$ be the monomials of g where $g(q)$ is attained. Then $n \geq 2$ or $m \geq 2$. The monomials where "fg" attains it maximum are $\{i_r j_s | \, 1 \leq r \leq n \, , 1 \leq s \leq m\}$. The Newton polygon of these monomials is the Minkowski sum of the Newton polygons of $\{i_1, \ldots, i_n\}$ and $\{j_1, \ldots, j_m\}$, each one of these Newton polygons is the cell dual to the cell containing q in Δ_{fg}, Δ_f and Δ_g respectively. This process covers every cell of dimension 1 and 2 of Δ_{fg}. The zero dimensional cells correspond to points q belong neither to C_f nor to C_g. Let i, j be the monomials of f and g where the value at q is attained. Then the monomial of "fg" where ("fg")(q) is attained is ij. To sum up, every cell of Δ_{fg} in naturally the Minkowski sum of a cell u of f and a cell v of g. The possible combination of dimensions $(\dim(u), \dim(v), \dim(u + v))$ are:

- $(0, 0, 0)$, these cells do not correspond to points of C_{fg}.
- $(1, 0, 1)$, these are edges of C_{fg} that correspond to a maximal segment contained in an edge of C_f that does not intersect C_g.
- $(2, 0, 2)$, correspond to the vertices of C_{fg} that are vertices of C_f that do not belong to C_g.
- $(1, 1, 2)$, this combination defines a vertex of C_{fg} which is the unique intersection point of an edge of C_f with an edge of C_g.
- $(1, 1, 1)$ are the edges of C_{fg} that are the infinite intersection of an edge of C_f and an edge of C_g.
- $(1, 2, 2)$ corresponds with the vertices of C_{fg} that are a vertex of C_g belonging to an edge of C_f.
- $(2, 2, 2)$ This is a vertex of C_{fg} which is a common vertex of C_f and C_g.

and the obvious symmetric cases $(0, 1, 1)$, $(0, 2, 2)$ and $(2, 1, 2)$.

If the relative position of C_f, C_g is generic, then C_{fg} cannot contain any cell of type $(1, 1, 1)$, $(1, 2, 2)$ and $(2, 2, 2)$. That is, the intersection points q of C_f and C_g are always the unique intersection point of an edge of C_f and an edge of C_g. This is the *transversal case*. The definition of *intersection multiplicity*, as presented in [RGST05] for these cells $(1, 1, 2)$ is the following:

Definition 1.20. Let q be an intersection point of two tropical curves C_f and C_g. Suppose that q is the unique intersection line of an edge r of C_f and an edge s of C_g. Let $\overrightarrow{r}$ the primitive vector in $\mathbb{Z}^2$ of the support line of r. Let $\overrightarrow{s}$ be the corresponding primitive vector of s. Let u be the dual edge of r in Δ_f and let v be the dual edge of s in Δ_g, we call $m_u = \#(\overline{u} \cap \mathbb{Z}^2) - 1$ and $m_v = \#(\overline{v} \cap \mathbb{Z}^2) - 1$ the *weight* of the edges r and s respectively. The *intersection multiplicity* is

$$mult(q) = \left| m_u m_v \begin{vmatrix} \overrightarrow{r}_x & \overrightarrow{r}_y \\ \overrightarrow{s}_x & \overrightarrow{s}_y \end{vmatrix} \right|$$

the absolute value of the determinant of the primitive vectors times the weight of the edges.

If the curves are not in a generic relative position, let us perform a infinitesimal translation in C_f in a generic direction, every cell of Δ_{fg} of type $(0,0,0)$, $(1,0,1)$, $(2,0,2)$, $(1,1,2)$ stays invariant. The cells of type $(1,1,1)$ are subdivided into cells of type $(0,0,0)$ and $(0,1,1)$. That is, if two edges intersect in infinitely many points, after the translation, every intersection point will disappear. Note that the mixed volume of the cells of type $(1,1,1)$ is always 0, so these points are always of multiplicity zero (they are not proper intersection points in the sense of perturbations). If q is an intersection point corresponding to a cell of type $(2,1,2)$ or $(2,2,2)$, after the perturbation, this cell is subdivided into cells of type $(0,0,0)$, $(1,0,1)$, $(1,1,2)$, $(2,0,2)$. That is, no intersection point is a vertex of f or g. However, some transversal intersection points appear instead (of type (1,1,2)) in a neighbourhood of q. The intersection multiplicity of q is, in this case, the sum of the intersection multiplicities of the transversal intersection points.

Now we provide the notion of stable intersection of curves (See [RGST05]).

Definition 1.21. Let C_f, C_g be two tropical curves. Let C_f^ϵ, C_g^ϵ be two small generic perturbations of C_f, C_g such that their intersection is finite. The *stable intersection* of C_f and C_g is the limit set of intersection points of the perturbed curves $\lim_{\epsilon \to 0}(C_f^\epsilon \cap C_g^\epsilon)$.

From the previous comments it is clear that

Proposition 1.22. *Let C_f, C_g be two tropical curves, then the stable intersection of C_f and C_g is the set of intersection points with positive multiplicity.*

This stable intersection has very nice properties. From the definition, it follows that it is continuous under small perturbations on the curves. Moreover, it verifies a Berstein-Koushnirenko Theorem for tropical curves.

Theorem 1.23. *Let C_f, C_g be two tropical curves of Newton Polygons Δ_f, Δ_g. Then the number of stable intersection points, counted with multiplicity is the mixed volumes of the Newton polygons of the curves*

$$\sum_{q \in C_f \cap_{st} C_g} m(q) = \mathcal{M}(\Delta_f, \Delta_g) = vol(\Delta_f + \Delta_g) - vol(\Delta_f) - vol(\Delta_g)$$

Proof. See [RGST05] □

In particular, we have the following alternative definition of intersection multiplicity for plane curves:

Corollary 1.24. *Let f, g be two tropical polynomials of Newton Polygons Δ_f, Δ_g respectively. Let $q \in \mathcal{T}(f) \cap \mathcal{T}(g)$ be an intersection point. Let Λ_f, Λ_g be the cells of $Subdiv(\Delta_f)$, $Subdiv(\Delta_g)$ dual to the cell in the curve containing q respectively, then, the tropical intersection multiplicity of q is:*

$$mult(q) = \mathcal{M}(\Lambda_f, \Lambda_g) = vol(\Lambda_f + \Lambda_g) - vol(\Lambda_f) - vol(\Lambda_g).$$

Proof. From the classification of intersection points, q is an intersection point of multiplicity zero if and only if it belongs to a cell of type $(1,1,1)$ in C_{fg}. In this case $\mathcal{M}(\Lambda_f, \Lambda_g) = vol(\Lambda_f + \Lambda_g) - vol(\Lambda_f) - vol(\Lambda_g) = 0$, because an edge have no area. If q is a stable intersection point, let $f = \text{“}\sum_{i\in\Delta_f} a_i x^{i_1} y^{i_2}\text{”}, g = \text{“}\sum_{j\in\Delta_g} b_j x^{j_1} y^{j_2}\text{”}$, let $f_q = \text{“}\sum_{i\in\Lambda_f} a_i x^{i}\text{”}, \quad g_q = \text{“}\sum_{j\in\Lambda_g} b_j x^{j}\text{”}$ be truncated polynomials. It follows from the definition that the intersection multiplicity of q only depends in the behaviour or the mixed cell $\Lambda_f + \Lambda_g$ in the dual subdivision of Δ_{fg}. That is, the intersection multiplicity of q as intersection of C_f and C_g equals the intersection multiplicity of q as an intersection point of $\mathcal{T}(f_q)$ and $\mathcal{T}(g_q)$. But, by construction, the unique stable intersection point of $\mathcal{T}(f_q)$ and $\mathcal{T}(g_q)$ is q itself. Hence, by Theorem 1.23, the intersection multiplicity of q is

$$\mathcal{M}(\Lambda_f, \Lambda_g) = vol(\Lambda_f + \Lambda_g) - vol(\Lambda_f) - vol(\Lambda_g).$$

□

This stability approach to solve the intersection problem behaves reasonably well: two different lines always intersect in only one stable intersection point. Even in the most degenerate case that both lines are the same there is still only one stable intersection point. Analogously we would like to define a unique line through two different points. More generally, given a support $I = \{i_1, \ldots, i_\delta\}$ and $\delta - 1$ sufficiently generic points in the algebraic case, there is only one curve of support I passing through them. So, given $\delta - 1$ points, we would like to define the tropical curve of support I passing through them. Again, this problem is not well defined, as long as there are sets of $\delta - 1$ points such that there are infinitely many curves of support I. Disallowing these sets of points as a valid choice to define a curve of support I is not well suited with the kind of problems we will face in the following Chapters. But, again, among the family of curves of support I passing through a set of points, there is always a distinguished curve that can be continuously deformed as we perturb our original set of points. This yields the notion of *stable curve* through a set of points.

Let $I = \{i_1, \ldots, i_\delta\}$ be a support, $i_k = (i_k^1, i_k^2)$ and $P = \{q_1, \ldots, q_{\delta-1}\}$ a set of tropical points. We may identify the polynomials of support I with the affine tropical space $\mathbb{T}^{\delta-1}$ by the correspondence

$$\text{“}\sum_{i\in I} a_i x^{i}\text{”} \leftrightarrow [a_{i_1} : a_{i_2} : \ldots : a_{i_\delta}]$$

Thus, we are identifying the polynomials that only differ by a multiplicative constant $c \in \mathbb{T}$. Each point $q_j = (q_j^1, q_j^2)$ defines a hyperplane in $\mathbb{T}^n$ of equation

$$H_{q_j} = \mathcal{T}(\text{“ } y_{i_1}(q_j^1)^{i_1^1}(q_j^2)^{i_1^2} + \ldots + y_{i_\delta}(q_j^1)^{i_\delta^1}(q_j^2)^{i_\delta^2} \text{ ”}).$$

Then q_j belong to $\mathcal{T}(f)$ if and only if $[a_{i_1} : \ldots : a_{i_\delta}]$ belong to the variety H_{q_j}. Then, the intersection of the $\delta - 1$ hyperplanes $H_{q_1}, \ldots, H_{q_{\delta-1}}$ is the curve passing through the set of points. As in the case of the intersection of curves, the intersection of $\delta - 1$ hyperplanes on $\mathbb{T}^{\delta-1}$ may contain more than one point. Still (cf. [RGST05]) there is only one distinguished point that is stable under perturbations of the hyperplanes and correspond to a curve g of support I that passes through the set of points and can be continuously deformed by small translations of the points. Hence, we can define:

Definition 1.25. Let I be a support. $\delta = \delta(I)$. Let $q_1, \ldots, q_{\delta-1}$ be tropical points. Let $H_{q_j} = \mathcal{T}(\text{“ } y_{i_1}(q_j^1)^{i_1^1}(q_j^2)^{i_1^2} + \ldots + y_{i_\delta}(q_j^1)^{i_\delta^1}(q_j^2)^{i_\delta^2} \text{ ”})$ be the associated hyperplanes in the space $\mathbb{T}^{\delta-1}$. Let $[a_{i_1} : \ldots : a_{i_\delta}]$ be the stable intersection of the hyperplanes $H_{q_1}, \ldots, H_{q_{\delta-1}}$. The curve defined by “$\sum_{i \in I} a_i x^{i^1} y^{i^2}$” is called the *stable curve* of support I passing through $\{q_1, \ldots, q_{\delta-1}\}$. Moreover, this defining polynomial is concave in the sense of Definition 1.18.

However, this stable approach is not free from problems, let $a = (0, 0)$, $b = (-2, 1)$, $c = (-1, 3)$ be three points in the tropical plane. Let l_1 be the stable line (support $\{(0, 0), (1, 0), (0, 1)\}$) through a and b, and let l_2 be the stable line through a, c. In fact l_1 is the only line through a and b and l_2 is the unique line through a and c. Let p be the stable intersection point of l_1, l_2. Then, in this case, $l_1 =$ “$1x + 0y + 1$”, $l_2 =$ “$3x + 0y + 3$” and, finally, $p = (0, 1) \neq a$. But, in Projective geometry, if $\widetilde{a}$, $\widetilde{b}$,, $\widetilde{c}$ are three non collinear points, then $\widetilde{l_1}$, $\widetilde{l_2}$ are well defined and their intersection is exactly $\widetilde{a}$. So there are no solution for the problem:
Are there four points $\widetilde{a}$, $\widetilde{b}$, $\widetilde{c}$, $\widetilde{p}$ and two lines $\widetilde{l_1}$, $\widetilde{l_2}$ such that

$$\widetilde{a}, \widetilde{b}, \widetilde{p} \in \widetilde{l_1}, \quad \widetilde{a}, \widetilde{c}, \widetilde{p} \in \widetilde{l_2},$$

$$T(\widetilde{a}) = a, T(\widetilde{b}) = b, T(\widetilde{c}) = c, T(\widetilde{l_1}) = l_1, T(\widetilde{l_2}) = l_2, T(\widetilde{p}) = p?$$

This is an example of a tropical realization of an incidence structure that is not the projection of an algebraic realization of the same incidence structure. Contrary to the previous example, the problem here cannot be avoided by perturbations of the elements a, b, c (because l_1, l_2, p are defined from them). This is the kind of problems we are trying to solve in next Section.

1.3 Incidence Structures

The classical definition of incidence structure (see [Dem68]) is used to formalize finite geometries. Intuitively, an incidence structure is a set of points, a set of lines and a set of incidence relations of type *point p belongs to line L*. In our context, we are not only dealing with lines, but with arbitrary curves in the plane. Still we will control

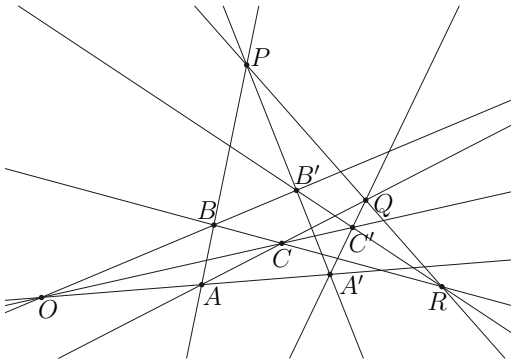


Figure 1.1: A realization of Desargues Theorem

which curves are acepted in an incidence structure. A first approach could be fixing the Newton polygon of the curves. However, without further effort in the proofs, we can fix the support of the curves. Hence, we introduce the notion of support in the plane.

Definition 1.26. The *support* of a hypersurface is a finite subset of $\mathbb{Z}^n$ modulo a translation by an integer vector in $\mathbb{Z}^n$. That is, let $\mathcal{P}^f(\mathbb{Z}^n)$ be the set of finite subsets of $\mathbb{Z}^n$ and let $\sim$ be the relation $A \sim B$ if and only if there is an integer vector $v \in \mathbb{Z}^n$ such that $A = v + B$. Then, the set of supports of $\mathbb{Z}^n$ is ${}^{\mathcal{P}^f(\mathbb{Z}^n)}\!/\!\sim$. Given a support $I \subseteq \mathbb{Z}^n$, $\delta = \delta(I)$ denotes the number of elements of I. $\Delta = cv(I)$, the convex hull of I in $\mathbb{R}^n$, is the *Newton polytope* of the hypersurface. Note that δ is invariant by translations, so it is well defined and Δ is well defined up to translations.

1.3.1 Abstract Formulation

Definition 1.27. A *finite incidence structure* is a tuple $G = (\mathfrak{p}, \mathfrak{B}, \mathfrak{I}, Sup)$, where

$$\mathfrak{p} \cap \mathfrak{B} = \emptyset, \quad \mathfrak{I} \subseteq \mathfrak{p} \times \mathfrak{B}$$

$$Sup : \mathfrak{B} \to {}^{\mathcal{P}^f(\mathbb{Z}^2)}\!/\!\sim$$

The elements of $\mathfrak{p}$ are called *points*, the elements of $\mathfrak{B}$ are *blocks* or *curves* and the elements of $\mathfrak{I}$ are *flags* or *incidence relations*. If $x \in \mathfrak{B}$, $Sup(x) \in {}^{\mathcal{P}^f(\mathbb{Z}^n)}\!/\!\sim$ is the support of x.

Every incidence structure $G = (\mathfrak{p}, \mathfrak{B}, \mathfrak{I}, Sup)$ is naturally identifiable with a labelled graph, the *Levi graph* of the incidence structure. This is the bipartite graph whose vertices are the elements of $\mathfrak{p} \cup \mathfrak{B}$ and its edges are the elements of $\mathfrak{I}$. Each element $x \in \mathfrak{B}$ has as label $Sup(x)$. These two notions of incidence structures will be used indistinctly.

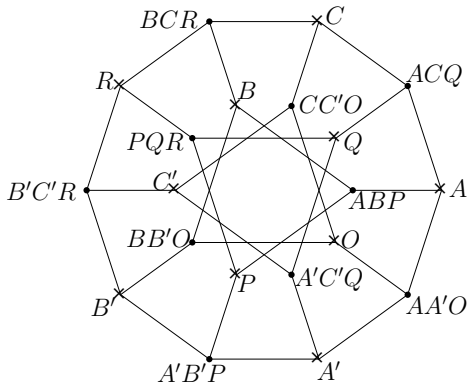


Figure 1.2: The graph of Desargues configuration

Example 1.28. Desargues Theorem states that two triangles are in perspective with respect to a point if and only they are perspective with respect to a line. Desargues configuration consists in ten points and ten lines. Its incidence structure is:

$$\mathfrak{p} = \{A, B, C, A', B', C', P, Q, R, O\},$$

$$\mathfrak{B} = \{AA'O, BB'O, CC'O, ABP, A'B'P, ACQ, A'C'Q, BCR, B'C'R, PQR\},$$

$$\mathfrak{I} = \{(X_1, X_1X_2X_3), (X_2, X_1X_2X_3), (X_3, X_1X_2X_3) \mid X_1X_2X_3 \in \mathfrak{B}\}.$$

As every curve in the structure is a line, the support map is constant

$$Sup(\mathfrak{B}) = \{(0,0), (1,0), (0,1)\}$$

Figure 1.1 shows an instance of Desargues configuration. Figure 1.2 represents the incidence graph G of Desargues configuration.

1.3.2 Tropical and Algebraic Realization

Definition 1.29. Let $G = (\mathfrak{p}, \mathfrak{B}, \mathfrak{I}, Sup)$ be an incidence structure. Denote by $n_{\mathfrak{p}}$, $n_{\mathfrak{B}}$ the cardinality of $\mathfrak{p}$, $\mathfrak{B}$ respectively. For each $y \in \mathfrak{B}$, let $\delta_y = \delta(Sup(y))$ the cardinal of the associated support. The algebraic support of G is the space

$$S_G = \prod_{x \in \mathfrak{p}} (\mathbb{K}^*)^2 \times \prod_{y \in \mathfrak{B}} (\mathbb{K}^*)^{\delta_y - 1}.$$

The tropical support of G is the space

$$S_G^t = \prod_{x \in \mathfrak{p}} \mathbb{T}^2 \times \prod_{y \in \mathfrak{B}} \mathbb{T}^{\delta_y - 1}.$$

We identify the space $(\mathbb{K}^*)^{\delta_y-1}$ (resp. $\mathbb{T}^{\delta_y-1}$) with the space of algebraic curves (resp. tropical curves) of support $Sup(y)$ (dehomogenizing the equation of the curve by a monomial). The dimension of S_G is $2n_{\mathfrak{p}} + \sum_{y\in\mathfrak{B}}(\delta_y - 1)$.

An algebraic realization (resp. tropical realization) of G is a point

$$(x_1, \ldots, x_{n_p}; y_1, \ldots, y_{n_c}) \in S_G \ (S_G^t)$$

such that, for every edge $(x_i, y_j) \in \mathfrak{I}$ we have that $x_i \in y_j$, identifying y_j with the plane (tropical) curve it represents. The set of algebraic realizations of G is an algebraic set R_G of S_G (resp. $R_G^t \subseteq S_G^t$).

A first problem we face at this level is that, in general, $T(R_G) \neq R_G^t$. This yields the following questions.

- When does $T(R_G)$ equal R_G^t?
- Given, $x \in R_G^t$, determine if x belongs to $T(R_G)$. In the affirmative case, compute a preimage $\widetilde{x}$ in R_G.

In particular, we try to answer these questions using the graph information of G.

This question could be approached using the notion of tropical basis. It would consist in taking the equations defining the variety R_G. A tropical basis can be computed from these defining equations (cf. [BJS$^+$07]), the projection of this basis is a set defining $T(R_G)$, so it would only rest to check if this basis defines R_G^t or not. This approach does not answer the problem of computing a preimage.

An alternative is to use the graph structure of G and, sometimes, we will not work with the hole variety R_G^t, but with a meaningful subset of it. This restriction in the set R_G^t will be clearer in the context of geometric constructions in Chapter 4. For the moment, we can derive some information from the graph structure alone.

1.4 Lifting of an Acyclic Graph

The main result in this Chapter is a complete solution when the incidence graph G is acyclic. In this case, every tropical realization of G can be lifted to the algebraic case.

Theorem 1.30. *Let G be an incidence structure such that its associated graph is acyclic. Then, $R_G = R_G^t$. That is, for every tropical realization x of G, there is an algebraic realization $\widetilde{x}$ of G that projects correctly $T(\widetilde{x}) = x$.*

Proof. Let G be the acyclic incidence graph. Reasoning on each connected component of G, we suppose, without loss of generality that G is a tree. Let x_0 be any node of G and let $\widetilde{x}_0$ be any lift of x to the algebraic context. The rest of the nodes can be inductively lifted from this one. Let y be an adjacent node to a node x that has already been lifted to $\widetilde{x}$. We distinguish two cases:

- $x \in \mathfrak{B}$ and $y \in \mathfrak{p}$. In this case x is a tropical curve, $\widetilde{x}$ is an algebraic curve projecting onto x and y is point in x. These are the conditions of Theorem 1.16. Thus, starting from y we can compute a point $\widetilde{y}$ belonging to $\widetilde{x}$ and projecting onto y.

- x is a point and y is a curve of support $I = Sup(y)$. y is a tropical curve of equation "$\sum_{i\in I} a_i z^i$", with variables $z = (z_1, z_2)$. The point $\widetilde{x}$ defines, in the configuration space of $\widetilde{y}$ the hypersurface H_x of curves of support I containing $\widetilde{x}$. Its equation is $\sum_{i\in I} a_i \widetilde{x}^i$, where the unknowns are the variables a_i. Moreover y belongs to the tropicalization of H_x. Thus, applying again Theorem 1.16, it can be computed a lift $\widetilde{y}$ of y passing through $\widetilde{x}$.

□

With this Theorem we present a partial answer to the question proposed. However, acyclic graphs are rather unattractive, because they cannot model many common situations. Even they cannot deal with the intersection of two conics, because there will be four intersection points (counted with multiplicities) connected to both curves and, hence a cycle in G. In next Chapters we will present some tools and a deeper understanding of the stable intersection of curves and the stable curve passing through a set of points. With these tools and the notion of geometric construction in Chapter 4 we will be able to extend the answer of Theorem 1.30

Chapter 2

Cramer's Rule and Points in General Position

Suppose given a support $I = \{i_1, \ldots, i_\delta\}$, $i_j = (i_j^1, i_j^2)$, a set of $\delta - 1$ tropical points $P = \{q_1, \ldots, q_{\delta-1}\}$ and a lift $\widetilde{P} = \{\widetilde{q}_1, \ldots, \widetilde{q}_{\delta-1}\}$ of the points in P to the algebraic torus $(\mathbb{K}^*)^2$. Let C be the stable tropical curve of support I passing through P and let $\widetilde{C}$ be an algebraic curve of support I passing through $\widetilde{P}$. This Chapter deals with the problem of determining the relationship of C and $\widetilde{C}$, paying special attention to the characterisation of sufficient conditions on the points $\widetilde{P}$ that ensure that $\widetilde{C}$ projects onto C.

Let us state the problem. Let I be a support, let $q_i = (q_i^1, q_i^2) \in \mathbb{T}^2$, $\widetilde{q}_i = (\widetilde{q}_i^1, \widetilde{q}_i^2) \in (\mathbb{K}^*)^2$, be tropical and algebraic points. The equations of a tropical and algebraic curve of support I are:

$$C \equiv \text{“}\sum_{i\in I} a_i x^{i^1} y^{i^2}\text{”} \qquad \widetilde{C} \equiv \sum_{i\in I} \widetilde{a}_i x^{i^1} y^{i^2}$$

If moreover we impose that $q_j \in C$ (resp $\widetilde{q}_j \in \widetilde{C}$), then the coefficients a_i (resp. $\widetilde{a}_i$) verify that:

$$(a_{i_1}, \ldots, a_{i_\delta}) \in \mathcal{T}\Big(\text{“}\sum_{i\in I} z_i (q_j^1)^{i^1} (q_j^2)^{i^2}\text{”}\Big) \quad 1 \le j \le \delta - 1 \tag{2.1}$$

$$\sum_{i\in I} \widetilde{a}_i (\widetilde{q}_j^1)^{i^1} (\widetilde{q}_j^2)^{i^2} = 0, \quad 1 \le j \le \delta - 1. \tag{2.2}$$

The coefficients a_i and $\widetilde{a}_i$ of the curves C and $\widetilde{C}$ are the solution of a linear system of equations in their respective framework. Hence, the comparison of the curves $T(\widetilde{C})$ and C can be given in terms of the comparison of two linear system of equations. Namely, the coefficients of the algebraic curve $\widetilde{C}$ can be computed solving an homogeneous linear system of $\delta - 1$ equations in δ unknowns. In the generic case, the homogeneous solution $[\widetilde{a}_{i_1} : \ldots : \widetilde{a}_{i_\delta}]$ is unique. It is known (see [RGST05]) that a tropical version of Cramer's rule can also be used to compute the coordinate vector $[a_{i_1} : \ldots : a_{i_\delta}]$ of the stable tropical curve C. With this notation, the problem is to determine whether

$$[T(\widetilde{a}_{i_1}) : \ldots : T(\widetilde{a}_{i_\delta})] = [a_{i_1} : \ldots : a_{i_\delta}].$$

Although it is always the case that $T(\widetilde{C})$ is a tropical curve of support I passing through P, it may happen that $T(\widetilde{C}) \neq C$. The contribution in this Chapter is a description of sufficient conditions for the equality $T(\widetilde{C}) = C$. These sufficient conditions are expressed in terms of the principal coefficient of the coefficients $\widetilde{a}_i$ in k^* of a polynomial of support I defining $\widetilde{C}$. Besides, we will prove that, if the principal coefficients of the points in $\widetilde{P}$ are generic in $(k^*)^2$, then $\widetilde{C}$ is a curve described as the zero set of a polynomial of support I and residually generic coefficients that projects onto C. Related to this problem, it will also be proposed a notion of families of tropical points in general position inside a tropical curve.

2.1 Matrices, Determinants and Pseudodeterminants

In this Section we present the basics relating algebraic and tropical determinants.

Definition 2.1. A *tropical matrix* of dimension $n \times m$ is a matrix with coefficients in $\mathbb{T}$. The *tropical determinant* of a square matrix is defined as:

$$\begin{vmatrix} x_{11} & \dots & x_{1n} \\ \vdots & & \vdots \\ x_{n1} & \dots & x_{nn} \end{vmatrix}_t = \text{“} \sum_{\sigma \in S_n} x_{1\sigma(1)} \cdots x_{n\sigma(n)} \text{”} = \max_{\sigma \in S_n} \{x_{1\sigma(1)} + \cdots + x_{n\sigma(n)}\}$$

where S_n is the permutation group of n elements. A square tropical matrix is called *singular* if the value of its tropical determinant is attained for at least two different permutations σ and τ. In other case it is called *regular*.

In the algebraic case, if $\widetilde{A} = (\widetilde{a}_{ij})$ is a $n \times n+1$ matrix defining a determined homogeneous system of equations, let $\widetilde{A}^i$ denote the matrix obtaining from $\widetilde{A}$ by deleting its i-th column. Then

$$[|A^1| : -|A^2| : \ldots : (-1)^n |A^{n+1}|]$$

is the unique projective solution of the system. In [RGST05], it is proved that the same fact happens with Cramer's rule and the stable tropical curve passing through a set of tropical points. More concretely

Theorem 2.2. *Let $A = (a_{i,j})$ be a $n \times n+1$ tropical matrix, consider the hyperplanes defined by the homogeneous equations $H_i = \text{“}\sum_{j=0}^{n+1} a_i x_i\text{”}$. Let x be the point given by homogeneous coordinates in $\mathbb{T}^n$*

$$x = [\ |A^1|_t : |A^2|_t : \ldots : |A^{n+1}|_t\ ]$$

Then, x is the stable intersection of the hyperplanes $H_1, \ldots, H_n$. Furthermore, x is the unique intersection point of the hyperplanes H_i if and only if each matrix $|A^i|$ is regular.

Next, some notation needed to state the main results is provided.

Definition 2.3. Let $A = (a_{ij})$ be a $n \times n$ tropical matrix. Let $B = (b_{ij})$ be a $n \times n$ matrix with coefficients over any ring R. Let $|A|_t$ be the tropical determinant of A. We define:

$$\Delta_A(B) = \sum_{\substack{\sigma \in \Sigma_n \\ \text{“}a_{1\sigma(1)} \cdots a_{n,\sigma(n)}\text{”} = |A|_t}} (-1)^{i(\sigma)} b_{1\sigma(1)} \cdots b_{n\sigma(n)}$$

the *pseudodeterminant* of B with respect to weight A.

This notation tries to capture the principal coefficient in k of the determinant of a matrix with entries in $\mathbb{K}$.

Lemma 2.4. *Let $A = (a_{ij})$ be a $n \times n$ tropical matrix, let $\widetilde{A} = (\widetilde{a}_{ij})$ be a $n \times n$ matrix with coefficients in $\mathbb{K}$ such that $T(\widetilde{A}) = A$ and let $Pc(\widetilde{A}) = (\alpha_{ij})$ be the matrix of principal coefficients of $\widetilde{A}$. That is, $\widetilde{a}_{ij} = \alpha_{ij} t^{-a_{ij}} + \cdots$. Then, $T(|\widetilde{A}|) = |A|_t$ if and only if $\Delta_A(Pc(\widetilde{A})) \neq 0$. In this case $\Delta_A(Pc(\widetilde{A})) = Pc(|\widetilde{A}|)$.*

Proof. In the expansion of the determinant of $\widetilde{A}$ we have that, for every permutation $\sigma \in S_n$, $T(\widetilde{a}_{1\sigma(1)} \cdots \widetilde{a}_{n\sigma(n)}) = \text{“}a_{1\sigma_1} \cdots a_{n\sigma(n)}\text{”}$. The permutations σ such that $a_{1\sigma_1} \cdots a_{n\sigma(n)}$ is maximal are exactly the permutations where the tropical determinant is attained. Thus, the coefficient of the term $t^{-|A|_t}$ in $|\widetilde{A}|$ is $\Delta_A(Pc(\widetilde{A}))$. If this coefficient is not zero, then $|\widetilde{A}|$ projects onto $|A|_t$. If the coefficient is zero, then $T(|\widetilde{A}|) > |A|_t$ and we cannot conclude what $Pc(|A|)$ is. □

2.2 Residual Conditions for the Compatibility of Linear Systems

It has been shown that the pseudodeterminant explicits the residual condition for the compatibility of a determinant with tropicalization. Thus, computing the residual condition provided by the pseudodeterminant on every component of a linear system of equations provides residual conditions for the compatibility of the solution of a linear system of equations in $\mathbb{K}$ with tropicalization.

Definition 2.5. Let $A = (a_{ij})$ be a $n \times (n+1)$ tropical matrix. Let $B = (b_{ij})$ be a matrix with coefficients in a ring R with the same dimension as A. We denote

$$\mathrm{Cram}_A(B) = (S_1, \ldots, S_{n+1})$$

where $S_i = \Delta_{A^i}(B^i)$ and A^i (respectively, B^i) denotes the corresponding submatrix obtained by deleting the i-th column in A (respectively, B).

In the definition, B is a $n \times (n+1)$ matrix. Each component of $\mathrm{Cram}_A(B)$ is a pseudodeterminant of the matrices obtained from A and B by deleting the i-th column. The pseudodeterminant $\Delta_{A^i}(B^i)$ is described by a set of permutations in the labels of the columns, $\{1, \ldots, i-1, i+1, \ldots, n+1\}$. In order to have a homogeneous notation on $\mathrm{Cram}_A(B)$ we will describe the pseudodeterminants by the permutations of the labels

$\{1,\dots,n+1\}$. The permutations σ allowed in the description of the pseudodeterminant of the submatrix B^i are those such that $\sigma(n+1)=i$. With this notation, the term of the pseudodeterminant $\Delta_{A^i}(B^i)$ is the term $(-1)^{i(\sigma)}\prod_{j=1}^{n} b_{j,\sigma(j)}$ and $i(\sigma)$ denotes the parity of σ restricted to $\{1,\dots,i-1,i+1,\dots,n-1\}$.

Lemma 2.6. *Suppose we are given a system of n linear homogeneous equations in $n+1$ variables in the semiring $\mathbb{T}$. Let A be the coefficient matrix of the system. Let $\widetilde{A}$ be any matrix such that $T(\widetilde{A})=A$. Let B be the matrix of principal coefficients of $\widetilde{A}$. If no element of $Cram_A(B)$ vanishes, then the linear system defined by $\widetilde{A}$ has only one projective solution and its tropicalization equals the stable solution $[|A^1|_t:\ldots:|A^{n+1}|_t]$*

Proof. Apply Lemma 2.4 to every component of the projective solution. □

If one pseudodeterminant $\Delta_{A^i}(B^i)=0$, there is a lack of information of what the principal coefficient of the determinant $|A^i|$ is and, more seriously, the control on the tropicalization $T(|A^i|)$ is lost. A careful look at these badly behaved systems yields the following:

Proposition 2.7. *Let A be a $n\times n+1$ tropical matrix. Let $x=[\ |A^1|_t:|A^2|_t:\ldots:|A^{n+1}|_t\ ]$ be the stable solution of the linear system of equations defined by A. Let $\widetilde{A}$ be any matrix in $\mathbb{K}^*$ projecting onto A and $B=Pc(A)$. Let $Cram_A(B)=(S_1,\dots,S_{n+1})$. Then:*

- *If every tropical determinant $|A^i|_t$ is regular, then $S_i\neq 0$, the homogeneous linear system defined by $\widetilde{A}$ has only one solution $\widetilde{x}$ and it projects onto x, $T(\widetilde{x})=x$.*
- *If $S_j=0$ and there is an index i such that $S_i\neq 0$, then the homogeneous linear system $\widetilde{A}$ has only one projective solution $\widetilde{x}$, that never tropicalizes correctly: $T(\widetilde{x})\neq x$.*
- *If $S_i=0$ for all i, we do not have any information. The linear system defined by $\widetilde{A}$ may be either determined or undetermined. If $\widetilde{x}$ is a solution of the system, both possibilities $T(\widetilde{x})=x$ and $T(\widetilde{x})\neq x$ can occur, even if the solution $\widetilde{x}$ is unique.*

Proof. If A^i is regular, then $|A^i|_t=$ "$a_{1,j_1}\cdots a_{n,j_n}$" is attained for only one permutation. It follows that $\Delta_A(B)=b_{1,j_1}\cdots b_{n,j_n}\neq 0\in k^*$ for any matrix B with entries in k^*. Hence, the algebraic system is determined, because at least the i-th projective coefficient $|\widetilde{A^i}|$ is not zero. Moreover, in this case it will always happen that $T(|\widetilde{A^i}|)=|A^i|_t$. If every tropical matrix A^i is regular, then we have the first item.

For the second item, if $S_j=0$, then $T(|\widetilde{A^j}|)<|A^j|_t$. It is even possible that $T(\widetilde{A^j})=-\infty$. But, as $S_i\neq 0$, then $T(|\widetilde{A^i}|)=|A^i|_t$, so the coefficient i can be used to dehomogenize. If follows that $\widetilde{x}$ is well defined (because $|\widetilde{A^i}|\neq 0$), but it cannot projects into x because they will always differ in the term j.

Finally, in the case where $S_i=0$ for every S we cannot decide if the system is determined without further information. This depends on the terms of higher order of the elements of $\widetilde{A}$. For an illustrative example, let $\mathbb{K}$ be the field of Puiseux series, let

$$A = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \qquad \widetilde{A}_1 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$
$$\widetilde{A}_2 = \begin{pmatrix} 1+t & 1+t^2 & 1+t^3 \\ 1 & 1 & 1 \end{pmatrix} \qquad \widetilde{A}_3 = \begin{pmatrix} 1+t & 1+2t & 1+3t \\ 1 & 1 & 1 \end{pmatrix}$$

The three matrices $\widetilde{A}_1$, $\widetilde{A}_2$, $\widetilde{A}_3$ projects into A. All of them satisfy that

$$\mathrm{Cram}_A(Pc(\widetilde{A})) = (0,0,0).$$

The tropical stable solution of the tropical system is the point $[0:0:0]$. The first algebraic system $\widetilde{A}_1$ is undetermined and it contains points such that $\widetilde{x} = [1:1:-2]$ that projects correctly onto $[0:0:0]$ and other points such that $\widetilde{x} = [1:t:-1-t]$ that does not. The second system $\widetilde{A}_2$ is a determined system such that its unique solution $\widetilde{x} = [t^2-t^3 : -t+t^3 : t-t^2]$ does not project into x. The last system $\widetilde{A}_3$ is a determined one. Its solution is $[-t:2t:-t] = [-1:2:-1]$, that projects correctly. □

2.3 Residual Conditions for the Tropical Compatibility of the Curve Through a Set of Points

Before establishing the relationship of the algebraic and tropical curve, let us check some properties of the pseudodeterminants. From Lemma 2.6, it follows that if the entries of the matrix B are indeterminates, then no pseudodeterminant $\Delta_A(B)$ vanishes and the algebraic determinant projects correctly. However, when working with the algebraic system of equations (2.2), it may happen that the entries of the matrix B are algebraically dependent elements. For example, if the curve is a conic $a_{xx}x^2 + a_{yy}y^2 + a_{xy}xy + a_x x + a_y y + a_1$, and we impose that it passes through a point (b_1, b_2), the terms b_1^2, b_2^2, $b_1 b_2$ will appear in the system of equations. These monomials are not algebraically independent. Nevertheless, in order to apply Lemma 2.6, it is only needed that the involved pseudodeterminants do not vanish. Now it is proved that, if the residual coefficients (γ_1, γ_2) of the points $(\widetilde{q}_1, \widetilde{q}_2)$ are indeterminates (or generic elements), then, the pseudodeterminants are never zero. The next is a rather technical Lemma that proves a stronger property.

Lemma 2.8. *Let $C_i = \{c_i^1, \ldots, c_i^{j_i}\}$, $1 \le i \le r$ be disjoint sets of variables. Suppose that we have $F_u = \{f_u^1, \ldots, f_u^{n+1}\} \subseteq k[\bigcup_{i=1}^r C_i]$, $1 \le u \le n$ sets of polynomials in the variables c_i^j. Suppose also that the following properties hold:*

- *For a fixed set F_u, f_u^l, with $1 \le l \le n+1$ are multihomogeneous polynomials in the sets of variables $C_{u^1}, \ldots, C_{u^{s_u}}$ with the same multidegree.*
- *If $u \neq v$ then F_u, F_v involve different sets of variables C_i.*
- *In a family F_u, if $l \neq m$ then the monomials of f_u^l are all different from the monomials of f_u^m.*

Let us construct the $n \times (n+1)$ matrix

$$B = (f_u^l)_{\substack{1 \le u \le n, \\ 1 \le l \le n+1}}$$

Let A be any $n \times (n+1)$ tropical matrix. Write

$$S = Cram_A(B) = (S_1, \ldots, S_{n+1}).$$

Then

1. *$S_1, \ldots, S_{n+1}$ are non identically zero multihomogeneous polynomials in the sets of variables $C_1, \ldots, C_r$ with the same multidegree.*
2. *If σ, τ are different permutations in Σ_{n+1} which appear in the expansion of S_l (and, therefore $\sigma(n+1) = \tau(n+1) = l$), then all resulting monomials in $\prod_{u=1}^n (A^l)_u^{\sigma(u)}$ are different from the monomials in $\prod_{u=1}^n (A^l)_u^{\tau(u)}$*
3. *If $l \neq m$, then S_l, S_m have no common monomials.*

Proof. First we prove *2*. If we have two different permutations σ, τ, there is a natural number v, $1 \le v \le n$ where the permutations differ, then the monomials in $f_v^{\sigma(v)}$, $f_v^{\tau(v)}$ are all different and these polynomials are the only factors of the products $\prod_{u=1}^n (A^l)_u^{\sigma(u)}$, $\prod_{u=1}^n (A^l)_u^{\tau(u)}$ where we find the variables which appear in the family F_v. It follows that these products cannot share any monomial. In particular, in the sum of several of these products, there is no cancellation of monomials, proving item *1*. So, in fact, we obtain that different minors share no monomial and we obtain immediately *3*. All those minors must have the same multidegree, which is just the concatenation of the multidegree of the family $F_1, \ldots, F_n$, by construction. □

Example 2.9. At this point it may be helpful to give an example of the Lemma. Consider the sets
$C_1 = \{x, y\}$, $C_2 = \{z\}$, $C_3 = \{m, n\}$, $C_4 = \{o, p, q\}$, $C_5 = \{r\}$.
$F_1 = \{x^2yz + y^3z, x^3z, 2xy^2z\}$
$F_2 = \{mnor^2, m^2or^2 + mnpr^2, n^2or^2 + m^2pr^2 + n^2pr^2\}$
Every polynomial in F_1 is multihomogeneous in C_1, C_2 with multidegree $(3, 1)$.
Every polynomial in F_2 is multihomogeneous in C_3, C_4, C_5 with multidegree $(2, 1, 2)$.
All the monomials in the polynomial are different.
Then, the matrix

$$B = \begin{pmatrix} x^2yz + y^3z & x^3z & 2xy^2z \\ mnor^2 & m^2or^2 + mnpr^2 & n^2or^2 + m^2pr^2 + n^2pr^2 \end{pmatrix}.$$

We take as matrix A in $\mathrm{Cram}_A(B)$, $A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 3 & 2 \end{pmatrix}$
$S_1 = (m^2or^2 + mnpr^2)(2xy^2z) = 2xy^2zm^2or^2 + 2xy^2zmnpr^2$
$S_2 = (x^2yz+y^3z)(n^2or^2+m^2pr^2+n^2pr^2)+(mnor^2)(2xy^2z) = x^2yzn^2or^2+x^2yzm^2pr^2+$

$x^2yzn^2pr^2 + y^3zn^2or^2 + y^3zm^2pr^2 + y^3zn^2pr^2 + 2xy^2zmnor^2$
$S_3 = (x^2yz+y^3z)(m^2or^2+mnpr^2) = x^2yzm^2or^2+x^2yzmnpr^2+y^3zm^2or^2+y^3zmnpr^2$.
Finally, we check that the polynomials S_1, S_2, S_3 share no monomial and are multihomogeneous in C_1, C_2, C_3, C_4, C_5 with multidegree $(3, 1, 2, 1, 2)$.

In the case of computing the curve $\widetilde{C}$ through a set of points $\widetilde{P}$, suppose that the points $\widetilde{q}_i$ are given in homogeneous coordinates with generic principal coefficients and tropicalization $[q_i^1 : q_i^2 : q_i^3]$.

$$\widetilde{q}_i = [\gamma_i^1 t^{-q_i^1} + \cdots : \gamma_i^2 t^{-q_i^2} + \cdots : \gamma_i^3 t^{-q_i^3} + \cdots].$$

Suppose also that the defining equation of $\widetilde{C}$ is homogenized adding a new variable z,

$$\widetilde{C} \equiv \sum_{i\in I} \widetilde{a}_i x^{i^1} y^{i^2} z^{r-i^1-i^2}.$$

Let $\widetilde{A}$ be the matrix of this homogenized linear systems and $B = Pc(\widetilde{A})$. We claim that the matrix B is in the conditions of Lemma 2.8. The j-th row of B is

$$B_j = \left((\gamma_j^1)^{i_1^1}(\gamma_j^2)^{i_1^2}(\gamma_j^3)^{r-i_1^1-i_1^2}, \ldots, (\gamma_j^1)^{i_\delta^1}(\gamma_j^2)^{i_\delta^2}(\gamma_j^3)^{r-i_\delta^1-i_\delta^2}\right)$$

Hence, in the hypothesis of Lemma 2.8, $C_i = \{\gamma_j^1, \gamma_j^2, \gamma_j^3\}$, each polynomial f_u^l is a different homogeneous monomial. So, the hypothesis holds. Thus, we conclude that for this homogenized system, the vector $\mathrm{Cram}_A(B)$, that contains a representative of the residues of the vector of coefficients of $\widetilde{C}$, belongs to the torus, $\mathrm{Cram}_A(B) \in (k^*)^n$. It follows that $[\widetilde{a}_1 : \ldots : \widetilde{a}_\delta] \in \mathbb{K}^*$. Finally, as every coefficient of every point $\widetilde{q}_i$ and $[\widetilde{a}_1 : \ldots : \widetilde{a}_\delta]$ is nonzero, we can dehomogenize everything. The pseudodeterminants $\Delta_{A^i}(Pc(\widetilde{A}^i))$ are nonzero provided that $Pc(\widetilde{q}_i) = (\gamma_i^1, \gamma_j^2)$ are generic. To sum up, we have the following.

Theorem 2.10. *Let I be a support, $\delta = \delta(I)$, $P = \{q_1, \ldots, q_{\delta-1}\}$, $q_j = (q_j^1, q_j^2)$ a set of tropical points, $\widetilde{P} = \{\widetilde{q}_1, \ldots, \widetilde{q}_{\delta-1}\}$ a set of algebraic points such that $\widetilde{q}_j = (\widetilde{q}_j^1, \widetilde{q}_j^2) = (\gamma_j^1 t^{-q_j^1} + \ldots, \gamma_j^2 t^{-q_j^2} + \ldots)$. Let C be the stable tropical curve of support I passing through P computed using Cramer's rule. Let*

$$A = ((q_j^1)^{i^1}(q_j^2)^{i^2}) \qquad \widetilde{A} = ((\widetilde{q}_j^1)^{i^1}(\widetilde{q}_j^2)^{i^2})$$

be the matrices of the linear system defining C and $\widetilde{C}$. For simplicity, it is assumed that the columns of A are indexed by the set I. Then, the pseudodeterminants are non identically zero polynomials in the set $\{\gamma_j^i, 1 \le j \le \delta - 1, 1 \le i \le 2\}$. If the pseudodeterminants verify that

$$\Delta_{A^i}(Pc(\widetilde{A}^i)) \neq 0, \quad i \in I.$$

then, there is only one curve $\widetilde{C}$ passing through $\widetilde{P}$ and $T(\widetilde{C}) = C$. That is, the pseudodeterminants provide residual sufficient conditions for the equality $T(\widetilde{C}) = C$.

In this case, let $\widetilde{f} = \sum_{i\in I} \widetilde{a}_i x^{i^1} y^{i^2}$ *be the polynomial of support* I *defining* $\widetilde{C}$ *computed by Cramer's rule, suppose that this polynomial is dehomogenized with respect to the index* i_0 *(*$\widetilde{a}_{i_0} = 1$*), then, the principal coefficients of* $\widetilde{a}_i$ *are*

$$(Pc(\widetilde{a}_1), \dots, Pc(\widetilde{a}_\delta)) = \Big(\frac{\Delta_{A^{i_1}}(Pc(\widetilde{A}^{i_1}))}{\Delta_{A^{i_0}}(Pc(\widetilde{A}^{i_0}))}, \dots, \frac{\Delta_{A^{i_\delta}}(Pc(\widetilde{A}^{i_\delta}))}{\Delta_{A^{i_0}}(Pc(\widetilde{A}^{i_0}))}\Big)$$

Proof. If no pseudodeterminant $\Delta_{A^i}(Pc(\widetilde{A}^i))$ vanishes, then $T(|\widetilde{A}^i|) = |A^i|_t$. In particular, no determinant $|\widetilde{A}^i|$ is zero. Let

$$\widetilde{C} \equiv \{\sum_{i\in I} |\widetilde{A}^i| x^{i_1} y^{i_2} = 0\}$$

be the unique algebraic curve of support I passing through $\widetilde{P}$ and projecting onto C, the curve defined by "$\sum_{i\in I} |A^i|_t x^{i_1} y^{i_2}$", i.e. the stable tropical curve through P.

Note that if no pseudodeterminant vanishes, the coordinates of $\widetilde{C}$ belongs to the algebraic torus in homogeneous coordinates $(\mathbb{PK}^*)^\delta$. Thus, if one wants an affine representation of the coordinates of the curve, it can be dehomogenized with respect to any index $i_0 \in I$ and still the result will project correctly into the (dehomogenized) equation of the tropical curve C. Furthermore, taking principal coefficients commutes with dehomogenization in $(\mathbb{PK}^*)^\delta$, so the last claim holds. □

2.4 Genericity of the Curve Through a Set of Points

We have shown sufficient conditions for the compatibility of the algebraic and tropical curve through a set of corresponding points. If the lifts of points $\widetilde{P}$ are residually generic, the algebraic curve $\widetilde{C}$ passing through them is unique. We know that this curve projects onto the stable curve through the tropical points, but it is not clear what is the residual relationship of its coefficients. This is important in the context of incidence configurations. Proofs such as the one in Theorem 1.30 are done recursively in the graph of the configuration. So, if using residually generic coefficients is an argument to Theorems such as 2.10 and we want to use this Theorem in an induction scheme, we should establish the residual genericity of the coefficients of the curve $\widetilde{C}$. This is the aim of this Section. We prove that if the points $\widetilde{q}_i$ are residually generic, then the coefficients of $\widetilde{C}$ are also residually generic.

Theorem 2.11. *Let* $I = \{l_1, \dots, l_\delta\}$, $l_k = (i_k, j_k)$ *be a support. Let* $P = \{q_1, \dots, q_{\delta-1}\}$ *be a set of tropical points. Let* C *be the stable tropical curve of support* I *passing through* P*. Let* $\widetilde{P} = \{\widetilde{q}_1, \dots, \widetilde{q}_{\delta-1}\}$*,* $Pc(\widetilde{q}_i) = (\gamma_i^1, \gamma_i^2)$ *and* $\widetilde{C}$ *the algebraic curve of support* I *passing through* $\widetilde{P}$*. Let* $\widetilde{f} = \sum_{(i,j)\in I} \widetilde{a}_{i,j} x^i y^j$ *be the algebraic curve representing* $\widetilde{C}$ *dehomogenized with respect to the index* $l_0 = (i_0, j_0)$*. Let* $\gamma_1 = \{\gamma_1^1, \dots, \gamma_{\delta-1}^1\}$*,* $\gamma_2 = \{\gamma_1^2, \dots, \gamma_{\delta-1}^2\}$ *Consider the map*

$$\begin{array}{rccl} \mathit{Cramer}: & k^{2\delta-2} & \longrightarrow & k^{\delta-1} \\ & (\gamma_1, \gamma_2) & \mapsto & \mathit{Cramer}(\gamma_1, \gamma_2) = \Big(\frac{\Delta_{A^{l_1}}(Pc(\widetilde{A}^{l_1}))}{\Delta_{A^{l_0}}(Pc(\widetilde{A}^{l_0}))}, \dots, \frac{\Delta_{A^{l_\delta}}(Pc(\widetilde{A}^{l_\delta}))}{\Delta_{A^{l_0}}(Pc(\widetilde{A}^{l_0}))}\Big) \end{array}$$

that represents the principal coefficients of $\widetilde{f}$ in terms of the principal coefficients of $\widetilde{P}$ (provided that the pseudodeterminants of Theorem 2.10 do not vanish). Then, the map Cramer is dominant, that is, if the principal coefficients of $\widetilde{P}$ are generic, then the polynomial $\widetilde{f}$ is generic among the polynomials of support I dehomogenized with respect to l_0.

Proof. Write $q_l = (q_l^1, q_l^2)$, $C = \mathcal{T}(\text{“}\sum_{ij} a_{ij}x^iy^j\text{”})$. Then, C is the curve defined by the stable solution of:

$$\text{“}\sum_{(i,j)\in I} a_{ij}(q_l^1)^i(q_l^2)^j\text{”}, 1 \leq l \leq N$$

and the lifts of C verify the relations

$$\sum_{(i,j)\in I} \widetilde{a}_{ij}(\widetilde{q}_l^1)^i(\widetilde{q}_l^2)^j = 0, 1 \leq l \leq N$$

Take the equations

$$\widetilde{f}_l = \sum_{(i,j)\in I} \widetilde{a}_{ij}x^iy^jt^{-a_{ij}-iq_l^1-jq_l^2}, 1 \leq l \leq N,$$

which correspond to a (tropical) translation of the problem to the point 0. We dehomogenize the tropical equation of C ($a_{i_0j_0} = 0$), and the algebraic equation of $\widetilde{C}$ ($\widetilde{a}_{i_0,j_0} = 1$) with respect to a term $(i_0, j_0) \in I$. The conditions on the principal coefficients α_{ij} of $\widetilde{a}_{ij}$ are:

$$f_l = \sum_{J_l} \alpha_{ij}(\gamma_l^1)^i(\gamma_l^2)^j, 1 \leq l \leq N,$$

where $J_l \subseteq I$ are the monomials such that $-a_{ij} - iq_l^1 - jq_l^2$ is minimized. Notice that, by construction, each J_l has at least two terms. Write $\alpha = \{\alpha_{ij}|(i,j) \neq (i_0,j_0)\}$, $\gamma_1 = \{\gamma_1^1, \ldots, \gamma_{\delta-1}^1\}$, $\gamma_2 = \{\gamma_1^2, \ldots, \gamma_{\delta-1}^2\}$. Each residual equation f_l is affine in the set of variables α, and the coefficients of this affine equations are monomials in $\{\gamma_l^1, \gamma_l^2\}$. Moreover, we know that there are nonzero solutions to this system. Without loss of generality, every polynomial f_l can be saturated with respect to the coordinate hyperplanes (that is, we eliminate redundant γ). These polynomials are still denoted by f_l. Thus, we have a system of equations in $3\delta - 3$ unknowns.

Let $\mathcal{V}$ be the Zariski closure of the image of the map:

$$\begin{array}{ccc} k^{2\delta-2} & \longrightarrow & k^{3\delta-3} \\ (\gamma_1, \gamma_2) & \mapsto & (\gamma_1, \gamma_2, \text{Cramer}(\gamma_1, \gamma_2)) \end{array}$$

It is clear that this is a birational map between the space $k^{2\delta-2}$ and $\mathcal{V}$. Let $\mathcal{I}$ be the ideal of $\mathcal{V}$. $\mathcal{I}$ is a prime ideal that contains the polynomials $(f_1, \ldots, f_{\delta-1})$ in $k[\alpha, \gamma_1, \gamma_2]$. By construction, the field of rational functions of the variety $\mathbb{L}$ is the field of fractions of the integer domain

$$\mathbb{L} = \text{Frac}\left(\frac{k[\gamma_1, \gamma_2, \alpha]}{\mathcal{I}}\right) = k(\gamma_1, \gamma_2)$$

In particular, γ_1, γ_2 is a transcendence basis of $k \subseteq \mathbb{L}$ and the dimension of $\mathbb{L}$ is $2\delta - 2$. For each f_l, if the variable γ_l^1 does not appear in f_l, then γ_l^2 is an element of $\mathbb{L}$ which is algebraic over $k(\alpha, \gamma_l^1)$. Analogously, if γ_l^2 does not appear in f_l, then γ_l^1 is algebraic over $k(\alpha, \gamma_l^2)$. If both variables appear in f_l, then just choose γ_l^j algebraic over $k(\alpha, \gamma_l^{3-j})$. In this way, the set $g = \alpha \cup \{\gamma_l^{3-j},\ 1 \leq l \leq \delta - 1\}$ is such that $\mathbb{L}$ is algebraic over $k(g)$. As $\#g = 2\delta - 2$, we conclude that g is a transcendence basis of $k \subseteq \mathbb{L}$. In particular, the set α is algebraically independent over k. This means that:

$$\mathcal{I} \cap k[\alpha] = \mathcal{I} \cap k[\gamma_1, \gamma_2] = 0 \tag{2.3}$$

Hence, the projection of $\mathcal{V}$ over the space of coordinates α is dense in $k^{\delta-1}$. But the image of the projection is the image of $k^{2\delta-2}$ by the map Cramer, so Cramer is dominant. □

2.5 Points in Generic Position in a Curve

In this Section we want to face the problem of determining points in general position in a curve. First, an adequate notion of tropical points in general position must be provided. There are slightly different approaches to this definition in the literature. All of them share the same idea, but apply to different problems, see for example [Mik05], [Mar06], or [GM07]. These notions are adequate for the enumerative problems, but not for the incidence structures we study. Moreover, we want to provide a notion of generic points in a fixed curve C. Informally, a set of points P is in general position inside a curve C if C is the unique curve of its type that contains P. Again, to formalize this we use the notion of stability:

Definition 2.12. Let C be a tropical curve of support I. A set of points $q_1, \ldots, q_n$, $n \leq \delta(I) - 1$ is in *generic position with respect to* C if there are tropical points $q_{n+1}, \ldots, q_{\delta-1}$ such that C is the stable curve of support I passing through $q_1, \ldots, q_{\delta-1}$.

One would like to characterise the points in general position in a curve C because, in general, it is not easy to check the Definition. A first result is the following:

Lemma 2.13. *Let C be a curve of support $I = \mathbb{Z}^2 \cap \Delta$, where Δ is a convex polygon. Suppose that the dual subdivision induced by C in Δ is a triangulation that has all points in $\Delta \cap I$ as vertices. Let $q_1, \ldots, q_{\delta-1}$ be different points in C such that every point q_i lies in the relative interior of an edge of C and two different points do not lie in the same edge. Let Γ be the graph contained in the subdivision of Δ consisting of those edges such that their dual contains a point q_i. Then Γ is a maximal tree contained in Subdiv(Δ), the vertices of Γ are exactly the points of I and C is the unique curve of support I passing through $q_1, \ldots, q_{\delta-1}$. In particular, $q_1, \ldots, q_{\delta-1}$ are points in general position in C*

Proof. We refer to [Mik05]. □

This Lemma only works for very special curves, because of the restriction on the support of the curve and the induced subdivision in Δ.

Definition 2.14. Let C be a tropical curve of support I and Newton Polygon Δ. Let Γ_0 be the skeleton of $Subdiv(\Delta)$ associated to C (the set of cells of dimension 0 and 1. This is always a connected graph). We modify Γ_0 as follows. We add to Γ_0 every point in $I \setminus \Gamma_0$ as follows.

If $x, \ldots, x_r \in I$ are the points of I lying in the interior of an edge e of Γ_0, then we add these points as 2-valent vertices of Γ_0 splitting the edge e into $r+1$ edges. If $x \in I$ lies in the relative interior of a polygon Δ_v of the subdivision, then x is added to Γ_0 as an isolated point. In this case, the resulting graph is no longer connected. The resulting graph is denoted by Γ.

Let q be a point in C. If q lies in an edge of C, let Δ_q be the dual edge in Γ_0, then $\Delta_q = e_1 \cup \ldots \cup e_d$ is refined as a union of edges in Γ. An *assignment* of q is a choice of one of the edges $e_1, \ldots, e_d$. In the case where q is a vertex of C, the dual cell Δ_q of this vertex is a polygon. Let S be the set of isolated points of I in Δ_q and $e_1, \ldots, e_d$ be the set of refined edges in the boundary $\Gamma \cap \partial\Delta_q$. An *assignment* of q is a choice of an element in $S \cup \{e_1, \ldots, e_d\}$.

If $q_1, \ldots, q_n$ are points (possibly repeated) in C, an *assignment of the points* is an assignment of each point q_i such that:

- Let $q_{i_1}, \ldots q_{i_r}$ be the points lying in the same edge of C, let $\Delta_q = e_1 \cup \ldots \cup e_d$ be the refined dual edge in Γ. It is required that the assignment of q_{i_j} is different from the assignment of q_{i_k} whenever $j \neq k$ (even in the case that $q_{i_j} = q_{i_k}$ is a repeated point).

- Let $q_{i_1}, \ldots, q_{i_r}$ be points identified with a vertex (that is, a vertex with multiplicity r). Let Δ_q be the polygon dual to the vertex. Let $l = \#\{\Delta_q \cap I\}$. It is required that at most l points are assigned to different points in S and that the $r-l$ other points are mapped to different refined edges of the boundary of Δ_q.

- The set of refined edges of Γ such that have assigned a point q_i form an acyclic subgraph of Γ.

Lemma 2.15. *Let C be a curve of support I. Let $q_1, \ldots, q_{\delta-1}$ be a list of points such that there exists an assignment in Γ. Then*

- *Every point of I that lies in the relative interior of a polygon Δ_v of $Subdiv(\Delta)$ is assigned to a point q_i.*

- *The set of assigned edges is a maximal tree in Γ that contains as vertices every non isolated vertex of Γ.*

Proof. The proof is inspired in the properties of lattice subdivisions of tropical curves presented in [Mik05]. Let S be the set of points of I lying in the relative interior of a polygon in $Subdiv(\Delta)$ and let l be the number of these points. Let $r = \delta - l$ be the number of non isolated vertices of Γ. Then, at most l points q_i are assigned to a point in S and at least $\delta - 1 - l = r - 1$ points are assigned to an edge on Γ. Then, from the property that the set of assigned edges of Γ is an acyclic graph. It follows that the number of assigned edges must be smaller than the number of vertices. That is, the

number of assigned edges must be exactly $r-1$. It follows that the graph of assigned edges is connected, i.e. a tree. Moreover, this tree is maximal, because it attains every non isolated vertex of Γ. Finally, the number of isolated points of Γ assigned to a point is l (every isolated point has been assigned). □

Lemma 2.16. *Let C be a tropical curve of support I and Newton polygon Δ. Let Γ be the refinement of Γ_0. Let $q_1,\dots,q_{\delta-1}$ be points in the curve. Suppose that if a vertex v of C coincides with r points q_i, then the dual polygon Δ_v contains exactly r point of I in its interior. Suppose that there is an assignment of the points. Then, C is the stable curve passing through $q_1,\dots,q_{\delta-1}$.*

Proof. Let $\widetilde{q}_i$ be lifts of the points q_i whose residual coefficients $\gamma_j = (\gamma_j^1, \gamma_j^2)$ are sufficiently generic. In order to define a curve $\widetilde{C}$, we have to compute lifts of the coefficients $\widetilde{a}_i$ of the polynomials defining C. Let f be the concave polynomial of support I defining C (see Definition 1.18), $f = \text{“}\sum_{i\in I} a_i x^{i^1} y^{i^2}\text{”}$ dehomogenized with respect to a vertex i_0 of the polygon Δ ($a_{i_0}=0$). Notice that, if $g = \text{“}\sum_{i\in I} b_i x^{i^1} y^{i^2}\text{”}$ is any tropical polynomial of support I such that $b_i = a_i$ if i is a vertex of $Subdiv(C)$ and $b_i \le a_i$ in other case, then f and g represents the same piecewise affine function and $\mathcal{T}(g) = C$. We will compute a polynomial g with this characteristics.

Given an edge e of $Subdiv(\Delta)$, let $e = e_1 \cup \ldots \cup e_{d-1}$ be the refinement in Γ, $e_k = [i_k, i_{k+1}]$. If there were two different edges e_k, e_l, $k<l$ that are not assigned to any point q_j, then, if $k+1=l$ then the vertex i_{k+1} would be a vertex of Γ that is not attained by Λ, if $k+1<l$ then either Λ does not attain a vertex of Γ (if $e_{k+1},\dots,e_l$ are not assigned) or Λ is not connected (if at least one e_j is assigned with $k<j<l$), contrary to the results in Lemma 2.15. Hence, for the case of an edge $\Delta_q = e_1 \cup \ldots \cup e_d$, at most one of the refined edges e_k is not assigned to any point. The residual values α_i for a point i of I contained in an edge of $Subdiv(\Delta)$ are computed recursively, starting from $\alpha_{i_0}=1$. By the maximal tree structure of Λ we can always suppose that we are in one of the following two cases:

*1)*The edge is $e=[i_1,\dots i_d]$, we only know the value of α_{i_1} and there are exactly $d-1$ points $q_{j_1},\dots q_{j_{d-1}}$ in the dual edge $V^e \subseteq C$. The non homogeneous residual system of equations associated to the points is:

$$\begin{cases} \alpha_{i_1}\gamma_{j_1}^{i_1} + \cdots + \alpha_{i_d}\gamma_{j_1}^{i_d} = 0 \\ \alpha_{i_1}\gamma_{j_2}^{i_1} + \cdots + \alpha_{i_d}\gamma_{j_2}^{i_d} = 0 \\ \qquad\qquad \cdots\cdots \\ \alpha_{i_1}\gamma_{j_{d-1}}^{i_1} + \cdots + \alpha_{i_d}\gamma_{j_{d-1}}^{i_d} = 0 \end{cases}$$

in the unknowns $\{\alpha_{i_2},\dots,\alpha_{i_d}\}$ and $\gamma_{j_l}^{i_l} = (\gamma_{j_l}^1)^{i_l^1}(\gamma_{j_l}^2)^{i_l^2}$. This system is determined, to show this, we may homogenize each row of the monomial matrix (γ) by a new variable $\gamma_{l_i}^3$, hence, we obtain a matrix that is in the hypothesis of Lemma 2.8 we conclude that its minors is a non identically zero multihomogeneous polynomial that will remain non identically zero after dehomogenizing each variable $\gamma_{l_i}^3 = 1$. The determination of α_{i_1} is just a dehomogenization of the solution. Hence, we conclude that there is only one

solution $\{\alpha_{i_2},\ldots,\alpha_{i_d}\}$ of this linear system in the algebraic torus over the residual field $(k^*)^{d-1}$. Notice that, using induction, each α_{i_j} is a non zero rational function in α_{i_0} and γ. Applying this steps recursively we can compute the values of every edge of integer length $d-1$ and $d-1$ assigned points. Notice that, in particular, we can compute the values of every α_i associated to a vertex of $Subdiv(\Delta)$ and that they are non zero.

2) The edge is $e=[a_{i_1},\ldots,a_{i_d}]$ and the values of α_{i_1} and α_{i_d} have been already computed. Necessarily, there are exactly $d-2$ points $q_{j_1},\ldots,q_{j_{d-2}}$ in the dual edge of e, because if there where more points, there would be a cycle in the graph Λ, contrary to the hypothesis, and if there where less points, Λ would not be a maximal tree. The residual conditions on the unknowns $\{\alpha_2,\ldots,\alpha_{d-1}\}$ for a non homogeneous system of $d-2$ linear equations in $d-2$ unknowns with a similar structure of the previous case. So, if the coefficients of γ_i are generic, there is only one solution (this time in k^{d-2} because the determination of the values of α_{i_1} and α_{i_d} do not correspond to just a dehomogenization). Again, applying induction, each α_i is rational function of α_{i_0} and γ.

Thus, if the coefficients γ are generic, all the values α_i corresponding to an index i that is not an isolated vertex of Γ can be computed from γ and α_{i_0} and its value is unique. It only rest to compute the values α_i corresponding to indices in I belonging to the relative interior of a polygon in $Subdiv(\Delta)$. In this case, the corresponding point q_i lie in a vertex $v\in C$. Let Δ_v be its dual polygon in $Subdiv(\Delta)$. Every coefficient corresponding to $\partial\Delta_v\cap I$ has been already computed. Let $\{j_1,\ldots,j_r\}=\partial\Delta_v\cap I$ and $\{k_1,\ldots,k_s\}=int(\Delta_v)\cap I$. There are s points q_i identified to v. The residual system of equations corresponding to these points is:

$$\begin{cases} \alpha_{k_1}\gamma_{l_1}^{k_1} & +\cdots+ & \alpha_{k_s}\gamma_{l_1}^{k_s} & = -\alpha_{j_1}\gamma_{l_1}^{j_1} & -\cdots- & \alpha_{j_r}\gamma_{l_1}^{j_r} \\ \alpha_{k_1}\gamma_{l_2}^{k_1} & +\cdots+ & \alpha_{k_s}\gamma_{l_2}^{k_s} & = -\alpha_{j_1}\gamma_{l_2}^{j_1} & -\cdots- & \alpha_{j_r}\gamma_{l_2}^{j_r} \\ & & \cdots\cdots & & & \\ \alpha_{k_1}\gamma_{l_s}^{k_1} & +\cdots+ & \alpha_{k_s}\gamma_{l_s}^{k_s} & = -\alpha_{j_1}\gamma_{l_s}^{j_1} & -\cdots- & \alpha_{j_r}\gamma_{l_s}^{j_r} \end{cases}$$

in the unknowns $\{\alpha_{k_1},\ldots,\alpha_{k_s}\}$. Again, if the values of γ are generic, there is only one solution in k^s.

So, starting from the value $\alpha_{i_0}=1$ the rest of the values are determined from γ. Let $\widetilde{a}_i$ be any element of $\mathbb{K}^*$ such that if $\alpha_i\neq 0$ then $Pt(\widetilde{a}_i)=\alpha_i t^{-a_i}$, and, if $\alpha_i=0$, then $Pt(\widetilde{a}_i)=t^{-a_i+1}$. Let $\widetilde{g}=\sum_{i\in I}\widetilde{a}_i x^{i^1}y^{i^2}$. Let $\widetilde{C}$ the algebraic curve defined by $\widetilde{g}$, its projection $T(\widetilde{C})$ is the curve C. But it may happen that $\widetilde{C}$ does not contains the points $\widetilde{q}_i$, because the computations have been done in the residual field. Anyway, by construction, the principal terms of $\widetilde{q}_i$ are in the hypothesis of applying Theorem 1.16, we can compute points $\widetilde{q}'_i$ lying in $\widetilde{C}$ such that $Pt(\widetilde{q}'_i)=Pt(\widetilde{q}_i)$. That is, there is a curve $\widetilde{C}$ passing through a set of lifts $\widetilde{q}'_i$ of q_i with generic residual coefficients in the sense of Theorem 2.10. Hence, $C=T(\widetilde{C})$ is the stable curve passing through $q_1,\ldots,q_{\delta-1}$. □

Theorem 2.17. *Let C be a curve of support I and Newton polygon Δ, let Γ be the refinement of the subdivision Δ. Let $q_1,\ldots,q_{\delta-1}$ be points in the curve. If there is an assignment of $q_1,\ldots,q_{\delta-1}$, then C is the stable curve of support I passing through the points.*

Proof. For each vertex v of C containing points $q_{j_1}, \ldots, q_{j_r}$, let $q_{j_{s+1}}, \ldots q_{j_r}$ be the points assigned to and edge of Γ and let $e_1, \ldots e_r$ be those edges. Perturb the point q_{j_i} in C translating it along the dual edge of e_i. Denote this point by q'_{j_i}. For the rest of points, take $q'_{i_j} = q_{i_j}$. The points $q'_1, \ldots q'_{\delta-1}$ are points in C in the conditions of Lemma 2.16. Hence, C is the stable curve through $\{q'_1, \ldots, q_{\delta-1}\}$. Making a limit process on each perturbed point $q'_{j_i} \to q_{j_i}$, the stable curve C trough the points $\{q'_1, \ldots, q_{\delta-1}\}$ stays invariant along the process. By the continuity of the stable curve through a set of points, we conclude that C is the stable curve through $q_1, \ldots, q_{\delta-1}$. □

It is conjectured that the conditions imposed in the preceding Theorem are also necessary in order to have the genericity of the points inside the curve. That is, we claim that given C a tropical curve and $q_1, \ldots, q_{\delta-1} \in C$, C is the stable curve through the points if and only if there is an assignment of the points. In many concrete examples it can be easily shown that this condition is a complete characterisation of a set of points in general position in a curve. But the problem is still open for an arbitrary curve.

Chapter 3

Tropical Resultants and the Stable Intersection of Curves

This Chapter deals with the study of the intersection of two tropical curves. As we have shown in Chapter 1, two different curves may share an infinite number of points. But, if one wants to relate Tropical and Algebraic Geometry, it is desirable to introduce a new concept of "intersection" such that two different curves without a common component only have a finite number of common points.

One approach towards this notion is through the notion of stable intersection as described in 1.21. Another potential solution is the following: given two tropical curves f and g, take two algebraic curves $\widetilde{f}$ and $\widetilde{g}$ projecting onto the tropical curves. Then, the intersection of the two algebraic curves $\widetilde{f} \cap \widetilde{g}$ will project into the intersection of the tropical curves, $T(\widetilde{f} \cap \widetilde{g}) \subseteq f \cap g$. Hence, one could define the intersection of f and g as $T(\widetilde{f} \cap \widetilde{g})$. This lifting approach is better suited in the context of comparison between tropical and algebraic configurations, because it relates directly the intersection with the lifts. But this is not a good definition because, for different elections of the algebraic curves $\widetilde{f}$, $\widetilde{g}$, the projection of the intersection points may differ. This is a problem that has been faced in Chapter 2 when dealing with the curve passing through a set of points. If the lifting of the points are not generic, the algebraic curve the points define can project into a non stable tropical curve through the original points.

On the other hand, regarding the definition of curves through lifts, one should expect that, for the case of two generic lifts of the curves $\widetilde{f}$ and $\widetilde{g}$, their intersection should project into a well defined tropical set. In this Chapter, we will prove that this intersection (via lifting) coincides with the stable intersection of the curves.

In order to prove this result, a similar scheme as in Chapter 2 is chosen. The main obstacle now is that, contrary to the case of the curve passing through a set of points, this is not a linear system any more, in the sense that there is not a linear system determining the coordinates of the points. Even more, a single intersection point of the given algebraic curves cannot be explicitly expressed in terms of the coefficients of the curves. This problem is partially avoided with the use of resultants.

For the case of planar curves, the univariate resultant of two defining equations

codifies the projection of the intersection points of the curves on one coordinate line (see, for example, [vdW03a]).

The main original result of the Chapter is a notion of tropical resultant with the same geometric properties of the classical one. Second, it is proved that, for two generic lifts of two tropical curves, its intersection projects onto the tropical stable intersection and that there is a correspondence with the tropical multiplicity (see Corollary 1.24) of a stable intersection point q and the algebraic points in the intersection projecting into it. With all this information, it is derived a formula relating the algebraic and tropical intersection multiplicity.

3.1 Univariate Resultants

Let us start with the notion of tropical resultant of two univariate polynomials. In algebraic geometry, the resultant of two univariate polynomials is a polynomial that solves the decision problem of determining if both polynomials have a common root.

Definition 3.1. Let $\widetilde{f} = \sum_{i=0}^{n} a_i x^i$, $\widetilde{g} = \sum_{j=0}^{m} b_j x^j \in \mathbb{K}[x]$, where $\mathbb{K}$ is an algebraically closed field. For simplicity, we assume that $a_0 a_n b_0 b_m \neq 0$. Let $p(\mathbb{K})$ be the prime filed of $\mathbb{K}$. Then, there is a unique polynomial in $p(\mathbb{K})[a_i, b_j]$ up to a constant factor, called the *resultant*, such that it vanishes if and only if $\widetilde{f}$ and $\widetilde{g}$ have a common root.

In the definition, it is asked the polynomials to be of effective degree n and m, this is in order to avoid the specialization problems that usually appear when using resultants. But the polynomials are also asked to have order zero. This restriction is demanded for convenience with tropicalization. Recall that the intersection of the varieties with the coordinate hyperplanes is always neglected. Hence, the definition of resultant will take this into account. Moreover, as the polynomials are always described by its support, the resultant will not be defined by the degree of the polynomials, but by their support. This approach will be convenient in the next Section, when there will be provided a notion of resultant for bivariate polynomials.

Definition 3.2. Let I, J be two finite subsets of $\mathbb{N}$ of cardinality at least 2 such that $0 \in I \cap J$. That is, the support of two polynomials that do not have zero as a root. Let $R(I, J, \mathbb{K})$ be the resultant of two polynomials with variable coefficients, $f = \sum_{i \in I} a_i x^i$, $g = \sum_{j \in J} b_j x^j$ over the field $\mathbb{K}$.

$$R(I, J, \mathbb{K}) \in \mathbb{Z}/(p\mathbb{Z})[a, b],$$

where p is the characteristic of the field $\mathbb{K}$). Let $R_t(I, J, \mathbb{K})$ be the tropicalization of $R(I, J, \mathbb{K})$. This is a polynomial in $\mathbb{T}[a, b]$, which is called the *tropical resultant* of supports I and J over $\mathbb{K}$.

So, our approach is to define the tropical resultant polynomial as the projection of the algebraic polynomial. In this point, one may obtain, for the same support sets I and J, different tropical resultants, one for each possible characteristic of $\mathbb{K}$. This is not good, in the sense that tropical geometry should not be determined by the characteristic

of the field we have used to define the projection. Hence, one has to take care of what is the common information of these polynomials. The answer is complete: the tropical variety they define is always the same. This variety is the image of any resultant variety over a field $\mathbb{K}$, so it will code the pairs of polynomials with fixed support that have a common root.

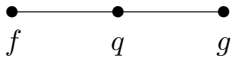
Lemma 3.3. *The tropical variety $\mathcal{T}(R_t(I,J,\mathbb{K}))$ does not depend on the field $\mathbb{K}$, but only on the sets I and J.*

Proof. Let $\mathcal{N}$ be the Newton Polytope of the resultant defined over a field $\mathbb{L}$ of characteristic zero, $\mathcal{N} \subseteq \mathbb{R}^{n+m+2}$. It is known that the monomials of $R(I,J,\mathbb{L})$ corresponding to vertices of $\mathcal{N}$ (extreme monomials) have always as coefficient ± 1 (See, for example, [GKZ90] or [Stu94]). Hence, the extreme monomials in $R(I,J,\mathbb{K})$ are independent of the characteristic of the field $\mathbb{K}$ and so is $\mathcal{N}$. If x is a monomial of $R(I,J,\mathbb{K})$ that does not correspond to a vertex of $\mathcal{N}$, then $x = \sum \lambda_i v_i$, $0 \leq \lambda_i \leq 1$, where v_i are vertices of $\mathcal{N}$. $T(\text{coeff}(v_i)) = T(\pm 1) = 0$ and, as coeff(x) is an integer (or an integer mod p), it is contained in the valuation ring, that is $0 \geq T(\text{coeff}(x)) \in \mathbb{T} \cup \{-\infty\}$. $T(\text{coeff}(x))$ is finite and not zero if and only we are dealing with a p-adic valuation and p divides coeff(x). It is $-\infty$ if and only if the characteristic of $\mathbb{K}$ divides the coefficient. So, the subdivision of the cell containing the monomials v_i induced by $R_t(I,J,\mathbb{K})$ described in Proposition 1.19 never contains x as a vertex, no matter what $\mathbb{K}$ is. We conclude that the subdivision of $\mathcal{N}$ dual to $\mathcal{T}(R_t(I,J,\mathbb{K}))$ is $\mathcal{N}$ itself. So $\mathcal{T}(R_t(I,J,\mathbb{K}))$ is always the polyhedral complex dual to $\mathcal{N}$ centered at the origin. This complex is independent of $\mathbb{K}$. □

Now it is proved that the resultant variety $R_t(I,J,\mathbb{K})$ has the same geometric meaning than the algebraic resultant variety $R(I,J,\mathbb{K})$.

Lemma 3.4. *Let I, J be two support subsets as before. Let $f =$ "$\sum_{i\in I} a_i x^i$", $g =$ "$\sum_{j\in J}^{m} b_j x^j$" be two univariate tropical polynomials of support I and J. Then, f and g have a common tropical root if and only if the point (a_i, b_j) belongs to the variety defined by $R_t(I,J,\mathbb{K})$.*

Proof. Suppose that (a_i, b_j) belongs to $R_t(I,J,\mathbb{K})$. By Theorem 1.16, we can compute an element $(\widetilde{a}_i, \widetilde{b}_j)$ in the variety defined by $R(I,J,\mathbb{K})$. In this case, $\widetilde{f} = \sum_{i\in I} \widetilde{a}_i x^i$ and $\widetilde{g} = \sum_{j\in J} \widetilde{b}_j x^j$ are lifts of f and g. Moreover, their coefficients belong to the algebraic resultant, so the algebraic polynomials have a common root $\widetilde{q}$ that is non zero by construction ($0 \in I \cap J$). Projecting to the tropical space, f and g have a common root $T(\widetilde{q})$. Conversely, if f and g have a common root q. Then these three elements are the realization of an acyclic incidence configuration in the line $\mathbb{T}$. We can adopt the proof of Theorem 1.30 to compute an algebraic lift. Namely, We may take any lift $\widetilde{f}$ of f, then lift q to a point $\widetilde{q} \in V(\widetilde{f})$ using Theorem 1.16 and, finally, lift g to a polynomial $\widetilde{g}$ having $\widetilde{q}$ as a root. By construction, $\widetilde{f}$, $\widetilde{g}$ share a common root $\widetilde{q}$, hence, their coefficients $(\widetilde{a}_i, \widetilde{b}_j)$ belong to the algebraic resultant variety. Projecting again, the coefficient vector $(a_i,\, b_j)$ of f and g belong to the tropical resultant. □



This Lemma about the geometric meaning of the resultant also shows that the variety defined by $R_t(I, J, \mathbb{K})$ does not depend on the field $\mathbb{K}$. At least as a set of points, because the tropical characterization of two polynomials having a common root does not depend of the field $\mathbb{K}$.

Example 3.5. Consider the easiest nonlinear case, $I = J = \{0, 1, 2\}$, the resultant of two quadratic polynomials. If $f = a+bx+cx^2$, $g = d+ex+fx^2$, the algebraic resultant in characteristic zero is $R_0 = f^2a^2 - 2facd + c^2d^2 - efba - ebcd + ce^2a + dfb^2$ and, over a characteristic 2 field it is $R_2 = f^2a^2 + c^2d^2 + efba + ebcd + ce^2a + dfb^2$. If $char(k) \neq 2$, the tropical polynomial is $P_1 = \text{“}0f^2a^2 + 0facd + 0c^2d^2 + 0efba + 0ebcd + 0ce^2a + 0dfb^2\text{”}$. If $char(\mathbb{K}) = 0$ and $char(k) = 2$, the tropical polynomial is $P_2 = \text{“}0f^2a^2 + (-1)facd + 0c^2d^2 + 0efba + 0ebcd + 0ce^2a + 0dfb^2\text{”}$. Finally, if $char(k) = char(\mathbb{K}) = 2$ then the tropical polynomial is $P_3 = \text{“}0f^2a^2 + 0c^2d^2 + 0efba + 0ebcd + 0ce^2a + 0dfb^2\text{”}$. The unique difference among these polynomials is the term $facd$. This monomial lies in the convex hull of the monomials f^2a^2 and c^2d^2 and it does not define a subdivision because its tropical coefficient is always ≤ 0. The piecewise affine functions $\max\{2f + 2a, f + a + c + d, 2c + 2d\}$, $\max\{2f + 2a, -1 + f + a + c + d, 2c + 2d\}$ and $\max\{2f + 2a, 2c + ad\}$ are the same. So the three polynomials define the same tropical variety.

3.2 Resultant of Two Curves

In this Section, the notion of univariate resultant is extended to the case where the polynomials are bivariate.

Definition 3.6. Let $\widetilde{f}$ and $\widetilde{g}$ be two bivariate polynomials. In order to compute the algebraic resultant with respect to x, we can rewrite them as polynomials in x.

$$\widetilde{f} = \sum_{i \in I} \widetilde{f}_i(y)x^i, \quad \widetilde{g} = \sum_{j \in J} \widetilde{g}_j(y)x^j,$$

where

$$\widetilde{f}_i = \sum_{k=o_i}^{n_i} A_{ik}t^{-\nu_{ik}}y^k, \ \widetilde{g}_j = \sum_{q=r_j}^{m_j} B_{jq}t^{-\eta_{jq}}y^q$$

and A_{ik}, B_{jq} are elements of valuation zero. Let p be the characteristic of $\mathbb{K}$, let $P(a_i, b_j, \mathbb{K}) = R(I, J, \mathbb{K}) \in \mathbb{Z}/(p\mathbb{Z})[a_i, b_j]$ be the algebraic univariate resultant of supports I, J. The *algebraic resultant* of $\widetilde{f}$ and $\widetilde{g}$ is the polynomial $P(\widetilde{f}_i, \widetilde{g}_j, \mathbb{K}) \in \mathbb{K}[y]$. Analogously, let $f = T(\widetilde{f})$, $g = T(\widetilde{g})$, $f = \text{“}\sum_{i \in I} f_i(y)x^i\text{”}$, $g = \text{“}\sum_{j \in J} g_j(y)x^j\text{”}$, where

$$f_i = \text{“}\sum_{k=o_i}^{n_i} \nu_{ik}y^k\text{”}, \ g_j = \text{“}\sum_{q=r_j}^{m_j} \eta_{jq}y^q\text{”}.$$

Let $P_t(a_i, b_j, \mathbb{K}) = R_t(I, J, \mathbb{K}) \in \mathbb{T}[a_i, b_j]$ be the tropical resultant of supports I and J. Then, the polynomial $P_t(f_i, g_j, \mathbb{K}) \in \mathbb{T}[y]$ is the *tropical resultant* of f and g.

Again, we have different tropical resultant polynomials, one for each possible characteristic of the fields. We want to check that this notion of tropical resultant also has a geometric meaning. In the algebraic setting, the roots of the resultant $P(\widetilde{f}_i, \widetilde{g}_j, \mathbb{K})$ are the possible y-th values of the intersection points $V(\widetilde{f}) \cap V(\widetilde{g})$. This is not the case of the tropical resultant, because $P_t(f_i, g_j, \mathbb{K})$ only has finitely many tropical roots, while the intersection $\mathcal{T}(f) \cap \mathcal{T}(g)$ may have infinitely many points and there may be infinitely many possible values of the y-th coordinates. Again, this indetermination is avoided with the notion of stable intersection. We will prove that the roots of $P_t(f_i, g_j, \mathbb{K})$ are the possible y-th values of the stable intersection $\mathcal{T}(f) \cap_{st} \mathcal{T}(g)$. This will be made in several steps, the first one is to check that $T(V(P(\widetilde{f}_i, \widetilde{g}_j, \mathbb{K}))) = \mathcal{T}(P_t(f_i, g_j, \mathbb{K}))$, provided that A_{ik}, B_{jq} are residually generic. Sometimes, for technical reasons, it is better to work with an affine representation of the resultant (For example, if $\widetilde{f} = \sum_{i \in I} a_i x^{i^1} y^{i^2}$, $\widetilde{g} = \sum_{j \in J} b_j x^{j^1} y^{j^2}$ we can suppose that $a_{i_0} = b_{j_0} = 1$). We prove that this dehomogenization process is also compatible with tropicalization. That is, if we divide each algebraic coefficient $A_{ik} t^{-\nu_{ik}}$ and $B_{jq} t^{-\eta_{jq}}$ by $A_{i_0 k_0} t^{-\nu_{i_0 k_0}}$ and $B_{j_0 q_0} t^{-\eta_{j_0 q_0}}$ respectively and substitute each coefficient ν_{ik}, η_{jq} by $\nu_{ik} - \nu_{i_0 k_0} =$ "$\nu_{ik}/\nu_{i_0 k_0}$" and $\eta_{iq} - \eta_{i_0 q_0}$ respectively, still we have that $T(V(P(\widetilde{f}_i, \widetilde{g}_j, \mathbb{K}))) = \mathcal{T}(P_t(f_i, g_j, \mathbb{K}))$.

Lemma 3.7. *Let $\widetilde{f} = \sum_{i \in I} \widetilde{f}_i x^i$, $\widetilde{g} = \sum_{j \in J} \widetilde{g}_j x^j \in \mathbb{K}[x, y]$, where the coefficients are $\widetilde{f}_i = \sum_{k=o_i}^{n_i} A_{ik} t^{-\nu_{ik}} y^k$, $\widetilde{g}_j = \sum_{q=r_j}^{m_j} B_{jq} t^{-\eta_{jq}} y^q$ and let $f = \sum_{i \in I} f_i(y) x^i$, $g = \sum_{j \in J} g_j(y) x^j$, $f_i =$ "$\sum_{k=o_i}^{n_i} \nu_{ik} y^k$", $g_j =$ "$\sum_{q=r_j}^{m_j} \eta_{jq} y^q$" be the corresponding tropical polynomials. Suppose that A_{ik}, B_{jq} are residually generic. Then $T(V(P(\widetilde{f}_i, \widetilde{g}_j, \mathbb{K}))) = \mathcal{T}(P_t(f_i, g_j, \mathbb{K}))$.*

Proof. First, we suppose that $char(k) = 0$. In general, the composition of polynomials does not commute with tropicalization, because, in the algebraic case, there can be a cancellation of terms when performing the substitution that does not occur in the tropical case. Recall that, by the nature of tropical operations, a cancellation of terms in the tropical development of the polynomial never happens. So, we have to check that there is never a cancellation of terms in the algebraic setting. First, it is proved that there is no cancellation of monomials when substituting the variables by polynomials without dehomogenizing. $P(a_i, b_j, \mathbb{K})$ is homogeneous in the set of variables a_i and in the set of variables b_j. As the substitution is linear in the variables A_{ik} and B_{jq}, $P(\widetilde{f}_i, \widetilde{g}_j, \mathbb{K})$ is homogeneous in A_{ij} and B_{jq}. If we have two different terms T_1, T_2 of $P(a_i, b_j, \mathbb{K})$, then there is a variable with different exponent in both terms. Assume for simplicity that this variable is a_1 with degrees d_1 and d_2 respectively. After the substitution, the monomials obtained by expansion of T_1 are homogeneous of degree d_1 in the set of variables A_{1k} and the monomials coming from T_2 are homogeneous of degree d_2 in the variables A_{1k}. Thus, it is not possible to have a cancellation of terms and we can conclude that the homogeneous polynomial projects onto the tropical homogeneous polynomial.

In the case we dehomogenize $\widetilde{f}$ and $\widetilde{g}$ with respect to the incides $(i_0 k_0)$, $(j_0 q_0)$ respectively. By the homogeneous case, we can suppose that all the variables $a_i \neq a_{i_0}$ and $b_j \neq b_{j_0}$ in $P(a_i, b_i, \mathbb{K})$ have already been substituted by the polynomials $\widetilde{f}_i$ and

$\widetilde{g}_j$ respectively. The only possibility to have a cancellation of terms is if there are two monomials of the form $Xa_{i_0}^{d_1}b_{j_0}^{d_2}$, $Xa_{i_0}^{d_3}b_{j_0}^{d_4}$ with $d_1+d_2=d_3+d_4$ and X is a monomial in the variables A_{ik}, B_{jq}. But, as the polynomial is multihomogeneous in A and B, it must happen that $d_1=d_3$ and $d_2=d_4$. That is, the original monomials where the same. So, a cancellation of terms is not possible and the dehomogenized polynomial projects into the dehomogenized tropical polynomial. In particular, $T(V(P(\widetilde{f}_i,\widetilde{g}_j,\mathbb{K})))=\mathcal{T}(P_t(f_i,g_j,\mathbb{K}))$.

Now suppose that $char(k)=p>0$. In this case, it is not necessarily true that the tropicalization of the algebraic resultant is the tropical resultant. But we are going to check that the monomials where these two tropical polynomials differ do not apport anything to the tropical variety $\mathcal{T}(f_i,g_i,\mathbb{K})$. So, we are going to compare the monomials in $P(\widetilde{f}_i,\widetilde{g}_j,\mathbb{K})$ and $P_t(f_i,g_j,\mathbb{K})$. The support of both polynomials is contained in the support of $P_t(f_i,g_j,\mathbb{L})$, where $\mathbb{L}$ is an equicharacteristic zero field. The first potential difference in the monomials are those obtained by expansion of a monomial m of the univariate resultant $P(a_i,b_j,\mathbb{K})=R(I,J,\mathbb{K})$ whose coefficient has valuation in $[-\infty,0)$. That is, p divides coeff(m). It happens that m is never a extreme monomial. That is, $m=\sum_l\lambda_l v_l$, $0\leq\lambda_l\leq 1$ and v_i are extreme monomials. So, for every r, coeff$(m)+m(f_i(r),g_j(r))\leq m(f_i(r),g_j(r))=\sum_l\lambda_l v_l(f_i(r),g_j(r))\leq \max\{v_l(f_i(r),g_j(r))\}$. Hence, the monomials of $m(f_i(y),g_j(y))$ never apport anything to the tropical variety defined by $P(\widetilde{f}_i,\widetilde{g}_j,\mathbb{K})$, because they are never greater than the monomials that appear by the extreme monomials. The other source of potential differences in the monomials is the decreasing of the tropicalizacion of some terms of the power $(\sum_{k=o_i}^{n_i}A_{ik}t^{-\nu_{ik}}y^k)^N$ due to some combinatorial coefficient $\binom{N}{m}$ divisible by p. But, in the tropical context, it happens that

$$(\text{“}\sum_{k=o_i}^{n_i}\nu_{ik}y^k\text{”})^N=\text{“}\sum_{k=o_i}^{n_i}\nu_{ik}^N y^{kN}\text{”}$$

as piecewise affine functions. The rest of the terms in the expansion do not contribute anything to the tropical variety. The only terms that may play a role are ν_{ik}^N, η_{jq}^M. So, even if the tropicalization of the polynomials $P(I,J,\mathbb{K})$ depends on the algebraic field $\mathbb{K}$, the tropical variety they define is always the same and it is the tropical variety defined by $P_t(f_i,g_j,\mathbb{K})$, including the weight of the cells. □

So, the previous Lemma provides a notion of tropical resultant for bivariate polynomials with respect to one variable. They also prove that this polynomials define the same variety as the projection of the algebraic resultant in the generic case. Our next goal is to provide a geometric meaning to the roots of the tropical resultant in terms of the stable intersection of the curves.

3.3 Computation of the Stable Intersection

Let f be a tropical polynomial of support I defining a curve, let Δ_f be the convex hull of I. By Proposition 1.19, the coefficients of f induce a regular subdivision in Δ_f dual

to f. This subdivision is essential in the definition of tropical multiplicity and stable intersection given in Chapter 1. Next, it is proved that, for sufficiently generic lifts $\widetilde{f}$ and $\widetilde{g}$, their intersection points correspond with stable intersection points of f and g.

Lemma 3.8. *Let f and g be two tropical polynomials in two variables. Let L be its stable intersection. Then, for any two lifts $\widetilde{f}$, $\widetilde{g}$ such that their coefficients are residually generic, the intersection of the algebraic curves projects into the stable intersection.*

$$T(\widetilde{f} \cap \widetilde{g}) \subseteq \mathcal{T}(f) \cap_{st} \mathcal{T}(g)$$

Proof. If every intersection point of f and g is stable, then there is nothing to prove. Let q be a non stable intersection point. This means that q belongs to the relative interior of two parallel edges of $\mathcal{T}(f)$ and $\mathcal{T}(g)$. The residual polynomials $\widetilde{f}_q$ and $\widetilde{g}_q$ can be written (after multiplication by a suitable monomial) as $\widetilde{f}_q = \sum_{i=0}^{n} \alpha_i (x^r y^s)^i$, $\widetilde{g}_q = \sum_{j=0}^{m} \beta_i (x^r y^s)^j$. If $\widetilde{f}$, $\widetilde{g}$ have a common point projecting into q then there is an algebraic relation among their residual coefficients. Namely, the resultant of the polynomials $\sum_{i=0}^{n} \alpha_i z^i$, $\sum_{j=0}^{m} \beta_i z^j$ with respect to z must vanish. If the residual coefficients of $\widetilde{f}$, $\widetilde{g}$ do not belong to the resultant defined by each non stable intersection cell, the intersection in the torus of $\widetilde{f}$, $\widetilde{g}$ projects into the stable intersection of f and g. □

So, there is a natural relation between the stable intersection of two tropical curves and the intersection of two generic lifts of the curves. On the other hand, the intersection of two generic lifts can be determined by the algebraic resultant of the defining polynomials. Applying tropicalization, this relationship links the notion of stable intersection with the resultants. To achieve a true bijection between the roots of the resultant and the intersection points of the curves, it is used the relationship between the tropical and algebraic resultants. So, one needs to concrete the generality conditions for the values values A_{ik}, B_{jq} that makes Lemma 3.7 and Proposition 3.7 hold. Next Lemma shows how to compute the residually conditions for the compatibility of the resultant.

Lemma 3.9. *Let $\widetilde{f}$, $\widetilde{g} \in \mathbb{K}[x, y]$. Then, there is a finite set of nonzero polynomials in the principal coefficients of the coefficients of $\widetilde{f}$, $\widetilde{g}$, that depends only on the tropicalization f and g such that, if no one of them vanishes, then*

$$T(Res_x(\widetilde{f}, \widetilde{g})) = \mathcal{T}(R(I, J, \mathbb{K})(f, g)).$$

Where $R(I, J, \mathbb{K})(f, g)$ is the evaluation of the tropical resultant of supports I and J in the coefficients of f and g as polynomials over x.

Proof. Write $\widetilde{f} = \text{“}\sum_{i,k} \widetilde{a}_{ik} x^i y^k\text{”}$, $\widetilde{g} = \text{“}\sum_{j,q} \widetilde{b}_{jq} x^j y^q\text{”}$, $Pc(\widetilde{a}_{ik}) = \alpha_{ik}$, $Pc(\widetilde{b}_{jq}) = \beta_{jq}$, $T(\widetilde{a}_{ik}) = a_{ik}$, $T(\widetilde{b}_{jq}) = b_{jq}$, $f = \text{“}\sum_{i,k} a_{ik} x^i y^k\text{”}$, $g = \text{“}\sum_{j,q} b_{jq} x^j y^q\text{”}$. Let I, J be the support of f and g with respect to x. Consider both resultants

$$R(I, J, \mathbb{K})(\widetilde{f}, \widetilde{g}) = \sum_{r=0}^{N} \widetilde{h}_r y^r \text{ and } R_t(I, J, \mathbb{K})(f, g) = \text{“}\sum_{r=0}^{N} h_r y^r\text{”}.$$

It happens that $T(\widetilde{h}_r) \leq h_r$ and the equality holds if and only if the term $\gamma_r(\alpha,\beta)t^{-h_r}$ of $\widetilde{h}_r$ is different from 0. As in the generic case the resultant projects correctly by Lemma 3.7, the polynomials γ_r corresponding to two consecutive points in the Newton diagram of "$\sum_{r=0}^{N} h_r y^r$" (see Definition 1.7) are non zero polynomials in $k[\alpha_{ik},\beta_{jq}]$. If no one of them vanish, the resultant tropicalizes correctly. □

Theorem 3.10. *Let $\widetilde{f}$, $\widetilde{g} \in \mathbb{K}[x,y]$. Then, it can be computed a finite set of polynomials in the principal coefficients of $\widetilde{f}$, $\widetilde{g}$ depending only on their tropicalization f, g such that, if no one of them vanish, the tropicalization of the intersection of $\widetilde{f}$, $\widetilde{g}$ is exactly the stable intersection of f and g. Moreover, the multiplicities are conserved.*

$$\sum_{\substack{\widetilde{q}\in\widetilde{f}\cap\widetilde{g}\\ T(\widetilde{q})=q}} mult(\widetilde{q}) = mult_t(q)$$

Proof. Lemma 3.9 provides a set S of polynomials in the principal coefficients of $\widetilde{f}$ and $\widetilde{g}$ such that, if no one vanishes, the algebraic resultants $\mathrm{Res}_x(\widetilde{f},\widetilde{g})$ and $\mathrm{Res}_y(\widetilde{f},\widetilde{g})$ define the same tropical varieties as $\mathrm{Res}_x(f,g)$ and $\mathrm{Res}_y(f,g)$. These two resultants define a finite set P that contains the stable intersection. The problem is that, in the tropical case, it is possible that the intersection of P with both curves may be strictly larger than the stable intersection of the curves, see Example 3.11. So, we need another polynomial in order to discriminate the points in this intersection that are not stable points. Take a, any natural number such that the affine function $x-ay$ is injective in the finite set P. Make the monomial change of coordinates $z = xy^{-a}$. The polynomial $\mathrm{Res}_y(\widetilde{f}(zy^a,y),\widetilde{g}(zy^a,y)) = \widetilde{R}(z) = \widetilde{R}(xy^{-a})$ encodes the values xy^{-a} of the common roots of $\widetilde{f}$ and $\widetilde{g}$. We add to the set S the restrictions in the principal coefficients of this resultant to be compatible with tropicalization according to Lemma 3.9. These values xy^{-a} of the algebraic intersection points correspond with the possible values $x-ay$ of the tropicalization of the roots. As the linear function is injective in P, then $\mathcal{T}(f)\cap\mathcal{T}(g)\cap\mathcal{T}(\mathrm{Res}_x(f,g))\cap\mathcal{T}(\mathrm{Res}_y(f,g))\cap\mathcal{T}(R(\text{“}xy^{-a}\text{”}))$ is exactly the tropicalization of the intersection points of any system $(\widetilde{f},\widetilde{g})$ verifying the restrictions of S. By, Lemma 3.8, this set is contained in the stable intersection of f and g.

To prove that the multiplicities are conserved, consider the field $\mathbb{K} = \mathbb{C}((t^{\mathbb{R}}))$ of generalized Puiseux series, in this case

$$\sum_{\substack{\widetilde{q}\in\widetilde{f}\cap\widetilde{g}\\ T(\widetilde{q})=q}} \mathrm{mult}(\widetilde{q}) \leq \mathrm{mult}_t(q).$$

because the sum on the left is bounded by the mixed volume of the residual polynomials $\widetilde{f}_q$, $\widetilde{g}_q$ over q by Bernstein-Koushnirenko Theorem (c.f. [Ber75] [Kus76] [Roj99]). This mixed volume is, by definition, the tropical multiplicity of q on the right. On the other hand, the sum on the left is, over any field, the sum of the multiplicities of the algebraic roots of $\widetilde{R}(xy^{-a})$ projecting onto q. By the previous results on the correct projection of the resultant, this multiplicity does not depend on $\mathbb{K}$, because it is the degree minus the order of the residual polynomial $R(xy^{-a})_{q_x-aq_y}$, or, equivalently, the multiplicity

of q as a root of $T(R(xy^{-a}))$. Moreover, this multiplicity is the mixed volume of the residual polynomials over q. That is, the inequality

$$\sum_{\substack{\widetilde{q}\in\widetilde{f}\cap\widetilde{g}\\ T(\widetilde{q})=q}} \mathrm{mult}(\widetilde{q}) \leq \mathrm{mult}_t(q)$$

holds for any field. The total number of roots of $\widetilde{f}$ and $\widetilde{g}$ counted with multiplicities in the torus equals the sum of multiplicities of the stable roots of f and g, because, in both cases, this is the degree minus the order of $R(xy^{-a})$. From this, we conclude that

$$\sum_{\substack{\widetilde{q}\in\widetilde{f}\cap\widetilde{g}\\ T(\widetilde{q})=q}} \mathrm{mult}(\widetilde{q}) = \mathrm{mult}_t(q)$$

Hence, the projection of the intersection of $\widetilde{f}$ and $\widetilde{g}$ is exactly the stable intersection. □

Example 3.11. Consider $f = g =$ "$0 + 1x + 1y + 1xy + 0x^2 + 0y^2$", two conics. Their stable intersection is the set $\{(-1,-1), (0,1), (1,0), (0,0)\}$. Compute the resultants: $\mathrm{Res}_x(f,g) =$ "$0 + 1y + 1y^2 + 1y^3 + 0y^4$", by symmetry $\mathrm{Res}_y(f,g) =$ "$0 + 1x + 1x^2 + 1x^3 + 0x^4$". Their roots are the lines $y = -1$, $y = 0$, $y = 1$ and $x = -1$, $x = 0$, $x = 1$ respectively. In both cases the multiplicity of the roots -1 and 1 is 1, while the multiplicity of 0 is 2. The intersection of this lines and the two curves gives the four stable points plus $(-1,1)$ and $(1,-1)$. We need another resultant that discriminates the points. See Figure 3.1. Take $x - 3y$, the first affine function $x - ay$ that is injective over these points. $f($"zy^3"$, y) =$ "$0 + 1y + 0y^2 + 1y^3z + 1y^4z + 0y^6z^2$". $\mathrm{Res}_y(f($"zy^3"$, y), g($"zy^3"$, y)) =$ "$6z^8+9z^9+9z^{10}+8z^{11}+6z^{12}$". Its roots are $0, 1, 2, -3$, all with multiplicity 1. It is easy to check now that the intersection of the two curves and the three resultants is exactly the stable intersection. The two extra points take the values -4, 4 in the monomial "xy^{-3}", moreover, every point has intersection multiplicity equal to one.

Two generic lifts of the cubics are of the form:

$$\widetilde{f} = a_1 + a_x t^{-1}x + a_y t^{-1}y + a_{xy}t^{-1}xy + a_{xx}x^2 + a_{yy}y^2$$

$$\widetilde{g} = c_1 + c_x t^{-1}x + c_y t^{-1}y + c_{xy}t^{-1}xy + c_{xx}x^2 + c_{yy}y^2$$

The residual conditions for the compatibility of the algebraic and tropical resultant with respect to x are:

$-\gamma_{xy}\ \gamma_{xx}\ \alpha_{xy}\ \alpha_{yy} - \gamma_{xy}\ \alpha_{xy}\ \alpha_{xx}\ \gamma_{yy} + \gamma_{xy}^2\ \alpha_{xx}\ \alpha_{yy} + \gamma_{yy}\ \gamma_{xx}\ \alpha_{xy}^2$, $-\gamma_x\ \gamma_{xx}\ \alpha_x\ \alpha_1 - \gamma_x\ \alpha_x\ \alpha_{xx}\ \gamma_1 + \gamma_1\ \gamma_{xx}\ \alpha_x^2 + \alpha_{xx}\ \gamma_x^2\ \alpha_1$, $\gamma_y\ \gamma_{xx}\ \alpha_x^2 - \gamma_x\ \gamma_{xx}\ \alpha_x\ \alpha_y + \alpha_{xx}\ \gamma_x^2\ \alpha_y - \gamma_x\ \alpha_x\ \alpha_{xx}\ \gamma_y$, $-\gamma_{xy}\ \alpha_{xy}\ \alpha_{xx}\ \gamma_y + \gamma_y\ \gamma_{xx}\ \alpha_{xy}^2 - \gamma_{xy}\ \gamma_{xx}\ \alpha_{xy}\ \alpha_y + \gamma_{xy}^2\ \alpha_{xx}\ \alpha_y$

For the resultant with respect to y, the compatibility conditions are:

$-\gamma_y\,\gamma_{yy}\,\alpha_y\,\alpha_1\,-\gamma_y\,\alpha_y\,\alpha_{yy}\,\gamma_1\,+\gamma_1\,\gamma_{yy}\,\alpha_y^2\,+\gamma_y^2\,\alpha_{yy}\,\alpha_1,\,\gamma_x\,\gamma_{yy}\,\alpha_y^2\,-\gamma_y\,\alpha_y\,\alpha_{yy}\,\gamma_x\,+\gamma_y^2\,\alpha_{yy}\,\alpha_x$
$-\gamma_y\,\gamma_{yy}\,\alpha_y\,\alpha_x,\,\gamma_{xy}^2\,\alpha_{yy}\,\alpha_x\,+\gamma_x\,\gamma_{yy}\,\alpha_{xy}^2\,-\gamma_{xy}\,\gamma_{yy}\,\alpha_{xy}\,\alpha_x\,-\gamma_{xy}\,\alpha_{xy}\,\alpha_{yy}\,\gamma_x,\,-\gamma_{xy}\,\gamma_{xx}\,\alpha_{xy}\,\alpha_{yy}$
$-\gamma_{xy}\,\alpha_{xy}\,\alpha_{xx}\,\gamma_{yy}\,+\gamma_{xy}^2\,\alpha_{xx}\,\alpha_{yy}\,+\gamma_{yy}\,\gamma_{xx}\,\alpha_{xy}^2.$

Finally, the third resultant is a degree twelve polynomial in the variable z. The residual conditions for its compatibility with the tropical resultant are:

$2\gamma_{yy}^2\,\gamma_{xx}\,\alpha_{xy}^3\,\alpha_{yy}\,\gamma_y\,\alpha_y\,\gamma_1\,\alpha_{xx}\,\gamma_{xy}\,-\gamma_{yy}^2\,\gamma_{xx}^2\,\alpha_{xy}^4\,\alpha_{yy}\,\gamma_y\,\alpha_y\,\gamma_1\,-2\gamma_{yy}^2\,\alpha_{xy}\,\gamma_{xy}^3\,\alpha_{xx}^2\,\alpha_y^2\,\gamma_1\,\alpha_{yy}$
$+\gamma_{xy}^4\,\alpha_{xx}^2\,\gamma_{yy}\,\alpha_{yy}^2\,\alpha_y^2\,\gamma_1\,-\gamma_{xy}^4\,\alpha_{xx}^2\,\gamma_{yy}\,\alpha_{yy}^2\,\alpha_y\,\gamma_y\,\alpha_1\,+\gamma_{yy}^2\,\alpha_{xy}^2\,\alpha_{yy}\,\gamma_y^2\,\alpha_{xx}^2\,\gamma_{xy}^2\,\alpha_1\,-\gamma_{xy}^2\,\gamma_{xx}^2$
$\alpha_{xy}^2\,\alpha_{yy}^3\,\gamma_y\,\alpha_y\,\gamma_1\,-2\gamma_{yy}\,\alpha_{xy}\,\gamma_{xy}^3\,\alpha_{xx}^2\,\alpha_{yy}^2\,\gamma_y^2\,\alpha_1\,+2\gamma_{yy}^2\,\gamma_{xx}^2\,\alpha_{xy}^3\,\gamma_{xy}\,\alpha_y\,\gamma_y\,\alpha_{yy}\,\alpha_1\,-2\gamma_{yy}^2\,\gamma_{xx}^2$
$\alpha_{xy}^3\,\gamma_{xy}\,\alpha_y^2\,\gamma_1\,\alpha_{yy}\,-\gamma_{xy}^2\,\gamma_{xx}^2\,\alpha_{xy}^2\,\gamma_{yy}\,\alpha_{yy}^2\,\alpha_y\,\gamma_y\,\alpha_1\,+\gamma_{xy}^2\,\gamma_{xx}^2\,\alpha_{xy}^2\,\gamma_{yy}\,\alpha_{yy}^2\,\alpha_y^2\,\gamma_1\,-4\gamma_{yy}^2\,\gamma_{xx}\,\alpha_{xy}^2$
$\gamma_{xy}^2\,\alpha_{xx}\,\alpha_y\,\gamma_y\,\alpha_{yy}\,\alpha_1\,-2\gamma_{yy}\,\gamma_{xx}^2\,\alpha_{xy}^3\,\gamma_{xy}\,\alpha_{yy}^2\,\gamma_y^2\,\alpha_1\,+2\gamma_{yy}^2\,\alpha_{xy}\,\gamma_{xy}^3\,\alpha_{xx}^2\,\alpha_y\,\gamma_y\,\alpha_{yy}\,\alpha_1\,+2\gamma_{yy}$
$\gamma_{xx}^2\,\alpha_{xy}^3\,\gamma_{xy}\,\alpha_{yy}^2\,\gamma_y\,\alpha_y\,\gamma_1\,+4\gamma_{yy}\,\gamma_{xx}\,\alpha_{xy}^2\,\gamma_{xy}^2\,\alpha_{yy}^2\,\gamma_y^2\,\alpha_{xx}\,\alpha_1\,+\gamma_{yy}^3\,\gamma_{xx}^2\,\alpha_{xy}^4\,\alpha_y^2\,\gamma_1\,-4\gamma_{yy}\,\gamma_{xx}$
$\alpha_{xy}^2\,\gamma_{xy}^2\,\alpha_{yy}^2\,\gamma_y\,\alpha_{xx}\,\alpha_y\,\gamma_1\,-\gamma_{yy}^3\,\gamma_{xx}^2\,\alpha_{xy}^4\,\alpha_y\,\gamma_y\,\alpha_1\,+2\gamma_{yy}^3\,\gamma_{xx}\,\alpha_{xy}^3\,\alpha_y\,\gamma_y\,\alpha_{xx}\,\gamma_{xy}\,\alpha_1\,-2\gamma_{yy}^3\,\gamma_{xx}$
$\alpha_{xy}^3\,\alpha_y^2\,\gamma_1\,\alpha_{xx}\,\gamma_{xy}\,-\gamma_{yy}^3\,\alpha_{xy}^2\,\alpha_{xx}^2\,\gamma_{xy}^2\,\alpha_y\,\gamma_y\,\alpha_1\,+\gamma_{yy}^3\,\alpha_{xy}^2\,\alpha_{xx}^2\,\gamma_{xy}^2\,\alpha_y^2\,\gamma_1\,+\gamma_{xy}^2\,\gamma_{xx}^2\,\alpha_{xy}^2\,\alpha_{yy}^3\,\gamma_y^2$
$\alpha_1\,-\gamma_{yy}^2\,\alpha_{xy}^2\,\alpha_{yy}\,\gamma_y\,\alpha_{xx}^2\,\gamma_{xy}^2\,\alpha_y\,\gamma_1\,-2\gamma_{yy}^2\,\gamma_{xx}\,\alpha_{xy}^3\,\alpha_{xx}\,\gamma_{xy}\,\alpha_{yy}\,\gamma_y^2\,\alpha_1\,+\gamma_{yy}^2\,\gamma_{xx}^2\,\alpha_{xy}^4\,\alpha_{yy}\,\gamma_y^2\,\alpha_1$
$-\gamma_{xy}^4\,\alpha_{xx}^2\,\alpha_{yy}^3\,\gamma_y\,\alpha_y\,\gamma_1\,+4\gamma_{yy}^2\,\gamma_{xx}\,\alpha_{xy}^2\,\gamma_{xy}^2\,\alpha_{xx}\,\alpha_y^2\,\gamma_1\,\alpha_{yy}\,+\gamma_{xy}^4\,\alpha_{xx}^2\,\alpha_{yy}^3\,\gamma_y^2\,\alpha_1\,+2\gamma_{xy}^3\,\alpha_{xx}\,\gamma_{xx}$
$\alpha_{xy}\,\gamma_{yy}\,\alpha_{yy}^2\,\alpha_y\,\gamma_y\,\alpha_1\,-2\gamma_{xy}^3\,\alpha_{xx}\,\gamma_{xx}\,\alpha_{xy}\,\gamma_{yy}\,\alpha_{yy}^2\,\alpha_y^2\,\gamma_1\,-2\gamma_{xy}^3\,\gamma_{xx}\,\alpha_{xy}\,\alpha_{xx}\,\alpha_{yy}^3\,\gamma_y^2\,\alpha_1\,+2\gamma_{xy}^3$
$\gamma_{xx}\,\alpha_{xy}\,\alpha_{xx}\,\alpha_{yy}^3\,\gamma_y\,\alpha_y\,\gamma_1\,+2\gamma_{yy}\,\alpha_{xy}\,\gamma_{xy}^3\,\alpha_{xx}^2\,\alpha_{yy}^2\,\gamma_y\,\alpha_y\,\gamma_1,$
$3\gamma_{xy}\,\gamma_{xx}^2\,\alpha_{xy}^4\,\gamma_y^2\,\alpha_y^2\,\gamma_1\,-3\gamma_{xy}\,\gamma_{xx}^2\,\alpha_{xy}^4\,\gamma_y^3\,\alpha_y\,\alpha_1\,-\gamma_{xx}^2\,\alpha_{xy}^5\,\gamma_y^3\,\alpha_y\,\gamma_1\,+3\gamma_{xy}^3\,\alpha_{xx}^2\,\gamma_y^2\,\alpha_{xy}^2\,\alpha_y^2\,\gamma_1$
$-\gamma_{xy}^5\,\alpha_{xx}^2\,\alpha_y^3\,\gamma_y\,\alpha_1\,+\gamma_{xy}^3\,\gamma_{xx}^2\,\alpha_{xy}^2\,\alpha_y^4\,\gamma_1\,+6\gamma_{xy}^3\,\alpha_{xx}\,\gamma_y\,\gamma_{xx}\,\alpha_{xy}^2\,\alpha_y^3\,\gamma_1\,-3\gamma_{xy}^4\,\alpha_{xx}^2\,\gamma_y\,\alpha_{xy}\,\alpha_y^3\,\gamma_1$
$-6\gamma_{xy}^3\,\alpha_{xx}\,\gamma_y^2\,\gamma_{xx}\,\alpha_{xy}^2\,\alpha_y^2\,\alpha_1\,+3\gamma_{xy}^4\,\alpha_{xx}^2\,\gamma_y^2\,\alpha_{xy}\,\alpha_y^2\,\alpha_1\,+\gamma_{xy}^5\,\alpha_{xx}^2\,\alpha_y^4\,\gamma_1\,-3\gamma_{xy}^3\,\alpha_{xx}^2\,\gamma_y^3\,\alpha_{xy}^2\,\alpha_y$
$\alpha_1\,-2\gamma_{xy}^4\,\gamma_{xx}\,\alpha_{xy}\,\alpha_{xx}\,\alpha_y^4\,\gamma_1\,+2\gamma_{xy}\,\gamma_{xx}\,\alpha_{xy}^4\,\gamma_y^3\,\alpha_{xx}\,\alpha_y\,\gamma_1\,-\gamma_{xy}^2\,\alpha_{xx}^2\,\gamma_y^3\,\alpha_{xy}^3\,\alpha_y\,\gamma_1\,-2\gamma_{xy}\,\gamma_{xx}$
$\alpha_{xy}^4\,\gamma_y^4\,\alpha_{xx}\,\alpha_1\,+2\gamma_{xy}^4\,\gamma_{xx}\,\alpha_{xy}\,\alpha_{xx}\,\alpha_y^3\,\gamma_y\,\alpha_1\,-\gamma_{xy}^3\,\gamma_{xx}^2\,\alpha_{xy}^2\,\alpha_y^3\,\gamma_y\,\alpha_1\,+\gamma_{xx}^2\,\alpha_{xy}^5\,\gamma_y^4\,\alpha_1\,+3\gamma_{xy}^2\,\gamma_{xx}^2$
$\alpha_{xy}^3\,\gamma_y^2\,\alpha_y^2\,\alpha_1\,-6\gamma_{xy}^2\,\alpha_{xx}\,\gamma_y^2\,\gamma_{xx}\,\alpha_{xy}^3\,\alpha_y^2\,\gamma_1\,+6\gamma_{xy}^2\,\alpha_{xx}\,\gamma_y^3\,\gamma_{xx}\,\alpha_{xy}^3\,\alpha_y\,\alpha_1\,-3\gamma_{xy}^2\,\gamma_{xx}^2\,\alpha_{xy}^3\,\gamma_y\,\alpha_y^3$
$\gamma_1\,+\gamma_{xy}^2\,\alpha_{xx}^2\,\gamma_y^4\,\alpha_{xy}^3\,\alpha_1,$
$\gamma_{xy}^3\,\alpha_{xx}^2\,\gamma_x^2\,\alpha_x\,\alpha_y^3\,\gamma_1\,+\gamma_x\,\gamma_{xx}^2\,\alpha_{xy}^3\,\alpha_x^2\,\gamma_y^3\,\alpha_1\,+\gamma_x^3\,\gamma_{xx}^2\,\alpha_{xy}^3\,\alpha_y^2\,\gamma_y\,\alpha_1\,+\gamma_{xy}^3\,\alpha_{xx}^2\,\alpha_x^3\,\gamma_y^2\,\alpha_y\,\gamma_1\,-\gamma_x^3$
$\alpha_{xy}\,\alpha_{xx}^2\,\gamma_{xy}^2\,\alpha_y^3\,\gamma_1\,+2\gamma_{xy}\,\gamma_{xx}^2\,\alpha_{xy}^2\,\gamma_x\,\alpha_x^2\,\gamma_y^2\,\alpha_y\,\alpha_1\,+2\gamma_{xy}^2\,\alpha_{xx}\,\gamma_{xx}\,\alpha_x^3\,\gamma_y^3\,\alpha_{xy}\,\alpha_1\,+4\gamma_{xy}^2\,\alpha_{xx}\,\gamma_x$
$\gamma_{xx}\,\alpha_x^2\,\gamma_y\,\alpha_{xy}\,\alpha_y^2\,\gamma_1\,-4\gamma_{xy}^2\,\alpha_{xx}\,\gamma_x\,\gamma_{xx}\,\alpha_x^2\,\gamma_y^2\,\alpha_{xy}\,\alpha_y\,\alpha_1\,-2\gamma_{xy}^3\,\alpha_{xx}^2\,\gamma_x\,\alpha_x^2\,\alpha_y^2\,\gamma_y\,\gamma_1\,+2\gamma_{xy}^3\,\alpha_{xx}^2$
$\gamma_x\,\alpha_x^2\,\alpha_y\,\gamma_y^2\,\alpha_1\,-\gamma_{xy}^3\,\alpha_{xx}^2\,\gamma_x^2\,\alpha_x\,\alpha_y^2\,\gamma_y\,\alpha_1\,-\gamma_x\,\gamma_{xx}^2\,\alpha_{xy}^3\,\alpha_x^2\,\gamma_y^2\,\alpha_y\,\gamma_1\,+\gamma_{xy}\,\gamma_{xx}^2\,\alpha_{xy}^2\,\gamma_x^2\,\alpha_x\,\alpha_y^3\,\gamma_1$
$-\gamma_{xy}\,\gamma_{xx}^2\,\alpha_{xy}^2\,\gamma_x^2\,\alpha_x\,\alpha_y^2\,\gamma_y\,\alpha_1\,+2\gamma_x^2\,\gamma_{xx}^2\,\alpha_{xy}^3\,\gamma_y\,\alpha_y^2\,\gamma_1\,\alpha_x\,-2\gamma_x^2\,\gamma_{xx}^2\,\alpha_{xy}^3\,\gamma_y^2\,\alpha_y\,\alpha_x\,\alpha_1\,+2\gamma_x^3\,\gamma_{xx}$
$\alpha_{xy}^2\,\gamma_{xy}\,\alpha_y^3\,\gamma_1\,\alpha_{xx}\,-2\gamma_x^3\,\gamma_{xx}\,\alpha_{xy}^2\,\gamma_{xy}\,\alpha_y^2\,\gamma_y\,\alpha_{xx}\,\alpha_1\,+\gamma_{xy}\,\gamma_{xx}^2\,\alpha_{xy}^2\,\alpha_x^3\,\gamma_y^2\,\alpha_y\,\gamma_1\,+\gamma_x^3\,\alpha_{xy}\,\alpha_{xx}^2\,\gamma_{xy}^2$
$\alpha_y^2\,\gamma_y\,\alpha_1\,+2\gamma_x\,\gamma_{xx}\,\alpha_{xy}^2\,\gamma_{xy}\,\alpha_x^2\,\gamma_y^2\,\alpha_{xx}\,\alpha_y\,\gamma_1\,-2\gamma_x\,\gamma_{xx}\,\alpha_{xy}^2\,\gamma_{xy}\,\alpha_x^2\,\gamma_y^3\,\alpha_{xx}\,\alpha_1\,-4\gamma_x^2\,\gamma_{xx}\,\alpha_{xy}^2$
$\gamma_{xy}\,\alpha_x\,\gamma_y\,\alpha_y^2\,\gamma_1\,\alpha_{xx}\,+4\gamma_x^2\,\gamma_{xx}\,\alpha_{xy}^2\,\gamma_{xy}\,\alpha_x\,\gamma_y^2\,\alpha_y\,\alpha_{xx}\,\alpha_1\,+2\gamma_x^2\,\alpha_{xy}\,\gamma_{xy}^2\,\alpha_x\,\alpha_y^2\,\alpha_{xx}^2\,\gamma_y\,\gamma_1\,-2\gamma_x^2$
$\alpha_{xy}\,\gamma_{xy}^2\,\alpha_x\,\alpha_y\,\alpha_{xx}^2\,\gamma_y^2\,\alpha_1\,-2\gamma_{xy}^2\,\alpha_{xx}\,\gamma_x^2\,\gamma_{xx}\,\alpha_x\,\alpha_{xy}\,\alpha_y^3\,\gamma_1\,+2\gamma_{xy}^2\,\alpha_{xx}\,\gamma_x^2\,\gamma_{xx}\,\alpha_x\,\alpha_{xy}\,\alpha_y^2\,\gamma_y\,\alpha_1$
$-\gamma_x^3\,\gamma_{xx}^2\,\alpha_{xy}^3\,\alpha_y^3\,\gamma_1\,-\gamma_{xy}^3\,\alpha_{xx}^2\,\alpha_x^3\,\gamma_y^3\,\alpha_1\,-2\gamma_{xy}^2\,\alpha_{xx}\,\gamma_{xx}\,\alpha_x^3\,\gamma_y^2\,\alpha_y\,\gamma_1\,\alpha_{xy}\,-\gamma_{xy}\,\gamma_{xx}^2\,\alpha_{xy}^2\,\alpha_x^3\,\gamma_y^3$
$\alpha_1\,-2\gamma_{xy}\,\gamma_{xx}^2\,\alpha_{xy}^2\,\gamma_x\,\alpha_x^2\,\gamma_y\,\alpha_y^2\,\gamma_1\,-\gamma_x\,\alpha_{xx}^2\,\gamma_{xy}^2\,\alpha_x^2\,\gamma_y^2\,\alpha_{xy}\,\alpha_y\,\gamma_1\,+\gamma_x\,\alpha_{xx}^2\,\gamma_{xy}^2\,\alpha_x^2\,\gamma_y^3\,\alpha_{xy}\,\alpha_1,$
$6\,\gamma_{xx}^2\,\alpha_{xx}\,\gamma_x^2\,\alpha_x^3\,\gamma_y\,\alpha_y^2\,\gamma_1\,-\gamma_{xx}^3\,\alpha_x^3\,\gamma_x^2\,\alpha_y^2\,\gamma_y\,\alpha_1\,-\gamma_{xx}^3\,\alpha_x^5\,\gamma_y^3\,\alpha_1\,-6\gamma_{xx}^2\,\alpha_{xx}\,\gamma_x^2\,\alpha_x^3\,\gamma_y^2\,\alpha_y\,\alpha_1$
$+6\gamma_{xx}\,\alpha_{xx}^2\,\gamma_x^3\,\gamma_y^2\,\alpha_x^2\,\alpha_y\,\alpha_1\,-\alpha_{xx}^3\,\gamma_x^5\,\alpha_y^3\,\gamma_1\,+\gamma_{xx}^3\,\alpha_x^5\,\gamma_y^2\,\alpha_y\,\gamma_1\,+3\gamma_{xx}^2\,\alpha_{xx}\,\gamma_x^3\,\alpha_x^2\,\alpha_y^2\,\gamma_y\,\alpha_1\,+\gamma_{xx}^3$
$\alpha_x^3\,\gamma_x^2\,\alpha_y^3\,\gamma_1\,+\alpha_{xx}^3\,\gamma_x^5\,\alpha_y^2\,\gamma_y\,\alpha_1\,-\alpha_{xx}^3\,\gamma_x^3\,\alpha_x^2\,\gamma_y^2\,\alpha_y\,\gamma_1\,+3\gamma_{xx}^2\,\alpha_{xx}\,\gamma_x\,\alpha_x^4\,\gamma_y^3\,\alpha_1\,-6\gamma_{xx}\,\alpha_{xx}^2\,\gamma_x^3\,\gamma_y$
$\alpha_x^2\,\alpha_y^2\,\gamma_1\,+2\gamma_{xx}^3\,\alpha_x^4\,\gamma_x\,\gamma_y^2\,\alpha_y\,\alpha_1\,-2\gamma_{xx}^3\,\alpha_x^4\,\gamma_x\,\gamma_y\,\alpha_y^2\,\gamma_1\,+\alpha_{xx}^3\,\gamma_x^3\,\alpha_x^2\,\gamma_y^3\,\alpha_1\,-3\gamma_{xx}^2\,\alpha_{xx}\,\gamma_x^3\,\alpha_x^2\,\alpha_y^3$
$\gamma_1\,+3\gamma_{xx}\,\alpha_{xx}^2\,\gamma_x^4\,\alpha_x\,\alpha_y^3\,\gamma_1\,-3\gamma_{xx}\,\alpha_{xx}^2\,\gamma_x^4\,\alpha_x\,\alpha_y^2\,\gamma_y\,\alpha_1\,-3\gamma_{xx}^2\,\alpha_{xx},\gamma_x\,\alpha_x^4\,\gamma_y^2\,\alpha_y\,\gamma_1\,-3\gamma_{xx}\,\alpha_{xx}^2$
$\gamma_x^2\,\alpha_x^3\,\gamma_y^3\,\alpha_1\,-2\alpha_{xx}^3\,\gamma_x^4\,\alpha_x\,\gamma_y^2\,\alpha_y\,\alpha_1\,+2\alpha_{xx}^3\,\gamma_x^4\,\alpha_x\,\gamma_y\,\alpha_y^2\,\gamma_1\,+3\gamma_{xx}\,\alpha_{xx}^2\,\gamma_x^2\,\alpha_x^3\,\gamma_y^2\,\alpha_y\,\gamma_1,$
$3\alpha_{xx}^3\,\gamma_x^4\,\alpha_x^2\,\alpha_1\,\gamma_1^2\,+3\gamma_{xx}^3\,\alpha_x^4\,\gamma_x^2\,\gamma_1\,\alpha_1^2\,+\gamma_{xx}^3\,\alpha_x^6\,\gamma_1^3\,+\alpha_{xx}^3\,\gamma_x^6\,\alpha_1^3\,-3\gamma_{xx}^3\,\alpha_x^5\,\gamma_x\,\gamma_1^2\,\alpha_1\,+9\gamma_{xx}\,\alpha_{xx}^2$

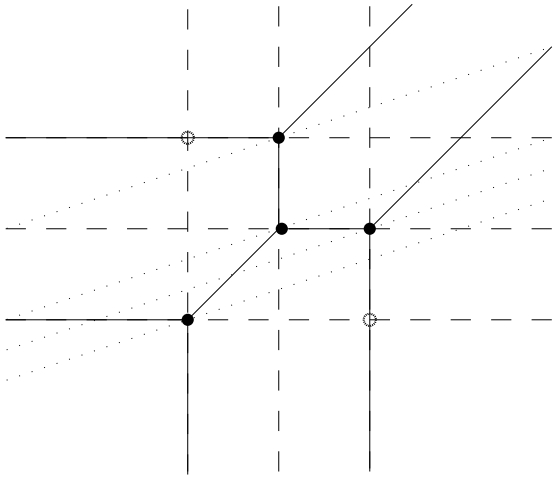


Figure 3.1: Three resultants are needed to compute the stable intersection.

$\gamma_x^4\ \alpha_x^2\ \alpha_1^2\ \gamma_1 + 3\gamma_{xx}\ \alpha_{xx}^2\ \gamma_x^2\ \alpha_x^4\ \gamma_1^3 + 3\gamma_{xx}^2\ \alpha_{xx}\ \gamma_x^4\ \alpha_x^2\ \alpha_1^3 - 3\alpha_{xx}^3\ \gamma_x^5\ \alpha_x\ \alpha_1^2\ \gamma_1 - 9\gamma_{xx}^2\ \alpha_{xx}\ \gamma_x^3\ \alpha_x^3\ \gamma_1$
$\alpha_1^2 - 3\gamma_{xx}^2\ \alpha_{xx}\ \gamma_x\ \alpha_x^5\ \gamma_1^3 - 3\gamma_{xx}\ \alpha_{xx}^2\ \gamma_x^5\ \alpha_x\ \alpha_1^3 + 9\gamma_{xx}^2\ \alpha_{xx}\ \gamma_x^2\ \alpha_x^4\ \gamma_1^2\ \alpha_1 - \alpha_{xx}^3\ \gamma_x^3\ \alpha_x^3\ \gamma_1^3 - \gamma_{xx}^3\ \alpha_x^3$
$\gamma_x^3\ \alpha_1^3 - 9\gamma_{xx}\ \alpha_{xx}^2\ \gamma_x^3\ \alpha_x^3\ \gamma_1^2\ \alpha_1$

3.4 Genericity of Intersection Points

Analogously to Section 2.5, it is studied in this Section the problem of determining the independence of the intersection points of two curves. Even stronger, the residual independence of the intersection points of two curves. Of course, it is not true in general that the intersection points of two curves are points in general position. A classical example is the intersection set P of two generic cubics in the plane. In this case, P has 9 points and all of them lie on two different cubics. As there is only one cubic passing through 9 points in general position, it follows that P cannot be a set of points in general position. Actually eight of the points determine the ninth ([EGH96]) However, taking strict subsets of P, it is expected that these sets of points are in general position. This is the aspect we want to explore. The election of appropriate subsets of the intersection points is done by geometric properties of the corresponding tropical intersection points.

Theorem 3.12. *Let C_1, C_2 be two curves of support I_1, I_2 and Newton polytopes Δ_1, Δ_2 respectively. Let $q = \{q_1, \ldots, q_n\}$ be a set of points contained in the stable intersection of C_1 and C_2 such that it is in general position (Definition 2.12) with respect to both curves. Let $\widetilde{C}_1$, (respectively $\widetilde{C}_2$) be a lift of C_1 (resp. C_2), expressed by a polynomial $\widetilde{f}$, (resp. $\widetilde{g}$) of support I_1, (resp. I_2) and dehomogenized with respect to an index i_0, (resp. j_0) that is a vertex of the Newton Polygon Δ_1, (resp. Δ_2). Suppose that the residual coefficients of the polynomials range over a dense Zariski open subset*

of $k^{\delta_1+\delta_2-2}$ and let $\widetilde{q}_i$ be lifts of the points q_i to the intersection of the algebraic curves. Then, the tuple of possible values of $(Pc(\widetilde{q}_1),\dots,Pc(\widetilde{q}_n))$ contains an open dense subset of k^{2n-2}. That is, if the residual coefficients of $\widetilde{f}$ and $\widetilde{g}$ are generic, so they are the tuple of coefficients of $\widetilde{q}_i$.

Proof. Let

$$f_1 = \text{“}\sum_{(i_1,i_2)\in I_1} a_i x^{i_1} y^{i_2}\text{”} \qquad f_2 = \text{“}\sum_{(j_1,j_2)\in I_2} b_j x^{j_1} y^{j_2}\text{”}$$

be two tropical polynomials defining C_1 and C_2 and let

$$\widetilde{f}_1 = \sum_{(i_1,i_2)\in I_1} \widetilde{a}_i x^{i_1} y^{i_2} \qquad \widetilde{f}_2 = \sum_{(j_1,j_2)\in I_2} \widetilde{b}_j x^{j_1} y^{j_2}$$

be the lifts of the curves. Without loss of generality, it is supposed that both polynomials are dehomogenized with respect to two monomials that are vertices of Δ_1 and Δ_2 respectively. Let $\alpha_i = Pc(\widetilde{a}_i)$, $\beta_j = Pc(\widetilde{b}_j)$, $(\gamma_{1l},\gamma_{2l}) = Pc(\widetilde{q}_l)$, $\alpha = \{\alpha_i\}$, $\beta = \{\beta_j\}$, $\gamma = \{\gamma_{kl}\}$. As the points are in general position, it must be the case $n \leq \min\{\delta_1,\delta_2\}-1$ The proof mimics the reasoning of Theorem 2.11. So, a parametrization of the residual coefficients of the curves and the points $\widetilde{q}_i$ is needed. The local equations $(\widetilde{f}_1)_{q_i}$, $(\widetilde{f}_2)_{q_i}$ form a linear system of equations in the residual coefficients of the points where the unknowns are the residual coefficients of the curves. This is a linear system of $2n$ equations in at most $\delta_1+\delta_2-2$ unknowns of full rank. It follows that we may take $\alpha_0 = \{\alpha_{i_1},\dots,\alpha_{i_{\delta_1-n-1}}\}$ residual coefficients of $\widetilde{f}_1$ as parameters such that the remaining system is determined. Analogously, we may take $\beta_0 = \{\beta_{i_1},\dots,\beta_{i_{\delta_2-n-1}}\}$ residual coefficients such that the remaining system of equations in determined. It follows that the remaining variables α_i, β_j are rational functions of α_0, β_0 and γ. These rational functions define the parametrization

$$\begin{array}{ccc} k^{\delta_1+\delta_2-2} & \to & k^{\delta_1+\delta_2+2n-2} \\ (\alpha_0,\beta_0,\gamma) & \mapsto & (\alpha,\beta,\gamma) \end{array}$$

of a variety $\mathcal{V}$ that can be identified with the vectors of principal coefficients (C_1,C_2,q). Let $\mathbb{L}$ be the field of fractions of $\mathcal{V}$. It is clear that every class γ_{ki} is algebraic over $k(\alpha,\beta)\subseteq\mathbb{L}$ and that $\mathbb{L} = k(\alpha_0,\beta_0,\gamma)$ by the parametrization. Thus, $\{\alpha_0,\beta_0,\gamma\}$ and $\{\alpha,\beta\}$ are transcendence bases of the field of rational functions of $\mathcal{V}$. It follows that $k[\alpha,\beta,\gamma]\cap k[\gamma] = 0$, that is, the set of possible tuples of residual coefficients of the points $\widetilde{q}_i$ contains a dense Zariski open set. □

Example 3.13. Consider the case of two conics $C_1 = \text{“}(-11)+2x+2y+2xy+0x^2+0y^2\text{”}$, $C_2 = \text{“}0+8x+14y+20xy+12x^2+14y^2\text{”}$, their stable intersection is the set of points $\{(2,-6),(-4,2),(-13,-14),(-6,-6)\}$. These four points are in general position with respect to C_1 and C_2 so, for any generic lifts of C_1, C_2, the residual coefficients of their intersection points are generic. However, consider now the case of two conics $C_1 = \text{“}0+(-10)x+(-10)y+(-10)xy+0x^2+0y^2\text{”}$ and $C_2 = \text{“}0+(-10)x+(-10)y+(-10)xy+1x^2+2y^2\text{”}$. They have only one intersection point of multiplicity 4, taking

the point three or four times yields to a set which is not in general position in none of the curves. Hence, the maximal number of intersection points that are in general position in both curves is 2. So, the drawback of this theorem is that the number n of points in general position in both curves is not uniform with respect to the supports. The following is a uniform result that holds for every pair of curves with prescribed support.

Theorem 3.14. *Suppose given two tropical curves C_1, C_2 with support I_1 and I_2 respectively. Let $\widetilde{C}_1$, $\widetilde{C}_2$ be two lifts of the curves whose principal coefficients are generic and let q be one stable intersection point. Then, the principal coefficients of $\widetilde{q}$ are generic. That is, if we impose polynomial conditions $F \neq 0$ to the coefficients of $\widetilde{C}_i$ then the possible coefficients of the point $\widetilde{q}$ contains a dense constructible set of k^2.*

Proof. One point q is always in genera position with respect to any curve, so we are in the hypothesis of Theorem 3.12 □

3.5 Some Remarks

As a consequence of Theorem 3.10, a new proof of Bernstein-Koushnirenko Theorem for plane curves over an arbitrary algebraically closed field can be derived from the classic Theorem over $\mathbb{C}$ ([Ber75], [Kus76]).

Corollary 3.15. *Let $\widetilde{f}$, $\widetilde{g}$ be two polynomials over $\mathbb{K}$, an algebraically closed. Let Δ_f, Δ_g be the Newton Polygon of the polynomials $\widetilde{f}$ and $\widetilde{g}$ respectively. Then, if the coefficients of $\widetilde{f}$ and $\widetilde{g}$ are generic, then the number of common roots of the curves in $(\mathbb{K}^*)^2$ counted with multiplicities is the mixed volume of the Newton Polygons*

$$\mathcal{M}(\Delta_f, \Delta_g) = vol(\Delta_f + \Delta_g) - vol(\Delta_f) - vol(\Delta_g)$$

Proof. If the coefficients of the polynomials are generic, the number of roots in the torus counted with multiplicities is the degree minus the order of the resultant of the two polynomials with respect to one of the variables. This number does only depend on the support of the polynomials, and it is equal to the mixed volume of the Newton Polygons, because this is the number of stable intersection points of two tropical curves of Newton polygons Δ_f, Δ_g. □

Remark 3.16. Another application of the techniques developed in this report is the computation of tropical bases. Theorem 1.16 proves that for a hypersurface $\widetilde{f}$, the projection $T(\{\widetilde{f} = 0\}) = \mathcal{T}(f)$. This is not true for general ideals. If $\mathcal{I} = (\widetilde{f}_1, \ldots, \widetilde{f}_m) \subseteq \mathbb{K}[x_1, \ldots, x_n]$ and $\mathcal{V}$ is the variety it defines in $(\mathbb{K}^*)^n$,

$$T(\mathcal{V}) \subseteq \bigcap_{i=1}^{m} \mathcal{T}(f_i),$$

but it is possible that both sets are different. A *tropical basis* is a set of generators $\widetilde{g}_1, \ldots, \widetilde{g}_r$ of $\mathcal{I}$ such that $T(\mathcal{V}) = \bigcap_{i=1}^{r} \mathcal{T}(g_r)$. In [BJS+07], it is proved that every ideal has a tropical basis and it is provided an algorithm for the case of a prime ideal $\mathcal{I}$.

An alternative for the computation of a tropical basis of a zero dimensional ideal in two variables is the following. Let $\mathcal{I} = (\widetilde{f}, \widetilde{g})$ be a zero dimensional ideal in two variables. Let $\widetilde{R}_x$, $\widetilde{R}_y$ be the resultants with respect to x and y of the curves. Let P be the intersection of the projections R_x and R_y. This is always a finite set that contains the projection of the intersection of $\widetilde{f}$, $\widetilde{g}$. It may happen that P if not contained in the stable intersection of the corresponding tropical curves f and g, though. Let a be a natural number such that $x - ay$ is injective in P. Let $\widetilde{R}_z = \mathrm{Res}_y(\widetilde{f}(zy^a, y), \widetilde{g}(zy^a, y))$ be another resultant. Then, it follows that $(\widetilde{f}, \widetilde{g}, \widetilde{R}_x, \widetilde{R}_y, \widetilde{R}_z)$ is a tropical basis of the ideal $(\widetilde{f}, \widetilde{g})$.

Remark 3.17. Along the Chapter, the notion of tropical resultant has been defined as the projection of the algebraic resultant. It is needed a precomputation of the algebraic resultant in order to tropicalize it. For the case of plane curves, it would be preferable to have a determinantal formula. That is, to prove that the determinant of the Sylvester matrix of two polynomials define the resultant variety. But the proof of the properties is achieved by a careful look to the polynomials involved, paying special attention to the cancellation of terms. In the case of the determinant of the Sylvester matrix, the tropical determinant of the Sylvester matrix is the projection of the permanent of the algebraic determinant. There are cancellation of terms even in the equicharacteristic zero case. It is conjectured that still the determinant of the Sylvester matrix is a tropical polynomial that defines the same tropical variety as the resultant does. The author has checked that it is the case for polynomials up to degree four with full support.

Chapter 4

Geometric Constructions

In this Chapter the notion of geometric construction is introduced. A geometric construction can be regarded as an abstract procedure that produces realizations (either tropical or algebraic) of an incidence configuration. If q is a point in a configuration G restricted to belong to two different curves C_1, C_2, it is natural to define q as an intersection point of C_1 and C_2. The main advantage of this approach is that it allows an easy comparison between algebraic and tropical realizations of an incidence structure G using the results in the previous Chapters.

4.1 The Notion of Geometric Construction

A geometric construction will be defined as an abstract procedure that provides an incidence structure G together with an orientation of G. Hence, we recall some notation for oriented (directed) graphs.

A directed graph is a graph such that each edge $\{x_1, x_2\}$ has a defined orientation $(x_1, x_2) = x_1 \to x_2$. Double orientations in the edges $x_1 \to x_2$ and $x_2 \to x_1$ are not allowed. For an oriented edge $x_1 \to x_2$, we say that x_1 is a *direct predecessor* of x_2 and that x_2 is a *direct successor* of x_1. An *oriented path* is a chain of oriented edges $x_1 \to x_2 \to \ldots \to x_n$. If there is an oriented path from x_1 to x_n, we say that x_1 is a *predecessor* of x_n and that x_n is a *successor* of x_1. An *oriented cycle* is an oriented path such that its starting node equals its ending node, $x_1 = x_n$. A directed graph without oriented cycles is called a *directed acyclic graph* (DAG). If G is a DAG, the nodes x of G that are not the successor of any other node are called *sources*. Any node x of a DAG G has associated a *depth*. If x is a source then its depth is 0. If x is not a source, let $y_1, \ldots, y_n$ be the direct predecessors of x. The depth of x is defined as:

$$depth(x) = 1 + max\{depth(y_1), \ldots, depth(y_n)\}$$

The depth of a DAG G is the maximal depth of its nodes.

Definition 4.1. A geometric construction is an abstract procedure consisting in:

- Input elements: two finite subsets $\mathfrak{p}_0$, $\mathfrak{B}_0$ such that $\mathfrak{p}_0 \cap \mathfrak{B}_0 = \emptyset$ and a support map
$$Sup : \mathfrak{B}_0 \to^{\mathcal{P}^f(\mathbb{Z}^2)} \diagup \sim$$
The set of incidence relations is the empty set $\mathfrak{I} = \emptyset$.

- Steps of the construction, a finite sequence of different steps:
  - Given a support I with $\delta(I) = n \geq 2$ and $n-1$ points $\{q_1, \ldots, q_{n-1}\}$ we add a new curve C of support I to $\mathfrak{B}$, we also add new oriented incidence conditions $q_i \to C$, $1 \leq i \leq n-1$.
  - Given two curves C_1, C_2 of support I_1, I_2 and Newton Polygons Δ_1, Δ_2 respectively, we add $M = \mathcal{M}(\Delta(I_1), \Delta(I_2))$ new points $q_1, \ldots, q_M$. We add the oriented incidence conditions $C_1 \to q_i$, $C_2 \to q_i$, $1 \leq i \leq M$.

- Output: an incidence graph G provided with an orientation.

A *tropical realization of a geometric construction* $\mathfrak{C}$ is a tropical realization of its associated graph G such that:

- If $x \in \mathfrak{B}$ is a curve and it is not an input element, let I be its support and let $\{y_1, \ldots, y_{\delta(I)-1}\}$ be the direct predecessors of x. Then x is exactly the stable curve of support I passing through the set of points $\{y_1, \ldots, y_{\delta(I)-1}\}$.

- If $x \in \mathfrak{p}$ and it is not an input point, let y_1, y_2 be the direct predecessors of x and let $\{x_1, \ldots, x_n\}$ be the common direct successors of y_1 and y_2. Then, $\{x_1, \ldots, x_n\}$ are exactly the stable intersection of y_1 and y_2, counted with multiplicities.

An *algebraic realization of a geometric construction* $\mathfrak{C}$ is an algebraic realization of its associated graph G such that:

- If $x \in \mathfrak{B} \setminus \mathfrak{B}_0$, let I be its support and let $\{y_1, \ldots, y_{\delta(I)-1}\}$ be the direct predecessors of x. Then, x is the unique curve of support I that passes through the points $\{y_1, \ldots, y_{\delta(I)-1}\}$.

- If $x \in \mathfrak{p}$ and it is not an input point, let y_1, y_2 be the direct predecessors of x and let $\{x_1, \ldots, x_n\}$, $n = \mathcal{M}(\Delta_1, \Delta_2)$ be the common direct successor of y_1 and y_2. Then, the curves y_1, y_2 intersect exactly in the finite set of points $\{x_1, \ldots, x_n\}$ where the points are counted with multiplicities.

Given an algebraic (resp. tropical) realization of the input elements of a geometric construction $\mathfrak{C}$, there can only be finitely many realizations of $\mathfrak{C}$ with these input elements, because the realizations of the rest of the elements are fixed by the input elements and the steps of the construction. The only possibility to have different realizations of $\mathfrak{C}$ with the same input elements is a permutation of the labels of the intersection (resp. stable intersection) of two curves y_1, y_2 and the consequent changes in the successor elements of y_1, y_2 in the construction.

It is clear that, in the tropical plane, every step of a construction can be performed. That is, given two curves C_1, C_2, we can always define the set of $\mathcal{M}(\Delta_1, \Delta_2)$ intersection points (counted with multiplicities). Analogously, the computation of the stable curve through a set of points is always well defined. Thus, in the tropical context, given a tropical realization of the input elements of $\mathfrak{C}$, there is always a realization of $\mathfrak{C}$ with these input elements. However, this is not the case in the algebraic case. Two different curves C_1, C_2 may share a common component. Here, we cannot define a finite intersection set with the nice properties the tropical stable intersection has. Even if the intersection set of the curves is finite, there may not be enough intersection points in the torus. For example, the lines $3x+2y+4$, $5x+y+2$ do not have any intersection point in the torus. These degenerate cases should be avoided. So, we need a notion of a well defined construction. A geometric construction is *well defined* if it is well defined for a generic realization of the input elements. That is, let R_0 be the space of algebraic realizations of the input elements $\mathfrak{p}_0 \cup \mathfrak{B}_0$. In this case, as the set of incidence conditions is empty, the realization space equals the support space, $R_0 = S_0$. Let L be the set of configurations such that every step of the construction $\mathfrak{C}$ is well defined (that is, the projection into R_0 of the algebraic realizations of $\mathfrak{C}$). The construction G is *well defined* if L is dense in R_0.

It is clear that the oriented graph G of a geometric construction $\mathfrak{C}$ never has an oriented cycle, so G is always a directed acyclic graph (DAG). The input elements are exactly the sources and every node of G has defined a depth. Usually, proofs are made by induction on the depth of G.

4.2 Relation of the Constructions and the Configurations

In practice, many interesting incidence configurations can be defined as a subgraph of the graph of a geometric construction. Sometimes we will have to add additional elements to fit the incidence configuration into the definition of geometric construction. Hence, we present a characterisation of the incidence graphs G that appear as a subgraph of the graph of a geometric construction.

Proposition 4.2. *Let G be an incidence graph provided with an orientation. Then it is the subgraph of the graph of a geometric construction if and only if*

- *G is a directed acyclic graph, (DAG).*
- *If x is a vertex of type $\mathfrak{p}$, then it has at most two direct predecessor.*
- *If x is a curve of support I, then x has at most $\delta(I) - 1$ direct predecessors.*
- *If x, y are two curves with a common direct successor, then they have at most $\mathcal{M}(\Delta_x, \Delta_y)$ common direct successors.*
- *If x and y are two curves with the same support I and both curves have exactly $\delta(I)$ direct predecessor, then the sets of direct predecessors are different.*

Moreover, G is exactly the graph of a geometric construction if and only if the previous inequalities are equalities for every node different from a source.

Proof. Let G be a graph satisfying all these conditions, a construction $\mathfrak{C}$ can be defined such that it contains G as a subgraph. Every source of G is defined as an input element. Suppose defined the construction of every element of depth up to i, the definition of the depth $i+1$ elements is as follows. Let x be a point of depth $i+1$, if it has two predecessors y, z, then they have at most $\mathcal{M}(\Delta_y, \Delta_z)$ common direct successors. If there are not enough intersection points, we add points of depth $i+1$ up to $\mathcal{M}(\Delta_x, \Delta_y)$ and define all of them (in particular x) as the intersection of y and z. If x is a point of depth $i+1$ that has only one direct predecessor y, we add a line z as an input curve (a curve of support $\{(0,0),(1,0),(0,1)\}$) as a direct predecessor of x and proceed as in the previous case. In the case where x is a curve of support I and depth $i+1$, there are at most $\delta(I)-1$ predecessors of x. Add to the construction $\mathfrak{C}$ as many input points as necessary up to $\delta(I)-1$ and define x as the curve passing through these points. Note that the last condition of the hypothesis disallow the construction to have repeated steps. If two curves x and y of the same support I have both $\delta(I)$ direct predecessors, then the set of direct predecessors is different, so x and y are curves obtained by different steps.

This method defines a construction $\mathfrak{C}$ that contains G as a subgraph. It is clear that G is exactly the graph of $\mathfrak{C}$ if and only if the equalities in the hypothesis hold. □

One might be tempted to add additional allowed steps to a construction besides the two steps defined in 4.1. In particular, a common step in Classical Geometry is to choose a point in a curve. Proposition 4.2 proves that this step does not increase the expressivity of the constructions. If $\mathfrak{C}$ is a geometric construction such that the additional steps of taking a curve through a point or taking a point inside a curve are allowed, then the graph of $\mathfrak{C}$ is the subgraph of another construction $\mathfrak{C}_1$ without these additional steps. So, in practice, we may work with this additional step with the agreement that *"choosing a point in a curve is essentially equivalent to add an input line (curve of support $\{(0,0),(1,0),(0,1)\}$) to our construction, intersect the line with the curve and choose an intersection point."* See for example Theorem 5.6 for an example of this technique of adding additional elements to a familiar incidence configuration in order to obtain a geometric construction.

The advantage of the construction method over a direct approach to the study of incidence configurations is that the problem is reduced to lifting the steps of the construction. This problem that has been solved in Chapters 2 and 3

4.3 Lift of a Construction

Let $\mathfrak{C}$ be a geometric construction of graph G. This Section deals with the problem of lifting a tropical instance of G obtained by the construction to an algebraic instance. Let H_0 be the set of input elements of $\mathfrak{C}$ and h a tropical realization of H_0. The steps of the construction define a tropical realization p of G. On the other hand, let

$\widetilde{h} = T^{-1}(h)$ be any algebraic realization of H_0 that projects onto h (recall that this lift is not unique). Then, there are two potential problems. First, it is possible that $\mathfrak{C}$ is not well defined in $\widetilde{h}$. Second, if the construction is well defined and $\widetilde{p}$ is the algebraic realization of G obtained from $\widetilde{h}$, it is possible that $T(\widetilde{p}) \neq p$. In this Section we study conditions for the lift $T^{-1}(h)$ such that the following Diagram commutes:

$$\begin{array}{ccc} (\mathbb{K}^*)^2 & & \mathbb{T}^2 \\ \text{Input } \widetilde{h} & \stackrel{T^{-1}}{\longleftarrow} & \text{Input } h \\ \mathfrak{C} \downarrow & & \downarrow \mathfrak{C} \\ \text{Output } \widetilde{p} & \stackrel{T}{\longrightarrow} & \text{Output } p \end{array} \tag{4.1}$$

A first step is, given an instance of a geometric construction, define sufficient residual conditions on the lifts $\widetilde{h}$ of the input h for the compatibility $T(\widetilde{p}) = p$. In order to do this, let $\{C_1, \ldots, C_n, q_1, \ldots, q_m\}$ be the input elements of a geometric construction $\mathfrak{C}$, curve C_i of support I_i, point $q_j \in (\mathbb{T}^*)^2$. Take $N = 2m + \sum_{i=1}^{n}(\delta(I_i) - 1)$ and let $\{\widetilde{f}_1, \ldots, \widetilde{f}_n, \widetilde{q}_1, \ldots, \widetilde{q}_m\}$ be a set of lifts of a concrete tropical instance of the input, $f_i = \sum_{(k,l)\in I_i} \widetilde{a}^i_{(k,l)} x^k y^l$, $\widetilde{q}_j = (\widetilde{q}^1_j, \widetilde{q}^2_j)$. We are going to compute a constructible set $\mathfrak{S} \subseteq (k^*)^N$, not always empty, that encodes the residual conditions for the compatibility of the algebraic and tropical construction. We are going to define two auxiliary sets T and V first. The set T is defined adding the residual restrictions obtained by Theorems 2.10 and 3.10 that ensure that each step of the construction is compatible with tropicalization. Let

$$f_i = \text{“} \sum_{(k,l)\in I_i} a^i_{(k,l)} x^k y^l \text{”}, 1 \leq i \leq n,$$

$$q_j = (q^1_j, q^2_j), 1 \leq j \leq m$$

be the tropical input elements. Take a generic lift of the input

$$\widetilde{f}'_i = \sum_{(k,l)\in I_i} \widetilde{a}^i_{(k,l)} x^k y^l, 1 \leq i \leq n,$$

$$\widetilde{q}'_j = (\widetilde{q}^1_j, \widetilde{q}^2_j), 1 \leq j \leq m$$

and $V_0 = \{\alpha^i_{(k,l)}, \gamma^r_j\}$ is a set of indeterminates where $Pc(\widetilde{a}^i_{(k,l)}) = \alpha^i_{(k,l)}$, $Pc(\widetilde{q}^i_j) = \gamma^i_j$. These indeterminates will describe $\mathfrak{S}$. Perform the construction with this data as follows.

Start defining the constructible set $T = (k^*)^N = \{x \in k^N | \alpha^i_{(k,l)} \neq 0, \gamma^r_j \neq 0, 1 \leq i \leq n, 1 \leq j \leq m\}$ and $V = V_0$. We are going to redefine T and V inductively at each step of the construction. Suppose that we have defined V and the constructible set $T \subseteq (k^*)^V$ for the construction up to a construction step. We redefine T after the step as follows: For the case of the computation of the curve C of support I passing through $\delta(I) - 1$ points, we have to solve a system of linear equations. The coefficients of $\widetilde{C}$ are rational functions of the variables V. Theorem 2.10 provides sufficient conditions in

the variables V for the system being compatible with tropicalization. This conditions are $\Delta_{A^i}(Pc(\widetilde{A}^i))$ where A is the tropical matrix of the system of linear equations. We add to V $\delta(I)-1$ new variables $s_1,\dots,s_{\delta-1}$ and we consider $T \subseteq (k^*)^{K+\delta-1}$. We add the conditions $\Delta_{A^i}(Pc(\widetilde{A}^i)) \neq 0$ to the definition of T and the equations $\Delta_{A^i}(Pc(\widetilde{A}^i)) - s_i\Delta_{A^{i_0}}(Pc(\widetilde{A}^{i_0})) = 0$, where i_0 is a dehomogenization variable of C. We follow the construction with C among our available objects.

Suppose now that our construction step consists in the intersection of two curves $\widetilde{f}$, $\widetilde{g}$ of support I_f, I_g respectively. This stable intersection can be determined using the technique of resultants presented in Chapter 3. That is, let $\widetilde{R}_x(x) = \mathrm{Res}_y(\widetilde{f},\widetilde{g})$, $\widetilde{R}_y(y) = \mathrm{Res}_x(\widetilde{f},\widetilde{g})$ be the algebraic resultants of the two algebraic curves. Let $R_x(x)$, $R_y(y)$ be the tropical resultants of the curves. Let a be a natural number such that $x-ay$ is injective in the finite set $f\cap g\cap R(x)\cap R(y)$, as in the conditions of Theorem 3.10. Let $\widetilde{R}_z(z) = \mathrm{Res}_y(\widetilde{f}(zy^a,y),\widetilde{g}(zy^a,y))$. If t_r are the variables of V corresponding with the principal coefficients of $\widetilde{f}$, $\widetilde{g}$, Theorem 3.10 provides sufficient conditions of the form $\widetilde{u}(t_r)\neq 0$ that ensures that the algebraic and tropical resultants are compatible. We add these polynomials $\widetilde{u}(t_r)\neq 0$ to the definition of T. In the tropical context, there are $M = \mathcal{M}(\Delta_f,\Delta_g)$ stable intersection points $b_j = (b_j^1, b_j^2)$. We add $2M$ new variables s_j^1, s_j^2, $1\leq j\leq M$ to V. Consider T contained in $(k^*)^{K+2M}$. For each tropical point b_j, let $s_{j_1},\dots,s_{j_n}$ be the algebraic points projecting into b_j. We take the following equations:

$$(\widetilde{R}_x)_{b_j^1} = \prod_{r=1}^{n}(x-s_{j_r}^1), \qquad (\widetilde{R}_y)_{b_j^2} = \prod_{r=1}^{n}(y-s_{j_r}^2),$$

$$(\widetilde{R}_z)_{\text{“}b_j^1(b_j^2)^{-a}\text{”}} = \prod_{r=1}^{n}(z-s_{j_r}^1(s_{j_r}^2)^{-a}).$$

In this way, the coefficients of $(\widetilde{R}_x)_{b_j^1}$, $(\widetilde{R}_y)_{b_j^2}$ and $(\widetilde{R}_z)_{\text{“}b_j^1(b_j^2)^{-a}\text{”}}$ are identified with symmetric functions in $s_{j_r}^1$, $s_{j_r}^2$ and $s_{j_r}^1(s_{j_r}^2)^{-a}$ respectively. We add these identifications to the definition of T. In this way, we ensure that there is a bijection between the roots of the resultants and the variables s_j. We also add the residual conditions of the curves over the intersection points $\widetilde{f}_{b_j}(s_j^1,s_j^2)=0$, $\widetilde{g}_{b_j}(s_j^1,s_j^2)=0$, and the conditions of the points being in the torus $s_j^1 s_j^2\neq 0$. We continue the construction with the points $(s_i^1 t^{-b_i^1}, s_i^2 t^{-b_i^2})$. Notice that we are only defining the principal terms of the elements, because this is all the information needed for the Theorem. After the whole construction, we have defined a constructible set T that characterizes the possible principal term of every element in the construction. Finally, $\mathfrak{S}$ is defined as the projection of the set defined by T into the space of variables V_0.

Definition 4.3. The set $\mathfrak{S}$ previously defined is called *the set of valid principal coefficients of the input elements*.

Theorem 4.4. *Let $\{C_1,\dots,C_n,q_1,\dots,q_m\}$ be the input elements of a geometric construction $\mathfrak{C}$, curve C_i of support I_i, point $q_j\in(\mathbb{T}^*)^2$. Take $N = 2m+\sum_{i=1}^{n}(\delta(I_i)-1)$ and let $\{\widetilde{f}_1,\dots,\widetilde{f}_n,\widetilde{q}_1,\dots,\widetilde{q}_m\}$ be a set of lifts of a concrete tropical instance of the*

input, $f_i = \sum_{(k,l)\in I_i} \widetilde{a}^i_{(k,l)} x^k y^l$, $\widetilde{q}_j = (\widetilde{q}^1_j, \widetilde{q}^2_j)$, $Pt(\widetilde{a}^i_{(k,l)}) = \alpha^i_{(k,l)} t^{-a^i_{k,l}}$, $Pt(\widetilde{q}^i_j) = \gamma^i_j t^{-q^i_j}$. *Let* $\mathfrak{S} \subseteq (k^*)^N$ *be the set of valid principal coefficients of the input. Then, if the vector*

$$\left(\alpha^1_{(k,l)}, \ldots, \alpha^n_{(k,l)}, \gamma^1_1, \ldots, \gamma^2_m\right) \in (k^*)^N$$

of principal coefficients lies in $\mathfrak{S}$*, the algebraic construction is well defined and the result projects onto the tropical construction.*

Proof. Suppose that the vector $(\alpha^1_{(k,l)}, \ldots, \alpha^n_{(k,l)}, \gamma^1_1, \ldots, \gamma^2_m)$ belongs to $\mathfrak{S}$. We are going to construct suitable algebraic data. Perform the steps of the construction. For the curve passing through a number of points, the set $\mathfrak{S}$ imposes that there is only one solution of the linear system we have to solve and that this solution projects correctly. For the case of the intersection of two curves, the resultants R_x, R_y, R_z are compatible with projection. So, the curves intersects in finitely many points in the torus and these points projects correctly onto the tropical points. So this step is also compatible with the tropicalization. □

In this theorem, it is not claimed that there is always a possible lift, as Theorem 1.30 does. It is possible that the set $\mathfrak{S}$ is empty. In this case, the theorem do not yield to any conclusion. In Section 4.7 we will discuss what can be said if $\mathfrak{S}$ is empty.

4.4 Admissible Constructions

This Section deals with the search of sufficient conditions for a construction $\mathfrak{C}$ that assert that the set $\mathfrak{S}$ is non empty for every realization h of the input. For example, let $\mathfrak{C}$ be a depth 1 construction. There are only two kind of elements, input elements and depth 1 elements. If the realization $\widetilde{h}$ of the input elements is generic, by Theorems 2.10 and 3.10, every depth 1 element is well defined and projects correctly. Thus, every depth 1 construction can be lifted to the algebraic plane. Furthermore, if the vector of coefficients of the depth 1 elements is generic, we would be able to construct some other depth 2 elements from them. By Theorems 2.11 and 3.14, we already know that every single depth 1 element is generic. However, it may happen that there are algebraic relations among the set of depth 1 elements that do not allow to apply induction in further steps. So, in order to use an induction scheme over the construction, we need to ensure that in future steps of the construction we will only use elements that are generic. Next Definition describes constructions such that this genericity of the elements always holds, whatever the input elements are.

Definition 4.5. Let $\mathfrak{C}$ be a geometric construction. Let G be the incidence graph with the orientation induced by the construction. The construction $\mathfrak{C}$ is *admissible* if, for every two nodes A, B of G, there is at most one oriented path from A to B. In the case where the construction is not admissible, let A, B two elements such that there is at least two paths from A to B. This is denoted by $A \rightrightarrows B$.

The main Theorem of the Chapter proves that if $\mathfrak{C}$ is an admissible geometric construction, then every tropical realization of $\mathfrak{C}$ can be lifted to a compatible algebraic realization.

Theorem 4.6. *Let $\mathfrak{C}$ be an admissible geometric construction. Then, for every tropical instance of the construction, the set $\mathfrak{S}$ defined in Theorem 4.4 is nonempty and dense in $(k^*)^N$. Moreover, for every element X of the construction, its possible values, as the input elements range over $\mathfrak{S}$, contains a dense open subset of its support space. In particular, every tropical instance of the construction $\mathfrak{C}$ can be lifted to the algebraic plane $(\mathbb{K}^*)^2$.*

Proof. We prove the Theorem by induction in the depth of the construction. If the construction is of depth 0, then there is nothing to prove, because the set of steps is empty and $\mathfrak{S} = (k^*)^N$ which is dense and the values of each element are dense in their respective space of configurations. Suppose the Theorem proved for admissible constructions of depth smaller or equal to i. Let $\mathfrak{C}$ be any admissible construction of depth $i+1$. For each element X of depth $i+1$, let $Y_1, \ldots, Y_n$ be the direct predecessors of X. By induction hypothesis, the set of possible values of Y_i contains a dense open set in its space of configurations. As the construction is admissible, the set of predecessors of Y_i is disjoint from the set of predecessors of Y_j, if $i \neq j$. Because if both elements had a common predecessor A, there would be a double path $A \rightrightarrows X$, contrary to the hypothesis. Hence, the coefficients $Y_1, \ldots, Y_n$ are completely independent and the possible tuples $(Y_1, \ldots, Y_n)$ are just the concatenation of possible values of coefficients of each element Y_i. By the results in the Theorems 2.11 and 3.14, as the elements Y_j are generic, so is X. That is, the possible values of X contains a dense open set of its support space. The conditions imposed by the definition of X to the auxiliary set T in Theorem 4.4 are a set of inequalities in the tuples $(Y_1, \ldots, Y_n)$ that are verified on an open set. Likewise, the restrictions in the elements Y_j impose other restrictions to the its predecessors. Again, this restrictions are verified in an open set, we are explaining this with more detail:

If Y_j is constructed from elements Z_{ji}, there is a set of restrictions $f_s(Z_{ji}) \neq 0, s \in S$ that ensure that Y_j is well defined and it is compatible with tropicalization. Let $g_l(Y_1, \ldots, Y_n) \neq 0$, $l \in L$ be the polynomials imposed by X to be well defined and compatible with tropicalization. In addition to this, if $Y_j = (Y_j^1, \ldots, Y_j^{n_j})$, each variable Y_j^r is algebraic over the field $p(k)(Z_{ji})$, where $p(k)$ is the prime field of k. If we multiply each polynomial $g_l(Y_1, \ldots, Y_n)$ by its conjugates in the normal closure of $p(k)(Z_{ji}) \subseteq p(k)(Z_{ji}, Y_i)$, we obtain some polynomials $G_l(Z_{j1}, \ldots, Z_{jn})$. If neither $G_l(Z_{ij})$ nor $f_s(Z_{ij})$ are zero, then the elements Y_i and X are well defined and are compatible with projection. These polynomials define possible valid principal coefficients for the subconstruction $Z_{ji} \to Y_i \to X$. Applying this method recursively, we obtain a set of conditions in the input elements. Let $\mathfrak{S}_i$ the set of good input elements for every subconstruction of $\mathfrak{C}$ consisting on the elements of depth up to i. By induction hypothesis, $\mathfrak{S}_i$ is non empty and contains an open Zariski set. Intersecting this set with the open sets induced by each element X of depth $i+1$ to be compatible with tropicalization, we obtain that the required set $\mathfrak{S}_{i+1}$ contains a dense open Zariski set. □

Now, we show an example of a non admissible construction $\mathfrak{C}$ with a tropical realization that cannot be lifted to the algebraic plane.

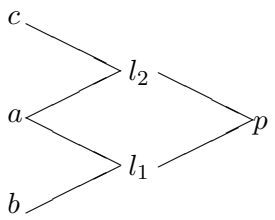


Figure 4.1: The construction graph of p

Example 4.7. Recall the following example from Chapter 1: Suppose we are given a, b, c three points in the plane. Let $l_1 = \overline{ab}$, $l_2 = \overline{ac}$ be the lines through these points and $p = l_1 \cap l_2$. The construction of l_1 and l_2 is admissible, but not the construction of p, because of the double path $a \rightrightarrows p$.

So, after specialization, there may be some algebraic relations making $\mathfrak{S}$ empty. For example, take $a = (0, 0)$, $b = (-2, 1)$, $c = (-1, 3)$. Tropically, the construction yields $l_1 =$ "$1x + 0y + 1$", $l_2 =$ "$3x + 0y + 3$" and, finally, $p = (0, 1) \neq a$. But, for every lift of the points a, b, c to the algebraic plane $\mathbb{K}$ such that the construction is well defined, we will obtain that $\widetilde{p} = \widetilde{a}$, so no lift is ever compatible with tropicalization. If we follow the proof of Theorem 4.4, the lifts of the input elements must be of the form:

$$\widetilde{a} = (\alpha_1, \alpha_2),\ \widetilde{b} = (\beta_1 t^2, \beta_2 t^{-1}),\ \widetilde{c} = (\gamma_1 t, \gamma_2 t^{-3}),$$

where terms of bigger order do not affect the result. In this case,

$$\widetilde{l_1} = \frac{-\beta_2 t^{-1} + \alpha_2}{\alpha_1\beta_2 t^{-1} - \alpha_2\beta_1 t^2} x + \frac{-\alpha_1 + \beta_1 t^2}{\alpha_1\beta_2 t^{-1} - \alpha_2\beta_1 t^2} y + 1,$$

$$\widetilde{l_2} = \frac{-\gamma_2 t^{-3} + \alpha_2}{\alpha_1\gamma_2 t^{-3} + \alpha_2\gamma_1 t} x + \frac{-\alpha_1 + \gamma_1 t}{\alpha_1\gamma_2 t^{-3} + \alpha_2\gamma_1 t} y + 1.$$

Which tropicalize correctly to l_1 and l_2 (as expected, because the construction graphs of l_1 and l_2 are trees, hence admissible). Now, we want to construct $\widetilde{p}$. If we try to obtain the y-th coordinate of the root, we obtain that it has an order greater than -1. Actually, as $\widetilde{p}$ must be $\widetilde{a}$, the y-th coordinate must be of order 0.

We observe that the same lifting problem appears under small perturbations of a, b and c. So this example is not an isolated case and it cannot be avoided by perturbations of the input points as in the case of stable intersection. These bad conditioned cases arrive frequently when we are working with non trivial constructions. So, it is reasonable to work with more specific constructions, like admissible ones.

4.5 Limits of the Construction Method

Tropical geometric constructions are a useful tool when dealing with non-trivial incidence relations between varieties. It agrees naturally with the stable intersection of the curves taken in consideration. Moreover, it permits to arrange the computations focusing on the smaller set of input objects. This Section deals with the problem of quantifying how well do a realization of a construction behaves well with respect to tropicalization. In order to determine the potentially good situations, we focus on the following concepts:

- An abstract tropical geometric construction. That is, we do not specify the coordinates of the points, neither the concrete curves, only their support and the steps of the construction. Moreover, we ask it to be well defined in both fields $\mathbb{K}$ and k.
- The specialization of the input elements of the abstract construction to concrete elements.
- A concrete lift of a given set of input elements.

These concepts are manipulated by adding quantifiers relating them in order to obtain a statement like:
"K_1 *tropical construction* K_2 *specialization of the input data* K_3 *lift of these input data, diagram 4.1 commutes*".
Where K_1, K_2, $K_3 \in \{\forall, \exists\}$. We arrive naturally to the following problems:

Questions 4.8.

1. For all constructions, for all input tropical data and for all lifts of these tropical data, diagram 4.1 commutes.
2. For all constructions and for all input tropical data there exists a lift of these tropical data such that diagram 4.1 commutes.
3. For all construction, there is a choice of the input tropical data such that for all lift of these tropical data, diagram 4.1 commutes.
4. There exists a construction such that for all input tropical data and for all lifts of these tropical data, diagram 4.1 commutes.
5. For all constructions, there is a choice of input tropical data and there is a lift of these tropical data such that diagram 4.1 commutes.
6. There exists a construction such that for all input tropical data there is a lift of these tropical data such that diagram 4.1 commutes.
7. There exists a construction and there is suitable input tropical data such that for all lifts of these tropical data, diagram 4.1 commutes.

8. There exists a construction, particular input tropical data and a suitable lift of these tropical data such that diagram 4.1 commutes.

Clearly, these relations are not independent, ranking (non linearly) from item 1, which is the strongest, to item 8, the weakest one. Checking this problems gives an overview of the typical problems we find when dealing with incidence conditions in Tropical Geometry. The only statements that hold are items 5, 6, 7 and 8. For the sake of brevity, we will consider mostly the case where our curves are lines on the plane.

Proposition 4.9. *The only items of problem 4.8 that hold are 5, 6, 7 and 8.*

Proof.

• Take two tropical lines in the plane that intersects in only one point. Then, for all lifts of this two lines, the intersection point always tropicalizes to the tropical intersection. So statement 4.8.7 holds and, from this, we derive that 4.8.8 also does.

• Choose two curves that intersect in an infinite number of points. In Theorem 1.4, we are given a way to compute lifts that intersects in non stable points. So the property of agreement with tropicalization is not universal for the non transversal cases. This simple example shows that statement 4.8.1 does not hold. Using duality, we observe also that the concept of stable curve through a set of points does not work for every input data and every lift (ie. there will always be exceptional cases). Thus, since every tropical geometric construction consists of a sequence of these two steps (computing the stable curve through a set of points, or computing the stable intersection of two curves), we deduce that statement 4.8.4 neither holds. In particular, if we are able to find a construction such that for all input data we arrive to these exceptional cases, we will find a counterexample to question 4.8.3. An example of such a construction is as follows:

Input: Points a, b, c, d, e

Depth 1: Compute $l_1 := \overline{ab}$, $l_2 := \overline{ac}$, $l_3 := \overline{ad}$, $l_4 := \overline{ae}$

Depth 2: $p_{12} = l_1 \cap l_2$, $p_{13} = l_1 \cap l_3$, $p_{14} = l_1 \cap l_4$, $p_{23} = l_2 \cap l_3$, $p_{24} = l_2 \cap l_4$, $p_{34} = l_3 \cap l_4$

First, we compute four tropical lines through one fixed point a. If point a is exactly the vertex of one of the lines, then two of the input points are the same and there is an infinite number of lines passing through these two points. On the other hand, if a is never the center of the lines, it must be in one of the three rays. There are only three possibilities for the rays, the directions $(-1, 0)$ $(0, -1)$ and $(1, 1)$. As there are four lines involved, two of the branches must have the same directions, so these two lines intersect in an infinite number of points and we are done.

• To go further in the analysis, it is necessary to have more tools that takes care of more complicated constructions. Theorem 4.6 establishes that for an admissible construction and for all realization of the input elements, there always exists a lift of these elements such that all the steps of both constructions are coherent with the tropicalization. In particular, we have the validity of question 4.8.6 for every admissible construction.

• Also, a counterexample to 4.8.2 is given in Example 4.7. Take three points a, b, c. Construct the lines $l_1 = \overline{ab}$, $l_2 = \overline{ac}$ and the point $p = l_1 \cap l_2$. If we perform this construction in the projective plane with three points not in the same line, we will always find that $p = a$. But in the tropical case, taking $a = (0, 0)$, $b = (-2, 1)$, $c = (-1, 3)$, we arrive to $p = (0, -1) \neq a$. This simple example shows a concrete construction and input data such that for all lifts of the input elements, diagram 4.1 does not commute. Note that in this case there are double paths in the construction graph. If we follow the method exposed in Theorem 4.4, then, for all lifts, we arrive that the constructible set $\mathfrak{S}$ is contained in $0 \neq 0$. That is, the set of valid principal coefficients is empty.

• Finally, let us prove 4.8.5. This case of course cannot be restricted to the linear case. Suppose given a geometric construction, we choose as input data the most degenerate case possible: if we have a point, we choose the point to be $p_0 := (0, 0)$ and if we have a curve with prescribed support, we take all its coefficients equal to zero. As a set, it consist in some rays emerging from the origin $(0, 0)$ in perpendicular directions to the edges of the Newton polygon of the curve. The stable intersection of any two such curves is always the isolated point p_0 with the convenient multiplicity. The stable curve with prescribed polytope taking all elements equal to the origin is the one with all coefficient equal to zero. It only rests to check that there is a lift compatible with this tropical construction. As the construction is well defined, it is realizable for the generic input in $(k^*)^2$. This construction can be embedded in $(\mathbb{K}^*)^2$ with all the elements of order 0. □

4.6 Extension of the Results

As an application of the construction method and Theorem 4.6, we are able to extend Theorem 1.30 to a wider set of incidence configurations.

Theorem 4.10. *Let G be an incidence structure, suppose that we have a tropical realization p of G such that, for every curve C, the set of points incident to C are in generic position with respect to C. Then, the tropical realization can be lifted to an algebraic realization.*

Proof. For each curve C of support I, let $q_1, \ldots, q_n$ be the set of points incident to C. By definition of points in general position, we can extend this set to a set of points $q_1, \ldots, q_{\delta(I)-1}$ such that C is the stable curve through these points. Add to the configuration G these additional points for every curve C. We obtain in this way an incidence configuration G_1 that contains G as a substructure and such that every curve C of support I is exactly the stable curve passing through the points $q_1, \ldots, q_{\delta(I)-1}$. Hence, by Proposition 4.2, G_1 is the graph of a geometric construction $\mathfrak{C}$. The input elements are the set of points q_i and every curve is the stable curve through $\{q_1, \ldots, q_{\delta(I)-1}\}$. This construction is admissible, because it is of depth 1. By Theorem 4.6, every tropical instance p_1 of $\mathfrak{C}$ can be lifted to an algebraic instance $\widetilde{p_1}$ of $\mathfrak{C}$. In particular, the instance p of G we started from can be lifted to the algebraic plane. □

This Theorem shows how the notion of points in general position helps to the problem of lifting an incidence configuration. Our next goal is to apply this notion to more complex configurations coming from geometric constructions. The key idea for this application is that points in general position with respect to a curve C behave like generic points for the purposes of Theorem 4.6.

Theorem 4.11. *Suppose that we are given a non admissible geometric construction $\mathfrak{C}$ but such that, the only obstacle to be an admissible construction is that we have two curves C_1, C_2 with intersection $Q = \{q_1, \ldots, q_n\}$ such that Q is used twice to define some successor element x. That is, every double path $A \rightrightarrows B$ in $\mathfrak{C}$ can be restricted to a double path from both curves passing through Q,*

$$C_1 \rightrightarrows Q \rightrightarrows B \text{ and } C_2 \rightrightarrows Q \rightrightarrows B.$$

Suppose we have an instance p of this construction. If, for every element x which is the end of a double path, the set $Q_x = \{q_i \in Q \mid \exists q_i \to x\}$ is in general position in C_1 and C_2, then the tropical instance can be lifted to an algebraic realization $\widetilde{p}$ of the construction. More concretely, the set $\mathfrak{S}$ of Theorem 4.4 associated to p contains an open dense subset of $(k^*)^N$.

Proof. First, we are proving that, for any single node x of $\mathfrak{C}$, its construction can be lifted. Let x be a node of $\mathfrak{C}$. Let $\mathfrak{C}_x$ be the minimal subconstruction of $\mathfrak{C}$ such that it contains every input element of $\mathfrak{C}$ and the element x. This minimal subconstruction can be defined as follows. First, we consider as nodes of $\mathfrak{C}_x$ the input elements of $\mathfrak{C}$, the node x and every predecessor of x. The incidence conditions will be those induced by $\mathfrak{C}$. Second, we complete it with the necessary nodes of $\mathfrak{C}$ as in the proof of Proposition 4.2. Actually, the only nodes we have to add are the intersection points of two curves y_1, y_2 that have to be intersected (necessarily, these curves will be predecessors of x). Let $\mathfrak{S}_x$ be the set of valid input elements of the construction $\mathfrak{C}_x$. By the definition of $\mathfrak{S}$,

$$\mathfrak{S} = \bigcap_{x \in \mathfrak{p} \cup \mathfrak{B}} \mathfrak{S}_x$$

So, if every $\mathfrak{S}_x$ contains a non empty open Zariski set of $(k^*)^N$, the same occurs for $\mathfrak{S}$.

If $\mathfrak{C}_x$ is admissible, then $\mathfrak{S}_x$ contains a non empty Zariski set by Theorem 4.6. If $\mathfrak{C}_x$ is not admissible, the set Q_x contains at least two elements. Moreover, for every node y in $\mathfrak{C}_x$ it happens that $Q_y \subseteq Q_x$.

Consider now the minimal subconstruction $\mathfrak{C}_x^1$ containing every input element and the set Q_x. This construction is admissible, so $\mathfrak{S}_x^1$ is dense. On the other hand, the possible principal coefficients of the set Q_x form a dense set of its space of configurations by Theorem 3.12. Let $\mathfrak{C}_x^2$ the subconstruction obtained from $\mathfrak{C}_x$ by deleting every predecessor of the points in Q_x and the intersection of C_1 and C_2 not in Q_x. This construction is also admissible, because the curves C_1, C_2 have been deleted among other objects. Hence $\mathfrak{S}_x^2$ is also dense. The projections of the set $\mathfrak{S}_x^1$ and $\mathfrak{S}_x^2$ into the support space of Q_x contains an open dense subset, their intersection also contains a non empty dense subset. This means that there are values of the principal coefficients

of Q_x that are generic and compatible either with $\mathfrak{C}_x^1$ and $\mathfrak{C}_x^2$. It follows that for a residually generic lift of the input elements of $\mathfrak{C}_x$, very step will be well defined and compatible with tropicalization. Thus, $\mathfrak{S}_x$ is contains a dense subset of $(k^*)^N$. □

In contrast to Theorem 4.6, this Theorem does not work for tropical realization of a particular construction $\mathfrak{C}$, because it is stated in terms of the realization. It needs some additional hypothesis in the construction (some points are in general position) that depend on the concrete realization. It still has its applications, such as Theorem 5.9.

4.7 Impossibility for the Existence of a Lift

This Section deals with non admissible constructions, suppose that we have a non admissible geometric construction $\mathfrak{C}$ and a tropical instance of it such that the constructible set $\mathfrak{S}$ is empty. Then, we would still like to know if it is possible to lift the construction. The only result that affirms that it is impossible to have a lift is Proposition 2.7. We can provide a similar notion for the stable intersection of curves.

Proposition 4.12. *Let f, g be two tropical curves, let $\{\gamma_1, \ldots, \gamma_r\}$ be the residual conditions for the compatibility of the algebraic and tropical resultant $R(x)$ described in Lemma 3.9. These are the residual conditions $\gamma_i \neq 0$ such that i is part of two consecutive points in the Newton diagram (Definition 1.7) Then:*

- *If every polynomial γ_i is a monomial, then, the algebraic resultant is always compatible with tropicalization $T(\widetilde{R}(x)) = \mathcal{T}(R(x))$.*
- *If one polynomial γ_i is a monomial and it is, then the algebraic resultant $\widetilde{R}(x)$ is compatible with tropicalization if and only if the rest of the polynomials γ_j are non zero.*
- *If every polynomial γ_i is zero, we cannot derive any information about the compatibility.*

Proof. $\widetilde{R}(x) = \sum_{i=0}^{r} \widetilde{h}_i x^i$, $R(x) = \sum_{i=0}^{r}, h_i x^i$. If $\gamma_i \neq 0$ then the principal term of $\widetilde{h}_i$ is exactly $\gamma_i t^{-h_i}$. The conditions searched for the compatibility of the resultants is that the elements γ_i associated to an index i such that it is part of two consecutive points in the Newton diagram of the polynomial do not vanish. If one γ_i is a monomial, then it will never evaluate to zero. So the Newton diagram will not change if and only if the rest of the γ_j do not evaluate to zero. Hence we have the first two items. On the other hand, if every γ_i evaluates to zero, we cannot know how the Newton diagram of $\widetilde{R}(x)$ is, it may change or not. □

Definition 4.13. Let $\mathfrak{C}$ be a construction and p a tropical realization of it. Let x be a node of $\mathfrak{C}$. We say that x is a *fixed* element of $\mathfrak{C}$ if:

- x is an input element of $\mathfrak{C}$.

- x is the curve of support I passing through $\{y_1, \ldots, y_{\delta(I)-1}\}$ and at least one of the pseudodeterminants associated to the linear system defining x is regular (See Proposition 2.7).
- x is an intersection point of y_1 and y_2 and, if C_1, C_2 are the tropical realization of curves y_1, y_2, then, at least one the residual conditions $\gamma_{i_1}(x)$, $\gamma_{i_2}(y)$ and $\gamma_{i_3}(xy^{-a})$ of each resultant $R(x)$, $R(y)$, $R(xy^{-a})$ defined in Theorem 3.10 is a monomial.

Let $\mathfrak{C}$ be a geometric construction and p a tropical realization of $\mathfrak{C}$. Suppose that the set $\mathfrak{S}$ associated to the tropical realization is empty. Then, during the definition of the auxiliary set T in Theorem 4.4, there will be a step such that T was not empty before the step, but the restrictions added in this step forces T to be empty. This step consists in defining an element x. Let $h_1, \ldots, h_r$ be the residual polynomials codifying the compatibility of this algebraic step with tropicalization defined using Theorem 2.10 and 3.10. Suppose that at least one of the polynomials h_i does not evaluate to zero. Then:

- If every predecessor of x is fixed, by Propositions 2.7 and 4.12, there cannot be any lift of the tropical realization of $\mathfrak{C}$. Because for every lift of the input elements, every lift of the predecessors of x will tropicalize correctly, but the element x either is not well defined, or it will never tropicalizes correctly.
- If at least one predecessor of x is not fixed, then, there might be a lift of the tropical realization of $\mathfrak{C}$ or not. But at least, there cannot be any lift with residually generic input elements. There must be some algebraic relations among the residual coefficients of the algebraic input elements of $\mathfrak{C}$.

On the other hand, if every residual polynomial h_i evaluates to zero. We cannot conclude anything, there might be a lift of the realization or not. And this lift may work for the generic input or not. In this case the residual coefficient approach is not enough to answer the question.

For most geometric constructions the remarks above are enough. That is, if for one tropical realization its associated set $\mathfrak{S}$ is empty, then either we can deduce that for the generic lift of the input elements the algebraic construction will not project correctly. Or even that there will be no lift at all. In fact, for every geometric construction that we have faced during the development of this theory, every instance of every construction fell in this two cases. It is difficult to find a construction and an instance of the construction such that the construction method and the set $\mathfrak{S}$ does not provide any information. The following is the only one example of this peculiar behaviour.

Example 4.14. In this example, for convenience with the geometric language, we will think that the algebraic torus $(\mathbb{K}^*)^2$ is contained in the affine plane and this one contained in the projective plane. With this in mind, we can talk about concepts such at horizontal line (line of support $\{1, y\}$) or the line at the infinity. This is intended only to simplify notations and use a more natural language, but it does not interfere with the result itself.

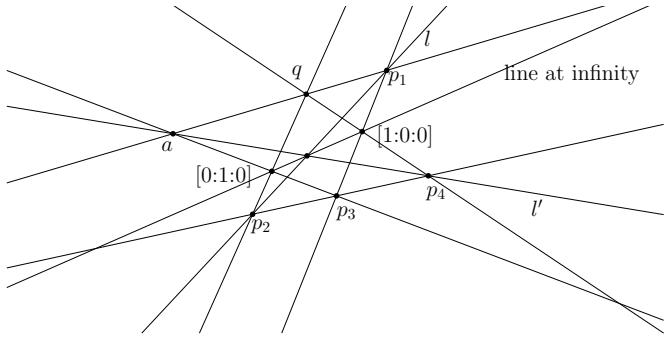


Figure 4.2: How to construct a parallel line through one point

First, we need a specific construction. Given a point a and a line l. We look for a geometric construction such that, in the algebraic plane, it defines the parallel of l passing through a. The difficulty is to define it with the restricted allowed steps of Definition 4.1.

l'=Parallel(a,l,q)

Input:					
points	a, q				
line	l				
Depth 1:					
curve	v_1	of support	$\{1, x\}$	passing through	a
curve	v_2	of support	$\{1, x\}$	passing through	q
curve	h_1	of support	$\{1, y\}$	passing through	q
curve	r_1	of support	$\{1, x, y\}$	passing through	$\{a, q\}$
Depth 2:					
point	$p_1 = l \cap r_1$				
point	$p_2 = l \cap v_2$				
Depth 3:					
curve	h_2	of support	$\{1, y\}$	passing through	p_1
Depth 4:					
point	$p_3 = h_2 \cap v_1$				
Depth 5:					
curve	r_2	of support	$\{1, x, y\}$	passing through	$\{p_2, p_3\}$
Depth 6:					

point $p_4 = r_2 \cap h_1$

Depth 7:

curve l' of support $\{1, x, y\}$ passing through $\{a, p_4\}$

In the algebraic case, if the input elements a, x, l are generic, then the construction yields a realization of the hypothesis of Pappus Theorem with one of the lines being the line at infinity and two of the points are points with projective coordinates $[0 : 1 : 0]$ and $[1 : 0 : 0]$, see Figure 4.2. Hence, by Pappus theorem, the lines l, l' intersects at the line at infinity. Thus, l' is the parallel to l passing through a. The same approach work if we replace l (a curve of support $\{1, x, y\}$) by a line passing through the affine origin of coordinates (curve of support $\{x, y\}$). We will use this construction as an auxiliary for the following:

Take as input points a, b, c, q, let $o = (0, 0)$ be the origin of coordinates in the affine plane $\mathbb{K}^2$, a line through a point p and o is just the curve through p of support $\{x, y\}$. Consider the following construction:

Depth 1: $l_1 = \overline{oa}$, $l_2 = \overline{ob}$, $l_3 = \overline{oc}$

Depth 2-8: $l_4 = Parallel(a, l_2, q)$, $l_5 = Parallel(b, l_1, q)$

Depth 9: $d = l_4 \cap l_5$

Depth 10: $l_6 = \overline{od}$

Depth 11-17: $l_7 = Parallel(d, l_3, q)$, $l_8 = Parallel(c, l_6, q)$

Depth 18: $z = l_7 \cap l_8$

Depth 19: $l_9 = \overline{az}$

In the affine plane, we have constructed the parallelograms $oadb$ and $odzc$. Hence, if $a = (a_1, a_2)$, $b = (b_1, b_2)$ and $c = (c_1, c_2)$, then $d = (a_1 + b_1, a_2 + b_2)$ and $z = (a_1 + b_1 + c_1, a_2 + b_2 + c_2)$. Notice that this construction if far from being an admissible one.

Take the following tropical input elements of this construction, $a = (0, 0)$, $b = (-1, -1)$, $c = (-2, -2)$ and $q = (2, -1)$. For this input, we have that $z = (0, 0)$ and $l_9 =$ "$0x + 0y + 0$". The constructible set $\mathfrak{S}$ associated to this input is empty. Lifts of the input elements are

$$\widetilde{a} = (\alpha_1 + \ldots, \alpha_2 + \ldots), \widetilde{b} = (\beta_1 t + \ldots, \beta_2 t + \ldots),$$

$$\widetilde{c} = (\gamma_1 t^2 + \ldots, \gamma_2 t^2 + \ldots), \widetilde{q} = (\eta_1 t^{-2} + \ldots, \eta_2 t + \ldots)$$

The algebraic computations of $\widetilde{z}$ leads to the point

$$\widetilde{z} = (\alpha_1 + \ldots, \alpha_2 + \ldots).$$

That is, the principal term of $\widetilde{a}$ and $\widetilde{z}$ are the same. So, we cannot compute the algebraic line $\widetilde{l_9}$ neither we cannot deduce if the generic lift of the input will work or if there will be a lift at all. However, it can be checked that the set $\mathfrak{S}_z$ associated to the subconstruction that defines z is nonempty and dense $\{\beta_2 - \eta_2 \neq 0, \alpha_2\beta_1 - \alpha_1\beta_2 \neq 0, -\alpha_1\gamma_2 + \gamma_1\alpha_2 \neq 0\} \cap (k^*)^8$.

In fact, for this construction and this tropical realization, the generic lift works and it is compatible with tropicalization. To explain this, we know that $\widetilde{z} = \widetilde{a} + \widetilde{b} + \widetilde{c}$. If $\widetilde{a} = (\widetilde{a}'_1, \widetilde{a}'_2), \widetilde{b} = (\widetilde{b}'_1 t, \widetilde{b}'_2 t), \widetilde{c} = (\widetilde{c}'_1 t^2, \widetilde{c}'_2 t^2), \widetilde{q} = (\widetilde{q}'_1 t^{-2}, \widetilde{q}'_2 t)$, where $\widetilde{a}'_i, \widetilde{b}'_i, \widetilde{c}'_i, \widetilde{q}'_i$ are elements of valuation zero. Then $\widetilde{z} = (\widetilde{a}'_1 + \widetilde{b}'_1 t + \widetilde{c}'_1 t^2, \widetilde{a}'_2 + \widetilde{b}'_2 t + \widetilde{c}'_2 t^2)$ and $\widetilde{l}_9 = (\widetilde{b}'_2 t + \widetilde{c}'_2 t^2)x + (-\widetilde{b}'_1 t - \widetilde{c}_1 t^2)y + (\widetilde{a}'_2 \widetilde{b}'_1 - \widetilde{a}'_1 \widetilde{b}'_2)t + (\widetilde{a}'_2 \widetilde{c}'_1 - \widetilde{a}'_1 \widetilde{c}'_2)t^2 = 0$. If $\alpha_2\beta_1 - \alpha_1\beta_2 \neq 0$ then $T(\widetilde{l}_9) = \text{“}(-1)x + (-1)y + (-1)\text{”} = \text{“}0x + 0y + 0\text{”} = l_9$.

As a negative example, take the same construction but we take as input element $b = (-1, -2)$, then we will arrive to the same situation of undecidability as above, the set $\mathfrak{S}$ is again empty. If we take as before generic lifts of the input elements, but this time $\widetilde{b} = (\widetilde{b}'_1 t, \widetilde{b}'_2 t^2)$. Now, $\widetilde{z} = (\widetilde{a}'_1 + \widetilde{b}'_1 t + \widetilde{c}'_1 t^2, \widetilde{a}'_2 + (\widetilde{b}'_2 + \widetilde{c}'_2)t^2)$ and $\widetilde{l}_9 = (\widetilde{b}'_2 + c2)tx + (-\widetilde{b}'_1 - \widetilde{c}'_1 t)y + \widetilde{a}'_2 \widetilde{b}'_1 + (\widetilde{a}'_2 \widetilde{c}'_1 - \widetilde{a}'_1 \widetilde{b}'_2 - \widetilde{a}'_1 \widetilde{c}'_2)t$. Then $T(\widetilde{l}_9) = \text{“}(-1)x + 0y + r\text{”}$, where $r \geq 0$. So it never tropicalizes correctly.

Chapter 5

Application: A Transfer Technique in Tropical Geometry

5.1 Notion of Constructible Theorem

In this Chapter we present the main application of the tools and results obtained so far. Many classical theorems in Projective Geometry deal with properties of configurations of points and curves. Thus, we can use the relationship between the algebraic and tropical configurations in order to transfer a Theorem from Classical Geometry to Tropical Geometry. So, we need a notion of *"Theorem"* is terms of configurations. We propose the following notion.

Definition 5.1. A *constructible incidence statement* is a triple (G, H, x) such that G is an incidence structure, H is a geometric construction, called the *hypothesis*, such that, considered as an incidence configuration, H is a full substructure of G, $H \subseteq G$. Moreover,

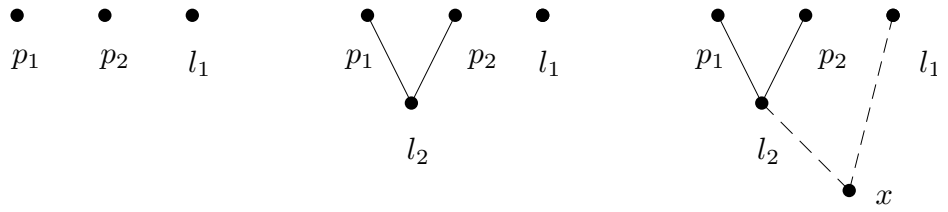
$$\{\mathfrak{p}_G \cup \mathfrak{B}_G\} \setminus \{\mathfrak{p}_H \cup \mathfrak{B}_H\} = \{x\},$$

there is only one vertex x of G which is not a vertex of H, this is called the *thesis node*.

Let H_0 be the set of input elements of H as a construction. Let $\mathbb{K}$ be an algebraically closed field. The incidence theorem *holds* in $\mathbb{K}$ or it is a *constructible incidence theorem* over $\mathbb{K}$ if it holds for the generic realization of H_0. That is, if there is a non empty open set L defined in the support space of H_0, $L \subseteq S_{H_0}$ such that:

- For every $\widetilde{h} \in L$, the construction H is well defined.
- If $\widetilde{p} \in R_H$ is the realization of H constructed from $\widetilde{h}$, then there is an element $\widetilde{x}$ such that $(\widetilde{p}, \widetilde{x})$ is a realization of G.

In the tropical context, the construction H is always well defined. Every realization h of the input of H defines a realization p of H by the construction. So, a constructible statement *holds* in the tropical plane or it is a *tropical constructible incidence theorem* if, for each realization p of H obtained by the construction, there is a tropical element x such that (p, x) is a tropical realization of G.



Input, H_0 Hypothesis H Graph G

Figure 5.1: Constructible incidence theorem

Example 5.2. There are many straightforward theorems that fit in this definition. For example, let $H_0 = \{p_1, p_2, l_1\}$, where p_1, p_2 are points and l_1 is a line. Let $\mathfrak{C}$ be the construction consisting in computing the line l_2 through p_1 and p_2. Let x be the thesis node representing a point and impose the conditions that x belongs to both lines l_1 and l_2. The vertices of G are $\{p_1, p_2, l_1, l_2\}$. The edges (incidence conditions) of G are those of H, $\{(p_1, l_2), (p_2, l_2)\}$ plus the edges connecting the thesis node $\{(x, l_1), (x, l_2)\}$. This statement only asserts that l_1, l_2 have a common point. So it holds in every field $\mathbb{K}$ and also in the tropical plane $\mathbb{T}^2$.

Of course, this notion is interesting if the thesis node x and the elements linked to it $h_1, \ldots, h_n$ form an incidence structure G_0 that is not realizable whenever the elements $h_1, \ldots, h_n$ are generic. For instance, the case where x is a line containing three points h_1, h_2 and h_3. Now we prove a transfer result for constructible incidence theorems.

Theorem 5.3. *Let $\mathcal{Z} = (G, H, x)$ be a constructible incidence statement. Suppose that the construction H is admissible. If $\mathcal{Z}$ holds in a concrete algebraically closed field $\mathbb{K}$, then it holds for every tropical plane $\mathbb{T}^2$.*

Proof. First, suppose that $\mathbb{T}$ is the value group of the algebraically closed field $\mathbb{K}$ such that $\mathcal{Z}$ holds. Let h be a tropical realization of the input elements of the hypothesis H. Let p be the tropical realization of H constructed from h. As H is an admissible construction, by Theorem 4.6, the set $\mathfrak{S}$ defined in $(k^*)^N$ associated to h contains a non empty open set. It follows that there is always a lift $\widetilde{h}$ of h belonging to L and such that its principal coefficients belong to the set $\mathfrak{S}$. Then, we can lift p to an algebraic realization $\widetilde{p}$ of H constructed from $\widetilde{h}$. As $\mathcal{Z}$ holds in $\mathbb{K}$, there is an element $\widetilde{x}$ such that $(\widetilde{p}, \widetilde{x})$ is a realization of G. It follows that its projection (p, x) is a tropical realization of G and $\mathcal{Z}$ holds in $\mathbb{T}$.

For the general case, the set L of good input elements of H is definable in the first order language of the prime field of $\mathbb{K}$. So, if the theorem holds in an algebraically closed field, it holds over any algebraically closed field of the same characteristic (see [Rob56]). In particular, fixed a tropical semifield $\mathbb{T}$, there is an algebraically closed

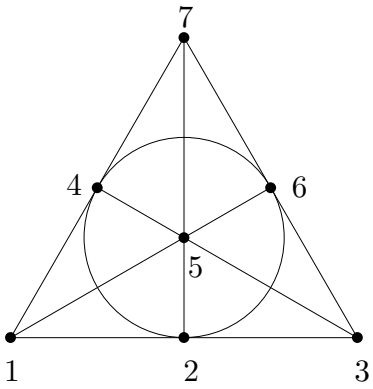


Figure 5.2: The configuration of Fano plane

valued field $\mathbb{L}$ of the same characteristic as $\mathbb{K}$ and whose valuation group is $\mathbb{T}$. Thus, if $\mathcal{Z}$ holds in $\mathbb{K}$, then it also holds in $\mathbb{L}$ and hence, it holds in $\mathbb{T}$. □

5.2 Examples of Theorems

In this Section, some examples of constructible incidence theorems are shown. They are all classic, but they are rewritten as constructible incidence theorems. There is an additional problem when expressing the theorems in this way. Usually, it is not enough to provide a naive construction of the hypothesis, because it is very likely that the resulting construction is not admissible and Theorem 5.3 does not apply. So, the presentation of the theorems might seem strange at first sight.

5.2.1 Fano Plane Configuration Theorem

This first example shows the dependence of the characteristic of the field $\mathbb{K}$ in order to derive the validity of a constructible incidence theorem in the tropical context. The classical Theorem deals with the configuration of points and lines in Fano plane, the projective plane over the field $\mathbb{F}_2$. The configuration of Fano plane consists in 7 lines and 7 points as represented in Figure 5.2. This configuration cannot be realized over a plane of characteristic zero. Over any projective plane over any field of characteristic 2, if seven points $1, 2, 3, 4, 5, 6, 7$ verifies that the triples $(1, 2, 3)$, $(1, 4, 7)$, $(3, 6, 7)$, $(1, 5, 6)$, $(2, 5, 7)$, $(1, 4, 7)$ are collinear, then the points $(2, 4, 6)$ are also collinear. This Theorem holds in a field $\mathbb{K}$ if and only if the field is of characteristic 2. About the tropicalization of this Theorem, it was proved to hold in the $\mathbb{T}^2$ by M. Vigeland using specific techniques ([Vig06]). See also [DSS05] for an application of this configuration to the comparison of different notions of the tropical rank of a tropical matrix.

Theorem 5.4 (Fano plane configuration Theorem)**.**
Construction of the hypothesis H:

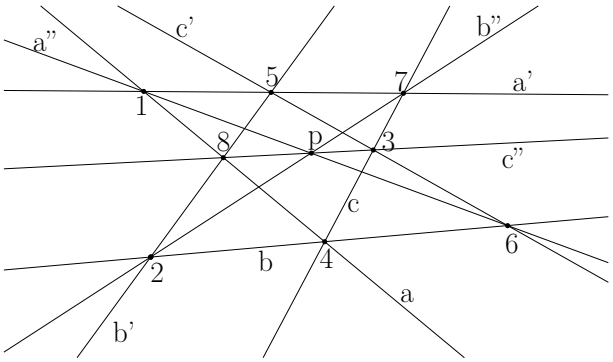


Figure 5.3: Pappus configuration

Input:			
points	$1, 3, 5, 7$		
Depth 1:			
lines	$a = \overline{13}$	$b = \overline{15}$	$c = \overline{17}$
	$d = \overline{35}$	$e = \overline{37}$	$f = \overline{57}$
Depth 2:			
points	$2 = a \cap f$	$4 = c \cap d$	$6 = b \cap e$
Thesis node:	*line* l		
Thesis:	*points* $2, 4, 6$ *are collinear (belong to* l*)*		

The construction of the hypothesis is admissible, so we can derive that the theorem holds in the tropical plane. In brief, this Theorem proves that, if we start with any set of points $1, 3, 5, 7$ *in which even we allow repetitions and we perform the construction steps above, then three new points* $2, 4, 6$ *will be obtained, and these three new points will necessarily lie on a common line* l*.*

5.2.2 Pappus Theorem

This classical theorem was studied from a tropical perspective in [RGST05]. There, the authors showed that a direct translation of the usual hypothesis of the theorem does not imply the thesis in the tropical context. On the other hand, they proposed a constructive version of this Theorem. We proved this constructive version of this Theorem in [Tab05] using a precursor technique of our construction method.

Theorem 5.5 (Pappus Theorem)**.**
Construction of the hypothesis H*:*

Input:	
points	*1, 2, 3, 4, 5*

Depth 1:			
lines	$a = \overline{14}$	$b = \overline{24}$	$c = \overline{34}$
	$a' = \overline{15}$	$b' = \overline{25}$	$c' = \overline{35}$
Depth 2:			
points	$6 = b \cap c'$	$7 = a' \cap c$	$8 = a \cap b'$
Depth 3:			
lines	$a'' = \overline{16}$	$b'' = \overline{27}$	$c'' = \overline{38}$
Thesis node:	*point* p		
Thesis:	*lines* a'', b'', c'', *are concurrent (pass through* p*).*		

5.2.3 Converse Pascal Theorem

Let 1, 2, 3, $1'$, $2'$, $3'$ be six points in the plane, let $7 = \overline{12'} \cap \overline{1'2}$, $8 = \overline{13'} \cap \overline{1'3}$, $8 = \overline{23'} \cap \overline{2'3}$. Converse Pascal Theorem proves that if $7, 8$ and 9 are collinear, then $1, 2, 3, 1', 2', 3'$ belong to a conic. The dimension of the space of realizations of a Pascal configuration is 11: 5 degrees of freedom comes from the conic and each point $1, 2, 3, 1', 2', 3'$ belonging to the conic adds one degree of freedom each. If we want to define a constructible theorem such that the thesis node is the conic, then the algebraic elements of the construction of the hypothesis can only be points and lines. By the nature of the steps of a construction, any construction that only uses points and lines will provide configurations whose realization space has even dimension (as it equals the dimension of the support space of the input elements). It follows that the dimension of the support space of any potential construction of a Pascal configuration H is even. So, we cannot obtain such a construction for this theorem. However, we can define a bigger construction such that it contains Pascal configuration as a substructure. Namely, we can add three arbitrary points points X_1, X_2, X_3 belonging to $\overline{AB'}$, $\overline{BC'}$, $\overline{CA'}$ respectively, see Figure 5.4. Hence our configuration G is Pascal configuration with three additional marked points X_1, X_2, X_3. Its dimension is now 14. This is a example of how an additional step *"choose a line through* A*"* can be modeled by adding the additional free point X_1 and then defining the line $\overline{AX_1}$.

Theorem 5.6 (Converse Pascal Theorem)**.**
Construction of the hypothesis H*:*

Input:			
points	A, B, C, X_1, X_2, X_3		
line	l		
Depth 1:			
lines	$L_{AB'} = \overline{AX_1}$	$L_{BC'} = \overline{BX_2}$	$L_{CA'} = \overline{CX_3}$
Depth 2:			
points	$P = L_{AB'} \cap l$	$Q = L_{BC'} \cap l$	$R = L_{CA'} \cap l$
Depth 3:			
lines	$L_{AC'} = \overline{AR}$	$L_{BA'} = \overline{BP}$	$L_{CB'} = \overline{CQ}$

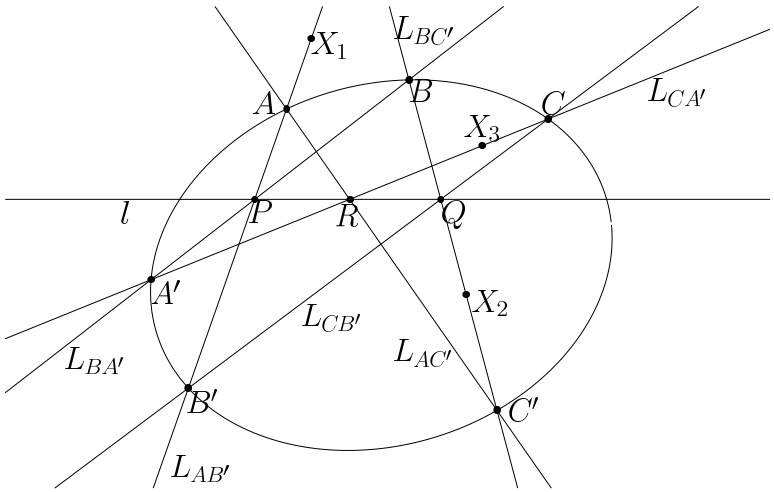


Figure 5.4: Converse Pascal Theorem

Depth 4:
points $A' = L_{CA'} \cap L_{BA'}$ $B' = L_{AB'} \cap L_{CB'}$ $C' = L_{AC'} \cap L_{BC'}$

Thesis node: *conic* R
Thesis: *points* A, B, C, A', B', C' *belong to conic* R.

5.2.4 Chasles Theorem

Chasles Theorem (c.f. [EGH96]) states that if $\{q_1, \ldots, q_9\}$ are the intersection points of two cubics, then any cubic passing through $\{q_1, \ldots, q_8\}$ also passes through q_9. This implies that given another free point q_0, there is always a cubic through $\{q_0, q_1, \ldots, q_9\}$. This version can be easily translated to the tropical context.

Theorem 5.7 (Chasles Theorem)**.**
Construction of the hypothesis H*:*

Input:
cubics C_1, C_2
point q_0

Depth 1:
points $\{q_1, \ldots, q_9\} = C_1 \cap C_2$

Thesis node: *cubic* R
Thesis: *points* $\{q_0, q_1, \ldots, q_9\}$ *belong to cubic* R.

It is not true that every cubic passing through eight of the intersection points passes through the ninth. See Figures 5.5 and 5.6. Let $f =$ "$0{+}1x{+}1y{+}1x^2{+}3xy{+}1y^2{+}0x^3{+}$

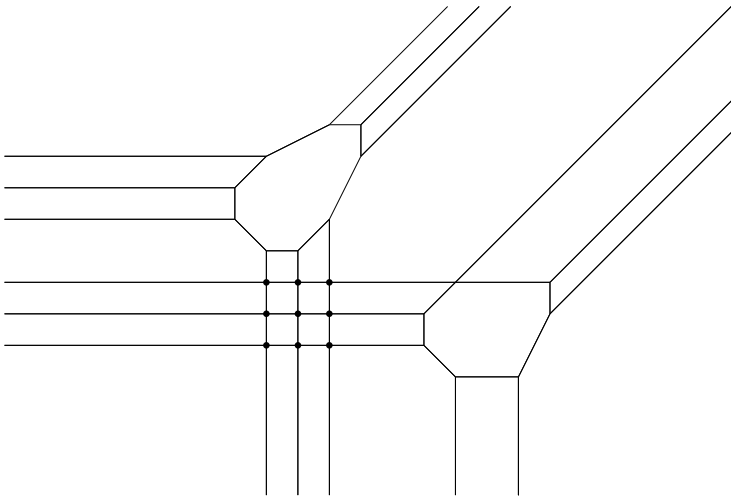


Figure 5.5: Tropical Chasles

$1x^2y+1xy^2+0y^3$, $g = 19+14x+20xy+24y+7x^2+12x^2y+23xy^2+28y^2+0x^3+31y^3$",

$$f \cap_{st} g = \begin{array}{lll} \{(-1,-3), & (0,-3), & (1,-3), \\ (-1,-4), & (0,-4), & (1,-4), \\ (-1,-5), & (0,-5), & (1,-5)\ \} \end{array}$$

Take $h =$ "$0+1x+5y+\frac{11}{2}xy+1x^2+9y^2+5x^2y+9xy^2+0x^3+12y^3$". This is a cubic passing through 8 of the stable intersection points of f and g but not through the nine.

An alternative to the Chasles Theorem that also holds in the tropical plane is the following. Take as $8+n$ points $\{q_1,\ldots,q_8\}$, $\{x_1,\ldots,x_n\}$, $n \geq 3$. All the steps are computing the cubic C_i passing through $\{q_1,\ldots,q_8,x_i\}$, $1 \leq i \leq n$. The thesis node is a point x and the thesis is that x belongs to C_i, $1 \leq i \leq n$. The difference with the previous version of Chasles theorem is that, by construction, the eight points $\{q_1,\ldots,q_8\}$ are always in general position in every cubic C_i. In our example, the points are not in general position neither in $\mathcal{T}(f)$ nor $\mathcal{T}(g)$.

An immediate generalization of Chasles Theorem is the following.

5.2.5 Cayley- Bacharach Theorem

The generalization of Chasles Theorem (cf [EGH96]) we discuss here is the following: let C_1, C_2 be plane curves of degrees d and e respectively, intersecting in de distinct points $Q = \{p_1,\ldots,p_{de}\}$. If C is any plane curve of degree $d+e-3$ containing all but one point of Q, then C contains every point of Q. The second version of Chasles Theorem given does not fit well to this theorem, but the generalization of the first version of Chasles Theorem is immediate, note that a curve of $d+e-3$ is determined by $\frac{d^2+e^2-3e-3d}{2}$ points:

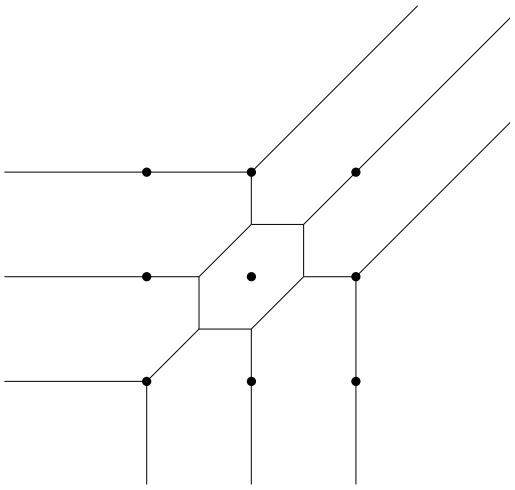


Figure 5.6: A cubic through 8 but not 9 points

Let $d, e \geq 3$ natural numbers, $l = 1 + \frac{d^2+e^2-3e-3d}{2}$

Theorem 5.8 (Cayley-Bacharach Theorem)**.**
Construction of the hypothesis H:

Input:	
degree d curve	C_1
degree e curve	C_2
points	$p_1, \ldots, p_l$
Depth 1:	
points	$\{q_1, \ldots, q_{de}\} = C_1 \cap C_2$
Thesis node:	*curve of degree* $d + e - 3$, R
Thesis:	*points* $\{q_1, \ldots, q_{de}\} \cup \{p_1, \ldots, p_l\}$ *belong to curve* R.

5.2.6 Weak Pascal Theorem

This Theorem is not in the context of Theorem 5.3 because the construction involved is not admissible. Nevertheless, for some tropical realization of the hypothesis, we will be in the context of Theorem 4.11. So this Theorem does not hold for every tropical input, we have to add conditions in the tropical realization.

Theorem 5.9 (Weak Pascal Theorem)**.**
Consider the following construction:

Input:			
conic	Z		
lines	L_1, L_2, L_3		
Depth 1:			
points	$\{A, B'\} = R \cap L_1, \{B, C'\} = R \cap L_2, \{C, A'\} = R \cap L_3$		
Depth 2:			
lines	$L_4 = \overline{AC'}$	$L_5 = \overline{BA'}$	$L_6 = \overline{CB'}$
Depth 3:			
points	$P = L_1 \cap L_5$	$Q = L_2 \cap L_6$	$R = L_3 \cap L_4$

If a tropical instance of this construction is such that each set of points $\{A, C'\}$, $\{B, A'\}$ and $\{C, B'\}$ is in generic position with respect to Z, then there is a line L (thesis node) that contains the P, Q and R.

Proof. This construction, in the algebraic context, provides instances of Pascal theorem. Hence, if the input is generic, then points $\widetilde{P}$, $\widetilde{Q}$, $\widetilde{R}$ are collinear. But this construction is not admissible, so Theorem 5.3 does not apply. Nevertheless, this construction is in the context of Theorem 4.11. The minimal multiples paths are $Z \rightrightarrows L_4$, $Z \rightrightarrows L_5$ and $Z \rightrightarrows L_6$. By Theorem 4.11, if each one of these three sets is in general position with respect to R, then this tropical instance can be lifted to the a generic instance in the algebraic framework. As Pascal Theorem holds in $\mathbb{K}$. $\widetilde{P}$, $\widetilde{Q}$ and $\widetilde{R}$ are collinear. So P, Q and R are collinear. □

Example 5.10. Let $Z =$ "$3y + 5 + 3y^2 + 0x^2 + 4x + 0xy$" $L_1 =$ "$1y + 0x + 0$" $L_2 =$ "$0y + 0x + 2$" $L_3 =$ "$(9/2)y + 0x + 3$", then $A = (3, 2)$, $B' = (1, 0)$, $B = C' = (2, 3/2)$, $C = (1, -3/2)$, $A' = (4, -1/2)$, $L_4 =$ "$3y + 2x + (9/2)$", $L_5 = (3/2)x + 4y + (11/2)$, $L_6 = 0x + 1y + 1$, $P = (5/2, 3/2)$, $Q = (2, 1)$, $R = (5/2, -3/2)$. The points p, Q and R are not collinear, in this example, the set $\{C, B'\}$ is not in generic position in Z.

However, for these input elements, the election of the points in the depth 1 steps is arbitrary. If we now take $A = (1, 0)$, $B' = (3, 2)$, $B = C' = (3/2, 2)$, $C = (4, -1/2)$ and $A' = (1, -3/2)$, now $L_4 =$ "$2y + (3/2)x + (5/2)$", $L_5 =$ "$2y + (3/2)x + (5/2)$", $L_6 =$ "$4y + 2x + 6$", $P = (1, 0)$, $Q = (2, 2)$, $R = (1, -3/2)$. In this case, the three sets of points are in generic position in Z, it can be checked that the three points belong to the tropical line of equation $L =$ "$2x + 2y + 3$".

Part II

Hypercircles for the Simplification of Parametric Curves

Chapter 6

Preliminaires

6.1 Fields of Definition and Zariski Topologies

In this Chapter we present the working context for the rest of the report. The general problem is the following. Let $\mathbb{K} \subseteq \mathbb{K}(\alpha)$ be an algebraic extension of fields. Let $\mathcal{V}$ be a variety defined as the zero set of a set of polynomials whose coefficients are in $\mathbb{K}(\alpha)$. We want to decide if the variety can be defined by a set of polynomials with coefficients in $\mathbb{K}$. Moreover, we want to study the geometric properties of $\mathcal{V}$ with respect to the ground field $\mathbb{K}$ and the algebraic extension $\mathbb{K}(\alpha)$. In particular, if $\mathcal{V}$ is a parametric variety (we are specially interested in the case of curves) given by a parametrization with coefficients in $\mathbb{K}(\alpha)$, we want to solve the analogous problems working with the parametrization alone.

Hence, we do not work in the familiar context of Algebraic Geometry over an algebraically closed fields. So, we have to rewrite the usual definitions and properties of varieties in this new, restricted, context. The result of this Chapter are natural. However, due to the generality of the Fields involved, the proofs are rather technical. We start with the basic definitions of algebraic variety and ideal associated to a variety. From now on, we will always suppose that all our fields are of characteristic zero.

Definition 6.1. Let $\mathbb{K} \subseteq \mathbb{L}$ be an extension of fields of characteristic zero and I an ideal of $\mathbb{K}[x_1, \ldots, x_n]$. The *algebraic variety* defined by I is:

$$\mathfrak{V}_{\mathbb{L}}(I) = \{v = (v_1, \ldots, v_n) \in \mathbb{L}^n \mid \forall f \in I,\ f(v_1, \ldots, v_n) = 0\}$$

We say that $\mathcal{V}$ is a variety *defined over* $\mathbb{K}$ of a $\mathbb{K}$-variety and that $\mathbb{K}$ is a *field of definition* of $\mathcal{V}$.

Definition 6.2. Let $\mathbb{K} \subseteq \mathbb{L}$ be an extension of fields and $\mathcal{V} \subseteq \mathbb{L}^n$ an arbitrary subset of $\mathbb{L}^n$. The *ideal of* $\mathcal{V}$ *with respect to* $\mathbb{K}$ is

$$\mathfrak{I}_{\mathbb{K}}(\mathcal{V}) = \{f \in \mathbb{K}[x_1, \ldots, x_n] \mid \forall (v_1, \ldots, v_n) \in \mathcal{V},\ f(v_1, \ldots, v_n) = 0\}$$

With these notions we have the following familiar properties

Proposition 6.3. *Let $\mathbb{K} \subseteq \mathbb{L}$ be a extension of fields. Let $\mathcal{V}$, $\mathcal{W}$ be arbitrary subsets of $\mathbb{L}^n$, and let I, J be ideals in $\mathbb{K}[x_1, ..., x_n]$. Then:*

1. $I \subseteq J \Rightarrow \mathfrak{V}_{\mathbb{L}}(J) \subseteq \mathfrak{V}_{\mathbb{L}}(I)$
2. $\mathcal{V} \subseteq \mathcal{W} \Rightarrow \mathfrak{I}_{\mathbb{K}}(\mathcal{W}) \subseteq \mathfrak{I}_{\mathbb{K}}(\mathcal{V})$
3. $\mathfrak{V}_{\mathbb{L}}(\sum_i I_i) = \bigcap_i \mathfrak{V}_{\mathbb{L}}(I_i)$
4. $\mathfrak{I}_{\mathbb{K}}(\bigcup_i \mathcal{V}_i) = \bigcap_i \mathfrak{I}_{\mathbb{K}}(\mathcal{V}_i)$
5. $\mathfrak{V}_{\mathbb{L}}(I \cap J) = \mathfrak{V}_{\mathbb{L}}(IJ) = \mathfrak{V}_{\mathbb{L}}(I) \cup \mathfrak{V}_{\mathbb{L}}(J)$
6. $\mathfrak{I}_{\mathbb{K}}(\mathfrak{V}_{\mathbb{L}}(I)) \supseteq I$ *and* $\mathfrak{I}_{\mathbb{K}}(\mathfrak{V}_{\mathbb{L}}(I))$ *is a radical ideal.*
7. *If $\mathcal{V} \subseteq \mathbb{L}^n$ is any subset, then $\mathfrak{V}_{\mathbb{L}}(\mathfrak{I}_{\mathbb{K}}(\mathcal{V})) \supseteq \mathcal{V}$ and the equality holds if and only if $\mathcal{V}$ is a $\mathbb{K}$-variety*
8. *(Hilbert's Nullstellensatz) If $\mathbb{L}$ is algebraically closed field, then $\mathfrak{I}_{\mathbb{K}}(\mathfrak{V}_{\mathbb{L}}(I)) = \sqrt{I}$.*

Proof. Straightforward. □

Definition 6.4. The family of the $\mathbb{K}$-varieties in $\mathbb{L}^n$ are the closed sets of a topology, the $\mathbb{K}$-*Zariski topology* of $\mathbb{L}^n$, it is denoted by $\tau_{\mathbb{K}}$. The topological closure of a set $\mathcal{V}$ with respect to the topology $\tau_{\mathbb{K}}$ is denoted by $\overline{\mathcal{V}^{\mathbb{K}}}$.

Remark 6.5. We recall here some properties of the $\mathbb{K}$-Zariski topology that can be checked in [ZS75b] and will be helpful along the text.

1. $\mathbb{L}^n$ is a compact space that is never Hausdorff for $n > 0$, the intersection of two nonempty open sets is never empty. That is, it is an *irreducible* topological space. It follows that every nonempty open set is dense.
2. If $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{F}$, then $\mathbb{F}^n$ is equipped with the topologies $\tau_{\mathbb{K}}$ and $\tau_{\mathbb{L}}$. In this case $\tau_{\mathbb{K}} \subseteq \tau_{\mathbb{L}}$.
3. If $\mathcal{V} \subseteq \mathbb{L}^n$ is any set, then $\overline{\mathcal{V}^{\mathbb{K}}} = \mathfrak{V}_{\mathbb{L}}(\mathfrak{I}_{\mathbb{K}}(\mathcal{V}))$.
4. The topology $\tau_{\mathbb{K}}$ is not, in general, a T_1 topology, because there are *indistinguishable* elements. For example, in $\mathbb{C}$ with the $\mathbb{Q}$-topology, the closure of $\sqrt[3]{2}$ and the closure of $\sqrt[3]{2}e^{\frac{4\pi i}{3}}$ are both the set $\{\sqrt[3]{2}, \sqrt[3]{2}e^{\frac{2\pi i}{3}}, \sqrt[3]{2}e^{\frac{4\pi i}{3}}\}$.

As in our context the extension of fields are fundamental, we will study a little bit deeper the different Zariski topologies of $\mathbb{F}^n$, specially the differences between the structure of a variety as changing the topology,

The following Lemma shows an easy to check but important fact about the set of generators of an ideal with respect to a field of definition.

Lemma 6.6. *Let $\mathbb{K} \subseteq \mathbb{K}(\alpha)$ be a normal algebraic extension of fields, $[\mathbb{K}(\alpha) : \mathbb{K}] = d$. Let $I = (f_1, \ldots, f_r) \subseteq \mathbb{K}(\alpha)[x_1, \ldots, x_n]$ be an ideal in $\mathbb{K}(\alpha)$ defined over $\mathbb{K}$, $f_j \in \mathbb{K}[x_1, \ldots, x_n]$, $1 \leq j \leq r$. Let*

$$g = \sum_{i=0}^{d-1} g_i \alpha^i \in \mathbb{K}(\alpha)[x_1, \ldots, x_n]$$

be a polynomial, with $g_i \in \mathbb{K}[x_1, \ldots, x_n]$, $0 \leq i \leq d-1$. Then $g \in I$ if and only if $g_i \in I, 0 \leq i \leq d-1$.

Proof. The if implication is trivial. For the other one, Let $\alpha = \alpha_1, \ldots, \alpha_d$ be the conjugates of α in $\mathbb{K}(\alpha)$. Let $\sigma_1, \ldots, \sigma_d$ be $\mathbb{K}$-automorphisms of $\mathbb{K}(\alpha)$ such that $\sigma_j(\alpha) = \alpha_j$, $1 \leq j \leq d$. It is remarkable that they do not need to form a group. Denote by $\sigma_j(h)$ the polynomial obtained by applying the automorphism σ_j to the coefficients of h.

If $g \in I$, then $g = \sum_{j=1}^{r} h_j f_j$ and $\sigma_l(g) = \sum_{j=1}^{r} \sigma_l(h_j)\sigma_l(f_j) = \sum_{j=1}^{r} \sigma_l(h_j) f_j \in I$. On the other hand, $\sigma_l(g) = \sum_{i=0}^{d-1} \sigma_l(\alpha^i) g_i$. Take the linear system

$$\begin{pmatrix} g \\ \sigma_2(g) \\ \vdots \\ \sigma_d(g) \end{pmatrix} = \begin{pmatrix} 1 & \alpha & \alpha^2 & \ldots & \alpha^{d-1} \\ 1 & \sigma_2(\alpha) & \sigma_2(\alpha^2) & \ldots & \sigma_2(\alpha^{d-1}) \\ & & \ldots & & \\ 1 & \sigma_d(\alpha) & \sigma_d(\alpha^2) & \ldots & \sigma_d(\alpha^{d-1}) \end{pmatrix} \begin{pmatrix} g_0 \\ g_1 \\ \vdots \\ g_{d-1} \end{pmatrix}$$

defined by a Vandermonde matrix. As the elements $\sigma_l(\alpha)$ are pairwise different, the linear system is regular and we can express each g_i as a combination of $g, \sigma_2(g), \ldots, \sigma_d(g)$. Hence,

$$(g_0, \ldots, g_{d-1}) = (g, \sigma_2(g), \ldots, \sigma_d(g)) \subseteq I$$

□

Given a $\mathbb{K}$-variety $\mathcal{V}$, we have two different ideals related to it, namely $\mathfrak{I}_{\mathbb{K}}(\mathcal{V})$ and $\mathfrak{I}_{\mathbb{L}}(\mathcal{V})$. In order to compare them, we need some more tools that we present next.

Definition 6.7. Let $f : A \to B$ be a ring homomorphism. Let $I \subseteq A$, $J \subseteq B$ be two ideals, the *extension* I^e of I is the ideal of B generated by $f(I)$. The *contraction* J^c of the ideal J is the ideal $f^{-1}(J)$.

Lemma 6.8. *Let $\mathbb{K}$ be a characteristic zero field and $\mathbb{L}$ an extension of $\mathbb{K}$. Consider the inclusion of rings $\mathbb{K}[x_1, \ldots, x_n] \subseteq \mathbb{L}[x_1, \ldots, x_n]$, Let I, J be two ideals in $\mathbb{K}[x_1, \ldots, x_n]$. Then:*

- *$I^{ec} = I$, every ideal is a contracted ideal.*
- *$(I \cap J)^e = I^e \cap J^e$*
- *$(I : J)^e = I^e : J^e$*
- *If I is radical, then I^e is radical.*

- $\sqrt{I^e} = (\sqrt{I})^e$

Proof. See, [ZS75b], Vol. II, Ch. VII, §11 □

Now, we present our first result concerning the relation of $\mathbb{L}$ and $\mathbb{K}$ varieties. More concretely, what is the relation of the topologies $\tau_{\mathbb{K}}$ and $\tau_{\mathbb{L}}$ in $\mathbb{L}^n$.

Proposition 6.9. *Let $\mathbb{K} \subseteq \mathbb{L}$ be a normal extension of fields. Then*

$$\overline{\mathcal{V}^{\mathbb{K}}} = \bigcup_{\sigma \in Aut(\mathbb{L}|\mathbb{K})} \sigma(\overline{\mathcal{V}^{\mathbb{L}}})$$

where $Aut(\mathbb{L}|\mathbb{K})$ is the set of $\mathbb{K}$-automorphisms of $\mathbb{L}$.

Proof. Write $I = \mathfrak{I}_{\mathbb{K}}(\mathcal{V})$. If $f \in \mathbb{L}[x_1, \ldots, x_n]$, $v \in \mathbb{L}^n$ and $\sigma \in Aut(\mathbb{L}|\mathbb{K})$, let $\sigma(f)$ be the polynomial obtained by applying σ to the coefficients of f. Let $\sigma(v)$ be the point in $\mathbb{L}^n$ obtained by applying σ to each component of v. Then

$$\sigma(\overline{\mathcal{V}^{\mathbb{L}}}) = \{\sigma(v) \mid v \in \overline{\mathcal{V}^{\mathbb{L}}}\} = \{\sigma(v) \mid \forall f \in \mathfrak{I}_{\mathbb{L}}(\mathcal{V}),\ f(v) = 0\}.$$

As $\sigma(f(v)) = \sigma(f)(\sigma(v))$ and $\sigma(f(v)) = 0$ if and only if $f(v) = 0$, the previous set can be described as

$$\begin{aligned} \{\sigma(v) \in \mathbb{L}^n |\ \forall f \in \mathfrak{I}_{\mathbb{L}}(\mathcal{V}), \sigma(f)(\sigma(v)) = 0\} = \\ = \{w \in \mathbb{L}^n \mid \forall f \in \mathfrak{I}_{\mathbb{L}}(\mathcal{V}),\ \sigma(f)(w) = 0\} = \\ = \{w \in \mathbb{L}^n \mid \forall f \in \sigma(\mathfrak{I}_{\mathbb{L}}(\mathcal{V})),\ f(w) = 0\} = \mathfrak{V}_{\mathbb{L}}(\sigma(\mathfrak{I}_{\mathbb{L}}(\mathcal{V}))) \end{aligned}$$

To sum up

$$\sigma(\overline{\mathcal{V}^{\mathbb{L}}}) = \mathfrak{V}_{\mathbb{L}}(\sigma(\mathfrak{I}_{\mathbb{L}}(\mathcal{V}))) \tag{6.1}$$

On the other hand, as $\mathfrak{I}_{\mathbb{L}}(\mathcal{V}) \supseteq I$, then

$$\sigma(\mathfrak{I}_{\mathbb{L}}(\mathcal{V})) \supseteq \sigma(\mathfrak{I}_{\mathbb{K}}(\mathcal{V})) = \mathfrak{I}_{\mathbb{K}}(\mathcal{V})$$

because σ is a $\mathbb{K}$-automorphism and the polynomials over $\mathbb{K}$ stay invariant. Thus, for each $\sigma \in Aut(\mathbb{L}|\mathbb{K})$, $\sigma(\overline{\mathcal{V}^{\mathbb{L}}}) \subseteq \overline{\mathcal{V}^{\mathbb{K}}}$ and we have the containment $\overline{\mathcal{V}^{\mathbb{K}}} \supseteq \bigcup_{\sigma \in Aut(\mathbb{L}|\mathbb{K})} \sigma(\overline{\mathcal{V}^{\mathbb{L}}})$. This containment holds even if $\mathbb{K} \subseteq \mathbb{L}$ is not normal.

Let $f_1, \ldots, f_r \in \mathbb{L}[x_1, \ldots, x_n]$ be generators of $\mathfrak{I}_{\mathbb{L}}(\mathcal{V})$. Let $\alpha \in \mathbb{L}$ be an element such that the algebraic extension $\mathbb{K} \subseteq \mathbb{K}(\alpha)$ is normal and $\mathbb{K}(\alpha)$ contains each coefficient of $f_1, \ldots, f_r$. Let $\sigma(\mathfrak{I}_{\mathbb{L}}(\mathcal{V})) = (\sigma(f_1), \ldots, \sigma(f_r))$. The set $\{\sigma(\alpha) \mid \sigma \in Aut(\mathbb{L}|\mathbb{K})\}$ is finite, because its elements are the conjugates of α. Moreover, as the extension is normal, $\sigma(f_j)$ belongs to $\mathbb{K}(\alpha)[x]$. The values of $\sigma(f_j)$ determine the ideal $\sigma(\mathfrak{I}_{\mathbb{L}}(\mathcal{V}))$, so the set of ideals $\{\sigma(\mathfrak{I}_{\mathbb{L}}(\mathcal{V}))|\ \sigma \in Aut(\mathbb{L}|\mathbb{K})\}$ is also finite. Let $\alpha = \alpha_1, \ldots, \alpha_d$ be the conjugates of α in $\mathbb{K}(\alpha)$ and let $\sigma_1, \ldots, \sigma_d$ be $\mathbb{K}$-automorphisms of $\mathbb{K}(\alpha)$ such that $\sigma_l(\alpha) = \alpha_l$, $1 \leq l \leq d$. We may suppose without loss of generality that these automorphisms are actually $\mathbb{K}$-automorphisms of $\mathbb{L}$ and that σ_1 is the identity. Now, $\bigcup_{\sigma \in Aut(\mathbb{L}|\mathbb{K})} \sigma(\overline{\mathcal{V}^{\mathbb{L}}})$ is, in fact, the finite union

$$\bigcup_{l=1}^{d} \sigma_l(\overline{\mathcal{V}^{\mathbb{L}}}) = \mathfrak{V}_{\mathbb{L}}(\bigcap_{l=1}^{d} \sigma_l(\mathfrak{I}_{\mathbb{L}}(\mathcal{V})))$$

where we have applied the Equality 6.1. For each l, $1 \leq l \leq d$, $\sigma_l(\mathfrak{I}_{\mathbb{L}}(\mathcal{V}))$ contains a set of generators whose coefficients belong to $\mathbb{K}(\alpha)$. By Lemma 6.8, as $(I \cap J)^e = I^e \cap J^e$, the ideal $J = \bigcap_{l=1\ldots d} \sigma_l(\mathfrak{I}_{\mathbb{L}}(\mathcal{V}))$ also has generators with coefficients in $\mathbb{K}(\alpha)$. Let $f \in J$ be one of these generators, f can be written as $f = \sum_{i=0}^{d-1} \alpha^i g_i$, where g_i are polynomials with coefficients in $\mathbb{K}$. By Lemma 6.6

$$g_0, \ldots, g_{d-1} \in J \subseteq \mathfrak{I}_{\mathbb{L}}(\mathcal{V}).$$

As $g_0, \ldots, g_{d-1} \in \mathbb{K}[x_1, \ldots, x_n]$, $g_0, \ldots, g_{d-1} \in \mathfrak{I}_{\mathbb{K}}(\mathcal{V})$. Thus, we deduce that there is a set of polynomials in $\mathbb{K}[x_1, \ldots, x_n]$ that generates J. Thus, $J \subseteq I\mathbb{L}[x_1, \ldots, x_n]$. Applying the operator $\mathfrak{V}_{\mathbb{L}}()$ we obtain that

$$\overline{\mathcal{V}^{\mathbb{K}}} = \mathfrak{V}_{\mathbb{L}}(I) = \mathfrak{V}_{\mathbb{L}}(I\mathbb{L}[x_1, \ldots, x_n]) \subseteq \mathfrak{V}_{\mathbb{L}}(J) = \bigcup_{\sigma \in Aut(\mathbb{L}|\mathbb{K})} \sigma(\overline{\mathcal{V}^{\mathbb{L}}})$$

and we have the other containment. □

Remark 6.10. We cannot eliminate, for this Proposition, the hypothesis of normality for the extension $\mathbb{K} \subseteq \mathbb{L}$, because, in this case, there may not be enough automorphisms to cover every element of $\overline{\mathcal{V}^{\mathbb{K}}}$. Take, for example, $\mathbb{K} = \mathbb{Q}$, $\mathbb{L} = \mathbb{Q}(\sqrt[8]{3}, i)$. Let $\mathcal{V} = \mathfrak{V}_{\mathbb{L}}(x^2 - \sqrt{3}) = \{\sqrt[4]{3}, -\sqrt[4]{3}\}$. Then, $\overline{\mathcal{V}^{\mathbb{Q}}} = \{\sqrt[4]{3}, -\sqrt[4]{3}, i\sqrt[4]{3}, -i\sqrt[4]{3}\}$. Let σ be an arbitrary $\mathbb{Q}$-automorphism of $\mathbb{L}$. Then, $\sigma(\sqrt[8]{3}) \in \{\sqrt[8]{3}, -\sqrt[8]{3}, i\sqrt[8]{3}, -i\sqrt[8]{3}\}$, the roots of $x^8 - 3$ in $\mathbb{Q}(\sqrt[8]{3}, i)$. Hence, $\sigma(\pm\sqrt[4]{3}) = \pm\sigma(\sqrt[8]{3})^2 \in \{\sqrt[4]{3}, -\sqrt[4]{3}\}$ and $\overline{\mathcal{V}^{\mathbb{K}}} \supsetneq \mathcal{V} = \bigcup_{\sigma \in Aut(\mathbb{L}|\mathbb{K})} \sigma(\overline{\mathcal{V}^{\mathbb{L}}})$, so Proposition 6.9 does not hold.

6.2 Irreducibility and Base Field

In this Section we explain some definitions and results usual in the context of algebraic varieties related with the irreducibility of the varieties with respect to the extension of fields.

Definition 6.11. Let $\mathbb{K} \subset \mathbb{L}$ be a extension of fields. A $\mathbb{K}$-variety $\mathcal{V} \subseteq \mathbb{L}^n$ is *irreducible* with respect to $\mathbb{K}$ if the following condition holds: if $\mathcal{V}_1$, $\mathcal{V}_2$ are $\mathbb{K}$-varieties and $\mathcal{V} = \mathcal{V}_1 \cup \mathcal{V}_2$, then $\mathcal{V} = \mathcal{V}_1$ or $\mathcal{V} = \mathcal{V}_2$.

Note that this notion of irreducibility depends on the fields $\mathbb{K}$, $\mathbb{L}$. This is a topological notion that depends on the Zariski topology considered. For example, let $\mathbb{L} = \mathbb{Q}(\sqrt{2})$, the variety $\mathfrak{V}_{\mathbb{Q}(\sqrt{2})}(x^2 - 2y^2)$ consists in the lines $\mathfrak{V}_{\mathbb{Q}(\sqrt{2})}(x - \sqrt{2}y) \cup \mathfrak{V}_{\mathbb{Q}(\sqrt{2})}(x + \sqrt{2}y)$. This variety is not irreducible with respect to $\mathbb{K} = \mathbb{Q}(\sqrt{2})$. However, it is irreducible with respect to $\mathbb{K} = \mathbb{Q}$; on the other hand, if $\mathbb{K} = \mathbb{L} = \mathbb{Q}$, then $\mathfrak{V}_{\mathbb{Q}}(x^2 - 2y^2)$ is just the point $(0, 0)$, which is irreducible.

Proposition 6.12. *Let $\mathbb{K} \subseteq \mathbb{L}$ be an extension of fields and $\mathcal{V} \subseteq \mathbb{L}^n$ a $\mathbb{K}$-variety. Then, $\mathcal{V}$ is irreducible with respect to $\mathbb{K}$ if and only if $I = \mathfrak{I}_{\mathbb{K}}(\mathcal{V})$ is a prime ideal of $\mathbb{K}[x_1, \ldots, x_n]$*

Proof. Suppose that $\mathcal{V}$ is not irreducible with respect to $\mathbb{K}$. Then, there are two $\mathbb{K}$-varieties $\mathcal{V}_1$, $\mathcal{V}_2$ such that $\mathcal{V} = \mathcal{V}_1 \cup \mathcal{V}_2$, $\mathcal{V} \neq \mathcal{V}_1$ and $\mathcal{V} \neq \mathcal{V}_2$. So, there are points $v_1 \in \mathcal{V} \backslash \mathcal{V}_1$, $v_2 \in \mathcal{V} \backslash \mathcal{V}_2$. Hence, there are two polynomials $f_1 \in \mathfrak{I}_{\mathbb{K}}(\mathcal{V}_1)$ and $f_2 \in \mathfrak{I}_{\mathbb{K}}(\mathcal{V}_2)$, with $f_1(v_1) \neq 0$, $f_2(v_2) \neq 0$ and hence $f_1,\ f_2 \notin \mathfrak{I}_{\mathbb{K}}(\mathcal{V})$. But $f_1 f_2 \in \mathfrak{I}_{\mathbb{K}}(\mathcal{V})$, because it vanishes at every point of $\mathcal{V}$. We conclude that $\mathfrak{I}_{\mathbb{K}}(\mathcal{V})$ is not a prime ideal.

For the reciprocal, suppose that $\mathcal{V}$ is irreducible and let f and g be two polynomials such that $fg \in I$. Let $\mathcal{V}_1 = \mathfrak{V}_{\mathbb{K}}(I + f) \subseteq \mathcal{V}$, $\mathcal{V}_2 = \mathfrak{V}_{\mathbb{K}}(I + g) \subseteq \mathcal{V}$. If $v \in \mathcal{V}$, then $fg(v) = 0$, so $f(v) = 0$ or $g(v) = 0$. Hence, $\mathcal{V} = \mathcal{V}_1 \cup \mathcal{V}_2$ and, as $\mathcal{V}$ is irreducible, it must coincide with one of them. Suppose that $\mathcal{V} = \mathcal{V}_1$. Then, $I = \mathfrak{I}_{\mathbb{K}}(\mathcal{V}) = \mathfrak{I}_{\mathbb{K}}(\mathfrak{V}_{\mathbb{K}}(I+f)) \supseteq I + f$ and $f \in I$, hence I is a prime ideal. □

We want to remark that this Proposition does not mean that if $\mathcal{V} = \mathfrak{V}_{\mathbb{L}}(I)$, where I is a prime ideal of $\mathbb{K}[x_1, \ldots, x_n]$, then $\mathcal{V}$ is irreducible. For example, let $\mathbb{K} = \mathbb{L} = \mathbb{R}$ be the field of the reals. Let $\mathcal{V} = \mathfrak{V}_{\mathbb{R}}(x^2(x-1)^2 + y^2)$. Then $\mathcal{V} = \{(0,0)\} \cup \{(1,0)\}$ is not an irreducible variety, but $(x^2(x-1)^2 + y^2)\mathbb{R}[x, y]$ is a prime ideal, because the polynomial is irreducible over $\mathbb{R}$.

6.3 $\mathbb{K}$-definability

In this Section we are looking for conditions that determines if a given field $\mathbb{K}$ is a field of definition of a $\mathbb{L}$-variety $\mathcal{V} \subseteq \mathbb{F}^n$ from an ideal I that defines a variety $\mathcal{V}$. Next, we are proving that the ideal $\mathfrak{I}_{\mathbb{F}}(\mathcal{V})$ contains the necessary information to deduce that a field is a field of definition of a variety.

Proposition 6.13. *Let $\mathbb{K} \subseteq \mathbb{F}$ be a field extension, where $\mathbb{F}$ is algebraically closed. Then $\mathbb{K}$ is a field of definition of a $\mathbb{F}$-variety $\mathcal{V}$ if and only if the ideal $\mathfrak{I}_{\mathbb{F}}(\mathcal{V})$ can be generated by elements of $\mathbb{K}[x_1, \ldots, x_n]$.*

Proof. If $\mathfrak{I}_{\mathbb{F}}(\mathcal{V}) = (f_1, \ldots, f_r) \subseteq \mathbb{F}[x_1, \ldots, x_n]$, where $f_1, \ldots, f_r$ are polynomials in $\mathbb{K}[x_1, \ldots, x_n]$, then $\mathfrak{V}_{\mathbb{F}}(f_1, \ldots, f_r) = \mathfrak{V}_{\mathbb{F}}(\mathfrak{I}_{\mathbb{F}}(\mathcal{V})) = \mathcal{V}$, so $\mathbb{K}$ is a field of definition of $\mathcal{V}$ considering $I = (f_1, \ldots, f_r)$.

For the reciprocal, let $I = \mathfrak{I}_{\mathbb{F}}(\mathcal{V})$ and suppose that $J \subseteq \mathbb{K}[x_1, \ldots, x_n]$ is an ideal such that $\mathfrak{V}_{\mathbb{F}}(J) = \mathcal{V}$. We may suppose, without loss of generality, that J is a radical ideal. Then, $\mathfrak{V}_{\mathbb{F}}(J^e) = \mathcal{V}$, where J^e is the extended ideal of J with respect to the canonical inclusion $\mathbb{K}[x_1, \ldots, x_n] \hookrightarrow \mathbb{F}[x_1, \ldots, x_n]$. By Hilbert's Nullstellensatz, $\sqrt{J^e} = I$, and, by Lemma 6.8, J^e is a radical ideal. Hence, $I = \sqrt{J^e} = J^e$ has a set of generators in $\mathbb{K}[x_1, \ldots, x_n]$. □

Remark 6.14.

- Let $\mathcal{V}$ be an $\mathbb{F}$-variety and consider the extension field $\mathbb{K} \subseteq \mathbb{F}$. Consider the ring extension $\mathbb{K}[x_1, \ldots, x_n] \subseteq \mathbb{F}[x_1, \ldots, x_n]$. Then, from Definitions 6.1 and 6.2, we have that

$$\mathfrak{I}_{\mathbb{K}}(\mathcal{V}) = \{f \in \mathbb{K}[x_1, \ldots, x_n] \mid \forall (v_1, \ldots, v_n) \in \mathcal{V},\ f(v_1, \ldots, v_n) = 0\} =$$

$$= \mathfrak{I}_{\mathbb{F}}(\mathcal{V}) \cap \mathbb{K}[x_1, \ldots, x_n]$$

that is, $\mathfrak{I}_{\mathbb{K}}(\mathcal{V})$ is the contraction of the ideal $\mathfrak{I}_{\mathbb{F}}(\mathcal{V})$ by the inclusion of rings $\mathbb{K}[x_1, \ldots, x_n] \subseteq \mathbb{F}[x_1, \ldots, x_n]$.

- From Lemma 6.8, every ideal in $\mathbb{K}[x_1, \ldots, x_n]$ is a contracted ideal with respect to the extension $\mathbb{K}[x_1, \ldots, x_n] \subseteq \mathbb{F}[x_1, \ldots, x_n]$. In the language of Commutative Algebra, Proposition 6.13 can be written as: *A $\mathbb{F}$-variety $\mathcal{V}$ is a $\mathbb{K}$-variety if and only is the ideal $\mathfrak{I}_{\mathbb{F}}(\mathcal{V})$ is a extended ideal for the inclusion $\mathbb{K}[x_1, \ldots, x_n] \subseteq \mathbb{F}[x_1, \ldots, x_n]$, if and only if $\mathfrak{I}_{\mathbb{F}}(\mathcal{V})$ is the extended ideal of $\mathfrak{I}_{\mathbb{K}}(\mathcal{V})$ for the previous inclusion.*

- The hypothesis that $\mathbb{F}$ is algebraically closed in Proposition 6.13 is necessary. For example, let $\mathbb{K} = \mathbb{Q}$, $\mathbb{F} = \mathbb{Q}(\sqrt[3]{2})$. $\mathcal{V} = \{\sqrt[3]{2}\}$ is a $\mathbb{Q}$-variety, because $\mathcal{V} = \mathfrak{V}_{\mathbb{F}}(x^3 - 2)$. However, $\mathfrak{I}_{\mathbb{F}}(\mathcal{V}) = (x - \sqrt[3]{2})$ is an ideal that cannot be generated by polynomials with coefficients in $\mathbb{Q}$.

Recall that our fields are all of characteristic zero, so the algebraic extensions considered are always separable.

Definition 6.15. A extension of fields $\mathbb{K} \subseteq \mathbb{L}$ is *regular* ([ZS75b], [Sam67]) if the extension is separable and every element of $\mathbb{L}$ that is algebraic over $\mathbb{K}$ belongs to $\mathbb{K}$. That is, if $\mathbb{K}$ is algebraically closed in $\mathbb{L}$.

This Theorem provides another characterisation of the fields of definition of a given variety $\mathcal{V}$.

Theorem 6.16. *Let $\mathbb{K}$ be a field, $\mathbb{F}$ its algebraic closure, $\mathcal{V}$ an irreducible $\mathbb{F}$-variety in $\mathbb{F}^n$, let $I = \mathfrak{I}_{\mathbb{K}}(\mathcal{V})$ (I is a prime ideal, because it is the contraction of the prime ideal $\mathfrak{I}_{\mathbb{F}}(\mathcal{V})$). Let T be the field of fractions of*

$$\frac{\mathbb{K}[x_1, \ldots, x_n]}{I}.$$

They are equivalent:

1. *$\mathbb{K}$ is a field of definition of $\mathcal{V}$.*
2. *$I\mathbb{F}[x_1, \ldots, x_n]$ is a prime ideal.*
3. *The extension $\mathbb{K} \subseteq T$ is regular.*
4. *For every field $\mathbb{L}$, the extension ideal $I\mathbb{L}[x_1, \ldots, x_n]$ is a prime ideal. In this case, we say that I is absolutely prime*

Proof. First, from [ZS75b], Theorem 39, page 230 we obtain the equivalence 3) $\Leftrightarrow$ 4). Let us prove the rest of the implications:
1)$\Rightarrow$2)
If $\mathbb{K}$ is a field of definition of $\mathcal{V}$, by Proposition 6.13, $\mathfrak{I}_{\mathbb{F}}(\mathcal{V})$ is generated by polynomials in $\mathbb{K}[x_1, \ldots, x_n]$, so it is an extended ideal (with respect to the inclusion $\mathbb{K}[x_1, \ldots, x_n] \hookrightarrow$

$\mathbb{F}[x_1,\ldots,x_n]$). As $\mathcal{V}$ is irreducible with respect to $\mathbb{F}$, the ideal $\mathfrak{I}_{\mathbb{F}}(\mathcal{V})$ is prime and 2) holds.
2)$\Rightarrow$ 3)
(c.f. [ZS75b]) As, $I^e = I\mathbb{F}[x_1,\ldots,x_n]$ is a prime ideal, then we have the following inclusion

$$T \longrightarrow \mathrm{Frac}\left(\frac{\mathbb{F}[x_1,\ldots,x_n]}{I\mathbb{F}[x_1,\ldots,x_n]}\right) = \mathbb{F}(x_1+I^e,\ldots,x_n+I^e) \tag{6.2}$$

that sends

$$(A(\overline{x})+I)/(B(\overline{x})+I) \mapsto (A(\overline{x})+I^e)/(B(\overline{x})+I^e)$$

Note that, if $A(\overline{x}) \in \mathbb{K}[x_1,\ldots,x_n]$ and $A(\overline{x}) \in I^e$, so $A(\overline{x}) \in I^{ec} = I$ and the inclusion 6.2 is well defined. Let $a \in T$ and let

$$f(y) = y^d + b_{d-1}y^{d-1} + \ldots + b_1 y + b_0,\ b_i \in \mathbb{K}$$

be its minimal polynomial over $\mathbb{K}$. Then, f splits in $\mathbb{F}[y]$ as

$$f(y) = \prod_{i=1}^{d}(y-\gamma_i)$$

and there are $A(\overline{x}), B(\overline{x}) \in \mathbb{K}[x_1,\ldots,x_n]$ such that $a = (A(\overline{x})+I)/(B(\overline{x})+I)$; in particular, $B(\overline{x}) \notin I$. We can make substitution in the minimal polynomial of a, eliminate denominators and compute the image of the result by the previous inclusion. We obtain

$$\prod_{i=1}^{d}((A(\overline{x})+I^e) - (\gamma_i B(\overline{x})+I^e)) = 0$$

That is,

$$\prod_{i=1}^{d}(A(\overline{x}) - \gamma_i B(\overline{x})) \in I^e$$

By hypothesis, I^e is prime and, hence, it contains $A(\overline{x}) - \gamma_i B(\overline{x})$ for some i, we can suppose that $i = 1$. Let σ_l be a $\mathbb{K}$-automorphism of $\mathbb{F}$ that send γ_1 to γ_l. This automorphism extends naturally to $\mathbb{F}[x_1,\ldots,x_n]$ and, as $I\mathbb{F}[x_1,\ldots,x_n]$ is generated by polynomials in $\mathbb{K}$, $I\mathbb{F}[x_1,\ldots,x_n]$ is globally invariant for the automorphisms σ_l. We deduce that

$$A(\overline{x}) - \gamma_l B(\overline{x}) \in I\mathbb{F}[x_1,\ldots,x_n],\ l = 1,\ldots,d$$

Suppose now that $d \geq 2$. Then, $A(\overline{x}) - \gamma_1 B(\overline{x}) \in I\mathbb{F}[x_1,\ldots,x_n]$, $A(\overline{x}) - \gamma_2 B(\overline{x}) \in I\mathbb{F}[x_1,\ldots,x_n]$. Subtracting these polynomials and multiplying by a suitable constant, $B(\overline{x}) \in I\mathbb{F}[x_1,\ldots,x_n] \subseteq \mathfrak{I}_{\mathbb{F}}(\mathcal{V})$. Hence, $B(\overline{x})$ is a polynomial in $\mathbb{K}[x_1,\ldots,x_n] \cap \mathfrak{I}_{\mathbb{F}}(\mathcal{V}) = I$ (see Remark 6.14). It follows that $B(\overline{x}) \in I$, which is a contradiction. So, $d = 1$ and the minimal polynomial of a over $\mathbb{K}$ is $y - \gamma_1$. That is, $a \in \mathbb{K}$ and the extension is regular.

4)⇒1)
From Proposition 6.9,

$$\mathfrak{V}_{\mathbb{F}}(I\mathbb{F}[x_1,\ldots,x_n]) = \overline{\mathcal{V}^{\mathbb{K}}} = \bigcup_{\sigma\in Aut(\mathbb{F}|\mathbb{K})} \sigma(\mathcal{V})$$

where the union is finite, it is enough to take a finite subset $\sigma_1,\ldots,\sigma_d$ of $Aut(\mathbb{F}|\mathbb{K})$, so

$$\overline{\mathcal{V}^{\mathbb{K}}} = \bigcup_{l=1}^{d} \sigma_l(\mathcal{V})$$

By hypothesis, $I\mathbb{F}[x_1,\ldots,x_n]$ is prime, so $\overline{\mathcal{V}^{\mathbb{K}}}$ is an irreducible variety with respect to $\mathbb{F}$ that has been written as the union of finitely many $\mathbb{F}$-varieties, so it must be one of them. Hence, for an index l, $\overline{\mathcal{V}^{\mathbb{K}}} = \sigma_l(\mathcal{V})$. So, $\mathcal{V} = \sigma_l^{-1}(\overline{\mathcal{V}^{\mathbb{K}}})$. But $\overline{\mathcal{V}^{\mathbb{K}}}$ is a $\mathbb{K}$-variety and globally invariant by the $\mathbb{K}$-automorphism σ_l. Thus, $\mathcal{V} = \overline{\mathcal{V}^{\mathbb{K}}}$ and $\mathcal{V}$ is a $\mathbb{K}$-variety. □

This Theorem provides several criteria to decide if a field $\mathbb{K}$ is a field of definition of a variety $\mathcal{V}$. Now we show that, even if there may be many field of definition, there is a minimum field of definition of any variety.

Theorem 6.17. *Let $\mathcal{V}$ be a $\mathbb{K}$-variety. Then, there is a minimum field of definition of $\mathcal{V}$. That is, there is a field $\mathbb{K}$ that is a field of definition of $\mathcal{V}$ and such that, if $\mathbb{L}$ is another field of definition of $\mathcal{V}$, then $\mathbb{K}\subseteq\mathbb{L}$.*

Proof. Let $\mathbb{F}$ be an algebraic closure of $\mathbb{K}$, $I = \mathfrak{I}_{\mathbb{F}}(\mathcal{V})$, let G be the reduced Gröbner basis of the ideal I with respect to any monomial ordering. Let Σ be the set of coefficients of the polynomials of G. Then, we affirm that $\mathbb{Q}(\Sigma)$ is the minimum field of definition of $\mathcal{V}$. In fact, as every coefficient of G is in $\mathbb{Q}(\Sigma)$ and G generates I, then $\mathbb{Q}(\Sigma)$ is a field of definition of $\mathcal{V}$. Let $\mathbb{L}$ be any field of definition of $\mathcal{V}$, then, there are polynomials $f_1,\ldots,f_r$ with coefficients in $\mathbb{L}$ that generate I. If the reduced Gröbner basis of I is computed from this set of generators $f_1,\ldots,f_r$ for the same monomial ordering as before, the result will be again G, because the reduced Gröbner basis is unique for a fixed ordering. Furthermore, this basis can be obtained by operations in the field $\mathbb{L}$ alone. It follows that $\mathbb{Q}(\Sigma)\subseteq\mathbb{L}$ and $\mathbb{Q}(\Sigma)$ is the minimum field of definition of $\mathcal{V}$. □

6.4 $\mathbb{K}$-birationality

The fundamental equivalence in the study of algebraic varieties is birationality. In this Section we present the notion of $\mathbb{K}$-birationality. This is given as a classical birational map that is defined by rational functions defined over $\mathbb{K}$. Still, there are several technical results that have to be solved.

Definition 6.18. Let $\mathbb{K}\subseteq\mathbb{L}\subseteq\mathbb{F}$ be a chain of fields, let $\mathcal{V}\subseteq\mathbb{F}^n$ be a $\mathbb{L}$-variety irreducible with respect to $\mathbb{L}$, $\mathfrak{I}_{\mathbb{L}}(\mathcal{V})$ is a prime ideal of $\mathbb{L}[x_1,\ldots,x_n]$, then $\mathfrak{I}_{\mathbb{K}}(\mathcal{V}) =$

$\mathfrak{I}_{\mathbb{L}}(\mathcal{V}) \cap \mathbb{K}[x_1, \ldots, x_n]$ is also a prime ideal of $\mathbb{K}[x_1, \ldots, x_n]$ and we can construct the integer domain

$$\mathbb{K}[\mathcal{V}] = \frac{\mathbb{K}[x_1, \ldots, x_n]}{\mathfrak{I}_{\mathbb{K}}(\mathcal{V})}.$$

This is the *ring of* $\mathbb{K}$*-polynomial functions* of $\mathcal{V}$. Its field of fractions $\mathbb{K}(\mathcal{V})$ is the *field of* $\mathbb{K}$*-rational functions* of $\mathcal{V}$.

$\mathbb{L}$ is naturally included in $\mathbb{L}(\mathcal{V})$. The transcendence degree of $\mathbb{L}(\mathcal{V})$ over $\mathbb{L}$ is the *dimension* of $\mathcal{V}$. If $\mathcal{V}$ is not irreducible with respect to $\mathbb{L}$, the dimension of $\mathcal{V}$ is the maximum of the dimensions of its $\mathbb{L}$-components. This dimension does not depend on the concrete field of definition $\mathbb{L}$.

Let $\mathcal{V} \subseteq \mathbb{F}^n$ be a variety irreducible with respect to $\mathbb{F}$, and let $\mathbb{K} \subseteq \mathbb{F}$ be an extension of fields. By Remark 6.14, we have that $\mathfrak{I}_{\mathbb{K}}(\mathcal{V}) = \mathfrak{I}_{\mathbb{F}}(\mathcal{V})^c$ in the extension $\mathbb{K}[x_1, \ldots, x_n] \subseteq \mathbb{F}[x_1, \ldots, x_n]$. The map

$$\begin{array}{ccc} \mathbb{K}[\mathcal{V}] & \longrightarrow & \mathbb{F}[\mathcal{V}] \\ f + I & \mapsto & f + \mathfrak{I}_{\mathbb{F}}(\mathcal{V}) \end{array}$$

where $I = \mathfrak{I}_{\mathbb{K}}(\mathcal{V})$, is well defined and is injective. Hence, this map induces an inclusion of the field of rational functions $\mathbb{K}(\mathcal{V})$ into $\mathbb{F}(\mathcal{V})$. By this map, every $\mathbb{K}$-rational function of $\mathcal{V}$ can be considered as a $\mathbb{F}$-rational function of $\mathcal{V}$ that admits a representation by polynomials in $\mathbb{K}[x_1, \ldots, x_n]$.

Now we interpret the $\mathbb{K}$-rational function $\phi \in \mathbb{K}(\mathcal{V}) \subseteq \mathbb{F}(\mathcal{V})$ as a map on a subset of $\mathcal{V}$.

Definition 6.19. Let $\mathcal{V}$ be a variety irreducible with respect to $\mathbb{F}$. Let $\phi \in \mathbb{K}(\mathcal{V})$ be a rational function. Then, the *domain* of ϕ denoted by $Dom(\phi)$ is the set:

$$Dom(\phi) = \{v \in \mathcal{V} \subseteq \mathbb{F}^n \mid \exists\ p/q = \phi \in \mathbb{F}(\mathcal{V}),\ q(v) \neq 0\}$$

So the $\mathbb{K}$-rational function can be interpreted as a map

$$\phi\ :\ Dom(\phi) \longrightarrow \mathbb{F}$$

such that, if $v \in Dom(\phi)$, let p/q be any representation of ϕ with $q(v) \neq 0$, we define $\phi(v) = p(v)/q(v)$. This definition does not depend on the representation of ϕ chosen. If p_1/q_1, p_2/q_2 are two representation of ϕ in $\mathbb{F}(\mathcal{V})$ such that $q_1(v) \neq 0$, $q_2(v) \neq 0$. Then, $p_1q_2 - p_2q_1 \in \mathfrak{I}_{\mathbb{F}}(\mathcal{V})$ so the polynomial vanishes at v, $p_1(v)q_2(v) - p_2(v)q_1(v) = 0$. From this, $p_1(v)/q_1(v) = p_2(v)/q_2(v)$ and $\phi(v)$ is well defined.

If ϕ is a rational function, then there is a representation of ϕ as p/q. As $q \notin \mathfrak{I}_{\mathbb{F}}(\mathcal{V})$, there is at least a point $v \in \mathcal{V}$ with $q(v) \neq 0$. In particular, $Dom(\phi)$ is never empty. Moreover, if $v \in Dom(\phi)$ and p/q is a representation of ϕ defined in v, then ϕ is defined in $\mathcal{V} \cap (\mathbb{F}^n \setminus \mathfrak{V}_{\mathbb{F}}(q))$, a nonempty open set of $\mathcal{V}$ for the topology $\tau_{\mathbb{F}}$. Hence, $Dom(\phi)$ is a nonempty open subset of $\mathcal{V}$.

Before showing the notion of $\mathbb{K}$-birationality, we present a Lemma that is interesting on its own.

Lemma 6.20. *Let $\mathcal{V} \subseteq \mathbb{F}^{n+m}$ be a $\mathbb{K}$-variety, $\mathbb{K} \subseteq \mathbb{F}$, $\mathbb{F}$ algebraically closed, $\mathfrak{I}_{\mathbb{F}}(\mathcal{V}) \subseteq \mathbb{F}[x_1, \ldots, x_n, y_1, \ldots, y_m]$. Let Π be the projection*

$$\begin{array}{rccc} \Pi : & \mathbb{F}^{n+m} & \longrightarrow & \mathbb{F}^m \\ & (v_1, \ldots, v_n, w_1, \ldots, w_m) & \mapsto & (w_1, \ldots, w_m) \end{array}$$

Let $\mathcal{W} = \overline{\Pi(\mathcal{V})^{\mathbb{F}}}$. Then, $\mathcal{W}$ is a $\mathbb{K}$-variety and

$$\mathfrak{I}_{\mathbb{F}}(\mathcal{W}) = \mathfrak{I}_{\mathbb{F}}(\mathcal{V}) \cap \mathbb{F}[y_1, \ldots, y_m]$$

Proof. It is well know (c.f. [CLO97]) that in this case

$$\mathfrak{I}_{\mathbb{F}}(\mathcal{W}) = \mathfrak{I}_{\mathbb{F}}(\mathcal{V}) \cap \mathbb{F}[y_1, \ldots, y_m]$$

Moreover, if $\{f_1, \ldots, f_r\}$ is a Gröbner basis of $\mathfrak{I}_{\mathbb{F}}(\mathcal{V})$ with respect to a block ordering $[x] > [y]$, then a set of generator of $\mathfrak{I}_{\mathbb{F}}(\mathcal{W})$ is $\{f_1, \ldots, f_r\} \cap \mathbb{F}[y_1, \ldots, y_m]$. Since $\mathbb{K}$ is a field of definition of $\mathcal{V}$, by Proposition 6.13 there is a set of generators $\{g_1, \ldots, g_s\}$ of $\mathfrak{I}_{\mathbb{F}}(\mathcal{V})$ with coefficients in $\mathbb{K}$. By the Gröbner basis algorithm, we can compute a set of generators of $\mathfrak{I}_{\mathbb{F}}(\mathcal{W})$ with coefficients in $\mathbb{K}$. Again, by Proposition 6.13, $\mathbb{K}$ is a field of definition of $\mathcal{W}$. □

Definition 6.21. Let $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{F}$ be a chain of fields and let $\mathcal{V} \subseteq \mathbb{F}^n$, $\mathcal{W} \subseteq \mathbb{F}^m$ be two $\mathbb{L}$-varieties irreducible with respect to $\mathbb{L}$. The varieties $\mathcal{V}$ and $\mathcal{W}$ are $\mathbb{K}$-*birational* if there are $\phi_1, \ldots, \phi_m \subseteq \mathbb{K}(\mathcal{V})$, $\psi_1, \ldots, \psi_n \subseteq \mathbb{K}(\mathcal{W})$ such that:

1. $\phi_1, \ldots, \phi_m$ are defined on a nonempty open subset $Dom(\Phi)$ of $(\mathcal{V}, \tau_{\mathbb{L}}|_{\mathcal{V}})$
2. $\psi_1, \ldots, \psi_n$ are defined on a nonempty open subset $Dom(\Psi)$ of $(\mathcal{W}, \tau_{\mathbb{L}}|_{\mathcal{W}})$
3. For every point $v = (v_1, \ldots, v_n) \in \mathcal{V}$ such that Φ is defined, we have that $\Phi(v) = (\phi_1(v), \ldots, \phi_m(v)) \in \mathcal{W}$ and the image $\Phi(Dom(\Phi))$ is a dense subset of $(\mathcal{W}, \tau_{\mathbb{L}}|_{\mathcal{W}})$.
4. For every point $w = (w_1, \ldots, w_m) \in \mathcal{W}$ where Ψ is defined, its image $\Psi(w) = (\psi_1(w), \ldots, \psi_n(w)) \in \mathcal{V}$ and the image $\Psi(Dom(\Psi))$ is a dense subset of $(\mathcal{V}, \tau_{\mathbb{L}}|_{\mathcal{V}})$.
5. If $v \in Dom(\Phi)$ and $\Phi(v) \in Dom(\Psi)$ then $\Psi(\Phi(v)) = v$
6. If $w \in Dom(\Psi)$ and $\Psi(w) \in Dom(\Phi)$ then $\Phi(\Psi(w)) = w$

Such a function $\Phi = (\phi_1, \ldots, \phi_m)$ is called a $\mathbb{K}$-*birational map* between $\mathcal{V}$ and $\mathcal{W}$.

This definition tries to be as general as possible. Hence, it is not asked that $\mathcal{V}$ or $\mathcal{W}$ are defined over $\mathbb{K}$, neither that they are irreducible over $\mathbb{F}$.

Theorem 6.22. *Let $\mathcal{V} \subseteq \mathbb{F}^n$, $\mathcal{W} \subseteq \mathbb{F}^m$ be two $\mathbb{F}$-varieties, $\mathbb{F}$ algebraically closed. Let $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{F}$ be an extension of fields and suppose that $\mathcal{V}$, $\mathcal{W}$ are $\mathbb{L}$-varieties irreducible with respect to $\mathbb{L}$ and that they are $\mathbb{K}$-birational by (Φ, Ψ). Then, $\mathbb{K}$ is a field of definition of $\mathcal{V}$ if and only if it is a field of definition of $\mathcal{W}$.*

Proof. By symmetry, it is enough to prove that if $\mathcal{V}$ is a $\mathbb{K}$-variety, so it is $\mathcal{W}$.

Let $\Phi = (\phi_1, \ldots, \phi_m) \in \mathbb{K}(\mathcal{V})$, $\Psi = (\psi_1, \ldots, \psi_n) \in \mathbb{K}(\mathcal{W})$ be the birational map between the varieties. Let $f_1, \ldots, f_r$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$ generating $\mathfrak{I}_{\mathbb{F}}(\mathcal{V})$ let p_j/r_j be a representation of ϕ_j with coefficients over $\mathbb{K}$. We define the ideal

$$J = (f_1, \ldots, f_m, q_1 y_1 - p_1, \ldots, q_m y_m - p_m, q_1 \ldots q_m z - 1)$$

in the ring $\mathbb{F}[x_1, \ldots, x_n, y_1, \ldots, y_m, z]$, but generated over $\mathbb{K}$. Let $\widetilde{\mathcal{W}} = \mathfrak{V}_{\mathbb{F}}(J) \subseteq \mathbb{F}^{n+m+1}$. It happens that $\widetilde{\mathcal{W}}$ contains the points $(\overline{x}, \overline{y}, h)$ such that $\overline{x} \in \mathcal{V}$, $\overline{y} = \Phi(\overline{x})$ and $0 \neq h = \prod_{j=1}^{m} q_j(\overline{x})$. Define the projection

$$\begin{array}{rccc} \Pi: & \mathbb{F}^{n+m+1} & \longrightarrow & \mathbb{F}^m \\ & (\overline{x}, \overline{y}, z) & \mapsto & \overline{y} \end{array}$$

Then,

$$\Pi(\widetilde{\mathcal{W}}) = \{\overline{y} \in \mathbb{F}^m \mid \exists\, \overline{x} \in \mathcal{V}, \overline{x} \notin \cup_{j=1\ldots m} \mathfrak{V}_{\mathbb{F}}(q_j), \Phi(\overline{x}) = \overline{y}\} \subseteq Im(\Phi)$$

is a subset of $\mathcal{W}$. Moreover, from Lemma 6.20, $\overline{\Pi(\widetilde{\mathcal{W}})^{\mathbb{F}}}$ is a $\mathbb{K}$-variety and $\overline{\Pi(\widetilde{\mathcal{W}})^{\mathbb{F}}} = \overline{\Pi(\widetilde{\mathcal{W}})^{\mathbb{K}}} = \overline{\Pi(\widetilde{\mathcal{W}})^{\mathbb{L}}}$. To prove that $\mathcal{W}$ is a $\mathbb{K}$-variety, it is enough to prove that $\Pi(\widetilde{\mathcal{W}})$ is $\mathbb{L}$-dense in $\mathcal{W}$. We already have proved the containment $\Pi(\widetilde{\mathcal{W}}) \subseteq Im(\Phi) \subseteq \mathcal{W}$. Thus, it suffices to prove that $\mathfrak{I}_{\mathbb{L}}(\Pi(\widetilde{\mathcal{W}})), \subseteq \mathfrak{I}_{\mathbb{L}}(Im(\Phi))$, the result will follow applying the operator $\mathfrak{V}_{\mathbb{L}}()$. Let $f \in \mathfrak{I}_{\mathbb{L}}(\Pi(\widetilde{\mathcal{W}}))$ and consider the rational function $f(\phi_1, \ldots, \phi_m) \in \mathbb{L}(\mathcal{V})$. The subset $\mathcal{V} \backslash \mathfrak{V}_{\mathbb{F}}(q_1, \ldots, q_m)$ is a nonempty open subset of $\mathcal{V}$, so it is dense. Let $v \in \mathcal{V} \backslash \mathfrak{V}_{\mathbb{F}}(q_1, \ldots, q_m)$, then $(\phi_1(v), \ldots, \phi_m(v)) \in \Pi(\widetilde{\mathcal{W}})$, so $f(\phi_1, \ldots, \phi_m)(v) = f(\phi_1(v), \ldots, \phi_m(v)) = 0$. This equality holds in a dense subset of $\mathcal{V}$, so $f(\phi_1, \ldots, \phi_m) = 0 \in \mathbb{L}(\mathcal{V})$. Now, if $v \in Dom(\Phi)$, then $f(\phi_1(v), \ldots, \phi_m(v)) = 0$. Hence, f vanishes in $Im(\Phi)$ and $f \in \mathfrak{I}_{\mathbb{L}}(Im(\Phi))$ □

Proposition 6.23. *Let $\mathcal{V} \subseteq \mathbb{F}^n$, $\mathcal{W} \subseteq \mathbb{F}^m$ be two $\mathbb{L}$-varieties irreducible with respect to $\mathbb{L}$, $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{F}$ a chain of fields, let $\mathbb{L}[\mathcal{V}] = \mathbb{L}[x_1, \ldots, x_n]/\mathfrak{I}_{\mathbb{L}}(\mathcal{V})$, $\mathbb{L}[\mathcal{W}] = \mathbb{L}[y_1, \ldots, y_m]/\mathfrak{I}_{\mathbb{L}}(\mathcal{W})$. Then, $\mathcal{V}$, $\mathcal{W}$ are $\mathbb{K}$-birational if and only if $\mathbb{L}(\mathcal{V}) \cong \mathbb{L}(\mathcal{W})$ are isomorphic, where the isomorphisms $f : \mathbb{L}(\mathcal{V}) \longrightarrow \mathbb{L}(\mathcal{W})$, $g : \mathbb{L}(\mathcal{W}) \longrightarrow \mathbb{L}(\mathcal{V})$ are such that, if we denote*

$$\overline{x_j} = x_j + \mathfrak{I}_{\mathbb{L}}(\mathcal{V}) \in \mathbb{L}(\mathcal{V}), \overline{y_i} = y_i + \mathfrak{I}_{\mathbb{L}}(\mathcal{W}) \in \mathbb{L}(\mathcal{W}),$$

then

$$f(\overline{x_j}) = \psi_j \in \mathbb{K}(\mathcal{W}) \subseteq \mathbb{L}(\mathcal{W}),\ 1 \leq j \leq n,$$

$$g(\overline{y_i}) = \phi_i \in \mathbb{K}(\mathcal{V}) \subseteq \mathbb{L}(\mathcal{V}),\ 1 \leq i \leq m,$$

In this case, $\Phi = (\phi_1, \ldots, \phi_m)$, $\Psi(\psi_1, \ldots, \psi_n)$ are $\mathbb{K}$-birational maps between $\mathcal{V}$ and $\mathcal{W}$.

Proof. From [Sha94], Chapter I, page. 28, we have the classical result that two varieties $\mathcal{V}$, $\mathcal{W}$ are birational in the classical sense if and only if its field of functions $\mathbb{L}(\mathcal{V})$, $\mathbb{L}(\mathcal{W})$ are isomorphic, where the isomorphisms are given by

$$\begin{array}{ccc} \mathbb{L}(\mathcal{V}) & \Leftrightarrow & \mathbb{L}(\mathcal{W}) \\ \overline{x_j} & \rightarrow & \psi_j \\ \phi_i & \leftarrow & \overline{y_i} \end{array}$$

Hence, $\mathcal{V}$, $\mathcal{W}$ are $\mathbb{K}$-birational if and only if $\phi_i \in \mathbb{K}(\mathcal{V})$, $\psi_j \in \mathbb{K}(\mathcal{W})$. □

Remark 6.24. This Proposition and the results about $\mathbb{K}$-birationality seem artificial. In the literature, two varieties $\mathcal{V}$ and $\mathcal{W}$ are birational if and only if the fields of rational functions $\mathbb{L}(\mathcal{V})$, $\mathbb{L}(\mathcal{W})$ are isomorphic. In our case, we want to prove that if $\mathcal{V}$ is a $\mathbb{K}$-variety and the map is birational from $\mathcal{V}$ to $\mathcal{W}$ is defined by rational functions defined over $\mathbb{K}$, then $\mathcal{W}$ is a $\mathbb{K}$-variety. Our definition of $\mathbb{K}$-birationality is adequate to this property. If one wants to give an equivalent condition to $\mathbb{K}$-birationality, it is not enough that their fields of rational functions are isomorphic. In fact, it is neither sufficient that $\mathbb{L}(\mathcal{V}) \cong \mathbb{L}(\mathcal{W})$ and $\mathbb{K}(\mathcal{V}) \cong \mathbb{K}(\mathcal{W})$, as proves the following example.

Let $\mathcal{V} = \{\sqrt[3]{2}\}$, $\mathcal{W} = \{\sqrt[3]{2}\xi\}$ where ξ is a primitive cubic root of unity. Let $\mathbb{K} = \mathbb{Q}$, $\mathbb{L} = \mathbb{F} = \mathbb{C}$. Then, $\mathbb{C}(\mathcal{V}) = \mathrm{Frac}(\frac{\mathbb{C}[x]}{x-\sqrt[3]{2}}) \cong \mathbb{C}$, $\mathbb{C}(\mathcal{W}) = \mathrm{Frac}(\frac{\mathbb{C}[x]}{x-\sqrt[3]{2}\xi}) \cong \mathbb{C}$, hence, the fields are isomorphic. On the other hand, $\mathfrak{I}_{\mathbb{Q}}(\mathcal{V}) = \mathfrak{I}_{\mathbb{Q}}(\mathcal{W}) = (x^3 - 2)$. So, $\mathbb{Q}(\mathcal{V}) = \mathbb{Q}(\mathcal{W}) = \frac{\mathbb{Q}[x]}{x^3-2}$ are also isomorphic. However, these two varieties are not $\mathbb{Q}$-birational. If this where the case, there would be a rational function $f \in \mathbb{Q}(x)$, $f : \mathcal{V} \longrightarrow \mathcal{W}$, that is, $f(\sqrt[3]{2}) = \sqrt[3]{2}\xi$, and we would conclude that $\sqrt[3]{2}\xi \in \mathbb{Q}(\sqrt[3]{2})$, that is false. So, $\mathcal{V}$, $\mathcal{W}$ cannot be $\mathbb{Q}$-birational.

6.5 $\mathbb{K}$-parametric Varieties

In this Section, we deal with the problem of parametric varieties in $\mathbb{L}^n$ given by a parametrization with coefficients in a subfield $\mathbb{K}$.

Definition 6.25. Let $\mathcal{V} \subseteq \mathbb{L}^n$ a $\mathbb{K}$-variety, $\mathbb{K} \subseteq \mathbb{L}$. $\mathcal{V}$ is a $\mathbb{K}$-*unirational variety* if there are rational functions

$$\phi_1 = \frac{p_1}{q_1}, \ldots, \phi_n = \frac{p_n}{q_n} \in \mathbb{K}(t_1, \ldots, t_m)$$

such that if

$$\mathcal{W} = \{(\phi_1(\underline{t}), \ldots, \phi_n(\underline{t})) \in \mathbb{K}^n |\ \underline{t} = (t_1, \ldots, t_m) \in \mathbb{K}^m, q_j(\underline{t}) \neq 0,\ 1 \leq j \leq n\}$$

then $\mathcal{V} = \overline{\mathcal{W}^{\mathbb{K}}}$. The tuple $(\phi_1, \ldots, \phi_m)$ is a $\mathbb{K}$-*parametrization* of $\mathcal{V}$. The field $\mathbb{K}$ is called a *parametrization field* or a *field of parametrization*.

The parametrization is *proper*, *faithful* or *birational* with respect to the field $\mathbb{K}$ if $\mathbb{K}(\phi_1, \ldots, \phi_n) = \mathbb{K}(t_1, \ldots, t_m)$. In this case, we call $\mathcal{V}$ a *rational variety*.

In the case where the dimension of $\mathcal{V}$ is 1, then $\mathcal{V}$ is a *parametric curve*.

It is not true that every unirational variety is a rational variety. See for example [Sha94], Chapter III, §5.4, page. 174-175. But, due to Lüroth's Theorem ([Wal50], Chapter V, §7, page. 149-151.) we can affirm that every parametric curve admits a proper parametrization.

Proposition 6.26. *Let $\mathcal{V} \subseteq \mathbb{L}^n$ be a unirational variety, $\mathbb{K} \subseteq \mathbb{L}$ a parametrization field of $\mathcal{V}$ and $(\phi_1, \ldots, \phi_n)$ a parametrization of $\mathcal{V}$ with coefficients in $\mathbb{K}$. Then:*

1. $\mathfrak{I}_{\mathbb{K}}(\mathcal{V}) = \{f \in \mathbb{K}[x_1, \ldots, x_n] \mid f(\phi_1, \ldots, \phi_n) \equiv 0\}$
2. *$\mathcal{V}$ is irreducible with respect to $\mathbb{K}$*
3. $\mathbb{K}(\mathcal{V}) \cong \mathbb{K}(\phi_1, \ldots, \phi_n)$

Proof. Consider the ring homomorphism:

$$\begin{array}{rccc} F: & \mathbb{K}[x_1, \ldots, x_n] & \longrightarrow & \mathbb{L}(t_1, \ldots, t_m) \\ & x_j & \mapsto & \phi_j \end{array}$$

First, consider the case $\mathbb{K} = \mathbb{L}$. Suppose that $f \in \mathfrak{I}_{\mathbb{L}}(\mathcal{V})$. Then, for every value $(t_1, \ldots, t_m)$ where the parametrization is defined we have that

$$f(\phi_1(t_1, \ldots, t_m), \ldots, \phi_n(t_1, \ldots, t_m)) = 0.$$

Hence, $f(\phi_1, \ldots, \phi_n) \equiv 0$. Conversely, if f is such that $f(\phi_1, \ldots, \phi_n) \equiv 0$, then f vanishes in $Im(\phi_1, \ldots, \phi_n)$. By definition of $\mathcal{V}$, $f \in \mathfrak{I}_{\mathbb{L}}(\mathcal{V})$. Finally, in the general case $\mathbb{K} \subsetneq \mathbb{L}$:

$$\mathfrak{I}_{\mathbb{K}}(\mathcal{V}) = \mathfrak{I}_{\mathbb{L}}(\mathcal{V}) \cap \mathbb{K}[x_1, \ldots, x_n] = \{f \in \mathbb{K}[x_1, \ldots, x_n] \mid f(\phi_1, \ldots, \phi_n) \equiv 0\}$$

For the second claim, note that $\mathfrak{I}_{\mathbb{K}}(\mathcal{V})$ is the kernel of the previous homomorphism F. Hence, $\mathfrak{I}_{\mathbb{K}}(\mathcal{V})$ is a prime ideal and $\mathbb{K}[x_1, \ldots, x_n]/\mathfrak{I}_{\mathbb{K}}(\mathcal{V})$ is an integer domain by Proposition 6.12. Then

$$\mathbb{K}[\mathcal{V}] = \frac{\mathbb{K}[x_1, \ldots, x_n]}{\mathfrak{I}_{\mathbb{K}}(\mathcal{V})} \cong \mathbb{K}[\phi_1, \ldots \phi_n]$$

and, finally

$$\mathbb{K}(\mathcal{V}) = \mathrm{Frac}\left(\frac{\mathbb{K}[x_1, \ldots, x_n]}{\mathfrak{I}_{\mathbb{K}}(\mathcal{V})}\right) \cong \mathbb{K}(\phi_1, \ldots, \phi_n)$$

□

Proposition 6.27. *Let $\mathcal{V} \subseteq \mathbb{L}^n$ be a parametric variety of dimension d, $\mathbb{K}$ a field of parametrization of $\mathcal{V}$, $\mathbb{K} \subseteq \mathbb{L}$; let $\phi_1(t_1, \ldots, t_m), \ldots, \phi_n(t_1, \ldots, t_m) \subseteq \mathbb{K}(t_1, \ldots, t_m)$ be a parametrization of $\mathcal{V}$. Then, $m \geq d$ and there is another parametrization of $\mathcal{V}$ with coefficients in $\mathbb{K}$ and d parameters $\psi_1, \ldots, \psi_n \subseteq \mathbb{K}(s_1, \ldots, s_d)$.*

Proof. See [Alo94] or [AGR01] □

So, from now on, we will always suppose that the number of parameters equals the dimension of the variety they define. Moreover, by Lüroth's Theorem, all the parametric curves will be given by a proper parametrization.

Proposition 6.28. *Let $\mathcal{V} \subseteq \mathbb{F}^n$, $\mathbb{F}$ algebraically closed, if $\mathbb{K}$ is a parametrization field of $\mathcal{V}$, then $\mathbb{K}$ is a field of definition of $\mathcal{V}$.*

Proof. It is a direct consequence of Lemma 6.20. To accomplish the hypothesis of the Lemma, $\mathcal{V}$ must be written as the projection of a $\mathbb{K}$-variety. But this is easy, let $\phi_1, \ldots, \phi_n$ be any parametrization of $\mathcal{V}$, $\phi_j = p_j/q_j \in \mathbb{K}(t_1, \ldots, t_m)$. Let

$$J = (x_1 q - p_1, \ldots, x_n q - p_n, q_1 \ldots q_n z - 1) \subseteq \mathbb{F}[t_1, \ldots, t_m, x_1, \ldots, x_n, z].$$

J is an ideal generated over $\mathbb{K}$. The projection

$$\begin{array}{rccc} \Pi: & \mathbb{F}^{m+n+1} & \longrightarrow & \mathbb{F}^n \\ & (t_1, \ldots, t_m, x_1, \ldots, x_n, h) & \mapsto & (x_1, \ldots, x_n) \end{array}$$

defines

$$\Pi(\mathfrak{V}_{\mathbb{F}}(J)) = \{\overline{x} \in \mathbb{F}^n \mid \exists \overline{t} \in \mathbb{F}^m,\ q_j(\overline{t}) \neq 0,\ \phi(\overline{t}) = \overline{x}\} = Im(\Phi).$$

Then, $\overline{\Pi(\mathfrak{V}_{\mathbb{F}}(J))^{\mathbb{F}}} = \mathcal{V}$ is a $\mathbb{K}$-variety. □

The reciprocal is not true, let us show a counterexample. Let $\mathcal{V}$ be the variety defined by $x^2 + y^2 - 6$ in $\mathbb{C}^2$. $\mathbb{Q}$ is field of definition of $\mathcal{V}$, but it is not a parametrization field.

If (ϕ_1, ϕ_2) where a parametrization of $\mathcal{V}$ over $\mathbb{Q}$, there would be a $t \in \mathbb{Q}$ such that both rational functions are defined and $(\phi_1(t), \phi_2(t)) \in \mathcal{V}$ and $\mathcal{V}$ would have points in $\mathbb{Q}^2$. If

$$\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right) \in \mathcal{V} \cap \mathbb{Q}^2,\ gcd(p_i, q_i) = 1,\ i = 1, 2$$

then $\frac{p_1^2}{q_1^2} + \frac{p_2^2}{q_2^2} = 6$, so $p_1^2 q_2^2 + p_2^2 q_1^2 = 6 q_1^2 q_2^2$. Then, $q_1^2 | p_1^2 q_2^2$, but, as $gcd(p_1, q_1) = 1$, this means that $q_1^2 | q_2^2$ and $q_1 | q_2$. Analogously, $q_2 | q_1$ and both elements are associated, so our point can be written as $\frac{p_1}{q}, \frac{p_2}{q}$ with $gcd(p_i, q) = 1$.

Now, $p_1^2 + p_2^2 = 6q^2$. From this, $p_1^2 + p_2^2 \equiv 0 \mod 3$, but $p_i^2 \equiv 0, 1 \mod 3$. So, $p_i^2 \equiv 0 \mod 3$. Then, $3|p_1$, $3|p_2$ and $9|p_1^2$, $9|p_2^2$. Thus, $9|6q^2 \Rightarrow 3|2q^2$. Finally, $3|q$ and p_1, q are not relatively prime, which is a contradiction with our hypothesis.

However, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{2})$ are two parametrization fields of $\mathcal{V}$, because we have the parametrizations of $\mathcal{V}$

$$\left(\frac{t^2 + 2t\sqrt{5} - 1}{1 + t^2}, -\frac{t^2\sqrt{5} - 2t - \sqrt{5}}{1 + t^2}\right)$$

$$\left(2\frac{t\sqrt{2} - 1 + t^2}{1 + t^2}, -\frac{t^2\sqrt{2} - 4t - \sqrt{2}}{1 + t^2}\right)$$

Both extensions are of degree 2 over $\mathbb{Q}$. As there are no intermediate field, there are no minimum field of parametrization of $\mathcal{V}$. What we can prove is that there are always *minimal* fields of parametrization.

Proposition 6.29. *Let $\mathcal{V} \subseteq \mathbb{K}^n$ be a parametric curve. Then, there are minimal quadratic fields of parametrization with respect to the inclusion.*

Proof. From [Che51] Chapter II §6 Theorem 6 we obtain that every parametric curve has a regular point, either with coefficients in the minimum field of definition or in an algebraic extension of this field of degree 2. On the other hand, there are algorithms to compute a parametrization of $\mathcal{V}$ from the generators of $\mathfrak{I}_{\mathbb{K}}(\mathcal{V})$, such that, if it is not possible to obtain a parametrization over the minimum field of definition of $\mathcal{V}$, it is found over an algebraic extension of degree 2 (because the parametrizations are obtained from a regular point). This algorithm is presented in [SW97] or [vH97]. □

Let us show a criterion to decide if a concrete field is a field of parametrization of a parametric curve.

Proposition 6.30. *Let $\mathcal{V} \subset \mathbb{F}^n$ be a parametric curve, $\mathbb{K} \subseteq \mathbb{F}$ be a extension of fields. Then $\mathbb{K}$ is a parametrization field of $\mathcal{V}$ if and only if $\#(\mathcal{V} \cap \mathbb{K}^n) = \infty$.*

Proof. It follows, for example, from the results of [SW91]. Suppose that $\mathbb{K}$ is a field of parametrization of $\mathcal{V}$. Let $(\phi_1, \ldots, \phi_n)$ be a parametrization of $\mathcal{V}$ with coefficients in $\mathbb{K}$. Then, one of the rational functions ϕ_j is non constant, without loss of generality, we may suppose that ϕ_1 is not a constant. Let $\phi_1 = \frac{p(t)}{q(t)}$ with $gcd(p(t), q(t)) = 1$ and let

$$S = \{x \in \mathbb{K} |\ \phi_j(x) \text{ is not defined for an index } j\},$$

that is, the set defined by each root of the denominators, so S is finite. If $\mathcal{V}$ had only a finite number of $\mathbb{K}$-rational points, the image by ϕ_1 over $\mathbb{K}$ would be finite and it would be defined by $\phi_1(\mathbb{K}) = \{k_1, \ldots, k_r\}$. So, $\mathbb{K}$ would be the union of subsets S and $S_l = \{x \in \mathbb{K} |\ \phi_1(x) = k_l\}$. Each S_l is finite, because it contains at most the roots of $p(x) - k_l q(x) = 0$ over $\mathbb{K}$. Hence, $\mathbb{K}$ would be expressed as the finite union of finite sets. But this is a contradiction with the fact that $\mathbb{K}$ is of characteristic zero.

For the reciprocal, in [SW91] it is shown an algorithm to parametrize a planar curve from a regular point, that is a point such that not all partial derivatives of the polynomial vanish. This algorithm provides a parametrization over the same field that contains the coordinates of the points. In our case, every curve $\mathcal{V}$ is $\mathbb{K}$-birational to a planar curve $\mathcal{W}$ and from [Sha94] Chapter I 1.5 we have that any curve has at most a finite number of singular points. As $\mathcal{V} \cap \mathbb{K}^n$ is infinite, we deduce that there must be a regular point in $\mathcal{W} \cap \mathbb{K}^2$ and, hence, a parametrization of $\mathcal{W}$ with coefficients in $\mathbb{K}$. Composing this parametrization with the $\mathbb{K}$-birational map from $\mathcal{W}$ to $\mathcal{V}$, we obtain a $\mathbb{K}$-parametrization of $\mathcal{V}$. □

Chapter 7

Weil and Witness Varieties

In this Chapter we associate, to every irreducible variety $\mathcal{V}$ defined over a field $\mathbb{K}(\alpha)$, another variety $\mathcal{W}$ (the Weil variety of $\mathcal{V}$), this time defined over $\mathbb{K}$. In some sense, $\mathcal{W}$ codifies the relation of $\mathcal{V}$ with the $\mathbb{K}$-varieties. First, we present the classical Weil method for implicit varieties. Next, we will apply the same technique to the case of parametric varieties given by a parametrization over $\mathbb{K}(\alpha)$.

7.1 Weil Variety

Let $\mathbb{K}$ be a characteristic zero field and $\mathbb{F}$ its algebraic closure. Let

$$\mathcal{V} = \mathfrak{V}_{\mathbb{F}}(f_1(x_1, \ldots, x_n), \ldots, f_r(x_1, \ldots, x_n)) \subseteq \mathbb{F}^n$$

be an algebraic variety of dimension m, irreducible with respect to $\mathbb{F}$, where $f_j \in \mathbb{F}[x_1, \ldots, x_n]$, $1 \leq j \leq r$. Let $\mathbb{L}$ be a finite algebraic extension of $\mathbb{K}$, $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{F}$ containing all the coefficients of the polynomials f_j. Without loss of generality, we may suppose that $\mathbb{L} = \mathbb{K}(\alpha)$ for some $\alpha \in \mathbb{F}$. Let $d = [\mathbb{L} : \mathbb{K}]$ be the degree of the extension and fix once and for all the base $\{1, \alpha, \ldots, \alpha^{d-1}\}$ of $\mathbb{L}$ as a $\mathbb{K}$-vector space.

Following Weil [Wei95], let us define the Weil variety associated to $\mathcal{V}$ as follows: replace each variable x_j by $x_{j0} + \alpha x_{j1} + \cdots + \alpha^{d-1} x_{j,d-1}$, where x_{ji} are new variables, and write f_k in this new set of variables:

$$f_k(x_{(1)}; \ldots; x_{(n)}) \in \mathbb{L}[x_{(1)}; \ldots; x_{(n)}],$$

where $x_{(j)}$ denotes the vector of variables $(x_{j0}; \ldots; x_{j,d-1})$. From the equality

$$\mathbb{L}[x_{(1)}; \ldots; x_{(n)}] = \mathbb{K}(\alpha)[x_{(1)}; \ldots; x_{(n)}],$$

we may express $f_k(x_{(1)}; \ldots; x_{(n)})$ as

$$f_{k0}(x_{(1)}; \ldots; x_{(n)}) + \alpha f_{k1}(x_{(1)}; \ldots; x_{(n)}) + \cdots + \alpha^{d-1} f_{k,d-1}(x_{(1)}; \ldots; x_{(n)})$$

with $f_{ki} \in \mathbb{K}[x_{(1)}; \ldots; x_{(n)}]$ uniquely determined.

Definition 7.1. The $\mathbb{K}$-variety $\mathcal{W}$ defined by the polynomials f_{ki} is the *Weil variety* associated to $\mathcal{V}$.

$$\mathcal{W} = \{f_{ki}(x_{(1)}; \ldots; x_{(n)}) = 0 \mid k = 1, \ldots, r, i = 0, \ldots, d-1\} \subseteq \mathbb{F}^{nd}$$

From the construction of $\mathcal{W}$, it follows that if $v = (v_{(1)}; v_{(2)}; \ldots; v_{(n)}) \in \mathcal{W}$, where each $v_{(j)}$ represents the d-tuple $(v_{j0}, \ldots, v_{j,d-1})$, then

$$v_V = \left(\sum_{i=0}^{d-1} v_{1i}\alpha^i, \ldots, \sum_{i=0}^{d-1} v_{ni}\alpha^i \right) \in \mathcal{V}$$

that is, v_V is in $\mathcal{V}$.

An easy check shows that the variety $\mathcal{W}$ just defined does not depend on the equations used to define V.

Lemma 7.2. *Suppose that*

$$\mathcal{V} = \{f_1(x_1, \ldots, x_n) = \ldots = f_r(x_1, \ldots, x_n) = 0\} =$$

$$\{g_1(x_1, \ldots, x_n) = \ldots = g_s(x_1, \ldots, x_n) = 0\} \subseteq \mathbb{F}^n$$

and that the coefficients of every polynomial f_k, g_j are in $\mathbb{L}$. Let $\mathcal{W}_f$, $\mathcal{W}_g$ be the Weil variety defined respectively from the set of of polynomials. Then $\mathcal{W}_f = \mathcal{W}_g$.

Proof. Let

$$\mathcal{W}_f = \{f_{ki} = 0,\ 1 \le k \le r, \quad 0 \le i \le d-1\}$$

$$\mathcal{W}_g = \{g_{jl} = 0,\ 1 \le j \le s, \quad 0 \le l \le d-1\}$$

where (f_{ki}), (g_{jl}) are obtained from the polynomials f_k, g_j during the construction of the varieties $\mathcal{W}_f$, $\mathcal{W}_g$. It suffices to show that $\sqrt{(f_{ki})} = \sqrt{(g_{jl})}$. As $f_k^N \in (g_1, \ldots, g_s)$, we have that $f_k^N = \sum_{j=1}^{s} g_j h_j$. Then

$$\left(\sum_{i=0}^{d-1} f_{ki}(x_{(1)}; \ldots; x_{(n)})\alpha^i \right)^N = f_k(\sum_{i=0}^{d-1} x_{1i}\alpha^i, \ldots, \sum_{i=0}^{d-1} x_{ni}\alpha^i)^N =$$

$$\sum_{j=1}^{s} \Big(g_j(\sum_{i=0}^{d-1} x_{1i}\alpha^i, \ldots, \sum_{i=0}^{d-1} x_{ni}\alpha^i) h_j(\sum_{i=0}^{d-1} x_{1i}\alpha^i, \ldots, \sum_{i=0}^{d-1} x_{ni}\alpha^i) \Big) =$$

$$\sum_{j=1}^{s} \Big((\sum_{l=0}^{d-1} g_{jl}(x_{(1)}; \ldots; x_{(n)})\alpha^l) h_j(\sum_{i=0}^{d-1} x_{1i}\alpha^i, \ldots, \sum_{i=0}^{d-1} x_{ni}\alpha^i) \Big) \in (g_{jl})$$

Hence, $\sum_{i=0}^{d-1} f_{ki}\alpha^i \in \sqrt{(g_{jl})}$, $1 \le k \le r$. As (g_{jl}) is an ideal with generators in $\mathbb{K}[x_1, \ldots, x_n]$, it follows from Lemma 6.8 that $\sqrt{(g_{jl})}$ is also an ideal defined over $\mathbb{K}$. Thus, by Lemma 6.6 $f_{ki} \in \sqrt{(g_{jl})}$ and $\sqrt{(f_{ki})} \subseteq \sqrt{(g_{jl})}$. By symmetry, we obtain the equality. □

Consider the extension of fields $\mathbb{K} \subseteq \mathbb{K}(\alpha) = \mathbb{L} \subseteq \mathbb{F}$. Let $\alpha = \alpha_1, \ldots, \alpha_d$ be the conjugates of α in $\mathbb{F}$ with respect to $\mathbb{K}$ and, for each $l = 1, \ldots, d$, take an automorphism σ_l of $\mathbb{F}|\mathbb{K}$ sending α onto α_l, $\sigma_1 = Id$. Denote by $\mathcal{V}^{\sigma_l}$ the conjugate of $\mathcal{V}$ via σ_l, that is,

$$\mathcal{V}^{\sigma_l} = \{f_1^{\sigma_l}(x_1^{\sigma_l}, \ldots x_n^{\sigma_l}) = \cdots = f_r^{\sigma_l}(x_1^{\sigma_l}, \ldots x_n^{\sigma_l}) = 0\} \subseteq \mathbb{F}^n$$

where $f_k^{\sigma_l}(x_1^{\sigma_l}, \ldots x_n^{\sigma_l})$ is the polynomial whose coefficients are the image under σ_l of the coefficients of f_k and $x_j^{\sigma_l}$ are some new variables. Notice that the $f_k^{\sigma_l}$ and hence $\mathcal{V}^{\sigma_l}$ do not depend on the particular $\mathbb{K}$-automorphism σ_l chosen as long as $\sigma_l(\alpha) = \alpha_l$. Also notice that $\mathcal{V}^{\sigma_l}$ is characterised by the fact that for every point in $\mathbb{F}^n$, $(v_1, \ldots, v_n) \in \mathcal{V}$ if and only if $(\sigma_l(v_1), \ldots, \sigma_l(v_n)) \in \mathcal{V}^{\sigma_l}$. Obviously $\mathcal{V}^{\sigma_l}$ is an algebraic variety isomorphic to $\mathcal{V}$ and, if the original equation system has all its coefficients in the base field, that is, if $f_k \in \mathbb{K}[x_1, \ldots, x_n]$, then $\mathcal{V} = \mathcal{V}^{\sigma_l}$, for every $l = 1, \ldots, d$. This may happen even if $\mathcal{V} \cap \mathbb{K}^n = \emptyset$, for example if $\mathcal{V} = \{x^2 + y^2 + 1 = 0\}$ and $\mathbb{K} = \mathbb{Q}$.

Take a point $v = (v_{(1)}; \ldots; v_{(n)}) \in \mathcal{W}$, where $v_{(j)} = (v_{j0}, \ldots, v_{j,d-1})$. As $\mathcal{W}$ is defined by polynomials with coefficients in $\mathbb{K}$, it is invariant by conjugation. Thus, $w = \sigma_l^{-1}(v) = (\sigma_l^{-1}(v_{(1)}); \ldots; \sigma_l^{-1}(v_{(n)}))$ is also in $\mathcal{W}$. In particular, by the above description of v_V, the point w_V belongs to $\mathcal{V}$, so its image by σ_l is in $\mathcal{V}^{\sigma_l}$, that is:

$$v_V^{\sigma_l} = \left(\sum_{i=0}^{d-1} v_{1i}\alpha_l^i, \sum_{i=0}^{d-1} v_{2i}\alpha_l^i, \ldots, \sum_{i=0}^{d-1} v_{ni}\alpha_l^i \right) \in \mathcal{V}^{\sigma_l}.$$

Hence, the linear automorphism $\Psi : \mathbb{F}^{nd} \to \mathbb{F}^{nd}$ given by

$$\begin{array}{lcl} (x_{10} \ \ldots \ x_{1,d-1}; & & \left(\sum_{i=0}^{d-1} x_{1i}\alpha^i \ \ldots \ \sum_{i=0}^{d-1} x_{ni}\alpha^i; \right. \\ x_{20} \ \ldots \ x_{2,d-1}; & & \sum_{i=0}^{d-1} x_{1i}\alpha_2^i \ \ldots \ \sum_{i=0}^{d-1} x_{ni}\alpha_2^i; \\ \ldots\ldots\ldots & \xrightarrow{\Psi} & \ldots\ldots\ldots \\ x_{n0} \ \ldots \ x_{n,d-1};) & & \left. \sum_{i=0}^{d-1} x_{1i}\alpha_d^i \ \ldots \ \sum_{i=0}^{d-1} x_{ni}\alpha_d^i \right) \end{array}$$

sends $\mathcal{W}$ into $\mathcal{V} \times \mathcal{V}^{\sigma_2} \times \cdots \times \mathcal{V}^{\sigma_d}$. Notice that, in the previous map, we represent the points in $\mathbb{F}^{nd}$ on the left side as a $n \times d$ matrix, where each row represents the vector of variables $x_{(j)}$, while, on the right side, the points are represented by a $d \times n$ matrix where the rows are the points v_V, $v_V^{\sigma_2}, \ldots, v_V^{\sigma_d}$ of the varieties $\mathcal{V}, \mathcal{V}^{\sigma_2} \ldots, \mathcal{V}^{\sigma_d}$ respectively.

Let $x = (x_0, x_1, \ldots, x_{d-1}) \in V \times V^{\sigma_1} \times \cdots \times V^{\sigma_{d-1}}$. Let $y = (y_{(0)}; \ldots; y_{(d-1)})$ be the preimage of x by ψ, then $\sum_{i=0}^{d-1} \alpha_l^i f_{ik}(y_0; \ldots; y_{d-1}) = f_k^{\sigma_l}(x_l) = 0$, $0 \leq r \leq d-1$. The matrix (α_l^i) is a Vandermonde matrix, so it is regular. Hence, we conclude that $f_{ik}(y) = 0, 0 \leq i \leq d-1, 1 \leq k \leq r$ and $y \in W$. To sum up:

The next result summarizes the basic properties of the Weil variety, as it can be checked in [ARS99]

Theorem 7.3.

1. *The automorphism $\Psi : \mathbb{F}^{nd} \to \mathbb{F}^{nd}$ maps $\mathcal{W}$ onto $\mathcal{V} \times \mathcal{V}^{\sigma_2} \times \cdots \times \mathcal{V}^{\sigma_d}$. Hence, they are linearly isomorphic varieties.*

2. *Let* $\widetilde{\mathcal{W}} = \mathcal{W} \cap \{x_{ji} = 0 \mid j = 1, \ldots, n, i \geq 1\}$. *The previous automorphism maps* $\widetilde{\mathcal{W}}$ *isomorphically onto the diagonal* Δ *of the product* $\mathcal{V} \times \mathcal{V}^{\sigma_2} \times \cdots \times \mathcal{V}^{\sigma_d}$, *which can be identified with the intersection* $\mathcal{V} \cap \mathcal{V}^{\sigma_2} \cap \cdots \cap \mathcal{V}^{\sigma_d}$. *This intersection is the greatest subset (in fact it is a subvariety) of* $\mathcal{V}$ *which is globally stable under conjugation*

Proof. The first item has already been commented. It holds by construction. For the second item, let $v = (v_{(1)}; v_{(2)}; \ldots; v_{(n)})$ be a point in $\widetilde{\mathcal{W}}$. Then each $v_{(j)}$ is of the form $(v_{j0}, 0, \ldots, 0)$. Hence, $v_V^{\sigma_l} = (v_{10}, \ldots, v_{n0}) \in \mathcal{V}^{\sigma_l}$. It follows that $\Psi(v) \in \Delta$. Conversely, if a point $(v, v, \ldots, v) \in \Delta$ is a point of $\mathcal{V}$ that belongs to all its conjugates, then $\Psi^{-1}(v, \ldots, v) = (v_{(1)}, \ldots, v_{(n)}) \in \mathcal{W}$ but in this case $v_{(j)} = (v, 0, \ldots, 0)$, so in fact $\Psi^{-1}(v, \ldots, v) \in \widetilde{\mathcal{W}}$. □

In particular, from the second item we have:

Corollary 7.4. *The following statements are equivalent:*

1. *The variety* $\mathcal{V}$ *is defined over* $\mathbb{K}$.
2. $\widetilde{\mathcal{W}}$ *is isomorphic to* $\mathcal{V}$.
3. $\mathcal{V} = \bigcap_{l=1}^{d} \mathcal{V}^{\sigma_l}$
4. $\mathcal{V} = \bigcup_{l=1}^{d} \mathcal{V}^{\sigma_l}$
5. $\mathcal{V} = \mathcal{V}^{\sigma_l}$, $1 \leq l \leq d$
6. $\dim(\widetilde{\mathcal{W}}) = \dim(\mathcal{V})$.

Proof.

• *1* $\Rightarrow$ *5* is obvious from Proposition 6.9, because if $\mathcal{V} = \mathfrak{I}_{\mathbb{F}}(f_1, \ldots, f_r)$, f_r with coefficients in $\mathbb{K}$, then $\mathcal{V}^{\sigma_l} = \mathfrak{I}_{\mathbb{F}}(\sigma_l(f_1), \ldots, \sigma_l(f_r)) = \mathfrak{I}_{\mathbb{F}}(f_1, \ldots, f_r) = \mathcal{V}$, $1 \leq l \leq d$. Also, it is trivial that *5* implies *3* and *4*.

• Suppose *4*, then we have that for all l, $\mathcal{V}^{\sigma_l} \subseteq \mathcal{V}$, applying σ_l^{-1} we obtain $\mathcal{V} \subseteq \mathcal{V}^{\sigma_l^{-1}}$ for all l. Let σ_s be the $\mathbb{K}$-automorphism of our family such that $\sigma_s(\alpha) = \sigma_l^{-1}(\alpha)$, then $\mathcal{V}^{\sigma_s} = \mathcal{V}^{\sigma_l^{-1}}$. It follows that $\mathcal{V} = \mathcal{V}^{\sigma_l}$ for every l. Hence we conclude that $\mathcal{V} = \mathcal{V}^{\sigma_l}$ for all l. Analogously, one proves that *3* implies *5*.

• If *3* holds, then, we have that $\mathcal{V}$ is isomorphic with the diagonal Δ, so with $\widetilde{\mathcal{W}}$ and we have *2*. Note also $\mathcal{W}$ is, by definition a $\mathbb{K}$-variety and that the isomorphism is $x \to (x_{(1)}; \ldots; x_{(n)})$, where $x_{(j)} = (x, 0, \ldots, 0)$, hence $\mathcal{W}$ and $\mathcal{V}$ are $\mathbb{K}$-birational. By Theorem 6.22 $\mathcal{V}$ is defined over $\mathbb{K}$ and *1* holds.

• It is clear that *2* implies *6*.

• Finally, suppose that *6* holds, note that $\widetilde{\mathcal{W}}$ is always isomorphic with $\cap_{l=1}^{d} \mathcal{V}^{\sigma_l}$ by an isomorphism defined over $\mathbb{K}$. Hence, it follows that $\cap_{l=1}^{d} \mathcal{V}^{\sigma_l} \subseteq \mathcal{V}$ are of the same dimension. As $\mathcal{V}$ is irreducible, is must happen that $\cap_{l=1}^{d} \mathcal{V}^{\sigma_l} = \mathcal{V}$ and hence *3*. □

Example 7.5. Let $k = \mathbb{R}$, $V := \{x^2 + y^2 + 1 = 0\} \subset \mathbb{C}^2$. Making the substitution $x = x_0 + i\,x_1$, $y = y_0 + i\,y_1$ yields

$$x^2 + y^2 + 1 = (x_0^2 - x_1^2 + y_0^2 - y_1^2 + 1) + i\,(2x_0x_1 + 2y_0y_1)$$

so the Weil variety $\mathcal{W}$ is the variety of $\mathbb{C}^4$ defined by the equations

$$x_0^2 - x_1^2 + y_0^2 - y_1^2 + 1 = 2x_0x_1 + 2y_0y_1 = 0.$$

The isomorphism ψ is given in this case by

$$(x_0, x_1, y_0, y_1) \mapsto (x_0 + i\,x_1, y_0 + i\,y_1, x_0 - i\,x_1, y_0 - i\,y_1)$$

and the variety $\widetilde{\mathcal{W}}$ is given by $x_0^2 + y_0^2 + 1 = x_1 = y_1 = 0$ which is isomorphic to V.

7.2 The Weil Variety in the Parametric Case

In this Section we try to adapt the Weil variety method to the case of dealing with a parametric variety. We suppose that $\mathbb{K}$ is a characteristic zero field, $\mathbb{F}$ its algebraic closure and $\mathbb{K}(\alpha) = \mathbb{L} \subseteq \mathbb{F}$ is an algebraic extension of $\mathbb{K}$, $[\mathbb{K}(\alpha) : \mathbb{K}] = d$.

Let $\mathcal{V}$ be a $\mathbb{L}$-parametric variety, given by the unirational parametrization

$$\begin{array}{rccc} \phi: & \mathbb{F}^m & \to & \mathbb{F}^n \\ & (t_1, \ldots, t_m) & \to & (\phi_1(t_1, \ldots, t_m), \ldots, \phi_n(t_1, \ldots, t_m)) \end{array}$$

where $\phi_k \in \mathbb{L}(x_1, \ldots, x_n)$. Hence, each coordinate function ϕ_k has a representation as a quotient

$$\phi_k(t_1, \ldots, t_m) = \frac{h_k(t_1, \ldots, t_m)}{g_k(t_1, \ldots, t_m)}, \quad h_k, g_k \in \mathbb{L}[x_1, \ldots, x_n].$$

Moreover, substituting g_k by the least common multiple of all the denominators g_k, we suppose, from now on, that the parametrization is reduced to a common denominator, denoted by $g(t_1, \ldots, t_m)$. Finally, we suppose also that there are no common components on the representation of the parametrization, $\gcd(h_1(t), \ldots, h_n(t), g(t)) = 1$.

Definition 7.6. Let $\phi = (\phi_1, \ldots, \phi_n)$ be as above, write $t_j = t_{j0} + t_{j1}\alpha + \cdots + t_{j,d-1}\alpha^{d-1}$, where t_{ji} are new parameters. The substitution of these expressions in ϕ define new rational functions $\mathbb{L}(t_{(1)}; \ldots; t_{(m)})$, where, as in the implicit case, $t_{(j)}$ denotes the vector of parameters $(t_{j0}, \ldots, t_{j,d-1})$. We will still denote these rational functions by ϕ_k.

As $\mathbb{L}(t_{(1)}; \ldots; t_{(m)}) = \mathbb{K}(t_{(1)}; \ldots; t_{(m)})(\alpha)$, each rational function have a unique expression of the form:

$$\phi_k = \phi_{k0}(t_{(1)}; \ldots; t_{(m)}) + \alpha\phi_{k1}(t_{(1)}; \ldots; t_{(m)}) + \cdots + \alpha^{d-1}\phi_{k,d-1}(t_{(1)}; \ldots; t_{(m)})$$

where each $\phi_{ki} \in \mathbb{K}(t_{(1)}; \ldots; t_{(m)})$. The unirational map $\Phi : \mathbb{F}^{md} \to \mathbb{F}^{nd}$ given by

$$\begin{array}{ccc} \big(t_{10} \;\; \ldots \;\; t_{1d-1}; & & \big(\phi_{10}(t_{(1)}; \ldots; t_{(m)}) \;\; \ldots \;\; \phi_{1d-1}(t_{(1)}; \ldots; t_{(m)}); \\ t_{20} \;\; \ldots \;\; t_{2d-1}; & & \phi_{20}(t_{(1)}; \ldots; t_{(m)}) \;\; \ldots \;\; \phi_{2d-1}(t_{(1)}; \ldots; t_{(m)}); \\ \ldots\ldots\ldots & \to & \ldots\ldots\ldots \\ t_{m0} \;\; \ldots \;\; t_{md-1}\big) & & \phi_{n0}(t_{(1)}; \ldots; t_{(m)}) \;\; \ldots \;\; \phi_{nd-1}(t_{(1)}; \ldots; t_{(m)})\big) \end{array}$$

is called the *parametrization obtained by development* of ϕ.

The next result extends the results in [ARS99] to parametric varieties of arbitrary dimension.

Theorem 7.7. *If $\mathcal{V}$ is a parametric variety, then its associated Weil variety $\mathcal{W}$ is also parametric; a parametrization of $\mathcal{W}$ can be obtained by the development of the parametrization of $\mathcal{V}$. Moreover, if the initial parametrization of $\mathcal{V}$ is birational, so is the induced parametrization of $\mathcal{W}$. Furthermore, the inverse map of $\mathcal{W}$ is obtained by development of the inverse map of ϕ.*

Proof. By the linear isomorphism between $\prod_{r=1}^{d} \mathcal{V}^{\sigma_r}$ and $\mathcal{W}$, as $\prod_{r=1}^{d} \mathcal{V}^{\sigma_r}$ is clearly a parametric variety, $\mathcal{W}$ is also parametric. Now, $(\phi_{10}, ..., \phi_{n,d-1})$ is a parametrization of $\mathcal{W}$ if and only if

$$\begin{pmatrix} \sum_{i=0}^{d-1} \phi_{1i}(t_{(1)};\ldots,t_{(m)})\alpha^i, & \ldots, & \sum_{i=0}^{d-1} \phi_{ni}(t_{(1)};\ldots,t_{(m)})\alpha^i; \\ \sum_{i=0}^{d-1} \phi_{1i}(t_{(1)};\ldots,t_{(m)})\alpha_2^i, & \ldots, & \sum_{i=0}^{d-1} \phi_{ni}(t_{(1)};\ldots,t_{(m)})\alpha_2^i; \\ & \cdots\cdots\cdots & \\ \sum_{i=0}^{d-1} \phi_{1i}(t_{(1)};\ldots,t_{(m)})\alpha_d^i, & \ldots, & \sum_{i=0}^{d-1} \phi_{ni}(t_{(1)};\ldots,t_{(m)})\alpha_d^i \end{pmatrix}$$

parametrices the variety $\prod_{r=1}^{d} \mathcal{V}^{\sigma_r}$. But in this product variety we have the following product parametrization: By conjugation, there is a parametrization $\phi^{\sigma_l}(t)$ of the variety $\mathcal{V}^{\sigma_l}$. In order to avoid confusion, denote by $t^{\sigma_l} = (t_1^{\sigma_1}, \ldots, t_m^{\sigma_l})$ the vector of parameters of the parametrization of $\mathcal{V}^{\sigma_l}$. Gluing up these parametrizations we obtain a parametrization of the product, $\Pi : (\mathbb{F}^m)^d \to \mathcal{V} \times \mathcal{V}^{\sigma_2} \times \cdots \times \mathcal{V}^{\sigma_d}$ given by:

$$(t, t^{\sigma_1}, \ldots, t^{\sigma_d}) \to (\phi(t), \phi^{\sigma_1}(t^{\sigma_1}), \ldots, \phi^{\sigma_{d-1}}(t^{\sigma_{d-1}}))$$

The linear isomorphism Ψ of the previous Section transforms this parametrization into a parametrization of $\mathcal{W}$.

An easy check shows that Φ is related to Π by the linear change of parameters $\eta : \mathbb{F}^{md} \to (\mathbb{F}^m)^d$ given by

$$\begin{pmatrix} t_{10} & \ldots & t_{1,d-1}; \\ t_{20} & \ldots & t_{2,d-1}; \\ \multicolumn{3}{c}{\cdots\cdots\cdots} \\ t_{m0} & \ldots & t_{m,d-1} \end{pmatrix} \longrightarrow \begin{pmatrix} \sum_{i=0}^{d-1} t_{1i}\alpha^i & \ldots & \sum_{i=0}^{d-1} t_{mi}\alpha^i; \\ \sum_{i=0}^{d-1} t_{1i}\alpha_2^i & \ldots & \sum_{i=0}^{d-1} t_{mi}\alpha_2^i; \\ \multicolumn{3}{c}{\cdots\cdots\cdots} \\ \sum_{i=0}^{d-1} t_{1i}\alpha_d^i & \ldots & \sum_{i=0}^{d-1} t_{mi}\alpha_d^i \end{pmatrix}$$

where each row on the right can be interpreted as the vector of parameters $t^{\sigma_l} = (t_1^{\sigma_l}, \ldots, t_m^{\sigma_l})$ that parametrizes $\mathcal{V}^{\sigma_l}$. So, $\mathcal{W}$ is parametrized by Φ.

To sum up, we have the commutative diagram of Figure 7.1 where the horizontal maps are linear isomorphisms and the vertical ones are the parametrizations of the Weil variety and the product variety.

$$\begin{array}{ccc} \mathcal{W} & \xrightarrow{\quad\psi\quad} & \mathcal{V}\times\mathcal{V}^{\sigma_2}\times\cdots\times\mathcal{V}^{\sigma_d} \\ \uparrow & & \uparrow \\ \Phi & & \Pi=\phi\times\phi^{\sigma_2}\times\cdots\times\phi^{\sigma_d} \\ | & & | \\ \mathbb{F}^{md} & \xrightarrow{\quad\eta\quad} & \mathbb{F}^m\times\mathbb{F}^m\ldots\times\mathbb{F}^m \end{array}$$

Figure 7.1: Main Diagram

Suppose that ϕ is birational. Then

$$\mathbb{F}(\phi_1(t),\ldots,\phi_n(t))=\mathbb{F}(t)$$

where $t=(t_1,\ldots,t_m)$, hence

$$\mathbb{F}(\phi_1^{\sigma_l}(t^{\sigma_l}),\ldots,\phi_n^{\sigma_1}(t^{\sigma_l}))=\mathbb{F}(t^{\sigma_l})$$

for every l. In particular, for each $l=1,\ldots,d$, there are rational functions $P_i^{\sigma_l}\in\mathbb{F}(x_1^{\sigma_l},\ldots,x_n^{\sigma_l})$ such that

$$P_k^{\sigma_l}(\phi_1^{\sigma_l}(t^{\sigma_l}),\ldots,\phi_n^{\sigma_l}(t^{\sigma_l}))=t_k^{\sigma_l}$$

Let $\psi_*P_k^{\sigma_l}$ be the rational function obtained through the isomorphism ψ (that is, it is obtained from $P_k^{\sigma_l}$ substituting each variable $x_j^{\sigma_l}$ by $x_{j0}+\alpha_l x_{j1}+\cdots+\alpha_l^{d-1}x_{j,d-1}$).

The inverse map of η in Figure 7.1 expresses the parameters t_{ji} as a linear function $\sum\lambda_{kl}t_k^{\sigma_l}$ of the parameters $t_k^{\sigma_l}$ for some $\lambda_{kl}\in\mathbb{F}$. Consider the rational function

$$Q_{ji}=\sum\lambda_{kl}(\psi_*P_k^{\sigma_l})\in\mathbb{F}(x_{(1)},\ldots,x_{(n)}).$$

Using the commutativity of the diagram one gets that:

$$t_{ji}=Q_{ji}(\phi_{10}(t_{(1)},\ldots,t_{(m)}),\ldots,\phi_{n,d-1}(t_{(1)},\ldots,t_{(m)}))$$

which proves that

$$\mathbb{F}(\phi_{01}(t_{(1)},\ldots,t_{(m)}),\ldots,\phi_{n,d-1}(t_{(1)},\ldots,t_{(m)}))=\mathbb{F}(t_{(1)},\ldots,t_{(m)}).$$

Thus, Φ is birational. Remark that a similar argument, reversing the order of reasoning in Figure 7.1 allows us to deduce that, if Φ is birational, so is Π and ϕ. □

As a consequence, we have the following.

Theorem 7.8. *Let $\widetilde{\mathcal{W}}$ be the subvariety of $\mathcal{W}$ defined in Theorem 7.3. Let $Y=\{t\in\mathbb{F}^{md}\mid\phi_{ki}(t)=0,i>0\}$. Then $\Phi^{-1}(t)(\widetilde{\mathcal{W}})\supseteq Y$, and thus $\Phi(Y)\subseteq\widetilde{\mathcal{W}}$ at every point where Φ is defined.*

Proof. This theorem follows from the construction of Y and $\widetilde{\mathcal{W}}$. □

Example 7.9. Let ϕ be the parametrization

$$\phi = \begin{cases} x(t) = \dfrac{-2ti}{1+t^2} \\ y(t) = \dfrac{i(1-t^2)}{1+t^2} \end{cases}$$

of the imaginary circle $\mathcal{V} = \{x^2 + y^2 + 1 = 0\}$. This parametrization is birational and, taking $P(x, y) = \dfrac{y-i}{x}$, we have that $P(x(t), y(t)) = t$. The conjugate variety of $\mathcal{V}$ over $\mathbb{Q}$ (that coincides with $\mathcal{V}$ itself) is parametrized by

$$\overline{\phi} = \begin{cases} \overline{x}(\bar{t}) = \dfrac{2\bar{t}i}{1+\bar{t}^2} \\ \overline{y}(\bar{t}) = \dfrac{-i(1-\bar{t}^2)}{1+\bar{t}^2} \end{cases}$$

The inverse of this birational map is now $\overline{P}(\overline{x}, \overline{y}) = \dfrac{\overline{y}+i}{\overline{x}}$. Recall that $\overline{x}, \overline{y}, \bar{t}$ are other new variables. Developing $P(x, y)$ and $\overline{P}(\bar{x}, \bar{y})$ after performing the substitutions $x = x_0 + ix_1$, $y = y_0 + iy_1$, $\bar{x} = x_0 - ix_1$, $\bar{y} = y_0 - iy_1$, we obtain the rational functions

$$\psi_* P = \frac{y_0x_0 + y_1x_1 - x_1}{x_1^2 + x_0^2} + i\,\frac{y_1x_0 - x_0 - y_0x_1}{x_1^2 + x_0^2}$$

$$\psi_* \overline{P} = \frac{y_0x_0 + y_1x_1 - x_1}{x_1^2 + x_0^2} - i\,\frac{y_1x_0 + x_0 + y_0x_1}{x_1^2 + x_0^2}$$

of the proof of the Theorem.

On the other hand, substituting $t = t_0 + it_1$, $\bar{t} = t_0 - it_1$ in the parametrization of $\mathcal{V}$, we obtain the parametrization of $\mathcal{W}$:

$$\begin{cases} x_0(t_0, t_1) = & -2\,\dfrac{t_0^2t_1 + t_1^3 - t_1}{t_0^4 + 2t_0^2t_1^2 + 2t_0^2 + t_1^4 - 2t_1^2 + 1} \\ x_1(t_0, t_1) = & -2\,\dfrac{t_0^3 + t_0t_1^2 + t_0}{t_0^4 + 2t_0^2t_1^2 + 2t_0^2 + t_1^4 - 2t_1^2 + 1} \\ y_0(t_0, t_1) = & \dfrac{4t_0t_1}{t_0^4 + 2t_0^2t_1^2 + 2t_0^2 + t_1^4 - 2t_1^2 + 1} \\ y_1(t_0, t_1) = & -\dfrac{-1 + t_0^4 + 2t_0^2t_1^2 + t_1^4}{t_0^4 + 2t_0^2t_1^2 + 2t_0^2 + t_1^4 - 2t_1^2 + 1} \end{cases}$$

Finally, taking into account that $t_0 = \frac{1}{2}(t + \bar{t})$ and $t_1 = \frac{1}{2i}(t - \bar{t})$, a simple substitution shows that

$$t_0 = \frac{1}{2}[\psi_* P(x_0(t_0, t_1), x_1(t_0, t_1), y_0(t_0, t_1), y_1(t_0, t_1)) + \psi_* \overline{P}(x_0(t_0, t_1), x_1(t_0, t_1), y_0(t_0, t_1), y_1(t_0, t_1))]$$

$$t_1 = \frac{1}{2i}[\psi_* P(x_0(t_0, t_1), x_1(t_0, t_1), y_0(t_0, t_1), y_1(t_0, t_1)) - \psi_* \overline{P}(x_0(t_0, t_1), x_1(t_0, t_1), y_0(t_0, t_1), y_1(t_0, t_1))]$$

is the inverse map of the parametrization of $\mathcal{W}$.

7.3 Witness Variety

In this Section we provide an analogous notion to the variety $\widetilde{\mathcal{W}}$, this time applied to the parametric case. We have seen in Corollary 7.4 that $\widetilde{\mathcal{W}}$ gives information on whether $\mathcal{V}$ is defined over k or not. However, $\widetilde{\mathcal{W}}$ is an object defined in terms of the implicit equations of $\mathcal{V}$ and we want to profit from the knowledge of a parametrization of $\mathcal{V}$. Now, in Theorem 7.8, we have introduced a kind of parametric analog of $\widetilde{\mathcal{W}}$, namely, Y. But only apparently.

In fact, with notation as in the previous Section, let $g(t)$ be the common denominator of ϕ. Then $g^{\sigma_l}(t^{\sigma_l})$ is the denominator of the parametrization $\phi^{\sigma_l} : \mathbb{F}^m \to \mathcal{V}^{\sigma_l}$. The automorphism η^{-1} maps the polynomials $g(t), g^{\sigma_2}(t^{\sigma_2}), \ldots, g^{\sigma_d}(t^{\sigma_d})$ into polynomials in $\mathbb{F}[t_{(1)}; \ldots; t_{(m)}]$ on the bottom-left side of Figure 7.1. Let δ be the product of all of them. By construction, δ is invariant by the isomorphisms $\sigma_1, \ldots, \sigma_d$, so it has its coefficients over the ground field $\mathbb{K}$, i.e.,

$$\delta = \prod_{i=1}^{d} \eta^{-1}(g^{\sigma_i}(t^{\sigma_i})) \in \mathbb{K}[t_{(1)}; \ldots; t_{(m)}].$$

Moreover, δ may be taken as the common denominator of Φ, that we shall assume from now on.

Remark 7.10. The open set $D_\delta = \{\delta \neq 0\} \subseteq \mathbb{F}^{md}$ corresponds by η with the open set $\{g(t) \neq 0\} \times \{g^{\sigma_2}(t^{\sigma_2}) \neq 0\} \times \cdots \times \{g^{\sigma_d}(t^{\sigma_d}) \neq 0\}$, hence the maps Φ, Π, in Figure 7.1, are regular on these open sets.

Unfortunately, we cannot ensure that Φ (respectively Π) defines a finite to one map over its image when it is restricted to D_δ (respectively $\eta(D_\delta)$). Neither in the case where Φ is birational, because it is possible that its inverse is not defined everywhere in the image of $\Phi(D_\delta)$ (respectively, the inverse of Π may not be defined over $\Pi(\eta(D_\delta))$), see Example 7.20.

However, the parametrizations Φ, Π are generically finite to one. More precisely, there is a Zariski open subset of $\mathcal{V} \times \mathcal{V}^{\sigma_2} \times \cdots \times \mathcal{V}^{\sigma_d}$ where the fiber of Π is a finite set of constant cardinality (always assuming that the varieties are over the algebraically closed field $\mathbb{F}$). In fact, there is an open subset $A \subseteq \mathcal{V}$ where ϕ has a constant finite number q of preimages, which coincides with the degree of the field $\mathbb{F}(\mathcal{V})$ of rational functions over $\mathcal{V}$ over the field $\mathbb{F}(\phi_1(t), \ldots, \phi_n(t)) \subseteq \mathbb{F}(t_1, \ldots, t_d)$ cf. [Sha94]. Consider now the open subset $\mathcal{A} = A \times A^{\sigma_2} \times \cdots \times A^{\sigma_d} \subseteq \mathcal{V} \times \mathcal{V}^{\sigma_2} \times \cdots \times \mathcal{V}^{\sigma_d}$ and let $B = \Pi^{-1}(\mathcal{A}) \subseteq (\mathbb{F}^m)^d$ and finally $U = \eta^{-1}(B)$. We have that the maps $\Phi : U \to \psi^{-1}(\mathcal{A})$ and $\Pi : B \to \mathcal{A}$ are regular with fiber of constant cardinality equal to q^d.

As stated before, we are interested in obtaining information about V, not through $\widetilde{W}$ but from Y. Now, it may happen that $\widetilde{\mathcal{W}}$ is contained in the closed set where the parametrization is not defined, that is, $\Phi^{-1}(\widetilde{\mathcal{W}}) \cap Y = \emptyset$, see Example 7.22. Nevertheless, this cannot happen when $\mathcal{V}$ is defined over $\mathbb{K}$. In fact, we have the following result:

Theorem 7.11. *The following statements are equivalent:*

a) The variety $\mathcal{V}$ is defined over $\mathbb{K}$.

b) There is an irreducible open set of $Y \cap D_\delta \cap U$ of dimension $\dim(\mathcal{V})$ where the restriction of Φ is dominant over $\widetilde{\mathcal{W}}$.

b') $\dim(V) = \dim(Y \cap D_\delta \cap U)$ and, over every irreducible open set of $Y \cap D_\delta \cap U$ of dimension $\dim(\mathcal{V})$, the restriction of Φ is dominant over $\widetilde{\mathcal{W}}$.

c) $\dim(Y \cap D_\delta \cap U) = \dim(\mathcal{V})$

Moreover, if these conditions hold and $\tau : \mathbb{F}^m \to Y \cap D_\delta \cap U$ is a unirational parametrization with coefficients over k of a component of $Y \cap D_\delta \cap U$ of dimension $\dim(\mathcal{V})$, then the composition $\psi \circ \Phi \circ \tau$ is a unirational parametrization of V. In particular, if $Y \cap D_\delta \cap U$ contains a parametric variety over k of the right dimension, V is k-parametrizable as well.

Proof. It always hold that

$$\dim(Y \cap D_\delta \cap U) \leq \dim(\widetilde{\mathcal{W}}) \leq \dim(\mathcal{V}).$$

The first inequality follows because Φ is finite to one in $Y \cap D_\delta \cap U$. The second inequality follows because $\widetilde{\mathcal{W}}$ is always isomorphic to $\cap \mathcal{V}^{\sigma_l} \subseteq \mathcal{V}$ by Theorem 7.3.

Suppose that $\mathcal{V}$ is defined over $\mathbb{K}$. Then, we know that $\widetilde{\mathcal{W}}$ is isomorphic to $\mathcal{V}$. Since $\mathcal{V}$ is parametrized by the unirational map $\phi(T) = h(T)/g(T)$, the image of the open set $\{g(T) \neq 0\} \subset \mathbb{F}^m$ where ϕ is defined and contains a Zariski non empty open set of $\mathcal{V}$. As $\mathcal{V}$ is irreducible, the intersection of this open set with the open set A, where the fiber of ϕ has constant cardinality, is a non empty open set of $\mathcal{V}$. Analogously, for every l, the image by ϕ^{σ_l} of $\{g^{\sigma_l} \neq 0\}$ contains a non empty open set of $\mathcal{V}^{\sigma_l} = \mathcal{V}$ where the fiber of the parametrization has constant cardinality. The intersection of all these open sets is an open set Ω of $\mathcal{V} = \mathcal{V} \cap \mathcal{V}^{\sigma_2} \cap \cdots \cap \mathcal{V}^{\sigma_d}$. The open set $\Omega \times \cdots \times \Omega \subset \mathcal{V} \times \cdots \times \mathcal{V}^{\sigma_d}$ determines an open set (identified with Ω) in the diagonal Δ of the product that is contained in the image of the definition set of Π and in the set where the fiber is finite and constant. Translating these data to the left column of Figure 7.1, we find an open set of $\widetilde{\mathcal{W}}$ which is contained in the image of the open set D_δ of definition of Φ, where the fiber has constant cardinality. Hence, $\Phi^{-1}(\widetilde{\mathcal{W}})$ contains an open set of $Y \cap D_\delta \cap U$ where the restriction of Φ is a finite to one map over $\widetilde{\mathcal{W}}$. It follows that the dimension of this open set is $\dim(\widetilde{\mathcal{W}}) = \dim(\mathcal{V})$. This proves that a) implies b).

Suppose now b), then as $Y \cap D_\delta \cap U$ contains an open set of dimension $\dim(\mathcal{V})$ and hence $\dim(Y \cap D_\delta \cap U) = \dim(\mathcal{V})$. Now, let B be any open subset of $Y \cap D_\delta \cap U$ of dimension $\dim(\mathcal{V})$. Since Φ is finite to one on this set, $\dim(\Phi(B)) = \dim(\mathcal{V})$ and $\Phi(B) \subseteq \widetilde{\mathcal{W}}$. But $\widetilde{\mathcal{W}}$ is an irreducible variety of dimension at most $\dim(\mathcal{V})$. Hence, $\Phi|_B$ is dominant and we have b').

Now, from b') it is clear that c) holds. Finally, if we have c) then $\dim(Y \cap D_\delta \cap U) \leq \dim(\widetilde{\mathcal{W}}) \leq \dim(\mathcal{V}) = \dim(Y \cap D_\delta \cap U)$, so, in particular $\dim(\widetilde{\mathcal{W}}) = \dim(\mathcal{V})$ and, by Corollary 7.4, $\mathcal{V}$ is defined over $\mathbb{K}$. □

For an example of what happens if $\Phi|_{Y\cap D_\delta\cap U}$ is a unirational map, but still $\mathcal{V}$ is not $\mathbb{K}$-definable, see Example 7.18.

The set U may be, in general, hard to compute (cf. [PDS04]), while the computation of D_δ and Y is mechanical by construction. We define:

Definition 7.12. Let Y, D_δ be as above. Let $\mathcal{Z}$ be the $\mathbb{F}$-Zariski closure of $Y \cap D_\delta$. This algebraic set is the *witness variety* of $\mathcal{V}$.

Unfortunately (contrary to the results of curves studied in [ARS97]) the witness variety is not enough in general to certify that $\mathcal{V}$ is defined over $\mathbb{K}$, because the previous theorem does not hold in general if we eliminate U in the statement, as it is shown in Example 7.20. There, it shown that it may even happen that $\mathcal{Z}$ is a parametric variety over $\mathbb{K}$ but $\mathcal{V}$ is not defined over $\mathbb{K}$. At least, Theorem 7.11 implies the witness variety provides a necessary condition on the rationality of $\mathcal{V}$, as remarked in the following corollary.

Corollary 7.13. *If $\mathcal{V}$ is defined over $\mathbb{K}$, then $Y \cap D_\delta$ contains an open subset of dimension* $\dim(\mathcal{V})$.

In the case where ϕ is birational, that is, $\mathbb{F}(\phi) = \mathbb{F}(t)$, Φ defines a isomorphism in the open set $D_\delta \cap U$ and Theorem 7.11 can be refined.

Proposition 7.14. *Suppose that ϕ defines a birational isomorphism with $\mathcal{V}$. Then, the variety $\mathcal{V}$ is defined over $\mathbb{K}$ if and only if $\mathcal{Z}$ has an irreducible component defined over $\mathbb{K}$ which is $\mathbb{K}$-birational to $\mathcal{V}$. Moreover, $\mathcal{V}$ is reparametrizable over $\mathbb{K}$ if and only if $\mathcal{Z}$ has an irreducible component parametrizable over $\mathbb{K}$ which is $\mathbb{K}$-birational to $\mathcal{V}$.*

Proof. If $\mathcal{V}$ is defined over $\mathbb{K}$, we know by Theorem 7.11 that the restriction $\Phi : Y \cap D_\delta \cap U \to \widetilde{\mathcal{W}}$ defines a finite to one map of degree equal to the degree of ϕ, in this case 1. That is, Φ defines over this restriction an algebraic isomorphism. As $\mathcal{V}$ is irreducible, the Zariski closure of $Y \cap D_\delta \cap U$ is an irreducible component of $\mathcal{Z}$, which is $\mathbb{K}$-birational to $\mathcal{V}$. Conversely, suppose that $\mathcal{Z}$ has a $\mathbb{K}$-component which is $\mathbb{K}$-birational to $\mathcal{V}$, then, by Theorem 6.22 $\mathcal{V}$ is $\mathbb{K}$-definable. Moreover, a $\mathbb{K}$-parametrization of $\mathcal{V}$ can be translated, by the map that defines the isomorphism, to some component of $\mathcal{Z}$ which should be (by the first part of this proposition) $\mathbb{K}$-birational with $\mathcal{V}$, and conversely; proving, in this way, the second statement. □

7.4 Hyperquadrics

Proposition 7.14 reduces, under the hypothesis of birationality, checking the $\mathbb{K}$-parametrizability of $\mathcal{V}$ to finding the same property over a suitable component of $\mathcal{Z}$. The key issue is that the component we are looking for over $\mathcal{Z}$ has necessarily to be of some special kind, an α-hyperquadric (as defined below) and, thus, this fact helps deciding if it exists, or not, one such component.

Let θ be an $\mathbb{F}$-automorphism of the field of rational functions in m variables

$$\theta : \mathbb{F}(t_1, \ldots, t_m) \to \mathbb{F}(t_1, \ldots, t_m)$$

that we suppose given by the substitution

$$t_1 = \theta_1(t_1, \ldots, t_m), \ldots, t_m = \theta_m(t_1, \ldots, t_m).$$

Suppose that the coefficients of θ_j belong to $\mathbb{L} = \mathbb{K}(\alpha)$ and develop each rational function θ_j in terms of the base elements:

$$\theta_j(t_1, \ldots, t_m) = \sum_{i=0}^{d-1} \theta_{ji}(t_1, \ldots, t_m)\alpha^i.$$

Definition 7.15. An α-hyperquadric is the variety in $\mathbb{F}^{md}$ parametrized by the components $\theta_{ji}(t_1, \ldots, t_m), j = 1, \ldots, m, i = 0, \ldots, d-1$ of an automorphism θ of $\mathbb{L}(t_1, \ldots, t_m)$ in the base $1, \alpha, \ldots, \alpha^{d-1}$

This definition has its origins in the work [ARS97] for the case of curves. With the help of this concept we may precise the parametrizations considered in the previous Section.

Now, suppose that $Y \cap D_\delta \cap U$ has a component that is an α-hyperquadric parametrized by

$$t_{ji} = \theta_{ji}(u_1, \ldots, u_m) \in \mathbb{K}(u_1, \ldots, u_m),$$

$j = 1, \ldots, n$, $i = 0, \ldots, d-1$. Composing with η and then with ϕ we have that

$$\phi(\eta(\theta_{(j)}(u))) = \left(\phi_1\Big(\sum_{i=0}^{d-1} \theta_{1i}(u)\alpha^i\Big), \ldots, \phi_n\Big(\sum_{i=0}^{d-1} \theta_{mi}(u)\alpha^i\Big)\right) = \phi(\theta_k(u))$$

is a parametrization of $\mathcal{V}$. Moreover, as the point $(\theta_{(1)}(u); \ldots; \theta_{(m)}(u))$ is in $\mathcal{Z}$, it happens that $\phi_{ki}(\theta_{(1)}(u); \ldots; \theta_{(m)}(u)) = 0$ for every $i > 0$. So $\psi(\Phi(\theta_{(j)}(u)))$ is a parametrization of the diagonal Δ and, by the commutativity of 7.1

$$\Pi(\eta(\theta_{(j)}(u)) = \psi(\Phi(\theta_{(j)}(u))) = (\phi_{10}(u), \ldots, \phi_{n0}(u))^d$$

Hence, $\phi_k(\theta(u)) = \phi_{k0}(u)$, so we obtain a parametrization of $\mathcal{V}$ with coefficients in $\mathbb{K}$. That is, the substitution $t_j = \sum_{i=0}^{d-1} \theta_{ji}(u)\alpha^i$, $j = 1, \ldots, m$ transforms the given parametrization into a parametrization over $\mathbb{K}$. Conversely, let $\phi(t)$ be a birational parametrization of $\mathcal{V}$ and suppose that $\mathcal{V}$ is parametrizable over $\mathbb{K}$. Let $\xi : \mathbb{F}^m \to \mathcal{V}$ be a rational parametrization of $\mathcal{V}$ over $\mathbb{K}$. In particular, $\mathcal{V}$ is defined over $\mathbb{K}$ and $\mathcal{V} = \mathcal{V}^{\sigma_l}$ for all l. In this case, the right column in Figure 7.1 corresponding to the parametrization ξ is

$$\begin{array}{rccc} \Pi_\xi = \xi \times \cdots \times \xi : & (\mathbb{F}^m)^d & \longrightarrow & \mathcal{V}^d \\ & (s, s^{\sigma_2}, \ldots, s^{\sigma_d}) & \mapsto & (\xi(s), \xi(s^{\sigma_2}), \ldots, \xi(s^{\sigma_d})) \end{array}$$

The points in the diagonal of the product corresponds to the values $s = s^{\sigma_2} = \cdots = s^{\sigma_d}$. The parametrizations ϕ and ξ are related by an isomorphism of the field of rational functions $\mathbb{F}(s_1, \ldots, s_m) \to \mathbb{F}(t_1, \ldots, t_m)$ that we suppose given by the substitution

$$t_1 = \theta_1(s_1, \ldots, s_m), \ldots, t_m = \theta_m(s_1, \ldots, s_m),$$

so $\xi(s) = \phi(\theta(s))$. Developing each rational function θ_j with respect to the base:

$$\theta_j(s) = \sum_{k=0}^{d-1} \theta_{jk}(s)\alpha^k$$

we have that

$$\eta(\theta_{10}(s), \ldots, \theta_{1,d-1}(s); \ldots; \theta_{m0}(s), \ldots, \theta_{m,d-1}(s)) = \\ = (\theta(s); \theta^{\sigma_2}(s); \ldots; \theta^{\sigma_d}(s))$$

for each s, and Π send these points into the diagonal. Finally, we get that the coefficients

$$t_{ji} = \theta_{ji}(s_1, \ldots, s_m) \in \mathbb{K}(u_1, \ldots, u_m),\ k = 1, \ldots, m,\ i = 1, \ldots, d-1$$

in the development of θ give a parametrization of the open set $Y \cap D_\delta \cap U$ of $\mathcal{Z}$ which is $\mathbb{K}$-birational to $\widetilde{\mathcal{W}}$. This provides the following result:

Theorem 7.16. *Suppose that ϕ is a birational parametrization, then:*

1. *if a component of $Y \cap D_\delta \cap U$ can be parametrized by $t_{ji} = \theta_{ji}(u_1, \ldots, u_m) \in \mathbb{K}(u_1, \ldots, u_m)$, a parametrization of $\mathcal{V}$ over $\mathbb{K}$ can be obtained from ϕ by the change of parameter $t_j = \sum_{i=0}^{d-1} \theta_{ji}(u)\alpha^i$.*
2. *if $\mathcal{V}$ is $\mathbb{K}$-parametrizable, then the variety $Y \cap D_\delta \cap U$ has a component which is parametrizable over $\mathbb{K}$ whose parametrization is given by the components of an automorphism of $\mathbb{L}(t_1, \ldots, t_m)$ in the base $\{1, \alpha, \ldots, \alpha^{d-1}\}$.*

Thus, $\mathcal{V}$ is $\mathbb{K}$-parametrizable if and only if $Y \cap D_\delta \cap U$ has one component which is an α-hyperquadric and the fiber of Φ on all the other components is non-generic.

This theorem provides information that may be useful from a computational point of view to determine whether a parametric variety is $\mathbb{K}$-parametrizable or not. In the following Chapter we will focus in the case where $\mathcal{V}$ is a curve.

7.5 Examples and Counterexamples

In this Section we provide Examples of how the results in this Chapter are applied, and also Counterexamples to the impossibility of relaxing the hypothesis of some Theorems.

First, all our assumptions on the Weil variety are given for an irreducible variety. In principle, the Weil variety can be applied to any variety, in Corollary 7.4 it is proved that $\mathcal{V}$ is defined over $\mathbb{K}$ if and only if $\dim(\mathcal{V}) = \dim(\widetilde{\mathcal{W}})$. Next, it is shown that the irreducibility is necessary for that Corollary.

Example 7.17. Let $\mathbb{K} = \mathbb{Q}$, $\alpha = \sqrt{2}$, $\mathcal{V} = \{x^2 + (-\sqrt{2} - 1)x + \sqrt{2} = 0\} = \{1, \sqrt{2}\} \subseteq \mathbb{F}$. By Theorem 6.17 $\mathcal{V}$ is not defined over $\mathbb{K}$. The equations of $\mathcal{W}$ are obtained after substitution x by $x_0 + \sqrt{2}x_1$, $\mathcal{W} = \mathfrak{V}_{\mathbb{F}}(y_0^2 + 2y_1^2 - y_0, 2y_0y_1 - y_0 - y_1 + 1) \subseteq \mathbb{F}^2$. $\widetilde{\mathcal{W}}$ is the variety defined by $\{y_1, y_0^2 - y_0, -y_0 + 1\}$. That is, $\widetilde{\mathcal{W}} = \{(1, 0)\}$. In this case $\dim(\widetilde{\mathcal{W}}) = \dim(\mathcal{V}) = 0$, but $\mathcal{V}$ is not defined over $\mathbb{K}$. Note that $\widetilde{\mathcal{W}}$ is isomorphic to $\{1\}$ which is the largest subset of $\mathcal{V}$ invariant by conjugation.

Let us show that the second item of Theorem 7.11 does not imply that $\mathcal{V}$ is a $\mathbb{K}$-variety if we drop the condition $\dim(\mathcal{V}) = \dim(\widetilde{\mathcal{W}})$.

Example 7.18. Let $\mathbb{K} = \mathbb{Q}$, $\phi = (t, \sqrt{2}t)$ a line in the plane. Its implicit equation is $y - \sqrt{2}x$, so

$$\mathcal{W} = \{y_0 - 2x_1 = y_1 - x_0 = 0\}.$$

$$\widetilde{\mathcal{W}} = \{y_0 - 2x_1 = y_1 - x_0 = x_1 = y_1 = 0\} = \{(0,0,0,0)\}.$$

The parametrization of $\mathcal{W}$ given by development of ϕ is:

$$\Phi(t_0, t_1) = (t_0, t_1, 2t_1, t_0).$$

$Y = \{t_1 = t_0 = 0\} = \{(0,0)\}$. Moreover, every polynomial is linear, hence $D_\delta = \mathbb{F}^2$, $U = Y$. Thus $Y \cap D_\delta \cap U$ is birational to $\widetilde{\mathcal{W}}$ by Φ. In particular $\dim(Y \cap D_\delta \cap U) = \dim(\widetilde{\mathcal{W}})$. But $\mathcal{V}$ is not $\mathbb{K}$-definable here. This happens because $\dim(\mathcal{V}) > \dim(\widetilde{\mathcal{W}})$.

Let us show that if we drop the condition of $\mathbb{K}$-definability in the component of $Y \cap D_\delta$ $\mathbb{K}$-birational to $\mathcal{V}$ then the Proposition 7.14 does not hold.

Example 7.19. Let $\mathbb{K} = \mathbb{Q}$, $\mathbb{L} = \mathbb{Q}(i)$, $\mathcal{V} = \{x + y + iz = 0\}$ given by the birational parametrization

$$\phi = (iu + iuv, iu - iuv^2, -2u - uv + uv^2)$$

with inverse

$$v = \frac{x - y}{x}, u = \frac{iz^2 + 2zy - iy^2}{2x - y}$$

Note that the parametrization is polynomial, so D_δ is the whole plane. $\mathcal{Z}$ is the variety defined by the ideal:

$$(u_0 + u_0v_0 - u_1v_1, u_0 - u_0v_0^2 + u_0v_1^2 + 2u_1v_0v_1, -2u_1 - u_0v_1 - u_1v_0 + 2u_0v_0v_1 + u_1v_0^2 - u_1v_1^2)$$

The components (over $\mathbb{C}$) of this ideal are:

$$(u_1, u_0), (v_1, v_0 - 2, u_0), (v_1, v_0 + 1)$$

$$(v_0 + v_1 i + 1, u_0 - u_1 i), (v_0 - v_1 i + 1, u_0 + u_1 i).$$

As $\mathcal{V}$ is not definable over $\mathbb{K}$, it cannot be $\mathbb{K}$-birational to none of the three first ideals. We are proving that the fourth component $\mathcal{Z}_4 = \{v_0 - v_1 i + 1, = u_0 + u_1 i = 0\}$ is $\mathbb{K}$-birational to $\mathcal{V}$. The birational map is:

$$\begin{array}{ccc|ccc} \mathbb{C}(\mathcal{V}) & \longrightarrow & \mathbb{C}(\mathcal{Z}_4) & \mathbb{C}(\mathcal{Z}_4) & \longrightarrow & \mathbb{C}(\mathcal{V}) \\ x & \mapsto & u_1 - v_0 & u_0 & \mapsto & z \\ y & \mapsto & v_0 & u_1 & \mapsto & x + y \\ z & \mapsto & u_0 & v_0 & \mapsto & y \\ & & & v_1 & \mapsto & \frac{z(y+1)}{x+y} \end{array}$$

This example does not contradict Proposition 7.14 since $\mathcal{V}$ is not $\mathbb{K}$-birational to a $\mathbb{K}$-component of $\mathcal{V}$ but to a $\mathbb{L}$-component of it.

Example 7.20. In this Example we show a plane that is not defined over $\mathbb{Q}$ but whose variety $\mathcal{Z}$ is another plane parametrized over $\mathbb{Q}$. Let $\alpha = \sqrt{2}$ and consider the following parametrization with coefficients in $\mathbb{Q}[\alpha]$ of the plane $\mathcal{V} = \{z = \alpha x + y\}$ plane in $\mathbb{C}^3$:

$$\phi = \begin{cases} x(u,v) = u \\ y(u,v) = uv \\ z(u,v) = \alpha u + uv \end{cases}$$

Clearly $\mathcal{V}$ is not a $\mathbb{Q}$-variety. Note that the given parametrization ϕ is one to one on every point of $\mathcal{V}$ such that $x \neq 0$. The fiber over the point $(0,0,0)$ is the whole axis $u = 0$ and the parametrization does not cover the points $\{x = 0, y \neq 0\}$. The parametrization obtained by development is given by the substitution $u = u_0 + u_1\alpha$ and $v = v_0 + v_1\alpha$, then:

$$\begin{cases} x(u_0,u_1,v_0,v_1) = u_0 + \alpha u_1 \\ y(u_0,u_1,v_0,v_1) = (u_0v_0 + 2u_1v_1) + \alpha(u_0v_1 + u_1v_0) \\ z(u_0,u_1,v_0,v_1) = (u_0v_0 + 2u_1 + 2u_1v_1) + \alpha(u_0 + u_0v_1 + u_1v_0) \end{cases}$$

As the parametrization is polynomial, there are no denominator, $\delta = 1$ and the set Y coincides with $\mathcal{Z}$. The equations of Y are $\{u_1 = u_0v_1 + u_1v_0 = u_0 + u_0v_1 + u_1v_0 = 0\}$, that is, $\{u_1 = u_0 = 0\}$. Hence $\mathcal{Z}$ is a plane defined over $\mathbb{Q}$ and $\dim(\mathcal{Z}) = \dim(V)$, but V cannot be defined over $\mathbb{Q}$. The apparent contradiction with Theorem 7.11 comes because the whole set $\mathcal{Z}$ is contained in the set of points where the parametrization does not have a finite fiber $\{u = 0\}$. So $\mathcal{Z} \cap U = \emptyset$, where U is the open set defined in Theorem 7.11. On the other hand, notice that $\mathcal{Z}$ is not $\mathbb{Q}$-birational to $\mathcal{V}$, so there is no contradiction with Proposition 7.14.

Substituting α by a d-th root of 2, we obtain a variety $\mathcal{Z}$ of dimension d, this shows that the witness variety can have arbitrarily high dimension.

Example 7.21. Here, we present a plane defined over $\mathbb{Q}$ such that the variety $\mathcal{Z}$ has two components of different dimensions. Let α be a cubic root of 2 and consider the following parametrization in $\mathbb{Q}[\alpha]$ of the plane $\mathcal{V} = \{z = x + y\}$ in $\mathbb{C}^3$:

$$\begin{cases} x(u,v) = \alpha u \\ y(u,v) = (\alpha + 2)uv \\ z(u,v) = \alpha u + (\alpha + 2)uv \end{cases}$$

As in the previous example, the parametrization is one to one in every point of $\mathcal{V}$ such that $x \neq 0$ and the fiber over the point $(0,0,0)$ is the axis $u = 0$. The substitutions $u = u_0 + u_1\alpha + u_2\alpha^2$, $v = v_0 + v_1\alpha + v_2\alpha^2$ give the following equations of $Y = \mathcal{Z}$ (again, $\delta = 1$):

$$\mathcal{Z} = \{u_0 = u_1 = 0, v_0 + v_2 = 0, v_1 + 2v_2 = 0\} \cup \{u_0 = u_1 = u_2 = 0\}$$

The second component of $\mathcal{Z}$ has dimension 3 in $\mathbb{C}^6$ and is completely contained in the closed set of $\mathbb{C}^6$ where the parametrization is not finite to one. So it does not give any information on the definability of $\mathcal{V}$ over $\mathbb{Q}$. Nevertheless, the first component is a finite

to one map and, by Theorem 7.11, this means that $\mathcal{V}$ is defined over $\mathbb{Q}$. Furthermore, it provides a parametrization of $\mathcal{V}$ over $\mathbb{Q}$. By Theorem 7.16, it suffices to take $u_0 = u_1 = 0$, $v_0 = -v_2$ and $v_1 = -2v_2$ (a parametrization of the first components with parameters v_2, u_2) in the previous change of coordinates. Hence, is we take $u = \alpha^2 s$, $v = (-1 - 2\alpha + \alpha^2)t$ we obtain the parametrization of $\mathcal{V}$:

$$\begin{cases} x(s,t) = s \\ y(s,t) = -5st \\ z(s,t) = s - 5st \end{cases}$$

Next example shows that the consideration of δ is essential even in the case of curves.

Example 7.22. Let α be a root of $z^4 - 2$ and take the following parametrization of a planar curve over $\mathbb{Q}[\alpha]$:

$$\begin{cases} x(t) = \dfrac{t}{t+1} \\ \\ y(t) = \dfrac{\alpha t}{t+1} \end{cases}$$

This curve is the line $y = \alpha x$ in $\mathbb{C}^2$, so it does not admit equations over $\mathbb{Q}$. The substitution of the parameters $t = t_0 + t_1\alpha + t_2\alpha^2 + t_3\alpha^3$ in the parametrization allows the computation of δ:

$$\begin{aligned} \delta \;=\; & 1 - 2\,{t_1}^4 + {t_0}^4 + 4\,{t_0}^3 - 16\,t_0\,t_1\,t_3 + 8\,{t_1}^2\,t_2\,t_0 - 16\,t_1\,{t_2}^2\,t_3 - 8\,t_1\,t_3\,{t_0}^2 + \\ & + 16\,t_2\,{t_3}^2\,t_0 - 4\,{t_2}^2 - 8\,t_1\,t_3 + 8\,{t_1}^2\,t_2 + 16\,t_2\,{t_3}^2 - 8\,{t_2}^2\,t_0 + \\ & + 8\,{t_1}^2\,{t_3}^2 - 4\,{t_2}^2\,{t_0}^2 + 4\,{t_2}^4 - 8\,{t_3}^4 + 4\,t_0 + 6\,{t_0}^2 \end{aligned}$$

The auxiliary variety Y is defined as the zero set of the polynomials:

$f_1 = -16{t_3}^4 + 6{t_0}^3 - 4{t_2}^2 - 4{t_1}^4 + 8{t_2}^4 + 2t_0 - 32t_1{t_2}^2t_3 + 2{t_0}^4 + 16{t_1}^2t_2t_0 - 16t_1t_3{t_0}^2 + 32t_2{t_3}^2t_0 - 24t_0t_1t_3 + 12{t_1}^2t_2 + 16{t_1}^2{t_3}^2 + 24t_2{t_3}^2 - 8{t_2}^2{t_0}^2 - 8t_1t_3 - 12{t_2}^2t_0 + 6{t_0}^2$

$f_2 = 4\,t_0\,t_1 - 8\,t_2\,t_3 + 4\,t_1\,{t_2}^2 - 4\,{t_1}^2\,t_3 + 2\,{t_0}^2\,t_1 + 2\,t_1 + 8\,{t_3}^3 - 8\,t_0\,t_2\,t_3$

$f_3 = 8\,t_2\,t_1\,t_3 - 2\,{t_1}^2 + 2\,t_2 - 4\,{t_2}^3 - 4\,{t_3}^2 + 4\,t_2\,t_0 - 2\,t_0\,{t_1}^2 + 2\,t_2\,{t_0}^2 - 4\,{t_3}^2\,t_0$

$f_4 = 4\,t_0\,t_1 - 8\,t_2\,t_3 + 4\,t_1\,{t_2}^2 - 4\,{t_1}^2\,t_3 + 2\,{t_0}^2\,t_1 + 2\,t_1 + 8\,{t_3}^3 - 8\,t_0\,t_2\,t_3$

$f_5 = 8\,t_2\,t_1\,t_3 - 2\,{t_1}^2 + 2\,t_2 - 4\,{t_2}^3 - 4\,{t_3}^2 + 4\,t_2\,t_0 - 2\,t_0\,{t_1}^2 + 2\,t_2\,{t_0}^2 - 4\,{t_3}^2\,t_0$

$f_6 = 2\,t_3 + 2\,t_3\,{t_0}^2 - 4\,t_1\,t_2\,t_0 - 4\,t_1\,{t_3}^2 + 4\,{t_2}^2\,t_3 - 4\,t_1\,t_2 + 2\,{t_1}^3 + 4\,t_3\,t_0$

It can be checked that Y contains the plane in $\mathbb{C}^4$:

$$\begin{aligned} t_0 + \alpha t_1 + \alpha^2 t_2 + \alpha^3 t_3 &= -1 \\ t_0 + \alpha_1 t_1 + \alpha_1^2 t_2 + \alpha_1^3 t_3 &= -1 \end{aligned}$$

and its conjugates. If we take the same parametrization with α of degree d arbitrarily high, we obtain a variety Y of dimension $d-2$ arbitrarily high. However, it is easy to see that these planes are contained in the zero set of $\delta = \prod_{i=0}^{3}(t_0 + \alpha_i t_1 + \alpha_i^2 t_2 + \alpha_i^3 t_3 + 1)$, so $Y \cap D_\delta = \{(0,0,0,0)\}$. This proves that $\mathcal{V}$ is not defined over $\mathbb{Q}$.

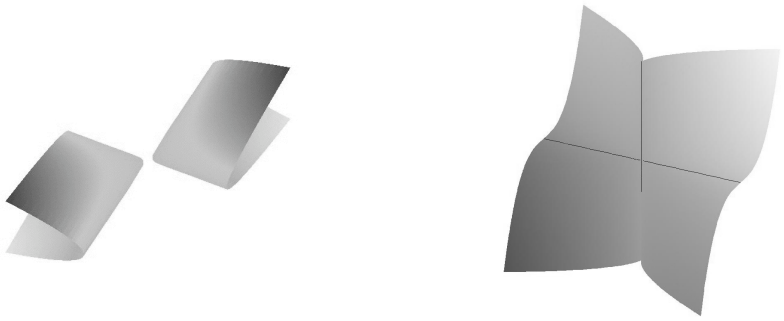


Figure 7.2: Projection of $\mathcal{Z}$ over the space (u_0, u_1, u_2) (left) and (u_0, v_1, v_2) (right)

Example 7.23. Let $\alpha = \sqrt[3]{2}$ and consider the surface parametrized by

$$\begin{cases} x(u,v) = -\dfrac{\alpha u^2 - \alpha^2 uv}{v} \\ y(u,v) = u - \alpha v \\ z(u,v) = \dfrac{\alpha^2 u^2}{v^2} \end{cases}$$

By the substitution $u = u_0 + u_1\alpha + u_2\alpha^2$ and $v = v_0 + v_1\alpha + v_2\alpha^2$ in $x(u,v)$, $y(u,v)$, $z(u,v)$ and by normalization, we obtain the denominator:

$$\delta = (4v_2^3 - 6v_2v_1v_0 + v_0^3 + 2v_1^3)^2,$$

and six polynomials in $\mathbb{Q}[u_0, u_1, u_2, v_0, v_1, v_2]$. The polynomials corresponding to α and α^2 in the numerators of $x(u_0 + u_1\alpha + u_2\alpha^2, v_0 + v_1\alpha + v_2\alpha^2)$, $y(u_0 + u_1\alpha + u_2\alpha^2, v_0 + v_1\alpha + v_2\alpha^2)$ and $z(u_0 + u_1\alpha + u_2\alpha^2, v_0 + v_1\alpha + v_2\alpha^2)$ define the set Y.

Using the computer algebra software Maple and Singular, we deduce that the witness variety $\mathcal{Z}$ represents a variety of dimension 2 whose implicit equations are:

$$-u_0u_1 + 2u_2^2 = 0, v_0 - u_1 = 0, v_1 - u_2 = 0, u_0v_2 - u_1u_2 = 0, 2u_2v_2 - u_1^2 = 0,$$

$$v_0^2 - 2v_1v_2, -v_0v_1 + u_0v_2, u_0v_0 - 2v_1^2, u_2 - v_1, u_1 - v_0,$$

this variety is parametrized by

$$\begin{cases} u_0 = 2s^2/t \\ u_1 = t \\ u_2 = s \end{cases} \qquad \begin{cases} v_0 = t \\ v_1 = s \\ v_2 = t^2/2s \end{cases}$$

The substitution

$$\begin{cases} u = 2\frac{s^2}{t} + \alpha t + \alpha^2 s \\ v = t + \alpha s + \frac{t^2}{2s}\alpha^2 \end{cases}$$

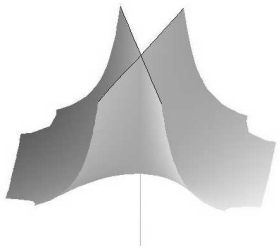


Figure 7.3: Whitney umbrella

transforms the given parametrization into the rational parametrization

$$\begin{cases} x(s,t) = \frac{-4s^3+2t^3}{t^2} \\ y(s,t) = \frac{2s^3-t^3}{st} \\ z(s,t) = \frac{4s^2}{t^2} \end{cases}$$

that represents the Whitney's umbrella $x^2 - zy^2 = 0$ (see Figure 7.3).

The previous substitution is in fact a change of variables, that is, a isomorphism between $\mathbb{C}(u,v)$ and $\mathbb{C}(s,t)$, with inverse

$$s := \frac{vu^2}{2v^2 + \alpha^2 uv + \alpha u^2}, \quad t := \frac{v^2 \alpha u}{2v^2 + \alpha^2 uv + \alpha u^2}$$

and hence, $\mathcal{Z}$ is a 2-dimensional hyperquadric associated to this isomorphism.

Chapter 8

Geometry of Hypercircles

In this Chapter we present a deep study of the geometry of hypercircles. Hypercircles are hypercuadrics of dimension 1. That is, hypercuadrics given by an automorphism of $\mathbb{F}(t)$ into itself. The best known family of hypercircles are circles themselves. Namely, let $\mathbb{R} \subseteq \mathbb{C}$ be our extension of fields, let $\frac{at+b}{ct+d} \in \mathbb{C}(t) \setminus \mathbb{C}$ be any unit under composition of $\mathbb{C}(t)$. Then, $u(t) = \phi_1(t) + i\phi_2(t)$, $\phi_1, \phi_2 \in \mathbb{R}(t)$. If $c \neq 0$ and $d/c \notin \mathbb{R}$, then $(\phi_1(t), \phi_2(t))$ parametrizes a real circle in $\mathbb{C}^2$. Hence, the geometric properties of hypercircles are in particular properties of circles (avoiding some *degenerate cases*, similar to the case where $d/c \in \mathbb{R}$ in this comparison, that produces a real line in the plane). Thus, we will try to obtain the geometric properties of hypercircles by comparison with circles in many cases.

8.1 First Properties of Hypercircles

In this Section we begin with the formal definition of a hypercircle. $\mathbb{L} = \mathbb{K}(\alpha)$ is an algebraic extension of a characteristic zero field $\mathbb{K}$ such that $[\mathbb{L} : \mathbb{K}] = n$.

Definition 8.1. An *α-hypercircle* is an α-hypercuadric of dimension 1. That is, let $u(t)$ be a unit in $\mathbb{L}(t)$, where $\mathbb{L} = \mathbb{K}(\alpha)$. Let

$$u(t) = \sum_{i=0}^{n-1} \phi_i(t)\alpha^i$$

where $\phi_i(t) \in \mathbb{K}(t)$, for $i = 0, \ldots, n-1$. The α-hypercircle $\mathcal{U}$ generated by $u(t)$ is the rational curve in $\mathbb{F}^n$ parametrized by $\phi(t) = (\phi_0(t), \ldots, \phi_{n-1}(t))$.

As we have fixed the base $\{1, \alpha, \ldots, \alpha^{n-1}\}$ of $\mathbb{K}(\alpha)(t)$, the expansion of $u(t)$ is unique. In Section 7.4 we have not given a way to compute the parametrization of a hypercuadric, but this is easy for the case of hypercircles. The parametrization can be obtained by rationalizing the denominator as follows: suppose given the unit $u(t) = \frac{at+b}{ct+d}$, $c \neq 0$ (remark that, if $c = 0$, it is straightforward to obtain $\phi(t)$), and the

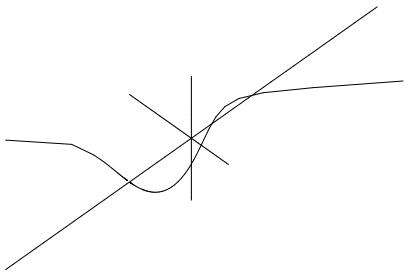


Figure 8.1: A hypercircle in $\mathbb{R}^3$

extension $\mathbb{K} \subseteq \mathbb{K}(\alpha)$. Let $M(t)$ be the minimal polynomial of $-d/c$ over $\mathbb{K}$. Compute the quotient $m(t) = \frac{M(t)}{ct+d} \in \mathbb{K}(\alpha)[t]$ and develop the unit as

$$\frac{at+b}{ct+d} = \frac{(at+b)m(t)}{M(t)} = \frac{p_0(t) + p_1(t)\alpha + \cdots + p_{n-1}(t)\alpha^{n-1}}{M(t)}$$

where $p_i(t) \in \mathbb{K}[t]$. From this, $\phi(t) = \left(\frac{p_0(t)}{M(t)}, \ldots, \frac{p_{n-1}(t)}{M(t)}\right)$ is the parametrization associated to $u(t)$. Remark that $\gcd(p_0(t), \ldots, p_{n-1}(t), M(t)) = 1$. Moreover, it is clear that $\mathbb{F}(\phi_0(t), \ldots, \phi_{n-1}(t)) = \mathbb{F}(t)$. So this parametrization is proper in $\mathbb{F}$, and it follows from the results in [AGR96] that also $\mathbb{K}(\phi_0(t), \ldots, \phi_{n-1}(t)) = \mathbb{K}(t)$.

Example 8.2. Let us consider the algebraic extension $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$, where $\alpha^3+2\alpha+2 = 0$. The unit $\frac{t-\alpha}{t+\alpha}$ has an associated hypercircle parametrized by

$$\phi(t) = \left(\frac{t^3+2t+2}{t^3+2t-2}, \frac{-2t^2}{t^3+2t-2}, \frac{2t}{t^3+2t-2}\right)$$

A picture of the spatial real curve is shown in Figure 8.1

As it stands, the definition of a hypercircle $\mathcal{U}$ depends on a given unit $u(t) \in \mathbb{L}(t)$ and on a primitive generator α of an algebraic extension $\mathbb{L}$. In what follows we will analyze the effect on $\mathcal{U}$ when varying some of these items, searching for a simple representation of a hypercircle to ease studying its geometry.

First notice that, given a unit $u(t) \in \mathbb{L}(t)$ and two different primitive elements α and β of the extension $\mathbb{K} \subseteq \mathbb{L}$, we can expand the unit in two different ways $u(t) = \sum_{i=0}^{n-1} \alpha^i \phi_i(t) = \sum_{i=0}^{n-1} \beta^i \psi_i(t)$. The hypercircles $\mathcal{U}_\alpha \cong (\phi_0(t), \ldots, \phi_{n-1}(t))$ and $\mathcal{U}_\beta \cong (\psi_0(t), \ldots, \psi_{n-1}(t))$ generated by $u(t)$ are different curves in $\mathbb{F}^n$, see Example 8.3. Nevertheless, let $\mathcal{A} \in \mathcal{M}_{n\times n}(\mathbb{K})$ be the matrix of change of basis from $\{1, \alpha, \ldots, \alpha^{n-1}\}$ to $\{1, \beta, \ldots, \beta^{n-1}\}$. Then, $\mathcal{A}(\phi_0(t), \ldots, \phi_{n-1}(t))^t = (\psi_0(t), \ldots, \psi_{n-1}(t))^t$. That is, it carries one of the curve onto the other. Thus, $\mathcal{U}_\alpha$ and $\mathcal{U}_\beta$ are related by the affine

transformation induced by the change of basis and, so, they share many important geometric properties.

In the sequel, if there is no confusion about the algebraic extension and the primitive element, we will simply call $\mathcal{U}$ a hypercircle.

Example 8.3. Let us consider the algebraic extension $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$, where $\alpha^4 + 1 = 0$. Let us take the unit $u(t) = \frac{t-\alpha}{t+\alpha}$. By normalizing $u(t)$, we obtain the parametrization $\phi(t)$ associated to $u(t)$:

$$\phi(t) = \left(\frac{t^4-1}{t^4+1}, \frac{-2t^3}{t^4+1}, \frac{2t^2}{t^4+1}, \frac{-2t}{t^4+1}\right).$$

This hypercircle $\mathcal{U}_\alpha$ is the zero set of $\{x_1x_2 - x_3x_0 - x_3, x_1^2 + x_3^2 - 2x_2, x_1x_0 + x_2x_3 - x_1, x_0^2 + x_3x_1 - 1\}$. Now, we take $\beta = \alpha^3 + 1$, instead of α, as the primitive element of $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$. The same unit $u(t)$ generates the β-hypercircle $\mathcal{U}_\beta$ parametrized by

$$\psi(t) = \left(\frac{t^4+2t^3-2t^2+2t-1}{t^4+1}, \frac{-6t^3+4t^2-2t}{t^4+1}, \frac{6t^3-2t^2}{t^4+1}, \frac{-2t^3}{t^4+1}\right),$$

which is different to $\mathcal{U}_\alpha$; note that $\psi(1) = (1, -2, 2, -1)$ that does not satisfy the equation $x_0^2 + x_3x_1 - 1 = 0$ of $\mathcal{U}_\alpha$.

On the other hand it is well known that a given parametric curve can be parametrized over a given field $\mathbb{S}$ by different proper parametrizations, precisely, those obtained by composing to the right a given proper parametrization by a unit in $\mathbb{S}(t)$. In this way, we have a bijection between α-hypercircles and the equivalence classes of units of $\mathbb{K}(\alpha)(t)$ under the equivalence relation "$u \sim v$ *if and only if* $u(t) = v(\tau(t))$ *for a unit* $\tau(t) \in \mathbb{K}(t)$" (fixing the correspondence, between a unit in $\mathbb{K}(\alpha)(t)$ and a hypercircle, by means of the expansion of the unit in terms of powers of α).

More interesting is to analyze, on a hypercircle defined by a unit $u(t)$, the effect of composing it to the left with another unit $\tau(t) \in \mathbb{K}(\alpha)(t)$, that is, of getting $\tau(u(t))$. For instance, $\tau(t)$ could be $\tau(t) = t + \lambda$ or $\tau(t) = \lambda t$, or $\tau(t) = 1/t$, with $\lambda \in \mathbb{K}(\alpha)^*$. Every unit is a sequence of compositions of these three simpler cases, for instance, when $c \neq 0$, we have

$$t \longmapsto ct \longmapsto ct + d \longmapsto \frac{1}{ct+d} \longmapsto \frac{bc-ad}{c}\frac{1}{ct+d} \longmapsto$$

$$\longmapsto \frac{a}{c} + \frac{bc-ad}{c}\frac{1}{ct+d} = \frac{at+b}{ct+d} = u(t).$$

Therefore, studying their independent effect is all we need to understand completely the behavior of a hypercircle under left composition by units.

For circles, adding a complex number to the unit that defines the circle correspond to a translation of the circle. Multiplying it by a complex number acts as the composition of a rotation and a dilation. And the application $\tau(t) = 1/t$ gives an inversion. The following lemma analyzes what happens in the general case.

Lemma 8.4. *Let $\mathcal{U}$ be the α-hypercircle generated by $u(t)$, and $\lambda = \sum_{i=0}^{n-1} \lambda_i \alpha^i \in \mathbb{K}(\alpha)^*$, where $\lambda_i \in \mathbb{K}$. Then,*

1. *$\lambda + u(t)$ is a unit generating the hypercircle obtained from $\mathcal{U}$ by the translation of vector $(\lambda_0, \ldots, \lambda_{n-1})$.*
2. *$\lambda u(t)$ is a unit generating the hypercircle obtained from $\mathcal{U}$ by the affine transformation over $\mathbb{K}$ given by the matrix of change of basis from $\mathcal{B}^\star = \{\lambda, \lambda\alpha, \ldots, \lambda\alpha^{n-1}\}$ to $\mathcal{B} = \{1, \alpha, \ldots, \alpha^{n-1}\}$.*

Proof. To prove (1), let $\phi(t) = (\phi_0(t), \ldots, \phi_{n-1}(t)) \in \mathbb{K}(t)^n$ be the parametrization of $\mathcal{U}$ obtained from $u(t)$. Then, $\lambda + u(t) = \sum_{i=0}^{n-1} (\lambda_i + \phi_i(t))\alpha^i$ generates the hypercircle parametrized by $(\lambda_0 + \phi_0(t), \ldots, \lambda_{n-1} + \phi_{n-1}(t)) \in \mathbb{K}(t)^n$, which is the translation of $\mathcal{U}$ of vector $(\lambda_0, \ldots, \lambda_{n-1})$. For the second assertion, let $\phi^\star(t) \in \mathbb{K}(t)^n$ be the parametrization of the hypercircle associated to the unit $\lambda u(t)$. The rational coordinates $\phi_i^\star(t)$ of $\phi^\star(t)$ are obtained from the matrix $\mathcal{A} = (a_{i,j}) \in \mathcal{M}_{n\times n}(\mathbb{K})$ of change of basis from $\mathcal{B}^\star$ to $\mathcal{B}$, for $i, j = 0, \ldots, n-1$. Indeed,

$$\lambda u(t) = \sum_{i=0}^{n-1} \phi_i(t)\lambda\alpha^i = \sum_{i=0}^{n-1} \phi_i(t) \left(\sum_{j=0}^{n-1} a_{ji}\alpha^j \right) = \sum_{j=0}^{n-1} \left(\sum_{i=0}^{n-1} a_{ji}\phi_i(t) \right) \alpha^j.$$

Then $\phi^\star(t)^t = \mathcal{A}\,\phi(t)^t$. □

Finally, the following lemma uses the previous results to transform affinely one hypercircle into another one whose unit is simpler.

Lemma 8.5. *Let $u(t) = \frac{at+b}{ct+d}$ be a unit and $\mathcal{U}$ its associated hypercircle.*

1. *If $c = 0$ then $\mathcal{U}$ is affinely equivalent over $\mathbb{K}$ to the line generated by $u^\star(t) = t$.*
2. *If $c \neq 0$ then $\mathcal{U}$ is affinely equivalent over $\mathbb{K}$ to the hypercircle $\mathcal{U}^\star$ generated by $u^\star(t) = \frac{1}{t+d/c}$*

Proof. This lemma follows from Lemma 8.4, taking into account that $u(t)$ is obtained from $u^\star(t)$ by the following composition:

$$u^\star(t) \mapsto \lambda_1 u^\star(t) \mapsto \lambda_1 u^\star(t) + \lambda_2 = u(t)$$

with suitable $\lambda_1, \lambda_2, u^\star$. If $c = 0$, then $\lambda_1 = \frac{a}{d} \neq 0$ and $\lambda_2 = \frac{b}{d}$ for $u^\star(t) = t$. Analogously, if $c \neq 0$, then $u(t)$ is obtained from $u^\star(t) = \frac{1}{t+d/c}$ taking $\lambda_1 = \frac{bc-ad}{c^2} \neq 0$ and $\lambda_2 = \frac{a}{c}$. □

Therefore the (affine) geometry of hypercircles can be reduced to those generated by a unit of type $\frac{1}{t+d}$ (then we say the unit is in *reduced form*). The simplest hypercircle of this kind is given by $\frac{1}{t+d}$, when $d \in \mathbb{K}$. It is the line parametrized by $(\frac{1}{t+d}, 0, \ldots, 0)$. In the complex case, units defining lines are precisely those given either by a polynomial unit in t (i.e. a unit without t at the denominator) or by a unit such that the root of the denominator is in $\mathbb{R}$. The same property holds for hypercircles.

Theorem 8.6. *Let $\mathcal{U}$ be the α-hypercircle associated to $u(t)$. Then, the following statements are equivalent:*

1. *$\mathcal{U}$ is a line.*
2. *$\mathcal{U}$ is associated to a polynomial unit.*
3. *The root of the denominator of every non polynomial unit generating $\mathcal{U}$ belongs to $\mathbb{K}$.*
4. *$\mathcal{U}$ is polynomially parametrizable (over $\mathbb{F}$).*
5. *$\mathcal{U}$ has one and only one branch (over $\mathbb{F}$) at infinity.*
6. *$\mathcal{U}$ is polynomially parametrizable over $\mathbb{K}$.*
7. *$\mathcal{U}$ has one and only one branch (over $\mathbb{K}$) at infinity.*

Proof. (1) $\Leftrightarrow$ (2). By definition, we know that hypercircles have a parametrization over $\mathbb{K}$. Thus, if $\mathcal{U}$ is a line, it can be parametrized as $(a_0t + b_0, \ldots, a_{n-1}t + b_{n-1})$, where $a_i\,, b_i \in \mathbb{K}$. Therefore, $u(t) = \left(\sum_{i=0}^{n-1} a_i\alpha^i\right) t + \sum_{i=0}^{n-1} b_i\alpha^i$ is a polynomial unit associated to $\mathcal{U}$. Conversely, let $u(t) = at + b \in \mathbb{L}(t)$, $a \neq 0$, be a polynomial unit associated to $\mathcal{U}$. Then $\mathcal{U}$ is the line parametrized by $\mathcal{P}(t) = (a_0t+b_0, \ldots, a_{n-1}t+b_{n-1}) \in \mathbb{K}[t]^n$, where $a = \sum_{i=0}^{n-1} a_i\,\alpha^i$ and $b = \sum_{i=0}^{n-1} b_i\,\alpha^i$.

(2) $\Leftrightarrow$ (3). Let $u(t) = at + b$ be a polynomial unit associated to $\mathcal{U}$, and let $u^\star(t)$ be another non polynomial unit associated to $\mathcal{U}$. Then, $u^\star(t) = u(\tau(t))$, where $\tau(t)$ is a unit of $\mathbb{K}\,(t)$. Therefore, the root of $u^\star(t)$ belongs to $\mathbb{K}$. Conversely, by Lemma 8.5, (3) implies (1), and we know that (1) implies (2).

(3) $\Leftrightarrow$ (4). Indeed, (3) implies (2) and therefore (4). Conversely, let $u(t)$ be a non-polynomial unit generating $\mathcal{U}$, and let $\phi(t) = (\phi_i)_{i=1,\ldots,n} \in \mathbb{K}(t)^n$ be the associated parametrization of $\mathcal{U}$. Then, $\phi(t)$ is proper, $\phi_i(t) = \frac{p_i(t)}{M(t)}$ with $\deg(p_i) \leq \deg(M)$ and $\gcd(p_0(t)\ldots p_{n-1}(t), M(t)) = 1$. Thus, the fact that $\mathcal{U}$ admits a polynomial parametrization, implies, by Abhyankar-Manocha-Canny's criterion of polynomiality (see [MC91]), that the denominator $M(t)$ is either constant or has only one root. Now, $M(t)$ can not be constant, since it is a minimal polynomial. Thus, M has only one root, and since it is irreducible, it must be linear. Moreover, since $M \in \mathbb{K}[t]$, its root is an element in $\mathbb{K}$.

(4) $\Leftrightarrow$ (5) This is, again, the geometric version of Abhyankar-Manocha-Canny's criterion. Same for (6) $\Leftrightarrow$ (7).

(4) $\Leftrightarrow$ (6) Obviously (6) implies (4). Conversely, if we have a polynomial parametrization over $\mathbb{F}$, it happens [AR07] that any proper parametrization must be either polynomial or in all its components the degree of the numerator must be smaller or equal than the degree of the denominator and, then, this denominator has only one single root over $\mathbb{F}$. So, since the parametrization $\phi(t)$ induced by the unit is proper, and by hypothesis $\mathcal{U}$ is polynomial, then $\phi(t)$ must be either polynomial (in which case we are done because $\phi(t)$ is over $\mathbb{K}$) or its denominator $M(t)$ has a single root $a \in \mathbb{F}$.

Now, reasoning as above one gets that $a \in \mathbb{K}$. So, a change of parameter, such as $t \mapsto \frac{1+as}{s}$ turns $\phi(t)$ into a $\mathbb{K}$-polynomial parametrization. □

As a corollary of this theorem, we observe that a parabola can never be a hypercircle, since it is polynomially parametrizable, but it is not a line. Nevertheless, it is easy to check that the other irreducible conics are indeed hypercircles for certain algebraic extensions of degree 2.

8.2 Main Geometric Properties.

This Section is devoted to the analysis on the main geometric properties of hypercircles. The key idea, when not dealing with lines, will be to use the reduction to units of the form $u(t) = \frac{1}{t+d}$, where $d \notin \mathbb{K}$ (see Lemma 8.5).

Theorem 8.7. *Let $\mathcal{U}$ be the α-hypercircle associated to the unit $u(t) = \frac{at+b}{t+d} \in \mathbb{K}(\alpha)(t)$ and let $r = [\mathbb{K}(-d) : \mathbb{K}]$. Then,*

1. *there exists an affine transformation $\chi : \mathbb{F}^n \longrightarrow \mathbb{F}^n$ defined over $\mathbb{K}$ such that the curve $\chi(\mathcal{U})$ is parametrized by*

$$\widetilde{\chi}(t) = \left(\frac{1}{M(t)}, \frac{t}{M(t)}, \ldots, \frac{t^{r-1}}{M(t)}, 0, \ldots, 0 \right).$$

2. *there exists a projective transformation $\rho : \mathbb{P}(\mathbb{F})^n \longrightarrow \mathbb{P}(\mathbb{F})^n$, defined over $\mathbb{K}$, such that the curve $\rho(\mathcal{U})$ is the rational normal curve of degree r in $\mathbb{P}(\mathbb{F})^n$, parametrized by*

$$\widetilde{\rho}(t : s) = [s^r : s^{r-1}t : \cdots : st^{r-1} : t^r : 0 : \cdots : 0].$$

Proof. For the case of lines the result is trivial. By Lemma 8.5, we can consider that $\mathcal{U}$ is the hypercircle associated to $u(t) = \frac{1}{t+d}$ and $r \geq 2$. Let $M(t) = t^r + k_{r-1}t^{k-1} + \cdots + k_0 \in \mathbb{K}[t], m(t) = \sum_{i=0}^{r-1} l_i t^i \in \mathbb{L}[t]$. With the notation of Section 8.1 and, since the numerator of $u(t)$ is 1, it holds that $m(t) = \sum_{i=0}^{n-1} p_i(t)\alpha^i$, $p_i(t) \in \mathbb{K}[t]$. Also, note that both $M(t)$ and the denominator of $u(t)$ are monic, and hence $l_{r-1} = 1$. First of all, we prove that there are exactly r polynomials in $\{p_i(t),\ i = 0, \ldots, n-1\} \subset \mathbb{K}[t]$ being linearly independent. For this purpose, we observe that the coefficients of $m(t)$, $\{1, l_{r-2}, \ldots, l_0\} \subset \mathbb{L}$, are linearly independent over $\mathbb{K}$. Indeed, from the equality $M(t) = (t+d)m(t)$, one has that $l_{r-i} = (-d)^{i-1} + (-d)^{i-2}k_{r-1} + \cdots + k_{r-i+1}$, for $i = 2, \ldots, r$. So, $\{1, l_{r-2}, \ldots, l_0\} \subset \mathbb{L}$ are $\mathbb{K}$–linearly independent, since otherwise one would find a non-zero polynomial of degree smaller than r vanishing at $-d$. Now, let $\vec{l_i} = (l_{i,0}, \ldots, l_{i,n-1})^t$ be the vector of coordinates of l_i in the base $\{1, \alpha, \ldots, \alpha^{n-1}\}$. Then, $\{\vec{1}, \vec{l_{r-2}}, \ldots, \vec{l_0}\} \subset \mathbb{K}^n$ are $\mathbb{K}$–linearly independent. Moreover, since $(p_0(t), \ldots, p_{n-1}(t))^t = \vec{1}t^{r-1} + \vec{l_{r-2}}t^{r-2} + \cdots + \vec{l_0}$, there are r polynomials p_{i_j}, $0 \leq i_1 < \cdots < i_r \leq n-1$, linearly independent. By simplicity, we assume w.l.o.g. that the first r polynomials are linearly independent. Observe that this is always possible

through a permutation matrix. The new curve, that we will continue denoting by $\mathcal{U}$, is not, in general, a hypercircle. In this situation, we proceed to prove (1) and (2).
In order to prove (1), let $\mathcal{A} \in \mathcal{M}_{n-r\times r}(\mathbb{K})$ be the matrix providing the linear combinations of the $n-r$ last polynomials in terms of the first r polynomials; i.e.

$$(p_r(t),\ldots,p_{n-1}(t))^t = \mathcal{A}(p_0(t),\ldots,p_{r-1}(t))^t.$$

Now, given the bases $\mathcal{B} = \{1,\ldots,t^{r-1}\}$ and $\mathcal{B}^\star = \{p_0(t),\ldots,p_{r-1}(t)\}$, let $\mathcal{M} \in \mathcal{M}_{r\times r}(\mathbb{K})$ be the transpose matrix of change of bases from $\mathcal{B}$ to $\mathcal{B}^\star$. Finally, the $n\times n$ matrix

$$\mathcal{Q} = \begin{pmatrix} \mathcal{M} & \mathcal{O}_{r,n-r} \\ -\mathcal{A} & I_{n-r} \end{pmatrix}$$

defines, under the previous assumptions, the affine transformation χ. Note that if $r = n$ then $\mathcal{Q} = \mathcal{M}$.
The proof of (2) is analogous to (1). Now, let consider the basis $\mathcal{B} = \{1,\ldots,t^{r-1},t^r\}$ and $\mathcal{B}^\star = \{p_0(t),\ldots,p_{r-1}(t),M(t)\}$. Let $\mathcal{A} \in \mathcal{M}_{n-r\times r+1}(\mathbb{K})$ be the matrix providing the linear combinations of the $n-r$ last polynomials in terms of basis $\mathcal{B}^\star$; i.e. $(p_r(t),\ldots,p_{n-1}(t))^t = \mathcal{A}(p_0(t),\ldots,p_{r-1}(t),M(t))^t$. Let $\mathcal{M} \in \mathcal{M}_{r+1\times r+1}(\mathbb{K})$ be the transpose matrix of change of bases from $\mathcal{B}$ to $\mathcal{B}^\star$. Finally, the $n+1\times n+1$ matrix

$$\mathcal{Q} = \begin{pmatrix} \mathcal{M} & \mathcal{O}_{r+1,n-r} \\ -\mathcal{A} & I_{n-r} \end{pmatrix}$$

defines, under the previous assumptions, the projective transformation ρ. Note that if $r = n$ then $\mathcal{Q} = \mathcal{M}$. □

As a direct consequence, we derive the following geometric properties of hypercircles.

Corollary 8.8. *In the hypothesis of Theorem 8.7*

1. *$\mathcal{U}$ defines a curve of degree r.*
2. *$\mathcal{U}$ is contained in a linear variety of dimension r and it is not contained in a variety of dimension $r-1$.*
3. *$\mathcal{U}$ is a regular curve in $\mathbb{P}(\mathbb{F})^n$.*
4. *The Hilbert function of $\mathcal{U}$ is equal to its Hilbert polynomial and $h_{\mathcal{U}}(m) = mn+1$.*

Proof. All these properties are well known to hold for the *rational normal curve of degree r* c.f. [Har92], [Har77], [Wal50]). □

In the following theorem, we classify the hypercircles that are affinely equivalent over $\mathbb{K}$. We will assume that the denominator of the generating units are not constant. The case where the units are polynomials are described in Theorem 8.6.

Theorem 8.9. *Let $\mathcal{U}_i$, $i = 1,2$, be α-hypercircles associated to $u_i(t) = \frac{a_i t+b_i}{t+d_i}$, and let $M_i(t)$ be the minimal polynomial of $-d_i$ over $\mathbb{K}$. Then, the following statements are equivalent:*

1. *$\mathcal{U}_1$ and $\mathcal{U}_2$ are affinely equivalent over $\mathbb{K}$.*
2. *There exists a unit $\tau(t) \in \mathbb{K}(t)$ such that it maps a root (and hence all roots) of $M_1(t)$ onto a root (resp. all roots) of $M_2(t)$.*

Proof. First of all note that, because of Theorem 8.6, the result for lines is trivial. For dealing with the general case, we observe that, by Lemma 8.5, we can assume that $u_i(t) = 1/(t + d_i)$. Next, suppose that $\mathcal{U}_1$ and $\mathcal{U}_2$ are affinely equivalent over $\mathbb{K}$. By Theorem 8.7, statement (1), $[\mathbb{K}(d_1) : \mathbb{K}] = [\mathbb{K}(d_2) : \mathbb{K}] = r$ and the curves $\mathcal{U}_1^\star := \chi(\mathcal{U}_1)$ and $\mathcal{U}_2^\star := \chi(\mathcal{U}_2)$ parametrized by $\tilde{\chi}_1(t) = (\frac{1}{M_1(t)}, \ldots, \frac{t^{r-1}}{M_1(t)})$ and $\tilde{\chi}_2(t) = (\frac{1}{M_2(t)}, \ldots, \frac{t^{r-1}}{M_2(t)})$, respectively, are affinely equivalent over $\mathbb{K}$; note that, for simplicity we have omitted the last zero components in these parametrizations. Therefore, there exists $\mathcal{A} = (a_{i,j}) \in GL(r, \mathbb{K})$ and $\vec{v} \in M_{r\times 1}(\mathbb{K})$, such that $\varphi(t) := \mathcal{A}\,\tilde{\chi}_1(t)^t + \vec{v}$ parametrizes $\mathcal{U}_2^\star$. In consequence, since $\varphi(t)$ and $\tilde{\chi}_2(t)$ are proper parametrizations of the same curve, there exists a unit $\tau(t) \in \mathbb{K}(t)$ such that $\varphi(t) = \tilde{\chi}_2(\tau(t))$. Then, considering the first component in the above equality, one gets that

$$(a_{1,1} + \cdots + a_{1,r}t^{r-1} + v_1 M_1(t))M_2(\tau(t)) = M_1(t).$$

Now, substituting t by $-d_1$, we obtain

$$(a_{1,1} + \cdots + a_{1,r}(-d_1)^{r-1} + v_1 M_1(-d_1))M_2(\tau(-d_1)) = M_1(-d_1) = 0.$$

Note that $a_{1,1}+\cdots+a_{1,r}(-d_1)^{r-1} \neq 0$, because $[\mathbb{K}(d_1) : \mathbb{K}] = r$. Also, note that $\tau(-d_1)$ is well defined, because $-d_1$ does not belong to $\mathbb{K}$. This implies that $M_2(\tau(-d_1)) = 0$. So, $\tau(-d_1)$ is a root of $M_2(t)$.

Conversely, let $\tau(t) = \frac{k_1 t+k_2}{k_3 t+k_4} \in \mathbb{K}(t)$ be a unit that maps the root γ of $M_1(t)$ onto the root β of $M_2(t)$, i.e. $\tau(\gamma) = \beta$. This relation implies that $\mathbb{K}(\gamma) = \mathbb{K}(\beta)$ and that $\deg(M_1(t)) = \deg(M_2(t)) = r$. Therefore, because of Theorem 8.7, it is enough to prove that the curves $\mathcal{U}_1^\star := \chi(\mathcal{U}_1)$ and $\mathcal{U}_2^\star := \chi(\mathcal{U}_2)$ are affinely equivalent over $\mathbb{K}$. Recall that $\mathcal{U}_i^\star$ is parametrized by $\varphi_i(t) := \tilde{\chi}(t) = \left(\frac{1}{M_i(t)}, \ldots, \frac{t^{r-1}}{M_i(t)}\right)$; here again, we omit the last zero components of the parametrization. In order to prove the result, we find an invertible matrix $\mathcal{A} \in GL(r, \mathbb{K})$ and a vector $\vec{v} \in M_{r\times 1}(\mathbb{K})$, such that $\mathcal{A}\,\varphi_1^t(t) + \vec{v} = \varphi_2^t(\tau(t))$. For this purpose, we consider the polynomial $M(t) = M_2(\tau(t))(k_3 t + k_4)^r \in \mathbb{K}[t]$. Now, since $\tau(t)$ is a unit of $\mathbb{K}(t)$, and the roots of $M_2(t)$ are not in $\mathbb{K}$, one gets that $\deg(M) = \deg(M_2) = r$. Moreover, since γ is a root of $M(t)$, and taking into account that $M_1(t)$ is the minimal polynomial of γ over $\mathbb{K}$ and that $\deg(M) = r = \deg(M_1)$, one has that there exists $c \in \mathbb{K}^*$ such that $M(t) = cM_1(t)$. Now, in order to determine $\mathcal{A}$ and $\vec{v}$, let us substitute $\tau(t)$ in the i-th component of $\varphi_2(t)$:

$$\frac{\tau(t)^i}{M_2(\tau(t))} = \frac{\tau(t)^i(k_3 t + k_4)^r}{M_2(\tau(t))(k_3 t + k_4)^r} = \frac{(k_1 t + k_2)^i(k_3 t + k_4)^{r-i}}{cM_1(t)}.$$

Since numerator and denominator in the above rational function have the same degree, taking quotients and remainders, $\varphi_2(t)$ can be expressed as

$$(\varphi_2(\tau(t)))_{i=1,\ldots,r} = (v_i + \frac{a_{i,1} + \cdots + a_{i,r}t^{r-1}}{M_1(t)})_{i=1,\ldots,r},$$

for some $v_i, a_{i,j} \in \mathbb{K}$. Take $\mathcal{A} = (a_{i,j})$ and $\vec{v} = (v_i)$. Then, $\mathcal{A}(\varphi_1(t))^t + \vec{v} = (\varphi_2(\tau(t))^t$. Finally, let us see that $\mathcal{A}$ is regular. Indeed, suppose that $\mathcal{A}$ is singular and that there exists a non trivial linear relation $\lambda_1 F_1 + \cdots + \lambda_r F_r = \vec{0}$, where F_i denotes the i-th row of $\mathcal{A}$. This implies that $\left(\lambda_1 \frac{1}{M_2(t)} + \cdots + \lambda_r \frac{t^{r-1}}{M_2(t)}\right) \circ \tau(t) = \lambda_1 v_1 + \cdots + \lambda_r v_r$ is constant, which is impossible because $\frac{\lambda_1 + \cdots + \lambda_r t^{r-1}}{M_2(t)}$ is not constant and $\tau(t)$ is a unit of $\mathbb{K}(t)$. □

In Corollary 8.8 we have seen that the degree of a hypercircle is given by the degree of the field extension provided by the pole of any non polynomial generating unit. Lines are curves of degree one, a particular case of this phenomenon. Now, we consider other kind of hypercircles of degree smaller than n. This motivates the following concept.

Definition 8.10. Let $\mathcal{U}$ be an α-hypercircle. If the degree of $\mathcal{U}$ is $[\mathbb{K}(\alpha) : \mathbb{K}]$, we say that it is a *primitive hypercircle*. Otherwise, we say that $\mathcal{U}$ is a *non-primitive hypercircle*.

Regarding the complex numbers as an extension of the reals, lines may be considered as circles when we define them through a Moebius transformation. Lines are the only one curves among these such that its degree is not $[\mathbb{C} : \mathbb{R}]$. The situation is more complicated in the general case.

8.3 Non-primitive Hypercircles

Apart from lines, which have been thoroughly studied in Theorem 8.6, there are other non-primitive hypercircles. This is not a big challenge because, as we will see, non-primitive hypercircles are primitive on another extension. Moreover, these cases reflect some algebraic aspects of the extension $\mathbb{K} \subseteq \mathbb{K}(\alpha) = \mathbb{L}$ in the geometry of the hypercircles. Actually, we will see that there is a correspondence between non-primitive hypercircles and the intermediate fields of $\mathbb{K} \subseteq \mathbb{L}$. More precisely, let $\mathcal{U}$ be a non-primitive hypercircle associated to $u(t) = \frac{1}{t+d}$, where $r = [\mathbb{K}(d) : \mathbb{K}] < [\mathbb{L} : \mathbb{K}] = n$. In this case, we have the algebraic extensions $\mathbb{K} \subseteq \mathbb{K}(d) \subsetneq \mathbb{L}$. We may consider $u(t)$ as a unit either in the extension $\mathbb{K} \subseteq \mathbb{K}(d)$ with primitive element d or in $\mathbb{K}(d) \subsetneq \mathbb{L}$ with primitive element α. In the first case, $u(t)$ defines a primitive hypercircle in $\mathbb{F}^r$. In the second case, as $u(t)$ is a $\mathbb{K}(d)$ unit, it defines a line. The analysis of $\mathcal{U}$ can be reduced to the case of the primitive hypercircle associated to $u(t)$ in the extension $\mathbb{K} \subseteq \mathbb{K}(d)$.

Theorem 8.11. *Let $\mathcal{U}$ be the non-primitive hypercircle associated to $u(t) = \frac{at+b}{t+d} \in \mathbb{K}(\alpha)(t)$. Let $\mathcal{V}$ be the hypercircle generated by the unit $\frac{1}{t+d}$ in the extension $\mathbb{K} \subseteq \mathbb{K}(d)$. Then, there is an affine inclusion from $\mathbb{F}^r$ to $\mathbb{F}^n$, defined over $\mathbb{K}$, that maps the hypercircle $\mathcal{V}$ onto $\mathcal{U}$.*

Proof. Taking into account Lemma 8.5, we may assume that $u(t) = \frac{1}{t+d}$. Let $\phi(t) = (\phi_0(t), \ldots, \phi_{n-1}(t)) \in \mathbb{K}(t)^n$ be the parametrization of $\mathcal{U}$, obtained from $u(t)$, with respect to the basis $\mathcal{B} = \{1, \alpha, \ldots, \alpha^{n-1}\}$. Similarly, let $\psi(t) = (\psi_0(t), \ldots, \psi_{r-1}(t)) \in \mathbb{K}^r(t)$ be the parametrization of the hypercircle $\mathcal{V}$, associated to $u(t)$, with respect to the basis $\mathcal{B}^\star = \{1, d, \ldots, d^{r-1}\}$, where $r = [\mathbb{K}(d) : \mathbb{K}]$. The matrix $\mathcal{D} = (d_{ji}) \in$

$\mathcal{M}_{n\times r}(\mathbb{K})$ whose columns are the coordinates of d^i with respect to $\mathcal{B}$ induces a $\mathbb{K}$-linear transformation $\chi : \mathbb{F}^r \mapsto \mathbb{F}^n$ that maps $\mathcal{V}$ onto $\mathcal{U}$. Indeed, as $u(t) = \sum_{i=0}^{r-1} \psi_i(t) d^i = \sum_{j=0}^{n-1} \phi_j(t)\alpha^j$, one has that

$$\sum_{i=0}^{r-1} \psi_i(t) d^i = \sum_{i=0}^{r-1} \psi_i(t) \left(\sum_{j=0}^{n-1} d_{j,i}\alpha^j \right) = \sum_{j=0}^{n-1} \left(\sum_{i=0}^{r-1} d_{j,i}\psi_i(t) \right) \alpha^j = \sum_{j=0}^{n-1} \phi_j(t)\alpha^j.$$

Then $\phi(t)^t = \mathcal{D}\,\psi(t)^t$. Moreover, χ is one to one, because $\operatorname{rank}(D) = r$. □

As a consequence of this theorem, every hypercircle is affinely equivalent, over $\mathbb{K}$, to a primitive hypercircle. Therefore, the study of hypercircles can be reduced to the study of primitives hypercircles. For the rest of the Chapter, we will suppose that all the hypercircles are primitive.

8.4 Properties at Infinity of a Hypercircle

Circles have a very particular structure at infinity, namely, they pass through the cyclic points, i.e. $[\pm i : 1 : 0]$. In this Section, we will see that a similar situation occurs for more general primitive hypercircles. More precisely, let $\mathcal{U}$ be the primitive hypercircle defined by the unit $u(t) = \frac{at+b}{t+d}$. By Corollary 8.8, $\mathcal{U}$ is a parametric affine curve of degree n. So, there are at most n different points in the hyperplane at infinity. Let $\phi(t) = (\phi_0(t), \ldots, \phi_{n-1}(t))$ be the parametrization of $\mathcal{U}$ generated by $u(t)$; recall that $\phi_i(t) = \frac{p_i(t)}{M(t)}$. Thus, projective coordinates of the points attained by $\phi(t)$ are given by $[p_0(t) : \cdots : p_{n-1}(t) : M(t)]$. Now, substituting t by every conjugate $\sigma(-d)$ of $-d$, we obtain

$$[p_0(\sigma(-d)) : \cdots : p_{n-1}(\sigma(-d)) : 0] = [\sigma(p_0(-d)) : \cdots : \sigma(p_{n-1}(-d)) : 0]$$

We prove next that these points are the points of the hypercircle at infinity.

Lemma 8.12. *Let $\mathcal{U}$ be a primitive hypercircle associated to the unit $u(t) = \frac{at+b}{t+d}$. The n points at infinity are*

$$P_j = [\sigma_j(p_0(-d)) : \cdots : \sigma_j(p_{n-1}(-d)) : 0],\ 1 \le j \le n$$

where σ_j are the $\mathbb{K}$-automorphisms of the normal closure of $\mathbb{L} = \mathbb{K}(\alpha)$ over $\mathbb{K}$.

Proof. First of all, observe that $\gcd(p_0, \ldots, p_{n-1}, M) = 1$, and hence P_j are well defined. Moreover, $p_i(-d) \neq 0$, for every $i \in \{0, \ldots, n-1\}$, since $p_i(t) \in \mathbb{K}[t]$ is of degree at most n and, thus, if $p_i(-d) = 0$, then $\frac{p_i(t)}{M(t)} = c \in \mathbb{K}$ and the hypercircle would be contained in a hyperplane. But this is impossible since $\mathcal{U}$ is primitive (see Corollary 8.8). It remains to prove that they are different points. Suppose that two different tuples define the same projective point. We may suppose that $P_1 = P_j$. P_1 verifies that $\sum_{i=0}^{n-1} p_i(-d)\alpha^i = (-ad + b)m(-d) \neq 0$ and P_j verifies that $\sum_{i=0}^{n-1} p_i(\sigma_j(-d))\alpha^i = (a\sigma_j(-d) + b)m(\sigma_j(-d)) = 0$. Thus, P_j is contained in the projective hyperplane $\sum_{i=0}^{n-1} \alpha^i x_i = 0$, but not P_1. Hence, $P_1 \neq P_j$. □

Let us check that, as in the case of circles, the points at infinity of primitive α-hypercircles do not depend on the particular hypercircle.

Theorem 8.13. *For a fixed extension $\mathbb{K} \subseteq \mathbb{K}(\alpha)$ of degree n, the set of points at the infinity $P = \{P_1, \ldots, P_n\}$ of any primitive hypercircle does not depend on the particular α-hypercircle $\mathcal{U}$, but only on the algebraic extension and on the primitive element α. Moreover, the set P is characterized by the following property:*

$$\{x_0 + \alpha_j x_1 + \cdots + \alpha_j^{n-1} x_{n-1} = 0\} \cap \overline{\mathcal{U}} = P \setminus \{P_j\},$$

where $\alpha_j = \sigma_j(\alpha)$ are the conjugates of α in $\mathbb{F}$, $1 \leq j \leq n$, and $\overline{\mathcal{U}}$ is the projective closure of $\mathcal{U}$.

Proof. Let $\mathcal{U}$ be the primitive α-hypercircle generated be a unit $u(t) = \frac{at+b}{t+d}$. $\overline{\mathcal{U}}$ has the projective parametrization $[p_0(t) : \cdots : p_{n-1}(t) : M(t)]$. Let $P_j = [\sigma_j(p_0(-d)) : \cdots : \sigma_j(p_{n-1}(-d)) : 0]$. Its evaluation in the equation of hyperplane $x_0 + \alpha_k x_1 + \ldots + \alpha_k^{n-1} x_{n-1}$, yields:

$$\sum_{i=0}^{n-1} \sigma_j(p_i(-d))\alpha_k^i = \sigma_k \left(\sum_{i=0}^{n-1} \sigma_k^{-1} \circ \sigma_j(p_i(-d))\alpha^i \right) =$$

$$\sigma_k \left((a(\sigma_k^{-1} \circ \sigma_j(-d)) + b) m(\sigma_k^{-1} \circ \sigma_j(-d)) \right).$$

If $j = k$, the previous expression equals $\sigma_k\left((-ad + b)m(-d)\right) \neq 0$. If $j \neq k$, then $\sigma_k^{-1} \circ \sigma_j(-d)$ is a conjugate of $-d$, different from $-d$, because $-d$ is a primitive element. So $m(\sigma_k^{-1} \circ \sigma_j(-d)) = 0$.

In order to show that this point does not depend on a particular hypercircle, take the n hyperplanes $x_0 + \alpha_k x_1 + \cdots + \alpha_k^{n-1} x_{n-1} = 0$, $k = 1 \ldots n$. Every point at infinity of a hypercircle is contained in exactly $n - 1$ of those hyperplanes. Also, any of these hyperplanes contains exactly $n - 1$ points at infinity of the hypercircle. One point at infinity may be computed by solving the linear system given by any combination of $n-1$ hyperplanes. The matrix of the linear system is a Vandermonde matrix, each row depending on the corresponding α_k, so there is only one solution. □

The following result shows that the points at infinity can be read directly from the minimal polynomial of α.

Proposition 8.14. *Let $M_\alpha(t)$ be the minimal polynomial of α over $\mathbb{K}$. Let $m_\alpha(t) = \frac{M_\alpha(t)}{t-\alpha} = \sum_{i=0}^{n-1} l_i t^i \in \mathbb{K}(\alpha)[t]$, where $l_{n-1} = 1$. Then, the points at infinity of every primitive α-hypercircle are $[l_0 : l_1 : \cdots : l_{n-2} : l_{n-1} : 0]$ and its conjugates.*

Proof. We consider the symmetric polynomial $r(x, y) = \frac{M_\alpha(x) - M_\alpha(y)}{x-y}$. Substituting (x, y) by (t, α) we obtain that

$$r(t, \alpha) = \frac{M_\alpha(t) - M_\alpha(\alpha)}{t - \alpha} = \frac{M_\alpha(t)}{t - \alpha} = m_\alpha(t).$$

That is, $m_\alpha(t)$ is symmetric in t and α. Take now the hypercircle induced by the unit $\frac{1}{t-\alpha} = \frac{m_\alpha(t)}{M_\alpha(t)}$. By Lemma 8.12, we already know that one point at infinity is $[p_0(\alpha) : \cdots : p_{n-1}(\alpha) : 0]$, where $m_\alpha(t) = \sum_{i=0}^{n-1} p_i(t)\alpha^i$. By symmetry, $\sum_{i=0}^{n-1} p_i(t)\alpha^i = \sum_{i=0}^{n-1} p_i(\alpha)t^i$. That is, $p_i(\alpha) = l_i$. Thus, the points at infinity are $[l_0 : l_1 : \cdots : l_{n-2} : 1 : 0]$ and its conjugates. □

Next result deals with the tangents of a hypercircle at infinity, and it explains again why parabolas can not be hypercircles.

Proposition 8.15. *The tangents to a primitive hypercircle at the points at infinity are not contained in the hyperplane at infinity.*

Proof. Let $\mathcal{U}$ be the primitive α-hypercircle generated by $\frac{at+b}{t+d}$, and $[p_0(t) : \cdots : p_{n-1}(t) : M(t)]$ the projective parametrization generated by the unit. In the proof of Lemma 8.12, we have seen that $p_{n-1}(t)$ is not identically 0, because $p_{n-1}(-d) \neq 0$. So, we can dehomogenize w.r.t. the variable x_{n-1}, obtaining the affine parametrization $(\frac{p_0(t)}{p_{n-1}(t)}, \ldots, \frac{p_{n-2}(t)}{p_{n-1}(t)}, \frac{M(t)}{p_{n-1}(t)})$ of $\mathcal{U}$ on another affine chart. We have to check that the tangents to the curve at the intersection points with the hyperplane $x_{n-1} = 0$ are not contained in this hyperplane. The points of $\mathcal{C}$ in the hyperplane $x_{n-1} = 0$ are obtained by substituting t by $\sigma(-d)$. The last coordinate of the tangent vector is

$$\frac{M'(t)p_{n-1}(t) - M(t)p'_{n-1}(t)}{p_{n-1}(t)^2}.$$

We evaluate this expression at $\sigma(-d)$. $M(\sigma(-d)) = 0$ and, as all its roots are different in $\mathbb{F}$, $M'(\sigma(-d)) \neq 0$. We also know that $\sigma(p_{n-1}(-d)) \neq 0$. Hence, the last coordinate of the tangent vector is non-zero. Thus, the tangent line is not contained in the hyperplane at infinity. □

Finally, we present a property of hypercircles that can be derived from the knowledge of its behavior at infinity. We remark a property of circles stating that given three different points in the plane, there is exactly one circle passing through them (which is a line if they are collinear). The result is straightforward if we recall that there is only one conic passing through five points. In the case of circles, we have the two points at infinity already fixed, so, given three points in the affine plane there will only be a conic (indeed a circle if it passes through the cyclic points at infinity) through them. Even if hypercircles are curves in n-space, surprisingly, the same occurs for hypercircles.

We are going to prove that, given 3 different points in $\mathbb{K}^n$, there is exactly one hypercircle passing through them. If the points are not in general position, the resulting hypercircle needs not to be a primitive one. First, we need a lemma that states what are the points over $\mathbb{K}$ of the hypercircle that are reachable by the parametrization.

Lemma 8.16. *Let $\mathcal{U}$ be the α–hypercircle, non necessarily primitive, associated to $u(t) = \frac{at+b}{t+d}$ with induced parametrization $\Phi(t)$. $\Phi(\mathbb{K}) = \mathcal{U} \cap \mathbb{K}^n \setminus \{\bar{a}\}$ with $a = \sum_{i=0}^{n-1} a_i\alpha^i$, $\bar{a} = (a_0, \ldots, a_{n-1})$.*

Proof. We already know that $\Phi(t)$ is proper and, obviously, $\Phi(\mathbb{K}) \subseteq \mathcal{U} \cap \mathbb{K}^n$, also, $\bar{a}$ is not reachable by $\Phi(t)$, since otherwise one would have that $a = u(\lambda)$ for some λ, and this implies that $ad - b = 0$, which is impossible since $u(t)$ is a unit. In order to prove the other inclusion, write as before $\phi_i(t) = \frac{p_i(t)}{M(t)}$, where $M(t)$ is the minimal polynomial of $-d$ over $\mathbb{K}$. Then, we consider the ideal I over $\mathbb{F}[t, \bar{x}]$ generated by $(p_0(t) - x_0 M(t), \ldots, p_{n-1}(t) - x_{n-1}M(t))$, where $\bar{x} = (x_0, \ldots, x_{n-1})$, and the ideal $J = I + (ZM(t) - 1) \subseteq \mathbb{F}[Z, t, \bar{x}]$. Let I_1 be the first elimination ideal of I; i.e. $I_1 = I \cap \mathbb{F}[\bar{x}]$ and let J_2 be the second elimination ideal of J; i.e. $J_2 = J \cap \mathbb{F}[\bar{x}]$. Observe that $I \subseteq J$ and therefore $I_1 \subseteq J_2$. Note that $\mathcal{U} = V(J_2)$; i.e. $\mathcal{U}$ is the variety defined by J_2 over $\mathbb{F}$. Thus $\mathcal{U} \subseteq V(I_1)$. Now, let us take $\bar{x} \in (\mathcal{U} \cap \mathbb{K}^n) \setminus \{\bar{a}\}$. Then $\bar{x} \in V(I_1)$. Observe that, by construction, the leading coefficient of $p_i(t) - x_i M(t)$ w.r.t. t is $a_i - x_i$. Therefore, since $\bar{x} \neq \bar{a}$ one has that at least one of the leading coefficients of the polynomials in I w.r.t. t does not vanish at $\bar{x}$. Thus, applying the Extension Theorem (see Theorem 3, pp. 117 in [CLO97]), there exists $t_0 \in \mathbb{F}$ such that $(t_0, \bar{x}) \in V(I)$. This implies that $p_i(t_0) - x_i M(t_0) = 0$ for $i = 1 \ldots n-1$. Let us see that $M(t_0) \neq 0$. Indeed, if $M(t_0) = 0$ then $p_i(t_0)$ is also zero for every index and therefore $\gcd(p_0(t), \ldots, p_{n-1}(t), M(t)) \neq 1$, which is impossible. Hence Φ is defined at t_0 and $\Phi(t_0) = \bar{x}$. To end up, we only need to show that $t_0 \in \mathbb{K}$. For this purpose, we note that the inverse of $\Phi(t)$ is given by

$$P(\bar{x}) = \frac{-d \sum x_i \alpha^i + b}{\sum x_i \alpha^i - a}$$

Now, since $\bar{x} \neq \bar{a}$ one deduces that $P(\bar{x})$ is well defined, and the only parameter value generating $\bar{x}$ is $t_0 = P(\bar{x})$. Hence, the gcd of the polynomials $p_i(t) - x_i M(t)$ is a power of $(t - t_0)$. Thus, taking into account that $p_i, M \in \mathbb{K}[t]$, one deduces that $t_0 \in \mathbb{K}$. Finally, it only remains to state that $\bar{a}$ is generated when t takes the value of the infinity of $\mathbb{K}$. But this follows taking $\Phi(1/t)$ and substituting by $t = 0$. □

Proposition 8.17. *Let $x_i = (x_{i0}, \ldots, x_{i,n-1}) \in \mathbb{K}^n \subseteq \mathbb{F}^n$, $1 \leq i \leq 3$ be three different points. Then, there exists only one α–hypercircle passing through them.*

Proof. Let $y_i = \sum_{j=0}^{n-1} x_{ij} \alpha^j \in \mathbb{K}(\alpha)$, $1 \leq i \leq 3$. Consider the following linear homogeneous system in a, b, c, d:

$$b = y_1 d,\ a + b = y_2(c + d),\ a = y_3 c$$

Observe that, if the three points are different, there is only one projective solution, namely $[a : b : c : d]$ where $a = y_1 y_3 - y_3 y_2$, $b = y_1 y_2 - y_1 y_3$, $c = y_1 - y_2$, $d = y_2 - y_3$.

Take the unit $u(t) = \frac{at+b}{ct+d}$. It verifies that $u(0) = y_1$, $u(1) = y_2$, $u(\infty) = y_3$. Then, the hypercircle associated to u passes through x_1, x_2, x_3. In order to prove that this hypercircle is unique, let v be the unit associated to a hypercircle passing through the three points and $\psi(t)$ the parametrization induced by $v(t)$. By Lemma 8.16, as $x_i \in \mathbb{K}^n$, the point x_i is reached for a parameter value t_i in $\mathbb{K} \cup \{\infty\}$. So, there are three values $t_1, t_2, t_3 \in \mathbb{K} \cup \{\infty\}$ such that $v(t_i) = y_i$. Let $\tau(t) \in \mathbb{K}(t)$ be the unique unit associated to the transformation of the projective line $\mathbb{P}(\mathbb{F})$ into itself given by

$\tau(0) = t_1$, $\tau(1) = t_2$, $\tau(\infty) = t_3$. Then $v(\tau(t)) = u(t)$ and both units represents the same hypercircle. □

8.5 Parametrization and Implicitation of a Hypercircle

In this Section, we will provide specific methods to parametrize and implicitate hypercircles. These methods show the power of the rich structure of hypercircles, simplifying problems that are usually much harder in general.

Given a unit $u(t)$ defining $\mathcal{U}$, it is immediate to obtain a parametrization of $\mathcal{U}$. Let $\mathcal{C}$ be any curve given by a proper parametrization over $\mathbb{K}(\alpha)$, let $\mathcal{Z}$ be the witness variety associated to $\mathcal{C}$, see Definition 7.12. Then, by Theorem 7.16, $\mathcal{C}$ is parametrizable over $\mathbb{K}$ is and only if $\mathcal{Z}$ is a α-hypercircle. Usually, the components of $\mathcal{Z}$ are obtained by implicit equations. The next proposition shows how to parametrize an α-hypercircle.

Proposition 8.18. *The pencil of hyperplanes $x_0 + x_1\alpha + \cdots + x_{n-1}\alpha^{n-1} = t$ parametrizes the primitive α–hypercircle $\mathcal{U}$.*

Proof. Let I be the implicit ideal of $\mathcal{U}$. Note that, since $\mathcal{U}$ is $\mathbb{K}-$rational it is $\mathbb{K}$-definable, and hence a set of generators of I can be taken in $\mathbb{K}[x_0, \ldots, x_{n-1}]$. Let $u(t)$ be any unit associated with $\mathcal{U}$ and $(\phi_0(t), \ldots, \phi_{n-1}(t))$ the induced parametrization. Let $v(t)$ be the inverse unit of $u(t)$, $u(v(t)) = v(u(t)) = t$. Then $(\phi_0(v(t)), \ldots, \phi_{n-1}(v(t))) = (\psi_0(t), \ldots, \psi_{n-1}(t)) = \Psi(t)$ is another parametrization of $\mathcal{U}$ which is no more defined over $\mathbb{K}$ but over $\mathbb{K}(\alpha)$. The later parametrization is in standard form [RSV04], that is

$$\sum_{i=0}^{n-1} \psi_i(t)\alpha^i = \left(\sum_{i=0}^{n-1} \phi_i(t)\alpha^i\right) \circ v(t) = u \circ v(t) = t.$$

This implies that the pencil of hyperplanes $H_t \equiv x_0 + x_1\alpha + \cdots + x_{n-1}\alpha^{n-1} - t$ parametrizes $\mathcal{U}$. Indeed, if $\Psi(t)$ is defined, $H_t \cap \mathcal{U}$ consists in $n-1$ points at infinity of $\mathcal{U}$ (Theorem 8.13) and $\Psi(t)$ itself. We deduce that $\psi_i(t) - x_i$ belongs to the ideal $I + H_t$, which has a set of generators in $\mathbb{K}(\alpha)(t)[x_0, \ldots, x_{n-1}]$. So, the parametrization $\Psi(t)$ can be computed from I. □

Notice that the obtained parametrization $\Psi(t)$ has coefficients over $\mathbb{K}(\alpha)$. Thus, it is not the parametrization induced by any associated unit $u(t)$. The interest of obtaining a unit associated to a hypercircle is that it helps us to solve the problem of reparametrizing a curve over an optimal field extension of $\mathbb{K}$, see [ARS99]. There, it is shown that given a parametrization $\Psi(t) \in \mathbb{K}(\alpha)^r$ of a curve there is a hypercircle associated to it. Any unit associated to the hypercircle reparametrizes the original curve over $\mathbb{K}$. To get a parametrization $\phi(t)$ over $\mathbb{K}$ or, equivalently, a unit $u(t)$ associated to $\mathcal{U}$, we refer to [RSV04]. In addition, note that the proof of Proposition 8.17 shows how to construct a unit associated to a hypercircle, when points over $\mathbb{K}$ are known, and therefore a parametrization of it.

The inverse problem, computing implicit equations of a hypercircle from the parametrization induced by an associated unit, can be performed using classic implicitation

methods. However, the special structure of hypercircles provides specific methods that might be more convenient.

Proposition 8.19. *Let $\mathcal{U}$ be a hypercircle associated to the unit $u(t)$, and let $v(t)$ be the inverse of $u(t)$. Let*

$$v\left(\sum_{i=0}^{n-1}\alpha^i x_i\right)=\sum_{i=0}^{n-1}\frac{r_i(x_0,\ldots,x_{n-1})}{s(x_0,\ldots,x_{n-1})}\alpha^i,$$

where $r_i, s\in\mathbb{K}[x_0,\ldots,x_{n-1}]$. Then, the ideal of $\mathcal{U}$ is the elimination ideal with respect to Z:

$$\mathcal{I}(\mathcal{U})=(r_1(\bar{x}),\ldots,r_n(\bar{x}),s(\bar{x})Z-1)\cap\mathbb{F}[x_0,\ldots,x_{n-1}].$$

Proof. Let $u(t)=\frac{at+b}{t+d}$, then $v(t)=\frac{-dt+b}{t-a}$. Now, consider

$$u\left(\sum_{i=0}^{n-1}\alpha^i x_i\right)=\sum_{i=0}^{n-1}\xi_i(x_0,\ldots,x_{n-1})\alpha^i$$

$$v\left(\sum_{i=0}^{n-1}\alpha^i x_i\right)=\sum_{i=0}^{n-1}\eta_i(x_0,\ldots,x_{n-1})\alpha^i$$

where $\xi_i,\ \eta_j\in\mathbb{K}(x_0,\ldots,x_{n-1})$ and $\eta_i=\frac{r_i(x_0,\ldots,x_{n-1})}{s(x_0,\ldots,x_{n-1})}$. The map $\xi:\mathbb{F}^n\longrightarrow\mathbb{F}^n$, $\xi=(\xi_0,\ldots,\xi_{n-1})$ is birational and its inverse is $\eta=(\eta_0,\ldots,\eta_{n-1})$. Indeed:

$$\sum_{i=0}^{n-1}\eta_i(\xi_0(\bar{x}),\ldots,\xi_{n-1}(\bar{x}))\alpha^i=v\left(\sum_{j=0}^{n-1}\alpha^j\xi_j(\bar{x})\right)=$$

$$=v\left(u\left(\sum_{i=0}^{n-1}\alpha^i x_i\right)\right)=\sum_{i=0}^{n-1}\alpha^i x_i$$

is an equality in $\mathbb{K}(\alpha)(x_0,\ldots,x_{n-1})$. We deduce that

$$\eta_i\big(\xi_0(x_0,\ldots,x_{n-1}),\ldots,\xi_{n-1}(x_0,\ldots,x_{n-1})\big)=x_i$$

It is clear that $\mathcal{U}$ is the image of the line $L\equiv\{x_1=0,\ldots,x_{n-1}=0\}$ under the map ξ, $\mathcal{U}=\xi(L)$. The set of points where ξ is not defined is the union of the hyperplanes $\sum_{i=0}^{n-1}\sigma_j(\alpha)^i x_i+\sigma_j(d)=0$, $1\le j\le n$. The intersection of these hyperplanes with L is the set of points $(-\sigma(d)_j,0,\ldots,0)$, $1\le j\le n$. Thus, for a generic $p\in L$, $\xi(p)$ is defined and belongs to $\mathcal{U}$. The result is similar for the inverse map η. The set of points where η is not defined is the union of the hyperplanes $\sum_{i=0}^{n-1}\sigma_j(\alpha)^i x_i-\sigma_j(a)=0$, $1\le j\le n$. These n hyperplanes intersect $\mathcal{U}$ in at most one affine point, see Proposition 8.18. So, for a generic $p\in\mathcal{U}$, $\eta(p)$ is again defined and belongs to L. Let us compute now the points $\bar{x}$ such that $\eta(\bar{x})$ is defined, but it does not belong to the domain of ξ. If $\bar{x}$ is such a point, then

$$\sum_{i=0}^{n-1}\sigma_j(\alpha)^i\eta_i(\bar{x})+\sigma_j(d)=0.$$

As η_i is defined over $\mathbb{K}$, applying σ_j to the definition of η, we obtain that

$$\sigma_j(v)\left(\sum_{i=0}^{n-1}\sigma_j(\alpha)^i x_i\right) = -\sigma_j(d)$$

But $\sigma_j(v) = \frac{-\sigma_j(d)t+\sigma_j(b)}{t-\sigma_j(a)}$. It follows from Lemma 8.16 that the value $-\sigma_j(d)$ cannot be reached, even in $\mathbb{F}$. Thus, the image of η is contained in the domain of ξ.

We are ready to prove the theorem, by verifying that the set $\mathcal{U} \setminus \{s = 0\}$, which is just eliminating a finite number of points in $\mathcal{U}$, is the set of points $\bar{x}$ such that $r_i(\bar{x}) = 0$, $i \geq 1$ and $s(\bar{x}) \neq 0$. If $\bar{x} \in \mathcal{U} \setminus \{s = 0\}$, then η is defined and $\eta(\bar{x}) = (\eta_0(\bar{x}), 0, \ldots, 0)$. Hence $\eta_i(\bar{x}) = r_i(\bar{x}) = 0$. Conversely, if $\bar{x}$ is a point such that $r_i(\bar{x}) = 0$ and $s(\bar{x}) \neq 0$, then $\eta(\bar{x})$ is defined and belongs to L. It is proved that ξ is defined in $\eta(\bar{x})$, so $\bar{x} = \xi(\eta(\bar{x})) \in \xi(L) = \mathcal{U}$. The thesis of the theorem follows taking the Zariski closure of $\mathcal{U} \setminus \{s = 0\}$. □

This method to compute the implicit equations of $\mathcal{U}$ is not free from elimination techniques, as it has to eliminate the variable Z. However, it has the advantage that it yields already an ideal in $\mathbb{F}[x_0, \ldots, x_{n-1}]$ defined over $\mathbb{K}$ and such that it describes a non trivial variety containing the hypercircle. Namely, $(r_1(\bar{x}), \ldots, r_{n-1}(\bar{x}))$ are polynomials over $\mathbb{K}$ whose zero set contains the hypercircle. The following example shows that the elimination step is necessary in some cases.

Example 8.20. Let $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$ be the algebraic extension defined by $\alpha^3 + \alpha^2 - 3 = 0$. Let us consider the unit $u(t) = \frac{(2+\alpha)t+\alpha}{t+1-\alpha}$. Its inverse is $v(t) = \frac{(\alpha-1)t+\alpha}{t-2-\alpha}$. A parametrization of $\mathcal{U}$ is

$$\phi(t) = \left(\frac{2t^3+6t^2+7t+3}{t^3+4t^2+5t-1}, \frac{t^3+6t^2+9t+2}{t^3+4t^2+5t-1}, \frac{t^2+4t+1}{t^3+4t^2+5t-1}\right)$$

A Gröbner basis of the ideal of the curve is
$I := \{x_1^2 - x_2x_0 - x_2x_1 - x_1 + x_2, x_0x_1 - x_2x_0 - 3x_2^2 - 2x_1 + 4x_2,$
$x_0^2 - 3x_2x_1 - 2x_0 + 2x_1 + 3x_2 - 2\}$.
Then, Proposition 8.19 states that this ideal is

$$I = (r_1(x_0, x_1, x_2), r_2(x_0, x_1, x_2), s(x_0, x_1, x_2)Z - 1) \cap \mathbb{F}[x_0, x_1, x_2]$$

where
$r_1 = 2 - 8x_2 + 4x_2x_0 + 6x_2^2x_0 + 17x_2x_1 + x_2x_0^2 + 3x_1 - 3x_1^2x_2 + x_0^3 - x_0^2x_1 + 4x_0x_1 - 12x_2^2 - 8x_1^2 + 9x_2^3 + 3x_1^3 - 3x_0^2 - 9x_0x_1x_2,$
$r_2 = -2 - 7x_2 + 4x_2x_0 - x_2x_1 + 8x_1 - 2x_0 - 2x_0x_1 + 6x_2^2 - 2x_1^2 + x_0^2,$
$s = 9x_2^3 + 6x_2^2x_0 - 12x_2^2 + 5x_2x_0 - 17x_2 - 3x_1^2x_2 - 9x_0x_1x_2 + x_2x_0^2 + 24x_2x_1 + 3x_1^3 + 8x_0 + 4x_0x_1 - 5x_0^2 - x_0^2x_1 + 5x_1 - 9x_1^2 - 7 + x_0^3.$
But, if we take $J = (r_1, r_2)$, then $J \subsetneq I$. The saturation of J with respect to I is
$J : I^\infty = (x_1^2 - x_0x_2 - x_1x_2 - 2x_1 + 3x_2 + 1, x_0x_1 - x_0x_2 - 3x_2^2 - x_0 - 2x_1 + 2x_2 + 2, x_0^2 -$

$3x_1x_2 - 4x_0 + 3x_2 + 4)$
This ideal corresponds to the union of the line

$$\begin{cases} -\alpha x_0 & & +3x_2 & = & -2\alpha \\ (\alpha+\alpha^2)x_0 & -3x_1 & & = & -3+2\alpha+2\alpha^2 \end{cases}$$

and its conjugates.

Next theorem shows an alternative method to implicitate a hypercircle without using any elimination techniques. It is based on properties of the normal rational curve of degree n.

Theorem 8.21. *Let $\varphi(t) = (\frac{q_0(t)}{N(t)}, \ldots, \frac{q_{n-1}(t)}{N(t)})$ be a proper parametrization of a primitive hypercircle $\mathcal{U}$ with coefficients in $\mathbb{F}$. Let I be the homogeneous ideal of the rational normal curve of degree n in $\mathbb{P}(\mathbb{F})^n$ given by a set of homogeneous generators $h_1(\bar{y}), \ldots, h_r(\bar{y})$, $\bar{y} = (y_0, \ldots, y_n)$. Let $\mathcal{Q} \in \mathcal{M}_{n+1\times n+1}(\mathbb{F})$ be the matrix of change of basis from $\{q_0(t), \ldots, q_{n-1}(t), N(t)\}$ to $\{1, t, \ldots, t^n\}$. Let*

$$f_i(\bar{x}) = h_i\left(\sum_{j=0}^{n} \mathcal{Q}_{0j}x_j, \ldots, \sum_{j=0}^{n} \mathcal{Q}_{nj}x_j\right),\ 1 \le i \le r.$$

Then $\{f_1, \ldots, f_r\}$ is a set of generators of the homogeneous ideal of $\mathcal{U}$.

Proof. If the parametrization is proper, $\{q_0(t), \ldots, q_{n-1}(t), N(t)\}$ is a basis of the polynomials of degree at most n. This follows from the fact shown in Corollary 8.8 that a primitive hypercircle is not contained in any hyperplane. Note that a projective point $\bar{x}$ belongs to $\mathcal{U}$ if and only if $\mathcal{Q}(\bar{x})$ belongs to the rational normal curve, if and only if $h_i(\mathcal{Q}(\bar{x})) = 0$, $1 \le i \le r$. □

Remark 8.22.

- It is well known that the set of polynomials $\{y_iy_{j-1} - y_{i-1}y_j \mid 1 \le i, j \le n\}$ is a generator set of I (see [Har92]).
- Notice that it is straightforward to compute Q from the parametrization. Therefore, we have an effective method to compute the implicit ideal of the projective closure of $\mathcal{U}$. The affine ideal of $\mathcal{U}$ can be obtained by dehomogenization $x_n = 1$.
- If the parametrization is given by polynomials over an algebraic extension $\mathbb{K}(\beta)$ of $\mathbb{K}$, then the coefficients of f_i belongs to $\mathbb{K}(\beta)$. Moreover, if we write $f_i(\bar{x}) = \sum_{j=0}^{m} f_{ij}(\bar{x})\beta^j$, with $f_{ij} \in \mathbb{K}[\bar{x}]$, then, $\{f_{ij}\}$ is a set of generators over $\mathbb{K}$ of the hypercircle $\mathcal{U}$.
- In practice, this method is much more suited to compute an implicitation of a hypercircle than the method presented in Proposition 8.19.

- Thus, this method provides a fast implicitation method for hypercircles. Note that the computation of $\mathcal{Q}$ can be performed, using linear algebra, in $O(n^3)$ field computations. Then, we have to compute up to $O(n^2)$ products of linear polynomials in n variables. Hence, the total amount of field operations is dominated by $O(n^4)$.

Example 8.23. The implicit equations of a hypercircle can be computed by classical implicitation methods, for example Gröbner basis or with the two methods presented in Proposition 8.19 and Theorem 8.21. Here, we present two cases that show the practical behavior of these methods. The first example considers the algebraic extension $\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$, where $\alpha^4 + \alpha^2 - 3$ and the unit $u = \frac{(1-\alpha^3)t+\alpha^2}{t+1+2\alpha-3\alpha^2}$. The parametrization of the hypercircle is given by

$$\phi_0 = \frac{t^4 + 15t^3 + 22t^2 + 101t - 195}{t^4 + 10t^3 - 17t^2 - 366t + 233}, \phi_1 = \frac{-11t^3 - 73t^2 + 65t - 114}{t^4 + 10t^3 - 17t^2 - 366t + 233},$$

$$\phi_2 = \frac{2t^3 + 57t^2 - 25t - 59}{t^4 + 10t^3 - 17t^2 - 366t + 233}, \phi_3 = \frac{-t^4 - 6t^3 + 4t^2 + 17t - 56}{t^4 + 10t^3 - 17t^2 - 366t + 233}.$$

The second example starts from the extension $\mathbb{Q} \subseteq \mathbb{Q}(\beta)$, where β is such that $\beta^4 + 3\beta + 1 = 0$. Here, the unit defining $\mathcal{U}$ is $u = \frac{(1+\beta-\beta^2)t+1+\beta^3}{t+1+\beta^2-\beta^3}$ and the parametrization induced by $u(t)$ is

$$\psi_0 = \frac{t^4 + 11t^3 + 47t^2 + 95t + 72}{t^4 + 13t^3 + 62t^2 + 126t + 81}, \psi_1 = \frac{t^4 + 7t^3 + 15t^2 + 17t + 9}{t^4 + 13t^3 + 62t^2 + 126t + 81},$$

$$\psi_2 = \frac{-t^4 - 10t^3 - 31t^2 - 23t}{t^4 + 13t^3 + 62t^2 + 126t + 81}, \psi_3 = \frac{t^3 + 13t^2 + 42t + 36}{t^4 + 13t^3 + 62t^2 + 126t + 81}.$$

The running times for computing the implicit ideal (using a Mac xserver with 2 processors G5 2.3 GHz, 2 Gb RAM Maple 10) are

	Example 1	Example 2
Gröbner basis method	0.411	0.332
Proposition 8.19	2.094	2.142
Theorem 8.21	0.059	0.021

8.6 Characterization of Hypercircles

At the beginning of the Chapter we Saw that real circles are hypercircles. A real circle can also be defined as a conic such that its homogeneous part is $x^2 + y^2$ and contains an infinite number of real points. The condition on the homogeneous part is equivalent to impose that the curve passes through the points at infinity $[\pm i : 1 : 0]$. Analogously, hypercircles are regular curves of degree n with infinite points over the base field passing through the points at infinity described in Theorem 8.13. The following result shows that this is a characterization of these curves.

Theorem 8.24. *Let $\mathcal{U} \subseteq \mathbb{F}^n$ be an algebraic set of degree n such that all whose components are of dimension 1. Then, it is a primitive α-hypercircle if and only if it has an infinite number of points with coordinates in $\mathbb{K}$ and passes through the set of points at infinity characterized in Theorem 8.13.*

Proof. The only if implication is trivial. For the other one, let $\mathcal{U} \subseteq \mathbb{F}^n$ be an algebraic set of pure dimension 1 and degree n passing through $P = \{P_1, \ldots, P_n\}$, the n points at infinity of a primitive α-hypercircle. Suppose that $\mathcal{U}$ has infinite points with coordinates in $\mathbb{K}$. Then, we are going to prove that $\mathcal{U}$ is irreducible. Let $\mathcal{W}$ be an irreducible component of $\mathcal{U}$ with infinite points in $\mathbb{K}$. Note that, since $\mathcal{W}$ is irreducible and contains infinitely many points over $\mathbb{K}$, the ideal $\mathcal{I}(\mathcal{W})$ over $\mathbb{F}$ is generated by polynomials over $\mathbb{K}$ (see Lemma 2 in [ARS97]). Let q be any point at infinity of $\mathcal{W}$; then $q \in P$. As $\mathcal{W}$ is $\mathbb{K}$-definable it follows that $\mathcal{W}$ also contains all conjugates of q. Thus, P is contained in the set of points at infinity of $\mathcal{W}$. It follows that $\mathcal{W}$ is of degree at least n; since $\mathcal{W} \subseteq \mathcal{U}, \mathcal{U} = \mathcal{W}$. Therefore, $\mathcal{U}$ is irreducible and $\mathcal{I}(\mathcal{U})$ is generated by polynomials with coefficients over $\mathbb{K}$. Now, consider the pencil of hyperplanes $H_t \equiv x_0 + x_1\alpha + \cdots + x_{n-1}\alpha^{n-1} - t$, where t takes values in $\mathbb{F}$. Notice that $\overline{H_t} \cap P = \{P_2, \ldots, P_n\}$. Thus, $P_1 \in \overline{\mathcal{U}} \setminus \overline{H_t}$ so, for all t, $\mathcal{U} \not\subseteq H_t$. Moreover, for every point $p = (p_0, \ldots, p_{n-1}) \in \mathcal{U}$, $t(p) = \sum_{i=0}^{n-1} p_i\alpha^i \in \mathbb{F}$ is such that $\overline{H}_{t(p)} \cap \overline{\mathcal{U}} = \{p, P_2, \ldots, P_n\}$. The cardinal of $\{t(p) \mid t \in \mathcal{U}\}$ is infinite, since otherwise, by the irreducibility of $\mathcal{U}$, it would imply that there is a t_0 such that $\mathcal{U} \subseteq H_{t_0}$, which is impossible. So, for generic t, the intersection is $\overline{H}_t \cap \overline{\mathcal{U}} = \{p(t), P_2, \ldots, P_n\}$. Let us check that the coordinates of $p(t)$ are rational functions in $\mathbb{K}(\alpha)(t)$. Take the ideal $\mathcal{I}(\mathcal{U})$ of $\mathcal{U}$. The ideal of $p(t)$ (as a point in $\mathbb{F}(t)^n$) is $I + H_t$, defined over $\mathbb{K}(\alpha)(t)$. The reduced Gröbner basis of the radical $I+H_t$ is of this kind $(x_0-\psi_0, \ldots, x_{n-1}-\psi_{n-1})$ and, by Theorem 6.17, it is also defined over $\mathbb{K}(\alpha)(t)[x_0, \ldots, x_{n-1}]$. Hence, $(\psi_0, \ldots, \psi_{n-1})$ is a $\mathbb{K}(\alpha)$-parametrization of $\mathcal{U}$. Thus, since $\mathcal{U}$ is irreducible, it is rational. Moreover $\sum_{i=0}^{n-1}(\psi_i(t))\alpha^i = t$ and the parametrization is proper. As the curve is rational and has an infinite number of points over $\mathbb{K}$, by Proposition 6.30, it is parametrizable over $\mathbb{K}$. Let $u(t)$ be a unit such that $\Psi \circ u(t) = (\phi_0(t), \ldots, \phi_{n-1}(t))$ is a parametrization over $\mathbb{K}$, where $\phi_i(t) \in \mathbb{K}(t)$ and $\sum_{i=0}^{n-1} \phi_i(t)\alpha^i = u(t)$. We conclude that $\mathcal{U}$ is the hypercircle associated to the unit $u(t)$. □

Remark from the proof of Proposition 6.30 that a parametric curve, definable over $\mathbb{K}$ and with a regular point over $\mathbb{K}$, is parametrizable over the same field; for this, it is enough to $\mathbb{K}$-birationally project the curve over a plane, such that the $\mathbb{K}$-regular point stays regular on the projection. Then, a small modification of the proof above, yields the following:

Theorem 8.25. *Let $\mathcal{U} \subseteq \mathbb{F}^n$ be a 1-dimensional irreducible algebraic set of degree n, definable over $\mathbb{K}$. Then, it is a primitive α-hypercircle if and only if it has a regular point with coordinates in $\mathbb{K}$ and passes through the set of points at infinity characterized in Theorem 8.13.*

Chapter 9

Applications of Hypercircles

9.1 Hypercircles and Witness Varieties

In this Section, we refine the results of Theorem 7.16 for the case of curves. Let $\mathcal{V}$ be a parametric curve given by a proper parametrization ϕ with coefficients in $\mathbb{K}(\alpha)$, $[\mathbb{K}(\alpha) : \mathbb{K}] = d$. Let $\mathcal{Z}$ be the witness variety associated to ϕ. By Theorem 7.16, $\mathcal{V}$ is $\mathbb{K}$-parametrizable if and only if $\mathcal{Z} \cap U$ contains a hypercircle as a component. For the case of curves we can provide better results.

Proposition 9.1. *Let $\mathcal{V} \subseteq \mathbb{F}^m$ be a parametric curve, given by a proper parametrization $\phi = (\phi_1, \ldots, \phi_m)$ with coefficients in $\mathbb{K}(\alpha)$. Let $\mathcal{Z}$ be the witness variety associated to ϕ. Then $\mathcal{V}$ is defined over $\mathbb{K}$ if and only if $\mathcal{Z}$ has infinitely many points.*

Proof. Let Φ be the parametrization of the Weil variety $\mathcal{W}$ obtained by development of ϕ. The witness variety $\mathcal{Z}$ is the Zariski closure of $Y \cap D_\delta$. Suppose that $\mathcal{Z}$ has infinitely many points. Then, there are infinitely many points in $Y \cap D_\delta$. Furthermore, the map Φ is finite to one. To prove this, let $v = (v_1, \ldots, v_n) \in \Phi(Y \cap D_\delta)$. Let $t = (t_0, \ldots, t_{d-1}) \in (Y \cap D_\delta)$ be a point such that $\Phi(t) = v$, then:

$$\sigma_l(\phi_j)(t_0 + \sigma_l(\alpha)t_1 + \ldots + \sigma_l(\alpha^{d-1})t_{d-1}) = \sum_{i=0}^{d-1} \sigma_l(\alpha)^i \phi_{ji}(t_0, \ldots, t_{d-1})$$

so, $\sum_{i=0}^{d-1} \sigma_l(\alpha)^i t_i$ is a solution of $\sigma_l(\phi_j)(y) = v_j$. As not every rational function ϕ_j is constant, there is an index j such that the equation $\sigma_l(\phi_j)(y) = v_j$ only has finitely many solutions $a_1, \ldots, a_s$. Necessarily, $t_0, \ldots, t_{d-1}$ is a solution of the linear system

$$\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_d \end{pmatrix} = \begin{pmatrix} 1 & \alpha & \alpha^2 & \ldots & \alpha^{d-1} \\ 1 & \sigma_2(\alpha) & \sigma_2(\alpha^2) & \ldots & \sigma_2(\alpha^{d-1}) \\ & & \cdot \ \cdot \ \cdot & \cdot \ \cdot & \\ 1 & \sigma_d(\alpha) & \sigma_d(\alpha^2) & \ldots & \sigma_d(\alpha^{d-1}) \end{pmatrix} \begin{pmatrix} t_0 \\ t_1 \\ \vdots \\ t_{d-1} \end{pmatrix}$$

with $y_i \in \{a_1, \ldots, a_s\}$, $1 \leq i \leq d$. Hence, there are only finitely many (at most s^d) solutions.

Thus, $\Phi(Y \cap D_\delta) \subseteq \widetilde{\mathcal{W}}$ has infinitely many points and $1 \leq \dim(\widetilde{\mathcal{W}}) \leq \dim(\mathcal{V}) = 1$. By Corollary 7.4, $\mathcal{V}$ is a $\mathbb{K}$-variety. Conversely, if $\mathcal{V}$ is a $\mathbb{K}$-variety, by Proposition 7.14, $\mathcal{Z}$ contains a component birational to $\mathcal{V}$. Hence, $\mathcal{Z}$ has infinitely many points. □

Now we prove that, in every case, $\mathcal{Z}$ has at most dimension 1.

Theorem 9.2. *Let $\mathcal{V} \subseteq \mathbb{F}^m$ be a parametric curve, given by a proper parametrization $\phi = (\phi_1, \ldots, \phi_m)$ with coefficients in $\mathbb{K}(\alpha)$. Let $\mathcal{Z}$ be the witness variety associated to ϕ. Then $\dim(\mathcal{Z}) \leq 1$ and $\mathcal{Z}$ has at most one $\mathbb{F}$-component of dimension 1.*

Proof. By hypothesis, the parametrization of $\mathcal{V}$ is proper, let

$$P(x_1, \ldots, x_n) \in \mathbb{K}(\alpha)(x_1, \ldots, x_n)$$

be the inverse of ϕ. Then, we have the algebraic identity $P(\phi_1(t), \ldots, \phi_n(t)) = t$. Let $P = \sum_{i=0}^{d-1} \alpha^i P_i(x_1, \ldots, x_n)$, with $P_i(x_1, \ldots, x_n) \in \mathbb{K}(x_1, \ldots, x_n)$, $0 \leq i \leq d-1$.

Define the map:

$$\begin{array}{rccc} \Lambda: & \mathbb{F}[x_0, \ldots, x_{d-1}] & \longrightarrow & \mathbb{F}(\mathcal{V}) \\ & x_i & \mapsto & P_i + \mathfrak{I}_{\mathbb{F}}(\mathcal{V}) \end{array}$$

$ker(\Lambda)$ is a prime ideal of $\mathbb{F}[x_0, \ldots, x_{d-1}]$, because the quotient is isomorphic to an integer domain. The dimension of $\mathcal{V}$ is one, so $\dim(ker(\Lambda)) \leq 1$. Our next objective is to show that $\dim(\mathfrak{I}_{\mathbb{F}}(\mathcal{Z})) \leq 1$. To prove this, let $f \in ker(\Lambda)$. Then, $f(\overline{P}_0, \ldots, \overline{P}_{d-1}) = \overline{0}$ in $\mathbb{F}(V)$. To show that $f \in \mathfrak{I}_{\mathbb{F}}(\mathcal{Z})$, it suffices to show that f vanishes in $Y \cap D_\delta$. By Theorem 7.7, if we substitute $x_j = \sum_{i=0}^{d-1} \alpha^i x_{ji}$ in P, and we write $P = \sum_{i=0}^{d-1} \alpha^i G_i(x_{10}, \ldots, x_{n,d-1})$, then $G_i(\phi_{10}, \ldots, \phi_{n,d-1}) = t_i$ in the change of parameters $t = \sum_{i=0}^{d-1} \alpha^i t_i$. On the other hand, if $s = (s_0, \ldots, s_{d-1}) \in Y \cap D_\delta$, then $\phi_{jk}(s) = 0$, $1 \leq j \leq n, k > 0$; $\phi_{j0}(s) = \phi_j(\sum_{i=0}^{d-1} \alpha^i s_i)$. So, if $s \in Y \cap D_\delta$

$$\sum_{i=0}^{d-1} \alpha^i P_i(\phi_{10}(s), \ldots, \phi_{n0}(s)) = \sum_{i=0}^{d-1} \alpha^i P_i(\phi_1(\sum_{i=0}^{d-1} s_i), \ldots, \phi_n(\sum_{i=0}^{d-1} s_i)) = \sum_{i=0}^{n-1} \alpha^i s_i$$

whenever it is defined. Moreover, if $s \in Y \cap D_\delta$, $\Phi_0(s) = (\phi_{10}(s), \ldots, \phi_{n0}(s)) \in \mathcal{V}$ (See Theorem 7.7).

First, $\widetilde{\mathcal{W}}$ is of dimension ≤ 1, hence, P_i is defined in all but finitely many points of $\widetilde{\mathcal{W}}$. Second, Φ_0 is a finite to one map that is defined in $Y \cap D_\delta$ (Since Φ is finite to one). Hence, $P \circ \Phi_0$ is defined in all but finitely many points of $Y \cap D_\delta$ and

$$P_i \circ (\Phi_0)(s_0, \ldots, s_{d-1}) = s_i.$$

Let $\mathcal{Z}_0$ be the (possibly empty) finite set of points where either Φ_0 or $P_i \circ \Phi_0$ is not defined. If, $s \in \mathcal{Z} \setminus \mathcal{Z}_0$, then $s_i = P_i(\Phi(s))$ and

$$f(s) = f(P_0(\Phi_0(s)), \ldots, P_{d-1}(\Phi_0(s))) = f(P_0, \ldots, P_{d-1})(\Phi_0(s)) = 0$$

because $\Phi_0(s) \in \mathcal{V}$ and $f(P_0, \ldots, P_{d-1}) = 0$ in $\mathbb{F}(\mathcal{V})$. Thus,

$$ker(\Lambda) \subseteq \mathfrak{I}_{\mathbb{F}}(\mathcal{Z} \setminus \mathcal{Z}_0)$$

Hence, $\dim(\mathcal{Z} \setminus \mathcal{Z}_0) \leq 1$. Finally, as $\mathcal{Z}_0$ is a finite set, we conclude that $\dim(\mathcal{Z}) \leq 1$.

Let $\mathcal{Z}_1 \cup \ldots \cup \mathcal{Z}_r$ be a decomposition of $\mathcal{Z} \setminus \mathcal{Z}_0$ in $\mathbb{F}$-irreducible sets. Then $ker(\Lambda) \subseteq \mathfrak{I}_{\mathbb{F}}(\mathcal{Z} \setminus \mathcal{Z}_0) = \mathfrak{I}_{\mathbb{F}}(\mathcal{Z}_1) \cap \ldots \cap \mathfrak{I}_{\mathbb{F}}(\mathcal{Z}_r)$. From this, $ker(\Lambda) \subseteq \mathfrak{I}_{\mathbb{F}}(\mathcal{Z}_i)$, $1 \leq i \leq r$. If some $\mathcal{Z}_i$ is 1-dimensional, then $ker(\Lambda) = \mathfrak{I}_{\mathbb{F}}(\mathcal{Z}_i)$, because they are two prime ideals of the same dimension. Furthermore, the rest of the components must be 0-dimensional, because $\mathfrak{I}_{\mathbb{F}}(\mathcal{Z}_i) \subseteq \mathfrak{I}_{\mathbb{F}}(\mathcal{Z}_j)$ $1 \leq j \leq r,\ j \neq i$. □

To sum up, there are only two possibilities for the witness variety:

Corollary 9.3.

- *$\mathcal{Z}$ is a finite set and $\mathcal{V}$ is not $\mathbb{K}$-definable.*
- $\dim(\mathcal{Z}) = 1$, *then $\mathcal{V}$ is $\mathbb{K}$-definable, the unique 1-dimensional component of $\mathcal{Z}$ is $\mathfrak{V}_{\mathbb{F}}(ker(\Lambda))$ and the 0-dimensional components of $\mathcal{Z}$ are either points where Φ_0 or $F_i(\Phi_0)$ are not defined. In this case $\mathcal{V}$ is $\mathbb{K}$-parametrizable if and only if the 1-dimensional component of $\mathcal{Z}$ is a hypercircle with respect to the extension $\mathbb{K} \subseteq \mathbb{K}(\alpha)$.*

Thus, if $\mathcal{V}$ is a parametric curve given by a parametrization in $\mathbb{K}(\alpha)$, we can decide, from the set $\mathcal{Z}$, if $\mathcal{V}$ is $\mathbb{K}$-definable or not. Notice that the computation of $\mathcal{Z}$ is done without computing the implicit ideal of $\mathcal{V}$. So this method may be an advantage when the computation of the implicit ideal is comparatively hard. For example, if $d << n$.

Our next goal is to show that, if $\mathcal{V}$ is $\mathbb{K}$-definable, then the 1-dimensional component of $\mathcal{Z}$ has the structure of an α-hypercircle, possibly for another extension different from $\mathbb{K} \subseteq \mathbb{K}(\alpha)$. Due to technical reasons, the results are exposed for the case $\mathbb{K} = \mathbb{Q}$. But it is conjectured that the results hold whenever $\mathbb{K}$ is the minimun field of definition of the curve $\mathcal{V}$.

Let $\mathcal{V}$ be a curve $\mathbb{Q}$ definable given by a parametrization over $\mathbb{Q}(\alpha)$. Suppose that $\mathcal{V}$ is not parametrizable over $\mathbb{Q}$. By Proposition 6.29, there are quadratic fields $\mathbb{Q}(\beta)$ of parametrization of $\mathcal{V}$. Let $M(t)$ be the minimal polynomial of α over $\mathbb{Q}$ and suppose that $M(t)$ is irreducible in $\mathbb{Q}(\beta)[t]$. Then, it follows from the construction of the witness variety that the witness variety $\mathcal{Z}_1$ associated to $\mathcal{V}$ with respect to the extension $\mathbb{K} \subseteq \mathbb{K}(\alpha)$ equals the witness variety $\mathcal{Z}_2$ with respect to the extension $\mathbb{K}(\beta) \subseteq \mathbb{K}(\beta, \alpha)$. The 1-dimensional component of $\mathcal{Z}$ is an α-hypercircle of base field $\mathbb{K}(\beta)$, but it is not an α-hypercircle of base field $\mathbb{K}$. Now we prove that there is always such an element β. We need some previous results about quadratic fields of parametrization of a curve.

Every parametric curve $\mathcal{V}$ that is $\mathbb{Q}$-definable is $\mathbb{Q}$-birational to a plane conic ([Che51], [SW97], [Sha94]). Hence, we can reduce the problem to a plane conic. By a $\mathbb{Q}$-projective transformation, we can suppose that $\mathcal{C}$ is given by a plane conic $ax^2 + by^2 + cz^2 = 0$, where $a, b, c \in \mathbb{Z}^*$ are squarefree, pairwise coprime integers. That is, abc is nonzero and squarefree. Suppose that there is no point with rational coefficients in $\mathcal{C}$. The aim is to construct infinitely many quadratic fields $\mathbb{L} = \mathbb{Q}[\sqrt{D}]$ such

that there are points in $\mathcal{C}$ with coefficients in $\mathbb{L}$. The idea is to cut the conic with lines of type $y = nx$, for n a crafted prime. Moreover, without loss of generality, we may look for an affine point ($z = 1$). The intersection points of the $\mathcal{C}$ and the line $y = nx$ are:

$$\left[\sqrt{\frac{-c}{a+bn^2}} : n\sqrt{\frac{-c}{a+bn^2}} : 1\right], \quad \left[-\sqrt{\frac{-c}{a+bn^2}} : -n\sqrt{\frac{-c}{a+bn^2}} : 1\right]$$

Note that $a + bn^2 \neq 0$ since the conic does not have rational points.

Lemma 9.4. *With the previous assumptions, let $n, m \in \mathbb{Q}^*$, then*

$$\mathbb{Q}\left(\sqrt{\frac{-c}{a+bn^2}}\right) = \mathbb{Q}\left(\sqrt{\frac{-c}{a+bm^2}}\right)$$

if and only if $f(n,m) = \frac{a+bn^2}{a+bm^2}$ is a square in $\mathbb{Q}$.

Proof. The proof is elementary. If $f(n,m)$ is a square in $\mathbb{Q}$, then

$$\sqrt{\frac{-c}{a+bm^2}} = \sqrt{f(n,m)}\sqrt{\frac{-c}{a+bn^2}}.$$

Thus, $\mathbb{Q}\left(\sqrt{\frac{-c}{a+bn^2}}\right) = \mathbb{Q}\left(\sqrt{\frac{-c}{a+bm^2}}\right)$

On the other hand, suppose that both fields are equal, then $\sqrt{\frac{-c}{a+bm^2}} = r + s\sqrt{\frac{-c}{a+bn^2}}$, $r, s \in \mathbb{Q}$ so

$$\frac{-c}{a+bm^2} = r^2 + s^2\frac{-c}{a+bn^2} + 2rs\sqrt{\frac{-c}{a+bn^2}}$$

It must be $rs = 0$; if $s = 0$, then $\frac{-c}{a+bm^2}$ is a square, contrary to the hypothesis that $\mathcal{C}$ does not have points with rational coordinates. So $r = 0$ and $\frac{a+bn^2}{a+bm^2} = s^2$ is a rational square. □

Lemma 9.5. *Let $p \equiv 1$ mod 4 be a prime and $e \not\equiv 0$ mod p an integer. Then, there is an integer n such that $1 + en^2$ is not a quadratic residue mod p.*

Proof. Suppose the contrary, that $1 + en^2$ is always a quadratic residue. Then $[1 + ex]$ is a bijection of $\mathbb{Z}/p\mathbb{Z}$ such that maps the quadratic residues mod p onto themselves. It follows that it is a bijection among the quadratic residues mod p. In particular, there is a $[n]$ such that $[1 + en^2] = [0]$, so $[e] = [-1][n]^{-2}$. As $p \equiv 1$ mod 4, $[-1]$ is a square. Hence, e is a square mod p and we may suppose that the bijection is $1 + x$. But, in that case, [1] is a square, and also [2], [3] etc. that is, every residue is a square mod p which is impossible. □

Proposition 9.6. *Given a, b, c as in Lemma 9.4, there is an infinite set S such that: every element in S is a prime $q \equiv 1 \mod 4$, $q \nmid ab$ and, if $p, q \in S$, then*

$$f(p,q) = \frac{a+bp^2}{a+bq^2}$$

is not a square in $\mathbb{Q}$.

Proof. We will define S inductively, starting from $S_1 = \{q_1\}$ with q_1 any prime $q_1 \equiv 1 \mod 4$ such that $q_1 \nmid ab$.

Suppose we have defined a set $S_N = \{q_1, \ldots, q_N\}$ such that q_i is prime, $q_i \equiv 1 \mod 4$, $q_i \nmid ab$ and if $i \neq j$ then $\frac{a+bq_i^2}{a+bq_j^2}$ is not a square in $\mathbb{Q}$. We want to construct the set S_{N+1}. Consider the residual polynomial in the variable n with coefficients in $\mathbb{Z}/q_j\mathbb{Z}$

$$[a + bn^2][a + bq_j^2]^{-1} = [1] + [a]^{-1}[bn^2] = [1 + en^2].$$

Note that $[e] \neq [0]$ is well defined because $q_j \nmid ab$. Let m_j be such that such that $[1 + em_j^2]$ is not a square. This m_j exists by Lemma 9.5. Let p be a prime such that $p \equiv 1 \mod 4$, $p \equiv m_j \mod q_j$, $(p, ab) = 1$. This prime always exists: from the Chinese remainder theorem, we can compute the unique class $M \mod 4q_1 \cdots q_N$, from the equations. It follows that M is a unit in the residue ring so we can apply Dirichlet's theorem and find a p such that, in addition, it does not divide ab. Take $q_{N+1} = p$ in S_{N+1}. By construction, $p \equiv 1 \mod 4$, $p \nmid ab$ and, in $\mathbb{Z}/q_i\mathbb{Z}$

$$[a + bp^2][a + bq_i^2]^{-1} = [a + bm_j^2][a + bq_i^2]^{-1} = [1 + em_j^2]$$

which is not a square mod q_i, so $\frac{a+bp^2}{a+bq_i^2}$ is not a square in $\mathbb{Q}$, $1 \leq i \leq N$. □

Example 9.7. Let $\mathcal{C} = x^2 + y^2 - 6z^2 = 0$ which does not have points in $\mathbb{Q}^2$. We look for a set integers such that $\frac{1+n^2}{1+m^2}$ is never a square. Take $q_1 = 5$. Now we search a $[n]$ such that $1 + n^2$ is not a square mod 5. For example $1 + 1^2 = 2$ is not a square mod 5. Now compute a prime q_2 such that:

$$q_2 \equiv 1 \mod 4, \quad q_2 \equiv 1 \mod 5$$

By the Chinese reminder Theorem. $q_2 \equiv 1 \mod 20$ and, we can take, for example $q_2 = 41$. Now we need to compute q_3, we impose $1 + n^2$ not to be a square mod 41, the first non square of this form is $1 + 4^2 = 17$. Again we have the following system of residual equations

$$q_3 \equiv 1 \mod 4,\ q_3 \equiv 1 \mod 5,\ q_3 \equiv 4 \mod 41$$

So, this time, $q_3 \equiv 701 \mod 820$. we can take $q_3 = 701$. Applying again this method, we arrive that the next prime must be $q_4 \equiv 266381 \mod 574820$ and , in particular we can take, $q_4 = 266381$. That is, the intersection of $\mathcal{C}$ with the lines $y = 5x$, $y = 41x$, $y = 701x$ and $y = 266381x$ gives four different quadratic fields of parametrization of the conic. In this case, we obtain:

$$\mathbb{Q}\Big(\sqrt{\frac{3}{13}}\Big), \mathbb{Q}(\sqrt{3}), \mathbb{Q}\Big(\sqrt{\frac{3}{245701}}\Big), \mathbb{Q}\Big(\sqrt{\frac{3}{35479418581}}\Big)$$

Theorem 9.8. *Let $\mathcal{V}$ be a $\mathbb{Q}$-definable curve, not $\mathbb{Q}$-parametrizable. Then, there are infinitely many distinct quadratic fields $\mathbb{Q}(\beta)$ such that $\mathcal{V}$ has regular points with coefficients in $\mathbb{Q}(\beta)$.*

Proof. Let $\mathcal{C} = \mathfrak{V}_{\mathbb{C}}(ax^2 + by^2 + cz^2)$ be a conic that is $\mathbb{Q}$-birational to $\mathcal{V}$. abc nonzero and squarefree. By Proposition 9.6, there is an infinite set S such that, for every $p, q \in S$, $f(p,q) = (a+bp^2)(a+bq^2)$ is not a rational square. Then, by Lemma 9.4, the set of fields

$$\mathbb{Q}\left(\frac{-c}{a+bs^2}\right), s \in S$$

is an infinite set of fields such that $\mathcal{V}$ has points with coordinates over them. □

Corollary 9.9. *Let $\mathcal{V}$ be a curve $\mathbb{Q}$-definable, that is not $\mathbb{Q}$-parametrizable given by a $\mathbb{Q}(\alpha)$ parametrization. Let $\mathcal{U}$ be the 1-dimensional component of the witness variety of $\mathcal{V}$. Then, there are infinitely many quadratic elements β such that $\mathcal{U}$ is a hypercircle for the extension $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\beta, \alpha)$.*

Proof. By the Theorem, there are infinitely many quadratic fields $\mathbb{Q}(\gamma)$ such that $\mathcal{V}$ has regular points over $\mathbb{Q}(\gamma)$. It follows that there are infinitely many fields quadratic of parametrization $\mathbb{Q}(\gamma)$. Let β be any of this quadratic elements such that β does not belong to the normal closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. There are infinitely many β satisfying this condition. Then, the minimal polynomial of α over $\mathbb{Q}(\beta)$ equals the minimal polynomial over $\mathbb{Q}$. Hence, by the computational definition of the witness variety, we obtain the same variety $\mathcal{U}$ when applying the method over the extension $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\beta, \alpha)$ and it is a hypercircle with respect to this extension. □

9.2 Birational Reparametrization of a Curve

In this Section, we present a example of the classical application of hypercircles to the algebraic reparametrization problem (see for example [ARS97], [ARS99], [RSV04] [SV01], [SV02]). Given a rational curve $\mathcal{C}$ defined over $\mathbb{K}$ by a proper parametrization over $\mathbb{K}(\alpha)$, we want to decide whether $\mathcal{C}$ can be parametrized over $\mathbb{K}$ and, in the affirmative case, find a change of parameter transforming the original parametrization into a parametrization over $\mathbb{K}$. By Corollary 9.3, the Weil variety $\mathcal{Z}$ associated to $\mathcal{C}$ has exactly one component $\mathcal{U}$ that is a curve. By Theorem 7.16, $\mathcal{C}$ is parametrizable over $\mathbb{K}$ if and only if $\mathcal{U}$ is an α-hypercircle for the extension $\mathbb{K} \subseteq \mathbb{K}(\alpha)$. Moreover, if $\mathcal{U}$ is a hypercircle, any generating unit u of $\mathcal{U}$ is the change of parameter needed to obtain a proper rational parametrization over $\mathbb{K}$ of $\mathcal{C}$.

In the following example, we illustrate how to use the knowledge of the geometry of hypercircles to help solving the problem. Suppose given the parametric curve $\mathcal{C}$ given by

$$(\eta_1(t), \eta_2(t)) = \left(\frac{(-2t^4 - 2t^3)\alpha - 2t^4}{6\alpha^2 t^2 + (4t^3 - 2)\alpha + t^4 - 8t}, \frac{-2t^4\alpha}{6\alpha^2 t^2 + (4t^3 - 2)\alpha + t^4 - 8t}\right)$$

where α is algebraic over $\mathbb{Q}$ with minimal polynomial $x^3 + 2$. We compute the Weil variety associated to $\mathcal{C}$ by writing $\eta_i(\sum_{j=0}^{2} t_j \alpha^j) = \sum_{j=0}^{2} \frac{q_{ij}(t_0,t_1,t_2)}{N(t_0,t_1,t_2)}$. In this situation $\mathcal{C}$ is $\mathbb{Q}-$definable if and only if

$$\mathcal{U} = \overline{\mathfrak{V}_{\mathbb{C}}(q_{11}, q_{12}, q_{21}, q_{22}) \setminus \mathfrak{V}_{\mathbb{C}}(N)}$$

is of dimension 1. Moreover, $\mathcal{C}$ is $\mathbb{Q}$-parametrizable if and only if the one-dimensional component of $\mathcal{V}$ is an α-hypercircle. For this example, the equations of $\mathcal{W}$ are:
$\mathcal{W} = \mathfrak{V}_{\mathbb{C}}(2t_0^3t_2 - 4t_2^4 + 3t_0^2t_1^2 + 2t_1^3t_2 + 2t_0t_2^2 + 2t_1^2t_2 - t_0^2t_1 + 6t_0t_1t_2^2, -6t_0^2t_1t_2 + t_0^4 + 2t_0t_1^2 - 8t_0t_2^3 - 2t_0t_1^3 + 2t_0^2t_2 - 4t_1t_2^2 - 12t_1^2t_2^2, 12t_2^2t_1^3 - 9t_0t_1t_2^3 + 6t_2^5 - 4t_0t_1^3 - 2t_0^2t_1t_2 + 4t_1^2t_2^2 - 4t_0t_2^3, 9t_0t_1^2t_2^2 - 9t_0^2t_2^3 - 2t_0^3t_2 - 2t_1^3t_2 + 6t_0t_1t_2^2 - 2t_2^4 + t_0^2t_1 - 2t_1^2t_2 - 2t_0t_2^2, 6t_0^2t_1t_2^2 + 12t_1^2t_2^3 - t_0^3t_1 - 2t_0t_1^2t_2 - 2t_0^2t_2^2 + 8t_1t_2^3, 6t_0^3t_2^2 + 9t_0t_1t_2^3 - 6t_2^5 + 2t_0t_1^3 - 2t_0^2t_1t_2 + 4t_1^2t_2^2 + 8t_0t_2^3, 18t_2t_1^4 + 36t_2^4t_1 + 14t_0^3t_2 + 32t_1^3t_2 + 12t_0t_1t_2^2 - 4t_2^4 - 7t_0^2t_1 + 14t_1^2t_2 + 14t_0t_2^2, 6t_0t_1^3t_2 + 2t_0t_1^2t_2 + t_0^3t_1 + 2t_0^2t_2^2 - 8t_1t_2^3 + 12t_2^4t_0, 9t_0^3t_2t_1 - 36t_2^4t_1 - 4t_0^3t_2 - 4t_1^3t_2 + 12t_0t_1t_2^2 - 4t_2^4 + 2t_0^2t_1 - 4t_1^2t_2 - 4t_0t_2^2, 6t_1^5 + 48t_1^2t_2^3 - 36t_2^4t_0 - 11t_0^3t_1 + 6t_1^4 + 14t_0t_1^2t_2 - 22t_0^2t_2^2 + 64t_1t_2^3, 3t_1^4t_0 + 6t_0t_1t_2^3 + 2t_0t_1^3 + t_0^2t_1t_2 - 2t_1^2t_2^2 + 2t_0t_2^3, 27t_2^4t_1^2 - 27t_0t_2^5 - 9t_0^2t_2^3 + 9t_2^4t_1 - 2t_0^3t_2 - 2t_1^3t_2 + 6t_0t_1t_2^2 - 2t_2^4 + t_0^2t_1 - 2t_1^2t_2 - 2t_0t_2^2, 6t_2^4t_0^2 + 12t_2^5t_1 - 5t_0t_1t_2^3 + 2t_2^5, t_0t_2^5t_1 + 2t_2^7)$

Thus the main point is to verify that this curve is a hypercircle. If $\mathcal{U}$ is a hypercircle, then its points at infinity must be as in Theorem 8.13. So, let us first of all check whether this is the case. The set of generators of the defining ideal form a Gröbner basis with respect to a graded order, thus to compute the points at infinity we take the set of leading forms of these polynomials. This yields:
$\{t_0^4 - 2t_0t_1^3 - 6t_0^2t_1t_2 - 12t_1^2t_2^2 - 8t_0t_2^3, 2t_0^3t_2 - 4t_2^4 + 3t_0^2t_1^2 + 2t_1^3t_2 + 6t_0t_1t_2^2, 9t_0t_1^2t_2^2 - 9t_0^2t_2^3, 12t_2^2t_1^3 - 9t_0t_1t_2^3 + 6t_2^5, 6t_0^2t_1t_2^2 + 12t_1^2t_2^3, 6t_0^3t_2^2 + 9t_0t_1t_2^3 - 6t_2^5, 18t_2t_1^4 + 36t_2^4t_1, t_0t_2^5t_1 + 2t_2^7, 6t_0t_1^3t_2 + 12t_2^4t_0, 9t_0^3t_2t_1 - 36t_2^4t_1, 6t_1^5 + 48t_1^2t_2^3 - 36t_2^4t_0, 3t_1^4t_0 + 6t_0t_1t_2^3, 27t_2^4t_1^2 - 27t_0t_2^5, 6t_2^4t_0^2 + 12t_2^5t_1\}$

The solutions of this system, after dehomogenizing $\{t_2 = 1\}$, are $t_0 = t_1^2, t_1^3 + 2 = 0$. That is, the points at infinity are of the form $[\alpha_i^2 : \alpha_i : 1 : 0]$, $\frac{x^3+2}{x-\alpha} = x^2 + \alpha x + \alpha^2$. Thus, by Proposition 8.14, the points at infinity of $\mathcal{U}$ are those of an α-hypercircle. This is not surprising, because, by Corollary 9.9, $\mathcal{U}$ is a hypercircle for, possibly, another extension $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\beta, \alpha)$.

Now, following Proposition 8.18, we may try to parametrize $\mathcal{U}$ by the pencil of hyperplanes $t_0 + \alpha t_1 + \alpha^2 t_2 - t$. Doing so, we obtain the parametrization

$$\left(\frac{(\alpha^2 + 2\alpha t + t^2)t}{3\alpha t + \alpha^2 + 3t^2}, \frac{-1/2\alpha^2 t^3}{3\alpha t + \alpha^2 + 3t^2}, \frac{-1/2\alpha t^2(t+\alpha)}{3\alpha t + \alpha^2 + 3t^2}\right).$$

Remark that this parametrization can also be computed by means of inverse computation techniques as described in [SV02]. Then, by direct computation, we observe that the parametric irreducible curve defined by this parametrization is of degree 3, passes through the point $(0, 0, 0)$ and this point is regular. Moreover, it is $\mathbb{Q}$-definable, since it is the only 1-dimensional component of $\mathcal{V}$ (see [ARS99]), which is, by construction, a $\mathbb{Q}$-definable variety. It follows from Theorem 8.25 that it is a hypercircle.

In [RSV04], it is presented an algorithm that takes a parametrization of a hypercircle over $\mathbb{K}(\alpha)$ and a base point $p \in \mathcal{U} \cap \mathbb{K}^n$ and returns a unit $u(t)$ generating the hypercircle. If we apply this algorithm to our example, the unit $u(t) = \frac{2}{2t+\alpha^2}$ is obtained. So, $\mathcal{V}$ is the hypercircle associated to $u(t)$ and $\mathcal{C}$ is parametrizable over $\mathbb{Q}$. In particular, the parametrization of $\mathcal{V}$ associated to $u(t)$ is $\left(\frac{2t^2}{2t^3+1}, \frac{-1}{2t^3+1}, \frac{-t}{2t^3+1}\right)$. Moreover, the unit $u(t)$ gives the change of parameter we need to compute a parametrization of $\mathcal{C}$ over the base

field (see [ARS99]), namely:

$$\eta\left(u(t)\right) = \left(\frac{t+1}{t^4}, \frac{1}{t^4}\right).$$

9.3 Optimal Affine Reparametrization of a Curve

In the previous Section, we have shown how the hypercircles help to solve the algebraic reparametrization problem. However, in order to obtain a generating unit of the hypercircle. It is needed a base point $p \in \mathcal{U} \cap \mathbb{K}^n$. The problem of obtaining a base point cannot be avoided and it is equivalent to obtain a generating unit u of the hypercircle, since from a unit $u(t) = \frac{at+b}{t+d}$ it is trivial to obtain a base point. Namely, substitute t by $v \in \mathbb{K}(\alpha)$ then $u(v) = \sum_{i=0}^{n-1} \alpha^i w_i$, $w_i \in \mathbb{K}$, $0 \leq i \leq n-1$, the point $(w_0, \ldots, w_{n-1})$ is in $\mathcal{U} \cap \mathbb{K}^n$. In this Section, we present an original method of optimal reparametrization by affine change of variables. As we will use the results in Section 9.1, we will always suppose that our base field in the rationals $\mathbb{Q}$. Suppose that $\mathcal{V}$ is given by a parametrization ϕ over $\mathbb{Q}(\alpha)$. We want to obtain reparametrizations of $\mathcal{V}$ by affine change of variables $t \mapsto v_1 t + v_0$ only. In this case, there is a minimun field (up to isomorphism) $\mathbb{Q}(\gamma)$ such that $\phi(v_1 t + v_2) \in \mathbb{Q}(\gamma)(t)$. That is, there are v_1, v_0 such that $\phi(v_1 t + v_0) \in \mathbb{Q}(\gamma)(t)$ and, for every pair $e_1, e_0 \in \mathbb{C}$, $e_1 \neq 0$, the field generated over $\mathbb{Q}$ by the coefficients of $\phi(e_1 t + e_0)$ contains (a field isomorphic to) $\mathbb{Q}(\gamma)$. Moreover, to obtain a reparametrization over $\mathbb{Q}(\gamma)$, we do not need a base point as in the previous Section. This is a generalization of the reparametrization problem for polynomially parametrizable curves in [SV01].

Lemma 9.10. *Let $\mathcal{V}$ be a $\mathbb{Q}$-definable curve given by a parametrization over $\mathbb{Q}(\alpha)$. Let $\mathcal{U}$ be the 1 dimensional component of the witness variety of $\mathcal{V}$. Then, there is at least one point at infinity of $\mathcal{U}$ that admits a representation over $\mathbb{Q}(\alpha)$.*

Proof. If $\mathcal{U}$ is a primitive α-hypercircle, the result follows from Proposition 8.14. If $\mathcal{U}$ is not a primitive hypercircle, then, by Theorem 8.11, $\mathcal{U}$ is $\mathbb{Q}$-affinely isomorphic to a primitive hypercircle $\mathcal{U}_1$ for the extension $\mathbb{Q} \subseteq \mathbb{Q}(d)$, where $d \in \mathbb{Q}(\alpha)$. Hence, at least one point at infinity of $\mathcal{U}_2$ has a representation over $\mathbb{Q}(d) \subseteq \mathbb{Q}(\alpha)$. As the affine isomorphism is defined over $\mathbb{Q}$, the corresponding point at infinity of $\mathcal{U}$ also admits a representation in $\mathbb{Q}(\alpha)$.

Suppose now that $\mathcal{V}$ is not $\mathbb{Q}$-parametrizable. Then, by Corollary 9.9, there are infinitely many quadratic elements β over $\mathbb{Q}$ such that $\mathcal{U}$ is a hypercircle with respect to the extension of fields $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\beta, \alpha)$. As there are only finite points at infinity, we conclude that there is a point p at infinity that admits a representation over infinitely many fields of the form $\mathbb{Q}(\beta, \alpha)$. Necessarily, this point admits a representation over $\mathbb{Q}(\alpha)$. □

Let $\mathcal{V}$ is parametric curve parametrizable over $\mathbb{Q}$ but such that it is given by a parametrization over $\mathbb{Q}(\alpha)$. $[\mathbb{Q} : \mathbb{Q}(\alpha)] = n$. Suppose that the associated hypercircle $\mathcal{U}$ to $\mathcal{V}$ is of degree $r < n$. Let $u(t) = \frac{at+b}{t+d} \in \mathbb{Q}(\alpha)(t)$ be a unit associated to $\mathcal{U}$.

Then $\mathbb{Q}(d) \subsetneq \mathbb{Q}(\alpha)$ and $[\mathbb{Q}(d) : \mathbb{Q}] = r$. By Theorem 8.11, $\mathcal{U}$ is $\mathbb{Q}$-isomorphic to the hypercircle defined by $\frac{1}{t+d}$ in $\mathbb{C}^r$. Here, we present how to compute the d from the implicit equations of $\mathcal{U}$ and a reparametrization of $\mathcal{V}$ over $\mathbb{Q}(d)$.

Proposition 9.11. *In this conditions, let $[a_1 : \ldots : a_n : 0]$ be a point at infinity of $\mathcal{U}$ given by a representation over $\mathbb{Q}(\alpha)$, suppose that it is dehomogenized with respect to an index i. Without loss of generality, we may suppose that $a_1 = 1$. Then, $\mathbb{Q}(d)$ is isomorphic to $\mathbb{Q}(a_1, \ldots, a_n)$.*

Proof. By Theorem 8.9, $\mathcal{U}$ is affinely equivalent over $\mathbb{Q}$ to the hypercircle $\mathcal{U}_1$ associated to $\frac{1}{t+d}$ and, hence, the (dehomogenized) points at infinity of $\mathcal{U}$ and $\mathcal{U}_1$ generate the same algebraic extension over $\mathbb{Q}$. So, without loss of generality, we may suppose that $u(t) = \frac{1}{t+d}$. Let $M(t) = t^r + k_{r-1}t^{r-1} + \cdots + k_0$ be the minimal polynomial of $-d$ over $\mathbb{Q}$ and let $m(t) = \frac{M(t)}{t+d} = l_{r-1}t^{r-1} + l_{r-2}t^{r-2} + \cdots + l_0 \in \mathbb{Q}(d)$. Let $\mathcal{U}_d \subseteq \mathbb{C}^r$ be the hypercircle associated to $u(t)$ for the extension of fields $\mathbb{Q} \subseteq \mathbb{Q}(d)$. By Proposition 8.14 the points at infinity of $\mathcal{U}_d$ are

$$[l_0 : l_1 : \cdots : l_{n-2} : l_{n-1} : 0]$$

and its conjugates. Notice that $l_{r-2} = k_{r-1} - d$, so $\mathbb{Q}(l_0, \ldots, l_r) = \mathbb{Q}(d)$. Finally, since the affine inclusion $\mathbb{C}^r \to \mathbb{C}^n$ that maps $\mathcal{U}_d$ onto $\mathcal{U}$ is defined over $\mathbb{Q}$, the field that generates the points at infinity is the same, by conjugation, $\mathbb{Q}(a_0, \ldots, a_{n-1})$ is isomorphic to $\mathbb{Q}(l_0, \ldots, l_{n-1}) = \mathbb{Q}(d)$. □

Once we know how to compute d, we have a method to reparametrize a curve over $\mathbb{Q}(d)$.

Theorem 9.12. *Let $\mathcal{V}$ be a curve $\mathbb{Q}$-definable given by a parametrization ϕ with coefficients in $\mathbb{Q}(\alpha)$. Let $[a_0 : \ldots : a_{n-1} : 0]$ be a point at infinity of the witness variety $\mathcal{U}$, given by a representation over $\mathbb{Q}(\alpha)$ and dehomogenized with respect to a coordinate i. Suppose that the degree of $\mathcal{U}$ is $r < n$. Then, $\mathcal{V}$ admits a reparametrization over $\mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\alpha)$, where $[\mathbb{Q}(\gamma) : \mathbb{Q}] = r$.*

Moreover, if $e_1, e_2 \in \mathbb{C}$, $e_1 \neq 0$ are algebraic numbers, let $\phi(e_1t + e_2)$ be another parametrization of $\mathcal{V}$ and let $\mathbb{L}$ be the field generated over $\mathbb{Q}$ by the coefficients of $\phi(e_1t + e_2)$, then

1. *$\mathbb{L}$ contains (a field isomorphic to) $\mathbb{Q}(\gamma)$.*
2. *$[\mathbb{L} : \mathbb{Q}] \geq r$.*
3. *If $[\mathbb{L} : \mathbb{Q}] = r$ then $\mathbb{L}$ is isomorphic to $\mathbb{Q}(\gamma)$.*
4. *There are $e_1', e_2' \in \mathbb{L}$ such that $e_1't + e_2'$ reparametrizes ϕ over (a field isomorphic to) $\mathbb{Q}(\gamma)$.*

Proof. Let γ be a primitive element of $\mathbb{Q}(a_0, \ldots, a_{n-1}) \subseteq \mathbb{Q}(\alpha)$. If $\mathcal{V}$ is not $\mathbb{Q}$-parametrizable, by Corollary 9.9, there is a β such that $\mathcal{U}$ is a hypercircle for the extension $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\beta, \alpha)$ and $\mathbb{Q}(\beta, \gamma) = \mathbb{Q}(\beta, a_0, \ldots, a_{n-1})$. If $\mathcal{V}$ is $\mathbb{Q}$-parametrizable,

just take $\beta \in \mathbb{Q}$. Let $u(t) = \frac{at+b}{t+d} \in \mathbb{Q}(\beta, \alpha)(t)$ be a unit associated to $\mathcal{U}$, then, by Proposition 9.11, $\mathbb{Q}(\beta, d)$ is isomorphic to $\mathbb{Q}(\beta, \gamma)$. By the transformation $t \to \frac{1}{s} - d$, it follows that $v(t) = (b - ad)s + a$ reparametrizes $\mathcal{V}$ over $\mathbb{Q}(\beta, \gamma)$. Let $\mathcal{U}_2$ be the witness variety of $\mathcal{V}$ with respect to the extension $\mathbb{Q}(\beta, \gamma) \subseteq \mathbb{Q}(\beta, \alpha)$. This witness variety is an α-hypercircle by Theorem 7.16. Moreover, $v(t)$ is a unit associated to $\mathcal{U}_2$ since it reparametrizes $\mathcal{V}$. By Theorem 8.6, $\mathcal{U}_2$ is a line in $\mathbb{C}^{n/r}$. Hence, it is trivial to parametrize $\mathcal{U}_2$ over any field of definition. Note that, in the computational procedure defining $\mathcal{U}_2$, the element β does not play any role. That is, the defining equations of $\mathcal{U}_2$ have coefficients in $\mathbb{Q}(\gamma)$. Hence, there is another polynomial unit $v_2(t) \in \mathbb{Q}(\gamma)[t]$ that reparametrizes $\mathcal{V}$ over the field $\mathbb{Q}(\gamma)$.

For the second part, let β be a quadratic element in the conditions of Corollary 9.9 such that does not belong to the normal closure of $\mathbb{L}(\alpha, v_1, v_2)$ over $\mathbb{Q}$. Let $u = \frac{at+b}{t+d}$ be the unit that reparametrizes $\mathcal{V}$ over $\mathbb{Q}(\beta)$. Let $\phi_v = \phi(v_1 t + v_2) \in \mathbb{L}(t)$. On the one hand,

$$w_1(t) = \frac{\frac{a-v_2}{v_1}t + \frac{b-v_2 d}{v_1}}{t+d} \in \mathbb{L}(\beta, \alpha, v_1, v_2)$$

reparametrizes ϕ_v over $\mathbb{Q}(\beta)$. On the other hand, by Theorem 7.16, there is another unit $w_2 = \frac{a't+b'}{t+d'} \in \mathbb{L}(\beta)(t)$ that reparametrizes ϕ_v over $\mathbb{Q}(\beta)$. Then, there is a unit $w_3 = \frac{a''t+b''}{t+d''} \in \mathbb{Q}(\beta)$ such that $w_1 = w_2 \circ w_3 \in \mathbb{L}(\beta)(t)$. Hence, $d \in \mathbb{L}(\beta)$. By the choose of β, $d \in \mathbb{L}$. So we have the first item, because $\mathbb{Q}(d)$ is isomorphic to $\mathbb{Q}(\gamma)$. The rest of the items follows easily from this one and the proof of the first part. □

Example 9.13. Let α be a root of $x^4-4x^3+12x^2-16x+8$, and let $\mathcal{V}$ be the parametric curve given by

$$x = \frac{-24 + 72\alpha - 36\alpha^2 + 24\alpha^3 + (176 - 208\alpha - 16\alpha^3 + 72\alpha^2)t - 16t^2}{-88 + 104\alpha - 36\alpha^2 + 8\alpha^3 + 16t},$$

$$y = \frac{-96 - 16\alpha + 72\alpha^2 - 8\alpha^3 + (32 + 32\alpha + 32\alpha^2)t + (96 - 128\alpha + 48\alpha^2 - 16\alpha^3)t^2}{-176 + 208\alpha - 72\alpha^2 + 16\alpha^3 + 32t}$$

The hypercircle $\mathcal{U}$ associated to this curve has implicit equations:

$$\{4t_2 + 12t_3 - 3, 5 + 2t - 1 - 16t_3, 2t_0^2 + 24t_3t_0 + 80t_3^2 - 10t_0 - 52t_3 + 15\}.$$

One can easily check that this hypercircle is non primitive, because it is contained in the hyperplane $4t_2 + 12t_3 - 3$. Moreover, from its equations, it is a conic. The points at infinity are:

$$[2\gamma : 8 : -2 : 1]$$

where γ is a root of $x^2+6x+10$. The roots of this polynomial in $\mathbb{Q}(\alpha)$ are $-4\alpha+3/2\alpha^2-1/2\alpha^3$ and $-6 + 4\alpha - 3/2\alpha^2 + 1/2\alpha^3$. Choose for example $\gamma = -4\alpha + 3/2\alpha^2 - 1/2\alpha^3$. Then, the minimal polynomial of α over $\mathbb{Q}(\gamma)$ is $x^2 + (-8 - 2\gamma)x + 8 + 2\gamma$. Now, we

rewrite the parametrization of $\mathcal{V}$ over this extension of fields:

$$x = \frac{(21+9\gamma)\alpha - 39 - 15\gamma + ((6\gamma+14)\alpha - 2\gamma - 2)t - 2t^2}{1+\gamma+(-3\gamma-7)\alpha + 2t}$$

$$y = \frac{-30 - 5\gamma + (6\gamma+27)\alpha + (-14 - 4\gamma + (18+4\gamma)\alpha)t + (2\gamma+6)t^2}{1+\gamma+(-3\gamma-7)\alpha + 2t}$$

we compute the hypercircle associated to the extension $\mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\gamma, \alpha)$. We know that it will be a line, in fact, the computation yields $2t_1 - 3\gamma - 7$, that can be parametrized by $(s, (3\gamma+7)/2)$. Hence, the affine substitution $t = t + (3\gamma+7)/2\alpha$ in the parametrization yields a parametrization over the subfield $\mathbb{Q}(\gamma)$

$$x = \frac{-3\gamma - 2t^2\gamma + 4t\gamma - 5 + 6t^2 - 4t^3}{5 - 8t + 4t^2}$$

$$y = 2\frac{7t\gamma + 2t^3\gamma - 3\gamma - 6t^2\gamma - 10 + 23t + 6t^3 - 19t^2}{5 - 8t + 4t^2}$$

Bibliography

[AGR96] C. Alonso, J. Gutiérrez, and T. Recio. A rational function decomposition algorithm using near-separated polynomials. *Extracta Mathematicae*, 11(3):475–479, 1996.

[AGR01] C. Alonso, J. Gutierrez, and R. Rubio. On the dimension and the number of parameters of a unirational variety. In *Cryptography and computational number theory (Singapore, 1999)*, volume 20 of *Progr. Comput. Sci. Appl. Logic*, pages 3–9. Birkhäuser, Basel, 2001.

[Alo94] C. Alonso. *Desarrollo, análisis e implementación de algoritmos para la manipulación de variedades paraméricas*. PhD thesis, Universidad de Cantabria, 1994.

[AM69] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[AR07] C. Andradas and T. Recio. Plotting missing points and branches of real parametric curves. *Applicable Algebra in Engineering, Communication and Computing*, 18(1-2):107–126, 2007.

[ARS97] C. Andradas, T. Recio, and J. R. Sendra. A relatively optimal rational space curve reparametrization algorithm through canonical divisors. In *Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation (Kihei, HI)*, pages 349–355 (electronic), New York, 1997. ACM.

[ARS99] C. Andradas, T. Recio, and J. R. Sendra. Base field restriction techniques for parametric curves. In *Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation (Vancouver, BC)*, pages 17–22 (electronic), New York, 1999. ACM.

[BCR98] J. Bochnak, M. Coste, and M.-F. Roy. *Real algebraic geometry*, volume 36 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1998. Translated from the 1987 French original, Revised by the authors.

[Ber75] D. N. Bernstein. The number of roots of a system of equations. *Akademija Nauk SSSR. Funkcional′ nyi Analiz i ego Priloženija*, 9(3):1–4, 1975.

[BJS+07] T. Bogart, A. Jensen, D. Speyer, B. Sturmfels, and R. Thomas. Computing tropical varieties. *Journal of Symbolic Computation*, 42(1-2):54–73, 2007.

[BN82] J. Bak and D. J. Newman. *Complex analysis*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1982.

[BW93] T. Becker and V. Weispfenning. *Gröbner bases*, volume 141 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1993. A computational approach to commutative algebra, In cooperation with Heinz Kredel.

[Che51] C. Chevalley. *Introduction to the Theory of Algebraic Functions of One Variable*. Mathematical Surveys, No. VI. American Mathematical Society, New York, N. Y., 1951.

[Cho88] S.-C. Chou. *Mechanical geometry theorem proving*, volume 41 of *Mathematics and its Applications*. D. Reidel Publishing Co., Dordrecht, 1988. With a foreword by Larry Wos.

[CLO97] D. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1997. An introduction to computational algebraic geometry and commutative algebra.

[Coh93] H. Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[Dem68] P. Dembowski. *Finite geometries*. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 44. Springer-Verlag, Berlin, 1968.

[DSS05] M. Develin, F. Santos, and B. Sturmfels. On the rank of a tropical matrix. In *Combinatorial and computational geometry*, volume 52 of *Math. Sci. Res. Inst. Publ.*, pages 213–242. Cambridge Univ. Press, Cambridge, 2005.

[EGH96] D. Eisenbud, M. Green, and J. Harris. Cayley-Bacharach theorems and conjectures. *American Mathematical Society. Bulletin. New Series*, 33(3):295–324, 1996.

[EKL04] M. Einsiedler, M. Kapranov, and D. Lind. Non archimedean amoebas and tropical varieties. *Preprint*, 2004.

[Gat06] A. Gathmann. Tropical algebraic geometry. *Jahresbericht der Deutschen Mathematiker-Vereinigung*, 108(1):3–32, 2006.

[GKZ90] I. M. Gel′fand, M. M. Kapranov, and A. V. Zelevinsky. Newton polytopes of the classical resultant and discriminant. *Advances in Mathematics*, 84(2):237–254, 1990.

[GKZ94] I. M. Gel′fand, M. M. Kapranov, and A. V. Zelevinsky. *Discriminants, resultants, and multidimensional determinants*. Mathematics: Theory & Applications. Birkhäuser Boston Inc., Boston, MA, 1994.

[GM07] A. Gathmann and H. Markwig. The numbers of tropical plane curves through points in general position. *Journal für die reine und angewandte Mathematik*, pages 155–177, 2007.

[GMar] A. Gathmann and H. Markwig. The caporaso-harris formula and plane relative gromov-witten invariants in tropical geometry. *Mathematische Annalen*, (to appear).

[GTZ88] P. Gianni, B. Trager, and G. Zacharias. Gröbner bases and primary decomposition of polynomial ideals. *Journal of Symbolic Computation*, 6(2-3):149–167, 1988. Computational aspects of commutative algebra.

[Har77] R. Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[Har92] J. Harris. *Algebraic geometry*, volume 133 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992. A first course.

[IKS03] I. Itenberg, V. Kharlamov, and E. Shustin. Welschinger invariant and enumeration of real rational curves. *International Mathematics Research Notices*, 2003(49):2639–2653, 2003.

[IKS04] I. V. Itenberg, V. M. Kharlamov, and E. I. Shustin. Logarithmic equivalence of the Welschinger and the Gromov - Witten invariants. *Rossiĭskaya Akademiya Nauk. Moskovskoe Matematicheskoe Obshchestvo. Uspekhi Matematicheskikh Nauk*, 59(6(360)):85–110, 2004.

[IKS05] I. Itenberg, V. Kharlamov, and E. Shustin. Logarithmic asymptotics of the genus zero Gromov-Witten invariants of the blown up plane. *Geometry and Topology*, 9:483–491 (electronic), 2005.

[Ite04] I. Itenberg. Amibes de variétés algébriques et dénombrement de courbes (d'après G. Mikhalkin). *Astérisque*, 294:ix, 335–361, 2004.

[Jac85] N. Jacobson. *Basic algebra. I*. W. H. Freeman and Company, New York, second edition, 1985.

[KLP03] F.-V. Kuhlmann, H. Lombardi, and H. Perdry. Dynamic computations inside the algebraic closure of a valued field. In *Valuation theory and its applications, Vol. II (Saskatoon, SK, 1999)*, volume 33 of *Fields Inst. Commun.*, pages 133–156. Amer. Math. Soc., Providence, RI, 2003.

[KR00] M. Kreuzer and L. Robbiano. *Computational commutative algebra. 1*. Springer-Verlag, Berlin, 2000.

[KR06] K. H. Kim and F. W. Roush. Kapranov rank vs. tropical rank. *Proceedings of the American Mathematical Society*, 134(9):2487–2494 (electronic), 2006.

[Kus76] A. Kushnirenko. Newton polytopes and the bezout theorem. *Functional Analysis and Its Applications*, 10(3):233–235, 1976.

[Lan84] S. Lang. *Algebra*. Addison-Wesley Publishing Company Advanced Book Program, Reading, MA, second edition, 1984.

[Mar06] H. Markwig. *The enumeration of plane tropical curves*. PhD thesis, Technische Universität Kaiserslautern, July 2006.

[MC91] D. Manocha and J. Canny. Rational curves with polynomial parametrization. *Computer Aided Design*, 23(9):653–653, 1991.

[Mik03] G. Mikhalkin. Counting curves via lattice paths in polygons. *Comptes Rendus Mathématique. Académie des Sciences. Paris*, 336(8):629–634, 2003.

[Mik05] G. Mikhalkin. Enumerative tropical algebraic geometry in $\mathbb{R}^2$. *Journal of the American Mathematical Society*, 18(2):313–377 (electronic), 2005.

[PDS04] S. Pérez-Díaz and J. R. Sendra. Computation of the degree of rational surface parametrizations. *Journal of Pure and Applied Algebra*, 193(1-3):99–121, 2004.

[PDSS02] S. Pérez-Díaz, J. Schicho, and J. R. Sendra. Properness and inversion of rational parametrizations of surfaces. *Applicable Algebra in Engineering, Communication and Computing*, 13(1):29–51, 2002.

[RGST05] J. Richter-Gebert, B. Sturmfels, and T. Theobald. First steps in tropical geometry. In *Idempotent mathematics and mathematical physics*, volume 377 of *Contemp. Math.*, pages 289–317. Amer. Math. Soc., Providence, RI, 2005.

[Rob56] A. Robinson. *Complete theories*. North-Holland Publishing Co., Amsterdam, 1956.

[Roj99] J. M. Rojas. Toric intersection theory for affine root counting. *Journal of Pure and Applied Algebra*, 136(1):67–100, 1999.

[RS97a] T. Recio and J. R. Sendra. Real reparametrizations of real curves. *Journal of Symbolic Computation*, 23(2-3):241–254, 1997. Parametric algebraic curves and applications (Albuquerque, NM, 1995).

[RS97b] T. Recio and J. R. Sendra. A really elementary proof of real Lüroth's theorem. *Revista Matemática de la Universidad Complutense de Madrid*, 10(Special Issue, suppl.):283–290, 1997. Real algebraic and analytic geometry (Segovia, 1995).

[RSTV06a] T. Recio, J. R. Sendra, L. F. Tabera, and C. Villarino. Fast computation of the implicit ideal of an hypercircle. In *Actas de AGGM 2006*, pages 258–265, 2006.

[RSTV06b] T. Recio, J. R. Sendra, L. F. Tabera, and C. Villarino. Generalizing circles over algebraic extensions. *Manuscript*, 2006.

[RSV04] T. Recio, J. R. Sendra, and C. Villarino. From hypercircles to units. In *ISSAC 2004*, pages 258–265. ACM, New York, 2004.

[Sam67] P. Samuel. *Méthodes d'algèbre abstraite en géométrie algébrique*. Seconde édition, corrigée. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 4. Springer-Verlag, Berlin, 1967.

[Sha94] I. R. Shafarevich. *Basic algebraic geometry. 1*. Springer-Verlag, Berlin, second edition, 1994. Varieties in projective space, Translated from the 1988 Russian edition and with notes by Miles Reid.

[Shu06] E. Shustin. A tropical calculation of the Welschinger invariants of real toric del Pezzo surfaces. *Journal of Algebraic Geometry*, 15(2):285–322, 2006.

[Spe05] D. Speyer. *Tropical geometry*. PhD thesis, University of California, Berkeley, Spring 2005.

[SS04a] D. Speyer and B. Sturmfels. The tropical Grassmannian. *Adv. Geom.*, 4(3):389–411, 2004.

[SS04b] D. Speyer and B. Sturmfels. The tropical Grassmannian. *Advances in Geometry*, 4(3):389–411, 2004.

[Stu94] B. Sturmfels. On the Newton polytope of the resultant. *Journal of Algebraic Combinatorics. An International Journal*, 3(2):207–236, 1994.

[Stu96] B. Sturmfels. *Gröbner bases and convex polytopes*, volume 8 of *University Lecture Series*. American Mathematical Society, Providence, RI, 1996.

[Stu02] B. Sturmfels. *Solving systems of polynomial equations*, volume 97 of *CBMS Regional Conference Series in Mathematics*. Published for the Conference Board of the Mathematical Sciences, Washington, DC, 2002.

[SV01] J. R. Sendra and C. Villarino. Optimal reparametrization of polynomial algebraic curves. *International Journal of Computational Geometry & Applications*, 11(4):439–453, 2001.

[SV02] J. R. Sendra and C. Villarino. Algebraically optimal parametrizations of quasi-polynomial algebraic curves. *Journal of Algebra and its Applications*, 1(1):51–74, 2002.

[SW91] J. R. Sendra and F. Winkler. Symbolic parametrization of curves. *Journal of Symbolic Computation*, 12(6):607–631, 1991.

[SW97] J. R. Sendra and F. Winkler. Parametrization of algebraic curves over optimal field extensions. *Journal of Symbolic Computation*, 23(2-3):191–207, 1997. Parametric algebraic curves and applications (Albuquerque, NM, 1995).

[Tab03] L. F. Tabera. Geometría algebraica de las extensiones y restricciones de cuerpos. Tesina de Licenciatura, Universidad de Cantabria, 2003.

[Tab05] L. F. Tabera. Tropical constructive Pappus' theorem. *International Mathematics Research Notices*, 2005(39):2373–2389, 2005.

[Tab06a] L. F. Tabera. Computing the algebraic counterpart of a tropical plane geometric construction. In *Proceedings of Transgressive Computing 2006: a conference in honor of Jean Della Dora*, pages 357–364, 2006.

[Tab06b] L. F. Tabera. Constructive proof of extended kapranov theorem. In *Actas del X Encuentro de Álgebra Computacional y Aplicaciones, EACA 2006*, pages 178–181, 2006.

[Tha64] A. I. Thaler. On the Newton polytope. *Proceedings of the American Mathematical Society*, 15:944–950, 1964.

[The06] T. Theobald. On the frontiers of polynomial computations in tropical geometry. *Journal of Symbolic Computation*, 41(12):1360–1375, 2006.

[vdD00] L. van den Dries. Classical model theory of fields. In *Model theory, algebra, and geometry*, volume 39 of *Math. Sci. Res. Inst. Publ.*, pages 37–52. Cambridge Univ. Press, Cambridge, 2000.

[vdW03a] B. van der Waerden. *Algebra. Volume I. Based in part on lectures by E. Artin and E. Noether. Transl. from the German 7th ed. by Fred Blum and John R. Schulenberger. 1st paperback ed.* New York, NY: Springer. xiv, 265 p., 2003.

[vdW03b] B. van der Waerden. *Algebra. Volume II. Based in part on lectures by E. Artin and E. Noether. Transl. from the German 5th ed. by John R. Schulenberger. 1st paperback ed.* New York, NY: Springer. xii, 284 p., 2003.

[vH97] M. van Hoeij. Rational parametrizations of algebraic curves using a canonical divisor. *Journal of Symbolic Computation*, 23(2-3):209–227, 1997. Parametric algebraic curves and applications (Albuquerque, NM, 1995).

[Vig04] M. D. Vigeland. The group law on a tropical elliptic curve. *Preprint*, 2004.

[Vig06] M. D. Vigeland. Tropical fano theorem. *Personal communication*, 2006.

[Vil07] C. Villarino. *Algoritmos de optimalidad algebraica y de cuasi-polinomialidad para curvas racionales*. PhD thesis, Universidad de Alcalá, 2007.

[Wal50] R. J. Walker. *Algebraic Curves*. Princeton Mathematical Series, vol. 13. Princeton University Press, Princeton, N. J., 1950.

[Wei62] A. Weil. *Foundations of algebraic geometry*. American Mathematical Society, Providence, R.I., 1962.

[Wei79] A. Weil. *Scientific works. Collected papers. Vol. II (1951–1964)*. Springer-Verlag, New York, 1979.

[Wei95] A. Weil. Adèles et groupes algébriques. In *Séminaire Bourbaki, Vol. 5*, pages Exp. No. 186, 249–257. Soc. Math. France, Paris, 1995.

[ZS75a] O. Zariski and P. Samuel. *Commutative algebra. Vol. I*. Springer-Verlag, New York, 1975. With the cooperation of I. S. Cohen, Corrected reprinting of the 1958 edition, Graduate Texts in Mathematics, No. 28.

[ZS75b] O. Zariski and P. Samuel. *Commutative algebra. Vol. II*. Springer-Verlag, New York, 1975. Reprint of the 1960 edition, Graduate Texts in Mathematics, Vol. 29.

Index