Automated proof of theorems in geometries over division rings

Conijn, B.J.

Award date:
2011

Eindhoven University of Technology
Department of Mathematics and Computer Science

Automated proof of theorems in geometries over division rings

B.J. Conijn

July 15, 2011

Summary

This document describes the problems that arise when the theory of Gröbner bases is applied to theorems in non-commutative geometries.

Analytical geometry gives a means to rewrite geometric theorems into a set of hypothesis polynomial equations and a thesis polynomial equation. If the geometry is commutative, then the Gröbner basis of the hypothesis ideal can be computed. This basis can then be used to prove that the thesis equation can be derived from the hypothesis polynomials. How such a proof is constructed and why it is correct is explained in chapter 1.

The theory of Gröbner bases is limited to commutative polynomials. It is relatively easy to generalize the theory to work for non-commutative polynomials as well. However, this generalization has one severe problem: there exists no algorithm for computing a non-commutative Gröbner basis. The non-commutative version of Buchberger's algorithm however, can still be used to compute the non-commutative Gröbner basis for *some* ideals. This and other differences between the commutative and non-commutative Gröbner bases are discussed in chapter 2.

In chapter 3, we construct a geometry over a division ring and argue why non-commutative Gröbner bases can not be used for proving theorems in geometries over division rings.

This document was written as part of the author's bachelor project. This project was supervised by Hans Sterk and is part of the bachelor's program *Applied Mathematics* at the Eindhoven University of Technology.

Contents

Chapter 1

Geometric proofs using Gröbner bases

By choosing a coordinate system strategically, Thales' theorem can be proved by rewriting only a single polynomial equation. This is shown in the first section. In general, a geometric theorem will have more than one hypothesis equation. The theory of Gröbner bases can be used to program a computer to rewrite these hypothesis equations into the thesis polynomial. This theory is shortly explained in the sections 3, 4, 5 and 6. For a thorough explanation we refer to [1] and [6]. Using this theory it is possible to programmatically generate proofs for certain classes of geometric theorems. The structure of such a proof is given in the second section and an example in the last.

1.1 Introduction

In standard Euclidean geometry, we usually prove theorems using classical techniques, like incidence, congruence and applying other theorems. Such proofs tend to require some creativity to write. An alternative is parameterizing the Euclidean space, which allows us to apply algebraic techniques for proving theorems. Here is a simple example:

Theorem 1.1.1 (Thales)**.** *Given a circle c, a line l through the center of the circle and a point P on the circle, but not on the line. Let M_1 and M_2 being the two intersections of c and l (see figure 1.1). Then the lines M_1P and PM_2 are perpendicular.*

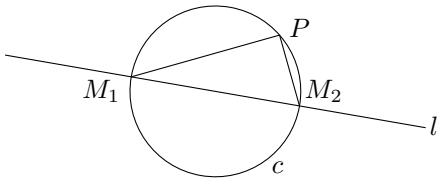

Figure 1.1: Geometric configuration of Thales' theorem.

Proof. We choose a coordinate system. Let the center of the circle be the origin of this system. Choose the x-axis, such that $M_1 = (-1, 0)$ and $M_2 = (1, 0)$. Choose the y-axis, such that it's perpendicular to the x-axis and intersects with the circle at $(0, 1)$ and $(0, -1)$. Point P has coordinate (x, y).

Having chosen the coordinate system, we can now write down the algebraic equations for the hypothesis and the thesis.

Hypothesis Because point P is on the unit circle, we have:

$$x^2 + y^2 = 1.$$

Thesis Two lines are perpendicular if their inner product is zero, hence we have to prove that

$$(x, y - -1) \cdot (x, y - 1) = 0.$$

This follows from the hypothesis by simple rewriting:

$$(x, y - -1) \cdot (x, y - 1) = x^2 + y^2 - 1 = 0.$$

□

1.2 Structure of a proof

In our proof of Thales' theorem we use a standard recipe for obtaining the proof. The first step is rewriting the theorem as a set of polynomial equations. The equations that describe what is given are called the hypothesis. That what must be proven is the thesis. If we can derive the thesis equation from the hypothesis equations, then the theorem is proved.

Thales' theorem can be proved by rewriting only a single polynomial equation. In general, a geometric theorem will have more than one hypothesis equation and rewriting these equations into the thesis polynomial by hand can be both difficult and time consuming. One technique that can be used is as follows:

- The equations are rewritten such that the right-hand side of all equations is zero. The left hand side of the hypothesis equations are called the hypothesis polynomials, the left hand side of the thesis equation is called the thesis polynomial.
- Then repeatedly, reduce the thesis polynomial modulo one of the hypothesis polynomials, until the thesis polynomial can no longer be reduced.
- If the thesis polynomial end up being zero, the original thesis polynomial is a combination of the hypothesis polynomials. The hypothesis polynomials all equal zero. Hence the thesis polynomial also equals zero, which proves the theorem.

There are two important issues with this method. First, the definition of the modulo reduction is unclear. We will solve this by using a monomial order, which we define in section 1.4. Second, the thesis polynomial obtained by repeating the second step depends on the order in which the hypothesis polynomials are chosen. Hence if the remaining thesis polynomial is not zero, it might have been possible to reduce it to zero using the hypothesis polynomials in a different order. To solve this problem, we need to rewrite the set of hypothesis polynomials into a Gröbner basis, before doing the reduction.

1.3 Ideal

Before we can properly define 'Gröbner basis', we need to define 'ideal'. In this chapter we only use ideals of polynomials. Therefore, we only define it here for polynomials. We refer to definition 2.5.1 for the general definition that does not assume commutativity.

Definition 1.3.1 (Polynomial ideal)**.** Let $H = \{h_1, \ldots, h_n\}$ be a finite set of polynomials. Then the ideal generated by H is given by:

$$\langle H \rangle = \langle h_1, \ldots, h_n \rangle := \left\{ \sum_{i=1}^{n} a_i h_i \;\middle|\; a_1, \ldots, a_n \text{ are } n \text{ polynomials} \right\}.$$

Hence an ideal is a set of polynomials. The set H is called a basis of $\langle H \rangle$. There are a few operations that can be applied to a basis, such that the ideal it generates does not change:

- Add an element from the ideal to the basis: let $v \in \langle h_1, \ldots, h_n \rangle$, then $\langle h_1, \ldots, h_n \rangle = \langle h_1, \ldots, h_n, v \rangle$.
- Remove a zero element from the basis: $\langle h_1, \ldots, h_n, 0 \rangle = \langle h_1, \ldots, h_n \rangle$.
- Add a multiple of one of the polynomials to another: let $i, j \in \{1, \ldots, n\}$ and polynomial a be given, such that $i \neq j$, then $\langle h_1, \ldots, h_j \ldots, h_n \rangle = \langle h_1, \ldots, h_j + ah_i, \ldots, h_n \rangle$.
- Multiply a polynomial by a constant.

We can now rewrite geometric theorems into ideal membership problems. Let T be a geometric theorem. Let H be the set of hypothesis polynomials of T and let t be its thesis polynomial. The theorem T is true if $t \in \langle H \rangle$.[1]

1.4 Monomial order

We still need to clear up the definition of modulo reduction. This definition requires a monomial order to be chosen.

A monomial is a single term of a polynomial, without the constant factor. For example, x^2yz^5, y^3 and 1 are monomials and $x + y$, 0, $-z$ and $12xy^2$ are not. Multiplying two monomials yields another monomial. Having a monomial order allows us to sort the monomials.

Definition 1.4.1 (Monomial order)**.** Let $<$ be a relation on monomials. Then $<$ is a monomial order if and only if :

- the relation is a total ordering, for each distinct pair of monomials a and b either $a < b$ or $b < a$;
- the relation is invariant under multiplication, let a, b and c be monomials, then $a < b \implies a \cdot c < b \cdot c$;
- the relation is a well ordering, for each set of monomials S there exists an $x \in S$ such that $\{\ a \in S \mid a < x\ \} = \emptyset$.

Most books about Gröbner bases then define the following three functions for polynomials:

- $lm(p)$: the leading monomial. That is, the largest monomial in the polynomial p with respect to the monomial ordering.
- $lc(p)$: the coefficient of the leading monomial.
- $lt(p)$: the term of p. That is the leading monomial with its coefficient. $lt(p) = lc(p) \cdot lm(p)$.

These functions can then be used to define divisibility and the module reduction operation.

Definition 1.4.2 (Divisibility)**.** A polynomial p is said to be divisible by q if there exists a polynomial r such that $p = r \cdot q$.

Definition 1.4.3 (Modulo reduction)**.** Let p and q be polynomials. Now we have that $p \equiv p + r \cdot q \pmod{q}$ for any polynomial r. Let $s = p + r \cdot q$, for any polynomial r such that $lm(q)$ does not divide any of the terms in s, then s is the reduction of p modulo q, which we will denote as: $p \bmod q$.

[1] There exists a stronger theorem, based on Hilbert's nullstellensatz, that says that T is true if and only if $t \in \sqrt{\langle H \rangle}$. Here $\sqrt{\langle H \rangle}$ is the radical of $\langle H \rangle$, which is defined as $\sqrt{\langle H \rangle} = \{\ a \mid \exists n : a^n \in \langle H \rangle\ \}$. A concise description of this theorem and a proof can be found in [6, section 4.2].

1.5 Gröbner basis

Definition 1.5.1 (Gröbner basis)**.** Let $H = \{h_1, \ldots, h_n\}$ be a basis. Then H is a Gröbner basis if and only if for each $p \in \langle H \rangle$ there exist a $q \in H$, such that $lm(q)$ divides $lm(p)$.

This means that whenever we have a Gröbner basis H and a polynomial $p \in \langle H \rangle$ with $p \neq 0$, we can find a $q \in H$, such that $lm(p \mod q) < lm(p)$. Note that $p \mod q \in \langle H \rangle$, hence we can use $p \mod q$ as the new value for p and repeat this procedure until $p = 0$.

If we apply this procedure to any polynomial p, once the procedure ends, $p \in \langle H \rangle$ if and only if the last value of p was 0. So this procedure can be used to check whether a polynomial is a member of an ideal.

1.6 Buchberger algorithm

A basis $H = \{h_1, \ldots, h_n\}$ is usually not a Gröbner basis. The *Buchberger algorithm* can be used to convert a basis into a Gröbner basis. Let $lcm(a, b)$ be the least-common-multiple of the monomials a and b. The basic idea behind the Buchberger algorithm is as follows:

- Sort $h_1, \ldots, h_n$, such that $lm(h_1) < \ldots < lm(h_n)$.
- For each i, replace h_i with $\frac{1}{lc(h_i)} h_i$.
- For each pair h_i, h_j, add the following polynomial to the basis:

$$\frac{lcm(lm(h_i), lm(h_j))}{lm(h_i)} h_i - \frac{lcm(lm(h_i), lm(h_j))}{lm(h_j)} h_j.$$

- For each $i, j \in \{1, \ldots, n\}$ (in arbitrary order), replace h_i with $h_i \mod h_j$.
- Remove polynomials that are 0.

These steps are then repeated until the basis no longer changes. Then it is a Gröbner basis.

The theory of Gröbner bases and the Buchberger algorithm gives a powerful tool, with which we can easily test whether a given polynomial is in the ideal generated by a set of polynomials. One can program a computer to do this testing. Combined with algebraic geometry, this can be used to programmatically generate proofs for some geometric theorems. One program that implements Gröbner bases and the Buchberger algorithm is *Singular*[2].

1.7 Example

We have proven Thales' theorem in the first section of this chapter. This was easy because we chose a specific coordinate system. If a coordinate system is given, we can still write down the thesis and hypothesis polynomials. However, now we would need to use Gröbner bases for the proof. To show how Gröbner bases can help with proving a geometric theorem, we will prove Thales' theorem again, but now with a given coordinate system.

Theorem 1.7.1 (Thales)**.** *Let (x_c, y_c) be the center of a circle with radius r. Let (x_1, y_1), (x_2, y_2) and (x_3, y_3) be points on the circle. If the points (x_1, y_1), (x_c, y_c) and (x_2, y_2) are distinct and collinear, then the vectors $(x_1 - x_3, y_1 - y_3)$ and $(x_2 - x_3, y_2 - y_3)$ are perpendicular.*

Proof. Again we write down the algebraic equations for the hypothesis and thesis.

Hypothesis

$$\begin{aligned}(x_1 - x_c)^2 + (y_1 - y_c)^2 &= r^2 \\ (x_2 - x_c)^2 + (y_2 - y_c)^2 &= r^2 \\ (x_3 - x_c)^2 + (y_3 - y_c)^2 &= r^2 \\ (x_1 + x_2) &= 2x_c \\ (y_1 + y_2) &= 2y_c\end{aligned}$$

Thesis

$$(x_1 - x_3)(x_2 - x_3) + (y_1 - y_3)(y_2 - y_3) = 0$$

We run the Singular script in section A.1. This gives the following Gröbner basis: $\langle 2y_c - y_1 - y_2,\ 2x_c - x_1 - x_2,\ x_1x_2 - x_1x_3 - x_2x_3 + x_3^2 + y_1y_2 - y_1y_3 - y_2y_3 + y_3^2,\ x_1^2 + x_2^2 - 2x_1x_3 - 2x_2x_3 + 2x_3^2 + y_1^2 + y_2^2 - 2y_1y_3 - 2y_2y_3 + 2y_3^2 - 4r^2,\ x_2^3 - 3x_2^2x_3 + 3x_2x_3^2 - x_3^3 + x_2y_1^2 - x_3y_1^2 - x_1y_1y_2 + x_3y_1y_2 + x_2y_2^2 - x_3y_2^2 + x_1y_1y_3 - 2x_2y_1y_3 + x_3y_1y_3 + x_1y_2y_3 - 2x_2y_2y_3 + x_3y_2y_3 - x_1y_3^2 + 2x_2y_3^2 - x_3y_3^2 - 4x_2r^2 + 4x_3r^2\rangle$
Calculating the thesis polynomial modulo this Gröbner basis gives:

$$(x_1 - x_3)(x_2 - x_3) + (y_1 - y_3)(y_2 - y_3) = 0$$

Which proves the theorem. □

Chapter 2

Non-commutative Gröbner bases

The theory of Gröbner bases is limited to commutative fields. However, an extension to the theory is available, known as non-commutative Gröbner bases, which makes it possible to use it with division rings. In this chapter we will build up the algebraic structures used by non-commutative Gröbner bases and investigate whether and how these non-commutative Gröbner bases can be computed. For an introduction to non-commutative Gröbner bases, we refer to [3].

The first two sections are a refresher on various basic algebraic structures. The third section addresses various problems encountered when defining skew polynomials. The solutions for these problems impose a few restrictions on skew polynomials. In the forth section a method is shown that allows us to circumvent these restrictions. Some examples of division rings that are modified to meet the requirements are given in the sixth section.

In the fifth and seventh section we modify the definitions of ideals and monomial order such that they no longer depend on commutativity. The required changes for the Buchberger algorithm are discussed in the eighth section. In the last section it is noted that in general computing a non-commutative Gröbner basis is not possible.

2.1 Commutativity

To understand what non-commutative Gröbner bases are, we first need to know what commutativity is.

Definition 2.1.1 (Commutativity)**.** Let $\diamond : R \times R \to R$ be a binary operator, then $\diamond$ is said to be commutative if $\forall a, b \in R : a \diamond b = b \diamond a$.

The *commutativity* property is usually part of an algebraic structure. The *monoid* and *group* are two such structures that can be commutative. We will need these structures in the next section, so here are their definitions.

Definition 2.1.2 (Monoid)**.** Let R be a set and $\diamond : R \times R \mapsto R$ a binary operator, then $(R, \diamond)$ is a monoid if and only if :

- the operator $\diamond$ is associative: $\forall a, b, c \in R : a \diamond (b \diamond c) = (a \diamond b) \diamond c$;
- there is an identity element: $\exists e \in R : \forall a \in R : e \diamond a = a = a \diamond e$.

We can prove that the identity element of a monoid is unique: let e and e' be identity elements, then $e = e \diamond e' = e'$. If the operator of a monoid is commutative, then it is called a *commutative monoid*. The monomials from chapter 1 form such a commutative monoid. If we require that every element in a monoid has an inverse, we get what is called a group.

Definition 2.1.3 (Group)**.** Let $(R, \diamond)$ be a monoid, then $(R, \diamond)$ is a group if and only if each element has an inverse: $\forall a \in R : \exists b \in R : a \diamond b = e = b \diamond a$.

Much like the uniqueness of the identity element of the monoid, every element has an unique inverse: let $a \in R$ and let b, b' be inverses of a, then $b = b \diamond e = b \diamond (a \diamond b') = (b \diamond a) \diamond b' = e \diamond b' = b'$. If the operator of a group is commutative, then it is called a *commutative group* or an *abelian group*. If a group is not commutative, it's said to be non-commutative.

2.2 Division ring

Commutative Gröbner bases consist of polynomials over a *field*. For non-commutative Gröbner bases we want to use a *division ring* instead of a field.[1] A field is a division ring with a commutative multiplicative operator. This section lists the definitions of the ring, division ring and field. Some properties of these structures are also given. We start with the ring, which is a combination of a monoid and a group and therefore has two binary operators.

Definition 2.2.1 (Ring)**.** Let R be a set and let $+, \cdot : R \times R \mapsto R$ be binary operators, then $(R, +, \cdot)$ is a ring if and only if :

- $(R, +)$ is a commutative group;
- $(R, \cdot)$ is a monoid;
- the distributive laws hold: $\forall a, b, c \in R : a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$.

The polynomials from chapter 1 form a ring. As we will be doing many calculations with rings, here follow some notational definitions:

- the identity elements of the $+$ and $\cdot$ operators will be written as 0 and 1 respectively;
- we will write -1 for the additive inverse of 1, hence $1 + -1 = 0$;
- the $\cdot$ is often omitted and has higher precedence than $+$;
- formulas like $a + -1 \cdot b$ will be written as $a - b$;
- $aa \ldots a$ will be written as a^n, such that $a^n = a \cdot a^{n-1}$ and $a^0 = 1$.

This allows us to write more compact formulas. For example, we can rewrite $(a \cdot b) + (a \cdot a \cdot c)$ as $ab + a^2c$. Note that $0 = 0 \cdot a = (1 + -1) \cdot a = 1 \cdot a + -1 \cdot a = a + -a$, hence $-a$ is the additive inverse of a. Also note that $-1 \cdot a = a \cdot -1$, even though $\cdot$ is not necessarily commutative.

One property of a ring is that anything multiplied by 0 yields 0 as a result. This is proven by $0 = a \cdot 0 - (a \cdot 0) = a \cdot (0 + 0) - (a \cdot 0) = a \cdot 0 + a \cdot 0 - (a \cdot 0) = a \cdot 0$ and similarly for $0 = 0 \cdot a$. It is possible that $0 = 1$, but then $\forall a \in R : a = 1 \cdot a = 0 \cdot a = 0$ and thus R consists of only a single element. As this case is uninteresting, we assume $0 \neq 1$. This assumption implies that there can not exist a $b \in R$, such that $0 \cdot b = 1$. If we assume that for any $a \in R, a \neq 0$, there exists a $b \in R$ such that $a \cdot b = 1$, we get what is called a *division ring*.

Definition 2.2.2 (Division Ring)**.** Let $(R, +, \cdot)$ be a ring, then $(R, +, \cdot)$ is a division ring if and only if $(R \setminus \{0\}, \cdot)$ is a group.

A different name for division ring is 'skew field'. If a is an element of a division ring and n a negative integer, a^n denotes the multiplicative inverse of a^{-n}. Obviously 0^n is undefined for negative n. A special case of division ring is when the operator $\cdot$ is commutative. This is called a field.

Definition 2.2.3 (Field)**.** Let $(R, +, \cdot)$ be a division ring, then $(R, +, \cdot)$ is a field if and only if $\cdot$ is commutative.

[1] When commutativity is dropped, we have to redefine the notion of polynomial. This gives some complications concerning the use if a division ring. These complications are discussed in section 2.3 and 2.4.

2.3 Skew polynomials

For non-commutative Gröbner bases, we need something similar to polynomials, but without the commutativity. Something like $3aca + 2b^2a + 1 + ab$. These will be called *skew polynomials*. However, we first need to define them. Finding a definition for skew polynomials, such that we can work with them similarly as with ordinary commutative polynomials, happens to be a bit difficult. Here follows a first, but unsuccessful attempt at defining such skew polynomials.

Definition 2.3.1 (Ambiguous polynomial ring)**.** Let $k = (R, +, \cdot)$ be a ring and $X = \{x_1, \ldots, x_n\}$ a set of indeterminate variables. Let A be the closure of $R \cup X$ under $+$ and $\cdot$. Then $(A, +, \cdot)$, denoted as $k[x_1, \ldots, x_n]$, is a polynomial ring.

This definition is ambiguous, as we do not state the properties of the indeterminate variables with respect to $+$ and $\cdot$. We could solve this by saying that these variables follow the properties of a ring, but then we would still be using the closure of a set, which makes it a bad definition. However, even if we could remove the use of 'closure', there is still one problem left: we can't define the concept of monomial in a way that is similar to the commutative monomial definition. In the commutative case, polynomials are sums of monomials multiplied by coefficients. The coefficients could be separated from the monomials, because the underlying ring was commutative. In the non-commutative case, the coefficients and monomial can be mixed, for example: $x_1ax_2bx_3$, with $a, b \in R$. Due to the lack of commutativity, we can't separate the coefficient from the monomial. Therefore, to solve this problem, we require R to be a field.[2] We will first define the monomials.

Definition 2.3.2 (Skew monomial monoid)**.** Let $X = \{x_1, \ldots, x_n\}$ a set of indeterminate variables. Let A be the set of finite lists of elements from X, including the empty list. Let the operator $\cdot : A \times A \to A$ be defined, such that $a \cdot b$ is the concatenation of a and b, for all $a, b \in A$. Then $(A, \cdot)$ is the skew monomial monoid. The elements of A are called skew monomials. The set A will be denoted as $\langle x_1, \ldots, x_n \rangle$.

In computer science X is usually called an *alphabet*, the elements of A are called *words* and '$\cdot$' is known as the concatenation operator.

We can now define the skew polynomial ring. Here follows a successful attempt at defining the skew polynomials. The definition is concise and probably useful for implementing the non-commutative Buchberger algorithm discussed in section 2.8. However, the definition is a bit artificial and therefore less useful for the understanding of skew polynomials.

Definition 2.3.3 (Skew polynomial ring)**.** Let $k = (R, +, \cdot)$ be a field. Let $A = \langle x_1, \ldots, x_n \rangle$ and $(A, \cdot)$ be a skew monomial monoid. Let

$$B = \{\ f \mid f : A \to R \ \wedge\ \#\{\ x \mid x \in A \ \wedge\ f(x) \neq 0\ \} \in \mathbb{Z}\ \}.$$

Then $k\langle x_1, \ldots, x_n \rangle := (B, +, \cdot)$ is a skew polynomial field, with for all $a, b \in B$ and $x \in A$:

$$(a + b)(x) = a(x) + b(x);$$

$$(a \cdot b)(x) = \sum_{\substack{y,z \in A \\ y \cdot z = x}} a(y) \cdot b(z).$$

Elements from this ring are denoted as $f(x_1)x_1 + \ldots + f(x_n)x_n$ for $f \in B$ and $\{x_1, \ldots, x_n\} = \{\ x \mid x \in A \ \wedge\ f(x) \neq 0\ \}$. The notational rules for ring formulas are applied here as well. So, for example, we can write: $3aca + 2b^2a + 1 + ab \in \mathbb{R}\langle a, b, c \rangle$.

The skew polynomial ring is also known as a *free algebra* over k or a *free ideal ring*.

[2] Even if the indeterminate variables are non-commutative they still have commutative behavior when multiplied by an element from the field. This allows the coefficient to be separated from the monomial. This is proven in the next section.

2.4 Field extraction

The requirement that R must be a field seems a too limiting requirement, especially when we want to prove theorems in geometries over division rings. To work around this limitation we take a division sub-ring of our division ring, that actually is a field. We use this field as the basis for our skew-polynomial ring and add the elements missing from our sub-ring as indeterminate variables (see section 2.6 for examples). Theorem 2.4.2 states that it is always possible to extract a field from a division ring. This theorem also tells us that we can indeed separate the coefficient and monomial of a polynomial's terms and calculate with them.

Definition 2.4.1 (Division sub-ring)**.** Let $(R, +, \cdot)$ be a division ring, then $(S, +, \cdot)$ is a division sub-ring of $(R, +, \cdot)$ if and only if $S \subset R$ and $(S, +, \cdot)$ is a division ring.

Theorem 2.4.2. *Every division ring $(R, +, \cdot)$ has a division sub-ring $(S, +, \cdot)$ that is a field. Additionally $\forall s \in S, r \in R : s \cdot r = r \cdot s$.*

Proof. We will prove this theorem by constructing a set S, such that $(S, +, \cdot)$ is a field.

Let $S_1 = \{0, 1\}$ and for all $i \in \mathbb{N}$ let

$$S_{i+1} = S_i \cup \{\ -a \mid a \in S_i\ \} \cup \{\ a^{-1} \mid a \in S_i^*\ \} \cup \{\ a + b \mid a, b \in S_i\ \} \cup \{\ a \cdot b \mid a, b \in S_i\ \}$$

Let $S = \bigcup_{i=1}^{\infty} S_i$, which is the closure of S_1 under the operations of the division ring k. Now $(S, +, \cdot)$ is a division sub-ring.

We will prove that $s \in S_{i+1}, r \in R$ implies that $s \cdot r = r \cdot s$ by induction to i. For $i = 0$ we have $s = 0$ or $s = 1$. So for any $r \in R$ we have $0 \cdot r = 0 = r \cdot 0$ and $1 \cdot r = r = r \cdot 1$. Hence for $i = 0$ the theorem holds. For $i \geq 1$ let $s \in S_{i+1}$ and $r \in R$. Now we have 5 different cases.

- $\exists a \in S_i : s = a$: It follows from the induction hypothesis that $s \cdot r = r \cdot s$.
- $\exists a \in S_i : s = -a$: From the induction hypothesis we have that $-s \cdot r = r \cdot -s$. It follows that $s \cdot r = r \cdot s$.
- $\exists a \in S_i : s = a^{-1}$: If $r = 0$ then $s \cdot r = 0 = r \cdot s$, otherwise it follows from the induction hypothesis that $r^{-1} \cdot s^{-1} = s^{-1} \cdot r^{-1}$, which implies that $s \cdot r = r \cdot s$.
- $\exists a, b \in S_i : s = a + b$: From the induction hypothesis we have $a \cdot r = r \cdot a$ and $b \cdot r = r \cdot b$. Adding them yields $a \cdot r + b \cdot r = r \cdot a + r \cdot b$. Applying the distributive laws gives $(a + b) \cdot r = r \cdot (a + b)$, hence $s \cdot r = r \cdot s$.
- $\exists a, b \in S_i : s = a \cdot b$: From the induction hypothesis we have $a \cdot r = r \cdot a$ and $b \cdot r = r \cdot b$. Using these properties we can rewrite $s \cdot r = (a \cdot b) \cdot r = a \cdot (b \cdot r) = a \cdot (r \cdot b) = (a \cdot r) \cdot b = (r \cdot a) \cdot b = r \cdot (a \cdot b) = r \cdot s$.

This completes the induction, which proves that $\forall s \in S, r \in R : s \cdot r = r \cdot s$. Since S is constructed such that $+$ and $\cdot$ are closed under S and $S \subset R$, we have that $(S, +, \cdot)$ is a field. □

This result allows us to think of division rings as generated by a field with some non-commutative elements added. The extracted field will be used as the set of coefficients of the polynomial ring. The non-commutative elements are added as indeterminate variables. Properties of the non-commutative elements are added to the ideal. This gives a quotient ring (see section 2.6) that behaves the same as the original division ring.

2.5 Ideal

Like the polynomials, the ideals must also be adapted to work without commutativity. Here we have to make a choice as well. In an ideal we can multiply an element with a scalar and obtain a new element in the ideal. In the non-commutative case it matters whether the scalar is multiplied at the left or the right side. We choose to multiply on both sides. This means that we will get a so called 'two-sided ideal'. Here is the definition:

Definition 2.5.1 (Ideal)**.** Let $(R, +, \cdot)$ be a ring and $I \subset R$, then I is an ideal if and only if $(I, +)$ is a group and for all $a \in R$ and $x \in I$ we have $a \cdot x \in I$ and $x \cdot a \in I$.

Similarly to what we did in chapter 1, we can convert any $H \subset R$ into an ideal by taking the set of all linear combinations (of a finite number) of elements from H. We define:

$$\langle H \rangle := \left\{ \sum_{i=1}^{n} a_i h_i + h_i b_i \;\middle|\; a_1, \ldots, a_n, b_1, \ldots, b_n \in R, h_1, \ldots, h_n \in H \right\}.$$

2.6 Quotient ring

The algebraic structure created by $(R, +, \cdot)$ modulo the ideal I is called a *quotient ring*.

Definition 2.6.1 (Quotient Ring)**.** Let $(R, +, \cdot)$ be a ring and let $I \subset R$ be an ideal. Let $\equiv_I \in R \times R$ be an equivalence relation with $a \equiv_I b \iff a - b \in I$. Now we define R/I as the equivalence classes of $\equiv_I$: $R/I := \{ \{ a + x \mid x \in I \} \mid a \in R \}$. We define the binary operators $+$ and $\cdot$ on R/I as $a + b = \{ x + y \mid x \in a, y \in b \}$ and $a \cdot b = \{ x \cdot y + z \mid x \in a, y \in b, z \in I \}$ for $a, b \in R/I$. Note that both operators are closed, which means that $a + b \in R/I$ and $a \cdot b \in R/I$. The ring $(R/I, +, \cdot)$ is called the quotient ring of $(R, +, \cdot)$ modulo I.

Examples of quotient rings are the complex numbers and the quaternions.

Example 2.6.2 (Complex numbers)**.** The complex numbers $\mathbb{C}$ are generated by $\mathbb{R}$ and i, with the property $i^2 = -1$. This is written down as: $\mathbb{C} = \mathbb{R}\langle i \rangle / \langle i^2+1 \rangle$. Commutativity of the element i follows from it being the only indeterminate variable.

Example 2.6.3 (Quaternions)**.** The quaternions $\mathbb{H}$ are generated by $\mathbb{R}$ and i, j and k, with the property $i^2 = j^2 = k^2 = ijk = -1$. This is written down as: $\mathbb{H} = \mathbb{R}\langle i, j, k \rangle / \langle i^2+1, j^2+1, k^2+1, ijk+1 \rangle$.

2.7 Skew monomial order

Computing a commutative Gröbner basis requires a monomial order to be chosen. We will adapt the definition of a monomial order to no longer require commutativity.

Definition 2.7.1 (Skew monomial order)**.** Let $<$ be a relation on skew monomials. Then $<$ is a skew monomial order if and only if :

- the relation is a total ordering, for each distinct pair of monomials a and b either $a < b$ or $b < a$;
- the relation is invariant under multiplication, let a, b and c be monomials, then $a < b \implies a \cdot c < b \cdot c \wedge c \cdot a < c \cdot b$;
- the relation is a well ordering, for each set of monomials S there exists an $x \in S$ such that $\{ a \in S \mid a < x \} = \emptyset$.

One example of a skew monomial order is sorting by length first and then lexicographically. The functions lm, lt and lc can trivially be modified to work for skew polynomials. Reduction of a mod b is done by repeatedly finding terms in a that can be written as $v \cdot lm(b) \cdot w$ and subtracting $v \cdot b \cdot w$ from a, until no such term is left. Divisibility can be defined as b divides a if and only if $(a \mod b) = 0$.

2.8 Non-commutative Buchberger algorithm

The non-commutative Buchberger algorithm is a basically the same as the original algorithm (see section 1.6). Commutative algebraic structures are replaced by the non-commutative ones. The *least common multiple* requires some work though.

The algorithm has a step where it uses the *least common multiple*. (In this step new polynomials are added to the basis that are in the basis' ideal, but might not be reducible to 0 with the current basis.) The *least common multiple* is not clearly defined for skew monomials. For example: axa and aya have the multiples $axaya$ and $ayaxa$. We can disambiguate this by using a skew-monomial order. However, using only the least common multiple for generating the Gröbner basis is insufficient.[3] For example, consider the ideal $\langle abb - a, bba \rangle$. If we use only the *least common multiple*, we would get $abb - a, bba, aa$ as basis. However, $aba = ab(bba) - (abb - a)ba$ is an element of the ideal, but its leading monomial is not divided by any of the leading monomials of the basis. Hence the generated basis is not a Gröbner basis. Therefore the step that uses the least common multiple must be modified such that it adds the following set of polynomials for each ordered pair of polynomials (x, y) (including the pairs $x = y$) already in the basis:

$$S(x, y) := \{\ vx - yw \mid v \cdot lm(x) = lm(y) \cdot w \wedge |w| < |lm(x)| \wedge |v| < |lm(y)|\ \},$$

with v, w being monomials and $|a|$ denoting the degree of monomial a.

The non-commutative Buchberger algorithm has been implemented in GBNP[4], which is a package for the computer algebra system GAP 4. We will use this software and package for computing non-commutative Gröbner bases.

2.9 Uncomputability

Non-commutative Gröbner bases can be used to solve an undecidable problem known as the *word problem*.[5] That means that an algorithm that computes non-commutative Gröbner bases can not exist. Hence an algorithm that claims to compute non-commutative Gröbner bases is either incorrect or does not always terminate. The latter is the case with the non-commutative Buchberger algorithm. Here follows an example in which a badly chosen skew monomial order results in computing an infinite Gröbner basis. The algorithm was terminated after a few iterations.

Example 2.9.1 (Infinite Gröbner basis)**.** Consider the ideal $< x^2 - xy >$. With the monomial ordering $y \succ x$, this gives the Gröbner basis $< xy - x^2 >$. However, by using the ordering $x \succ y$, we end up with the infinite Gröbner basis $< x^2 - xy, xyx - xy^2, xy^2x - xy^3, xy^3x - xy^4, \ldots >$. See appendix A.2 for the GAP code.

Chapter 3

Geometry over a division ring

Without a specification of non-commutative geometry, we can't use non-commutative Gröbner bases to prove non-commutative geometric theorems. In the last section of this chapter we will argue why, regardless of the geometry specification, proving will not work. However, we still give the definition of a non-commutative geometry.

3.1 Definitions

There does not seem to be a generally accepted definition for non-commutative geometries. Hence, we define one that is similar to Euclidean geometry. This geometry will use the division ring $k = (R, +, \cdot)$ as its basis and will be n dimensional. We will not consider projective geometry, because we will not use our specification for proving theorems anyway.

An Euclidean geometry is also a vector space. The definition of a vector space does not assume commutativity of the multiplication operator, hence we can simply copy the definition.

Definition 3.1.1 (Vector Space)**.** $k^n = (R^n, +, \cdot)$ is the n-dimensional vector space of k and has the following operators:

- operator $+ : R^n \times R^n \mapsto R^n$, given by $(a_1, \ldots, a_n) + (b_1, \ldots, b_n) := (a_1 + b_1, \ldots, a_n + b_n)$;
- operator $\cdot : R \times R^n \mapsto R^n$, given by $a \cdot (b_1, \ldots, b_n) := (a \cdot b_1, \ldots, a \cdot b_n)$.

Just like in Euclidean geometry, a point is just an element from the vector space.

Definition 3.1.2 (Point)**.** An element $p \in k^n$ is called a point.

We can think of points as if they are vectors. If the vector does not point to the origin, then it has a direction. Scaling this vector does not affect its direction. Hence given the vectors a and b, having the same direction, there is a unique $v \in R, v \neq 0$ such that $a = v \cdot b$. Note that v can be equal to -1, hence a and $-a$ both have the same direction. If we now take the set of points that are the origin or have the same direction as a, then we have something that resembles a line through the origin. This line can be translated to get lines that go through other points than the origin. We will use this as the definition of a line.

Definition 3.1.3 (Line)**.** For any $a, t \in k^n$ and $a \neq 0$, the set $L(a, t) \subset k^n$, given by $L(a, t) = \{\ v \cdot a + t \mid v \in k\ \}$, is called a line.

Euclidean geometry has a notion of parallelism. We will also define a notion of parallelism for our non-commutative geometry.

Definition 3.1.4 (Parallel)**.** Let $L(a, t)$ and $L(b, s)$ be two lines. If there exists a $p \in k^n$, such that $L(a, t) = \{\ p + q \mid q \in L(b, s)\ \}$, then the two lines are parallel.

We also define the concept of intersection.

Definition 3.1.5 (Intersection)**.** Two lines $L(a,t)$ and $L(b,s)$ intersect if and only if $L(a,t) \cap L(b,s) \neq \emptyset$.

With these definitions, a line both intersects with itself and is parallel to itself.

3.2 Properties

There are a few basic properties about affine geometries we could verify. These properties are:

- for every distinct pair of points there exists a unique line that contains these two points;
- for every distinct pair of lines, the lines have at most one point in common;
- for every line l and point p there is a unique line through p parallel to l.

If we could prove these properties using non-commutative Gröbner bases, we would do that here. However these properties are about existence and uniqueness, therefore it is difficult or even impossible to formulate the properties as hypothesis and thesis polynomials. As proving these properties by other means, does not help proving other properties using non-commutative Gröbner bases, we will not prove them. However we will give some equations for denoting the special lines and points mentioned. In these equations z is an auxiliary variable. Also we give how the primitives can be constructed to have the given property.

Property	**Equation**	**Construction**
Lines $L(a,t)$ and $L(b,s)$ are parallel.	$\forall i \in \{1,\ldots,n\} : z \cdot a_i = b_i$	$L(a,t)$ and $L(a,s)$
Line $L(a,t)$ goes through point p	$\forall i \in \{1,\ldots,n\} : z \cdot a_i + t_i = p_i$	$L(a,p)$

3.3 Problems

As we mentioned earlier, non-commutative Gröbner bases can probably not be used for proving theorems in geometries over division rings. This is due to some unresolved problems, that we will discuss here. The first problem is encountered when trying to do division.

In the commutative case, if we have an equation containing divisions, we can always rewrite that equation such that the division is removed. This is done by rewriting the fractions: $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{db}$ and $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ and removing the denominator: $\frac{a}{b} = 0 \implies a = 0$. In the non-commutative case, we have left and right sided fractions. Not all sums and products of theses fractions can be rewritten, such that the division is removed.

To work around this problem, an auxiliary variable can be introduced that will represent the inverse. For example, if something is divided by x, the auxiliary variable z and the equation $xz = 1$ is added. Instead of dividing by x we can now multiply by z. However, this workaround only moves the problem, because $zx - 1$ is not in the ideal $\langle xz - 1 \rangle$. We can decide to add the equation $zx - 1$ to the ideal as well and hope that this solves the problem, but investigating why this problem occurs might prove more insightful.

We have that $\forall x, z \in k : xz - 1 = 0 \implies zx - 1 = 0$. The reason that, despite this implication, $zx - 1 \notin \langle xz - 1 \rangle$ is because x and z are indeterminate variables and not elements of k. They do not even represent elements from k. The problem is that we assumed that we can represent geometric objects as polynomial equations, while in they are actually sets of the solutions of these equations. Such sets are known as varieties.

Definition 3.3.1 (Variety)**.** Let S be a set of polynomials. The set $\{\ x \mid \forall f \in S : f(x) = 0\ \}$ is a variety.

In the commutative case we could get away with using the polynomial equations, because of the Hilbert nullstellensatz. This theorem states that radical ideals and varieties are interchangeable.[1] In the non-commutative case this theorem does not hold. We believe that this is the reason why we did not succeed in using non-commutative Gröbner bases for proving theorems in geometries over division rings.

[1] This is explained and proven in both [1] and [6].

Appendix A

Listings

A.1 Thales

For proving Thales' theorem for the second time in section 1.1.1 we used Singular[2]. The following script shows that the hypothesis polynomial is in the thesis ideal.

```
1  ring f=0,(x(0..3),y(0..3),r),dp;
2  setring f;
3
4  poly c1 = (x(1)-x(0))^2+(y(1)-y(0))^2-r^2;
5  poly c2 = (x(2)-x(0))^2+(y(2)-y(0))^2-r^2;
6  poly c3 = (x(3)-x(0))^2+(y(3)-y(0))^2-r^2;
7  poly m1 = x(1)+x(2)-2*x(0);
8  poly m2 = y(1)+y(2)-2*y(0);
9  ideal thesis = c1,c2,c3,m1,m2;
10 poly hypothesis = (x(1)-x(3))*(x(2)-x(3))+(y(1)-y(3))*(y(2)-y
       (3));
11
12 printf("## grobner basis:");
13 ideal basis = groebner(thesis);
14 basis;
15
16 printf("## hypothesis modulo grobner basis:");
17 reduce(hypothesis,basis);
```

A.2 Finite and infinite non-commutative Gröbner basis

This script shows that a badly chosen monomial order can cause the Gröbner basis to be infinite. The function `test` computes the Gröbner basis of $xx - xy$ using a skew monomial order based on the order of the arguments. The algorithm is terminated if a Gröbner basis is not computed within 10 iterations.

```
1  LoadPackage("GBNP");;
2
3  test := function(arg)
4          local A,x,y,gb;;
5          A:=FreeAssociativeAlgebraWithOne(Rationals,arg);;
6          GBNP.ConfigPrint(A);;
7          x:=A.x;; y:=A.y;;
8          gb:=SGrobner(GP2NPList([x*x-x*y]),10);;
9          PrintNPList(gb.G);;
10         if not gb.completed then
11                 Print("and more ...\n");;
12         fi;;
13 end;;
14
15 test("x","y");;
16 test("y","x");;
```

Output:

```
gap> test("x","y");;
 xy - x^2
gap> test("y","x");;
 x^2 - xy
 xyx - xy^2
 xy^2x - xy^3
 xy^3x - xy^4
 xy^4x - xy^5
 xy^5x - xy^6
 xy^6x - xy^7
 xy^7x - xy^8
 xy^8x - xy^9
 xy^9x - xy^10
 xy^10x - xy^11
and more ...
```

Bibliography

[1] Ralf Fröberg. *An Introduction to Gröbner Bases.* John Wiley & Sons Ltd, 1997.

[2] H. Schoenemann G.-M. Greuel, G. Pfister. Singular 3-0-4 (a computer algebra system for polynomial computations), Nov 2007.

[3] Benjamin J. Keller. *Algorithms and Orders for Finding Noncommutative Gröbner Bases.* PhD thesis, Virginia Polytechnic Institute and State University, 1997.

[4] A.M. Cohen & J.W. Knopper. *Gröbner bases of noncommutative polynomials (GAP 4 package).* TU/e, POB 513, 5600 MB Eindhoven, the Netherlands, May 2007.

[5] Teo Mora. An introduction to commutative and non-commutative gröbner bases. *Theoretical Computer Science*, 134:131–173, 1994.

[6] David A. Cox & John Little & Donal O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra.* Springer-Verlag New York, Inc., 2007.