Isometry Group, Words and Proofs of Geometric Theorems

Dominique Michelucci
LE2I, Computer Science Department, University of Dijon, France
Dominique.Michelucci@u-bourgogne.fr

ABSTRACT

This paper shows that considering the group generated by orthogonal symmetries relatively to lines may give very short and readable proofs of geometric theorems. A short and readable proof of the fundamental Pascal's theorem is provided for illustration.

General Terms

Words, rewriting methods, orthogonal symmetries group, isometry, involution, Knuth-Bendix

Keywords

Words, Groups, Rewriting, Geometry

1. INTRODUCTION

The classical method to prove geometric theorems of the Euclidean plane resorts to computer algebra [2, 3], for instance Grobner bases: the hypothesis and the conclusion of the geometric theorem are represented by polynomials involving points coordinates, and the theorem holds when the conclusion polynomial lies inside the ideal or the radical of the polynomials of the hypothesis.

Is it possible to represent the hypothesis and the conclusion of the geometric theorem with words (to be defined below), and to prove theorems with rewriting methods [4]?

A word is just a sequence of identifiers, also called letters. Words can be concatenated. A subword is a subsequence of consecutive letters in a word. A set of relations specifies equalities between subwords, and thus possible substitutions, for instance: $ABCD = EF$. The word problem is to prove that two given words are, or are not, equivalent modulo a given set of relations. Groups with a finite presentation can be defined this way: letters denote generators of the group, and relations give equalities, *ie* constraints on the group. Generators and relations are the presentation of the group. All finite groups have a finite presentation. Some infinite groups have also a finite presentation, *ie* a finite number of generators and relations.

The word problem is not decidable in general, but many instances of the word problem are decidable and interesting. Knuth and Bendix proposed a today classic method to solve the word problem. The main idea is to orient rules, so that complicated subwords are replaced with simpler ones: rules simplify. For equality to be decidable, all possible reduction chains of a given word must yield the same irreducible word, which is called its normal form. The idea of Knuth and Bendix is to consider critical pairs, *ie* words which can be reduced in two ways; each time a word w can be reduced into u with a first reduction path, and to v with a second reduction path, and u and v are not identical, a new relation: $u = v$ is inserted, and oriented. When we are lucky, a finite number of rules is inserted, *ie* the completion algorithm terminates; then the equality is decidable in the theory. Buchberger has outlined the similarity between critical pairs of Knuth and Bendix method, and his method for computing Grobner bases. Unfortunately, the Knuth and Bendix method usually does not terminate in presence of commutativity rules. Thus a terminating algorithm is needed for the approach proposed in this paper to be interesting.

We consider geometric theorems of the Euclidean plane. To reduce the problem of proving geometric theorems to the word problem, each line in the problem is represented by a letter, which stands for the orthogonal symmetry relatively to this line; this symmetry leaves invariant each point of this line.

Geometric axioms give a first set of relations, *eg* for each line L, the symmetry along L is an involution thus $LL = \epsilon$ (ϵ is the empty word; it represents the identity map, *ie* the neutral element of the group); moreover words like $(ABC)^2$ (where $(ABC)^2$ stands for $ABCABC$), more generally all concatenations of square of words with odd lengths, describe translations, and translations commute, thus $\forall A$, B, C, U, V, W: $(ABC)^2(UVW)^2 = (UVW)^2(ABC)^2$ is a possible axiom. However a finite presentation of the group is beyond the scope of this paper.

The hypothesis of the theorem give a second set of relations; for instance the concurrence of 3 lines A, B, C is expressed by $(ABC)^2 = \epsilon$; the conclusion of the theorem is also represented with some relation. In our case, the theorem holds when the conclusion word reduces to the empty word: for instance if $(AB)^2$ reduces to ϵ, it proves that lines A and B are either equal or orthogonal.

Previous works. This approach is reminiscent to Bachmann's axiomatisation of geometry (see the related chapter

SAC'08 March 16-20, 2008, Fortaleza, Ceará, Brazil

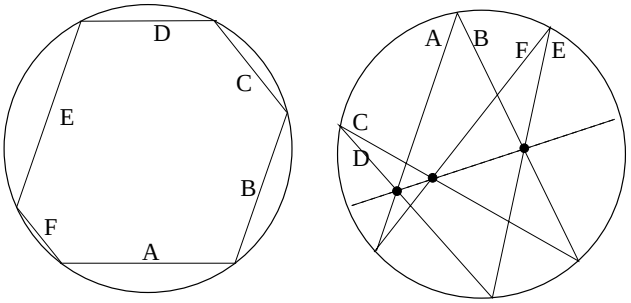

Figure 1: Pascal's theorem: opposite sides are parallel (left) or meet in 3 aligned points (right).

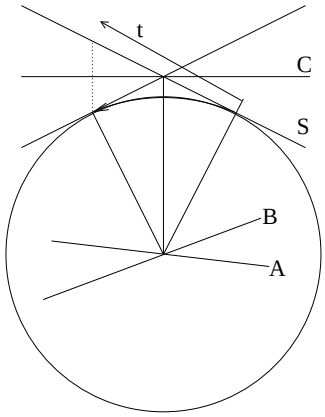

Figure 3: ABC is a glide symmetry: construction of the translation vector and of S the axis of symmetry.

in Henle's book [5] and Yves Martin's thesis [6]). Bachmann's approach was not computational, he did not focus on the Euclidean plane, but rather classified possible geometries; he used both symmetries w.r.t. lines and points; as far as I know, he did not prove Pascal's theorem, and did not attempt to syntaxically characterize words which are translations or orthogonal symmetries.

Organisation of the paper. The theory proposed in this paper gives a very readable proof of Pascal's theorem, one of the essential theorems of the Euclidean plane, and of the projective plane. This proof is given and commented in section 3. The impatient reader can jump to section 3. The needed background is presented before: geometric theorems, especially the basic Pascal's theorem; the isometry group: symmetries, rotations, translations; a conjectured characterization of translations as concatenations of squares of odd words; how conjugations are used to transport properties and proofs. The paper concludes with the questions which must be solved for this approach to be feasible.

2. BACKGROUND

2.1 Some geometric theorems

After Pascal's theorem, the 3 opposite sides of any hexagon inscribed in a conic meet in 3 points aligned on a Pascal's line. Since there are 5!/2=60 distinct cycles through the 6 points, there are 60 Pascal lines. Pappus's theorem is a special case of Pascal's theorem, when the conic degenerates into a couple of lines. It is known that Pascal and Pappus's theorems are logically equivalent: any one can be proved from the other.

Blaise Pascal proved his theorem in the case of a circle; then, using arguments of projective geometry due to Girard Desargues, he extended it to any conic. Actually, it is sufficient to prove Pascal's theorem in the even more special -and easier- case: for any hexagon inscribed in a circle, so that two pairs of two opposite sides are parallel, the two remaining sides are parallel as well. It is said that the Pascal line, along which opposite sides meet, is "sent to infinity".

The theory presented here is able to prove this simplest case of Pascal's theorem, which is very encouraging. Indeed, Pascal' and Pappus's theorems are essential in Euclidean geometry: any plane fulfiling Pascal's or Pappus's properties can be used to define a commutative field. Geometric constructions for the sum and the product are shown in Fig. 2 (I am not sure who to credit for these constructions, likely von Staudt. It is possible to replace the circle with another conic, *ie* a pair of lines [1]); all the proofs of commutativity, associativity, distributivity, etc use Pascal's or Pappus's properties. Another argument which shows the basic nature of Pascal's theorem is that Raymond Pouzergues [7] used it to provide very concise and visual proofs of numerous geometric theorems, in projective geometry but also in metric geometry (search "hexamys" on the web).

This paper asks if proving geometric problems reduces to word problems. Algebra reduces to geometry. Thus algebra should also reduce to word problems... This reduction is only theoretical up to now: this paper does not prove that the group has a finite presentation, and no method is proposed for the related word problem.

2.2 Words, symmetries, isometries

Orthogonal symmetries generate the non commutative group of isometries: "even" isometries are rotations, translations, or the identity; they form a subgroup; "odd" isometries are orthogonal symmetries or glide symmetries; the square of an orthogonal symmetry is the identity; the square of a glide symmetry is a translation.

The empty word is denoted ϵ. Its length is zero. It represents the identity mapping. Upper case letters denote orthogonal symmetries. They also denote the geometric line which is the axis of the orthogonal symmetry, the distinction being made by the context. By convention, the orthogonal symmetries in a word are applied from left to right. Orthogonal symmetries are involutions, so $AA = BB = CC = \ldots = \epsilon$. An even (odd) word is a word with an even (odd) number of upper case letters. Even (odd) words denote even (odd) isometries.

Lower case letters denote words. The inverse of a word w is its reverse $\bar{w}$, for example if $w = ABCD$ then $\bar{w} = DCBA$. w^2 is a shortcut for ww, and w^3 a shortcut for www, etc.

Each commutativity of transforms a and b gives a relation $ab = ba$, equivalent to the cycle $ab\bar{a}\bar{b} = \epsilon$; all cycles due to commutativity have even lengths, as well as the cycles $AA = BB = \ldots = \epsilon$. Thus all resulting cycles will have even length. It is consistent with the algebraic view, where odd isometries have determinant -1, and even isometries have determinant +1.

Every circular permutation of a cycle $w = \epsilon$ or its reverse

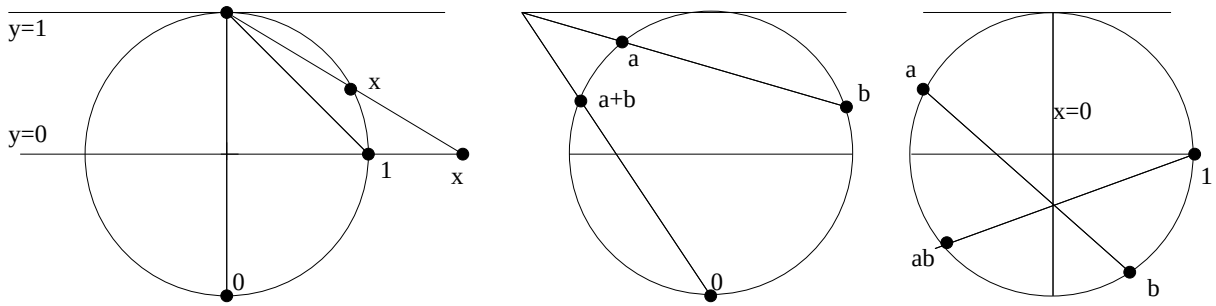

Figure 2: Real numbers are represented by points on a circle. Construction of $a+b$ and ab from given a, b.

$\bar{w} = \epsilon$ gives another cycle. This holds because all upper case letters denote involutions. A consequence is that the convention "apply transforms from left to right" does not matter.

A palindrome is its own inverse. All palindromes with even length reduce to ϵ. All palindromes with odd length represent orthogonal symmetries.

Words representing orthogonal symmetries can be replaced with a new upper case letter. For instance, if $X = ABA$, then the rotation AX equals the rotation BA (proof: $X = ABA \Rightarrow AX = AABA = BA$), thus X is the line symmetric of B relatively to A.

The product AB of two orthogonal symmetries is a translation when lines A and B are parallel, and a rotation when A and B meet. The centre is the intersection point of the lines A and B, the angle is twice the angle of the two lines A and B. The inverse rotation is BA.

A word with odd length like ABC is usually a glide symmetry, and an orthogonal symmetry in degenerate cases. Anyway, it is always the composition of a translation t_v (null in the degenerate case) and an orthogonal symmetry S relatively to a line S parallel to the vector of the translation t_v, so t_v and S commute: $t_v S = S t_v$. See Fig. 3. The square of the glide symmetry is $t_v S t_v S = t_v t_v S S = t_v t_v$, thus it is the square of the translation part.

Thus, for all words w with odd length, w^2 denotes a translation (possibly the identity). This property holds only in 2D: it is wrong in 3D, for orthogonal symmetries relatively to planes, even if the planes all pass through a common point. Circular permutations of w^2 are translations too, see below. Further I will conjecture that every translation is a concatenation of squares of odd words.

Concurrent or parallel lines. When three lines A, B, C concur (or are parallel), the rotations (or the translations) AB and BC commute, so $(BC)(AB) = (AB)(BC) = AC$, or: $(ABC)^2 = \epsilon$. The 3!=6 cycles of ABC can be deduced.

Parallel lines. If lines A and B are parallel, words AB and BA represent translations. Translations commute, *ie* for all translations represented by a word t (for instance $t = (IJK)^2$), $ABt = tAB$, and $BAt = tBA$.

The theory can prove that A parallel to B, and A parallel to C implies B parallel to C. Proof: A and B are parallel thus $ABt = tAB \Rightarrow tA = ABtB$. A and C are parallel thus $ACt = tAC$: we saw that tA equals $ABtB$. Thus we get $ACt = (tA)C = (ABtB)C$. Premultiply both sides with BA and simplify. $ACt = ABtBC \Rightarrow (BA)(ACt) = (BA)(ABtBC) \Rightarrow BCt = tBC$. Thus BC is a translation, since it commutes with the translation t. Thus corresponding lines B and C are parallel. QED.

Parallelogram. Suppose four lines A, B, C, D define a parallelogram: A, B are parallel, as well as C, D. Thus AB, BA, CD, DC are translations and commute. It implies that $\Phi_4(A, B, C, D) = (AB)(CD)(BA)(DC) = \epsilon$.

Quadrilateral inscribed in a circle. Let A, B, C, D be four lines such that the intersection points $A \cap B, B \cap C, C \cap D, D \cap A$ exist and lie on a common circle. Then the transform $ABCD$ is a translation (for any 4 generic lines, $ABCD$ is a rotation), which commute with all other translations. Hint: the sum of opposite angles of a quadrilateral inscribed in a circle is π.

Orthogonal lines. If lines A and B are orthogonal, then $AB = BA$ is the rotation with angle π around the intersection point of lines A and B. A and B commute only when $A = B$ or when A and B are orthogonal. $AB = BA$ implies that $(AB)^2 = ABAB = ABBA = \epsilon$.

Equal angles. The angle between lines A and B equals the angle between A' and B' iff $ABB'A'$ is a translation. The angles are opposite iff $ABA'B'$ is a translation.

Parallel triangles. There is a translation which maps a triangle A, B, C to a triangle with parallel sides A', B', C' iff homologuous sides are parallel, and $(ABC)^2 = (A'B'C')^2$. Proof: let t be the translation which maps the two triangles. Then $(A'B'C')^2 = (tA\bar{t}tB\bar{t}tC\bar{t})^2 = t(ABC)^2\bar{t}$, then use commutativity of translations: t, $\bar{t}$ and $(ABC)^2$, and conclude. QED. Remark that no axiom is needed to guarantee that there is a unique translation vector from $A \cap B$ to $A' \cap B'$ (which imposes constraints on C and C'), or, in other words, to guarantee that there is a unique line through two different points, contrarily to Bachmann's axiomatization.

2.3 Definitions and formulas

$$\Phi_4(A, B, C, D) = (AB)(CD)(BA)(DC) \quad (1)$$

$$\Phi_2(a, b) = ab\bar{a}\bar{b} \quad (2)$$

$$\Phi_4(A, B, C, D) = \Phi_2(AB, CD) \quad (3)$$

$$\Phi_4(A, B, C, D) = C(CAB)^2(BAD)^2C \quad (4)$$

$$= \left(C(CAB)^2(BAD)^2\right)^2 (DAB)^2(BAC)^2 \quad (5)$$

$$AwA = (Aw)^2\bar{w} \quad (6)$$

2.4 Which words are translations?

Translations form a commutative normal subgroup. Each commutativity relation $tt' = t't$ gives a relation, so it is essential to understand which words denote translations.

This section presents several ways to generate or characterize words which are translations.

The simplest rule is: the square of any odd word is a translation (or the identity), because the odd word is either a glide symmetry or an orthogonal symmetry. Actually, I conjecture that all translations are compositions of squares of odd words. No proof in this paper uses this conjecture.

The concatenation of two translations is another translation, but no axiom is needed, it results from basic manipulations on words. Proof: suppose t and t' are two translations, so they commute with a third "generic" translation noted Θ for convenience: by hypothesis $t\Theta = \Theta t$ and $t'\Theta = \Theta t'$. Then $(tt')\Theta = t(t'\Theta) = t(\Theta t') = (t\Theta)t' = (\Theta t)t' = \Theta(tt')$: thus tt' commutes with Θ. So tt' is a translation. QED.

Translations are stable by conjugations: assume t is a translation, we want to prove LtL is a translation. Lt has an odd number of letters. Thus $(Lt)^2$ is a translation. Now, $\bar{t}$ is a translation too. Thus $(Lt)^2\bar{t} = LtL$ is a translation. QED. Note that if t is a composition of squares, then LtL is also a composition of squares: $LtL = (Lt)^2\bar{t}$. Note that circular permutations of a word are just conjugations, with the first or the last letter of the word. Thus: any circular permutation of a word denoting a translation denotes a translation as well, and: any circular permutation of a concatenation of squares of odd words is also a concatenation of squares of odd words.

In passing: conjugations (and circular permutations) of orthogonal symmetries are orthogonal symmetries; proof: $s^2 = \epsilon \Rightarrow (AsA)^2 = AsAAsA = AssA = AA = \epsilon$. QED. And clearly, conjugations (and circular permutations) of odd palindromes are odd palindromes.

Another way to generate translations use $\Phi_4(A,B,C,D) = (AB)(CD)(BA)(DC)$; any circular permutation can be used instead but this one is easier to remember, because of its resemblance with a commutator. Then $\Phi_4(A,B,C,D)$ is a translation. This axiom is wrong in 3D, for symmetries relatively to generic planes, or planes with a common point (spheric geometry). To give a geometric justification for this axiom in 2D, just observe that $(AB)(CD)$ and $(BA)(DC)$ are two rotations with opposite angles; the composition of two such rotations is a translation. But we can prove it with words: remark that $\Phi_4(A,B,C,D) = C(CAB)^2(BAD)^2C$. The conjugation by C can be eliminated with $CtC = (Ct)^2\bar{t}$ where $t = (CAB)^2(BAD)^2$. So it seems that all translation words can be expressed as a concatenation of squares of odd words. I don't know if it is possible to express all translations as the product of squares of words with 3 letters each. Another useful relation: $(ABC)^2 = \Phi_4(A,B,C,B)$ completes this equivalence between Φ_4 and square triples.

Alternatively, we can generate translations with only Φ_2 where $\Phi_2(a,b) = ab\bar{a}\bar{b}$ where a and b are even. Note that $\Phi_4(A,B,C,D)$ is just $\Phi_2(AB,CD)$. To prove that $\Phi_2(a,b)$ is a translation iff both a and b are even words, remark that ab and $\bar{a}\bar{b}$ are either both translations, or rotations with opposite angles. In both cases, their composition is a translation. Φ_2 is stable by conjugations: $\Phi_2(ga\bar{g}, gb\bar{g}) = ga\bar{g}gb\bar{g}g\bar{a}\bar{g}g\bar{b}\bar{g} = gab\bar{a}\bar{b}\bar{g} = g\Phi_2(a,b)\bar{g}$.

2.5 Commutations of translations and glide symmetries

Let $t = wA$ be a word denoting a translation. Then w is a glide symmetry with an axis, and a translation vector, parallel to the line A. Proof: Aw is translation too (since it is a circular permutation of $t = wA$). Thus wA and Aw commute. Then $w^2A = (wA)(Aw)A = (Aw)(wA)A = Aw^2$. Thus w^2 commute with A. Moreover w^2 is a translation because w is odd. The vector of the translation w^2 is parallel to the line A, since w^2 and A commute. The translation vector of the glide symmetry w is half the translation vector of w^2. Thus w is a glide symmetry with an axis, and a translation vector, parallel to the line A. QED.

2.6 Conjugations, and the transfer principle

Let G be a line, the corresponding symmetry maps the line A to the line A', the symmetry of which is: $A' = GAG$. We prove that the line A, its image A' by the symmetry G, and the axis of symmetry: the line G, are concurrent (or parallel): $AA'G = A(GAG)G = AGA$, and squaring gives: $(AA'G)^2 = (AGA)^2 = AGAAGA = AGGA = AA = \epsilon$. QED. In passing, it proves a particular case of the Desargue theorem about perspective triangles, when they are symmetric relatively to a line.

Let w an even word, denoting a translation or a rotation or the identity. The image of the line A is the line A', and the symmetry wrt A' is: $A' = wA\bar{w}$. Similarly for a line B, which is mapped to a line B' with $B' = wB\bar{w}$ (note that $wB\bar{w}$ is a palindrome, thus an orthogonal symmetry, as B'). We prove that the angle between lines A and B is not modified by the transformation w. It suffices to prove that$(AB)(BA')$ is a translation, *ie* angles of the rotations AB and $B'A'$ are opposite. $ABB'A' = ABwB\bar{w}wA\bar{w} = ABwBA\bar{w}$ is equal to $\Phi_2(AB,w)$ (remember that w is even) thus it is a translation. QED.

Actually, this proof can be extended to odd words w: in this case, the angle between lines A and B is the opposite of the angle between lines A' and B': orthogonal and glide symmetries reverse orientations. Thus we consider $ABA'B'$ this time, we want to prove it is a translation. We have: $ABA'B' = ABwA\bar{w}wB\bar{w} = ABwAB\bar{w}$. This is equal to $(ABw)^2\bar{w}^2$, the composition of two translations, thus it is a translation. QED.

Which lines are invariant by a symmetry G? Let X be such a line. Then $X' = GXG = X \Rightarrow GX = XG$. Symmetries G and X commute, thus lines G and X are orthogonal, or equal.

Actually, conjugacy makes possible to transfer any property expressable with a cycle $f(L_1, L_2, L_3 \ldots) = \epsilon$, from a figure involving lines L_i to the image of this figure, which are the lines L'_i, with $L'_i = wL_i\bar{w}$. Then $f(L'_i) = wf(L_i)\bar{w} = w\bar{w} = \epsilon$.

Actually, it also works when w denotes a mapping which is not an isometry, but a projective mapping, *ie* a bijection which preserves incidences. Note that if t_1 and t_2 are two translations in a figure, and $t'_1 = wt_1\bar{w}$ and $t'_2 = wt_2\bar{w}$ are the images of t_1 and t_2 by w, generally t'_1 and t'_2 are no more translations when w is not an isometry; but they still commute: $t'_1t'_2 = (wt_1\bar{w})(wt_2\bar{w}) = wt_1t_2\bar{w} = wt_2t_1\bar{w} = (wt_2\bar{w})(wt_1\bar{w}) = t'_2t'_1$. Indeed, commutativity of t_1 and t_2 is expressed by the cycle: $t_1t_2\bar{t_1}\bar{t_2} = \epsilon$, so this cycle is preserved by conjugacy with w. Incidence is expressed by a cycle, so these transforms conserve incidence: if lines $L_1L_2L_3$ concur or are parallel: $(L_1L_2L_3)^2 = \epsilon$, then $(L'_1L'_2L'_3)^2 = w(L_1L_2L_3)^2\bar{w} = \epsilon$, so their images L'_1, L'_2, L'_3 concur (or are parallel) as well.

Blaise Pascal used conjugations by projective mappings to extend his theorem from a circle to a conic. Conjugation

can also be used to send the Pascal's line at infinity, which means opposite sides of the hexagon become parallel.

2.7 Protocol

If this approach ever leads to an algorithm (up to now, it is just wishful thinking), the protocol to prove a theorem will be as follows. Users will specify facts with cycles, for instance to specify concurrences of 3 lines A, B, C, users will say that $(ABC)^2 = \epsilon$. The software will generate automatically relations for the isometry group. The conclusion will be a cycle too: for instance, the concurrence of lines U, V, W is proved iff the normal form of $(UVW)^2$ is ϵ; the lines U and V are parallel iff the normal form of $UV\Theta VU\bar{\Theta}$ is ϵ, where Θ is some translation $(IJK)^2$; the lines U and V are orthogonal (or equal) if $UVUV$ reduces to ϵ; the quadrilateral $ABCD$ is inscribed in a circle if $ABCD$ is a translation (*ie* commutes with an ad-hoc translation Θ); etc.

This supposes the group has a finite presentation, and that there is a computable standard form for this group.

Possible other difficulties: the formalism of Grobner bases, makes possible to express inequalities, for instance: x is non zero if $xy - 1 = 0$ where y is a new, free, variable. A question is how to express inequalities with the word formalism. It should be possible, since algebra reduces to geometry (Fig. 2). Another difficulty, reminiscent to the distinction ideal/radical, is that there is no axiom such that if the square (or another power) of a translation is the identity, then the translation is the identity. After all, it may happen in finite fields, and discrete planes.

3. PASCAL'S THEOREM

3.1 The proof

The background is now sufficient to present the proof of Pascal's theorem.

The lines $ABCDEF$ are cocyclic: the vertices $A \cap B, B \cap C, C \cap D, D \cap E, E \cap F, F \cap A$ lie on a circle. Moreover A is parallel to D, and B is parallel to E. We want to prove that C is parallel to F. ABC is the beginning of a cocyclic quadrilateral: let L be the line passing through $A \cap F$ and $C \cap D$. Then $ABCL$ and $LFED$ are two cocyclic quadrilaterals, thus $ABCL$ and $LFED$ are two translations. Their composition: $(ABCL)(LFED) = ABCFED$ is a translation as well. In the sequel, isTrans(w) means that w denotes a translation.

isTrans($ABC\,FED$)
$\Rightarrow$ isTrans($BCFEDA$) by circular permutation
$\Rightarrow$ isTrans($BCFEDA\;AD$) because isTrans(AD)
$\Rightarrow$ isTrans($BCFE$) by collapse of $DAAD$
$\Rightarrow$ isTrans($EBCF$) by circular permutation
$\Rightarrow$ isTrans($BE\;EBCF$) because isTrans(BE)
$\Rightarrow$ isTrans(CF) by collapse of $BEEB$
$\Rightarrow$ C and F are parallel. QED.

3.2 Comments

Is it possible to prove a more general variant of the Pascal's theorem, using only substitutions between words? Maybe. But I have not found it up to now: with the words formalism, proofs are easy to read but terribly difficult to find. At least, the reader should be convinced that this question is indeed a word problem, where rewriting methods are relevant.

If it is not possible to prove the general variant, it means that some axioms are missing.

Remember that classical geometric proofs usually use conjugations with some projective transform α (a 1-1 mapping which preserves collinearities and concurrences, *ie* relations: $(ABC)^2 = \epsilon$) such as a polarity or an homography. Indeed there is such a projective transform α which maps an hexagon inscribed in a conic to an hexagon inscribed in a circle with a Pascal's line at infinity (btw, the existence of α can be an axiom). These transforms make possible to transfer properties, such as collinearities. Unfortunately, these projective transforms are not isometries, so they escape my formalism. Two approaches can be considered: either use other involutions, which are not isometries but homographies or polarities, in the spirit of Desargue (Desargue introduced involutive homographies in projective geometry); or formalize and automatize the method of sending a line at infinity.

4. CONCLUSION: A NEW PLAY-GROUND?

This paper investigates whether it is possible to reduce proving geometric theorems to a word problem, treatable (?) with some rewriting method. This approach gives a concise and readable proof of Pascal's theorem, the fundamental theorem of the Euclidean and the projective plane, which is encouraging. A conjecture which naturally arises is that *all Euclidean geometry can be explained by the involutivity of orthogonal symmetries and the commutativity of squares of odd words.*

For this proving approach to become computational, the following questions must be answered: is there a finite presentation of the group generated by a finite number of orthogonal symmetries? Is there a terminating rewriting method, *ie* a normal form for these words? Of course I mean a method independent of computer algebra, coordinates, polynomials, etc.

Such a method would provide a new insight for proving geometric theorems, but also for computer algebra. Other questions which arise were presented in passing. A future work is to investigate other involutions, from projective geometry, in the wake of Desargue.

5. REFERENCES

[1] J. E. Bonin. *Introduction to matroid theory.* The George Washington University. On line.

[2] S.-C. Chou. *Mechanical Geometry theorem Proving.* D. Reidel Publishing Company, 1988.

[3] D. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry.* Springer-Verlag, New York, 1998.

[4] N. Dershowitz and D. A. Plaisted. Rewriting. In *Handbook of Automated Reasoning, chap 9, vol. 1.* Elsevier, 2001.

[5] M. Henle. *Modern Geometries: Non-Euclidean, Projective, and Discrete Geometry.* 1997, 2001.

[6] Y. Martin. *Axiomatique de Bachmann: L'approche algébrique ultime pour la géométrie plane.* PhD thesis, IUFM de la Réunion, 2002. On line.

[7] R. Pouzergues. Les hexamys. Technical report, IREM, Nice, 1993. http://hexamys.free.fr/.