Preliminary version of a paper published in:
A. Koslow and A. Buchbaum (eds.) *The Road to Universal Logic. Festschrift for 50th Birthday of Jean-Yves Béziau, Vol.* I,
Series: *Studies in Universal Logic*, 2015, XII, 191-220.

Hexagonal Logic of the Field $\mathbb{F}_8$ as a Boolean Logic with Three Involutive Modalities

René Guitart

In friendly homage to Jean-Yves Béziau, on the occasion of his 50th birthday

Abstract. We consider the Post-Malcev full iterative algebra $\mathbb{P}_8$ of all functions of all finite arities on a set $\underline{8}$ with 8 elements, e.g. on the Galois field $\mathbb{F}_8$. We prove that $\mathbb{P}_8$ is generated by the logical operations of a canonical boolean structure on $\mathbb{F}_8 = \mathbb{F}_2^3$, plus three involutive $\mathbb{F}_2$-linear transvections A, B, C, related by circular relations and generating the group $\mathrm{GL}_3(\mathbb{F}_2)$. It is known that $\mathrm{GL}_3(\mathbb{F}_2) = \mathrm{PSL}_2(\mathbb{F}_7) = \mathrm{G}_{168}$ is the unique simple group of order 168, which is the group of automorphisms of the Fano plane. Also we obtain that $\mathbb{P}_8$ is generated by its boolean logic plus the three cross product operations $R\times$, $S\times$, $I\times$.
Especially our result could be understood as a *hexagonal logic*, a natural setting to study the logic of functions on a hexagon; precisely it is a *hexagonal presentation of the logic of functions on a cube with a selected diagonal.*

Mathematics Subject Classification (2010). 00A06, 03B45, 03B50, 03G05, 06Exx, 06E25, 06E30, 11Txx.

Keywords. Hexagon of opposition, borromean object, specular logic, boolean algebra, modality, many-valued logics, finite fields, Fano plane.

1. Introduction: How and why to generate functions on $\underline{8}$?

Our concrete result is formulated in elementary terms in Theorem 8.1. Its geometrical formulation is in Proposition 7.7, and others variations are given by Propositions 7.4 (for A, B, C), 6.11 and 6.12 (for r, s, i and r^{-1}, s^{-1}, s^{-1}), and 5.6 and 5.7 (for the calculus of avatars); these variations have their own interest *and* are steps in the proof of 8.1.

The question is to generate the system of all the functions of all finites arities on a set $\underline{8} = \{\underline{0}, \underline{1}, \underline{2}, \underline{3}, \underline{4}, \underline{5}, \underline{6}, \underline{7}\}$ with 8 elements.

The method is to emphasize the hexagon character of the situation, at the level of the data ($\mathbb{F}_8$), as well as at the level of functions elements of ($\mathbb{P}_8$);

then we explore arithmetic and geometry around the Fano plane with 7 points and the Galois field $\mathbb{F}_8$ with 8 elements; and mainly we look at polynomial equations, computation of cross products, and the geometry of the cube $\mathbb{F}_2^3$. The advantage of the method is to obtain a solution in which a hexagonal symmetry is assumed among elements: the hexagonal symmetry among the data is reproduced among the solutions.

In section 2, the beginning of the paper provides motivations, in the context of splitting paradoxes in analysis of discourses. It is explained what we mean by a hexagon seen as a cube with a selected diagonal, and hexagonal functions.

In section 3 we represent $\underline{8}$ by the Galois' field $\mathbb{F}_8$, we develop the analysis of the field $\mathbb{F}_8$ and its hexagonal generation, in relation with the Fano plane. We introduce the Galois's field structure and arithmetical calculus with the roots R, S, I of $X^3 + X^2 + 1 = 0$.

In section 4 are developed the geometry of $\mathbb{F}_8$ as a $\mathbb{F}_2$-vectorial space, with scalar, cross and mixed products, its canonical boolean logic, and the galoisian data of the Frobenius map.

In section 5, with the help of results of sections 3 and 4, we obtain the representation of $\mathbb{P}_8$ by sums of conjunctions of avatars. This would be enough in order to solve some logical paradoxes, in the style [8] with $\mathbb{F}_4$.

In section 6 we prove that $\mathbb{F}_8$ admits a unique strictly auto-dual basis, showing that the canonical logic on $\mathbb{F}_8$ is really canonical. With the result of section 5 and the analysis of $\mathrm{GL}_3(\mathbb{F}_2)$ from [7], this is used to prove the R, S, I generation of $\mathbb{P}_8$.

In section 7 we arrive to the A, B, C presentation by three involutive transvections (plus the canonical boolean structure), and we end by the $R^\times, S^\times, I^\times$ presentation.

In the conclusive section 8 we stress the decoration of a hexagon by functions of $\mathbb{P}_8$, and — as announced at the beginning of this introduction — we reach Theorem 8.1.

Warning on notations — We will see in Proposition 5.5 that any function $f : \mathbb{F}_8 \to \mathbb{F}_8$ could be represented by a polynomial P, and especially it is true for linear functions. But a linear f is also representable by matrices M relative to the canonical basis κ, and in principle we have to not confuse f, P and M. This is important for product and composition. If we write NM we mean the *composition* of the matrice N applied to M, and gf means $g \circ f$ the composition of g applied to f, and in particular f^2 means $f \circ f$, the composite of f with f, defined by $f^2(u) = f(f(u))$. But by QP we mean the *product* of Q and P, P^2 means the square of P defined by $P^2(u) = (P(u))^2$. The reader will make the distinction according to the context.

Convention: If necessary, in order to avoid too much confusions, if M is a matrice of f and P a polynomial of the same f,we introduce

$$P_f = P = \underline{M}, \quad M_f = M = \hat{P},$$

in such a way that $\underline{N}\,\underline{M}$ is the product of polynomial QP, and $\hat{Q}\hat{P}$ is the composition of matrices NM. This is useful especially in sections 6 and 7.

2. $\mathbb{F}_8$ and the oriented hexagon

2.1. The square and the splitting of paradoxes in $\mathbb{F}_4$

In [6], [7], [8] we have introduced the use of a Galois field of characteristic 2 as a logical tool to analyze paradoxical sentences. It was a continuation of [5], as an arithmetical version of the idea of point of view and *speculation*. It was related to the picture of a hexagon and ideas of *borromean object* and *boolean manifold*. We gave explicit results in the 2-dim case $\mathbb{F}_4$, using two facts: the shape of the system of various boolean structures on $\mathbb{F}_4$ — alias the system of $\mathbb{F}_2$-basis on $\mathbb{F}_4$ — and the existence of the Frobenius map $(-)^2 : \mathbb{F}_4 \to \mathbb{F}_4 : x \mapsto x^2$, which, in this logical context is considered as a new type of modality, expressing a *galoisian undiscernability*.

The field $\mathbb{F}_4$ with four elements is the arithmetic of a square with a fixed oriented diagonal $0 \to 1$, and two other undiscernable corners α and ω, $\mathbb{F}_4 = \{0, 1, \alpha, \omega\}$, with $\alpha + \beta = \alpha\beta = 1$, in such a way that the polynomial $X^2 + X + 1$ (paradoxical i.e. without roots in $\mathbb{F}_2$) splits in $\mathbb{F}_4$. The logic of the square, i.e. the organization of the system $\mathbb{P}_4$ of functions $\mathbb{F}_4^k \to \mathbb{F}_4$, was presented in [8]; in this 'logic' several hexagonal pictures appear, which allow to understand this logic as a 'borromean logic', as a 'boolean manifold'. This logic was shown to be useful for the splitting of paradoxes and analysis of paradoxical sentences.

2.2. The cube and the question of the hexagonal symmetry of $\mathbb{P}_8$

2.2.1. Splitting of paradoxes in $\mathbb{F}_8$. Now we consider the field $\mathbb{F}_8$. This case is interesting because $\mathbb{F}_8 = \mathbb{F}_{2^3}$ is the smallest case of a 3-dim space over a field (it is the first *cubic field*) and consequently in this space we can imagine knots, borromeam links, etc. analogous to curves in $\mathbb{R}^3$.

The field $\mathbb{F}_8$ with 8 elements is the arithmetic supported by a cube with a fixed diagonal $0 \to 1$, that is to say by an oriented hexagon (see 2.3). It will be generated by 3 elements R, S, I, roots of $X^3 + X^2 + 1$ (paradoxical i.e. without roots in $\mathbb{F}_2$). We denote it by (cf. Proposition 3.6):

$$\mathbb{F}_8 = \{0, 1, R, S, I, R', S', I'\}$$

Of course the work done with $\mathbb{F}_4$ could be repeated with the Galois'field $\mathbb{F}_8$; proceeding in this way again we would split some paradoxes, observe various hexagonal pictures, and borromean objects, etc.

2.2.2. Hexagonal symmetry of $\mathbb{P}_8$. But here this question of splitting paradoxes (2.2.1) is not our direct aim. Rather we would like to study *the logic* of *the hexagon itself*, i.e. the system $\mathbb{P}_6$ of functions on 6 elements with a special central symmetry. For that we have to understand the structure of $\mathbb{P}_8$ and mainly its *hexagonal symmetry*.

A first tool is the existence on $\mathbb{F}_8$ of a *canonical* boolean logic, in which $false = 0$ and $true = 1$; so the use of these boolean functions in the presentation of the system $\mathbb{P}_8$ implicitly emphasizes the axis $0 - 1$ in the cube, and reduces symmetries of the cube to symmetries of the hexagon (see 2.3).

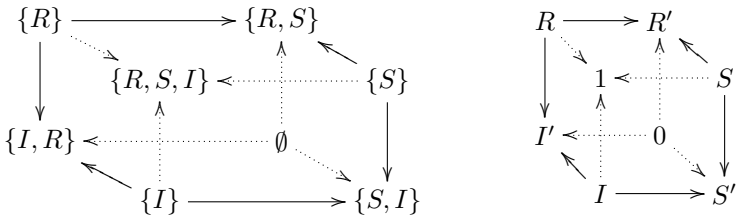
As $6 = 8 - 2 = 2^3 - 2^1$, it would be possible to consider a *hexagonal function* (2.3) as a function on $\mathbb{F}_8$ which never takes the value 0, and with value 1 if and only if one of the variables is 0 or 1; so $\mathbb{P}_6 \subset \mathbb{P}_8 = \mathbb{P}(\mathbb{F}_8)$, and we can describe $\mathbb{P}_6$ with the help of the nice structure of $\mathbb{F}_8$ which is both a field *and* a boolean algebra.

A second tool is the group of colineations of the Fano plane. The Fano plane is almost the same thing that a hexagon (cf. Remark 2.2, Remark 3.5). On one side this group is $\mathrm{PSL}_2(\mathbb{F}_7)$, and on this other side it is $\mathrm{GL}_3(\mathbb{F}_2)$ (cf. [4]). The ternary symmetry of the hexagon will be taken into account by generating this group with the 3 transvections A, B, C with circular relations (Proposition 7.1).

2.3. Hexagonal functions

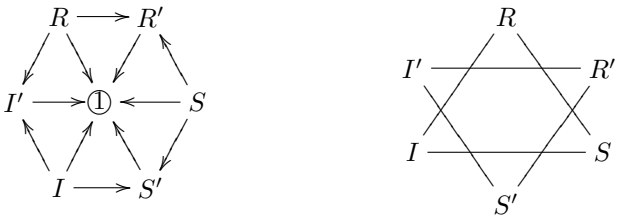
2.3.1. The hexagon in logic. We want to increase the value of a mixed logico-geometrical discipline, in which a given diagram stipulates a system of possible points of view acting on propositions as modalities. It is easy to deduce this plan from the Sesmat's approach. The very special case of a hexagonal diagram [16], [2], [3] is very fundamental, and a nice convincing modern re-examination and development is given by Jean-Yves Béziau [1]. In [7],[8], turning around the idea of hexagon, we prefer to work with the notion of *borromean object*; but the first aspect of a borromean object is its hexagonal appearance, and the second aspect is the exactness of diagonals, in some sense equivalent to the description of opposite corners as complements (as in a logical hexagon of oppositions).

2.3.2. From the cube to the hexagon, and to hexagonal functions. Jacques Lacan introduced the *RSI logic* for psychoanalysis, with R = Real, S = Symbolic, I = Imaginary, explaining that discourses work under these three modalities linked in a borromean way, as are linked Father, Son and Holly Spirit, the three hypostases of God in ChristianTrinity. In homage to Lacan, here we will used these three letters in our presentations and computations. The geometrical cube K_3 is the shape of a boolean logical cube $\mathcal{P}(\{R, S, I\})$, drawn as follows, with $R' = \{R, S\}, S' = \{S, I\}, I' = \{I, R\}$, $1 = \{R, S, I\}$, $0 = \emptyset$.



So our basic picture will be the view of the cube orthogonal to its axis $0 - 1$, i.e. the *hexagon*:

Definition 2.1. The *hexagon* is the picture



The set of elements of this hexagon which are different from 0 and 1 is denoted by $\mathcal{H} = \{R, S, I, R', S', I'\}$, and often — abusively — the hexagon itself also will be denoted by $\mathcal{H}$.
A *hexagonal function* is a function $h : \mathcal{H}^k \to \mathcal{H}$, with $k \in \mathbb{N}$, and the set of these functions is denoted by $\mathbb{P}(\mathcal{H}) = \cup_{n\in\mathbb{N}}\mathcal{H}^{\mathcal{H}^k}$; it is the Post-Malcev algebra $\mathbb{P}_6$ on 6 elements, as defined in [13] or [10].

Remark 2.2. 1 — Let us remark that, with these notations, the *complement* R^c of R is not R' but

$$R^c = S', S^c = I', I^c = R'.$$

In fact in our future computations, R' will be the *inverse* of R:

$$R' = R^{-1}, S' = S^{-1}, I' = I^{-1}.$$

2 — In Proposition 3.4 we will recover this hexagon as the Fano plane, and in fact automorphisms of this $\mathbb{F}_2$-projective plane will play a decisive part in our analysis.

Remark 2.3. As explained in 2.2.2, we could consider that

$$\mathbb{P}(\mathcal{H}) = \cup_{n\in\mathbb{N}}\mathcal{H}^{\mathcal{H}^k} \subset \cup_{n\in\mathbb{N}}\mathbb{F}_8^{\mathbb{F}_8{}^k} = \mathbb{P}(\mathbb{F}_8),$$

and so $\mathbb{P}_6$ appears as a sub-Post-Malcev algebra of $\mathbb{P}_8$. But what we do here is only to give a presentation of $\mathbb{P}_8$ which 'respects' the presence of $\mathbb{P}_6$ in $\mathbb{P}_8$; we don't claim that our generators A, B, C or the canonical logical functions are in fact in $\mathbb{P}_6$; and we don't claim that our 'hexagonal functions' i.e. functions on the hexagon (elements of $\mathbb{P}_6$) are the functions respecting the 'geometry of the hexagon'. Just we say that if someone wants to describe these last 'geometrical' functions among the functions of $\mathbb{P}_6$ then, after a precise determination of what he means by 'geometry of the hexagon', he could use our presentation of $\mathbb{P}_6$ in $\mathbb{P}_8$ with the logical functions and the A, B, C as a natural setting. Because this A, B, C presentation shows the hexagonal symmetry of $\mathbb{P}_8$.
The use of elements external to $\mathbb{P}_6$ in order to present elements of $\mathbb{P}_6$ becomes natural if we want a maximal logical component in our analysis, because the set $\mathcal{H}$ has not for cardinal a power of 2, but it could be embedded in a boolean algebra of cardinal 8 as well as the set of its elements which are different from false and truth. In this way the hexagonal symmetry of $\mathbb{P}_8$ could act on $\mathbb{P}_6$.
But in fact, reversing the problem, we precisely claim that any 'geometry of

the hexagon' will be determined by the data of any sub-algebra of $\mathbb{P}_6$ compatible with the symmetry of the A, B, C presentation (cf. Proposition 7.4). So our exclusive purpose will be to clearly understand the hexagonal presentation of $\mathbb{P}_8$, which mixes arithmetical, geometrical and logical aspects.

3. Circular presentation of arithmetic in $\mathbb{F}_8$ with R, S, I

In this section we describe the finite field with 8 elements, and we emphasize its presentation as a $\mathbb{F}_2$-algebra with a circular presentation. This presentation will be useful in the sequel, for the study of geometry and of logic. In this section we use this presentation to study third degree equations in $\mathbb{F}_8$, reducible to linear and second degree, and so with geometrical interpretations. We obtain the reduced third degree paradoxes in $\mathbb{F}_8$.

3.1. Splitting $X^3 + X^2 + 1 = 0$ and $X^3 + X + 1 = 0$

Proposition 3.1. *Let $\mathbb{F}_2 = (\{0, 1\}, +, \times)$ be the field of integers modulo 2. The polynomials $X^3 + X^2 + 1$ and $X^3 + X + 1$ are reciprocal i.e. exchanged by $X \mapsto X^{-1}$, the roots of the first are linearly independent, but the roots of the second are linearly dependent. They are the two irreducible polynomials of degree 3 over $\mathbb{F}_2$, the fields $\mathbb{F}_2[X]/(X^3 + X^2 + 1)$ and $\mathbb{F}_2[X]/(X^3 + X + 1)$ are isomorphic, with 8 elements. Both are realization of a splitting field of $X^8 - X$ over $\mathbb{F}_2$, i.e. the smallest extension of $\mathbb{F}_2$ in which $X^8 - X$ split in a product of linear factors:*

$$X^8 - X = X(X - 1)(X^3 + X^2 + 1)(X^3 + X + 1).$$

Futhermore the 'squaring' Frobenius map $(-)^2 : x \mapsto x^2$ is $\mathbb{F}_2$-linear i.e.

$$(x + y)^2 = x^2 + y^2.$$

Proof. The sum of the roots of the second polynomial is 0; and the sum of the roots of the first is 1. The squaring $(-)^2$ is linear, because we are in characteristic 2. Clearly $X^3 + X^2 + 1$ and $X^3 + X + 1$ have no root in $\mathbb{F}_2$, and, as they are of degree 3, they are irreducible, and the quotients rings are fields. The decomposition for $X^8 - X$ is proved by expansion of the right side. Then, for every element x in the field (whatever copy of it is chosen) we have $x^8 - x = 0$, and for elements $x \neq 0$ we have $x^7 = 1$, i.e. $x^{-1} = x^6$. The determination up to isomorphism of finite fields, one exactly for each cardinal p^n, for p prime and n integer, is known since 1893 [14]: it works here for $p = 2$, $n = 3$, and $2^3 = 8$. For recent classic manuals, see [12], [15]. □

Proposition 3.2. *In the field with 8 elements defined in Proposition 3.1, an element a is a root of $X^3 + X^2 + 1 = 0$ if and only if $b = a + 1$ is a root of $X^3 + X + 1 : 0$; then every element is a power of a and a power of b, with the correspondence:*

$$a = b^3, a^2 = b^6, a^3 = b^2, a^4 = b^5, a^5 = b, a^6 = b^4;$$

$$b = a^5, b^2 = a^3, b^3 = a, b^4 = a^6, b^5 = a^4, b^6 = a^2.$$

The roots of X^3+X^2+1 are a, a^2 and a^4, the powers of a^2, which are exchanged by the powers of $(-)^2$, the roots of X^3+X+1 are b, b^2 and b^4, the powers of b^2, which are exchanged by the powers of $(-)^2$.

Proof. It is easily checked. At first $(a+1)^3+(a+1)+1=0$. From $a^3=a^2+1$ we obtain $a^4=a^2+a+1$, $a^5=a+1$, $a^6=a^2+a$, $a^7=1$, and with $b=a+1$ we obtain $b=a^5$, $b^2=a^3$, $b^3=a$, etc., as announced. For the distribution of roots, we verify for a^2 that $0=a^4(a^3+a^2+1)=1+a^6+a^4=(a^2)^3+(a^2)^2+1$, and for a^4 with $a^5=b=a+1$ we get $0=a^5+a+1=a^{12}+a^8+1=(a^4)^3+(a^4)^2+1$. □

Proposition 3.3. *We consider $\mathbb{F}_2[Y]/(Y^3+Y^2+1)=\mathbb{F}_2(\alpha)$, with α an abstract root of Y^3+Y^2+1, e.g. $\alpha=Y$, and $\mathbb{F}_2[Z]/(Z^3+Z+1)=\mathbb{F}_2(\beta)$ with β an abstract root of Z^3+Z+1, e.g. $\beta=Z$. An explicit isomorphism A between these two fields and its inverse B are given by*

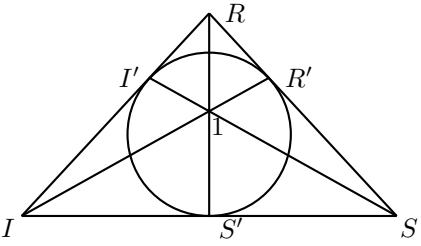
$$A(\alpha^n)=\beta^{3n}, \quad B(\beta^n)=\alpha^{5n}.$$

Proof. It results from Proposition 3.2, where both $\mathbb{F}_2(\alpha)$ and $\mathbb{F}_2(\beta)$ are realized as "the" splitting field of $X^8-X=0$, and as $\mathbb{F}_2(a)$ and $\mathbb{F}_2(b)$, with $\alpha=a$, and $\beta=b$: at this level, the maps A and B become the identity map. As $b=a+1$ and $a=b+1$, we get $B(\beta)=\alpha+1$, $A(\alpha)=\beta+1$, etc. □

3.2. The circular presentation by R, S, I

Proposition 3.4. *The projective plane over $\mathbb{F}_2$ — the Fano plane — is constructible with 7 points named $1, R, S, I, R', S', I'$, as on the picture, where are drawn 7 'straight lines' named:*

$$R^\perp=\{S,S',I\}, S^\perp=\{I,I',R\}, I^\perp=\{R,R',S\},$$
$$R'^\perp=\{R',1,I\}, S'^\perp=\{S',1,R\}, I'^\perp=\{I',1,S\},$$
$$1^\perp=\{R',S',I'\}.$$



Remark 3.5. This plane is important for us especially through its group of projective automorphisms, which is $\mathrm{G}_{168}=\mathrm{PSL}_2(\mathbb{F}_7)=\mathrm{GL}_3(\mathbb{F}_2)$. The involutions A, B, C that we will introduce in Proposition 7.1 are geometrical maps (colineations) on this plane.

Proposition 3.6. *A concrete model isomorphic to the fields in Proposition* 3.1 *is*

$$\mathbb{F}_8=\{0,1,R,S,I,R',S',I'\},$$

where the addition is described by $x+x=0$, when $x \in \mathbb{F}_8$, and by lines in the Fano plane (Proposition 3.4): if $x, y \in \mathbb{F}_8$, $x \neq y$, then $x+y=z$ is equivalent to : $\{x, y, z\}$ is one of the 7 lines in the Fano plane. So we can use the Fano plane as an addition table in $\mathbb{F}_8$, and simultaneously, by the use of exponent, as a multiplication table. This allows us to grasp $\mathbb{F}_8$ in a flash.

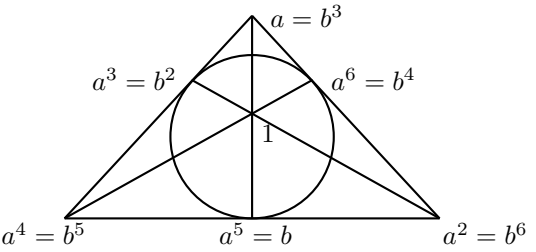
Proof. The field $\mathbb{F}_8$ can be described in multiplicative terms, as in Proposition 3.2, with the a or the b terms. Multiplying $a^3+a^2+1=0$ by powers of a we obtain:

$$a^2+a^5+a^4=0; \quad a^4+a^3+a=0; \quad a+a^6+a^2=0;$$

$$a^6+1+a^4=0; \quad a^5+1+a=0; \quad a^3+1+a^2=0;$$

$$a^6+a^5+a^3=0.$$

This allows us to replace: $R=a$, $S=a^2$, $I=a^4$, $R'=a^6$, $S'=a^5$, $I'=a^3$.



□

Proposition 3.7. *As a field of characteristic 2, the field $\mathbb{F}_8$ could be presented in a circulary symmetrical way — and we shall name this* the R, S, I presentation *— with the following relations among the elements:*

$$RSI=1, \quad RS+SI+IR=0, \quad R+S+I=1,$$

$$R^2=S, \quad S^2=I, \quad I^2=R.$$

Proof. The first line of equations expresses that R, S, I are the three roots of X^3+X^2+1, and the second line precises how the Frobenius squaring transforms them. We have to prove that this determines completely all calculations in $\mathbb{F}_8$ as a field of characteristic 2. We introduce

$$R' := I+1 = R+S, \quad S' := R+1 = S+I, \quad I' := S+1 = I+R.$$

We have $R(S+I)=SI$, $R^2(S+I)=RSI=1$, $S(S+I)=1$, and so $SI=I+1$, $SI=R'$. And then $RSI=1$ means that $RR'=1$. Similarly we have $IR=S'$, $SS'=1$, $RS=I'$, $II'=1$. Also $S+I=S'=R+1$, etc.
Products u.u' := uu' and sums u+u' are given by the tables:

$\cdot$	R	S	I	R'	S'	I'
R	S	I'	S'	1	R'	I
S	I'	I	R'	R	1	S'
I	S'	R'	R	I'	S	1
R'	1	R	I'	S'	I	S
S'	R'	1	S	I	I'	R
I'	I	S'	1	S	R	R'

$+$	R	S	I	R'	S'	I'	1
R	0	R'	I'	S	R'	I	S'
S	R'	0	S'	R	I	1	I'
I	I'	S'	0	1	S	R	R'
R'	S	R	1	0	I'	S'	I
S'	R'	I	S	I'	0	R'	R
I'	I	1	R	S'	R'	0	S
1	S'	I'	R'	I	R	S	0

□

Remark 3.8. It is easy to check that

$$R'S'I' = 1, R'S' + S'I' + I'R' = 1, R' + S' + I' = 0$$

i.e. that R', S' and I' are the roots of $X^3 + X + 1$, and that

$$I'^2 = R', R'^2 = S', S'^2 = I'.$$

With R', S', I' and these last relations another circular presentation is possible — complementary to the one with the R, S, I. But we do prefer the R, S, I, because of their linear independence (Proposition 4.1).

Remark 3.9. The conditions $R^2 = S$, $S^2 = I$, $I^2 = R$ are 'almost' not necessary. In fact the other conditions imply that $R^2 = S$ or $R^2 = I$, i.e. $(R^2+S)(R^2+I) = 0$, or $R^4+R^2(S+I)+SI = 0$, $R^4+R(RS+RI)+SI = 0$, $R\neg 4+RSI+SI = 0$, $R^4+1+R^{-1} = 0$, or $R^5+R+1 = 0$. And this formula is equivalent to $R^5(R^3 + R^2 + 1) = 0$, since we know a priori that $R^7 = 1$, from the general theory, as the degree of $X^3 + X^2 + 1$ is 3 and as $8 = 2^3$.

3.3. Linear and polynomial equations in $\mathbb{F}_8$, paradoxes in $\mathbb{F}_8$

In $\mathbb{F}_8 = \mathbb{F}_2^3$ we can discuss and solve $\mathbb{F}_2$-linear equations, and in the field $\mathbb{F}_8$ some polynomial equations in one variable with degree 1, 2, 3. We show that reduced third degree equations are paradoxical i.e. without solutions when they correspond to bijective linear maps.

Proposition 3.10. *$\mathbb{F}_8$ is a $\mathbb{F}_2$-linear space, and (R, S, I) is a basis of it (see Proposition 4.1).*
Each $\mathbb{F}_2$-linear map $f = \mathbb{F}_8 \to \mathbb{F}_8$, with $f(R) = e_1, f(S) = e_2, f(I) = e_3$, is given by a unique expression

$$f(u) = au^4 + bu^2 + cu.$$

The discussion of the equation $f(u) = u'$ comes back to a the discussion of a system in $\mathbb{F}_8^3$ with parameter and unknown in $\mathbb{F}_2$.

Proof. Clearly $m(-)$, with $m \in \mathbb{F}_8$ and $(-)^2$ are linear, and so $f(u) = au^4 + bu^2 + cu$ is linear. Conversely, given a $\mathbb{F}_2$-linear map $f : \mathbb{F}_8 \to \mathbb{F}_8$ we can find $a, b, c \in \mathbb{F}_8$ such that $f(u) = au^4 + bu^2 + cu$, i.e. solution of the system

$$aR^4 + bR^2 + cR = f(R); aS^4 + bS^2 + cS = f(S); aI^4 + bI^2 + cI = f(I),$$

because this $\mathbb{F}_8$-linear system, where $\mathbb{F}_8$ is a commutative field, has for determinant 1, and the solutions can be expressed via the determinant; we find

$$a = e_2R + e_3S + e_1I;$$
$$b = e_3R + e_1S + e_2I;$$
$$c = e_1R + e_2S + e_3I.$$

Let us remark that in any case, with $u = xR + yS + zI$, $x, y, z \in \{0, 1\}$, $u' = x'R + y'S + z'I$, $x', y', z' \in \{0, 1\}$, the linear equation

$$au^4 + bu^2 + cu = u',$$

with $a, b, c \in \mathbb{F}_8$ is equivalent to the following system, with $x', y', z' \in \{0, 1\}$:

$$cx + ay + bz = x'; \quad bx + cy + az = y'; \quad ax + by + cz = z',$$

with determinant $(a+b+c)(a^2+b^2+c^2+ab+bc+ca)$, and there is a unique solution if and only if: $a + b + c = 1$ and $a^2 + b^2 + ab + a + b + 1 \neq 0$, and the solution $(x_1, y_1, z_1) \in \mathbb{F}_8^3$ given by Cramer's formulas is in fact in $\mathbb{F}_2^3$, i.e. is such that $x_1^2 = x_1$, $y_1^2 = y_1$, $z_1^2 = z_1$.

□

Proposition 3.11. *Each $\mathbb{F}_2$-linear form on $\mathbb{F}_8$, $f = \mathbb{F}_8 \to \mathbb{F}_2$ is given by scalar product with a vector c (as introduced in Proposition 4.1):*

$$f(u) = < c, u > := \mathrm{tr}(cu) = c^4u^4 + c^2u^2 + cu.$$

Proof. The map $< c, - >$ is linear. For a linear form we need $f(u) \in \{0, 1\}$ i.e. for every u, $f(u)^2 = u$, i.e. $b^2u^4 + c^2u^2 + a^2u = au^4 + bu^2 + cu$, i.e. $b = c^2$, $a = c^4$. □

Proposition 3.12. *With the notations of Proposition 3.10, let $f : \mathbb{F}_8 \to \mathbb{F}_8$ be a $\mathbb{F}_2$-linear map given by*

$$f(u) = au^4 + bu^2 + cu.$$

This f is bijective if and only if

$$\Delta := a^7 + b^7 + c^7 + abc(a^3b + b^3c + c^3a) \neq 0.$$

If f is bijective, its inverse f^{-1} is given by:

$$f^{-1}(v) = lv^4 + mv^2 + nv,$$

with l, m, n polynomial functions of e_1, e_2, e_3, and rational functions of a, b, c.

Proof. f is bijective if and only if (e_1, e_2, e_3) is a basis, i.e. if and only if $[e_1, e_2, e_3] = 1$ (cf. Proposition 4.4). Then f^{-1} is the map sending e_1, e_2, e_3 on R, S, I, i.e. is given by $f^{-1}(v) = lv^4 + mv^2 + nv$, with the system of equations:

$$le_1^4 + me_1^2 + ne_1 = R; \quad le_2^4 + me_2^2 + ne_2 = S; \quad le_3^4 + me_3^2 + ne_3 = I,$$

with determinant 1, and the solutions are given by the Cramer's formulas:

$$l = (e_2^2e_3 + e_2e_3^2)R + (e_3^2e_1 + e_3e_1^2)S + (e_1^2e_2 + e_1e_2^2)I,$$
$$m = (e_2^4e_3 + e_2e_3^4)R + (e_3^4e_1 + e_3e_1^4)S + (e_1^4e_2 + e_1e_2^4)I,$$

$$n = (e_2^4e_3^2 + e_2^2e_3^4)R + (e_3^4e_1^2 + e_3^2e_1^4)S + (e_1^4e_2^2 + e_1^2e_2^4)I.$$

Also, writing $f^{-1}(f(u)) = u$ we have the system

$$lc^4 + mb^2 + na = 0; \quad la^4 + mc^2 + nb = 0; \quad lb^4 + ma^2 + nc = 1.$$

This system has a unique solution if its determinant Δ is $\neq 0$, and the solution is given by Cramer's formulas:

$$l = \frac{b^3 + c^2a}{\Delta}; \quad m = \frac{a^5 + bc^4}{\Delta}; \quad n = \frac{c^6 + a^4b^2}{\Delta}.$$

□

Proposition 3.13. *In $\mathbb{F}_8$ we consider the second degree equation*

$$ax^2 + bx + c = 0, \quad \textit{with} \quad a \neq 0.$$

1— If $a = 0$ and $b \neq 0$ there is a unique solution $x_1 = b^6c$.
2— If $a \neq 0$ and $b = 0$ there is a unique solution $x_1 = a^3c^4$.
3— If $a, b \neq 0$ and $c = 0$, there are two solutions $x_1 = 0$ and $x_2 = a^6b$.
4— If $a, b, c \neq 0$, there are solutions if and only if $a^3b^3c^3 + ac + b^2 = 0$, and these solutions are:

$$x_1 = a^5b^3c^6, \quad x_2 = ab^4c^2.$$

Proof. The standard method with $\Delta = b^2 - 4ac$ and division by $2a$ is not available in characteristic 2. Rather we introduce $x = \frac{b}{a}y$, and the equation becomes $y^2 + y = \frac{ac}{b^2} := d$, $d \neq 0$.
For any y, we have $(y^2 + y)^4 + (y^2 + y)^2 + (y^2 + y) = 0$, and the necessary condition: $d^4 + d^2 + d = 0$, i.e. $d^3 = d + 1$, and the announced condition.
In this case $d^{12} = d^4+1$, one solution is $y_1 = d^{-1} = d^6$, the other is $y_2 = y_1+1$, that is to say that $x_1 = a^5b^3c^6$, $x_2 = x_1 + \frac{b}{a} = ab^4c^2$.
Proposition 4.5 and Proposition 4.6 give a geometric interpretation of the second degree equation. □

Proposition 3.14. *In $\mathbb{F}_8$ the third degree equation*

$$ax^3 + bx^2 + cx + d = 0$$

can be solved as follows:
1 — If $a = 0$, discussion and solution are given in Propositions 3.13.
2— If $a \neq 0$, with $x = u + a^6b$ and multiplying by u we obtain a linear equation as in Proposition 3.10*:*

$$au^4 + (a^6b^2 + c)u^2 + (a^6bc + d)u = 0$$

Example. 1 — Generally the equation

$$Ru^4 + Su^2 + Iu = u'$$

has no solution. Applying Proposition 3.10 we obtain that this equation has a solution if and only $u' = 0$ or 1, and the solution is $u = 0$ or 1.
2 — The equation

$$Ru^2 + Su + I = 0$$

has no solution, as we see by Proposition 3.13.
3 — The equation

$$u^2 + Su + 1 = 0$$

admits 2 solutions, R and R'.

Proposition 3.15. *If $f(u) = au^4 + bu^2 + cu$ is a bijective $\mathbb{F}_2$-linear map on $\mathbb{F}_8$, with $a \neq 0$, then the polynomial $au^3 + bu + c = 0$ has no root in $\mathbb{F}_8$, and so it expresses a paradox in $\mathbb{F}_8$. In this way we exactly get the different reduced (= without term in degree 2) third degree equations without solutions in $\mathbb{F}_8$, which are less than 168.*

Proof. f is bijective if and only if $f(u) = 0$ has only 0 as a solution. The second point results from the fact that $\mathrm{GL}_2(\mathbb{F}_2)$ is of cardinal 168. □

4. Construction of $\mathbb{F}_8$ from its 3-dimensional vectorial geometry and its 3-circular boolean logic

We develop the 3 dimensional geometry of $\mathbb{F}_8$, starting from the circular presentation with R, S, I, and we introduce the '*canonical*' boolean algebra on $\mathbb{F}_8$. Then we re-construct the multiplication of the field, starting from the geometry (scalar, cross, and mixed products), or from the logic (conjunction and negation), with the help of the Frobenius squaring $(-)^2$. This allows us to prove that any function on $\mathbb{F}_8$ is a boolean combination of '*avatars*' of its variables. From the logical point of view, the squaring u^2 of u is a kind of modality, as well as the 6 associated avatars $u^{(i)}$, with $2 \leq i \leq 7$. These avatar-like operations $(-)^{(i)}$ are organized in a commutative monoïd $\mathbb{A}$. So the full logic of $\mathbb{F}_8$ appears as a boolean logic with a 3-circular automorphism, as well as with modalities coming from the action of $\mathbb{A}$.

4.1. Geometrical tools in $\mathbb{F}_8$

4.1.1. Scalar, cross and mixed products.

Proposition 4.1. *$\mathbb{F}_2$ is a sub-field of the field $\mathbb{F}_8$, and so $\mathbb{F}_8$ is an $\mathbb{F}_2$-algebra of dimension 3. A basis is given by $\kappa = (R, S, I)$. Given $u = xR + yS + zI$ and $u' = x'R + y'S + z'I$, with $x, y, z, x', y', z' \in \mathbb{F}_2$, we define the* trace *and the* scalar product *by*

$$\mathrm{tr}(u) = x + y + z, \quad < u, u' >= xx' + yy' + zz'.$$

We have $\mathrm{tr}(u) =< u, u >$, and the values:

$$\mathrm{tr}(u) = 0 \Leftrightarrow u \in \{0, R', S', I'\}, \quad \mathrm{tr}(u) = 1 \Leftrightarrow u \in \{1, R, S, I\}.$$

We introduce the cross product *(also named crossed product or vector product) and the* mixed product *(also named scalar triple product) by:*

$$u \times u' = (yz' - zy')R + (zx' - xz')S + (xy' - yx')I,$$

$$[u, u', u''] =< u, u' \times u'' >=< u \times u', u'' > .$$

Then (u, u', u'') *is a basis of* $\mathbb{F}_8$ *over* $\mathbb{F}_2$ *if and only if* $[u, u', u''] = 1$. *Furthermore we have (*double cross product *formula):*

$$u \times (u' \times u'') =< u, u'' > u' - < u, u' > u''.$$

Proof. There is no linear relation between R, S and I: $R, S, I \neq 0$, $R + S = R' \neq 0$, $S+I = S' \neq 0$, $I+R = I' \neq 0$, $R+S+I = 1 \neq 0$. For $\mathrm{tr}(u) =< u, u >$ we have $x^2 = x$, $y^2 = y$, $z^2 = z$. Clearly tr is linear, $<,>$ and $\times$ are bilinear, both symmetrical (we are in characteristic 2). It is elementary to check that if $(x, y, z) \neq (0, 0, 0)$ and $(x', y', z') \neq (0, 0, 0)$ then $u \times u' = 0$ if and only if $u = u'$. We have $[u, u', u''] \neq 1$ exactly if $[u, u', u''] = 0$, and this means that $u = 0$, or $u \neq 0$ and $u = u'$, or $u \neq 0$ and $u = u''$, or $u \neq 0$ and $u = u' + u''$. Another proof results from the formula for $[u, u', u'']$ in Proposition 4.3. The last formula could be verified directly. □

Proposition 4.2. *As a linear space of characteristic* 2 *equipped with a bilinear (anti)symmetric multiplication* $\times$, $\mathbb{F}_8$ *could be presented in a circulary symmetrical way — and we shall name this* the R, S, I linear multiplicative presentation *— by the following relations among the elements:*

$$R \times S = I, \quad S \times I = R, \quad I \times R = S.$$

Then, because of the linear relations

$$R' = R + S, \quad S' = S + I, \quad I' = I + R, \quad 1 = R + S + I,$$

the cross product $\times$ *is given by the table:*

$\times$	R	S	I	R'	S'	I'	1
R	0	I	S	I	S'	S	S'
S	I	0	R	I	R	I'	I'
I	S	R	0	R'	R	S	R'
R'	I	I	R'	0	1	1	R'
S'	S'	R	R	1	0	1	S'
I'	S	I'	S	1	1	0	I'
1	S'	I'	R'	R'	S'	I'	0

4.1.2. Geometrical operations from the operations of the field.

Proposition 4.3. *The space* $\mathbb{F}_8$ *yields the* $\mathbb{F}_2$*-linear map of* squaring $(-)^2$ *(Frobenius map). For any* u, *the elements* u, u^2, u^4 *are said to be* conjugate, *they are:*

$$u = xR + yS + zI, \quad u^2 = zR + xS + yI, \quad u^4 = yR + zS + xI,$$

and their sum is the trace *of* u*:*

$$\mathrm{tr}(u) = u + u^2 + u^4 = x + y + z.$$

The scalar product is the trace of the product:

$$< u, u' >= \mathrm{tr}(uu') = uu' + (uu')^2 + (uu')^4 = xx' + yy' + zz',$$

and if $u = xR + yS + zI$, *then* $x = \mathrm{tr}(uR), y = \mathrm{tr}(uS), z = \mathrm{tr}(uI)$.
The cross product and mixed product from Proposition 4.1 *are given by*

$$u \times u' = (uu'(u+u'))^2,$$

$$[u, u', u''] = uu'u''(u+u')(u'+u'')(u''+u)(u+u'+u'').$$

So, all the vectorial analysis in $\mathbb{F}_8$ *according to the tools in Proposition* 4.1 *is expressible in terms of polynomial functions with coefficients in* $\mathbb{F}_2$.

Proof. We have $\mathrm{tr}(uR) = xR + x^2S + x^4I$, $\mathrm{tr}(uR)R = u^2 + u^4 + u^4R + (u+u^2)S$; with similar formulas for $\mathrm{tr}(uS)S$ and $\mathrm{tr}(uI)I$, the sum of the three is u.
We compute $(yz' - y'z)R = (yz' + y'z)R$ as $(\mathrm{tr}(uS)\mathrm{tr}(u'I) + \mathrm{tr}(u'S)\mathrm{tr}(uI))R$, and we obtain

$$(yz' - y'z)R = (u+u')S' + (uu'^3 + u'u^3)S + (u^3 + u'3)I'.$$

With similar formulas for the other two terms, the sum of the three provides the announced formula.
If we use the formulas for the scalar product and for the cross product

$$[u, u', u''] = u(u'^2u''^4 + u'^4u''^2) + u'(u''^2u^4 + u''^4u^2) + u''(u^2u'^4 + u^4u'^2),$$

and this is also given by the proposed formula for the mixed product. □

Proposition 4.4. *We have*

$$[u, u', u''] = \begin{vmatrix} x & x' & x'' \\ y & y' & y'' \\ z & z' & z'' \end{vmatrix} = \begin{vmatrix} u & u' & u'' \\ u^2 & u'^2 & u''^2 \\ u^4 & u'^4 & u''^4 \end{vmatrix} \in \{0, 1\}.$$

The value is 1 *if and only if* (u, u', u'') *is a basis.*

Proof. The first determinant is equivalent to the definition of $[u, u', u'']$ — and it is in $\{0, 1\}$, and the second is equivalent to the last formula in the previous proof. Let us remark that another determinant expression for $[u, u', u'']$ — the so called *conjunctive determinant* of Definition 4.13 — will be obtained in Proposition 4.14. □

4.1.3. The equation $a \times u = b$.

Proposition 4.5. *In* $\mathbb{F}_8$, *let* $a \neq 0, b \neq 0$; *the equation*

$$a \times u = b.$$

has a solution if and only if $< a, b >= 0$, *and then there are two solutions:*

$$u_1 = a^4b^3, \quad u_2 = a^2b.$$

Proof. If $a \times u = b$, then $0 = [a, a, u] =< a, b >$, and the condition is necessary. For the converse, using the double cross product formula (in Proposition 4.1), with $u_0 = a \times b$ we have $a \times (a \times b) =< a, a > b$,and if $< a, a > \neq 0$ we get a solution $u'_1 =< a, a >^{-1} a \times b$, and another $u'_2 = u'_1 + a$. But if $< a, a >= 0$ (i.e. if $a = 1, R', S'$ or I') this method fails. So if we start with the algebraic formula for $\times$ given in Proposition 4.3, and $(au(a+u))^2 = b$, we obtain $au(a+u) = b^4$, $au^2 + a^2u = b^4$, and with Proposition 3.13 we obtain solutions if and only if $(aa^2b^4)^3 + (ab^4) + (a^2)^2 = 0$, or equivalently if

$(ab)^4 + (ab)^2 + ab = 0$. Then the solutions are $u_1 = a^5(a^2)^3(b^4)^6 = a^4b^3$ and $u_2 = a(a^2)^4(b^4)^2 = a^2b$. Of course $u_2 = u_1 + a$. □

Proposition 4.6. *In $\mathbb{F}_8$, a convenient change of variable $x = \lambda u$ transforms any second degree equation $ax^2 + bx + c = 0$ into a vectorial division problem $A \times u = B$, and so the equation obtains a geometrical meaning. Conversely the multiplication and the algebraic structure of field of $\mathbb{F}_8$, not only help solving algebraic equations, but also geometrical linear problems.*

Proof. Propositions 3.13 and 4.5 provide a passage between $ax^2 + bx + c = 0$ and $A \times u = B$: with $x = \frac{b}{a}y$ and $u = av$ these equations are equivalent to $y^2 + y = \frac{ac}{b^2}$ and $u^2 + u = (AB)^4$, and if we take A and B such that $AB = a^2b^3c^2$, the second degree equation is equivalent to the vectorial division, the correspondence between solutions being given by $x_i = \frac{b}{aA}u_i$, for $i = 1, 2$. □

4.2. The canonical logic of $\mathbb{F}_8$

4.2.1. Definition of $\wedge$ and $\neg$.

Proposition 4.7. *If we define the* canonical conjunction $\wedge$*, the canonical disjunction $\vee$, and the* canonical negation $\neg$ *on $\mathbb{F}_8$ by*

$$u \wedge u' = xx'R + yy'S + zz'I, \quad u \vee u' = (x \vee x')R + (y \vee y')S + (z \vee z')I,$$
$$\neg u = (x+1)R + (y+1)S + (z+1)I,$$

then we obtain on $\mathbb{F}_8$ a structure of boolean algebra, with atoms R, S and I, with 'false' $= 0$ and 'truth' $= 1$, with also $+$ as 'symmetric difference' i.e.

$$u + u' = (u \wedge \neg u') \vee (\neg u \wedge u').$$

Proof. Obviously the structure is boolean, because it is componentwise in $\mathbb{F}_2$; it could be named 'canonical' because it is associated to the very special basis (R, S, I) characterized among all the bases by an arithmetical property (see Proposition 6.2). The $\neg u = u + 1$ results from $1 = R + S + I$. □

4.2.2. Relations between the logic, the field structure, and the geometry.

Proposition 4.8. *If we dispose of the squaring $(-)^2$, of the canonical conjunction $\wedge$ and of the cross product $\times$, then the product of $\mathbb{F}_8$ is:*

$$uu' = (u \wedge u')^2 + u \times u' + (u \times u')^2.$$

The boolean operations are expressible with the field operations:

$$u \wedge u' = u^4u'^4 + u^4u'^2 + u^2u'^4 + u^2u' + uu'^2, \quad \neg u = u + 1$$
$$u \vee u' = u^4u'^4 + u^4u'^2 + u^2u'^4 + u^2u' + uu'^2 + u + u',$$
$$u \Rightarrow u' = u^4u'^4 + u^4u'^2 + u^2u'^4 + u^2u' + uu'^2 + u' + 1.$$

Proof. For this relation between $u \wedge u'$, uu', and $u \times u'$ we compute

$$u^2u' + uu'^2 = uu'(u+u') = (u \times u')^4 = (zx' - z'x)R + (xy' - x'y)S + (yz' - y'z)I,$$

and also $(u^2u' + uu'^2)^2$ and $(u^2u' + uu'^2)^4$, and then we verify the formula for uu', or, equivalently, the formula for $u \wedge u'$ (using $u^8 = u$, $v^8 = v$). Then $u \vee u' = u \wedge u' + u + u'$, $u \Rightarrow u' = u \wedge u' + u + 1$. □

Remark 4.9. In principle, our formula $uu' = (u \wedge u')^2 + u \times u' + (u \times u')^2$ in Proposition 4.7 provides a construction respectful of the circular symmetry or symmetry of the situation: on the one hand the $\times$ is circular ... and symmetric — $R \times S = I, S \times I = R, I \times R = S$, and $R \times S = S \times R, ...$, the $(-)^2$ is circular — $R^2 = S, S^2 = I, I^2 = R$; on the other hand the $\wedge$ is symmetric $R \wedge R = R, R \wedge S = S \wedge R = 0, ...$ It is a kind of decomposition of the product in circular and non-circular components.

Proposition 4.10. *We have*

$$< u, u' >= \mathrm{tr}(u \wedge u').$$

Proof. From the formula for uu' in Proposition 4.8 we get by addition of uu', $(uu'^2$ and $(uu')^4$, $< u, u' >= u \wedge u' + (u \wedge u')^2 + (u \wedge u')^4 = \mathrm{tr}(u \wedge u')$. □

Remark 4.11. The value of $< u, u' >$ depends only on $u \wedge u'$, and the canonical conjunction could be seen as an enriched scalar product; so it could be considered as a kind of 'geometrical operation'. The operation $(-)^2$ also has a geometrical meaning : it is a rotation $R \mapsto S \mapsto I \mapsto R$. Hence our formula $uu' = (u \wedge u')^2 + u \times u' + (u \times u')^2$ is a geometrical reconstruction of the field law in the 3-dim space $\mathbb{F}_8$, which is possible because of the characteristic 2. Of course in characteristic 0 the situation would be completely different, and it is well known that it is impossible to construct a field structure on $\mathbb{R}^3$; rather the cross product in $\mathbb{R}^3$ could be understood as a part of a field structure on $\mathbb{R}^4$ (the quaternion field). The same can be do with $\mathbb{F}_2^3$ in $\mathbb{F}_2^4$, but also in addition to that, in characteristic 2 the situation could be tighten in 3 dimensions (as we have seen in the field $\mathbb{F}_8$).

Proposition 4.12. *In* $\mathbb{F}_8$ *the operation* $(-)^2$ *commutes with* $\times$, $+$, $\wedge$, *and* $\neg$*:*

$$(u \times u')^2 = u^2 \times u'^2, \quad (u + u')^2 = u^2 + u'^2,$$

$$(u \wedge u')^2 = u^2 \wedge u'^2, \quad (\neg u)^2 = \neg(u^2).$$

So $(-)^2$ *is linear and boolean.*

Proof. We have $u \times u' = (yz - zy')R + (zx' - xz')S + (xy' - yx')I$, $(u \times u')^2 = (xy' - yx')R + (yz' - zy')S + (zx' - xz')I$, which is equal to $u^2 \times u'^2$ with $u^2 = zR + xS + yI$ and $u'^2 = z'R + x'S + y'I$. For the second formula the two members are equal to $zz'R + xx'S + yy'I$. □

Definition 4.13. In $\mathbb{F}_8$ equipped with $\wedge$ and $+$, we define the *conjunctive determinant* of 3 elements $u, u', u'' \in \mathbb{F}_8$ as $\det_\wedge(u, u', u'') = u \wedge u'^4 \wedge u''^2 + u^4 \wedge u' \wedge u''^2 + u^2 \wedge u' \wedge u''^4 + u \wedge u'^2 \wedge u''^4 + u^4 \wedge u'^2 \wedge u'' + u^2 \wedge u'^4 \wedge u'',$

$$= \begin{vmatrix} u & u' & u'' \\ u^2 & u'^2 & u''^2 \\ u^4 & u'^4 & u''^4 \end{vmatrix}_\wedge ,$$

this notation meaning that in order to expand this 'determinant', we have to use $\wedge$ instead of product.

Proposition 4.14. *In the $\mathbb{F}_8 = \mathbb{F}_{2^3}$, equipped with squaring $(-)^2$ and conjunction $\wedge$, the field product is*

$$uu' = u^2 \wedge u'^2 + u \wedge u'^4 + u^4 \wedge u' + u^4 \wedge u'^2 + u^2 \wedge u'^4,$$

the cross product is

$$u \times u' = u^4 \wedge u'^2 + u^2 \wedge u'^4,$$

the scalar product is

$$< u, u' >= u \wedge u' + u^2 \wedge u'^2 + u^4 \wedge u'^4,$$

and the mixed product is the conjunctive determinant from Definition 4.13*:*

$$[u, u', u''] = \det_\wedge(u, u', u'').$$

Proof. The formula $u \wedge u' = u^4u'^4 + u^4u'^2 + u^2u'^4 + u^2u' + uu'^2$ from Proposition 4.7 will be completely 'reversed', with an expression of uu' as a composition of $\wedge$ and $(-)^2$; just we have to add the following:

$$u^2 \wedge u'^2 = uu' + uu'^4 + u^4u' + u^4u'^2 + u^2u'^4,$$
$$u \wedge u'^4 + u^4 \wedge u' = u^4u' + uu'^4,$$
$$u^4 \wedge u'^2 + u^2 \wedge u'^4 = u^4u'^2 + u^2u'^4.$$

The last formula also implies the announced formula for $u \times u'$.
For the scalar product we expand $uu' + u^2u'^2 + u^4u'^4$. For the mixed product we expand $< u, u' \times u'' >=< u, u'^4 \wedge u''^2 + u'^2 \wedge u''^2 >$, assuming the commutations from Proposition 4.12: $[u, u', u''] = u \wedge u'^4 \wedge u''^2 + u^4 \wedge u' \wedge u''^2 + u^2 \wedge u' \wedge u''^4 + u \wedge u'^2 \wedge u''^4 + u^4 \wedge u'^2 \wedge u'' + u^2 \wedge u'^4 \wedge u''$, i.e. the announced conjunctive determinant (cf. Definition 4.13). □

Proposition 4.15. *We have*

$$Ru = R' \wedge u^4 + S' \wedge u^2 + I \wedge u,$$

and the squared boolean expression of geometrical operations:

$$R \times u = S \wedge u^4 + I \wedge u^2,$$
$$< R, u >= I \wedge u^4 + S \wedge u^2 + R \wedge u.$$

Proof. A consequence of formulas in Proposition 4.14. □

5. Presentation of $\mathbb{P}_8$ by boolean combination of logical avatars

5.1. From powers of u to sums of conjunctions of u, u^2, u^4

Proposition 5.1. *Given $u \in \mathbb{F}_8$ we can express powers of u as sums of conjunctions of the powers u, u^2, u^4:*

$$u = u, u^2 = u^2, u^3 = u + u^4 + u \wedge u^2, u^4 = u^4, u^5 = u^2 + u^4 + u \wedge u^4,$$
$$u^6 = u + u^2 + u^2 \wedge u^4, u^7 = (u + u^2 + u^4) + (u \wedge u^2 + u^2 \wedge u^4 + u^4 \wedge u) + u \wedge u^2 \wedge u^4;$$

And conversely the previous conjunctions are polynomials:

$$u \wedge u^2 = u + u^3 + u^4, u^2 \wedge u^4 = u + u^2 + u^6, u^4 \wedge u = u^2 + u^4 + u^5,$$
$$u \wedge u^2 \wedge u^4 = u + u^2 + u^3 + u^4 + u^5 + u^6 + u^7.$$

Proof. With the formula for uu' (Proposition 4.14), and the commutation of $(-)^2$ with $\wedge$ (Proposition 4.12), we expand $u^3 = uu^2$, $u^5 = uu^4$, $u^6 = u^2u^4$, and $u^7 = u^6u$. □

5.2. Variant with cross product

Proposition 5.2. *We have:*

$$u \wedge u^2 = u^4 + u \times u^2, \quad u^2 \wedge u^4 = u + u^2 \times u^4, \quad u^4 \wedge u = u^2 + u^4 \times u.$$

Proof. From Proposition 4.14 with have $u \times u' = u^4 \wedge u'^2 + u^2 \wedge u'^4$, and we obtain $u \times u^2$, etc. □

5.3. Conjunctive avatars

Definition 5.3. For u a variable on $\mathbb{F}_8$, the set of *conjunctive avatars* or *avatars* of u is the set of functions

$$\mathbb{A}(u) = \{u, u^2, u^4, u \wedge u^2, u^2 \wedge u^4, u^4 \wedge u, u \wedge u^2 \wedge u^4\},$$

and they can be expressed with product or with cross products (Proposition 5.1 and Proposition 5.2).
In fact we have:

$$\mathbb{A}(0) = \{0\}, \mathbb{A}(1) = \{1\},$$

$$\mathbb{A}(R) = \mathbb{A}(S) = \mathbb{A}(I) = \{0, R, S, I\},$$

$$\mathbb{A}(R') = \mathbb{A}(S') = \mathbb{A}(I') = \{0, R, S, I, R', S', I'\}.$$

Our notations for avatars of u, or elements of $\mathbb{A}(u)$, are: $u^{(1)} = u, u^{(2)} = u^2, u^{(3)} = u \wedge u^2, u^{(4)} = u^4, u^{(5)} = u \wedge u^4, u^{(6)} = u^2 \wedge u^4, u^{(7)} = u \wedge u^2 \wedge u^4$. And also we introduce the notation $u^{(0)} = u^0 = 1$.

Proposition 5.4. *The 'avatarian' functions $(-)^{(i)}$ in Definition* 5.3 *are organized in a commutative monoïd $\mathbb{A}$ given by the table:*

∘	1	2	4	3	5	6	7
1	1	2	4	3	5	6	7
2	2	4	1	6	3	5	7
4	4	1	2	5	6	3	7
3	3	6	5	7	7	7	7
5	5	3	6	7	7	7	7
6	6	5	3	7	7	7	7
7	7	7	7	7	7	7	7

Proof. We have just to check the compositions. For the associativity, in the expression $a \circ (b \circ c) = (a \circ b) \circ c$, both sides are equal to 7 if one of the a, b, c is 7, or if two of them are in $\{3, 5, 6\}$; in the other cases the compositions are multiplications of numbers modulo 7, so is associative. □

5.4. Construction of $\mathbb{P}_8$

5.4.1. $\mathbb{P}_8$ by polynomial expressions.

Proposition 5.5. *Any function $Z : \mathbb{F}_8^k \to \mathbb{F}_8$ is a polynomial with variables $u_1, u_2, \ldots, u_k$ with coefficients in $\mathbb{F}_8$.*

Proof. We know that if $u - w \neq 0$, then $(u-w)^7 = 1$, and then for any $w \in \mathbb{F}_8$ the *indicator function* of w is the polynomial function

$$[w](u) = 1 - (u-w)^7 = \begin{cases} 1 & \text{if } u = w, \\ 0 & \text{if } u \neq w. \end{cases}$$

Then if $E \subseteq \mathbb{F}_8$, the *indicator function* or the *characteristic function* of E is the sum

$$[E](u) = \sum_{w \in E} [w](u) = \begin{cases} 1 & \text{if } u \in E, \\ 0 & \text{if } u \notin E. \end{cases}$$

and more generally, when $k = 1$, for an arbitrary function Z we have

$$Z(u_1) = \sum_{z \in \mathbb{F}_8} \sum_{\{w \in \mathbb{F}_8; Z(w) = z\}} z[w](u_1),$$

if $k = 2$, then Z is given by

$$Z(u_1, u_2) = \sum_{z \in \mathbb{F}_8} \sum_{\{(w_1, w_2) \in {\mathbb{F}_8}^2; Z(w_1, w_2) = z\}} z[w_1](u_1) z[w_2](u_2),$$

expression in which in fact

$$z[w_1](u_1) z[w_2](u_2) = z \wedge [w_1](u_1) \wedge z[w_2](u_2),$$

as the functions $[u_1]$ and $u_2]$ are with values in $\{0, 1\}$. Let us remark that every function $Z : A^k \to A$ on a commutative unitary ring A is polynomial, if and only A is a finite field [9]; it is the case of $\mathbb{F}_8$. We remark that the point in the Heisler's theorem is that if A is a finite unitary commutative ring and if the indicator of 1, i.e. $[1](u)$ is polynomial, then as $[1](0) = 0$, we have $[1](u) = ug(u)$ with $g(u)$ a polynomial, and then if $u \neq 0$ we have $ug(u) = 1$, i.e. $g(u)$ is an inverse of u. Here we just need that $[1](u) = 1 - (1-u)^7$. □

5.4.2. $\mathbb{P}_8$ by sums of conjunctions of avatars and constants.

Proposition 5.6. *Any function $Z : \mathbb{F}_8^k \to \mathbb{F}_8$ with variables $u_1, u_2, \ldots, u_k$ is a sum of conjunctions of constants in $\mathbb{F}_8$ and the various u_i, ${u_i}^2$ and ${u_i}^4$, $1 \leq i \leq k$.*
For example in the case $k = 2$ any function Z has a presentation where $d_{i,j} \in \{0, 1, R, S, I\}$, $0 \leq i, j \leq 7$:

$$Z(u_1, u_2) = \sum_{i,j} d_{i,j} \wedge {u_1}^{(i)} \wedge {u_2}^{(j)}.$$

So the full logic of $\mathbb{F}_8$, i.e. the Post-Malcev full iterative algebra $\mathbb{P}_8 = \mathbb{P}(\mathbb{F}_8) = \bigcup_{n \geq 1} {\mathbb{F}_8}^{{\mathbb{F}_8}^n}$ of all functions of all arities on $\mathbb{F}_8$ (as defined in [13] *and* [10]*), is generated by its canonical boolean operations $\wedge$ and $\neg$, the 3 constant functions R, S, I* and *the 3-circular automorphism $(-)^2$.*

Proof. It is a consequence of Proposition 5.5 and details in its proof, and Proposition 4.14. Any monomial $cu_1{}^{n_1}u_2{}^{n_2}...$ in Z in 5.5 is reducible to the case where $n_j \leq 7$, and we apply the formula for the product in 4.14, using commutation of $(-)^2$ with $\wedge$ (Proposition4.12). For example any monomial $cu_1{}^m u_2{}^n$ is a sum of terms of the form $d \wedge (u_1{}^{p_1} \wedge u_1{}^{p_2} \wedge u_1{}^{p_3} \wedge u_2{}^{q_1} \wedge u_2{}^{q_2} \wedge u_2{}^{q_3})$, with $p_i, q_j \in \{0, 1, 2, 4\}$. This is explicitly done with Proposition 5.1. See also Proposition 4.15.
A variant is to use of $Z(u_1, u_2) = \sum_{Z(w_1,w_2)=z} z \wedge [w_1](u_1) \wedge z[w_2](u_2)$, and to represent directly each indicator $[w]$ with $\wedge$, with Proposition 5.1 to expand $[w](u) = 1 + (u - w)^7$. But also we have

$$u \wedge u^2 \wedge u^4 = [1](u), \quad \text{and} \quad (u+w+1) \wedge (u+w+1)^2 \wedge (u+w+1)^4 = [w](u).$$

The fact that the coefficients $d_{i,j}$ could be limited to values $0, 1, R, S, I$ results from $R' = R + S, S' = S + I, I' = I + R$. □

5.4.3. $\mathbb{P}_8$ by sums of products by constants of conjunctions of avatars.

Proposition 5.7. *With the hypothesis and notations of Proposition* 5.6*, every function could be written as*

$$Z(u_1, u_2) = \sum_{i,j} c_{i,j}(u_1{}^{(i)} \wedge u_2{}^{(j)}),$$

where $c_{i,j} \in \{0, 1, R, S, I\}$, $0 \leq i, j \leq 7$*, i.e. with canonical boolean operations* $\wedge$ *and* $\neg$*, the* 3 *bijective linear functions* $R^{\cdot} : w \mapsto Rw, S^{\cdot} : w \mapsto Sw, I^{\cdot} : w \mapsto Iw$ and *the* 3*-circular automorphism* $(-)^2$.

6. Auto-dual bases, change of bases in $\mathbb{F}_8$, R, S, I borromean generations of $\mathrm{GL}_3(\mathbb{F}_2)$ and of $\mathbb{P}_8$

Dual bases and change of coordinates are exposed, and auto-dual bases in $\mathbb{F}_8$ are recognized. This allows to generate the simple group $\mathrm{GL}_3(\mathbb{F}_2)$ by 3 linear transformations $R^{\cdot}, S^{\cdot}, I^{\cdot}$. So this group is 'borromean'. We have also another borromean presentation by 3 linear involutions A, B, C. Then the Post-Malcev algebra $\mathbb{P}_8$ could be generated by the canonical boolean functions and the three linear involutions A, B, C.

6.1. Dual bases

Two bases $\beta = (e_1, e_2, e_3)$ and $\beta^* = (e_1^*, e_2^*, e_3^*)$ are *dual* if $\mathrm{tr}(e_i e_j^*) = \delta_{i,j}$, where $\delta_{i,j}$ is Kronecker's symbol (with value 1 if $i = j$, and 0 if $i \neq j$). A basis $\beta = (e_1, e_2, e_3)$ is said to be *strictly auto-dual* if $\mathrm{tr}(e_i e_j) = \delta_{i,j}$, and *auto-dual* if, for a permutation σ on $\{1, 2, 3\}$, β and $\beta_\sigma = (e_{\sigma 1}, e_{\sigma 2}, e_{\sigma 3})$ are dual, i.e. such that $\mathrm{tr}(e_i e_j^*) = \delta_{i,j}$, with $e_j^* = e_{\sigma(j)}$.

Proposition 6.1. *If* $\beta = (e_1, e_2, e_3)$ *is a basis of* $\mathbb{F}_8$ *over* $\mathbb{F}_2$*, then we obtain a dual basis* $\beta^* = (e_1^*, e_2^*, e_3^*)$ *by:*

$$e_1^* = e_2 \times e_3, \quad e_2^* = e_3 \times e_1, \quad e_3^* = e_1 \times e_2,$$

and then $(\beta^*)^* = \beta$, *and the coordinates of* $u = u_1e_1 + u_2e_2 + u_3e_3$ *are:*

$u_1 = \mathrm{tr}(ue_1^*) = [u, e_2, e_3]$, $u_2 = \mathrm{tr}(ue_2^*) = [e_1, u, e_3]$, $u_3 = \mathrm{tr}(ue_3^*) = [e_1, e_2, u]$,

that is to say

$$u_1 = u^4 + (e_2e_3 + (e_2 + e_3)^2)u^2 + e_2e_3(e_2 + e_3), \text{etc.}$$

Also we have

$$u_1 = [\{e_1, e_1 + e_2, e_1 + e_3, e_1 + e_2 + e_3\}](u).$$

Especially we obtain

$$e_i^* = \sum_{j=1,2,3} < e_i^*, e_j^* > e_j, \quad e_i = \sum_{j=1,2,3} < e_i, e_j > e_j^*.$$

Proof. By construction $< e_1, e_1^* >= [e_1, e_2, e_3] = 1$, $< e_1, e_2^* >= [e_1, e_3, e_1] = 0$, etc. For $(\beta^*)^* = \beta$, for example we have $e_2^* \times e_3^* = (e_3 \times e_1) \times (e_1 \times e_2) = ((e_3 \times e_1).e_2)e_1 + ((e_3 \times e_1).e_1)e_2 = [e_3, e_1, e_2]e_1 = e_1$, etc. Then $[u, e_2, e_3] = u_1[e_1, e_2, e_3] + u_2[e_2, e_2, e_3] + u_3[e_3, e_2, e_3] = u_1 + 0 + 0 = u_1$, etc. The next formula comes from the formula for $[u, e_2, e_3]$ in Proposition 4.3; and the last two formulas are an application of the previous.
For the relation with $[\{e_1, e_1 + e_2, e_1 + e_3, e_1 + e_2 + e_3\}]$ we can argue directly that the four vectors $e_1, e_1 + e_2, e_1 + e_3, e_1 + e_2 + e_3$ are different, and the four others are $0, e_2, e_3, e_2 + e_3$, i.e. exactly those u with component $u_1 = 0$ on e_1. So it is the mixed product $[u, e_2, e_3]$, because this one is 0 if and only u, e_2, e_3 are linearly dependent, that is to say $u \in \{0, e_2, e_3, e_2 + e_3\}$. □

An element u is said to be *normal* over $\mathbb{F}_2$ if (u, u^2, u^4) is a basis, which is called a *normal basis*. If furthermore u is *primitive*, i.e. if the powers of u generate $\mathbb{F}_8\backslash\{0\}$, then the basis is said to be *normal primitive*.

Proposition 6.2. *There are* 28 *bases of* $\mathbb{F}_8$, *or* 168 *when the order of terms is specified. Up to a circular permutation, there is only one* normal basis*:*

$$\kappa = (R, S, I) = \kappa^*,$$

which is even a normal primitive basis*. Up to a circular permutation, this* κ *is also the only* strictly auto-dual basis*, and there are* 3 *other auto-dual bases (not strict), which are:*

$$r = (R', I', 1), \quad s = (1, S', R') \quad i = (S', 1, I'),$$

each one being its own dual, but with another order of terms:

$$r^* = (I', R', 1), \quad s^* = (1, R', S'), \quad i^* = (I', 1, S').$$

Up to the order of terms, each basis $\phi = (f_1, f_2, f_3)$ *is of the form*

$$\phi = t_\phi\beta = (t_\phi e_1, t_\phi e_2, t_\phi e_3),$$

with $\beta = (e_1, e_2, e_3)$ *one of the four auto-dual bases* κ, r, s *or* i, *and with* $t_\phi = f_1 + f_2 + f_3$. *The dual of such a basis* $\lambda\beta$ *is given by*

$$\phi^* = (t_\phi\beta)^* = t_\phi^{-1}\beta^*.$$

Proof. There are 35 sets of 3 distinct elements $\neq 0$ of $\mathbb{F}_8$, and those which are not among the 7 which are lines in the Fano plane are exactly those which are bases. Especially (R', S', I') is not a basis. A trio (u, v, w) of three distinct elements $\neq 0$ is a basis if and only if in the Fano plane the 3 points do not form a line, i.e. if and only if $u + v + w \neq 0$.
The existence of normal basis in a finite field comes back to K. Hensel (1888), in a non-constructive manner. Even always there is a primitive normal basis [11]. In a finite field there is not always an auto-dual basis: for example $\mathbb{F}_{16}$ has no such basis. But there exists such a basis in $\mathbb{F}_{2^n}$ if n is odd [12, p. 73, p. 129, ex. 3.77]; it is the case of $\mathbb{F}_8$. For $\mathbb{F}_8$ the basis (R, S, I) is precisely primitive normal and strictly auto-dual, and the only one in this case (with also of course (S, I, R) and (I, R, S)).
We can give an explicit proof of this last point, taking as in Proposition 6.1, a basis $\beta = (e_1, e_2, e_3)$, its dual $\beta^* = (e_1^* = e_2 \times e_3, e_2^* = e_3 \times e_1, e_3^* = e_1 \times e_2)$; then $\beta = \beta^*$ if and only if $< e_i, e_j >= \delta_{i,j}$, if and only if

$$e_1 = e_2 \times e_3, \quad e_2 = e_3 \times e_1, \quad e_3 = e_1 \times e_2.$$

Then $< e_1, e_1 >= [e_1, e_2, e_3] = 1$, and so $e_1 \in \{R, S, I, 1\}$, and similarly $e_2, e_3 \in \{R, S, I, 1\}$. In fact $e_1 \neq 1$, because $1 \times X \in \{R', S', I', 0\}$ (see table in Proposition 4.2). So $\{e_1, e_2, e_3\} = \{R, S, I\}$.
With the same table in Proposition 4.2 we verify that $R' \times I' = 1$, $I' \times 1 = I'$, $R' \times 1 = R'$, and so r and r^* are dual bases (not strictly). The same is available for s and for i.
Up to a permutation of e_1, e_2 and e_3, the other case of duality is

$$e_1 = e_2 \times e_3, \quad e_3 = e_3 \times e_1, \quad e_2 = e_1 \times e_2.$$

In this case $< e_1, e_1 >= 1, < e_2, e_2 >= 0, < e_3, e_3 >= 0$, i.e. $e_1 \in \{R, S, I, 1\}$, $e_2, e_3 \in \{R', S', I'\}$. If for example $e_2 = R'$ and $e_3 = S'$, then $e_1 = R' \times S' = 1$.
To conclude our proof we have just to check that the different values of $t\beta$, with $t \in \mathbb{F}_8 \backslash \{0\}$ and $\beta \in \{\kappa, r, s, i\}$ provide exactly the 28 possibilities of bases.
Finally for the computation of the dual bases, we put $\underline{\phi} = \{f_1, f_2, f_3\}$, $\lambda\underline{\phi} = \{\lambda f_1, \lambda f_2, \lambda f_3\}$, and $\underline{\phi}^* = \{f_2 \times f_3, f_3 \times f_1, f_1 \times f_2\}$,, in such a way that, with $\underline{\kappa} = \{R, S, I\}$, $\underline{r} = \{R', I', 1\}$, etc., and $\lambda \in \mathbb{F}_8 \backslash \{0\}$ we have to verify that $(\lambda\underline{\kappa})^* = \lambda^{-1}\underline{\kappa}$, $(\lambda\underline{r})^* = \lambda^{-1}\underline{r}^*$, etc. Because of symmetry, only these two cases are to be checked. We do it with the tables for product and cross product given in the proof of Proposition 3.7 and in Proposition 4.2. □

Proposition 6.3. *If $\epsilon = (e_1, e_2, e_3)$ and $\phi = (f_1, f_2, f_3)$ are two bases, and if $u = u_1 f_1 + u_2 f_2 + u_3 f_3$, let $T(u)$ be the element with the same coordinates on ϵ:*

$$u = u_1 f_1 + u_2 f_2 + u_3 f_3, \quad T(u) = u_1 e_1 + u_2 e_2 + u_3 e_3.$$

in such a way that

$$T(f_1) = e_1, \quad T(f_2) = e_2, \quad T(f_3) = e_3,$$
$$T^{-1}(e_1) = f_1, \quad T^{-1}(e_2) = f_2, \quad T^{-1}(e_3) = f_3,$$

then, with $v = v_1e_1 + v_2e_2 + v_3e_3$, *we have*

$$T(u) = \mathrm{tr}(uf_1^*)e_1 + \mathrm{tr}(uf_2^*)e_2 + \mathrm{tr}(uf_3^*)e_3,$$
$$T^{-1}(v) = \mathrm{tr}(ve_1^*)f_1 + \mathrm{tr}(ve_2^*)f_2 + \mathrm{tr}(ve_3^*)f_3.$$

This transformation T *is linear and if necessary more explicitly denoted by* $T = T^{\epsilon\leftarrow\phi}$. *Its matrix relative to* ϕ *is* $\Theta = (\mathrm{tr}(f_i^\star e_j))$.
Furthermore if coordinates of u *on* ϕ *and* ϵ *are given,* $u = \sum_j u_j e_j$ *and* $u = \sum_i u'_i f_i$, *then the exchange of coordinates is given by composition with* Θ*:*

$$u'_i = \sum_j \mathrm{tr}(f_i^\star e_j)u_j.$$

Proof. It is an immediate application of Proposition 6.1. The matrix of T with source basis ϕ and target ϵ is I_3, and the matrix of T relative to ϕ is the matrix of Id with source basis ϵ and target ϕ. The last formula comes from the description of e_j on ϕ: $e_j = \sum_i (\mathrm{tr}(f_i^* e_j)f_i$, etc. □

Proposition 6.4. *With the notations of Proposition* 6.2, *we consider the* 3 *linear transformations* r°, s°, i°, *sending* κ *on* r, κ *on* s, *and* κ *on* i. *Their matrices relatively to* κ *are — abusively — denoted only by* r,s *and* i*:*

$$r = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}, \quad s = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}, \quad i = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix},$$

and their polynomial forms are (cf. convention 1, *and Proposition* 3.12.*):*

$$\underline{r}(u) = R'u^4 + u^2 + I'u; \quad \underline{s}(u) = S'u^4 + u^2 + R'u; \quad \underline{i}(u) = I'u^4 + u^2 + S'u.$$

Proposition 6.5. *The multiplications by* R, S *or* I, *used in Proposition* 5.7, *and denoted by* $R^\cdot, S^\cdot, I^\cdot$, *are given by matrices denoted only by:*

$$R = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}, \quad S = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}, \quad I = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix},$$

and the polynomial forms (cf. Proposition 3.12.*):*

$$\underline{R}(u) = Ru; \quad \underline{S}(u) = Su; \quad \underline{I}(u) = Iu.$$

Proposition 6.6. *The three cross products with* R, S, I, *i.e.* $u \mapsto R \times u$, $u \mapsto S \times u$, $u \mapsto I \times u$, *are given by matrices:*

$$R^\times = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \quad S^\times = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \quad I^\times = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix},$$

with the polynomial forms (cf. Proposition 3.12.*):*

$$\underline{R^\times}u = Su^4 + Iu^2, \quad \underline{S^\times}u = Iu^4 + Ru^2, \quad \underline{I^\times}u = Ru^4 + Su^2.$$

Furthermore — as in the Lie algebra $\mathfrak{so}(3)$ *of the Lie group* $\mathrm{SO}(3)$ *— we have the commutators relations:*

$$[R^\times, S^\times] = I^\times, \quad [S^\times, I^\times] = R^\times, \quad [I^\times, R^\times] = S^\times.$$

Proposition 6.7. *The inverses of matrices r, s, i are*

$$r^{-1} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}, \quad s^{-1} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}, \quad i^{-1} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix},$$

with the polynomial forms

$$\underline{r^{-1}}(u) = Ru^4+Iu^2+Ru; \quad \underline{s^{-1}}(u) = Su^4+Ru^2+Su; \quad \underline{i^{-1}}(u) = Iu^4+Su^2+Iu,$$

and we have

$$\underline{r^{-1}} + \underline{s^{-1}} + \underline{i^{-1}} = \mathrm{tr}.$$

Proof. We can use Propositions 3.10 and 3.12, or directly compute $r^{-1} = r^6$, $s^{-1} = s^6$, $i^{-1} = i^6$. □

Proposition 6.8. *We have*

$$\underline{r} + \underline{s} + \underline{i} = (-)^2,$$

$$R = ir^2, \quad S = rs^2, \quad I = si^2.$$

Proof. The formula $R = ir^2$ was given in [7, Proposition 15, p.152]. It is easy to check, as well as the formula for $(-)^2$. □

Proposition 6.9. *Given $\phi = (f_1, f_2, f_3) = t_\phi\beta$ one of the 28 bases of $\mathbb{F}_8$, as in Proposition 6.2, let ϕ° be the linear map sending κ to ϕ, and let F its matrix relative to κ. Then F is of the form HB, with $H \in \{I_3, R^\cdot, S^\cdot, I^\cdot, R'^\cdot, S'^\cdot, I'^\cdot\}$ and $B \in \{I_3, R^\circ, S^\circ, I^\circ\}$, and every element M of $\mathrm{GL}_3(\mathbb{F}_2)$ could be written in a unique way as a composition of such an HB and a permutation P:*

$$M = HBP.$$

Proof. It is [7, Proposition 17, p.153]. □

Proposition 6.10. *The group $\mathrm{GL}_3(\mathbb{F}_2)$ is generated by $r^\circ, s^\circ, i^\circ$, as well as by their inverses.*

Proof. It is as in [7, Proposition 18, p.154], a consequence of 6.9. □

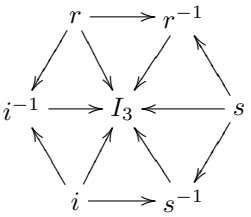
Proposition 6.11. *With the hypothesis and notations of Proposition 5.6, every function in $\mathbb{P}_8$ could be written with canonical boolean operations $\wedge$ and $\neg$, and the three linear maps $r^\circ, s^\circ, i^\circ$ with matrices r, s, i.*

Proof. With Proposition 6.8, in Proposition 5.7 we could replace the operations $(-)^2$, $R^\cdot, S^\cdot, I^\cdot$ by $r^\circ, s^\circ, i^\circ$. □

Proposition 6.12. *With the hypothesis and notations of Proposition 5.6, every function in $\mathbb{P}_8$ could be written with canonical boolean operations $\wedge$ and $\neg$, and the three linear maps $r^{\circ -1}, s^{\circ -1}, i^{\circ -1}$ with matrices r^{-1}, s^{-1}, i^{-1}.*

Proof. It results from 6.11 and the fact that the r, s, i are formulable with their inverses, in $\mathrm{GL}_3(\mathbb{F}_2)$ (Proposition 6.10). □

Remark 6.13. If in the picture of the hexagon in Definition 2.1 we emphasize that $R' = R^{-1}$, then now we get an analogous decoration of the hexagon by elements of $\mathbb{P}_8$:



7. A, B, C and $R^\times, S^\times, I^\times$ borromean generations of $\mathrm{GL}_3(\mathbb{F}_2)$ and of $\mathbb{P}_8$

7.1. Generation by A, B, C

Proposition 7.1. *In the Proposition* 6.10*, we introduce, with* $r^6 = r^{-1}$ *etc.*

$$r^t = rir^6, \quad s^t = srs^6, \quad i^t = isi^6;$$

they are the transposed matrices of r, s, i*, and we define*

$$A = r^t i^t, \quad B = s^t r^t, \quad C = i^t s^t.$$

These A, B, C *are the matrices of* 3 *transvections given by*

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

$$A^2 = B^2 = C^2 = I_3,$$

$$r = ACB, \quad s = BAC, \quad i = CBA,$$

and the transposed matrices of A, B, C *are*

$$A^t = (CB)^2, \quad B^t = (AC)^2, \quad C^t = (BA)^2,$$

and $\mathrm{GL}_3(\mathbb{F}_2)$ *is generated by* A, B, C*.*
Furthermore we have the polynomial forms:

$$\underline{A}(u) = R'u^4 + Iu^2 + Su; \ \underline{B}(u) = S'u^4 + Ru^2 + Iu; \ \underline{C}(u) = I'u^4 + Su^2 + Ru.$$

Proof. So the borromean structure of $\mathrm{GL}_3(\mathbb{F}_2)$ could act on the set $\mathbb{F}_8$, which is also a boolean algebra, and so we obtain another borromean presentation of $\mathbb{P}_8$, as in the next Proposition. For polynomial forms we use Proposition 3.10. □

Proposition 7.2. *We have*

$$\underline{A} + \underline{B} + \underline{C} + \mathrm{Id}_{\mathbb{F}_8} = (-)^2,$$

$$R = (CB)^2 A(CB), \quad S = (AC)^2 B(AC), \quad I = (BA)^2 C(BA).$$

Proof. For $(-)^2$ it is immediate by addition of the 3 matrices A, B, C, and for $R^{\cdot}$ from Proposition 6.8 we have $R = ir^2$, and with Proposition 7.1, $R = (CB)^2 A(CB)$. □

Proposition 7.3. *The commutators of the A, B, C are:*

$$[A,B] = AB + BA = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix},$$

$$[B,C] = BC + CB = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix},$$

$$[C,A] = CA + AC = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix},$$

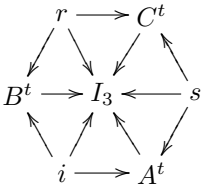
and

$$\underline{[A,B]} + \underline{[B,C]} + \underline{[C,A]} = (-)^4$$

Proposition 7.4. *With the hypothesis and notations of Proposition* 5.6*, every function in $\mathbb{P}_8$ could be written with canonical boolean operations $\wedge$ and $\neg$, and the three linear involutive transvections given by A, B, C.*

Proof. From Proposition 6.11 and Proposition 7.1, from Proposition 7.2. □

Remark 7.5. If in the picture of the hexagon in Definition 2.1 we emphasize that $R' = SI$, then we get an analogous decoration of the hexagon by elements of $\mathbb{P}_8$:



7.2. Generation by $R^\times, S^\times, I^\times$

Proposition 7.6. *We have*

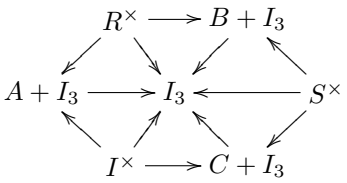
$$R^\times S^\times = A + I_3, \quad S^\times R^\times = [B,C],$$
$$S^\times I^\times = B + I_3, \quad I^\times S^\times = [C,A],$$
$$I^\times R^\times = C + I_3, \quad R^\times I^\times = [A,B].$$

Proof. An immediate verification with matrices. □

Proposition 7.7. *With the hypothesis and notations of Proposition* 5.6*, every function in $\mathbb{P}_8$ could be written with canonical boolean operations $\wedge$ and $\neg$, and the three cross products given by $R^\times, S^\times, I^\times$.*

Proof. A consequence of Proposition 7.4 and Proposition 7.6. □

Remark 7.8. If in the picture of the hexagon in Definition 2.1 we emphasize that $R' = SI$, then now we get an analogous decoration of the hexagon by elements of $\mathbb{P}_8$:



8. Conclusion: hexagonal presentations of an 8-valuated logic, going from a decoration by $\mathbb{F}_8$ to decorations by $\mathbb{P}_8$

We consider that the logic of an object W 'is' the organization of $\mathbb{P}(W)$ the Post-Malcev algebra of functions of all arities on this object, $f : W^k \to W$, and especially the logic of $\underline{8} = \{\underline{0}, \underline{1}, \underline{2}, \underline{3}, \underline{4}, \underline{5}, \underline{6}, \underline{7}\}$ or of the cube $\{0,1\}^3$ is the organization of functions $f : (\{0,1\}^3)^k \to \{0,1\}^3$, i.e. the algebra $\mathbb{P}(\{0,1\}^3) = \mathbb{P}_8$.

At first we have shown that the set $\{0,1\}^3$ as a field $\mathbb{F}_8$, could be presented as a Fano plane plus a zero, as an hexagon (cf. Definition 2.1 and section 3), and we began with a decoration of an hexagon by elements of $\mathbb{F}_8$.

Then studying the arithmetic and the geometry on $\mathbb{F}_8$, we proved that $\mathbb{P}(\mathbb{F}_8) = \mathbb{P}_8$ could be generated by a boolean calculus with conjunctive avatars.

After that, we proved that $\mathbb{P}_8$ itself admits a hexagonal generations, by canonical boolean operations plus (r, s, i) or plus (r^{-1}, s^{-1}, i^{-1}), or plus A, B, C, or $R^\times, S^\times, I^\times$, and we have drawn corresponding decorations of the hexagon.

Now to conclude, forgetting our arithmetical and geometrical tools and intermediary arguments, as the different ways of thinking with hexagons and the avatars, we express our main result from Proposition 7.7 in layman's terms:

Theorem 8.1. *Given a set with* 8 *elements, represented as* $\{0,1\}^3$*, the set of all the functions* $f : (\{0,1\}^3)^k \to \{0,1\}^3$*, for all* $k \in \mathbb{N}$*, is generated by composition of the* 6 *following functions (modulo* 2*) of arities* 2 *and* 1*:*

$$\big((x,y,z),(x',y',z')\big) \mapsto (x+x', y+y', z+z');$$

$$\big((x,y,z),(x',y',z')\big) \mapsto (x.x', y.y', z.z');$$

$$(x,y,z) \mapsto (x+1, y+1, z+1);$$

$$(x,y,z) \mapsto (0,z,y); \quad (x,y,z) \mapsto (z,0,x); \quad (x,y,z) \mapsto (y,x,0).$$

References

[1] J.-Y. Béziau, The Power of the Hexagon, *Log. Univers.*, 6 (1-2), 2012: 1-43.

[2] R. Blanché, Sur l'opposition des concepts, *Theoria*, 19, 1953.

[3] R. Blanché, *Structures intellectuelles*, Vrin, 1966.

[4] L.E. Dickson, *Linear Groups*, Dover Publ., 1958 (1st ed. 1900).

[5] R. Guitart, L'idée de logique spéculaire, *Journées Catégories, Algèbres, Esquisses, Néo-esquisses*, Caen, 27-30 september 1994.

[6] R. Guitart, Moving logic, from Boole to Galois, Colloque International "Charles Ehresmann : 100 ans", 7-9 october 2005, Amiens, *Cahiers Top Géo Diff Cat.* vol. XLVI-3, 2005, 196-198.

[7] R. Guitart, Klein's group as a borromean object, *Cahiers Top. Géo. Diff. Cat.* vol. L-2, 2009, 144-155.

[8] R. Guitart, A Hexagonal Framework of the Field $\mathbb{F}_4$ and the Associated Borromean Logic, *Log. Univers.*,6 (1-2), 2012: 119-147.

[9] Brother J. Heisler, A characterization of finite fields, *The Am. Math. Monthly* 74, 1967, p. 537-538, and p. 1211.

[10] D. Lau, *Function Algebras on finite sets*, Springer, 2006.

[11] H.W. Lenstra Jr. and R.J. Schoof, Primitive normal basis for finite fields, *Math. Comp.*, 48, 1987, 217-231.

[12] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, C.U.P., 1994.

[13] A. I. Malcev, Iterative algebra and Post's varieties (Russian), *Algebra i Logika (Sem.)* 5, 1966, 5-24.

[14] E.H. Moore, Mathematical Papers, Chicago Congress of 1893, pp. 208-242; *Bull. Amer. Math. Soc.*, December, 1893.

[15] P. Ribenboim, *L'arithmétique des corps*, Hermann, Paris, 1972.

[16] A. Sesmat, *Logique: 1. Les définitions, les jugements. 2. Les raisonnements, la logistique*, Hermann, 1951.

René Guitart
IMJ-PRG Université Paris Diderot
Bâtiment Sophie Germain
75013 Paris
France
e-mail: rene.guitart@orange.fr