Iso-Galois Fields

Arun S. Muktibodh
Department of Mathematics
Mohota College of Science
Nagpur-440009
India
e-mail: amukti2000@yahoo.com

Abstract

Rugero Maria Santilli [8], [9], [10] and [11] defined iso-fields of characteristic zero. In this paper we extend this definition to define Iso-Galois fields which are essentially of non-zero characteristic. Iso-Galois fields of first and second kind are also defined with specific examples. We have also proved some results regarding the structure of these constructs.

keywords:- Isounit, Isofield, Galois field and Iso-Galois field.

1 Introduction

During a talk at the conference *Differental Geometric Methods in Mathematical Physics* held in Clausthal, Germany, in 1980, Ruggero Maria Santilli submitted new numbers based on certain axiom preserving generalization of the multiplication, today known as *isotopic numbers* or *isonumbers* in short. This generalization induced the so-called isotopies of the conventional multiplication with consequential generalization of the multiplicative unit, where the Greek word "isotopy" suggested the meaning "same topology". Subsequently, Rugero Maria Santilli submitted a new conjugation, under the name *isoduality* which yields an additional class of numbers, today known as *isodual isonumbers*.
The discovery of isonumbers was made with the specific need of quantitative representation of the transition from :
a) *exterior dynamical problem*, i.e., particles moving in the homogeneous and isotropic vacuum (empty space) with consequential local-differential and potential-cannonical equations of motion, to
b) the *interior dynamical problem*, i.e., extended and therefore deformable particles moving within an inhomogeneous and anisotropic physical medium, with consequential equations of motion of the most general known nonlinear, nonlocal-integral and nonpotential-noncanonical type.
We appraise the readers with some basic ideas of Santilli's isofields and some related results.

1.1 Santilli's Isofield

Definition 1.1. *Given a field F with elements $\alpha, \beta, \gamma, \ldots$, sum $\alpha + \beta$, multiplication $\alpha\beta$, and respective units 0 and 1, "Santilli's isofields" are rings of elements $\hat{\alpha} = \alpha\hat{1}$ where α are elements of F and $\hat{1} = \hat{T}^{-1}$ is a positive-definite $n \times n$ matrix generally outside F equipped with the same sum $\hat{\alpha} + \hat{\beta}$ of F with related additive unit $\hat{0} = 0$ and a new multiplication $\hat{\alpha} * \hat{\beta} = \hat{\alpha}\hat{T}\hat{\beta}$, under which $\hat{1} = \hat{T}^{-1}$ is the new left and right unit of F in which case $\hat{F}$ satisfies all axioms of a field.*

The 'isofields' $\hat{F} = \hat{F}(\hat{\alpha}, +, \hat{\times})$ are given by elements $\hat{\alpha}, \hat{\beta}, \hat{\gamma} \ldots$ characterized by one-to-one and invertible maps $\alpha \to \hat{\alpha}$ of the original element

$\alpha \in F$ equipped with two operations $(+, \hat{\times})$, the conventional addition $+$ of F and a new multiplication $\hat{\times}$ called "isomultiplication" with corresponding conventional additive unit 0 and a generalized multiplicative unit $\hat{1}$, called "multiplicative isounit" under which all the axioms of the original field F are preserved.

If the conventional field is chosen to be alternative under the operation of conventional multiplication then the resulting isofield is also isoalternative under isomultiplication.
If the given algebraic structure is a noncommutative division ring (e.g. ring of quaternions) then the resulting isoalgebraic structure is also noncommutative under the isomultiplication.

This new algebraic structure has revolutionized contemporary mathematics and found its applications in so far unexplored (unexplained) and unknown territories of quantum mechanics and quantum chemistry.
The resulting new theory of numbers has become the basis of recent studies of **nonlinear-nonlocal, non-Hamiltonian systems** in nuclear particle and statistical physics. Santilli iso-numbers, which are the mathematical basis of Hadronic Mechanics, are also introduced and reviewed in [2].

Isofields are of two types, **isofield of first kind**; wherein the isounit does not belong to the original field, and **isofield of second kind**; wherein the isounit belongs to the original field. The elements of the isofield are called as **isonumbers**. This leads to number of new terms and parallel developments of conventional mathematics.

We mention two important propositions by Santilli [10].

Proposition 1.1. *The necessary and sufficient condition for the lifting (where the multiplication is lifted but elements are not)* $F(a, +, \times) \longrightarrow (\hat{F}, +, \hat{\times}), \hat{\times} = \times\hat{T}\times, \hat{1} = \hat{T}^{-1}$ *to be an isotopy (that is for* $\hat{F}$ *to verify all axioms of the original field F) is that* $\hat{T}$ *is a non-null element of the original field* F*.*

e.g. We can start with the field of real numbers $\Re$ and construct an isotopic field $\hat{\Re}$ with a new multiplicative identity as $\hat{1} = \frac{1}{2}$ where $\hat{T} = 2$ as the isounit. So, if $a \in \Re$ then $\hat{a} = a.\frac{1}{2}$. Thus the product of two iso numbers $\hat{a}$ and $\hat{b}$ will be $\hat{a}\hat{\times}\hat{b} = \frac{a}{2}.2.\frac{b}{2} = \frac{ab}{2} = \widehat{ab}$.

Proposition 1.2. *The lifting (where both the multiplication and the elements are lifted)*
$F(a, +, \times) \longrightarrow (\hat{F}, +, \hat{\times}), \hat{a} = a \times \hat{1}, \hat{\times} = \times\hat{T}\times, \hat{1} = \hat{T}^{-1}$ *constitutes an isotopy even when the multiplicative isounit* $\hat{1}$ *is not an element of the original field.*

The following three theorems [5] directly follow from the definition of isofield.

Proposition 1.3. *If* $(F, +, \times)$ *is a field and* $(\hat{F}, \hat{+}, \hat{\times})$ *is the corresponding isofield such that the isounit* $\hat{I} \in F$ *then* $(F, +, \times) \cong (\hat{F}, \hat{+}, \hat{\times})$.

Clearly, the map $x \longmapsto \hat{x}$ is an isomorphism.

Proposition 1.4. *If* $(F, +, \times)$ *is a field and* $(\hat{F}, \hat{+}, \hat{\times})$ *is the corresponding isofield such that the isounit* $\hat{I} \notin F$ *then* $(F, +, \times)$ *is isotopic to* $(\hat{F}, \hat{+}, \hat{\times})$.

Proposition 1.5. *Isofield corresponding to a non-commutative field is isotopic to the original field.*

The noncommutative ring of Quaternions is an example of this type.

1.2 Galois fields

Finite fields were first introduced by Galois in 1830 in his proof of the unsolvability of the general quintic equation. Hence finite fields are also called as Galois fields. When Cayley invented matrices a few decades later, it was natural to investigate groups of matrices over finite fields. In fact, the groups of matrices over the finite fields have become the most important class of groups. Finite fields have vast applications in computer science, coding theory, information theory, and cryptography.

Thus, Galois fields are finite fields. Finite fields are of nonzero characteristic. Every finite field is of prime-power order, and for every power of a prime there is a unique Galois field of this order.
Santilli's isofields are defined for the fields of characteristic zero, and hence for infinite fields.
Our main purpose is to apply Santilli's ideas to the fields of non-zero characteristic and seek for further development in this direction.
In this paper we answer the open problems posed in [5],

- Can we construct finite isofields of first kind ?
- Can we construct finite isofields of second kind ?

in the affirmative.

2 Iso-Galois fields

Definition 2.1. *If F is an iso-field and F is finite, then F is called an Iso-Galois field.*

Definition 2.2. *Let F be a Galois field. If G is an Iso-Galois field of F wherein the prescribed multiplicative identity is from the field F itself, then the Iso-Galois field G is called an* ***Iso-Galois field of second kind****.*

Definition 2.3. *Let F be a Galois field. If G is an Iso-Galois field of F wherein the prescribed multiplicative identity is not from the field F, then the Iso-Galois field G is called an* ***Iso-Galois field of first kind****.*

If G is an Iso-Galois field constructed from the field F then we call the field F as the **trivial iso-field**.

3 Iso-Galois fields of second kind

Consider a Galois field F_8 as a set of following matrices of integers modulo 2.

$$(0)=\begin{pmatrix}0&0&0\\0&0&0\\0&0&0\end{pmatrix},(1)=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix},(2)=\begin{pmatrix}0&1&0\\0&0&1\\1&1&0\end{pmatrix},(3)=\begin{pmatrix}0&0&1\\1&1&0\\0&1&1\end{pmatrix},$$
$$(4)=\begin{pmatrix}1&1&0\\0&1&1\\1&1&1\end{pmatrix},(5)=\begin{pmatrix}0&1&1\\1&1&1\\1&0&1\end{pmatrix},(6)=\begin{pmatrix}1&1&1\\1&0&1\\1&0&0\end{pmatrix},(7)=\begin{pmatrix}1&0&1\\1&0&0\\0&1&0\end{pmatrix}$$

For an isofield it will be sufficient to consider the multiplication table of non-zero elements of F_8.

$\cdot$	(1)	(2)	(3)	(4)	(5)	(6)	(7)
(1)	1	2	3	4	5	6	7
(2)	2	3	4	5	6	7	1
(3)	3	4	5	6	7	1	2
(4)	4	5	6	7	1	2	3
(5)	5	6	7	1	2	3	4
(6)	6	7	1	2	3	4	5
(7)	7	1	2	3	4	5	6

Let us choose the iso-element $\hat{T}=(4)\equiv 4\in F_8$ in the above composition table. Then the iso-unit element is $\hat{1}=\frac{1}{\hat{T}}=\frac{1}{4}=4^{-1}=5$. By using the fact that for $a\in F_8$, $\hat{a}=a\cdot\frac{1}{\hat{T}}=a\cdot 5$. We construct the corresponding isonumbers. Thus,
$\hat{2}=2\cdot\frac{1}{4}=2\cdot 5=6$. Similarly, $\hat{3}=7$, $\hat{4}=1$, $\hat{3}=7$, $\hat{4}=1$, $\hat{5}=2$, $\hat{6}=3$ and $\hat{7}=4$.
We now construct the corresponding composition table for the isonumbers using the fact that the isomultiplication $\hat{\times}$ is defined as $\hat{a}\hat{\times}\hat{b}=\hat{a}\hat{T}\hat{b}$.
e.g. $\hat{6}\hat{\times}\hat{7}=6\cdot 4\cdot 7=1$ using above composition table. Thus the corresponding isomultiplication table (or iso-composition table) for isonumbers will be;

$\hat{\times}$	$\widehat{(1)}$	$\widehat{(2)}$	$\widehat{(3)}$	$\widehat{(4)}$	$\widehat{(5)}$	$\widehat{(6)}$	$\widehat{(7)}$
$\widehat{(1)}$	4	5	6	7	1	2	3
$\widehat{(2)}$	5	6	7	1	2	3	4
$\widehat{(3)}$	6	7	1	2	3	4	5
$\widehat{(4)}$	7	1	2	3	4	5	6
$\widehat{(5)}$	1	2	3	4	5	6	7
$\widehat{(6)}$	2	3	4	5	6	7	1
$\widehat{(7)}$	3	4	5	6	7	1	2

Note that the numbers in the iso-composition table are isonumbers.

Remark. *1. The function $f : F_8 \to F_8$ defined by $f(x) = 5x$ is not an isomorphism. However,*
2. The isofunction $\hat{f} : x \to \hat{x}$ is an isomorphism.

We generalize these observations in the following Theorem.

Theorem 3.1. *If F is a Galois field such that $\hat{F}$ is an Iso-Galois field of second kind, where $\hat{T} \in F$ is an isoelement and $\hat{x} = \hat{T}^{-1}x$, $x \in F$ then the function $f : F \to F$ defined by $x \mapsto \hat{T}^{-1}x$ is not an isomorphism but is an isotopism, whereas the isofunction $\hat{f} : F \to \hat{F}$ is an isomorphism.*

Proof. It is easy to verify that the function f is a translation from F to F and hence is not an isomorphism. It is an isotopism because we have prescribed a new identity and the result follows from [5].
If we consider the isofunction $\hat{f} : F \to \hat{F}$ then for $x, y \in F$, $\hat{f}(x.y) = \hat{T}^{-1}x.y$ whereas $\hat{f}(x)\hat{\times}\hat{f}(y) = \hat{x}\hat{\times}\hat{y} = \hat{T}^{-1}x.\hat{T}.\hat{T}^{-1}y = \hat{T}^{-1}x.y$. Thus $\hat{f}(x.y) = \hat{f}(x)\hat{\times}\hat{f}(y)$. □

Theorem 3.2. *If F is a Galois field of order p^m and n is the number of involutions in F then there exist $p^m - n - 1$ number of distinct Iso-Galois fields of kind two of F.*

Proof. The multiplicative group of F will obviously contain $p^m - 1$ number of non-zero elements. Every involution and its inverse will obviously give

rise to the same Iso-Galois field of second kind. Therefore the total number of distinct Iso-Galois fields would be $p^m - n - 1$. □

4 Iso-Galois fields of First kind

Consider a Galois field F of order 16 represented by the polynomials $a + bx + cx^2 + dx^3$, a, b, c and d are integers modulo 2. The polynomials are generated by the powers of x using the rule $x^4 = 1 + x$.
The elements of the field are; $(0) = (0,0,0,0)$, $(1) = (1,0,0,0)$, $(2) = (0,1,0,0)$, $(3) = (0,0,1,0)$, $(4) = (0,0,0,1)$, $(5) = (1,1,0,0)$, $(6) = (0,1,1,0)$, $(7) = (0,0,1,1)$, $(8) = (1,1,0,1)$, $(9) = (1,0,1,0)$, $(10) = (0,1,0,1)$, $(11) = (1,1,1,0)$, $(12) = (0,1,1,1)$, $(13) = (1,1,1,1)$, $(14) = (1,0,1,1)$, $(15) = (1,0,0,1)$ with the following composition table for multiplication;

·	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	2	3	4	5	6	7	8	9	10	11	12	13	14	15	1
3	3	4	5	6	7	8	9	10	11	12	13	14	15	1	2
4	4	5	6	7	8	9	10	11	12	13	14	15	1	2	3
5	5	6	7	8	9	10	11	12	13	14	15	1	2	3	4
6	6	7	8	9	10	11	12	13	14	15	1	2	3	4	5
7	7	8	9	10	11	12	13	14	15	1	2	3	4	5	6
8	8	9	10	11	12	13	14	15	1	2	3	4	5	6	7
9	9	10	11	12	13	14	15	1	2	3	4	5	6	7	8
10	10	11	12	13	14	15	1	2	3	4	5	6	7	8	9
11	11	12	13	14	15	1	2	3	4	5	6	7	8	9	10
12	12	13	14	15	1	2	3	4	5	6	7	8	9	10	11
13	13	14	15	1	2	3	4	5	6	7	8	9	10	11	12
14	14	15	1	2	3	4	5	6	7	8	9	10	11	12	13
15	15	1	2	3	4	5	6	7	8	9	10	11	12	13	14

The set $F_1 = \{0, 1, 6, 11\}$ forms a subfield of F. We consider an element $\hat{T} = 2$ such that $\hat{T}$ does not belong to F_1 and form an Iso-Galois field of F_1. The isoelement $\hat{1} = \frac{1}{\hat{T}} = \hat{T}^{-1} = 2^{-1} = 15$. The numbers of F_1 are converted

to following isonumbers as $\hat{1} = 15$, $\hat{6} = 6.15 = 5$ and $\hat{11} = 11.15 = 10$. Thus the isofield is $\hat{F}_1 = \{0, 15, 5, 10\}$ with the following composition table for isomultiplication.

$\hat{\times}$	15	5	10
15	15	5	10
5	5	10	15
10	10	15	5

e.g the isoproduct of 5 and 10 is given by $5.\hat{T}.10 = 5.2.10 = 15$.
Similarly, if $\hat{T} = 7$ then $\hat{1} = \frac{1}{\hat{T}} = 7^{-1} = 10$. The numbers of F_1 are converted to following isonumbers as $\hat{1} = 10$, $\hat{6} = 6.10 = 15$ and $\hat{11} = 11.10 = 5$. Thus the isofield is $\hat{F}_1 = \{0, 10, 15, 5\}$ with the following composition table for isomultiplication.

$\hat{\times}$	10	15	5
10	10	15	5
15	15	5	10
5	5	10	15

Theorem 4.1. *If F is a Galois field of order p^n and F_1 is a subfield of F of order p^m such that $F \setminus F_1$ has r number of involutions, then there exist $p^m - p^n - r$ number of distinct Iso-Galois fields of first kind of F_1.*

Proof. F_1 is a subfield of F implies $m|n$. Let $n = m + r$. Then
$o(F \setminus F_1) = p^n - p^m = p^{m+r} - p^m = p^m(p^r - 1) \dots (1)$.
Case I : If $p = 2$ then $(1) \Rightarrow o(F \setminus F_1)$ is even.
Case II ; If $p \neq 2$ then $p^r - 1$ is even and again $o(F \setminus F_1)$ is even.
Also, if $x \in F \setminus F_1$ then x^{-1} also belongs to $F \setminus F_1$. Thus, each $x \in F \setminus F_1$ gives rise to one isofield of first kind of F_1. Now, if x is an involution then $x = x^{-1}$ and hence x and x^{-1} will give rise to same isofield. If there are r number of involutions in $F \setminus F_1$ then the number of elements which give rise to distinct isofields will be $p^n - p^m - r$. Hence the result. □

References

[1] R. H. Bruck, *A Survey of Binary Systems*, Springer Verlag, (1958).

[2] Christian Corda, *Introduction to Santilli iso-numbers* American Institute of Physics, AIP Conf. Proc. 1479, 1013 (2012); doi: 10.1063/1.4756316.

[3] Chun-Xuan Jiang, *Foundations of Santilli's Isonumber Theory, with applictions to New Cryptograms, Fermat's Theorem and Goldbach's Conjecture*, International Academic Press, America-Europe-Asia, 2002.

[4] J. K. Kadeisvili and N. Kamiya, *A characterization of Isofields and their isoduals*, Hadronic J. 16, 155-172,(1993).

[5] A. S. Muktibodh, *Foundations of Isomathematics*, American Institute of Physics, AIP Conference Proceedings 1558, 707 (2013); doi: 10.1063/1.4825589.

[6] Ruggero Maria Santilli, *isonumbers and genonumbers of dimension 1,2,4,8, their isoduals and pseudoduals, and "hidden numbers" of dimension 3,5,6,7*, algebras, groups and geometries 10, 273-322 (1993).

[7] R. M. Santilli, *Foundations of Hadronic Chemistry*, Kluwer Academic Publisher, Dordrecht, 2001.

[8] R. M. Santilli, Isotopies of contemporary mathematical structures, I; Isotopies of fields, vector spaces, transformation theory, Lie Algebras, analytic mechanics and space-time symmetries, Algebras, groups and Geometries 8, 169-266 (1991).

[9] R. M. Santilli, Isotopies of contemporary mathematical structures, II; Isotopies of symplectic geometry, affine geometry, Riemanian geometry and Einstein gravitation, Algebras, Groups and Geometries, 8, 275-390 (1991).

[10] R. M. Santilli, Elements of Hadronic Mechanics, Vol. I (1995) [15a], Vol. II, second edition (1995) [15b] Academy of Sciences, Kiev, http://www.santilli-foundation.org/docs/Santilli-300.pdf http://www.santilli-foundation.org/docs/Santilli-301.pdf.

[11] R. M. Santilli, Hadronic Mathematics, Physics and Chemistry, Vols. I [4a], II [4b], III [4c], IV [4d] and V [4e] , New York : International Academic Press , also in http://www.i-b-r.org/Hadronic-Mechanics.htm.

Acknowledgements: I profoundly thank Dr. Svetlin Georgiev, France, for the fruitful interactions and discussions I had with him, during his visit to India in October 2013.