Isopermutation group

A. S. Muktibodh

Citation: AIP Conference Proceedings **1648**, 510002 (2015); doi: 10.1063/1.4912707
View online: http://dx.doi.org/10.1063/1.4912707
View Table of Contents: http://scitation.aip.org/content/aip/proceeding/aipcp/1648?ver=pdfcov
Published by the AIP Publishing

Isopermutation Group

A. S. Muktibodh

Department of Mathematics, Mohota College of Science, NAGPUR-440009
India
E-mail: amukti2000@yahoo.com

Abstract. The concept of 'Isotopy' as formulated by Ruggero Maria Santilli [1, 2, 3] plays a vital role in the development of Iso mathematics. Santilli defined iso-fields of characteristic zero. In this paper we extend this definition to define Iso-Galois fields [4] which are essentially of non-zero characteristic. Isotopically isomorphic realizations of a group define isopermutation group which gives a clear cut distinction between automorphic groups and isotopic groups.

Keywords: Galois field, iso-Galois field, isotopically isomorphic realization of a group and isopermutation group.
PACS: 11.10.Nx

INTRODUCTION

During a talk at the conference *Differential 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 [1]. This generalization induced the so-called isotopies of the conventional multiplication with consequential generalization of the multiplicative unit, where the Greek word "isotopy" implied 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* [1]. The new ' Isomathematics' eventually led Santilli to formulate a new scientific branch now a days called Hadronic Mechanics.
In this paper we plan to extend the subject of Santilli's iso-field to define Iso-Galois fields [4] which are essentially of non-zero characteristic. In doing so we will start with a brief review of Santilli isomathematics [5] and [6]. Isotopically isomorphic realizations of a group define isopermutation group which gives a clear cut distinction between automorphic groups and isotopic groups. The preliminary results of our efforts are given below [4].

Santilli's Isofield

Definition 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 multiplying unit of F in which case $\hat{F}$ satisfies all axioms of a field.*

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 [5, 6]. 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 [7]. Santilli iso-numbers, which are the mathematical basis of Hadronic Mechanics, are also introduced and reviewed in [8].

Santilli's Isofields [1] and [5] 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.

Proceedings of the International Conference on Numerical Analysis and Applied Mathematics 2014 (ICNAAM-2014)
AIP Conf. Proc. 1648, 510002-1–510002-5; doi: 10.1063/1.4912707

We mention two important propositions by Santilli [2] which classify isofields of second kind and isofields of first kind respectively.

Proposition 1. *The necessary and sufficient condition for the lifting (where the multiplication is lifted but elements are not) $F(a,+,\times) \longrightarrow \hat{F}(a,+,\hat{\times})$, $\hat{\times} = \times\hat{T}\times$, $\hat{1} = \hat{T}^{-1}$ 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.*

Proposition 2. *The lifting (where both the multiplication and the elements are lifted) $F(a,+,\times) \longrightarrow \hat{F}(\hat{a},+,\hat{\times})$, $\hat{a} = a\times\hat{1}$, $\hat{\times} = \times\hat{T}\times$, $\hat{1} = \hat{T}^{-1}$ constitutes an isotopy even when the multiplicative isounit $\hat{1}$ is not an element of the original field.*

In [4] we answer the open problems posed in [10], namely;

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

in the affirmative.

ISO-GALOIS FIELDS

Definition 2. *A field having finite number of elements is called a Galois field.*

In view of Proposition 1 we can easily derive the following new Proposition.

Proposition 3. *The necessary and sufficient condition for the lifting (where the multiplication and elements both are lifted) $F(a,+,\times) \longrightarrow \hat{F}(\hat{a},+,\hat{\times})$, $\hat{\times} = \times\hat{T}\times$, $\hat{1} = \hat{T}^{-1}$ 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.*

Thus for a given field $F(a,+,\times)$ with a non-null element $\hat{T} \in F$ we can construct two types of isofields isotopic to F as;

1. The isofield $\hat{F}_m = \hat{F}(a,+,\hat{\times})$ isotopic to F in which only the multiplication is lifted but the elements are not lifted.
2. The isofield $\hat{F}_{em} = \hat{F}(\hat{a},+,\hat{\times})$ isotopic to F in which the elements and the multiplication both are lifted.

Given a field F the following two Propositions give the relationship between the $\hat{F}_m$ and $\hat{F}_{em}$.

Proposition 4. *If F is a field, $a,b \in F$ and, x and y are the corresponding isotopic (or conventional) products of a and b in $\hat{F}_m$ and $\hat{F}_{em}$ respectively (i.e. $x \in \hat{F}_m$ and $y \in \hat{F}_{em}$), then $x = y\hat{T}^2$ where $\hat{T}$ is the isotopic element for $\hat{F}_m$ and $\hat{F}_{em}$.*

Proposition 5. *If F is a field such that $\hat{T}$ is a non-null element of F, then lifting of multiplication in F by $\hat{T}$ without lifting the elements of F identically is same as simultaneous isotopic lifting of elements in F and multiplication by $\hat{T}^{-1}$.*

e.g. consider the the field of reals $\mathbb{R}$. Let the isotopic element be 3. Then lifting of the product of 5 and 7 by 3 yields $5\hat{\times}7 = 5.3.7 = 105$. Also, lifting the numbers 5 and 7 by 3 and product by $\frac{1}{3}$ yields the same result; $(5.3).\frac{1}{3}.(7.3) = 5.3.7 = 105$.

Corollary 1. *Every isofield of second kind with isoelement $\hat{T}$ is an isofield of first kind with isoelement $\frac{1}{\hat{T}}$.*

Definition 3. *If F is an iso-field and F is finite, then F is called an Iso-Galois field.*

Definition 4. *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 5. *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**.

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.

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 $\hat{1} = \frac{1}{\hat{T}} = \frac{1}{4} = 4^{-1} = 5$. We can construct the corresponding composition table for isomultiplication in $\hat{F}_m$ using the fact that the isomultiplication $\hat{\times}$ is defined as $a \hat{\times} b = a\hat{T}b$.
e.g. $6 \hat{\times} 7 = 6 \cdot 4 \cdot 7 = 1$ using original composition table.
Similarly, we can construct the corresponding composition table for isomultiplication in $\hat{F}_{em}$ using the fact that the isomultiplication $\hat{\times}$ is defined as $\hat{a} \hat{\times} \hat{b} = \frac{a}{\hat{T}} \hat{T} \frac{b}{\hat{T}}$.
We know that for $a \in F_8$, $\hat{a} = a \cdot \frac{1}{\hat{T}} = a \cdot 5$. Hence first 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 $\hat{7} = 4$.
Also the isoproduct of the isonumbers $\hat{6}$ and $\hat{7}$ is $\hat{6} \hat{\times} \hat{7} = 3 \cdot 4 \cdot 4 = 2$ using original composition table.

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

Theorem 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.*

Theorem 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.*

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; $(0) = (0,0,0,0)$, $(1) = (1,0,0,0)$, $(2) = (0,1,0,0)$, $(3) = (0,0,1,0)$, $(4) = (0,0,0,1)$, $(5) = (1,1,0,0)$, $(6) = (0,1,1,0)$, $(7) = (0,0,1,1)$, $(8) = (1,1,0,1)$, $(9) = (1,0,1,0)$, $(10) = (0,1,0,1)$, $(11) = (1,1,1,0)$, $(12) = (0,1,1,1)$, $(13) = (1,1,1,1)$, $(14) = (1,0,1,1)$, $(15) = (1,0,0,1)$ 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 isounit $\hat{1} = \frac{1}{\hat{T}} = \hat{T}^{-1} = 2^{-1} = 15$. 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 we get the isofield is $\hat{F}_1 = \{0,15,5,10\}$ with isomultiplication of the type; 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 corresponding isomultiplication.

Theorem 3. *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 $p^n - p^m - r$ number of distinct Iso-Galois fields of first kind of F_1.*

ISOTOPICALLY ISOMORPHIC REALIZATION

Santilli's isofields have multiplicative group which is isotopically isomorphic realization (when the isounit is from the field itself) or isotopically isomorphic representation (when the isounit is from outside the field) of the multiplicative group of the original field. For a given group G if we consider all permutations of the group elements, then there exist permutations which are the right regular representations, and permutations which are the left regular representations of G. In this case, each permutation is actually an isogroup with respect to the induced isounit and isomultiplication. Thus the permutation group of a group G always contains the group of automorphisms of G and the group of isopermutations (left and right) of G. Hence representation of a group G as (left and/or right) isopermutation group can have extensive applications in cryptography, coding theory and biological sciences wherein the codes and the keys are to be continuously changing for the strongest security.

Isotopism of the fields [1, 2, 3] defined by R.M. Santilli induces isotopism of the groups in the following manner.

Definition 6. *If G is a group then the permutation f_l (or f_r) of the elements of G by $a \in G$ from the left (or right) is an isogroup $\widehat{G}$ with isomultiplication $\widehat{\times}$ defined on it. We say that $\widehat{G}$ is the* ***left-isotopically isomorphic realization*** *(or* ***right-isotopically isomorphic realization****) of the group G.*

Thus, G itself is the isotopically isomorphic realization (both left and right) of the group G where $a = e$.

Definition 7. *If G is a group then the set of all f_ls (or f_rs) corresponding to the left-isotopically isomorphic realizations (or right-isotopically isomorphic realizations) of G is called the* ***left-isopermutation group*** *(or* ***right-isopermutation group****).*

Definition 8. *A group for which both left-isopermutation group and right-isopermutation group coincide is called an* ***Iso-permutation group****.*

Remark:- 1) Note that if the group G is abelian then both left-isotopically isomorphic realizations and right-isotopically isomorphic realizations of G are same. Hence G is an isopermutation group.
2) Also, the left-isopermutation group of G is the left regular representation of G which is faithful. Similarly, the right-isopermutation group of G is the right-regular representation of G which is faithful.

Proposition 6. *The isomorphic realizations of a group G consist of a class of automorphisms of the group G and the class of translations of the group G by the elements from the group G itself.*

Proposition 7. *Permutations which represent the isotopically isomorphic groups of a group G form a subgroup of the group S_G.*

Proposition 8. *If G is an abelian group of order n then the number of isotopically isomorphic realizations of G is n.*

Proposition 9. *If G is a non-abelian group of order n then the number of isotopically isomorphic realizations of G is* $2n-1$.

Proposition 10. *Holomorph of a group is the semidirect product of Aut(G) and left-isopermutation group (or right-isopermutation group) of G.*

Proposition 11. *If G is a group then the left-isopermutation group of G (right-isopermutation group of G) is the centralizer of right-isopermutation group of G (left-isopermutation group of G) in the holomorph of the group G.*

The work is in progress to cover additional relevant aspects of isopermutation group and will also be presented at ICNAAM 2014 in its Session 109 hosted by the R. M. Santilli Foundation being held at Rhodes, Greece during September 22-26, 2014.

Acknowledgements: I sincerely thank Santilli Foundation for full finanancial support to present my work at ICNAAM 2014 in its Session 109 hosted by the R. M. Santilli Foundation being held at Rhodes, Greece during September 22-26, 2014. I would also like to thank Professor R.M.Santilli, Professor Richard Anderson, Professor Christian Corda, Professor Svetlin Georgiev and Professor Anil Bhalekar for their valuable suggestions and comments.

REFERENCES

1. R. M. 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*, Vol. 10, 273-322 (1993). http://www.santilli-foundation.org/docs/Santilli-34.pdf
2. R. M. Santilli, *Foundations of Hadronic Chemistry*, Kluwer Academic Publisher, Dordrecht, 2001. http://www.santilli-foundation.org/docs/Santilli-113.pdf.
3. R. M. Santilli, Isotopies of contemporary mathematical structures, II; Isotopies of symplectic geometry, affine geometry, Riemanian geometry and Einstein gravitation, *Algebras, Groups and Geometries*, Vol. 8, 275-390, (1991).
4. A. S. Muktibodh, Iso-Galois fields, *Hadronic Journal*, Vol. 36 (2), 225 (2013).
5. R. M. Santilli, *Elements of Hadronic Mechanics*, Vol. I and II, Ukraine Academy of Sciences, Kiev, second edition 1995
   http://www.santilli-foundation.org/docs/Santilli-300.pdf
   http://www.santilli-foundation.org/docs/Santilli-301.pdf
6. R. M. Santilli, *Hadronic Mathematics, Mechanics and Chemistry*. Vol. I, II, III, IV and V, Palm Harbor, FL 34682, U.S.A.: International Academic Press, 2008.
   http://www.i-b-r.org/docs/HMMC-1-02-26-08.pdf,
   http://www.i-b-r.org/docs/HMMC-II-01-19-08.pdf.
   http://www.i-b-r.org/docs/HMMC-III-02-26-08.pdf.
   http://www.i-b-r.org/docs/HMMC-12-15-08.pdf.
   http://www.i-b-r.org/docs/HMMC-V-01-26-08.pdf.
   http://www.i-b-r.org/Hadronic-Mechanics.htm
7. J. V. Kadeisvili, The Rutherford-Santilli Neutron, *Hadronic Journal*,Vol. 31, 1-114 (2008)
   http://www.i-b-r.org/Rutherford-Santilli-II. pdf
8. Christian Corda, Introduction to Santilli iso-numbers, *American Institute of Physics, AIP Conf. Proc.* Vol.. 1479, 1013 (2012); doi: 10.1063/1.4756316.
9. R. M. Santilli, Nonlocal-Integral Isotopies of Differential Calculus, Mechanics and Geometries in Isotopies of Contemporary Mathematical Structures, P. Vetro Editor, *Rendiconti Circolo Matematico Palermo, Suppl.*, Vol. 42, 7-82 (1996).
   http://www.santilli-foundation.org/docs/Santilli-37.pdf
10. A. S. Muktibodh, Foundations of Isomathematics, *American Institute of Physics, AIP Conference Proceedings*, Vol. 1558,707 (2013); DOI: 10.1063/1.4825589.
11. R. M. Santilli, *Foundation of Theoretical Mechanics*, Vol. I, Springer-Verlag, Heidelberg, Germany (1978)
    http://www.santilli-foundation.org/docs/Santilli-209.pdf
12. *Foundation of Theoretical Mechanics*, Vol. II, Springer-Verlag, Heidelberg, Germany, (1982)
    http://www.santilli-foundation.org/docs/santilli-69.pdf
13. Chun-Xuan Jiang, *Foundations of Santilli's Isonumber Theory, with applictions to New Cryptograms, Fermat's Theorem and Goldbach's Conjecture*, International Academic Press, Palm Harbor,2002.
14. D. J. S. Robinson, *A course in the Theory of Groups*, 2nd edition, Springer-Verlag, Newyork, 1996.