Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Enrico G. Beltrametti, Alberto Blasi

On rotations and Lorentz transformations in a Galois space-time

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **46** (1969), n.4, p. 390–394.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1969_8_46_4_390_0>

Geometrie finite. — *On rotations and Lorentz transformations in a Galois space–time.* Nota di ENRICO G. BELTRAMETTI e ALBERTO BLASI, presentata [*] dal Socio B. SEGRE.

RIASSUNTO. — Un precedente studio delle proprietà del gruppo delle rotazioni e del gruppo di Lorentz (proprio ed improprio) operanti in uno spazio-tempo di Galois d'ordine p primo e $\equiv 3 \pmod 4$, vengono qui generalizzate al caso di una geometria d'ordine p^n, dove n è dispari e p è soggetto alla sopraddetta condizione. Si discutono e si dimostrano esplicitamente, in quest'ultimo caso più generale, le condizioni di irriducibilità delle rappresentazioni modulari dei gruppi in questione.

1.—INTRODUCTION.

In previous papers [1, 2, 3] we examined the relativistic transformation groups in a finite space-time thought of as a Galois geometry over a primitive field GF (p) with $p \equiv 3 \pmod 4$. This condition on p allowed a distinction of the elements of GF (p) into "positive" and "negative" ones, in analogy to the real numbers; moreover it allowed the construction of a completely ordered subset of GF (p), which satisfies some elementary physical requirements. In the above context we studied the properties of the rotation and Lorentz groups, we found explicitly their modular representations defined on GF (p^2) and gave criteria to single out the irreducible ones.

In this note we first extend the results to the case of a finite space-time built on a Galois field GF (p^n) with $p \equiv 3 \pmod 4$, n odd [1]; in the last Section we exhibit rigorous proofs of the result concerning the classification of the irreducible modular representations.

2.—EXTENSION TO GF (p^n).

To extend the result given in references [1, 2, 3] to the more general case of a basic field GF (p^n), we must impose two requirements on the field itself. First, if x is a square element of GF (p^n), the opposite $-x$ should be a not-square, i.e. the element -1 should be not-square, in analogy with the real numbers. Secondly, it should be possible to consider GF (p^{2n}) as the "complexification" of GF (p^n) with some definition of complex conjugate.

Now, let w be a primitive root in GF(p); since $w, w^2 \cdots w^{p-1}$ and zero span the whole field and $w^{p-1} = 1$, [4], we shall have $w^{(p-1)/2} = -1$. The condition for (-1) to be a not-square becomes $\frac{p-1}{2} = 2k - 1$ or $p \equiv 3 \pmod 4$.

[*] Nella seduta del 19 aprile 1969.

[1] We deeply thank Professor Beniamino Segre for suggesting this generalization.

Passing to GF (p^n) we know, [4], that the not-squares of GF (p) remain such in GF (p^n) if and only if n is odd, while for n even they become squares. Then $p \equiv 3 \pmod 4$ and n odd insure the first requirement is met. Moreover, by the above remark, there is an element $i \in \mathrm{GF}(p^{2n})$ such that $i^2 = -1$. We are now able to prove that any $z \in \mathrm{GF}(p^{2n})$ can be written as $x + iy$, with $x, y \in \mathrm{GF}(p^n)$ and its complex conjugate is $z^* = z^{p^n} = x - iy$.

In fact, $\mathrm{GF}(p^{2n}) = \mathrm{GF}(p^n) \otimes \mathrm{GF}(p^n)$ by a dimensionality argument; moreover $i^{p^n} = -i$ according to simple calculations with primitive roots in GF (p^{2n}), so that

$$(x + iy)^{p^n} = \sum_{k=0}^{p^n} \binom{p^n}{k} x^{p^n-k} (iy)^k = x^{p^n} + (iy)^{p^n} +$$

$$+ \sum_{k=1}^{p^n-1} p^n \left[\frac{(p^n - 1)(p^n - 2) \cdots (p^n - k + 1)}{k!} \right] x^{p^n-k} (iy)^k$$

and, by Fermat's theorem [4], $x^{p^n} = x$, $(iy)^{p^n} = -iy$ while the remaining sum contains a p as a factor and hence is congruent to zero. For different proofs of these results cfr. B. Segre [9], n. 5.

We only mention that the length of the Euclidean chain, defined as the set of consecutive elements which are transitively ordered [1], contains at least as many elements as the Euclidean chain in GF (p).

We shall now briefly sketch the procedure to generalize the results to the case of a Galois geometry of order p^n, $p \equiv 3 \pmod 4$, n odd: the process is carried out for the sole rotation group and, as one might expect, the only change is the replacement of p by p^n, with all the propositions given in [1, 2, 3] still valid. Construct a 3-dimensional finite geometry with vectors (x_1, x_2, x_3) where $x_1, x_2, x_3 \in \mathrm{GF}(p^n)$; the proper rotation group $\mathrm{R}(3, p^n)$ is the group of linear homogeneous transformations r:

$$x'_i = \sum_{j=1} r_{ij} x_j , \qquad \det \; r = 1,$$

which leave invariant the quadratic form $x_1^2 + x_2^2 + x_3^2$. Its order is $\Omega_{\mathrm{R}(3,p^n)} = p^n (p^{2n} - 1)$, [5]. This group is one-to-two homomorphic to the group $\mathrm{SU}^{(\pm)}(2, p^{2n})$ of 2×2 matrices of the form

$$u = \begin{pmatrix} \alpha & \beta \\ -\beta^* & \alpha^* \end{pmatrix} \quad , \quad \alpha, \beta \in \mathrm{GF}(p^{2n}), \qquad \det \; u = \pm 1,$$

(remark that $uu^\dagger = u^\dagger u = \det(u)$). The order of $\mathrm{SU}^{(\pm)}(2, p^{2n})$ is $\Omega_{\mathrm{SU}^{(\pm)}(2,p^{2n})} = 2 p^n (p^{2n} - 1)$ and the explicit formulae of the mapping are the same as those given in ref. [1]. The subgroup $\mathrm{SU}^{(\pm)}(2, p^{2n}) = \{u \mid u \in \mathrm{SU}^{(\pm)}(2, p^{2n}), \det(u) = 1\}$ individuates a subgroup $\mathrm{R}^{(+)}(3, p^n)$ of $\mathrm{R}(3, p^n)$ whose order is $1/2 \; \Omega_{\mathrm{R}(3,p^n)}$.

The explicit construction of the irreducible modular representations is easily carried out for $\mathrm{SU}^{(\pm)}(2, p^{2n})$; this group has $2 p^n$ equivalence classes individuated by the trace and the determinant of the defining matrix. According to a heuristic procedure, justified rigorously in the next section, there should be $2\,p^n$ inequivalent irreducible representations of the group $\mathrm{SU}^{(\pm)}(2\,,\,p^{2n})$. Consider the monomials

$$f_m^{(j)}(\xi\,,\,\eta)=\mathrm{N}_m^{(j)}\,\xi^{j+m}\,\eta^{j-m}\,,\qquad \text{with}\quad \mathrm{N}_m^{(j)},\,\xi\,,\,\eta\in\mathrm{GF}\,(p^{2n})$$

where j and m are both integers or half-integers and $-j\leq m\leq j\,,\,j\geq 0$; under a transformation u^{-1} of $\mathrm{SU}^{(\pm)}(2\,,\,p^{2n})$ acting on the pair $\xi\,,\,\eta$,

$$f_m^{(j)}(\xi\,,\,\eta)\rightarrow f_m^{(j)}((\alpha^*\,\xi-\beta\eta)\,,\,(\beta^*\,\xi+\alpha\eta))=\sum_{m'}\mathrm{D}_{m',m}^{(j,0)}(u)\,f_{m'}^{(j)}(\xi\,,\,\eta)$$

where

$$\mathrm{D}_{m',m}^{(j,0)}(u)=\frac{\mathrm{N}_m^{(j)}}{\mathrm{N}_{m'}^{(j)}}\sum_{k=\max(0,m-m')}^{\min(j+m,j-m')}\binom{j+m}{k}\binom{j-m}{k+m'-m}\alpha^{j-m'-k}\,\alpha^{*\,j+m-k}\,(-\beta)^k\,\beta^{*\,k-m+m'}.$$

Thus we have individuated a series of representations $\mathrm{D}^{(j,0)}(u)$ labeled by the integer or half-integer index j. Since $\mathrm{D}^{(j,0)}(u)$ has dimensionality $(2\,j+1)$, these representations are all inequivalent. Another series of inequivalent representations is obtained setting $\mathrm{D}_{m,m'}^{(j,1)}(u)=\det(u)\,\mathrm{D}_{m,m'}^{(j,0)}(u)$; in the next section we shall treat in detail the problem of the irreducibility of these two series, and the outcome will be that both $\mathrm{D}^{(j,0)}$ and $\mathrm{D}^{(j,1)}$ are irreducible for $j\leq\frac{p^n-1}{2}$, while they are reducible for $j>\frac{p^n-1}{2}$. The extension to the proper and improper Lorentz group is performed exactly in the same manner as in [1, 2, 3]: all the results there discussed remain valid if p is changed into p^n.

3.—Proof of the irreducibility conditions.

We shall here provide rigorous proofs of the results stated in [1, 2, 3] about the irreducible modular representations of the relativity groups.

The need for such proofs stems from the fact that the theorems about equivalence classes and irreducible representations no longer hold in their classical form. In particular Schur's lemma now reads [6]: given an irreducible modular representation $\mathrm{D}(g)$ of a group G, the only matrix which commutes with $\mathrm{D}(g)\,,\,\forall\,g\in\mathrm{G}$ is a multiple of the unit matrix. This is a necessary (but not sufficient) condition for a modular representation to be irreducible.

About equivalence classes we have [7]: let G be a finite group and K a field of characteristic p; if K is a splitting field for G, then the number of irreducible, inequivalent representations of G over K is equal to the number of p–regular equivalence classes of G. K is a splitting field for G if any irreducible modular representation of G over K remains irreducible for any extension of K. An element x of G is p-regular if $x^k=1$ with kP (k non divisible by p); a p–regular class is formed by p–regular elements. Note that if an equivalence class contains a p–regular element, then the whole class is p-regular since $(yxy^{-1})^k = yx^k y^{-1}$.

Let us remark that a sufficient condition for K to be a splitting field for G is that all the m–th roots of 1 belong to K, where m is the least common multiple of the orders of the elements of G, [8]. We then prove:

PROPOSITION 1. *The group* $\mathrm{SU}^{(\pm)}(2\,,p^{2n})$ *has all its equivalence classes* p*–regular and* $\mathrm{GF}(p^{2n})$ *is a splitting field for the group.*

We shall consider only the subgroup $\mathrm{SU}^{(+)}(2\,,p^{2n})$, since the extension to the whole group is trivial. $\mathrm{SU}^{(+)}(2\,,p^{2n})$ has p^n equivalence classes individuated by the p^n values of the trace of the general element: then each equivalence class contains an element of the form $v = \begin{pmatrix} a & c \\ -c^* & a \end{pmatrix}$ with $a \in \mathrm{GF}(p^n)$, $c \in \mathrm{GF}(p^{2n})$ and $a + cc^* = 1$. Now, the nonsingular matrix

$$\mathrm{T} = t \begin{pmatrix} 1 & \dfrac{c}{\sqrt{a^2 - 1}} \\ \dfrac{c^*}{\sqrt{a^2-1}} & 1 \end{pmatrix}, \qquad (t \in \mathrm{GF}(p^{2n}))$$

is such that $\mathrm{T}v\mathrm{T}^{-1} = \begin{pmatrix} \mathrm{L}^+ & 0 \\ 0 & \mathrm{L}^- \end{pmatrix}$ where $\mathrm{L}^\pm = a \pm \sqrt{a^2 - 1}$ are the eigenvalues of v. Then, if $v^k = 1$ it follows $(\mathrm{T}v\mathrm{T}^{-1})^k = \mathrm{T}v^k\mathrm{T}^{-1} = 1$ and so $(\mathrm{L}^\pm)^k = 1$, but since $\mathrm{L}^\pm \in \mathrm{GF}(p^{2n})$, k is either equal to $p^{2n} - 1$ or to one of its divisors, [4], and in any case kp, which implies v is p–regular.

Hence all equivalence classes contain a p–regular element and are therefore p–regular. Moreover, the least common multiple of the orders of the elements of G is at most $p^{2n} - 1$, and we know all $(p^{2n} - 1)$–th roots of 1 belong to $\mathrm{GF}(p^{2n})$ [4]. This proves $\mathrm{GF}(p^{2n})$ is a splitting field for $\mathrm{SU}^{(+)}(2\,p^{2n})$.

For what concerns the irreducibility we have:

PROPOSITION 2. *The representations* $\mathrm{D}^{(j,e)}(u)\,, 0 \leq j \leq \dfrac{p^n - 1}{2}\,,\ e = 0\,,1$ *are all the irreducible, inequivalent modular representations of* $\mathrm{SU}^{(\pm)}(2\,,p^{2n})$.

Let us restrict to the subgroup $\mathrm{SU}^{(+)}(2\,,p^{2n})$ and to $\mathrm{D}^{(j)}(u) \equiv \mathrm{D}^{(j,0)}(u)$ since the extension to the general case is obvious. The proof of the irreducibility is by induction on the index j. $\mathrm{D}^{(0)}$ is irreducible since it is one dimensional; suppose the same is true for $j = l$ and assume $\mathrm{D}^{(l+1)}$ is reducible. The reducibility assumption ensures the existence of a $2(l+1)+1$ square matrix V such that

$$\mathrm{VD}^{(l+1)}(u)\,\mathrm{V}^{-1} = \left(\begin{array}{c|c} \mathrm{A}(u) & 0 \\ \hline \mathrm{C}(u) & \mathrm{B}(u) \end{array}\right), \qquad \forall u \in \mathrm{SU}^{(+)}(2\,,p^{2n}),$$

where $\mathrm{A}(u)$ and $\mathrm{B}(u)$ are irreducible representations according to the induction hypothesis; furthermore $\mathrm{A}(u)$ is equivalent to $\mathrm{D}^{(s)}(u)$ and $\mathrm{B}(u)$ is equivalent to $\mathrm{D}^{(l-s+(1/2))}(u)$ for some index $s < l + 1$. It follows:

$$\mathrm{Tr}(\mathrm{D}^{(l+1)}(u)) = \mathrm{Tr}(\mathrm{A}(u)) + \mathrm{Tr}(\mathrm{B}(u)) = \mathrm{Tr}(\mathrm{D}^{(s)}(u)) + \mathrm{Tr}(\mathrm{D}^{(l-s+(1/2))}(u)).$$

The above relation, applied to the particular element $u = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^* \end{pmatrix}$, yields [1]

$$\sum_{m=-l-1}^{l+1} \alpha^{l+1-m}\, \alpha^{*\,l+1+m} = \sum_{r=-s}^{s} \alpha^{s-r}\, \alpha^{*\,s+r} + \sum_{t=-l+s-(1/2)}^{l-s+(1/2)} \alpha^{l-s+(1/2)-t}\, \alpha^{*\,l-s+(1/2)+t}.$$

Notice that the l.h.s. polynomial contains powers of $\alpha\alpha^*$ different from those of the r.h.s. and the equality cannot be satisfied with $\alpha \in \mathrm{GF}(p^{2n})$ unless $2(l+1) \geq p^n$, in which case $\alpha^{2(l+1)} = \alpha^{2(l+1)-p^n+p^n} = \alpha^{*\,2(l+1)-p^n}$ and $\alpha^{*\,(2l+1)} = \alpha^{(2l+1)-p^n}$ so that the role of α and α^* is interchanged and the degree of the polynomial in $\alpha\alpha^*$ is lowered by p^n. We have thus proved that $\mathrm{D}^{(j,0)}(u)$ are irreducible for $j \leq \frac{p^n-1}{2}$ but we still have to show they are certainly reducible for $j > \frac{p^n-1}{2}$. This is accomplished by applying Schur's Lemma, i.e. by showing that, if $j > \frac{p^n-1}{2}$, there exists a nondiagonal matrix $\mathrm{A}^{(j)}$ which commutes with all the representative elements.

Consider again $u = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^* \end{pmatrix}$; the condition $[\mathrm{D}^{(j,0)}(u), \mathrm{A}^{(j)}] = 0$ implies [1]

$$\mathrm{A}^{(j)}_{m,m'}\,(\alpha^{(m-m')(p^n-1)} - 1) = 0 \qquad \text{which gives}$$

$$\mathrm{A}^{(j)}_{m,m'} = a_m\, \delta_{m,m'} + b_m\, \delta_{m',\, m-k(p^n+1)}$$

where k is any integer.

Now $\forall u \in \mathrm{SU}^{(+)}(2, p^{2n})$ the commutation condition $[\mathrm{A}^{(j)}, \mathrm{D}^{(j,0)}(u)]_{m,m'} = 0$ yields, choosing $b_m = 0$, $a_m\, \mathrm{D}^{(j,0)}_{m,m'}(u) = a_{m'}\, \mathrm{D}^{(j,0)}_{m,m'}(u)$ which can be satisfied for $a_m \neq a_{m'}$ considering that $\mathrm{D}^{(j,0)}_{m,m'}(u) = 0$, $\forall u \in \mathrm{SU}^{(+)}(2, p^{2n})$ if $j \geq \frac{p^n+1}{2}$, $j > m \geq p^n - j, -j + p^n - 1 > m' \geq j - p^n + 1$ [1].

Thus a non diagonal matrix $\mathrm{A}^{(j)}$ exists, which commutes with the representation $\mathrm{D}^{(j,0)}(u)$ if $j \geq \frac{p^n+1}{2}$: this completes the proof of the irreducibility conditions.

References.

[1] E. Beltrametti and A. Blasi, « J. Math. Phys. », *9*, 1027 (1968).

[2] E. Beltrametti and A. Blasi, « Nuovo Cimento », *55 A*, 301 (1968).

[3] E. Beltrametti and A. Blasi, « Atti Acc. Naz. Lincei Cl. Sc. Fis. Mat. Natur. », *44*, 384 (1968).

[4] L. Dickson, *Linear Groups*, Ch. I (Dover Publ. Inc. New York 1958).

[5] *Ibid.*, Ch. VII.

[6] C. Curtis and I. Reiner, *Represe tation theory of finite groups and associative algebras*, p. 181 (J. Wiley & Sons Inc. New Yor 1962).

[7] *Ibid.*, pp. 587 and 591.

[8] *Ibid.*, pp. 475 and 590.

[9] B. Segre, *Forme e geometrie herr itiane, con particolare riguardo al caso finito*, « Annali di Matematica », (4) *70*, 1 (1965).