Lecture notes from a series of lectures delivered at the Summer Study Institute on Combinatorial Mathematics and Its Applications in the Natural Sciences, held on June 2-27, 1969, in Chapel Hill, and sponsored by the U.S. Air Force Office of Scientific Research under Air Force Grant No. AFOSR-68-1406 and the U.S. Army Research Office (Durham) under Grant No. DA-ARO-D-31-124-G910.

0	7	8	9	1	3	5	2	4	6
6	1	7	8	9	2	4	3	5	0
5	0	2	7	8	9	3	4	6	1
4	6	1	3	7	8	9	5	0	2
						8	6	1	3
						7	0	2	4
						6	1	3	5
						0	7	8	9
						1	9	7	8
						2	8	9	7

0	6	5	4	9	8	7	1	2	3
7	1	0	6	5	9	8	2	3	4
8	7	2	1	0	6	9	3	4	5
9	8	7	3	2	1	0	4	5	6
1	9	8	7	4	3	2	5	6	0
3	2	9	8	7	5	4	6	0	1
5	4	3	9	8	7	6	0	1	2
2	3	4	5	6	0	1	7	8	9
4	5	6	0	1	2	3	8	9	7
6	0	1	2	3	4	5	9	7	8

C O M B I N A T O R I A L
M A T H E M A T I C S
Y E A R

February 1969 - June 1970

RELATIVITY GROUPS IN A FINITE SPACE-TIME

by

E.G. Beltrametti* and A. Blasi*

Institute of Statistics Mimeo Series No. 600.13
Department of Statistics
Univeristy of North Carolina at Chapel Hill

JUNE 1969

*Istituto di Fisica Teorica dell'Università di Genova, Italy
Istituto Nazionale di Fisica Nucleare-Sez.di Genova

Relativity Groups in a Finite Space-time

by

E.G. Beltrametti and A. Blasi
Istituto di Fisica Teorica dell'Università di Genova, Italy
Istituto Nazionale di Fisica Nucleare-Sez.di Genova

INTRODUCTION. In these lectures, we shall discuss some points concerning the question: how far can the physical space-time be thought of as a finite collection of points whose space co-ordinates x_1, x_2, x_3 and time co-ordinate x_0 take values in some finite set (k) containing k marks? To be sure, the question is quite unpopular in physics since the language of dynamical physical laws is the one of differential equations. In spite of this, it may be shown that some symmetry properties of the finite space-time look attractive for physical interpretations. We shall be mainly concerned with the symmetries displayed by standard relativity groups, namely three-dimensional rotations, proper and improper Lorentz transformations acting onto the finite space-time. This imposes that (k) be closed under linear transformations $x'_\mu = \Sigma_\nu\, l_{\mu\nu}\, x_\nu$, x_ν, $l_{\mu\nu} \in (k)$ which leave invariant some quadratic form of the variables x_0, x_1, x_2, x_3; thus we are naturally led to assume the set (k) to be a finite field $GF(k)$ [1].

Letting $c_0, c_1, \ldots, c_{k-1}$ be the elements of $GF(k)$, denote by $c_i + c_j$ (addition) and by $c_i c_j$ (multiplication) the two binary operations in the field: in particular

---

Lecture notes from a series of lectures delivered at the Summer Study Institute on Combinatorial Mathematics and Its Applications in the Natural Sciences, held on June 2-27, 1969, in Chapel Hill, and sponsored by the U.S. Air Force Office of Scientific Research under Air Force Grant No. AFOSR-68-1406 and the U.S. Army Research Office (Durham) under Grant No. DA-ARO-D-31-124-G910.

(i) a unique element, say c_0, exists having the properties of "zero" under addition $(c_i + c_0 = c_i, \forall c_i)$: it will also be denoted by 0; the unique element giving 0 when added to c_i will be denoted by $-c_i$;

(ii) a unique element, say c_1, exists having the properties of "unity" under multiplication $(c_i c_1 = c_i, \forall c_i)$: it will also be denoted by 1; the unique element giving 1 when multiplied by c_i will be denoted by c_i^{-1} or $\frac{1}{c_i}$.

As well known, a finite field $GF(k)$ exists only if $k=p^n$, p being a prime, n an integer: moreover $GF(p^n)$ is uniquely determined by the number p^n of its elements, since all finite fields of the same order are isomorphic. The integral mark obtained by iterating m times the sum $1+1+\ldots+1$ will be denoted by m. Let us recall in particular that

$$px = 0, \qquad \forall x \in GF(p^n), \tag{0.1}$$

i.e., $GF(p^n)$ has characteristic p, and that Fermat's theorem holds:

$$x^{p^n} = x, \qquad \forall x \in GF(p^n) \tag{0.2}$$

The finite space-time we are concerned with is thus what is usually called a Galois geometry. From a mathematical point of view, these geometries have been extensively studied especially by the school of B. Segré [2]. The problem of whether a Galois geometry can be adopted for a description of the physical space is not at all straightforward; it has been worked out some years ago by the Finnish school of G. Järnefelt and P. Kustaanheimo [3], showing that, under some restrictions on the order p^n, they are actually nonheretical for physical purposes. This problem will be shortly accounted for in Section 1.

We shall not try any reformulation of dynamical physical theories within a Galois geometry: in fact, little has been done in this direction [4]; let us only mention that any field theory would be free from usual divergencies since all integrals would become finite sums. Beyond this dynamical aspect of the problem, H.R. Coish [5] and I.S. Shapiro [6] pointed out the appearence of a number of symmetry properties caused by the very fact of finiteness of space and which are independent of the number of points in it, (i.e., independent of the order of the basic coordinate field $GF(p^n)$); the last author particularly suggested the relevance of these properties for the fundamental theory of weak interactions of elementary particles. In the present study, we are moving along similar lines; part of the results has been already given in previous papers [7,8]. In Section 2, the three-dimensional rotation group and the proper homogeneous Lorentz group over a Galois geometry are defined and their homomorphisms with 2×2 matrix groups are worked out. The relevant modular representations are then discussed in Sections 3,4. Adjoining the space reflection to the proper Lorentz group, we come to some relevant properties of Dirac spinors over a finite field (Section 5): in particular we shall treat (Section 6) the properties displayed by bispinor sesquilinear forms (e.g., the ones occurring in weak-interaction Hamiltonian). If the abelian group of space-time translations is also taken into account one is led to the study of the so called Poincaré group and some problems arise concerning its modular representations: this is shortly discussed in Section 7.

1. COMMENTS ON THE PHYSICALLY ALLOWED FINITE FIELDS. In constructing a new physical theory on finite fields, one has to bear in mind a correspondence principle with classical physical schemes. Thus one needs some minimal algorithm of algebraic operations in $GF(p^n)$ analogous to the usual algebra. It is first of all required to introduce "positive" and "negative" numbers so that the usual rules of signs hold true for algebraic operations. For this purpose, let us recall that the elements of $GF(p^n)$ may be divided into "squares" and "not squares": $x \in GF(p^n)$ is said to be a square if $y \in GF(p^n)$ exists such that $x=y^2$, otherwise it is called a not-square: the element 0 is not recognized either as positive nor as negative and the number of squares equals the one of not squares. Of course, the property of being a square or a not square is combined under multiplication according to the sign rule: in this respect, squares and not squares may be assumed as positive and negative elements respectively. However, in order to have consistency with the sign rules when transposing monomials from one side of an equality to the other, we further require the opposite $-x$ of a square element $x \in GF(p^n)$ to be a not square (and viceversa). Thus the element -1 should be a not square, in analogy with real numbers. Now, let w be a primitive root in $GF(p)$; since $w, w^2 \ldots w^{p-1}$ and 0 span the whole field and $w^{p-1} = 1$, we shall have $w^{\frac{p-1}{2}} = -1$. The condition for (-1) to be a not-square becomes $\frac{p-1}{2} = 2k-1$ or $p \equiv 3 \pmod{4}$. Passing to $GF(p^n)$ we know, 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 we get the requirement

$$p \equiv 3 \pmod{4}, \qquad n \text{ odd}. \tag{1.1}$$

As a further step in the analogy with usual algebra, the condition (1.1) allows us to introduce a "complexification" of $GF(p^n)$. In fact, any element of $GF(p^n)$ becomes a square element of $GF(p^{2n})$: in particular there is an element $i \in GF(p^{2n})$ such that $i^2 = -1$. We are now able to prove that any $z \in GF(p^{2n})$ can be written as $x+iy$, $x,y \in GF(p^n)$, and the complex conjugate $z^* = x-iy$ is obtained as the p^n-th power of z. Actually, by a dimensionality argument, we get $GF(p^{2n}) = GF(p^n) \otimes GF(p^n)$ and by use of (1.1) it easily follows

$$(1.2) \qquad i^{p^n} = -i,$$

hence we get (see (0.2))

$$(1.3) \qquad (x+iy)^{p^n} = \sum_{k=0}^{p^n} \binom{p^n}{k} x^{p^n-k}(iy)^k = x^{p^n} + (iy)^{p^n} = x-iy = (x+iy)^*$$

since the remaining terms in the sum have coefficients divisible by p and vanish because of (0.1).

We may give a meaning to the notion of "greater than" ($>$) and "smaller than" ($<$) defining $x > y$ or $x < y$ according to whether $x-y$ square (positive) or not square (negative). However, it is important to recognize that the sum of two squares can be a not square, so that there is lack of transitivity for inequalities. As a consequence, a geometry whose points have co-ordinates in $GF(p^n)$ would be deprived of usual metric relations: this raises the question of whether a finite geometry can have anything to do with physical space. In this respect, it may be shown [3] that, under conditions like (1.1) the transitive ordering may be ensured over a subset E of N consecutive elements of $GF(p^n)$: a very rough estimate gives $N \sim \ell n\, p$. This ordered region has been called Euclidean, since metrics can formally be introduced in it.

It should be borne in mind, however, that E is not an algebraic field.

Consider, e.g., a three-dimensional space over $GF(p^n)$: the subspace of points having co-ordinates in E looks like a finite lattice with usual geometric relations. By allowing p to become suitably large, this lattice may approximate the observed physical space with arbitrarily high accuracy; however, we are left with the problem that it is not closed with respect to algebraic operations of the basic field $GF(p^n)$.

We believe that such difficulty is not crucial "a priori": according to Shapiro [6], it cannot be taken for granted that the suggestion to use a space-time manifold devoid of metrical properties is wrong, for in the microcosmos the classical space-time concepts lose their direct physical content and exist inasmuch as there exists a theory inherently consistent and in agreement with experiments.

To avoid notational complications, we shall assume $n=1$ from here on: it will be clear that the results given in the next sections hold unchanged if p is replaced by p^n.

We quote some results about quadratic equations. The number ν of sets of solutions $(x_1, x_2, \ldots, x_{2m})$ in $GF(p^n)$ of the equation, $c_1 x_1^2 + c_2 x_2^2 + \ldots + c_{2m} x_{2m}^2 = d$, m integer, c_i and d non-zero elements of $GF(p^n)$ is given by

$$\nu = p^{n(2m-1)} - \eta p^{n(m-1)}$$

where $\eta = 1$ if $(-1)^m c_1 c_2 \ldots c_{2m}$ is square

$= -1$ " is not-square.

Similarly, for $c_1x_1^2 + \dots + c_{2m+1}x_{2m+1}^2 = d$

$$\nu = p^{2nm} + wp^{nm},$$

where $w = 1$ $\quad (-1)^m dc_1c_2 \dots c_{2m+1}$ is square

$= -1$ $\quad$ " $\quad$ is not-square.

2. Lorentz and Rotation Proper Groups over GF(p).

Define the proper Lorentz group $L(4,p)$ as the group of invertible linear substitutions

(2.1) $$x'_\mu = \sum_{\nu=0}^{3} \ell_{\mu\nu} x_\nu; \quad \mu = 0,1,2,3; \quad x_\mu, \ell_{\mu\nu} \in GF(p); \quad \det \ell = +1,$$

which leave $x_0^2 - x_1^2 - x_2^2 - x_3^2$ invariant, (ℓ stands for the 4×4 matrix with elements $\ell_{\mu\nu}$) i.e., $\ell^T g \ell = g$, $g = \text{diag}(1, -1, -1, -1)$. The subgroup $R(3,p)$ of the proper three dimensional rotations is similarly formed by the substitutions:

(2.2) $$x'_i = \sum_{j=1}^{3} r_{ij} x_j; \quad i = 1,2,3; \quad x_i, r_{ij} \in GF(p); \quad \det r = +1,$$

leaving $x_1^2 + x_2^2 + x_3^2$ invariant. We denote by r the 4×4 matrix over $GF(p)$ with $r_{00} = 1$, $r_{0i} = r_{i0} = 0$. Note that $r^T r = I$.

$L(4,p)$ and $R(3,p)$ are finite groups of order

(2.3) $$\Omega_{L(4,p)} = p^2 (p^4 - 1), \quad \Omega_{R(3,p)} = p(p^2 - 1) .$$

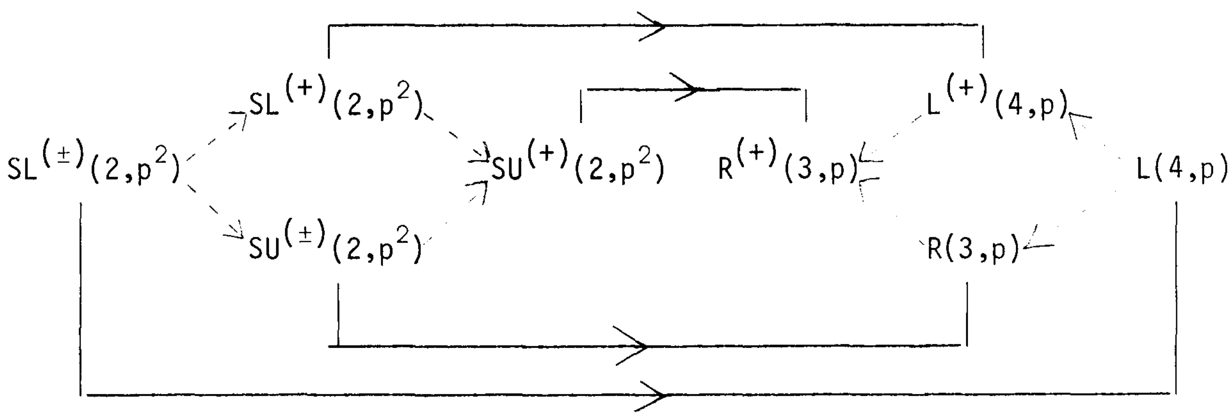
Consider now the group $SL^{(\pm)}(2,p^2)$ of 2×2 matrices over $GF(p^2)$:

$$(2.4)\qquad a = \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \in SL^{(\pm)}(2,p^2); \quad \alpha,\beta,\gamma,\delta \in GF(p^2); \quad \det a = \pm 1;$$

it is a finite group of order $2\Omega_{L(4,p)}$, while the subgroup $SL^{(+)}(2,p^2)$ formed by the matrices having determinant $+1$ has order $\Omega_{L(4,p)}$. Consider also the subgroup $SU^{(\pm)}(2,p^2)$ of $SL^{(\pm)}(2,p^2)$ formed by the matrices

$$(2.5)\qquad u = \begin{pmatrix}\alpha & \beta\\ -\beta^* & \alpha^*\end{pmatrix} \in SU^{(\pm)}(2,p^2); \quad \alpha,\beta \in GF(p^2); \quad \det u = \pm 1\ ,$$

where we notice that the condition $\det u = \alpha\alpha^* + \beta\beta^* = \pm 1$ may be solved in a finite field for both choices of the sign, since a sum of square elements may be a non-square element. $SU^{(\pm)}(2,p^2)$ has order $2\Omega_{R(3,p)}$ while its unitary subgroup $SU^{(+)}(2,p^2)$ formed by the matrices having determinant $+1$ has order $\Omega_{R(3,p)}$. The orders of these groups show that it is impossible to have, according to the simplest analogy with the classical case, a 1 to 2 homomorphism of $L(4,p)$ onto $SL^{(+)}(2,p^2)$ and of $R(3,p)$ onto $SU^{(+)}(2,p\ )$. Indeed, denoting by (┌──>──┐) a 2 to 2 homomorphism and by (– – –>) the transition to a subgroup, one may prove the scheme [5]



Explicitly, the homomorphism between $SL^{(\pm)}(2,p^2)$ and $L(4,p)$, associates to the pair a, $-a$ the Lorentz transformation

$$(2.6) \qquad \ell_{\mu\nu} = \tfrac{1}{2}\,(\det a)\ \mathrm{Sp}(\sigma_\mu\, a\, \sigma_\nu\, a^\dagger), \quad a \in SL^{(\pm)}(2,p^2),$$

where $\sigma_0, \sigma_1, \sigma_2, \sigma_3$ are the usual Pauli matrices and $a^\dagger$ is the hermitian conjugate of a, (of course the factor $\frac{1}{2}$ in (2.6) stands for the inverse of the "integral mark" $(1+1)$ of $GF(p)$). The remaining homomorphisms shown in the previous scheme are particular cases of (2.6). Let us remark that the elements of $R^{(+)}(3,p)$ may be thought of as those rotations for which $\mathrm{Sp}(r)$ is a square in $GF(p)$. A characterization of this kind could also be given for the subgroup $L^{(+)}(4,p)$ homomorphic to $SL^{(+)}(2,p^2)$.

3. Modular Representations of $R(3,p)$ and $L(4,p)$ (Curtis and Reiner [9], Wigner [10], Hamermesh [12]).

When facing the representation problem of the finite geometry groups, we need to choose the field on which the representations have to be defined. Besides the usual possibility of building representations over the complex number field (C-representations), another possibility is self suggesting, i.e., of building representations over a finite field (modular representations). About modular representations, we should say that the classical definition works backwards. Anyway, about their properties more could be said than what has been written here.

List of classical theorems.

(i) No. of equivalence classes = number of irreducible representations. (Proof can be given by group algebra.)

(ii) $\Sigma_k (\dim IR_k)^2 = \Omega_G$.

In our case, we have to consider the formula

$$S_n = \frac{n}{3}(n+1)(n+\tfrac{1}{2})$$

which is the sum of the squares of the first n integer numbers, which applied to 'p' does not yield the correct expression.

(iii) Theorem on unitary equivalence of representations of finite order groups, (Wigner) also fails since there is a sum over all representative elements.

Here we shall be mainly concerned with modular representations: they may be built up explicitly [7] *but some care must be paid, for a number of classical theorems no longer apply* [9]. Classical theorems which do not hold include:

MASHKE THEOREM: every reducible representation of a finite group is decomposable.

This theorem does not hold, since the proof rests on the sum over all group elements, which yields a multiplicative factor equal to the order of the group; but which $\equiv 0 \pmod p$ if their order is divisible by p.

PROOF: We need to find a projection F which decomposes the vector space into a direct sum of invariant subgroups and this projection must commute with all the group representatives. For E, we set $F = \frac{1}{\Omega_G} \Sigma_{x \in G} T(x) E T(x)^{-1}$ which does the trick as long as Ω_G is not divisible by p. In particular, *Schur's lemma now read:* given an irreducible modular representation $D(g)$ of a group G, the only matrix which commutes with $D(g)$, $\forall g \in G$, is a multiple of the unit matrix. This is a necessary (but not sufficient) condition for a modular representation to be irreducible.

A few words on the distinction between p-regular and p-singular elements: Example, why shall we need only p-regular classes $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ matrix with elements in GF(p). If it happens that we can diagonalise it $\to \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ with λ_1 and $\lambda_2 \in GF(p)$, then if the matrix has period k $\Rightarrow (\lambda_1)^k = (\lambda_2)^k = 1$ which at most can be p-1 since

$$x^{p-1} = 1 \qquad \forall\ x \in GF(p),$$

while if the matrix has period np then

$$(\lambda_1)^{np} = [(\lambda_1)^p]^n = (\lambda_1)^n \neq 1$$

and the matrix can not be represented in the field.

The *classical theorem linking equivalence classes to irreducible representations* becomes: 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 $k \nmid p$ (k not 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 $(yxy^{-1})^k = yx^ky^{-1}$.

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.

Consider first the group $SU^{(\pm)}(2,p^2)$ which is homomorphic to R(3,p). We shall make use of Weyl's method by introducing as a basis of the carrier space the homogeneous monomials in $GF(p^2)$,

$$f_m^{(j)}(\xi,\eta) = N_m^{(j)}\xi^{j+m}\eta^{j-m} \quad : N_m^{(j)},\xi,\eta \in GF(p^2),$$

where $j+m$ and $j-m$ are both positive integer numbers, i.e., j and m are both integers or half integers with $-j \leq m \leq j$, $j \geq 0$.

$u \in SU^{(\pm)}(2,p^2)$ is written in the form

$$u = [\alpha,\beta] = \begin{pmatrix} \alpha & \beta \\ -\beta^* & \alpha^* \end{pmatrix} \qquad \alpha\alpha^* + \beta\beta^* = \pm 1$$

under U, we set

$$\begin{aligned} T^{(0)}(u)f_m^{(j)}(\xi,\eta) &= N_m^{(j)}(\alpha^*\xi - \beta\eta)^{j+m}(\beta^*\xi + \alpha\eta)^{j-m} \\ &= f_m^{(j)}(u^{-1}\binom{\xi}{\eta}) \\ &= \sum_{m'} D_{m',m}^{(j,0)}(u)f_{m'}^{(j)}(\xi,\eta) \end{aligned}$$

which defines a representation of $SU^{(\pm)}(2,p^2)$ of dimensionality $(2j+1)$, with $D_{m',m}^{(j,0)}(u) \in GF(p^2)$ given by

(3.1)

$$D_{m',m}^{(j,0)}(u) = \frac{N_m^{(j)}}{N_{m'}^{(j)}} \sum_{k=\max(0,m-m')}^{\min(j+m,j-m')} \binom{j+m}{k}\binom{j-m}{k+m'-m}\alpha^{j-m'-k}\alpha^{*\,j+m-k}\beta^k(-\beta^*)^{k-m+m'} .$$

Eq. (3.1) is just the familiar one [10] but α and β are now elements of $GF(p^2)$, (see eq. (2.5)), as well as the normalization factors $N_m^{(j)}$ (to be specified later). Moreover, it will be proved that the representation $D^{(j)}(u)$ is irreducible if and only if $j \leq \frac{p-1}{2}$.

Clearly, if $D^{(j)}(u)$ is a representation, also

$$\det u \cdot D^{(j)}(u)$$

is a representation of $SU^{(\pm)}(2,p^2)$: it is not equivalent to $D^{(j)}(u)$ and is likewise irreducible if and only if $j \le \frac{p-1}{2}$. Thus, the dimensionality label j no longer suffices to specify the representation: introducing a new two-valued label e, all the irreducible representations found so far will be written in the form:

$$D^{(j,0;e)}(u) = (\det u)^e D^{(j)}(u) \qquad \begin{array}{l} j = 0,\tfrac{1}{2},1,\ldots, \frac{p-1}{2} \\ e = 0,1 . \end{array} \tag{3.2}$$

Now we provide the proofs for the above statements about irreducible representations.

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

We shall consider only the subgroup $SU^{(+)}(2,p^2)$, since the extension to the whole group is trivial. $SU^{(+)}(2,p\ )$ has p equivalence classes individuated *by the* p *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 $a \in GF(p)$, $c \in GF(p^2)$ and $a^2 + cc^* = 1$. Now, the nonsingular matrix

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

is such that $TvT^{-1} = \begin{pmatrix} L^{+} & 0 \\ 0 & L^{-} \end{pmatrix}$ where $L^{\pm} = a \pm \sqrt{a^2-1}$ are the eigenvalues of v. Then, if $v^k = 1$ it follows $(TvT^{-1})^k = Tv^kT^{-1} = 1$ and so $(L^{\pm})^k = 1$, but since $L^{\pm} \in GF(p^2)$, k is either equal to p^2-1 or one of its divisors, and in any case $k \nmid p$, 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^2-1, and we know all (p^2-1)-th roots of 1 belong to $GF(p^2)$. This proves $GF(p^2)$ is a splitting field for $SU^{(+)}(2,p^2)$. Similarly it is proved that $GF(p^2)$ is a splitting field for $SU^{(\pm)}(2,p^2)$ so that the number of irreducible, inequivalent representations over $GF(p^2)$ is equal to the number of equivalence classes of $SU^{(\pm)}(2,p^2)$, namely $2p$.

Moreover, we get:

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

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

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

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

$$Tr(D^{(\ell+1)}(u)) = Tr(A(u)) + Tr(B(u)) = Tr(D^{(s)}(u)) + Tr(D^{(\ell-s+\frac{1}{2})}(u)).$$

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

$$\sum_{m=-\ell-1}^{\ell+1} \alpha^{\ell+1-m} \alpha^{*\,\ell+1+m} = \sum_{r=-s}^{s} \alpha^{s-r} \alpha^{*\,s+r} + \sum_{t=-\ell+s-\frac{1}{2}}^{\ell-s+\frac{1}{2}} \alpha^{\ell-s+\frac{1}{2}-t} \alpha^{*\,\ell-s+\frac{1}{2}+t} .$$

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 $\alpha \in GF(p^2)$ unless $2(\ell+1) \geq p$, in which case $\alpha^{2(\ell+1)} = {}^{2(\ell+1)-p+p} = \alpha^{*\,2(\ell+1)-p}$ and $\alpha^{*\,2(\ell+1)} = \alpha^{2(\ell+1)-p}$ so that the role of α and α^* is interchanged and the degree of the polynomial in $\alpha\alpha^*$ is lowered by p. We have thus proved that $D^{(j,0)}(u)$ are irreducible for $j \leq \frac{p-1}{2}$ but we still have to show they are certainly reducible for $j > \frac{p-1}{2}$. This is simply shown by referring to the Weyl basis of monomials $f_m^{(j)}(\xi,\eta) = N_m^{(j)} \xi^{j+m} \eta^{j-m}$; if $j > \frac{p-1}{2}$ the monomials corresponding to $m > \frac{p-1}{2}$ and $m < -\frac{p-1}{2}$ form an invariant subspace: infact set $j = \frac{p}{2} + j'$ and $m = \frac{p}{2} + m'$ then

$$f_m^{(j)}(\xi,\eta) = N_m^{(j)} \xi^{\frac{p}{2}+j'+\frac{p}{2}+m'} \eta^{\frac{p}{2}+j'-\frac{p}{2}-m'} = N_m^{(j)} \xi^{p+j'+m'} \eta^{j'-m'}$$

or

$$f_m^{(j)}(\xi,\eta) = N_m^{(j)} \xi^* \xi^{j'+m'} \eta^{j'-m'} .$$

Thus, under a transformation of the group

$$f_m^{(j)}(\xi,\eta) \rightarrow N_m^{(j)}(\alpha^*\xi - \beta\eta)^* \sum_{m''} D^{(j')}_{m'',m'}(u)\ f^{(j')}_{m''}(\xi,\eta) \ ,$$

i.e., a linear combination of monomials of the same type. This concludes the proofs of irreducibility for modular representations.

Through the homomorphism, Eqs. (3.1), (3.2) determine the corresponding representations of $R(3,p)$; remarking that $D^{(j,0;e)}(-u) = (-1)^{2j}D^{(j,0;e)}(u)$ it is seen that for integer j's the true representations of $R(3,p)$ are obtained, while for half-integer j's one gets representations of $R(3,p)$ up to a sign ambiguity (as in the classical case).

By a procedure similar to the one used for $SU^{(\pm)}(2,p^2)$, one may find out the irreducible modular representations of $SL^{(\pm)}(2,p^2)$; they have the explicit form

$$D^{(j,k;e)}(a) = (\det a)^e D^{(j)}(a) \otimes (D^{(k)}(a))^*, \begin{cases} j,k=0, \ ,1,\ldots,\frac{p-1}{2} \\ e=0,1 \end{cases} \quad ,$$

where $D^{(j)}(a)$ is obtained from (3.1) replacing α^* and $(-\beta^*)$ by δ and γ respectively (see eq. (2.4)). The number of equivalence classes of $SL^{(\pm)}(2,p^2)$ is $2p^2$; therefore all the irreducible representations are exhausted by (3.3) since the previous Proposition 1 is easily extended to $SL^{(\pm)}(2,p^2)$. (See, Brauer and Nesbitt, Ann. Math. 42, 556 (1941).)

It is easily seen that $(D^{(k)}(u))^*$ is equivalent to $D^{(k)}(u)$: from (3.3) it then follows that all the inequivalent irreducible representations of $SU^{(\pm)}(2,p^2)$ may be written as $D^{(j,0;e)}(u)$, according to the notation used in (3.2).

In the following, we shall be mainly concerned with the spinor representations, namely $j+k = \frac{1}{2}$, and it is worthwhile to remark that

$$D^{(\frac{1}{2},0;e)}(a) = (\det a)^e\, a. \tag{3.4}$$

4. UNITARY RAY-REPRESENTATIONS. Unitarity: Here we mean the property, applied only to matrices such that $UU^+ = U^+U = 1$ and nothing about matrices. As remarked in previous notes, the theorem about unitarity fails for modular representations. The proof by Wigner may be sketched very briefly: it amounts to setting $A = \Sigma_{x\in G}\, D(x) \cdot D^+(x)$, $A = A^+$ and diagonalize it, take square roots and so on. In our case, $A = 0$ for j half integer.

Consider now the unitarity character of the modular representations of $R(3,p)$. Choosing $N_m^{(j)}$ in (3.1) such that $N_m^{(j)} \cdot N_m^{(j)*} = \frac{(2j)!}{(j+m)!(j-m)!}$, it is easily found

$$(D^{(j,0;e)}(u))^+ = (\det u)^{2j}(D^{(j,0;e)}(u))^{-1} = (\det u)^{2j}(D^{(j,0;e)}(u^{-1})), \tag{4.1}$$

so that $D^{(j,0;e)}(u)$ *is unitary for integer* j, *but it is not for half-integer* j, *contrary to the classical case.*

At first sight, one could guess that, owing to the finite order of the group, the non unitary representations could be made unitary by a suitable equivalence transformation; this is not the case since the classical theorem ensuring this possibility is no longer valid for modular represen-

tations; in fact, the proof of the theorem fails if one works on a field in which a sum of positive elements may be non-positive [12]. Indeed, one may easily prove that such an equivalence relation does not exist in our case [7].

Q.M. and Ray Representations: A symmetry group in q.m. is intended as a group which leaves invariant the physically observable values, i.e., the measurements. Such measurments are expressed in terms of probability of a certain quantity to attain a given value in the experiment at hand. For instance, suppose that system is in a state $\psi \in H$, the probability that it will end up in state $\phi \in H$ is given by $|(\phi,\psi)|$. Then, for what measurements may one associate a ray $\{e^{i\theta}\phi\}$ rather than a vector ϕ to a physical state? In terms of rays, the representation of our group which acts on H need no longer be a vector representation but rather a ray representation, i.e., a representation as a phase factor. In general, we might try to keep vectors associated to states in q.m. and employ ray representations for the symmetry group. (The question arises whether a ray representation is equivalent to a vector representation.)

Def. Ray Representation. $D(u)D(u') = \omega(u,u')D(uu')$, which in the case we want it unitary, we must have $|\omega(u,u')| = 1$. Furthermore, $\omega(u,u')$ must satisfy other relations which come from associativity of multiplication. Anyway, changing from $D(u) \to D'(u) = e^{i\phi}D(u)$ will not change matters at all for what concerns a ray representation, (Hamermesh [12]).

However, the unitarity of the $R(3,p)$ modular representations may be recovered by letting them become *ray-representations* [12] (actually, to describe the transformation laws of physical states in quantum mechanics, one only needs ray-representations). To show this, let us introduce, instead of (3.2)

(4.2) $\tilde{D}^{(j,0;e)}(u) = D^{(j,0;e)}(\chi_u u), \quad \chi_u\chi_u{}^* = \det u, \quad \chi_u \in GF(p^2),$

where we remark that the equation for χ_u has $p+1$ solutions for both choices $\det u = +1$ and $\det u = -1$ [14]. The unitarity relation

(4.3) $\tilde{D}^{(j,0;e)}(u) \cdot (\tilde{D}^{(j,0;e)}(u))^\dagger = 1$

may now be deduced from (4.1), but $D^{(j,0;e)}(u)$ obeys the group multiplication law up to a phase factor. To be more explicit, consider the spinor representation $D^{(\frac{1}{2},0;e)} = (\det u)^e \cdot u$ (see eq. (3.4)) and the corresponding

(4.4) $\tilde{D}^{(\frac{1}{2},0;e)} = (\det u)^e \chi_u u, \quad \chi_u\chi_u{}^* = \det u, \quad \chi_u \in GF(p^2):$

its multiplication rule reads

(4.5)

$$\tilde{D}^{(\frac{1}{2},0;e)}(u) \cdot \tilde{D}^{(\frac{1}{2},0;e)}(u') = \omega_{u,u'}\, \tilde{D}^{(\frac{1}{2},0;e)}(uu'), \quad \omega_{u,u'} = \frac{\chi_u\ \chi_{u'}}{\chi_{uu'}},$$

and it follows $\omega_{u,u'} \cdot \omega^*_{u,u'} = \dfrac{\det u\ \ \det u'}{\det u\ \ u'} = 1, \quad \omega_{uu',u''}\omega_{u,u'} = \omega_{u,u'u''}\omega_{u',u''}$, so that all properties of a ray-representation are met by the factor system $\{\omega_{u,u'}\}$.

The unitary class of equivalence associated to the unitary ray-representation $\tilde{D}(u)$ *is formed by all representation* $\tilde{D}'(u) = c_u V\tilde{D}(u)V^{-1}$, V *being any unitary matrix and* c_u *any solution of* $c_u \cdot c^*_u = 1$, *i.e., what we call a "phase factor".*

We may thus state that all the ray representations deduced from (4.4), by changing the choice of χ_u, belong to the same unitary class of equivalence: in fact the choice χ'_u, would correspond to $c_u = \frac{\chi'_u}{\chi_u}$ and, clearly $\frac{\chi'_u}{\chi_u}\left(\frac{\chi'_u}{\chi_u}\right)^* = 1$.

Similarly, the two ray representations $\tilde{D}^{(\frac{1}{2},0;0)}(u)$ and $\tilde{D}^{(\frac{1}{2},0;1)}(u)$ belong to the same unitary class of equivalence, since $\tilde{D}^{(\frac{1}{2},0;1)}(u) = (\det u)\tilde{D}^{(\frac{1}{2},0;0)}(u)$ and $\det u$ is either $+1$ or -1, i.e., a phase factor. As a representative of this equivalence class, let us assume

$$\tilde{D}^{(\frac{1}{2})}(u) = \chi_u u, \tag{4.6}$$

χ_u *being a fixed solution of* $\chi_u\chi_u^* = \det u$.

To meet a classical analogy, we now look for representations of $SL^{(\pm)}(2,p^2)$ which become unitary when restricted to $SU^{(\pm)}(2,p^2)$: this is done by a generalization of the vector representations (3.3), into ray-representations according to the procedure previously discussed. In place of $D^{(\frac{1}{2},0;e)}(a)$ (given by (3.4)), we introduce

$$\tilde{D}^{(\frac{1}{2},0;e)}(a) = (\det a)^e \chi_a a, \quad \chi_a\chi_a^* = \det a, \quad \chi_a \in GF(p^2): \tag{4.7}$$

the unitarity property (4.3) is met by restriction to $SU^{(\pm)}(2,p^2)$ and the multiplication rule

(4.8)
$$\tilde{D}^{(\frac{1}{2},0;e)}(a) \cdot \tilde{D}^{(\frac{1}{2},0;e)}(a') = \omega_{a,a'}\tilde{D}^{(\frac{1}{2},0;e)}(aa'), \quad \omega_{a,a'} = \frac{\chi_a \chi_{a'}}{\chi_{aa'}}$$

exhibits the properties of a ray-representation. By allowing χ_a to assume different solutions in (4.7), one obtains ray-representations of the same equivalence class; the same happens going from $e=0$ to $e=1$; one may thus assume, as a representative of the equivalence class

(4.9) $$\tilde{D}^{(\frac{1}{2},0)}(a) = \chi_a a,$$

where the label e has been omitted, and χ_a is a fixed solution of $\chi_a \chi_a^* = \det a$. Similar remarks hold for the case $j=0$, $k=\frac{1}{2}$; by the same procedure, we individuate an equivalence class whose representative we choose to be

(4.10) $$\tilde{D}^{(0,\frac{1}{2})}(a) = \chi_a a^*.$$

$\tilde{D}^{(\frac{1}{2},0)}(a)$ and $\tilde{D}^{(0,\frac{1}{2})}(a)$ become equivalent only when restriced to $SU^{(\pm)}(2,p^2)$.

Property of Gauge Transformations and Multivalued Representation.

A multivalued representation, where with the matrix u is associated the set of representatives $(j = \frac{1}{2})$

$$\{\chi_u(u)\}, \quad \chi_u\chi_u^* = \det u,$$

which associates p+1 representatives to a group element thus enlarging the rotation group to that of 2×2 $GF(p^2)$ matrices with $|\det| = 1$ and thus it coincides with the extended orthogonal group defined by Coish. According to his reasoning, one could then define a gauge transformation which could possibly be associated with change.

The identification of

$$C = \{\chi_a a, \quad a \in SU^{\pm}(2,p^2)\} \qquad \chi_a\chi_a^* = \det a$$

with the extended orthogonal group of Coish might be carried out as follows

i) solutions of $\chi\chi^* = 1$ $\xi^k = \chi_k$ $k = 1,2,\ldots,p+1$, $\xi = \beta^{p-1}$

ii) solutions of $\Gamma\Gamma^* = -1 = \xi^{k+\frac{1}{2}}$ $k = 1,2,\ldots,p+1$, $\xi = \rho^{p-1}$

we set

$$\left.\begin{aligned} C^+ &= \{\xi^k a \quad \forall\ a \in SL^{(+)}\} \\ C^- &= \{\xi^{k+} a \quad \forall\ a \in SL^{(-)}\} \end{aligned}\right\} \not\Rightarrow\ C = C^+ \cup C^-$$

$$\overline{C} = \{\eta:\ \det(\eta)\det(\eta)^* = 1\}$$

$\overline{C} \supset C$, conversely since $\forall\ \eta \in \overline{C}$

$$|\det(\eta)| = 1 \Rightarrow \det(\eta) = \xi^j \begin{cases} j \text{ even} \Rightarrow \xi^{j/2} \text{ still solution and hence} \\ \quad \det(\eta/\xi^{j/2}) = 1 \\ j \text{ odd} \Rightarrow \xi^{j/2} \text{ satisfies } \xi^{j/2}\cdot(\xi^{j/2})^* = -1 \\ \quad \text{and } \eta = i\xi^{j/2} b \quad b \in SL^{(-)} \end{cases} .$$

See Coish [5] for what should be done about change.

5. DIRAC SPINOR REPRESENTATION. The possibility of having a two dimensional representation (the group $SL^{(\pm)}(2,p^2)$ itself) of the proper Lorentz group $L(4,p)$ is related to the possibility of summarizing Eqs. (2.1) and (2.6) in the alternative form

$$\hat{x}' = (\det a)a\hat{x}a^\dagger = \tilde{D}^{(\frac{1}{2},0)}(a)\hat{x}(\tilde{D}^{(\frac{1}{2},0)}(a))^\dagger, \quad \text{where} \tag{5.1}$$

$$\hat{x} = \sum_\mu \sigma_\mu x_\mu, \quad a \in SL^{(\pm)}(2,p^2) .$$

Let us now consider the extended Lorentz group $\mathcal{L}(4,p)$, obtained by adjoining the space reflection operation P to the proper group $L(4,p)$. It is easily seen that, as in the classical case, it is impossible to have a two dimensional representation of $L(4,p)$ con $\hat{X}$. In fact, transforming with P, we get the non linear relation

$$(5.2)\qquad \hat{X} \overset{P}{\rightarrow} \hat{X}^{(P)} = E(\hat{X})^* E^{-1}, \qquad E = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} .$$

To have a linear representation of $L(4,p)$ we need to adopt a 4×4 basis, e.g.,

$$(5.3)\qquad \hat{X} = \begin{pmatrix} \hat{X} & 0 \\ 0 & \hat{X}^{(P)} \end{pmatrix} ,$$

on which P induces the transformation

$$(5.4)\qquad \hat{X} \overset{P}{\rightarrow} \hat{X}' = \begin{pmatrix} \hat{X}^{(P)} & 0 \\ 0 & \hat{X} \end{pmatrix} = \gamma_0^\dagger \hat{X} \gamma_0 , \qquad \gamma_0 = \gamma_0^\dagger = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} .$$

Let us write the transformation induced by $L(4,p)$ in the form

$$(5.5)\qquad \hat{X} \xrightarrow{L(4,p)} \hat{X}' = S(a)\, \hat{X} S(a)^\dagger ,$$

where the hermitian conjugation ensures that $\hat{X}'$ individuate coordinates in $GF(p)$. According to the discussion of the previous section, the restriction of $S(a)$ to $SU^{(\pm)}(2,p^2)$ is required to be unitary: looking at Eqs. (5.1), (5.2), (5.3) and taking into account Eqs. (4.9), (4.10), one is thus led to write

$$(5.6)\qquad S(a) = \begin{pmatrix} \tilde{D}^{(\frac{1}{2},0)}(a) & 0 \\ 0 & \theta_a\, E\, \tilde{D}^{(0,\frac{1}{2})}(a)\, E^{-1} \end{pmatrix} = \chi_a \begin{pmatrix} a & 0 \\ 0 & \theta_a\, E\, a^*\, E^{-1} \end{pmatrix} ,$$

where, up to now, θ_a is restricted, by (5.5), to be any solution of

$$\theta_a \theta_a^* = 1, \qquad \theta_a \in GF(p^2) .$$

However, we have still to impose that $S(a)$ be a ray representation as a whole: this corresponds to the physical requirement of having no more arbitrariness than an overall phase factor in the definition of the four-component spinor which transforms according to $S(a)$. Taking into account Eqs. (4.8) and (5.6), it is easily proved that this requirement implies

$$\theta_a \theta_{a'} = \theta_{aa'} ,$$

i.e., the factors θ_a must provide an one-dimensional vector representation of $SL^{(\pm)}(2,p^2)$. According to (3.3), there are thus the two choices

$$\theta_a = 1, \qquad \theta_a = \det a:$$

from (5.6), we then deduce the two ray-representations (we make use of the identity $\mathcal{E}a^*\mathcal{E}^{-1} = (\det a)a^{\dagger\,-1})$

$$S^{(e)}(a) = \chi_a \begin{pmatrix} a & 0 \\ 0 & (\det a)^{e+1} a^{\dagger\,-1} \end{pmatrix} \qquad e = 0,1. \tag{5.7}$$

The corresponding 4×4 spinor representations of $L(4,p)$ may now be constructed: they will be denoted by $(\gamma_0, S^{(e)}(a))$, where γ_0 is the representative of the space-reflection P, according to (5.4). Of course $(\gamma_0, S^{(0)}(a))$ and $(\gamma_0, S^{(1)}(a))$ are ray-representations (we do not need to write the explicit form of the factor systems which characterize their multiplication rules): it is important to emphasize that they are inequivalent. Therefore, two kind of Dirac spinors are possible: the one transforming under $(\gamma_0, S^{(0)}(a))$ which will be denoted as $\psi^{(0)}$ and the one transforming under $(\gamma_0, S^{(1)}(a))$ which be denoted as $\psi^{(1)}$.

This doubling is peculiar of the finite version $L(4,p)$ of the Lorentz group; its root lies in the appearence of both signs in the determinant of the matrices forming $SL^{(\pm)}(2,p^2)$, the group homorphic to $L(4,p)$.

Let us finally remark that the problem of spinor representations of the finite Lorentz group has been treated also by I.S. Shapiro [5], although he is concerned only in two-dimensional spinors giving up the possibility of representing explicitly the operation of space reflection.

6. PROPERTIES OF BI-SPINOR FORMS. We shall now discuss some peculiarities of the Dirac spinors $\psi^{(e)}$, which could be of physical relevance. Consider two spinors $\psi^{(e)}$, $\phi^{(e)}$ and their bilinear (more precisely: sesquilinear) forms

$$\psi^{(e)\dagger} B_{(\tau)} \phi^{(e)} \tag{6.1}$$

$B_{(\tau)}$ being some 4×4 matrix whose tensor nature is specified by a set of indices shortly denoted by (τ). Such quantities, often called "currents" in physical literature, are the one appearing, e.g., in electromagnetic and weak-interaction Hamiltonians. We shall now raise the question of whether a choice of $B_{(\tau)}$ exists making (6.1) covariant with respect to $L(4,p)$. As a guide, let us recall that in the classical continuous case the analogous question leads to the construction of five covariant currents, i.e., a scalar and a pseudo-scalar a vector and an axial vector, a second order tensor.

We omit at once the currents

$$\psi^{(e)\dagger} B_{(\tau)} \phi^{(e')} , \qquad e \neq e',$$

for they cannot be made covariant with respect to $L(4,p)$, as it could be deduced from the following analysis.

The transformation law of the current (6.1) under the space reflection P and the proper subgroup $L(4,p)$ is given by

(6.2) $$\psi^{(e)^\dagger} B_{(\tau)} \phi^{(e)} \xrightarrow{P} \psi^{(e)^\dagger} \cdot \gamma_0^\dagger \cdot B_{(\tau)} \cdot \gamma_0 \cdot \phi^{(e)},$$

note $\gamma_0^\dagger = \gamma_0$

(6.3) $$\psi^{(e)^\dagger} B_{(\tau)} \phi^{(e)} \xrightarrow{L(4,p)} \psi^{(e)^\dagger} \cdot S^{(e)}(a)^\dagger \cdot B_{(\tau)} \cdot S^{(e)}(a) \cdot \phi^{(e)}.$$

To answer the previous question, one has thus to check whether $\gamma_0 \cdot B_{(\tau)} \cdot \gamma_0$ and $S^{(e)}(a)^\dagger \cdot B_{(\tau)} \cdot S(a)$ are related to $B_{(\tau)}$ according to the transformation laws, under P and $L(4,p)$ respectively, which characterize

- a scalar:

(S) $$\begin{cases} \gamma_0 B \gamma_0 = B \\ S^{(e)}(a)^\dagger B S^{(e)}(a) = B; \end{cases}$$

- a pseudo scalar:

(PS) $$\begin{cases} \gamma_0 B \gamma_0 = -B \\ S^{(e)}(a) B S^{(e)}(a) = B; \end{cases}$$

- a vector:

(V) $$\begin{cases} \gamma_0 B_\mu \gamma_0 = -(-1)^{\delta_{0\mu}} B_\mu, \qquad \mu = 0,1,2,3 \ , \\ S^{(e)}(a)^\dagger B_\mu S^{(e)}(a) = \frac{1}{2} (\det a) \sum_{\nu=0}^{3} Sp(\sigma_\mu a \sigma_\nu a^\dagger) B_\nu \ ; \end{cases}$$

- an axial-vector:

$$(A)\quad \begin{cases} \gamma_0\, B_\mu\, \gamma_0 = (-1)^{\delta_{0\mu}}\, B_\mu \\ S^{(e)}(a)^\dagger\, B_\mu\, S^{(e)}(a) = \frac{1}{2}\,(\det a) \sum_{\nu=0}^{3} Sp(\sigma_\mu a \sigma_\nu a^\dagger)\, B_\nu ; \end{cases}$$

- a 2^{nd}-order tensor:

$$(T)\quad \begin{cases} \gamma_0\, B_{\mu\nu}\, \gamma_0 = (-1)^{\delta_{0\mu}+\delta_{0\nu}}\, B_{\mu\nu}, \qquad \mu,\nu = 0,1,2,3 \quad , \\ S^{(e)}(a)^\dagger\, B_{\mu\nu}\, S^{(e)}(a) = \frac{1}{4} \sum_{\rho,\lambda=0}^{3} Sp(\sigma_\mu a \sigma_\rho a^\dagger) Sp(\sigma_\nu a \sigma_\lambda a^\dagger) B_{\rho\lambda} \ . \end{cases}$$

To solve these equations, it is useful to introduce the notation

$$(6.4)\qquad B_{(\tau)} = \begin{pmatrix} b^{(1)}_{(\tau)} & b^{(2)}_{(\tau)} \\ b^{(3)}_{(\tau)} & b^{(4)}_{(\tau)} \end{pmatrix}$$

and correspondingly (see (5.4), (5.7))

$$(6.5)\qquad \gamma_0\, B_{(\tau)}\, \gamma_0 = \begin{pmatrix} b^{(4)}_{(\tau)} & b^{(3)}_{(\tau)} \\ b^{(2)}_{(\tau)} & b^{(1)}_{(\tau)} \end{pmatrix} ,$$

$$(6.6)\quad S^{(e)}(a)^\dagger B_{(\tau)} S^{(e)}(a) = \begin{pmatrix} (\det a)\ a^\dagger b_{(\tau)}{}^{(1)} a & (\det a)^e\ a^\dagger b_{(\tau)}{}^{(2)} a^{\dagger\,-1} \\ (\det a)^e a^{-1} b_{(\tau)}{}^{(3)} a & (\det a) a^{-1} b_{(\tau)}{}^{(4)} a^{\dagger\,-1} \end{pmatrix} .$$

Of course, the homogeneous equations (S), (PS), (V), (A), (T) have to be satisfied by the $B_{(\tau)}$'s identically with respect to $a \in SL^{(\pm)}(2,p^2)$;

the label e appears as a parameter and only for $e=0$ these equations formally reproduce the classical continuous case. A straightforward calculation leads to the following results

$$(A)\quad \begin{cases} \text{if} \quad e = 0: & B = \gamma_0 \; ; \\ \text{if} \quad e = 1: & \text{no solution;} \end{cases}$$

$$(PS)\quad \begin{cases} \text{if} \quad e = 0: & B = \gamma_0\gamma_5, \quad \gamma_5 = i \quad \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}; \\ \text{if} \quad e = 1: & \text{no solution;} \end{cases}$$

$$(V)\quad \text{for both} \quad e = 0,1: \quad B_\mu = \gamma_0\gamma_\mu, \quad \gamma_\ell = \begin{pmatrix} 0 & -\sigma_\ell \\ \sigma_\ell & 0 \end{pmatrix}, \quad \ell = 1,2,3;$$

$$(A)\quad \text{for both} \quad e = 0,1: \quad B_\mu = \gamma_0\gamma_5\gamma_\mu \; ;$$

$$(T)\quad \begin{cases} \text{if} \quad e = 0: & B_{\mu\nu} = \gamma_0\gamma_\mu\gamma_\nu \; ; \\ \text{if} \quad e = 1: & \text{no solution .} \end{cases}$$

The relevant feature of these results is the very special role played by the vector and axial-vector currents, the ones of paramount importance in elementary particle physics.

Referring to the construction of hamiltonians which occur in weak interaction theory, the problem arises of multiplying two currents to obtain a scalar or a pseudo-scalar quantity.

According to our previous analysis, if at least one of these currents is built up with spinors of the kind $e=1$, then necessarily only vector and axial-vector currents can be used in such hamiltonians, according to the empirical evidence. It could be tempting to associate the leptons to the choice $e=1$: the V,A currents appearing in weak interactions would then be the unique possibility in the framework of a finite geometry.

The γ matrices we have defined obey the relations

$$\gamma_{\mu\nu} + \gamma_{\nu\mu} = 2g_{\mu\nu}, \qquad \mu,\nu = 0,1,2,3 \qquad g = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix},$$

$$\gamma_5 = \gamma_0\,\gamma_1\,\gamma_2\,\gamma_3\;;$$

thus they provide a realization of Dirac matrices (which coincides, up to a factor $(-i)$, with Weyl's representation). In analogy to the classical case, the sixteen matrices γ_0, $\gamma_0\gamma_5$, $\gamma_0\gamma_\mu$, $\gamma_0\gamma_5\gamma_\mu$, $\gamma_0\gamma_\mu\gamma_\nu$ $(\mu < \nu)$, are a complete set and this ensures that the currents we have examined are the only irreducible ones. Of course, the particular realization of the γ's we have found is related to the particular choice of the 4×4 basis made in (5.3).

7. Poincaré Group over GF(p).

The Poincaré or inhomogeneous Lorentz group $P(4,p)$ is the group of linear transformations

$$x_\mu \to x'_\mu = \sum_\nu \ell_{\mu\nu}\, x_\nu + a_\mu; \quad \ell \in L(4,p),\ \text{i.e.,}\ \ell^T g \ell = g,\ \det \ell = 1;$$

$$x_\mu, a_\mu \in GF(p).$$

Its elements are denoted by (a,ℓ) with composition law $(a,\ell)(a',\ell') = (a + \ell a', \ell\ell')$ where a stands for the 4-vector $(a_0, a_1, a_2, a_3) \cdot (a,\ell)^{-1} = (-\ell^{-1}a, \ell^{-1})$.

The subgroup of translations $T(4,p) = \{(a,1), \forall a\}$ is Abelian invariant since $(a',\ell')^{-1}(a,1)(a',\ell') = (\ell'^{-1} a,1) \in T(4,p)$; thus $P(4,p)$ has a semidirect product structure. The order of $P(4,p)$ is $p^6(p^4-1)$, i.e., the product of the order p^4 of $T(4,p)$ with the order $p^2(p^4-1)$ of $L(4,p)$

We shall now briefly recall the procedure (due to Wigner) to construct the irreducible representations of the usual Poincaré group; this classical sketch will clarify the physical meaning of the numbers associated with irreducible representations.

First one finds the irreducible representations of the translation subgroup; since this is abelian, they are one dimensional and individuated by a character $\chi_q(a)$ which satisfies $\chi_q(a_1)\,\chi_q(a_2) = \chi_q(a_1 + a_2)$, $|\chi_q(a)| = 1$, hence $\chi_q(a) = e^{-i(a,q)}$ where $q = (q_0,q_1,q_2,q_3)$ and $(a,q) = a_0q_0 - \vec{a}\,\vec{q}$. These characters are then classified into orbits or equivalence classes; the orbit (q) which contains the character χ_q contains also every character $\chi_{\Lambda q}$ where Λ belongs to the proper orthochronous Lorentz group $L_\uparrow^+$. To every orbit (q) one associates a "little group" $G_q \subset L^+$ which leaves invariant a point of the orbit (different points on the same orbit have isomorphic little groups). There are four different orbits individuated by the 4-vectors

a) $(m,0,0,0)$, b) $(m,m,0,0)$, c) $(0,m,0,0)$, d) $(0,0,0,0)$

with corresponding little groups $R(3,p)$, E_2, L_{2+1}, $L_\uparrow^+$.

Each orbit is characterized by a "quantum number" which is the length of the representative vector; it is clear that only the orbits of type a) and b) are of direct physical interest, for the associated "quantum numbers" are m and 0 and they individuate particles of mass m or zero mass (e.g., mesons and photons respectively). The orbit of type c) corresponds to an imaginary mass and that of type d) to a particle with null four-momentum.

If then, one knows the irreducible representations of the little groups, it is possible to reconstruct the representations of the whole group. The little groups provide a second "quantum number", which in case a) is the spin $j \geq 0$ integer or half-integer, and in case b) is the helicity, integer of half-integer also. In principle, the same reasoning can be applied to modular representations, but care must be paid when treating the translation subgroup $T(4,p)$.

About abelian groups, we have [9]:

Given an abelian group H of order h and exponent s and a finite field K of characteristic p, if p/s, H has less than h distinct irreducible one dimensional representations over K.

The theorem applies to $T(4,p)$ since its order is p^4, moreover, even if $GF(p)$ were a splitting field for $T(4,p)$ all $T(4,p)$ equivalence classes but one are p-singular. In fact, chosen $(a,1) \in T(4,p)$ we have $(a,1)^n = (na,1)$ so that the least integer for which $(na,1) = (0,1)$ is p if $a \neq 0$. This implies that $T(4,p)$ has just one irreducible modular representation, i.e., the identical one. Forced, as we are, to abandon the idea of strictly modular irreducible representations of $T(4,p)$ we may proceed along two different lines in order to recover results of physical interest:

(i) extend the base field to a larger one, which is essentially the field obtained adjoining to $GF(p)$ the complex numbers $e^{2\pi i n/p}$ $n = 0,1,\dots,p-1$.

(ii) give up the requirement of irreducibility and substitute it with that of indecomposability for the representations of $T(4,p)$

The first alternative leads back to a classification completely analogous to the classical one, the representatives of the translations are labelled by 4-vectors $q = (q_0,q_1,q_2,q_3)$ and $(a,1)$ corresponds to $\chi_q(a) = \exp\left(\frac{2\pi i(qa)}{p}\right)$, where

$$(qa) = q_0a_0 - q_1a_1 - q_2a_2 - q_3a_3 .$$

To these representations one may apply the theory of induced representations with results completely analogous to the previous given ones, the specturm of the momenta q is obviously contained in $GF(p)$. This procedure has the serious drawback that we now don't exactly know on what type of space the matrices operate, due to the extension of the base field.

The second alternative has a branching point with two possibilities:

I) <u>Theorem</u> (Curtis & Reiner). A cyclic group of order p^s has exactly p^s indecomposable inequivalent representations over $GF(p)$ which have dimension $1, 2, \dots, p^s$.

Since $T(4,p)$ is the direct product of 4 $T(1,p)$ groups, we need only find the indecomposable representations of $T(1,p)$ which are given by

$$1, \quad \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & a & a^2 \\ 0 & 1 & 2a \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & a & a^2 & a^3 \\ 0 & 1 & 2a & 3a^2 \\ 0 & 0 & 1 & 3a \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

and so forth, repeating the preceeding matrix, adding a last row of zeros except the last element which is one and completing the last column with the expansion of $(a+1)^n$, n being the dimensionality of the matrix itself. Obviously, we have p of them since $a^p = 1 \;\forall\; a \in GF(p)$.

To these representations, we cannot apply the theory of induced representations as sketched here, even though we might obtain from each one of them a representation of the whole group $P(4,p)$. This procedure, on the other hand, does not insure to obtain indecomposable representations of $P(4,p)$ nor that we have a sufficient number of them.

II) We can employ 2-dimensional indecomposable representations of $T(4,p)$ labelled by a 4-vector $q = (q_0,q_1,q_2,q_3)$ and defined through

$$(a,\ 1) \rightarrow \begin{pmatrix} 1 & (aq) \\ 0 & 1 \end{pmatrix} .$$

To these, we can apply the theory of induced representations, regaining all the results already shown in (i) and with the bonus that we do not have to extend the base field. This which looks like a possible choice to make, for we have p^4 inequivalent indecomposable representations which possibly give rise to indecomposable representations through the little groups of $P(4,p)$, suffers from need of theorems. We have not been able to prove neither completeness nor indecomposability for the induced representations of $P(4,p)$ and the subject is still open to investigations.

REFERENCES.

[1] For a general treatment of Galois field theory, see, e.g., B. Segre: "Lezioni di geometria moderna", Vol. 1 (Bologna, 1948); L. Dickson: "Linear groups" (New York, 1958).

[2] See, e.g., B. Segre: "Introduction to Galois geometries", Atti Accad. Naz. Lincei Mem. Cl. Sc. Fis. Mat. Natur. 8, 135 (1967).

[3] G. Järnefelt: Ann. Acad. Sci. Fennicae A. I., No. 96 (1951); P. Kustaanheimo: Publ. Astron. Obs. Helsinki, No. 32 (1949); No. 34 (1952); No. 52 (1957); No. 55 (1957).

[4] H. Joos: Journ. Math. Phys. 5, 155 (1964); Y. Ahmavaara: Journ. Math. Phys. 6, 87, 220 (1965); 7, 197, 201 (1966).

[5] H. R. Coish: Phys. Rev. 114, 383 (1959).

[6] I. S. Shapiro: Nucl. Phys. 21, 474 (1960).

[7] E. G. Beltrametti and A. A. Blasi: Journ. Mat. Phys. 9, 1027 (1968).

[8] E. G. Beltrametti and A. A. Blasi: Nuovo Cimento 55A, 301, (1968); Atti Acc. Naz. Lincei, Cl. Sc. Fis. Mat. Natur. 44, 384 (1968).

[9] For a general treatment of modular representations, see C. W. Curtis and I. Reiner: "Representation theory of finite groups and associative algebras" (New York, 1962), Chap. 12.

[10] See, e.g., E. P. Wigner: "Group theory and its applications to the quantum mechanics of atomic spectra" (New York, 1959), formula (15.21).

[11] See, e.g., the book of ref. [10], Chap. 9, p. 74, 75.

[12] See, e.g., M. Hamermesh: "Group Theory", Chap. 12 (Reading, Mass., 1962).

[13] See Dickson's book quoted in ref. [1], p. 47, 48.