Zeitschrift: L'Enseignement Mathématique

Herausgeber: Commission Internationale de l'Enseignement Mathématique

Band: 22 (1976)

Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: FINITE GEOMETRIES IN THE THEORY OF THETA CHARACTERISTICS

Autor: Rivano, Neantro Saavedra

Kapitel: §2 FINITE GEOMETRIES ON SETS OF CHARACTERISTICS

DOI: https://doi.org/10.5169/seals-48185

1.5 *Some notation.* a) Let J be a vector space over $\mathbf{Z}/2\mathbf{Z}$, S a J-torsor. Let's put

$$E(S) = J \amalg S$$

the disjoint union of J, S; on this set there is a structure of vector space over $\mathbf{Z}/2\mathbf{Z}$. In fact there is an exact sequence

$$0 \to J \to E(S) \to \mathbf{Z}/2\mathbf{Z} \to 0$$

where J is sent identically onto itself, and the inverse image of 0 (resp. 1) in $E(S)$ is J (resp. S). The addition law in $E(S)$ reduces to the given one on J when both elements are in J, is the action of J on S when one element is in J and the other in S, and finally $s + s'$ (for $s, s' \in S$) is the unique element $x \in J$ such that $x + s = s'$ (or equivalently $x + s' = s$).

b) Given the standard pair (J_o, e_o), as in 0.5. I will write $S_o = Q(J_o, e_o)$, $Q_o = Q_{e_o}$. Both J_o, S_o identify to $(\mathbf{Z}/2\mathbf{Z})^{2g}$, but the following notations will be used in compliance with tradition, where $u_1, \ldots, u_{2g}$ is the canonical basis. An element of the form

$$\sum_{i=1}^{g} (\varepsilon_i u_i + \varepsilon_i' u_{i+g})$$

will be written $\begin{pmatrix} \varepsilon \\ \varepsilon' \end{pmatrix}$ or $\begin{bmatrix} \varepsilon \\ \varepsilon' \end{bmatrix}$ whether it is seen in J_o or S_o respectively, where ε, ε' are row vectors. In particular, the addition law in $E(S_o)$ is the following:

$$\begin{pmatrix} \varepsilon \\ \varepsilon' \end{pmatrix} + \begin{pmatrix} \eta \\ \eta' \end{pmatrix} = \begin{pmatrix} \varepsilon + \eta \\ \varepsilon' + \eta' \end{pmatrix}$$

$$\begin{pmatrix} \varepsilon \\ \varepsilon' \end{pmatrix} + \begin{bmatrix} \eta \\ \eta' \end{bmatrix} = \begin{bmatrix} \varepsilon + \eta \\ \varepsilon' + \eta' \end{bmatrix}$$

$$\begin{bmatrix} \varepsilon \\ \varepsilon' \end{bmatrix} + \begin{bmatrix} \eta \\ \eta' \end{bmatrix} = \begin{pmatrix} \varepsilon + \eta \\ \varepsilon' + \eta' \end{pmatrix}$$

§ 2 Finite geometries on sets of characteristics

2.0 Let's fix for paragraph § 2 a symplectic torsor (S, Q) over a symplectic pair (J, e) of genus g. The letter Σ will stand for either the set S^+ of S^-, its cardinality is $2^{g-1}(2^g \pm 1)$ (recall that according to 1.1 we assume all symplectic torsors are even). *We will exclude from consideration in this section the trivial case where* Σ *has only one element.* This corresponds to $g = 1$ and $\Sigma = S^-$.

In this paragraph a very simple combinatorial structure will be put on Σ (the *finite geometry*) that will allow us to reconstitute (J, e), (S, Q) from Σ. In particular, the symplectic group $Sp\,(J, e) \simeq Sp\,(S, Q)$ will be interpreted as the group of automorphisms of a combinatorial structure. Let's denote this symplectic group by Γ.

2.1 The addition in $E\,(S)$ (see 1.5.a) defines a map

$$\begin{aligned} \Sigma \times \Sigma &\to J \\ (s, s') &\to s + s'\,; \end{aligned} \tag{2.1.1}$$

its image will be written $\Sigma + \Sigma$. For any $x \in J$, $x \neq 0$, the set of non-ordered pairs $\{s, s'\}$ such that $x = s + s'$ will be written $\Sigma\,(x)$. Then, the following holds:

2.1.1 PROPOSITION. *One has* $J = \Sigma + \Sigma$ *and* $|\,\Sigma\,(x)\,| = 2^{g-2}\,(2^{g-1} \pm 1)$ *for any* $x \neq 0$.

2.1.2 *Proof.* Let's show first how the first conclusion implies the second. As the group Γ acts on both $\Sigma \times \Sigma$ and J, in a way compatible with the map (2.1.1), and transitively on $J - \{0\}$, it is clear that $|\,\Sigma\,(x)\,|$ is the same for any $x \neq 0$, and half the cardinality of the inverse image of x by the map (2.1.1). Because this map is surjective, and the inverse image of 0 is the diagonal, one has

$$2\,|\,\Sigma\,(x)\,| \cdot (|\,J\,| - 1) = |\,\Sigma\,|^2 - |\,\Sigma\,|\,.$$

Replacing the values $|\,J\,| = 2^{2g}$, $|\,\Sigma\,| = 2^{g-1}\,(2^g \pm 1)$ one finds the answer.

Now, turning back to the proof that $J = \Sigma + \Sigma$, writing $A = \Sigma + \Sigma$, we have that

$$e\,(x, y) = 0 \quad x \in A, y \notin A\,.$$

Indeed, $x = s + s'$ for some s, $s' \in \Sigma$, and if $t = y + s$, $t' = y + s'$, it must be that $t \notin \Sigma$, $t' \notin \Sigma$, otherwise y would belong to A; but by definition of a symplectic torsor

$$Q\,(s) + Q\,(s') + Q\,(t) + Q\,(t') = e\,(x, y)$$

and as $Q\,(s) = Q\,(s')$, $Q\,(t) = Q\,(t')$, this equals 0. Finally, with the exception of the case where Σ consists of only one element that was excluded in 2.0, $A \neq \{0\}$, and the proposition follows from the lemma

2.1.3 *Lemma.* If $A \subset J$ contains 0 and $e(x, y) = 0$ for $x \in A$, $y \notin A$, then either $A = \{0\}$ or $A = J$.

2.1.4 *Proof of the lemma.* If $A \neq \{0\}$ and $\neq J$, there would be $x \neq 0$, $y \neq 0$ with $x \in A$, $y \in B = \complement A$. As $e(x, B) = 0$, $e(A, y) = 0$, and the form e is non degenerate, it should be

$$|A| < 2^{2g-1} \qquad |B| < 2^{2g-1}.$$

But $|A| + |B|$ must equal 2^{2g}, and there is a contradiction.

2.2 The symplectic group Γ acts on S through the identification $\Gamma = Sp(S, Q)$ (1.4), and in particular Γ acts on $\Sigma = S^{\pm}$. As a corollary to 2.1, we have that *the action of* Γ *on* Σ *is faithful*, i.e. that the map

$$\Gamma \to \operatorname{Aut}(\Sigma)$$

is injective, with the trivial exception where $|\Sigma| = 1$.

This follows at once from the compatibility of the actions of Γ on $\Sigma \times \Sigma$, J with the map (2.1.1).

2.3 A *quartet* in Σ is a quadruple $(s_1, s_2, s_3, s_4) \in \Sigma^4$ such that $s_1 + s_2 + s_3 + s_4 = 0$, where the addition is performed in $E(S)$ (1.5.a). If $\Sigma_{(4)} \subset \Sigma^4$ denotes the set of quartets, $\Sigma_{(4)}$ has the following properties

(i) $\Sigma_{(4)}$ is globally invariant under the permutation group in four letters acting on Σ^4 by coordinate exchanges.

(ii) $\Sigma_{(4)} \subset (\Sigma^2)^2$ is an equivalence relation on Σ^2.

In fact, these two properties alone for a subset of Σ^4 (Σ an arbitrary set) define what naturally could be seen as the generalization of equivalence relations, when 4-relations are considered instead of 2-relations. In this case we have a further and very restrictive property:

(iii) The projection maps $\Sigma_{(4)} \to \Sigma^3$ are injective.

A *triplet* in Σ is a triple $(s_1, s_2, s_3) \in \Sigma^3$ that can be completed to a quartet, i.e. that belongs to the image of any of the projection maps in (iii) above, or still such that $s_1 + s_2 + s_3 \in \Sigma$. The set of triplets will be denoted by $\Sigma_{(3)}$. It is clear that any of the four projection maps sets a corresponding bijection $\Sigma_{(4)} \to \Sigma_{(3)}$.

We will also need the notion of *sextet* in Σ; these are sextuples $(s_1, \ldots, s_6) \in \Sigma^6$ such that $s_1 + \ldots + s_6 = 0$; they constitute a set $\Sigma_{(6)}$. Clearly n-ets could be defined in general but there will be no use for them, and even our interest for the sextets will be short-lived (see 2.5). Observe that $\Sigma_{(6)}$ is an equivalence relation on Σ^3 and is symmetric.

Also, for any $n \geqslant 2$, consider the following relation R_n in Σ^n:

$(s_1, ..., s_n)\ R_n\ (t_1, ..., t_n)$ if there are $i, j \in \{1, ..., n\}$ with $i \neq j$ such that $s_k = t_k$ if $k \neq i$, $k \neq j$ and $(s_i, s_j, t_i, t_j) \in \Sigma_{(4)}$.

If $\bar{R}_n$ is the equivalence relation on Σ^n generated by R_n, two n-uples will be said to be *congruent* if they are equivalent under $\bar{R}_n$. For example, the relation $R_2 = \bar{R}_2$ coincides with $\Sigma_{(4)}$.

Observe, finally, that because of 2.1.1, any couple (resp. quadruple) of elements of Σ can be completed to a triplet or a quartet (resp. to a sextet). From this same observation, the number of elements in $\Sigma_{(3)}$, $\Sigma_{(4)}$, $\Sigma_{(6)}$ can be computed

$$| \Sigma_{(3)} | = | \Sigma_{(4)} | = 2^{3g-3} (2^g \pm 1)^2 (2^{g-1} \pm 1)$$
$$| \Sigma_{(6)} | = 2^{5g-5} (2^g \pm 1)^4 (2^{g-1} \pm 1) .$$

2.4 Proposition. *The data of* $\Sigma_{(4)}$, $\Sigma_{(6)}$ *on* Σ *enables us to reconstitute* (J, e) *and the symplectic torsor* (S, Q). *In particular,*

$$J \simeq \Sigma^2 / \Sigma_{(4)}$$
$$S \simeq \Sigma^3 / \Sigma_{(6)} .$$

2.4.1 *Proof.* It is clear by definition of $\Sigma_{(4)}$, $\Sigma_{(6)}$ and by proposition 2.1.1 that the maps $\Sigma \times \Sigma \to J$, $\Sigma \times \Sigma \times \Sigma \to S$ defined by the addition in $E(S)$ induce identifications

$$J \simeq \Sigma^2 / \Sigma_{(4)}$$
$$S \simeq \Sigma^3 / \Sigma_{(6)} .$$

We have next to reconstitute from $\Sigma_{(4)}$ and $\Sigma_{(6)}$

a) *The addition in* J. Let $x, y \in J$ be represented respectively by the couples (s_1, s_2), (s_3, s_4). Then $x + y$ is represented by (s_3, s_6), where $(s_1, ..., s_6) \in \Sigma_{(6)}$.

b) *The bilinear form* e. Let $x, y \in J$ be represented respectively by the couples (s_1, s_2), $(s_3, s_4) \in \Sigma^2$. Then $e(x, y) = 0$ if both (s_1, s_3, s_4) and (s_2, s_3, s_4) belong or do not belong to $\Sigma_{(3)}$, and $e(x, y) = 1$ otherwise.

c) *The action of* J *on* S. Let $x \in J$, $s \in S$ be represented respectively by $(s_1, s_2) \in \Sigma^2$, $(s_3, s_4, s_5) \in \Sigma^3$. Then $x + s$ is represented by $(s_5, s_6, s_7) \in \Sigma^3$, where $(s_1, s_2, s_3, s_4, s_6, s_7) \in \Sigma_{(6)}$ is any completion into a sextet of $(s_1, ..., s_4)$.

d) *The map* Q. Let $s \in S$ be represented by $(s_1, s_2, s_3) \in \Sigma^3$. If $\Sigma = S^+$, $Q(s)$ equals 0 or 1 according to (s_1, s_2, s_3) belongs to $\Sigma_{(3)}$ or not. If $\Sigma = S^-$, the opposite is valid.

2.5 PROPOSITION. *The data of* $\Sigma_{(3)}$, $\Sigma_{(4)}$ *on the set* Σ *are equivalent, and* $\Sigma_{(6)}$ *can be constructed from* $\Sigma_{(4)}$.

2.5.1 *Proof.* It is clear that $\Sigma_{(3)}$ is defined in terms of $\Sigma_{(4)}$. Conversely, to define $\Sigma_{(4)}$ from $\Sigma_{(3)}$, one observes that $(s_1, s_2, s_3, s_4) \in \Sigma^4$ is a quartet if and only if the following holds: for any $s \in \Sigma$, $(s, s_1, s_2) \in \Sigma_{(3)} \Leftrightarrow (s, s_3, s_4) \in \Sigma_{(3)}$; the proof of this fact is left as an exercise for the reader. As for the last assertion, let's remark first that it is trivial in the case $g = 2$, $\Sigma = S^-$, because as $|\Sigma| = 6$ there can be only one non-trivial sextet. This exceptional case settled the following lemma—where in addition to the assumption in 2.0 the preceding case is excluded from consideration—shows that in the remaining cases the sextets are the sextuples *congruent* (2.3) to those sextets containing a triplet. As these last ones are clearly defined in terms of $\Sigma_{(4)}$, the proposition is proved.

2.5.2 *Lemma.* If $\Sigma = S^+$ (resp. $\Sigma = S^-$) any quadruple (resp. sextuple) is congruent to a quadruple (resp. sextuple) containing a triplet.

2.5.3 *Proof of the lemma.* Let $(s_1, \ldots, s_6) \in \Sigma^6$ be a sextuple. For any pair $(t, t') \in \Sigma^2$, the number of elements $s \in \Sigma$ such that (s, t, t') is a triplet equals $2^{g-1}(2^{g-1} \pm 1)$ following 2.1.1. Thus, if

$$T_1 = \{s \in \Sigma / (s, s_1, s_2) \in \Sigma_{(3)}\}$$
$$T_2 = \{s \in \Sigma / (s, s_3, s_4) \in \Sigma_{(3)}\}$$
$$T_3 = \{s \in \Sigma / (s, s_5, s_6) \in \Sigma_{(3)}\}$$

we have $|T_i| = N = 2^{g-1}(2^{g-1} \pm 1)$ for $i = 1, 2, 3$. It is easily seen that $3N > |\Sigma| = 2^{g-1}(2^g \pm 1)$ and that if $\Sigma = S^+$ (so that $\pm$ becomes $+$ everywhere) then $2N > |\Sigma|$. This implies that some two of the sets T_1, T_2, T_3 meet, and that T_1, T_2 meet if $\Sigma = S^+$ and the lemma follows.

2.6 THEOREM. *The data of* $\Sigma_{(4)}$ *(or* $\Sigma_{(3)}$*) on* Σ *enable us to reconstitute the whole situation:* $(J, e), (S, Q)$.

This is an immediate consequence of 2.4, 2.5. The structure $\Sigma_{(4)}$ will be sometimes called the *finite geometry* on Σ, although I acknowledge it is not one in the usual sense.

2.7 COROLLARY. *Let* $(S, Q), (S', Q')$ *be symplectic torsors of genus* g *over* $(J, e), (J', e')$, *and let* $\Sigma = S^{\pm}, \Sigma' = S'^{\pm}$. *Then, there are canonical bijections*

$$\begin{aligned}\mathrm{Isom}((J, e), (J', e')) &\simeq \mathrm{Isom}((S, Q), (S', Q')) \\ &\simeq \mathrm{Isom}((\Sigma, \Sigma_{(4)}), (\Sigma', \Sigma'_{(4)})) .\end{aligned}$$

In particular, there are group isomorphisms

$$\mathrm{Sp}(J, e) \simeq \mathrm{Sp}(S, Q) \simeq \mathrm{Aut}(\Sigma, \Sigma_{(4)}) .$$

§ 3 SYMPLECTIC TORSORS DEFINED BY FINITE SETS

In this paragraph, X will be a finite set.

3.1 *The basic construction.* Starting from X one has

a) The set 2^X of subsets of X, with the operation of symmetric difference:

$$A + B = A \cup B - A \cap B \quad A, B \in 2^X$$

b) A map $p: 2^X \to \mathbf{Z}/2\mathbf{Z}$ defined by

$$p(A) = |A|(2) \quad A \in 2^X$$

c) A map $e: 2^X \times 2^X \to \mathbf{Z}/2\mathbf{Z}$ defined by

$$e(A, B) = |A \cap B|(2) \quad A, B \in 2^X$$

d) A map $Q: 2^X_- \to \mathbf{Z}/2\mathbf{Z}$ defined by

$$Q(B) = \frac{|B| + 1}{2}(2) \quad B \in 2^X_-$$

where $2^X_- = p^{-1}(1)$ is the set of subsets of odd order of X.

e) A map $q_o = 2^X_+ \to \mathbf{Z}/2\mathbf{Z}$ defined by

$$q_0(A) = \frac{|A|}{2}(2) \quad A \in 2^X_+$$

where $2^X_+ = p^{-1}(0)$.

Then, it is easily verified that

α) 2^X is a vector space over $\mathbf{Z}/2\mathbf{Z}$, of dimension $|X|$.

β) p is linear

γ) e is bilinear