II. THE ABSTRACT THEORY OF CHARACTERISTICS

II. THE ABSTRACT THEORY OF CHARACTERISTICS

§ 1 SYMPLECTIC TORSORS

1.1 *Definitions.* Recall that, if Γ is a group, a Γ-torsor (or torsor over Γ) is a non-void set endowed with a simply transitive action of Γ on it. Let (J, e) be a symplectic pair, a *symplectic torsor* over (J, e) is a pair (S, Q) of a J-torsor S and a mapping $Q: S \to \mathbf{Z}/2\mathbf{Z}$ having the property

$$(1.1.1) \quad Q(s) + Q(x+s) + Q(y+s) + Q(x+y+s) = e(x, y)$$

where $s \in S$, $x, y \in J$. It is clearly equivalent to ask this property for a fixed $s \in S$ or for all $s \in S$, and it may be thought of as meaning that Q "is a quadratic form." Indeed, any $s \in S$ sets an identification $J \xrightarrow{\sim} S$ $(x \mapsto x+s)$, and through this identification Q becomes the map $x \mapsto Q(x+s)$. The above property means that the map $q_s: J \to \mathbf{Z}/2\mathbf{Z}$ defined by

$$(1.1.2) \qquad q_s(x) = Q(x+s) + Q(s)$$

is a quadratic form whose associated bilinear form is e. According to 0.4, two possibilities may and do arise for Q: either $Q^{-1}(0)$ has $2^{g-1}(2^g+1)$ or $2^{g-1}(2^g-1)$ elements, where $g = \dim J/2$ will be called the *genus* of (S, Q). In the first case, (S, Q) will be said to be *even*, *odd* in the second. In what follows, *all symplectic torsors will be even* unless otherwise stated. This because the symplectic torsors that will appear most often will be even and because of the following simple construction. If (S, Q) is an even (resp. odd) symplectic torsor over (J, e), and $\bar{Q}$ is defined by $\bar{Q}(s) = Q(s) + 1$, then $(S, \bar{Q})$ is an odd (resp. even) symplectic torsor over (J, e).

For a given (S, Q) the following notation will be used

$$S^+ = Q^{-1}(0) \quad S^- = Q^{-1}(1).$$

The elements of S will be often called *characteristics*, those in S^+ are *positive*, those in S^- are *negative*.

1.2 *Morphisms.* Let (S, Q), (S', Q') be symplectic torsors respectively over (J, e), (J', e'). For any map $f: S \to S'$ we define a map $\sigma_f: J \times S \to J'$ by the property

$$f(x+s) = \sigma_f(x, s) + f(s);$$

this can be done because S' is a J'-torsor. Now, the following cocycle-type property for σ_f is immediately checked, where $x, y \in J$, $s \in S$

$$\sigma_f(x+y+s) = \sigma_f(x, y+s) + \sigma_f(y, s),$$

and from it one infers the equivalence of the following statements:

(i) For any $s, s' \in S$, $x \in J$

$$\sigma_f(x, s) = \sigma_f(x, s').$$

(ii) For some $s \in S$, any $x, y \in J$

$$\sigma_f(x+y, s) = \sigma_f(x, s) + \sigma_f(y, s)$$

(iii) For any $s \in S$, $x, y \in J$

$$\sigma_f(x+y, s) = \sigma_f(x, s) + \sigma_f(y, s).$$

So, when these statements hold, one gets a group homomorphism $\sigma_f: J \to J'$ and has $f(x+s) = \sigma_f(x) + f(s)$.

An *isomorphism* of (S, Q) onto (S', Q') is a bijection $f: S \to S'$ verifying statements (i) to (iii) above, and also the condition

$$Q' \circ f = Q.$$

It is clear in this case that $\sigma_f: J \to J'$ is an isomorphism compatible with e, e'. The group of automorphisms of (S, Q) will be denoted $Sp(S, Q)$, so the mapping $f \to \sigma_f$ is a group homomorphism $Sp(S, Q) \to Sp(J, e)$.

1.3 *An example.* For any given (J, e) there is a canonical example of an even symplectic torsor, namely $(Q(J, e), Q_e)$. The J-torsor $Q(J, e)$ was introduced in 0.2, the map Q_e in 0.3 where it was also remarked that it has property (1.1.1) and that $Q_e^{-1}(0)$ has $2^{g-1}(2^g+1)$ elements.

If (J, e), (J', e') are two symplectic pairs, and if $\sigma: J \to J'$ is a linear isomorphism compatible with e, e', a map $Q(\sigma): Q(J, e) \to Q(J', e')$ was defined in 0.4, where it was shown that it is an isomorphism of symplectic torsors. Clearly $Q(\sigma)$ is canonical in any conceivable way.

Indeed, if one still dares in these days to use the language of category theory, what I just did was to define a functor from the category of symplectic pairs to the category of even symplectic torsors (morphisms = isomorphisms, in both cases). In section 1.4 we will see that this is an equivalence of categories.

1.4 *Uniqueness of symplectic torsors.* It will be shown here, that for a given symplectic pair (J, e) there is essentially only one symplectic torsor over it. Let (S, Q) be such an object; then there is a map

$$f_s: S \to Q(J, e),$$

defined by the rule $s \mapsto q_s$, where q_s was defined in (1.1.2). Let us prove that f_s is an isomorphism of symplectic torsors inducing the identity $id_J: J \to J$. The formula

$$q_{x+s}(y) = (x + q_s)(y)$$

is a mere restatement of condition (1.1.1), and the formula

$$Q_e \circ f_s = Q$$

follows from the fact that (S, Q) is even and from the meaning of the Arf invariant recalled in 0.3.

The isomorphisms f_s are canonical, in the following sense. If (S, Q), (S', Q') are symplectic torsors over (J, e), (J', e'), $f: S \to S'$ is an isomorphism of symplectic torsors inducing an isomorphism $\sigma: J \to J'$, then the following square commutes

$$\begin{array}{ccc} S & \xrightarrow{f} & S' \\ {\scriptstyle f_s}\downarrow & & \downarrow{\scriptstyle f_{s'}} \\ Q(J, e) & \xrightarrow{Q(\sigma)} & Q(J', e') \end{array}$$

Recalling the definitions, one has to check for $s \in S$, $x \in J$ that

$$Q\big(\sigma(x) + f(s)\big) + Q\big(f(s)\big) = Q(x + s) + Q(s)$$

which is immediate from the definition of isomorphism in 1.2.

It comes out of this that for any isomorphism $\sigma: J \to J'$ there exists one and only one isomorphism $f: S \to S'$ inducing it. In particular, the group homomorphism at the end of 1.2.

$$Sp(S, Q) \to Sp(J, e)$$

is an isomorphism. A useful application of this is the following: If by some unspecified means one is able to construct two symplectic torsors over a pair (J, e), there is a unique isomorphism between them inducing the identity of J.

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

$$\Sigma \times \Sigma \to J \qquad (2.1.1)$$
$$(s, s') \to s + s' ;$$

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

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

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

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

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*

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

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

δ) Q has the following property (compare 1.1.1)

$$Q(B) + Q(A+B) + Q(A'+B) + Q(A+A'+B) = e(A, A')$$

whenever $B \in 2^X_-$, $A, A' \in 2^X_+$

ε) q_o is a quadratic form inducing the restriction of e to 2^X_+.

In the proof of these, one uses the following identity

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

3.2 Let's assume in the following three sections that X is of odd order, $|X| = 2g + 1$.

3.2.1 PROPOSITION. *The bilinear form e on 2^X_+ is alternate and non-degenerate. If 2^X_+ acts on 2^X_- by translations, $(2^X_-, Q)$ is a symplectic torsor over $(2^X_+, e)$ which is even for $g \equiv 2, 3$ (4) and odd for $g \equiv 0, 1$ (4).*

3.2.2 *Proof.* It is clear that e is alternate on 2^X_+. It is also non degenerate, because if $A \in 2^X_+$, $A \neq \phi$, let $x \in A$; then $A' = (X-A) \cup \{x\}$ is of even order, and $e(A, A') = 1$. It is also clear that $(2^X_-, Q)$ is a symplectic torsor over $(2^X_+, e)$ (because of 3.1 δ) and the definition of symplectic torsor.

To find out when this torsor is even or odd, we first observe that it is clearly odd for $g = 0, 1$ (look at it), then apply descending induction using the following fact (to be proved below). Let's call ε_g the type of the torsor corresponding to an X with $|X| = 2g + 1$ (and $g \geqslant 2$), thus $\varepsilon_g = \pm 1$; then $\varepsilon_g = \varepsilon_{g-1}$ if g is odd, and $\varepsilon_g = -\varepsilon_{g-1}$ if g is even.

Proof of this fact: take a fixed $A_o \subset X$ of order two. The set of $B \in 2^X_-$ such that $Q(B) = Q(A_o+B) = 0$ (recall that $Q(B) = 0$ means that $|B| \equiv 1$ (4)) has cardinality $2^{g-1}(2^{g-1}+\varepsilon_g)$ by definition of ε_g and proposition 2.1.1. But clearly this number is also twice the cardinality of the set of subsets C of $X - A_o$ such that $|C| \equiv 2g - 1$ (4) (in fact any such B defines a C by $C = X - (A_o \cup B)$ and this map is two-fold) and the number of these is $2^{g-2}(2^{g-1}+\varepsilon_{g-1})$ or $2^{g-2}(2^{g-1}-\varepsilon_{g-1})$ according to $2g - 1 \equiv 1$ (4) or $2g - 1 \equiv 3$ (4), i.e. g odd or even. This proves the fact and completes the proof of the proposition.

3.3 If Q is odd, let us agree to modify Q in the way described in 1.1 to obtain an even torsor $\bar{Q}$. With this convention, the following notation will be adopted:

$$J_X = 2^X_+ \quad e_X = e$$
$$S_X = 2^X_- \quad Q_X = Q$$

or $\bar{Q}$ according to the value of g mod 4.

The identification $S_X \simeq Q(J_X, e_X)$ in 1.4 may be made explicit: if $B \in S_X$, B becomes the following quadratic form

$$B(A) = |A \cap B| + \frac{|A|}{2}(2).$$

Let's now make explicit the condition for a triple (B_1, B_2, B_3) of elements of either S_X^+ or S_X^- to be a *triplet* (2.3). This means that

$$Q_X(\Sigma B_i) = \Sigma Q_X(B_i),$$

and this is equivalent to

$$\sum_{i<j} |B_i \cap B_j| \equiv 1\,(2),$$

or still to

$$|\cup B| \equiv |\cap B_i|\,(2).$$

3.4 The quadratic form q_o on J_X singled out in 3.1 e) corresponds through the identification $Q(J_X, e_X) = S_X$ to X itself. As $Q(X) \equiv g + 1\,(2)$, it results from the last part of 3.2.1 that the Arf invariant of q_o is 0 for $g \equiv 0, 3\,(4)$, 1 for $g \equiv 1, 2\,(4)$. In other words, $q_o \in S_X^+$ for $g \equiv 0, 3\,(4)$, $q_o \in S_X^-$ for $g \equiv 1, 2\,(4)$.

3.5 Let's assume in this and the next sections that X is of even order, $|X| = 2g + 2$. Then, the linear map p passes to the quotient $2^X / \{0, X\}$. This quotient identifies naturally with the set of partitions of X into two subsets, and will be denoted $P_2(X)$. If $p: P_2(X) \to \mathbf{Z}/2\mathbf{Z}$ still denotes the induced map, we will write

$$P_2^+(X) = p^{-1}(0)$$
$$P_2^-(X) = p^{-1}(1).$$

With respect to the bilinear form e, X is orthogonal to 2_+^X, then inducing an alternate bilinear form, still denoted by e, on $P_2^+(X)$. This form is *non-degenerate*. To prove this, observe that if $A \in 2_+^X$, A different from $\varnothing$ and X, and $x \in A$, $x' \notin A$; then, if $A' = \{x, x'\}$, $e(A, A') = 1$.

3.6 Two cases may appear in this situation.

a) g is even. Then, the map $Q: 2_-^X \to \mathbf{Z}/2\mathbf{Z}$ passes to the quotient $P_2^-(X)$, so this becomes a symplectic torsor over $(P_2^+(X), e)$. But in this case the canonical quadratic form q_o does not pass to the quotient $P_2^+(X)$.

b) g is odd. Then, the map Q does not pass to the quotient, but q_o does, so there is a natural characteristic.

3.7 The following construction would help in developing the case where $|X|$ is even along the lines of 3.2-3.5, which I won't do. Let X be of odd order $|X| = 2g + 1$, and define $X' = X \amalg \{X\}$, thus $|X'| = 2g + 2$. We have a natural linear map

$$2^X \to 2^{X'}$$

and this is compatible with p, e, Q, q_o. Composing this with the passage to the quotient, I have a linear isomorphism

$$2^X \to P_2(X'),$$

and by compatibility with p, p', isomorphisms

$$2_+^X \to P_2^+(X')$$
$$2_-^X \to P_2^-(X').$$

The first is compatible with e, e', and with the canonical quadratic forms if g is odd. The second is compatible with Q, Q' if g is even.

§ 4 Basis and fundamental sets

4.1 *Normal basis.* Let (J, e) be a symplectic pair. A *normal basis* for (J, e) is a basis $(x_i)_{i \in I}$ for J with the property that $e(x_i, x_j) = 1$ for $i \neq j$, the set of ordered normal basis (i.e. for $I = \{1, ..., 2g\}$ if $2g = \dim J$) will be denoted $ONB(J, e)$. The symplectic group $\mathrm{Sp}(J, e)$ clearly acts on $ONB(J, e)$ and it does it simply transitively, because if two ordered normal bases for (J, e) are given, the unique linear automorphism transforming one into the other is obviously symplectic.

I have not yet shown that the set $ONB(J, e)$ is non-empty, this we will see as a consequence of the following construction, that relates symplectic basis (0.1) with normal basis. The set $SB(J, e)$ of symplectic basis is a torsor over $Sp(J, e)$, thus if $ONB(J, e)$ is non-empty, both torsors should be isomorphic and indeed there would be as many isomorphisms as elements in the group $Sp(J, e)$. What I proceed to exhibit now is a definite isomorphism

$$\alpha: SB(J, e) \to ONB(J, e)$$

with inverse β. If

$$x \in SB(J, e), x = (x_1, ..., x_g, x_1', ..., x_g')$$

let's put $y = \alpha(x)$, then by definition

$$y_{2k-1} = x_1 + \ldots + x_k + x_1' + \ldots + x_{k-1}'$$
$$y_{2k} = x_1 + \ldots + x_{k-1} + x_1' + \ldots + x_k' \quad k = 1, \ldots, g .$$

As for the inverse, if $y \in ONB(J, e)$, and $x = \beta(y)$, then one gets from the definition of α

$$x_k = y_1 + \ldots + y_{2k-2} + y_{2k-1}$$
$$x_k' = y_1 + \ldots + y_{2k-2} + y_{2k} \quad k = 1, \ldots, g .$$

It is clear from this definition that α is compatible with the actions of $Sp(J, e)$ on both sets.

4.2 *Azygetic sets.* Let (S, Q) be a symplectic torsor over a symplectic pair (J, e). A subset $A \subset S$ is *azygetic* if for any three different elements $s_1, s_2, s_3 \in A$ one has $Q(s_1) + Q(s_2) + Q(s_3) + Q(s_1 + s_2 + s_3) = 1$, or equivalently if $e(s_1, +s_2, s_1 + s_3) = 1$. A is *homogeneous* if Q is constant on it, i.e. if either $A \subset S^+$ or $A \subset S^-$. And the subset A is *linearly independent* if for some (or equivalently, for any) $s \in A$, the subset $s + (A - \{s\}) \subset J$ is linearly independent, or equivalently if $A + A$ spans a subspace of J of dimension $|A| - 1$.

Let A be an azygetic subset, $s \in A$, and let $B = s + (A - \{s\})$, I will show that the only possible linear relation on B is $\sum_{X \in B} x = 0$. Indeed, if $\Sigma \lambda_x x = 0$ is such a relation, for any $y \in B$, one has

$$0 = e(y, \sum_x \lambda_x x) = \sum_x \lambda_x e(y, x) = \sum_{\substack{x \in B \\ x \neq y}} \lambda_x$$

$$\sum_{x \neq y} \lambda_x = 0$$

Adding these equations for any $y, y' \in B$, one concludes that $\lambda_y = \lambda_{y'}$, which was to be shown. As a consequence of this, it follows that any azygetic subset of odd order is linearly independent, and that an azygetic subset has at most $2g + 2$ elements. It is easy to verify that if A is an azygetic subset of odd order and if $s = \sum_{t \in A} t$, $A \cup \{s\}$ is still azygetic.

4.3 *Basis for symplectic torsors.* A *basis* for a symplectic torsor (S, Q) over (J, e) is a maximal homogeneous, linearly independent, azygetic subset of S. A basis has exactly $2g + 1$ elements, where g is the genus of (S, Q). This comes from the fact that any symplectic torsor is isomorphic to one of the form (S_X, Q_X) constructed in § 3 because of the uniqueness result in 1.4, that for S_X, $X \subset S_X$ is clearly a basis with $2g + 1$ elements, and that a linearly independent subset can have at most $2g + 1$ elements.

The set of ordered basis for (S, Q) will be denoted by $OB(S, Q)$, the group $Sp(S, Q)$ acts on it.

The following construction is fundamental. Let $X \subset S$ be a basis, we have then a map

$$F_X: 2^X \to E(S)$$

(cf. 1.5.a) for the definition of $E(S)$), defined by

$$F_X(A) = \sum_{s \in A} s$$

It is clear that F_X is a group homomorphism, that sends subsets of X of even (resp. odd) order into J (resp. S), thereby inducing a linear homomorphism

$$\sigma_X: 2_+^X \to J$$

and a map compatible with the respective group actions

$$f_X: 2_-^X \to S\,.$$

To proceed further, let's choose a total order on X, $X = \{s_o, \ldots, s_{2g}\}$. Then, the $X_i = \{s_o, s_i\}$ (resp. $x_i = s_o + s_i$) for $i = 1, \ldots, 2g$ constitute an ordered normal basis for 2_+^X (resp. J), and as $\sigma_X(X_i) = x_i$ we have that σ_X is a symplectic isomorphism. It follows that f_x is a bijection, and indeed f_x defines an isomorphism of symplectic torsors between (S_X, Q_X) and (S, Q). To see this, we have to prove that if $A, A' \subset X$ are such that $|A| \equiv |A'|$ (4), then

$$Q\left(\sum_{s \in A} s\right) = Q\left(\sum_{s \in A'} s\right).$$

We know that Q is constant on X, and the condition on X of being azygetic means that for any three different $s_1, s_2, s_3 \in X$, $Q(s_1 + s_2 + s_3)$ is different from the value of Q on X. From this remark, the fact to be proved follows easily by induction and using the defining property (1.1.1) of symplectic torsors. For example, if $|A| = 5$, and we order $A = \{s_1, \ldots, s_5\}$, we have

$$Q(\Sigma s_1) + Q(s_1) = Q(s_1 + s_2 + s_3) + Q(s_1 + s_4 + s_5)$$

because $e(s_2 + s_3, s_4 + s_5) = 0$, thus

$$Q(s_1) = Q(\Sigma s_i)\,.$$

Summing up: starting from a basis $X \subset S$, one gets an isomorphism of symplectic pairs

$$\sigma_X: (J_X, e_X) \xrightarrow{\sim} (J, e)$$

underlying an isomorphism of symplectic torsors

$$f_X : (S_X, Q_X) \xrightarrow{\sim} (S, Q) .$$

As a consequence of this, we have that a basis is necessarily contained in S^+ for $g \equiv 0, 1\ (4)$, in S^- for $g \equiv 2, 3\ (4)$ (cf. 3.2.1).

4.4 PROPOSITION. *The set* $OB(S, Q)$ *of ordered basis for a symplectic torsor* (S, Q) *is a torsor over the group* $Sp(S, Q)$. *Moreover, the map*

$$OB(S, Q) \to ONB(J, e)$$

defined by

$$(s_i)_{0 \leq i \leq 2g} \mapsto (s_0 + s_i)_{1 \leq i \leq 2g}$$

is an isomorphism of torsors over $Sp(S, Q) \simeq Sp(J, e)$.

4.4.1 *Proof.* The map defined above is clearly compatible with the actions of $Sp(S, Q)$, $Sp(J, e)$ and the isomorphism between these groups described in 1.4. To prove the proposition, it is enough to show that this map is bijective. As $OB(S, Q)$ is non-empty and $ONB(J, e)$ is a torsor, this map is onto. It is injective too, because starting from the $x_i = s_o + s_i$ I can recover the s_i in the following way. If $s = \sum_{0 \leq i \leq 2g} s_i$, by the identification $S \simeq Q(J, e)$ in 1.5, s corresponds to the unique quadratic form q_s on J whose value on each of the x_i is 1 as it can be easily seen, thus s can be defined in terms of the x_i; but then

$$s_i = s + \sum_{j \neq i} x_j \ (0 \leqslant i \leqslant 2g, 1 \leqslant j \leqslant 2g) .$$

4.5 *Fundamental sets.* A *fundamental set* for a symplectic torsor (S, Q) is a maximal azygetic subset $F \subset S$. Any basis X for S defines a fundamental set, it suffices to put $F_X = X \cup \{s_X\}$, where $s_X = \sum_{s \in X} s$. Also, if F is a fundamental set and if $x \in J$, $x + F$ is a fundamental set too, as it is easily seen. In fact, for any fundamental set F, there exists a basis X and an $x \in J$ such that $F = x + F_X$. Let $F = \{t_o, \ldots, t_{2g+1}\}$ be an ordering of F, it is clear that if

$$x_i = t_0 + t_i \ (1 \leqslant i \leqslant 2g + 1) ,$$

the x_i for $1 \leqslant i \leqslant 2g$ constitute a normal basis for J, thus there exists a unique ordered basis $X = \{s_o, \ldots, s_{2g}\}$ for S such that $x_i = s_o + s_i$ (4.4). Then, if $x = s_o + t_o$, we have $t_i = x + s_X$, because $\Sigma t_i = 0$ and $s_X = \Sigma s_i$.

Observe that a fundamental set arising from a basis is homogeneous iff g is even. Indeed, it is homogeneous iff $2g + 1 \equiv 1\ (4)$, i.e. iff g is even.

It follows from the last part of prop. 3.2.1 that, in this case, the number of odd characteristics in the fundamental sets is congruent to g mod 4. We will see that this is a general fact.

4.5.1 PROPOSITION. *Let* $O(F)$ *be the number of odd characteristics in a fundamental set* F. *Then* $O(F) \equiv g\ (4)$. *Conversely, for any* $l \equiv g\ (4)$, *and* $l \leqslant 2g + 2$, *there are fundamental sets* F *with* $O(F) = l$.

4.5.2 *Proof.* We may safely restrict ourselves to the case where the symplectic torsor is S_X with its standard basis X, and $F = \{A\} + (X \cup \{X\})$ where $A \subset X$ is of even order $|A| = 2k$ (cf. 4.3). Then, in F there are $2k$ characteristics corresponding to subsets of X with $2k - 1$ elements, $2(g-k) + 1$ characteristics with $2k + 1$ elements, and 1 characteristic with $2(g-k) + 1$ elements, namely the ones obtained adding A to respectively the characteristics of the form $\{s\}$ $(s \in A)$, $\{s\}$ $(s \notin A)$, X. When g is even the second and third types have the same parity; when g is odd the first and third types have the same parity. From these remarks, it is easy to see that the number of elements of the same parity in F and $X \cup \{X\}$ are congruent mod 4, and that with this only restriction, this number can be arbitrary for F by conveniently choosing A. The proposition follows from this and from what was said just before its statement.

4.5.3 In Coble [1], additional material on fundamental sets may be found.

REFERENCES

[1] COBLE, A. An application of finite geometry to the characteristic theory of the odd and even theta functions. *Trans. A.M.S. 7* (1906), pp. 241-276.

[2] FAY, J. Theta functions on Riemann surfaces. *Lecture Notes in Mathematics, No. 352*, Springer Verlag (1973).

[3] IGUSA, J. *Theta Functions.* Springer Verlag (1972).

[4] MUMFORD, D. On the equations defining Abelian varieties I. *Invent. Math. 1* (1966), pp. 287-354.

[5] —— Theta characteristics of an algebraic curve. *Ann. Scient. ENS 4* (1971), pp. 181-192.

[6] WEBER, H. *Lehrbuch der algebra*, Band 2, Braunschweig (1896).

(Reçu le 20 février 1976)

Neantro Saavedra Rivano

Dept. de Matemática
Universidad Simón Bolívar
Apartado 5354
Caracas, Venezuela