§3 Symplectic torsors defined by finite sets

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **22 (1976)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **25.05.2024**

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*

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

In particular, there are group isomorphisms

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

§ 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 $p \colon 2^X \to \mathbf{Z}/2\mathbf{Z}$ defined by

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

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

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

d) A map $Q \colon 2^X_- \to \mathbf{Z}/2\mathbf{Z}$ 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 $I = \{1, \ldots, 2g\}$ 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

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

with inverse β. If

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

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