§4 Basis and fundamental sets

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **12.07.2024**

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 $I = \{1, \dots, 2g\}$ 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

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

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

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

(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

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

and a map compatible with the respective group actions

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

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

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

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

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

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