Bollettino
Unione Matematica Italiana

Marina Rosanna Marchisio

Abelian surfaces and products of elliptic curves

Bollettino dell'Unione Matematica Italiana, Serie 8, Vol. **1-B** (1998), n.2, p. 407–427.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=BUMI_1998_8_1B_2_407_0>

Bollettino dell'Unione Matematica Italiana, Unione Matematica Italiana, 1998.

Bollettino U. M. I.
(8) **1**-B (1998), 407-428

Abelian Surfaces and Products of Elliptic Curves.

Marina Rosanna Marchisio (*)

Sunto. – *Si dà una nuova e completa dimostrazione del risultato cruciale del metodo di Ruppert che consente di stabilire in maniera effettiva quando una superficie abeliana è isomorfa o isogena a un prodotto di curve ellittiche.*

Introduction.

In this paper we study the relationship between abelian surfaces and products of elliptic curves. In particular we study the problem to decide, with relatively simple calculations, whether an abelian surface, given its period matrix, is isomorphic or isogenous to a product of elliptic curves.

This problem was solved by Ruppert in [R] and its method was successively explained in [LB]. However in these two expositions the proof of the crucial proposition (see (2.11) below) is only outlined, whilst all details, even the essential ones, are left to the reader.

We thought that it would have been useful to give a new proof of (2.11), complete of all details, and to illustrate the method in all possible cases in order to show its effectiveness. Finally we apply it to an example.

1. – Preliminaries

(1.1) Definition. – *A complex torus* $X = V/\Lambda$, *with* V *vector space over* $\boldsymbol{C}$ *of dimension* g, Λ *lattice of* V *with a hermitian defined positive form* $H \colon V \times V \to \boldsymbol{C}$ *and such that* $H(\Lambda \times \Lambda) \subseteq \boldsymbol{Z}$, *is called* abelian variety *of dimension* g.

(1.2) Definition. – *An abelian variety of dimension* 2 *is called* abelian surface; *a complex torus* $X = V/\Lambda$ *of dimension* 1 *is called* elliptic curve *and it is always an abelian variety* (*see* [K]).

(*) I would like to thank Prof. Bert van Geemen for having pointed out to me this problem and for the useful suggestions.

(1.3) DEFINITION. – *Let* $X = V/\Lambda$ *be an abelian variety with* $\dim V = g$, *choose bases* $e_1, \ldots, e_g$ *of* V *and* $\lambda_1, \ldots, \lambda_{2g}$ *of the lattice* Λ. *Write* λ_i *in terms of the basis* $e_1, \ldots, e_g$:

$$\lambda_i = \sum_{j=1}^{g} \lambda_{ji} e_j \,.$$

The matrix:

$$\Pi = \begin{pmatrix} \lambda_{11} & \cdots & \cdots & \lambda_{1,2g} \\ \vdots & \vdots & \vdots & \vdots \\ \lambda_{g,1} & \cdots & \cdots & \lambda_{g,2g} \end{pmatrix} \in M(g \times 2g, \boldsymbol{C})$$

is called a period matrix *for* X.

The period matrix Π determines the complex torus X completely, but certainly it depends on the choice of the bases for V and Λ.

We consider products of elliptic curves E_1, E_2 which are, as is easily seen, abelian surfaces:

$$E_1 \times E_2 = \boldsymbol{C}/\Lambda_1 \times \boldsymbol{C}/\Lambda_2 \simeq \boldsymbol{C}^2/(\Lambda_1 \times \Lambda_2) = \boldsymbol{C}^2/\Lambda \,.$$

Recall that a homomorphism $f\colon X \to X'$ corresponds to a unique $\boldsymbol{C}$-linear map $F\colon V \to V'$ with $F(\Lambda) \subseteq \Lambda'$ inducing the homomorphism f.

(1.4) DEFINITION. – *Let* $\Phi\colon X \to X'$ *be a homomorphism between two abelian varieties of equal dimension. If* Φ *is surjective,* Φ *is called* isogeny.

X and X' are called *isogenous* if there exists an isogeny $\Phi\colon X \to X'$.

Let $\Phi\colon X \to X'$ be a homomorphism between abelian varieties of equal dimension; then

$$\Phi \text{ surjective} \Leftrightarrow \ker \Phi \text{ finite} \,.$$

2. – Ruppert's method.

The aim of this method is to see when an abelian surface is isomorphic or isogenous to a product of elliptic curves.

Let $\Lambda \cong \boldsymbol{Z}^4 \subseteq \boldsymbol{C}^2$ be a lattice. We consider an alternating form:

$$\alpha \colon \Lambda \times \Lambda \to \boldsymbol{C}$$

defined by

$$\alpha(u, v) = \det(u, v) = u_1 v_2 - u_2 v_1 \qquad (u = (u_1, u_2),\, v = (v_1, v_2) \in \boldsymbol{C}^2)\,,$$

so that α is bilinear and $\alpha(v, v) = 0$ for all $v \in \Lambda$, hence $\alpha(v, u) = -$ $\alpha(u, v)$.

(2.1) Definition. – *The form α is called* hyperbolic *if there is a decomposition of Λ*:

$$\Lambda = \Lambda_1 \oplus \Lambda_2$$

into submodules Λ_1 and Λ_2 which are isotropic with respect to α.

In other words:

α hyperbolic $\Leftrightarrow$ $\exists$ basis $\lambda_1, \lambda_2,\ \mu_1,\ \mu_2$ of Λ s.t. $\alpha(\lambda_1, \lambda_2) = \alpha(\mu_1, \mu_2) = 0$.

By abuse of notation we denote the extension of α to $\Lambda \otimes \boldsymbol{Q}$ also by α.

(2.2) Definition. – *The form*

$$\alpha \colon (\Lambda \otimes \boldsymbol{Q})^2 \to \boldsymbol{C}$$

is called hyperbolic over Q *if there is a decomposition:*

$$\Lambda \otimes \boldsymbol{Q} = V_1 \oplus V_2$$

into 2 subvector spaces which are isotropic with respect to α.

In other words:

α hyperbolic over $\boldsymbol{Q}$ $\Leftrightarrow$ $\exists$ a basis $\lambda_1, \lambda_2, \mu_1, \mu_2$ of $\Lambda \otimes \boldsymbol{Q}$

s. t. $\alpha(\lambda_1, \lambda_2) = \alpha(\mu_1, \mu_2) = 0$.

Both notions are independent of the choice of the coordinates of $\boldsymbol{C}^2$ since a coordinate transformation A in $\boldsymbol{C}^2$ changes α by a multiplicative constant; in fact $\alpha(Au, Av) = \det(A)\alpha(u, v)$ because:

$$\det(Au, Av) = \det\left(A \cdot \begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix}\right) = \det(A) \cdot \det\left(\begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix}\right).$$

(2.3) PROPOSITION. – *For an abelian surface $X = \boldsymbol{C}^2/\Lambda$ the following conditions are equivalent*:

(i) *X is isomorphic* (*respectively isogenous*) *to a product of elliptic curves*;

(ii) *the form α is hyperbolic* (*respectively hyperbolic over $\boldsymbol{Q}$*). ■

See [LB], p. 313, for the proof.

(2.4) REMARK. – Consider $\Lambda = \langle \lambda_1, \dots, \lambda_4 \rangle_{\boldsymbol{Z}}$ where $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ is a basis of Λ. Call $\alpha_{ij} = \alpha(\lambda_i, \lambda_j)$; then we have, with $u = \sum n_i \lambda_i$ and $v = \sum m_i \lambda_i \in \Lambda$:

$$\alpha(u, v) = \sum_{ij} \underbrace{n_i m_j}_{\in \boldsymbol{Z}} \alpha(\lambda_i, \lambda_j) =$$

$$(n_1 m_2 - n_2 m_1)\, \alpha_{12} + (n_1 m_3 - n_3 m_1)\, \alpha_{13} + (n_1 m_4 - n_4 m_1)\, \alpha_{14} +$$

$$(n_2 m_3 - n_3 m_2)\, \alpha_{23} + (n_2 m_4 - n_4 m_2)\, \alpha_{24} + (n_3 m_4 - n_4 m_3)\, \alpha_{34}\,.$$

This proves that $\alpha(\Lambda \times \Lambda) \subseteq \boldsymbol{Z} \cdot \alpha_{12} + \boldsymbol{Z} \cdot \alpha_{13} + \dots + \boldsymbol{Z} \cdot \alpha_{34}$.

Let $M = \langle \dots, \alpha_{ij}, \dots \rangle_{\boldsymbol{Z}}$ be the $\boldsymbol{Z}$-submodule of $\boldsymbol{C}$ generated by the values of α on $\Lambda \times \Lambda$.

Note that $\alpha(\Lambda \times \Lambda)$, in general, is not a $\boldsymbol{Z}$-module (in $\boldsymbol{C}$) (on the contrary of what is written in the book [LB], p. 314).

In fact consider

$$\begin{tikzcd}
\boldsymbol{Z}^4 \arrow[r, phantom, "\times"] \arrow[d, phantom, "\cap"] & \boldsymbol{Z}^4 \arrow[r, "\varphi"] \arrow[d, phantom, "\cap"] & \boldsymbol{Z}^6 \arrow[r, phantom, "\simeq"] \arrow[d, phantom, "\cap"] & \wedge^2 \boldsymbol{Z}^4 \arrow[d, phantom, "\cap"] \\
\boldsymbol{C}^4 \arrow[r, phantom, "\times"] & \boldsymbol{C}^4 \arrow[r, "\varphi_{\boldsymbol{C}}"] & \boldsymbol{C}^6 \arrow[r, phantom, "\simeq"] & \wedge^2 \boldsymbol{C}^4
\end{tikzcd}$$

where $\varphi_{\boldsymbol{C}}$ (= «α») is the Plücker embedding, see [G], p. 211. If we consider $\omega = e_0 \wedge e_1 + e_2 \wedge e_3$ then $\omega \in \wedge \boldsymbol{Z}^4 \subseteq \boldsymbol{C}^4$ but $\omega \notin \mathrm{Im}(\varphi_{\boldsymbol{C}})$ (ω has $p_{01} = 1$, $p_{23} = 1$ and other $p_{ij} = 0 \Rightarrow p_{01} p_{23} = 1 \neq 0 \Rightarrow \omega \notin \mathrm{Im}(\varphi_{\boldsymbol{C}})$).

(2.5) DEFINITION. – *The* rank *of an alterning form $\alpha \colon \Lambda \times \Lambda \to \boldsymbol{C}$ is the rank of the free $\boldsymbol{Z}$-submodule M ($\subseteq \boldsymbol{C}$) so $M \cong \boldsymbol{Z}^r$.*

If $y_1, \ldots, y_r$ is a basis of the $\boldsymbol{Z}$-module M, we can write:

$$\alpha(u, v) = \underbrace{\alpha_1(u, v)}_{\in \boldsymbol{Z}} y_1 + \ldots + \underbrace{\alpha_r(u, v)}_{\in \boldsymbol{Z}} y_r$$

with $\alpha_i \colon \Lambda \times \Lambda \to \boldsymbol{Z}$ alternating forms.

Note that the forms $\alpha_1, \ldots, \alpha_r$ are necessarily linearly independent over $\boldsymbol{Z}$.

Moreover it is clear that α is hyperbolic (over $\boldsymbol{Q}$) if and only if $\alpha_1, \ldots, \alpha_r$ are hyperbolic (over $\boldsymbol{Q}$) all with the same decomposition of Λ (respectively $\Lambda \otimes \boldsymbol{Q}$).

In fact if $\lambda_1, \lambda_2, \mu_1, \mu_2$ is a basis of Λ such that $0 = \alpha(\lambda_1, \lambda_2) = \alpha(\mu_1, \mu_2)$, we have:

$$0 = \alpha(\lambda_1, \lambda_2) = \alpha_1(\lambda_1, \lambda_2)\, y_1 + \ldots + \alpha_r(\lambda_1, \lambda_2)\, y_r\,,$$

$$0 = \alpha(\mu_1, \mu_2) = \alpha_1(\mu_1, \mu_2)\, y_1 + \ldots + \alpha_r(\mu_1, \mu_2)\, y_r$$

$$\Leftrightarrow \alpha_1(\lambda_1, \lambda_2) = \ldots = \alpha_r(\lambda_1, \lambda_2) = \alpha_1(\mu_1, \mu_2) = \ldots = \alpha_r(\mu_1, \mu_2) = 0\,,$$

because $y_1, \ldots, y_r$ are linearly independent.

(2.6) LEMMA. – *Let α be hyperbolic* (*respectively hyperbolic over $\boldsymbol{Q}$*) *of rank r. Then $2 \leqslant r \leqslant 4$.*

PROOF. – $r \geqslant 1$ since α is nondegenerate, i.e. $\forall v \in \Lambda$, $v \neq 0$, there exists $w \in \Lambda$ such that $\alpha(v, w) \neq 0$; moreover $r \geqslant 2$. In fact note that $\mathrm{rk}_{\boldsymbol{Z}}(\ldots, \alpha_{ij}, \ldots) = \mathrm{rk}_{\boldsymbol{Z}}(\ldots, \det(A\lambda_i, A\lambda_j), \ldots) = \mathrm{rk}_{\boldsymbol{Z}}(\ldots, (\det A)\cdot \alpha_{ij}, \ldots) \geqslant 2$ for any invertible matrix A. Take a basis of Λ such that λ_1, λ_2 are linearly independent over $\boldsymbol{C}$ (this is possible because if $\lambda_2, \lambda_3, \lambda_4 \in \lambda_1 \cdot \boldsymbol{C}$ then $\Lambda \subseteq \boldsymbol{C}$). Choose A such that $A \cdot \lambda_1 = e_1$ and $A \cdot \lambda_2 = e_2$. We obtain

$$\Pi = \begin{pmatrix} 1 & 0 & z_1 & w_1 \\ 0 & 1 & z_2 & w_2 \end{pmatrix}$$

and

$$\alpha_{12} = 1\,,$$

$$z_1 = -\alpha_{23}\,,$$

$$w_1 = -\alpha_{24}\,,$$

$$z_2 = \alpha_{13}\,,$$

$$w_2 = \alpha_{14}\,.$$

If $r = 1$ then z_i and w_i with $i = 1, 2 \in \boldsymbol{Z}$ and Λ would not be a lattice.

Moreover $r \leqslant 6$ for what we have seen before; finally $\alpha(\lambda_1, \lambda_2) = \alpha(\lambda_3, \lambda_4) = 0$ with $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ $\boldsymbol{Z}$-basis of Λ, therefore:

$$\operatorname{Im} \alpha \subseteq \boldsymbol{Z} \cdot \alpha_{13} + \boldsymbol{Z} \cdot \alpha_{14} + \boldsymbol{Z} \cdot \alpha_{23} + \boldsymbol{Z} \cdot \alpha_{24}$$

i.e. $r \leqslant 4$. ■

We start to consider the case $r = 2$, the «happiest» case.

(2.7) Proposition. – *Any alternating form $\alpha\colon \Lambda \times \Lambda \rightarrow \boldsymbol{C}$ of rank 2 is hyperbolic.* ■

See [R] for the proof.

An immediate consequence is the following theorem of Shioda and Mitani, see [Sh].

(2.8) Corollary. – *An abelian surface which is isogenous to a product of isogenous elliptic curves with complex multiplication is isomorphic to a product of elliptic curves.* ■

There exists a generalization of this corollary for abelian varieties of arbitrary dimension given by C. Schoen, see [S], p. 115-123, which says:

(2.9) Proposition. – *If X is an abelian variety of dimension g, isogenous to a product $\times_{i=1}^{g} E$ with E an elliptic curve with complex multiplication, then X is isomorphic to a product of elliptic curves.* ■

It remains to consider forms of rank 3 and 4.

(2.10) Remark. – We first recall some properties of the well known *Plücker quadric* (also called Klein quadric).

Let K be a field. Let x_{ij} with $0 \leqslant i < j \leqslant 3$ be the coordinates of $\boldsymbol{P}^5 = \boldsymbol{P}(\wedge^2 K^4)$. The Plücker quadric is defined by the equation:

$$x_{01} x_{23} - x_{02} x_{13} + x_{03} x_{12} = 0 .$$

The 2-dimensional subvector spaces of the vector space K^4 (points of the grassmannian of the lines of $\boldsymbol{P}^3$) correspond bijectively to the points of the Plücker quadric.

For any 2-dimensional subvector space $U = \langle u, v \rangle_K = \{hu + kv\colon h, k \in K\}$ with ${}^t u = (u_0, \ldots, u_3)$ and ${}^t v = (v_0, \ldots, v_3) \in K^4$ the elements:

$$p_{ij} := u_i v_j - u_j v_i$$

are the Plücker coordinates of U and

$$p(U) := (p_{01}\colon p_{02}\colon p_{03}\colon p_{12}\colon p_{13}\colon p_{23})$$

is the corresponding point on the quadric Q.

If V is another 2-dimensional subvector space of K^4 then

$$K^4 = U \oplus V \Leftrightarrow \text{the line } \overline{p(U)P(V)} \text{ is not contained in } Q\,.$$

Given a skew symmetric matrix A, we define an alternating form

$$A\colon K^4 \times K^4 \to K$$

$$A(u, v) := \sum_{ij=0}^{3} a_{ij} u_i v_j = \sum_{i<j} a_{ij} p_{ij} \qquad (\text{with } a_{ij} = -a_{ji} \in K)$$

and a hyperplane of $\boldsymbol{P}^5 = \boldsymbol{P}(\wedge^2 K^4)$ by

$$H(A) = \left\{ \sum_{0 \leq i < j \leq 3} a_{ij} x_{ij} = 0 \right\}.$$

Then a 2-dimensional subvector space U of K^4 is isotropic with respect to A ($A(u, v) = 0$ where $U = \langle u, v \rangle_K$) if and only if its corresponding point $p(U) \in Q$ lies on $H(A)$.

Let $\alpha = \alpha_1 y_1 + \ldots + \alpha_r y_r$ be the alternating form associated to the abelian surface $X = \boldsymbol{C}^2/\Lambda$ as above. Since the forms $\alpha_1, \ldots, \alpha_r$ are linearly independent over $\boldsymbol{Z}$, the intersection

$$E(\alpha) = H(\alpha_1) \cap \ldots \cap H(\alpha_r)$$

is a $(5-r)$-plane in $\boldsymbol{P}^5$.

(2.11) Proposition. – *a) α is hyperbolic if and only if there are distinct rational points q_1 and q_2, i.e. $q_i \in \boldsymbol{P}(\wedge^2 \boldsymbol{Q}^4)$, in $Q \cap E(\alpha)$ such that the following conditions hold:*

1) *the line joining the distinct rational points q_1 and q_2 is not contained in Q;*

2) *for every prime p statement* 1) *holds modulo p.*

b) α is hyperbolic over $\boldsymbol{Q}$ if and only if there are distinct rational points q_1 and q_2 in $Q \cap E(\alpha)$ such that 1) *holds.*

Proof. – *a)* α is hyperbolic if there are two $\boldsymbol{Z}$-submodules Λ_1 and Λ_2 of rank 2 of Λ such that $\Lambda = \Lambda_1 \oplus \Lambda_2$ and Λ_1 and Λ_2 are isotropic with respect to α_ν for $\nu = 1, \ldots, r$. $\Lambda = \Lambda_1 \oplus \Lambda_2 \Leftrightarrow \Lambda \otimes F = (\Lambda_1 \otimes F) \oplus (\Lambda_2 \otimes F)$ for $F = \boldsymbol{Q}$ and $F = \boldsymbol{F}_p$ for every prime p. By what we have said above this means that the line joining $p(\Lambda_1 \otimes F)$ and $p(\Lambda_2 \otimes F)$ is not contained in the Plücker quadric Q over F, for $F = \boldsymbol{Q}$ and $F = \boldsymbol{F}_p$ for all primes p.

The other implication is less obvious than this.

By hypothesis we have that $\exists q_1, q_2 \in Q \cap E(\alpha)$, distinct rational points, such that:

1) the line $\langle q_1, q_2 \rangle$ with q_1, q_2 distinct rational points is not contained in $Q/\boldsymbol{Q}$ ($=$ over $\boldsymbol{Q}$);

2) $\overline{q_1}$, $\overline{q_2}$ (images of q_i in $\boldsymbol{P}(\wedge^2 \boldsymbol{F}_p)$ are distinct points and the line $\langle \overline{q_1}, \overline{q_2} \rangle$ is not contained in $Q/\boldsymbol{F}_p$.

The statement 1) implies that there exist $V_1 \cong \boldsymbol{Q}^2 \subseteq \boldsymbol{Q}^4$ and $V_2 \cong \boldsymbol{Q}^2 \subseteq \boldsymbol{Q}^4$, $\langle q_1, q_2 \rangle \nsubseteq Q$ hence $\boldsymbol{Q}^4 = V_1 \oplus V_2$ (V_1 and V_2 are isotropic).

We define:

$$\Lambda_1 := V_1 \cap \Lambda \qquad \text{and} \qquad \Lambda_2 := V_2 \cap \Lambda\,.$$

Since $V = \Lambda \otimes \boldsymbol{Q}$ and the V_i are isotropic with respect to α, we have already $\alpha(\Lambda_i \times \Lambda_i) = 0$. Now we have to show:

$$\Lambda = \Lambda_1 \oplus \Lambda_2\,.$$

We give an easy example to show that this does not follow from $V = V_1 \oplus V_2$.

Consider $V = \boldsymbol{Q}^2$, $V_1 = \langle (1, 1) \rangle_{\boldsymbol{Q}}$, $V_2 = \langle (1, -1) \rangle_{\boldsymbol{Q}}$ and $\Lambda = \boldsymbol{Z}^2 \subseteq \boldsymbol{Q}^2$.

Then $V = V_1 \oplus V_2$ and we have:

$$\Lambda_1 = \Lambda \cap \langle (1, 1) \rangle_{\boldsymbol{Q}} = \langle (1, 1) \rangle_{\boldsymbol{Z}}\,, \qquad \Lambda_2 = \Lambda \cap \langle (1, -1) \rangle_{\boldsymbol{Q}} = \langle (1, -1) \rangle_{\boldsymbol{Z}}\,.$$

But $\boldsymbol{Z}^2 \neq \langle (1, 1) \rangle_{\boldsymbol{Z}} \oplus \langle (1, -1) \rangle_{\boldsymbol{Z}}$ because for example

$$\boldsymbol{Z}^2 \ni (1, 0) \neq (a + b, a - b) \qquad \text{for any } a, b \in \boldsymbol{Z}\,.$$

Also modulo 2 it isn't true that

$$(\boldsymbol{Z}/2\boldsymbol{Z})^2 = (\overline{1}, \overline{1})_{(\boldsymbol{Z}/2\boldsymbol{Z})} \oplus (\overline{1}, \overline{-1})_{(\boldsymbol{Z}/2\boldsymbol{Z})}$$

(modulo 2 we have that $-\overline{1} = \overline{1}$ because $-1 \equiv 1$ mod 2).

We could also use the fact that

$$\boldsymbol{Z}^2 = \langle (a, b), (c, d) \rangle_{\boldsymbol{Z}} \Leftrightarrow \det \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \pm 1\,.$$

In the previous example however $\det \begin{pmatrix} a & c \\ b & d \end{pmatrix} = -2 \neq \pm 1$.

We continue the proof. Note that

$$\Lambda = \Lambda_1 + \Lambda_2 \Rightarrow \Lambda = \Lambda_1 \oplus \Lambda_2\,.$$

In fact if $\lambda \in \Lambda_1 \cap \Lambda_2$ it follows that $\boldsymbol{Z}\lambda \subseteq \Lambda_1 \cap \Lambda_2 \Rightarrow \boldsymbol{Q}\lambda \subseteq V_1 \cap V_2 \Rightarrow V \neq V_1 \oplus V_2$, a contradiction. Hence $\Lambda = \Lambda_1 + \Lambda_2$ implies $\Lambda = \Lambda_1 \oplus \Lambda_2$ and we must show $\Lambda = \Lambda_1 + \Lambda_2$.

Consider the exact sequence $\Lambda_1 + \Lambda_2 \to \Lambda \to T \to 0$, $T = \Lambda/(\Lambda_1 + \Lambda_2)$. We want to show that $T=0$ because then $\Lambda=\Lambda_1+\Lambda_2$. Tensorizing with $\boldsymbol{F}_p$, we find

$$\boldsymbol{F}_p^2+\boldsymbol{F}_p^2\to\boldsymbol{F}_p^4\to T\otimes_{\boldsymbol{Z}}\boldsymbol{F}_p\to 0\,.$$

The condition 2) implies that for every p prime

$$\Lambda/p\Lambda=\Lambda_1/p\Lambda_1\oplus\Lambda_2/p\Lambda_2\,;$$

so for every p prime

$$\boldsymbol{F}_p^2+\boldsymbol{F}_p^2=\boldsymbol{F}_p^4\,.$$

In fact the $q_i\in Q\cap E(\alpha)\,/\boldsymbol{F}_p$, corresponding to $\Lambda_i\otimes_{\boldsymbol{Z}}\boldsymbol{F}_p$, are distinct and the line $\langle q_1, q_2\rangle\not\subseteq Q/\boldsymbol{F}_p$. Then $T\otimes_{\boldsymbol{Z}}\boldsymbol{F}_p=0\ \forall p$ prime $\Rightarrow T/pT=0\ \forall p$ prime. (Note that in this point we have used in essential way the condition 2) of the hypothesis.)

Since T is a finitely generated abelian group we have

$$T\cong\boldsymbol{Z}^r\oplus\boldsymbol{Z}/e_1\boldsymbol{Z}\oplus\boldsymbol{Z}/e_2\boldsymbol{Z}\oplus\ldots\oplus\boldsymbol{Z}/e_k\boldsymbol{Z}$$

with $e_1\,|e_2\ldots|e_k$.

By condition 1)

$$T\otimes\boldsymbol{Q}=\boldsymbol{Q}^4/(V_1\oplus V_2)=0\,.$$

On the other hand:

$$T\otimes\boldsymbol{Q}\simeq(\boldsymbol{Z}^r\otimes\boldsymbol{Q})\oplus(\boldsymbol{Z}/e_1\boldsymbol{Z}\oplus\ldots)\otimes\boldsymbol{Q}=\boldsymbol{Q}^r\oplus(\boldsymbol{Z}/e_1\boldsymbol{Z}\otimes\boldsymbol{Q}\oplus\ldots)\,.$$

Thus $T\otimes\boldsymbol{Q}=0$ gives $r=0$ so T is a finite group.

We know that $T/pT=0\forall p$ prime. Suppose for absurd that $e_k\neq 0$, i.e. that there is torsion. Choose p such that $p|e_k\Rightarrow e_k=p\cdot m$. Then we have the absurdity

$$0=T/pT\supseteq(\boldsymbol{Z}/e_k\boldsymbol{Z})\otimes\boldsymbol{F}_p\simeq(\boldsymbol{Z}/pm\boldsymbol{Z})/p(\boldsymbol{Z}/pm\boldsymbol{Z})\simeq\boldsymbol{Z}/p\boldsymbol{Z}\neq 0;$$

in fact $M\otimes_{\boldsymbol{Z}}\boldsymbol{F}_p\simeq M/pM$ and the last isomorphism follows from the theorem of isomorphism of the quotient group of a quotient group, see [B], p. 121.

Hence, in conclusion, $T/pT=0\forall p\Rightarrow T=0\Rightarrow\Lambda=\Lambda_1+\Lambda_2\Rightarrow\Lambda=\Lambda_1\oplus\Lambda_2\Rightarrow\alpha$ hyperbolic. This proves *a*).

Assertion *b*) follows similarly. ■

(2.12) REMARK. – What we have seen above in the proof of the Prop. (2.11) can be applied in an interesting way in the study of the degree of an isogeny.

Consider $\Lambda_1+\Lambda_2\subseteq\Lambda$, $V=V_1\oplus V_2$ and φ: $\boldsymbol{C}/\Lambda_1\times\boldsymbol{C}/\Lambda_2\to\boldsymbol{C}^2/\Lambda$.

Now we study the following diagram which has exact rows:

$$\begin{tikzcd}
 & & & N = \ker\varphi \arrow[d] & \\
0 \arrow[r] & \Lambda_1 \oplus \Lambda_2 = C_1 \arrow[r] \arrow[d, "\partial_C"', "\simeq"] & \boldsymbol{C} \oplus \boldsymbol{C} = D_1 \arrow[r] \arrow[d, "\partial_D"', "\simeq"] & \boldsymbol{C}/\Lambda_1 \oplus \boldsymbol{C}/\Lambda_2 = Y_1 \arrow[r] \arrow[d, "\partial_E"', "\varphi"] & 0 \\
0 \arrow[r] & \Lambda = C_0 \arrow[r] & \boldsymbol{C}^2 = D_0 \arrow[r] & \boldsymbol{C}^2/\Lambda = Y_0 \arrow[r] & 0
\end{tikzcd}$$

We can apply the zig-zag lemma, see [M], p. 136, and obtain the long exact sequence in homology:

$$\ldots \to H_1(D) \to H_1(Y) \to H_0(C) \to H_0(D)$$

i.e.

$$\ldots \to \underbrace{\underbrace{\ker(\partial_D)}_{0} / \underbrace{\mathrm{Im}\,(D_2)}_{0}}_{0} \to N \to \underbrace{\Lambda/\mathrm{Im}\,\underbrace{(\Lambda_1 \oplus \Lambda_2)}_{\Lambda_1 + \Lambda_2}}_{T} \to \underbrace{\boldsymbol{C}^2/(\boldsymbol{C} \oplus \boldsymbol{C})}_{0}$$

i.e.

$$0 \to N \to T \to 0$$

from which $N \simeq T$.

Thus if $\Lambda \neq \Lambda_1 \oplus \Lambda_2$ then there exists an isogeny $E_1 \times E_2 \to A$ and we obtain the exact sequence

$$0 \to \underbrace{N}_{\Lambda/(\Lambda_1 + \Lambda_2)} \to E_1 \times E_2 \to A \to 0$$

and

$N/pN \neq 0 \Leftrightarrow T/pT \neq 0 \Leftrightarrow$ mod. p the points q_1, q_2 are equal

or the line $\overline{q_1 q_2}$ isn' t contained in Q .

We have that

$$(\text{degree isogeny } E_1 \times E_2 \to A) = \# N$$

and $p \mid \# N \Leftrightarrow N/pN \neq 0$ («essential» primes for the condition 2) of the Proposition (2.11)). Let's see an example.

Assume that $Q \cap E(\alpha)$ has equation $x_1^2 + x_2^2 - x_3^2 = 0$ (conic in $\boldsymbol{P}^2$). Let $q_1 = (1, 0, 1)$ and $q_2 = (0, 1, 1)$ (so $q_1 \neq q_2$ for any p). Only modulo 2 this conic is singular (double line), so N has only elements of order powers of 2.

(2.13) REMARK. – The Prop. (2.11) holds also for $r = 2$, so the Proposition (2.7) can be deduced from this.

(2.14) REMARK. – We discuss separately the cases when the rank r of α is 2, 3, 4 (see Lemma (2.6)).

Case $r = 2$.

Then $E(\alpha)$ is a 3-plane in $\boldsymbol{P} \wedge^2 \boldsymbol{Q}^4$ given by 2 linear equations and $Q \cap E(\alpha)$ is a quadric in $\mathbf{P}^3$ given by a symmetric matrix $F \in M_4(\boldsymbol{Z})$. The rank of F can be 0, 1, 2, 3 or 4, but the cases 0, 1 do not occur (see below), and $Q \cap E(\alpha)$ will be respectively:

- $\mathrm{rk} F = 2$, two distinct planes,
- $\mathrm{rk} F = 3$, quadric cone,
- $\mathrm{rk} F = 4$, smooth quadric.

We have proved above that α is always hyperbolic (see Prop. (2.7)). We can prove easily that α is hyperbolic over $\boldsymbol{Q}$ directly.

If $\mathrm{rk}\, F$ is different from 0, 1, then there exist two distinct rational points, q_1 and q_2, such that the line joining q_1 and q_2 is not contained in Q and this also holds modulo p for all primes p. In fact we note that $Q \subseteq \boldsymbol{P}^5$ is the Grassmannian of the line of $\boldsymbol{P}^3$ and on it there are two rulings of 2-planes corresponding to all lines throught a point $p \in \boldsymbol{P}^3$ and to all lines contained in a 2-plane $\pi \subseteq \boldsymbol{P}^3$, see [H], p. 291. Moreover in $\boldsymbol{P}^5$ we have that $(\boldsymbol{P}^2/\boldsymbol{Q}) \cap (\boldsymbol{P}^3/\boldsymbol{Q}) =$ a point $\in \boldsymbol{P}^5/\boldsymbol{Q}$, so on $Q \cap E(\alpha)$ there are a lot of distinct rational points that aren't all contained in a line. We conclude that α is hyperbolic over $\boldsymbol{Q}$.

Now we exclude the case that $\mathrm{rk} F = 1$, that is, $E(\alpha) \cap \boldsymbol{P}^5$ is a double plane. We know that Q is smooth and all smooth quadrics of $\boldsymbol{P}^5$ are isomorphic to it. Note that $Q \cap E(\alpha)$, with $E(\alpha) \cong \boldsymbol{P}^2$ linear space of dim. 2, is different from $2\boldsymbol{P}^2$ (double plane). If in fact, for example, $Q \cap E(\alpha)$ is the double plane π with equation $x_4 = x_5 = 0$, the equation of Q will be of the type:

$$x_4 \underbrace{l(x_0, \dots, x_5)}_{\text{linear}} + x_5 \underbrace{l(x_0, \dots, x_5)}_{\text{linear}} = 0\,.$$

The matrix associated to Q would be of the type

$$M = \left(\begin{array}{cccc|cc} 0 & 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & 0 & * & * \\ \hline * & * & * & * & * & * \\ * & * & * & * & * & * \end{array}\right)$$

hence $\det M = 0$. But this isn't possible because Q is a smooth quadric and so the determinant of the matrix associated to it is different from 0. Obviously also $\mathrm{rk} F \neq 0$ and then $\mathrm{rk} F = 2$ or 3 or 4.

Case $r = 3$.

$E(\alpha)$ is a 2-plane given by 3 linear equations, thus $Q \cap E(\alpha)$ is a conic in $\boldsymbol{P}^2$ given by a symmetric matrix $F \in M_3(\boldsymbol{Z})$.

The rank of F can be 0, 1, 2 or 3.

a) $\operatorname{rk} F = 0 \Rightarrow Q \cap E(\alpha)$ is also $\boldsymbol{P}^2$ (that is, $E(\alpha) \subseteq Q$.)

There exist no $q_1, q_2 \in Q \cap E(\alpha)$ such that the line joining q_1 and q_2 is not contained in Q. We can conclude that α is not hyperbolic.

b) $\operatorname{rk} F = 1 \Rightarrow Q \cap E(\alpha)$ is a line l counted twice.

There exist no $q_1, q_2 \in Q \cap E(\alpha) = l$ such that the line joining q_1 and q_2 (which is again l) is not contained in Q. We can concude that α is not hyperbolic.

c) $\operatorname{rk} F = 2 \Rightarrow Q \cap E(\alpha)$ consists of two different lines l_1 and l_2 and the point $l_1 \cap l_2$ is the singular point of $Q \cap E(\alpha)$.

Either the singular point of $Q \cap E(\alpha)$ is the unique rational point and so α is not hyperbolic.

For example if $E(\alpha)$ has equations:

$$x_{23} = x_{01}\,, \qquad x_{02} = 0\,, \qquad x_{12} = x_{03}$$

then $Q \cap E(\alpha)$ has equation $x_{01}^2 + x_{03}^2 = 0$ i.e. $(x_{01} + ix_{03})(x_{01} - ix_{03}) = 0$ and (0:0:1) is the unique rational point.

Or we have that $Q \cap E(\alpha)$ is defined by the product of two linear forms with coefficients in $\boldsymbol{Q}$. Now we have:

α is hyperbolic $\Leftrightarrow$ the 2 lines l_1, l_2 of $Q \cap E(\alpha)$ are distinct modulo $p (\forall p$ prime).

The implication $\Rightarrow$ is obvious. We have to show the other implication. It is not sufficient to say take a point q_1 on l_1 (not on l_2) and a point q_2 on l_2 (not on l_1) as it is stated in Ruppert's paper because if, for example, $E(\alpha)$ has equation $x_{02} = x_{03} = x_{12} = 0$ and we take the points $(x_{01}\colon x_{23}\colon x_{13}) = (0:2:1), (2:0:1)$, $l_1\colon x = 0$, $l_2\colon y = 0$ and $p = 2$, then mod p the points are not distinct.

Consider two lines with equations

$$\begin{cases} ax + by + cz = 0\,, \\ a'x + b'y + c'z = 0\,. \end{cases}$$

We will simplify these equations. In case $a \neq 0$, $b \neq 0$ let $a = da'$ and $b = db'$

where g.c.d. $(a', b') = 1 \Rightarrow qa' + rb' = 1$. We can consider the transformation

$$\begin{pmatrix} q & r \\ -b' & a' \end{pmatrix}$$

where $\begin{pmatrix} q & r \\ -b' & a' \end{pmatrix} \in \mathrm{GL}_2(\boldsymbol{Z})$ with determinant 1.

The equations of the two lines become

$$\begin{cases} dx + cz = 0\,, \\ a'x + b'y + c'z = 0\,. \end{cases}$$

We may assume g.c.d. $(d, c) = 1$ and, with an analogous tranformation, we obtain

$$\begin{cases} x = 0\,, \\ a'x + b'y + c'z = 0\,. \end{cases}$$

With the same trick we obtain

$$\begin{cases} x = 0\,, \\ a'x + d'y = 0\,. \end{cases}$$

By the assumption, for all primes p, modulo p: $Z(x = 0) \neq Z(a'x + d'y = 0)$. Thus $\nexists p$, s.t. $p | d' \Rightarrow d' = \pm 1$.

Now we have, with $a'' = \pm a'$,

$$\begin{cases} x = 0\,, \\ a''x + y = 0\,. \end{cases}$$

If we substitute: $y = -a''x + y$ then we obtain

$$\begin{cases} x = 0\,, \\ y = 0\,. \end{cases}$$

Let $q_1 = (0:1:0)$ in $x = 0$ (not in $y = 0$), and $q_2 = (1:0:0)$ in $y = 0$ (not in $x = 0$), then the line $z = 0$ joining q_1 and q_2 is not contained in $Z(xy = 0)$ modulo p for any p.

d) $\mathrm{rk} F = 3 \Rightarrow Q \cap E(\alpha)$ is a smooth conic in $\boldsymbol{P}^2$.

It can happen that $Q \cap E(\alpha)$ has no rational points. In this case α

is not hyperbolic. For example if $E(\alpha)$ has equations

$$x_{23} = x_{01}\,, \qquad x_{02} = x_{13}\,, \qquad x_{12} = x_{03}\,,$$

then $E(\alpha) \cap Q$ has equation $x_{01}^2 + x_{02}^2 + x_{03}^2 = 0$.

If the condition 1) of the Prop. (2.11) is satisfied then using the Hasse-Minkowski theorem we have (see [R], p. 298, for the proof.)

$$\alpha \text{ hyperbolic} \Leftrightarrow \forall\ p \text{ divisor of } \det F\,,$$

$$\exists \text{ a rat. not sing. point on } Q \cap E(\alpha) \bmod p\,.$$

Case $r = 4$.

$E(\alpha)$ is a 1-plane given by four linear equations and $Q \cap E(\alpha)$ is a quadric in $\boldsymbol{P}^1$ given by a symmetric matrix $F \in M_2(\boldsymbol{Z})$.

The rank of F can be 0, 1 or 2.

a) $\mathrm{rk} F = 0 \Rightarrow Q \cap E(\alpha) = \boldsymbol{P}^1 \Rightarrow \alpha$ is not hyperbolic.

b) $\mathrm{rk} F = 1 \Rightarrow Q \cap E(\alpha)$ is a point counted twice $\Rightarrow \alpha$ is not hyperbolic.

c) $\mathrm{rk} F = 2 \Rightarrow Q \cap E(\alpha) = 2$ different points.

If q_1 e q_2 are rational the condition 1) of the Prop. (2.11) holds. Then we want the condition 2) so we have:

$$\alpha \text{ hyperbolic} \Leftrightarrow \text{the quadric } Q \cap E(\alpha) \text{ is two distinct rat. points}$$

$$\text{which are different mod } p, \ \forall \text{ prime } p\,.$$

The hyperbolicity of α over $\boldsymbol{Q}$ can be characterized similarly.

3. – Applications.

From what we have explained above it follows that Ruppert's method to see when an abelian surface is isomorphic or isogenous to a product of curves, is effective. Given a period matrix of X it's relatively simple to apply it. There is an example in [R], we give another example following an exercise suggested by [LB].

(3.1) EXAMPLE. – Let C be a projective curve of genus 2 with non trivial reduced automorphism group. Recall that to every smooth projective curve C over $\boldsymbol{C}$ of genus g we can associate an abelian variety $J(C)$ of dimension g called the Jacobian of C.

According to O. Bolza, see [Bo], the curve C is isomorphic to one of the following 6 types of curves:

Type	Equation	$\overline{\text{Aut}\, C}$ red. aut. gr. of C	$\Pi = (Z, 1)$ Period Mat. of $J(C)$
I	$y^2 = (x^2 - a^2)(x^2 - b^2)(x^2 - 1)$	$\boldsymbol{Z}/2\boldsymbol{Z}$	$Z = \begin{pmatrix} z & \frac{1}{2} \\ \frac{1}{2} & z' \end{pmatrix}$
II	$y^2 = (x^2 - a^2)(x^2 - a^{-2})$	D_2	$Z = \begin{pmatrix} z & \frac{1}{2} \\ \frac{1}{2} & z \end{pmatrix}$
III	$y^2 = x(x^3 - a^3)(x^3 - a^{-3})$	D_3	$Z = \begin{pmatrix} 2z & z \\ z & 2z \end{pmatrix}$
IV	$y^2 = x^6 - 1$	D_6	$Z = \begin{pmatrix} \frac{2i}{\sqrt{3}} & \frac{i}{\sqrt{3}} \\ \frac{i}{\sqrt{3}} & \frac{2i}{\sqrt{3}} \end{pmatrix}$
V	$y^2 = x(x^4 - 1)$	σ_4	$Z = \begin{pmatrix} \frac{-1 + i\sqrt{2}}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{-1 + i\sqrt{2}}{2} \end{pmatrix}$
VI	$y^2 = x(x^5 - 1)$	$\boldsymbol{Z}/5\boldsymbol{Z}$	$Z = \begin{pmatrix} 1 - \varepsilon^4 & -\varepsilon^2 - \varepsilon^4 \\ -\varepsilon^2 - \varepsilon^4 & \varepsilon \end{pmatrix}$ con $\varepsilon = e\left(\frac{2\pi i}{5}\right)$

We can see that all types, except VI, are a specialization of type I.

Using Ruppert's method we want to show that:

a) If C is of type I, its Jacobian J is isogenous to a product of elliptic curves. In general, for example if $1, z, z', zz'$ are linearly independent over $\boldsymbol{Q}$, J is not isomorphic to a product of elliptic curves.

b) If C is of type II, its Jacobian J is isogenous to a product of elliptic curves if and only if z is contained in some imaginary quadratic field.

c) If C is of type III, IV or V its Jacobian J is isomorphic to a product of elliptic curves.

d) If C is of type VI, its Jacobian J is a simple abelian surface.

a)

$$\Pi = \begin{pmatrix} z & \frac{1}{2} & 1 & 0 \\ \frac{1}{2} & z' & 0 & 1 \end{pmatrix}.$$

If we call the columns of Π $\lambda_1, \lambda_2, \lambda_3, \lambda_4$, basis of Λ in function of e_1, e_2 basis of $\boldsymbol{C}^2$, we have that:

$$\begin{aligned} \alpha(\lambda_1, \lambda_2) &= -\frac{1}{4} + zz', & \alpha(\lambda_2, \lambda_3) &= -z', \\ \alpha(\lambda_1, \lambda_3) &= -\frac{1}{2}, & \alpha(\lambda_2, \lambda_4) &= \frac{1}{2} \\ \alpha(\lambda_1, \lambda_4) &= z, & \alpha(\lambda_3, \lambda_4) &= 1. \end{aligned}$$

They generate

$$\boldsymbol{Z}\cdot\frac{1}{2} + \boldsymbol{Z}\cdot z + \boldsymbol{Z}\cdot(-z') + \boldsymbol{Z}\cdot\left(-\frac{1}{4} + zz'\right)$$

$\Rightarrow \operatorname{rk}\alpha \leqslant 4$.

If $1/2$, z, $-z'$, $-1/4 + zz'$ are linearly independent over $\boldsymbol{Q}$ then $r = 4$. Consider the decomposition of α:

$$\alpha = \alpha_1 \cdot \underbrace{1/2}_{y_1} + \alpha_2 \cdot \underbrace{z}_{y_2} + \alpha_3 \cdot \underbrace{(-z')}_{y_3} + \alpha_4 \cdot \underbrace{(-1/4 + zz')}_{y_4}.$$

To obtain the equations of $E(\alpha)$ we write:

$$\begin{aligned} \alpha(u, v) = \alpha(n_1\lambda_1 + n_2\lambda_2 + n_3\lambda_3 + n_4\lambda_4,\ m_1\lambda_1 + m_2\lambda_2 + m_3\lambda_3 + m_4\lambda_4) = \\ (n_1m_2 - n_2m_1)\underbrace{\alpha(\lambda_1, \lambda_2)}_{y_4} + (n_1m_3 - n_3m_1)\underbrace{\alpha(\lambda_1, \lambda_3)}_{-y_1} + \\ (n_1m_4 - n_4m_1)\underbrace{\alpha(\lambda_1, \lambda_4)}_{y_2} + (n_2m_3 - n_3m_2)\underbrace{\alpha(\lambda_2, \lambda_3)}_{y_3} + \\ (n_2m_4 - n_4m_2)\underbrace{\alpha(\lambda_2, \lambda_4)}_{y_1} + (n_3m_4 - n_4m_3)\underbrace{\alpha(\lambda_3, \lambda_4)}_{2y_1}, \end{aligned}$$

from which

$$\alpha(u, v) = (-n_1 m_3 + n_3 m_1 + n_2 m_4 - n_4 m_2 + 2n_3 m_4 - 2n_4 m_3)\, y_1 + \\ +(n_1 m_4 - n_4 m_1)\, y_2 + (n_2 m_3 - n_3 m_2)\, y_3 + (n_1 m_2 - n_2 m_1)\, y_4 = \\ (-p_{13} + p_{24} + 2p_{34})\, y_1 + p_{14} y_2 + p_{23} y_3 + p_{12} y_4 \,.$$

Note that the indices are 1, 2, 3, 4 instead of 0, 1, 2, 3.

$Q \cap E(\alpha)$ has equations:

$$\begin{cases} x_{13} = x_{24} + 2x_{34}\,, \\ x_{12} = x_{14} = x_{23} = 0\,, \\ x_{12} x_{34} - x_{13} x_{24} + x_{14} x_{23} = 0\,, \end{cases}$$

from which $2x_{34} x_{24} + x_{24}^2 = 0$ which is a quadric in $\boldsymbol{P}^1$.

In char 2 it is $x_{24}^2 = 0$ i.e. a double point then α is not hyperbolic. But α is hyperbolic over $\boldsymbol{Q}$ then X is isogeneous to a product of elliptic curves.

We note that if $1/2, z, -z', 1/4 - zz'$ are linearly independent over $\boldsymbol{Q}$ then also $1, z, z', zz'$ are linearly independent over $\boldsymbol{Q}$ hence, in general, X is not isomorphic to a product of elliptic curves.

b)

$$\Pi = \begin{pmatrix} z & \frac{1}{2} & 1 & 0 \\ \frac{1}{2} & z & 0 & 1 \end{pmatrix}.$$

Using what we have seen in *a*) and putting $z = z'$ we find:

$$\alpha(\lambda_1, \lambda_2) = -\frac{1}{4} + z^2\,, \quad \alpha(\lambda_2, \lambda_3) = z\,,$$

$$\alpha(\lambda_1, \lambda_3) = -\frac{1}{2}\,, \quad \alpha(\lambda_2, \lambda_4) = \frac{1}{2}\,,$$

$$\alpha(\lambda_1, \lambda_4) = z\,, \quad \alpha(\lambda_3, \lambda_4) = 1\,.$$

If $1/2, z, -1/4 + z^2$ are linearly independent over $\boldsymbol{Q}$, then $r = 3$ and we can consider the decomposition:

$$\alpha = \alpha_1 \cdot \underbrace{1/2}_{y_1} + \alpha_2 \cdot \underbrace{(z)}_{y_2} + \alpha_3 \cdot \underbrace{(-1/4 + z^2)}_{y_3}.$$

If $A \in M_4(\boldsymbol{Z})$ is the matrix associated to α, to obtain the equations of $E(\alpha)$ we write:

$$\alpha(u, v) = \alpha_1(u, v)\, y_1 + \alpha_2(u, v)\, y_2 + \alpha_3(u, v)\, y_3\,,$$

$$\alpha(u, v) = {}^t uAv = ({}^t uA_1 v)\, y_1 + ({}^t uA_2 v)\, y_2 + ({}^t uA_3 v)\, y_3\,,$$

$$\alpha(u, v) = \alpha(n_1\lambda_1 + n_2\lambda_2 + n_3\lambda_3 + n_4\lambda_4,\ m_1\lambda_1 + m_2\lambda_2 + m_3\lambda_3 + m_4\lambda_4) =$$

$$(n_1m_2 - n_2m_1)\ \underbrace{\alpha(\lambda_1, \lambda_2)}_{y_3} + (n_1m_3 - n_3m_1)\ \underbrace{\alpha(\lambda_1, \lambda_3)}_{-y_1} +$$

$$(n_1m_4 - n_4m_1)\ \underbrace{\alpha(\lambda_1, \lambda_4)}_{y_2} + (n_2m_3 - n_3m_2)\ \underbrace{\alpha(\lambda_2, \lambda_3)}_{y_2} +$$

$$(n_2m_4 - n_4m_2)\ \underbrace{\alpha(\lambda_2, \lambda_4)}_{y_1} + (n_3m_4 - n_4m_3)\ \underbrace{\alpha(\lambda_3, \lambda_4)}_{2y_1}$$

from which

$$\alpha(u, v) = (-n_1m_3 + n_3m_1 + n_2m_4 - n_4m_2 + 2n_3m_4 - 2n_4m_3)\, y_1 +$$

$$(n_1m_4 - n_4m_1 + n_2m_3 - n_3m_2)\, y_2 + (n_1m_2 - n_2m_1)\, y_3 =$$

$$(-p_{13} + p_{24} + 2p_{34})\, y_1 + (p_{14} + p_{23})\, y_2 + p_{12}\, y_3\,.$$

$Q \cap E(\alpha)$ is a quadric in $\boldsymbol{P}^2$ with equations:

$$\begin{cases} x_{14} = -x_{23}\,, \\ x_{12} = 0\,, \\ x_{13} = x_{24} + 2x_{34}\,, \\ x_{12}x_{34} - x_{13}x_{24} + x_{14}x_{23} = 0\,. \end{cases}$$

$\Rightarrow x_{24}^2 + 2x_{34}x_{24} + x_{23}^2 = 0$ $(\mathrm{rg}\, F = 3)$.

In char 2 we have $x_{24}^2 + x_{23}^2 = (x_{24} + x_{23})^2$ double line.

$\Rightarrow X$ is isogenous to a product of elliptic curves, but X is not isomorphic to a product of elliptic curves.

Moreover z is contained in a imaginary quadratic field $\Leftrightarrow z = x + y\sqrt{-d}$ with $d > 0$, $x, y \in \boldsymbol{Q}$ $\Leftrightarrow z$ is a root of an equation of degree 2 with coefficients over $\boldsymbol{Q}$ irreducible in $\boldsymbol{Q}$.

$az^2 + bz + c = 0$ with $a, b, c \in \boldsymbol{Q}$ and $a \neq 0 \Leftrightarrow z^2 + (b/a)z + (d/a) = 0$ if and only if $-1/4 + z^2 = -(b/a)\,z - c/a - 1/4 \Leftrightarrow -1/4 + z^2$ is a linear combination of 1 and $z \Leftrightarrow \mathrm{rk}\,\alpha = 2 \Leftrightarrow \alpha$ is hyperbolic $\Leftrightarrow X$ is isomorphic to a product of elliptic curves.

c) We consider the type III, types IV and V are analogous.

Consider $z = a + ib$ with $b \neq 0$ i. e. $z \in \boldsymbol{C}$.

$$\Pi = \begin{pmatrix} 2z & z & 1 & 0 \\ z & 2z & 0 & 1 \end{pmatrix},$$

$$\begin{cases} \alpha(\lambda_1, \lambda_2) = -z^2 + 4z^2 = 3z^2\,, & \alpha(\lambda_2, \lambda_3) = -2z\,, \\ \alpha(\lambda_1, \lambda_3) = -z\,, & \alpha(\lambda_2, \lambda_4) = z\,, \\ \alpha(\lambda_1, \lambda_4) = 2z\,, & \alpha(\lambda_3, \lambda_4) = 1\,. \end{cases}$$

If $1, z, z^2$ are linearly independent over $\boldsymbol{Q}$ then $\operatorname{rk}\alpha = 3$.

We can consider the decomposition of α:

$$\alpha = \alpha_1 \cdot \underbrace{1}_{y_1} + \alpha_2 \cdot \underbrace{(z)}_{y_2} + \alpha_3 \cdot \underbrace{z^2}_{y_3}.$$

If $A \in M_4(\boldsymbol{Z})$ is the matrix associated to α to obtain the equations of $E(\alpha)$ we write:

$$\alpha(u, v) = \alpha_1(u, v)\, y_1 + \alpha_2(u, v)\, y_2 + \alpha_3(u, v)\, y_3\,,$$

$$\alpha(u, v) = {}^t uAv = ({}^t uA_1 v)\, y_1 + ({}^t uA_2 v)\, y_2 + ({}^t uA_3 v)\, y_3\,,$$

$$\begin{aligned}\alpha(u, v) = \alpha(n_1\lambda_1 + n_2\lambda_2 + n_3\lambda_3 + n_4\lambda_4,\ m_1\lambda_1 + m_2\lambda_2 + m_3\lambda_3 + m_4\lambda_4) = \\ (n_1 m_2 - n_2 m_1)\, \underbrace{\alpha(\lambda_1, \lambda_2)}_{3y_3} + (n_1 m_3 - n_3 m_1)\, \underbrace{\alpha(\lambda_1, \lambda_3)}_{-y_2} + \\ (n_1 m_4 - n_4 m_1)\, \underbrace{\alpha(\lambda_1, \lambda_4)}_{2y_2} + (n_2 m_3 - n_3 m_2)\, \underbrace{\alpha(\lambda_2, \lambda_3)}_{-2y_2} + \\ (n_2 m_4 - n_4 m_2)\, \underbrace{\alpha(\lambda_2, \lambda_4)}_{y_2} + (n_3 m_4 - n_4 m_3)\, \underbrace{\alpha(\lambda_3, \lambda_4)}_{y_1}\end{aligned}$$

from which

$$\begin{aligned}\alpha(u, v) = (n_3 m_4 - n_4 m_3) y_1 + \\ (-n_1 m_3 + n_3 m_1 + 2n_1 m_4 - 2n_4 m_1 - 2n_2 m_3 + 2n_3 m_2 + n_2 m_4 - n_4 m_2)\, y_2 + \\ (3n_1 m_2 - 3n_2 m_1)\, y_3 = p_{34} y_1 + (-p_{13} + 2p_{14} - 2p_{23} + p_{24})\, y_2 + 3p_{12} y_3\,.\end{aligned}$$

$Q \cap E(\alpha)$ is a quadric in $\boldsymbol{P}^2$ of equations:

$$\begin{cases} x_{34} = x_{12} = 0\,, \\ x_{13} = 2x_{14} - 2x_{23} + x_{24}\,, \\ x_{12} x_{34} - x_{13} x_{24} + x_{14} x_{23} = 0\,. \end{cases}$$

$\Rightarrow -2x_{14}x_{24} + 2x_{23}x_{24} - x_{24}^2 + x_{14}x_{23} = 0$ ($\operatorname{rk} F = 3$ always).

$\Rightarrow \alpha$ is hyperbolic $\Rightarrow X$ is isomorphic to a product of elliptic curves.

Moreover if $1, z, z^2$ are linearly independent over $\boldsymbol{Q}$ (i.e. z^2 linear combination of 1 and z) $\Rightarrow \operatorname{rk}\alpha = 2 \Rightarrow \alpha$ is hyperbolic $\Rightarrow X$ is isomorphic to a product of elliptic curves.

d)

$$\Pi = \begin{pmatrix} 1 - \varepsilon^4 & -\varepsilon^2 - \varepsilon^4 & 1 & 0 \\ -\varepsilon^2 - \varepsilon^4 & \varepsilon & 0 & 1 \end{pmatrix}$$

with $\varepsilon = e(2\pi i/5) = e^{2\pi i/5}$.

Note that

$$\varepsilon^5 = (e^{2\pi i/5})^5 = e^{2\pi i} = 1$$

from which

$$\varepsilon^5 - 1 = (\varepsilon - 1)(\varepsilon^4 + \varepsilon^3 + \varepsilon^2 + \varepsilon + 1) = 0 \, .$$

Since $\varepsilon - 1 \neq 0$ we have that $\varepsilon^4 + \varepsilon^3 + \varepsilon^2 + \varepsilon + 1 = 0$ from which $\varepsilon^2 = -\varepsilon^4 - \varepsilon^3 - \varepsilon - 1$.

$$\begin{aligned} &\alpha(\lambda_1, \lambda_2) = -\varepsilon^4 - \varepsilon^3 - \varepsilon - 1 = \varepsilon^2 \, , && \alpha(\lambda_2, \lambda_3) = -\varepsilon \, , \\ &\alpha(\lambda_1, \lambda_3) = \varepsilon^2 + \varepsilon^4 \, , && \alpha(\lambda_2, \lambda_4) = -\varepsilon^2 - \varepsilon^4 \, , \\ &\alpha(\lambda_1, \lambda_4) = 1 - \varepsilon^4 = -(\varepsilon^2 + \varepsilon^4) + \varepsilon^2 + 1 \, , && \alpha(\lambda_3, \lambda_4) = 1 \, . \end{aligned}$$

If $1, \varepsilon, \varepsilon^2, \varepsilon^2 + \varepsilon^4$ are linearly independent over $\boldsymbol{Q}$ then $\operatorname{rk} \alpha = 4$.

We can consider the decomposition of α:

$$\alpha = \alpha_1 \cdot \underbrace{1}_{y_1} + \alpha_2 \cdot \underbrace{\varepsilon}_{y_2} + \alpha_3 \cdot \underbrace{\varepsilon^2}_{y_3} + \alpha_4 \cdot \underbrace{(\varepsilon^2 + \varepsilon^4)}_{y_4} .$$

To obtain the equations of $E(\alpha)$ we write

$$\begin{aligned} \alpha(u, v) = {} & \alpha(n_1\lambda_1 + n_2\lambda_2 + n_3\lambda_3 + n_4\lambda_4, m_1\lambda_1 + m_2\lambda_2 + m_3\lambda_3 + m_4\lambda_4) = \\ & (n_1 m_2 - n_2 m_1) \underbrace{\alpha(\lambda_1, \lambda_2)}_{y_3} + (n_1 m_3 - n_3 m_1) \underbrace{\alpha(\lambda_1, \lambda_3)}_{y_4} + \\ & (n_1 m_4 - n_4 m_1) \underbrace{\alpha(\lambda_1, \lambda_4)}_{y_1 + y_3 - y_4} + (n_2 m_3 - n_3 m_2) \underbrace{\alpha(\lambda_2, \lambda_3)}_{-y_2} + \\ & (n_2 m_4 - n_4 m_2) \underbrace{\alpha(\lambda_2, \lambda_4)}_{-y_4} + (n_3 m_4 - n_4 m_3) \underbrace{\alpha(\lambda_3, \lambda_4)}_{y_1} \end{aligned}$$

from which

$$\begin{aligned} \alpha(u, v) = {} & (n_1 m_4 - n_4 m_1 + n_3 m_4 - n_4 m_3)\, y_1 + \\ & (-n_2 m_3 + n_3 m_2)\, y_2 + (n_1 m_2 - n_2 m_1 + n_1 m_4 - n_4 m_1)\, y_3 + \\ & (n_1 m_3 - n_3 m_1 - n_1 m_4 + n_4 m_1 - n_2 m_4 + n_4 m_2)\, y_4 = \\ & (p_{14} + p_{34}) y_1 + (-p_{23}) y_2 + (p_{12} + p_{14}) y_3 + (p_{13} - p_{14} - p_{24}) y_4 \, . \end{aligned}$$

$Q \cap E(\alpha)$ has equations:

$$\begin{cases} x_{14} = -x_{34} , \\ x_{23} = 0 , \\ x_{12} = -x_{14} , \\ x_{13} = x_{14} + x_{24} , \\ x_{12}x_{34} - x_{13}x_{24} + x_{14}x_{23} = 0 , \end{cases}$$

from which $x_{14}^2 - x_{14}x_{24} - x_{24}^2 = 0$ which is a quadric in $\boldsymbol{P}^1$.

If we call $x_{14} = x$, $x_{24} = y$ and $t = y/x$ we find the equation $-t^2 - t + 1 = 0$ with coefficients over $\boldsymbol{Q}$ which doesn't have roots in $\boldsymbol{Q} \Rightarrow$ the quadric $Q \cap E(\alpha)$ doesn't have rational points $\Rightarrow \alpha$ is not hyperbolic and α is not hyperbolic over $\boldsymbol{Q} \Rightarrow X$ is not isomorphic to a product of elliptic curves and X is not isogenous to a product of elliptic curves, but X is a simple abelian surface.

REFERENCES

[B] B. Baumslag - B. Chandler, *Teoria dei gruppi*, Collana Schaum (1983).

[Bo] O. Bolza, *On binary sextics with linear transformations onto themselves*, Am. J. Math., **10** (1888), 47-70.

[G] Ph. Griffiths - J. Harris, *Principles of Algebraic Geometry*, John Wiley & Sons (1978).

[H] J. Harris, *Algebraic Geometry, a first course*, Springer-Verlag (1992).

[K] G. R. Kempf, *Complex Abelian Varieties and Theta Functions*, Springer-Verlag (1991).

[LB] H. Lange - Birkenhake C., *Complex Abelian Varieties*, Springer-Verlag (1992).

[M] J. Munkres, *Elements of Algebraic Topology*, The Benjiamin Cumming Publishing Company (1984).

[R] W. Ruppert, *When is an abelian surface isomorphic or isogeneous to a product of elliptic curves?*, Math. Zeit., **203** (1990), 293-299.

[S] C. Schoen, *Produkte Abelscher Varietäten und Moduln über Ordnungen*, J. Reine Angew. Math., **429** (1992), 115-123.

[Sh] T. Shioda - N. Mitani, *Singular abelian surfaces and binary quadratic forms*, in *Classification of Algebraic Varieties and Compact Complex Manifolds*, Lecture Notes in Math., vol. 412, 255-287, Springer-Verlag (1974).

Dipartimento di Matematica, Università degli Studi di Torino
Via Carlo Alberto, 10 - 10123 Torino, Italia

email: marchisio@dm.unito.it

Pervenuta in Redazione
il 20 marzo 1997