Mathematisch Instituut
Roetersstraat 15
Amsterdam The Netherlands

# SIMPLE ABELIAN VARIETIES HAVING A PRESCRIBED FORMAL ISOGENY TYPE

by

H.W. Lenstra Jr. and F. Oort

Report 73-02

Received May 17, 1973

May 1973

# Simple abelian varieties having a prescribed formal isogeny type.

Hendrik W. Lenstra jr. and Frans Oort.

## 1. Introduction.

In general a splitting of the isogeny type of the formal group of an abelian variety should not give an analogous splitting of the isogeny type of the abelian variety. Honda gave an example of an abelian surface (in characteristic p) where the formal group up to isogeny splits into two different factors, but such that the abelian variety is simple (cf. [3], page 93). However Manin asked whether it could be possible that the isogeny class of any abelian surface with no points of order $p$ (the analogue of supersingular elliptic curves) is split (cf. [4], page 79, line 16 from below). Surprisingly the question by Manin has a positive answer in any dimension: a "supersingular" abelian variety is isogenous to a product of elliptic curves (cf. [5], theorem 3.2). However this is the only exception to the general principle alluded above: in this paper we prove that for any formal isogeny type which has at least one factor different from $G_{1,1}$ (the condition $t > 0$ in section 2 below), there exists a simple abelian variety having this isogeny type for its formal group.
Using the classification, due to Honda and Serre, of isogeny classes of abelian varieties over finite fields with the help of Weil numbers, in fact a proof of this is nothing but an excercise in algebraic number theory.
Notations: We fix a prime number $p$. For an abelian variety $A$ we denote by $\hat{A}$ its formal group, and we freely use the classification of such formal groups over an algebraically closed field of characteristic $p$ as given by Manin (cf. [4], II.4.). We use $\sim$ to indicate the isogeny relation. By $\Omega$ we denote an algebraic closure of the prime field in characteristic $p$; by $\mathbb{F}_q$ we denote the field having $q$ elements.

## 2. The construction of a simple abelian variety.

Let $(n_i)_{i=1}^t$, $(m_i)_{i=1}^t$ be two sequences of integers such that

$$t > 0$$
$$n_i > m_i \geq 0 \quad \text{for} \quad 1 \leq i \leq t$$
$$(n_i, m_i) = 1 \quad \text{for} \quad 1 \leq i \leq t \quad (\text{so } n_i = 1 \text{ if } m_i = 0),$$

and let $h$ be a nonnegative integer.

We want to construct a simple abelian variety $A$ over $\Omega$ such that

$$\hat{A} \sim \Big(\bigoplus_{\substack{i=1 \\ m_i=0}}^{t} G_{1,0}\Big) + \Big(\bigoplus_{\substack{i=1 \\ m_i>0}}^{t} (G_{n_i,m_i} + G_{m_i,n_i})\Big) + h \cdot G_{1,1}.$$

Put

$$g = \sum_{i=1}^{t} (n_i + m_i) + h.$$

In section 3 we shall construct two field extensions $\mathbb{Q} \subset K \subset L$ such that:

(2.1) $[K : \mathbb{Q}] = g$;

(2.2) $K$ is totally real;

(2.3) there are no intermediate fields $\mathbb{Q} \subsetneq K' \subsetneq K$;

(2.4) the prime ideal factorization of $p$ in $K$ is

$$(p) = \Big(\prod_{i=1}^{t} \underline{p}_i^{n_i+m_i}\Big) \cdot \Big(\prod_{j=1}^{h} \underline{q}_j\Big),$$

where $\underline{p}_i$, $\underline{q}_j$ are different prime ideals in the ring of integers in $K$, and all residue class degrees $f(\underline{p}_i/(p))$ and $f(\underline{q}_j/(p))$ are 1;

(2.5) $[L : K] = 2$; let the nontrivial $K$-automorphism of $L$ be denoted by $\rho$;

(2.6) $L$ is totally imaginary (i.e. there is no field homomorphism $L \to \mathbb{R}$);

(2.7) either $g = 1$, in which case $t = 1$, $n_1 = 1$, $m_1 = 0$, $h = 0$ and $K = \mathbb{Q}$, or $K \neq \mathbb{Q}$, and then there is no $r \in \mathbb{Q}$ for which $L = K(\sqrt{r})$;

(2.8) the primes $\underline{p}_i$ $(1 \leq i \leq t)$ split completely in $L$:

$$\underline{p}_i = \underline{r}_i \cdot \rho(\underline{r}_i), \quad \underline{r}_i \neq \rho(\underline{r}_i),$$

and the $\underline{q}_j$ $(1 \leq j \leq h)$ ramify:

$$\underline{q}_j = \underline{s}_j^2, \qquad \underline{s}_j = \rho(\underline{s}_j).$$

By (2.2) and (2.5), (2.6), $L$ is a CM-field [3]. Let the ideal $\underline{a}$ in $L$ be defined by

$$\underline{a} = \Big(\prod_{i=1}^{t} (\underline{r}_i^{n_i} \cdot \rho(\underline{r}_i)^{m_i})\Big) \cdot \prod_{j=1}^{h} \underline{s}_j.$$

Then we have

$$\underline{a} \cdot \rho(\underline{a}) = (p),$$

so $\underline{a}$ is an "ideal of type $(A_o)$ of order 1" (terminology from [3]).

(2.9) Lemma.

Let $\nu > 0$ be an integer, and suppose $\pi \in L$ is an algebraic integer for which

$$\pi \cdot \rho(\pi) = p^{\nu}, \quad (\pi) = \underline{a}^{\nu}.$$

Then $L = \mathbb{Q}(\pi)$.

Proof of (2.9). We first show

(2.10) $\pi \notin K$.

In fact, $\pi \in K$ would imply $\pi^2 = \pi.\rho(\pi) = p^\nu$, so $\underline{a}^{2\nu} = (\pi^2) = (p)^\nu$, which means

$$\prod_{i=1}^{t} (\underline{r}_i^{2\nu n_i} \cdot \rho(\underline{r}_i)^{2\nu m_i}) \cdot \prod_{j=1}^{h} \underline{s}_j^{2\nu} = \prod_{i=1}^{t} (\underline{r}_i^{\nu(n_i+m_i)} \cdot \rho(\underline{r}_i)^{\nu(n_i+m_i)}) \cdot \prod_{j=1}^{h} \underline{s}_j^{2\nu}.$$

This contradicts unique factorization, since $t > 0$, $n_1 > m_1$, $\underline{r}_1 \neq \rho(\underline{r}_1)$, $\nu \neq 0$, so (2.10) is proved. It follows that

(2.11) $\quad L = K(\pi)$.

If $K = \mathbb{Q}$, we are done. So assume $K \neq \mathbb{Q}$. We assert

(2.12) $\quad \pi + \rho(\pi) \notin \mathbb{Q}$.

Otherwise we would have $\pi + \rho(\pi) \in \mathbb{Q}$ and $\pi.\rho(\pi) = p^\nu \in \mathbb{Q}$. But then $\pi$ is imaginary quadratic over $\mathbb{Q}$, so $\mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{r})$ for some $r \in \mathbb{Q}$. By (2.11) this implies $L = K(\sqrt{r})$, $r \in \mathbb{Q}$, contradicting (2.7).

This proves (2.12).

We do have $\pi + \rho(\pi) = \mathrm{Tr}_{L/K}(\pi) \in K$, so (2.12) and (2.3) yield $K = \mathbb{Q}(\pi + \rho(\pi))$. Using $\rho(\pi) = \frac{p^\nu}{\pi}$ we find

$$\mathbb{Q}(\pi) = \mathbb{Q}(\pi + \tfrac{p^\nu}{\pi})(\pi) = \mathbb{Q}(\pi + \rho(\pi))(\pi) = K(\pi) = L,$$

thus proving (2.9).

By lemma 1 of [3] there exists a $\nu \in \mathbb{Z}$, $\nu > 0$, and an algebraic integer $\pi \in L$ such that

$$\pi.\rho(\pi) = p^\nu, \quad (\pi) = \underline{a}^\nu.$$

Applying (2.9) to $\pi^\mu$ we find

(2.13) $\quad \mathbb{Q}(\pi^\mu) = L$ for every integer $\mu > 0$.

In the terminology of [3] this means

$$L = \mathbb{Q}(\underline{a}^\infty) = \mathbb{Q}(\pi^\infty).$$

Let $A$ be a simple abelian variety over $\mathbb{F}_{p^\nu}$ corresponding to $\pi$, by the main theorem of [3]. We show that $A$ satisfies our requirements. As in [6], we put

$$\mathrm{End}_{M(\mathbb{F}_{p^\nu})}(A) = \mathbb{Q} \otimes \mathrm{End}_{\mathbb{F}_{p^\nu}}(A).$$

We identify $\pi$ with the Frobenius endomorphism $\pi_A \in \mathrm{End}_{M(\mathbb{F}_{p^\nu})}(A)$.

(2.14) Lemma.

$$\mathrm{End}_{M(\mathbb{F}_{p^\nu})}(A) = \mathbb{Q}(\pi).$$

Proof of (2.14). $E = \mathrm{End}_{M(\mathbb{F}_{p^\nu})}(A)$ is a division algebra with center $\mathbb{Q}(\pi) = L$. To show $E = L$ it suffices to check that $E$ splits locally everywhere. This is done with the help of théorème 1 of [6]:

(a) by (2.6), $L$ does not have real places;

(b) $E$ splits automatically at finite places $v$ not lying over $p$;

(c) let $v$ lie over $p$. If $v$ corresponds to $\underline{r}_i$, then

$$\mathrm{inv}_v(E) \equiv \frac{v(\pi)}{v(p^\nu)} \cdot [L_v : \mathbb{Q}_p] = \frac{n_i \cdot \nu}{(n_i+m_i)\cdot\nu} \cdot (n_i+m_i) = n_i \equiv 0 \mod 1.$$

Similarly, for $\rho(\underline{r}_i)$ we get

$$\mathrm{inv}_v(E) \equiv m_i \equiv 0 \mod 1.$$

If $v$ belongs to $\underline{s}_j$, then

$$\mathrm{inv}_v(E) \equiv \frac{v(\pi)}{v(p^\nu)} \cdot [L_v : \mathbb{Q}_p] = \frac{\nu}{2\cdot\nu} \cdot 2 = 1 \equiv 0 \mod 1.$$

This proves (2.14).

From (2.14) it follows that the characteristic polynomial of the Frobenius endomorphism is equal to the irreducible polynomial of $\pi$ over $\mathbb{Q}$. Since we know all p-adic values of $\pi$, we can apply theorem (4.1) of [4] to compute $\hat{A}$. We find

$$\hat{A} \sim \Big(\bigoplus_{\substack{i=1\\ m_i=0}}^{t} G_{1,0}\Big) + \Big(\bigoplus_{\substack{i=1\\ m_i>0}}^{t} (G_{n_i,m_i} + G_{m_i,n_i})\Big) + h.G_{1,1},$$

as desired.

Let $\mu$ be a positive integer. The degree of the characteristic polynomial of $\pi_A^\mu$ is equal to

$$2.\dim A = [E : L]^{\frac{1}{2}} \cdot [L : \mathbb{Q}] = [L : \mathbb{Q}] = 2g.$$

By (2.13) it follows that this polynomial is irreducible over $\mathbb{Q}$. Hence $A$ remains simple over $\mathbb{F}_{p^{\nu\mu}}$, for every $\mu$. We conclude that $A$ remains simple over $\Omega$, as required.

## 3. The construction of the desired CM-field.

For a field $F$, let $\mathrm{Mon}(g, F)$ denote the set of monic polynomials of degree $g$ over $F$. If $F$ is a topological field, $\mathrm{Mon}(g, F)$ has a natural topology such that $\mathrm{Mon}(g, F) \cong F^g$ as topological spaces.

Suppose $f \in \mathrm{Mon}(g, \mathbb{Q})$ satisfies

(3.1) $f$ has $g$ real zeros;

(3.2) the Galois group of the splitting field $M$ of $f$ over $\mathbb{Q}$ is isomorphic to the full permutation group $S_g$ of order $g!$;

(3.3) $\mathbb{Q}_p[X]/f\,\mathbb{Q}_p[X] \cong \Big(\coprod_{i=1}^{t} \mathbb{Q}_p(p^{\frac{1}{2}(n_i+m_i)})\Big) \times \mathbb{Q}_p{}^h$.

Then $K = \mathbb{Q}[X]/f\,\mathbb{Q}[X]$ is a field (by (3.2)) which obviously satisfies (2.1), (2.2) and (2.4). We assert that also (2.3) holds. In fact, the intermediate field $\mathbb{Q} \subset K \subset M$ corresponds to the subgroup $S_g \supset S_{g-1} \supset \{1\}$. Since there are no subgroups $S_g \supsetneq H \supsetneq S_{g-1}$, (2.3) follows by Galois theory.

Let $p_1$, $p_2$, $p_3$ be three rational primes, different from $p$. Choose monic polynomials $f_1$, $f_2$, $f_3 \in \mathbb{Z}[X]$ of degree $g$ such that :

(3.4) $(f_1 \bmod p_1)$ is irreducible over $\mathbb{F}_{p_1}$ ;

(3.5) if $g > 2$, then $(f_2 \bmod p_2) \in \mathbb{F}_{p_2}[X]$ is the product of a linear factor and an irreducible factor of degree $g - 1$;

(3.6) if $g > 3$, then $f_3 \in \mathbb{F}_{p_3}[X]$ is the product of an irreducible quadratic factor and one or two different irreducible factors of odd degree.

By [7, §66], condition (3.2) is satisfied if for $i = 1, 2, 3$ we have:

$(3.7)_i$ the coefficients of $f$ are integers at $p_i$, and $f \equiv f_i \bmod p_i$.

So to construct $K$, it suffices to show that conditions (3.1), (3.3), $(3.7)_{1,2,3}$ can be satisfied simultaneously.

Each one of the sets

$$U_{-1} = \{f \in \mathrm{Mon}(g, \mathbb{R}) \mid (3.1) \text{ holds}\},$$
$$U_0 = \{f \in \mathrm{Mon}(g, \mathbb{Q}_p) \mid (3.3) \text{ holds}\},$$
$$U_i = \{f \in \mathrm{Mon}(g, \mathbb{Q}_{p_i}) \mid (3.7)_i \text{ holds}\} \quad (i = 1, 2, 3)$$

is nonempty and open (cf. [1, ch. 2, §6] for $U_0$). By the approximation theorem [1, ch. 1, §4], $\mathrm{Mon}(g, \mathbb{Q})$ is dense in

$$\mathrm{Mon}(g, \mathbb{R}) \times \mathrm{Mon}(g, \mathbb{Q}_p) \times \prod_{i=1}^{3} \mathrm{Mon}(g, \mathbb{Q}_{p_i})$$

under the natural inclusion. Hence there exists a polynomial

$$f \in \mathrm{Mon}(g, \mathbb{Q}) \cap \prod_{i=-1}^{3} U_i.$$

Therefore, a field $K$ satisfying (2.1) - (2.4) exists.

Next we construct $L$. If $K \neq \mathbb{Q}$, let $\underline{\ell}_1$, $\underline{\ell}_2$ be different primes of $K$ lying over the same rational prime $\ell$, $\ell \neq p$. Such $\ell$ and $\underline{\ell}_i$ exist, cf. [2]. Let $v_{\underline{p}}$ denote the normalized exponential valuation at the prime $\underline{p}$. By the approximation theorem, there exists an $a \in K$ such that:

(3.8) if $K \neq \mathbb{Q}$, then $v_{\underline{\ell}_1}(a) \not\equiv v_{\underline{\ell}_2}(a) \bmod 2$;

(3.9) $v_{\underline{q}_j}(a) = 1 \quad (1 \leq j \leq h)$;

(3.10) $a$ is a square in each of the local fields $K_{\underline{p}_i}$, $1 \leq i \leq t$;

(3.11) $\sigma(a) < 0$ for every field homomorphism $\sigma : K \to \mathbb{R}$.

From (3.8) we see $a \notin \mathbb{Q} \cdot K^2$ if $K \neq \mathbb{Q}$. Therefore $L = K(\sqrt{a})$ satisfies (2.5) and (2.7). Also (2.6) and (2.8) hold, by (3.11) and (3.9), (3.10). This finishes the construction of $L$ and $K$.

References.

1. E. Artin, Algebraic numbers and algebraic functions, Gordon & Breach, New York 1967.

2. A. Dress, Zu einem Satz aus der Theorie der algebraischen Zahlen, Journal reine angew. Math., 216 (1964) 218 - 219.

3. T. Honda, Isogeny classes of abelian varieties over finite fields, Journal Math. Soc. Japan, 20 (1968) 83 - 95.

4. Yu. I. Manin, The theory of commutative formal groups over fields of finite characteristic, Russian Math. Surveys, 18 , 6 (1963) 1- 83.

5. F. Oort, Subvarieties of moduli spaces, to appear (Aarhus Preprint Series, 1972/73, no 44).

6. J. Tate, Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda), Sém. Bourbaki 21 (1968/69) no. 352 , pp. 95 - 110, Lecture Notes in Math. 179, Springer, Berlin etc., 1971.

7. B.L. van der Waerden, Algebra, Erster Teil, Springer, Berlin etc., 1966[7].