Hypersymmetric abelian varieties

Ching-Li Chai[1] & Frans Oort

last version, 15-II-2008

Dedicated to John Coates,
for his 60th birthday.

Abstract We introduce the notion of a *hypersymmetric abelian variety* over a field of positive characteristic p. We show that every symmetric Newton polygon admits a hypersymmetric abelian variety having that Newton polygon; see 2.5 and 4.8. Isogeny classes of absolutely simple hypersymmetric abelian varieties are classified in terms of their endomorphism algebras and Newton polygons. We also discuss connections with abelian varieties of PEL-type, i.e. abelian varieties with extra symmetries, especially abelian varieties with real multiplications.

Introduction

The notion of a *hypersymmetric abelian variety* over a field of positive characteristic p is an analog of the notion of an abelian variety of CM-type over a field of characteristic zero. Recall that an abelian variety A over an algebraically closed field of dimension g is said to admit *sufficiently many complex multiplications*, abbreviated smCM, also called "of CM-type", if its endomorphism algebra $\mathrm{End}^0(A) := \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ contains a semi-simple commutative algebra of rank $2g$ over $\mathbb{Q}$; see [19], pp. 43/44; [4], page 63; [13], page 347; [10], I.3; see [16] and [17] for further properties and references. In a moduli space of abelian varieties of PEL-type over a base field of characteristic zero, those points whose underlying abelian varieties have smCM are often called "CM points", or "special points"; they are of fundamental importance to arithmetic.

Although the notion of abelian varieties with smCM still makes sense over a base field of positive characteristic p, they are "too abundant" in characteristic p: Tate showed that every abelian variety over $\mathbb{F} := \overline{\mathbb{F}_p}$ has smCM. In other words, in a moduli space of polarized abelian varieties over an algebraically closed field $K \supseteq \mathbb{F}_p$, a point is a CM-point if it is rational over $\mathbb{F}$; having smCM does not make an abelian variety over characteristic p "special enough".

If we require that an abelian variety A over a field $K \supseteq \mathbb{F}_p$ has "as many endomorphisms as allowed by the slope constraint", then we obtain a class of abelian varieties which are indeed "special". We call them "*hypersymmetric abelian varieties*"; see Definition 2.1 for a precise definition. An example of a hypersymmetric abelian variety is a g-fold product of an ordinary elliptic curve over $\overline{\mathbb{F}_p}$ with itself; the Hecke orbit of such a point in the Siegel modular variety $\mathcal{A}_g$ is easily seen to be dense in $\mathcal{A}_g$, c.f. Larsen's example on p. 443 of [1].

The notion of hypersymmetric abelian varieties was motivated by the Hecke orbit problem over a field of positive characteristic p. As will be shown in [3], the Zariski closure of a prime-to-p Hecke orbit of a point x_0 in the Siegel modular variety is dense in the irreducible component of the *central leaf* $\mathcal{C}(x_0)$ passing through x_0; see [18] for the notion of a central

[1]Partially supported by a grant DMS04-00482 from the National Science Foundation

leaf, and [2] for a survey of the Hecke orbit problem. Hypersymmetric points are useful for proving the irreducibility of central leaves and for computing the naive p-adic monodromy of central leaves; see 10.4 and 14.1 of [2].

The major theme of this article is the existence problem of a hypersymmetric abelian variety with a prescribed Newton polygon and/or ring of endomorphisms. We show that for any given symmetric Newton polygon ξ, there exists a hypersymmetric abelian variety with Newton polygon ξ; see 4.8. Furthermore, we give a necessary and sufficient condition for the existence of a *simple* hypersymmetric abelian variety over $\overline{\mathbb{F}_p}$ with a given symmetric Newton polygon; see Theorems 4.7, 3.3, see 3.6 and see Prop. 4.1. The same method also gives a partial converse to the Honda-Tate theorem. In Section 6 we give a necessary and sufficient condition for the existence of hypersymmetric abelian varieties on a given Newton polygon stratum in a Hilbert modular variety.

In Section 7 we explore the possibility of a characteristic-p version of the André-Oort conjecture, replacing CM-points in characteristic zero by hypersymmetric points in characteristic p. We show that the naive analog is false: there are subvarieties in the moduli space of abelian varieties, which are not Shimura subvarieties but have a dense set of hypersymmetric points. This phenomenon reflects the fact that there exist modular varieties of PEL-type in characteristic p such that every rational point over $\overline{\mathbb{F}_p}$ is a hypersymmetric point. Whether this is "the only reason" for the naive analog of the André-Oort conjecture to be false is an open question; a precise formulation of this question is given at the end of Section 7.

The authors would like to thank the referee for a very careful reading.

§1. Notation

(1.1) Let p be a prime number, fixed in this article. All abelian varieties and p-divisible groups are defined over a field of characteristic p. We write $\mathbb{F} = \overline{\mathbb{F}_p}$ for an algebraic closure of $\mathbb{F}_p$. For an abelian variety A we write $X = A[p^\infty]$ for its p-divisible group.

(1.2) Newton polygons with slopes between 0 and 1 will be denoted by a symbol like ζ or ξ. When we write $\zeta = \sum_i (m_i, n_i)$ we intend to say that the (lower convex) Newton polygon starting from the origin of the plane, such that the multiplicity of a slope ν is equal to $\sum (m_i + n_i)$, summation taken over i such that $m_i/(m_i + n_i) = \nu$. In the notation above, it is understood that $m_i, n_i \in \mathbb{Z}_{\geq 0}$ and $\gcd(m_i, n_i) = 1$ for all i.

A Newton polygon ξ is said to be *symmetric* if the multiplicity of ν in is equal to the multiplicity of $1 - \nu$ for every slope ν that appears in ξ. We say that two Newton polygons are *disjoint* if they have no slopes in common. Every symmetric Newton polygon ξ can be written as a sum of disjoint symmetric Newton polygons, each having at most two slopes.

Every symmetric Newton polygon ξ can be written in a unique way in the following *standard form*

$$\rho_0\,(1,1) + \sum_{i=1}^{s} \rho_i\,((m_i, n_i) + (n_i, m_i)), \quad \gcd(m_i, n_i) = 1 \quad \forall i,$$

where $\rho_0, \rho_1, \ldots, \rho_s \in \mathbb{Z}_{\geq 0}$, and $m_i > n_i \geq 0$ for $i = 1, \ldots, s$, and $(m_i, n_i) \neq (m_j, n_j)$ if

$1 \leq i \neq j \leq s$. The coefficients $\rho_0, \rho_1, \ldots, \rho_s$ are called the *multiplicities of the simple parts* of ξ. Define $g(\xi) = \rho_0 + \sum_{1 \leq i \leq s} \ \rho_i{\cdot}(m_i + n_i)$.

(1.3) According to the Dieudonné-Manin classification of p-divisible groups over an algebraically closed field, see [12], page 35, every p-divisible group X over an algebraically closed field $k \supset \mathbb{F}_p$ is isogenous to a direct product of isoclinic p-divisible groups $G_{m,n}$, with $m, n \in \mathbb{Z}_{\geq 0}$ and $\gcd(m, n) = 1$, with $\dim(G_{m,n}) = m$; in this case $G_{m,n}$ has height $m + n$ and is isoclinic of slope $m/(m + n)$. The Newton polygon of a p-divisible group X isogenous to $\prod_i G_{m_i,n_i}$ is

$$\sum_i (m_i, n_i) =: \mathcal{N}(X)\,.$$

For an abelian variety A over a field $K \supset \mathbb{F}_p$, the Newton polygon attached to $A[p^\infty]$ is a symmetric Newton polygon $\mathcal{N}(A)$, and it can be written in standard form as above. Then we have $\dim(A) = g(\xi)$. We hope there will be no confusion caused by the formal sum expressing ξ and the summation as in the formula for g.

(1.4) Let A be an abelian variety over a field K. An isogeny

$$A \quad \sim \quad \sum_{1 \leq i \leq r} \ A_i^{\mu_i},$$

is called a *primary isogeny decomposition* of A if:

- $\mu_i \in \mathbb{Z}_{>0}$;
- for every $1 \leq i \leq r$ the abelian variety A_i is simple;
- for $1 \leq i < j \leq r$ the abelian varieties A_i and A_j are non-isogenous.

The Poincaré-Weil theorem says that every abelian variety over a field admits a primary isogeny decomposition over this field. Here we shall use this over an algebraically closed field.

(1.5) As Tate proved, see [20], an abelian variety defined over a finite field admits smCM. If an abelian variety over field $K \supset \mathbb{F}_p$ admits smCM, than over $\overline{K} = k$ this abelian variety is isogenous with an abelian variety defined over a finite field, as was proved by Grothendieck, see [16]. These results will be used without further mention.

§2. Hypersymmetric abelian varieties

(2.1) Definition. Let B be an abelian variety over a field $K \supset \mathbb{F}_p$. We say that B is *hypersymmetric* if the natural map

$$\mathrm{End}\left(B \times_{\mathrm{Spec}(K)} \mathrm{Spec}(\overline{K})\right) \otimes_{\mathbb{Z}} \mathbb{Z}_p \quad \xrightarrow{\sim} \quad \mathrm{End}\left(B[p^\infty] \times_{\mathrm{Spec}(K)} \mathrm{Spec}(\overline{K})\right)$$

is an isomorphism. If confusion might arise we will say “K-hypersymmetric”.

Using the result of Grothendieck in [16] we see that 2.1 is equivalent with:

(2.2) Definition. Let B be an abelian variety over a field $K \supset \mathbb{F}_p$; we say that B is *hypersymmetric* if there exist an abelian variety A defined over $\mathbb{F} := \overline{\mathbb{F}_p}$ and an isogeny

$$B \times_{\mathrm{Spec}(K)} \mathrm{Spec}(\overline{K}) \sim A \times_{\mathrm{Spec}(\overline{\mathbb{F}_p})} \mathrm{Spec}(\overline{K}),$$

such that the natural map

$$\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_p \quad \xrightarrow{\sim} \quad \mathrm{End}(A[p^\infty])$$

is an isomorphism.

(2.3) Remark. An abelian variety B over an algebraically closed field $k \supset \mathbb{F}_p$ is hypersymmetric if and only if

$$\mathrm{End}(B) \otimes_{\mathbb{Z}} \mathbb{Q}_p \xrightarrow{\sim} \mathrm{End}(B[p^\infty]) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

is an isomorphism. In particular, if an abelian variety B is isogenous to a hypersymmetric abelian variety A, then B is hypersymmetric.

(2.4) Remark. Tate proved that for an abelian variety A defined over a finite field $\mathbb{F}_q$, the natural homomorphism

$$\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_p \quad \xrightarrow{\sim} \quad \mathrm{End}(A[p^\infty])$$

is an isomorphism. This shows that $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is identified with the $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_q)$-invariant endomorphisms of $\mathrm{End}\left(A[p^\infty] \times_{\mathrm{Spec}(\mathbb{F}_q)} \mathrm{Spec}(\mathbb{F})\right)$. Suppose that

$$\mathrm{End}(A) \xrightarrow{\sim} \mathrm{End}\left(A \times_{\mathrm{Spec}(\mathbb{F}_q)} \mathrm{Spec}(\mathbb{F})\right),$$

then A is hypersymmetric if and only if every element of the ring of endomorphisms of the p-divisible group $A[p^\infty] \times_{\mathrm{Spec}(\mathbb{F}_q)} \mathrm{Spec}(\mathbb{F})$ is fixed by every element of $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_q)$. From this we see that there are "many" abelian varieties over a finite field which are not hypersymmetric. Also we see that for a hypersymmetric abelian variety this Galois action is "in diagonal form" for every isoclinic part of $A[p^\infty]$. This can be made precise as follows.

Let K be a finite field and let B be an abelian variety over K. Then B is hypersymmetric if and only if there exists a positive integer n such that the n-th power of the Frobenius π_B of B lies in the center of $\mathrm{End}^0\left(B[p^\infty] \times_{\mathrm{Spec}(K)} \mathrm{Spec}(\mathbb{F})\right)$. *In other words, any two eigenvalues of the action of π_B on the Dieudonné module of* $B[p^\infty] \times_{\mathrm{Spec}(K)} \mathrm{Spec}(\mathbb{F})$ *which have the same p-adic absolute value, differ by a root of unity.*

(2.5) Proposition. (i) *Every elliptic curve defined over a finite field is a hypersymmetric abelian variety.* (This handles the cases $\xi = (1,0) + (0,1)$ and $\xi = (1,1)$.)

(ii) *Suppose $\xi = (m,n) + (m,n)$ with coprime integers $m > n > 0$. Then there exists a hypersymmetric abelian variety with Newton polygon equal to ξ.*

(iii) *If A is hypersymmetric, and $\mu \in \mathbb{Z}_{>0}$ then A^μ is hypersymmetric.*

(iv) *Suppose A and B are hypersymmetric abelian varieties over an algebraically closed field $k \supset \mathbb{F}_p$ such that $\mathcal{N}(A)$ and $\mathcal{N}(B)$ have no slopes in common, i.e.* $\mathrm{Hom}(A[p^\infty], B[p^\infty]) = 0$*; then $A \times B$ is hypersymmetric.*

(v) *For every symmetric Newton polygon ξ and every prime number p, there exists a hypersymmetric abelian variety over $\overline{\mathbb{F}_p}$ whose Newton polygon is ξ.*

PROOF. For an ordinary elliptic curve E over a finite field we know that $\mathrm{End}^0(E)$ has rank two over $\mathbb{Q}$ (it is an imaginary quadratic extension of $\mathbb{Q}$); for a supersingular elliptic curve E over $\mathbb{F}$ we know that $\mathrm{End}^0(E)$ has rank four over $\mathbb{Q}$ (these facts follow from [20], but in this case this was already known to Deuring.) From these facts (i) follows.

By [21], page 98 (= page 352-4) "Un exemple spécial (Problème de Manin)" we see that (ii) holds.

The statements (iii) and (iv) are proved in a straight-forward way. Hence the statement (v) for an arbitrary symmetric Newton polygon follows. $\square$

§3. A classification up to isogeny

In this section we give a characterization of hypersymmetric simple abelian varieties.

(3.1) For a simple abelian variety A of dimension g over a field K we write

$$\mathbb{Q} \quad \subset \quad L := \mathrm{Centre}(D) \quad \subset \quad D := \mathrm{End}^0(A),$$

with

$$[D : L] =: d^2, \quad [L : \mathbb{Q}] =: e;$$

if A admits smCM then $ed = 2g$. In the case when $K = \mathbb{F}_q$ is a finite field and $\pi = \pi_A = \mathrm{Fr}_{A,q}$ is the geometric Frobenius endomorphism, we have $L = \mathbb{Q}(\pi_A)$. In the case when $K = \mathbb{F}$, there exists $r = p^i$ such that A is defined over $\mathbb{F}_r$ and $L = \mathbb{Q}(\pi_{A_{\mathbb{F}_r}})$, where $A_{\mathbb{F}_r}$ is an abelian variety over $\mathbb{F}_r$ such that $A \cong A_{\mathbb{F}_r} \times_{\mathrm{Spec}(\mathbb{F}_r)} \mathrm{Spec}(\mathbb{F})$.

(3.2) Lemma. *Let A be a simple abelian variety over a field K of characteristic p. Let $X := A[p^\infty]$ be the p-divisible group attached to A. Let $v_1, \cdots, v_t$ be the places of L above the rational prime $p \in \mathbb{Q}$. The decomposition $L \otimes_{\mathbb{Q}} \mathbb{Q}_p = L_{v_1} \times \cdots \times L_{v_t}$ induces a decomposition $X \sim \prod X_{v_i}$ of X up to isogeny.*

In case K is a finite field, $L = \mathbb{Q}(\pi_A)$, the decomposition $L \otimes_{\mathbb{Q}} \mathbb{Q}_p = L_{v_1} \times \cdots \times L_{v_t}$ induces a decomposition $X \sim \prod X_{v_i}$ of X up to isogeny; each of the factors X_{v_i} is isoclinic.

In case K is a finite field and A is a K-hypersymmetric, i.e. we assume $\mathrm{End}(A) \cong \mathrm{End}(A_{\overline{K}})$, *simple abelian variety over K, different factors X_{v_i} have different slopes,* i.e. the decomposition is the splitting into isoclinic factors up to isogeny. *Moreover, we have*

$$D_{v_i} \quad \xrightarrow{\sim} \quad \mathrm{End}^0(X_{v_i}),$$

and $L_v = \mathbb{Q}_p$ for every v dividing p, i.e. p splits completely in $L/\mathbb{Q}$.

Proof. We have $L \hookrightarrow \mathrm{End}^0(X)$. From this the splitting up to isogeny as in the first part of the lemma follows.

In case $K = \mathbb{F}_q$, we see that $\pi = \pi_A$ acts as a power of Frobenius; the value $v_i(\pi)$ determines the slope of the p-divisible group on which D_{v_i} acts non-trivially; we see that X_{v_i} is isoclinic of this slope.

In case A is hypersymmetric it follows that $D_{v_i} \xrightarrow{\sim} \mathrm{End}^0(X_{v_i})$. If the slopes of X_{v_i} and X_{v_j} with $i < j$ would be the same, we would see that $D_{v_i} \times D_{v_j}$ would operate in block form on the isoclinic $X_{v_i} \times X_{v_j}$; this would imply that $D \otimes \mathbb{Z}_p$ does not map surjectively on $\mathrm{End}(A[p^\infty])$, a contradiction with the fact that A is hypersymmetric; hence the X_{v_i} are the isoclinic parts. We see:

$$L_{v_i} = \mathrm{Centre}(D_{v_i}) \cong \mathrm{Centre}(\mathrm{End}^0(X_{v_i})) = \mathbb{Q}_p.$$

This finishes the proof of the lemma. □

(3.3) Theorem. *Let A be a simple abelian variety over $\mathbb{F}$. Then: a necessary and sufficient condition for A to be hypersymmetric is that p is totally split in $L/\mathbb{Q}$, and the slopes of X_{v_i} and X_{v_j} are different, for every pair of primes $v_i \neq v_j$ of $L/\mathbb{Q}$ both dividing p.*

Proof. By the previous lemma we know that the last two conditions are satisfied for a hypersymmetric simple abelian variety.

Suppose the last two conditions are satisfied. Let $v_1, \cdots, v_t$ be the primes in L above p; here $t = [L : \mathbb{Q}]$. Write $\mathcal{N}(X_i) = \rho_i{\cdot}(m_i, n_i)$ and $h_i = m_i + n_i$ for $1 \le i \le t$. Write $\rho_i{\cdot}h_i - d = \varepsilon_i$. As $[D : L] = [D_{v_i} : L_{v_i}] = d^2$ and $D_{v_i} \subset \mathrm{End}^0(X_{v_i})$ we have $\varepsilon_i \ge 0$ for every i. As A has smCM we have $2g = td$. Moreover we have $2g = \sum \rho_i h_i$. Hence

$$td = 2g = \sum \rho_i h_i = \sum (d + \varepsilon_i) = td + \sum \varepsilon_i.$$

This shows that $\varepsilon_i = 0$ for all i, and we have

$$\dim_{\mathbb{Q}_p}(D_{v_i}) = d^2 = \rho_i^2 h_i^2 = \dim_{\mathbb{Q}_p} \mathrm{End}^0(X_{v_i}) \qquad \forall i = 1, \ldots, s\,.$$

Hence $D_{v_i} \cong \mathrm{End}^0(X_{v_i})$ for all $i = 1, \ldots, s$, and $D \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \mathrm{End}^0(A[p^\infty])$. Therefore A is hypersymmetric. □

(3.4) Definition. We say that a symmetric Newton polygon is *balanced* if

$$\xi = \sum_{1 \le i \le s} \rho_i{\cdot}((m_i, n_i) + (n_i, m_i))$$

with $m_i > n_i \ge 0$ and $\gcd(m_i, n_i) = 1$ for all $i = 1, \ldots, s$, such that

- $(m_i, n_i) \neq (m_j, n_j)$ whenever $i \neq j$,
- there exists $d \in \mathbb{Z}_{>0}$ with $\rho_i{\cdot}(m_i + n_i) = d$ for all i, and
- $\gcd(\rho_1, \cdots, \rho_s) = 1$.

Equivalently, a symmetric Newton polygon ξ is balanced if

- it does not contain a slope equal to $1/2$,
- all slopes of ξ have the same multiplicity, and
- the greatest common divisor of the multiplicities of the simple parts of ξ is equal to 1.

(3.5) Lemma. *Suppose A is a simple, hypersymmetric abelian variety over $\mathbb{F}$ with Newton polygon $\mathcal{N}(A) = \xi$. Then one of the following cases holds:*

- *either $A = E$ is a supersingular elliptic curve, $\xi = (1, 1)$;*
- *or ξ is balanced.*

PROOF. In the case when A is not a supersingular elliptic curve, we have to show that $\mathcal{N}(A) = \xi$ is balanced. In this case $L \neq \mathbb{Q}$, see [21], case (a) on page 97. Hence $[L : \mathbb{Q}]$ is even. By Lemma 3.2 we see that $L_{v_i} = \mathbb{Q}_p$ for all i, and the number of mutually different slopes of $A[p^\infty]$ equals the number of places of L above p equals. This shows that the number of different slopes of $A[p^\infty]$, being equal to $[L : \mathbb{Q}]$, is even, and we conclude that the slope $1/2$ does not appear.

Notation: we write v_i for the place of L related with the slope $m_i/(m_i + n_i)$, and v_{2s-i} for the place of L related with the slope $n_i/(m_i + n_i)$.

For every $1 \leq i \leq 2s$ we have $D_{v_i} \xrightarrow{\sim} \mathrm{End}^0(X_{v_i})$. This proves $\rho_i^2 \cdot (m_i + n_i)^2 = [D : L] =: d^2$.

Let $\gcd(\rho_1, \cdots, \rho_s) = b$. Consider a simple p-divisible group Y having slope $m/(m + n)$; then $\mathrm{End}^0(Y)$ is a division algebra, central over $\mathbb{Q}_p$ with invariant equal to $m/(m+n)$. Hence the invariant of $\mathrm{End}^0(X_{v_i})$ equals $m_i/(m_i + n_i)$ and the invariant of $\mathrm{End}^0(X_{v_{2s+1-i}})$ equals $n_i/(m_i + n_i)$ for each $i \leq s$. This shows that for every prime v of L above p we have $(d/b)\cdot \mathrm{inv}_v(D) \in \mathbb{Z}$. As D is a central division algebra of dimension d^2 over L , this proves that $b = 1$. $\square$

(3.6) Conclusion. Let A be a hypersymmetric, non-supersingular abelian variety over $K = \mathbb{F}_q$, with $q = p^a$. Suppose A is absolutely simple and suppose all endomorphisms of $A_{\mathbb{F}}$ are already defined over K, i.e. $\mathrm{End}(A) = \mathrm{End}(A_{\mathbb{F}})$. Write $\mathcal{N}(A) = \xi$. Then:

(i) $\mathbb{Q}(\pi_A) = L := \mathrm{Centre}(\mathrm{End}^0(A))$.

(ii) $\xi := \mathcal{N}(A)$ is balanced.

(iii) The field L is a CM-field such that $[L : \mathbb{Q}] = 2s$, where s is the number of different slopes of $A[p^\infty]$. Moreover the rational prime p is completely split in $L/\mathbb{Q}$, i.e. $L \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \mathbb{Q}_p \times \cdots \times \mathbb{Q}_p = (\mathbb{Q}_p)^{2s}$ as $\mathbb{Q}_p$-algebras.

(iv) There is a natural bijection between the set of isoclinic parts of the Newton polygon ξ and the set of places of L above p, defined as follows. Suppose that v_i is a place of L above p, corresponding to an isoclinic part ξ_i of the Newton polygon ξ. Then $D \otimes_L L_{v_i}$ is a central simple algebra over $L_{v_i} \cong \mathbb{Q}_p$ with Brauer invariant $v_i(\pi)/v_i(q) = \nu_i$, the slope of the corresponding isoclinic part of ξ.

§4. Existence results for hypersymmetric abelian varieties

(4.1) Proposition. *For every balanced Newton polygon ξ, there exists an absolutely simple hypersymmetric abelian variety A defined over $\overline{\mathbb{F}}_p$ with $\mathcal{N}(A) = \xi$.*

(4.2) Lemma. *For every positive integer s, there exists a totally real number field E with $[E : \mathbb{Q}] = s$ such that $E \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \mathbb{Q}_p \times \cdots \times \mathbb{Q}_p$ as $\mathbb{Q}_p$-algebras.*

Proof. Immediate from Ekedahl's version [7] of Hilbert irreducibility theorem with weak approximation. □

(4.3) Remark. For every real number X, denote by $N_{s,p}(X)$ the number of isomorphism classes of totally real number fields E such that p is completely split in E over $\mathbb{Q}$, with $[E : \mathbb{Q}] = s$, $\mathrm{disc}(E) \leq X$, and the Galois group $\mathrm{Gal}(F/\mathbb{Q})$ of the Galois closure of E is isomorphic to the symmetric group S_s. Then one can show that

$$N_{s,p}(X) \gg X^{\frac{1}{2}+\frac{1}{s^2}}$$

by adapting the proof of [8, Theorem 1.1].

(4.4) Proposition. *Let E be a totally real number field, and let $w_1, \ldots, w_s$ be the places of E above p. Let $\nu_1, \ldots, \nu_s$ be rational numbers such that $0 \leq \nu_1, \ldots, \nu_s < \frac{1}{2}$. Then there exists a power q of p and an element $b \in \mathcal{O}_E$ such that*

(i) *$b \in \mathcal{O}_w^\times$ for every finite place w of E which is prime to p,*

(ii) *$\frac{w_i(b)}{w_i(q)} = \nu_i$, for $i = 1, \ldots, s$,*

(iii) *$|\iota(b)^2| < 4q$ for every embedding $\iota : E \hookrightarrow \mathbb{R}$ of E.*

Proof. In case $E = \mathbb{Q}$ this is an elementary statement, c.f. the "exemple spécial" on p. 98 of [20]. So we may assume that $[E : \mathbb{Q}] > 1$.

Choose an integer $d_0 > 0$ such that $d_0\nu_i \in \mathbb{N}$ for $i = 1, \cdots, s$. Let $e_i = e(E_{w_i}/\mathbb{Q}_p)$ be the absolute ramification index of E_{w_i}, and let $\mathfrak{p}_i$ be the prime ideal of $\mathcal{O}_E$ corresponding to w_i. Denote by I_0 the $\mathcal{O}_E$-ideal $\prod_{i=1}^s \mathfrak{p}_i^{d_0\nu_i e_i}$. Choose a positive integer d_1 such that $I_0^{d_1}$ is a principal $\mathcal{O}_E$-ideal. Pick an element $b_1 \in \mathcal{O}_E$ such that $I_0^{d_1} = b_1\mathcal{O}_E$. We want to show that there exists a positive integer n and a unit $u \in \mathcal{O}_E^\times$ such that the required properties (i), (ii), (iii) hold for $b = b_1^n\, u$ and $q = p^{d_0 d_1 n}$. It is clear that conditions (i), (ii) hold for every $n \in \mathbb{Z}_{>0}$ and every $u \in \mathcal{O}_E^\times$. So it suffices to show that there exists a constant n_0 such that for all integers $n \geq n_0$, there exists a unit $u \in \mathcal{O}_E^\times$ such that the required property (iii) holds for $b = b_1^n\, u$ and $q = p^{d_0 d_1 n}$.

Let $\iota_1, \ldots, \iota_h : E \hookrightarrow \mathbb{R}$ be the h embeddings of E in $\mathbb{R}$, and $h = [E : \mathbb{Q}]$. The condition $|\iota_j(b_1^n \cdot u)| < 2 \cdot p^{nd_0d_1/2}$ means that

$$\log|\iota_j(u)| < \log 2 - n\log|\iota_j(b_1)| + \frac{n}{2} \cdot d_0 d_1 \cdot \log|p|\,, \qquad j = 1, \ldots, h. \qquad (*)$$

Let V be the subspace of $\mathbb{R}^h$ consisting of all vectors $v \in \mathbb{R}^h$ such that the sum of the coordinates of v is equal to 0. Let $\beta : \mathcal{O}_E^\times \to V$ be the map such that for

$$\beta(u) = (\log|\iota_1(u)|, \ldots, \log|\iota_h(u)|)$$

$\beta(\mathcal{O}_E^\times)$ is a cocompact lattice in V by Dirichlet's unit theorem. Let

$$\Delta_n = \left\{ (x_1, \ldots, x_s) \in V \mid x_j < \log 2 - n \log|\iota_j(b_1)| + \frac{n}{2} \cdot d_0 d_1 \cdot \log p, \quad j = 1, \ldots, h \right\}$$

for $n \in \mathbb{Z}_{>0}$. By Minkowski's theorem, it suffices to show that the subset Δ_n is a non-empty convex subset of V for all $n > 0$, and the volume of Δ_n goes to infinity as $n \to \infty$.

We state an easy result on subsets of V defined by a system of linear inequalities such as $(*)$ The proof is omitted.

Sublemma. *Let $a_1, \ldots, a_h$ be real numbers such that $a_1 + \cdots + a_h > 0$. Then*

$$S = \{(x_1, \ldots, x_s) \in V \mid x_j < a_j \quad j = 1, \ldots, h\}$$

is a non-empty convex subset of V. Moreover, the volume of S with respect to the inner product on S induced by the standard inner product on $\mathbb{R}^h$ is equal to $\frac{\sqrt{h}}{(h-1)!}(a_1 + \ldots + a_h)^{h-1}$. □

Let $D_n = h \log 2 - n \sum_{j=1}^h \log|\iota_j(b_1)| + \frac{nh}{2} d_0 d_1 \cdot \log p$. By the product formula, we have

$$\sum_{j=1}^h \log|\iota_j(b_1)| = \sum_{i=1}^s d_0 d_1 \cdot \nu_i e_i f_i \cdot \log p\,,$$

where $f_i = [\kappa_{w_i} : \mathbb{F}_p]$ is the degree of the residue field of w_i over $\mathbb{F}_p$. Hence

$$D_n = h \log 2 + n \cdot d_0 d_1 \cdot \log p \cdot D_1\,,$$

where

$$D_1 = -\sum_{i=1}^s \nu_i e_i f_i + \frac{h}{2}\,.$$

Since $\sum_{i=1}^s e_i f_i = h$, and $\nu_i < \frac{1}{2}$ for $i = 1, \ldots, s$, we have $D_1 > 0$. By the Sublemma, Δ_n is non-empty for all $n > 0$, and the volume of Δ_n is

$$\frac{\sqrt{h}}{(h-1)!}(h \cdot \log 2 + n \cdot d_0 d_1 \cdot \log p \cdot D_1)^{h-1} \to \infty \quad \text{as} \quad n \to \infty\,.$$

This finishes the proof of Prop. 4.4. □

(4.5) Remark. (i) The assumption in Prop. 4.4 on the rational numbers ν_i's can be weakened to:

$$0 \le \nu_1, \ldots, \nu_s \le \frac{1}{2}, \quad \nu_1 + \cdots + \nu_s < \frac{s}{2}\,.$$

The proof works without change.

(ii) In addition to the weakening of the condition on the ν_i's above, the conclusion of Prop. 4.4 can be strengthened by adding the following requirement on b:

(iv) $\mathbb{Q}(b) = E$.

Again the same argument works, because Δ_n is a non-empty convex cone, while imposing the condition that $\mathbb{Q}(b) = E_1$ for a proper subfield E_1 of E corresponds to a closed subcone of $\Delta_{n,E_1} \subset \Delta_n$, which has volume zero. So for $n \gg 0$ there exists a unit $u \in \Delta_n$ whose image in V lies in Δ_n but not in Δ_{n,E_1} for every proper subfield E_1 of E.

Proof of Proposition 4.1. Let $\nu_1, \ldots, \nu_s, 1 - \nu_1, \ldots, 1 - \nu_s$ be the distinct slopes of the given balanced Newton polygon ξ with $\nu_i < \frac{1}{2}$ for $1 \leq i \leq s$. By Lemma 4.1, there exists a totally real number field E such that $[E : \mathbb{Q}] = s$ and $E \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \mathbb{Q}_p \times \cdots \times \mathbb{Q}_p$. Let $b \in \mathcal{O}_E$ and let q be a power of p satisfying the properties (i), (ii), (iii) in Prop. 4.4. Let α be a zero of the quadratic polynomial $X^2 + bX + q$. Then α is a q-Weil number, and Prop. 4.1 follows from the Honda-Tate theory. $\square$

(4.6) Lemma. *Let A be abelian variety over $\mathbb{F}$, and let $A \sim \sum_{1 \leq i \leq r} A_i^{\mu_i}$ be a primary isogeny decomposition. The abelian variety A is hypersymmetric if and only if:*

(a) *for every $1 \leq i \leq r$ the abelian variety A_i is hypersymmetric, and*

(b) *for every $1 \leq i < j \leq r$ the Newton polygons $\mathcal{N}(A_i)$ and $\mathcal{N}(A_j)$ are disjoint.*

Lemma 4.6 generalizes 2.5 (iv). The proof is straight forward. $\square$

We characterize isogeny classes of hypersymmetric abelian varieties. Previous results can be summarized in the following theorem.

(4.7) Theorem. (1) *Let A be hypersymmetric abelian variety over $\mathbb{F}$ and let*

$$A \sim \sum_{1 \leq i \leq r} A_i^{\mu_i}$$

be a primary isogeny decomposition. Then:

(a) *either A_i is a supersingular elliptic curve, or $\mathcal{N}(A_i)$ is balanced;*

(b) *for $j \neq j'$ the Newton polygons $\mathcal{N}(A_j)$ and $\mathcal{N}(A_{j'})$ are disjoint;*

(c) *if A_i is not supersingular, the center of $\mathrm{End}^0(A_i)$ equals $L_i = \mathbb{Q}(\pi_{A_i})$, with properties as in* 3.6.

(2) *Suppose given a symmetric Newton polygon ξ. Suppose $\xi = \sum \mu_j \xi^{(j)}$, where:*

(a) *every $\xi^{(j)}$ is either supersingular of height 2 or balanced, and*

(b) *for $j < j'$ the Newton polygons $\xi^{(j)}$ and $\xi^{(j')}$ are disjoint.*

Then there exists a hypersymmetric abelian variety over $\mathbb{F}$, with $\mathcal{N}(A) = \xi$, such that there exits a primary isogeny decomposition $A \sim \sum_j A_j^{\mu_j}$ of A with $\mathcal{N}(A_j) = \xi^{(j)}$.

(4.8) Corollary. *For every symmetric Newton polygon ξ and every prime number p there exists a hypersymmetric abelian variety A over $\mathbb{F}$ with $\mathcal{N}(A) = \xi$.*

(4.9) Proposition. *For every symmetric Newton polygon ξ which is not supersingular, there exist infinitely many isogeny classes of hypersymmetric abelian varieties over $\mathbb{F} = \overline{\mathbb{F}_p}$ with Newton polygon equal to ξ.*

There are many ways to prove this proposition. An abstract proof can be given along the lines of [11]. We give two proofs. The first proof is based on a concrete example. In the second proof we show directly the existence of a Weil number with prescribed slopes in a given imaginary quadratic field.

First Proof. It suffices to show this in case $\xi = (m,n) + (n,m)$ for coprime integers $m > n \geq 0$. Write $h = m+n$. Write $\varepsilon := h-2n$; note that $m > n$ hence $\varepsilon = h-2n = m+n-2n > 0$.

For every $b \in \mathbb{Z}_{>1}$ let π_b be a zero of the polynomial

$$f_b := T^2 + p^{2bn}(1-2p^{b\varepsilon})T + p^{2bh}, \quad \varepsilon := h-2n = m-n.$$

The discriminant of this polynomial is

$$D_b := (p^{2bn}(1-2p^{b\varepsilon})^2 - 4p^{2bh} = -p^{4bn}(4p^{b\varepsilon}-1) < 0.$$

Hence π_b is a p^{2bh}-Weil number. Let A_b be an abelian variety over $\mathbb{F}_{p^{2bh}}$ contained in the isogeny class defined by π_b. We see that the center of the ring $\mathrm{End}^0\Big(A_b \times_{\mathrm{Spec}(\mathbb{F}_{p^{2bh}})} \mathrm{Spec}(\mathbb{F})\Big)$ is equal to $\mathbb{Q}(\pi_b)$. We see that $\mathcal{N}(A_b) = (m,n) + (n,m)$.

Claim.

$$\#\big(\{\ell \mid \ell \text{ is a prime number and } \exists b \in \mathbb{Z}_{>0} \text{ such that } \ell \text{ divides } (4p^{b\varepsilon}-1)\}\big) = \infty.$$

Proof of the claim (we thank Frits Beukers for reminding us to use the S-unit equation). Let $S = \{\ell_1, \cdots, \ell_r\}$ be a finite set of rational primes. If $A = (a_1, \cdots, a_r) \in (\mathbb{Z})^r$ we write symbolically $L^A = \ell_1^{a_1} \times \cdots \times \ell_r^{a_r}$. We write $\mathbb{Z}_S := \{a/L^A \mid a \in \mathbb{Z},\ \ A = (a_1, \cdots, a_r)\}$. We see that its multiplicative group of units $(\mathbb{Z}_S)^* = \{\pm L^B/L^A\}$ is finitely generated. A conjecture by Julia Robinson, proved by a theorem of Siegel and Mahler, says:

$$\#\left(\{\lambda \mid \lambda \in (\mathbb{Z}_S)^*, \quad \lambda - 1 \in (\mathbb{Z}_S)^*\}\right) < \infty$$

is a *finite set*, see [9], Theorem 3.1 in 8.3 on page 194 (Note: the Siegel-Mahler finiteness theorem is much more general, but we only need this special case). Suppose the set S^0 of *all* primes dividing at least one of the numbers $4p^{b\varepsilon}-1$ with $b \in \mathbb{Z}_{>0}$ is finite, say $S^0 = \{\ell_3, \cdots, \ell_r\}$. Write $\ell_1 = 2$, $\ell_2 = p$, and $S = \{2, p, \ell_3, \cdots, \ell_r\}$; we see that $\lambda_b := 4p^{b\varepsilon} \in (\mathbb{Z}_S)^*$ and also $\lambda_b - 1 \in (\mathbb{Z}_S)^*$ for all $b \in \mathbb{Z}_{>0}$; this is a contradiction with the Siegel-Mahler finiteness theorem. This proves the claim.

We see that for infinitely many primes ℓ there exists $b \in \mathbb{Z}_{>0}$ such that ℓ ramifies in the number field $\mathbb{Q}(\pi_b)$. Hence the set $\{\mathbb{Q}(\pi_b) \mid b \in \mathbb{Z}_{>0}\}/\cong_{\mathbb{Q}}$ is an infinite set of isomorphism classes of quadratic fields. We conclude that the set

$$\{A_b \times_{\mathrm{Spec}(\mathbb{F}_{p^{2bh}})} \mathrm{Spec}(\mathbb{F}) \mid b \in \mathbb{Z}_{>1}\},$$

where A_b is an abelian variety over $\mathbb{F}_{p^{2bh}}$ contained in the isogeny class corresponding to π_b, gives an infinite number of $\mathbb{F}$-isogeny classes with Newton polygon equal to $(m,n)+(n,m)$.
$\square$

Second proof. It suffices to show that, for any imaginary quadratic field L such that p splits in L and any pair of coprime natural numbers $m > n \geq 0$, there exists a hypersymmetric abelian variety A over $\mathbb{F}_q$ for some power q of p such that $\mathcal{N}(A) = (m, n) + (n, m)$, and $\mathbb{Q}(\pi_{A,q}) = L$. By Honda-Tate, this is equivalent to showing the existence of an element $\pi \in \mathcal{O}_L[1/p]^\times$ such that $\frac{v(\pi)}{\bar{v}(\pi)} = \frac{n}{m}$, where v and $\bar{v}$ are the two normalized p-adic valuations of L above p; note that every element of $\mathcal{O}_K[1/p]^\times$ is a Weil number for a suitable power of p. Consider the map

$$\alpha : \mathcal{O}_K[1/p]^\times \longrightarrow \mathbb{Z}^2, \qquad \alpha(x) \mapsto (v(x), \bar{v}(x)) .$$

By Dirichlet's unit theorem, the image of α is a subgroup of finite index in $\mathbb{Z}^2$. Therefore there exists an element $\pi \in \mathcal{O}[1/p]^\times$ such that $\alpha(\pi) = (a, b) \neq (0, 0)$ such that $a/b = n/m$. $\square$

(4.10) Remark. The proof of Prop. 4.1 and the second proof of Prop. 4.9 are based on strategies which are somewhat different. In the proof of 4.1, one first constructs a suitable totally real number field with suitable properties using the Hilbert irreducibility theorem, then one writes down a quadratic polynomial with coefficients in the previously constructed totally real number field, which defines a Weil number having the required properties. This strategy was employed in [11]. In the second proof of 4.9, one finds a suitable Weil number in a given CM-field. In the next section we will combine the two methods to give a partial converse to the Honda-Tate theorem in [21].

§5. Construction of abelian varieties with given invariants

(5.1) In this section we indicate in which way (not necessarily hypersymmetric) abelian varieties over finite fields with prescribed invariants can be constructed. This generalizes the main result of [11] and can be considered a partial converse of the Honda-Tate theorem as in [21]; also see 2.27 and 4.14 of [15]. It is only a partial converse because we have no control of the finite field over which the abelian variety can be defined.

(5.2) Invariants. In Theorem 1 of [21] we see in which way a simple abelian variety A of $\dim(A) = g$ over a finite field $K = \mathbb{F}_q$ determines invariants:

$$A \mapsto (\xi, e, d, \{i_v\}) ,$$

where $\xi = \mathcal{N}(A)$, $e = [L : \mathbb{Q}]$ with $L = \mathrm{Centre}(D) = \mathrm{Centre}(\mathrm{End}^0(A))$, $d = \sqrt{[D : L]}$, and where Brauer invariants of the central division algebra $D = \mathrm{End}^0(A)$ over $\mathbb{Q}(\pi_A) = L$, at places of L above p are given by the i_v's, where v runs over all places of L above p, and $i_v \in \mathbb{Q}/\mathbb{Z}$ for each v. Notice that the Brauer invariants of D at all finite places of L outside p vanish, and L is a quadratic extension of a totally real number field unless L is totally real; in case L is totally real then A is supersingular and D is positive definite at all archimedean places of L. The invariants $(\xi, e, d, \{i_v\})$ are submitted to the following constraints:

$$de = 2g, \quad d = \mathrm{lcm}_v(\mathrm{denom}(i_v)), \quad i_v \equiv \frac{v(\pi_A)}{v(q)}[L_v : \mathbb{Q}_p] \pmod{\mathbb{Z}} ,$$

and the Newton polygon ξ has slopes $v(\pi_A)/v(q)$, with multiplicities $d\,[L_v : \mathbb{Q}_p]$, for all places v of L above p. Also note that from a q-Weil number $\pi = \pi_A$ one can reconstruct $\mathbb{Q} \subset L \subset D$

and the above invariants $(\xi, e, d, \{i_v\})$, and the isogeny class of A is determined by the q-Weil number π.

Remark. In the definition of the invariant of an endomorphism algebra of a p-divisible group, and hence in the definition of the invariants i_v used here, we follow [21]; this coincides with the definitions given in [5], see page 80; for a simple p-divisible group X of dimension d and of height h we define its (Frobenius-) slope as d/h, and the central $\mathbb{Q}_p$-algebra $\mathrm{End}^0(X)$ has invariant d/h; in [15], page 19, and in [6], page 227 the invariant defined there is the opposite in sign of the one considered here.

As a partial converse to Theorem 1 of [21] we have:

(5.3) Theorem. *Suppose a set of invariants $(\xi, e, d, \{i_v\})$ is given, submitted to the conditions stated above. Then there exists a simple abelian variety A over $\mathbb{F} = \overline{\mathbb{F}_p}$ which gives these invariants.*

Taking $d = 1$ we have the main result of [11].

In case A is supersingular, equivalently a power of π is real, this result is well known, see [21], page 97.

Convention. For an abelian variety we write its Newton polygon in standard form

$$\mathcal{N}(A) = \rho_0 \,(1,1) + \sum_{i=1}^{s} \rho_i \,((m_i, n_i) + (n_i, m_i))$$

with $\rho_0 \in \mathbb{Z}_{\geq 0}$, and $\rho_1, \ldots, \rho_s \in \mathbb{Z}_{>0}$, and $m_i > n_i \geq 0$ for $i = 1, \ldots, s$, and $m_i \neq m_j$ if $1 \leq i \neq j \leq s$.

In this section we suppose A to be non-supersingular. Equivalently: $s > 0$. For an abelian variety over a finite field K this means $\pi_A \notin \mathbb{R}$.

The following theorem is a more precise form of Theorem 5.3.

(5.4) Theorem. *Let $\xi = \rho_0 \cdot (1,1) + \sum_{i=1}^{s} \rho_i \cdot ((m_i, n_i) + (n_i, m_i))$ be a symmetric Newton polygon written in standard form. Suppose $s > 0$. Write $h_i = m_i + n_i$ for $i = 1, \ldots s$.*

Suppose given: integers $r_1, \ldots, r_s > 0$, and $d_{i,j} > 0$, where the index (i,j) runs through $1 \leq i \leq s$, $1 \leq j \leq r_i$.

If $\rho_0 > 0$, suppose also that we are given integers $r_0 > 0$, and $d_{0,1}, \ldots, d_{0,r_0} > 0$, and an integer t with $0 \leq t \leq r_0$. Write $d'_{0,j} = d_{0,j}$ for $1 \leq j \leq t$, and $d'_{0,j} = 2d_{0,j}$ for $t < j \leq r_0$. We use the convention that $r_0 = 0$ if $\rho_0 = 0$.

Let h' be the least common multiple of the natural numbers $h_i/\gcd(h_i, d_{ij})$, where the index runs through all $i = 1, \ldots, s$, all $j = 1, \ldots, r_i$. Let h be the least common multiple of h' and the natural numbers $2/\gcd(2, d'_{0j})$ for $1 \leq j \leq r_0$. In other words, $h = 2h'$ if $\rho_0 > 0$, h' is odd, and $d'_{0,j}$ is odd for some $j = 1, \ldots, r_0$; otherwise $h = h'$. Assume that

$$h \cdot \sum_{j=1}^{r_i} d_{ij} = \rho_i \cdot h_i \quad \textit{for} \quad i = 1, \ldots, r$$

and

$$h \cdot \sum_{j=1}^{r_0} d_{0j} = \rho_0 \,.$$

Then there exist

- *a simple abelian variety A over $\overline{\mathbb{F}}_p$,*
- *a totally imaginary quadratic extension L of a totally real number field E,*
- *an isomorphism from L to the center of the division algebra $D := \mathrm{End}(A)^0$,*
- *finite extension fields $E_{ij}/\mathbb{Q}_p$, $i = 1, \ldots, s$, $j = 1, \ldots, r_i$,*
- *finite extension fields $E_{0j}/\mathbb{Q}_p$, $j = 1, \ldots, r_0$, if $\rho_0 > 0$,*
- *quadratic extension fields $\tilde{E}_{0j}/E_{0j}$ if $\rho_0 > 0$ and $t < j \le r_0$,*
- *an isomorphism $E \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \prod_{i,j} E_{ij}$, where the indices (i,j) runs through all pairs such that $0 \le i \le s$, $1 \le j \le r_i$,*
- isomorphisms $(L/E) \otimes_E E_{0j} \cong \tilde{E}_{0j}/E_{0j}$ if $\rho_0 > 0$ and $t < j \le r_0$,

such that the following statements hold.

(i) $\dim_E(D) = 2{\cdot}h^2$.

(ii) $[E_{ij} : \mathbb{Q}_p] = d_{ij}$ *for all* $i = 0, \ldots, s$, *all* $j = 1, \ldots, r_i$.

(iii) *Let w_{ij} be the place of E above p corresponding to the factor E_{ij} of $E \otimes_{\mathbb{Q}} \mathbb{Q}_p$. Then L/E splits over $w_{i,j}$ for all $i = 1, \ldots, s$, all $j = 1, \ldots, r_i$.*

(iv) *If $\rho_0 > 0$, then L/E splits over $w_{0,j}$ for all j with $1 \le j \le t$.*

(v) Let $A[p^\infty] \sim \prod_{i,j} X_{i,j}$ be a decomposition of $A[p^\infty]$ up to isogeny, corresponding to the decomposition $E \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \prod_{i,j} E_{ij}$ of $E \otimes_{\mathbb{Q}} \mathbb{Q}_p$. *Then*

$$\mathcal{N}(X_{ij}) = \frac{d_{ij} \cdot h}{h_i} \cdot ((m_i, n_i) + (n_i, m_i)) \qquad \forall i = 1, \ldots, s, \quad \forall j = 1, \ldots, r_i \,,$$

and

$$\mathcal{N}(X_{0j}) = d_{0j}\, h \cdot (1, 1).$$

(vi) *The local Brauer invariant $\mathrm{inv}_v(D/L)$ at the two places of L above a place w_{ij} of E with $i \ge 1$ are $\frac{m_i \cdot d_{ij}}{m_i + n_i} \pmod{\mathbb{Z}}$ and $\frac{n_i \cdot d_{ij}}{m_i + n_i} \pmod{\mathbb{Z}}$ respectively.*

(vii) *If $\rho_0 > 0$, then the local Brauer invariant $\mathrm{inv}_v(D/E)$ at a place of L above a place w_{0j} is equal to $\frac{d'_{0j}}{2} \pmod{\mathbb{Z}}$ for all $j = 1, \ldots, r_0$.*

(5.5) Remark. (a) Note that for

$$\mathcal{N}(A) = \rho_0 \cdot (1,1) + \sum_{i=1}^{s} \rho_i \cdot ((m_i, n_i) + (n_i, m_i)) = \xi \,,$$

(v) implies that $\dim(A) = h \cdot [E : \mathbb{Q}]$, and that $e/2 = [E : \mathbb{Q}]$ is given by $e/2 = \sum_{1=0}^{s} \sum_{j=1}^{r_i} d_{i,j}$.

(b) If $\xi = \sum_{j=1}^{r_i} \rho_i \cdot ((m_i, n_i) + (n_i, m_i))$ is balanced, $\rho_0 = 0$, we can choose $r_1 = 1 = \cdots = r_s$ and the abelian variety given by the construction is *hypersymmetric*.

(5.6) Lemma. *Let L/E be a totally imaginary quadratic extension of a totally real number field E, and let p be a prime number. Then there exists a power q of p and a short exact sequence*

$$0 \longrightarrow W_0^L(q) \xrightarrow{\alpha} \bigoplus_{v|p} \mathbb{Z} \cdot v \xrightarrow{\beta} \bigoplus_{w|p} \mathbb{Z} \cdot w \longrightarrow 0$$

where v ranges over all places of L above p and w ranges over all places of E above p, with

$$W_0^L(q) = \left\{ \pi \in \mathcal{O}_L[1/p]^\times : |\iota(\pi)| = 1 \ \forall \iota : L \hookrightarrow \mathbb{C}, \text{ and } ||\pi||_w \in q^{\mathbb{Z}} \ \ \forall w|p \right\} \big/ \text{(modulo torsion)}$$

The maps α and β are defined by

$$\alpha(\pi) = \sum_{v|p} \log_q(||\pi||_v) \cdot v \,, \qquad \beta \ : \ \sum_{v|p} n(v) \cdot v \ \mapsto \ \sum_{w|p} \left(\sum_{v|w} n(v) \right) \cdot w \,.$$

Proof. This is Prop. 2.27 of [15]; it is a consequence of the theory of complex multiplication, due to Shimura and Taniyama. Note that in [15], Prop. 2.27 is placed under the blanket assumption on p. 425 that L is Galois over $\mathbb{Q}$. Although an examination of the argument shows the statement of Lemma 5.6 remains valid without the assumption that L is Galois over $\mathbb{Q}$, it is perhaps more convincing to reduce 5.6 to the case when L is Galois over $\mathbb{Q}$.

Choose a CM field L_1 containing L such that $L_1/\mathbb{Q}$ is a Galois extension. We have a commutative diagram,

$$\begin{tikzcd}
0 \arrow[r] & W_0^{L_1}(q) \arrow[r, "\alpha_1"] \arrow[d, "\mathrm{Nm}_{L_1/L}"'] & \bigoplus_{v_1|p} \mathbb{Z} \cdot v_1 \arrow[r, "\beta_1"] \arrow[d, "\gamma"] & \bigoplus_{w_1|p} \mathbb{Z} \cdot w_1 \arrow[r] \arrow[d, "\delta"] & 0 \\
0 \arrow[r] & W_0^{L}(q) \arrow[r, "\alpha"] & \bigoplus_{v|p} \mathbb{Z} \cdot v \arrow[r, "\beta"] & \bigoplus_{w|p} \mathbb{Z} \cdot w \arrow[r] & 0
\end{tikzcd}$$

where the top row is the sequence for the CM field L_1 as in the statement of 5.6, the map $\mathrm{Nm}_{L_1/L}$ is induced by the relative norm, and the maps γ, δ are defined by

$$\gamma \ : \ \sum_{v_1|p} n(v_1) \cdot v_1 \ \mapsto \ \sum_{v|p} \left(\sum_{v_1|v} n(v_1) \right) \cdot v \,, \qquad \delta \ : \ \sum_{w_1|p} n(w_1) \cdot w_1 \ \mapsto \ \sum_{w|p} \left(\sum_{w_1|w} n(w_1) \right) \cdot w$$

Clearly α and α_1 are injective, while β and β_1 are surjective. It is easy to see that the map

$$\gamma : \mathrm{Ker}\,(\beta_1)) \to \mathrm{Ker}\,(\beta))$$

is a surjection. Therefore the exactness of the bottom row follows from the exactness of the first row. ∎

(5.7) Lemma. *Let p be a prime number. Suppose we are given integers $s \geq 1$, $r_0 \geq 0$, $r_1, \ldots, r_s \geq 1$, and integers $d_{ij} \geq 1$, where i runs through all integers from 1 to s, and j runs through all integers from 1 to r_i. If $r_0 > 0$, suppose furthermore that we are given integers $d_{01}, \ldots, d_{0r_0} \geq 1$ and an integer t with $0 \leq t \leq r_0$. Then there exist*

(a) *a totally real number field E,*

(b) *a totally imaginary quadratic extension field L of E,*

(c) *finite extension fields E_{ij} of $\mathbb{Q}_p$ with $[E_{ij} : \mathbb{Q}_p] = d_{ij}$, for pairs (i, j) such that $0 \leq i \leq s$ and $1 \leq j \leq r_j$,*

(d) *a ring isomorphism $E \otimes_{\mathbb{Q}} \mathbb{Q}_p \xrightarrow{\sim} \prod_{i,j} E_{ij}$, where the indices i, j run through all pairs (i, j) such that $0 \leq i \leq s$ and $1 \leq j \leq r_j$,*

with the following properties.

(i) *Let w_{ij} be the place of E corresponding to the factor E_{ij} of $E \otimes_{\mathbb{Q}} \mathbb{Q}_p$, $0 \leq i \leq s$, $1 \leq j \leq r_j$. Then L/E is split over w_{ij} if either $i \geq 1$, or if $i = 0$ and $1 \leq j \leq t$.*

(ii) *$L \otimes_E E_{0j}/E_{0j}$ is a quadratic extension of fields if $t < j \leq r_0$.*

(iii) *No proper subfield of L is a CM-field. In other words, $M \cap E = M$ for every subfield M of L.*

Proof. Let $d = \sum_{i,j} d_{ij}$, where the indices i, j runs through all pairs (i, j) such that $0 \leq i \leq s$, $1 \leq j \leq r_s$. We may and do assume that $d > 1$. Choose and fix a prime number ℓ different from p. The first step is to apply Ekedahl's version of Hilbert irreducibility to obtain a totally real number field E and a ring isomorphism $E \otimes_{\mathbb{Q}} \mathbb{Q}_p \xrightarrow{\sim} \prod_{i,j} E_{ij}$ as in (d), where $E_{i,j}$ is a finite extension field of $\mathbb{Q}_p$ with $[E_{i,j} : \mathbb{Q}_p] = d_{ij}$, satisfying the following properties.

(iv) Let E' be the Galois closure of E over $\mathbb{Q}$. Then the Galois group $\mathrm{Gal}(E'/\mathbb{Q}) \cong S_d$.

(v) $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ is a finite unramified extension field of $\mathbb{Q}_\ell$ if d is even.

(vi) $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \cong \mathbb{Q}_\ell \times F_1$, where F_1 is a finite unramified extension field of $\mathbb{Q}_\ell$ if d is odd.

By the weak approximation theorem, we can find a suitable element $b \in E^\times$ which is not a square in $E^\times$ such that the quadratic extension $E(\sqrt{b})/E$ is totally imaginary and satisfies the required properties (i), (ii), and

(vii) $E(\sqrt{b})/E$ is unramified and inert above ℓ if d is even,

(viii) $E(\sqrt{b})/E$ is unramified and inert above the degree $d - 1$ place of E above ℓ, and splits above the degree-one place of E above ℓ, if d is odd.

We claim that $L := E(\sqrt{b})$ has no proper CM-subfield. Otherwise, since $\mathrm{Gal}(E'/\mathbb{Q}) \cong S_d$ we see that L contains an imaginary quadratic field K. Then $\mathrm{Gal}(E' \cdot K/\mathbb{Q}) \cong S_d \times (\mathbb{Z}/2\mathbb{Z})$, which is not possible by properties (vii) and (viii). $\square$

Proof of Theorem 5.4. The statement of 5.4 means that there exists a power q of p and a q-Weil number π such that $L := \mathbb{Q}(\pi)$ is a CM-field with the following properties.

(1) Let E be the maximal totally real subfield of L. Then there is a ring isomorphism $E \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \prod_{i,j} E_{ij}$, where the indices i, j runs through all pairs (i,j) such that $0 \le i \le s$, $1 \le j \le r_i$, such that $[E_{i,j} : \mathbb{Q}_p] = d_{ij}$ for all (i,j).

(2) Statements (i), (ii) of 5.7 holds.

(3) Let v_{ij} and v'_{ij} be the two places of L above w_{ij} if either $i \ge 1$, or if $i = 0$ and $1 \le j \le t$.

Then

$$\left\{ \frac{v_{ij}(\pi)}{v_{ij}(q)}, \frac{v'_{ij}(\pi)}{v'_{ij}(q)} \right\} = \left\{ \frac{m_i}{m_i + n_i}, \frac{n_i}{m_i + n_i} \right\}.$$

Let L be a CM-field satisfying the properties in Lemma 5.7. Apply Lemma 5.6 to an element

$$c \cdot \sum_{\substack{1 \le i \le s \\ 1 \le j \le r_s}} \left[\left(\frac{m_i}{m_i + n_i} - \frac{1}{2} \right) d_{ij} \cdot v_{ij} + \left(\frac{n_i}{m_i + n_i} - \frac{1}{2} \right) d_{ij} \cdot v'_{ij} \right] \quad \in \quad \oplus_{v|p} \mathbb{Z} \cdot v,$$

where c is a positive even integer divisible by $m_i + n_i$ for $i = 1, \ldots, s$. The existence of a q-Weil number satisfying the above properties (1), (2), (3) follows. ∎

§6. Hypersymmetric abelian varieties with real multiplication

(6.1) Definition. Let F be a totally real number field. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be the prime ideals of $\mathcal{O}_F$ above p.

(1) An $\mathcal{O}_F$-*linear abelian variety of* HB-type over a field K is a pair (A, ι), where A is an abelian variety over K, and $\iota : \mathcal{O}_F \to \mathrm{End}_K(A)$ is a ring homomorphism such that $\iota(1) = \mathrm{Id}_A$ and such that $\dim(A) = [F : \mathbb{Q}]$.

(2) A *Newton polygon of* HB-type *attached to* F is a family of the form

$$\{(F_{\mathfrak{p}_i}, \xi_i) \,|\, i = 1, \ldots, r\},$$

where each ξ_i is a Newton polygon such that

- either ξ_i is equal to $[F_{\mathfrak{p}_i} : \mathbb{Q}_p] \cdot (1,1)$,
- or ξ_i is of the form $\xi_i = \mu_i(m_i, n_i) + \mu_i(n_i, m_i)$, with $\mu_i \in \mathbb{Z}_{>0}$ and $\mu_i \cdot (m_i + n_i) = [F_{\mathfrak{p}_i} : \mathbb{Q}_p]$ and $(m_i, n_i) = 1$, $m_i \neq n_i$.

(3) Let (A, ι) be an $\mathcal{O}_F$-linear abelian variety of HB-type over a field K of characteristic p, where F is a totally real number field. We have a canonical decomposition

$$A[p^\infty] = \oplus_{i=1}^r A[\mathfrak{p}_i^\infty]$$

of the p-divisible group attached to A, where $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are the prime ideals of $\mathcal{O}_F$ above p. Each $A[\mathfrak{p}_i^\infty]$ is a p-divisible group with action by $\mathcal{O}_{F_{\mathfrak{p}_i}}$. Let ξ_i be the Newton polygon of the p-divisible group $A[\mathfrak{p}_i^\infty]$. Then $\{(F_{\mathfrak{p}_i}, \xi_i) \mid i = 1, \ldots, r\}$ is a Newton polygon of HB-type attached to F; see [22], Lemma 3.1. We call it the *Newton polygon of* HB-type *attached to* (A, ι). It is known that every Newton polygon of HB-type is realized by an $\mathcal{O}_F$-linear abelian variety of HB-type; see [22], Thm. 7.3(1).

(6.2) Lemma. *Let F be a totally real number field, and let (A, ι) be an $\mathcal{O}_F$-linear abelian variety of* HB-type *over a field K. Then A is isogenous to a multiple of a simple abelian variety: $A \sim B^a$, where B is a simple abelian variety over K.*

Proof. Let $A \sim \sum_{1 \le i \le s} A_i^{\mu_i}$ be a primary isogeny decomposition. Then

$$\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q} \cong \prod_{i=1}^{s} \mathrm{M}_{\mu_i}(D_i),$$

where $D_i = \mathrm{End}^0(A_i)$. In particular, F can be embedded into $\mathrm{End}(A_i^{\mu_i})^0$ for $i = 1, \ldots, s$. We suppose that $s > 1$, and we will obtain a contradiction. We have $[F : \mathbb{Q}] \le 2\,\mu_i \dim(A_i)$ for $i = 1, \ldots, s$. Adding these inequalities, we get $s \cdot \dim(A) \le 2 \dim(A)$, therefore $s = 2$, and $[F : \mathbb{Q}] = 2\,\mu_i \dim(A_i)$ for $i = 1, 2$. Consequently the abelian varieties $A_1^{\mu_1}$ and $A_2^{\mu_2}$ both have smCM, hence they are isogenous to abelian varieties B_1, B_2 defined over some finite field. Since F is totally real, and the Frobenii of B_1 and B_2 belong to F, we see that B_1 and B_2 are supersingular, hence isogenous. This is a contradiction. ∎

Remark. The statement of 6.2 holds when the base field K has characteristic 0. As pointed out by the referee, there is an alternative proof, valid in all characteristics. Replace the argument in the next-to-last sentence of the proof above by the following general fact: if B is an abelian variety and F is a totally real number field contained in $\mathrm{End}^0(B)$, then $[F : \mathbb{Q}] \mid \dim(B)$. This fact is surely well-known to the experts, and can be "read off" from the table on p. 202 of [14], by considering the dimensions of totally real number fields which can be embedded in $\mathrm{M}_n(\mathrm{End}^0(X))$ in each of the cases I–IV of *loc. cit.*

(6.3) Proposition. *Let F be a totally real number field, and let $\{(F_{\mathfrak{p}_i}, \xi_i) \mid i = 1, \ldots, r\}$ be a Newton polygon of* HB-*type attached to F. Then there exists an $\mathcal{O}_F$-linear abelian variety (A, ι) over $\mathbb{F}$ of* HB-*type such that A is hypersymmetric if and only if:*

(1) *either $\xi_i = [F_{\mathfrak{p}_i} : \mathbb{Q}_p] \cdot (1, 1)$ for all $i = 1, \ldots, r$,*

(2) *or $\xi_i \neq [F_{\mathfrak{p}_i} : \mathbb{Q}_p] \cdot (1, 1)$ for all $i = 1, \ldots, r$, and there exists a subfield $E \subset F$ such that*

  (a) *E splits completely over p, i.e. $E \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \mathbb{Q}_p \times \cdots \times \mathbb{Q}_p$;*

  (b) *if $\mathfrak{p}_{i_1} \cap \mathcal{O}_E = \mathfrak{p}_{i_2} \cap \mathcal{O}_E$, $1 \le i_1, i_2 \le r$, then $[F_{\mathfrak{p}_{i_2}} : \mathbb{Q}_p] \cdot \xi_{i_1} = [F_{\mathfrak{p}_{i_1}} : \mathbb{Q}_p] \cdot \xi_{i_2}$;*

  (c) *if $\mathfrak{p}_{i_1} \cap \mathcal{O}_E \neq \mathfrak{p}_{i_2} \cap \mathcal{O}_E$, $1 \le i_1, i_2 \le r$, then ξ_{i_1} and ξ_{i_2} are disjoint;*

  (d) *the multiplicity of every slope of $\xi := \sum_{i=1}^{r} \xi_i$ is equal to $[F : E]$.*

Remark. (i) The conditions (a)–(d) in (2) above imply that ξ is a multiple of a balanced Newton polygon ξ'.

(ii) The existence of examples of Newton polygon strata in Hilbert modular varieties on which there are no hypersymmetric abelian varieties was pointed out to the first author by Chia-Fu Yu.

Proof of Prop. 6.3. Suppose that $\{(F_{\mathfrak{p}_i}, \xi_i) \mid i = 1, \ldots, r\}$ is a Newton polygon of HB-type attached to an $\mathcal{O}_F$-linear abelian variety (A, ι) of HB-type such that A is hypersymmetric and not supersingular. By Lemma 6.2, A is isogenous to a multiple of a simple abelian variety B, necessarily hypersymmetric. Assume that B is not supersingular. Then the center L of $\mathrm{End}^0(B)$ is a totally imaginary quadratic extension of a totally real number field E, and L splits completely above p by Prop. 3.6. Moreover the multiplicity of every slope of A is equal to $2 \cdot \dim(A)/[L : \mathbb{Q}]$. Let E be the maximal totally real subfield of L. The subring M of $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ generated by F and L is a commutative semi-simple algebra such that every field factor of M is a CM field of degree at least $2\,[F : \mathbb{Q}] = 2\dim(A)$. Therefore M is a totally imaginary quadratic extension of F. In particular F contains E, and the multiplicity of every slope of A is equal to $2 \cdot \dim(A)/[L : \mathbb{Q}] = [F : E]$. The statements (a), (b), (c) follow from Prop. 3.6.

To prove the "if" part of Prop. 6.3, we first assume that condition (1) holds, that is, each ξ_i has only one slope $\frac{1}{2}$. Let $A = E^g$, where $g = [F : \mathbb{Q}]$ and E is a supersingular elliptic curve over $\mathbb{F}$. Then $\mathrm{End}(A) \cong \mathrm{M}_g(D_{p,\infty})$, where $D_{p,\infty}$ is a quaternion division algebra over $\mathbb{Q}$ exactly ramified at p and ∞. It is well-known that $\mathcal{O}_F$ can be embedded in $\mathrm{M}_g(D_{p,\infty})$. Any embedding ι gives us an $\mathcal{O}_F$-linear abelian variety (A, ι) of HB-type satisfying the required conditions.

Finally, assume that the condition (2) holds. Let $\xi := \sum_{i=1}^{r} \xi_i = \mu \cdot \xi'$, where ξ' is a balanced Newton polygon. According to Prop. 4.1 and Prop. 4.4 there exists a hypersymmetric simple abelian variety B over $\mathbb{F}$ such that $\mathcal{N}(B) = \xi'$, and the center L of the division algebra $\mathrm{End}^0(B)$ is a totally imaginary quadratic extension of E. It suffices to show that there exists an E-linear embedding $F \hookrightarrow \mathrm{M}_\mu(D)$, for then one can find a hypersymmetric abelian variety A over $\mathbb{F}$-isogenous to B^μ and an $\mathcal{O}_E$-linear embedding $\iota : \mathcal{O}_F \hookrightarrow \mathrm{End}(A)$, and the Newton polygon attached to the $\mathcal{O}_F$-linear abelian variety (A, ι) of HB-type is $\{(F_{\mathfrak{p}_i}, \xi) \mid i = 1, \ldots, r\}$. Let M be the composition of the field extensions F/E and L/E, so that M is a totally imaginary quadratic extension of F. The conditions (a)–(d) imply that the central simple algebra $\mathrm{M}_\mu(D) \otimes_L M$ over M splits at all places above p, hence it is split, because the division algebra D over L splits at all finite places of L. Therefore there exists an L-linear embedding $M \hookrightarrow \mathrm{M}_\mu(D)$. $\square$

From the point of view of Shimura varieties, the notion of hypersymmetric points needs to be modified when considering the reduction of Shimura varieties. Otherwise hypersymmetric points may not even exist on a Newton polygon stratum of the reduction of a Shimura variety. We give a proposed definition for modular varieties of PEL-type.

(6.4) Definition. Let $(\Gamma, *)$ be a finite dimensional semi-simple algebra over $\mathbb{Q}$ with positive involution. Let $\mathcal{O}_\Gamma$ be an order of Γ. Let A be an abelian variety over an algebraically closed field $k \supset \mathbb{F}_p$, and let $\iota : \mathcal{O}_\Gamma \to \mathrm{End}(A)$ be a ring homomorphism such that $\iota(1) = \mathrm{Id}_A$. We say that (A, Γ, ι) is (Γ, ι)-*hypersymmetric* if the natural map

$$\mathrm{End}_{\mathcal{O}_\Gamma}(A) \otimes_{\mathbb{Z}} \mathbb{Q}_p \to \mathrm{End}_{\mathcal{O}_\Gamma \otimes_{\mathbb{Z}} \mathbb{Z}_p}(A[p^\infty]) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

is an isomorphism.

(6.5) Remark. In 6.4, suppose furthermore that $\lambda : A \to A^t$ is a polarization of A, and the ring homomorphism ι is compatible with the involution $*$ on B and the Rosati involution $*_\lambda$ on $\mathrm{End}^0(A)$ attached to λ. Then the condition for (A, Γ, ι) to be (Γ, ι)-hypersymmetric is equivalent to the condition that the natural map

$$\left(\mathrm{End}^0_{\mathcal{O}_\Gamma}(A)\right)^{*=-1} \otimes_{\mathbb{Q}} \mathbb{Q}_p \to \left(\mathrm{End}_{\mathcal{O}_\Gamma \otimes_{\mathbb{Z}} \mathbb{Z}_p}(A[p^\infty]) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p\right)^{*_\lambda=-1}$$

is an isomorphism. The latter condition is more natural from the point of view of Shimura varieties.

§7. Hypersymmetric points and special points

We study some density properties of hypersymmetric points in subvarieties of the moduli space $\mathcal{A}_g$ of g-dimensional principally polarized abelian varieties. The base field in this section is $\mathbb{F} = \overline{\mathbb{F}_p}$

(7.1) Remark. One can show that in any given Newton polygon stratum W_ξ of the moduli space $\mathcal{A}_{g,1} \otimes \mathbb{F}_p$ of g-dimensional principally polarized abelian varieties over $\mathbb{F}$, the set of hypersymmetric points is dense in W_ξ. In fact, one can show that for any hypersymmetric point x_0 in W_ξ, the set of hypersymmetric points in W_ξ isogenous to x_0 is dense in W_ξ. This follows from the irreducibility of W_ξ for non-supersingular ξ, and the rigidity result and the action of the local stabilizer subgroup as explained in [2]. Similarly, one can show that in any given central leaf $\mathcal{C}$ in $\mathcal{A}_g$ in the sense of [18], the set of hypersymmetric points is dense in $\mathcal{C}$.

(7.2) One might wonder whether hypersymmetric abelian varieties over $\mathbb{F}$ are the right analog of CM abelian varieties in characteristic zero. However we will see that an obvious analogous formulation of the André-Oort conjecture does not hold for hypersymmetric abelian varieties over $\mathbb{F}$.

Let us write $\mathbb{A}^1 = \mathcal{A}_{1,1} \otimes \mathbb{F}$ for the moduli space of elliptic curves over $\mathbb{F}$; we write $\mathbb{A}^1 \subset \mathbb{P}^1 = \mathbb{P}^1_{\mathbb{F}}$, and $\infty \in \mathbb{P}^1$ for the point corresponding with a degenerate elliptic curve. We say $(x, y) \in \mathbb{P}^1 \times \mathbb{P}^1$ is supersingular if x and y are supersingular j-values. We say $(x, y) \in \mathbb{P}^1 \times \mathbb{P}^1$ is hypersymmetric if $E_x \times E_y$ is hypersymmetric, i.e. all cases where $E_x \sim E_y$, i.e. either (x, y) is supersingular, or $E_x \sim E_y$ is ordinary, or one is supersingular and the other is ordinary.

Note that not every curve in $\mathbb{P}^1 \times \mathbb{P}^1$ is a modular curve, i.e. is not the reduction mod p of a Shimura curve. In fact, let $S \subset \mathbb{A}^1 \subset \mathbb{P}^1$ be the set of supersingular points and let $C \subset \mathbb{P}^1 \times \mathbb{P}^1$ be an irreducible curve containing a point $(x, y) \in C$ with $x \in S$ and $x \notin S$. Then C is not modular. Hence the following proposition provides us with examples of non-modular curves with dense sets of hypersymmetric points.

(7.3) Proposition. *Every curve C in the product $\mathbb{P}^1 \times \mathbb{P}^1$ of two j-lines over $\mathbb{F}$ contains a dense set of hypersymmetric points.*

Before giving a proof we fix some notations. Note that in any horizontal line $\{x\} \times \mathbb{A}^1 \subset \mathbb{P}^1 = \mathbb{P}^1_{\mathbb{F}}$ the hypersymmetric points are dense; for x supersingular, take all ordinary y; for x ordinary, use the fact that the Hecke orbit $\mathcal{H}(x)$ of E_x in $\mathcal{A}_{1,1} \otimes m$ is non-finite, see [1], Prop. 1 on page 448; hence $\mathcal{H}(x) \subset \mathcal{A}_{1,1}$ is dense. The same argument proves this fact for a vertical line. Hence it suffices to prove the proposition under the extra condition that C is an irreducible curve of bidegree (d_1, d_2) with $d_1 > 0$ and $d_2 > 0$; here $d_1 = (C \cdot (\{\mathrm{pt}\} \times \mathbb{P}^1))$, and $d_2 = (C \cdot (\mathbb{P}^1 \times \{\mathrm{pt}\}))$.

We consider the morphism $\mathrm{Fr}_{p^n} : \mathbb{P}^1 \to \mathbb{P}^1$. We write $\mathcal{F}_n = \Gamma(\mathrm{Fr}_{p^n}) \subset \mathbb{P}^1 \times \mathbb{P}^1$ for the graph of this morphism. Note that $\mathcal{F}_n$ is irreducible of bidegree $(1, p^n)$.

(7.4) Lemma. *Suppose $p^n > d_2$. Let $P \in C \cap \mathcal{F}_n$. Then the local intersection number of C and $\mathcal{F}_n$ at P satisfies $i_P(C, \mathcal{F}_n) \leq d_2$.*

Proof. Choose local affine coordinates in a neighborhood of $P \in \mathbb{P}^1 \times \mathbb{P}^1$ such that $P = (0, 0)$. Write $g \in \mathbb{F}[X, Y]$ for an irreducible polynomial defining C in this neighborhood. Note that

$$\dim_{\mathbb{F}} (\mathbb{F}[X, Y]/)/(g, Y)) = \dim_{\mathbb{F}} (\mathbb{F}[X]/(g(X, 0))\,.$$

Let $H = \mathbb{P}^1 \times \{0\}$ be the horizontal line defined as the set of zeros of Y. We see:

$$0 \quad < \quad i_P(C, H) = \deg_X(g(X, 0)) \quad \leq \quad d_2.$$

Moreover

$$\mathbb{F}[X, Y]/(g, Y - X^{p^n}) \cong \mathbb{F}[X]/(g(X, X^{p^n}));$$

as $p^n > d_2$ we see that $g(X, X^{p^n}) \equiv g(X, 0) \pmod{X^{d_2}}$. Hence

$$i_P(C, \mathcal{F}_n) \quad = \quad i_P(C, H) \quad \leq \quad d_2.$$

This proves the lemma. □

Proof of 7.3. We know

$$\sum_P i_P(C, \mathcal{F}_n) = d_1 {\cdot} p^n + d_2 \quad \text{and} \quad i_P(C, \mathcal{F}_n) \leq d_2 \quad \forall P.$$

Hence

$$\#\,(C \cap \mathcal{F}_n) \quad \geq \quad \frac{d_1 {\cdot} p^n + d_2}{d_2} \quad > \quad \frac{d_1}{d_2} {\cdot} p^n.$$

If $(x, y) = P \in (C \cap \mathcal{F}_n)(\mathbb{F})$ there is an isogeny $\mathrm{Fr}_{p^n} : E_x \to E_y$; hence $P \in C(\mathbb{F})$ is hypersymmetric. As $\#\,(C \cap \mathcal{F}_n) \to \infty$ for $n \to \infty$ this proves the proposition. □

(7.5) Remark. Here is another class of counter-examples to the "obvious analog" of the André-Oort conjecture. Let $g \geq 2$ be an integer. Let $N \geq 3$ be an integer, $(N,p) = 1$. Let X be a central leaf in $\mathcal{A}_{g-1,N}$. As remarked in 7.1, there exists a countable set of hypersymmetric points $\{x_i : i \in \mathbb{Z}_{>0}\}$ in $X(\mathbb{F})$ which is Zariski dense in X. Let f be a non-constant rational map from X to the modular curve $\mathcal{A}_{1,N}$, i.e. there exists a dense open subset $U \subset X$ such that f is represented by a morphism $f_U : U \to \mathcal{A}_{1,N}$. Let $\Gamma(f)$ be the graph of f, i.e. $\Gamma(f)$ is the Zariski closure in $\mathcal{A}_{g-1,N} \times \mathcal{A}_{1,N}$ of the graph of f_U. We have a natural embedding $\iota : \mathcal{A}_{g-1,N} \times \mathcal{A}_{1,N} \hookrightarrow \mathcal{A}_{g,N}$. Passing to a countable subset if necessary, we may assume that $x_i \in U$ for all $i \in \mathbb{Z}_{>0}$, and $f(x_i)$ is an ordinary point of $\mathcal{A}_{1,N}$ corresponding to an ordinary elliptic curve over $\mathbb{F}$. Let $z_i := \iota(x_i, f(x_i))$ for each i. Then $\{z_i : i \in \mathbb{Z}_{>0}\}$ is a countable set of hypersymmetric points of $\Gamma(f)(\mathbb{F})$ which is Zariski dense in $\Gamma(f)$. Notice that the subscheme $\iota(\Gamma(f))$ is contained in a central leaf $\mathcal{C}$ of $\mathcal{A}_{g,N}$ by hypothesis, but in general $\iota(\Gamma(f))$ is not the intersection of $\mathcal{C}$ with a Shimura subvariety $\mathcal{M}$ of $\mathcal{A}_g$.

(7.6) Remark. As an analog of the André-Oort conjecture, one may wonder whether every irreducible component of the Zariski closure of an infinite set of hypersymmetric points in a central leaf $\mathcal{C}$ in $\mathcal{A}_g$ is "cut out" by the reduction of a Shimura subvariety. As Proposition 7.3 and Remark 7.5 show, that is not correct. The reason is that, the reduction of some Shimura subvarieties, for example a modular curve or a Shimura curve, have the property that every point is hypersymmetric. One might wonder whether this is "the only obstruction". Below we formulate statement in this direction as a *question*.

Question. Let $\mathcal{C}$ be a central leaf in $\mathcal{A}_{g,N}$ over $\mathbb{F}$, where $N \geq 3$ is an integer, $(N,p) = 1$. Suppose that Z is an irreducible subvariety of $\mathcal{C}$ such that the set of all hypersymmetric points on Z is dense in X. *Does there exist a (reduction of a) Shimura subvariety $\mathcal{M}$ of $\mathcal{A}_{g,N}$, attached to a Shimura input data (G,X), with the following properties?*

(i) The simply connected covering $G^{\mathrm{sc}}_{\mathrm{der}}$ of the derived group G_{der} of the reductive G is a product $G^{sc}_{\mathrm{der}} \cong G_1 \times G_2$, inducing a decomposition of Shimura input data $(G,X) = (G_1,X_1) \times (G_2,X_2)$.

(ii) The reduction modulo p of the Shimura varieties $\mathrm{Sh}(G_1,X_1)$ and $\mathrm{Sh}(G_2,X_2)$ give rise to Shimura varieties $\mathcal{M}_1$, $\mathcal{M}_2$ over $\mathbb{F}$, with $\dim(\mathcal{M}_1) = 1$.

(iii) There exist a finite morphism $f : \mathcal{M}_1 \times \mathcal{M}_2 \to \mathcal{A}_{g,N}$, a finite isogeny correspondence, $h : \mathcal{A}_{g,N} \leftarrow I \to \mathcal{A}_{g,N}$ and a central leaf $\mathcal{C}_2$ in $\mathcal{M}_2$ such that

$$Z \subseteq h(f(\mathcal{M}_1 \times \mathcal{C}_2))$$

and

$$\mathrm{pr}_2\left((\mathcal{M}_1 \times \mathcal{C}_2) \cap f^{-1}(h^{-1}(Z)\right) = \mathcal{C}_2\,.$$

References

[1] C.-L. Chai – *Every ordinary symplectic isogeny class in positive characteristic is dense in the moduli space.* Invent. Math. **121** (1995), 439–479.

[2] C.-L. Chai – *Hecke orbits on Siegel modular varieties.* Progress in Mathematics **235**, Birkhäuser, 2004, pp. 71–107.

[3] C.-L. Chai & F. Oort – *Hecke Orbits.* [In preparation]

[4] P. Deligne – *Hodge cycles on abelian varieties.* In: Hodge cycles, motives and Shimura varieties (Ed. P. Deligne et al). Lecture Notes Math. 900, Springer-Verlag 1982 ; pp. 9–100.

[5] M. Demazure – *Lectures on p-divisible Groups.* Lecture Notes Math. 302, Springer-Verlag 1972.

[6] A. J. de Jong & F. Oort – *Purity of the stratification by Newton polygons.* Journ. A.M.S. **13** (2000), 209–241.

[7] T. Ekedahl – *An effective version of Hilbert's irreducibility theorem.* Séminaire de Théorie des Nombres, Paris 1988–89. Progress in Math. **91**, Birkhäuser, 1990, pp. 241–249.

[8] J. Ellenberg & Akshay Venkatesh – *The number of extensions of a number field with fixed degree and bounded discriminant.* To appear in Ann. Math.

[9] S. Lang – *Fundamentals of Diophantine Geometry.* Springer-Verlag 1983.

[10] S. Lang – *Complex Multiplication.* Grundlehren Math. Wiss., Vol 255, Springer-Verlag 1983.

[11] H. W. Lenstra jr. & F. Oort – *Simple abelian varieties having a prescribed formal isogeny type.* Journ. Pure Appl. Algebra **4** (1974), 47–53.

[12] Yu. I. Manin – *The theory of commutative formal groups over fields of finite characteristic.* Usp. Math. **18** (1963), 3–90; Russ. Math. Surveys **18** (1963), 1–80.

[13] D. Mumford – *A note on Shimura's paper "Discontinuous groups and abelian varieties".* Math. Ann **181** (1969), 345–351.

[14] D. Mumford – *Abelian Varieties.* Tata Inst. Fund. Res. Studies in Math. **5**, Oxford University Press, 1974.

[15] J. S. Milne – *Motives over finite fields.* Proc. Symp. Pure. Math. **55**, Part 1, 1994, 401–459.

[16] F. Oort – *The isogeny class of a CM-type abelian variety is defined over a finite extension of the prime field.* Journ. Pure Appl. Algebra **3** (1973), 399–408.

[17] F. Oort – *Endomorphism algebras of abelian varieties.* Algebraic Geometry and Commut. Algebra in honor of M. Nagata (Ed. H. Hijikata et al), Kinokuniya Cy Tokyo, Japan, 1988, Vol II, 469–502.

[18] F. Oort – *Foliations in moduli spaces of abelian varieties.* Journ. A. M. S. **17** (2004), 267–296.

[19] G. Shimura & Y. Taniyama – *Complex multiplication of abelian varieties and its applications to number theory.* Publ. Math. Soc. Japan 6, 1961.

[20] J. Tate – *Endomorphisms of abelian varieties over finite fields.* Invent. Math. **2** (1966), 134–144.

[21] J. Tate – *Classes d'isogénie de variétés abéliennes sur un corps fini (d'après T. Honda).* Sém. Bourbaki, **21** , 1968/69, Exp. 352, LNM **179**, 1971, pp. 95–110.

[22] C.-F. Yu – *On reduction of Hilbert-Blumenthal varieties.* Ann. Inst. Fourier Grenoble, **53** (2003), 2105–2154.

Ching-Li Chai
Department of Mathematics
University of Pennsylvania
Philadelphia, PA 19104-6395
USA
email: chai@math.upenn.edu

Frans Oort
Mathematisch Instituut
Budapestlaan 6
NL - 3584 CD TA Utrecht
The Netherlands
email:oort@math.uu.nl

Postbus 80010
NL - 3508 TA Utrecht
The Netherlands