ARTHUR OGUS

Supersingular $K3$ crystals

Astérisque, tome 64 (1979), p. 3-86
<http://www.numdam.org/item?id=AST_1979__64__3_0>

SUPERSINGULAR K3 CRYSTALS

by

Arthur OGUS

(Berkeley)

-:-:-:-

§0. INTRODUCTION.

This paper is intented as propaganda for the machinery of crystalline cohomology, and in particular for the philosophy that F-crystals are a partial analogue, in characteristic p, to Hodge structures in characteristic zero. An extremely rudimentary start along this road, for "abstract" F-crystals and Hodge structures, was made in [15] ; here we turn to crystals arising geometrically, especially from supersingular abelian varieties and K3 surfaces. As we shall see, it is reasonable to hope that the moduli of such varieties are given by the moduli of their F-crystals, which in fact form explicit "period-spaces".

Here is a plan of the paper : The first section contains some refinements of generally known facts concerning crystalline Chern classes, e.g. an integral version of Bloch's theorem relating flat and crystalline cohomology (1.7), conditions guaranteeing that $c_1 : \mathrm{Pic} \otimes \mathbb{Z}/p\mathbb{Z} \to H^2_{DR}$ is injective (1.4), and a formula for certain second order obstructions to extending invertible sheaves in a family (1.15).

The second section gives applications of these results to families of polarized K3 surfaces. In particular, we slightly refine Deligne's proof of liftability of a K3 by bounding the ramification ; this allows us to prove that if $p > 2$, the map $\mathrm{Aut}(X) \to \mathrm{Aut}\, H^2_{\mathrm{cris}}(X/W)$ is injective. We also show that the geometric generic fiber of a versal family of polarized K3's is ordinary and has base number $\rho = 1$.

The next three sections are devoted to the classification of those F-crystals which have the slopes and Hodge numbers of the crystalline cohomology of a supersingular surface with $p_g = 1$, which we call "supersingular K3 crystals". In section three we give the basic structure theorems and explicit "coarse moduli". Section four introduces a fine moduli space for such crystals, suitably rigidified. This space turns out to have a beautiful smooth compactification, with a clear "modular" interpretation. In the fifth section we discuss families of crystals, make precise the term "fine moduli", and study the period map arising from a family of K3 surfaces. As Artin showed, K3 surfaces with $\rho = 22$ fit in 9 dimensional versal families ; we show that (after suitably rigidifying) the period map to our fine moduli space is étale. This is the local Torelli theorem, and, I hope, the first step towards a global Torelli theorem for supersingular K3 surfaces.

In the sixth section, we look at supersingular abelian varieties of dimension n. We prove a Torelli theorem : If Y and Y' are supersingular abelian varieties of dimension $n \geq 2$, and if there exists an isomorphism : $H^1_{\mathrm{cris}}(Y/W) \to H^1_{\mathrm{cris}}(Y'/W)$ compatible with Frobenius and the trace map, then Y and Y' are isomorphic. It is interesting to note that this is <u>false</u> if $n = 1$, or if the trace map is forgotten, and in particular the interpretation of H^1 in terms of p-divisible groups is inadequate for such a result.

The final section is devoted to the Torelli problem for K3 surfaces in characteristic $p > 2$ with $\rho = 22$, which takes the following forms :

0.1 <u>Conjecture</u>. X <u>and</u> X' <u>are isomorphic iff there exists an isomorphism</u>

$H^2_{cris}(X/W) \to H^2_{cris}(X'/W)$ compatible with Frobenius and cup-product.

0.2 Conjecture. Suppose $\theta : NS(X) \to NS(X')$ is an isomorphism, compatible with cup-product and with effective divisor classes, and suppose θ fits into a commutative diagram :

$$\begin{array}{ccc} NS(X) & \xrightarrow{\theta} & NS(X') \\ c_1 \downarrow & & \downarrow c_1 \\ H^2_{DR}(X/k) & \xrightarrow{\cong} & H^2_{DR}(X'/k). \end{array}$$

Then θ is induced by an isomorphism $X' \to X$.

We attempt to prove this by following the proof in characteristic zero. The key step is the proof when X is assumed to be a Kummer surface ; this turns out to be possible in characteristic p as well ((7.13) and (7.15)). In characteristic zero, one then checks that the set of Kummer points in the period space is dense, and concludes by the local Torelli theorem. Unfortunately, in characteristic p, the set of Kummer points forms a closed one-dimensional subset of the period space, so this method fails. The only way I can think of to pursue the conjecture is to prove that the period map is proper, at least in a neighborhood of the Kummer points. As a matter of fact, since the period space is compact, it seems reasonable to hope that supersingular K3's cannot degenerate in any serious way. This would prove that the period space is in fact a fine moduli space of (rigidified) supersingular K3 surfaces.

At this point I would like to express my immense gratitude to the many people who showed an interest in this work and who provided many helpful discussions, including L. Illusie, P. Berthelot, J. Milne, T. Shioda and especially P. Deligne. Of course, this paper was very much inspired by Artin's original paper on supersingular K3 surfaces [2], and in fact began as the exercise of systematically replacing flat cohomology by crystalline cohomology in that paper. I would also like to thank the C.N.R.S. and the I.H.E.S. for their support and hospitality during the main part of the research that went into this paper, as well as Orsay for the preparation of the manuscript.

§1. DEFORMATIONS AND OBSTRUCTIONS.

We begin with some simple but important refinements of some well-known relationships between the crystalline and flat cohomologies. It is convenient to make the following standard hypotheses :

1.1 Hypotheses. Assume that X is smooth and proper over an algebraically closed field k, and additionally that :

1.1.1 The Hodge to De Rham spectral sequence :

$$E_1^{pq} = H^q(X,\Omega^p_{X/k}) \Rightarrow H^{p+q}_{DR}(X/k) \text{ degenerates at } E_1.$$

1.1.1^{bis} The conjugate spectral of De Rham cohomology :

$$E_2^{pq} = H^p(X,\underline{H}^q(\Omega^{\cdot}_{X/k})) \Rightarrow H^{p+q}_{DR}(X/k) \text{ degenerates at } E_2.$$

1.1.2 The crystalline cohomology groups $H^i_{cris}(X/W(k))$ are torsion free.

We remind the reader that the Cartier operator induces a (Frobenius inverse linear) isomorphism $C : \underline{H}^q(\Omega^{\cdot}_{X/k}) \to \Omega^q_{X/k}$, hence also an isomorphism : $C : H^p(X,\underline{H}^q(\Omega^{\cdot}_{X/k})) \to H^p(X,\Omega^p_{X/k})$. It follows that 1.1.1 and 1.1.1^{bis} are equivalent ; if they are satisfied, we can view C as an isomorphism : $C : gr^p_{F_{con}} H^{p+q}_{DR}(X/k) \to gr^q_{F_{Hodge}} H^{p+q}_{DR}(X/k)$. Recall also that 1.1 $(= 1.1.1+1.1.2)$ is satisfied if X has a smooth lifting X'/W with $H^q(X',\Omega^p_{X'/W})$ torsion free (Hodge theory), or if X is a K3 surface [20].

1.2 <u>Proposition</u>. <u>If</u> X <u>satisfies</u> 1.1.1 <u>and if</u> π_{Hodge} <u>and</u> π_{con} <u>are the natural projections</u>, <u>the following sequence is exact</u> :

$$0 \to H^2(X_{fl},\mu_p) \to F^1_{Hodge} \cap F^1_{con} H^2_{DR}(X/k) \xrightarrow{\pi_{Hodge} - C \circ \pi_{con}} gr^1_{F_{Hodge}} H^2_{DR}(X/k).$$

<u>Proof</u>. First of all, I claim that if $\underline{Z}^1_{X/k}$ is the sheaf of closed one-forms on X, there is a natural isomorphism :

1.2.1 $$H^1(X,\underline{Z}^1_{X/k}) \xrightarrow{\simeq} F^1_{\text{Hodge}} \cap F^1_{\text{con}} .$$

To prove this, consider the exact sequence of complexes :

$$0 \to \underline{Z}^1_{X/k}[-1] \to F^1_{\text{Hodge}}\Omega^{\cdot}_{X/k} \to Q^{\cdot} \to 0.$$

It is clear that $\underline{H}^q(Q^{\cdot}) = 0$ if $q < 2$ and that the map $\underline{H}^q(F^1\Omega^{\cdot}_{X/k}) \to \underline{H}^q(Q^{\cdot})$ is an isomorphism for $q \geq 2$. Since $H^1(X,Q^{\cdot}) = 0$, the map $H^1(X,\underline{Z}^1_{X/k}) \to H^2(X,F^1\Omega^{\cdot}_{X/k})$ is injective. Since the maps :

$$H^2(X,Q^{\cdot}) \to H^0(X,\underline{H}^2(Q^{\cdot})) \leftarrow H^0(X,\underline{H}^2(F^1\Omega^{\cdot}_{X/k})) \to H^0(X,\underline{H}^2(\Omega^{\cdot}_{X/k}))$$

are isomorphisms, we get an exact sequence :

1.2.2
$$\begin{array}{ccccccc} 0 \to & H^1(X,\underline{Z}^1_{X/k}) & \to & H^2(X,F^1\Omega^{\cdot}_{X/k}) & \to & H^0(X,\underline{H}^2(\Omega^{\cdot}_{X/k})) \\ & \downarrow & & \downarrow & & \downarrow \cong \\ 0 \to & F^1_{\text{con}}H^2_{DR}(X/k) & \to & H^2_{DR}(X/k) & \to & H^0(X,\underline{H}^2(\Omega^{\cdot}_{X/k})) . \end{array}$$

The hypothesis (1.1.1) implies that the middle vertical arrow is injective, with image F^1_{Hodge}, and this establishes (1.2.1).

To prove the proposition, we use Milne's isomorphism : $H^2(X_{fl},\mu_p) \cong H^1(X_{\acute{e}t},\mathcal{O}^*_X/\mathcal{O}^{*p}_X)$, and his exact sequence (on $X_{\acute{e}t}$) :

$$0 \to \mathcal{O}^*_X/\mathcal{O}^{*p}_X \xrightarrow{d\log} \underline{Z}^1_{X/k} \xrightarrow{\text{inc-C}} \Omega^1_{X/k} \to 0,$$

hence

$$H^0(X_{\acute{e}t},\underline{Z}^1_{X/k}) \xrightarrow{\text{inc-C}} H^0(X_{\acute{e}t},\Omega^1_{X/k}) \to H^2(X_{fl},\mu_p) \to H^1(X_{\acute{e}t},\underline{Z}^1_{X/k}) \xrightarrow{\text{inc-C}} H^1(X_{\acute{e}t},\Omega^1_{X/k}).$$

Now hypothesis (1.1.1) implies that the map inc : $H^0(X_{\acute{e}t},\underline{Z}^1_{X/k}) \to H^0(X_{\acute{e}t},\Omega^1_{X/k})$ is an isomorphism. Since C is Frobenius-inverse linear and k is algebraically closed, inc-C is therefore surjective. Using the interpretation (1.2.1) of $H^1(X_{\acute{e}t},\underline{Z}^1_{X/k})$, we find the proposition. □

1.3 Corollary. *If X satisfies (1.1.1) and if $\xi \in H^2(X_{fl},\mu_p)$ is such that $d\log(\xi)$ lies in F^2_{Hodge} or F^2_{con}, then in fact it lies in $F^2_{\text{Hodge}} \cap F^2_{\text{con}}$.*

Proof. If $d\log(\xi)$ lies in F^2_{Hodge}, $C \circ \pi_{\text{con}}(d\log(\xi)) = \pi_{\text{Hodge}}(d\log(\xi)) = 0$. Since C is an isomorphism, $\pi_{\text{con}}(d\log(\xi)) = 0$, and $d\log(\xi)$ lies in F^2_{con}. The converse is proved similarly. □

1.4 Corollary. *If X satisfies (1.1.1), the map : $c_1 = \text{Pic}(X) \otimes \mathbb{F}_p \to H^2_{DR}(X/k)$ is injective, and factors through $F^1_{\text{Hodge}} \cap F^1_{\text{con}}$. If $c_1(L)$ lies in F^2_{Hodge} or F^2_{con}, it lies in $F^2_{\text{Hodge}} \cap F^2_{\text{con}}$.*

Proof. We have $\text{Pic}(X) \otimes \mathbb{F}_p \hookrightarrow H^1(X_{\acute{e}t}, \mathcal{O}^*_X/\mathcal{O}^{*p}_X) \cong H^2(X_{fl}, \mu_p)$, so this follows immediately from (1.2) and (1.3). □

1.5 Corollary. *If X satisfies (1.1), the cokernel of the map : $c_1 : \text{Pic}(X) \to H^2_{\text{cris}}(X/W)$ is torsion free.*

Proof. In this case we know that $H^2_{\text{cris}}(X/W) \otimes \mathbb{Z}/p\mathbb{Z} \cong H^2_{DR}(X/k)$, so (1.5) follows from the injectivity of c_1 mod p. □

1.6 Corollary. *If X satisfies (1.1) and if the rank of $NS(X)$ equals the rank of $H^2_{\text{cris}}(X/W)$, then the map $NS(X) \otimes \mathbb{Z}_p \to H^2_{\text{cris}}(X/W)^{F=p}$ is an isomorphism.* □

1.7 Corollary (Illusie). *If X satisfies (1.1) the map : $H^2(X_{fl}, \mathbb{Z}_p(1)) \to H^2_{\text{cris}}(X/W)^{F=p}$ is an isomorphism.* □

For the proof of the above result, I refer to forthcoming work of Illusie. I would like to explain at this point that in fact my starting point was (1.4), and that Illusie and Milne pointed out to me that the same proof gave the injectivity of $H^2(X_{fl}, \mu_p) \to H^2_{DR}(X/k)$.

1.8 Remark. It can be said that the Cartier operator above is playing a role analogous to complex conjugation in characteristic zero. Namely, if L is a line bundle on a smooth proper X over $\mathbb{C}$, its Chern class $c_1(L) \in F^1H^2_{DR}(X/\mathbb{C})$ is the obstruction to endowing L with an integrable connection, while its Hodge Chern class

$\pi_{Hodge} c_1(L) \in gr^1_F H^2_{DR}(X/\mathbb{C})$ is the obstruction to endowing L with any connection. We know that in fact if the latter vanishes, $c_1(L) \in F^2 H^2_{DR}(X/\mathbb{C})$, but since $c_1(L) \in H^2(X,\mathbb{R})$, $\overline{c_1(L)} = c_1(L)$, hence $c_1(L) \in F^2 \cap \overline{F^2} = \{0\}$. The same thing is true for varieties in characteristic p (satisfying (1.1)) with $F^2_{Hodge} \cap F^2_{con} = 0$, by corollary (1.4). It is interesting to note that $c_1(L)$ is still the obstruction to finding an integrable connection on L, and that if $c_1(L)$ vanishes, we can in fact find a p-integrable connection (this is essentially the surjectivity of $H^o(\text{inc-C})$). □

1.9 Remark. If $F^1_{Hodge} \cap F^2_{con} = 0$ (and (1.1) holds) (i.e. in the "ordinary" case), we can say more : we know [15, 3.13] that the F-crystal $(H^2_{cris}(X/W), F^*)$ is then a direct sum of twists of unit root crystals, and hence $H^2_{cris}(X/W)^{F=p} \otimes W$ is a direct summand of $H^2_{cris}(X/W)$. Thus, the maps :

$$H^2(X_{fl},\mu_p) \otimes k \to H^2_{DR}(X/k)$$

and $\quad \text{Pic}(X) \otimes k \to H^2_{DR}(X/k)$, and even $\quad \text{Pic}(X) \otimes k \to H^1(X,\Omega^1_{X/k})$

are injective. In the supersingular case, by contrast, these maps are not injective (in fact we shall see that their kernels classify supersingular K3 crystals). □

1.10 Example. The most extreme form of supersingularity in degree two occurs when the Hodge and conjugate filtrations coincide ; I like to call this case "superspecial". If X is superspecial (and satisfies (1.1)), then the natural map : $W \otimes H^2(X_{fl},\mathbb{Z}_p(1)) \to H^2_{cris}(X,\underline{J}_{X/W})$ is an isomorphism, and if Tate's conjecture is satisfied then the same is true with NS(X) in place of $H^2(X_{fl},\mathbb{Z}_p(1))$. To prove this, we use Mazur's theorem [4, 8.26] which implies that when X is superspecial, $H^2_{cris}(X/W,\underline{J}_{X/W})$ is stable under $p^{-1}F^*$. In fact, since the slopes of the latter are all zero, $p^{-1}F^*$ induces an automorphism of this space, and hence it is spanned by its fixed vectors. Notice, for example, that this applies to the product of two supersingular elliptic curves. □

We will apply the above results to study the problem of prolonging an invertible sheaf in a family. In this context it is convenient to give ourselves the following version of assumption (1.1) :

1.11 <u>Assumption</u>. If $X \xrightarrow{f} T$ is a smooth proper family of (possibly formal) schemes, assume :

1.11.1 The Hodge groups $R^q f_* \Omega^p_{X/T}$ are locally free $\mathcal{O}_T$-modules.

1.11.2 The (relative) Hodge to de Rham spectral sequence degenerates at E_1.

In what follows, we shall take T to be affine, for simplicity of notation. First we recall that classical obstruction theory tells us that if $S \subseteq T$ is defined by a square zero ideal I, and if L is a line bundle on $X_S = X \times_T S$, then the obstruction $o_T(L)$ to prolonging L to X lies in $H^2(X_S, \mathcal{O}_{X_S}) \otimes I \cong H^2(X, f^*(I))$: $o_T(L)$ is simply the image of L under the natural coboundary arising from the exact sequence :

1.12.1
$$o \to f^*(I) \xrightarrow{\epsilon} \mathcal{O}_X^* \to \mathcal{O}_{X_S}^* \to o,$$

where $\epsilon(\alpha) = 1 + \alpha$.

Next we recall Deligne's generalization and crystalline interpretation. Instead of assuming $I^2 = 0$, suppose instead that I admits a nilpotent PD structure γ, and use γ to define an exact sequence :

1.12.2
$$o \longrightarrow f^*(I) \xrightarrow{\epsilon_\gamma} \mathcal{O}_X^* \to \mathcal{O}_{X_S}^* \longrightarrow o$$

where $\epsilon_\gamma(\alpha) = \sum_{o}^{\infty} \gamma_n(\alpha)$. Then the coboundary of L is an element $o_{T,\gamma}(L)$ of $H^2(X, f^*(I))$, which can be identified in the following way : The crystalline Chern class of L gives us a global section of $R^2 f_{S\,cris\,*} \mathcal{O}_{X_S/\mathbb{Z}_p}$ on $(S_{cris}/\mathbb{Z}_p)$, and the PD structure γ enables us to evaluate $c_1(L)$ on the object (T, I, γ) of $\mathrm{Cris}(S/\mathbb{Z}_p)$. Furthermore, the lifting X of X_S provides us with an isomorphism : $(R^2 f_{S\,cris\,*} \mathcal{O}_{X_S/\mathbb{Z}_p})_{(T,I,\gamma)} \simeq H^2_{DR}(X/T)$, which is where we view $c_1(L)_{T,\gamma}$. Since

$c_1(L)_{T,\gamma}$, maps to the ordinary Chern class of L in $H^2_{DR}(X_S/S)$, which lies in the first level of the Hodge filtration, we see that the image of $c_1(L)_{T,\gamma}$ in $H^2(X,\mathcal{O}_X)$ in fact lies in $H^2(X,f^*I))$. It is an enormous tautology that this image is simply $\mathcal{O}_{T,\gamma}(L)$ [8].

As a corollary of the above, we see :

1.12 Proposition (Deligne). With the notations above, L extends to X iff its crystalline Chern class $c_1(L) \in H^2_{cris}(X_S/T) \cong H^2_{DR}(X/T)$ lies in F^1_{Hodge}. □

After applying this yoga step-by-step, one can deduce :

1.13 Corollary (Deligne-Illusie) [8]. Suppose $S = \mathrm{Spec}\ k$, $T = \mathrm{Spf}\ k[[t_1\ldots t_n]]$, and that the crystalline Chern class $c_1 \in H^2_{cris}(X_S/W)$ prolongs to a horizontal section of $H^2_{cris}(X/W[[t_1\ldots t_n]])$. Then L prolongs to X. □

If now X is smooth over a formal power series ring A, the obstruction to extending L from $X_o = X \times_A k$ to $X_n = X \times_A A/m^{n+1}$ can be made explicit in terms of the Kodaira-Spencer mapping, provided $n < p$. In that case the ideal $I = m/m^{n+1}$ of k in A/m^{n+1} can be endowed with the trivial PD structure γ (with $\gamma_p = 0$). For example, if $n = 1$, the reader can easily verify that the above gives the classical result :

1.14 Corollary. The obstruction $o(L) \in H^2(X_o,\mathcal{O}_{X_o}) \otimes m/m^2$ is simply the cup product of the Hodge Chern class $\pi_{Hodge}c_1(L)$ of L with the Kodaira-Spencer class $\tau \in H^1(X_o,T^1_{X_o/k}) \otimes m/m^2$.

In particular, if $c_1(L)$ lies in F^2_{Hodge}, this obstruction vanishes. Here is a nice formula for the second order obstruction in this case.

1.15 Corollary. If $c_1(L)$ lies in F^2_{Hodge}, and if $p > 2$, then the obstruction to extending L to X_2 is given by the image of $2.c_1(L)$ under the "square" of

Kodaira-Spencer :

$$F^2_{Hodge}H^2_{DR}(X_o/k) \to gr^1_F H^1_{DR}(X_o/k) \otimes m/m^2 \to gr^0_F H^2_{DR}(X_o, \mathcal{O}_{X_o}) \otimes m/m^2 \otimes m/m^2$$
$$\downarrow$$
$$H^2(X_o, \mathcal{O}_{X_o}) \otimes m^2/m^3 \ .$$

Proof. This works because any crystal on $(\underline{\text{Spec}}\, k/k)$ is constant : If H' is such a crystal and if (B, I, γ) is an object of $\text{Cris}(\underline{\text{Spec}}\, k/k)$, then the value H'_B of H' on B is simply $H'_k \underset{k}{\otimes} B$. Now let H be the crystal on $(\underline{\text{Spec}}\, A/k)_{cris}$ coming from the de Rham cohomology $H_{DR}(X/A)$ together with its Gauss-Manin connection ∇, and let H' be its restriction to $(\underline{\text{Spec}}\, k/k)_{cris}$. If our B is also an A-algebra, we also know that $H'_B = H_{cris}(X_o/B) \cong H_{DR}(X \underset{A}{\times} B/B)$, and there is a well-known formula for the isomorphism :

$$H_{DR}(X_o/k) \underset{k}{\otimes} B \cong H'_B \cong H_{DR}(X/A) \underset{A}{\otimes} B.$$

For notational clarity, I will write this out only in two variables, with $A \cong k[[X, Y]]$. If $h \in H_{DR}(X/A)$ is any lifting of $h_o \in H_{DR}(X_o/k)$,

$$\epsilon(h_o \otimes 1) = (1 - \partial_X + \gamma_2(X)\partial_X^2 - \gamma_3(X)\partial_X^3 + \ldots)(1 - \partial_Y + \gamma_2(Y)\partial_Y^2 - \ldots)h.$$

Apply this when h_o is a Chern class lying in $F^2H^2_{DR}(X/k)$, and $B = A/m^3$. Choose a lifting $h \in F^2H^2_{DR}(X/A)$ of h_o. Since we are taking γ to be trivial, $\gamma_n = 0$ if $n \geq 3$. Moreover, we are only interested in the image of $\epsilon(h_o \otimes 1) \bmod F^1$, and so by Griffiths transversality, we can neglect $\partial_X h$, $\partial_Y h$, and h. We are left with :

$$\epsilon(h_o \otimes 1) = \frac{1}{2} X^2 \partial_X^2(h) + XY\, \partial_X(\partial_Y(h)) + \frac{1}{2} Y^2\, \partial_Y^2(h)$$
$$= \frac{1}{2} (X^2 \partial_X^2(h) + XY\, \partial_X \partial_Y(h) + XY\, \partial_Y \partial_X(h) + Y^2 \partial_Y^2(h)).$$

Since the Kodaira-Spencer map is simply the graded map associated to $X\partial_X + Y\partial_Y$ (which is linear), the corollary is clear. □

We end this section with a remark concerning the behavior of p-divisibility of line bundle under specialization. Artin's work on supersingular K3 surfaces [2] (to which we shall return) shows that a line bundle can become a p^{th} power when specialized. The next result shows that this cannot happen for *ordinary* varieties.

1.16 *Proposition*. *Suppose that* $f : X \to T$ *satisfies* (1.11), *and that for some closed point* $t \in T$, $H(X_t/k)$ *is ordinary*. *Then if* $\bar{\tau}$ *is a geometric generic point specializing to* t, *the specialization map* : $NS(X_{\bar{\tau}}) \otimes \mathbb{Z}/p\mathbb{Z} \to NS(X_t) \otimes \mathbb{Z}/p\mathbb{Z}$ *is injective*.

Proof. After localizing, we may assume that $H^2_{DR}(X/T)$ is ordinary. Then in particular the inverse Cartier operator induces an isomorphism :

$$\begin{array}{ccc} F_T^* H^1(X, \Omega^1_{X/T}) & \xrightarrow{\tilde{\varphi}} & H^1(X, \Omega^1_{X/T}) \\ C^{-1} \quad \downarrow \cong & & \uparrow \cong \\ F^1_{con}/F^2_{con} & \xrightarrow{\text{proj}} & F^1_{Hodge}/F^2_{Hodge} \end{array}$$

If $L \in NS(X)$, its Hodge Chern class $\xi \in H^1(X, \Omega^1_{X/T})$ is fixed by φ. Hence if L_1 is divisible by p, $\xi \in \cap\, m_t^{(p^i)} H^1(X, \Omega^1_{X/T}) = 0$. But then $\xi_{\bar{\tau}} = 0$ as well, and (1.9) implies that L is divisible by p in $NS(X_{\bar{\tau}})$. The proposition follows. □

§2. VERSAL DEFORMATIONS OF POLARIZED K3 SURFACES.

In this section we apply the results of §1 to K3 surfaces in characteristic $p > 0$. The "superspecial" K3 surfaces play an exceptional role ; note that a K3 surface is superspecial iff $F^2_{con} \cap F^2_{Hodge} \neq \{0\}$, i.e. iff $F^{\cdot}_{con} = F^{\cdot}_{Hodge}$. It is easy to see that, in characteristic $p > 2$, the Kummer surface associated to a product of supersingular elliptic curves is superspecial.

Let X_o/k be a K3 surface. Since X_o has no tangent vector fields, it satisfies hypothesis (1.1). Moreover, the versal formal k-deformation X/S of X_o lies over $S = \underline{\mathrm{Spf}}\ k[[t_1 \ldots t_{20}]]$ and satisfies (1.11). The mappings
$\nabla^{[2]} : T^1_{S/k} \to \mathrm{Hom}[gr^2_F H^2_{DR}(X/S), gr^1_F H^2_{DR}(X/S)]$ and
$\nabla^{[1]} : T^1_{S/k} \to \mathrm{Hom}[gr^1_F H^2_{DR}(X/S), gr^o_F H^2_{DR}(X/S)]$ induced by the Gauss-Manin connection ∇ are isomorphisms, and for any $D \in T^1_{S/k}$, $\nabla^{[2]}(D)$ is the negative transpose of $\nabla^{[1]}(D)$. For computational purposes, it will be convenient to choose a basis ω of $H^o(X, \Omega^2_{X/S})$; then ∇ composed with cup product with ω induces an isomorphism :

2.1.1 $\qquad \rho_\omega : H^1(X, \Omega^1_{X/S}) \to \Omega^1_{S/k}.$

Evaluating this at zero, we view it as an isomorphism :

2.1.2 $\qquad \rho_\omega : H^1(X_o, \Omega^1_{X_o/k}) \to m/m^2$

where m is the maximal ideal of the closed point of S. If $\alpha \in H^1(X, \Omega^1_{X/S})$, to compute $\rho_\omega(\alpha)$, choose a lifting $\alpha' \in F^1H^2_{DR}(X/S)$ of α. Then $\rho_\omega(\alpha)$ is just $<\nabla\alpha', \omega> = -<\alpha', \nabla\omega>$, (since $<\alpha', \omega> = 0$).

Let L_o be a line bundle on X_o, and recall from [8] that there is a maximal closed formal subscheme $\Sigma(L_o)$ over which L_o can be prolonged. Moreover $\Sigma(L_o)$ is defined by a single equation, hence has codimension zero or one.

2.2 Proposition. Suppose L_o is not a p^{th} power. Then :

2.2.1 $\Sigma(L_o)$ <u>is smooth of codimension one unless</u> $c_1(L_o) \in F^2_{Hodge}H^2_{DR}(X_o/k)$, <u>and this cannot happen unless</u> X_o <u>is superspecial</u>.

2.2.2 <u>If</u> X_o <u>is superspecial and</u> $c_1(L_o) \in F^2H^2_{DR}(X_o/k)$, $\Sigma(L_o)$ <u>has an ordinary quadratic singularity</u> (characteristic $\neq 2$).

<u>Proof.</u> The obstruction theory (1.14) tells us that :

2.2.3 The ideal of $\Sigma(L_o)$ mod m^2 is generated by $\rho_\omega\, \pi_{Hodge}(c_1(L_o)) \in m/m^2$.

Thus, if $c_1(L_o) \notin F^2H^2_{DR}(X_o/k)$, this ideal is not contained in m^2, and since it is principal, $\Sigma(L_o)$ is smooth. Moreover, (1.4) tells us that if $c_1(L_o) \in F^2_{Hodge}H^2_{DR}(X_o/k)$, then it also lies in $F^2_{con}H^2_{DR}(X_o/k)$; since it is nonzero, X_o is superspecial. Moreover, in this case $c_1(L_o)$ forms a <u>basis</u> for F^2_{Hodge}, and we can take $\omega = c_1(L_o)$. In order to be as explicit as possible, let us also choose a basis for $H^1(X_o, \Omega^1_{X_o/k})$. Since the cup product pairing on this space is nondegenerate, we can choose the basis $(\xi_1 \ldots \xi_{10}, \eta_1 \ldots \eta_{10})$ such that $<\xi_i, \eta_i> = 1$ and all other products are zero. The isomorphism $H^1(X_o, \Omega^1_{X_o/k}) \to m/m^2$ then furnishes us with a basis $s_1 \ldots s_{10}$, $t_1 \ldots t_{10}$ for m/m^2, hence with a system of coordinates for A : If $\zeta \in H^2(X_o, \mathcal{O}_{X_o})$ is the dual basis to ω, and if we lift everything to $H^2_{DR}(X/A)$, we have : $\nabla\xi_i = ds_i \otimes \zeta$, $\nabla\eta_i = dt_i \otimes \zeta$. From the fact that F^2 is the annihilator of F^1, and since $< , >$ is horizontal, we find : $\nabla\omega = -\sum ds_i \otimes \eta_i - \sum dt_i \otimes \xi_i$. Thus, $\rho(\omega) = -\sum s_i \otimes \eta_i - \sum t_i \otimes \xi_i$, and $\rho^2(\omega) = -2\sum s_i t_i$. By (1.15), we see that the equation for $\Sigma(L_o)$ is precisely $\sum s_i t_i$ mod m^3. Notice that after another change of coordinates, we can even assume that the equation is $\sum s_i t_i$. □

This allows us to improve slightly on a result of Deligne :

2.3 <u>Corollary</u>. <u>Any nonsuperspecial</u> K3 <u>surface over</u> k <u>can be lifted to</u> W(k). <u>If</u> $p > 2$, <u>any</u> K3 <u>can be lifted to</u> $W[\sqrt{p}]$.

Proof. The versal W-deformation of a K3 lies over $W[[X_1 \ldots X_{20}]]$. Let L_o be an ample primitive bundle on X_o; then over $\Sigma(L_o) \subseteq \operatorname{Spec} W[[X_1 \ldots X_{20}]]$ we have an honest K3 surface. If X_o is not superspecial, $\Sigma(L_o)$ is smooth, and we can obviously find a W-valued point of $\Sigma(L_o)$ extending the given k-valued point at the origin. Otherwise, the equation for $\Sigma(L_o)$ has the form : $-s_1t_1 + \ldots s_{10}t_{10} + pg$ for suitable coordinates s and t. If $\pi^2 = p$, we have to find elements σ_i, τ_i of $W[\pi]$ such that $(\pi\sigma_i, \pi\tau_i)$ satisfy this equation, i.e. such that $\sigma_1\tau_1 + \ldots \sigma_{10}\tau_{10} + g(\pi\sigma, \pi\tau) = 0$. Mod π, solve these equations with (say) $\sigma_1 = 1$. Then by Hensel's lemma, they can be solved in $W[\pi]$. □

2.4 Remark. We shall see in section 7 that if Tate's conjecture is verified, there is only one superspecial K3, and it can be lifted to W.

2.5 Corollary. *If $p > 2$ or if X_o is not superspecial, the map $\operatorname{Aut}(X_o) \to \operatorname{Aut} H^2_{cris}(X_o/W)$ is injective.*

Proof. Let $\pi = p$ unless $p > 2$ and X_o is superspecial in which case let $\pi = \sqrt{p}$. Choose a lifting X of X_o to $R = W[\pi]$. Since the ramification of R is less than p, (π) has a PD structure γ, and hence we have a canonical isomorphism : $H^2_{cris}(X_o/W) \otimes_W R \cong H^2_{cris}(X_o/R) \cong H^2_{DR}(X/R)$. Local Torelli for K3's implies that any automorphism of X_o which is compatible with the Hodge filtration $F^{\cdot}_X H^2_{DR}(X/R)$ lifts to X. (This follows, for example, from [8], or [6].) Of course if $\alpha_o \in \operatorname{Aut}(X_o)$ acts as the identity on $H^2_{cris}(X_o/W)$, it preserves any filtration, hence lifts to an automorphism α of X. Since α acts as the identity on $H^2_{DR}(X/R)$, α is the identity in characteristic zero, by [18, §2, Prop. 2] and hence is the identity over R as well. □

We now look at the singularities of the nonordinary locus of a versal family X/S of K3 surfaces. We recall the definition : The absolute Frobenius endomorphism F_X of X induces an F_S^*-linear endomorphism of $H^2(X,\mathcal{O}_X)$, hence an $\mathcal{O}_S$-linear map : $F_S^* H^2(X,\mathcal{O}_X) \to H^2(X,\mathcal{O}_X)$. Since $H^2(X,\mathcal{O}_X)$ is free of rank one, it is clear that the support of the cokernel of this map is (scheme theoretically) defined by a principal ideal (h). This support is the "nonordinary" locus.

2.6 Proposition. Suppose X_o is not ordinary. Then $V(h) \subseteq S$ is smooth of codimension one, unless X_o is superspecial. In this case, if $p > 2$, $V(h)$ has an ordinary quadratic singularity.

Proof. Recall that (as a consequence of (1.1)) the Frobenius map $F_S^* H^2_{DR}(X/S) \to H^2_{DR}(X/S)$ factors through an isomorphism $F_S^* H^2(X,\mathcal{O}_X) \to F^2_{con} H^2_{DR}(X/S)$. Choose a basis ω for $H^o(X,\Omega^2_{X/S})$, let ζ be the dual basis for $H^2(X,\mathcal{O}_X)$, and let $\alpha = F^*(\zeta)$ be the induced basis for $F^2_{con} H^2_{DR}(X/S)$. It is clear that $<\omega,\alpha> = h$ is an equation for the nonordinary locus. (In particular, X_o is nonordinary iff $F^2_{con}(0) \subseteq F^1_{Hodge}(0)$ iff $F^1_{con}(0) \supseteq F^2_{Hodge}(0)$.) Moreover, α is horizontal, so $dh = <\nabla\omega,\alpha>$. Thus, if X_o is not ordinary, h lies in m, and via the isomorphism ρ_ω (2.1.2), we see that $h \pmod{m^2}$ is $-\rho_\omega(\alpha(0))$. In particular, $h \in m^2$ iff $\alpha(0) \in F^2_{Hodge} H^2_{DR}(X_o/k)$, i.e. iff X_o is superspecial. This tells us that if X_o is not superspecial, $V(h)$ is smooth of codimension one. Moreover, the tangent space to $V(h)$ becomes identified, via the dual of ρ_ω, with $F^1_{Hodge} \cap F^1_{con}/F^2_{Hodge}$.

Now suppose $p > 2$ and X_o is superspecial. Choose a basis $(\omega, \xi_i, \eta_i, \zeta)$ for $H^2_{DR}(X/S)$ adapted to the Hodge filtration, and such that $<\xi_i,\eta_i> = 1$, $<\omega,\rho> = 1$, and the others equal zero. Let $m/m^3 \subseteq A_2 = A/m^3$ have the trivial PD structure, and prolong $\omega(0)$, $\xi_i(0)$, $\eta_i(0)$, $\zeta(0)$ to a horizontal basis for $H^2_{DR}(X/S) \otimes_A A_2$, using γ. Call the new basis α, β_i, γ_i, δ, and note that since $F^{\cdot}_{con}(0) = F^{\cdot}_{Hodge}(0)$ and $F^{\cdot}_{con}$ is horizontal, this basis is adapted to the conjugate filtration.

Moreover, since the cup product is horizontal, the intersection matrix in this basis is the same as in the original one. In particular, $h = <\omega,\alpha>$ is the coefficient of δ in an expansion $\omega = u\alpha + \sum f_i\beta_i + \sum g_i\gamma_i + h\delta$ of ω. It is clear that the f_i's and g_i's lie in m, h lies in m^2, and u is a unit. Since this basis is horizontal, $\nabla\omega$ is just $\sum df_i \otimes \beta_i + \sum dg_i \otimes \gamma_i \bmod m + F^2$, and it follows that (f_i, g_i) form coordinates for A_2. Now use the fact that $<\omega,\omega> = 0$, and find $0 = 2(uh + \sum f_i g_i)$. In other words, there exist coordinates $s_1 \ldots s_{10}$, $t_1 \ldots t_{10}$ for A such that the ideal of $V(h)$ is generated by $\sum s_i t_i \bmod m^3$. This proves that $V(h)$ has an ordinary quadratic singularity, and (since $h \neq 0$) that $V(h)$ has codimension one again. □

2.7 Remark. A K3 surface is superspecial iff $F^\cdot = F^\cdot_{con}$; this makes sense infinitesimally also. However, since the conjugate filtration is horizontal, it is clear (from local Torelli) that any infinitesimal family of superspecial K3's is trivial. □

2.8 Remark. The above result shows that $V(h) \subseteq S$ is of codimension one (i.e. that $V(h) \neq S$) except when $p=2$ and X_o is superspecial. To treat this and similar cases in which precise local calculations seem out of reach, the following principle is often useful : Suppose that S/k is smooth (of finite type now), that (H,∇) is a coherent locally free $\mathcal{O}_S$-module with integrable connection, and that $F \subseteq H$ is a local direct summand which is "modular" : i.e. the connection induces an injection : $T^1_{S/k} \to \mathrm{Hom}[F, H/F]$. Then the dimension of S is less than or equal to $\mathrm{rank}(F)\,\mathrm{rank}(H/F)$. We will apply this in the following situation : Suppose there also exists a local direct summand $N \subseteq H$ which is horizontal. It is clear that there is a largest closed subscheme $\Sigma(F,N) \subseteq S$ on which $F \subseteq N$ (take the ideal generated by matrix coefficients of the map $F \to H(N)$). Then the dimension of $\Sigma(F,N)$ is necessarily less than or equal to $\mathrm{rank}(F)[\mathrm{rank}(N) - \mathrm{rank}(F)]$. □

2.9 Theorem. Let $(X/T, H)$ be a versal k-deformation of a polarized K3 surface (X_o, H_o), with $(H_o) \subseteq \mathrm{Pic}(X_o)$ a direct summand. Then the geometric generic fiber $X_{\bar\tau}$ is ordinary, and $\mathrm{Pic}(X_{\bar\tau})$ is generated by $H_{\bar\tau}$.

Proof. We know that $c_1(H_o)$ is not zero in $F^1H^2_{DR}(X_o/k)$, and this remains true on an open set. Let $H^2_{prim}(X_o/k)$ be the annihilator of $c_1(H_o)$ under cup product ; this contains $c_1(H_o)$ iff $H_o.H_o$ is divisible by p. Versality tells us that we have an isomorphism :

$$T^1_{T/k}(0) \to \mathrm{Hom}[H^o(X_o, \Omega^2_{X_o/k}), H^1_{prim}(X_o, \Omega^1_{X_o/k})] .$$

After replacing T by an open neighborhood of the origin, we may assume that (X/T,H) is a versal deformation of (X_t, H_t) for every $t \in T$, and we may also assume that $H_t \subseteq \mathrm{Pic}(X_t)$ is a direct summand for every such t. Then we can replace the origin by any other closed point, and hence throughout the proof we can replace T by any nonempty étale T'/T. In particular, we may assume that T is smooth. Its dimension is nineteen or (so far as we know now) possibly twenty.

The Gauss-Manin connection induces an injection :

$$T^1_{T/k} \to \mathrm{Hom}[F^2 H^2_{DR}(X/T), H^2_{DR}(X/T)/F^2H^2_{prim}(X/T)] .$$

Apply remark (2.8) with $F = F^2_{Hodge}$ and $N = F^2_{con}$, and conclude that the set of superspecial points has dimension zero. Deleting these points, we see by (2.1) that T is smooth of dimension 19. Moreover, $c_1(H_t) \notin F^2_{con}(t)$ for every t, by (1.5), and hence $F^2_{con} + \mathcal{O}_T \otimes c_1(H)$ is a local direct summand of $H^2_{DR}(X/T)$. Since it is also horizontal, we can again apply our remark, with $F = F^2_{Hodge}$ and $N = F^2_{con} + \mathcal{O}_T \otimes c_1(H)$. We find that the set of points with $F^2_{Hodge}(t) \subseteq F^2_{con}(t) + k \otimes c_1(H_t)$ has dimension ≤ 1, and hence we can delete this set also.

Now consider the nonordinary locus $V \subseteq T$; if $t \in V$, the tangent space to V at t can be identified with $\mathrm{Hom}[F^2_{Hodge}(t), (F^1_{con}(t) \cap F^1_{prim}(t))/F^2_{Hodge}(t)]$. But notice : $F^1_{prim}(t)$ cannot be contained in $F^1_{con}(t)$; for otherwise we would have $F^2_{con}(t) \subseteq F^2_{Hodge}(t) + k \otimes c_1(H_t)$, hence either $F^2_{con}(t) \subseteq k \otimes c_1(H_t)$ or $F^2_{Hodge}(t) \subseteq F^2_{con}(t) + k \otimes c_1(H_t)$ - both of which we have ruled out. This tells us that V is smooth of dimension 18 - and it too can be deleted.

We are now in the following situation : $f : X \to T$ is a smooth family of ordinary polarized K3 surfaces, versal at every point t of T. Then the map induced by Kodaira-Spencer :

$$H^1(X_t, \Omega^1_{X_t/k}) / \pi(c_1(H_t)) \otimes k \to m_t/m_t^2 \otimes H^2(X_t, \mathcal{O}_{X_t})$$

is an isomorphism for every point, and hence

$$H^1(X, \Omega^1_{X/T}) / \pi c_1(H) \otimes \mathcal{O}_T \to \Omega^1_{T/k} \otimes H^2(X, \mathcal{O}_X)$$

is also an isomorphism. This remains true if we replace T by $\operatorname{Spec} k(\tau)$, where τ is the generic point, or by $\operatorname{Spec} k(\tau')$, for any separable extension $k(\tau')$ of $k(\tau)$. Since $H^1(X, \mathcal{O}_X) = 0$, the Picard scheme of $X_\tau/k(\tau)$ is unramified, and hence after some separable extension, we may assume $\operatorname{Pic}(X_\tau) = \operatorname{Pic}(X_{\bar\tau})$. But it is clear that $\operatorname{Im}(\operatorname{Pic}(X_\tau)) \otimes k(\tau)$ forms a horizontal subspace of $H^2_{DR}(X_\tau/k(\tau))$, hence is killed by the above map. Counting dimensions, we see that $\operatorname{Im}(\operatorname{Pic}(X_\tau) \otimes k(\tau) \to H^1(X_\tau, \Omega^1_{X_\tau}))$ has dimension one, and hence the same is true over $k(\bar\tau)$. But since $X_{\bar\tau}$ is ordinary, the map is injective (1.9). Since $(H_{\bar\tau})$ is a direct summand of $\operatorname{Pic}(X_{\bar\tau})$, it must generate it. □

§3. THE CLASSIFICATION OF SUPERSINGULAR K3 CRYSTALS.

This section is devoted to an explicit classification of the F-crystals that could conceivably occur as the crystalline cohomology of a supersingular K3 surface. This classification gives computational meaning to the conjectured Torelli theorem (0.1), and it also enables us to construct the "period space" which puts the crystals together. For the time being, however, we work purely punctually, over an algebraically closed field k of characteristic $p > 2$.

3.1 Definition. A "K3 crystal of rank n over k" is a free W(k)-module H of rank n, endowed with a Frobenius linear endomorphism $\Phi : H \to H$ and a symmetric bilinear form $< , >_H : H \otimes H \to W$, satisfying :

a) $p^2 H \subseteq \mathrm{Im}(\Phi)$.

b) $\Phi \otimes \mathrm{id}_k$ has rank one.

c) $< , >_H$ is perfect.

d) $< \Phi X, \Phi Y >_H = p^2 F_W^* < X, Y >_H$.

In the language of F-crystals, a) says that (H, Φ) has "level" or "weight" 2 ; it is equivalent to the existence of a $V : H \to H$ such that $\Phi \circ V = V \circ \Phi = p^2$. Property b) says that the Hodge number h^0 is one. By definition, c) means that the associated linear map $\beta_H : H \to \mathrm{Hom}_W[H,W] = H^\vee$ is an isomorphism. The last property is simply the compatibility of duality with the F-crystal structure. It is easy to verify that the associated filtrations $F^\bullet_{Hodge}$ and $F^\bullet_{con}$ on $H \otimes k$ [15] are autodual : $\mathrm{Ann}(F^i) = F^{2-i}$. By Mazur's theorem [4,8.26], the crystalline cohomology of a surface with $p_g = 1$ satisfying (1.1) is a K3 crystal.

A morphism of K3 crystals is a W-linear map compatible with Φ and $<,>$. Notice that any morphism between K3 crystals of the same rank is an isomorphism. Two K3 crystals are said to be "isogenous" iff there is a map $H \otimes \mathbb{Q} \to H' \otimes \mathbb{Q}$ compatible with Φ and $< , >$ in the obvious sense.

Recall that the isogeny class of the pair (H,Φ) (forgetting $<,>_H$) is determined by its Newton polygon [12]. We shall say that (H,Φ) is "supersingular" iff all its slopes are one. Our object is to classify all supersingular K3 crystals up to isomorphism.

3.2 Definition. The "Tate module" T_H of a K3 crystal H is the $\mathbb{Z}_p$-module given by :

$$T_H = \{x \in H : \Phi x = px\}.$$

Roughly speaking, here is how the classification of supersingular K3 crystals works : First of all, T_H inherits a bilinear form $<,>_T : T_H \otimes T_H \to \mathbb{Z}_p$ (which is no longer perfect). The isogeny class of this form determines the isogeny class of H. Furthermore, only two isogeny classes can occur, and the isogeny class cannot change in a family. One additional numerical invariant σ_o determines the isomorphism class of $<,>_T$; this σ_o can decrease with specialization. The isomorphism class of H is then determined as follows : The dual T_H^* inherits a (twisted) bilinear form $<,>^*$, and the form on H induces a map $H \to T_H^* \otimes W$. It turns out that the image of H in $T_H^* \otimes k$ is a maximal isotropic subspace which lies in a "special position", and the set of all such spaces classify all supersingular K3 crystals with given T up to isomorphism.

Here are precise statements of the results. The proofs will be given later.

Recall from [21, IV] the invariants classifying a quadratic form over $\mathbb{Q}_p$: its rank $\in \mathbb{N}$, its Hasse invariant $e \in \{\pm 1\}$, and its discriminant

$$d \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z} \times \mathbb{F}_p^*/\mathbb{F}_p^{*2} \xrightarrow{\sim} \{\pm 1\} \times \{\pm 1\}.$$

We will denote the latter isomorphism as follows : If $x \in \mathbb{Q}_p^*$, write $(-1)^{\mathrm{ord}_p(x)}$ to keep track of the first factor, and $(\frac{\bar{x}}{p})$ for the second, where $\bar{x}$ is the reduction mod p of $p^{-\mathrm{ord}_p(x)}x$, and $(\frac{-}{p})$ is the Legendre symbol.

3.3 Theorem. The Tate module T_H of a supersingular K3 crystal is free of rank n, and its bilinear form is nondegenerate. Its isogeny invariants are as follows : $(-1)^{\mathrm{ord}_p(d)} = +1$, $e = -1$, and $(\frac{\bar{d}}{p}) = \pm 1$. A supersingular K3 crystals of rank n is determined up to isogeny by $(\frac{\bar{d}}{p})$.

3.4 Theorem. Let d be the discriminant of $< , >_T$, computed in any basis, and let $\mathrm{ord}_p(d) = 2\sigma_o$. Then $(T, < , >_T)$ is determined up to isomorphism by σ_o and $(\frac{\bar{d}}{p})$. More precisely, there is an orthogonal decomposition :

$$(T, < , >_T) = (T_o, p< , >_{T_o}) \oplus (T_1, < , >_{T_1})$$

where $< , >_{T_o}$ and $< , >_{T_1}$ are perfect forms of rank $2\sigma_o$ and σ_1, respectively, and with discriminants given by :

$$(\frac{\bar{d}_o}{p}) = -(\frac{-1}{p})^{\sigma_o}, \quad (\frac{\bar{d}_1}{p}) = -(\frac{\bar{d}}{p})(\frac{-1}{p})^{\sigma_o}.$$

3.5 Theorem. H is determined up to isomorphism by the kernel $\bar{H}$ of $T \otimes k \to H \otimes k$. Moreover :

3.5.1 $\bar{H}$ is a totally isotropic subspace of $T_o \otimes k$ of dimension σ_o.

3.5.2 The dimension of $\bar{H} + (\mathrm{id}_{T_o} \otimes F_k^*)\bar{H}$ is $\sigma_o + 1$.

3.5.3 There are no $\mathbb{F}_p$-rational subspaces of $T_o \otimes k$ between $\bar{H}$ and $T_o \otimes k$ thus, $T_o \otimes \mathbb{F}_p \to H \otimes k$ is injective.

3.5.4 Every $\bar{H}$ satisfying the above conditions corresponds to a K3 crystal.

We begin the proof of the above assertions (as well as some more precise ones) with some estimates concerning the Tate module of a K3 crystal. For generalizations of these estimates, we refer the reader to Katz's article [11] in these proceedings.

3.6 Lemma. Let (H, Φ) be an F-crystal over k with $h^o = 1$. The following are equivalent :

a) Φ^n is divisible by p^{n-1}.

b) The slopes of Φ are all $\geq 1 - 1/n$.

Proof. It is clear that a) implies b) ; we prove the converse by induction on n. If $n = 1$, there is nothing to prove, so we may assume $n \geq 2$. Since the slopes of Φ are $\geq 1 - 1/n \geq 1 - 1/n-1$, the induction hypothesis allows us to write $\Phi^{n-1} = p^{n-2}\psi$ for some $\psi : H \to H$. The slopes of ψ are $\geq (n-1)(1-1/n) - (n-2) = 1/n > 0$, and hence ψ has no unit root part. The reduction ψ_o of ψ mod p is therefore nilpotent. Since Φ and ψ commute, the image of Φ_o is ψ_o-invariant, and since this image is one dimensional, ψ_o is zero on Im Φ_o. This tells us that $\psi \circ \Phi$ is divisible by p, i.e. that Φ^n is divisible by p^{n-1}. □

3.7 Definition. If (H,Φ) is an F-crystal on k, "E_H" $= \{x \in H: \Phi^n x \in p^n H$ for all $n \geq 0\}$, and "L_H" $= \sum_n p^{-n}\Phi^n H$.

It is clear that $E_H \subseteq H$ is the largest submodule on which Φ is divisible by p, and that $L_H \subseteq H \otimes Q$ is the smallest submodule containing H on which Φ is divisible by p.

3.8 Corollary. If (H,Φ) has $h^0 = 1$ and all slopes ≥ 1, then $pH \subseteq pL_H \subseteq E_H \subseteq H$.

Proof. We know from the lemma that $\Phi^n H \subseteq p^{n-1} H$ for all n, and hence $pL_H \subseteq H$. But then pL_H is a submodule of H on which the action of Φ is divisible by p, whence $pL_H \subseteq E_H$. □

3.9 Corollary. Let (H,Φ) be an F-crystal with $h^0 = 1$ and all slopes $= 1$. Then the natural map : $(E_H, \Phi_E) \to (H, \Phi_H)$ is an isogeny of F-crystals, and the natural map $(T_H \otimes W, p \otimes F_W) \to (E_H, \Phi_E)$ is an isomorphism of F-crystals.

Proof. The first statement follows from the previous result. It implies that Φ_E has all slopes one, hence that $p^{-1}\Phi_E$ has all slopes zero - i.e. is a unit root crystal. Such a crystal is spanned by its Tate module, [10, 5.5] and the corollary follows. □

Of course, the above result is true without the hypothesis $h^o = 1$. [12]

From now on, H will denote a supersingular K3 crystal. Of course, the arrows in the above corollary are compatible with the natural dualities on H, on E_H, and on T_H. The pairing $<\ ,\ >_H$ allows us to identify the dual $M^\vee = \mathrm{Hom}[M,N]$ of any W-lattice $M \subseteq H \otimes \mathbb{Q}$ with $\{x \in H \otimes Q : <x, y>_H \in W \text{ for all } y \in M\}$, in the obvious way. We make this identification without further comment.

3.10 <u>Lemma</u>. <u>With the above notations</u>, $E_H = L_H^\vee$ <u>and</u> $L_H^\vee = E_H$. <u>Moreover, the</u> k-<u>vector spaces</u> L_H/H <u>and</u> H/E_H <u>are naturally dual</u>, <u>and the images of</u> E_H <u>and</u> pL <u>in</u> $H \otimes k$ <u>are the annihilators of one another</u>.

<u>Proof</u>. If M is a submodule of H containing pH, then $M' = pM^\vee$ is another. Of course, the images of M' and of M in the (self-dual) vector space $H \otimes k$ are the annihilators of one another and $M'' = M$. Moreover, the W-dual of the exact sequence :

$$o \to M \to H \to H/M \to o \qquad \text{is}$$

$$o \to H \to M^\vee \to \mathrm{Ext}^1_W(H/M, W) \to o,$$

and the natural isomorphism $\mathrm{Ext}^1_W(H/M,W) \leftrightarrow \mathrm{Hom}_k(H/M,k)$ shows that $M^\vee/H$ and H/M are dual as k-vector spaces. Thus, the lemma reduces to the assertion that $E' = pL$.

To prove this, notice that if $\Phi M = pM$, then $\Phi M^\vee = pM^\vee$, and $\Phi M' = pM'$. Since $\Phi E = pE$, $\Phi E^\vee = pE^\vee$, and by minimality of L, $L \subseteq E^\vee$, hence $pL \subseteq E'$. Since also $\Phi L = pL$, $\Phi(pL) = p(pL)$, so $\Phi(pL)') = p(pL)'$, and by maximality of E, $(pL)' \subseteq E$. Then $E' \subseteq pL$, and the lemma is proved. □

3.11 <u>Corollary</u>. <u>The</u> p-<u>adic ordinal of the discriminant of the quadratic form</u> $<\ ,\ >$ <u>restricted to</u> E <u>is</u> $2\sigma_o$, <u>where</u>

$$\sigma_o = \dim L/H = \dim H/E = 1/2 \dim L/E \geq 1.$$

<u>Proof</u>. This ordinal is the length of the cokernel of the map $E \to E^\vee$, i.e. of

$E \to L$. This length is the sum of the lengths of H/E and L/H. Since Φ is not divisible by p, $E \neq H$, and $\sigma_0 \geq 1$. □

We now come to the key step in the classification.

3.12 Proposition. The form $< , >_H$ restricted to pL is divisible by p; let $< , >_L$ be the form on L obtained by dividing by p, i.e.:

$$<x,y>_L = p^{-1}<px,py>_H \quad \text{for} \quad x, y \in L. \quad \text{Then:}$$

3.12.1 The corresponding map $\beta_L : L \to L^\vee$ has cokernel killed by p, and the annihilator of the corresponding form on L/pL is E/pL.

3.12.2 The image $\bar{H}$ of H in L/E is a totally isotropic subspace of dimension σ_0.

3.12.3 Let φ denote the automorphism of L/E induced by $p^{-1}\Phi$. Then:

a) $\bar{H} + \varphi\bar{H}$ has dimension $\sigma_0 + 1$

b) $\sum \varphi^i \bar{H} = L/E$.

Proof. In the notation of the proof of (3.10), we have $E' = pL$, hence $(pL)' = E$. Thus $pL \subseteq E = (pL)' = p(pL)^\vee$, which says precisely that $< , >_H$ is divisible by p when restricted to pL. Since $pL^\vee = pE \subseteq pL$, if $f \in L^\vee$, $pf = \beta_H(py)$ for some $y \in L$, and then $pf = \beta_L(y)$, so $\operatorname{cok}(\beta_L)$ is killed by p. Now the annihilator of the form induced by $< , >_L$ on $L \otimes k$ is just the image of

$$\{x \in L : <x,y>_L \in pW \ \forall y \in L\} = \{x \in L : <px,py>_H \in p^2W \ \forall y \in L\}$$
$$= \{x \in L : <x,py>_H \in pW \ \forall y \in L\} = L \cap (pL)' = L \cap E = E.$$

This proves (3.12.1).

It is obvious from the definition of $< , >_L$ that $\bar{H}$ is totally isotropic, and we have already proved that $\bar{H}$ has dimension σ_0. This proves (3.12.2).

To prove (3.12.3), let $A^i H = \{x : \Phi x \in p^i H\}$, and recall that H/A^1H has dimension one. Now that map $p^{-1}\Phi : H \to L$ sends A^1H to H, and the induced map: $H/E \to L/H$ factors through H/A^1H. In fact, it is clear that $p^{-1}\Phi$ induces a bijection:

$$H/A^1H \xrightarrow{\simeq} \varphi(\overline{H})/\overline{H} \cap \varphi(\overline{H}) \subseteq L/E.$$

Since H/A^1H has dimension one, $\overline{H}+\varphi(\overline{H})$ has dimension σ_o+1. Finally, note that $L = \sum(p^{-1}\Phi)^i H$, so $L/E = \sum \varphi^i(H/E) = \sum \varphi^i \overline{H}$. □

We are now ready to compute the isomorphism type of the quadratic form $< , >_T : T_H \otimes T_H \to \mathbb{Z}_p$.

3.13 Proposition. The Tate module T of a supersingular K3 crystal satisfies :

3.13.1 The p-adic ordinal of its discriminant is $2\sigma_o$, with $\sigma_o \geq 1$.

3.13.2 Its Hasse invariant e is -1.

3.13.3 T admits an orthogonal decomposition :

$(T, < , >_T) \cong (T_o, p < , >_{T_o}) \oplus (T_1, < , >_{T_1})$, where $< , >_{T_o}$ and $< , >_{T_1}$ are perfect forms.

Proof. We have already proved the first statement in (3.11), because the p-adic ordinal of $< , >_T$ can be computed after tensoring with W. The third statement follows from the following lemma.

3.14 Lemma. A quadratic form $< , >: \Gamma \otimes \Gamma \to \mathbb{Z}_p$ admits an orthogonal decomposition (3.13.3) iff the cokernel of the corresponding linear map $\beta_\Gamma : \Gamma \to \Gamma^*$ is killed by p.

Proof. Suppose that $p\,\mathrm{cok}(\beta_\Gamma) = 0$; then $\Gamma/p\Gamma^* \cong (\Gamma \otimes \mathbb{F}_p)/\mathrm{Ann}(\Gamma \otimes \mathbb{F}_p)$, and we proceed by induction on the dimension of this vector space. If it's zero, $< , >_\Gamma$ is divisible by p and $p^{-1} < , >_\Gamma$ is necessarily a perfect pairing. If not, there exists an $x \in \Gamma$ with $<x,x>_\Gamma$ not divisible by p. Then if Γ' is the orthogonal complement of x, we have an orthogonal decomposition : $\Gamma \cong (x) \oplus \Gamma'$, and it is clear that the induction hypothesis applies to Γ'. This proves the nontrivial implication of the lemma. □

3.15 Lemma. If $(\Gamma, < , >_\Gamma)$ satisfies (3.13.1) and (3.13.3), the following are equivalent :

a) Γ has Hasse invariant -1.

b) $\Gamma_o \otimes \mathbb{F}_p$ is not neutral, i.e. admits no rational totally isotropic subspace of dimension σ_o.

c) $\left(\frac{d_o}{p}\right) = -\left(\frac{-1}{p}\right)^{\sigma_o}$.

Proof. There are just two isomorphism classes of quadratic forms of rank $2\sigma_o$ over $\mathbb{F}_p$, and they are classified by the discriminant $d_o \in \mathbb{F}_p^*/\mathbb{F}_p^{*2}$, i.e. by $\left(\frac{d_o}{p}\right) \in \{\pm 1\}$. For example, the neutral form of rank $2\sigma_o$ is a sum of σ_o hyperbolic planes and has $d_o = (-1)^{\sigma_o}$. This is the equivalence of (b) and (c).

To prove the equivalence of (a) and (c), we have to compute the Hasse invariant of Γ in terms of the decomposition (3.13.3). For this, the following two formulas are useful.

3.15.1 $e(\Gamma_1 \oplus \Gamma_2) = e(\Gamma_1)e(\Gamma_2)(d_1,d_2)$, where (d_1,d_2) is the Hilbert symbol of the discriminants of Γ_1 and Γ_2.

3.15.2 If $<\,,\,>_{\Gamma'} = p<\,,\,>_{\Gamma}$, then $e(\Gamma')=e(\Gamma)\left(\frac{-1}{p}\right)^{(r-1)\nu+\left[\frac{r}{2}\right]}\left(\frac{\bar{d}}{p}\right)^{r+1}$ where r is the rank of Γ, d is its discriminant, and $\nu = \mathrm{ord}_p(d)$.

These formulas are simple computational consequences of the definition of e and the bilinearity of the Hilbert symbol [21,III,IV]. In our special case, they become very simple : Let $<\,,\,>_{\Gamma_o'} = p<\,,\,>_{\Gamma_o}$; then $\mathrm{ord}_p(d_o') = 2\sigma_o$ is even and $\mathrm{ord}_p(d_1) = 0$, hence $(d_o',d_1) = e(\Gamma_1) = 1$ and $e(\Gamma_o' \oplus \Gamma_1) = e(\Gamma_o')$. Moreover, $e(\Gamma_o') = \left(\frac{-1}{p}\right)^{\sigma_o}\left(\frac{d_o}{p}\right)$, whence the equivalence of (a) and (c). □

In order to prove Proposition (3.13), we have only to observe that the existence of a totally isotropic subspace $\bar{H}$ of $T_o \otimes k$ of dimension σ_o such that $\bar{H} + (\mathrm{id}_{T_o} \otimes F_k^*)(\bar{H})$ has dimension $\sigma_o + 1$ implies that T_o is not neutral. Of course, this sort of thing is well known, but here is a proof : The family of all totally isotropic subspaces of dimension σ_o of $T_o \otimes k$ is the set of k-points of a smooth projective algebraic variety called Gen in [SGA7, XII,2.7]. This scheme is in fact defined over $\mathbb{F}_p$, and its Stein factorization is given by a morphism $e : \mathrm{Gen} \to Z$, where Z is the spectrum of an algebra of rank 2 over $\mathbb{F}_p$ [loc. cit. Prop. 2.8]. Moreover, if K and K' correspond to k-points of Gen, then $e(K) = e(K')$ iff $K+K'/K$ is even dimensional [loc. cit. Prop. 1.12] and hence $e(\bar{H}) \neq e(\mathrm{id} \otimes F_k^*)(\bar{H})$. This says that the action of $\mathrm{Gal}(k/\mathbb{F}_p)$ on $Z(k)$ is nontrivial. Since Z is a fortiori the spectrum of either $\mathbb{F}_p \times \mathbb{F}_p$ or of $\mathbb{F}_{p^2}$, it must be the latter, and so $Z(\mathbb{F}_p)$ is empty. □

3.16 Remark. The direct sum decomposition of (3.13.3) is not unique, but nonetheless the isomorphism classes of T_o and T_1 are determined by that of T. In fact, the isomorphism class of a perfect form over $\mathbb{Z}_p$ is determined by its reduction mod p, and $T_o \otimes \mathbb{F}_p$ and $T_1 \otimes \mathbb{F}_p$ are functorial in T. To see this, note that $T_1 \otimes \mathbb{F}_p \cong (T \otimes \mathbb{F}_p)/\mathrm{Ann}(T \otimes \mathbb{F}_p) \cong T/p\,T^*$, with the evident quadratic forms. Also, as an $\mathbb{F}_p$-vector space, $T_o \otimes \mathbb{F}_p \cong \mathrm{Ann}(T \otimes \mathbb{F}_p)$, and the form can be found as follows : The form $< , >_T$ restricted to $pT^* \subseteq T$ is divisible by p, dividing by p gives us a form $< , >_{T^*}$ on T^*, and multiplication by p induces an isometry :

3.16.1 $$T^*/T \xrightarrow{\cong} (T^* \otimes \mathbb{F}_p)/\mathrm{Ann}(T^* \otimes \mathbb{F}_p) \xrightarrow{\text{"p"}} T_o \otimes \mathbb{F}_p .$$

In the context of Proposition (3.12), we can give an interpretation of $\bar{H} \subseteq T_o \otimes k \cong L/E$, using the interpretation $T_o \otimes k = \mathrm{Ann}(T \otimes k) \subseteq T \otimes k$; it is simply the kernel of the natural map $E \otimes k \to H \otimes k$. This follows from the diagram :

3.16.2 $$\begin{array}{ccccccccc} o \to & H/E & \xrightarrow{p} & E/pE & \to & H/pH & \to & H/E & \to o \\ & \downarrow & & \uparrow & & & & & \\ & L/E & \xrightarrow{\sim} & \mathrm{Ann}(E/pE). & & & & & \end{array}$$

Notice that by contrast, the map $T_H \otimes \mathbb{F}_p \to H$ is injective. □

3.17 Definition. A "K3-lattice (over $\mathbb{Z}_p$)" is a free $\mathbb{Z}_p$-module Γ of finite rank, together with a quadratic form $< , >_\Gamma : \Gamma \otimes \Gamma \to \mathbb{Z}_p$ satisfying (3.13.1) through (3.13.3).

3.18 Corollary. A K3-lattice is determined up to isogeny by its rank and by $(\frac{\bar{d}}{p}) \in \{\pm 1\}$, and up to isomorphism by the additional specification of $\sigma_o = \frac{1}{2}\mathrm{ord}_p(d)$. □

It is clear that if H is a supersingular K3 crystal, the natural map : $(T_H \otimes W, \mathrm{id} \otimes F_W^*) \to (H, \Phi)$ is an isogeny, compatible with the quadratic forms. In particular, H is determined up to isogeny by $T_H \otimes \mathbb{Q}_p$, and hence by $(\frac{\bar{d}}{p})$. Thus, we have proved all the assertions of Theorems (3.3) and (3.4).

3.19 Definition. Let V be an $\mathbb{F}_p$-vector space of dimension $2\sigma_o$, with a non-degenerate nonneutral quadratic form $\langle\ ,\ \rangle_V$, and let $\varphi = \mathrm{id}_V \otimes F_k^* : V \otimes k \to V \otimes k$. Then a "strictly characteristic subspace of $V \otimes k$" is a k-subspace $K \subseteq V \otimes k$ such that :

1) K is totally isotropic and has dimension σ_o.

2) $\varphi(K) + K$ has dimension $\sigma_o + 1$.

3) $V \otimes k = \sum_{i=0}^{\infty} \varphi^i K$, i.e. there is no $\mathbb{F}_p$-rational subspace of V between V and K.

A "characteristic subspace of $V \otimes k$" is one which satisfies 1) and 2), but not necessarily 3).

Now let $\mathbb{C}3(k)$ be the category whose objects are pairs (T,K), where T is a K3-lattice over $\mathbb{Z}_p$ and $K \subseteq T_o \otimes k$ is a strictly characteristic subspace. The morphisms $(T,K) \to (T',K')$ are defined to be the isomorphisms $T \to T'$ sending K to K', in the obvious sense. (We should note that $T_o \otimes \mathbb{F}_p$ depends functorially on T, because $T_o \otimes \mathbb{F}_p$ is $\mathrm{Ann}(T \otimes \mathbb{F}_p)$, or by (3.16).) Let $\mathbb{K}3(k)$ be the category whose objects are supersingular K3 crystals over k, and with only isomorphisms as morphisms.

3.20 Theorem. There is an equivalence of categories : $\mathbb{K}3(k) \xrightarrow{\gamma} \mathbb{C}3(k)$.

Proof. γ is defined as follows : If H is an object of $\mathbb{K}3(k)$, T_H is a K3-lattice, and $\bar{H} = \ker(T \otimes k \to H \otimes k)$ is a strictly characteristic subspace of $T_o \otimes k$

(cf. 3.16). For reasons which will become apparent later, we work instead with the subspace $K_H = \varphi^{-1}(\bar{H}) \subseteq T_o \otimes k$, which of course is also strictly characteristic. It is clear that this construction defines a functor $\gamma : \mathbb{K}3(k) \to \mathbb{C}3(k)$, with $\gamma(H) = (T_H, K_H)$.

To define the quasi-inverse, we give a slightly more general construction : Let T be a K3-lattice and $K \subseteq T_o \otimes k$ a characteristic subspace, (not necessarily strict). Set $E = T \otimes W$, $L = T^* \otimes W$, $\bar{K} = \varphi(K) \subseteq L/E \cong T_o \otimes k$, and define $H \subseteq L$ to be the inverse image of $\bar{K}$. The W-module L has an F-crystal structure given by $\Phi = p(\mathrm{id}_{T^*} \otimes F_W^*)$, and H is a subcrystal, because $\Phi(H) \subseteq p(\mathrm{id} \otimes F_W^*)L = pL \subseteq H$. Then $(H, \Phi) \hookrightarrow (L, \Phi)$ is an isogeny of F-crystals, and the slopes of (H, Φ) are all one. To define $< , >_H$, note that (by a general formula) the p-adic ordinal of the discriminant of $< , >_L$ (cf. (3.16)) on the sublattice H of L is twice the length of L/H plus the ordinal of the discriminant of $< , >_L$, i.e. $2\sigma_o + rk(T) - 2\sigma_o = rk(T)$. On the other hand, since $\bar{K}$ is isotropic, $< , >_L$ is divisible by p on H, and we can define $< x, y >_H = p^{-1} < x, y >_L$. Then the discriminant of $< , >_H$ is a unit, and $< , >_H$ is perfect. Moreover, it is clear that

$$< \Phi x, \Phi y >_H = p^{-1} < p(\mathrm{id} \otimes F_W^*)x,\ p(\mathrm{id} \otimes F_W^*)y >_L = p < x, y >_L = p^2 < x, y >_H .$$

To prove that H is a K3 crystal, it remains only for us to compute h^o. For later applications, it will be convenient for us to be more precise by computing the Hodge filtration of $H \otimes k$. Recall that by definition, $F^i(H \otimes k)$ is the image of $A^i H \to H \otimes k$, where $A^i H = \{x \in H : \Phi(x) \in p^i H\}$. I claim that the diagram below has exact rows :

$$\begin{array}{ccccccccc}
\varphi(K) & \hookrightarrow & T \otimes k & \to & H \otimes k & \to & \varphi(K) & \to & o \\
\| & & \|\wr & & \uparrow & & \uparrow & & \\
\varphi(K) & \hookrightarrow & T \otimes k & \to & F^1(H \otimes k) & \to & K \cap \varphi(K) & \to & o \\
\| & & \uparrow & & \uparrow & & \uparrow & & \\
\varphi(K) & \hookrightarrow & K + \varphi(K) & \to & F^2(H \otimes k) & \to & o & &
\end{array} \qquad (3.20.1)$$

Since $\varphi(K)$ is simply the image of H in $(T^* \otimes k)/(T \otimes k) \cong T_o \otimes k$, the first row is clear. Now an $x \in L = T^* \otimes W$ lies in A^1H iff $x \in H$ and $(p^{-1}\Phi)(x) \in H$, i.e. iff the image of x lies in $\bar{H} \cap \varphi^{-1}(\bar{H}) = \varphi(K) \cap K$. Moreover, $T \otimes W$ is obviously contained in A^1H, and hence we get the second row of the diagram. For the bottom row : $x \in A^2H$ iff $x \in H$ and $(p^{-1}\Phi)(x) \in pH$, i.e. iff $x = py$ with $y \in L$ and $(p^{-1}\Phi)(y) \in H$. Recalling that multiplication by p induces our isomorphism : $L/E \cong T_o \otimes k \subseteq T \otimes k$, we see the claim.

This proves that H is a supersingular K3 crystal. It is clear that $E \subseteq H$ is a submodule on which Φ is divisible by p, and hence $E \subseteq E_H$ and $T \subseteq T_H$. It follows that $\bar{K} = \ker(T \otimes k \to H \otimes k)$ contains the kernel of $T \otimes k \to T_H \otimes k$, which is defined over $\mathbb{F}_p$. If now we assume K to be strictly characteristic, any rational subspace of $\varphi(K)$ is zero. Then $T \otimes k \to T_H \otimes k$ and $T \to T_H$ are isomorphisms. This implies that $\gamma(H) = (T,K)$, and hence that we have a quasi-inverse to γ. Since γ is easily seen to be fully faithful, this completes the proof. □

Our next task is the classification of elements of $\mathbb{C}3(k)$. In order really to be able to compute, it is necessary to introduce explicit invariants. However, for geometry, it is more convenient to rigidify further and represent a functor. Since both approaches are useful, we sketch them each, beginning with the invariants.

Let $\mathbb{C}_{\sigma_o}(k)$ denote the category of pairs (V,K), with $K \subseteq V \otimes k$ strictly characteristic and with $\dim V = 2\sigma_o$ (3.19), and with isomorphisms as morphisms. If (V,K) is an object of $\mathbb{C}_{\sigma_o}(k)$, it is easy to see that $\ell_K = K \cap \varphi(K) \cap \ldots \varphi^{\sigma_o - 1}(K) \subseteq V \otimes k$ is a line, and that $\ell_K + \ldots \varphi^{\sigma_o-1}(\ell_K) = \varphi^{\sigma_o-1}(K)$ is another strictly characteristic subspace. Then $\ell_K + \ldots \varphi^{2\sigma_o-1}(\ell_K) = V \otimes k$, and if e is a basis of ℓ_K, $\{e_i = \varphi^{i-1}(e) \quad i = 1\ldots 2\sigma_o\}$ forms a basis of $V \otimes k$, with $\{e_i : i = 1 \ldots \sigma_o\}$ a basis of $\varphi^{\sigma_o-1}(K)$. It follows that $\langle e_1, e_{\sigma_o+1}\rangle \neq 0$, and hence we can find e_1, unique up to a $(p^{\sigma_o}+1)$ root of unity, such that $\langle e_1, e_{\sigma_o+1}\rangle = 1$. Define :

3.21.1 $\qquad a_i(e,V,K) = \langle e_1, e_{\sigma_o+i+1}\rangle$ for $i = 1 \ldots \sigma_o - 1$.

If e is replaced by ζe, with $\zeta \in \mu_{p^{\sigma_o+1}}(k)$, then a_i is replaced by $\zeta^{p^{\sigma_o+i}+1} a_i = \zeta^{1-p^i} a_i$.

3.21 Theorem. The above coordinates induce a bijection :

$$\mathbb{C}_{\sigma_o}(k)/\mathrm{Isom} \longrightarrow A^{\sigma_o-1}(k)/\mu_{p^{\sigma_o+1}}(k).$$

Proof. The main step is the following computation :

3.22 Lemma. In the basis $(e_1 \dots e_{2\sigma_o})$, the intersection matrix $\langle e, e\rangle_{V\otimes k}$ has the form :

$$\begin{pmatrix} 0 & A \\ A^t & 0 \end{pmatrix}, \quad \text{where } A \text{ is the } \sigma_o \times \sigma_o\text{-matrix :}$$

$$A = \begin{pmatrix} 1 & a_1 & a_2 & a_3 & \dots & a_{\sigma_o-1} \\ 0 & 1 & F(a_1) & F(a_2) & \dots & F(a_{\sigma_o-2}) \\ 0 & 0 & 1 & F^2(a_1) & \dots & F^2(a_{\sigma_o-3}) \\ & & & \dots & & \\ 0 & 0 & \dots & \dots & \dots & 1 \end{pmatrix}.$$

The Frobenius-linear endomorphism φ of $V\otimes k$ has "matrix" : $\varphi(e_i) = e_{i+1}$ for $i = 1\dots 2\sigma_o-1$, $\varphi(e_{2\sigma_o}) = \lambda_1 e_1 + \dots \lambda_{\sigma_o} e_{\sigma_o} + \mu_1 e_{\sigma_o+1} + \dots \mu_{\sigma_o} e_{2\sigma_o}$. The λ's and μ's are determined by : $\lambda_1 = 1$, $\mu_1 = 0$, and :

$$A^t\lambda = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \qquad A\mu = \begin{pmatrix} ? \\ F(a_{\sigma_o-1}) \\ \vdots \\ F^{\sigma_o-1}(a_1) \end{pmatrix}.$$

Proof. The formula for the intersection matrix follows from the definitions and the fact that $\langle\varphi(x),\varphi(y)\rangle = F\langle x,y\rangle$ for $x, y \in V\otimes k$; the only thing that needs proof is the computation of the λ's and μ's. Notice that the formulas above do determine λ and μ uniquely, because A^t and A with its first row deleted are invertible.

If u and v are column matrices in k of length σ_o, set

$z = u_1e_1 + \dots u_{\sigma_o}e_{\sigma_o} + v_1e_{\sigma_o+1} + \dots v_{\sigma_o}e_{2\sigma_o} \in V \otimes k$. Then we have the formula :

3.22.1 $$< z, \varphi(e_{2\sigma_o})> = u^tA\mu + v^tA^t\lambda.$$

Apply this with $u = 0$ and with $v = \epsilon_j$, the j^{th} standard basis vector. Then $z = e_{\sigma_o+j}$, and $v^tA^t\lambda$ is the j^{th} row of $A^t\lambda$. Formula (3.22.1) tells us that this row is $< e_{\sigma_o+j}, \varphi(e_{2\sigma_o}) >= F<e_{\sigma_o+j-1}, e_{2\sigma_o}> = 1$ if $j = 1$, 0 if $j > 1$. Next take $v = 0$ and $u = \epsilon_{j+1}$, so $z = e_{j+1}$ and $u^tA\mu$ is the $(j+1)^{st}$ row of $A\mu$, which must be $<e_{j+1}, \varphi(e_{2\sigma_o}) > = F^j < e_1, e_{2\sigma_o-j+1} > = F^j(a_{\sigma_o-j})$. Finally, take $u = \lambda$ and $v = \mu$. We have $0 = <e_{2\sigma_o}, e_{2\sigma_o}> = <\varphi(e_{2\sigma_o}), \varphi(e_{2\sigma_o}) > = \lambda^tA\mu + \mu^tA^t\lambda = 2\lambda^tA\mu$. But $\lambda^tA = \epsilon_1$, so $\mu_1 = 0$. □

Let us now prove the theorem. Suppose first of all that $f : (V,K) \to (V',K')$ is an isomorphism in $\mathbb{C}_{\sigma_o}(k)$, i.e. f is an isometry $V \to V'$ such that $f \otimes id_k$ sends K to K'. Then $f \otimes id_k$ sends ℓ_k to $\ell_{k'}$, and hence a normalized basis vector of ℓ_k to one of $\ell_{k'}$. It is then apparent that (V,K) and (V',K') have the same coordinates. If, conversely, (V,K) and (V',K') have the same coordinates, then we can choose e and e' so that $a_i(e, V, K) = a_i(e', V', K')$ for all i. Then by the lemma, the map $V \otimes k \to V' \otimes k$ sending e_i to e_i' for all i is an isometry, and in fact sends φ to φ'. This last fact implies that it descends to an isometry $V \to V'$. Clearly it also sends ℓ_K to $\ell_{K'}$ hence K to K'. To prove that the map $\mathbb{C}_{\sigma_o}(k) \to A^{\sigma_o-1}(k)/\mu_{p^{\sigma_o+1}}(k)$ is surjective, start with elements $(a_1, \dots a_{\sigma_o-1})$ of $A^{\sigma_o-1}(k)$ and use the formulas of the lemma to define an intersection form and a Frobenius linear endomorphism φ of $k^{2\sigma_o}$. Since $\lambda_1 = 1$, φ is bijective, and hence defines an $\mathbb{F}_p$-form V for $k^{2\sigma_o}$. Since $F<x,y> = <\varphi(x), \varphi(y)>$ for $x,y \in k^{2\sigma_o}$, the intersection form descends to an $\mathbb{F}_p$-valued form on V. Finally, it is clear that the first σ_o standard basis vectors of $k^{2\sigma_o}$ span a strictly characteristic subspace K' of V; we take $K = \varphi^{1-\sigma_o}(K')$, and evidently $a_i(V,K) = a_i$. □

3.23 <u>Corollary</u>. <u>Fix</u> $(\frac{d}{p}) \in \{\pm 1\}$ <u>and</u> σ_o, $n \in N$, <u>and consider the set</u> $K3(\sigma_o, n, (\frac{d}{p}))$ <u>of isomorphism classes of supersingular</u> K3 <u>crystals over</u> k <u>with these invariants</u>. <u>This set is empty unless</u> $n \geq 2\sigma_o \geq 2$ <u>and either</u> $n > 2\sigma_o$ <u>or</u> $(\frac{d}{p}) = -(\frac{-1}{p})^{\sigma_o}$. <u>If it is not empty, the coordinates above identify it with</u> $A^{\sigma_o - 1}/\mu_{p^{\sigma_o}+1}(k)$.

<u>Proof</u>. The numerical conditions above are just the conditions that there should exist a K3 lattice with invariants $(\sigma_o, n, (\frac{d}{p}))$, and such a lattice T is unique up to noncanonical isomorphism. Furthermore, it is clear that $\mathrm{Aut}(T) \to \mathrm{Aut}(T_o \otimes \mathbb{F}_p)$ is surjective. Thus, if (T,K) and (T',K') are two objects of $\mathbb{C}3(k)$ with the same invariants and the same coordinates a_i, the objects $(T_o \otimes \mathbb{F}_p, K)$ and $(T'_o \otimes \mathbb{F}_p, K')$ are isomorphic, hence so are (T,K) and (T',K'), and hence so are the corresponding crystals. It is equally clear that we can construct crystals with arbitrary coordinates. □

3.24 <u>Remark</u>. It may be of some interest to observe that the techniques above give another proof that if (V,K) is an object of $\mathbb{C}_{\sigma_o}(k)$, then the discrimiant d_o of V satisfies $(\frac{d_o}{p}) = -(\frac{-1}{p})^{\sigma_o}$. Let $(x_1 \ldots x_{2\sigma_o})$ be a basis for $V \otimes k$ as in Lemma (3.22), and let $(x^1 \ldots x^{2\sigma_o})$ be the dual basis. Then the map $\beta \otimes \mathrm{id}_k : V \otimes k \to V^* \otimes k$ corresponding to $< , >_V$ has matrix $\begin{pmatrix} 0 & A \\ A^t & 0 \end{pmatrix}$ with respect to these two bases, and its determinant is $(-1)^{\sigma_o}(\det A)^2 = (-1)^{\sigma_o}$. This computation is only valid over k, but that is easily remedied : This determinant is also the matrix of $\lambda = \Lambda^{2\sigma_o}(\beta \otimes \mathrm{id}_k) : \Lambda^{2\sigma_o}(V \otimes k) \longrightarrow \Lambda^{2\sigma_o}(V^* \otimes k)$ with respect to the two bases $x = x_1 \wedge \ldots x_{2\sigma_o}$ and $y = x^1 \wedge \ldots x^{2\sigma_o}$, i.e. $\lambda(x) = (-1)^{\sigma_o} y$. But Lemma (3.22) allows us to compute the action of Frobenius on x :
$\varphi(x) = \varphi(x_1) \wedge \ldots \varphi(x_{2\sigma_o}) = x_2 \wedge \ldots x_{2\sigma_o} \wedge (x_1 + \ldots) = -x$. Choose $\lambda \in k$ such that $\lambda^{p-1} = -1$; then if $x' = \lambda x$, $\varphi(\lambda x) = \lambda x$, so that $x' = \lambda x$ is an $\mathbb{F}_p$-basis for $\Lambda^{2\sigma_o} V$. The dual basis, with respect to the form $< , >_V$, is $y' = \lambda^{-1} y$, and hence the matrix d_o for λ with respect to these bases is $\lambda^2(-1)^{\sigma_o}$. Now $\mathbb{F}_p(\lambda) = \mathbb{F}_{p^2}$, so that λ^2

is an element of $\mathbb{F}_p^*$ which is not a square, so $(\frac{d_o}{p}) = (\frac{\lambda^2}{p})(\frac{-1}{p})^{\sigma_o} = -(\frac{-1}{p})^{\sigma_o}$. □

3.25 Example. There is a unique isomorphism class of supersingular K3 crystals with $\sigma_o = 1$ (provided, of course, n and $(\frac{\bar{d}}{p})$ are fixed and satisfy the conditions of (3.23)).

3.26 Remark. If X is a surface satisfying (1.1) and with $p_g(X) = 1$, then $H^2_{cris}(X/W)$ is a K3-crystal. It is clear from (1.2) that the flat cohomology of X can be computed from its crystalline cohomology. In particular, if $H^2_{cris}(X/W)$ is supersingular, we can express $H^2(X_{fl}, \mu_p)$ in terms of our parameters. It is not hard to see that $H^2(X_{fl}, \mu_p)$ can be identified with the group :

$$\{x \in T \otimes \mathbb{Z}/p\mathbb{Z} : \varphi(x) + \varphi^2(x) \in \varphi(K) + \varphi^2(K)\}/\varphi(K).$$

It seems clear that the subgroup corresponding to those x such that $x \in T_o \otimes \mathbb{Z}/p\mathbb{Z}$ is Artin's $U(X_{fl}, \mu_p)$, but I have not checked this carefully, nor have I explicitly calculated Artin's period map. □

§4. RIGIDIFIED CRYSTALS.

In order to deal with jumps in σ_o, and for (conjectural) geometric applications, it is convenient to classify "rigidified K3 crystals", in the following sense :

4.1 Definition. Let T be a K3-lattice (3.17), and let H be a K3-crystal of the same rank. Then a "T-structure on H" is a map : $i : T \to T_H$ which is compatible with the intersection forms. An "isomorphism" of K3-crystals with T-structure is an isomorphism $f : H \to H'$ such that $f \circ i = i'$.

4.2 Remark. If H and T are as above, then H admits a T-structure iff $\sigma_o(H) \le \sigma_o(T)$, and in fact there is a natural bijection between $\mathrm{Aut}(T_H)\backslash\{$T-structures on $H\}$ and the set of isotropic subspaces of $T_o \otimes \mathbb{F}_p \cong T^*/T$ of dimension $\sigma_o(T) - \sigma_o(H)$. To see this, note that $i : T \to T_H$ is necessarily injective, and $W = T_H/T$ has length $\sigma_o(T) - \sigma_o(H)$. Moreover, $T_H \subseteq T^*$, and $W \subseteq T^*/T \cong T_o \otimes \mathbb{F}_p$ corresponds to the kernel of i mod p, which is clearly invariant under the (left) action of $\mathrm{Aut}(T_H)$. Conversely, if $W \subseteq T^*/T$ is isotropic of dimension $\sigma_o(T) - \sigma_o(H)$, then the inverse image $T(W)$ of W in T^* is (with the form $1/p < , >_{T^*}$) a K3-lattice with the same invariant σ_o as H, hence there exists an isomorphism $T(W) \xrightarrow{\cong} T_H$.

4.3 Proposition. If $i : T \to T_H$ is a T structure on a K3 crystal H, then $\bar{H} = \ker(T_o \otimes k \to H \otimes k)$ is a characteristic subspace of $T_o \otimes k$, as is $K_H = \varphi^{-1}(\bar{H})$. The correspondance $i \mapsto K_H$ defines a bijection between the set of isomorphism classes of crystals with T-structure and the set of characteristic subspaces of $T_o \otimes k$.

Proof. The proof is exactly the same as in the special case $i = \mathrm{id}_{T_H}$ given above. Perhaps we should explain how T_H can be computed from $K \subseteq T_o \otimes k$: Since $\cap\, \varphi^i K \subseteq V \otimes k$ is φ-invariant, it is $W_K \otimes k$ for some isotropic $W_K \subseteq V$. The construction of the previous paragraph then defines a new K3-lattice T_{W_K} and a map $i : T \to T_{W_K}$. It is easy to see that T_{W_K} is the Tate module of the K3 crystal H associated to K, and that this map i is the corresponding T-structure. □

4.4 Remark. If $i : T \to T_H$ and $i' : T \to T_{H'}$ are T-structures on H and H' and if K and K' are the corresponding characteristic subspaces, the following are equivalent :

i) K and K' are conjugate under $\mathrm{Aut}(T_o \otimes \mathbb{F}_p)$.

ii) K and K' are conjugate under Aut(T).

iii) There exists a commutative diagram :

$$\begin{array}{ccc} T & \xrightarrow{i} & H \\ \cong\downarrow & & \downarrow\cong \\ T & \xrightarrow{i'} & H' \end{array}$$

iv) H and H' are isomorphic.

Proof. Since the map $\mathrm{Aut}(T) \to \mathrm{Aut}(T_o \otimes \mathbb{F}_p)$ is obviously surjective, i) implies ii). In fact, the only nonobvious implication is "iv) implies i)". If there exists an isomorphism $\alpha : H \to H'$, then $\sigma_o(H) = \sigma_o(H')$, and hence $W = \ker(i \otimes \mathbb{F}_p)$ and $W' = \mathrm{Ker}(i' \otimes \mathbb{F}_p)$ are two isotropic subspaces of $T_o \otimes \mathbb{F}_p$ of the same dimension. By Witt's theorem, there is an automorphism of $T_o \otimes \mathbb{F}_p$ taking one to another, and hence we may assume that $W = W'$. Then i and i' induce isomorphisms : $W^{\perp}/W \to T_o(H) \otimes \mathbb{F}_p$ and $W^{\perp}/W \to T_o(H') \otimes \mathbb{F}_p$, respectively, and by functoriality we see that α induces an automorphism of $W^{\perp}/W$. Since $W^{\perp}/W$ is an orthogonal direct summand of $T_o \otimes \mathbb{F}_p$, we can extend this automorphism to $T_o \otimes \mathbb{F}_p$. This proves that iv) implies i). □

4.5 Note. The isomorphisms $H \to H'$ in (iv) and iii) are not necessarily the same. However, if $\sigma_o(T) = \sigma_o(H)$, they can be chosen to be the same, and Aut(H) becomes identified with the stabilizer subgroup $G(K_H) \subseteq \mathrm{Aut}(T)$ of K_H. (In general, this subgroup is a subgroup of finite index in Aut(H), viz., the stabilizer of the image of T).

The above proposition motivates a more detailed study of characteristic subspaces of $T_o \otimes k$. It is apparent that this should be the set of k-points of a suitable scheme. I find it remarkable, however, that it turns out to be complete.

The most convenient way to construct and study the scheme in question is by introducing the functor it represents. Let V be an $\mathbb{F}_p$-vector space, and recall that if A is an $\mathbb{F}_p$-algebra, $\mathrm{Quot}^r_V(A)$ is by definition the set of isomorphism classes of locally free rank r quotients of $V \otimes A$; of course this functor is representable. We will find it convenient to work with the equivalent notion of direct summands of $V \otimes A$: $\ker^d_V(A) = \{\text{direct summands } K \text{ of } V \otimes A \text{ which have rank } d\}$. Clearly if $\dim V = 2\sigma_o$, $\ker^d_V(A) \cong \mathrm{Quot}^{2\sigma_o - d}_V(A)$. The only thing that requires a bit of caution with this notation is the functoriality : if $\theta : A \to B$ and $K \subseteq V \otimes A$ is a direct summand, then $\theta^*(K) \subseteq V \otimes B$ is the B-module generated by the image of K under $\mathrm{id}_V \otimes \theta$. For example, if k is a perfect field and F is Frobenius, $F^*(K) = \varphi(K)$, where $\varphi = \mathrm{id}_V \otimes F^*$.

If K_1 and K_2 are direct summands of $V \otimes A$, it is not necessarily the case that $K_1 + K_2$ is a direct summand of $V \otimes A$, and hence its formation is not compatible with base change. However, if $\theta : A \to B$, there is a natural surjective map : $\theta^*(K_1 + K_2) \to \theta^*(K_1) + \theta^*(K_2)$, and hence an <u>isomorphism</u> : $\theta^*(V \otimes A/K_1 + K_2) \xrightarrow{\cong} (V \otimes B)/\theta^*(K_1) + \theta^*(K_2)$. It is easy to see, in fact, that formation of $K_1 + K_2$ commutes with arbitrary base change iff $K_1 + K_2$ is projective iff $K_1 + K_2$ is again a direct summand, or (if A is reduced) iff $K_1(t) + K_2(t)$ has constant rank on <u>Spec</u>(A). Moreover, if these conditions are satisfied, $(K_1 + K_2)/K_1$, $(K_1 + K_2)/K_2$, $K_1 \cap K_2$, and $(V \otimes A)/K_1 \cap K_2$ are projective, and their formation commutes with base change.

Let $\langle\ ,\ \rangle_V$ be a nonneutral quadratic form on the $2\sigma_o$-dimensional $\mathbb{F}_p$-vector space V. If A is an $\mathbb{F}_p$-algebra, a "generatrix of $V \otimes A$" is a direct summand K of $V \otimes A$ whose rank is σ_o such that $\langle\ ,\ \rangle_V \big|_K = 0$. The set $\underline{\underline{\mathrm{Gen}}}_V(A)$ of generatrices of $V \otimes A$ is functorial in A. A generatrix is called "characteristic" iff $K + F^*_A(K)$ is a direct summand of rank $\sigma_o + 1$, and $\underline{\underline{M}}_V$ denotes the functor taking A

to the set of characteristic generatrices of $V \otimes A$.

4.6 Proposition. $\underline{\underline{M}}_V$ is representable by an $\mathbb{F}_p$-scheme M_V and a universal characteristic generatrix $K_M \in \underline{\underline{M}}_V(M_V)$. Moreover :

4.6.1 M_V is smooth and projective, of dimension $\sigma_o - 1$.

4.6.2 There is a natural isomorphism from the tangent bundle of M_V to $\mathrm{Hom}[K_M \cap F^*_M(K_M), F^*_M(K_M)/K_M \cap F^*_M(K_M)]$, induced by the canonical connection on $F^*_M(K_M)$.

Proof. Recall again from [SGA 7, XII, 2.8] that the functor $\underline{\underline{\mathrm{Gen}}}$: $A \mapsto \{\text{generatrices of } V \otimes A\}$ is represented by a smooth projective $\mathbb{F}_p$-scheme Gen, together with a universal object K_G. Thus, over Gen, we have a diagram (with exact rows) :

4.6.3
$$\begin{array}{ccccccccc} o & \longrightarrow & K_G & \longrightarrow & V \otimes \mathcal{O}_G & \longrightarrow & Q & \longrightarrow & o \\ & & \downarrow & & \downarrow \beta & & \downarrow & & \\ o & \longrightarrow & Q^\vee & \longrightarrow & V^\vee \otimes \mathcal{O}_G & \longrightarrow & K_G^\vee & \longrightarrow & o . \end{array}$$

The vertical arrows are isomorphisms.

It is now convenient to introduce the functors $\underline{\underline{P}}$: $A \mapsto \{(K_1, K_2) \in \underline{\underline{\mathrm{Gen}}}(A) \times \underline{\underline{\mathrm{Gen}}}(A) :$ $K_1 + K_2$ is projective of rank $\sigma_o + 1\}$ and $\underline{\underline{\mathbb{P}K}}_G$, the functor represented by the projective bundle associated to K_G. There are evident morphisms $\pi_i : \underline{\underline{P}} \to \underline{\underline{\mathrm{Gen}}}$ and $\pi : \mathbb{P}K_G \to \underline{\underline{\mathrm{Gen}}}$, and a commutative diagram :

$$\begin{array}{ccc} \underline{\underline{P}} & \xrightarrow{\alpha} & \underline{\underline{\mathbb{P}K}}_G \\ & \pi_2 \searrow \quad \swarrow \pi & \\ & \underline{\underline{\mathrm{Gen}}} & \end{array}$$

with α given as follows : If $(K_1, K_2) \in \underline{\underline{\mathrm{Gen}}}$, then $K_i = \pi_i^*(K_G)$, and $(K_1+K_2)/K_1 \cong K_2/K_1 \cap K_2$ is an invertible quotient of $\pi_2^*(K_G)$.

I claim that α is in fact an isomorphism of functors. To see the inverse, let $K_G \otimes A \to \mathcal{L} \to o$ be an A-valued point of $\underline{\underline{\mathbb{P}K}}_G$; then its kernel $W \subseteq K \underset{G}{\otimes} A$ is a direct factor of rank $\sigma_o - 1$. The annihilator $W^\perp$ of W is a direct summand of $V \otimes A$, of rank σ_o+1, and $W^\perp/W$ is projective of rank 2. Moreover, the quadratic form on $W^\perp/W$ induced by $\langle\, ,\, \rangle_V$ is nondegenerate, and hence defines a smooth quadric in $\mathbb{P}(W^\perp/W)$ - i.e. an étale cover of A of degree 2. Since $K = K_G \otimes A$ is isotropic, K/W defines an A-valued point of the quadric, so the covering is split. That is, there is a unique "other section", corresponding to an isotropic line $L \subseteq W^\perp/W$, and we have a hyperbolic decomposition : $W^\perp/W = K/W \oplus L$. The inverse image K' of L in $W^\perp$ is an isotropic direct summand of $W^\perp$, hence of $V \otimes A$, and $K + K' = W^\perp$. Thus, (K',K) is a point of $\underline{\underline{P}}(A)$, with $K' \cap K = W$ and $K/K' \cap K \cong \mathcal{L}$. It is easy to check that this defines the inverse of α. Of course, we could have interchanged the roles of π_1 and π_2.

Now it is clear that $\underline{\underline{M}}_V(A) = \{K \in \underline{\underline{Gen}}(A) : (K, \varphi(K)) \in \underline{\underline{P}}(A)\}$, i.e. that we have a Cartesian diagram :

$$\begin{array}{ccc}
\underline{\underline{M}}_V & \xhookrightarrow{\text{incl}} & \underline{\underline{Gen}} \\
\downarrow & & \downarrow \Gamma_F \\
\underline{\underline{P}} & \xhookrightarrow[(\pi_1,\pi_2)]{} & \underline{\underline{Gen}} \times \underline{\underline{Gen}}
\end{array}$$

where Γ_F is the graph of Frobenius. It follows that $\underline{\underline{M}}_V$ is represented by the corresponding fiber product of schemes, with $\text{incl}^*(K_G)$ as universal object.

To prove that M_V is smooth, we verify that P and Γ_F intersect transversally in Gen $\times$ Gen, that is, that their tangent spaces generate the tangent space of Gen$\times$Gen. Since the differential of Frobenius is zero, $(\Gamma_F)_* : T_{Gen} \to T_{Gen\times Gen}|_{Gen} \cong T_{Gen} \oplus T_{Gen}$ is just $y \mapsto (y,0)$. The map $T_P \to (T_{Gen} \oplus T_{Gen})|_P$ is just $x \mapsto (\pi_{1*}(x), \pi_{2*}(x))$, and we know that π_i is smooth. Thus, $(\pi_1,\pi_2)_* - (\Gamma_F)_* : T_P \oplus T_{Gen} \to T_{Gen} \oplus T_{Gen}$ sends (x,y) to $\delta(x,y) \overset{=}{\text{def}}$ $(\pi_{1*}(x)-y, \pi_{2*}(x))$, which is evidently surjective. In fact, we obtain an exact ladder of bundles on M_V :

$$\begin{array}{ccccccccc}
o & \to & T_{M_V} & \to & T_P \oplus T_{Gen} & \xrightarrow{\delta} & T_{Gen} \oplus T_{Gen} & \to & o \\
 & & \| \wr & & \uparrow (id, \pi_{1*}) & & \uparrow (o, id) & & \\
o & \to & T_{P/Gen} & \to & T_P & \xrightarrow{\pi_{2*}} & T_{Gen} & \to & o \quad .
\end{array}$$

In other words, the tangent space to M_V can be identified with the relative tangent space of $\pi_2 : P \to \text{Gen}$, i.e. with $T_{\mathbb{P}K/\text{Gen}}$, and hence M_V is smooth of dimension $\sigma_o - 1$. Moreover, recall that $T_{\mathbb{P}K/\text{Gen}} \cong \text{Hom}[W, \mathcal{O}_{\mathbb{P}K}(1)]$, where $o \to W \to \pi_2^* K \to \mathcal{O}_{\mathbb{P}K}(1) \to o$ is the canonical exact sequence, and where the isomorphism is induced by the "second variation" associated to the standard connection $\nabla : \pi_2^* K \to \Omega^1_{\mathbb{P}K/\text{Gen}} \otimes \pi_2^* K = d \otimes_{\mathcal{O}_{\text{Gen}}} \text{id}_K$. If we restrict to M_V, $\pi_2^* K \cong F^* K_M$, $W \cong K_M \cap F^* K_M$, and $\mathcal{O}_{\mathbb{P}K}(1) \cong F^* K_M / K_M \cap F^* K_M$. To prove (4.6.2), we therefore have only to check that the following diagram commutes :

$$\begin{array}{ccc} \pi_2^* K_G & \xrightarrow{\nabla} & \Omega^1_{P/\text{Gen}} \otimes \pi_2^* K \\ \downarrow & & \downarrow \\ F_M^* K_M & \xrightarrow{\nabla} & \Omega^1_{M_V} \otimes F_M^* K_M . \end{array}$$

In other words, we have to verify that the horizontal sections of $\pi_2^* K_G |_M$ are the sections of K_M. Since $\pi_2 \circ \text{incl} = \pi_1 \circ \text{incl} \circ F_M$, this is clear. □

4.7 <u>Examples</u>. If $\sigma_o = 1$, Gen(k) is clearly just two points, with $\text{Aut}(k/\mathbb{F}_p)$ acting nontrivially - i.e. Gen $\cong$ <u>Spec</u> $\mathbb{F}_{p^2}$. If $\sigma_o = 2$, $\langle\ ,\ \rangle_V$ defines a nonsingular quadric X in $\mathbb{P}^3$, and $X \times k$ is isomorphic to $(\mathbb{P}^1 \times \mathbb{P}^1) \times k$. Again, $\text{Aut}(k/\mathbb{F}_p)$ interchanges the two factors. Points of Gen(k) just correspond to the rulings on $\mathbb{P}^1 \times \mathbb{P}^1 \times k$, and hence Gen $\cong \mathbb{P}^1 \times \mathbb{F}_{p^2}$, viewed as an $\mathbb{F}_p$-scheme. Now it is clear that if $K \in \text{Gen}(k)$, $\varphi(K) \neq K$, hence $K + \varphi(K)$ has dimension 3, and K is characteristic. Thus $M_V = \text{Gen}$. If $\sigma_o = 3$, $\langle\ ,\ \rangle$ defines a nonsingular quadric in $\mathbb{P}^5$, which is a twisted form of the Grassmanian G(2,4) of lines in $\mathbb{P}^3$. The points of Gen(k) correspond to planes in G(2,4), and the two families of these are respectively the planes of lines containing some point $p \in \mathbb{P}^3$ or contained in some hyperplane $H \subseteq \mathbb{P}^3$. Frobenius interchanges these families, hence gives us some morphism $\mathbb{P}^3 \to \mathbb{P}^{3\vee}$. It follows from the above that $M_V \subseteq \mathbb{P}^3 \amalg \mathbb{P}^{3\vee}$ corresponds to a nonsingular hypersurface in each factor.

4.8 Remark. The spaces M_V can be regarded as compactifications of the moduli space of K3 crystals with fixed σ_o, and it is easy to be fairly explicit about the divisor at ∞. For each σ'_o, let $\underline{\underline{M}}_V^{\sigma'_o}(k) \subseteq \underline{\underline{M}}_V(k)$ be the subset corresponding to crystals H with $\sigma_o(H) \leq \sigma'_o$, and let $\underline{\underline{U}}_V^{\sigma'_o}(k)$ correspond to $\sigma_o(H) = \sigma'_o$. Recall that if $K \in \underline{\underline{M}}_V(k)$, then $\sigma_o(H_K) = \sigma_o - \dim(W_K)$, where $W_K = \bigcap_i \varphi^i(K)$. It is clear that $\underline{\underline{M}}_V^{\sigma'_o}(k)$ is a closed subset of $\underline{\underline{M}}_V(k)$ and that $\{\underline{\underline{U}}_V^{\sigma'_o}(k)\}$ form a partition of $\underline{\underline{M}}_V(k)$ into locally closed subsets. For each totally isotropic subspace W of V, let $\underline{\underline{M}}_{V,W}(k) = \{K \in \underline{\underline{M}}_V(k) : W \subseteq K\}$, and note that there is a natural bijection :

$$\underline{\underline{M}}_{V,W}(k) \cong \underline{\underline{M}}_{W^\perp/W}(k).$$

Moreover, $\underline{\underline{M}}_V^{\sigma'_o}(k)$ admits a finite decomposition :

$$\underline{\underline{M}}_V^{\sigma'_o}(k) = \cup\{\underline{\underline{M}}_{V,W}(k) : \dim W = \sigma_o - \sigma'_o\},$$

i.e. is a union of smooth spaces, which are simply similar moduli spaces of smaller dimension. The intersection properties of these components are also easy to see : if W_1 and W_2 are totally isotropic, $\underline{\underline{M}}_{V,W_1}(k) \subseteq \underline{\underline{M}}_{V,W_2}(k)$ iff $W_1 \supseteq W_2$, and $\underline{\underline{M}}_{V,W_1}(k) \cap \underline{\underline{M}}_{V,W_2}(k) = \underline{\underline{M}}_{V,W_1+W_2}(k)$, which is empty unless W_1+W_2 is also totally isotropic. $\square$

We will now attempt to explain the relationship between the parameters (3.21) and the moduli space M_V. Suppose $K \in U_V^{\sigma_o}(k)$; then $L(K) = K \cap \varphi(K) \cap \ldots \varphi^{\sigma_o - 1}(K)$ is a line in $V \otimes k$, and in fact the map $L(K) \to \varphi^{\sigma_o - 1}(K/K \cap \varphi(K))$ is an isomorphism. It is not hard to see that this holds universally on $U = U_V^{\sigma_o}$:
$L_U = K_M \cap F^*(K_M) \ldots \cap (F^*)^{\sigma_o - 1}(K_M)$ is a rank one direct factor of $V \otimes \mathcal{O}_M$, and $L_U \to (F^*)^{\sigma_o - 1}(K_M/K_M \cap F^* K_M)$ is an isomorphism. Moreover, the quadratic form $< , >_V$ induces an isomorphism: $L_U \otimes (F^*)^{\sigma_o} L_U \to \mathcal{O}_U$, i.e. a trivialization of $L_U^{p^{\sigma_o}+1}$. Let $\widetilde{U} \to U$ be the associated finite étale cover, over which there exists a section e of $L_{\widetilde{U}}$ such that $<e, (F^*)^{\sigma_o} e> = 1$. The sections a_i of $\Gamma(\widetilde{U}, \mathcal{O}_{\widetilde{U}})$ defined by $a_i = <e, (F^*)^{\sigma_o + i} e>$ give us a morphism $\widetilde{U} \to A^{\sigma_o - 1}$. We will see that this mor-

phism is finite, whence $\tilde{U}$ and U are affine.

In order to be really precise, it is convenient to introduce some additional functors. Recall that if A is an $\mathbb{F}_p$-algebra, $\varphi : V \otimes A \to V \otimes A$ is the F_A^*-linear endomorphism $id_V \otimes F_A^*$.

4.9 Definition. A "strictly characteristic line in $V \otimes A$" is an $\ell \subseteq V \otimes A$ such that :

4.9.1 The natural map : $\ell \oplus F^* \ell \oplus \ldots (F^*)^{2\sigma_0 - 1}(\ell) \to V \otimes A$ is an isomorphism.

4.9.2 $K(\ell) \underset{\text{def}}{=} \ell \oplus F^* L \oplus \ldots (F^*)^{\sigma_0 - 1}(\ell)$ is totally isotropic.

A "strictly characteristic vector" in $V \otimes A$ is an $e \in V \otimes A$ which spans a strictly characteristic line, such that $<e, (F^*)^{\sigma_0}(e)> = 1$. The set of strictly characteristic lines (resp. vectors) in $V \otimes A$ is denoted by $\underline{\underline{L}}_V(A)$ (resp. $\underline{\underline{\tilde{L}}}_V(A)$).

4.10 Proposition. The functors $\underline{\underline{\tilde{L}}}$, $\underline{\underline{L}}$, $\underline{\underline{\tilde{U}}}$ and $\underline{\underline{U}}$ are representable by affine schemes of finite type over $\mathbb{F}_p$. There is a commutative diagram :

$$\begin{array}{ccccccc} \tilde{L} & \xrightarrow{\tilde{\mu}} & \tilde{U} & \xrightarrow{\tilde{\lambda}} & \tilde{L} & \xrightarrow{\tilde{\alpha}} & A^{\sigma_0 - 1} \\ \downarrow & & \downarrow & & \downarrow & & \\ L & \xrightarrow{\mu} & U & \xrightarrow{\lambda} & L & & \end{array} .$$

The maps $\tilde{L} \to L$ and $\tilde{U} \to U$ are Galois (viz. finite and étale) with group $\mu_p^{\sigma_0 + 1}(k)$, and $\tilde{\alpha}$ is Galois with group $O(V, < , >_V)$. The composite $\tilde{\alpha} \circ \tilde{\lambda}$ is simply the map a (3.21.1), and $\tilde{\lambda} \circ \tilde{\mu}$, $\tilde{\mu} \circ \tilde{\lambda}$, $\lambda \circ \mu$, $\mu \circ \lambda$ are $(F_{abs})^{\sigma_0 - 1}$.

Proof. The functor : $A \mapsto V \otimes A$ is represented by the spectrum of $\mathrm{Sym}(V^*)$, together with a "universal section" e of V, and the subfunctor :
$A \mapsto \{e \in V \otimes A : e, \varphi(e) \ldots \varphi^{2\sigma_0 - 1}(e)$ is a basis for $V \otimes A\}$ is represented by the affine open subset obtained by inverting the determinant δ of the matrix made up of these vectors. It is clear that $\underline{\underline{\tilde{L}}}$ corresponds to the closed subscheme $\tilde{L}$ of this scheme defined by the ideal generated by $\{<e,e>, <e, \varphi(e)> \ldots <e, \varphi^{\sigma_0 - 1} e>, <e, \varphi^{\sigma_0}(e)> - 1\}$, which is again affine.

Define $t_i = \langle e, \varphi^{\sigma_o+i}(e)\rangle \in \Gamma(\tilde{L}, \mathcal{O}_{\tilde{L}})$; then $t_1 \ldots t_{\sigma_o-1}$ define a map $\alpha : \tilde{L} \to A^{\sigma_o-1}$, which is Galois with group O(V). In fact, the proof of (3.22) used nothing other than the invertibility of the matrix for $\langle\ ,\ \rangle$, and is just as valid over $\tilde{L}$. Thus, there exist elements $\lambda_2 \ldots \lambda_{\sigma_o}, \mu_2 \ldots \mu_{\sigma_o} \in \Gamma(A^{\sigma_o-1}, \mathcal{O}_{A^{\sigma_o-1}})$ such that $\varphi^{2\sigma_o}(e) = e + \lambda_2\varphi(e) + \ldots \lambda_{\sigma_o}\varphi^{\sigma_o-1}(e) + \mu_2\varphi^{\sigma_o+1}(e) + \ldots \mu_{\sigma_o}\varphi^{2\sigma_o-1}(e)$. These are obviously finite and étale equations for the coordinates of e over A^{σ_o-1}.

It is clear that the map $\tilde{L} \to L$ sending e to span(e) identifies $\underline{\underline{L}}$ as the quotient of $\underline{\underline{\tilde{L}}}$ by $\mu_{p^{\sigma_o+1}}(k)$, hence $\underline{\underline{L}}$ is represented by another affine scheme L. Define μ by $\ell \mapsto K(\ell)$ and λ by $K \mapsto \ell_K = K \cap \varphi(K) \ldots \cap \varphi^{\sigma_o-1}(K)$. Then $(\lambda\circ\mu)(\ell) = \varphi^{\sigma_o-1}(\ell)$ and $(\mu\circ\lambda)(K) = \varphi^{\sigma_o-1}(K)$, hence $\lambda\circ\mu$ and $\mu\circ\lambda$ are $(F_{abs})^{\sigma_o-1}$, and U is also affine. Notice that $\underline{\underline{\tilde{U}}}(A) = \{(K,e) : K \in U(A),\ e \in \ell_K,\ \langle e, \varphi^{\sigma_o}(e)\rangle = 1\}$; set $\tilde{\lambda}(K,e) = e \in \tilde{L}(A)$, and $\tilde{\mu}(e) = (K(\text{span}(e)), \varphi^{\sigma_o-1}(e))$. It is clear that $\alpha\circ\tilde{\lambda}$ is simply (3.21.1). Since in the proof of (3.22) we showed that the set theoretic fibers of $\alpha\circ\tilde{\lambda}$ are a torsor under O(V), it is clear that O(V) is the Galois group of α. □

We are now ready to find the connected components of M_V. It turns out that, just like Gen_V, M_V is connected over F_p, but has two geometric components. More precisely, recall that $H^0(\text{Gen}_V, \mathcal{O}_{\text{Gen}}) \cong Z_V$ (the center of $C^+(V)$) is isomorphic to $\mathbf{F}_{p^2}$, via a map $e : \text{Gen}_V \to \text{Spec } Z_V$. Since O(V) acts nontrivially on Z_V, we have no right to identify Z_V with $\mathbb{F}_{p^2}$. It is easy to check, however, that if $W \subseteq V$ is isotropic, the natural map $\text{Gen}_{W^\perp/W} \to \text{Gen}_V$ induces a natural isomorphism $Z_V \to Z_W$, and we can therefore identify these two fields. Via the natural maps $M_V \to \text{Gen}_V \to \text{Spec } Z_V$ we obtain a structure of a Z_V-scheme on M_V.

4.11 <u>Proposition. With the above structure of $Z_V \cong \mathbb{F}_{p^2}$-scheme, M_V is absolutely irreducible</u>.

<u>Proof</u>. The proof is by induction on σ_o. The cases of $\sigma_o = 1$, 2 and 3 are

covered by the explicit calculations (4.7), and the induction step works if $\sigma_o \geq 3$. Assuming the proposition for $\sigma_o - 1$, note that if $\dim V = 2\sigma_o$, $U_V^{\sigma_o} \subseteq M_V$ is an affine open subset of the smooth projective scheme M_V, and hence its complement $M_V^{\sigma_o - 1}$ meets every geometric component. Thus it suffices to prove that $M_V^{\sigma_o - 1}$ is geometrically connected. But $M_V^{\sigma_o - 1} = \cup \{M_{V,W} : W \subseteq V$ is an isotropic line$\}$, and each $M_{V,W} \cong M_{W^\perp/W}$ is geometrically connected by the induction hypothesis. Hence it suffices to prove that the $M_{W,W'}$s intersect enough. This follows from :

4.12 Lemma. Suppose $\sigma_o \geq 3$ and ℓ, ℓ' are isotropic lines in V. Then there exists a sequence $(\ell_o, \ldots \ell_n)$ of isotropic lines such that $\ell = \ell_o$, $\ell' = \ell_n$, and such that ℓ_i and ℓ_{i+1} span an isotropic plane.

Proof. The isotropic lines in V correspond to $\mathbb{F}_p$-valued points of the non-singular quadric $Q(V) \subseteq \mathbb{P}V$ defined by $< , >_V$. Since $\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$ interchanges the families of characteristic subspaces, the trace of Frobenius on middle dimensional cohomology is zero, and the number of such points is given by : $1+p+\ldots+p^{2\sigma_o-2}-p^{\sigma_o-1}$. The isotropic planes in V correspond to lines in $Q(V)$. Fix a $q \in Q(V)$; then the lines through q correspond to the points in $Q(q^\perp/q)$. Since this is again a "non-neutral" quadric, there are $1+\ldots p^{2\sigma_o-4}-p^{\sigma_o-2}$ such lines. Each line contains p points other than q, and two such lines intersect only in q. Thus, the set $S(q)$ of points q' such that q and q' are contained in a line has $p(1+\ldots p^{2\sigma_o-4}-p^{\sigma_o-2})+1$ elements.

Now suppose $\sigma_o = 3$, and fix a line L contained in $Q(V)$. Notice that if q and q' span L, and if $q'' \in S(q) \cap S(q')$, then the span of q, q', q'' is contained in Q, and is defined over $\mathbb{F}_p$. Since there are no $\mathbb{F}_p$-rational planes contained in Q, this span must be L. Thus, $S(q) \cap S(q') = L$, and hence $\cup\{S(q) : q \in L\}$ is the disjoint union $\amalg \{S(q) - L\} \amalg L$, which has $(p+1)p^3 + (1+p) = 1+p+p^3+p^4$ elements. Since this accounts for all the points in Q, the lemma is proved in this case.

In general, suppose ℓ, ℓ' are isotropic in V. If ℓ and ℓ' are orthogonal, there is nothing to prove. If not, they span a hyperbolic plane W. The orthogonal complement $W^{\perp}$ of W is again nonneutral, and we can write $W^{\perp} = V' \oplus V''$ with V'' hyperbolic, V' of dimension 4 and nonneutral. Then $V = W \oplus V' \oplus V''$. The proof for $\sigma_0 = 3$ allows us to work inside $W \oplus V'$, proving the general case. □

§5. FAMILIES OF CRYSTALS.

In order to explain precisely the sense in which our parameters are moduli, we have to speak about families of F-crystals, ideally over an arbitrary base scheme S. Unfortunately, technical difficulties involving PD envelopes prevent us from dealing effectively even with an S as simple as $k[X,Y]/(X^2,XY,Y^2)$. I have therefore chosen to restrict attention to the case of a smooth base scheme (although, with considerable effort, local complete intersections could probably also be handled). We will see that there is a universal K3 crystal H_M with T-structure over the moduli space M_V, so that any K3 crystal with T-structure over a smooth S is canonically isomorphic to $f^*(H_M)$, for a unique $f : S \longrightarrow M_V$. Moreover, we will show that the supersingular locus in the versal deformation of a supersingular polarized elliptic K3 is a union of smooth schemes Σ, that on a finite étale cover $\tilde{\Sigma}$ of Σ the associated crystal admits a T-structure, and that the corresponding period mapping $\tilde{\Sigma} \longrightarrow M_V$ is étale.

Let S be a smooth k-scheme (where k is still an algebraically closed field of characteristic $p > 2$). For the notion of an F-crystal on $(S/W(k))_{cris}$, and of the Hodge and conjugate filtrations attatched to such a crystal, we must refer the reader to [15]. A "K3-crystal on (S/W)" is such an F-crystal H, endowed with a perfect pairing: $H \otimes H \longrightarrow \mathcal{O}_{S/W}$ (a morphism of crystals) such that $\langle \tilde{\Phi}(x), \tilde{\Phi}(y) \rangle = p^2 F^* \langle x, y \rangle$ for any two sections x,y of F^*H, and such that $gr_F^{\cdot} H_S$ is a locally free $\mathcal{O}_S$-module, with $gr_F^0 H_S$ of rank one. The base-changing results of [15, 1.12] show that formation of the Hodge and conjugate filtrations is compatible with pull-back $f : S' \longrightarrow S$, and hence f^*H will again be a K3 crystal. Moreover, if $\pi : X \longrightarrow S$ is a family of K3 surfaces, then $R^2\pi_{cris*}\mathcal{O}_{X/W}$ is a K3 crystal on (S/W).

5.1 <u>Proposition. If</u> H <u>is a</u> K3 <u>crystal on</u> (S/W), <u>then the following are equivalent</u> :

i) <u>For every closed point</u> s <u>of</u> S, <u>the</u> F-<u>crystal</u> $H(s)$ <u>on</u> (k/W) <u>is supersingular</u>.

i)^{bis} <u>For every geometric point</u> s <u>of</u> S, <u>the</u> F-<u>crystal</u> $H(s)$ <u>on</u> $(k(s)/W(k(s))$ <u>is supersingular</u>.

ii) <u>If</u> $(S', F_{S'})$ <u>is a local lifting of</u> (S, F_S) <u>to</u> W, <u>then the map</u> $\Phi^{(n)}_{S'} : (F^n_{S'})^* H_{S'} \longrightarrow H_{S'}$ <u>is divisible by</u> p^{n-1}.

<u>Proof</u>. Fix a local lifting $(S', F_{S'})$ of (S, F_S) to W. For each closed $s \in S$, there is a unique Teichmuller point $s' : \operatorname{Spec} W \longrightarrow S'$ "prolonging" s, and the F-crystal $H(s)$ is just $(s')^* \Phi_S : F^*_W (s')^* H_{S'} \cong (s')^* F^*_{S'} H_{S'} \longrightarrow (s')^* H_{S'}$. Since a matrix in $\mathcal{O}_{S'}$ is divisible by p^{n-1} iff all its Teichmuller values are, the equivalence of (i) and (ii) follows easily from (3.6), and clearly (ii) implies (i)^{bis} implies (i). It is perhaps also worthwhile to remark that the equivalence of (i)^{bis} and (ii) can be made to work in a slightly more general context, e. g. if S is the spectrum of a local ring. □

We shall say that a K3-crystal on (S/W) is "supersingular" iff it satisfies the above conditions. I would like to remark that one of the problems with nonsmooth S is the lack of an adequate definition of a family of supersingular crystals : (i) is clearly inadequate (e. g. if S is not reduced) and (ii) seems unmanageable because of the presence of p-torsion in PD envelopes. If we stick to the smooth case, however, everything works nicely. It is even possible to introduce an analogue of the Tate module T_H in a relative setting. Notice, however, that since Artin's invariant σ_o can jump in a family, we cannot expect formation of T_H to commute with base change.

Recall that there is an equivalence of categories between p-adic constant tordu sheaves on S and unit root F-crystals on (S/W) [10, 5.5], i. e. F-crystals E such that the map $\Phi : F^* E \longrightarrow E$ is an isomorphism. Since S is locally liftable over W, nothing changes if we replace $\tilde{\Phi}$ by $p\tilde{\Phi}$ (i. e. the Tate twist functor is fully faithful). Let us agree to call an F-crystal for which Φ is p times an isomorphism a "Tate crystal".

5.2 Proposition. A supersingular K3 crystal H on (S/W) contains a universal Tate crystal E_H. That is, there is a morphism $i : E_H \longrightarrow H$, such that any $i' : E' \longrightarrow H$ with E' a Tate crystal factors uniquely through i. Dually, there is a universal morphism $H \longrightarrow L_H$, with L_H a Tate crystal.

Proof. We begin with L_H. Choose for the moment a local lifting $(S', F_{S'})$ of (S, F_S). By the previous result, we know that $\tilde{\Phi}^{(n)}_{S'} : (F_{S'})^{n*} H_{S'} \longrightarrow H_{S'}$ is divisible by p^{n-1}, and since S' is noetherian, $\sum_{n=0}^{\infty} p^{1-n} \operatorname{Im}(\tilde{\Phi}^{(n)}_{S'})$ is a coherent subsheaf $L_{S'}$ of $H_{S'}$. It is clear that $L_{S'}$ is invariant under the connection $\nabla_{S'}$, and under $p^{-1} \Phi_{S'}$. Now H necessarily has level 2, so there exists a $V_{S'} : H_{S'} \longrightarrow F^* H_{S'}$ such that $V_{S'} \circ \tilde{\Phi}_{S'}$ and $\tilde{\Phi}_{S'} \circ V_{S'}$ are multiplication by p^2. If $x = \sum p^{1-n} \tilde{\Phi}^{(n)}_{S'} (x_n)$ is a section of $L_{S'}$, $p^{-1} V_{S'}(x) = \sum p^{-n} V_{S'} \tilde{\Phi}^{(n)}_{S'} (x_n) = F^*_{S'}(\sum p^{2-n} \tilde{\Phi}^{(n-1)}(x_n) \in F^*_{S'} L_{S'})$. Since $(p^{-1} \Phi_{S'}) \circ (p^{-1} V_{S'})$ is the identity, $p^{-1}\Phi_{S'}$ is an isomorphism. It follows that $(L_{S'}, p^{-1}\Phi_{S'})$ is a Tate crystal (and in particular that $L_{S'}$ is locally free).

It is obvious from the definition that $pH \subseteq L_{S'}$, and we define $j : H \longrightarrow L_{S'}$ to be multiplication by p followed by the inclusion. Suppose $j' : H \longrightarrow L'$, with L' a Tate crystal, and suppose $x \in L_{S'}$. Then $px \in H_{S'}$, and in fact px can be written $px = \sum p^{1-n} \tilde{\Phi}^{(n)}_{S'} (x_n)$. Then $j'(px) = \sum p^{1-n} \tilde{\Phi}^{(n)}_{S'} (j'(x_n)) = py$, where $y = \sum p^{-n} \tilde{\Phi}^{(n)}_{S'} (j'(x_n))$. It is clear that $x \longmapsto y$ defines the unique homomorphism making the diagram commute. This universal property implies that $L_{S'}$ is unique up to unique isomorphism, and hence allow us to glue these local constructions and obtain L_H globally. We simply take $i : E_H \longrightarrow H$ to be the dual of $H \longrightarrow L_H$, followed by the inverse of $\beta_H : H \xrightarrow{\cong} H^\vee$ (induced by $\langle \ , \ \rangle_H$). □

Notice that $pH \subseteq E_H$, so that we have $E_H \longrightarrow H \longrightarrow E_H$, the composition being multiplication by p. It follows that for any s, $E_H(s) \longrightarrow H(s) \longrightarrow E_H(s)$ is still multiplication by p, and so $E_H(s) \longrightarrow H(s)$ is injective. By the universal nature of $E_{H(s)}$, we see that $E_H(s)$ must be contained in $E_{H(s)}$, but in general we will not have equality. Indeed, it is clear that just as before, the discriminant of $\langle \ , \ \rangle|_{E_H} = p^{2\sigma_o}$ for some σ_o, and that $\sigma_o = \sigma_o(H(s)) +$ length$(E_{H(s)}/E_H(s))$ for every geometric point s of S. If S is irreducible, and if $\bar{\eta}$ is a geometric generic point, then since $\bar{\eta}$ is flat over S, formation of E commutes with pull back to $\bar{\eta}$, i. e. $E_{H(\bar{\eta})} = E_H(\bar{\eta})$, and so $\sigma_o = \sigma_o(H(\bar{\eta}))$. This implies that σ_o decreases under specialization. (In fact, it will follow from the representability theorem below and the stratification of M_V that σ_o is semicontinuous.)

The dictionary between Tate crystals and p-adic representations implies that on some (possibly infinite) étale covering $\tilde{S}$ of S, E_S becomes constant, i. e. isomorphic to the pull back of some K3-lattice via the structure map $\pi : \tilde{S} \longrightarrow$ Spec W. We will denote $\pi^*(T)$ simply by T. Thus on $\tilde{S}$, H admits a T-structure, that is, a map $T \longrightarrow E_H$. The category of K3-crystals with T-structure is defined just as before ; again, the only automorphisms in this category are the identity maps.

Fix a K3-lattice T, let $V = T_o \otimes \mathbb{F}_p$, and $M = M_V \times \operatorname{Spec} k$, where M_V is the moduli space (4.6). We will construct a universal K3-crystal with T-structure on (M/W).

5.3 <u>Theorem</u>. <u>There is a</u> K3-<u>crystal with</u> T-<u>structure</u> $i_M : T \longrightarrow H$ <u>on</u> (M/W) <u>with the following universal property</u> : Any K3-<u>crystal with</u> T-<u>structure</u> <u>over a smooth</u> (S/k) <u>is isomorphic to</u> $f^*(i_M)$, <u>for some unique</u> $f : S \longrightarrow M$.

<u>Proof</u>. Let $\underline{\underline{M}}_T$ be the functor which to any smooth S assigns the set of isomorphism classes of K3-crystals on (S/W) with T-structure. We have to find an isomorphism of functors : $\underline{\underline{M}}_V \longleftrightarrow \underline{\underline{M}}_T$. It suffices to consider smooth affine schemes ; we will write $\underline{\underline{M}}_V(A) = \underline{\underline{M}}_V(S)$ if $S = \operatorname{Spec} A$.

To construct the arrow $\underline{\underline{M}}_V \longrightarrow \underline{\underline{M}}_T$, let A' be a lifting of A to W and $F^*_{A'}$ a lifting of its Frobenius. Then the value of the F-crystal T^* on $S' = \operatorname{Spec} A'$ is simply $T^* \otimes_{\mathbf{Z}_p} A'$, and its Frobenius $\Phi_{S'}$ is $p\, id_{T^*} \otimes F^*_{A'}$. We have $T^*/T \cong V$, hence a natural map $T^*_{S'} \longrightarrow V \otimes A$. If $K \in \underline{\underline{M}}_V(A)$, let $H_{S'}$ be the inverse image of $F^*(K)$ in $T^*_{S'}$. Since $F^*(K) \subseteq V \otimes A$ is horizontal $H_{S'} \subseteq T^*_{S'}$ is also. It is apparent, just as before, that $\Phi_{S'}$ maps $H_{S'}$ to itself and that $H_{S'}$ inherits a perfect pairing. The only new feature is that everything is compatible with the connections, which is clear.

We must check that this construction is compatible with base change. Suppose B' is an A'-algebra which is p-torsion free, and that $F_{B'}$ is a lifting of the absolute Frobenius of $B = B'/pB'$ which is compatible with $F_{A'}$. Then I claim that the F-crystal $H_{B'}$, obtained by applying the above construction to the image K_B of K under $M_V(A) \longrightarrow M_V(B)$, is simply $H_{A'} \otimes_{A'} B'$. To see this, tensor the exact sequence :

$$0 \longrightarrow H_{A'} \longrightarrow T^* \otimes_{\mathbf{Z}_p} A' \longrightarrow (V \otimes A)/F^*_A(K) \longrightarrow 0$$

with B' obtain :

$$0 \longrightarrow H_{A'} \otimes B \longrightarrow T^* \otimes_{\mathbf{Z}_p} B' \longrightarrow (V \otimes B)/F^*_B(K_B) \longrightarrow 0.$$

Clearly the only thing that needs to be checked is the injectivity of $H_{A'} \otimes B \longrightarrow T^* \otimes_{\mathbf{Z}_p} B'$, i. e. that $\operatorname{Tor}_1^{A'}((V \otimes A)/F^*_A(K), B') = 0$. Since $(V \otimes A)/F^*_A(K)$ is a projective A-module, this reduces to $\mathrm{Tor}_1^{A'}(A, B') = 0$, which is true because B' is p-torsion free.

In particular, the above paragraph tells us that if $A' \longrightarrow W$ is a Teichmuller point, $H_{S'} \otimes W$ is precisely the F-crystal on (k/W) obtained by specializing K and applying the dictionary (4.3). This implies that $H_{S'}(s)$ is a K3 crystal at every point, hence that $H_{S'}$ is a K3 crystal. Hence [15,1.7] the connection on $H_{S'}$ is nilpotent, and we have the right to call $H_{S'}$ an F-crystal, since the connection allows us to compare different liftings. Thus, we have indeed an arrow : $\underline{\underline{M}}_V(A) \longrightarrow \underline{\underline{M}}_T(A)$, whose functoriality we have already established.

The construction of the inverse is essentially similar : If $i : T \longrightarrow H \in M_T(A)$, $(T^* \otimes \mathcal{O}_S)/(\mathrm{Im}\, H_S)$ has rank $\sigma_o(T)$ at every point, hence is locally free. We conclude that $\mathrm{Im}\, H_S \hookrightarrow T_o \otimes \mathcal{O}_S$ is a local direct factor, whose formation therefore commutes with base change. Moreover, since it is <u>horizontal</u>, and S is smooth, it descends through Frobenius, i. e. it is $F_S^*(K_S)$ for some unique $K_S \subseteq T_o \otimes \mathcal{O}_S$. Since K_S is characteristic at every point, it is characteristic, and hence defines an element of $\underline{\underline{M}}_V(A)$. It is clear that this is inverse to the map $\underline{\underline{M}}_V \longrightarrow \underline{\underline{M}}_T$. □

Recall from [15, § 2] that an F-crystal over any smooth base S gives rise to a Kodaira-Spencer map : $\rho : \mathrm{gr}_F^{\cdot} H_S \longrightarrow \mathrm{gr}_F^{\cdot -1} H_S \otimes \Omega^1_{S/k}$, induced by the connection. We can use this to relate our universal K3-crystal with T-structure to the tangent space of M. First of all, the punctual calculation of the Hodge filtration of H globalizes to become the following diagram :

5.4.1
$$\begin{array}{ccccccccc}
0 \longrightarrow & F^*(K) & \longrightarrow & T\otimes\mathcal{O}_M & \longrightarrow & H_M & \longrightarrow & F^*(K) & \longrightarrow 0 \\
& \| & & \| & & \uparrow & & \uparrow & \\
0 \longrightarrow & F^*(K) & \longrightarrow & T\otimes\mathcal{O}_M & \longrightarrow & F^1H_M & \rightarrow & K\cap F^*(K) & \longrightarrow 0 \\
& \| & & \uparrow & & \uparrow & & \uparrow & \\
0 \longrightarrow & F^*(K) & \longrightarrow & K+F^*(K) & \longrightarrow & F^2H_M & \rightarrow & 0. &
\end{array}$$

Evidently the image of $T \otimes \Theta_M$ in $F^1 H_M$ is a horizontal subspace of H_M, and contains $F^2 H_M$. Thus the Kodaira-Spencer map factors :

5.4.2
$$\begin{array}{ccc} gr_F^1 H_M & \searrow & \\ \downarrow & & \\ gr_F^1 H_M/\mathrm{Im}(T\otimes \Theta_M) & \longrightarrow & gr_F^o H_M \otimes \Omega^1_{M/k} \\ \downarrow \cong & & \downarrow \cong \\ K \cap F^*(K) & \longrightarrow & F^*(K)/K\cap F^*(K) \otimes \Omega^1_{M/k} \end{array}$$

It is clear that the bottom arrow is precisely the dual of the canonical isomorphism (4.6.2) which calculates the tangent space to M. Since this construction is compatible with pull-back, we conclude :

5.4 <u>Corollary</u>. <u>If</u> $i : T \longrightarrow H$ <u>is a K3-crystal with T-structure on (S/W) and if</u> $f : S \longrightarrow M$ <u>is the corresponding map, we get a commutative diagram</u> :

$$\begin{array}{ccc} T^1_{S/k} & \xrightarrow{df} & f^* T^1_{M/k} \\ \text{Kodaira-Spencer} \downarrow & & \downarrow \cong \\ \mathrm{Hom}\left[gr_F^1 H_S/\mathrm{Im}(T\otimes\Theta_S), gr_F^o H_S\right] & \xrightarrow{\sim} & \mathrm{Hom}\left[K_S\cap F^*(K_S), F^*(K_S)/K_S\cap F^*(K_S)\right] \end{array}$$

Let us now try to relate our period space to families of K3 surfaces. If we had developed a theory valid over a singular parameter space, we could work directly with the construction T_H. As it is, however, we must resort to $\underline{Pic}_X$. Thus, we have to restrict our attention to K3's with $\rho = 22$ (i. e. we have to assume Tate's conjecture). Fortunately, Artin has proved the abundance of these [2]. I would also like to explain how his result follows from the crystalline theory.

5.5 <u>Proposition (Artin)</u>. <u>Let</u> $f : X \longrightarrow S$ <u>be a family of K3 surfaces, with each</u> $X(s)$ <u>supersingular. Assume that</u> S <u>is connected and that for some point</u> s <u>of</u> S, $\rho(X(s)) = 22$. <u>Then the same is true at every point</u>.

If, moreover, S is the spectrum of a complete local domain and $\bar{\eta}$ is a geometric generic point, the map $\mathrm{Pic}(X) \longrightarrow \mathrm{Pic}\, X(\bar{\eta})$ is an isomorphism.

Proof. First assume that S is the spectrum of a formal power series ring. Then $H = R^2 f_{\mathrm{cris}*} \mathcal{O}_{X/W}$ forms a supersingular K3 crystal on (S/W). Assume that the closed fiber X_o has $\rho = 22$, so that by (1.6), $NS(X_o) \otimes \mathbf{Z}_p \xrightarrow{\simeq} T_{H(o)}$. Now the cokernel of the map $T_{H(o)} \longrightarrow T_{H(o)}$ is killed by p, so that $p\, c_1(L_o) \in T_H(o)$ for any $L_o \in \mathrm{Pic}(X_o)$. Since T_H is a Tate crystal on a Henselian scheme S, the map $T_H^{\nabla} \longrightarrow T_{H(o)}$ is an isomorphism, so $p\, c_1(L_o)$ extends to a global section of H. By (1.13), this implies that L_o^p extends to S.

Now suppose $f : X \longrightarrow S$ is as in the statement of the proposition. By specialization and generalization via discrete valuation rings, one sees easily that $\rho = 22$ everywhere. Moreover, the relative Picard scheme $\underline{\mathrm{Pic}}_X$ is representable by a scheme which is proper and unramified over S (but only locally of finite type, of course) [1, 7.3]. This implies the last statement. □

Now let X_o be a K3-surface with $\rho = 22$. As Artin observed in [2, § 4], it follows from the theory of quadratic forms that the intersection form on $NS(X_o)$ cannot be divisible by p; this allows us to find an ample line bundle L_o on X_o such that $L_o.L_o$ is not divisible by p. Moreover, we know by (1.6) that $NS(X_o) \otimes \mathbf{Z}_p$ is canonically isomorphic to the Tate module T_{H_o} of $H_o = H^2_{\mathrm{cris}}(X_o/W)$, hence $\sigma_o \leq 10$ (cf. also (7.6) and its proof). This will enable us to control the period map associated to a deformation of X_o. Consider first the versal deformation (X, L) of (X_o, L_o), which lives over $S = \underline{\mathrm{Spec}}\, k[[t_1 \ldots t_{19}]]$. According to Artin, the closed subscheme $S_\infty \subseteq S$ defined by the condition that the formal Brauer group of X/S have infinite height over S_∞ is defined by 10 equations [2, § 7], and $X(\bar{s})$ has $\rho = 22$ iff $\bar{s}$ is a (geometric) point of S_∞.

5.6 Theorem. Every irreducible component Σ of $(S_\infty)_{red}$ is smooth of dimension 9, and the p-adic ordinal of the intersection form on the Neron Severi group of the generic fiber X_η is 20. The K3-crystal H_Σ of $X|_\Sigma$ on Σ has a natural $NS(X_\eta)\otimes \mathbf{Z}_p$-structure, and the corresponding period map $\Sigma \to M$ is étale.

Proof. It follows from (5.5) and its proof that the natural map : $\mathrm{Pic}(X|_\Sigma) \to \mathrm{Pic}(X_\eta)$ is an isomorphism, and we identify these groups. If $\bar{s}$ is a geometric point of Σ and $W(\bar{s})$ is the Witt ring of $k(\bar{s})$, we obtain a natural map : $\mathrm{Pic}(X_\eta)\otimes W(\bar{s}) \longrightarrow H^2_{cris}(X(\bar{s})/W(\bar{s}))$, which is compatible with the quadratic forms. Moreover, if $\bar{\eta}$ is a geometric generic point, $\mathrm{Pic}(X_\eta) \xrightarrow{\cong} \mathrm{Pic}(X_{\bar{\eta}})$, and so $\mathrm{Pic}(X_\eta)\otimes \mathbf{Z}_p = T_\eta$ is a K3-lattice, and we can view the map : $T_\eta \longrightarrow H^2_{cris}(X(\bar{s})/W(\bar{s}))$ as a T_η-structure on $H^2_{cris}(X(\bar{s})/W(\bar{s}))$.

Consider in particular the closed point s_o of S, corresponding to the maximal ideal m of $k[[t_1 \ldots t_{19}]]$. After choosing a basis ω of $H^o(X_o, \Omega^2_{X_o/k})$, recall that we get an isomorphism (2.12) :

$$\rho : H^1(X_o, \Omega^1_{X_o/k})/k.c_1(L_o) \longrightarrow m/m^2 .$$

Let I be the ideal defining Σ ; since the elements of $\mathrm{Pic}(X_\eta) \cong \mathrm{Pic}(X|_\Sigma)$ extend to Σ, it is clear from the obstruction theory (2.23) that $\rho(\mathrm{Pic}(X_\eta)) \subseteq I/I \cap m^2$. We obtain a diagram :

$$\begin{array}{ccccccc}
\mathrm{Pic}(X_\eta)\otimes k & \longrightarrow & F^1H^2_{DR}(X_o/k) & \longrightarrow & F^1H^2_{DR}(X_o/k)/\mathrm{Im}(\mathrm{Pic}(X_\eta)\otimes k) & & \\
\downarrow{\scriptstyle \rho''} & & \downarrow{\scriptstyle \rho} & & \downarrow{\scriptstyle \bar{\rho}} & & \\
I/I\cap m^2 & \longrightarrow & m/m^2 & \longrightarrow & \bar{m}/\bar{m}^2 & \longrightarrow & 0
\end{array}$$

Notice that $H^2_{DR}(X_o/k)/\mathrm{Im}(\mathrm{Pic}(X_\eta)\otimes k) \cong H^2_{cris}(X_o/W)/(T_\eta \otimes W)$ has length $\sigma_o(T_\eta)$, hence $F^1/\mathrm{Im}(\mathrm{Pic}(X_\eta)\otimes k)$ has length $\sigma_o(T_\eta) - 1 \le 9$. On the other hand, since $(S_\infty)_{red}$ is defined by 10 equations, $\dim(\Sigma) \ge 9$, hence $\dim(\bar{m}/\bar{m}^2) \ge 9$. But $\bar{\rho}$ is surjective, hence $\sigma_o(T_\eta) = 10$, $\dim(\bar{m}/\bar{m}^2) = 9$, and

$\bar{\rho}$ is an isomorphism. This tells us that Σ is smooth, and we can view $T_\eta \longrightarrow H^2_{cris}(X|_\Sigma)$ as a T_η-structure on a K3-crystal on Σ. Thanks to our identification (5.4) of the derivative of the period map, we see that it is étale. □

5.7 Remark. If we choose a K3-lattice T with $\sigma_0(T) = 10$, then for each Σ there is an isomorphism $T \xrightarrow{\cong} T_\eta$, hence we obtain a T-structure on H_Σ. Evidently this T-structure is canonical, up to the action of $\mathrm{Aut}(T)$. By an argument dual to (4.2), one sees easily that this orbit is determined by the kernel of the dual map : $T_H^\vee \otimes \mathbf{F}_p \longrightarrow T_\eta^\vee \otimes \mathbf{F}_p$, which is a totally isotropic subspace L of $(T_H^\vee)_0 \otimes \mathbf{F}_p$ of dimension $\sigma_0(T_H^\vee) - \sigma_0(T_\eta^\vee) = \sigma_1(T_\eta) - \sigma_1(T_H) = 10 - \sigma_0(T_H)$.

§6. THE TORELLI THEOREM FOR SUPERSINGULAR ABELIAN VARIETIES.

In characteristic $p > 0$, there are roughly $\frac{p-1}{12}$ isomorphism classes of supersingular elliptic curves, all isogenous, and all with isomorphic crystalline cohomology. Any supersingular abelian variety of dimension $n \geq 2$ is isogenous to a product of such elliptic curves, and it turns out that such varieties have moduli. In [14], it is proved that deformations of a supersingular abelian variety are classified by deformations of the associated Dieudonné module, and a classifying space of the corresponding Dieudonné modules is constructed. Regarding the Dieudonné module of an abelian variety X as its H^1_{cris}, we find an extra bit of structure coming from the trace map of crystalline cohomology. It turns out that this will allow us to refine the work of [14], to obtain a Torelli theorem for supersingular abelian varieties of dimension $n \geq 2$.

If Y is an abelian variety of dimension n over an algebraically closed field k of characteristic $p > 0$, $H^1_{cris}(Y/W)$ is a free W-module of rank $2n$ with an F^*_W-linear endomorphism Φ, plus an isomorphism : $tr : \Lambda^{2n} H^1_{cris}(Y/W) \to W$ coming from cup-product : $\Lambda^{2n} H^1_{cris}(Y/W) \xrightarrow{\simeq} H^{2n}_{cris}(Y/W)$ followed by the trace map : $H^{2n}_{cris}(Y/W) \to W$. Notice that if $f : Y_1 \to Y_2$ is an isogeny, then via the isomorphism tr, $\Lambda^{2n} f$ is carried to multiplication by $\deg(f)$. In particular, the relative Frobenius morphism induces multiplication by p^n, and $tr \circ \Lambda^n \Phi = p^n F^*_W \circ tr$.

6.1 Definition. An "abelian crystal of genus n" is an F-crystal (H, Φ) of rank $2n$ and weight one, with nonzero Hodge numbers $h^0 = h^1 = n$, together with an isomorphism of crystals : $tr : \Lambda^{2n} H \to W[-n]$.

6.2 Theorem. If $n \geq 2$, the functor H^1_{cris} defines a bijection between the isomorphism classes of supersingular abelian varieties of dimension n and of supersingular abelian crystals of genus n.

Proof. The proof of injectivity rests on two well-known basic facts and one "miracle". The first basic fact says that a morphism of abelian varieties which induces the zero map on $\mathbb{Z}/\ell\mathbb{Z}$-cohomology (respectively, on de Rham cohomology), is divisible by ℓ (respectively by p). Thus, we have :

6.3 Lemma. If Y_1 and Y_2 are abelian varieties, the maps :

$$\mathrm{Hom}[Y_1,Y_2] \otimes \mathbb{Z}_\ell \to \mathrm{Hom}[H^1(Y_2,\mathbb{Z}_\ell),H^1(Y_1,\mathbb{Z}_\ell)]$$

and

$$\mathrm{Hom}[Y_1,Y_2] \otimes \mathbb{Z}_p \to \mathrm{Hom}[H^1_{cris}(Y_2/W),\ H^1_{cris}(Y_1/W)]$$

are injective, with torsion free cokernels. □

The "miracle", which is also well-known, is the following :

6.4 Lemma. If Y_1 and Y_2 are supersingular and of the same dimension, the above arrows are isomorphisms. (Of course, in the target of the second arrow, we take only maps of F-crystals).

Proof. Since we know the cokernels are torsion free, it suffices to prove that the maps become isomorphisms after we tensor with $\mathbb{Q}$. Thus we may replace Y_1 and Y_2 by any isogenous varieties, e.g. by $E \times \ldots E$, where E is a supersingular elliptic curve. By the Kunneth formula, it suffices to consider the case $Y_1 = Y_2 = E$. But then $H=\mathrm{End}(E)\otimes \mathbb{Q}$ is known to be a division algebra of rank 4 over $\mathbb{Q}$, and this implies that the ℓ-adic map : $H \otimes \mathbb{Q}_\ell \to \mathrm{End}(H^1(E,\mathbb{Q}_\ell))$ is an isomorphism. To check the claim when $\ell = p$, we have only to verify that $\mathrm{End}(H^1_{cris}(E/W) \otimes \mathbb{Q})$ has rank 4 over $\mathbb{Q}_p$. This follows from the following well-known :

6.5 Lemma. If E is a supersingular elliptic curve, $H^1_{cris}(E/W)$ admits a basis ω, η such that $\Phi(\omega) = p\eta$, $\Phi(\eta) = \omega$. In this basis, End $H^1_{cris}(E/W)$ becomes identified with "matrices" of the form :

$$\omega \longmapsto F^*(a)\omega + pF^*(b)\eta$$
$$\eta \longmapsto b\omega + a\eta$$

where a and b lie in $W(\mathbb{F}_{p^2})$. □

This is an easy calculation which we leave to the reader. Recall that (as follows from the above) H is a quaternion algebra of rank 4, split everywhere except at p and ∞, and that the reduced norm map $H \to \mathbb{Q}$ is simply the degree. Of course, the degree of an element is always positive, and in fact the map $H \to \mathbb{Q}^+$ is surjective (as follows, for instance, from [21, V §2, cor. 2]).

The second basic ingredient of the proof is the strong approximation theorem for semi-simple simply connected groups. I thank P. Deligne for explaining this theorem to me. We shall apply it as follows : if Y is a supersingular abelian variety of dimension n, consider the group $G(\mathbb{Q})$ of invertible elements of $\mathrm{End}(Y) \otimes \mathbb{Q}$ of degree one - clearly this is the set of $\mathbb{Q}$-points of an algebraic group G over $\mathbb{Q}$. It follows from the above that we have natural (anti) isomorphisms :

$$G(\mathbb{Q}_\ell) \longrightarrow \mathrm{Sl}\,(H^1(Y_{et}, \mathbb{Q}_\ell))$$
$$G(\mathbb{Q}_p) \longrightarrow \mathrm{Aut}(H^1_{cris}(Y/W) \otimes \mathbb{Q}, \Phi, tr).$$

In particular, $G(\mathbb{C})$ is isomorphic to $\mathrm{Sl}_{2n}(\mathbb{C})$, which is semi-simple and simply connected. Moreover, if $n \geq 2$, $G(\mathbb{R})$ is noncompact, and the strong approximation theorem implies that $G(\mathbb{Q})$ is dense in $G(\mathbb{A}_f)$, where $\mathbb{A}_f$ is the ring of finite adèles [19].

To prove the theorem, proceed as follows : Since Y_1 and Y_2 are supersingular, they are isogenous ; that is, there exists an element φ of $\mathrm{Hom}[Y_1, Y_2] \otimes \mathbb{Q}$ with $\deg(\varphi) > 0$. Since now : $(\mathrm{End}(Y_2) \otimes \mathbb{Q})^* \to \mathbb{Q}^+$ is surjective, we may as well assume that $\deg(\varphi) = 1$. For each ℓ, choose an isomorphism : $\theta_\ell : H^1(Y_1, \mathbb{Z}_\ell) \to H^1(Y_2, \mathbb{Z}_\ell)$ compatible with the trace maps -this is clearly possible- and let $\theta_p : H^1_{cris}(Y_1/W) \to H^1_{cris}(Y_2/W)$ be the given isomorphism of abelian crystals. For each ℓ, $H^1(\varphi, \mathbb{Q}_\ell)$ is a map $H^1(Y_2, \mathbb{Q}_\ell) \to H^1(Y_1, \mathbb{Q}_\ell)$, and it is integral for almost all ℓ. Composing this with θ_ℓ, we get an automorphism of $H^1(Y_2, \mathbb{Q}_\ell)$, hence a point of $G(\mathbb{Q}_\ell)$, and putting all these together, with $\theta_p \circ H^1_{cris}(\varphi)$ as well, we obtain a point $g \in G(\mathbb{A}_f)$. The subgroup K consisting of the stabilizer of $\prod_\ell H^1(Y_2, \mathbb{Z}_\ell) \times H^1(Y_2/W)$ is a compact open subgroup, so by strong approximation, the double coset space $G(\mathbb{Q})\backslash G(\mathbb{A}_f)/K$ is a single point. This means that after we multiply g by an element of K - which corresponds to a change in our choice of θ_ℓ's and θ_p - g lies in $G(\mathbb{Q})$. But then after modifying φ by this element g, we find that $\varphi \in \mathrm{Hom}[Y_1, Y_2] \otimes \mathbb{Q}$ has degree one and maps $H^1(Y_2, \mathbb{Z}_\ell) \to H^1(Y_1, \mathbb{Z}_\ell)$ for all ℓ, and also $H^1(Y_2/W) \to H^1(Y_1/W)$. This implies that φ is in fact a morphism ... hence an isomorphism.

This completes the proof of injectivity. We leave the proof of surjectivity to the reader. (Follow the method of [14] and (6.10).) □

6.6 Remark. It is of course well-known to arithmeticians that one counts the abelian varieties isogenous to a given Y by looking at the double coset space $G(\mathbb{Q})\backslash G(\mathbb{A}_f)/K$, where $G = (\mathrm{End}(Y) \otimes \mathbb{Q})^*$. If I am belaboring the obvious, it is only because it was new to me, and to explain the role of the trace map. It is not hard to show by example that it is vital to the above theorem, except in such special cases as the following :

6.7 Corollary. There is a unique isomorphism class of abelian varieties of dimension $n \geq 2$ such that $F^1_{\mathrm{Hodge}} H^1_{DR} = F^1_{\mathrm{con}} H^1_{DR}$: the class of the product of any n supersingular elliptic curves.

Proof. It is easy to see that any such product satisfies $F^1_{\mathrm{Hodge}} = F^1_{\mathrm{con}}$. Conversely, if $F^1_{\mathrm{con}} = F^1_{\mathrm{Hodge}}$, Φ^2 on H^1_{cris} is divisible by p, and $p^{-1}\Phi^2$ is bijective, so we may choose a basis of H^1_{cris} which is fixed by $p^{-1}\Phi^2$. Select from such a basis n elements $\eta_1 \ldots \eta_n$ which project to a basis of $\mathrm{gr}^o_F H^1_{DR}$, and let $\omega_i = \Phi(\eta_i)$. Since Φ induces an isomorphism : $\mathrm{gr}^o_F H^1_{DR} \to \mathrm{gr}^1_{F_{\mathrm{con}}} H^1_{DR} = \mathrm{gr}^1_F H^1_{DR}$, the ω's and η's together form a basis of H^1_{cris}, adapted to the filtration $F^\bullet$. Obviously, $\Phi(\omega_i) = p\eta_i$. This shows that the isomorphism class of H^1_{cris} is unique ; we still have to check the trace structure : $\mathrm{tr} : \Lambda^{2n}H^1 \to W[-n]$. Let $\omega \wedge \eta = \omega_1 \wedge \ldots \omega_n \wedge \eta_1 \wedge \ldots \eta_n$; then $\mathrm{tr}\, p^n(-1)^n \omega\wedge\eta = \mathrm{tr}\, \Phi(\omega\wedge\eta) = \Phi \mathrm{tr}(\omega\wedge\eta) = p^n F^*_W \mathrm{tr}(\omega\wedge\eta)$, so $\xi = \mathrm{tr}(\omega\wedge\eta) \in W^*$

satisfies $F_W^* \xi = (-1)^n \xi$. This determines ξ up to multiplication by an element of $\mathbb{Z}_p^*$, so to see that the isomorphism class of (H^1, tr) is unique, we have to check that $\det : \mathrm{Aut}(H^1, \Phi) \to \mathrm{Aut}(\Lambda^{2n} H^1) \cong \mathbb{Z}_p^*$ is surjective. Let $\alpha \in \mathrm{Aut}\, H^1$ act on ω_1 and η_1 via the formula (6.5) and as the identity on the other basis vectors ; then $\det(\alpha) = a F^*(a) - p b F^*(b)$. It is clear that any element of $\mathbb{Z}_p^*$ can be expressed in this form. □

6.8 Remark. It also follows from strong approximation that the maps :

$$\mathrm{Aut}(Y) \longrightarrow \mathrm{Sl}\, H^1(Y_{\text{ét}}, \mathbb{Z}/\ell^n \mathbb{Z})$$

$$\mathrm{Aut}(Y) \longrightarrow \mathrm{Aut}(H^1_{\mathrm{cris}}(Y/W_n), \Phi, tr)$$

are surjective for any $\ell \neq p$ and any ℓ. One can also work simultaneously with any finite set of primes, including p.

Supersingular abelian crystals (without the trace structure) have been completely classified in [14]. (To take care of the trace structure, one has only to divide by a slightly smaller group). In our study of Kummer surfaces we will need this classification in the genus 2 case, which we review below. In particular, we will prove that a supersingular abelian surface is determined up to isomorphism by the associated K3 crystal H^2_{cris}. Notice that $H^2_{\mathrm{cris}}(Y/W) \cong \Lambda^2 H^1_{\mathrm{cris}}(Y/W)$, and the bilinear form is simply the map : $\Lambda^2 H^1 \otimes \Lambda^2 H^1 \to \Lambda^4 H^1 \xrightarrow[\sim]{tr} W[-2]$.

6.9 Proposition. *Suppose $p \neq 2$. The above construction defines a functor Λ^2 from the category of supersingular abelian crystals of genus 2 to the category of supersingular K3 crystals of rank 6. This functor induces an injection on isomorphism classes of objects, and its essential image consists of those K3 crystals with $\sigma_0 = 1$ or 2.*

Proof. It is clear that if F is either the Hodge or conjugate filtration, $F^1(\Lambda^2 H \otimes k)$ is the first level of the Koszul filtration attatched to $F^1(H \otimes k)$, and hence $\Lambda^2 H$ has the Hodge numbers of a K3 crystal. Moreover, $\Lambda^2 H$ is supersingular iff H is. It is easy to dispose of the "superspecial" case $\sigma_o = 1$: $\sigma_o(\Lambda^2 H) = 1$ iff $F^1_{Hodge}(\Lambda^2 H \otimes k) = F^1_{con}\Lambda^2(H \otimes k)$ iff $F^1_{Hodge}(H \otimes k) = F^1_{con}(H \otimes k)$.

To deal with the general case, it is convenient to rigidify our abelian crystals : Fix a superspecial abelian crystal S ; then an "S-structure" on H is a morphism of F-crystals $i : H \to S$ of degree p. It is easy to see that such a structure exists if H is superspecial. If not, we use :

6.10 Lemma. If H is a supersingular abelian F-crystal of genus 2 which is not superspecial, let $S(H) = \{x \in H \otimes \mathbb{Q} : \Phi(x) \in H$ and $V(x) \in H\}$. Then S(H) is superspecial, and there is a unique map $tr : \Lambda^4 S(H) \to W[-2]$ such that the inclusion $H \to S(H)$ has degree p. Any S-structure on H factors uniquely through an isomorphism $S(H) \to S$.

Proof. First of all, notice that $F^1_{con} \cap F^1_{Hodge}$ is a line in $H \otimes k$, and we can choose a basis (e_1, e_2, e_3, e_4) for H whose reduction mod p is adapted to the flag $F^1_{con} \cap F^1_{Hodge}$, F^1_{Hodge}, $F^1_{Hodge} + F^1_{con}$. It is clear that $(p^{-1}e_1, e_2, e_3, e_4)$ $= (s_1, s_2, s_3, s_4)$ is a basis for S(H), and that S(H) is invariant under Φ and V. Hence S(H) becomes an F-crystal, of weight one. I claim that mod p, its Hodge and conjugate filtrations are equal to the span of $\{s_2, s_3\}$, i.e. to the image of $(F^1_{Hodge} + F^1_{con})\, H \otimes k \to S(H) \otimes k$. We let the reader check this for himself, using the observation that Φ^3 is divisible by p. Thus, S(H) is superspecial, and S(H)/H has length one. Therefore $\Lambda^4 S(H)/\Lambda^4 H$ also has length one, and the existence and uniqueness of tr are clear.

If $i : H \to S$ is an S-structure, S/H has length one, and since Φ and V are nilpotent on S/pS, they are zero on S/H, i.e. $\Phi(S) \subseteq H$ and $V(S) \subseteq H$. This implies that i factors through a map $S(H) \to S$, which must be an isomorphism since its degree will be one. □

6.11 Lemma. *If $i : H \to S$ is an S-structure on H, then H contains $A^1 S$, and the image ℓ_H of H in $gr^o_F(S \otimes k)$ is a line. This defines a bijection between the set of isomorphism classes of $H \to S$ and the set of lines in $gr^o_F(S \otimes k)$.*

Proof. This is straightforward. A much more general statement is proved in [14]. □

Now if $i : H \to S$ is an S-structure, we get a morphism of crystals : $\Lambda^2 i : \Lambda^2 H \to \Lambda^2 S$ which multiplies the intersection form by p. Since the map $\Lambda^2 H \otimes k \to \Lambda^2 gr^o_F(S \otimes k)$ is zero, the map $\Lambda^2 i$ factors through $M^1 \Lambda^2 S$, which is $T(\Lambda^2 S) \otimes W$ (1.10). Hence we get a map $T^*(\Lambda^2 H) \to T(\Lambda^2 S)$ which is now compatible with the intersection forms. Dualizing, our map becomes $T^*(\Lambda^2 S) \to T(\Lambda^2 H)$, which is a $T^*(\Lambda^2 S)$-structure on $\Lambda^2 H$. Notice that $\sigma_o(T^*(\Lambda^2 S)) = 2$, hence $\sigma_o(\Lambda^2 H) \leq 2$, with equality iff this map is an isomorphism.

6.12 Lemma. *Let $T = T^*(\Lambda^2 S)$, let $\mathbb{P}$ be the projective space of lines in $gr^o_F(S \otimes k)$, and let M be the moduli space (4.6) of characteristic subspaces of T_o. Then Λ^2 induces an isomorphism between $\mathbb{P}$ and M^+, one of the two geometric components of $M \times \operatorname{Spec} k$.*

Proof. This can be done in many ways. I prefer to calculate explicitly.

Since $E(\Lambda^2 S) = M^1$, $pE(\Lambda^2 S)^\vee$ is the inverse image of $F^2(\Lambda^2 S) \otimes k$, and so $E/pE^\vee \cong gr^1_F(\Lambda^2 S \otimes k) \cong gr^o_F(S \otimes k) \otimes gr^1_F(S \otimes k)$. This is $(T^*/T) \otimes k = T_o \otimes k$. The quadratic form on $T_o \otimes k$ comes about as follows : From $tr : \Lambda^4 S \otimes k \to k$ we get a map : $(\Lambda^2 gr^o_F) \otimes (\Lambda^2 gr^1_F) \xrightarrow{\cong} k$, which in turn defines a symmetric pairing on $gr^o_F \otimes gr^1_F$: $\langle a \otimes b, c \otimes d \rangle = tr(a \wedge b \wedge c \wedge d) = -tr(a \wedge c \wedge b \wedge d) = -\langle a \wedge c, b \wedge d \rangle$. If ℓ is a line in $\Lambda^2 gr^o_F$, $\ell \otimes \Lambda^2 gr^1_F$ is a maximal isotropic in $gr^o_F \otimes gr^1_F$, and it is clear that $\ell \longmapsto \ell \otimes \Lambda^2 gr^1_F$ defines a bijection whose image is one of the two families of maximal isotropics. (The other family consists of subspaces of the form $\Lambda^2 gr^o_F \otimes \ell$). □

To finish the proof of the proposition, we have to eliminate the S-structure. Suppose H and H' are abelian crystals with $\Lambda^2 H \cong \Lambda^2 H'$. To prove that $H \cong H'$, first choose S-structures $i : H \to S$ and $i' : H' \to S$, and look at the associated T-structures $T \to \Lambda^2 H$, $T \to \Lambda^2 H'$. Since $\Lambda^2 H$ and $\Lambda^2 H'$ are isomorphic, we know that the corresponding characteristic subspaces are conjugate by Aut(T). Clearly it suffices to prove that this implies that the lines ℓ_H and $\ell_{H'}$ are conjugate under Aut(S). In other words, we must prove :

6.13 Lemma. The bijection $\mathbb{P}(k) \to M^+(k)$ induces a bijection : $\mathbb{P}(k)/\mathrm{Aut}(S) \to M^+(k)/\mathrm{Aut}(T)$.

Proof. To calculate Aut(S), recall that if $q = p^2$, $Z \underset{\text{def}}{=} \{z \in S : \Phi^2(z) = pz\}$ is a free $\mathbb{W}_q$-module, and $Z \otimes_{\mathbb{W}_q} W \cong S$ (cf. (6.7)). Clearly Z is Φ-invariant, and hence the filtration $F^\cdot = F^\cdot_{\text{Hodge}} = F^\cdot_{\text{con}}$ descends to $Z \otimes \mathbb{F}_q \hookrightarrow S \otimes k$. Choose a basis $\omega_1, \omega_2, \eta_1, \eta_2$ for Z as in (6.7), which then induces a basis for $Z \otimes \mathbb{F}_q$ adapted to $F^\cdot$. Clearly any element of Aut(S) acts on Z and preserves $F^\cdot$, and in fact is given by formula (6.5), with a and b 2×2 matrices with coefficients in $\mathbb{W}_q$. Since we are considering only automorphisms of S as an abelian crystal, we also require this matrix to have determinant one.

6.13.1 Claim. Let $Z^i = \mathrm{gr}^i_F(Z \otimes \mathbb{F}_q)$. Then the image of : $\mathrm{Aut}(S) \to \mathrm{Aut}(Z^o)$ consists of those elements g^o such that $\det(g^o)^{p+1} = 1$.

Proof. The p-linear map Φ induces a p-linear isomorphism : $\theta : Z^o \to Z^1$, whose inverse is the (p-linear !) map induced by $p^{-1}\Phi$. If $g \in \mathrm{Aut}(S)$, let g^i be the corresponding element of $\mathrm{Aut}(Z^i)$; note that $g^1 = \theta^{-1} g^o \theta$. The determinant of g mod p is thus $1 = \det(g^1)\det(g^o) = F^*(\det g^o)\det(g^o) = \det(g^o)^{p+1} = \mathrm{Nm}_{\mathbb{F}_q/\mathbb{F}_p}(\det g^o)$. Conversely, if $\det(g^o)^{p+1} = 1$, let a be a 2×2 matrix with coefficients in W_q satisfying $\det(a)\, F^*(\det a)) = 1$ and lifting g^o (in the basis ω, η). Then the endomorphism of S with this a and with $b = 0$ is an automorphism of S lifting g^o.

6.13.2 Claim. The image of $\mathrm{Aut}(S) \to \mathrm{Aut}(T_o \otimes \mathbb{F}_p)$ is the special orthogonal group.

Proof. We have $T_o \otimes \mathbb{F}_q \cong Z^o \otimes Z^1$, and the $\mathbb{F}_p$-rational structure is given by the p-linear automorphism φ of $Z^o \otimes Z^1$ sending $x \otimes y$ to $-\theta^{-1}(y) \otimes \theta(x)$. Let G^o be the subgroup of $\mathrm{Aut}(Z^o)$ consisting of elements with $(\det)^{p+1} = 1$. It is clear that we have a commutative :

6.13.3
$$\begin{array}{ccccc} \mathrm{Aut}(S) & \longrightarrow & \mathrm{Aut}(T) & & \\ \downarrow & & & \searrow & \\ G^o & \xrightarrow{\rho^o} & SO(T_o \otimes \mathbb{F}_p) & \longrightarrow & O(T_o \otimes \mathbb{F}_p) . \end{array}$$

The group μ_{p+1} of (p+1) st roots of unity embeds diagonally in G^o, and it is easy to check that this is precisely the kernel of ρ^o. Since we have an exact sequence :

$$1 \to Sl(Z^o) \to G^o \xrightarrow{\det} \mu_{p+1} \to 1,$$

the cardinality of the image of G^o is the same as the cardinality of $Sl(Z^o)$, i.e. $(q^2-1)q$. But the cardinality of our nonsplit special orthogonal group on $T_o \otimes \mathbb{F}_p$ is $p^2(p^2-1)(p^2+1)$, which is the same. This establishes the claim.

To prove lemma (6.13), and hence the proposition, note that if ℓ and ℓ' are lines in $Z^o \otimes k$ such that $\ell \otimes Z^1$ and $\ell' \otimes Z^1$ are conjugate by some $\tau \in \mathrm{Aut}(T_o \otimes \mathbb{F}_p)$, then in fact $\tau \in SO(T_o \otimes \mathbb{F}_p)$, since elements with $\det = -1$ interchange the two families. Since τ is the image of an element of $\mathrm{Aut}(S)$, this completes the proof. □

6.14 Corollary. If X and X' are supersingular abelian surfaces with isomorphism K3 crystals $H^2_{cris}(X/W) \cong H^2_{cris}(X'/W)$, then X and X' are isomorphic. □

6.15 Corollary. Any supersingular abelian surface admits a principal polarization. □

§7. TOWARDS A TORELLI THEOREM FOR SUPERSINGULAR K3 SURFACES

In this section we go as far as we can towards the proof of conjectures (0.1.2), and in particular we give a proof when $\sigma_o \leq 2$. The main tool is a careful analysis of the Neron-Severi group of a supersingular K3. Throughout this section, p is odd.

7.1 Proposition. *Suppose X/k is a smooth surface satisfying (1.1) and with $p_g = 1$ and $\rho = \beta_2$. Then the discriminant of the intersection form on NS(X) is $(-1)^{\rho-1}p^{2\sigma_o}$, where σ_o is the Artin invariant (3.4) attached to $H^2_{cris}(X/W)$, and the Hasse invariants of $NS(X)\otimes\mathbb{Q}$ are given by* :

$$e_p = -1, \quad e_2 = (-1)^{[\frac{\rho-1}{2}]+1}, \quad e_\ell = +1 \text{ for } \ell \neq 2, p, \infty.$$

Proof. Recall from (1.6) that $NS(X)\otimes\mathbb{Z}_p \to T_H$ is an isomorphism, and of course it is compatible with the intersection form [3]. This implies that the p-adic ordinal of the discriminant is $2\sigma_o$ and that $e_p = -1$ (3.3). This rest of the argument is the same as Artin's [2, §4] : If $\ell \neq p$, $NS(X)\otimes\mathbb{Z}_\ell \cong H^2(X_{\acute{e}t},\mathbb{Z}_\ell)$, and hence by Poincaré duality, the discriminant is prime to ℓ. For $\ell \neq 2$, this implies that $e_\ell = +1$. The Hodge index theorem tells us that the signature of $NS(X)\otimes\mathbf{R}$ is $(1,\rho-1)$, hence $e_\infty = (-1)^{\frac{(\rho-1)(\rho-2)}{2}} = (-1)^{[\frac{\rho-1}{2}]}$, and the discriminant is $(-1)^{\rho-1}p^{2\sigma_o}$. The Hilbert reciprocity theorem says that $\prod_\ell e_\ell = e_\infty$, so $e_2 = e_p e_\infty = (-1)^{[\frac{\rho-1}{2}]+1}$. □

7.2 Remark. For certain surfaces we can give alternative proofs that $e_p = -1$. For example, if X has a lifting X' to characteristic zero, $H^2(X'_{\mathbb{C}},\mathbb{Q})$ has a non-degenerate quadratic form with discriminant ± 1, hence its Hasse invariants $\{e'\}$ satisfy $e'_\ell = +1$ for $\ell \neq 2, \infty$, and hence $e'_2 = e'_\infty$. By the Hodge index theorem, $H^2(X'_{\mathbb{C}},\mathbf{R})$ has signature $(3,\rho-3)$, hence $e'_\infty = (-1)^{\frac{(\rho-3)(\rho-4)}{2}} = -e_\infty$. But $H^2(X'_{\mathbb{C}},\mathbb{Q}_2) \cong H^2(X_{\acute{e}t},\mathbb{Q}_2)$, so $e_2 = e'_2 = -e_\infty$, hence $e_p = e_2 e_\infty = -e_\infty^2 = -1$. □

By using the Neron-Severi group of a supersingular abelian surface as a substitute for integral homology, we will obtain a characteristic p analogue of Shioda's description [23] of the isomorphisms between abelian surfaces. Shioda begins by making a subtle point: If $Y/\mathbb{C}$ is an abelian surface, the isomorphism $\Lambda^2 H^1(Y) \to H^2(Y)$ provides $H^2(Y)$ with an "orientation". This may be though of in the following way : If $w \subseteq H^1(Y)$ is a three dimensional subspace, $\Lambda^2 w \subseteq \Lambda^2 H^1(Y)$ is a totally isotropic subspace, and if w' is another one, $\Lambda^2 w \cap \Lambda^2 w'$ is even dimensional, hence $\Lambda^2 w$ and $\Lambda^2 w'$ lie in the same family. This distinguishes a family of totally isotropic subspaces, hence an element in the center of the Clifford algebra attached to H^2, which "is" the orientation. (Away from characteristic two, we can think of this more concretely as follows: If $w \subseteq H$ is as above, we have a canonical pairing $w \otimes H/w \to \mathbb{Q}$, hence $\det(w) \otimes \det(H/w) \xrightarrow{\cong} \mathbb{Q}$. Taking the inverse of this composed with the Koszul isomorphism $\det(w) \otimes \det(H/w) \to \det(H/w) \to \det(H)$ gives an element ξ_w of $\det(H)$ satisfying $< \xi_w, \xi_w > = (-1)^{\frac{1}{2}\dim(H)} = -1$, which classifies the family in which w lies).

Since we are in characteristic p, we cannot use rational cohomology directly. If Y is supersingular, we have for every $\ell \neq p$: $NS(Y) \otimes \mathbb{Z}_\ell \cong H^2(Y_{ét}, \mathbb{Z}_\ell) \cong \Lambda^2 H^1(Y_{ét}, \mathbb{Z}_\ell)$, which defines an orientation ξ_ℓ on $NS(Y) \otimes \mathbb{Z}_\ell$ for every ℓ. (In fact, these descend to an orientation on NS(Y), but we will not need this fact.) Here is our analogue of Shioda's result :

7.3 Theorem. Let X_1 and X_2 be supersingular abelian surfaces, and let $\theta : NS(X_1) \to NS(X_2)$ be an isometry which takes effective cycles to effective cycles and preserves the orientations on $NS(X_i) \otimes \mathbb{Q}_2$. Then the following are equivalent :

a) θ is induced by an isomorphism $X_2 \to X_1$.

b) θ extends to an isomorphism :

$$H^2_{DR}(X_1/k) \to H^2_{DR}(X_2/k)$$

c) θ extends to an isomorphism of F-crystals

$$H^2_{cris}(X_1/W) \to H^2_{cris}(X_2/W).$$

Proof. It is clear that a) implies b) and c). Moreover, if b) holds, so does c). Indeed, $NS(X_i) \otimes \mathbb{Z}_p \cong T(H^2_{cris}(X_i/W)$, by (1.6), so we can think of the characteristic spaces $K_i = \mathrm{Ker}(T_i \otimes k \to H_i \otimes k)$ as being simply the kernels of $NS(X_i) \otimes k \to H^2_{DR}(X_i/k)$. Thus c) follows from the classification (4.3) of crystals in terms of characteristic subspaces.

The basis for the implication of a) by c) is the isomorphism $\mathrm{Spin}(6) \cong \mathrm{Sl}(4)$, which for us will take the following form : If c) holds, we know that $X_1 \cong X_2$, by (6.14), and hence we may assume that $X_1 = X_2 = X$. Let G as above be the (opposite) group of elements of $\mathrm{End}(X) \otimes \mathbb{Q}$ of degree one, regarded as an algebraic group over $\mathbb{Q}$. Then G acts on $NS(X) \otimes \mathbb{Q}$, preserving the quadratic form $Q(x) = \frac{1}{2} <x,x>$ and the orientation. This defines a representation from G to the special orthogonal group SO attached to Q, which evidently factors through $G/\pm \mathrm{id}$. Moreover, G is simply connected, so we find a natural map from G to the universal cover Spin of SO. Since these groups are connected and simply connected and have the same dimension, the map is an isomorphism.

7.3.1. For the definition and basic properties of the Spin group, we refer to [6, §9 N° 5]. We shall need to know that if A is a field extension of $\mathbb{Q}$, there is an exact sequence :

$$\mathrm{Spin}(A) \longrightarrow SO(A) \xrightarrow{Nsp} A^*/A^{*2}.$$

The "spinorial norm" Nsp can be calculated as follows : Any element $\alpha \in O(A)$ can be written as a product of reflections $\tilde{e}_i$, where $\tilde{e}_i : x \mapsto x - <x,e_i>Q(e_i)^{-1}e_i$ and $e_i \in N \otimes A$ is a nonsingular vector. Then if $\alpha = \tilde{e}_1 \ldots \tilde{e}_m$, $Nsp(\alpha)$ is the class of the product : $Q(e_1)\ldots Q(e_m)$.

Now to prove the theorem, let θ be an automorphism of $NS(X)$ which preserves the orientation on $NS(X) \otimes \mathbb{Q}_2$; then of course $\det(\theta) = 1$, and we can try to compute the spinorial norm of $\theta \in \mathbb{Q}^*/\mathbb{Q}^{*2}$. In fact :

7.3.2. <u>Claim</u>. If θ is as above and extends to an automorphism of $H^2_{cris}(X/W)$, $Nsp(\theta) = \pm 1$ in $\mathbb{Q}^*/\mathbb{Q}^{*2}$.

To prove this it suffices to show that $ord_\ell Nsp(\theta)$ is even for every ℓ. If $\ell \neq p$, $NS(X) \otimes \mathbb{Z}_\ell \cong H^2(X_{\acute{e}t}, \mathbb{Z}_\ell)$, so by Poincaré duality the form is nondegenerate and this implies, at least if $\ell \neq 2$, that $\theta \otimes id_{\mathbb{Z}_\ell}$ can be written as a product of integral reflections, hence that $Nsp(\theta) \in \mathbb{Z}_\ell^*/\mathbb{Z}_\ell^{*2}$. (The argument of [6, §6 N° 4] works without change). If $\ell = 2$, one can use the fact that the intersection form on $NS(X)$ is <u>even</u> (by Riemann-Roch), hence Q is integral, and [6, §6 Ex. 28] works over the maximal unramified extension of $\mathbb{Z}_2$, so $Nsp(\theta) \in \mathbb{Z}_2^*/\mathbb{Z}_2^{*2}$. For $\ell = p$, use c) to extend $\theta \otimes id_W$ to $H^2_{cris}(X/W)$; computing the Nsp there shows that $Nsp(\theta) \in \mathbb{Z}_p^*/\mathbb{Z}_p^{*2}$. This proves the claim.

7.3.3. <u>Claim</u>. If θ is as above, $\pm\theta$ is induced by an automorphism of X.

To prove this, first note that $Nsp(-id) = -1$. Indeed, by a general formula, the spinorial norm of $(-id)$ is the discriminant of the quadratic form, which here is $-p^{2\sigma_o}$. Hence $Nsp(\pm\theta) = 1$, so there is a $g \in G(\mathbb{Q})$ which acts as $\pm\theta$. For every ℓ, g acts on $H^1(X_{\acute{e}t}, \mathbb{Q}_\ell)$, and Λ^2 of this action induces an automorphism of $H^2(X_{\acute{e}t}, \mathbb{Z}_\ell)$. It is easy to see that this implies that each $H^1(g, \mathbb{Z}_\ell)$ is integral. Since the same thing works in crystalline cohomology, g comes from an actual morphism $X \to X$, which is an automorphism since its degree is one. It is clear that this proves the theorem, because if θ takes effective cycles to effective cycles, $-\theta$ does not, and hence $-\theta$ cannot be induced by an automorphism of X. □

We now return to K3 surfaces. Our main goal is the proof of Conjecture (0.1) when $\sigma_o \leq 2$. The first step is the determination of the Neron-Severi group.

7.4 <u>Theorem</u>. <u>Let</u> X_1 <u>and</u> X_2 <u>be two</u> K3 <u>surfaces with</u> $\rho = 22$, <u>in charac-</u>

teristic $p > 2$. Then :

7.4.1. There exists an isometry (i.e., an isomorphism compatible with the intersection forms) : $\mathbb{Q} \otimes NS(X_1) \xrightarrow{\cong} \mathbb{Q} \otimes NS(X_2)$.

7.4.2. If X_1 and X_2 have the same invariant σ_0, there is an isometry : $NS(X_1) \xrightarrow{\cong} NS(X_2)$.

7.4.3. If there exists an isomorphism of K3 crystals : $H^2_{cris}(X_1/W) \xrightarrow{\cong} H^2_{cris}(X_2/W)$, then there exists a commutative diagram :

$$\begin{array}{ccc} H^2_{cris}(X_1/W) & \xrightarrow{\cong} & H^2_{cris}(X_2/W) \\ \uparrow & & \uparrow \\ NS(X_1) & \xrightarrow{\cong} & NS(X_2). \end{array}$$

Proof. The first statement is an immediate consequence of (7.1) and the classification of quadratic forms [21, V, 3.3]. The proof of (7.4.2) is more delicate. Like (6.2), it rests on the strong approximation theorem for semi-simple simply connected groups. However, since the group of isometries of a quadratic form is neither connected nor simply connected, we have to do some work before we can apply it. These methods are of course standard, cf. [17].

First let us note that if X_1 and X_2 are as in (7.4.2), then for every prime ℓ, there is an isometry $NS(X_1) \otimes \mathbb{Z}_\ell \cong NS(X_2) \otimes \mathbb{Z}_\ell$. For $\ell = p$, this follows from (3.4) and (1.6), and for odd $\ell \neq p$ it follows from the fact that a quadratic form over $\mathbb{Z}_\ell$ whose discriminant d is an ℓ-adic unit is determined by its reduction modulo ℓ, hence by $d \in \mathbb{Z}_\ell^*/\mathbb{Z}_\ell^{*2}$, which in our case is -1. For $\ell = 2$, recall that by the Riemann-Roch theorem on a K3 surface, $L\cdot L = 2[\chi(L)-\chi(\mathcal{O}_X)]$, so the intersection form on $NS(X_i)$ is even. Define $Q(v) = \frac{1}{2} <v,v>$ for $v \in NS(X_i)$; so $<v,w> = Q(v+w) - Q(v) - Q(w)$, and Q is an element of $\mathrm{Hom}_{\mathbb{Z}}[\Gamma_2(NS), \mathbb{Z}] \cong S^2(NS^\vee)$. This Q then defines a quadric in $\mathbb{P}(NS^\vee)$, and the associated bilinear form $< , >$ is its derivative. Since this form defines an isomorphism $NS \to NS^\vee$ away from p, the quadric is smooth over Spec $\mathbb{Z}[\frac{1}{p}]$. By Hensel's lemma, for $\ell \neq p$, the quadric over $\mathbb{Z}_\ell$ is determined by its reduction mod ℓ, hence by its discriminant, even for

$\ell = 2$. In fact, one has the following well-known "canonical form" :

7.5 Lemma. Let $<\ ,\ >$ be a symmetric bilinear form on a free $\mathbb{Z}_\ell$ module of even rank, with discriminant are ℓ-adic unit. Then :

7.5.1. If $\ell \neq 2$, there is a basis in which the matrix for $<\ ,\ >$ is :

$$\begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix} \oplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \cdots \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

7.5.2. If $<\ ,\ >$ is even, there is a basis in which the matrix is :

$$\begin{pmatrix} 2 & 1 \\ 1 & a \end{pmatrix} \oplus \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus \cdots \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad . \square$$

Let me remark that using (7.5.2), one can verify the computation above that our $e_2 = -1$.

In the calculations which follow, we will rely on the following consequence of lemma (7.5) :

7.6 Lemma. If X is as above, then :

7.6.1. For $\ell \neq p$, $NS(X) \otimes \mathbb{Z}_\ell$ contains a hyperbolic orthogonal direct summand W_ℓ, with basis $\{x_\ell, y_\ell\}$ in which the intersection matrix is $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

7.6.2. For $\ell = p$, $NS(X) \otimes \mathbb{Z}_p$ admits an orthogonal decomposition : $NS(X) \otimes \mathbb{Z}_p \cong T_o \oplus T_1$, as in (3.4), and T_1 admits an orthogonal decomposition : $T_1 = W'_p \oplus W_p$, where W'_p is neutral and W_p has a basis $\{x_p, y_p\}$ in which the intersection matrix is $\begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix}$, where $(\frac{\lambda}{p}) = -(\frac{-1}{p})$.

Proof. The first statement is clear. As for the second, recall that T_o has rank $2\sigma_o$ and T_1 has rank $22-2\sigma_o$. Here is another proof of Artin's observation that $\sigma_o \leq 10$: We know that the discriminant d of NS(X) is $-p^{2\sigma_o}$, and we also know that the discriminant d_o of $(T_o, <\ >_{T_o})$ satisfies $(\frac{d_o}{p}) = -(\frac{-1}{p})^{\sigma_o}$. If $\sigma_o = 11$, these formulas are incompatible ! Hence T_1 has rank ≥ 2, and therefore admits a basis as in (7.5.1). Note that the Legendre symbol of the discriminant d_1 of T_1 is $-(\frac{-1}{p})^{\sigma_1}$, where $\sigma_1 = 11-\sigma_o$ is half its rank. Thus, T_1 is also nonneutral. □

To prove (7.4.2), first choose an isometry $\varphi : NS(X_2) \otimes \mathbb{Q} \to NS(X_1) \otimes \mathbb{Q}$, and notice that the set of such isometries is a torseur under the (left) action of the group $O(\mathbb{Q})$ of automorphisms of $(NS(X_1) \otimes \mathbb{Q}, < , >)$. (This is the set of $\mathbb{Q}$-rational points of an algebraic group O over $\mathbb{Q}$). Next, for each ℓ, choose an isometry $\psi_\ell : NS(X_1) \otimes \mathbb{Z}_\ell \to NS(X_2) \otimes \mathbb{Z}_\ell$; the set of such isometries is a torseur under the (right) action of the group $K_\ell = \mathrm{Aut}(NS(X_1) \otimes \mathbb{Z}_\ell) \subseteq O(\mathbb{Q}_\ell)$. Putting these together, we get an isometry $\psi : NS(X_1) \otimes \hat{\mathbb{Z}} \to NS(X_2) \otimes \hat{\mathbb{Z}}$, which we can modify by an element of $K = \prod_\ell K_\ell \subseteq O(\mathbb{A}_f)$. It is clear that we will have found an isomorphism $NS(X_2) \to NS(X_1)$ when we arrange matters so that $\varphi \otimes id_{\hat{\mathbb{Z}}} = (\psi \otimes id_{\mathbb{Q}})^{-1}$. In other words, if we let $g = (\varphi \otimes id_{\hat{\mathbb{Z}}}) \circ (\psi \otimes id_{\mathbb{Q}})$ (as an element of $O(\mathbb{A}_f)$), we have to show that by multiplying on the left by $O(\mathbb{Q})$ and on the right by K, we can obtain $g = 1$. This amounts to :

7.7 Lemma. $O(\mathbb{Q})\backslash O(\mathbb{A}_f)/K$ is a single point.

Proof. The idea is to reduce to the spin group.

Step 1. If $SO \subseteq O$ is the subgroup consisting of the elements with det = 1, the map :

$$SO(\mathbb{Q})\backslash SO(\mathbb{A}_f)/K \cap SO(\mathbb{A}_f) \to O(\mathbb{Q})\backslash O(\mathbb{A}_f)/K$$

is surjective.

Proof. Clearly it suffices to prove that if $g \in O(\mathbb{A}_f)$, there is a $k \in K$ such that $gk \in SO(\mathbb{A}_f)$. We can do this prime by prime, so it is enough to check that for every ℓ, there is a $k_\ell \in K_\ell$ such that $\det(k_\ell) = -1$. For $\ell \neq p$, let k_ℓ be the element which interchanges x_ℓ and y_ℓ in (7.6.1) and is the identity on $W_\ell^\perp$, and let k_p send x_p to $-x_p$, y_p to y_p, and be the identity on $W_p^\perp$.

Step 2. If Spin is the spinor group corresponding to the quadratic form Q on

$NS(X_2) \otimes \mathbb{Q}$, and if $\tilde{K} \subseteq Spin(\mathbb{A}_f)$ is the inverse image of K, then the map :

$$Spin(\mathbb{Q}) \backslash Spin(\mathbb{A}_f)/\tilde{K} \longrightarrow SO(\mathbb{Q}) \backslash SO(\mathbb{A}_f)/K \cap SO(\mathbb{A}_f)$$

is surjective.

Proof. Since Q is an indefinite form of rank ≥ 5, it represents zero [21, IV, §3 Cor. 2], and this implies that the sequence :

$$Spin(\mathbb{Q}) \longrightarrow SO(\mathbb{Q}) \xrightarrow{Nsp} \mathbb{Q}^*/\mathbb{Q}^{*2} \to 1$$

is exact, [6, §9 N° 5]. The same is true with $\mathbb{Q}_\ell$ in place of $\mathbb{Q}$ for every ℓ, and hence we also find an exact sequence :

$$Spin(\mathbb{A}_f) \longrightarrow SO(\mathbb{A}_f) \xrightarrow{Nsp} \mathbb{A}_f^*/\mathbb{A}_f^{*2} \to 1.$$

It is clear that we must prove that the image of $SO(\mathbb{Q}).(K \cap SO(\mathbb{A}_f))$ fills up $\mathbb{A}_f^*/\mathbb{A}_f^{*2}$. Since $Nsp(\mathbb{Q})$ fills up $\mathbb{Q}^*/\mathbb{Q}^{*2}$, we have only to prove that $Nsp(K \cap SO(\mathbb{A}_f))$ fills up $\hat{\mathbb{Z}}^*/\hat{\mathbb{Z}}^* \cap \mathbb{A}_f^{*2}$. For $\ell \neq p$, let x_ℓ and y_ℓ be as in (7.6), and for each a $a \in \mathbb{Z}_\ell^*$ consider $w = x_\ell + y_\ell$, $v = x_\ell + ay_\ell$. Then $Q(w) = 1$ and $Q(v) = a$, so the product of the reflections $\tilde{w} \circ \tilde{v}$ lies in $K_\ell \cap SO(\mathbb{Q}_\ell)$ and has spinorial norm $Q(w)Q(v) = a$. (cf. (7.3.1)). For $\ell = p$, it is still true that on W_p, the form Q represents every element of $\mathbb{Z}_p^*$ [21, IV, 2.2, cor.], so again we can find u and v with $Q(u) = 1$, $Q(v) =$ any $a \in \mathbb{Z}_p^*$, and the rest of the proof is the same.

Step 3. $Spin(\mathbb{Q}) \backslash Spin(\mathbb{A}_f)/\tilde{K}$ is a single point.

Proof. Spin is a semi-simple, simply connected group, and since the form is indefinite, $Spin(\mathbb{R})$ is noncompact. By the strong approximation theorem, $Spin(\mathbb{Q})$ is dense in $Spin(\mathbb{A}_f)$, hence meets the open set $\tilde{K}$. The lemma and (7.4.2) are proved. □

The proof of (7.4.3) is essentially the same argument, but slightly refined at p. Instead of using an arbitrary isomorphism $\psi_p : NS(X_1) \otimes \mathbb{Z}_p \longrightarrow NS(X_2) \otimes \mathbb{Z}_p$, observe that we can choose ψ_p to be compatible with an isomorphism $H^2_{cris}(X_1/W) \to H^2_{cris}(X_2/W)$, by (4.4). Notice that we can modify ψ_p by any element of the stabilizer subgroup $G_H \subseteq Aut(NS(X_1) \otimes \mathbb{Z}_p)$ of the characteristic subspace K_H. It is clear that the elements k_p of $Aut(NS(X_1) \otimes \mathbb{Z}_p)$ we constructed in steps 1 and 2 lie in G_H. Thus we conclude that $\mathrm{Spin}(\mathbb{Q})\backslash \mathrm{Spin}(\mathbb{A}_f)/\widetilde{G}_H \to O(\mathbb{Q})\backslash O(\mathbb{A}_f) / G_H$ is still surjective. Since $\widetilde{G}_H$ is again open, the strong approximation theorem still applies. ☐

Theorem (7.4) has the following important refinement :

7.8 Proposition. The isomorphism in (7.4.2) or (7.4.3) can be chosen to preserve effective classes.

Proof. On a K3 surface X, $\mathrm{Pic}(X) \xrightarrow{\cong} NS(X)$, and a line bundle L corresponds to an effective class iff $h^0(L) \neq 0$. If $\varphi : NS(X_1) \to NS(X_2)$ is an isometry, we will show that, after composing φ with some reflections in $NS(X_2)$ and $\pm$ id, we obtain an isomorphism preserving effective classes. These reflections will be obtained as follows : If $e \in NS(X_2)$ has $<e,e> = -2$, then $\tilde{e}(x) = x+<x,e>x$ is an isometry of $NS(X_2)$ - reflection through the orthogonal complement of e. Let e also stand for the first Chern class of e in $H^2_{cris}(X_2/W)$, and notice that since $\Phi(e) = pe$, $\tilde{e}$ extends (use the same formula) to an automorphism of the K3-crystal $H^2_{cris}(X_2/W)$. Thus, we can use this extension to modify the top part of diagram (7.4.3).

Let R be the subgroup of Aut(NS(X)) generated by the above reflections, and recall that an element h of NS(X) is called "pseudo-ample" if $h^2 > 0$ and $h.c \geq 0$ for every effective c.

7.9 Lemma. If $h^2 > 0$, there is a $w \in R$ such that $w(\pm h)$ is pseudoample.

Proof. This lemma is usually proved, in characteristic zero, by obscure references to the theory of reflections. Here is Deligne's simple and direct argument :

Recall that if C is an irreducible curve on the K3 surface X, $C^2 \geq -2$ (adjunction formula) and, conversely, if L is a line bundle with $L^2 \geq -2$, $L^{\pm 1}$ is effective. In particular we may assume that h is effective.

Suppose there exists an irreducible curve C with $h \cdot C < 0$ - if not, h is pseudoample. By Riemann-Roch, the (projective) dimension of the complete linear system $|C|$ is $\geq 1+\frac{1}{2}C^2$, so that if $C^2 \geq 0$, there exists a $C' \in |C|$ other than C. Since C' is irreducible, $|C|$ has no fixed components, so $h \cdot C \geq 0$, a contradiction. Consequently $C^2 = -2$.

Thus, we may consider the reflection $\tilde{e}$, where e is the class of C in $NS(X)$. Set $h' = \tilde{e}(h)$; since $(h')^2 = h^2 > 0$, $\pm h'$ is effective. If $-h'$ is effective, choose an effective curve Z' in $-h'$ and an effective Z in h, and notice that since $h' = h - ae$, where $a = -e.h > 0$, $Z+Z'$ belongs to ae. But the complete linear system $|ae|$ is simply aC itself, since C is irreducible and of negative self intersection, so this tells us that as divisors, $Z+Z' = aC$ - which is absurd.

We conclude that $h' = \tilde{e}(h)$ is still effective. Continuing in this way, we find a sequence $e_1 \ldots e_n \ldots$ such that each $h^{(i)} = \tilde{e}_i \circ \ldots \tilde{e}_1(h)$ is effective. Since it is impossible to have an infinite sequence of this form, we must eventually reach a pseudoample class. □

To prove Proposition (7.8), let $h_1 \in NS(X_1)$ be ample, and use the lemma to arrange matters so that $h_2 = \varphi(h_1)$ is pseudoample. Then if C is the class in $NS(X_1)$ of an irreducible curve, $\varphi(C)^2 = C^2 \geq -2$, hence $\pm\varphi(C)$ is effective. But $\varphi(C)\cdot\varphi(h_1) = C\cdot h_1 > 0$, and since $\varphi(h_1)$ is pseudoample, it is indeed $\varphi(C)$ that is effective, and the proposition is proved. (In fact, as in [7.3.2], it is also true that $\varphi(h_1)$ is ample). □

7.10 <u>Theorem</u>. <u>A supersingular</u> K3 <u>surface is Kummer iff</u> $\rho = 22$ <u>and</u> $\sigma_0 = 1$ <u>or</u> 2.

<u>Proof</u>. First let us recall the relationship between the cohomology of an abelian variety Y and the associated Kummer surface X. The involution $-id_Y$ of Y has as its fixed point set the 2-division points of Y, which we identify with $H_1(Y_{ét}, \mathbb{Z}/2\mathbb{Z})$. Let $q : \tilde{Y} \to Y$ be the blowing-up of Y at these 16 points : Then $-id$ acts on $\tilde{Y}$ and (since the derivative of $-id_Y$ is $-id$) the resulting automorphism has

the exceptional locus $\{\tilde{E}_y : y \in H_1(Y_{\acute{e}t}, \mathbb{Z}/2\mathbb{Z})\}$ as its fixed point set. The quotient map $\pi : \tilde{Y} \to X$ is a double cover, ramified precisely along $\{\tilde{E}_y\}$, and X is (the smooth minimal model of) the K3 surface associated to Y. The image E_y of $\tilde{E}_y$ in X is a smooth rational curve with $E_y^2 = -2$, and $E_y \cdot E_{y'} = 0$ if $y \neq y'$. Let $\Pi_Y \subseteq NS(X)$ be the subgroup generated by $\{E_y\}$.

If Y is supersingular, we can construct the analogue of the special cycles [18, §5] in $NS(X)$. I like to think of this in the following way : If $V \subseteq H_1(Y_{\acute{e}t}, \mathbb{Z}/2\mathbb{Z})$ is a 2-dimensional subspace, $\Lambda^2 V \subseteq \Lambda^2 H_1(Y_{\acute{e}t}, \mathbb{Z}/2\mathbb{Z})$ is a line, and its image in $\Lambda^2 H^1(Y_{\acute{e}t}, \mathbb{Z}/2\mathbb{Z})$ via Poincaré duality contains a unique nonzero vector v. This establishes a bijection between the set of all such planes and the set of all nonzero isotropic vectors in $\Lambda^2 H^1(Y_{\acute{e}t}, \mathbb{Z}/2\mathbb{Z})$, (where isotropic means $Q(v) = \frac{1}{2} <v, v> = 0$). We will allow ourselves to identify these two sets.

As an example, suppose that $Y_o \subseteq Y$ is an elliptic curve. Then the image of $H_1(Y_o, \mathbb{Z}/2\mathbb{Z}) \to H_1(Y, \mathbb{Z}/2\mathbb{Z})$ is a two-dimensional subspace, and the corresponding vector $v \in H^2(Y, \mathbb{Z}/2\mathbb{Z})$ is just the reduction modulo 2 of the cohomology class of Y_o. Notice that by (6.8), if Y is supersingular, $\mathrm{Aut}(Y) \to \mathrm{Aut}(H_1(Y, \mathbb{Z}/2\mathbb{Z})$ is surjective, and hence acts transitively on the set of two dimensional subspaces. Since we know Y contains at least one elliptic curve, it follows that every $v \in H^2(Y, \mathbb{Z}/2\mathbb{Z})$ is the cohomology class of some elliptic curve $Y_v \subseteq Y$. Let us fix a choice of some Y_v for each v, and let $A_v = \pi_* q^*(Y_v) \in \Pi_Y^\perp \subseteq NS(X)$.

7.11 Lemma. The relationship between $NS(Y)$, $H_1(Y_{\acute{e}t}, \mathbb{Z}/2\mathbb{Z})$ and $NS(X)$ is given by :

7.11.1. On the submodule $\Pi_Y^\perp \oplus \Pi_Y$ of $NS(X)$, the intersection form $< , >$ and the map π^* are divisible by 2. In fact $\frac{1}{2}\pi^*$ induces an isometry :

$$\frac{1}{2}\pi^* : (\Pi_Y^\perp \oplus \Pi_Y, \tfrac{1}{2} < , >) \to (NS(\tilde{Y}), < , >)$$

taking $\Pi_Y^\perp$ to $q^* NS(Y)$.

7.11.2. The images of the A_v's span $\Pi_Y^\perp \otimes \mathbb{Z}/2\mathbb{Z}$, and the image of $\frac{1}{2}\pi^*(A_v)$

<u>in</u> $NS(\tilde{Y}) \otimes \mathbb{Z}/2\mathbb{Z}$ <u>is</u> $q^*(v)$.

7.11.3. <u>A subset</u> w <u>of</u> $H_1(Y_{ét}, \mathbb{Z}/2\mathbb{Z})$ <u>containing zero and of cardinality eight is a subgroup iff</u> $G_w \underset{def}{=} \Sigma \{E_y : y \in w\}$ <u>lies in</u> $2NS(X)$.

<u>Proof</u>. Clearly $q^*(Y_v) = \tilde{Y}_v + \Sigma\{\tilde{E}_y : y \in v\}$, where $\tilde{Y}_v$ is the strict transform of Y_v. The image F_v of $\tilde{Y}_v$ in X is a rational curve, and $\pi_*\tilde{Y}_v = 2F_v$. I claim :

7.11.4. $A_v = 2F_v + \sum_{y \in v} E_y$.

$\pi^*(A_v) = 2q^*Y_v$.

$< F_v, E_y > = 1$ if $y \in v$, $= 0$ otherwise.

$<F_v, A_{v'}> \equiv \text{card}(v \cap v')$ mod 2, i.e. $= < v, v' >$.

These are all clear, except perhaps the last one. But $<F_v, A_{v'}> = \frac{1}{2} <A_v, A_{v'}> = \frac{1}{4} < \pi^* A_v, \pi^* A_{v'}> = < Y_v, Y_{v'}>$. Mod 2, this is the intersection product $< v, v' >$, which is 1 iff the corresponding planes intersect only in zero.

Now choose a basis $y_1 \ldots y_4$ for $H_1(Y_{ét}, \mathbb{Z}/2\mathbb{Z})$, and for $i < j$ let v_{ij} be the vector in $H^2(Y_{ét}, \mathbb{Z}/2\mathbb{Z})$ corresponding to the plane spanned by y_i and y_j – the reduction mod 2 of the cohomology class of an elliptic curve $Y_{ij} \subseteq Y$. It is clear that $\{v_{ij}\}$ is a hyperbolic basis for $H^2(Y_{ét}, \mathbb{Z}/2\mathbb{Z})$: $< v_{ij}, v_{rs} > = 0$ unless $\{i,j\}$ is the complement $\{r', s'\}$ of $\{r,s\}$. I claim that the images of A_{ij} in $NS(X) \otimes \mathbb{Z}/2\mathbb{Z}$ are linearly independent, and hence that they form a basis for $\Pi_Y^\perp \otimes \mathbb{Z}/2\mathbb{Z} \subseteq NS(X) \otimes \mathbb{Z}/2\mathbb{Z}$. Indeed, if $\Sigma n_{ij} A_{ij} \equiv 0$ mod $2NS(X)$, then $n_{r's'} \equiv < \Sigma n_{ij} A_{ij}, F_{rs} > \equiv 0$ mod 2. This implies that $\{A_{ij}\}$ form a basis of $\Pi_Y^\perp \otimes \mathbb{Z}_2$, and it follows that π^* and $< , >$ are divisible by 2. Statements (7.11.1) and (7.11.2) follow immediately.

To prove (7.11.3) let w be a hyperplane. We copy the argument of [18] : Choose a two dimensional subspace $v \subseteq w$ and an x in w but not in v. The translate Y'_v of Y_v by x is obviously homologous to Y_v, not so for its strict transform $\tilde{Y}'_v$. We have, if $v' = x+v$:

$$q^*(Y_v) = q^*(Y'_v) = \tilde{Y}'_v + \Sigma\{\tilde{E}_{y'} : y' \in v'\},$$

hence :

$$A_v = 2F'_v + \Sigma \{E_{y'} : y' \in v'\}.$$

Since $v \cup v' = w$, adding these gives :

$$2A_v = 2F_{v'} + 2F_v + \Sigma \{E_y : y \in w\},$$

and hence $\Sigma \{E_y : y \in w\}$ is divisible by 2.

For the converse, observe that it suffices to prove that $x+y \in w$ whenever x and $y \in w$, and we may assume that x and y are independent. Let v be the plane they span. Then $G_w \cdot F_v = \mathrm{card}(w \cap v) = 4$ and $v \subseteq w$. □

Since $\Pi_Y^{\perp} \otimes \Pi_Y \to NS(X)$ is an isomorphism away from 2, it is clear from the lemma that the p-adic ordinal of the discriminants of $NS(X)$ and of $NS(Y)$ are the same. Hence by (6.9), if X is Kummer, $\sigma_0(X) = 1$ or 2.

To prove the converse, suppose that X is a K3 surface with $\rho = 22$ and $\sigma_0 = 1$ or 2. Construct a Kummer surface X' with the same σ_0. We know by (7.8) and (7.4.2) that there is an isomorphism $\theta : NS(X') \to NS(X)$ carrying effective cycles to effective cycles. Then for each i, the line bundle $\mathcal{L}_i = \theta(\mathcal{O}_{X'}(E'_i))$ has $\mathcal{L}_i \cdot \mathcal{L}_i = -2$ and $h^0(\mathcal{L}_i) \neq 0$. I claim that any $E_i \in |\mathcal{L}_i|$ is irreducible. If not, $E_i = Z_1 + Z_2$ with Z_1 and Z_2 effective, hence E'_i is linearly equivalent to a sum of effective divisors on X'. Since we know that the complete linear system $|E'_i|$ is simply E_i, this is impossible. It follows that each E_i is in fact a smooth rational curve, and $E_i . E_j = -2\,\delta_{ij}$. Moreover, the sum ΣE_i is divisible by 2 in $\mathrm{Pic}(X)$. The proposition now follows from :

7.12 Lemma. Suppose X is a K3 surface and $E_1 \ldots E_{16}$ are irreducible curves on X with $E_i . E_j = -2\,\delta_{ij}$ and with $E = \Sigma E_i$ divisible by 2 in $NS(X)$. Then there is a Kummer surface structure $Y \dashrightarrow X$ such that $\Pi_Y = \mathrm{span}\{E_1 \ldots E_{16}\}$.

Proof. Let $\mathcal{L} \in \mathrm{Pic}(X)$ be the bundle with $\mathcal{L}^{\otimes 2} \cong I_E$. The map : $\mathcal{L}^{\otimes 2} \to I_E \to \mathcal{O}_X$ defines a multiplication on $\mathcal{O}_X \oplus \mathcal{L}$, and $\mathrm{Spec}_X\, \mathcal{O}_X \oplus \mathcal{L}$ is a double covering $\widetilde{X}$ of X, ramified along E. Moreover, $\pi^* E_i = \widetilde{E}_i$ is a disjoint union of rational curves of self intersection -1, and hence can be blown down ; let $q : \tilde{X} \to Y$ be the resulting map. I claim that Y is an abelian surface and that X is the associated Kummer surface. To check this, first note that $h^0(\mathcal{L}) = h^2(\mathcal{L}) = 0$, so by Riemann-Roch, $h^1(\mathcal{L}) = -\frac{1}{2}\mathcal{L}^2 - 2 = 2$. But $H^1(Y, \mathcal{O}_Y) \cong H^1(\tilde{X}, \mathcal{O}_{\tilde{X}}) \cong H^1(X, \pi_* \mathcal{O}_{\tilde{X}}) = H^1(X, \mathcal{L})$, so $h^1(Y, \mathcal{O}_Y) = 2$ and $\beta_1(Y) \leq 4$. On the other hand, it is easy to check that $\chi_{top}(Y) = \chi_{top}(\tilde{X}) - 16 = 0$, and $\beta_2(Y) = \beta_2(\tilde{X}) - 16 \geq \beta_2(X) - 16 = 6$. This implies that $\beta_2(Y) = 6$, and that $\beta_1(Y) = 4$ $= 2h^1(Y, \mathcal{O}_Y)$. Since also $\omega_{\tilde{X}} = \pi^*(\omega_X)(\tilde{E}) = \mathcal{O}_{\tilde{X}}(\tilde{E}) = q^*(\omega_Y)(\tilde{E})$, ω_Y is trivial, and it follows that Y is abelian [5, thm. 6]. Choose any of the 16 points $q(\tilde{E}_i)$ as origin to endow Y with a group structure. The involution of $\tilde{X}/X$ descends to an involution τ on Y, with 16 points as fixed points. Since $\tau^2 = -1$, its eigenvalues on ℓ-adic cohomology are all ± 1. The trace formula tells us that the value of its characteristic polynomial at $+1$ is 16, whence all eigenvalues are -1, and hence $\tau = -\text{id}$. This completes the proof. □

7.13 Theorem. *Suppose X and X' are K3 surfaces with $\rho = 22$ and $\sigma_0 = 1$ or 2, and with isomorphic K3 crystals. Then X and X' are isomorphic.*

Proof. We already know that X and X' are Kummer, but we can say more : Choose an isomorphism $\theta : NS(X) \to NS(X')$ preserving effective cycles and extending to crystalline cohomology (by (7.8)), and a Kummer structure $Y \dashrightarrow X$ on X. Then by lemma (7.12), there is a Kummer structure $Y' \dashrightarrow X'$ such that $\Pi_{Y'} = \theta(\Pi_Y)$. Now $H^2_{cris}(X/W) \cong \pi_* q^* H^2_{cris}(Y/W) \oplus (\Pi_Y \otimes W)$, and $\pi_* q^* H^2_{cris}(Y/W)$ is the orthogonal complement of $\Pi_Y \otimes W$. The same is true for X', and hence it is clear that θ induces an isomorphism of K3 crystals : $H^2_{cris}(Y/W) \to H^2_{cris}(Y'/W)$. Thus, by (6.9), Y is isomorphic to Y', hence X is isomorphic to X'. □

7.14 Corollary. *There is a unique isomorphism class of K3 surfaces with $\rho = 22$ and $\sigma_0 = 1$, viz. the Kummer surface associated to any product of supersingular elliptic curves.* □

I recently learned in correspondance with Rudakov that he and Shafarevitch have also obtained this result, as well as Theorem (7.10).

It is perhaps premature, but I would like to indulge in some further speculations about a Torelli theorem for rigidified K3 surfaces. For each σ_o between 1 and 10, we know that there is a K3 surface with $\sigma_o(X) = \sigma_o$, and that the isomorphism class of its Neron-Severi group is unique. Choose an element N of this isomorphic class. If X is a K3 surface with $\rho = 22$, then by an "N-structure on X" we mean a map : $i : N \to NS(X)$ which is compatible with the intersection form. A "morphism of K3 surfaces with N-structure" is an isomorphism $X \to X'$ compatible with the N-structures in the obvious sense. If T is a K3 - lattice, then a "T-structure on X" is simply a T-structure on $H^2_{cris}(X/W)$. There is an obvious functor from K3 surfaces with N-structure to K3 surfaces with $N \otimes \mathbb{Z}_p$-structure, and the same argument as in (7.4.3) shows that this functor induces a bijection on isomorphism classes. In particular, if $N \to NS(X)$ is a K3-surface with N-structure, we can compute the "periods" of the associated K3 crystal with $N \otimes \mathbb{Z}_p$-structure. These periods are simply the point of $M_{N_o \otimes \mathbb{F}_p}(k)$ given by the Frobenius pull-back of

$$\mathrm{Ker} : N \otimes k \to H^2_{DR}(X/k).$$

Suppose that (X,i) and (X',i') are two K3 surfaces with N-structure, and that they have the same periods. Then there is a commutative diagram :

$$\begin{array}{ccc} N & \longrightarrow & H^2_{cris}(X/W) \\ & \searrow & \theta \downarrow \cong \\ & & H^2_{cris}(X'/W) \end{array}$$

and θ is unique. Moreover, since $N \to NS(X)$ and $N \to NS(X')$ are isomorphisms away from p and since $NS(X) \otimes \mathbb{Z}_p$ and $NS(X') \otimes \mathbb{Z}_p$ are the Tate modules of the corresponding crystals, it is clear that θ induces an isomorphism $NS(X) \to NS(X')$.

7.15 Conjecture. Suppose (X,i) and (X',i') are K3 surfaces with

N-structures which have the same periods, and suppose that the induced isomorphism $\theta : NS(X) \to NS(X')$ preserves effective cycles. Then θ is induced by an isomorphism of K3 surfaces with N-structure (necessarily unique, by (2.5)).

Proof when $\sigma_0 \leq 2$: Begin with the same proof as in (7.13). Thus, X and X' are Kummer surfaces, $\theta : NS(X) \to NS(X')$ and is an isomorphism preserving effective cycles and also the ramification locus of the double covers $\tilde{Y} \to X$, $\tilde{Y}' \to X'$. In other words, there is a bijection $\beta : H_1(Y, \mathbb{Z}/2\mathbb{Z}) \to H_1(Y', \mathbb{Z}/2\mathbb{Z})$ such that $\theta(E_y) = E'_{\beta(y)}$. By our choice of origins, $\beta(0) = 0$. In fact :

7.16 Lemma. The map β is a homomorphism.

Proof. It is clear from (7.11.3) that β preserves hyperplanes. If now x and y lie in $H_1(Y_{\acute{e}t}, \mathbb{Z}/2\mathbb{Z})$, I claim that $\beta(x+y) = \beta(x) + \beta(y)$. Indeed, we may assume that x and y are nonzero and that $x \neq y$. Then $\beta(x)$ and $\beta(y)$ are linearly independent and span a plane. If $\beta(x+y) \neq \beta(x) + \beta(y)$, then $\beta(x+y)$ does not lie in this plane, and hence there exists a hyperplane w containing $\beta(x)$ and $\beta(y)$ but not $\beta(x+y)$. Since $\beta^{-1}(\omega)$ is a hyperplane containing x and y, this is impossible. □

7.17 Lemma. The isomorphism $\frac{1}{2}\pi^* : \Pi_Y^\perp \to NS(Y)$ (7.11.1) mod 2 carries θ to $(\Lambda^2\beta)^{tr}$. That is, if $\rho : \Lambda^2 H_1 \to H^2$ is the isomorphism induced by Poincaré duality, the following diagram commutes :

$$\begin{array}{ccccc}
\Pi_Y^\perp \otimes \mathbb{Z}/2\mathbb{Z} & \xrightarrow[\cong]{\frac{1}{2}\pi^*} & H^2(Y_{\acute{e}t}, \mathbb{Z}/2\mathbb{Z}) & \xleftarrow[\cong]{\rho} & \Lambda^2 H_1(Y_{\acute{e}t}, \mathbb{Z}/2\mathbb{Z}) \\
\theta \downarrow \cong & & \theta' \downarrow \cong & & \cong \downarrow \Lambda^2\beta \\
\Pi_{Y'}^\perp \otimes \mathbb{Z}/2\mathbb{Z} & \xrightarrow[\cong]{\frac{1}{2}\pi^*} & H^2(Y'_{\acute{e}t}, \mathbb{Z}/2\mathbb{Z}) & \xleftarrow[\cong]{\rho} & \Lambda^2 H_1(Y'_{\acute{e}t}, \mathbb{Z}/2\mathbb{Z}).
\end{array}$$

Proof. Define θ' so that the square on the right commutes : if $V \subseteq H_1(Y_{\acute{e}t}, \mathbb{Z}/2\mathbb{Z})$ is a plane corresponding to an isotropic $v \in H^2(Y_{\acute{e}t}, \mathbb{Z}/2\mathbb{Z})$, then $\theta'(v)$ corresponds to $\beta(V)$, and $H^2(Y_{\acute{e}t}, \mathbb{Z}/2\mathbb{Z})$ is spanned by such vectors. Now by (7.11.2), $\frac{1}{2}\pi^* A_V$ mod 2 is simply v. But $A_V = 2F_V + \Sigma\{E_y : y \in V\}$, hence :

$$\begin{aligned}\theta(A_v) &= 2\,\theta(F_v) + \Sigma\,\{\theta(E_y) : y \in V\}\\ &= 2\,\theta(F_v) + \Sigma\,\{E_{\beta(y)} : y \in V\}\\ &= 2\,\theta(F_v) + \Sigma\,\{E_{y'} : y' \in \beta(V)\}.\end{aligned}$$

On the other hand, $<\theta(F_v), E_{\beta(y)}> = <F_v, E_y> = 0$ if $y \in V$, $= 1$ otherwise, i.e. $<\theta(F_v), E_{\beta(y)}> = <F_{\theta'(v)}, E_{\beta(y)}>$ for all y. This tells us that $\theta(F_v) - F_{\theta'(v)} \in \Pi^{\perp}_{Y'}$, and hence we see that $\theta(A_v) \equiv A_{\theta'(v)} \bmod 2\,\Pi^{\perp}_{Y'}$. By (7.11.1), $\frac{1}{2}\pi^{*}\theta(A_v) \equiv \frac{1}{2}\pi^{*}A_{\theta'(v)}$ mod 2 NS(Y'), i.e. $\frac{1}{2}\pi^{*}\theta(A_v)$ maps to $\theta'(v) = \theta'\,\frac{1}{2}\pi^{*}(A_v)$ mod 2. □

We can now prove (7.15) : Let $\theta' : NS(Y) \to NS(Y')$ be the isometry induced by θ. It follows from (7.17) that θ' mod 2 <u>preserves</u> the distinguished family of totally isotropic subspaces of H^2 (the hyperplanes in H^1), hence it also preserves them over $\mathbb{Z}_2$. Since θ' also preserves periods and effective cycles, we know by (7.3) that there is an isomorphism $f : Y' \to Y$ inducing θ'. Let $g : X' \to X$ be the corresponding map of Kummer surfaces ; I claim that g acts as θ on NS(X). This is clear on $\Pi^{\perp}_{Y}$; we must also check that $g^{*}(E_y) = \theta(E_y)$; i.e. that $f^{-1}(y) = \beta(y)$, for $y \in H_1(Y_{\text{ét}}, \mathbb{Z}/2\mathbb{Z})$. But notice : the automorphism $H_1(f) \circ \beta$ of $H_1(Y_{\text{ét}}, \mathbb{Z}/2\mathbb{Z})$ has as its second exterior power $(\Lambda^2 f_{*}) \circ \Lambda^2 \beta_{*}$. Lemma (7.11) implies that this is the identity, and since we are in characteristic two, $H_1(f) \circ \beta$ is also the identity. □

REFERENCES

[1] ARTIN, M. "Algebrization of Formal Moduli I" in Global Analysis, Princeton University Press, (1969) pp. 21-72.

[2] ARTIN, M. "Supersingular K3 Surfaces", Ann. Scient. de l'E.N.S., tome 7 fasc. 4 (1974) pp. 543-568.

[3] BERTHELOT, P. (Manuscript in preparation).

[4] BERTHELOT, P., and OGUS, A. Notes on Crystalline Cohomology, Princeton University Press (1978).

[5] BOMBIERI, F., and MUMFORD, D. "Enriques' classification of surfaces in char. p II" in Complex Analysis and Algebraic Geometry, Cambridge University Press (1977).

[6] BOURBAKI, N. Eléments de mathématique-algèbre, Fascicule XXIV, Livre II, Chapitre 9, "Formes sesquilinéaires et formes quadratiques" Hermann (1959).

[7] BURNS, D. and RAPOPORT, M. "On the Torelli problem for Kählerian K-3 Surfaces" Ann. Scient. de l'E.N.S. tome 8 fasc. 2 (1975) pp. 235-273.

[8] DELIGNE, P., and ILLUSIE L. "Relèvements des Surfaces K3 en caractéristique zéro" (Sém. de Géométrie Algébrique d'Orsay, à paraître).

[9] DELIGNE, P. and LUSZTIG, G. "Representations of Reductive Groups over Finite Fields" Ann. of Math. 103 (1976) pp. 103-161.

[10] KATZ, N. "Travaux de Dwork" Sém. Bourbaki 409 (1972), Lecture Notes in Mathematics N° 317, Springer (1973) pp. 167-200.

[11] KATZ, N. "Slope Filtration of F-crystals" (In these proceedings).

[12] MANIN, Y. "The theory of commutative formal groups over fields of finite characteristic", Russian Math. Surveys 18 (1963) pp. 1-80.

[13] MUMFORD, D. Abelian Varieties, Oxford University Press (1970).

[14] ODA, T. and OORT, F. "Supersingular Abelian Varieties" to appear in Kyoto Symposium on Algebraic Geometry.

[15] OGUS, A. "F-crystals and Griffiths Transversality" to appear in Kyoto Symposium on Algebraic Geometry.

[16] OGUS, A. "Griffiths transversality in crystalline cohomology" Ann. of Math. 108 (1978) pp. 395-419.

[17] O'MEARA, O. Introduction to Quadratic Forms, Springer Verlag (1963).

[18] PJATECKII-SAPIRO, I. and SAFAREVIC, I. "A Torelli theorem for algebraic surfaces of type K3" Math. U.S.S.R. Isvestija Vol. 5 (1971) pp. 547-588.

[19] PRASAD, G. "Strong approximation for semi-simple groups over function fields" Ann. of Math. 105 (1977) pp. 553-572.

[20] RUDAKOV, A. and SHAFAREVITCH, I. "Inseparable morphisms of algebraic surfaces" Akad. Sc. SSSR Tom. 40 n° 6 (1976), pp. 1264-1307.

[21] SERRE, J.-P. Cours d'Arithmétique, Collection SUP, Presses Universitaires de France (1970).

[22] SGA 7II - Groupes de Monodromie en Géométrie Algébrique. Springer Lecture Notes in Math. N° 340 (1973).

[23] SHIODA, T. "The period map of abelian surfaces" Journal of the Faculty of Science of the University of Tokyo Sec. IA vol. 25 N° 1 (1978) pp. 47-59.