Integral crystalline Tate classes on Mumford's fourfolds

The proof explained, from the basics

A companion to the note *Integral crystalline Tate classes of codimension two at supersingular points of Mumford's fourfolds*

Produced by large language models
not reviewed by the author or by any human expert

October 2026

Contents

Preface iv
Status iv
What the proof claims iv
Who this is for v
How the companion is organized v
Boxes and exercises vi
Conventions vi
What this companion does and does not establish vi

Part I. The question 1

Chapter 1. The question and the answer 2
1.1. The theorems and their proof in two pages 2
1.2. Integral versus rational 3
1.3. Mumford's fourfolds and the model 4
1.4. The theorems 5
1.5. The plan of the proof 6
1.6. What was known 7

Chapter 2. Abelian varieties in characteristic p and their cycles 8
2.1. Abelian varieties, cycles and specialization in two pages 8
2.2. Complex abelian varieties: a reminder 9
2.3. Abelian varieties 9
2.4. Supersingular abelian varieties 10
2.5. p-divisible groups 12
2.6. Cycles and intersection numbers 12
2.7. Reduction and specialization 13

Part II. Linear algebra of Frobenius 14

Chapter 3. Witt vectors, Frobenius and Dieudonné modules 15
3.1. Witt vectors and Dieudonné modules in two pages 15
3.2. Witt vectors 15
3.3. Semilinear maps and their matrices 16
3.4. Lang's lemma 17
3.5. Dieudonné modules 17
3.6. Slopes and the Newton polygon 19
3.7. The a-number 20
3.8. The module of a supersingular elliptic curve 20
3.9. Monomial modules and words 20

Chapter 4. Crystalline cohomology and integral Tate classes 23
4.1. Integral Tate classes in two pages 23
4.2. Crystalline cohomology of abelian varieties 23
4.3. Tate classes 24
4.4. The crystalline cycle class 25

4.5. Algebraic classes and divisor products 26
4.6. The rational statement 26
4.7. The intersection pairing and discriminants 27

Chapter 5. Monomial modules and the min-plus calculus 28
5.1. Monomial lattices and min-plus formulas in two pages 28
5.2. Monomial lattices 29
5.3. Monomial Dieudonné modules 29
5.4. The descent lemma 30
5.5. Worked examples 31
5.6. Products and the index 31
5.7. Endomorphisms and the span of pull-backs 32
5.8. Independence of p, and how the exact computations work 33

Part III. The gap at Mumford's fourfolds 35

Chapter 6. Mumford's fourfolds 36
6.1. Mumford's families in two pages 36
6.2. The group and the Shimura datum 37
6.3. Very general members and the exceptional classes 38
6.4. The integral model 39
6.5. The lattice at p is a tensor induction 40
6.6. Data for every prime 42

Chapter 7. The Dieudonné module at a supersingular point 43
7.1. The model in two pages 43
7.2. Frobenius as a group element 43
7.3. Crystals of rank two 45
7.4. Slopes: μ-ordinary or supersingular 45
7.5. The model 46
7.6. The p-divisible group $\mathscr{G}_p$ 46

Chapter 8. The gap: four missing classes 48
8.1. The gap in two pages 48
8.2. The cube basis and Frobenius 49
8.3. The four sets 49
8.4. The index proposition 49
8.5. The eigensets of an inert quadratic action 52
8.6. The Weil lattice and the majority lattice 53

Chapter 9. Endomorphisms move one Weil class onto the gap 54
9.1. Endomorphisms and the structure of the gap in two pages 54
9.2. Endomorphisms of X and of (M, F) 55
9.3. The endomorphism proposition 55
9.4. Proof of Theorem A(a) 57

Part IV. Filling the gap with one Weil cycle 59

Chapter 10. Weil classes, Hermitian forms and unimodular lattices 60
10.1. Weil classes in two pages 60
10.2. Abelian varieties of Weil type 61
10.3. Hermitian forms 62
10.4. Unimodular Hermitian lattices at an inert prime 63
10.5. Schoen's step in lattice form 64

Chapter 11. Markman's classes and Hypothesis (M) 66

11.1. Markman's classes in two pages 66
11.2. The construction 67
11.3. Hypothesis (M) 68
11.4. Chern classes of complexes and of cycles 69
11.5. The integral Weil cycle on the sixfolds 71
11.6. Why integer coefficients matter 73
11.7. The status of the dependency 73
11.8. The Weil coefficient 74

Chapter 12. A fourfold with complex multiplication 77
12.1. The CM fourfold in two pages 77
12.2. The statement 78
12.3. The field K and the torus 78
12.4. The algebra of complex multiplication 79
12.5. Integrality and supersingular reduction 79
12.6. The diagonal action 80
12.7. Unimodularity at p 82

Chapter 13. A p-integral Weil cycle and its specialization 84
13.1. The specialization argument in two pages 84
13.2. The Weil cycle on the CM fourfold 84
13.3. The projector 86
13.4. The Gram determinant 87
13.5. The specialized classes span the Weil lattice 88

Part V. The theorems and beyond 89

Chapter 14. The theorems, and what they rest on 90
14.1. The whole proof in two pages 90
14.2. The transport lemma 91
14.3. Proof of Theorem A 91
14.4. Proof of Theorem B 92
14.5. Proof of Theorem C 92
14.6. The exceptional Hodge classes 93
14.7. What the proof rests on 93

Chapter 15. Other supersingular fourfolds 96
15.1. Other monomial modules in two pages 96
15.2. Monomial modules and their cycle decompositions 96
15.3. Isomorphisms between decompositions 97
15.4. The Fourier source 98
15.5. The monomial-module proposition 99
15.6. The four undecided modules 100

Appendix A. Glossary of symbols 102

Appendix B. Hints and solutions 106

Bibliography 121

Preface

Status

This companion, like the note it explains, was produced by large language models, instances of the Claude models of Anthropic running as autonomous agents, in October 2026. The proofs it explains were checked only by other instances of the same models, and such checks may share the blind spots of the models that wrote the proofs. The companion was not reviewed by the author or by any human expert, and no human expert has checked the proofs. It is published together with the note as an explanation of its proofs, and it may contain errors in its explanations, examples and remarks, in addition to any errors in the proofs themselves.

The note *Integral crystalline Tate classes of codimension two at supersingular points of Mumford's fourfolds* (October 2026) states the proofs concisely, for specialists, and the code for the exact computations on which the proofs rely is published with it. This companion explains the same proofs from the basics. It is meant to be read on its own: it states everything it uses, proves what can be proved in a few pages, and cites the published literature for the rest.

What the proof claims

Let $p \geq 5$ be a prime and X a supersingular abelian fourfold over $\bar{\mathbb{F}}_p$. Its integral crystalline Tate classes of codimension 2 form a free $\mathbb{Z}_p$-module $T^4(X)$ of rank 70, and the products of two divisor classes span a sublattice $S(X)$ of full rank. The classes of algebraic cycles span a lattice $\mathrm{Alg}^2(X)$ between the two. Rationally the three agree, so the integral question is whether the finite group $T^4(X)/\mathrm{Alg}^2(X)$ vanishes. Chapter 1 sets this up.

The proof explained here answers the question at the supersingular points of Mumford's families of abelian fourfolds, at primes p that are inert in the cubic field of the family and at which its quaternion algebra splits, for the hyperspecial levels given by tensor-induced lattices. At every such point, $T^4(X)/S(X) \cong (\mathbb{Z}/p)^4$: the divisor classes miss exactly four independent classes, and the endomorphisms of X move a single Weil class onto all four (Theorem A(a) of Chapter 1). The proof of the second half assumes Hypothesis (M): that three statements made in the proof of a theorem of a preprint of Markman, on the algebraicity of Weil classes on abelian sixfolds, hold, together with the other statements of the preprint that the proof cites. From them the proof derives that an explicit integral class on a family of abelian sixfolds of Weil type is the class of an algebraic cycle with integer coefficients. Under Hypothesis (M), one algebraic Weil class with the right p-adic normalization exists, so $\mathrm{Alg}^2(X) = T^4(X)$, which is the integral crystalline Tate conjecture in codimension 2 for X (Theorem A(b)). Under Hypothesis (M), the same then holds on every abelian fourfold over $\bar{\mathbb{F}}_p$ with the same p-divisible group (Theorem C(b)). At primes that are unramified and not inert in the cubic field, under the analogous conditions on the quaternion algebra and the level, divisor classes suffice and $T^4(X) = S(X)$ (Theorem B). Beyond Mumford's families, the monomial supersingular Dieudonné modules of height 8 and dimension 4 fall into fourteen isomorphism classes: the conjecture holds unconditionally on the fourfolds of nine of them, under Hypothesis (M) on those of one, and the methods explained here leave the remaining four undecided (Chapter 15).

The proof uses no p-adic comparison theorem. Intersection numbers, which specialization preserves, fix the p-adic normalization of the one class that is needed. The computer-assisted parts are exact computations with integers: the exponents of lattices that, in a well-chosen basis, are given by explicit min-plus formulas that do not depend on p (Chapter 5). One coefficient that the proof derives in general is also confirmed, for six values of a parameter, by an exact computation in an imaginary quadratic field (Chapter 11).

Who this is for

The companion is written for a master's student in mathematics who knows linear algebra, including tensor and exterior products, groups, rings, fields and modules over principal ideal domains, the p-adic numbers, how a prime splits in a number field, and some algebraic geometry: varieties, morphisms, divisors. Complex abelian varieties are reviewed where they are needed (Chapters 2 and 10). The companion does not assume Witt vectors, Dieudonné modules, crystalline cohomology, Shimura varieties, Hermitian lattices over local fields or derived categories. Witt vectors and Dieudonné modules are developed from the definitions (Chapter 3). Crystalline cohomology, integral models of Shimura varieties and derived categories enter only through a few precisely stated facts, which are explained and given with references but not proved.

How the companion is organized

Part I states the question and the theorems and recalls abelian varieties in characteristic p. Part II develops the linear algebra of Frobenius: Witt vectors and Dieudonné modules, integral Tate classes, and the min-plus calculus that computes them for monomial modules. Part III goes to Mumford's fourfolds, finds their Dieudonné module at a supersingular point, computes the gap $T^4/S \cong (\mathbb{Z}/p)^4$ and shows how endomorphisms act on it. Part IV produces one algebraic Weil class: Weil classes and Hermitian lattices, Markman's classes and Hypothesis (M), a fourfold with complex multiplication, and the specialization argument. Part V proves the theorems, lists everything the proof rests on, and treats other supersingular fourfolds.

Fast path. Chapter 1, then the first section of every following chapter, then Chapter 14. The first sections are written so that they read consecutively as one sketch of the proof. Each says what its chapter proves, the one idea behind it, and one example:

chapter	first section	topic
2	Section 2.1	abelian varieties in characteristic p, cycles, specialization
3	Section 3.1	Witt vectors and Dieudonné modules
4	Section 4.1	integral Tate classes and divisor products
5	Section 5.1	monomial lattices and min-plus formulas
6	Section 6.1	Mumford's families and their integral models
7	Section 7.1	the Dieudonné module at a supersingular point
8	Section 8.1	the four missing classes
9	Section 9.1	endomorphisms and the structure of the gap
10	Section 10.1	Weil classes and unimodular Hermitian lattices
11	Section 11.1	Markman's classes and Hypothesis (M)
12	Section 12.1	a fourfold with complex multiplication
13	Section 13.1	one Weil cycle and its specialization
14	Section 14.1	the proofs of the theorems
15	Section 15.1	other supersingular fourfolds

Full path. Chapter 1 to Chapter 15 in order. A reader who knows Dieudonné theory can read only the first sections of Chapters 3 and 4. A reader who wants to see where the computations enter can take Chapters 5, 8, 9 and 15, and one who wants to see where the proof depends on Markman's preprint can take Chapters 11, 13 and 14.

Boxes and exercises

Each chapter opens with a blue box, *Where we are*, that says what the chapter contributes to the proof and what it needs from earlier chapters, and closes with a remark on where its results are used. Yellow boxes, *Intuition*, say in plain words what an object or a step means. Green boxes, *What just happened*, sum up a long argument. Red boxes, *Remark on the proof*, mark places where the argument is terse, where it relies on a fact that is cited rather than proved, or where it rests on a computation.

The exercises stand right after the concept they need, and most of them are computations with the numbers of the proof: the orbits of Frobenius on the eight basis vectors of the model, the exponents of a few Tate lattices, a Gram determinant at $p = 5$. They are meant to be done when met, with pen and paper. Each has a full solution in Chapter B, preceded by a hint, so that a reader can look at the hint first and the solution only if the hint is not enough.

Conventions

The table collects the conventions that cause most confusion. Each is fixed once, in the chapter named in the table, and used without change afterwards.

object	convention
the prime	$p \geq 5$ throughout, unless a statement says otherwise
rings	$W = W(\bar{\mathbb{F}}_p)$, the Witt vectors of $\bar{\mathbb{F}}_p$, with Frobenius σ; $\mathbb{Z}_{p^r} = W(\mathbb{F}_{p^r})$, $\mathbb{Q}_{p^r} = \mathbb{Z}_{p^r}[1/p]$ (Chapter 3)
Dieudonné module	$M(X) = H^1_{\text{cris}}(X/W)$, the contravariant Dieudonné module of $X[p^\infty]$ (Chapter 3)
Frobenius, Verschiebung	F is σ-semilinear, $F(\lambda x) = \sigma(\lambda)F(x)$, and $V = pF^{-1}$ is σ^{-1}-semilinear; for a matrix A, $F = A\sigma$ means $F(x) = A\sigma(x)$ with σ applied to coordinates
cohomology	$H^n_{\text{cris}}(X/W) = \bigwedge^n M(X)$, with F acting as $\bigwedge^n F$ and an endomorphism α as $\alpha^* = \bigwedge^n \alpha^*$ (Chapter 4)
Tate classes	for supersingular X and even n, $T^n(X) = \{x \in H^n_{\text{cris}}(X/W) : Fx = p^{n/2}x\}$; $S(X) \subseteq T^4(X)$ is spanned by products of two classes in $T^2(X)$; $\text{Alg}^i(X)$ is the $\mathbb{Z}_p$-span of classes of codimension-i cycles (Chapter 4)
words	a monomial Dieudonné module is named by binary words, one per cycle of basis vectors, whose letters are the exponents: $Fe_i = p^{w_i} e_{i+1}$; the word 01 is the module of a supersingular elliptic curve E_0 (Chapter 3)
the model	$\mathbb{M} = W^2 \otimes W^2 \otimes W^2$ with $F(x_1 \otimes x_2 \otimes x_3) = \sigma x_3 \otimes A\sigma x_1 \otimes \sigma x_2$, $A = \left(\begin{smallmatrix} 0 & p \\ 1 & 0 \end{smallmatrix}\right)$, the Dieudonné module at every supersingular point of Mumford's families at an inert prime, for tensor-induced levels (Chapters 1 and 7)
action of K	for an imaginary quadratic field K acting on an abelian variety, the type (g_+, g_-) counts the multiplicities of the two embeddings of K on $H^{1,0}$, or on $H^0(X, \Omega^1)$ in characteristic p (Chapter 10)
Hermitian forms	the Riemann form ψ on H_1 is $\text{Tr}_{K/\mathbb{Q}} \circ \mathcal{H}$ for a skew-Hermitian form $\mathcal{H}$, and $h = \theta\mathcal{H}$ with $\theta^2 = -d_0$ is Hermitian (Chapter 10)
reserved letters	k the totally real cubic field and B the quaternion algebra of Mumford's family; K an imaginary quadratic field and $K' = kK$; R the algebra of complex multiplication; E_0 a supersingular elliptic curve; $\mathscr{G}_p$ the p-divisible group of $\mathbb{M}$

What this companion does and does not establish

This companion explains the proofs, and it does not certify them. Writing a proof out in more detail makes it easier to check, but it does not make it checked. The worked examples test special cases with small numbers. They can expose an error in a formula or a number,

but they do not replace the exact computations of the proof, which can only be checked by rerunning them or by redoing them by other means. Chapter 14 puts the whole proof on a few pages and lists what it rests on: Hypothesis (M), the standard facts that are cited with references rather than proved, and the computations.

Part I

The question

CHAPTER 1

The question and the answer

Where we are. This chapter states the question, the three theorems that answer it, and the plan of their proof. It needs nothing beyond the preface. The objects that appear in the statements (crystalline cohomology, integral Tate classes, Mumford's families, Hypothesis (M)) are introduced here informally and defined precisely in later chapters, which are named at each point.

1.1. The theorems and their proof in two pages

Let $p \geq 5$ be a prime and X an abelian variety of dimension g over $\bar{\mathbb{F}}_p$. Its first crystalline cohomology $M(X) = H^1_{\mathrm{cris}}(X/W)$ is a free module of rank $2g$ over the ring $W = W(\bar{\mathbb{F}}_p)$ of Witt vectors, with a Frobenius F, and its higher cohomology is the exterior algebra, $H^n_{\mathrm{cris}}(X/W) = \bigwedge^n M(X)$. When X is supersingular, the classes x in degree $2i$ with $Fx = p^i x$ form a free $\mathbb{Z}_p$-module $T^{2i}(X)$ of rank $\binom{2g}{2i}$, the *integral crystalline Tate classes*. Inside it lie the classes of algebraic cycles of codimension i, which span a sublattice $\mathrm{Alg}^i(X)$, and in degree 4 the products of two divisor classes, which span a sublattice $S(X)$. So

$$S(X) \subseteq \mathrm{Alg}^2(X) \subseteq T^4(X).$$

After tensoring with $\mathbb{Q}$ all three agree. The *integral crystalline Tate conjecture in codimension* 2 for X asks whether $\mathrm{Alg}^2(X) = T^4(X)$, that is, whether the finite group $T^4(X)/\mathrm{Alg}^2(X)$ vanishes. In codimension 1 the answer is yes for every supersingular X, and the content of codimension 2 lies in the classes that are not products of divisor classes, measured by the finite group $T^4(X)/S(X)$.

For an abelian fourfold, T^4 has rank $\binom{8}{4} = 70$. The companion explains a proof that, for one specific supersingular p-divisible group $\mathscr{G}_p$ of height 8, every abelian fourfold X with $X[p^\infty] \cong \mathscr{G}_p$ has $T^4(X)/S(X) \cong (\mathbb{Z}/p)^4$, and that $\mathrm{Alg}^2(X) = T^4(X)$ if Hypothesis (M) holds. The group $\mathscr{G}_p$ is the one that occurs at every supersingular point of Mumford's families of abelian fourfolds at a prime p that is inert in their cubic field, for the hyperspecial levels given by tensor-induced lattices (Theorems A and C). At primes that are unramified and not inert in the cubic field, with the quaternion algebra of the family split above p and the lattice at p a tensor induction as in (h4), the supersingular points have $T^4 = S$ (Theorem B).

The proof has two halves. The first half is linear algebra. At an inert prime, for such a level, the Dieudonné module of a supersingular point is the explicit module $\mathbb{M}$ of (1.1) below, and in its basis e_s, $s \in \{0,1\}^3$, Frobenius sends each basis vector to a power of p times another basis vector. In such a basis every lattice the proof needs, T^4, S and the span of the pull-backs by endomorphisms, is spanned by multiples $p^{n_J} e_J$ of the wedge products e_J of basis vectors, and the exponents n_J are given by explicit formulas of min-plus type, sums and maxima and minima of the integers 0 and 1 that do not depend on p (Chapter 5). Evaluating them for the 70 wedge products of degree 4 shows that S misses exactly four classes, each by one factor of p, so that $T^4/S \cong (\mathbb{Z}/p)^4$ (Chapter 8). The same calculus shows that the endomorphisms of X move a single Weil class, a class attached to an action of an imaginary quadratic field, onto all four missing classes (Chapter 9). So one algebraic class with the right normalization at p is all that is missing.

The second half produces that class. Hypothesis (M) (Hypothesis (M)) is that three statements made in the proof of a theorem of a preprint of Markman hold, together with

the other statements of the preprint that the proof cites; from them Proposition 11.5 derives that an explicit integral class on the abelian sixfolds of Weil type of one family is the class of an algebraic cycle with integer coefficients. Schoen's degeneration argument carries these cycles to a fourfold X_{CM} in Mumford's family with complex multiplication, chosen so that its first homology is a unimodular Hermitian lattice at p; the result is a cycle on X_{CM} whose Weil component has a coefficient that is a unit at p (Chapters 10 to 12). The fourfold X_{CM} reduces to a supersingular point. Two cycles built from this one by an endomorphism have an intersection matrix whose determinant is a unit at p, and since specialization preserves intersection numbers, their specializations span the whole rank-2 lattice of integral Weil classes at the supersingular point (Chapter 13). No p-adic comparison theorem is needed. Finally, isogenies of degree prime to p carry the result to every abelian fourfold with p-divisible group $\mathscr{G}_p$ (Chapter 14).

Example 1.1 (the ranks). For an abelian fourfold, $M(X)$ has rank 8, so $H^2_{\mathrm{cris}}(X/W) = \bigwedge^2 M(X)$ has rank $\binom{8}{2} = 28$ and $H^4_{\mathrm{cris}}(X/W)$ has rank $\binom{8}{4} = 70$. For a supersingular X these are the ranks of $T^2(X)$ and $T^4(X)$. For $X = E_0 \times E_0$, with E_0 a supersingular elliptic curve, $M(X)$ has rank 4 and $T^2(X)$ has rank $\binom{4}{2} = 6$. The Néron–Severi group of $E_0 \times E_0$ has rank 6 as well: two classes from the factors and four from the graphs of a basis of $\mathrm{End}(E_0)$, which has rank 4 (Chapter 2). This equality of ranks is the rational form of the statement $\mathrm{NS}(X) \otimes \mathbb{Z}_p \cong T^2(X)$ of Fact 4.10.

1.2. Integral versus rational

The precise definitions are in Chapter 4, and this section explains why the question is about a finite group and why it is posed only for supersingular varieties.

For a supersingular abelian variety X of dimension g over $\bar{\mathbb{F}}_p$ and even n, the integral crystalline Tate classes are

$$T^n(X) = \{x \in H^n_{\mathrm{cris}}(X/W) : \ Fx = p^{n/2}x\},$$

a free $\mathbb{Z}_p$-module of rank $\binom{2g}{n}$ (Definition 4.3). The crystalline cycle class of an algebraic cycle of codimension i lies in $T^{2i}(X)$ when $i \le 2$ (Fact 4.6), and $\mathrm{Alg}^i(X)$ is the $\mathbb{Z}_p$-span of these classes (Definition 4.8). The lattice $S(X) \subseteq T^4(X)$ is the $\mathbb{Z}_p$-span of the products $x \wedge y$ with $x, y \in T^2(X)$ (Definition 4.9). Two facts relate the three lattices. First, every class in $T^2(X)$ is a $\mathbb{Z}_p$-combination of classes of divisors, $\mathrm{NS}(X) \otimes \mathbb{Z}_p \cong T^2(X)$ (Fact 4.10); since the class of an intersection is the product of the classes, $S(X) \subseteq \mathrm{Alg}^2(X)$. Second, $S(X)$ has finite index in $T^4(X)$ (Proposition 4.12). So $S(X) \otimes \mathbb{Q} = \mathrm{Alg}^2(X) \otimes \mathbb{Q} = T^4(X) \otimes \mathbb{Q}$, the rational statement holds, and what is left is the finite group $T^4(X)/\mathrm{Alg}^2(X)$, which is a quotient of $T^4(X)/S(X)$ (Exercise 1.3).

Intuition 1.2 (where the missing classes are). Rationally every Tate class is a polynomial in divisor classes. Integrally, a Tate class x with $px \in S(X)$ but $x \notin S(X)$ is a class that divisor classes only reach after multiplication by p. The theorems below say that for the fourfolds with p-divisible group $\mathscr{G}_p$ there are exactly four independent such classes, and that, under Hypothesis (M), algebraic cycles reach them.

Why only supersingular varieties. For an abelian variety that is not supersingular, the module of F-fixed classes can be larger than the span of algebraic classes, already in degree 2. Let E and E' be ordinary elliptic curves over $\bar{\mathbb{F}}_p$ that are not isogenous, and $X = E \times E'$. The Dieudonné module of an ordinary elliptic curve is $(W, \sigma) \oplus (W, p\sigma)$ (Example 3.9), so $M(X) = M_{\mathrm{et}} \oplus M_{\mathrm{mult}}$, where F is a σ-semilinear bijection of M_{et} and p times one of M_{mult}, both of rank 2; these are the parts of slope 0 and 1 (Chapter 3). So

$$\textstyle\bigwedge^2 M(X) = \bigwedge^2 M_{\mathrm{et}} \ \oplus \ (M_{\mathrm{et}} \otimes M_{\mathrm{mult}}) \ \oplus \ \bigwedge^2 M_{\mathrm{mult}}$$

has parts of slope 0, 1 and 2 and of ranks 1, 4 and 1. The classes with $Fx = px$ lie in the middle part and form a free $\mathbb{Z}_p$-module of rank 4 (Exercise 1.2). On the other

hand $\mathrm{NS}(X)\otimes\mathbb{Q}$ is the subspace of $\mathrm{End}(X)\otimes\mathbb{Q}$ fixed by the Rosati involution (see e.g. [Mil08, Chapter I, Proposition 14.2]). Since E and E' are not isogenous, $\mathrm{Hom}(E,E')=0$ and $\mathrm{End}(X)\otimes\mathbb{Q}=(\mathrm{End}(E)\times\mathrm{End}(E'))\otimes\mathbb{Q}$, and the Rosati-fixed part of each factor is $\mathrm{NS}(E)\otimes\mathbb{Q}=\mathbb{Q}$, by the same proposition. So $\mathrm{NS}(X)$ has rank 2, and two of the four F-fixed directions are not spanned by algebraic classes even rationally. For this reason $T^n(X)$ is defined in this companion only for supersingular X, where no such phenomenon occurs (Proposition 4.12).

Exercise 1.1. Let M be a free module of rank 8. Compute the ranks of $\bigwedge^n M$ for $0\le n\le 8$. Given a basis $e_1,\dots,e_8$, how many unordered pairs $\{J,J'\}$ of disjoint 2-element subsets of $\{1,\dots,8\}$ are there, and how many such pairs have a given union?

Exercise 1.2. In the surface $E\times E'$ above, assume that M_{et} has a basis e_1,e_2 with $Fe_i=e_i$ and M_{mult} a basis e_3,e_4 with $Fe_j=pe_j$ (this is the case over $\overline{\mathbb{F}}_p$, by Lang's lemma, Lemma 3.5). Show that $\{x\in\bigwedge^2 M(X) : Fx=px\}$ is the $\mathbb{Z}_p$-span of the four vectors $e_i\wedge e_j$, $i\in\{1,2\}$, $j\in\{3,4\}$, and that no nonzero vector of $\bigwedge^2 M_{\mathrm{et}}\oplus\bigwedge^2 M_{\mathrm{mult}}$ satisfies $Fx=px$.

Exercise 1.3. Let $L\subseteq L'\subseteq L''$ be free $\mathbb{Z}_p$-modules of the same finite rank. Show that L''/L' is a quotient of L''/L, so that $L''/L=0$ implies $L''/L'=0$, and that $[L'':L]=[L'':L'][L':L]$.

Exercise 1.4. Let $L'\subseteq L$ be free $\mathbb{Z}_p$-modules of rank n with $[L:L']=p^4$ and $pL\subseteq L'$. Show that $L/L'\cong(\mathbb{Z}/p)^4$.

1.3. Mumford's fourfolds and the model

Mumford constructed from certain data families of abelian fourfolds of Hodge type whose members have trivial endomorphism ring, $\mathrm{End}(X_{\mathrm{gen}})=\mathbb{Z}$, at a very general point [Mum69, Section 4]; the group of the corresponding Shimura datum becomes, over $\overline{\mathbb{Q}}$, the image of $\mathbb{G}_m\times\mathrm{SL}_2^3$ acting on $\mathbb{C}^2\otimes\mathbb{C}^2\otimes\mathbb{C}^2$ (see e.g. [SZ16, Section 2]). So these fourfolds are not described by their endomorphisms and polarization alone. The data are a totally real cubic field k and a quaternion algebra B over k that is split at exactly one of the three real places and whose corestriction to $\mathbb{Q}$ is a matrix algebra (Chapter 6). Moonen and Zarhin showed that for a very general member X_{gen}, whose Hodge group is a $\mathbb{Q}$-form of an almost direct product of three copies of SL_2, the self-product $X_{\mathrm{gen}}\times X_{\mathrm{gen}}$ carries Hodge classes of degree 4 that are not in the span of products of divisor classes [MZ99]. This makes the reductions of Mumford's fourfolds modulo p natural test cases for integral questions about cycles of codimension 2. What the theorems below do and do not imply for the Hodge classes on $X_{\mathrm{gen}}\times X_{\mathrm{gen}}$ is discussed in Remark 14.3.

The Shimura varieties of these families have integral models at the primes where the level is hyperspecial (Kisin, Fact 6.4), and at a prime p that is inert in k, for the hyperspecial levels given by tensor-induced lattices (the hypotheses (6.2) of Section 1.4), their supersingular points all have the same Dieudonné module, which is the following module $\mathbb{M}$ (Proposition 7.4). Let $W=W(\overline{\mathbb{F}}_p)$, let σ be its Frobenius, and let

$$A=\begin{pmatrix}0 & p\\ 1 & 0\end{pmatrix},\qquad Ae_0=e_1,\quad Ae_1=pe_0,$$

in the standard basis e_0,e_1 of W^2. The *model* is

$$\mathbb{M}=W^2\otimes W^2\otimes W^2,\qquad F(x_1\otimes x_2\otimes x_3)=\sigma x_3\otimes A\sigma x_1\otimes\sigma x_2, \tag{1.1}$$

where σ acts on coordinates. It has the *cube basis* $e_s=e_{s_1}\otimes e_{s_2}\otimes e_{s_3}$, indexed by the vertices $s=(s_1,s_2,s_3)$ of the cube $\mathcal{C}=\{0,1\}^3$, written as strings such as $s=011$. Since $Ae_{s_1}=p^{s_1}e_{1-s_1}$, Frobenius permutes the basis up to powers of p:

$$Fe_s=p^{s_1}e_{(s_3,1-s_1,s_2)}.$$

Everything the proof needs to know about the supersingular points is in this formula. The module $\mathbb{M}$ is a Dieudonné module of height 8 and dimension 4 (Exercise 1.5), all of whose

slopes are $\frac{1}{2}$ (Chapter 8). Let $\mathscr{G}_p$ be the p-divisible group over $\bar{\mathbb{F}}_p$ whose Dieudonné module is $\mathbb{M}$; it exists and is unique up to isomorphism by Dieudonné theory (Fact 3.10), and it depends only on p. It is the product of the p-divisible group of a supersingular elliptic curve and one of height 6 (Remark 7.6).

EXERCISE 1.5. Show that $\mathbb{M}$ is a Dieudonné module of height 8 and dimension 4 in the sense of Definition 3.8: $F(\mathbb{M}) = W^2 \otimes AW^2 \otimes W^2$ contains $p\mathbb{M}$, and $\mathbb{M}/F(\mathbb{M})$ has length 4. Using the formula $Fe_s = p^{s_1} e_{(s_3, 1-s_1, s_2)}$, list the four basis vectors e_s that are not in $F(\mathbb{M})$.

1.4. The theorems

Fix (k, B) as above, Mumford's Shimura datum attached to it, a lattice Λ in its rational representation $\mathbb{V} = \mathbb{Q}^8$ with a symplectic form ψ, and a level $\mathsf{K} = \mathsf{K}_p \mathsf{K}^p$ with K_p the stabilizer of $\Lambda \otimes \mathbb{Z}_p$. Let $\mathscr{S}$ be Kisin's integral model of the Shimura variety at a prime above p and $\mathcal{A} \to \mathscr{S}$ the abelian scheme (Chapter 6). The hypotheses (6.2) at p are: $p \geq 5$; p is inert in k; B is split at the place of k above p; and the lattice $\Lambda \otimes \mathbb{Z}_p$ is, up to a power of p, the tensor induction of a lattice in the plane on which $B \otimes_k k_p$ acts, which makes the level at p hyperspecial. For fixed (k, B, Λ) the last two hold for all but finitely many p, and for every $p \geq 5$ there are data satisfying all four (Lemma 6.10).

The theorems use the following objects, all defined later. For an isomorphism $M(X) \cong \mathbb{M}$, the *Weil lattice* $\mathcal{L} \subseteq T^4(X)$ is a lattice of rank 2 such that $\mathcal{L} \otimes_{\mathbb{Z}_p} W$ is spanned by the top exterior powers of the two eigenspaces of an action of $\mathbb{Z}_{p^2}$ on $(M(X), F)$ of type $(2,2)$, diagonal in the cube basis (Definition 8.6), and $\mathcal{N} \subseteq T^4(X)$ is the analogous *majority lattice* of an action of type $(1,3)$ (Definition 8.8). Hypothesis (M) is that three statements made in a preprint of Markman hold, together with the other statements of the preprint cited in Chapter 11; it is stated in Hypothesis (M), the integral statement that the proof derives from it is Proposition 11.5, and the status of the dependency is discussed in Section 11.7.

THEOREM A (supersingular points at inert primes). *Assume (6.2), and let $t \in \mathscr{S}(\bar{\mathbb{F}}_p)$ be a point at which $X = \mathcal{A}_t$ is supersingular.*

(a) $T^4(X)/S(X) \cong (\mathbb{Z}/p)^4$. More precisely, for an isomorphism $M(X) \cong \mathbb{M}$, the lattice $N = S(X) + \mathcal{N}$ satisfies $N/S(X) \cong (\mathbb{Z}/p)^2$ and is stable under the pull-backs α^*, $\alpha \in \mathrm{End}(X)$; the quotient $T^4(X)/N \cong (\mathbb{Z}/p)^2$ is the image of $\mathcal{L}$; and for every $x \in T^4(X) \setminus N$ the lattice $S(X)$ and the classes $\alpha^* x$, $\alpha \in \mathrm{End}(X)$, span $T^4(X)$. Hence $T^4(X)/S(X)$ is, as a module over $\mathrm{End}(X)$, a non-split extension of $T^4(X)/N$ by $N/S(X)$.

(b) Assume Hypothesis (M). Then $\mathrm{Alg}^2(X) = T^4(X)$: the integral crystalline Tate conjecture holds in codimension 2 on X. Moreover, the Künneth component in $H^2_{\mathrm{cris}}(X/W) \otimes H^2_{\mathrm{cris}}(X/W)$ of every class in $T^4(X \times X)$ lies in $\mathrm{Alg}^2(X \times X)$.

THEOREM B (supersingular points at non-inert primes). *Let $p \geq 5$ be a prime that is unramified and not inert in k, assume that B is split at every place of k above p and that $\Lambda \otimes \mathbb{Z}_p = p^j \mathrm{Cor}(\Lambda_0)$ for an $O_k \otimes \mathbb{Z}_p$-lattice Λ_0 (conditions (h3) and (h4), read with $k_p = k \otimes \mathbb{Q}_p$, which is a product of fields when p is not inert), and let $t \in \mathscr{S}(\bar{\mathbb{F}}_p)$ be a point at which $X = \mathcal{A}_t$ is supersingular. Then $T^4(X) = S(X)$, and the Künneth component in $H^2_{\mathrm{cris}}(X/W) \otimes H^2_{\mathrm{cris}}(X/W)$ of $T^4(X \times X)$ is spanned by the corresponding components of products of divisor classes on $X \times X$. In particular $\mathrm{Alg}^2(X) = T^4(X)$, without Hypothesis (M).*

THEOREM C (every fourfold with p-divisible group $\mathscr{G}_p$). *Let $p \geq 5$ and let X be an abelian fourfold over $\bar{\mathbb{F}}_p$ with $X[p^\infty] \cong \mathscr{G}_p$.*

(a) $T^4(X)/S(X) \cong (\mathbb{Z}/p)^4$, and the statements of Theorem A(a) hold for X.

(b) Assume Hypothesis (M). Then $\mathrm{Alg}^2(X) = T^4(X)$, and the Künneth component in $H^2_{\mathrm{cris}}(X/W) \otimes H^2_{\mathrm{cris}}(X/W)$ of every class in $T^4(X \times X)$ lies in $\mathrm{Alg}^2(X \times X)$.

The proof of Theorem A(a) is in Section 9.4. The proofs of the rest, which put together all chapters, are in Chapter 14. Theorem C is not a statement about Mumford's families, but its proof goes through them: it proves (b) at one supersingular point of one family and transports it. Part (a) of Theorems A and C is a statement about the module $\mathbb{M}$ alone.

Other monomial modules. The model $\mathbb{M}$ is *monomial*: in a suitable basis Frobenius maps basis vectors to multiples of basis vectors. Supersingular monomial Dieudonné modules of height 8 and dimension 4 are named by binary words (Definition 3.17), and Chapter 15 compares them. Their twenty cycle decompositions give fourteen isomorphism classes. The integral crystalline Tate conjecture in codimension 2 holds, without Hypothesis (M), on every abelian fourfold whose Dieudonné module lies in one of nine of these classes, it holds under Hypothesis (M) for the class of $\mathbb{M}$ (Theorem C), and the methods explained here leave the remaining four undecided.

1.5. The plan of the proof

Figure 1.1 shows the steps and the chapters where they are explained.

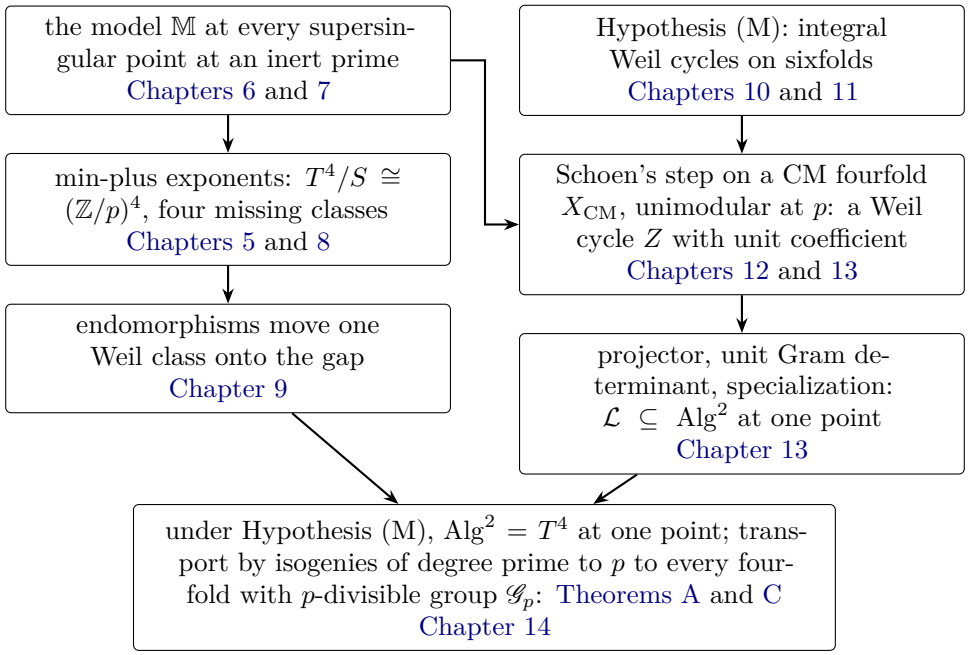


FIGURE 1.1. The steps of the proof of Theorems A and C and the chapters that explain them. The left column is linear algebra over W and uses no algebraic cycles; the right column produces one algebraic class.

(1) *The model.* Kisin's integral model carries crystalline tensors that force the Dieudonné module of a point at an inert prime, when the lattice at p is a tensor induction as in (h4), to be a tensor product of three modules of rank 2, permuted cyclically by Frobenius, with the Hodge filtration in one slot. At a supersingular point this pins the module down to $\mathbb{M}$ (Proposition 7.4). In particular all supersingular points have p-divisible group $\mathscr{G}_p$.
(2) *The gap.* In the cube basis, T^4, S and every other lattice of the proof are spanned by multiples $p^{n_J} e_J$ of wedge products, with exponents given by explicit min-plus formulas (Lemma 5.3). An exact computation of these integers gives $T^4/S \cong (\mathbb{Z}/p)^4$, carried by four wedge products indexed by four special subsets of the cube (Proposition 8.2).
(3) *One Weil class suffices.* Two of the four special subsets are the eigensets of an action of $\mathbb{Z}_{p^2}$ of type $(2,2)$, and their wedge products span the Weil lattice $\mathcal{L}$. The endomorphism proposition, which rests in part on a second exact computation, shows that S together with the pull-backs of any primitive element of $\mathcal{L}$ by endomorphisms is all of T^4 (Proposition 9.4 and Section 9.4). So the conjecture at a supersingular point follows from $\mathcal{L} \subseteq \mathrm{Alg}^2$.
(4) *A Weil cycle with unit coefficient.* Choose an imaginary quadratic field K inert at p and a point t_{CM} of Mumford's family with complex multiplication by $K \times kK$, whose abelian variety X_{CM} has a first homology that is a unimodular Hermitian lattice over O_K

at p and whose reduction is supersingular (Proposition 12.2 and Lemma 12.6). Under Hypothesis (M), Schoen's degeneration argument carries an algebraic Weil cycle with integer coefficients from an abelian sixfold of Weil type (Proposition 11.5) to X_{CM}, through an isogeny of degree prime to p, and gives a cycle Z on X_{CM} whose Weil component is $\nu_Z\omega + \bar{\nu}_Z\bar{\omega}$ with ν_Z a unit at p (Proposition 13.2).

(5) *Specialization by intersection numbers.* A projector P, a polynomial in one endomorphism, cuts out the Weil part; the two cycles PZ and its translate by an endomorphism have a Gram determinant that is a unit at p. Specialization preserves intersection numbers, so the specialized classes span a sublattice of $\mathcal{L}$ of unit discriminant, which is all of $\mathcal{L}$ (Proposition 13.4).

(6) *Transport.* Two supersingular abelian varieties with isomorphic p-divisible groups are related by an isogeny of degree prime to p, which identifies T^4, S and Alg^2 (Lemma 14.2). This carries the result from the one point of (4) to every abelian fourfold with p-divisible group $\mathscr{G}_p$.

What the proof rests on. Besides Hypothesis (M), whose exact form and status are in Chapter 11, the proof uses a lemma on Chern classes in families, proved in Section 11.4 from results of Atiyah and Hirzebruch, of Borel and Haefliger, and of Grothendieck, and a number of standard facts that are cited with references and not proved here, among them Dieudonné theory, the comparison of homomorphisms of abelian varieties with homomorphisms of Dieudonné modules, the properties of the crystalline cycle class and of specialization, and Kisin's results on the integral model. Each is stated as a Fact at the place where it is first needed, with one sentence on its status, and Section 14.7 lists all of them together with the exact computations.

1.6. What was known

A preprint of Broe claims the Tate conjecture for abelian fourfolds over finite fields, through Markman's Weil classes, and deduces the crystalline Tate conjecture for them [Bro26, Theorem 1.1 and Corollary 8.1(ii)]. A preprint of Milne states that it deduces a similar statement for the integral Tate conjecture [Mil25] from the failure of the integral Hodge conjecture for very general principally polarized abelian varieties of dimension at least 4, which is claimed in a preprint of Engel, de Gaay Fortman and Schreieder [EGS25]. A preprint of Scavia and Suzuki claims applications of its results on direct summands of products of Jacobians to the integral Tate conjecture for divisors and 1-cycles on abelian varieties over finitely generated fields, and to a p-adic version of it over finite fields [SS25]. The same authors constructed non-algebraic classes of degree 4 over finite fields that vanish over the algebraic closure [SS24]. Cadoret and Pirutka give, assuming variational realization conjectures, uniform bounds for the obstructions to the integral Tate conjecture in one-dimensional families over infinite finitely generated fields [CP26]. Gregory proved that torsion codimension-2 cycles on supersingular abelian varieties are algebraically trivial [Gre23]. For Mumford's families, that the Newton polygon jumps only at supersingular points is stated, under a mild assumption on p, in [SZ16]; Chapter 7 proves the statement it needs, because the explicit module $\mathbb{M}$ is needed. A preprint of Chen claims that some of Mumford's fourfolds have infinitely many supersingular primes [Che25].

Where this is used. The model (1.1) is derived in Chapter 7 and analyzed in Chapters 8 and 9. Theorems A to C are proved in Section 9.4 and Chapter 14.

CHAPTER 2

Abelian varieties in characteristic p and their cycles

Where we are. This chapter collects the facts about abelian varieties over $\bar{\mathbb{F}}_p$ that the proof uses: isogenies and their degrees, supersingular abelian varieties, p-divisible groups, Chow groups and intersection numbers, and the specialization of cycles from characteristic 0 to characteristic p. It needs the question chapter; familiarity with complex abelian varieties helps but is not required. Most statements are standard and are cited with references. Two of them carry weight in the proof and are stated as Facts: Oort's theorem on supersingular abelian varieties (Fact 2.6) and the properties of specialization (Fact 2.9).

2.1. Abelian varieties, cycles and specialization in two pages

An abelian variety over an algebraically closed field is a connected smooth projective group variety. Over $\mathbb{C}$ it is a complex torus $\mathbb{C}^g/L$, and multiplication by an integer n has kernel $(\mathbb{Z}/n)^{2g}$. Over $\bar{\mathbb{F}}_p$ the same holds for n prime to p, but the p-torsion is smaller: the group of $\bar{\mathbb{F}}_p$-points of order dividing p is $(\mathbb{Z}/p)^l$ for some $0 \le l \le g$, the p-rank. The extreme case $l = 0$ for elliptic curves defines the supersingular elliptic curves, and an abelian variety is supersingular if it is isogenous to a product of them (Definition 2.5). All supersingular elliptic curves over $\bar{\mathbb{F}}_p$ are isogenous to each other, so every supersingular abelian variety of dimension g is isogenous to E_0^g for one fixed supersingular elliptic curve E_0 (Fact 2.6).

An isogeny of degree prime to p does not change the integral questions at p. The p-part of an abelian variety is recorded by its p-divisible group $X[p^\infty]$, the system of the finite group schemes $X[p^n]$ (Definition 2.7), and an isogeny of degree prime to p induces an isomorphism of p-divisible groups (Exercise 2.6). This is why the theorems of Chapter 1 are stated for all abelian fourfolds with a given p-divisible group: the lattices T^4 and S depend only on $X[p^\infty]$, and isogenies of degree prime to p move algebraic cycles between supersingular varieties with the same p-divisible group (Lemma 14.2).

Algebraic cycles are recorded in Chow groups $\mathrm{CH}^i(X)$, with an intersection product, pull-backs, push-forwards, and the degree of a 0-cycle; together these give intersection numbers. The algebraic classes the proof needs at a supersingular point are not constructed in characteristic p. They are constructed on a fourfold X_{CM} over a number field and then specialized along an abelian scheme over a discrete valuation ring whose special fiber is the supersingular fourfold. Specialization of cycles is a ring homomorphism that preserves degrees of 0-cycles and commutes with pull-backs by endomorphisms (Fact 2.9). Consequently it preserves intersection numbers, and this is the property that controls the specialized classes integrally in Chapter 13.

Example 2.1 (a supersingular elliptic curve over $\mathbb{F}_5$). Let E be the elliptic curve $y^2 = x^3+1$ over $\mathbb{F}_5$; the cubic x^3+1 has discriminant $-27 \not\equiv 0 \bmod 5$, so E is smooth. The values of x^3+1 at $x = 0, 1, 2, 3, 4$ are $1, 2, 4, 3, 0$ modulo 5, and the squares modulo 5 are $0, 1, 4$. So the affine points are $(0, \pm 1)$, $(2, \pm 2)$ and $(4, 0)$, and with the point at infinity $\#E(\mathbb{F}_5) = 6 = p+1$. The trace of Frobenius $p+1-\#E(\mathbb{F}_5)$ is 0, and this makes E supersingular. Indeed, the Frobenius endomorphism π of E has a characteristic polynomial $X^2 - aX + p$ with $a = p+1-\#E(\mathbb{F}_p)$, and π satisfies it (see e.g. [Mil08, Chapter I, Proposition 10.20, and Chapter II, Theorem 1.1 and its proof]). For $a = 0$ this gives $\pi^2 = -p$, so $[p] = -\pi^2$; since π raises coordinates to the p-th power, it is injective on $E(\bar{\mathbb{F}}_p)$, and so $[p]$ kills no point other than 0: the p-rank is 0.

2.2. Complex abelian varieties: a reminder

The characteristic-p theory is easiest to understand next to the complex one, which reappears in Chapters 10 to 12. We recall it briefly; for the description as a complex torus with a Riemann form see e.g. [Mil08, Chapter I, Section 2].

A complex abelian variety of dimension g is a complex torus $X = \mathbb{C}^g/L_X$, with $L_X \cong \mathbb{Z}^{2g}$ a lattice, that admits an embedding into projective space. Its homology is $H_1(X,\mathbb{Z}) = L_X$, and its cohomology is the exterior algebra

$$H^n(X,\mathbb{Z}) = \textstyle\bigwedge^n H^1(X,\mathbb{Z}), \qquad H^1(X,\mathbb{Z}) = \operatorname{Hom}(L_X,\mathbb{Z}),$$

the complex counterpart of Fact 3.10(c). The complex structure gives the Hodge decomposition $H^1(X,\mathbb{C}) = H^{1,0} \oplus H^{0,1}$, with $H^{1,0}$ the space of holomorphic 1-forms, of dimension g, and $H^n(X,\mathbb{C}) = \bigoplus_{i+j=n} \bigwedge^i H^{1,0} \otimes \bigwedge^j H^{0,1}$. A *Hodge class* of degree $2i$ is a class in $H^{2i}(X,\mathbb{Q})$ of type (i,i); classes of algebraic cycles of codimension i are Hodge classes, and the Hodge conjecture asks for the converse with rational coefficients. A polarization corresponds to a *Riemann form*, an integral alternating form on L_X satisfying positivity conditions with respect to the complex structure, and $\mathrm{NS}(X)$ is identified with $H^2(X,\mathbb{Z}) \cap H^{1,1}$. An endomorphism α acts on L_X, and its pull-back on $H^n(X,\mathbb{Z})$ is $\bigwedge^n$ of its action on H^1.

In characteristic p the lattice $H^1(X,\mathbb{Z})$ is replaced by the Dieudonné module $M(X)$, a lattice over W instead of over $\mathbb{Z}$, and the Hodge decomposition by the Frobenius F. The space $H^{1,0}$ of holomorphic 1-forms has the counterpart $VM(X)/pM(X) \cong H^0(X,\Omega^1)$ (Fact 3.10(d)). Hodge classes are replaced by Tate classes, the classes fixed by $p^{-i}F$ in degree $2i$ (Chapter 4). An action of an imaginary quadratic field K on X splits $H^{1,0}$, respectively $H^0(X,\Omega^1)$, into the two eigenspaces of K, and the pair of their dimensions is the *type* of the action (Definition 10.2). This is how the type $(2,2)$ that singles out the Weil lattice in Chapter 8 is read off in characteristic p.

2.3. Abelian varieties

We recall the basic theory over $\bar{\mathbb{F}}_p$; most of it holds over any algebraically closed field, and a reference is [Mil08, Chapter I]. Nothing in this section is proved here, except where a proof is given.

An *abelian variety* X over $\bar{\mathbb{F}}_p$ is a connected smooth projective variety with a structure of algebraic group; the group law is commutative, and $g = \dim X$ is its dimension. A *homomorphism* $X' \to X$ is a morphism of varieties that is a group homomorphism. An *isogeny* is a surjective homomorphism with finite kernel between abelian varieties of the same dimension; its *degree* is the degree of the field extension of function fields, which equals the order of the kernel as a finite group scheme. For an integer $n \neq 0$, multiplication by n is an isogeny $[n]\colon X \to X$ of degree n^{2g} (Exercise 2.4). If $f\colon X' \to X$ is an isogeny, there is an isogeny $f'\colon X \to X'$ with $f \circ f' = [\deg f]$ and $f' \circ f = [\deg f]$; being isogenous is an equivalence relation.

The *dual* abelian variety $X^\vee$ parametrizes line bundles on X that are algebraically equivalent to 0, and the *Poincaré bundle* $\mathcal{P}$ on $X \times X^\vee$ is the universal such line bundle, trivial on $X \times \{0\}$ and $\{0\} \times X^\vee$. A line bundle $\mathscr{L}$ on X defines a homomorphism $\mathrm{pol}_{\mathscr{L}}\colon X \to X^\vee$, sending x to the translate of $\mathscr{L}$ by x tensored with $\mathscr{L}^{-1}$, and a *polarization* is an isogeny of the form $\mathrm{pol}_{\mathscr{L}}$ with $\mathscr{L}$ ample. The *Néron–Severi group* $\mathrm{NS}(X)$ is the group of line bundles modulo algebraic equivalence; it is free of finite rank, and $\mathscr{L} \mapsto \mathrm{pol}_{\mathscr{L}}$ embeds it into $\operatorname{Hom}(X, X^\vee)$.

The *endomorphism ring* $\mathrm{End}(X)$ is a free $\mathbb{Z}$-module of finite rank, at most $4g^2$. A polarization $\mathrm{pol}_{\mathscr{L}}$ defines the *Rosati involution* $\alpha \mapsto \alpha^\dagger = \mathrm{pol}_{\mathscr{L}}^{-1} \circ \alpha^\vee \circ \mathrm{pol}_{\mathscr{L}}$ on $\mathrm{End}(X) \otimes \mathbb{Q}$, and $\mathrm{NS}(X) \otimes \mathbb{Q}$ is identified with the subspace of elements α with $\alpha^\dagger = \alpha$ (see e.g. [Mil08, Chapter I, Proposition 14.2]). For an elliptic curve the Rosati involution of the principal polarization sends an isogeny to its dual.

Intuition 2.2 (the Néron–Severi group as symmetric endomorphisms). A line bundle $\mathscr{L}'$ on X gives the homomorphism $\mathrm{pol}_{\mathscr{L}'}\colon X \to X^\vee$, and composing with the inverse of a polarization turns it into an element of $\mathrm{End}(X)\otimes\mathbb{Q}$. The symmetry of the intersection pairing becomes the condition $\alpha^\dagger = \alpha$. So the rank of $\mathrm{NS}(X)$ is the dimension of the space of symmetric elements of the endomorphism algebra.

Example 2.3 ($\mathrm{NS}(E_0\times E_0)$). Let E_0 be a supersingular elliptic curve over $\bar{\mathbb{F}}_p$. Its endomorphism ring $\mathrm{End}(E_0)$ has rank 4, and $\mathrm{End}(E_0)\otimes\mathbb{Q}$ is a quaternion algebra over $\mathbb{Q}$: it is a division algebra of dimension 4 because E_0 is simple, and it is not commutative, because $\mathrm{End}(E_0)\otimes\mathbb{Q}_p$ is the quaternion division algebra over $\mathbb{Q}_p$ (Fact 4.10 and Example 5.8). On it the Rosati involution fixes exactly $\mathrm{NS}(E_0)\otimes\mathbb{Q} = \mathbb{Q}$, so $\alpha+\alpha^\dagger$ and $\alpha\alpha^\dagger$ are rational for every α, which makes $\dagger$ the canonical involution $\alpha\mapsto\bar\alpha$ (Exercise 2.1). On $X = E_0\times E_0$ with the product polarization, $\mathrm{End}(X)\otimes\mathbb{Q}$ is the algebra of 2×2 matrices with quaternion entries and the Rosati involution is $(\alpha_{ij})\mapsto(\bar\alpha_{ji})$. A matrix fixed by it has rational diagonal entries and an arbitrary off-diagonal entry α_{12}, which determines $\alpha_{21} = \bar\alpha_{12}$. So $\mathrm{NS}(E_0\times E_0)$ has rank $1+1+4=6$: the two fibers $\{0\}\times E_0$ and $E_0\times\{0\}$, and four classes coming from the graphs of a basis of $\mathrm{End}(E_0)$.

Exercise 2.1. Let B_0 be a quaternion algebra over $\mathbb{Q}$ and $\dagger$ an involution of B_0 (an anti-automorphism of order 2) whose fixed elements are exactly $\mathbb{Q}$. Show that $\alpha^\dagger = \mathrm{trd}(\alpha)-\alpha$ for every $\alpha\in B_0$, where $x^2-\mathrm{trd}(\alpha)x+\mathrm{nrd}(\alpha)$ is the reduced characteristic polynomial: for $\alpha\notin\mathbb{Q}$, the elements $\lambda=\alpha+\alpha^\dagger$ and $\lambda'=\alpha\alpha^\dagger$ are rational, so $\alpha^2-\lambda\alpha+\lambda'=0$, and a monic quadratic polynomial over $\mathbb{Q}$ that vanishes at $\alpha\notin\mathbb{Q}$ is unique.

Polarizations and degrees. A polarization $\mathrm{pol}_{\mathscr{L}}$ has degree $\chi(\mathscr{L})^2$, where $\chi(\mathscr{L})$ is the Euler characteristic, which by the Riemann–Roch theorem for abelian varieties is $(\mathscr{L}^g)/g!$ (see e.g. [Mil08, Chapter I, Theorem 11.1]). A polarization is *principal* if it has degree 1, as for the theta divisor of a Jacobian or the product polarization of E_0^g. If the degree is prime to p, the polarization is an isogeny $X\to X^\vee$ of degree prime to p and so identifies $X[p^\infty]$ with $X^\vee[p^\infty]$ (Exercise 2.6); on Dieudonné modules this means $M(X)\cong M(X)^\vee$ (Chapter 3). This is the property that singles out the self-dual modules in Chapter 15, and in Chapter 12 a polarization that is perfect at p is what makes the first homology of the fourfold X_{CM} a unimodular lattice at p.

Endomorphisms of supersingular varieties. An isogeny $f\colon X'\to X$ identifies $\mathrm{End}(X)\otimes\mathbb{Q}$ with $\mathrm{End}(X')\otimes\mathbb{Q}$, by $\alpha\mapsto f'\alpha f/\deg f$ in the notation above. So by Fact 2.6(a) every supersingular abelian variety of dimension g has $\mathrm{End}(X)\otimes\mathbb{Q}\cong\mathrm{Mat}_g(\mathrm{End}(E_0)\otimes\mathbb{Q})$, of dimension $4g^2$ over $\mathbb{Q}$, and $\mathrm{Hom}(X',X)$ has rank $4\dim X\dim X'$ for supersingular X,X' (Exercise 2.3). This is the largest possible rank, and it is the rank used in Fact 4.10.

Exercise 2.2. Show in the same way that $\mathrm{NS}(E_0^g)$ has rank $g(2g-1)$, and that this is 28 for $g=4$.

Exercise 2.3. Show that for supersingular abelian varieties X of dimension g and X' of dimension g' over $\bar{\mathbb{F}}_p$, $\mathrm{Hom}(X',X)\otimes\mathbb{Q}\cong\mathrm{Mat}_{g\times g'}(\mathrm{End}(E_0)\otimes\mathbb{Q})$, of dimension $4gg'$, using isogenies to E_0^g and $E_0^{g'}$.

Exercise 2.4. Let $\mathscr{L}$ be an ample line bundle on X with $[-1]^*\mathscr{L}\cong\mathscr{L}$. Using the facts that then $[n]^*\mathscr{L}\cong\mathscr{L}^{\otimes n^2}$, that the self-intersection number $(\mathscr{L}^g)=\deg\left(c_1(\mathscr{L})^g\right)$ of an ample line bundle is positive, and that a finite surjective morphism f between varieties of dimension g satisfies $((f^*\mathscr{L})^g)=\deg f\cdot(\mathscr{L}^g)$, show that $\deg[n]=n^{2g}$.

2.4. Supersingular abelian varieties

For n prime to p, the kernel of $[n]$ on $X(\bar{\mathbb{F}}_p)$ is $(\mathbb{Z}/n)^{2g}$, as over $\mathbb{C}$. For $n=p$ the isogeny $[p]$ has degree p^{2g} but is not separable, and its kernel $X[p]$ is a finite group scheme of order p^{2g} whose group of $\bar{\mathbb{F}}_p$-points is $(\mathbb{Z}/p)^l$ with $0\le l\le g$. The integer l is the *p-rank*, and X is

ordinary if $l = g$. An elliptic curve is either ordinary ($l = 1$) or *supersingular* ($l = 0$). An elliptic curve is supersingular exactly when the Newton slopes of its Dieudonné module are $\frac{1}{2}, \frac{1}{2}$ rather than $0, 1$ (see e.g. [Lie16, Section 3.4.1]). By a result of Deuring there are only finitely many supersingular elliptic curves over $\bar{\mathbb{F}}_p$ up to isomorphism, roughly $p/12$ of them (see e.g. [Lie16, Section 3.4.1]), and any two are isogenous (Fact 2.6).

Group schemes of order p. Over $\bar{\mathbb{F}}_p$ there are three group schemes of order p: the constant group $\mathbb{Z}/p$, the multiplicative group $\boldsymbol{\mu}_p$ of p-th roots of unity, and the additive group $\boldsymbol{\alpha}_p$, the kernel of $x \mapsto x^p$ on the additive group. Only $\mathbb{Z}/p$ has p points; $\boldsymbol{\mu}_p$ and $\boldsymbol{\alpha}_p$ have one point but are not trivial. For an ordinary elliptic curve, $E[p] \cong \boldsymbol{\mu}_p \times \mathbb{Z}/p$. For a supersingular one, $E[p]$ has no point other than 0; it is a non-split extension of $\boldsymbol{\alpha}_p$ by $\boldsymbol{\alpha}_p$. The number of copies of $\boldsymbol{\alpha}_p$ in $X[p]$, the dimension of $\mathrm{Hom}(\boldsymbol{\alpha}_p, X)$ over $\bar{\mathbb{F}}_p$, is the a-number $a(X)$, which in Chapter 3 is defined and computed through Dieudonné modules. It is 1 for a supersingular elliptic curve and g for E_0^g, and it can distinguish supersingular varieties that are isogenous but not isomorphic.

Frobenius and Verschiebung. Over $\bar{\mathbb{F}}_p$ every abelian variety X has a relative Frobenius isogeny $X \to X^{(p)}$, raising coordinates to the p-th power, of degree p^g and purely inseparable, and a Verschiebung isogeny $X^{(p)} \to X$ with composite $[p]$. On the Dieudonné module of Chapter 3 they induce the operators F and V, with $FV = VF = p$; this is the origin of the letters. For a supersingular elliptic curve the kernel of Frobenius is $\boldsymbol{\alpha}_p$, and so is the kernel of Verschiebung, which matches the equality $FM = VM$ proved for $M(E_0)$ in Proposition 3.16.

Example 2.4 (the same curve at $p = 7$). At $p = 7$ the curve $y^2 = x^3 + 1$ of Example 2.1 behaves differently. Modulo 7 the cubes are $0, 1, 1, 6, 1, 6, 6$ for $x = 0, \dots, 6$, so $x^3 + 1$ takes the values $1, 2, 2, 0, 2, 0, 0$, and the squares modulo 7 are $0, 1, 2, 4$. The value 1 gives 2 points, each of the three values $2 = 3^2$ gives 2 points, and each of the three values 0 gives 1 point; with the point at infinity $\#E(\mathbb{F}_7) = 2+6+3+1 = 12$, so the trace of Frobenius is $7+1-12 = -4 \neq 0$, and the argument of Example 2.1 does not apply. The characteristic polynomial of Frobenius is now $X^2 + 4X + 7$, and $\pi^2 = -4\pi - 7$ is not of the form $-p$ times an automorphism.

Definition 2.5 (supersingular). An abelian variety X over $\bar{\mathbb{F}}_p$ is *supersingular* if it is isogenous to a product of supersingular elliptic curves. It is *superspecial* if it is isomorphic to a product of supersingular elliptic curves.

Fact 2.6 (Oort). *Fix a supersingular elliptic curve E_0 over $\bar{\mathbb{F}}_p$.*

(a) Every supersingular abelian variety of dimension g over $\bar{\mathbb{F}}_p$ is isogenous to E_0^g.

(b) An abelian variety over $\bar{\mathbb{F}}_p$ is supersingular if and only if all slopes of its Dieudonné module are $\frac{1}{2}$ (slopes are defined in Chapter 3).

Oort calls an abelian variety supersingular if its formal group is isogenous to a power of the formal group of slope $\frac{1}{2}$, that is, if all slopes of its Dieudonné module are $\frac{1}{2}$, and proves that such a variety of dimension g is isogenous to E^g for a supersingular elliptic curve E [Oor74, Theorem 4.2]. For elliptic curves the two notions of supersingularity agree (see e.g. [Lie16, Section 3.4.1]). Applied to a supersingular elliptic curve, Oort's theorem shows that any two supersingular elliptic curves are isogenous, which with the definition gives (a). Slopes do not change under isogeny, so (a) and the elliptic case give one direction of (b), and Oort's theorem gives the other.

By part (a), a supersingular X admits an isogeny $E_0^g \to X$, so it is the quotient of E_0^g by a finite subgroup scheme, and a quotient by a subgroup scheme of p-power order can change the p-divisible group. So a supersingular abelian variety need not be superspecial. The fourfolds of the theorems are of this kind: their Dieudonné module $\mathbb{M}$ has a-number 2 (Chapter 3), while a superspecial fourfold has a-number 4. Conversely, every F- and V-stable W-lattice in $M(E_0^g) \otimes \mathbb{Q}$ is, after multiplication by a power of p, the Dieudonné module of a quotient of E_0^g by a finite subgroup scheme; this follows from Dieudonné theory, and Section 15.2 explains it for the monomial modules. It is how all the monomial modules of Chapter 15 occur as Dieudonné modules of abelian fourfolds.

Exercise 2.5. Count the points of $y^2 = x^3 + 1$ over $\mathbb{F}_{11}$. (Hint: $x \mapsto x^3$ is a bijection of $\mathbb{F}_{11}$.) Is the curve supersingular?

2.5. p-divisible groups

The finite group schemes $X[p^n]$ form a system $X[p] \subseteq X[p^2] \subseteq \cdots$ with inclusions and multiplication by p maps between them.

Definition 2.7 (p-divisible group). The *p-divisible group* of an abelian variety X of dimension g is the system $X[p^\infty] = (X[p^n])_{n\geq 1}$. It has *height* $2g$, meaning that $X[p^n]$ has order p^{2gn}, and *dimension* g, the dimension of its tangent space at the origin. A homomorphism $f\colon X' \to X$ induces a homomorphism $f[p^\infty]\colon X'[p^\infty] \to X[p^\infty]$.

The p-divisible group is the part of X that crystalline cohomology sees: by Dieudonné theory (Chapter 3) it is determined by its Dieudonné module, which is $H^1_{\text{cris}}(X/W)$. For an ordinary elliptic curve, $E[p^\infty]$ is an extension of an étale group by a multiplicative one, which over $\bar{\mathbb{F}}_p$ splits. For a supersingular elliptic curve it is connected of height 2 and dimension 1, and it is the same for all supersingular elliptic curves (Equation (3.1)). Two supersingular abelian varieties with isomorphic p-divisible groups are related by an isogeny of degree prime to p (Lemma 14.2); the converse direction is the following exercise.

Exercise 2.6. Let $f\colon X' \to X$ be an isogeny whose degree is prime to p. Show that $f[p^\infty]$ is an isomorphism. (Use f' with $f \circ f' = [\deg f]$, $f' \circ f = [\deg f]$ and the fact that $[\deg f]$ is an automorphism of every $X[p^n]$.)

2.6. Cycles and intersection numbers

Let Y be a smooth projective variety over a field. The *Chow group* $\mathrm{CH}^i(Y)$ is the group of cycles of codimension i, formal $\mathbb{Z}$-combinations of irreducible closed subvarieties of codimension i, modulo rational equivalence. The following operations are standard (see e.g. [The, Tags 0B0G, 0B0H and 0AZ1]):

(a) an *intersection product* that makes $\mathrm{CH}^\bullet(Y) = \bigoplus_i \mathrm{CH}^i(Y)$ a commutative graded ring; for subvarieties meeting properly it is the sum of the components of the intersection with their intersection multiplicities;
(b) for a morphism $f\colon Y' \to Y$ of smooth projective varieties, a *pull-back* ring homomorphism $f^*\colon \mathrm{CH}^\bullet(Y) \to \mathrm{CH}^\bullet(Y')$, and a *push-forward* $f_*\colon \mathrm{CH}^i(Y') \to \mathrm{CH}^{i+\dim Y - \dim Y'}(Y)$, related by the projection formula $f_*(f^*x \cdot y) = x \cdot f_*y$;
(c) the *degree* $\deg\colon \mathrm{CH}^{\dim Y}(Y) \to \mathbb{Z}$ of 0-cycles, $\sum n_i[x_i] \mapsto \sum n_i$ over an algebraically closed field.

For cycles $x \in \mathrm{CH}^i(Y)$ and $y \in \mathrm{CH}^{\dim Y - i}(Y)$, the *intersection number* is $\deg(x \cdot y)$. The divisor classes, $\mathrm{CH}^1(Y)$ modulo algebraic equivalence, form $\mathrm{NS}(Y)$.

Example 2.8 (intersection numbers on $E \times E$). Let E be an elliptic curve over $\bar{\mathbb{F}}_p$, and on $E \times E$ consider the fibers $E_1 = \{0\} \times E$ and $E_2 = E \times \{0\}$, two copies of E, and, for an endomorphism α of E, the graph $\Gamma_\alpha = \{(y, \alpha y)\}$. The curves E_1 and E_2 meet transversally in the origin, so $\deg(E_1 \cdot E_2) = 1$, and $\deg(E_1 \cdot E_1) = \deg(E_2 \cdot E_2) = 0$ because a fiber can be moved off itself. The graph meets E_1 in the origin only, $\deg(\Gamma_\alpha \cdot E_1) = 1$, and it meets E_2 in $\{(y, 0) : \alpha y = 0\}$, the kernel of α; counted with multiplicities, $\deg(\Gamma_\alpha \cdot E_2) = \deg \alpha$. In the same way two graphs meet along $\{(y, \alpha y) : \alpha y = \alpha' y\}$, the kernel of $\alpha - \alpha'$, and $\deg(\Gamma_\alpha \cdot \Gamma_{\alpha'}) = \deg(\alpha - \alpha')$, with the convention $\deg 0 = 0$. These intersection numbers are standard, and the companion uses them only in this example; when $\alpha - \alpha'$ is separable the intersection is transversal and consists of $\deg(\alpha - \alpha')$ points. For the diagonal Γ_1 and the antidiagonal Γ_{-1}, this gives $\deg(\Gamma_1 \cdot \Gamma_{-1}) = \deg[2] = 4$: the two curves meet in the four points (y, y) with $2y = 0$, which are distinct because $p \neq 2$. For $E = E_0$ the graphs of a $\mathbb{Z}$-basis of $\mathrm{End}(E_0)$, with E_1 and E_2, give the six classes of Example 2.3, and the formula $\deg(\Gamma_\alpha \cdot \Gamma_{\alpha'}) = \deg(\alpha - \alpha')$ expresses their intersection matrix through the degree, which on $\mathrm{End}(E_0)$ is the reduced norm of the quaternion algebra.

For abelian varieties the main sources of cycles are divisors, intersections of them, and images and inverse images of cycles under homomorphisms. For an endomorphism α of X, the pull-back α^* acts on $\mathrm{CH}^\bullet(X)$, and on $X \times X$ the projections $\mathrm{pr}_1, \mathrm{pr}_2$ and homomorphisms $X \times X \to X$, $(y_1, y_2) \mapsto \alpha_1 y_1 + \alpha_2 y_2$, give pull-backs from X to $X \times X$. These are the cycles that appear in Chapter 9, where a single cycle class and its pull-backs by all endomorphisms are shown to span everything that divisor classes do not reach.

2.7. Reduction and specialization

Let O be a discrete valuation ring whose fraction field has characteristic 0 and whose residue field is contained in $\bar{\mathbb{F}}_p$. An *abelian scheme* $\mathcal{X}$ over O is a smooth proper group scheme over O with connected fibers; its generic fiber $\mathcal{X}_{\mathrm{gen}}$ and its special fiber $\mathcal{X}_{\mathrm{sp}}$ are abelian varieties, and $\mathcal{X}_{\mathrm{gen}}$ is said to have *good reduction*, with reduction $\mathcal{X}_{\mathrm{sp}}$. Abelian varieties with complex multiplication over a number field acquire good reduction everywhere after a finite extension (see e.g. [Mil05, Proposition 10.5], applied to the simple isogeny factors); this is how the fourfold X_{CM} of Chapter 12 gets a supersingular reduction.

Fact 2.9 (Néron property and specialization). *Let O be as above.*

(a) If $\mathcal{X}$ and $\mathcal{X}'$ are abelian schemes over O, every homomorphism $\mathcal{X}'_{\mathrm{gen}} \to \mathcal{X}_{\mathrm{gen}}$ of the generic fibers extends uniquely to a homomorphism $\mathcal{X}' \to \mathcal{X}$ over O. In particular endomorphisms of $\mathcal{X}_{\mathrm{gen}}$ extend to $\mathcal{X}$ and reduce to endomorphisms of $\mathcal{X}_{\mathrm{sp}}$.

(b) Assume moreover that O is complete. Let $\mathcal{Y}$ be a smooth projective scheme over O. There is a specialization map $\mathrm{sp}\colon \mathrm{CH}^\bullet(\mathcal{Y}_{\mathrm{gen}}) \otimes \mathbb{Q} \to \mathrm{CH}^\bullet(\mathcal{Y}_{\mathrm{sp}}) \otimes \mathbb{Q}$ *that maps the class of a subvariety to the class of the special fiber of its closure, is a ring homomorphism, and is compatible with push-forwards and pull-backs along morphisms of smooth projective O-schemes, in particular with degrees of 0-cycles and with pull-backs by endomorphisms of $\mathcal{Y}$ over O.*

Part (a) is the Néron mapping property: an abelian scheme over O is the Néron model of its generic fiber (see e.g. [Mil08, Chapter I, Remark 17.2]). For (b) see e.g. [GM87, Appendix B, B.3], and [The, Tag 0H4H] for specialization of cycles over a discrete valuation ring. Rational coefficients are no restriction for the proof, which only specializes cycles with coefficients in $\mathbb{Z}_{(p)}$ and compares intersection numbers.

Intuition 2.10 (what specialization does). A cycle on the generic fiber is a combination of subvarieties defined over the fraction field. Taking their closures in $\mathcal{Y}$ and intersecting with the special fiber gives cycles on $\mathcal{Y}_{\mathrm{sp}}$. The theorem behind Fact 2.9(b) is that this is well defined on Chow groups and compatible with intersection products, so that numbers computed by intersecting cycles on the generic fiber, in characteristic 0, can be read off on the special fiber, in characteristic p.

Exercise 2.7. Using Fact 2.9(b), show that $\deg(\mathrm{sp}\, x \cdot \mathrm{sp}\, y) = \deg(x \cdot y)$ for $x \in \mathrm{CH}^i(\mathcal{Y}_{\mathrm{gen}})$ and $y \in \mathrm{CH}^{\dim \mathcal{Y}_{\mathrm{gen}} - i}(\mathcal{Y}_{\mathrm{gen}})$ and that $\mathrm{sp}(\alpha^* x) = \alpha_{\mathrm{sp}}^* \,\mathrm{sp}\, x$ for an endomorphism α of $\mathcal{Y}$ over O with special fiber α_{sp}.

Where this is used. Supersingularity and Fact 2.6 enter the definition of integral Tate classes (Chapter 4) and the comparison of homomorphisms with Dieudonné modules (Fact 4.10). Isogenies of degree prime to p carry the theorems between varieties with the same p-divisible group (Lemma 14.2). Intersection numbers and Fact 2.9 are the tools of the specialization step (Chapter 13).

Part II

Linear algebra of Frobenius

CHAPTER 3

Witt vectors, Frobenius and Dieudonné modules

Where we are. This chapter sets up the linear algebra in which the whole first half of the proof takes place: modules over the Witt vectors W with a Frobenius-semilinear operator F. It needs the p-adic numbers and finite fields. It introduces Witt vectors, semilinear maps and their matrices, Lang's lemma, Dieudonné modules and the facts that connect them with abelian varieties, slopes, the a-number, the module of a supersingular elliptic curve, and the binary words that name monomial Dieudonné modules. The convention $M(X) = H^1_{\mathrm{cris}}(X/W)$ (contravariant) and the convention for matrices of semilinear maps are fixed here.

3.1. Witt vectors and Dieudonné modules in two pages

The ring $W = W(\bar{\mathbb{F}}_p)$ is the complete discrete valuation ring with uniformizer p and residue field $\bar{\mathbb{F}}_p$ that is unramified over $\mathbb{Z}_p$. It has a unique automorphism σ lifting the Frobenius $x \mapsto x^p$ of $\bar{\mathbb{F}}_p$, and its fixed elements are $W^\sigma = \mathbb{Z}_p$. A map F between W-modules is σ-semilinear if it is additive and $F(\lambda x) = \sigma(\lambda)F(x)$. Linear algebra with such maps behaves like linear algebra over $\mathbb{Z}_p$ after a base change: by Lang's lemma, a σ-semilinear bijection of a free W-module M of finite rank has a basis of fixed vectors, so $M = M^F \otimes_{\mathbb{Z}_p} W$ with M^F a free $\mathbb{Z}_p$-module of the same rank (Lemma 3.5). This is the mechanism by which integral Tate classes, which are fixed vectors over $\mathbb{Z}_p$, are computed from lattices over W in Chapters 4 and 5.

A Dieudonné module is a free W-module M of finite rank with a σ-semilinear F and a σ^{-1}-semilinear V such that $FV = VF = p$. For an abelian variety X over $\bar{\mathbb{F}}_p$ of dimension g, the first crystalline cohomology $M(X) = H^1_{\mathrm{cris}}(X/W)$ is a Dieudonné module of rank $2g$, it determines the p-divisible group $X[p^\infty]$ up to isomorphism, and $VM(X)/pM(X)$ is the space of global 1-forms on X (Fact 3.10). The slopes of F measure how divisible by p its iterates are, and X is supersingular exactly when all slopes are $\frac{1}{2}$ (Fact 2.6).

The simplest example is the module of a supersingular elliptic curve E_0:

$$M(E_0) \cong (W^2, A\sigma), \qquad A = \begin{pmatrix} 0 & p \\ 1 & 0 \end{pmatrix}, \qquad Fe_0 = e_1, \quad Fe_1 = pe_0$$

(Proposition 3.16). Frobenius sends each basis vector to a basis vector times a power of p; the exponents read along the cycle $e_0 \to e_1 \to e_0$ form the binary word 01. Every module in this companion is built from such cycles. A *monomial* Dieudonné module is named by a multiset of binary words, one for each cycle of basis vectors, with $Fe_i = p^{w_i} e_{i+1}$ along a cycle with letters w_i (Definition 3.17). The model $\mathbb{M}$ of (1.1) is the monomial module $01 + 000111$ (Chapter 8). Its a-number, the dimension of $M/(FM + VM)$, which counts the cyclic occurrences of 10 in the words, is $1 + 1 = 2$.

3.2. Witt vectors

We recall the facts we need; for the existence, uniqueness and first properties of rings of Witt vectors see e.g. [Lie16, Section 1.4]. For $r \geq 1$ there is, up to isomorphism, exactly one complete discrete valuation ring with uniformizer p and residue field $\mathbb{F}_{p^r}$, the ring of Witt vectors $W(\mathbb{F}_{p^r})$, written

$$\mathbb{Z}_{p^r} = W(\mathbb{F}_{p^r}), \qquad \mathbb{Q}_{p^r} = \mathbb{Z}_{p^r}[1/p].$$

It is the ring of integers of the unramified extension $\mathbb{Q}_{p^r}$ of $\mathbb{Q}_p$ of degree r, and it is generated over $\mathbb{Z}_p$ by a primitive (p^r-1)-th root of unity. The Galois group of $\mathbb{Q}_{p^r}/\mathbb{Q}_p$ is cyclic of order r, generated by the *Frobenius* σ, the unique automorphism that induces $x \mapsto x^p$ on the residue field. For $r \mid r'$ there are compatible inclusions $\mathbb{Z}_{p^r} \subseteq \mathbb{Z}_{p^{r'}}$.

Let $W = W(\bar{\mathbb{F}}_p)$ be the p-adic completion of the union of all $\mathbb{Z}_{p^r}$, and $W[1/p]$ its fraction field. Then W is a complete discrete valuation ring with uniformizer p and residue field $\bar{\mathbb{F}}_p$, and σ extends to an automorphism of W by continuity. Every $y \in \bar{\mathbb{F}}_p$ has a unique *Teichmüller lift* $[y] \in W$ that is 0 or a root of unity of order prime to p reducing to y; it satisfies $[yz] = [y][z]$ and $\sigma[y] = [y^p]$, and every element x of W has a unique expansion

$$x = \sum_{i \geq 0} [x_i] p^i, \qquad x_i \in \bar{\mathbb{F}}_p.$$

Example 3.1 (a Teichmüller lift at $p = 5$). The Teichmüller lift $[2] \in \mathbb{Z}_5$ is the fourth root of unity congruent to 2 modulo 5, a square root of -1. It can be found by successive approximation. Writing $x = 2 + 5y_1$, $x^4 \equiv 16 + 160y_1 \equiv 16 + 10y_1 \bmod 25$, and $x^4 \equiv 1$ forces $y_1 \equiv 1$, so $x \equiv 7 \bmod 25$. Writing $x = 7 + 25y_2$, $x^4 \equiv 2401 + 34300y_2 \equiv 26 + 50y_2 \bmod 125$, and $x^4 \equiv 1$ forces $y_2 \equiv 2$. So $[2] \equiv 57 = 2 + 1 \cdot 5 + 2 \cdot 5^2 \bmod 125$, and indeed $57^2 = 3249 \equiv -1 \bmod 125$. Equivalently $[2] = \lim_n 2^{5^n}$, since y^{p^n} converges to the Teichmüller lift of $y \bmod p$ for any integer y.

Proposition 3.2 (fixed rings). *The fixed rings are $W^\sigma = \mathbb{Z}_p$ and, more generally, $W^{\sigma^r} = \mathbb{Z}_{p^r}$ for $r \geq 1$.*

Proof. Since σ is a ring automorphism that preserves p, $\sigma(\sum [x_i]p^i) = \sum [x_i^p]p^i$, and by uniqueness of the expansion x is fixed by σ^r if and only if $x_i^{p^r} = x_i$ for all i, that is, $x_i \in \mathbb{F}_{p^r}$ for all i. The elements $\sum [x_i]p^i$ with all $x_i \in \mathbb{F}_{p^r}$ are exactly the elements of $\mathbb{Z}_{p^r}$, because $\mathbb{Z}_{p^r}$ is complete, contains the Teichmüller lifts of $\mathbb{F}_{p^r}$ (the (p^r-1)-th roots of unity and 0), and has the same expansion with digits in $\mathbb{F}_{p^r}$. □

Example 3.3 ($\mathbb{Z}_{p^2}$ as a quadratic extension). Let $\xi \in \mathbb{Z}_p^\times$ be a unit whose reduction is not a square in $\mathbb{F}_p$. Then $x^2 - \xi$ is irreducible modulo p, so $\mathbb{Z}_p[\sqrt{\xi}]$ is a complete discrete valuation ring with uniformizer p and residue field $\mathbb{F}_{p^2}$, hence $\mathbb{Z}_p[\sqrt{\xi}] = \mathbb{Z}_{p^2}$. The Frobenius sends $\sqrt{\xi}$ to a root of $x^2 - \xi$, so to $\pm\sqrt{\xi}$, and modulo p it acts by $\sqrt{\xi} \mapsto \sqrt{\xi}^p = \xi^{(p-1)/2}\sqrt{\xi} \equiv -\sqrt{\xi}$, by Euler's criterion. So $\sigma(\sqrt{\xi}) = -\sqrt{\xi}$. For instance at $p = 5$ one can take $\xi = 2$, since the squares modulo 5 are 1 and 4.

3.3. Semilinear maps and their matrices

Let M, M' be W-modules and $r \in \mathbb{Z}$. A map $\Phi\colon M \to M'$ is *σ^r-semilinear* if it is additive and $\Phi(\lambda x) = \sigma^r(\lambda)\Phi(x)$ for $\lambda \in W$. On $M = W^n$ with its standard basis, write $\sigma(x)$ for the vector obtained by applying σ to the coordinates. Every σ-semilinear $\Phi\colon W^n \to W^n$ is of the form

$$\Phi(x) = \gamma\sigma(x)$$

for a unique matrix $\gamma \in \mathrm{Mat}_n(W)$, whose j-th column is Φ of the j-th basis vector. We write $\Phi = \gamma\sigma$, and this is the meaning of $F = A\sigma$ throughout the companion. Composition and change of basis follow from $\sigma(\gamma x) = \sigma(\gamma)\sigma(x)$:

$$(\gamma\sigma)(\gamma'\sigma) = \gamma\sigma(\gamma')\sigma^2, \qquad \gamma''^{-1}(\gamma\sigma)\gamma'' = \gamma''^{-1}\gamma\sigma(\gamma'')\sigma \quad (\gamma'' \in \mathrm{GL}_n(W)).$$

So in the basis given by the columns of γ'', the matrix of $\gamma\sigma$ is $\gamma''^{-1}\gamma\sigma(\gamma'')$, which is in general not conjugate to γ in the usual sense. For a matrix with entries in $\mathbb{Z}_p$, such as A, $\sigma(A) = A$.

Example 3.4 (the module of E_0). On $M = W^2$ with $F = A\sigma$, $A = \left(\begin{smallmatrix} 0 & p \\ 1 & 0 \end{smallmatrix}\right)$, we have $F^2 = A\sigma(A)\sigma^2 = A^2\sigma^2 = p\sigma^2$, since $A^2 = p$. The map F is injective with image $AW^2 = \{(p\lambda, \lambda')\}$, which contains pM, so $V = pF^{-1}$ is defined on M. From $F^{-1}(y) = \sigma^{-1}(A^{-1}y)$ we get $V(y) = \sigma^{-1}(pA^{-1}y) = \sigma^{-1}(Ay) = A\sigma^{-1}(y)$, because $pA^{-1} = A$. So $V = A\sigma^{-1}$: $Ve_0 = e_1$

and $Ve_1 = pe_0$. Modulo p, $F(\lambda e_0 + \lambda' e_1) = \sigma(\lambda)e_1 + p\sigma(\lambda')e_0 \equiv \sigma(\lambda)e_1$, so $\ker(F \bmod p)$ is the line spanned by e_1, which is VM/pM.

3.4. Lang's lemma

The following lemma is used every time a statement over W is brought down to $\mathbb{Z}_p$ or to $\mathbb{Z}_{p^r}$.

LEMMA 3.5 (Lang). *Let $r \geq 1$, let M be a free W-module of finite rank n, and let Φ be a σ^r-semilinear bijection of M. Then $M^\Phi = \{x \in M : \Phi x = x\}$ is a free $\mathbb{Z}_{p^r}$-module of rank n, and the map $M^\Phi \otimes_{\mathbb{Z}_{p^r}} W \to M$ is an isomorphism. In other words, M has a basis of Φ-fixed vectors.*

PROOF. *Rank* 1. Let $M = We$ and $\Phi(e) = \lambda e$, so $\Phi(xe) = \lambda\sigma^r(x)e$ with $\lambda \in W^\times$ because Φ is bijective. We look for a unit x with $\lambda\sigma^r(x) = x$. Modulo p this is $\bar\lambda \bar x^{p^r} = \bar x$, which has the nonzero solutions $\bar x$ with $\bar x^{p^r-1} = \bar\lambda^{-1}$ in the algebraically closed field $\bar{\mathbb{F}}_p$. Suppose $x^{(i)} \in W^\times$ satisfies $\lambda\sigma^r(x^{(i)}) = x^{(i)} + p^i y$. Put $x^{(i+1)} = x^{(i)} + p^i z$. Then $\lambda\sigma^r(x^{(i+1)}) - x^{(i+1)} = p^i(y + \lambda\sigma^r(z) - z)$, and this is divisible by p^{i+1} if $\bar\lambda \bar z^{p^r} - \bar z + \bar y = 0$, an equation of degree p^r in $\bar z$ which has a solution in $\bar{\mathbb{F}}_p$. The sequence $(x^{(i)})$ converges, and its limit x is a unit with $\lambda\sigma^r(x) = x$, so xe is a fixed basis vector. (Here and below, $\bar y$ denotes the reduction modulo p.)

General rank. The reduction $\bar\Phi$ of Φ modulo p is a σ^r-semilinear bijection of the $\bar{\mathbb{F}}_p$-vector space M/pM, and such a map has a basis of fixed vectors (see e.g. [Oor01]); this is Lang's theorem for GL_n over a finite field. Lift a fixed basis of M/pM to elements $x'_1, \dots, x'_n$ of M, a basis by Nakayama's lemma. The approximation of the rank-1 case, applied coordinatewise in this basis, in which $\bar\Phi$ is σ^r on coordinates and the equations $\bar z_i - \bar z_i^{p^r} = \bar y_i$ are solvable in $\bar{\mathbb{F}}_p$, turns each x'_j into a Φ-fixed vector congruent to x'_j modulo p. These fixed vectors $x_1, \dots, x_n$ form a basis of M by Nakayama's lemma. Finally, if $y = \sum \lambda_j x_j$ with $\lambda_j \in W$ is fixed, then $\sum \sigma^r(\lambda_j)x_j = \sum \lambda_j x_j$, so $\lambda_j \in W^{\sigma^r} = \mathbb{Z}_{p^r}$ (Proposition 3.2). Hence $M^\Phi = \bigoplus_j \mathbb{Z}_{p^r} x_j$, and $M^\Phi \otimes_{\mathbb{Z}_{p^r}} W \to M$ is an isomorphism. □

EXAMPLE 3.6 (the swap). Let $\Phi = \gamma\sigma$ on W^2 with $\gamma = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, so $\Phi(x, y) = (\sigma y, \sigma x)$. A vector (x, y) is fixed if and only if $y = \sigma(x)$ and $x = \sigma(y) = \sigma^2(x)$, that is $x \in \mathbb{Z}_{p^2}$ and $y = \sigma(x)$. So $(W^2)^\Phi = \{(x, \sigma x) : x \in \mathbb{Z}_{p^2}\}$, a free $\mathbb{Z}_p$-module of rank 2 with basis $(1, 1)$ and $(\sqrt{\xi}, -\sqrt{\xi})$, in the notation of Example 3.3. These two vectors form a basis of W^2, since $\det \begin{pmatrix} 1 & \sqrt{\xi} \\ 1 & -\sqrt{\xi} \end{pmatrix} = -2\sqrt{\xi}$ is a unit for odd p. The map Φ permutes the two standard basis vectors, and its fixed vectors over $\mathbb{Z}_p$ live over $\mathbb{Z}_{p^2}$: this is exactly the shape of the Weil lattice in Chapter 8, where $p^{-2}\bigwedge^4 F$ exchanges e_{T_+} and e_{T_-}.

Intuition 3.7 (descending from W). Lang's lemma says that a σ^r-semilinear bijection carries no information beyond the $\mathbb{Z}_{p^r}$-module of its fixed vectors. Fixed vectors over $\mathbb{Z}_p$ are what we are after (Tate classes, endomorphisms commuting with F), and the lemma lets us compute their W-span instead, which is often a lattice with an explicit form.

EXERCISE 3.1. Let $\lambda \in W^\times$. Find all solutions $x \in W$ of $\sigma(x) = \lambda x$ modulo p, and then, given one solution x_1 modulo p, write down the equation that a correction $x_1 + pz$ must satisfy modulo p^2. Do the same for $\lambda = -1$ and compare with Example 3.3.

3.5. Dieudonné modules

DEFINITION 3.8 (Dieudonné module). A *Dieudonné module* is a free W-module M of finite rank with a σ-semilinear map F and a σ^{-1}-semilinear map V such that $FV = VF = p$. Its *height* is its rank and its *dimension* is $\dim_{\bar{\mathbb{F}}_p} M/FM$. A morphism is a W-linear map commuting with F and V. The *dual* of M is $M^\vee = \mathrm{Hom}_W(M, W)$ with $F^\vee(y) = \sigma \circ y \circ V$ and $V^\vee(y) = \sigma^{-1} \circ y \circ F$ for $y \in M^\vee$.

Since F is injective on M (because $VF = p$ is), $V = pF^{-1}$ is determined by F, and a free W-module with an injective σ-semilinear F is a Dieudonné module exactly when $pM \subseteq FM$. One checks $F^\vee V^\vee = V^\vee F^\vee = p$ directly from $FV = VF = p$. The map V induces an isomorphism $M/FM \to VM/VFM = VM/pM$, so the dimension is also $\dim VM/pM$.

If $F = \gamma\sigma$ in a basis, the inclusions $pM \subseteq FM = \gamma M \subseteq M$ say that the elementary divisors of the matrix γ are 1 and p, and $\dim M/FM = n'$ says that p occurs n' times. So a Dieudonné module of height n and dimension n' has *Hodge polygon* $(1^{n-n'}, p^{n'})$: in suitable bases of the source and the target, F is $\operatorname{diag}(1, \dots, 1, p, \dots, p)\sigma$. For $M(E_0)$ this is $A = \left(\begin{smallmatrix} 0 & p \\ 1 & 0 \end{smallmatrix}\right)$ with elementary divisors $(1, p)$, and for the model $\mathbb{M}$ of (1.1) the elementary divisors are $(1^4, p^4)$, as for every abelian fourfold.

Example 3.9 (the three basic modules). The module (W, σ), of height 1 and dimension 0, is the Dieudonné module of the étale group $\mathbb{Q}_p/\mathbb{Z}_p$; the module $(W, p\sigma)$, of height 1 and dimension 1, is that of the multiplicative group $\boldsymbol{\mu}_{p^\infty}$; and they are dual to each other. An ordinary elliptic curve E over $\bar{\mathbb{F}}_p$ has $E[p^\infty] \cong \boldsymbol{\mu}_{p^\infty} \times \mathbb{Q}_p/\mathbb{Z}_p$ and $M(E) \cong (W, \sigma) \oplus (W, p\sigma)$, that is $F = \operatorname{diag}(1, p)\sigma$, with the same Hodge polygon as $M(E_0)$. The two modules are not isomorphic: $F^2 = \operatorname{diag}(1, p^2)\sigma^2$ on the first and $F^2 = p\sigma^2$ on the second, and in the first $\ker(F \bmod p)$ and FM/pM are the two different lines spanned by e_1 and e_0, while for E_0 they coincide. The slopes of Section 3.6 make the difference precise.

Fact 3.10 (Dieudonné theory). *(a) The contravariant Dieudonné functor $\mathscr{G} \mapsto M(\mathscr{G})$ is an anti-equivalence between p-divisible groups over $\bar{\mathbb{F}}_p$ and Dieudonné modules, under which height and dimension correspond.*

(b) For an abelian variety X of dimension g over $\bar{\mathbb{F}}_p$, $M(X) = H^1_{\mathrm{cris}}(X/W)$ is free of rank $2g$ and is the Dieudonné module of $X[p^\infty]$; the Dieudonné module of $X^\vee[p^\infty]$ is $M(X)^\vee$. A homomorphism $\alpha\colon X' \to X$ induces $\alpha^*\colon M(X) \to M(X')$, the Dieudonné module map of $\alpha[p^\infty]$.

(c) $H^\bullet_{\mathrm{cris}}(X/W) = \bigwedge^\bullet M(X)$, compatibly with Frobenius, which acts on $H^n_{\mathrm{cris}}(X/W)$ as $\bigwedge^n F$, and with pull-backs, which act as $\bigwedge^n \alpha^*$.

(d) $VM(X)/pM(X) = \ker(F \bmod p)$ is identified with $H^0(X, \Omega^1)$, compatibly with the action of endomorphisms.

For (a) see e.g. [Oda69, Corollary 3.16, Definition 3.17 and Proposition 3.18], where the anti-equivalence is stated for the categories of finite group schemes and of Dieudonné modules of finite length and extended to p-divisible groups, and for the dual module of an abelian variety in (b) [Oda69, Definition 3.6 and Proposition 3.23]. For (b) and (c) see e.g. [Lie16, Examples 1.8(1) and Section 3.4], and for the contravariant Dieudonné module over finite fields see e.g. [Hai05, (14.3.1)]. For (d) see [Oda69, Corollary 5.11]. Some references use the covariant Dieudonné module, which is the dual of the contravariant one; in this companion every statement is translated once into the contravariant convention $M(X) = H^1_{\mathrm{cris}}(X/W)$. With the convention of Definition 3.8, the identity $VM/pM = \ker(F \bmod p)$ in (d) holds for every Dieudonné module: if $Fx \in pM$, say $Fx = py = FVy$, then $x = Vy$, and conversely $FVy = py$.

If $f\colon X' \to X$ is an isogeny whose degree is prime to p, then $f[p^\infty]$ is an isomorphism (Exercise 2.6), and by Fact 3.10(a),(b) so is $f^*\colon M(X) \to M(X')$. So the Dieudonné module is an invariant of an abelian variety up to isogenies of degree prime to p, and so are the lattices T^n and S built from it in Chapter 4; this is what makes the transport lemma (Lemma 14.2) work.

Exercise 3.2. Let $M = W^n$ and $F = \gamma\sigma$ with $\gamma \in \mathrm{Mat}_n(W)$ such that $p\gamma^{-1}$ also has entries in W. Show that $V = \sigma^{-1} \circ (p\gamma^{-1})$, that is, $V(y) = \sigma^{-1}(p\gamma^{-1}y)$, that (M, F, V) is a Dieudonné module of dimension $v_p(\det\gamma)$, and check $VM/pM = \ker(F \bmod p)$ for $\gamma = A$ and for $\gamma = \operatorname{diag}(1, p)$.

3.6. Slopes and the Newton polygon

An *F-isocrystal* is a finite-dimensional $W[1/p]$-vector space I with a σ-semilinear bijection F; a Dieudonné module M gives the isocrystal $M \otimes \mathbb{Q} = M[1/p]$. For coprime integers $l \geq 0$, $n \geq 1$ let $I_{l/n}$ be the isocrystal with basis $e_1, \dots, e_n$ and $Fe_j = e_{j+1}$ for $j < n$, $Fe_n = p^l e_1$, so that $F^n = p^l \sigma^n$ in this basis.

FACT 3.11 (Dieudonné–Manin). *(a) Every F-isocrystal over $W[1/p]$ is isomorphic to a direct sum of the $I_{l/n}$, and the multiset of* slopes *l/n, each counted n times, is determined by the isocrystal. The slopes of a Dieudonné module lie in $[0,1]$.*

(b) Let Φ be an injective σ^r-semilinear endomorphism of a free W-module of finite rank. If all slopes of Φ are positive, the reduction of Φ modulo p is nilpotent.

For (a) see e.g. [Lie16, Theorem 3.4], which classifies F-crystals up to isogeny; that the slopes of a Dieudonné module lie in $[0,1]$ follows from [Lie16, Proposition 3.7], by which the Newton polygon lies on or above the Hodge polygon with the same end points, since the Hodge polygon of a Dieudonné module has slopes 0 and 1 only. For (b) see e.g. [Jon98, Section 4.5], which treats σ-semilinear maps; for $r > 1$ apply it to the σ-crystal induced from (M, Φ), whose slopes are those of Φ divided by r. For a σ^r-semilinear map the slopes are defined in the same way with σ^r in place of σ. The *Newton polygon* of M is the convex polygon whose segments have the slopes of M as slopes, with horizontal length the multiplicities. A Dieudonné module is *supersingular* if all its slopes are $\frac{1}{2}$; by Fact 2.6(b), X is supersingular if and only if $M(X)$ is. In particular, for supersingular X all slopes of F on $M(X)$ are positive, and F is nilpotent modulo p.

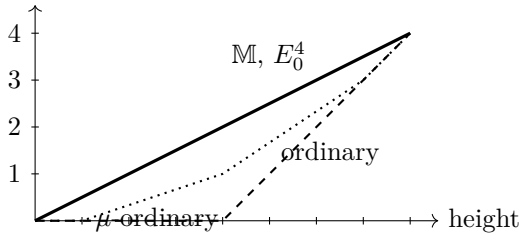


FIGURE 3.1. Newton polygons of three Dieudonné modules of height 8 and dimension 4: supersingular (all slopes $\frac{1}{2}$), ordinary (slopes 0 and 1, each four times), and the μ-ordinary polygon of Mumford's families (slopes $0, \frac{1}{3}, \frac{2}{3}, 1$ with multiplicities $1, 3, 3, 1$, Chapter 7). All three end at $(8, 4)$, because the sum of the slopes is the dimension.

EXAMPLE 3.12 (0011 and $01+01$ are isogenous). On $M = M_{0011}$ (Definition 3.17) we have $Fe_0 = e_1$, $Fe_1 = e_2$, $Fe_2 = pe_3$, $Fe_3 = pe_0$. Put $e'_0 = e_0$, $e'_1 = Fe_0 = e_1$, $e'_2 = p^{-1}e_2$ and $e'_3 = e_3$, a basis of $M[1/p]$. Then

$$Fe'_0 = e'_1, \qquad Fe'_1 = e_2 = pe'_2, \qquad Fe'_2 = p^{-1} \cdot pe_3 = e'_3, \qquad Fe'_3 = pe_0 = pe'_0,$$

so the W-span M' of $e'_0, \dots, e'_3$ is the module of the word 0101, which contains M with index p. So M_{0011} and M_{0101} are isomorphic after inverting p, and both have slopes $\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}$, those of M_{01+01}. But they are not isomorphic as Dieudonné modules: their a-numbers are 1 and 2 (Example 3.19). The module of 0101 is isomorphic to that of $01+01$, by Lang's lemma (Chapter 15). This is the Dieudonné-module form of the fact that a supersingular abelian surface is isogenous to E_0^2 but need not be isomorphic to it.

The slopes of M, counted with multiplicity, add up to $v_p(\det \gamma)$ for any matrix γ with $F = \gamma\sigma$, which is the dimension of M; this is a property of the isocrystal, since a change of lattice multiplies $\det \gamma$ by $\det(\gamma')^{-1}\sigma(\det \gamma')$, which has valuation 0, and on $I_{l/n}$ the determinant has valuation l. So the Newton polygon starts at $(0,0)$ and ends at (n, n'), where the Hodge polygon of Section 3.5, with $n - n'$ slopes 0 and n' slopes 1, ends as well.

Example 3.13 (slopes in rank 2). Let Φ be a σ^r-semilinear map of a free W-module of rank 2 with elementary divisors $(1, p)$, the situation of $M(E)$ for an elliptic curve E and of the rank-two lemma (Lemma 7.2). By Fact 3.11 its isocrystal is either a sum of two isocrystals of rank 1, with integer slopes in $[0, 1]$ adding up to 1, that is slopes 0 and 1, or a single simple isocrystal of rank 2, whose two equal slopes add up to 1, that is slopes $\frac{1}{2}, \frac{1}{2}$. So the slopes are u and $1-u$ with $u \in \{0, \frac{1}{2}\}$: ordinary or supersingular, nothing in between. In the first case Φ is not nilpotent modulo p; in the second it is, and the rank-two lemma shows that the module is then $(W^2, A\sigma^r)$.

Intuition 3.14 (slopes as orders of divisibility). A slope u means that F^n behaves like $p^{un}\sigma^n$ on the corresponding part, so the n-th iterate of F divides by p exactly un times. For a supersingular module every vector is divided by p once in every two applications of F, up to bounded error; for E_0 this holds on the nose, $F^2 = p\sigma^2$.

3.7. The a-number

Definition 3.15 (a-number). The *a-number* of a Dieudonné module is $a(M) = \dim_{\bar{\mathbb{F}}_p} M/(FM + VM)$, and $a(X) = a(M(X))$ for an abelian variety X.

A superspecial abelian variety of dimension g is a product of supersingular elliptic curves, so by Proposition 3.16 below its Dieudonné module is $M(E_0)^g$, of a-number g (Section 3.9). So a supersingular abelian variety of a-number less than g is not superspecial. For a supersingular elliptic curve, $FM = VM$ (as the proof of Proposition 3.16 shows), so $a = \dim M/FM = 1$.

3.8. The module of a supersingular elliptic curve

Proposition 3.16. *Let E_0 be a supersingular elliptic curve over $\bar{\mathbb{F}}_p$. There is a basis e_0, e_1 of $M(E_0)$ in which*

$$M(E_0) \cong (W^2, A\sigma), \qquad A = \begin{pmatrix} 0 & p \\ 1 & 0 \end{pmatrix}, \qquad Fe_0 = e_1, \quad Fe_1 = pe_0. \tag{3.1}$$

Proof. By Fact 3.10 $M = M(E_0)$ is a Dieudonné module of height 2 and dimension 1, and by Fact 2.6 its slopes are $\frac{1}{2}, \frac{1}{2}$, so $\bar{F} = F \bmod p$ is nilpotent (Fact 3.11). The image FM/pM and the kernel VM/pM of $\bar{F}$ are lines in the plane M/pM. If they were different, $\bar{F}$ would map its image injectively into itself and would not be nilpotent. So $FM = VM$, and $F^2M = FVM = pM$. Hence $\Pi = p^{-1}F^2$ is a σ^2-semilinear bijection of M, and by Lemma 3.5 $M = M^\Pi \otimes_{\mathbb{Z}_{p^2}} W$ with M^Π a free $\mathbb{Z}_{p^2}$-module of rank 2. Since F commutes with Π, it preserves M^Π, and so does $V = pF^{-1} = F\Pi^{-1}$; in particular $FM^\Pi = VM^\Pi$. Choose $e_0 \in M^\Pi \setminus FM^\Pi$, which exists because $FM^\Pi \otimes W = FM \neq M$, and put $e_1 = Fe_0$. Then $Fe_1 = F^2e_0 = p\Pi e_0 = pe_0$. If e_1 were in pM^Π, say $e_1 = py = FVy$, then $e_0 = Vy \in VM^\Pi = FM^\Pi$, which is not the case. So $e_1 \in FM^\Pi \setminus pM^\Pi$ spans the line FM^Π/pM^Π, and $e_0 \notin FM^\Pi$ spans a complement, so e_0, e_1 is a basis of M^Π/pM^Π and, by Nakayama's lemma, of M^Π and of M. In this basis $F(\lambda e_0 + \lambda' e_1) = \sigma(\lambda)e_1 + p\sigma(\lambda')e_0$, which is $F = A\sigma$. □

The same argument, for a σ^r-semilinear map of rank 2 with positive slopes and image of colength 1, is the rank-two lemma of Chapter 7 (Lemma 7.2), which pins down the Dieudonné module at the supersingular points of Mumford's families. In particular all supersingular elliptic curves over $\bar{\mathbb{F}}_p$ have isomorphic p-divisible groups, which we write $E_0[p^\infty]$.

3.9. Monomial modules and words

The basis of Proposition 3.16 is permuted by F up to powers of p. Modules with such a basis are the subject of the rest of Part II.

Definition 3.17 (words and monomial modules). A *word* is a finite sequence $w = w_0 w_1 \cdots w_{n-1}$ of letters $w_i \in \{0,1\}$ with as many 0s as 1s, considered up to cyclic rotation. Its module M_w has basis $e_0, \dots, e_{n-1}$, indices modulo n, and

$$Fe_i = p^{w_i} e_{i+1}, \qquad Ve_{i+1} = p^{1-w_i} e_i,$$

extended σ-semilinearly, respectively σ^{-1}-semilinearly. For a multiset of words $w, w', \dots$ the module $M_{w+w'+\dots} = M_w \oplus M_{w'} \oplus \cdots$ is written with plus signs. A Dieudonné module isomorphic to some $M_{w+w'+\dots}$ is *monomial*.

So M_{01} is the module of E_0 in (3.1), and $M_{01+01+\dots+01}$, with g copies, is the module of E_0^g. A rotation of a word renumbers the basis and gives an isomorphic module. The following properties are read off directly.

(i) *Dieudonné module.* $FV = VF = p$ on basis vectors, and M_w has height n and dimension equal to the number of letters 1, which is $n/2$.

(ii) *Slopes.* $F^n e_i = p^{\sum_j w_j} e_i = p^{n/2} e_i$, so $F^n = p^{n/2}\sigma^n$ in the basis (e_i) and all slopes are $\frac{1}{2}$ (Exercise 3.5). Monomial modules in this sense are supersingular.

(iii) *Duality.* In the dual basis $(e_i^\vee)$ of $M_w^\vee$, $F^\vee(e_i^\vee) = \sigma \circ e_i^\vee \circ V$ takes the value $\sigma(e_i^\vee(Ve_{j+1})) = \sigma(e_i^\vee(p^{1-w_j} e_j))$ on e_{j+1}, which is p^{1-w_i} for $j = i$ and 0 otherwise, so $F^\vee e_i^\vee = p^{1-w_i} e_{i+1}^\vee$. The dual of M_w is the module of the *complementary word*, with 0 and 1 exchanged.

(iv) *a-number.* Modulo p, FM_w is spanned by the e_{i+1} with $w_i = 0$ and VM_w by the e_i with $w_i = 1$. So $e_j \notin FM_w + VM_w$ exactly when $w_{j-1} = 1$ and $w_j = 0$, and $a(M_w)$ is the number of cyclic occurrences of 10 in w, summed over the words of a multiset.

Example 3.18 (self-dual words). The complement of 01 is 10, a rotation of 01, so $M(E_0) \cong M(E_0)^\vee$, in accordance with $E_0 \cong E_0^\vee$. The complement of 000111 is 111000, again a rotation, so the model $\mathbb{M} \cong M_{01+000111}$ is self-dual; so are 0011 and every word of the form $0^n 1^n$. The word 00101011 is not: its complement is a rotation of 00110101 (Exercise 3.4). A polarization of degree prime to p is an isogeny $X \to X^\vee$ that induces an isomorphism of p-divisible groups, so an abelian variety with such a polarization has a self-dual Dieudonné module; this is why self-duality appears in Chapter 15.

Example 3.19 (a-numbers). The word 0011 has one cyclic occurrence of 10 (the last letter 1 followed by the first letter 0), so $a(M_{0011}) = 1$; a supersingular abelian surface with this module is not superspecial. The multiset $01 + 01$ has $a = 1 + 1 = 2$, the module of $E_0 \times E_0$. The word 000111 has $a = 1$, and $01 + 000111$, which is the model $\mathbb{M}$ (Chapter 8), has $a = 2$. A superspecial fourfold has the module $01 + 01 + 01 + 01$ with $a = 4$.

Exercise 3.3. Show that the a-number of a word is the number of maximal blocks of consecutive 1s, counted cyclically. Compute the a-numbers of 00101011, 00100111, 00011011 and 01010101.

Exercise 3.4. Find the complementary words of 00101011 and of 00100111, and write each as the rotation that begins with the longest block of 0s. Is either word isomorphic to its dual by a rotation?

Exercise 3.5. Let w be a binary word of length n with l letters 1, not necessarily balanced, and M_w as in Definition 3.17. Show that $F^n = p^l \sigma^n$ in the basis (e_i) and that all slopes of M_w equal l/n.

Exercise 3.6. Let $\Phi = \gamma\sigma$ on W^3, with γ the cyclic permutation matrix sending $e_1 \mapsto e_2 \mapsto e_3 \mapsto e_1$. Determine $(W^3)^\Phi$ and give a basis of it over $\mathbb{Z}_p$. For which p is your basis also a basis of W^3?

Exercise 3.7. Show that the Dieudonné modules (W, σ) and $(W, p\sigma)$ of Example 3.9 are dual to each other in the sense of Definition 3.8, and that the module $(W^2, \mathrm{diag}(1,p)\sigma)$ of an ordinary elliptic curve is self-dual, with a-number 0.

Where this is used. Lang's lemma is the engine of the descent lemma (Lemma 5.3), of the rank-two lemma (Lemma 7.2) and of the comparison of cycle decompositions in Chapter 15. Fact 3.10 identifies crystalline cohomology with exterior powers of $M(X)$ (Chapter 4) and the type of an action on $H^0(X, \Omega^1)$ with eigenvalue counts on VM/pM (Lemma 8.4). The words name the model $\mathbb{M} = M_{01+000111}$ and the other monomial modules of Chapter 15.

CHAPTER 4

Crystalline cohomology and integral Tate classes

Where we are. This chapter defines the three lattices of the question, $T^n(X)$, $\mathrm{Alg}^i(X)$ and $S(X)$, for a supersingular abelian variety X over $\bar{\mathbb{F}}_p$, and proves the two facts that turn the question into one about a finite group: $S(X) \subseteq \mathrm{Alg}^2(X)$, and $S(X)$ has finite index in $T^4(X)$. It also introduces the intersection pairing on $T^4(X)$ and the discriminant lemma that the specialization step uses. It needs the chapters on abelian varieties and on Dieudonné modules. The crystalline cycle class (Fact 4.6) and the comparison of homomorphisms with Dieudonné modules (Fact 4.10) are cited, not proved.

4.1. Integral Tate classes in two pages

Let X be a supersingular abelian variety of dimension g over $\bar{\mathbb{F}}_p$ and $M = M(X)$ its Dieudonné module. Crystalline cohomology is the exterior algebra of M, and Frobenius acts on $H^n_{\mathrm{cris}}(X/W) = \bigwedge^n M$ as $\bigwedge^n F$. For even n, the integral crystalline Tate classes are the vectors on which F acts as $p^{n/2}$,

$$T^n(X) = \{x \in \textstyle\bigwedge^n M : \ Fx = p^{n/2}x\},$$

equivalently the fixed vectors of the σ-semilinear map $\varphi = p^{-n/2}\bigwedge^n F$ that lie in $\bigwedge^n M$. Since X is supersingular, all slopes of φ are 0, so by Lang's lemma its fixed vectors span $\bigwedge^n M \otimes \mathbb{Q}$ over $W[1/p]$, and $T^n(X)$ is a free $\mathbb{Z}_p$-module of rank $\binom{2g}{n}$ (Proposition 4.4).

Classes of algebraic cycles of codimension $i \le 2$ lie in $T^{2i}(X)$ (Fact 4.6); they span $\mathrm{Alg}^i(X)$. Divisor classes give all of T^2: $\mathrm{NS}(X) \otimes \mathbb{Z}_p \cong T^2(X)$ (Fact 4.10), so codimension 1 is settled. The products of two classes in T^2 span $S(X) \subseteq \mathrm{Alg}^2(X)$. Rationally they span everything, because the even part of an exterior algebra is generated in degree 2 (Proposition 4.12). So

$$S(X) \subseteq \mathrm{Alg}^2(X) \subseteq T^4(X) \qquad \text{with} \qquad [T^4(X) : S(X)] < \infty,$$

and the question is how large the finite group T^4/S is and whether algebraic cycles fill it.

The cup product pairs $T^4(X)$ with itself into $T^8(X) = \mathbb{Z}_p[\mathrm{pt}]$ for a fourfold, and for algebraic classes the pairing is the intersection number. A sublattice of full rank of a lattice with a $\mathbb{Z}_p$-valued form, if its discriminant is a unit, is the whole lattice (Lemma 4.13). This is the mechanism by which intersection numbers computed in characteristic 0 pin down a lattice of classes in characteristic p in Chapter 13.

Example 4.1 (T^2 of E_0). In the basis of (3.1), $F(e_0 \wedge e_1) = Fe_0 \wedge Fe_1 = e_1 \wedge pe_0 = -pe_0 \wedge e_1$. A class $x = \lambda e_0 \wedge e_1$, $\lambda \in W$, is Tate if $Fx = \sigma(\lambda)(-p)e_0 \wedge e_1$ equals px, that is, if $\sigma(\lambda) = -\lambda$. With ξ a non-square unit as in Example 3.3, $\sigma(\sqrt{\xi}) = -\sqrt{\xi}$, so $\lambda/\sqrt{\xi}$ is fixed by σ and lies in $\mathbb{Z}_p$ (Proposition 3.2). Hence

$$T^2(E_0) = \mathbb{Z}_p \cdot \sqrt{\xi} e_0 \wedge e_1,$$

of rank $1 = \binom{2}{2}$, matching $\mathrm{NS}(E_0) = \mathbb{Z} \cdot [\mathrm{pt}]$.

4.2. Crystalline cohomology of abelian varieties

By Fact 3.10(c), $H^n_{\mathrm{cris}}(X/W) = \bigwedge^n M(X)$ for an abelian variety X over $\bar{\mathbb{F}}_p$, with Frobenius $\bigwedge^n F$ and with the pull-back by a homomorphism α acting as $\bigwedge^n \alpha^*$. In the wedge basis $e_J = e_{j_1} \wedge \cdots \wedge e_{j_n}$, for $J = \{j_1 < \cdots < j_n\}$ a subset of an ordered basis (e_j) of $M(X)$, this makes everything explicit: $\bigwedge^n F(e_J) = Fe_{j_1} \wedge \cdots \wedge Fe_{j_n}$, σ-semilinearly extended. Throughout,

wedge bases are taken in a fixed increasing order and statements about them hold up to sign; no sign is ever needed beyond that.

For a product, $(X \times X')[p^\infty] = X[p^\infty] \times X'[p^\infty]$, so $M(X \times X') = M(X) \oplus M(X')$, and the exterior algebra of a direct sum gives the *Künneth decomposition*

$$H^n_{\mathrm{cris}}(X \times X'/W) = \bigoplus_{i+j=n} \textstyle\bigwedge^i M(X) \otimes \bigwedge^j M(X'),$$

which is preserved by Frobenius. We call the summand with (i,j) the Künneth (i,j)-component. Since F preserves the decomposition, the projection to a component of a class with $Fx = p^{n/2}x$ has the same property.

Example 4.2 (degree 2 on a product). For supersingular X and X', the Künneth decomposition of $T^2(X \times X')$ is

$$T^2(X \times X') = T^2(X) \;\oplus\; T^{1,1} \;\oplus\; T^2(X'), \qquad T^{1,1} = T^2(X \times X') \cap (M(X) \otimes M(X')).$$

The middle part is the place of the classes of graphs of homomorphisms. Indeed $M(X) \otimes M(X')$ is identified with $\mathrm{Hom}_W(M(X'^\vee), M(X))$ through $M(X') = M(X'^\vee)^\vee$, and under this identification $p^{-1}(F \otimes F)$ becomes $\alpha \mapsto F\alpha F^{-1}$, and the classes fixed by $p^{-1}F$ correspond to the maps commuting with F, which by Fact 4.10 are the pull-backs by elements of $\mathrm{Hom}(X, X'^\vee) \otimes \mathbb{Z}_p$. The ranks agree: $T^{1,1}$ has rank $(2\dim X)(2\dim X')$, the rank of $\mathrm{Hom}(X, X'^\vee)$. For $X = X' = E_0$ this is 4, the rank of $\mathrm{End}(E_0)$, and it accounts for the four classes of graphs in $\mathrm{NS}(E_0 \times E_0)$ beyond the two fibers (Example 2.3); in Example 4.5 these are the two summands of rank 2. On $X \times X$ for a fourfold X, products of two classes in $T^{1,1}$ are the divisor products in the Künneth component $\bigwedge^2 M \otimes \bigwedge^2 M$ other than the products $T^2(X) \otimes T^2(X)$; both kinds enter the endomorphism proposition (Proposition 9.4(iv)).

4.3. Tate classes

Definition 4.3 (integral crystalline Tate classes). Let X be a supersingular abelian variety over $\bar{\mathbb{F}}_p$ and n even. The *integral crystalline Tate classes* of degree n are

$$T^n(X) = \{x \in H^n_{\mathrm{cris}}(X/W) : \; Fx = p^{n/2}x\}.$$

Write $\varphi = p^{-n/2}\bigwedge^n F$, a σ-semilinear bijection of $\bigwedge^n M(X) \otimes \mathbb{Q}$; then $T^n(X)$ is the set of φ-fixed vectors in $\bigwedge^n M(X)$.

The definition is made only for supersingular X. For other abelian varieties the same formula defines a $\mathbb{Z}_p$-module that can be larger than the span of algebraic classes even rationally, as the surface $E \times E'$ of Section 1.2 shows.

Proposition 4.4 (rank). *Let X be supersingular of dimension g and n even. Then $T^n(X)$ is a free $\mathbb{Z}_p$-module of rank $\binom{2g}{n}$, the map $T^n(X) \otimes_{\mathbb{Z}_p} W \to \bigwedge^n M(X)$ is injective, and its image has finite index.*

Proof. Write $M = M(X)$. By Fact 2.6 all slopes of M are $\frac{1}{2}$, so by Fact 3.11 $M \otimes \mathbb{Q}$ has a basis $e'_1, \dots, e'_{2g}$ in which F is the direct sum of g copies of $A\sigma$. Let M' be the W-span of this basis, a lattice in $M \otimes \mathbb{Q}$ on which $F^2 = p\sigma^2$. Then $\bigwedge^n F^2 = p^n\sigma^2$ on $\bigwedge^n M'$, so $\varphi^2 = \sigma^2$ maps $\bigwedge^n M'$ onto itself. The lattice $L = \bigwedge^n M' \cap \varphi(\bigwedge^n M')$ therefore satisfies $\varphi(L) = \varphi(\bigwedge^n M') \cap \bigwedge^n M' = L$, and φ is a σ-semilinear bijection of L. By Lemma 3.5, $L = L^\varphi \otimes_{\mathbb{Z}_p} W$ with L^φ free of rank $\binom{2g}{n}$. Every φ-fixed vector x of $\bigwedge^n M \otimes \mathbb{Q}$ has $p^l x \in L$ for large l, so the φ-fixed vectors form the $\mathbb{Q}_p$-vector space $L^\varphi \otimes \mathbb{Q}$. The lattices $\bigwedge^n M$ and L are commensurable: $p^j L \subseteq \bigwedge^n M \subseteq p^{-j} L$ for some $j \geq 0$. Taking φ-fixed vectors gives $p^j L^\varphi \subseteq T^n(X) \subseteq p^{-j} L^\varphi$, so $T^n(X)$ is free of rank $\binom{2g}{n}$. Tensoring the second inclusion with the flat $\mathbb{Z}_p$-module W shows that $T^n(X) \otimes W \to p^{-j} L$ is injective, and its image contains $p^j L$, which has finite index in $\bigwedge^n M$. □

EXAMPLE 4.5 (T^2 of $E_0 \times E_0$). Let $M = M(E_0) \oplus M(E_0)$ with basis e_0, e_1 of the first summand and e_0', e_1' of the second, as in (3.1), and $\varphi = p^{-1}\bigwedge^2 F$. The six wedge products fall into four φ-orbits:

$$\varphi(e_0 \wedge e_1) = -e_0 \wedge e_1, \qquad \varphi(e_0' \wedge e_1') = -e_0' \wedge e_1',$$
$$\varphi(e_0 \wedge e_0') = p^{-1} e_1 \wedge e_1', \quad \varphi(e_1 \wedge e_1') = p e_0 \wedge e_0', \qquad \varphi(e_0 \wedge e_1') = e_1 \wedge e_0', \quad \varphi(e_1 \wedge e_0') = e_0 \wedge e_1'.$$

As in Example 4.1, the first two orbits give the Tate classes $\sqrt{\xi} e_0 \wedge e_1$ and $\sqrt{\xi} e_0' \wedge e_1'$. For $x = \lambda p e_0 \wedge e_0' + \lambda' e_1 \wedge e_1'$ the equation $\varphi(x) = x$ reads $\lambda' = \sigma(\lambda)$ and $\lambda = \sigma(\lambda')$, so $\lambda \in \mathbb{Z}_{p^2}$ and $\lambda' = \sigma(\lambda)$; for $x = \lambda e_0 \wedge e_1' + \lambda' e_1 \wedge e_0'$ it reads the same. Hence $T^2(E_0 \times E_0)$ is

$$\mathbb{Z}_p \sqrt{\xi} e_0 \wedge e_1 \;\oplus\; \mathbb{Z}_p \sqrt{\xi} e_0' \wedge e_1' \;\oplus\; \{\lambda p e_0 \wedge e_0' + \sigma(\lambda) e_1 \wedge e_1'\} \;\oplus\; \{\lambda e_0 \wedge e_1' + \sigma(\lambda) e_1 \wedge e_0'\},$$

with λ running over $\mathbb{Z}_{p^2}$ in the last two summands, of rank $1 + 1 + 2 + 2 = 6$, which is the rank of $\mathrm{NS}(E_0 \times E_0)$ (Example 2.3). The W-span $T^2 \otimes W$ is spanned by $e_0 \wedge e_1$, $e_0' \wedge e_1'$, $p e_0 \wedge e_0'$, $e_1 \wedge e_1'$, $e_0 \wedge e_1'$, $e_1 \wedge e_0'$, and has index p in $\bigwedge^2 M$. This exponent 1 at $e_0 \wedge e_0'$ is an instance of the orbit rule of Chapter 5.

EXERCISE 4.1. Show that the lattice $T^2(E_0)$ of Example 4.1 does not depend on the choice of the non-square unit ξ, and that its generator has trace a unit of $\mathbb{Z}_p$ under the trace $\int$ of Fact 4.6, using only $\int F z = p\sigma(\int z)$. Conclude that $T^2(E_0)$ is spanned by the class of a point.

EXERCISE 4.2. Let X be a supersingular abelian fourfold. Give the ranks of T^2, T^4, T^6, T^8, and show that $\int$ maps $T^8(X)$ isomorphically onto $\mathbb{Z}_p$.

4.4. The crystalline cycle class

For a smooth projective variety Y over $\bar{\mathbb{F}}_p$, crystalline cohomology $H^\bullet_{\mathrm{cris}}(Y/W)$ is a graded W-algebra with a Frobenius, and the following properties connect it with cycles.

FACT 4.6 (the crystalline cycle class). *For a smooth projective variety Y over $\bar{\mathbb{F}}_p$ there is a cycle class map*

$$\mathrm{cl}\colon \mathrm{CH}^i(Y) \to H^{2i}_{\mathrm{cris}}(Y/W) \otimes \mathbb{Q}$$

which is compatible with products, pull-backs, and push-forwards along morphisms of smooth projective varieties, and a trace $\int\colon H^{2\dim Y}_{\mathrm{cris}}(Y/W) \to W$, an isomorphism when Y is connected, with $\int F z = p^{\dim Y}\sigma(\int z)$ and $\int \mathrm{cl}(y) = \deg y$ for 0-cycles y. Classes of codimension at most 2 are integral and Tate: $\mathrm{cl}(y) = c_1(\mathcal{O}(y))$ for a divisor y and $\mathrm{cl}(y) = -c_2(\mathcal{O}_y)$ for a cycle y of codimension 2, with integral crystalline Chern classes, so they lie in $H^{2i}_{\mathrm{cris}}(Y/W)$ and satisfy $F\,\mathrm{cl}(y) = p^i\,\mathrm{cl}(y)$.

For the cycle class and its compatibility with products and pull-backs see [GM87, I, Theorem 4.3.1], for push-forwards [GM87, II, Theorem 1.1.3], and for $F\,\mathrm{cl}(y) = p^i\,\mathrm{cl}(y)$ [GM87, Lemma B.2.2(a) and Remark B.2.3] and [Pet03, Proposition 7.13]. For the trace, see e.g. [Lie16, Section 1.5(2) and Example 3.2], the latter applied to the pairing of 1 with z, and at finite level see e.g. [GM87, II, proof of Lemma 1.1.9]. The integrality in codimension 2, with $\mathrm{cl}(y) = -c_2(\mathcal{O}_y)$ for an integral subscheme y of codimension 2 and integral crystalline Chern classes, is in [GM87, I, Theorem 4.3.1]. See [Pet03, Sections 5–7] for the corresponding statements in rigid cohomology and their comparison with crystalline Chern classes.

Intuition 4.7 (why codimension 2 is integral). Rationally, a cycle class is a polynomial in Chern classes, with denominators. In codimension 1 and 2 no denominator occurs, because c_1 and c_2 of the structure sheaf of a cycle give its class up to sign. In higher codimension the denominators $(i-1)!$ of the Riemann–Roch theorem without denominators appear, which are units at p as long as $i \le p$; in this companion only codimension ≤ 2 and the degree of 0-cycles are needed.

For an abelian fourfold X, the trace identifies $H^8_{\mathrm{cris}}(X/W) = \bigwedge^8 M(X)$ with W, and by Exercise 4.2 it identifies $T^8(X)$ with $\mathbb{Z}_p$, the class of a point corresponding to 1. So the cup product defines a symmetric $\mathbb{Z}_p$-bilinear form

$$T^4(X) \times T^4(X) \to \mathbb{Z}_p, \qquad (x, y) \mapsto \int x \wedge y,$$

and for cycles z, z' of codimension 2, $\int \mathrm{cl}(z) \wedge \mathrm{cl}(z') = \deg(z \cdot z')$ by Fact 4.6.

4.5. Algebraic classes and divisor products

Definition 4.8 (algebraic classes). For a supersingular abelian variety X over $\bar{\mathbb{F}}_p$ and $i \le 2$, $\mathrm{Alg}^i(X) \subseteq T^{2i}(X)$ is the $\mathbb{Z}_p$-span of the classes $\mathrm{cl}(z)$ of cycles $z \in \mathrm{CH}^i(X)$. The *integral crystalline Tate conjecture in codimension i* for X is the statement $\mathrm{Alg}^i(X) = T^{2i}(X)$.

Definition 4.9 (divisor products). For a supersingular abelian variety X over $\bar{\mathbb{F}}_p$, $S(X) \subseteq T^4(X)$ is the $\mathbb{Z}_p$-span of the products $x \wedge y$ with $x, y \in T^2(X)$. More generally $S^{2i}(X) \subseteq T^{2i}(X)$ is the $\mathbb{Z}_p$-span of the products of i classes in $T^2(X)$, so that $S = S^4$.

Fact 4.10 (homomorphisms and Dieudonné modules). *(a) For abelian varieties X, X' over $\bar{\mathbb{F}}_p$, the map $\mathrm{Hom}(X', X) \otimes \mathbb{Z}_p \to \mathrm{Hom}(M(X), M(X'))^F$, $\alpha \mapsto \alpha^*$, to the W-linear maps commuting with F, is injective with torsion-free cokernel.*

(b) If X and X' are supersingular, both sides have rank $4 \dim X \dim X'$, and the map is an isomorphism. In particular $\mathrm{End}(X) \otimes \mathbb{Z}_p \cong \mathrm{End}(M(X), F)$, where $\alpha \mapsto \alpha^*$ reverses the order of composition.

(c) Consequently, for every supersingular abelian variety X over $\bar{\mathbb{F}}_p$, the cycle class induces an isomorphism $\mathrm{NS}(X) \otimes \mathbb{Z}_p \cong T^2(X)$.

For (a) see e.g. [Jon98, proof of Theorem 2.6], where it is stated over fields finitely generated over $\mathbb{F}_p$; over $\bar{\mathbb{F}}_p$ it follows by passing to a finite field over which the abelian varieties and a given homomorphism of Dieudonné modules are defined. For (b), both sides have rank $4 \dim X \dim X'$, the left-hand side by Fact 2.6(a) and Exercise 2.3, the right-hand side by the argument below; a map of free $\mathbb{Z}_p$-modules of the same rank that is injective with torsion-free cokernel is an isomorphism. Statement (c) is deduced from (b) applied to $\mathrm{Hom}(X, X^\vee)$, through the embedding of $\mathrm{NS}(X)$ into $\mathrm{Hom}(X, X^\vee)$ as the symmetric homomorphisms (Section 2.3) and the description of T^2 of a product in Example 4.2; the companion does not write out this deduction. Over $\bar{\mathbb{F}}_p$ statement (c) is false without supersingularity: for the surface $E \times E'$ of Section 1.2 the right-hand side has rank 4 and the left-hand side rank 2. The rank in (b) for the right-hand side can be seen directly: $\mathrm{Hom}_W(M(X), M(X'))$ with the σ-semilinear operator $\alpha \mapsto F\alpha F^{-1}$ has all slopes 0, so by the argument of Proposition 4.4 its fixed vectors form a lattice of full rank $(2 \dim X)(2 \dim X')$.

Corollary 4.11. *For a supersingular abelian variety X over $\bar{\mathbb{F}}_p$, $\mathrm{Alg}^1(X) = T^2(X)$ and $S(X) \subseteq \mathrm{Alg}^2(X)$.*

Proof. By Fact 4.10(c) every class in $T^2(X)$ is a $\mathbb{Z}_p$-combination of classes of divisors, which is the first statement. For divisors z, z', $\mathrm{cl}(z) \wedge \mathrm{cl}(z') = \mathrm{cl}(z \cdot z')$ by Fact 4.6, so products of two classes in $T^2(X)$ are $\mathbb{Z}_p$-combinations of classes of cycles of codimension 2. □

Exercise 4.3. Explain why the integral crystalline Tate conjecture in codimension 1 for supersingular abelian varieties needs no input about algebraic cycles beyond Fact 4.10, and why the same argument does not give codimension 2: which step fails?

4.6. The rational statement

Proposition 4.12 (the rational statement). *Let X be a supersingular abelian variety over $\bar{\mathbb{F}}_p$. For every i, $S^{2i}(X)$ has finite index in $T^{2i}(X)$. In particular $S(X) \otimes \mathbb{Q} = \mathrm{Alg}^2(X) \otimes \mathbb{Q} = T^4(X) \otimes \mathbb{Q}$, and $T^4(X)/\mathrm{Alg}^2(X)$ is a finite quotient of $T^4(X)/S(X)$.*

PROOF. Write $M = M(X)$ and $M_{\mathbb{Q}} = M \otimes \mathbb{Q}$, a vector space over $W[1/p]$. By Proposition 4.4 with $n = 2$, the $W[1/p]$-span of $T^2(X)$ is $\bigwedge^2 M_{\mathbb{Q}}$. The $W[1/p]$-span of the products of i elements of $\bigwedge^2 M_{\mathbb{Q}}$ is $\bigwedge^{2i} M_{\mathbb{Q}}$, because every basis vector $e'_{j_1} \wedge \cdots \wedge e'_{j_{2i}}$ is the product of the i vectors $e'_{j_1} \wedge e'_{j_2}, \ldots, e'_{j_{2i-1}} \wedge e'_{j_{2i}}$ (Exercise 4.4). Hence the $W[1/p]$-span of $S^{2i}(X)$ is $\bigwedge^{2i} M_{\mathbb{Q}}$. Since $S^{2i}(X) \subseteq T^{2i}(X)$ and $T^{2i}(X) \otimes W \to \bigwedge^{2i} M$ is injective (Proposition 4.4), so is $S^{2i}(X) \otimes W \to \bigwedge^{2i} M$ by flatness of W over $\mathbb{Z}_p$, and the rank of $S^{2i}(X)$ is $\dim \bigwedge^{2i} M_{\mathbb{Q}} = \binom{2g}{2i}$, the rank of $T^{2i}(X)$. Two free $\mathbb{Z}_p$-modules of the same finite rank, one inside the other, differ by a finite group. The last statement follows from Corollary 4.11 and Exercise 1.3. □

EXERCISE 4.4. Show that the even part of the exterior algebra of a finite-dimensional vector space over a field is generated, as an algebra, by its part of degree 2. Then show that over $\mathbb{Z}$ the 2-form $x = e_1 \wedge e_2 + e_3 \wedge e_4$ has $x \wedge x = 2e_1 \wedge e_2 \wedge e_3 \wedge e_4$, so that the square of an integral 2-form can be divisible by an integer although the form is not.

The last part of Exercise 4.4 is a first sign of where integral and rational statements differ: a product of two classes may be divisible by a constant that is not a unit. At $p \geq 5$ the constants 2 and 3! are units, but the min-plus exponents of Chapter 5 produce genuine divisibility by p.

4.7. The intersection pairing and discriminants

Let L be a free $\mathbb{Z}_p$-module of finite rank n with a symmetric bilinear form $\langle\ ,\ \rangle\colon L \times L \to \mathbb{Z}_p$ that is nondegenerate, that is, nondegenerate after tensoring with $\mathbb{Q}$. The *discriminant* $\operatorname{disc} L$ is the determinant of the Gram matrix $(\langle x_i, x_j \rangle)$ in a basis (x_i) of L. A change of basis by $\gamma \in \mathrm{GL}_n(\mathbb{Z}_p)$ multiplies it by $\det(\gamma)^2$, a unit, so the p-adic valuation $v_p(\operatorname{disc} L)$ is well defined, and $v_p(\operatorname{disc} L) \geq 0$ because the form is $\mathbb{Z}_p$-valued.

LEMMA 4.13 (discriminants of sublattices). *Let $L' \subseteq L$ be a sublattice of full rank. Then $\operatorname{disc} L' = [L : L']^2 \operatorname{disc} L$ up to a unit of $\mathbb{Z}_p$. In particular, if $\operatorname{disc} L'$ is a unit, then $L' = L$.*

PROOF. Let (x_i) be a basis of L and (x'_i) one of L', and write $x'_j = \sum_i \gamma_{ij} x_i$ with $\gamma \in \mathrm{Mat}_n(\mathbb{Z}_p)$. The Gram matrix of L' is $\gamma^{\top} \mathrm{Gr}(L) \gamma$, where $\mathrm{Gr}(L)$ is that of L, so $\operatorname{disc} L' = \det(\gamma)^2 \operatorname{disc} L$. By the elementary divisor theorem over the principal ideal domain $\mathbb{Z}_p$, $L/L' \cong \bigoplus_i \mathbb{Z}_p/p^{n_i}$ with $\sum n_i = v_p(\det \gamma)$, so $[L : L'] = p^{v_p(\det \gamma)}$, which is $\det \gamma$ up to a unit. If $\operatorname{disc} L'$ is a unit, then $0 = v_p(\operatorname{disc} L') = 2v_p([L : L']) + v_p(\operatorname{disc} L)$ with both terms ≥ 0, so $[L : L'] = 1$. □

Intuition 4.14 (a lattice cannot hide behind a unit discriminant). The discriminant measures the volume of a fundamental domain, squared. A proper sublattice has a larger fundamental domain, by the factor $[L : L']$, and a lattice with a $\mathbb{Z}_p$-valued form cannot have a discriminant smaller than a unit. So if two classes in a rank-2 lattice with $\mathbb{Z}_p$-valued form have a Gram determinant that is a unit, they span the lattice, whatever the lattice is.

EXERCISE 4.5. Let $L = \mathbb{Z}_p^2$ with Gram matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and L' the span of $(1, 0)$ and $(1, p)$. Compute $[L : L']$, the Gram matrix of L' and both discriminants, and check Lemma 4.13. Then explain why no sublattice of index p in any lattice with a $\mathbb{Z}_p$-valued form can have a unit discriminant.

Where this is used. The lattices T^4 and S are computed for monomial modules in Chapters 5 and 8, and the index $[T^4 : S]$ is the subject of Proposition 8.2. Fact 4.10 identifies endomorphisms of X with those of $(M(X), F)$ in Chapter 9. Fact 4.6 and Lemma 4.13 are the two inputs of the specialization argument (Proposition 13.4), and the Künneth decomposition defines the component T_{22} of Definition 9.3.

CHAPTER 5

Monomial modules and the min-plus calculus

Where we are. This chapter contains the computational engine of the proof. For a Dieudonné module whose Frobenius maps a basis to multiples of basis vectors, every lattice the proof needs is spanned by multiples $p^{n_J}e_J$ of wedge products of basis vectors, and the exponents n_J are given by explicit formulas built from sums, maxima and minima of the integers 0 and 1. The chapter proves this for the Tate lattices (the descent lemma, Lemma 5.3), for products, for endomorphisms and for spans of pull-backs, and explains why the exponents do not depend on p. It needs the chapters on Dieudonné modules and on Tate classes.

5.1. Monomial lattices and min-plus formulas in two pages

Let M be a free W-module with basis $(e_s)_{s\in\mathcal{C}}$, indexed by a finite set $\mathcal{C}$ (for the model $\mathbb{M}$ the cube of Equation (1.1)), and suppose that Frobenius permutes the basis up to powers of p: $Fe_s = p^{w(s)}e_{\pi(s)}$, with π a permutation of $\mathcal{C}$ and $w(s)\in\{0,1\}$. The modules of words of Definition 3.17 and the model $\mathbb{M}$ are of this kind. Then $\bigwedge^n F$ permutes the wedge basis e_J, $J\subseteq\mathcal{C}$, $|J|=n$, up to signs and powers of p, and so does $\varphi = p^{-n/2}\bigwedge^n F$:

$$\varphi(e_J) = \pm p^{w(J)-n/2}e_{\pi(J)}, \qquad w(J)=\sum_{s\in J} w(s).$$

The Tate lattice T^n is the lattice of φ-fixed vectors. The descent lemma says that its W-span is

$$T^n\otimes W = \bigoplus_{|J|=n} p^{n_J}We_J,$$

where the exponents $n_J\geq 0$ are determined along each orbit of π on n-sets by two conditions: $n_{\pi(J)}-n_J = w(J)-\frac{n}{2}$, so that φ permutes the vectors $p^{n_J}e_J$ up to sign, and the smallest exponent in each orbit is 0. Equivalently n_J is the largest partial sum of the numbers $w(\pi^{-i}J)-\frac{n}{2}$ along the orbit, the *orbit rule* (5.1).

The W-span $S\otimes W$ of the lattice S of divisor products is then spanned by the products $p^{n_{J_1}}e_{J_1}\wedge p^{n_{J_2}}e_{J_2}$ of pairs of basis vectors of $T^2\otimes W$, so its exponent at e_J, $|J|=4$, is the smallest sum $n_{J_1}+n_{J_2}$ over the splittings $J=J_1\sqcup J_2$ into two 2-sets, and $[T^4:S]=p^{\sum_J(n_J^S-n_J)}$ (5.2). The same reasoning applies to endomorphisms, which form a lattice monomial in the matrix units, and to the span of their pull-backs. Here the polarization identity, with 4! a unit because $p\geq 5$, reduces spans over all endomorphisms to spans over monomial generators, whose values on wedge products are single monomials.

The point is that every number in the first half of the proof is an integer computed from the integers $w(s)\in\{0,1\}$ by additions, maxima and minima: a min-plus expression, independent of p. Proving $T^4/S\cong(\mathbb{Z}/p)^4$ for the model amounts to evaluating such expressions for 70 subsets J (Chapter 8).

Example 5.1 (one exponent of $E_0\times E_0$). For 01+01, with basis e_0,e_1,e_0',e_1' and $Fe_0=e_1$, $Fe_1=pe_0$ and the same on the primed vectors, take $n=2$ and $J=\{e_0,e_0'\}$. Then $w(J)=0$ and $\pi(J)=\{e_1,e_1'\}$ with $w(\pi(J))=2$. So $n_{\pi(J)}-n_J=0-1=-1$ and $n_J-n_{\pi(J)}=2-1=1$; with the smallest exponent 0 this gives $n_{\{e_1,e_1'\}}=0$ and $n_{\{e_0,e_0'\}}=1$. This is the exponent found by hand in Example 4.5: the Tate class $\lambda pe_0\wedge e_0'+\sigma(\lambda)e_1\wedge e_1'$ has the factor p at $e_0\wedge e_0'$.

5.2. Monomial lattices

Let $(e_s)_{s\in\mathcal{C}}$ be a basis of a free W-module M of finite rank. A *monomial lattice* with respect to this basis is a W-submodule of $M\otimes\mathbb{Q}$ of the form

$$L(n)=\bigoplus_{s\in\mathcal{C}} p^{n_s}We_s,\qquad n=(n_s)\in\mathbb{Z}^{\mathcal{C}}.$$

Monomial lattices are described by their exponent vectors, and the lattice operations become operations on exponents:

$$L(n)\cap L(n')=L(\max(n,n')),\qquad L(n)+L(n')=L(\min(n,n')),$$
$$L(n')\subseteq L(n)\iff n'\geq n,$$

componentwise, and if $L(n')\subseteq L(n)$ then $L(n)/L(n')\cong\bigoplus_s W/p^{n'_s-n_s}$ has length $\sum_s(n'_s-n_s)$ over W. The image of a monomial lattice under a map that sends each e_s to a unit multiple of $p^{l_s}e_{\pi'(s)}$, for a permutation π', is again monomial, with exponent n_s+l_s at $e_{\pi'(s)}$; this is how F and φ act.

The lattices we want to know are $\mathbb{Z}_p$-lattices such as T^4 and S, and they are computed through their W-spans. The following elementary facts allow this.

Lemma 5.2 (base change to W). *Let $L'\subseteq L$ be free $\mathbb{Z}_p$-modules of the same finite rank. Then $L'\otimes_{\mathbb{Z}_p}W\to L\otimes_{\mathbb{Z}_p}W$ is injective, its cokernel is $(L/L')\otimes W$, whose length over W equals the length of L/L' over $\mathbb{Z}_p$, and $L\cap(L'\otimes W)=L'$ inside $L\otimes W$. In particular $[L:L']=p^n$ with n the length of $(L\otimes W)/(L'\otimes W)$, and for two submodules L_1,L_2 of L of full rank, $L_1\subseteq L_2$ if and only if $L_1\otimes W\subseteq L_2\otimes W$.*

Proof. The module W is torsion-free over the discrete valuation ring $\mathbb{Z}_p$, hence flat, which gives the injectivity and the cokernel. Write $L/L'\cong\bigoplus_i\mathbb{Z}/p^{n_i}$. Then $(L/L')\otimes W\cong\bigoplus_i W/p^{n_i}$, of length $\sum n_i$ over W, and the map $L/L'\to(L/L')\otimes W$ is injective because each $\mathbb{Z}/p^{n_i}\to W/p^{n_i}$ is. An element $x\in L$ that lies in $L'\otimes W$ maps to 0 in $(L/L')\otimes W$, hence to 0 in L/L', so $x\in L'$. For the last statement apply this to $L_1\cap L_2\subseteq L_1$: $L_1\otimes W\subseteq L_2\otimes W$ gives $(L_1\cap L_2)\otimes W=L_1\otimes W$ by flatness, so $L_1/(L_1\cap L_2)$ has length 0. □

Exercise 5.1. In W^3 with the standard basis, let $L_1=pW\oplus W\oplus p^2W$ and $L_2=W\oplus p^3W\oplus pW$. Compute $L_1\cap L_2$ and L_1+L_2, and the lengths of $(L_1+L_2)/L_1$ and of $L_2/(L_1\cap L_2)$. Check that they agree, as the isomorphism $(L_1+L_2)/L_1\cong L_2/(L_1\cap L_2)$ requires, and show the agreement for arbitrary exponent vectors.

5.3. Monomial Dieudonné modules

From now on M is a free W-module with basis $(e_s)_{s\in\mathcal{C}}$, π is a permutation of the finite set $\mathcal{C}$, and $w\colon\mathcal{C}\to\{0,1\}$ is a function that is *balanced* on every orbit J of π, $\sum_{s\in J}w(s)=|J|/2$. Frobenius is the σ-semilinear map

$$Fe_s=p^{w(s)}e_{\pi(s)}.$$

Every orbit has even length, since it carries as many 0s as 1s, and the order q of π, the least common multiple of the orbit lengths, is even. Along an orbit of length l, F^l multiplies each e_s by $p^{l/2}$, so

$$F^q=p^{q/2}\sigma^q$$

in the basis (e_s). These are exactly the monomial Dieudonné modules of Definition 3.17: each orbit is a cycle, and reading w along it gives a word.

For $J\subseteq\mathcal{C}$ with $|J|=n$ let e_J be the wedge product of the e_s, $s\in J$, in a fixed order, and $w(J)=\sum_{s\in J}w(s)$. Then

$$\textstyle\bigwedge^n F(e_J)=\pm p^{w(J)}e_{\pi(J)},$$

because $\bigwedge^n F(e_J)$ is the wedge of the $p^{w(s)}e_{\pi(s)}$, $s\in J$, which is $e_{\pi(J)}$ up to the sign of a reordering. So π acts on the n-sets, and $\bigwedge^n F$ is again monomial, with the weight $w(J)$ in place of $w(s)$.

5.4. The descent lemma

For even n let $T^n = \{x \in \bigwedge^n M : \bigwedge^n F(x) = p^{n/2}x\}$, as in Definition 4.3, and let $S^n \subseteq T^n$ be the $\mathbb{Z}_p$-span of the products of $n/2$ elements of T^2, as in Definition 4.9; so $S = S^4$.

LEMMA 5.3 (descent). *Let n be even. Then $T^n \otimes_{\mathbb{Z}_p} W = \bigoplus_{|J|=n} p^{n_J} W e_J$ with*

$$n_J = \max_{0\le j<q} \sum_{i=1}^{j} \Big(w(\pi^{-i}(J)) - \frac{n}{2} \Big), \tag{5.1}$$

and T^n has rank $\binom{|\mathcal{C}|}{n}$. Moreover $S^n \otimes W = \bigoplus_{|J|=n} p^{n_J^S} W e_J$ with

$$n_J^S = \min_{J = J_1 \sqcup \cdots \sqcup J_{n/2}} (n_{J_1} + \cdots + n_{J_{n/2}}) \tag{5.2}$$

over the partitions of J into 2-sets, and $[T^n : S^n] = p^{\sum_J (n_J^S - n_J)}$.

PROOF. Put $\varphi = p^{-n/2}\bigwedge^n F$ on $\bigwedge^n M \otimes \mathbb{Q}$. It is σ-semilinear, $\varphi(e_J) = \pm p^{w(J)-n/2} e_{\pi(J)}$, and $\varphi^q = \sigma^q$ in the basis (e_J), because $F^q = p^{q/2}\sigma^q$ on M gives $\bigwedge^n F^q = p^{nq/2}\sigma^q$.

Step 1: a φ-stable lattice. Let $L_\varphi = \bigcap_{0\le j<q} \varphi^j(\bigwedge^n M)$. Since $\varphi^q(\bigwedge^n M) = \sigma^q(\bigwedge^n M) = \bigwedge^n M$, applying φ permutes the q lattices in the intersection cyclically, so $\varphi(L_\varphi) = L_\varphi$. As φ is injective, it is a σ-semilinear bijection of L_φ.

Step 2: Lang. By Lemma 3.5 with $r = 1$, $L_\varphi = L_\varphi^\varphi \otimes_{\mathbb{Z}_p} W$, where L_φ^φ is the $\mathbb{Z}_p$-module of φ-fixed vectors in L_φ, free of rank equal to the rank of L_φ.

Step 3: the fixed vectors are T^n. A vector of $\bigwedge^n M$ fixed by φ equals φ^j of itself, so it lies in every $\varphi^j(\bigwedge^n M)$ and hence in L_φ. Conversely $L_\varphi \subseteq \bigwedge^n M$. So $L_\varphi^\varphi = T^n$ and $T^n \otimes W = L_\varphi$.

Step 4: the exponents. The lattice $\varphi^j(\bigwedge^n M)$ is the W-span of the vectors $\varphi^j(e_{J'})$, because φ^j is σ^j-semilinear and σ is bijective on W. Iterating the formula for φ gives $\varphi^j(e_{J'}) = \pm p^{\sum_{i=0}^{j-1}(w(\pi^i J')-n/2)} e_{\pi^j(J')}$. Writing $J = \pi^j(J')$, the exponent of $\varphi^j(\bigwedge^n M)$ at e_J is $\sum_{i=1}^{j}(w(\pi^{-i}J) - n/2)$. So each $\varphi^j(\bigwedge^n M)$ is monomial, and their intersection is monomial with the maximal exponents, which is (5.1). The term $j = 0$ shows $n_J \ge 0$, and since every J occurs, L_φ has full rank $\binom{|\mathcal{C}|}{n}$.

Step 5: products. By bilinearity, $S^n \otimes W$ is the W-span of the products of $n/2$ elements of $T^2 \otimes W$, which by Step 4 is spanned by the $p^{n_{J'}} e_{J'}$, $|J'| = 2$. A product $p^{n_{J_1}} e_{J_1} \wedge \cdots \wedge p^{n_{J_{n/2}}} e_{J_{n/2}}$ is $\pm p^{n_{J_1}+\cdots+n_{J_{n/2}}} e_J$ if the J_i are disjoint with union J, and 0 otherwise. So $S^n \otimes W$ is monomial with the exponents (5.2); it is the W-span of S^n inside $\bigwedge^n M$ by Lemma 5.2. Finally, by Lemma 5.2 the index $[T^n : S^n]$ is p to the length of $(T^n \otimes W)/(S^n \otimes W)$, which is $\sum_J (n_J^S - n_J)$. □

What just happened. The lattice of Tate classes is invisible over $\mathbb{Z}_p$ but explicit over W: it is the intersection of the q lattices $\varphi^j(\bigwedge^n M)$, each of which is monomial because φ permutes the wedge basis up to powers of p. Lang's lemma says that this intersection is exactly the W-span of the Tate classes. Products of Tate classes are computed on the monomial generators, and indices over $\mathbb{Z}_p$ are read off over W.

The orbit rule. Formula (5.1) depends only on the orbit of J under π and on the weights w along it. It has an equivalent form that is easier to evaluate. Let $J_0, J_1 = \pi(J_0), \ldots, J_{l-1}$ be the orbit of J_0, of length $l \mid q$, and let $\widetilde{n}_i = \sum_{j<i}(w(J_j) - n/2)$ be the partial sums along it, with $\widetilde{n}_l = 0$ because the sum over an orbit of $w(J) - n/2$ vanishes (a multiple of it is the sum over q steps, which vanishes since $\varphi^q = \sigma^q$). Then

$$n_{J_i} = \widetilde{n}_i - \min_{0\le j<l} \widetilde{n}_j.$$

In words: along the orbit, the exponents change by $n_{\pi(J)} - n_J = w(J) - n/2$, so that $\varphi(p^{n_J} e_J) = \pm p^{n_{\pi(J)}} e_{\pi(J)}$, and the constant of integration is fixed by requiring the smallest

exponent in the orbit to be 0 (Exercise 5.2). So φ permutes the vectors $p^{n_J}e_J$ up to sign, and $T^n \otimes W$ is the largest φ-stable lattice of this shape inside $\bigwedge^n M$.

Intuition 5.4 (what the exponent n_J measures). A Tate class with a nonzero coefficient at e_J also has nonzero coefficients along the whole φ-orbit of J, because φ moves them around. Along the orbit, each step multiplies by $p^{w(J)-n/2}$, sometimes dividing by p and sometimes multiplying. For the class to stay integral at every point of the orbit, its coefficient at e_J must be divisible by p^{n_J}, the largest total division that the steps leading to J can accumulate.

EXERCISE 5.2. Prove the equivalence of (5.1) and the orbit rule $n_{J_i} = \widetilde{n}_i - \min_j \widetilde{n}_j$, and deduce $n_{\pi(J)} = n_J + w(J) - \frac{n}{2}$.

5.5. Worked examples

EXAMPLE 5.5 (the orbit rule step by step). Take the word 0011: basis e_0, e_1, e_2, e_3 with $Fe_0 = e_1$, $Fe_1 = e_2$, $Fe_2 = pe_3$, $Fe_3 = pe_0$, so $w = (0, 0, 1, 1)$, $\pi(i) = i + 1$ modulo 4, and $q = 4$. For $n = 2$ the 2-set $\{0, 1\}$ has the orbit

$$\{0,1\} \to \{1,2\} \to \{2,3\} \to \{3,0\} \to \{0,1\}, \qquad w = 0,\ 1,\ 2,\ 1,$$

so the steps $w - 1$ are $-1, 0, +1, 0$ and the partial sums $\widetilde{n}_i$ are $0, -1, -1, 0$. Their minimum is -1, so the exponents are $n_{\{0,1\}} = 1$, $n_{\{1,2\}} = 0$, $n_{\{2,3\}} = 0$, $n_{\{3,0\}} = 1$. Check with $\varphi = p^{-1}\bigwedge^2 F$: up to sign

$$\varphi(pe_{\{0,1\}}) = e_{\{1,2\}}, \qquad \varphi(e_{\{1,2\}}) = e_{\{2,3\}}, \qquad \varphi(e_{\{2,3\}}) = pe_{\{3,0\}}, \qquad \varphi(pe_{\{3,0\}}) = pe_{\{0,1\}},$$

writing $e_{\{i,j\}} = e_i \wedge e_j$. So φ permutes the four vectors $pe_{\{0,1\}}, e_{\{1,2\}}, e_{\{2,3\}}, pe_{\{3,0\}}$ cyclically, and the Tate classes supported on this orbit are $\lambda pe_{\{0,1\}} + \sigma(\lambda)e_{\{1,2\}} + \sigma^2(\lambda)e_{\{2,3\}} + \sigma^3(\lambda)pe_{\{3,0\}}$ up to signs, with $\lambda \in \mathbb{Z}_{p^4}$: a $\mathbb{Z}_p$-module of rank 4. With formula (5.1) instead: the predecessors of $J = \{0, 1\}$ are $\{3, 0\}, \{2, 3\}, \{1, 2\}$ with $w - 1 = 0, +1, 0$, partial sums $0, 1, 1$, maximum (with the empty sum 0) equal to 1.

EXAMPLE 5.6 ($01 + 01$ against 0011). For $E_0 \times E_0$, the module $01 + 01$ with basis e_0, e_1, e_0', e_1', the six exponents of T^2 are

$$n_{\{e_0,e_1\}} = 0, \quad n_{\{e_0',e_1'\}} = 0, \quad n_{\{e_0,e_0'\}} = 1, \quad n_{\{e_1,e_1'\}} = 0, \quad n_{\{e_0,e_1'\}} = 0, \quad n_{\{e_1,e_0'\}} = 0,$$

in agreement with Example 4.5: $T^2 \otimes W$ has index p^1 in $\bigwedge^2 M$. For the word 0011 the six exponents are computed in Exercise 5.3; their sum is 2, so there $T^2 \otimes W$ has index p^2 in $\bigwedge^2 M$. The two modules are isogenous (Example 3.12) and their Tate lattices are commensurable, but the position of T^2 inside $\bigwedge^2 M$ differs. In both cases there is a single 4-set, all of $\mathcal{C}$, with $n_J = 0$ and $n_J^S = 0$: the product $p^{n_{\{0,2\}}}e_{\{0,2\}} \wedge p^{n_{\{1,3\}}}e_{\{1,3\}}$ has exponent $0 + 0$ for 0011, and $e_0 \wedge e_1$ times $e_0' \wedge e_1'$ has exponent 0 for $01 + 01$. So $T^4 = S$ for both modules; for $E_0 \times E_0$ this matches the fact that the class of a point is the product of the classes of the two fibers $\{0\} \times E_0$ and $E_0 \times \{0\}$.

EXERCISE 5.3. Compute n_J for all six 2-sets J of the word 0011, and check that every φ-orbit contains a 2-set with exponent 0.

5.6. Products and the index

Formula (5.2) gives $S = S^4$ through the minimum of $n_{J_1} + n_{J_2}$ over the three splittings of a 4-set J into two 2-sets, and the triple products S^6 through the minimum over the fifteen splittings of a 6-set into three 2-sets. The difference $n_J^S - n_J \geq 0$ is the *defect* of J: by the lemma, $[T^4 : S] = p^{\sum_J (n_J^S - n_J)}$. A positive defect means that the Tate class $p^{n_J}e_J$ of $T^4 \otimes W$ is reached by products of Tate classes of degree 2 only after multiplication by $p^{n_J^S - n_J}$.

EXAMPLE 5.7 (a defect in dimension 3). For the word 001011 of length 6, with $w = (0,0,1,0,1,1)$ and $J = \{e_0, e_1, e_2, e_4\}$, the orbit rule gives $n_J = 0$, while each of the three splittings $\{0,1\} \sqcup \{2,4\}$, $\{0,2\} \sqcup \{1,4\}$, $\{0,4\} \sqcup \{1,2\}$ has $n_{J_1} + n_{J_2} = 1$. So $n_J^S = 1$, a defect (Exercise 5.4). Evaluating all $\binom{6}{4} = 15$ four-sets of this module gives $[T^4 : S] = p^6$; that number is the output of an exact evaluation of the formulas, not derived here by hand.

EXERCISE 5.4. Verify the exponents claimed in Example 5.7: compute n_J for $J = \{0,1,2,4\}$ and $n_{J'}$ for the six 2-sets J' that occur in its splittings, using the orbit rule.

EXERCISE 5.5. Let $L(n') \subseteq L(n)$ be monomial W-lattices that are the W-spans of $\mathbb{Z}_p$-lattices $L' \subseteq L$. Show that $[L : L'] = p^{\sum_s (n'_s - n_s)}$, and that L/L' is killed by p if every difference $n'_s - n_s$ is at most 1.

5.7. Endomorphisms and the span of pull-backs

The same descent applies to homomorphisms. On $\mathrm{End}_W(M)$, the W-linear endomorphisms of M, let

$$\mathrm{Ad}_F(\alpha) = F\alpha F^{-1},$$

a σ-semilinear bijection of $\mathrm{End}_W(M) \otimes \mathbb{Q}$. Its fixed vectors in $\mathrm{End}_W(M)$ are the W-linear maps commuting with F, the ring $\mathrm{End}(M,F)$. In the matrix units $e_{ss'}$, $e_{ss'}(e_{s'}) = e_s$ and $e_{ss'}(e_{s''}) = 0$ for $s'' \neq s'$,

$$\mathrm{Ad}_F(e_{ss'}) = p^{w(s)-w(s')} e_{\pi(s)\pi(s')},$$

since $Fe_{ss'}F^{-1}$ sends $e_{\pi(s')}$ to $Fe_{ss'}(p^{-w(s')}e_{s'}) = p^{w(s)-w(s')}e_{\pi(s)}$ and the other basis vectors to 0. So Ad_F is monomial on the pairs (s,s'), with weight $w(s) - w(s')$ and with 0 in place of $n/2$, and $\mathrm{Ad}_F^q = \sigma^q$. The proof of Lemma 5.3 applies word for word:

$$\mathrm{End}(M,F) \otimes W = \bigoplus_{s,s'} p^{m_{ss'}} W e_{ss'}, \qquad m_{ss'} = \max_{0 \le j < q} \sum_{i=1}^{j} \Big(w(\pi^{-i}s) - w(\pi^{-i}s') \Big).$$

EXAMPLE 5.8 ($\mathrm{End}(M(E_0), F)$). For the word 01, the pairs $(0,0)$ and $(1,1)$ form an orbit of weight 0, so $m_{00} = m_{11} = 0$. The pairs $(0,1) \to (1,0) \to (0,1)$ have weights $w(0) - w(1) = -1$ and $w(1) - w(0) = +1$; the orbit rule gives $m_{01} = 1$ and $m_{10} = 0$. So

$$\mathrm{End}(M(E_0), F) \otimes W = \left\{ \begin{pmatrix} \lambda_{00} & p\lambda_{01} \\ \lambda_{10} & \lambda_{11} \end{pmatrix} : \lambda_{ij} \in W \right\},$$

and $\mathrm{End}(M(E_0), F)$ itself, the fixed vectors of Ad_F, consists of the matrices $\left(\begin{smallmatrix} \lambda & p\sigma(\lambda') \\ \lambda' & \sigma(\lambda) \end{smallmatrix}\right)$ with $\lambda, \lambda' \in \mathbb{Z}_{p^2}$, a free $\mathbb{Z}_p$-module of rank 4, which by Fact 4.10 is $\mathrm{End}(E_0) \otimes \mathbb{Z}_p$. This is the maximal order of the quaternion division algebra over $\mathbb{Q}_p$ (see e.g. [Voi21, Corollary 13.3.14 and Theorem 13.3.11], with $\mathbb{Q}_{p^2}$ the unramified quadratic extension of $\mathbb{Q}_p$).

EXAMPLE 5.9 (endomorphisms of 0011 and of $01 + 01$). For the word 0011, with $w = (0,0,1,1)$, the pairs (s,s') of basis indices fall into four orbits of length 4 under $(s,s') \mapsto (s+1, s'+1)$. For instance the orbit $(0,2) \to (1,3) \to (2,0) \to (3,1)$ has weights $w(s) - w(s') = -1, -1, +1, +1$ and partial sums $0, -1, -2, -1$, so $m_{02} = 2$, $m_{13} = 1$, $m_{20} = 0$, $m_{31} = 1$. All sixteen exponents, rows indexed by the target s and columns by the source s', are

$$(m_{ss'})_{0011} = \begin{pmatrix} 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \qquad (m_{ss'})_{01+01} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

the second for the basis e_0, e_1, e'_0, e'_1 of $01 + 01$. The exponents add up to 8 and to 4: the lattice $\mathrm{End}(M,F) \otimes W$ has index p^8, respectively p^4, in $\mathrm{End}_W(M)$. The two modules are isogenous, so their endomorphism algebras over $\mathbb{Q}_p$ are the same, the 2×2 matrices over the quaternion division algebra; at p the surface with a-number 1 has the smaller order.

Polarization. The pull-back of a class $x \in \bigwedge^4 M$ by $\alpha \in \mathrm{End}(M,F)$ is $\bigwedge^4\alpha(x)$, which is not linear in α. For $\alpha_1,\dots,\alpha_4 \in \mathrm{End}_W(M)$ let

$$D(\alpha_1,\dots,\alpha_4)(x_1\wedge x_2\wedge x_3\wedge x_4) = \sum_{\pi'\in\mathfrak{S}_4} \alpha_{\pi'(1)}x_1\wedge\alpha_{\pi'(2)}x_2\wedge\alpha_{\pi'(3)}x_3\wedge\alpha_{\pi'(4)}x_4,$$

the *polarized form* of $\alpha\mapsto\bigwedge^4\alpha$. It is W-multilinear and symmetric in the α_i, and $D(\alpha,\alpha,\alpha,\alpha) = 4!\bigwedge^4\alpha$. Expanding $\bigwedge^4(\sum_{i\in J}\alpha_i)$ and using inclusion–exclusion gives the *polarization identity*

$$D(\alpha_1,\dots,\alpha_4) = \sum_{\emptyset\neq J\subseteq\{1,2,3,4\}} (-1)^{4-|J|}\bigwedge^4\Big(\sum_{i\in J}\alpha_i\Big)$$

(Exercise 5.6). Both identities have integer coefficients, so for a $\mathbb{Z}_p$-submodule $\mathcal{R}\subseteq\mathrm{End}_W(M)$ and a set $\Xi\subseteq\bigwedge^4 M$, the $\mathbb{Z}_p$-span of the $D(\alpha_1,\dots,\alpha_4)(x)$, $\alpha_i\in\mathcal{R}$, $x\in\Xi$, is contained in the span of the $\bigwedge^4\alpha(x)$, $\alpha\in\mathcal{R}$, $x\in\Xi$, and contains $4!$ times it. If $p\geq 5$, $4!$ is a unit and the two spans are equal.

Monomial generators. For matrix units, $D(e_{s^{(1)}s'^{(1)}},\dots,e_{s^{(4)}s'^{(4)}})(e_J)$, where $J = \{s''^{(1)},\dots,s''^{(4)}\}$, is a single signed basis vector or 0: a term $e_{s^{(\pi'(1))}s'^{(\pi'(1))}}(e_{s''^{(1)}})\wedge\cdots$ is nonzero only if $s'^{(\pi'(i))} = s''^{(i)}$ for all i, which for distinct $s''^{(i)}$ happens for at most one π', and then the term is $\pm e_{\{s^{(1)},\dots,s^{(4)}\}}$ or 0. Now let $\mathcal{R} = \mathrm{End}(M,F)$, so $\mathcal{R}\otimes W$ is monomial with exponents $m_{ss'}$, and let Ξ be a $\mathbb{Z}_p$-lattice with $\Xi\otimes W = \bigoplus p^{n^\Xi_J} W e_J$ monomial. By multilinearity, the W-span of the polarized values is spanned by the values on the monomial generators $p^{m_{ss'}}e_{ss'}$ and $p^{n^\Xi_J}e_J$. Hence:

Proposition 5.10 (spans of pull-backs). *Let $p\geq 5$. The $\mathbb{Z}_p$-span $\mathrm{End}^*\,\Xi$ of the classes $\bigwedge^4\alpha(x)$, $\alpha\in\mathrm{End}(M,F)$, $x\in\Xi$, satisfies*

$$(\mathrm{End}^*\,\Xi)\otimes W = \bigoplus_{|J'|=4} p^{n'_{J'}} W e_{J'}, \qquad n'_{J'} = \min_{|J|=4}\Big(n^\Xi_J + \min_{\pi'\colon J\to J'}\sum_{s\in J} m_{\pi'(s)s}\Big),$$

with π' running over the bijections $J\to J'$.

The inner minimum is the min-plus analog of the 4×4 minor of α with columns J and rows J', which is the matrix entry of $\bigwedge^4\alpha$ from e_J to $e_{J'}$. In degree 2 the analog is easy to see: the entry of $\bigwedge^2\alpha$ from $e_{\{s'^{(1)},s'^{(2)}\}}$ to $e_{\{s^{(1)},s^{(2)}\}}$ is the minor $\alpha_{s^{(1)}s'^{(1)}}\alpha_{s^{(2)}s'^{(2)}} - \alpha_{s^{(1)}s'^{(2)}}\alpha_{s^{(2)}s'^{(1)}}$. For $\alpha\in\mathrm{End}(M,F)\otimes W$ its valuation is at least $\min(m_{s^{(1)}s'^{(1)}}+m_{s^{(2)}s'^{(2)}}, m_{s^{(1)}s'^{(2)}}+m_{s^{(2)}s'^{(1)}})$, and this bound is attained by $\alpha = p^{m_{s^{(1)}s'^{(1)}}}e_{s^{(1)}s'^{(1)}} + p^{m_{s^{(2)}s'^{(2)}}}e_{s^{(2)}s'^{(2)}}$ or by the analogous sum for the other bijection. So the span of the minors over all α is exactly the monomial lattice with the min-plus exponent, which is the content of the proposition in degree 2. The same proposition holds for homomorphisms between two monomial modules, with the exponents of the Hom-lattice, and for push-forwards, which act on $\bigwedge^4$ through complementary minors (Chapter 15).

Exercise 5.6. Write out the polarization of $\alpha\mapsto\bigwedge^2\alpha$: show that $\bigwedge^2(\alpha_1+\alpha_2) - \bigwedge^2\alpha_1 - \bigwedge^2\alpha_2 = D(\alpha_1,\alpha_2)$ with $D(\alpha_1,\alpha_2)(x_1\wedge x_2) = \alpha_1x_1\wedge\alpha_2x_2 + \alpha_2x_1\wedge\alpha_1x_2$, and that $D(\alpha,\alpha) = 2\bigwedge^2\alpha$. Give an example over $\mathbb{Z}$ of a group $\mathcal{R}$ of endomorphisms and a vector x such that the values $D(\alpha_1,\alpha_2)(x)$, $\alpha_i\in\mathcal{R}$, span a proper sublattice of the span of the values $\bigwedge^2\alpha(x)$, $\alpha\in\mathcal{R}$, and explain why the two spans agree over $\mathbb{Z}_p$ for odd p.

5.8. Independence of p, and how the exact computations work

Every exponent in this chapter is obtained from the integers $w(s)\in\{0,1\}$ by finitely many additions, maxima and minima: the orbit rule for n_J and $m_{ss'}$, minima over splittings for n^S_J, minima over bijections and generators for spans of pull-backs, and componentwise comparisons for inclusions. None of these operations involves p. The prime enters only through two facts: Lang's lemma, which holds for every p, and the polarization step, which

needs 4! to be a unit, that is $p \geq 5$. So for a given monomial module, every index and every inclusion between these lattices is the same for all $p \geq 5$.

The exact computations of the proof evaluate these expressions. For a monomial module they list the orbits of π on basis vectors, on n-sets and on pairs of basis vectors; evaluate the orbit rule for every subset and every matrix unit; take the minima over splittings for products and over bijections and generators for spans of pull-backs, repeating until a span is stable when a closure under endomorphisms is wanted; and compare exponents. All arithmetic is with small integers. For the model $\mathbb{M}$ there are $\binom{8}{2} = 28$ two-sets, $\binom{8}{4} = 70$ four-sets and 64 matrix units, whose exponents $m_{ss'}$ take the value 0 twenty-eight times, 1 twenty-seven times, 2 eight times and 3 once. A reader can redo any single exponent by hand with the orbit rule, as in the examples above; the computations do this for all of them at once.

The limits of the calculus. The descent lemma uses two features of a monomial module: a basis in which $F^q = p^{q/2}\sigma^q$, which makes L_φ an intersection of finitely many lattices, and a basis permuted by F up to powers of p, which makes these lattices monomial. For a Dieudonné module that is not monomial the second feature is missing, the lattices $\varphi^j(\bigwedge^n M)$ are not monomial in a common basis, and the exponents are no longer min-plus expressions. The theorems of this companion concern monomial modules for this reason, and Chapter 15 treats all monomial supersingular modules of height 8.

Where this is used. The descent lemma and (5.2) give the index proposition for the model (Proposition 8.2) and the non-inert case of Theorem B. Proposition 5.10 gives the endomorphism proposition (Proposition 9.4) and the comparison of all monomial modules in Chapter 15.

Part III

The gap at Mumford's fourfolds

CHAPTER 6

Mumford's fourfolds

Where we are. This chapter introduces the families of abelian fourfolds whose supersingular points the theorems are about, and their integral models at a prime p. It contributes three things to the proof: the hypotheses (6.2) at p, the facts about Kisin's integral model that the next chapter uses (Fact 6.4), and the description of the lattice at p as a tensor induction (Proposition 6.7), which is what makes the Dieudonné module at a supersingular point a tensor product of three modules of rank 2. It also shows that suitable data exist for every prime $p \geq 5$ (Lemma 6.10), which is what lets Theorem C cover every such p. It needs Chapters 1 and 2, Lang's lemma (Lemma 3.5), and algebraic groups at the level of definitions: tori, reductive groups, restriction of scalars.

6.1. Mumford's families in two pages

Mumford's construction starts from a totally real cubic field k and a quaternion algebra B over k that is split at exactly one of the three real places of k and whose corestriction to $\mathbb{Q}$ is the matrix algebra $\mathrm{Mat}_8(\mathbb{Q})$ [Mum69]. The corestriction acts on $\mathbb{V} = \mathbb{Q}^8$, and the group $G \subset \mathrm{GL}(\mathbb{V})$ generated by the scalars and by the image of the elements of reduced norm 1 of B becomes, over $\overline{\mathbb{Q}}$, the image of $\mathbb{G}_m \times \mathrm{SL}_2^3$ acting on a triple tensor product $U_1 \otimes U_2 \otimes U_3$ of planes (see e.g. [SZ16, Section 2]). A Hodge structure that varies only in the first tensor factor turns $\mathbb{V}$ into the first homology of abelian fourfolds, and these fourfolds form one-dimensional families, the connected components of the Shimura curves $\mathrm{Sh}_{\mathsf{K}}(G, \mathbb{X})$. A very general member has endomorphism ring $\mathbb{Z}$, and yet its Hodge classes are governed by G, a group of dimension 10, rather than by the group of symplectic similitudes, of dimension 37. This is what makes these fourfolds a test case for questions about cycles that divisors do not answer.

At a prime p where B splits and the level is hyperspecial, as it is under the conditions (6.2) below, Kisin constructed an integral model $\mathscr{S}$ with an abelian scheme $\mathcal{A} \to \mathscr{S}$, and at every point t of characteristic p the Dieudonné module $M(\mathcal{A}_t)$ carries crystalline tensors, fixed by Frobenius, that cut out the same group G (Fact 6.4). So the structure of G at p becomes structure on $M(\mathcal{A}_t)$. The key fact is that at p the representation $\mathbb{V} \otimes \mathbb{Q}_p$ is a *tensor induction*: $B \otimes_k k_p \cong \mathrm{Mat}_2(k_p)$ acts on a plane U_p over $k_p = k \otimes \mathbb{Q}_p$, and over W the three embeddings of k_p split U_p into three planes whose tensor product is $\mathbb{V} \otimes W$. The conditions assume that the lattice $\Lambda \otimes \mathbb{Z}_p$ of the integral model is itself, up to a power of p, the tensor induction of a lattice in U_p, so that over W it is a tensor product $\Lambda_1 \otimes \Lambda_2 \otimes \Lambda_3$ of three lattices of rank 2, and Proposition 6.7 shows that the level at p is then hyperspecial. When p is inert in k, Frobenius permutes the three factors cyclically, and Chapter 7 turns this into the model $\mathbb{M}$ of (1.1).

The theorems need data (k, B, Λ) satisfying the hypotheses (6.2) at the given prime, and Lemma 6.10 constructs them for every $p \geq 5$: a cubic polynomial that is irreducible modulo p and has three real roots, and the quaternion algebra ramified exactly at two of the real places.

Example 6.1 (the data at $p = 5$). Let $k = \mathbb{Q}[x]/(x^3 - 4x + 1)$. The discriminant of $x^3 + \lambda_1 x + \lambda_0$ is $-4\lambda_1^3 - 27\lambda_0^2$, here $256 - 27 = 229$, which is positive, so the cubic $x^3 - 4x + 1$ has three real roots and k is totally real. Its values at $x = 0, 1, 2, 3, 4$ are $1, -2, 1, 16, 49$, which are $1, 3, 1, 1, 4$ modulo 5; so it has no root modulo 5, and a cubic without roots over a field is irreducible. Since 5 does not divide the discriminant 229, Dedekind's criterion applies, and 5

is inert in k: the residue field of k at 5 is $\mathbb{F}_{125}$, and $k \otimes \mathbb{Q}_5 = \mathbb{Q}_{5^3}$. Let B be the quaternion algebra over k ramified exactly at two of the three real places. Its local invariants are $\frac{1}{2}$ at those two places and 0 everywhere else, so the corestriction has invariant $\frac{1}{2}+\frac{1}{2}=0$ at the real place of $\mathbb{Q}$ and 0 at every prime, and $\mathrm{Cor}_{k/\mathbb{Q}} B \cong \mathrm{Mat}_8(\mathbb{Q})$ (see e.g. [Che25, Section 2.1.2] for this B). Since B is unramified at every finite place, it is split at the place above 5.

6.2. The group and the Shimura datum

Let k be a totally real cubic field with real embeddings $\infty_1, \infty_2, \infty_3 \colon k \to \mathbb{R}$, and B a quaternion algebra over k, a central simple k-algebra of dimension 4, with

$$B \otimes_{k,\infty_1} \mathbb{R} \cong \mathrm{Mat}_2(\mathbb{R}), \qquad B \otimes_{k,\infty_2} \mathbb{R} \cong B \otimes_{k,\infty_3} \mathbb{R} \cong \mathbb{H},$$

where $\mathbb{H}$ is Hamilton's quaternion algebra. The *corestriction* $\mathrm{Cor}_{k/\mathbb{Q}} B$ is a central simple $\mathbb{Q}$-algebra of dimension $4^3 = 64$ which over $\overline{\mathbb{Q}}$ is the tensor product of the three algebras $B \otimes_{k,\tau} \overline{\mathbb{Q}}$, one for each embedding $\tau \colon k \to \overline{\mathbb{Q}}$; it comes with a multiplicative map $\mathrm{Cor} \colon B \to \mathrm{Cor}_{k/\mathbb{Q}} B$, which over $\overline{\mathbb{Q}}$ sends x to the tensor product of its three images. Mumford's condition is $\mathrm{Cor}_{k/\mathbb{Q}} B \cong \mathrm{Mat}_8(\mathbb{Q})$. It holds for the quaternion algebra B ramified exactly at ∞_2 and ∞_3 (see e.g. [Che25, Section 2.1.2]), which is the only case the proofs use. In general, the local invariants of $\mathrm{Cor}_{k/\mathbb{Q}} B$ are the sums of those of B at the places above, a standard property of corestriction that the companion uses only in Exercise 6.2 and does not prove.

Fix such an isomorphism, so that $\mathrm{Cor}_{k/\mathbb{Q}} B$ acts on $\mathbb{V} = \mathbb{Q}^8$. Let B^1 be the algebraic group over $\mathbb{Q}$ of elements of B of reduced norm 1, that is, the group $\mathrm{Res}_{k/\mathbb{Q}} \mathrm{SL}_1(B)$. Mumford's group $G \subset \mathrm{GL}(\mathbb{V})$ is the algebraic subgroup generated by the scalars $\mathbb{G}_m$ and by $\mathrm{Cor}(B^1)$. After extending scalars to $\overline{\mathbb{Q}}$, $B \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} \cong \mathrm{Mat}_2(\overline{\mathbb{Q}})^3$, B^1 becomes SL_2^3, $\mathbb{V} \otimes \overline{\mathbb{Q}}$ becomes $U_1 \otimes U_2 \otimes U_3$ with $U_i = \overline{\mathbb{Q}}^2$ the standard representation of the i-th factor, and

$$G_{\overline{\mathbb{Q}}} = \text{image of } \ \mathbb{G}_m \times \mathrm{SL}_2^3 \to \mathrm{GL}(U_1 \otimes U_2 \otimes U_3), \qquad (\lambda, \gamma_1, \gamma_2, \gamma_3) \mapsto \lambda\gamma_1 \otimes \gamma_2 \otimes \gamma_3.$$

Every element of GL_2^3 is a scalar times an element of SL_2 in each factor, over $\overline{\mathbb{Q}}$, so $G_{\overline{\mathbb{Q}}}$ is also the image of GL_2^3 under $(\gamma_1, \gamma_2, \gamma_3) \mapsto \gamma_1 \otimes \gamma_2 \otimes \gamma_3$. The kernel of this map is the torus of triples of scalars with product 1 (Exercise 6.1), so G has dimension $3 \cdot 4 - 2 = 10$.

Example 6.2 (the eight weights). Let e_i^+, e_i^- be the standard basis of U_i, and let the diagonal torus of SL_2^3 act by $\mathrm{diag}(\lambda_i, \lambda_i^{-1})$ on U_i. For a sign vector $\epsilon = (\epsilon_1, \epsilon_2, \epsilon_3) \in \{\pm\}^3$ the vector $e^\epsilon = e_1^{\epsilon_1} \otimes e_2^{\epsilon_2} \otimes e_3^{\epsilon_3}$ is an eigenvector with eigenvalue $\lambda_1^{\epsilon_1}\lambda_2^{\epsilon_2}\lambda_3^{\epsilon_3}$, where $\lambda_i^{\pm}$ means $\lambda_i^{\pm 1}$. The eight characters $\lambda_1^{\pm 1}\lambda_2^{\pm 1}\lambda_3^{\pm 1}$ are pairwise distinct, so $U_1 \otimes U_2 \otimes U_3$ is the sum of eight weight lines indexed by $\{\pm\}^3$. In Chapter 12 a torus of G defined over $\mathbb{Q}$ acts through these eight characters, and the Galois group permutes the sign vectors; the cube $\{0,1\}^3$ of the model $\mathbb{M}$ is the same set of eight vectors in other coordinates.

Exercise 6.1. Show that $\gamma_1 \otimes \gamma_2 \otimes \gamma_3 = 1$ on $U_1 \otimes U_2 \otimes U_3$, for $\gamma_i \in \mathrm{GL}_2$, holds exactly when $\gamma_i = \lambda_i \cdot 1$ with $\lambda_1\lambda_2\lambda_3 = 1$. Deduce that the kernel of $\mathrm{GL}_2^3 \to \mathrm{GL}_8$ is a split torus of dimension 2.

Exercise 6.2. Let B be ramified exactly at the set $\mathrm{Ram}(B)$ of places of k, with $\infty_1 \notin \mathrm{Ram}(B)$. Granting that corestriction adds local invariants, show that $\mathrm{Cor}_{k/\mathbb{Q}} B \cong \mathrm{Mat}_8(\mathbb{Q})$ if and only if, for every place v of $\mathbb{Q}$, the number of places of $\mathrm{Ram}(B)$ above v is even. Check that this holds when $\mathrm{Ram}(B) = \{\infty_2, \infty_3\}$, and give an example of a set $\mathrm{Ram}(B)$ containing finite places for which it holds.

The Hodge structures. Over $\mathbb{R}$, the group of reduced norm 1 elements is $B^1(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R}) \times \mathbb{H}^1 \times \mathbb{H}^1$, where $\mathbb{H}^1 \cong \mathrm{SU}(2)$ is compact, and G is the image of $\mathbb{G}_m \times B^1$. Let $u_0 \colon S^1 \to B^1(\mathbb{R})$, on the circle $S^1 = \{z \in \mathbb{C} : z\bar{z} = 1\}$, be 1 at the two ramified real places and, at ∞_1, the restriction to S^1 of the embedding $\mathbb{C} \to \mathrm{Mat}_2(\mathbb{R})$, $x + iy \mapsto \left(\begin{smallmatrix} x & y \\ -y & x \end{smallmatrix}\right)$. The map $(r, z) \mapsto (r, u_0(z))$ on $\mathbb{R}^\times \times S^1$ induces a homomorphism $\mathbf{h} = \mathbf{h}_0 \colon \mathbb{C}^\times \to G(\mathbb{R})$, and $\mathbb{X}$ is its $G(\mathbb{R})$-conjugacy class (see e.g. [SZ16, Section 2]). So $\mathbf{h}$ is non-trivial only in the

factor of ∞_1, where it acts on the real plane $U_1(\mathbb{R})$ through the complex structure of $\mathbb{C} = \mathbb{R}^2$. Then $\mathcal{J} = \mathbf{h}(\mathrm{i})$ is a complex structure on $\mathbb{V}_\mathbb{R}$ with $\mathcal{J}^2 = -1$, and $\mathbb{V}_\mathbb{R}/L$ is a complex torus of dimension 4 for every lattice $L \subset \mathbb{V}$. The $G(\mathbb{R})$-conjugacy class $\mathbb{X}$ of $\mathbf{h}$ is a union of two copies of the upper half-plane: only the factor of ∞_1 moves $\mathbf{h}$; there $\mathrm{SL}_2(\mathbb{R})$ moves it within one copy, and the element $\mathrm{diag}(1,-1) \otimes 1 \otimes 1$ of $G(\mathbb{R})$ conjugates $\mathbf{h}$ to $z \mapsto \mathbf{h}(\bar{z})$, which lies in the other copy. The pair $(G, \mathbb{X})$ is a Shimura datum, and the Shimura varieties $\mathrm{Sh}_\mathsf{K}(G,\mathbb{X}) = G(\mathbb{Q})\backslash\mathbb{X} \times G(\mathbb{A}_f)/\mathsf{K}$ are curves. Mumford's families are the abelian schemes over their connected components.

The symplectic form. The second exterior power of a tensor product decomposes as $\bigwedge^2(U \otimes U') \cong \bigwedge^2 U \otimes \mathrm{Sym}^2 U' \oplus \mathrm{Sym}^2 U \otimes \bigwedge^2 U'$. Applying this twice, with $\bigwedge^2 U_i$ the trivial representation of SL_2,

$$\bigwedge^2(U_1 \otimes U_2 \otimes U_3) \cong \mathbf{1} \oplus \mathrm{Sym}^2 U_2 \otimes \mathrm{Sym}^2 U_3 \oplus \mathrm{Sym}^2 U_1 \otimes \mathrm{Sym}^2 U_2 \oplus \mathrm{Sym}^2 U_1 \otimes \mathrm{Sym}^2 U_3, \tag{6.1}$$

of dimensions $1+9+9+9 = 28$. So the SL_2^3-invariant alternating forms on $\mathbb{V} \otimes \overline{\mathbb{Q}}$ form a line, spanned by the tensor product of the three determinant forms of the U_i, and since this line is defined over $\mathbb{Q}$ it contains a nonzero rational form ψ. Hence $G \subset \mathrm{GSp}(\mathbb{V}, \psi)$, and ψ is unique up to a scalar. With the appropriate sign, ψ is a Riemann form for the complex structures of $\mathbb{X}$, that is, $(G, \mathbb{X})$ maps to the Siegel datum of $(\mathbb{V}, \psi)$ (see e.g. [SZ16, Section 2]), so that the complex tori $\mathbb{V}_\mathbb{R}/L$ are abelian fourfolds.

The reflex field. The cocharacter $z \mapsto \mathbf{h}_\mathbb{C}(z, 1)$ attached to $\mathbf{h}$ is non-trivial only in the tensor factor of ∞_1. An automorphism of $\mathbb{C}$ permutes the three factors as it permutes the embeddings of k, so it preserves the conjugacy class of the cocharacter exactly when it fixes $\infty_1(k)$. The reflex field of $(G, \mathbb{X})$ is therefore $\infty_1(k) \cong k$.

Exercise 6.3. A cocharacter of $G_\mathbb{C}$ has the form $z \mapsto z^{n_0}\mathrm{diag}(z^{n_1}, z^{-n_1}) \otimes \mathrm{diag}(z^{n_2}, z^{-n_2}) \otimes \mathrm{diag}(z^{n_3}, z^{-n_3})$ in suitable bases, with $n_0, n_i \in \frac{1}{2}\mathbb{Z}$ and $n_i \geq 0$ for $i = 1, 2, 3$. Show that its weights on $U_1 \otimes U_2 \otimes U_3$ take exactly two values differing by 1, each four times, as they must for the Hodge structure of an abelian fourfold, if and only if exactly one of n_1, n_2, n_3 is non-zero and it equals $\frac{1}{2}$. For the cocharacter attached to Mumford's $\mathbf{h}$, which factor has $n_i \neq 0$?

6.3. Very general members and the exceptional classes

A very general member X_{gen} of Mumford's families, one outside a countable union of proper analytic subsets of the base, has $\mathrm{End}(X_{\mathrm{gen}}) = \mathbb{Z}$ [Mum69, Section 4], and its Hodge group is a $\mathbb{Q}$-form of an almost direct product of three copies of SL_2 [MZ99], much smaller than the symplectic group of $(\mathbb{V}, \psi)$. So the endomorphisms and the polarization do not determine which classes on powers of X_{gen} are Hodge classes. Moonen and Zarhin showed that the self-product $X_{\mathrm{gen}} \times X_{\mathrm{gen}}$ carries Hodge classes in $H^4(X_{\mathrm{gen}} \times X_{\mathrm{gen}}, \mathbb{Q})$ that are not in the span of products of divisor classes [MZ99]. By the count in the intuition box below, two of them, independent modulo that span, lie in the Künneth component $H^2(X_{\mathrm{gen}}) \otimes H^2(X_{\mathrm{gen}})$. What the theorems of this companion imply for them, and what they do not imply, is the subject of Remark 14.3.

Intuition 6.3 (why there are two exceptional classes). The Hodge group of a very general X_{gen} is a $\mathbb{Q}$-form of an almost direct product of three copies of SL_2 [MZ99], which by Mumford's construction acts on H^1 through $U_1 \otimes U_2 \otimes U_3$, and the Hodge classes in tensor constructions on $H^1(X_{\mathrm{gen}}, \mathbb{Q})$ are the invariants of the Hodge group. By (6.1), $H^2(X_{\mathrm{gen}}, \overline{\mathbb{Q}})$ is a sum of four pairwise non-isomorphic irreducible representations of SL_2^3, so the invariants in $H^2 \otimes H^2$, which is $\mathrm{End}(H^2)$ up to duality, form a space of dimension 4. Divisor classes on $X_{\mathrm{gen}} \times X_{\mathrm{gen}}$ come from the invariant line of each factor $H^2(X_{\mathrm{gen}})$ and from the invariant line of $H^1 \otimes H^1$, and their products contribute two dimensions to $H^2 \otimes H^2$: the product of the two polarizations and the component of the square of the

class of $H^1 \otimes H^1$. So four Hodge classes and two products of divisors: two classes are exceptional.

6.4. The integral model

Fix a lattice $\Lambda \subset \mathbb{V}$ on which ψ is integral, a prime p, and a level $\mathsf{K} = \mathsf{K}_p\mathsf{K}^p \subset G(\mathbb{A}_f)$ in which K_p is the stabilizer of $\Lambda \otimes \mathbb{Z}_p$ in $G(\mathbb{Q}_p)$ and K^p is a neat compact open subgroup of $G(\mathbb{A}_f^p)$. Kisin constructed an integral model $\mathscr{S}$ of $\mathrm{Sh}_{\mathsf{K}}(G, \mathbb{X})$ over the localization at a prime above p of the ring of integers of the reflex field, together with an abelian scheme $\mathcal{A} \to \mathscr{S}$ that extends the family on the generic fiber [Kis10]. For a point $t \in \mathscr{S}(\bar{\mathbb{F}}_p)$ we write $\mathcal{A}_t$ for the abelian fourfold over $\bar{\mathbb{F}}_p$ at t. The theorems assume the following conditions at p:

(6.2)
$$\text{(h1)}\ \ p \geq 5; \qquad \text{(h2)}\ \ p \text{ is inert in } k; \qquad \text{(h3)}\ \ B \otimes_k k_p \cong \mathrm{Mat}_2(k_p);$$
$$\text{(h4)}\ \ \Lambda \otimes \mathbb{Z}_p = p^j \,\mathrm{Cor}(\Lambda_0) \text{ for a } \mathbb{Z}_{p^3}\text{-lattice } \Lambda_0 \subset U_p \text{ and some } j \in \mathbb{Z}.$$

Under (h2), $k_p = k \otimes \mathbb{Q}_p$ is the unramified cubic extension $\mathbb{Q}_{p^3}$ of $\mathbb{Q}_p$, and the reflex field has a single prime above p, with residue field $\mathbb{F}_{p^3}$. Condition (h3) says that B is split at that prime; then $B \otimes_k k_p$ acts on a plane U_p over k_p and $\mathbb{V} \otimes \mathbb{Q}_p$ is its tensor induction $\mathrm{Cor}(U_p)$, which is explained, together with the tensor induction $\mathrm{Cor}(\Lambda_0)$ of a lattice, in Section 6.5. Condition (h4) says that the lattice at p is, up to a power of p, such a tensor induction. By Proposition 6.7, (h4) implies that the closure of G in $\mathrm{GL}(\Lambda \otimes \mathbb{Z}_{(p)})$ is reductive, so that K_p is a hyperspecial subgroup of $G(\mathbb{Q}_p)$. For fixed (k, B, Λ), conditions (h3) and (h4) hold for all but finitely many p, and for every prime $p \geq 5$ some data satisfy all four conditions (Lemma 6.10).

The group G is cut out by tensors. Kisin chooses finitely many tensors $\mathfrak{t}_i$ in spaces built from $\Lambda \otimes \mathbb{Z}_{(p)}$ and its dual by tensor products, whose common stabilizer in $\mathrm{GL}(\Lambda \otimes \mathbb{Z}_{(p)})$ is the closure of G. At each point the abelian variety carries realizations of these tensors in its cohomology, and the following statements say how they look in crystalline cohomology at a point of characteristic p.

Fact 6.4 (Kisin's integral model). *Assume (h1)–(h4), so that $p \geq 5$ and K_p is hyperspecial (Proposition 6.7).*

(a) Every $t \in \mathscr{S}(\bar{\mathbb{F}}_p)$ lifts to a point of $\mathscr{S}$ with values in the ring of integers of a finite extension of $W[1/p]$.

(b) For $t \in \mathscr{S}(\bar{\mathbb{F}}_p)$ there are tensors $\mathfrak{t}_{i,0}$ in the tensor spaces of $M(\mathcal{A}_t)$, fixed by Frobenius, and an isomorphism $M(\mathcal{A}_t) \cong \Lambda^\vee \otimes W$ that carries each $\mathfrak{t}_{i,0}$ to $\mathfrak{t}_i \otimes 1$.

(c) The tensors $\mathfrak{t}_{i,0}$ correspond to the p-adic étale realizations of the $\mathfrak{t}_i$ on a lift under the p-adic comparison isomorphism, which is functorial; so an endomorphism of a lift of $\mathcal{A}_t$ that fixes the étale realizations reduces to an endomorphism of $\mathcal{A}_t$ that fixes the $\mathfrak{t}_{i,0}$.

(d) A point of $\mathrm{Sh}_{\mathsf{K}}(G, \mathbb{X})$ defined over a number field, whose abelian variety has good reduction at a prime above p, extends to a point of $\mathscr{S}$ over the localization of the ring of integers at that prime.

(e) An abelian variety with complex multiplication over a number field has potentially good reduction: it acquires good reduction at every prime after a finite extension of the field.

For (a), $\mathscr{S}$ is smooth [Kis10], so t lifts. Statement (b) is in [KP18, Section 4.2], which works at parahoric level, including hyperspecial level. For (c), the correspondence between crystalline and étale tensors is [KP18, p. 4.2.1], and for the functoriality of the comparison isomorphism see e.g. [Mad19, Remark 3.3.10]. For (d), $\mathscr{S}$ is the normalization of the closure of $\mathrm{Sh}_{\mathsf{K}}(G, \mathbb{X})$ in the moduli scheme of polarized abelian schemes with prime-to-p level structure [Kis10, (2.3.3) and Theorem (2.3.8)], hence finite over that closure, which is of finite type over a Dedekind domain of characteristic 0 (see e.g. [The, Tags 0335 and 035S]); the point extends to the moduli scheme by the Néron property (see e.g. [Mil08, Chapter I, Remark 17.2]), and then to $\mathscr{S}$ because a finite morphism satisfies the valuative criterion. For (e) see e.g. [Mil05,

Proposition 10.5], which is stated for complex multiplication by a CM field and is applied to the simple isogeny factors.

Intuition 6.5 (what the tensors buy). The isomorphism of Fact 6.4(b) is not compatible with Frobenius: Frobenius on $M(\mathcal{A}_t)$ is some σ-semilinear map, unknown a priori. What is known is that it fixes the tensors, and these cut out G. So in the basis given by (b), Frobenius is an element of $G(W[1/p])$ composed with the standard σ-semilinear map. All supersingular points of the family are then controlled by one group-theoretic question, which Chapter 7 answers.

6.5. The lattice at p is a tensor induction

Assume (h2) and (h3). Then $k_p = \mathbb{Q}_{p^3}$, its ring of integers is $\mathbb{Z}_{p^3}$, and there are three embeddings $\tau_1, \tau_2, \tau_3 \colon \mathbb{Z}_{p^3} \to W$, which we number so that $\tau_2 = \sigma \circ \tau_1$ and $\tau_3 = \sigma \circ \tau_2$; then $\sigma \circ \tau_3 = \tau_1$. The algebra $B \otimes_k k_p \cong \mathrm{Mat}_2(k_p)$ acts on a plane U_p over k_p, unique up to isomorphism.

Definition 6.6 (tensor induction). Let $\Lambda_0 \subset U_p$ be a $\mathbb{Z}_{p^3}$-lattice, and put $\Lambda_i = \Lambda_0 \otimes_{\mathbb{Z}_{p^3},\tau_i} W$ for $i = 1, 2, 3$, three free W-modules of rank 2. The map $x \otimes \lambda \mapsto x \otimes \sigma(\lambda)$ is a σ-semilinear bijection $\Lambda_i \to \Lambda_{i+1}$, indices modulo 3, which we also write σ. The *slot permutation* is the σ-semilinear bijection

$$\varsigma \colon \Lambda_1 \otimes \Lambda_2 \otimes \Lambda_3 \to \Lambda_1 \otimes \Lambda_2 \otimes \Lambda_3, \qquad \varsigma(x_1 \otimes x_2 \otimes x_3) = \sigma x_3 \otimes \sigma x_1 \otimes \sigma x_2,$$

and the *tensor induction* of Λ_0 is the $\mathbb{Z}_p$-module $\mathrm{Cor}(\Lambda_0)$ of its fixed vectors.

By Lang's lemma (Lemma 3.5), $\mathrm{Cor}(\Lambda_0)$ is free of rank 8 over $\mathbb{Z}_p$ and $\mathrm{Cor}(\Lambda_0) \otimes_{\mathbb{Z}_p} W = \Lambda_1 \otimes \Lambda_2 \otimes \Lambda_3$. A basis e_0', e_1' of Λ_0 gives bases $e_0' \otimes 1, e_1' \otimes 1$ of all three Λ_i, and in these bases $\sigma \colon \Lambda_i \to \Lambda_{i+1}$ is σ applied to coordinates; we call such bases *related by* σ. The space $\mathrm{Cor}(U_p) = \mathrm{Cor}(\Lambda_0) \otimes \mathbb{Q}$ does not depend on Λ_0, the algebra $\mathrm{Mat}_2(k_p)$ acts on it through the norm map, and $\mathbb{V} \otimes \mathbb{Q}_p \cong \mathrm{Cor}(U_p)$, because $\mathrm{Cor}_{k/\mathbb{Q}} B \otimes \mathbb{Q}_p$ is the corestriction of $\mathrm{Mat}_2(k_p)$ and has a unique simple module. An element $\gamma \in \mathrm{GL}_2(k_p)$ acts on $\mathrm{Cor}(U_p)$ by $\mathrm{Cor}(\gamma)$, which over W is $\gamma_1 \otimes \gamma_2 \otimes \gamma_3$ with γ_i the image of γ under τ_i; it lies in $G(\mathbb{Q}_p)$, because it lies in $G(\overline{\mathbb{Q}}_p)$ and in $\mathrm{GL}(\mathbb{V} \otimes \mathbb{Q}_p)$.

Proposition 6.7 (the hyperspecial lattice). *Assume (h2)–(h4), and let $\mathcal{G}$ be the closure of G in $\mathrm{GL}(\Lambda \otimes \mathbb{Z}_{(p)})$. Then:*

(a) $\Lambda \otimes W = p^j \Lambda_1 \otimes \Lambda_2 \otimes \Lambda_3$, and $\Lambda^\vee \otimes \mathbb{Z}_p = p^{-j}\,\mathrm{Cor}(\Lambda_0^\vee)$ for the dual lattice $\Lambda_0^\vee$ of Λ_0, so that the statements below hold for $\Lambda^\vee$ with Λ_0 replaced by $\Lambda_0^\vee$;

(b) $\mathcal{G}$ is reductive, and over W it is the image of GL_2^3 acting on $\Lambda_1 \otimes \Lambda_2 \otimes \Lambda_3$, that is, $\mathbb{G}_m \cdot \mathrm{SL}_2^3$; in particular K_p is hyperspecial;

(c) $G(W[1/p])$ is the image of $\mathrm{GL}_2(W[1/p])^3$, and the stabilizer $G(W)$ of $\Lambda \otimes W$ in $G(W[1/p])$ is the image of $\mathrm{GL}_2(W)^3$, under $(\gamma_1, \gamma_2, \gamma_3) \mapsto \gamma_1 \otimes \gamma_2 \otimes \gamma_3$;

(d) the W-lattices in $\Lambda \otimes W[1/p]$ that are stable under $G(W)$ are the $c(\Lambda \otimes W)$, $c \in W[1/p]^\times$.

Proof. *Step 1: the kernel torus.* Over $W[1/p]$, $k_p \otimes_{\mathbb{Q}_p} W[1/p] \cong W[1/p]^3$ through the τ_i, so $G_{W[1/p]}$ is the image of GL_2^3 acting on $\mathrm{Cor}(U_p) \otimes W[1/p] = \bigotimes_i U_p \otimes_{k_p,\tau_i} W[1/p]$. The kernel $\mathbb{T}'$ of $\mathrm{GL}_2^3 \to \mathrm{GL}_8$ is the split torus of triples of scalars $(\lambda_1, \lambda_2, \lambda_3)$ with $\lambda_1\lambda_2\lambda_3 = 1$ (Exercise 6.1). From the exact sequence $1 \to \mathbb{T}' \to \mathrm{GL}_2^3 \to G_{W[1/p]} \to 1$ and Hilbert's Theorem 90, $H^1(W[1/p], \mathbb{T}') = 0$ for the split torus $\mathbb{T}' \cong \mathbb{G}_m^2$, every element of $G(W[1/p])$ comes from $\mathrm{GL}_2(W[1/p])^3$. This is the first half of (c). Statement (a) is (h4) after extending scalars to W, together with $\mathrm{Cor}(\Lambda_0)^\vee = \mathrm{Cor}(\Lambda_0^\vee)$, which holds because over W the dual of $\Lambda_1 \otimes \Lambda_2 \otimes \Lambda_3$ is $\Lambda_1^\vee \otimes \Lambda_2^\vee \otimes \Lambda_3^\vee$.

Step 2: the stabilizer. Let $\gamma = \gamma_1 \otimes \gamma_2 \otimes \gamma_3$ with $\gamma_i \in \mathrm{GL}_2(W[1/p])$ preserve $\Lambda_1 \otimes \Lambda_2 \otimes \Lambda_3$. Write $\gamma_i = \gamma_i' \mathrm{diag}(p^{n_i}, p^{n_i'}) \gamma_i''$ with $\gamma_i', \gamma_i'' \in \mathrm{GL}_2(W)$ (elementary divisors). Then the elementary divisors of γ are p to the eight sums $l_1 + l_2 + l_3$, $l_i \in \{n_i, n_i'\}$, and they are all p^0

because $\gamma \in \mathrm{GL}_8(W)$. This forces $n_i = n_i'$ for each i and $n_1+n_2+n_3 = 0$, so $\gamma_i = p^{n_i}\gamma_i'\gamma_i''$ and $\gamma = (p^{n_1}\gamma_1'\gamma_1'') \otimes (p^{n_2}\gamma_2'\gamma_2'') \otimes (p^{n_3}\gamma_3'\gamma_3'')$ with $\sum n_i = 0$, which is also $(\gamma_1'\gamma_1'') \otimes (\gamma_2'\gamma_2'') \otimes (\gamma_3'\gamma_3'')$. So the stabilizer of $\Lambda_1 \otimes \Lambda_2 \otimes \Lambda_3$ in $G(W[1/p])$ is the image of $\mathrm{GL}_2(W)^3$, and by (a) so is the stabilizer of $\Lambda \otimes W$. This is the second half of (c).

Step 3: the closure is reductive. The map $\mathrm{GL}_{2,W}^3 \to \mathrm{GL}(\Lambda \otimes W)$ has kernel the split torus $\mathbb{T}'$ over W, as one sees by comparing matrix entries of $\gamma_1 \otimes \gamma_2 \otimes \gamma_3$, so it induces a monomorphism of the reductive group scheme $\mathrm{GL}_{2,W}^3/\mathbb{T}'$ into $\mathrm{GL}(\Lambda \otimes W)$. A monomorphism of a reductive group scheme into a separated group scheme is a closed immersion [DG70, Exp. XVI, Corollaire 1.5(a)]. Its image is therefore a closed subgroup scheme, flat over W, with generic fiber $G_{W[1/p]}$; so it is the closure of $G_{W[1/p]}$ in $\mathrm{GL}(\Lambda \otimes W)$. This closure is $\mathcal{G}_W$, because forming the closure commutes with the flat base change $\mathbb{Z}_{(p)} \to W$ (see e.g. [The, Tag 081I]). So $\mathcal{G}_W$ is the reductive group $\mathrm{GL}_{2,W}^3/\mathbb{T}' = \mathbb{G}_m \cdot \mathrm{SL}_2^3$, and with it $\mathcal{G}$ is reductive. Its group of $\mathbb{Z}_p$-points, the stabilizer K_p of $\Lambda \otimes \mathbb{Z}_p$, is then a hyperspecial subgroup. This is (b).

Step 4: stable lattices. The reduction of $\Lambda_1 \otimes \Lambda_2 \otimes \Lambda_3$ modulo p is the external tensor product of the three standard representations of $\mathrm{SL}_2(\bar{\mathbb{F}}_p)^3$, which is irreducible (Exercise 6.5), and $\mathrm{GL}_2(W) \to \mathrm{GL}_2(\bar{\mathbb{F}}_p)$ is surjective. Let L be a $G(W)$-stable lattice, scaled by an element of $W[1/p]^\times$ so that $L \subseteq \Lambda \otimes W$ and $L \not\subseteq p(\Lambda \otimes W)$. Its image modulo p is a nonzero subspace stable under $\mathrm{SL}_2(\bar{\mathbb{F}}_p)^3$, hence everything, and by Nakayama's lemma $L = \Lambda \otimes W$. This is (d). □

Remark 6.8 (why (h4) is a hypothesis). Hyperspecial subgroups of $G(\mathbb{Q}_p)$ can also be described through the Bruhat–Tits building of G, and one could start from the assumption that K_p is hyperspecial. The proof uses the explicit form (h4) of the lattice, and Proposition 6.7 shows that it implies hyperspeciality. Lemma 6.10 shows that (h4) costs nothing for the theorems: it holds for all but finitely many p, and it can be arranged at every $p \geq 5$.

Exercise 6.4. Let p be a prime, $U = \bar{\mathbb{F}}_p^2$ with standard basis e^+, e^-, and let $\mathrm{SL}_2(\mathbb{F}_{p^3})$ act on $U \otimes U \otimes U$ by $\gamma \mapsto \gamma \otimes \gamma^{(p)} \otimes \gamma^{(p^2)}$, with basis vectors $e^\epsilon = e^{\epsilon_1} \otimes e^{\epsilon_2} \otimes e^{\epsilon_3}$. Let N_i be the nilpotent map $e^- \mapsto e^+$, $e^+ \mapsto 0$ in slot i and $\mathsf{N}_J = \prod_{i \in J} \mathsf{N}_i$ for $J \subseteq \{1,2,3\}$.

(a) Show that $\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right)$, $x \in \mathbb{F}_{p^3}$, acts as $\sum_J x^{l_J} \mathsf{N}_J$ with $l_J = \sum_{i \in J} p^{i-1}$, and that the eight exponents l_J are distinct and smaller than p^3.

(b) Using that a nonzero polynomial of degree less than p^3 cannot vanish on all of $\mathbb{F}_{p^3}$, show that an invariant subspace $\mathcal{U}$ satisfies $\mathsf{N}_J\mathcal{U} \subseteq \mathcal{U}$ for every J. Deduce that a nonzero $\mathcal{U}$ contains e^{+++}, and, with the lower unipotent matrices, every e^ϵ. So the representation is irreducible.

(c) Let p be unramified but not inert in k, and let $\mathrm{SL}_2(O_k/p)$ act on $U \otimes U \otimes U$ through the reductions of the three embeddings $\tau_i \colon O_k \otimes \mathbb{Z}_p \to W$. Adapt (a) and (b) to show that this representation is irreducible as well.

Remark 6.9 (stable lattices under a finite group). Already the finite group $\mathrm{SL}_2(\mathbb{F}_{p^3})$, acting through $\gamma \mapsto \mathrm{Cor}(\gamma)$ modulo p, acts irreducibly on $(\Lambda_1 \otimes \Lambda_2 \otimes \Lambda_3)/p$ (Exercise 6.4). The same Nakayama argument as in Step 4 then shows that the $\mathbb{Z}_p$-lattices in $\mathrm{Cor}(U_p)$ stable under $\mathrm{Cor}(\mathrm{SL}_2(\mathbb{Z}_{p^3}))$ are the $p^j\,\mathrm{Cor}(\Lambda_0)$. This is not used in the proofs.

Exercise 6.5. Let e_i^+, e_i^- be the standard basis of $U_i = \bar{\mathbb{F}}_p^2$. Show that $U_1 \otimes U_2 \otimes U_3$ is irreducible under $\mathrm{SL}_2(\bar{\mathbb{F}}_p)^3$: first, using the diagonal torus and Example 6.2, that an invariant subspace is a sum of the lines $\bar{\mathbb{F}}_p e^\epsilon$; then, using the unipotent matrices $\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ x & 1 \end{smallmatrix}\right)$ in one factor at a time, that an invariant subspace containing one e^ϵ contains all of them.

What just happened. At a prime where B splits, the 8-dimensional representation $\mathbb{V} \otimes \mathbb{Q}_p$ is the tensor induction of a plane U_p over k_p, and (h4) asks that the lattice of the integral model be, up to a power of p, the tensor induction of a lattice Λ_0 in that plane, which makes the level hyperspecial. Over W this is a tensor product $\Lambda_1 \otimes \Lambda_2 \otimes \Lambda_3$ of

three lattices of rank 2, the group G becomes GL_2^3 modulo a torus, and σ acts by the slot permutation ς, which moves each factor to the next one.

6.6. Data for every prime

LEMMA 6.10 (data for every prime). *For fixed (k, B, Λ), (h3) and (h4) hold for all but finitely many p. For every prime $p \geq 5$ there are $(k, B, \Lambda, \mathsf{K}^p)$ as above satisfying (h1)–(h4).*

PROOF. *All but finitely many p.* Fix a maximal order $\mathcal{O}_B \subset B$, and let $\mathrm{Nm}\colon B \to \mathrm{Cor}_{k/\mathbb{Q}} B = \mathrm{End}(\mathbb{V})$ be the norm map of Section 6.2, a homogeneous polynomial map of degree 3 defined over $\mathbb{Q}$. For all but finitely many p: p is unramified in k; B is split at the places above p, which is (h3), so that $\mathcal{O}_B \otimes \mathbb{Z}_p = \mathrm{End}_{O_{k_p}}(\Lambda_0)$ for an O_{k_p}-lattice $\Lambda_0 \subset U_p$; and $\mathrm{Nm}(\mathcal{O}_B \otimes \mathbb{Z}_p)$ preserves $\Lambda \otimes \mathbb{Z}_p$, because the coefficients of Nm in a $\mathbb{Z}$-basis of $\mathcal{O}_B$ are finitely many elements of $\mathrm{End}(\mathbb{V})$, all integral on $\Lambda \otimes \mathbb{Z}_p$ for almost all p. Over W, Nm becomes $(x_1, x_2, x_3) \mapsto x_1 \otimes x_2 \otimes x_3$ on $\mathrm{Mat}_2(W)^3$. Its polarization is trilinear, its values on $\mathcal{O}_B \otimes \mathbb{Z}_p$ are integral combinations of values of Nm, and it takes the value $x_1 \otimes x_2 \otimes x_3$ at $(x_1, 0, 0)$, $(0, x_2, 0)$, $(0, 0, x_3)$ (Exercise 6.6). So the W-span of $\mathrm{Nm}(\mathcal{O}_B \otimes \mathbb{Z}_p)$ is $\mathrm{End}_W(\mathrm{Cor}(\Lambda_0) \otimes W)$, and as W is faithfully flat over $\mathbb{Z}_p$, the $\mathbb{Z}_p$-span is $\mathrm{End}_{\mathbb{Z}_p}(\mathrm{Cor}\,\Lambda_0) \cong \mathrm{Mat}_8(\mathbb{Z}_p)$. The lattices stable under $\mathrm{End}_{\mathbb{Z}_p}(\mathrm{Cor}\,\Lambda_0)$ are the $p^j \mathrm{Cor}(\Lambda_0)$, $j \in \mathbb{Z}$, which gives (h4).

The field. Every irreducible cubic over $\mathbb{F}_p$ can be brought to the form $x^3 + \lambda_1 x + \lambda_0$ by a substitution $x \mapsto x - \lambda$, since $3 \in \mathbb{F}_p^\times$. Choose integers λ_1, λ_0 with $x^3 + \lambda_1 x + \lambda_0$ irreducible modulo p. Changing λ_1 by a multiple of p, we may assume that $\lambda_1 < 0$ and $|\lambda_1|$ is so large that the discriminant $-4\lambda_1^3 - 27\lambda_0^2$ is positive. Then $Q = x^3 + \lambda_1 x + \lambda_0$ is irreducible over $\mathbb{Q}$, because it is irreducible modulo p, and it has three real roots. An irreducible polynomial over a finite field is separable, so p does not divide the discriminant of Q, hence not the index of $\mathbb{Z}[x]/(Q)$ in the ring of integers of $k = \mathbb{Q}[x]/(Q)$, and by Dedekind's criterion p is inert in k: this is (h2).

The quaternion algebra. For every finite set of real and finite places of k of even cardinality there is a quaternion algebra over k ramified exactly there (see e.g. [Voi21, Main Theorem 14.6.1]). Let B be ramified exactly at ∞_2 and ∞_3. Then B is split at exactly one real place and at every finite place, in particular at the prime above p, which is (h3), and $\mathrm{Cor}_{k/\mathbb{Q}} B \cong \mathrm{Mat}_8(\mathbb{Q})$ (see e.g. [Che25, Section 2.1.2]). (h1) is the assumption $p \geq 5$.

The lattice. The group $G_{\mathbb{Q}_p}$ is unramified, so it has hyperspecial subgroups (see e.g. [Mil05, Section 16]). Concretely, take $\Lambda_p = \mathrm{Cor}(\Lambda_0)$ for a $\mathbb{Z}_{p^3}$-lattice $\Lambda_0 \subset U_p$, extend Λ_p to a lattice $\Lambda \subset \mathbb{V}$ with $\Lambda \otimes \mathbb{Z}_p = \Lambda_p$, rescale ψ so that it is integral on Λ, and choose any neat K^p. Then (h4) holds with $j = 0$. □

EXERCISE 6.6. Let $N(u) = u_1 \otimes u_2 \otimes u_3$ for $u = (u_1, u_2, u_3) \in \mathrm{Mat}_2(W)^3$, and put $T(u, v, w) = N(u + v + w) - N(u + v) - N(u + w) - N(v + w) + N(u) + N(v) + N(w)$. Show that T is W-trilinear and symmetric, that $T(u, u, u) = 6N(u)$, and that $T((x_1, 0, 0), (0, x_2, 0), (0, 0, x_3)) = x_1 \otimes x_2 \otimes x_3$. Deduce that if $\mathcal{O} \subseteq \mathrm{Mat}_2(W)^3$ is a $\mathbb{Z}_p$-module whose W-span is $\mathrm{Mat}_2(W)^3$, then the W-span of $N(\mathcal{O})$ contains every $x_1 \otimes x_2 \otimes x_3$.

EXERCISE 6.7. Verify the claims of Example 6.1. Then show that $x^3 - 3x + 1$ has three real roots, discriminant 81, and no root modulo 7, so that it gives data for $p = 7$. Why does $x^3 - 4x + 1$ not work at $p = 7$?

Where this is used. Proposition 6.7 and Fact 6.4(b) give the tensor decomposition of the Dieudonné module in Chapter 7. Fact 6.4(c)–(e) are used in Chapter 12 to construct a fourfold with complex multiplication, lift its endomorphisms and reduce it to a supersingular point. Lemma 6.10 is used in the proof of Theorem C in Chapter 14, and the exceptional classes of Section 6.3 return in Remark 14.3.

CHAPTER 7

The Dieudonné module at a supersingular point

Where we are. This chapter proves that at a prime p inert in k, every supersingular point of Mumford's families has the same Dieudonné module, the model $\mathbb{M}$ of (1.1), and hence the same p-divisible group $\mathscr{G}_p$ (Proposition 7.4). Everything in Part III that computes lattices works in $\mathbb{M}$, so this is the bridge from Mumford's families to linear algebra. The chapter needs Dieudonné modules, slopes and Lang's lemma (Chapter 3) and the tensor induction of Chapter 6. The one tool not met in earlier chapters is a lemma on crystals of rank 2 (Lemma 7.2), proved completely.

7.1. The model in two pages

Let $t \in \mathscr{S}(\bar{\mathbb{F}}_p)$ and $M = M(\mathcal{A}_t)$. Kisin's crystalline tensors identify M with $\Lambda^\vee \otimes W$ (Fact 6.4), and by Proposition 6.7 this is, up to a power of p, a tensor product $\Lambda_1 \otimes \Lambda_2 \otimes \Lambda_3$ of three lattices of rank 2 over W. The Frobenius σ of W moves each tensor factor to the next one: $1 \otimes \sigma$ acts as the slot permutation $\varsigma(x_1 \otimes x_2 \otimes x_3) = \sigma x_3 \otimes \sigma x_1 \otimes \sigma x_2$. Since F and ς both fix the tensors, $F = \beta\varsigma$ with β in $G(W[1/p])$, so $\beta = \beta_1 \otimes \beta_2 \otimes \beta_3$ is a tensor product of three 2×2 matrices. That is all the structure there is, and the rest of the chapter extracts its consequences in four steps.

First, the elementary divisors of F on M are $1, 1, 1, 1, p, p, p, p$, because M/FM has length $\dim \mathcal{A}_t = 4$. The elementary divisors of a tensor product of matrices are the products of elementary divisors of the factors, so exactly one slot component β_i is not a scalar times an invertible matrix over W. Second, a change of basis by an element $\gamma_1 \otimes \gamma_2 \otimes \gamma_3$ of $G(W)$ replaces β_i by $\gamma_i \beta_i \sigma(\gamma_{i-1})^{-1}$, which allows us to make the two other slot components equal to 1. Then F^3 preserves each slot, and on the distinguished slot it is a σ^3-semilinear map $\Phi = \beta_2 \sigma^3$ of a module of rank 2. Third, the slopes of F are determined by those of Φ: either M is μ-ordinary, with slopes $0, \frac{1}{3}, \frac{2}{3}, 1$, or it is supersingular, with all slopes $\frac{1}{2}$; ordinary reduction never occurs. Fourth, in the supersingular case a lemma on crystals of rank 2 shows that Φ is $A\sigma^3$ in a suitable basis, with the matrix $A = \left(\begin{smallmatrix} 0 & p \\ 1 & 0 \end{smallmatrix}\right)$ of a supersingular elliptic curve. Then $F(x_1 \otimes x_2 \otimes x_3) = \sigma x_3 \otimes A\sigma x_1 \otimes \sigma x_2$, which is the model (1.1).

The model depends on nothing but p. So all supersingular points, of all Mumford families at all primes satisfying (h1)–(h4), have the same p-divisible group $\mathscr{G}_p$, and it splits as the p-divisible group of a supersingular elliptic curve times one of height 6 (Remark 7.6).

Example 7.1 (F^6 on the model). In the cube basis e_s of $\mathbb{M}$, $Fe_s = p^{s_1} e_{(s_3, 1-s_1, s_2)}$ (Chapter 1). Starting from e_{000}:

$$e_{000} \xrightarrow{F} e_{010} \xrightarrow{F} e_{011} \xrightarrow{F} e_{111} \xrightarrow{F} pe_{101} \xrightarrow{F} p^2 e_{100} \xrightarrow{F} p^3 e_{000},$$

where each arrow multiplies by p^{s_1} of the vector it starts from: $s_1 = 0, 0, 0, 1, 1, 1$ along the cycle. The other two vectors form the cycle $e_{001} \mapsto e_{110} \mapsto pe_{001}$. So $F^6 e_s = p^3 e_s$ for all eight s, that is, $F^6 = p^3 \sigma^6$ in this basis. A module on which some power F^n is $p^{n/2}\sigma^n$ is isoclinic of slope $\frac{1}{2}$, so $\mathbb{M}$ is supersingular.

7.2. Frobenius as a group element

Assume (h1)–(h4), and let $t \in \mathscr{S}(\bar{\mathbb{F}}_p)$ and $M = M(\mathcal{A}_t)$. By Proposition 6.7(a), $\Lambda^\vee \otimes \mathbb{Z}_p$ is, up to a power of p, the tensor induction of the dual lattice of Λ_0; to keep notation light

we write Λ_0 for that dual lattice and $\Lambda_i = \Lambda_0 \otimes_{\mathbb{Z}_{p^3},\tau_i} W$ for its slot lattices. Then Fact 6.4(b) gives an isomorphism

$$M \cong \Lambda^\vee \otimes W = p^{-j}\Lambda_1 \otimes \Lambda_2 \otimes \Lambda_3$$

that carries the crystalline tensors $\mathfrak{t}_{i,0}$ to $\mathfrak{t}_i \otimes 1$. Under it, $1 \otimes \sigma$ on $\Lambda^\vee \otimes W$ is the slot permutation ς of Definition 6.6, and in bases of the Λ_i related by σ it reads $\varsigma(x_1 \otimes x_2 \otimes x_3) = \sigma x_3 \otimes \sigma x_1 \otimes \sigma x_2$, with σ acting on coordinates.

The tensors $\mathfrak{t}_i \otimes 1$ are defined over $\mathbb{Z}_p$, so ς fixes them, and F fixes them by Fact 6.4(b). Hence $\beta = F\varsigma^{-1}$, a $W[1/p]$-linear automorphism of $M \otimes \mathbb{Q}$, fixes all $\mathfrak{t}_i \otimes 1$, so it lies in $G(W[1/p])$, and by Proposition 6.7(c)

$$F = \beta\varsigma, \qquad \beta = \beta_1 \otimes \beta_2 \otimes \beta_3, \qquad \beta_i \in \mathrm{GL}_2(W[1/p]). \tag{7.1}$$

We call $\beta_1, \beta_2, \beta_3$ the *slot components* of F. They are determined up to scalars $\lambda_1, \lambda_2, \lambda_3 \in W[1/p]^\times$ with $\lambda_1\lambda_2\lambda_3 = 1$.

One slot carries the Hodge filtration. Since $\dim \mathcal{A}_t = 4$, the kernel of F modulo p, which is $VM/pM \cong H^0(\mathcal{A}_t, \Omega^1)$ (Fact 3.10), has dimension 4. So FM/pM has dimension 4, $pM \subseteq FM$, and the elementary divisors of F, those of M/FM, are $(1,1,1,1,p,p,p,p)$. Since ς maps M bijectively onto itself, $FM = \beta M$, and these are the elementary divisors of β. Write the elementary divisors of β_i as $p^{n_i}, p^{n_i'}$ with $n_i \le n_i'$. The elementary divisors of $\beta_1 \otimes \beta_2 \otimes \beta_3$ are p to the eight sums $l_1 + l_2 + l_3$ with $l_i \in \{n_i, n_i'\}$ (Exercise 7.1). These sums range from $n_1 + n_2 + n_3$ to $n_1' + n_2' + n_3'$, and they must take the values 0 and 1 only, so

$$(n_1' - n_1) + (n_2' - n_2) + (n_3' - n_3) = 1.$$

Exactly one slot component is not a scalar times an element of $\mathrm{GL}_2(W)$. A cyclic renumbering of the slots does not change the form of ς, so we may assume that it is β_2. Moving scalars between the slots, we may assume $\beta_1, \beta_3 \in \mathrm{GL}_2(W)$ and $\beta_2 \in \mathrm{GL}_2(W)\mathrm{diag}(1,p)\,\mathrm{GL}_2(W)$.

Exercise 7.1. Let n_i, n_i' be integers for $i = 1,2,3$. Write the matrix of $\bigotimes_i \mathrm{diag}(p^{n_i}, p^{n_i'})$ in the basis $e_{s_1} \otimes e_{s_2} \otimes e_{s_3}$ and read off its elementary divisors. Deduce the statement about $\beta_1 \otimes \beta_2 \otimes \beta_3$ used above, writing $\beta_i = \gamma_i' \mathrm{diag}(p^{n_i}, p^{n_i'})\gamma_i''$ with $\gamma_i', \gamma_i'' \in \mathrm{GL}_2(W)$.

Normalizing two slots. An automorphism $\gamma = \gamma_1 \otimes \gamma_2 \otimes \gamma_3$ of M with $\gamma_i \in \mathrm{GL}_2(W)$ lies in $G(W)$, so it preserves the tensors, and replaces F by $\gamma F \gamma^{-1}$. A short computation (Exercise 7.2) gives $\varsigma\gamma\varsigma^{-1} = \sigma(\gamma_3) \otimes \sigma(\gamma_1) \otimes \sigma(\gamma_2)$, so

$$\gamma F \gamma^{-1} = \beta'\varsigma, \qquad \beta_i' = \gamma_i \beta_i \sigma(\gamma_{i-1})^{-1}, \quad \text{indices modulo 3.} \tag{7.2}$$

Take $\gamma_2 = 1$, $\gamma_3 = \beta_3^{-1}$ and $\gamma_1 = \sigma(\gamma_3)\beta_1^{-1}$, all in $\mathrm{GL}_2(W)$. Then $\beta_3' = \gamma_3\beta_3 = 1$ and $\beta_1' = \gamma_1\beta_1\sigma(\gamma_3)^{-1} = 1$, and $\beta_2' = \beta_2\sigma(\gamma_1)^{-1}$ still lies in $\mathrm{GL}_2(W)\mathrm{diag}(1,p)\,\mathrm{GL}_2(W)$. From now on $\beta_1 = \beta_3 = 1$ and

$$F(x_1 \otimes x_2 \otimes x_3) = \sigma x_3 \otimes \beta_2 \sigma x_1 \otimes \sigma x_2.$$

Applying this three times (Exercise 7.3),

$$F^3(x_1 \otimes x_2 \otimes x_3) = \sigma^2(\beta_2)\sigma^3 x_1 \otimes \beta_2 \sigma^3 x_2 \otimes \sigma(\beta_2)\sigma^3 x_3. \tag{7.3}$$

So F^3 preserves each slot, and on slot 2 it is the σ^3-semilinear map $\Phi = \beta_2\sigma^3$ of Λ_2. On slots 1 and 3 it is the conjugate of Φ by σ^2 and by σ. The pair (Λ_2, Φ) is a *σ^3-crystal of rank* 2: a free W-module of rank 2 with an injective σ^3-semilinear map, here with $p\Lambda_2 \subset \Phi\Lambda_2 \subset \Lambda_2$ and $\Lambda_2/\Phi\Lambda_2$ of length 1. Newton slopes of σ^r-crystals are defined as for σ-crystals (Chapter 3), with σ^r in place of σ.

Exercise 7.2. Verify $\varsigma\gamma\varsigma^{-1} = \sigma(\gamma_3) \otimes \sigma(\gamma_1) \otimes \sigma(\gamma_2)$ by evaluating both sides on $y_1 \otimes y_2 \otimes y_3$, and deduce (7.2).

Exercise 7.3. Compute F^2 and F^3 for $F(x_1 \otimes x_2 \otimes x_3) = \sigma x_3 \otimes \beta_2 \sigma x_1 \otimes \sigma x_2$ and verify (7.3). Then put $\beta_2 = A$, which has entries in $\mathbb{Z}_p$, and deduce $F^3 e_s = p^{s_1+s_2+s_3} e_{(1-s_1,1-s_2,1-s_3)}$ on the cube basis. Compare with Example 7.1.

7.3. Crystals of rank two

The following lemma is where supersingularity enters. Its hypotheses are exactly those of (Λ_2, Φ) above in the supersingular case, with $r = 3$.

LEMMA 7.2 (the rank-two lemma). *Let U be a free W-module of rank 2 and Φ a σ^r-semilinear map of U, $r \geq 1$, with $pU \subset \Phi U \subset U$, $U/\Phi U$ of length 1, and all Newton slopes positive. Then there is a basis of U in which $\Phi = A\sigma^r$, with $A = \left(\begin{smallmatrix} 0 & p \\ 1 & 0 \end{smallmatrix}\right)$: there are e_0, e_1 with $\Phi e_0 = e_1$ and $\Phi e_1 = pe_0$.*

PROOF. Put $V_U = p\Phi^{-1}$, which maps U into U because $pU \subset \Phi U$. Let $\bar\Phi$ be the reduction of Φ modulo p, a σ^r-semilinear map of the plane U/pU over $\bar{\mathbb{F}}_p$. Its image is $\Phi U/pU$, a line because $U/\Phi U$ has length 1. Its kernel is $V_U U/pU$: indeed $\Phi x \in pU$ if and only if $x \in p\Phi^{-1}U = V_U U$. The kernel is also a line, since the image is.

Suppose the two lines were different. Then $\bar\Phi$ maps its image line $\Phi U/pU$ into itself, and not to zero because $\Phi U/pU$ meets the kernel only in 0. So $\bar\Phi$ restricts to a bijection of $\Phi U/pU$ and $\bar\Phi^n \neq 0$ for every n. But all slopes of Φ are positive, so $\bar\Phi$ is nilpotent (Fact 3.11(b), which is stated for σ^r-semilinear maps). This contradiction shows $\Phi U = V_U U$, and then $\Phi^2 U = \Phi V_U U = pU$.

So $\Pi = p^{-1}\Phi^2$ is a σ^{2r}-semilinear bijection of U. By Lang's lemma (Lemma 3.5) the module $U^\Pi = \{x \in U : \Pi x = x\}$ is free of rank 2 over $W^{\sigma^{2r}} = \mathbb{Z}_{p^{2r}}$ and $U = U^\Pi \otimes_{\mathbb{Z}_{p^{2r}}} W$. Since Φ commutes with Π, it maps U^Π into itself, and so does $V_U = \Phi\Pi^{-1}$; the equality $\Phi U = V_U U$ descends to $\Phi U^\Pi = V_U U^\Pi$, because both sides are the Π-fixed vectors of the same W-module.

Since $\Phi U^\Pi \otimes W = \Phi U \neq U$, there is $e_0 \in U^\Pi \setminus \Phi U^\Pi$. Put $e_1 = \Phi e_0$. Then $\Phi e_1 = \Phi^2 e_0 = p\Pi e_0 = pe_0$. If e_1 were in pU^Π, then $e_0 \in p\Phi^{-1}U^\Pi = V_U U^\Pi = \Phi U^\Pi$, which is not the case. So modulo p, $\bar e_1$ is a nonzero vector of the line $\Phi U^\Pi/pU^\Pi$ and $\bar e_0$ is outside that line, and $\bar e_0, \bar e_1$ are a basis of U^Π/pU^Π. By Nakayama's lemma e_0, e_1 is a basis of U^Π over $\mathbb{Z}_{p^{2r}}$, hence of U over W, and in it $\Phi = A\sigma^r$. □

What just happened. Positive slopes force the image and the kernel of Φ modulo p to be the same line. Then $\Phi^2 = p \cdot$ (a bijection), Lang's lemma descends everything to a module where that bijection is the identity, and one vector e_0 outside the image together with $e_1 = \Phi e_0$ is the required basis. The matrix A is the one of the Dieudonné module of a supersingular elliptic curve, $M(E_0) = (W^2, A\sigma)$ (Equation (3.1)); the lemma says that every rank-2 crystal of this shape is that one, up to replacing σ by σ^r.

7.4. Slopes: μ-ordinary or supersingular

The determinant of β_2 has valuation 1, so the Newton slopes of (Λ_2, Φ) are u and $1-u$ for some $0 \leq u \leq \frac12$. If $u < \frac12$, the two slopes are distinct and each occurs once, and an isoclinic σ^3-crystal of rank 1, $W[1/p]x$ with $\Phi x = \lambda x$, has slope $v_p(\lambda) \in \mathbb{Z}$; so $u = 0$. Otherwise $u = \frac12$. The slopes of F^3 on M are the sums of one slope from each slot, by (7.3), because slopes add under tensor products, and the slopes of F are one third of those of F^3. Choosing the slope u in some of the three slots and $1-u$ in the others, the slopes of F are

$$\tfrac13\{3u,\ 1+u,\ 2-u,\ 3-3u\} \qquad \text{with multiplicities } 1,3,3,1. \tag{7.4}$$

EXAMPLE 7.3 (the two cases). For $u = 0$ the slopes are $0, \frac13, \frac23, 1$ with multiplicities $1,3,3,1$. This Newton polygon is called *μ-ordinary*. It is not ordinary, which would mean slopes 0 and 1 with multiplicity 4 each: Mumford's fourfolds have no ordinary reduction at a prime inert in k. For $u = \frac12$ the four numbers $3u$, $1+u$, $2-u$, $3-3u$ are all $\frac32$, so every slope is $\frac12$: the supersingular case. No other Newton polygon occurs.

EXERCISE 7.4. Derive (7.4) in detail: list the eight choices of slopes in the three slots, compute the sum for each, and divide by 3. Check that the slopes of F add up to $4 = \dim \mathcal{A}_t$ for every u, as they must for an abelian fourfold.

7.5. The model

PROPOSITION 7.4 (the model). *Assume (h1)–(h4), and let $t \in \mathscr{S}(\bar{\mathbb{F}}_p)$. Then $M = M(\mathcal{A}_t)$ is either μ-ordinary, with slopes $0, \frac{1}{3}, \frac{2}{3}, 1$ of multiplicities $1, 3, 3, 1$, or supersingular. In the supersingular case (M, F) is isomorphic to the model $\mathbb{M}$ of (1.1). In particular all supersingular $\mathcal{A}_t$, $t \in \mathscr{S}(\bar{\mathbb{F}}_p)$, have p-divisible group isomorphic to $\mathscr{G}_p$.*

PROOF. By Section 7.2, after an automorphism of M in $G(W)$, $F(x_1 \otimes x_2 \otimes x_3) = \sigma x_3 \otimes \beta_2 \sigma x_1 \otimes \sigma x_2$ with $\beta_2 \in \mathrm{GL}_2(W)\mathrm{diag}(1, p)\,\mathrm{GL}_2(W)$, and by Section 7.4 the slopes are those of (7.4) with $u \in \{0, \frac{1}{2}\}$. This proves the dichotomy. In the supersingular case $u = \frac{1}{2}$, so (Λ_2, Φ) with $\Phi = \beta_2 \sigma^3$ satisfies the hypotheses of Lemma 7.2 with $r = 3$, and there is $\gamma' \in \mathrm{GL}_2(W)$ with $\gamma' \beta_2 \sigma^3 (\gamma')^{-1} = A$. Conjugate by $\gamma = \sigma^2(\gamma') \otimes \gamma' \otimes \sigma(\gamma')$. By (7.2) the new slot components are

$$\sigma^2(\gamma') \cdot 1 \cdot \sigma(\sigma(\gamma'))^{-1} = 1, \qquad \gamma' \beta_2 \sigma(\sigma^2(\gamma'))^{-1} = A, \qquad \sigma(\gamma') \cdot 1 \cdot \sigma(\gamma')^{-1} = 1,$$

so $F(x_1 \otimes x_2 \otimes x_3) = \sigma x_3 \otimes A\sigma x_1 \otimes \sigma x_2$ on $p^{-j}\Lambda_1 \otimes \Lambda_2 \otimes \Lambda_3$. Multiplication by p^j, which commutes with F, then identifies (M, F) with (1.1). The last assertion follows from Dieudonné theory (Fact 3.10): $\mathcal{A}_t[p^\infty]$ is determined up to isomorphism by (M, F). □

The isomorphism of the proposition is an isomorphism of Dieudonné modules; it does not claim to respect the tensors, the polarization or the action of any endomorphism, and nothing later needs it to. When an endomorphism has to be followed through the identification, as in Chapter 12, this is done explicitly.

EXAMPLE 7.5 (the a-number of $\mathbb{M}$ by hand). The a-number is $a(\mathbb{M}) = \dim \mathbb{M}/(F\mathbb{M} + V\mathbb{M})$ (Definition 3.15). Modulo p, $Fe_s = p^{s_1} e_{\pi(s)}$ with $\pi(s) = (s_3, 1 - s_1, s_2)$, so $F\mathbb{M}$ modulo p is spanned by the $e_{\pi(s)}$ with $s_1 = 0$, which are the $e_{s'}$ with middle coordinate $s'_2 = 1$. Since $V = pF^{-1}$, $Ve_{\pi(s)} = p^{1-s_1} e_s$, so $V\mathbb{M}$ modulo p is spanned by the e_s with $s_1 = 1$. The two spans together contain every e_s except e_{000} and e_{001}, so $a(\mathbb{M}) = 2$. In the language of words (Definition 3.17) the two cycles of Example 7.1 carry the words 000111 and 01, and each has one cyclic transition from 1 to 0.

EXERCISE 7.5. Repeat the computation of Example 7.5 for the module of the same shape with A in slot 1 instead of slot 2, that is, $F(x_1 \otimes x_2 \otimes x_3) = A\sigma x_3 \otimes \sigma x_1 \otimes \sigma x_2$. Find the cycles of Frobenius on the cube basis and their words, and explain why the result is isomorphic to $\mathbb{M}$.

7.6. The p-divisible group $\mathscr{G}_p$

REMARK 7.6 (what $\mathscr{G}_p$ is). The two cycles of Frobenius on the cube basis (Example 7.1) span F- and V-stable direct summands of $\mathbb{M}$, so $\mathscr{G}_p$ is a product of two p-divisible groups. The cycle $e_{001} \mapsto e_{110} \mapsto pe_{001}$ is the module $(W^2, A\sigma)$ of word 01, the Dieudonné module of a supersingular elliptic curve E_0. The six-cycle has word 000111 and is generated as a module over F and V by $y = e_{000}$: by Example 7.1 $F^3 y = e_{111}$, and V runs the cycle backwards, $Ve_{000} = e_{100}$, $Ve_{100} = e_{101}$, $Ve_{101} = e_{111}$, so $V^3 y = e_{111} = F^3 y$. Hence

$$\mathscr{G}_p \cong E_0[p^\infty] \times \mathscr{G}'_p,$$

where $\mathscr{G}'_p$ has height 6 and dimension 3 and its Dieudonné module is generated by one element y with $F^3 y = V^3 y$. Each factor has a-number 1, and $a(\mathscr{G}_p) = 2$.

So $\mathscr{G}_p$ is supersingular but not superspecial: a superspecial fourfold has a-number 4. For Mumford's families, that the Newton polygon jumps only at supersingular points is stated, under a mild assumption on p, in [SZ16]. The proof above is included because the later chapters need the explicit module.

Where this is used. Proposition 7.4 is the first step of the plan in Chapter 1. The model is analyzed in Chapters 8 and 9. In Chapter 12 the dichotomy of Proposition 7.4 shows that a reduction of a fourfold with complex multiplication is supersingular, and the conjugation formula (7.2) describes the automorphisms of $(\mathbb{M}, F)$. In Chapter 14 the last assertion of Proposition 7.4 lets one supersingular point stand for all of them.

CHAPTER 8

The gap: four missing classes

Where we are. This chapter computes the gap T^4/S for the model $\mathbb{M}$ of (1.1), the Dieudonné module of every abelian fourfold with p-divisible group $\mathscr{G}_p$. The answer is $(\mathbb{Z}/p)^4$, carried by the wedge products of four special subsets of the cube $\mathcal{C} = \{0,1\}^3$: the two regular tetrahedra $\mathsf{T}_+, \mathsf{T}_-$ inscribed in the cube and two majority sets $\mathsf{M}_+, \mathsf{M}_-$ (Proposition 8.2). The tetrahedra are the eigensets of an action of $\mathbb{Z}_{p^2}$ of type $(2,2)$, and their wedge products span the Weil lattice $\mathcal{L}$, which carries half of the gap (Lemma 8.4). The chapter needs the min-plus calculus of Chapter 5 and the model (1.1). Its main statement rests on an exact computation.

8.1. The gap in two pages

In the cube basis $e_s = e_{s_1} \otimes e_{s_2} \otimes e_{s_3}$ of the model, Frobenius is monomial:

$$Fe_s = p^{s_1} e_{\pi(s)}, \qquad \pi(s_1, s_2, s_3) = (s_3, 1 - s_1, s_2).$$

The permutation π has two orbits on the eight vertices of the cube, one of length 6 and one of length 2, and the exponents s_1 read along them are the words 000111 and 01. So $\mathbb{M}$ is the monomial module $01 + 000111$, and the descent lemma (Lemma 5.3) computes $T^4 \otimes W = \bigoplus p^{n_J} W e_J$ and $S \otimes W = \bigoplus p^{n_J^S} W e_J$ over the 70 four-element subsets J of the cube. The result of evaluating the orbit rule and the minima over splittings is that $n_J^S = n_J$ except for the four sets

$$\mathsf{T}_+ = \{000, 011, 101, 110\}, \qquad \mathsf{T}_- = \{001, 010, 100, 111\},$$
$$\mathsf{M}_+ = \{000, 001, 011, 101\}, \qquad \mathsf{M}_- = \{010, 100, 110, 111\},$$

where the defect $n_J^S - n_J$ is 1. Hence $[T^4 : S] = p^4$, and since every defect is 1, T^4/S is killed by p: $T^4/S \cong (\mathbb{Z}/p)^4$ (Proposition 8.2).

The sets have a meaning. A diagonal action of $\mathbb{Z}_{p^2}$ on $\mathbb{M}$ commuting with F, with characters ι or $\bar{\iota}$ on the basis vectors, must have characters that alternate along the orbits of π, because F is σ-semilinear and σ exchanges ι and $\bar{\iota}$. Exactly four subsets of the cube can be the ι-eigenset of such an action, and they are the four sets above (Lemma 8.4). The type of the action, read on $\ker(F \bmod p) = \langle e_s : s_1 = 1 \rangle \cong H^0(X, \Omega^1)$, is $(2,2)$ for the tetrahedra and $(1,3)$, $(3,1)$ for the majority sets. For an action of type $(2,2)$ the top exterior powers of the two eigenspaces are e_{T_+} and e_{T_-}, so half of the gap consists of *Weil classes*, and the integral ones form the rank-2 Weil lattice $\mathcal{L}$ (Definition 8.6).

Example 8.1 (the defect at T_+). The orbit of T_+ under π is $\{\mathsf{T}_+, \mathsf{T}_-\}$, and both sets contain two vertices with $s_1 = 1$, so the steps of the orbit rule are $2-2 = 0$ and $n_{\mathsf{T}_+} = n_{\mathsf{T}_-} = 0$: the vectors e_{T_+} and e_{T_-} lie in $T^4 \otimes W$. The three splittings of T_+ into two 2-sets each pair the vertex 000 with one of $011, 101, 110$, and the orbit rule gives $n_{\{000,s\}} = 1$ for each of these s and 0 for the complementary pairs (Section 8.4). So every product of two Tate classes of degree 2 reaches e_{T_+} only with a factor p: $n^S_{\mathsf{T}_+} = 1$, a defect of 1.

8.2. The cube basis and Frobenius

Recall the model $\mathbb{M} = W^2 \otimes W^2 \otimes W^2$ with $F(x_1 \otimes x_2 \otimes x_3) = \sigma x_3 \otimes A\sigma x_1 \otimes \sigma x_2$ and $Ae_0 = e_1$, $Ae_1 = pe_0$. For basis vectors σ does nothing, and $Ae_{s_1} = p^{s_1} e_{1-s_1}$. So

$$Fe_s = p^{w(s)} e_{\pi(s)}, \qquad \pi(s_1, s_2, s_3) = (s_3, 1 - s_1, s_2), \qquad w(s) = s_1. \tag{8.1}$$

Frobenius takes the third slot to the first, the first slot through A to the second, and the second to the third; the factor p appears when the first slot is e_1. The permutation π acts on the eight vertices as follows:

s	000	010	011	111	101	100	001	110
$\pi(s)$	010	011	111	101	100	000	110	001
$w(s) = s_1$	0	0	0	1	1	1	0	1

So π has the two orbits

$$(000, 010, 011, 111, 101, 100) \qquad \text{and} \qquad (001, 110),$$

on which the exponents read 000111 and 01. In the language of Definition 3.17, $\mathbb{M} \cong M_{01+000111}$: renumbering the basis along the orbits identifies the two. In particular $\mathbb{M}$ is a supersingular Dieudonné module of height 8 and dimension 4, its a-number is $1 + 1 = 2$, and the order of π is $q = 6$, so $F^6 = p^3\sigma^6$ in the cube basis. Modulo p, F kills exactly the e_s with $s_1 = 1$, so

$$\ker(F \bmod p) = VM/pM = \langle e_s : s_1 = 1 \rangle,$$

which by Fact 3.10(d) is the space of 1-forms $H^0(X, \Omega^1)$ when $M(X) \cong \mathbb{M}$.

Exercise 8.1. Verify the table of π from (8.1), the two orbits and their words, and $F^6 = p^3\sigma^6$. Check that π has no fixed vertex and that $\pi^3(s) = (1 - s_1, 1 - s_2, 1 - s_3)$ for every vertex s.

8.3. The four sets

The following four 4-element subsets of the cube carry the gap:

$$\begin{aligned} \mathsf{T}_+ &= \{000, 011, 101, 110\}, & \mathsf{T}_- &= \{001, 010, 100, 111\}, \\ \mathsf{M}_+ &= \{000, 001, 011, 101\}, & \mathsf{M}_- &= \{010, 100, 110, 111\}. \end{aligned} \tag{8.2}$$

The sets T_+ and T_- are the vertices with an even, respectively odd, number of coordinates equal to 1: the two regular tetrahedra inscribed in the cube. The sets M_+ and M_- are the vertices at which, after the change of coordinates $s \mapsto s' = (s_1, s_2, 1 - s_3)$, the majority of the three coordinates of s' is 0, respectively 1; equivalently, the majority of the signs $(-1)^{s'_i}$ is $+$, respectively $-$. Each pair consists of complementary sets, and π exchanges the two sets of each pair (Exercise 8.2).

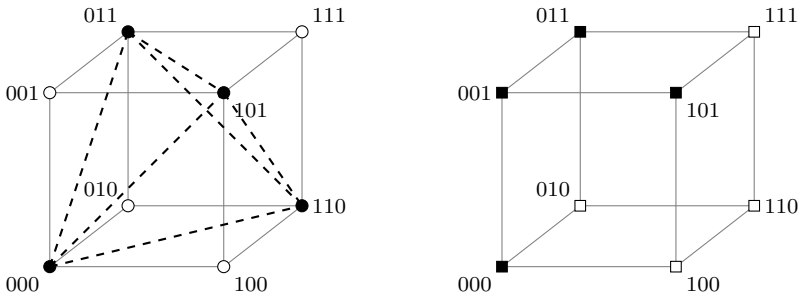
Exercise 8.2. Show that $\pi(\mathsf{T}_+) = \mathsf{T}_-$, $\pi(\mathsf{T}_-) = \mathsf{T}_+$, $\pi(\mathsf{M}_+) = \mathsf{M}_-$ and $\pi(\mathsf{M}_-) = \mathsf{M}_+$, and compute $w(J) = \sum_{s \in J} s_1$ for the four sets.

8.4. The index proposition

Proposition 8.2 (the gap, computer-assisted). *For the model $\mathbb{M}$, $n_J^S = n_J$ for every 4-set $J \subseteq \mathcal{C}$ except the four sets (8.2), where*

$$(n_J, n_J^S) = (0, 1) \quad \text{for } J = \mathsf{T}_+, \mathsf{T}_-, \mathsf{M}_-, \qquad (n_J, n_J^S) = (1, 2) \quad \text{for } J = \mathsf{M}_+.$$

Hence $T^4/S \cong (\mathbb{Z}/p)^4$, spanned by the images of the $p^{n_J} e_J$, $J \in \{\mathsf{T}_+, \mathsf{T}_-, \mathsf{M}_+, \mathsf{M}_-\}$, in $(T^4/S) \otimes W$. Moreover $T^6 = S^6$: every Tate class of degree 6 is a $\mathbb{Z}_p$-combination of products of three classes in T^2.



T_+ (filled), T_- (open) $\quad$ M_+ (filled), M_- (open)

FIGURE 8.1. The cube $\mathcal{C} = \{0,1\}^3$ with the first coordinate to the right, the second into the page and the third upwards. Left: the tetrahedra T_+ (filled, with its edges dashed) and T_- (open). Right: the majority sets M_+ (filled) and M_- (open). The vertices with $s_1 = 1$, on the right face of each cube, span $\ker(F \bmod p)$; they meet T_+, T_-, M_+, M_- in 2, 2, 1, 3 vertices.

PROOF. By Lemma 5.3 the exponents of $T^4 \otimes W$ and $S \otimes W$ are n_J and n_J^S, given by the orbit rule (5.1) for the 28 two-sets and 70 four-sets and by (5.2). Their values are an exact computation with integers described below. It gives the stated exponents, so $[T^4 : S] = p^{\sum_J (n_J^S - n_J)} = p^4$. Every defect is 1, so $p(T^4 \otimes W) \subseteq S \otimes W$, and $pT^4 \subseteq S$ by Lemma 5.2. A finite $\mathbb{Z}_p$-module of order p^4 killed by p is $(\mathbb{Z}/p)^4$ (Exercise 1.4). The image of $T^4 \otimes W$ in $(T^4/S) \otimes W$ is spanned by the images of the $p^{n_J} e_J$ with $n_J^S > n_J$. For degree 6 the same computation, with n_J for the 28 six-sets and the minima over the splittings into three 2-sets, gives equal exponents. □

Remark on the proof 8.1: the computation behind Proposition 8.2. The proposition rests on evaluating, for the model, the orbit rule for all $\binom{8}{2} = 28$ two-sets and $\binom{8}{4} = 70$ four-sets and the minimum over the three splittings for each four-set, and comparing; and the same for the 28 six-sets and their fifteen splittings into three 2-sets. All quantities are integers built from the eight values $w(s) = s_1$ by sums, maxima and minima, so the computation is exact and the same for every p. Its output is the list of the four defect sets with the exponents stated. The computation also lists the 4-sets J with $\pi(J)$ equal to the complement of J, which are again the four sets (as Lemma 8.4 proves by hand), and the numbers $|J \cap \{s_1 = 1\}|$. Every individual exponent can be checked by hand as in Example 8.1 and the computations below; the proposition needs all of them.

The exponents at T_+, by hand. Two orbits of 2-sets suffice for the three splittings of T_+. Applying π to $\{000, 011\}$ gives the orbit

$$\{000,011\} \to \{010,111\} \to \{011,101\} \to \{111,100\}$$
$$\to \{101,000\} \to \{100,010\} \to \{000,011\},$$

with weights $w = 0,1,1,2,1,1$, steps $w - 1 = -1,0,0,+1,0,0$, partial sums $\widetilde{n} = 0,-1,-1,-1,0,0$ and minimum -1. The orbit rule $n = \widetilde{n} - \min \widetilde{n}$ gives the exponents $1,0,0,0,1,1$. In the same way the orbit

$$\{000,110\} \to \{010,001\} \to \{011,110\} \to \{111,001\}$$
$$\to \{101,110\} \to \{100,001\} \to \{000,110\}$$

has weights $1,0,1,1,2,1$, steps $0,-1,0,0,+1,0$, partial sums $0,0,-1,-1,-1,0$, and exponents $1,1,0,0,0,1$. So

$$n_{\{000,011\}} = n_{\{000,101\}} = n_{\{000,110\}} = 1, \qquad n_{\{101,110\}} = n_{\{011,110\}} = n_{\{011,101\}} = 0.$$

Each splitting of T_+ pairs 000 with one of $011, 101, 110$ and the other two vertices with each other, so $n_{J_1} + n_{J_2} = 1 + 0$ for all three, and $n^S_{\mathsf{T}_+} = 1$. On the other hand $n_{\mathsf{T}_+} = 0$ (Example 8.1). The reason no splitting reaches 0 is visible in the orbit rule: going backwards from each of $\{000, 011\}$, $\{000, 101\}$, $\{000, 110\}$, one meets a 2-set whose two vertices both have first coordinate 1, a step $+1$, before meeting one whose two vertices both have first coordinate 0, a step -1; so the maximal partial sum in (5.1) is at least 1.

Intuition 8.3 (what the defect means). The vector e_{T_+} itself, or rather the Tate class $\lambda e_{\mathsf{T}_+} \pm \sigma(\lambda) e_{\mathsf{T}_-}$ with λ a unit (Lemma 8.4), is an integral Tate class of degree 4. Writing it as a combination of products of integral Tate classes of degree 2 is possible only after multiplying by p: every way of splitting e_{T_+} into two wedge factors passes through a factor that is Tate only with a coefficient p. Rationally nothing is missing; integrally one factor of p is missing at each of the four sets.

All exponents of degree 2. The two orbits used above are two of the six orbits of π on the 28 two-sets. The following table lists all of them, each 2-set followed by its exponent n_J in parentheses and the orbit read from left to right; every row is obtained from its first entry by the orbit rule, as above.

orbit						
I	$000, 001$ (2)	$010, 110$ (1)	$001, 011$ (1)	$110, 111$ (0)	$001, 101$ (1)	$100, 110$ (1)
II	$000, 010$ (2)	$010, 011$ (1)	$011, 111$ (0)	$101, 111$ (0)	$100, 101$ (1)	$000, 100$ (2)
III	$000, 011$ (1)	$010, 111$ (0)	$011, 101$ (0)	$100, 111$ (0)	$000, 101$ (1)	$010, 100$ (1)
IV	$000, 110$ (1)	$001, 010$ (1)	$011, 110$ (0)	$001, 111$ (0)	$101, 110$ (0)	$001, 100$ (1)
V	$000, 111$ (0)	$010, 101$ (0)	$011, 100$ (0)			
VI	$001, 110$ (0)					

The orbit V consists of the three antipodal pairs on the orbit of length 6 of π, each with weight 1, and orbit VI is the orbit $\{001, 110\}$ of length 1, the summand M_{01} of E_0. The exponents add up to 18, so $T^2 \otimes W$ has index p^{18} in $\bigwedge^2 \mathbb{M}$. With this table, n^S_J for any 4-set is the minimum of three sums of two entries, which makes every value of n^S_J in Proposition 8.2 checkable by hand; the values of n_J for 4-sets need the orbit rule on 4-sets.

The four defects, by hand. With the table, the three splittings of each of the four sets give:

J	splitting 1	splitting 2	splitting 3	(n_J, n^S_J)
T_+	$\{000, 011\}\{101, 110\}$: $1 + 0$	$\{000, 101\}\{011, 110\}$: $1 + 0$	$\{000, 110\}\{011, 101\}$: $1 + 0$	$(0, 1)$
T_-	$\{001, 010\}\{100, 111\}$: $1 + 0$	$\{001, 100\}\{010, 111\}$: $1 + 0$	$\{001, 111\}\{010, 100\}$: $0 + 1$	$(0, 1)$
M_+	$\{000, 001\}\{011, 101\}$: $2 + 0$	$\{000, 011\}\{001, 101\}$: $1 + 1$	$\{000, 101\}\{001, 011\}$: $1 + 1$	$(1, 2)$
M_-	$\{010, 100\}\{110, 111\}$: $1 + 0$	$\{010, 110\}\{100, 111\}$: $1 + 0$	$\{010, 111\}\{100, 110\}$: $0 + 1$	$(0, 1)$

The exponents n_J in the last column come from the two orbits $\{\mathsf{T}_+, \mathsf{T}_-\}$ and $\{\mathsf{M}_+, \mathsf{M}_-\}$ of π on 4-sets, with weights $2, 2$ and $1, 3$. So the four defects of Proposition 8.2 can be checked completely by hand. What the computation adds is that the other 66 four-sets have no defect.

Sets without defect. For contrast, take the face $J = \{000, 001, 010, 011\}$ of the cube on which $s_1 = 0$, so $w(J) = 0$. Its orbit under π has length 6, with weights $0, 2, 2, 4, 2, 2$, steps $-2, 0, 0, +2, 0, 0$ and partial sums $0, -2, -2, -2, 0, 0$, so $n_J = 2$: the class $p^2 e_J$ is the first multiple of e_J in $T^4 \otimes W$. The splitting $\{000, 011\} \sqcup \{001, 010\}$ has $n_{\{000,011\}} + n_{\{001,010\}} = 1 + 1 = 2$, using the two orbits computed above, so $n^S_J = 2 = n_J$, since always $n^S_J \geq n_J$: products of degree-2 Tate classes reach this class without loss. The opposite face $\{100, 101, 110, 111\}$ lies in the same orbit, has $n = 0$, and the splitting $\{100, 111\} \sqcup \{101, 110\}$ has exponent $0 + 0$. Over all 70 four-sets, the computation gives $n_J = 0$ for 31 of them, $n_J = 1$ for 27, $n_J = 2$ for 11 and $n_J = 3$ for one; so $\sum_J n_J = 52$, while $\sum_J n^S_J = 56$, the difference 4 being the four defects.

A characterization of the four sets. The orbits of π on the 70 four-sets have lengths 6, 3 and 2, and the orbits of length 2 are exactly $\{\mathsf{T}_+, \mathsf{T}_-\}$ and $\{\mathsf{M}_+, \mathsf{M}_-\}$. Indeed, π^2 acts on the vertices with the two 3-cycles $(000, 011, 101)$ and $(010, 111, 100)$ and the two fixed points 001 and 110, so a 4-set with $\pi^2(J) = J$ is the union of one 3-cycle and one fixed point, and the four such unions are the four sets. This is the same computation as in Lemma 8.4(i) below: a 4-set with $\pi(J)$ equal to its complement satisfies $\pi^2(J) = J$. Neither observation is used in the proof.

Exercise 8.3. Using the orbit rule, compute n_J for the 2-sets $\{000, 001\}$, $\{001, 011\}$ and $\{001, 101\}$, and use them, with the exponents computed above, to verify $n_{\mathsf{M}_+} = 1$ and $n^S_{\mathsf{M}_+} = 2$.

Exercise 8.4. Explain why the fact that all four defects equal 1 implies that T^4/S is killed by p, and what the quotient would be if instead one defect were 2 and two were 1.

8.5. The eigensets of an inert quadratic action

Let K be an imaginary quadratic field in which p is inert, so $O_K \otimes \mathbb{Z}_p = \mathbb{Z}_{p^2}$, and let $\iota, \bar\iota\colon \mathbb{Z}_{p^2} \to W$ be its two embeddings; $\sigma \circ \iota = \bar\iota$ because σ restricts to the nontrivial automorphism of $\mathbb{Z}_{p^2}$. Consider an action of $\mathbb{Z}_{p^2}$ on $(\mathbb{M}, F)$, that is, a ring homomorphism $\mathbb{Z}_{p^2} \to \mathrm{End}(\mathbb{M}, F)$, which is *diagonal* in the cube basis: each $\lambda \in \mathbb{Z}_{p^2}$ acts by $e_s \mapsto \iota_s(\lambda) e_s$ with characters $\iota_s \in \{\iota, \bar\iota\}$. Let $J_\iota = \{s : \iota_s = \iota\}$ be the ι-eigenset.

Lemma 8.4 (eigensets). *(i) $\pi(J_\iota)$ is the complement of J_ι, and J_ι is one of the four sets (8.2). Conversely, each of the four sets is the ι-eigenset of exactly one diagonal action.*
(ii) If the action is the reduction of an action of O_K on an abelian scheme over a discrete valuation ring of characteristic 0 whose generic fiber has type $(2,2)$, then $J_\iota \in \{\mathsf{T}_+, \mathsf{T}_-\}$.
(iii) In the situation of (ii), the Weil part $\bigwedge^4_W M_\iota \oplus \bigwedge^4_W M_{\bar\iota}$ of $\bigwedge^4 \mathbb{M}$, with M_ι and $M_{\bar\iota}$ the ι- and $\bar\iota$-eigenspaces, is $We_{\mathsf{T}_+} \oplus We_{\mathsf{T}_-}$.

Proof. (i) For $\lambda \in \mathbb{Z}_{p^2}$, F applied to $\iota_s(\lambda) e_s$ gives $\sigma(\iota_s(\lambda)) p^{s_1} e_{\pi(s)}$, while the action of λ on $Fe_s = p^{s_1} e_{\pi(s)}$ gives $\iota_{\pi(s)}(\lambda) p^{s_1} e_{\pi(s)}$. Since the action commutes with F, $\iota_{\pi(s)} = \sigma \circ \iota_s = \bar\iota_s$. So membership in J_ι alternates along both orbits of π, which gives $\pi(J_\iota) = \mathcal{C} \setminus J_\iota$. On the orbit $(000, 010, 011, 111, 101, 100)$ of length 6, J_ι contains either $\{000, 011, 101\}$ or $\{010, 111, 100\}$; on the orbit $(001, 110)$ it contains 001 or 110. The four combinations are

$$\{000, 011, 101\} \cup \{110\} = \mathsf{T}_+, \qquad \{000, 011, 101\} \cup \{001\} = \mathsf{M}_+,$$
$$\{010, 111, 100\} \cup \{001\} = \mathsf{T}_-, \qquad \{010, 111, 100\} \cup \{110\} = \mathsf{M}_-.$$

Conversely, for each of the four sets the characters $\iota_s = \iota$ on the set and $\bar\iota$ off it satisfy $\iota_{\pi(s)} = \bar\iota_s$, so the diagonal action they define commutes with F.

(ii) By Fact 3.10(d), $\ker(F \bmod p) = \langle e_s : s_1 = 1\rangle$ is $H^0(X, \Omega^1)$ of the special fiber, compatibly with endomorphisms, so the type of the action in characteristic p is $(|J_\iota \cap \{s_1 = 1\}|, |J_{\bar\iota} \cap \{s_1 = 1\}|)$. Let $\mathcal{X}$ be the abelian scheme over the discrete valuation ring O, which we may enlarge so that it contains $\mathbb{Z}_{p^2}$. The module $H^0(\mathcal{X}, \Omega^1)$ is free of rank 4 over O and its formation commutes with base change to both fibers. Since p is unramified in K, $O_K \otimes O \cong O \times O$ through ι and $\bar\iota$, so $H^0(\mathcal{X}, \Omega^1)$ is the direct sum of the two eigenmodules, each free over O. Their ranks are the same on both fibers. So the type is $(2,2)$ on the special fiber too, and $|J_\iota \cap \{s_1 = 1\}| = 2$. The four sets meet $\{s_1 = 1\} = \{100, 101, 110, 111\}$ in $\{101, 110\}$, $\{100, 111\}$, $\{101\}$ and $\{100, 110, 111\}$, that is in $2, 2, 1, 3$ vertices. So J_ι is T_+ or T_-.

(iii) M_ι is the W-span of the e_s, $s \in J_\iota$, so $\bigwedge^4_W M_\iota = We_{J_\iota}$, and $M_{\bar\iota}$ is spanned by the e_s with s in the complement. With $J_\iota \in \{\mathsf{T}_+, \mathsf{T}_-\}$ the complement is the other tetrahedron. □

Example 8.5 (the types of the four actions). The table records, for each of the four diagonal actions, the vertices of the eigenset with $s_1 = 1$ and the type:

J_ι	$J_\iota \cap \{s_1 = 1\}$	type	(n_J, n_J^S)	name
$\mathsf{T}_+ = \{000, 011, 101, 110\}$	$\{101, 110\}$	$(2,2)$	$(0,1)$	tetrahedron
$\mathsf{T}_- = \{001, 010, 100, 111\}$	$\{100, 111\}$	$(2,2)$	$(0,1)$	tetrahedron
$\mathsf{M}_+ = \{000, 001, 011, 101\}$	$\{101\}$	$(1,3)$	$(1,2)$	majority set
$\mathsf{M}_- = \{010, 100, 110, 111\}$	$\{100, 110, 111\}$	$(3,1)$	$(0,1)$	majority set

The proof does not need an explanation of why the four eigensets of diagonal actions are exactly the four defect sets of Proposition 8.2; it uses only that both statements hold.

Exercise 8.5. Verify the counts $|J \cap \{s_1 = 1\}| = 2, 2, 1, 3$ for $\mathsf{T}_+, \mathsf{T}_-, \mathsf{M}_+, \mathsf{M}_-$, and check that the two actions with eigensets T_+ and T_- are conjugate to each other: they differ by exchanging ι and $\bar{\iota}$.

8.6. The Weil lattice and the majority lattice

Definition 8.6 (the Weil lattice). For an abelian fourfold X over $\bar{\mathbb{F}}_p$ with an isomorphism $M(X) \cong \mathbb{M}$, the *Weil lattice* is

$$\mathcal{L} = T^4(X) \cap (We_{\mathsf{T}_+} \oplus We_{\mathsf{T}_-}).$$

Proposition 8.7 (structure of $\mathcal{L}$). *The Weil lattice $\mathcal{L}$ is a free $\mathbb{Z}_p$-module of rank 2 with $\mathcal{L} \otimes W = We_{\mathsf{T}_+} \oplus We_{\mathsf{T}_-}$. Every element of $\mathcal{L} \setminus p\mathcal{L}$ has the form $\lambda e_{\mathsf{T}_+} \pm \sigma(\lambda) e_{\mathsf{T}_-}$ with $\lambda \in W^\times$, with a sign that depends only on the ordering of the wedge basis, not on the element.*

Proof. Let $\varphi = p^{-2} \bigwedge^4 F$. Since $\pi(\mathsf{T}_+) = \mathsf{T}_-$, $\pi(\mathsf{T}_-) = \mathsf{T}_+$ and $w(\mathsf{T}_+) = w(\mathsf{T}_-) = 2$, $\varphi(e_{\mathsf{T}_+}) = (-1)^{j_1} e_{\mathsf{T}_-}$ and $\varphi(e_{\mathsf{T}_-}) = (-1)^{j_2} e_{\mathsf{T}_+}$ for some integers j_1, j_2. So φ is a σ-semilinear bijection of $\mathcal{L}_W = We_{\mathsf{T}_+} \oplus We_{\mathsf{T}_-}$, and by Lemma 3.5 $\mathcal{L}_W = \mathcal{L}_W^\varphi \otimes W$, where $\mathcal{L}_W^\varphi$ is free of rank 2. A vector of $\mathcal{L}_W$ is φ-fixed exactly when it lies in T^4, so $\mathcal{L}_W^\varphi = \mathcal{L}$ and $\mathcal{L} \otimes W = \mathcal{L}_W$. A vector $\lambda e_{\mathsf{T}_+} + \lambda' e_{\mathsf{T}_-}$ is fixed if and only if $\lambda' = (-1)^{j_1}\sigma(\lambda)$ and $\lambda = (-1)^{j_2}\sigma(\lambda')$. By Lemma 5.2, $\mathcal{L} \cap p(\mathcal{L} \otimes W) = p\mathcal{L}$, and $\lambda e_{\mathsf{T}_+} + (-1)^{j_1}\sigma(\lambda) e_{\mathsf{T}_-}$ lies in $p(\mathcal{L} \otimes W)$ if and only if p divides λ. □

Definition 8.8 (the majority lattice). For X as in Definition 8.6, the *majority lattice* is $\mathcal{N} = T^4(X) \cap (We_{\mathsf{M}_+} \oplus We_{\mathsf{M}_-})$.

By the same argument, now with $w(\mathsf{M}_+) = 1$ and $w(\mathsf{M}_-) = 3$, φ maps pe_{M_+} to $\pm e_{\mathsf{M}_-}$ and e_{M_-} to $\pm pe_{\mathsf{M}_+}$, so it is a bijection of $pWe_{\mathsf{M}_+} \oplus We_{\mathsf{M}_-}$, and

$$\mathcal{N} \otimes W = pWe_{\mathsf{M}_+} \oplus We_{\mathsf{M}_-},$$

in accordance with $n_{\mathsf{M}_+} = 1$ and $n_{\mathsf{M}_-} = 0$. The lattice $\mathcal{N}$ is the analog of $\mathcal{L}$ for the actions of type $(1,3)$ and $(3,1)$, but it is not the lattice of Weil classes of an action of type $(2,2)$, and in Chapter 9 it turns out to be the part of the gap that endomorphisms cannot leave.

Exercise 8.6. Let $\varphi(e_{\mathsf{T}_+}) = (-1)^{j_1} e_{\mathsf{T}_-}$ and $\varphi(e_{\mathsf{T}_-}) = (-1)^{j_2} e_{\mathsf{T}_+}$. Show that the φ-fixed vectors in $We_{\mathsf{T}_+} \oplus We_{\mathsf{T}_-}$ are the $\lambda e_{\mathsf{T}_+} + (-1)^{j_1}\sigma(\lambda) e_{\mathsf{T}_-}$ with $\sigma^2(\lambda) = (-1)^{j_1+j_2}\lambda$, and that whether $j_1 + j_2$ is even or odd they form a free $\mathbb{Z}_p$-module of rank 2. (For odd $j_1 + j_2$ use a square root $\sqrt{\xi'} \in \mathbb{Z}_{p^4}$ of a unit $\xi' \in \mathbb{Z}_{p^2}$ that is not a square modulo p, which satisfies $\sigma^2(\sqrt{\xi'}) = -\sqrt{\xi'}$.)

Where this is used. The gap $T^4/S \cong (\mathbb{Z}/p)^4$ is Theorem A(a) and Theorem C(a). The lattices $\mathcal{L}$ and $\mathcal{N}$ and the eigenset lemma are the input of the endomorphism proposition (Proposition 9.4) and of the proof of Theorem A(a) in Section 9.4. The eigenset lemma also identifies the Weil part of a fourfold with complex multiplication at its supersingular reduction (Proposition 12.2), and Proposition 8.7 is what makes a unit Gram determinant decide the specialized classes (Proposition 13.4).

CHAPTER 9

Endomorphisms move one Weil class onto the gap

Where we are. This chapter shows how the endomorphisms of a fourfold X with $M(X) \cong \mathbb{M}$ act on the gap $T^4/S \cong (\mathbb{Z}/p)^4$, and proves Theorem A(a). The result is that the gap is a non-split extension of $(\mathbb{Z}/p)^2$ by $(\mathbb{Z}/p)^2$, and that S together with the pull-backs of a single class in $T^4 \setminus N$ is all of T^4; in particular one Weil class with a unit coefficient suffices. This reduces Theorem A(b) to showing that the Weil lattice $\mathcal{L}$ is algebraic, which is the subject of Part IV. The chapter needs the chapters on Tate classes, on the min-plus calculus and on the gap. Its main statement, the endomorphism proposition, rests on an exact computation.

9.1. Endomorphisms and the structure of the gap in two pages

Algebraic classes are stable under pull-back by endomorphisms. So once one class x in the gap is known to be algebraic, all the classes $\alpha^* x$, $\alpha \in \mathrm{End}(X)$, are algebraic too, and the question becomes how much of T^4 they fill together with S. For a supersingular X, the comparison of homomorphisms with Dieudonné modules (Fact 4.10) identifies $\mathrm{End}(X) \otimes \mathbb{Z}_p$ with the ring $\mathrm{End}(M, F)$ of W-linear maps of $M = M(X)$ commuting with F (Fact 4.10), and spans over $\mathrm{End}(X)$ equal spans over $\mathrm{End}(M, F)$ (Lemma 9.2). For the model, $\mathrm{End}(M, F) \otimes W$ is monomial in the matrix units, and by the polarization argument of Chapter 5 every span of pull-backs is a monomial lattice with min-plus exponents. Evaluating them gives the endomorphism proposition (Proposition 9.4): S is stable; $S + \mathcal{L}$ has index p^2 in T^4 but S together with the pull-backs of $\mathcal{L}$ is all of T^4; $S + \mathcal{N}$ is stable and has index p^2.

The structure of the gap follows (Section 9.4). The lattice $N = S + \mathcal{N}$ gives a stable subgroup $N/S \cong (\mathbb{Z}/p)^2$ of the gap, and the quotient $T^4/N \cong (\mathbb{Z}/p)^2$ is the image of the Weil lattice $\mathcal{L}$. Take any $x \in T^4 \setminus N$. Modulo N it is a primitive element $\lambda e_{\mathsf{T}_+} \pm \sigma(\lambda) e_{\mathsf{T}_-}$ of $\mathcal{L}$ with λ a unit. The diagonal action of $\mathbb{Z}_{p^2}$ with eigenset T_+ lies in $\mathrm{End}(M, F)$, and its idempotent, an element of $\mathrm{End}(M, F) \otimes W$, cuts out the coordinate λe_{T_+}; since λ is a unit, the pull-backs of x reach e_{T_+} and likewise e_{T_-}, hence all of $\mathcal{L}$, and then everything. So every class outside N generates the gap, and no complement of N/S is stable: the extension does not split.

Example 9.1 (the idempotent of the diagonal action). Let $\xi \in \mathbb{Z}_p^\times$ be a non-square, so $\mathbb{Z}_{p^2} = \mathbb{Z}_p[\sqrt{\xi}]$ (Example 3.3), and let $\lambda = \iota(\sqrt{\xi}) \in W$, so that $\bar{\iota}(\sqrt{\xi}) = \sigma(\lambda) = -\lambda$. The diagonal action with eigenset T_+ (Lemma 8.4) lets $\sqrt{\xi}$ act by

$$[\sqrt{\xi}]e_s = \lambda e_s \quad (s \in \mathsf{T}_+), \qquad [\sqrt{\xi}]e_s = -\lambda e_s \quad (s \in \mathsf{T}_-).$$

This commutes with F, so $[\sqrt{\xi}] \in \mathrm{End}(\mathbb{M}, F)$, and since p is odd and λ is a unit,

$$\mathrm{pr}_{\mathsf{T}_+} = \tfrac{1}{2}(1 + \lambda^{-1}[\sqrt{\xi}]) \in \mathrm{End}(\mathbb{M}, F) \otimes W$$

is the projection onto the span of the e_s, $s \in \mathsf{T}_+$, along the span of the e_s, $s \in \mathsf{T}_-$. Its fourth exterior power $\bigwedge^4 \mathrm{pr}_{\mathsf{T}_+}$ sends e_{T_+} to itself and every other e_J to 0: it is the coordinate projection of $\bigwedge^4 \mathbb{M}$ onto $W e_{\mathsf{T}_+}$. The element $\mathrm{pr}_{\mathsf{T}_+}$ is not in $\mathrm{End}(\mathbb{M}, F)$ itself, because $\lambda \notin \mathbb{Z}_p$; it is a W-combination of the elements 1 and $[\sqrt{\xi}]$ of $\mathrm{End}(\mathbb{M}, F)$, which is all the argument needs.

9.2. Endomorphisms of X and of (M, F)

Let X be an abelian fourfold over $\bar{\mathbb{F}}_p$ with $M(X) \cong \mathbb{M}$; it is supersingular because $\mathbb{M}$ is. By Fact 4.10(b), $\alpha \mapsto \alpha^*$ identifies $\mathrm{End}(X) \otimes \mathbb{Z}_p$ with $\mathrm{End}(\mathbb{M}, F)$, reversing the order of composition, which plays no role for spans. For a subset $\Xi \subseteq T^4(X)$ write $\mathrm{End}^*\,\Xi$ for the $\mathbb{Z}_p$-span of the classes $\alpha^* x$, $\alpha \in \mathrm{End}(X)$, $x \in \Xi$.

Lemma 9.2 (spans over $\mathrm{End}(X)$). *Let $p \geq 5$. For every $\Xi \subseteq T^4(X)$, the $\mathbb{Z}_p$-span of the $\alpha^* x$ over $\alpha \in \mathrm{End}(X)$ and $x \in \Xi$ equals the $\mathbb{Z}_p$-span of the $\bigwedge^4 \alpha(x)$ over $\alpha \in \mathrm{End}(\mathbb{M}, F)$, and its W-span equals the W-span of the $\bigwedge^4 \alpha(x)$ over $\alpha \in \mathrm{End}(\mathbb{M}, F) \otimes W$ and x in the W-span of Ξ.*

Proof. Write $\mathcal{R} = \mathrm{End}(X)$, a free $\mathbb{Z}$-module of finite rank whose image $\mathcal{R}^*$ spans $\mathrm{End}(\mathbb{M}, F)$ over $\mathbb{Z}_p$. By the polarization identity of Section 5.7, the polarized values $D(\alpha_1^*, \dots, \alpha_4^*)(x)$, $\alpha_i \in \mathcal{R}$, are $\mathbb{Z}$-combinations of values $\bigwedge^4 \alpha^*(x)$ with $\alpha \in \mathcal{R}$, and $\bigwedge^4 \alpha^*(x) = \frac{1}{24} D(\alpha^*, \alpha^*, \alpha^*, \alpha^*)(x)$ with 24 a unit. So the $\mathbb{Z}_p$-span of the $\alpha^* x$, $\alpha \in \mathcal{R}$, equals the $\mathbb{Z}_p$-span of the polarized values on $\mathcal{R}^*$. Since D is multilinear, the latter equals the $\mathbb{Z}_p$-span of the polarized values on the $\mathbb{Z}_p$-span $\mathrm{End}(\mathbb{M}, F)$ of $\mathcal{R}^*$, and by the same two identities this is the $\mathbb{Z}_p$-span of the $\bigwedge^4 \alpha(x)$, $\alpha \in \mathrm{End}(\mathbb{M}, F)$. The statement over W follows in the same way, D being W-multilinear in the α_i and W-linear in x. □

For the model, $\mathrm{End}(\mathbb{M}, F) \otimes W = \bigoplus_{s,s'} p^{m_{ss'}} W e_{ss'}$ is monomial in the 64 matrix units $e_{ss'} \colon e_{s'} \mapsto e_s$ (Section 5.7). Its exponents are given by the orbit rule on pairs of vertices, with weight $s_1 - s_1'$ and 0 in place of $n/2$. Evaluating it for all 64 pairs gives the following matrix, with rows indexed by the target s and columns by the source s', both in the order $000, 001, 010, 011, 100, 101, 110, 111$:

$$(m_{ss'}) = \begin{pmatrix} 0 & 1 & 1 & 2 & 1 & 2 & 2 & 3 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 2 \\ 0 & 1 & 0 & 1 & 1 & 2 & 1 & 2 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 2 & 0 & 1 & 1 & 2 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Its entries take the value 0 twenty-eight times, 1 twenty-seven times, 2 eight times and 3 once. Any entry can be checked by hand. For instance the pair $(000, 111)$ has the orbit $(000, 111) \to (010, 101) \to (011, 100) \to (111, 000) \to (101, 010) \to (100, 011)$ under π, with weights $-1, -1, -1, +1, +1, +1$ and partial sums $0, -1, -2, -3, -2, -1$, so $m_{000,111} = 0 - (-3) = 3$ and $m_{111,000} = -3 - (-3) = 0$. The diagonal matrix units e_{ss} have exponent 0, so every diagonal endomorphism over W is in $\mathrm{End}(\mathbb{M}, F) \otimes W$, among them the idempotent $\mathrm{pr}_{\mathsf{T}_+}$ of Example 9.1. The pair $(110, 001)$ lies in the orbit $(110, 001) \to (001, 110) \to (110, 001)$ of length 2, with weights $+1, -1$, so $m_{110,001} = 0$ and $m_{001,110} = 1$: the vertices 001 and 110 span the summand M_{01} of $\mathbb{M} \cong M_{01+000111}$, and these two entries are the exponents of $\mathrm{End}(M(E_0), F)$ found in Example 5.8.

9.3. The endomorphism proposition

For the self-product we need the Künneth component of degree $(2, 2)$ (Section 4.2).

Definition 9.3 (the Künneth $(2,2)$-component). For a supersingular abelian variety X, let $T_{22} \subseteq \bigwedge^2 M(X) \otimes \bigwedge^2 M(X)$ be the image of $T^4(X \times X)$ under the Künneth projection $H^4_{\mathrm{cris}}(X \times X/W) \to \bigwedge^2 M(X) \otimes \bigwedge^2 M(X)$.

Since F preserves the Künneth decomposition, the projection of a Tate class is a Tate class, and $T_{22} = T^4(X \times X) \cap (\bigwedge^2 M(X) \otimes \bigwedge^2 M(X))$. For a homomorphism $(\alpha_1, \alpha_2) \colon X \times X \to X$, $(y_1, y_2) \mapsto \alpha_1 y_1 + \alpha_2 y_2$, the pull-back on M is $x \mapsto (\alpha_1^* x, \alpha_2^* x) \in M(X) \oplus M(X)$.

PROPOSITION 9.4 (endomorphisms, computer-assisted). *Let X be an abelian fourfold over $\bar{\mathbb{F}}_p$ with $M(X) \cong \mathbb{M}$, $p \geq 5$, and let $\mathcal{L}$, $\mathcal{N}$ be the Weil and majority lattices (Definitions 8.6 and 8.8). Then:*

(i) $\mathrm{End}^*\, S \subseteq S$;
(ii) $[T^4 : S + \mathcal{L}] = p^2$ *and* $S + \mathrm{End}^*\, \mathcal{L} = T^4$;
(iii) $\mathrm{End}^*\, \mathcal{N} \subseteq S + \mathcal{N}$ *and* $[T^4 : S + \mathcal{N}] = p^2$;
(iv) T_{22} *is spanned by the Künneth* $(2,2)$*-components of the classes in* $S(X \times X)$ *and of the classes* $(\alpha_1, \alpha_2)^* x$, $x \in \mathcal{L}$, $\alpha_1, \alpha_2 \in \mathrm{End}(X)$.

PROOF. Statement (i) holds for a simple reason: a pull-back α^* commutes with F and is a ring homomorphism of $\bigwedge^\bullet M$, so it maps T^2 into T^2 and a product $x \wedge y$ to $\alpha^* x \wedge \alpha^* y$.

Statement (ii) follows by hand from Proposition 8.2. The lattice $(S + \mathcal{L}) \otimes W$ has the exponents of $S \otimes W$ except at e_{T_+} and e_{T_-}, where it has $0 = n_{\mathsf{T}_+} = n_{\mathsf{T}_-}$. So it differs from $T^4 \otimes W$ only at e_{M_+} (exponent 2 instead of 1) and at e_{M_-} (1 instead of 0), and $[T^4 : S + \mathcal{L}] = p^2$ by Lemma 5.2. For the second half, consider the endomorphisms $\alpha = 1 + e_{110,001}$ and $\alpha' = 1 + p e_{001,110}$ of $\mathbb{M}$, which lie in $\mathrm{End}(\mathbb{M}, F) \otimes W$ because $m_{110,001} = 0$ and $m_{001,110} = 1$. Since $e_{110,001}$ kills every basis vector except e_{001}, which it sends to e_{110},

$$\textstyle\bigwedge^4 \alpha(e_{\mathsf{T}_-}) = (e_{001} + e_{110}) \wedge e_{010} \wedge e_{100} \wedge e_{111} = e_{\mathsf{T}_-} \pm e_{\mathsf{M}_-},$$

and in the same way $\bigwedge^4 \alpha'(e_{\mathsf{T}_+}) = e_{000} \wedge e_{011} \wedge e_{101} \wedge (e_{110} + p e_{001}) = e_{\mathsf{T}_+} \pm p e_{\mathsf{M}_+}$. By Lemma 9.2, the W-span of $\mathrm{End}^*\, \mathcal{L}$ contains these vectors and $e_{\mathsf{T}_+}, e_{\mathsf{T}_-}$, hence e_{M_-} and $p e_{\mathsf{M}_+}$. So $(S + \mathrm{End}^*\, \mathcal{L}) \otimes W$ has exponent at most n_J at every e_J: 0 at $e_{\mathsf{T}_+}, e_{\mathsf{T}_-}, e_{\mathsf{M}_-}$, 1 at e_{M_+}, and $n^S_J = n_J$ elsewhere. As it lies in $T^4 \otimes W$, it equals $T^4 \otimes W$, and $S + \mathrm{End}^*\, \mathcal{L} = T^4$ by Lemma 5.2.

For (iii) and (iv), by Lemma 9.2 the spans may be taken over $\mathrm{End}(\mathbb{M}, F)$, and then, after $\otimes W$, over its monomial generators. By Lemma 5.3 and Proposition 5.10, every lattice in these statements is monomial over W with exponents given by min-plus expressions in the integers $w(s) = s_1$, and inclusions and indices are comparisons and sums of exponents (Lemma 5.2). For (iv) the same holds for the pull-backs along (α_1, α_2): by the proof of Lemma 9.2, applied to the maps $\gamma = (\alpha_1^*, \alpha_2^*) \colon \mathbb{M} \to \mathbb{M} \oplus \mathbb{M}$ that commute with F and to $\gamma \mapsto \bigwedge^4 \gamma$ followed by the Künneth projection, the span may be taken over the monomial generators $\gamma = (p^{m_{ss'}} e_{ss'}, 0)$ and $\gamma = (0, p^{m_{ss'}} e_{ss'})$. The $(2,2)$-entry of $\bigwedge^4 \gamma$ from e_J to $e_{J'_1} \otimes e_{J'_2}$ is a signed sum, over the splittings $J = J_1 \sqcup J_2$, of products of a 2×2 minor of α_1^* and one of α_2^*, and on polarized monomial generators each value is a single signed monomial. The $(2,2)$-components of the products of divisor classes on $X \times X$ are monomial with min-plus exponents in the same way. The values of these exponents are an exact computation, described below. The computation also confirms (i) and (ii). □

Remark on the proof 9.1: the computation behind Proposition 9.4. The computation evaluates, for the model, the exponents $m_{ss'}$ of $\mathrm{End}(\mathbb{M}, F) \otimes W$ by the orbit rule on the 64 pairs of vertices; the exponents of $\mathrm{End}^*\, \Xi$ for $\Xi = S, \mathcal{L}, \mathcal{N}$ by Proposition 5.10, as minima over 4-sets J and bijections $J \to J'$; and compares them with the exponents $n_{J'}$ of T^4 and $n^S_{J'}$ of S. For (iv) it computes the exponents of T_{22} by the orbit rule on the $28 \times 28 = 784$ pairs of 2-sets, those of the $(2,2)$-components of divisor products (products of classes of Künneth types $(2,0) \cdot (0,2)$ and $(1,1) \cdot (1,1)$), and those of the $(2,2)$-components of the pull-backs of $\mathcal{L}$, which split a 4-set into two 2-sets sent to the two factors. All quantities are integers built from the eight values s_1, so the result is exact and the same for every $p \geq 5$; the prime enters only through the unit 4! in Lemma 9.2. The outputs are: (i) inclusion; (ii) the indices p^2 and 1; (iii) inclusion and index p^2; (iv) the index of the span of divisor products alone in T_{22} is p^{24}, and with the pull-backs of $\mathcal{L}$ it is 1. Parts (i) and (ii) also have the hand proofs given above; parts (iii) and (iv) rest on the computation alone.

EXAMPLE 9.5 (the size of the Künneth component). For X a fourfold, $M(X\times X) = M\oplus M$ has rank 16, and $\bigwedge^4(M\oplus M) = \bigoplus_{i=0}^4 \bigwedge^i M\otimes\bigwedge^{4-i}M$ has rank $\binom{16}{4} = 1820 = 70+448+784+448+70$. The component of degree $(2,2)$ has rank $\binom{8}{2}^2 = 28\cdot 28 = 784$, so T_{22} is a free $\mathbb{Z}_p$-module of rank 784, and statement (iv) is a statement about 784 exponents. Divisor products alone span a sublattice of index p^{24} in it, and adding the pull-backs of the rank-2 lattice $\mathcal{L}$ along all homomorphisms $X\times X\to X$ closes the whole gap.

Intuition 9.6 (why $\mathcal{L}$ and not $\mathcal{N}$). Statement (iii) says that $\mathcal{N}$ is a dead end: whatever endomorphisms do to it, they stay inside $S+\mathcal{N}$, which misses p^2. Statement (ii) says the opposite for $\mathcal{L}$: alone it misses p^2 too, but its pull-backs by endomorphisms reach everything, including $\mathcal{N}$. The proof of (ii) shows how: the endomorphism $1+e_{110,001}$ of the elliptic-curve summand $M_{01} = \langle e_{001}, e_{110}\rangle$ of $\mathbb{M}$ replaces the vertex 001 of T_- by 110 and turns the Weil class into a majority class. In the opposite direction, from M_- back to T_-, the same move costs a factor p, because $m_{001,110} = 1$; statement (iii), which rests on the computation, says that no combination of moves gets from $\mathcal{N}$ to the Weil classes without such a loss. So the classes to look for are the Weil classes of an action of type $(2,2)$, and only one of them, with a unit coefficient, is needed. This is what Part IV constructs under Hypothesis (M).

EXERCISE 9.1. For endomorphisms α_1,α_2 of a free module M and an integer j, show that $\bigwedge^4(j\alpha_1+\alpha_2) = \sum_{i=0}^4 j^i D_i(\alpha_1,\alpha_2)$, where $D_i(\alpha_1,\alpha_2)(x_1\wedge\cdots\wedge x_4)$ is the sum of the terms with α_1 applied to exactly i of the x_l and α_2 to the others. Show that the D_i are determined by the values for $j = 0,1,2,3,4$ when $p\geq 5$, by inverting a Vandermonde matrix modulo p. (This is the device that extracts Künneth components in Chapter 14.)

9.4. Proof of Theorem A(a)

We prove the statements of Theorem A(a) for every abelian fourfold X over $\bar{\mathbb{F}}_p$ with an isomorphism $M(X)\cong\mathbb{M}$. At the supersingular points of Theorem A, $M(X)\cong\mathbb{M}$ by the model proposition (Proposition 7.4), so this proves Theorem A(a); for the fourfolds X of Theorem C, $M(X)\cong\mathbb{M}$ by Dieudonné theory, so it also gives Theorem C(a) (Chapter 14). Throughout, $S = S(X)$, $T^4 = T^4(X)$, $\mathcal{L}$ and $\mathcal{N}$ are taken with respect to the fixed isomorphism, and $N = S+\mathcal{N}$.

Step 1: the gap. $T^4/S\cong(\mathbb{Z}/p)^4$ by Proposition 8.2.

Step 2: $N/S\cong(\mathbb{Z}/p)^2$. The lattice $N\otimes W = S\otimes W+\mathcal{N}\otimes W$ is monomial with the smaller of the two exponents at each e_J. By Proposition 8.2 and $\mathcal{N}\otimes W = pWe_{\mathsf{M}_+}\oplus We_{\mathsf{M}_-}$, it has exponent $\min(2,1) = 1 = n_{\mathsf{M}_+}$ at e_{M_+}, exponent $\min(1,0) = 0 = n_{\mathsf{M}_-}$ at e_{M_-}, and n_J^S elsewhere. So $N\otimes W$ and $S\otimes W$ differ only at e_{M_+} and e_{M_-}, each by one power of p; by Lemma 5.2, N/S has order p^2 and is killed by p.

Step 3: N is stable. $\mathrm{End}^*S\subseteq S$ and $\mathrm{End}^*\mathcal{N}\subseteq S+\mathcal{N}$ by Proposition 9.4(i) and (iii), so $\mathrm{End}^*N\subseteq N$.

Step 4: T^4/N is the image of $\mathcal{L}$. The exponents of $N\otimes W$ are n_J except at e_{T_+} and e_{T_-}, where they are $n^S_{\mathsf{T}_+} = n^S_{\mathsf{T}_-} = 1$, while $\mathcal{L}\otimes W = We_{\mathsf{T}_+}\oplus We_{\mathsf{T}_-}$ (Proposition 8.7). So $(N+\mathcal{L})\otimes W = T^4\otimes W$, and $N+\mathcal{L} = T^4$ by Lemma 5.2. Moreover $p\mathcal{L}\otimes W = pWe_{\mathsf{T}_+}\oplus pWe_{\mathsf{T}_-}\subseteq S\otimes W$, so $p\mathcal{L}\subseteq S\subseteq N$. Since $T^4/N\cong\mathcal{L}/(\mathcal{L}\cap N)$ has order $p^4/p^2 = p^2 = [\mathcal{L}:p\mathcal{L}]$, we get $\mathcal{L}\cap N = p\mathcal{L}$, and $T^4/N\cong\mathcal{L}/p\mathcal{L}\cong(\mathbb{Z}/p)^2$.

Step 5: a class outside N generates. Let $x\in T^4\setminus N$. By Step 4, $x = y+x'$ with $y\in N$ and $x'\in\mathcal{L}$, and $x'\notin p\mathcal{L}$ because $x\notin N$. By Proposition 8.7, $x' = \lambda e_{\mathsf{T}_+}\pm\sigma(\lambda)e_{\mathsf{T}_-}$ with $\lambda\in W^\times$. Let $\mathrm{pr}_{\mathsf{T}_+}$ be the idempotent of Example 9.1. Then $\bigwedge^4\mathrm{pr}_{\mathsf{T}_+}(x') = \lambda e_{\mathsf{T}_+}$, and $\bigwedge^4\mathrm{pr}_{\mathsf{T}_+}(y)\in S\otimes W$: indeed $y\in S\otimes W+\mathcal{N}\otimes W$, the coordinate projection $\bigwedge^4\mathrm{pr}_{\mathsf{T}_+}$ maps the monomial lattice $S\otimes W$ into itself, and it kills e_{M_+} and e_{M_-}. So

$$\bigwedge^4\mathrm{pr}_{\mathsf{T}_+}(x)\equiv\lambda e_{\mathsf{T}_+}\pmod{S\otimes W}.$$

By Lemma 9.2, $\bigwedge^4 \mathrm{pr}_{\mathsf{T}_+}(x)$ lies in the W-span of $\mathrm{End}^*\{x\}$, because $\mathrm{pr}_{\mathsf{T}_+} \in \mathrm{End}(\mathbb{M}, F) \otimes W$. As λ is a unit, $e_{\mathsf{T}_+} \in (S + \mathrm{End}^*\{x\}) \otimes W$. The conjugate idempotent $\mathrm{pr}_{\mathsf{T}_-} = 1 - \mathrm{pr}_{\mathsf{T}_+}$, the projection onto the span of the e_s with $s \in \mathsf{T}_-$, gives e_{T_-} in the same way. So $(S + \mathrm{End}^*\{x\}) \otimes W \supseteq \mathcal{L} \otimes W$, and $S + \mathrm{End}^*\{x\} \supseteq \mathcal{L}$ by Lemma 5.2. The lattice $S + \mathrm{End}^*\{x\}$ is stable under $\mathrm{End}(X)$, since S is and $\alpha'^*\alpha^* x = (\alpha\alpha')^* x$. Hence it contains $S + \mathrm{End}^* \mathcal{L}$, which is T^4 by Proposition 9.4(ii).

Step 6: the extension does not split. Suppose N/S had an $\mathrm{End}(X)$-stable complement in T^4/S. The complement has order p^2 and contains the image of some $x \in T^4 \setminus N$. By Step 5, the $\mathrm{End}(X)$-translates of x together with S span T^4, so the complement is T^4/S, of order p^4, a contradiction. So T^4/S is a non-split extension of $T^4/N \cong (\mathbb{Z}/p)^2$ by $N/S \cong (\mathbb{Z}/p)^2$ as a module over $\mathrm{End}(X)$. This completes the proof of Theorem A(a).

What just happened. The gap has two layers. The bottom layer N/S, carried by the majority sets, is stable under endomorphisms. The top layer T^4/N is the reduction of the Weil lattice $\mathcal{L}$, and any class that reaches the top layer reaches everything, because the idempotent of the diagonal action of type $(2, 2)$ isolates its Weil coordinate, which is a unit, and the endomorphism proposition carries $\mathcal{L}$ onto all of T^4. Nothing in the argument uses algebraic cycles: it is linear algebra over W plus one exact computation.

Exercise 9.2. Let M be any monomial Dieudonné module as in Section 5.3 and let $\mathbb{Z}_{p^2}$ act diagonally on the basis with characters $\iota_s \in \{\iota, \bar{\iota}\}$. Show that the action commutes with F if and only if $\iota_{\pi(s)} = \bar{\iota}_s$ for all s, and deduce that such an action exists if and only if every orbit of π has even length, which is always the case.

Exercise 9.3. Let $\mathcal{U} = \mathbb{F}_{p^2} \oplus \mathbb{F}_{p^2}$, an $\mathbb{F}_p$-vector space of dimension 4, and let $\mathcal{R}$ be the set of maps $(y_0, y) \mapsto (\lambda y_0 + \gamma(y), \lambda y)$ with $\lambda \in \mathbb{F}_{p^2}$ and $\gamma\colon \mathbb{F}_{p^2} \to \mathbb{F}_{p^2}$ an arbitrary $\mathbb{F}_p$-linear map. Show that $\mathcal{R}$ is a ring under composition, that $\mathcal{U}_0 = \mathbb{F}_{p^2} \oplus 0$ is stable under $\mathcal{R}$, that $\mathcal{R}x = \mathcal{U}$ for every $x \notin \mathcal{U}_0$, and conclude that $\mathcal{U}$ is a non-split extension of $\mathcal{U}/\mathcal{U}_0 \cong (\mathbb{Z}/p)^2$ by $\mathcal{U}_0 \cong (\mathbb{Z}/p)^2$ as an $\mathcal{R}$-module. Which parts of the proof of Theorem A(a) do λ and γ imitate?

Exercise 9.4. Let pr_J be the projection of a free module with basis (e_s) onto the span of the e_s, $s \in J$, with $|J| = 4$, along the other basis vectors. Show that $\bigwedge^4 \mathrm{pr}_J(e_{J'}) = e_{J'}$ if $J' = J$ and 0 otherwise, for $|J'| = 4$, and describe $\bigwedge^2 \mathrm{pr}_J$.

Exercise 9.5. Compute the ranks of the five Künneth components of $\bigwedge^4(M \oplus M)$ for M of rank 8 and check that they add up to $\binom{16}{4}$.

Where this is used. Theorem A(a), proved here, is the first half of Theorems A and C. In the proof of Theorem A(b) (Chapter 14) the endomorphism proposition turns the inclusion $\mathcal{L} \subseteq \mathrm{Alg}^2$ at one supersingular point, produced in Chapter 13 under Hypothesis (M), into $\mathrm{Alg}^2 = T^4$, and part (iv) gives the algebraicity of the Künneth component T_{22}. The same computations for the other monomial modules are made in Chapter 15.

Part IV

Filling the gap with one Weil cycle

CHAPTER 10

Weil classes, Hermitian forms and unimodular lattices

Where we are. Under Hypothesis (M), Part IV produces one algebraic class in the Weil lattice $\mathcal{L}$ of the gap. This chapter supplies the linear algebra it needs: abelian varieties of Weil type and their Weil classes with coefficients in $\mathbb{Z}_{(p)}$, the Hermitian form of a polarization, with its conventions fixed once for the companion, unimodular Hermitian lattices at an inert prime, and Schoen's step in lattice form (Proposition 10.9), which moves a fourfold into the family of a given abelian sixfold by an isogeny of degree prime to p. It needs the reminder on complex abelian varieties in Chapter 2 and the p-adic numbers.

10.1. Weil classes in two pages

Let K be an imaginary quadratic field and X a complex abelian variety of dimension $2n$ on which K acts by endomorphisms (up to isogeny). The action splits the holomorphic 1-forms $H^{1,0}(X)$ into the eigenspaces of the two embeddings $\iota, \bar{\iota}$ of K into $\mathbb{C}$, and the pair of their dimensions (g_+, g_-), $g_+ + g_- = 2n$, is the *type* of the action. When $g_+ = g_- = n$, X is of *Weil type*. Then $H^1(X, \mathbb{Q}) \otimes K$ splits into two eigenspaces of dimension $2n$ over K, and the top exterior powers ω and $\bar{\omega}$ of these eigenspaces lie in $H^{2n}(X) \otimes K$. Weil observed that ω and $\bar{\omega}$ are of Hodge type (n, n), so the rational combinations $\nu\omega + \bar{\nu}\bar{\omega}$, $\nu \in K$, form a 2-dimensional space of Hodge classes, the *Weil classes*. For $n \geq 2$ a very general X of Weil type has Weil classes that are not combinations of products of divisor classes; that is the reason they are a test case for the Hodge conjecture, and the reason they appear in the gap T^4/S of Chapter 8.

The proof needs Weil classes with coefficients in $\mathbb{Z}_{(p)}$, and needs to know when an algebraic Weil class has a coefficient ν that is a unit at p. If p is inert in K and O_K acts on $H^1(X, \mathbb{Z}_{(p)})$, the eigenspaces have lattices H^1_ι, $H^1_{\bar{\iota}}$, ω is the top exterior power of an $O_{K,(p)}$-basis of H^1_ι, and the integral Weil classes at p are the $\nu\omega + \bar{\nu}\bar{\omega}$ with $\nu \in O_{K,(p)}$. A polarization makes $H_1(X, \mathbb{Z}_{(p)})$ a Hermitian lattice over $O_{K,(p)}$, and the one idea of this chapter is that *unimodular* Hermitian lattices at an inert prime are rigid: two of the same rank are isometric (Fact 10.7). Schoen's step uses this to compare the lattice of a fourfold, plus an auxiliary surface, with the lattice of a sixfold, and obtains an isogeny of degree prime to p between the product and a member of the sixfold's family (Proposition 10.9). Pull-backs and push-forwards along it change Weil coefficients only by units at p.

Example 10.1 ($K = \mathbb{Q}(\sqrt{-2})$ at $p = 5$). The squares modulo 5 are $0, 1, 4$, and $-2 \equiv 3$ is not among them, so 5 is inert in $K = \mathbb{Q}(\sqrt{-2})$: $O_K/5 = \mathbb{F}_5[\sqrt{-2}] \cong \mathbb{F}_{25}$, $K_5 = \mathbb{Q}_{25}$ and $O_{K,5} = \mathbb{Z}_{25}$. The norm $\mathrm{Nm}(x + y\sqrt{-2}) = x^2 + 2y^2$ of a nonzero element of $O_{K,5}$ has even valuation at 5, because $x^2 + 2y^2 \equiv 0 \bmod 5$ forces $x \equiv y \equiv 0$ (Exercise 10.3). The Hermitian form $h = \mathrm{diag}(1, -1)$ on $O_{K,5}^2$ has determinant -1, a unit, so the lattice $O_{K,5}^2$ is unimodular. Over K the form $\mathrm{diag}(1, -1)$ has signature $(1, 1)$. By contrast, the Hermitian space $\mathrm{diag}(1, -5)$ has determinant -5, of odd valuation; since a change of basis multiplies the determinant by a norm, which has even valuation, no lattice in this space is unimodular at 5.

10.2. Abelian varieties of Weil type

Let $K = \mathbb{Q}(\theta)$ with $\theta = \sqrt{-d_0}$, d_0 a positive squarefree integer. Fix embeddings $\overline{\mathbb{Q}} \subset \mathbb{C}$ and $\overline{\mathbb{Q}} \subset \overline{\mathbb{Q}}_p$, and an embedding of $W[1/p]$ into the completion of $\overline{\mathbb{Q}}_p$. Let $\iota\colon K \to \mathbb{C}$ be the embedding with $\operatorname{Im}\iota(\theta) > 0$, and $\bar\iota$ its conjugate. If p is unramified in K, the completion of $\iota(K) \subset \overline{\mathbb{Q}} \subset \overline{\mathbb{Q}}_p$ lies in $W[1/p]$, so ι also defines a ring homomorphism $O_K \otimes \mathbb{Z}_p \to W$, which we call ι as well, and $\bar\iota$ is the other one.

Definition 10.2 (type of a K-action). Let X be an abelian variety of dimension g with an embedding $K \hookrightarrow \operatorname{End}(X) \otimes \mathbb{Q}$.

(a) Over $\mathbb{C}$, the *type* of the action is the pair (g_+, g_-) of multiplicities of ι and $\bar\iota$ on $H^{1,0}(X) = H^0(X, \Omega^1)$, on which K acts by pull-back. So $g_+ + g_- = g$.

(b) Over $\overline{\mathbb{F}}_p$, with p unramified in K and $O_K \otimes \mathbb{Z}_p$ acting on $M(X)$, the *type* is the pair of multiplicities of ι and $\bar\iota$ on $VM(X)/pM(X) \cong H^0(X, \Omega^1)$ (Fact 3.10).

The action is of *Weil type* if $g_+ = g_-$.

The two definitions are compatible under reduction: if X is the special fiber of an abelian scheme over a discrete valuation ring of characteristic 0, with an action of an order of K of conductor prime to p, the eigen-ranks of O_K on the cotangent space of the abelian scheme are locally constant, because p is unramified in K, so the type of the special fiber equals the type of the generic fiber. This is how the type $(2,2)$ is read off at a supersingular point in Lemma 8.4.

Assume now that p is unramified in K and that O_K acts on $H^1(X, \mathbb{Z}_{(p)})$, which holds when $\operatorname{End}(X) \cap K$ is an order of conductor prime to p. Since $O_K \otimes O_K \to O_K \times O_K$, $\lambda \otimes \lambda' \mapsto (\lambda\lambda', \lambda\bar\lambda')$, becomes an isomorphism after inverting the discriminant of K, which is a unit at p, there is a decomposition

$$H^1(X, \mathbb{Z}_{(p)}) \otimes_{\mathbb{Z}_{(p)}} O_{K,(p)} = H^1_\iota \oplus H^1_{\bar\iota} \tag{10.1}$$

into free $O_{K,(p)}$-modules: on H^1_ι an element $\lambda \in O_K$, acting on the first factor by pull-back, acts as multiplication by λ in the second factor, and on $H^1_{\bar\iota}$ as multiplication by $\bar\lambda$. These are the *eigenlattices*. Complex conjugation on the coefficient $O_{K,(p)}$ exchanges them. Since $H^n(X) = \bigwedge^n H^1(X)$,

$$H^n(X, \mathbb{Z}_{(p)}) \otimes O_{K,(p)} = \bigoplus_{i+j=n} \textstyle\bigwedge^i H^1_\iota \otimes \bigwedge^j H^1_{\bar\iota},$$

and a class has *K-type* (i,j) if it lies in the summand $\bigwedge^i H^1_\iota \otimes \bigwedge^j H^1_{\bar\iota}$. An element $b \in O_K$ acts by pull-back on the K-type (i,j) by $b^i\bar b^j$.

Definition 10.3 (Weil classes). Let X be of Weil type for K, of dimension $2n$, with p and O_K as above. Let ω be the exterior product of an $O_{K,(p)}$-basis of H^1_ι, a generator of the rank-one module $\bigwedge^{2n} H^1_\iota$, and $\bar\omega$ its complex conjugate, which generates $\bigwedge^{2n} H^1_{\bar\iota}$. The *Weil part* of H^{2n} is the summand of K-types $(2n,0)$ and $(0,2n)$, and the *integral Weil classes at p* are

$$\{\nu\omega + \bar\nu\bar\omega : \ \nu \in O_{K,(p)}\} \ \subset \ H^{2n}(X, \mathbb{Z}_{(p)}),$$

a free $\mathbb{Z}_{(p)}$-module of rank 2.

The classes $\nu\omega + \bar\nu\bar\omega$ are fixed by complex conjugation on the coefficients, so they lie in $H^{2n}(X, \mathbb{Z}_{(p)})$, and every element of $H^{2n}(X, \mathbb{Z}_{(p)})$ in the Weil part has this form, because $\bigwedge^{2n} H^1_\iota$ is a direct summand of $H^{2n}(X, \mathbb{Z}_{(p)}) \otimes O_{K,(p)}$. So the integral Weil classes at p are a saturated sublattice: an integral Weil class at p is divisible by p in $H^{2n}(X, \mathbb{Z}_{(p)})$ exactly when $\nu \in pO_{K,(p)}$. If p is inert in K, $O_{K,(p)}$ is a local ring with maximal ideal $pO_{K,(p)}$, and a Weil class $\nu\omega + \bar\nu\bar\omega$ is primitive exactly when ν is a unit. The basis chosen for ω changes ω by a unit of $O_{K,(p)}$, which does not affect this.

Exercise 10.1. Let X be a complex abelian fourfold of Weil type $(2,2)$ for K. Show that $H^1_\iota \otimes_{O_K,\iota} \mathbb{C} = H^{1,0}_\iota \oplus H^{0,1}_\iota$, where $H^{1,0}_\iota$ is the ι-eigenspace in $H^{1,0}$ and $H^{0,1}_\iota$ is the complex conjugate of the $\bar\iota$-eigenspace in $H^{1,0}$, and that both have dimension 2. Deduce that ω has Hodge type $(2,2)$. What is the Hodge type of ω for a fourfold of type $(1,3)$?

10.3. Hermitian forms

Let $X = H_1(X,\mathbb{R})/H_1(X,\mathbb{Z})$ be a complex abelian variety, with complex structure $\mathcal{J}$ on $H_1(X,\mathbb{R})$. A polarization is given by its *Riemann form*, an alternating form $\psi\colon H_1(X,\mathbb{Z}) \times H_1(X,\mathbb{Z}) \to \mathbb{Z}$ with

$$\psi(\mathcal{J}x,\mathcal{J}y) = \psi(x,y), \qquad \psi(\mathcal{J}x,x) > 0 \ \text{ for } x \neq 0.$$

This fixes the sign once for the companion. With it, $\psi(\mathcal{J}x,y) + \mathrm{i}\psi(x,y)$ is a positive definite Hermitian form on the complex vector space $(H_1(X,\mathbb{R}),\mathcal{J})$, which is how a Riemann form is usually described (see e.g. [Mil08, Chapter I, Lemma 2.4 and the definition after it]). The Rosati involution of the polarization restricts to complex conjugation on K exactly when $\psi(\lambda x,y) = \psi(x,\bar\lambda y)$ for $\lambda \in K$ acting on $H_1(X,\mathbb{Q})$; the polarization is then called *compatible* with K.

Definition 10.4 (the Hermitian form of a polarization). Let ψ be compatible with K. The *skew-Hermitian form* of ψ is the unique form $\mathcal{H}\colon H_1(X,\mathbb{Q}) \times H_1(X,\mathbb{Q}) \to K$, K-linear in the first variable, with $\mathcal{H}(y,x) = -\overline{\mathcal{H}(x,y)}$ and

$$\psi = \mathrm{Tr}_{K/\mathbb{Q}} \circ \mathcal{H}.$$

The *Hermitian form* of ψ is $h = \theta\mathcal{H}$. Its *signature* is the pair (number of positive, number of negative) entries of a diagonal form of h over $\mathbb{R}$, and its *determinant* $\det h$ is the determinant of a Gram matrix of h in a K-basis, a rational number well defined modulo norms from K.

Explicitly, writing $\mathcal{H}(x,y) = \lambda + \lambda'\theta$ with $\lambda,\lambda' \in \mathbb{Q}$ and comparing $\psi(x,y) = 2\lambda$ and $\psi(\theta x,y) = \mathrm{Tr}(\theta\mathcal{H}(x,y)) = -2d_0\lambda'$,

$$\mathcal{H}(x,y) = \tfrac12\psi(x,y) - \tfrac{\theta}{2d_0}\psi(\theta x,y), \qquad h(x,y) = \tfrac{\theta}{2}\psi(x,y) + \tfrac12\psi(\theta x,y). \tag{10.2}$$

This formula proves uniqueness, and existence follows by checking that the right-hand side has the required properties (Exercise 10.2). A change of K-basis by a matrix γ multiplies $\det h$ by $\det\gamma \cdot \overline{\det\gamma} = \mathrm{Nm}(\det\gamma)$, and $\det h$ is rational because a Hermitian matrix has real determinant.

Proposition 10.5 (signature equals type). *If ψ is compatible with K and the action of K on X has type (g_+,g_-), then h has signature (g_+,g_-).*

Proof. On $H_1(X,\mathbb{R})$, θ commutes with $\mathcal{J}$, so $H_1(X,\mathbb{R}) = \mathcal{V}_+ \oplus \mathcal{V}_-$ with $\theta = \sqrt{d_0}\mathcal{J}$ on $\mathcal{V}_+$ and $\theta = -\sqrt{d_0}\mathcal{J}$ on $\mathcal{V}_-$. The tangent space of X at 0 is $(H_1(X,\mathbb{R}),\mathcal{J})$, so K acts on it through ι on $\mathcal{V}_+$ and through $\bar\iota$ on $\mathcal{V}_-$, and $H^{1,0}$, its complex dual, has the same multiplicities: $\dim_{\mathbb{C}}\mathcal{V}_+ = g_+$ and $\dim_{\mathbb{C}}\mathcal{V}_- = g_-$. Extend $\mathcal{H}$ and h to $H_1(X,\mathbb{R})$, which is a module over $K \otimes \mathbb{R} = \mathbb{C}$ through ι, so that θ acts as $\mathrm{i}\sqrt{d_0}$. For $x \in \mathcal{V}_+$ we have $\mathcal{J}x = \theta x/\sqrt{d_0}$, so $\mathcal{H}(\mathcal{J}x,x) = \mathrm{i}\mathcal{H}(x,x)$ and

$$\psi(\mathcal{J}x,x) = \mathrm{Tr}\,\mathcal{H}(\mathcal{J}x,x) = \mathrm{Tr}\left(\tfrac{1}{\sqrt{d_0}}\theta\mathcal{H}(x,x)\right) = \tfrac{2}{\sqrt{d_0}}h(x,x),$$

using that $h(x,x)$ is real. Positivity of ψ gives $h(x,x) > 0$ on $\mathcal{V}_+$. For $x \in \mathcal{V}_-$, $\mathcal{J}x = -\theta x/\sqrt{d_0}$ and the same computation gives $h(x,x) < 0$. The subspaces $\mathcal{V}_\pm$ are h-orthogonal, because $\mathcal{J}$ preserves h and acts on $\mathcal{V}_+ \times \mathcal{V}_-$ by $h(\mathrm{i}x,-\mathrm{i}y) = -h(x,y)$. So h has signature (g_+,g_-). □

Example 10.6 (the sign check on an elliptic curve). Let $K = \mathbb{Q}(\mathrm{i})$, $\theta = \mathrm{i}$, $d_0 = 1$, and $X = \mathbb{C}/\mathbb{Z}[\mathrm{i}]$ with K acting by multiplication, which has type $(1,0)$: the pull-back of $\mathrm{d}z$ by multiplication by λ is $\lambda\mathrm{d}z$. The form $\psi(x,y) = \mathrm{Im}(x\bar y)$ is integral on $\mathbb{Z}[\mathrm{i}]$, with $\psi(1,\mathrm{i}) = \mathrm{Im}(-\mathrm{i}) = -1$, and $\psi(\mathrm{i}x,x) = |x|^2 > 0$, so it is the Riemann form of the principal polarization in our convention. By (10.2), $h(x,y) = \frac{\mathrm{i}}{2}\mathrm{Im}(x\bar y) + \frac12\mathrm{Im}(\mathrm{i}x\bar y) = \frac{\mathrm{i}}{2}\mathrm{Im}(x\bar y) + \frac12\mathrm{Re}(x\bar y) = \frac12 x\bar y$,

which is positive definite: signature $(1,0)$, equal to the type. With the conjugate action, λ acting by multiplication by $\bar\lambda$, the type is $(0,1)$ and $h(x,y) = -\frac{1}{2}\bar x y$ is negative definite.

EXERCISE 10.2. Show directly from (10.2) and the compatibility $\psi(\lambda x, y) = \psi(x, \bar\lambda y)$ that $\mathcal{H}$ is K-linear in the first variable and skew-Hermitian, that $\operatorname{Tr}_{K/\mathbb{Q}} \mathcal{H} = \psi$, and that $h = \theta\mathcal{H}$ is Hermitian, $h(y,x) = \overline{h(x,y)}$.

10.4. Unimodular Hermitian lattices at an inert prime

Let p be inert in K, so that $K_p = K \otimes \mathbb{Q}_p = \mathbb{Q}_{p^2}$ and $O_{K,p} = \mathbb{Z}_{p^2}$, and the conjugation of K is the Frobenius σ of $\mathbb{Q}_{p^2}$. A *Hermitian lattice* over $O_{K,p}$ is a free $O_{K,p}$-module L of finite rank with a nondegenerate Hermitian form $h\colon L \times L \to K_p$. It is *unimodular* if $h(L,L) \subseteq O_{K,p}$ and L equals its dual $\{x \in L \otimes \mathbb{Q} : h(x,L) \subseteq O_{K,p}\}$, equivalently if the Gram matrix in an $O_{K,p}$-basis has entries in $O_{K,p}$ and a determinant that is a unit. The same definitions apply over $O_{K,(p)}$. A Hermitian lattice is unimodular exactly when its dual lattice is, so for questions of unimodularity at p it does not matter whether the form is put on H_1 or on H^1.

Since θ is a unit at p, $h = \theta\mathcal{H}$ and $\mathcal{H}$ have the same dual lattices and determinants that differ by θ^{rk}, a unit. So in what follows we say that $H_1(X, \mathbb{Z}_{(p)})$ is a *unimodular Hermitian lattice* when h, or equivalently $\mathcal{H}$, is unimodular on it.

FACT 10.7 (unimodular Hermitian lattices). *Let p be an odd prime inert in K.*
(a) Two unimodular Hermitian lattices over $O_{K,p}$ of the same rank are isometric.
(b) A nondegenerate Hermitian space over K_p contains a unimodular lattice if and only if its determinant has even valuation.

For (a) see e.g. [Yu12, Section 2], where it is attributed to [Jac62]; for (b) see e.g. [Yu12, Section 2] together with the fact that the norms from $K_p^\times$ are the elements of $\mathbb{Q}_p^\times$ of even valuation [Voi21, p. 13.2.5]. The necessity in (b) is Exercise 10.3: the determinant of a unimodular lattice is a unit, and a change of basis changes it by a norm from K_p, which has even valuation.

EXERCISE 10.3. Let p be inert in K. Show that the norm $\mathrm{Nm}(x) = x\bar x$ of every $x \in K_p^\times$ has even valuation, by writing $x = p^n\lambda$ with $\lambda \in O_{K,p}^\times$ and showing that $\mathrm{Nm}(\lambda)$ is a unit. For $K = \mathbb{Q}(\sqrt{-2})$ and $p = 5$, show directly that $x^2 + 2y^2 \equiv 0 \bmod 5$ implies $x \equiv y \equiv 0 \bmod 5$.

EXERCISE 10.4. Let $h = \operatorname{diag}(\lambda_1, \dots, \lambda_n)$ on K_p^n with $\lambda_i \in \mathbb{Q}_p^\times$. Show that the standard lattice $O_{K,p}^n$ is unimodular if and only if every λ_i is a unit, that $\det h = \lambda_1 \cdots \lambda_n$, and that the class of $v_p(\det h)$ modulo 2 does not depend on the basis. Using Fact 10.7(b), decide which of the spaces $\operatorname{diag}(1,-1)$, $\operatorname{diag}(5,-5)$, $\operatorname{diag}(1,-5)$ over $\mathbb{Q}_{25}$ contain a unimodular lattice.

Two more inputs concern Hermitian spaces over K itself. Nondegenerate Hermitian spaces over K of the same dimension are isometric if and only if they have the same signature and determinants that agree modulo norms from K, and every signature occurs together with every determinant of the matching sign; for this classification see e.g. [Sch98, Section 7], where Schoen uses it in the same argument. The second input is the following lemma, which replaces weak approximation for unitary groups by an explicit argument with the Cayley transform.

LEMMA 10.8 (approximation in the unitary group). *Let $\mathcal{V}$ be a nondegenerate Hermitian space over K, $\mathrm{U}(\mathcal{V})$ its unitary group, $\gamma_p \in \mathrm{U}(\mathcal{V})(\mathbb{Q}_p)$, and $\mathsf{S}_p \subseteq \mathrm{U}(\mathcal{V})(\mathbb{Q}_p)$ an open subgroup that contains the scalars of norm 1 in $O_{K,p}^\times$. Then the coset $\gamma_p\mathsf{S}_p$ contains an element of $\mathrm{U}(\mathcal{V})(\mathbb{Q})$.*

PROOF. For a scalar λ of norm 1, the element $\lambda\gamma_p$ has -1 as an eigenvalue only if $-\lambda^{-1}$ is an eigenvalue of γ_p, which happens for finitely many λ; the scalars of norm 1 in $O_{K,p}^\times$ are infinitely many. Replacing γ_p by $\lambda\gamma_p$ for a suitable λ, which does not change the coset $\gamma_p\mathsf{S}_p$,

we may assume that $\det(1+\gamma_p)\neq 0$. Let $\mathfrak{u}_{\mathcal{V}}$ be the $\mathbb{Q}$-vector space of K-linear maps γ of $\mathcal{V}$ that are skew-Hermitian, $h(\gamma x,y)=-h(x,\gamma y)$. The *Cayley transform* $\gamma\mapsto(1-\gamma)(1+\gamma)^{-1}$ is defined where $\det(1+\gamma)\neq 0$, is its own inverse, and maps unitary maps to skew-Hermitian ones and conversely (Exercise 10.5). So it is a homeomorphism between the open subsets where $\det(1+\gamma)\neq 0$ of $\mathrm{U}(\mathcal{V})(\mathbb{Q}_p)$ and of $\mathfrak{u}_{\mathcal{V}}\otimes\mathbb{Q}_p$, and it maps rational points to rational points. The open neighborhood $\gamma_p\mathsf{S}_p$ of γ_p corresponds to an open neighborhood of its transform in $\mathfrak{u}_{\mathcal{V}}\otimes\mathbb{Q}_p$, which contains a point of the dense subset $\mathfrak{u}_{\mathcal{V}}$, and the transform of that point lies in $\gamma_p\mathsf{S}_p\cap\mathrm{U}(\mathcal{V})(\mathbb{Q})$. □

Exercise 10.5. Let γ be a K-linear map with $\det(1+\gamma)\neq 0$ and $c(\gamma)=(1-\gamma)(1+\gamma)^{-1}$. Show that $1+c(\gamma)=2(1+\gamma)^{-1}$, so that $\det(1+c(\gamma))\neq 0$ and $c(c(\gamma))=\gamma$. Show that if γ is unitary for h, then $c(\gamma)$ is skew-Hermitian, and conversely, using that the adjoint of γ is γ^{-1}, respectively $-\gamma$.

Exercise 10.6. Let p be unramified in K and L a free $O_{K,p}$-module with a skew-Hermitian form $\mathcal{H}$ and $\psi=\mathrm{Tr}_{K/\mathbb{Q}}\circ\mathcal{H}$. Using that the inverse different $\{x\in K_p:\mathrm{Tr}(xO_{K,p})\subseteq\mathbb{Z}_p\}$ equals $O_{K,p}$ when p is unramified, show that the ψ-dual and the $\mathcal{H}$-dual of L coincide. So L is unimodular for $\mathcal{H}$ exactly when ψ is perfect on L.

10.5. Schoen's step in lattice form

Schoen showed how algebraicity of Weil classes on abelian sixfolds of Weil type implies it on fourfolds [Sch98]. The geometric idea is to multiply a fourfold X by an abelian surface X_2 of Weil type, so that $X\times X_2$ is isogenous to a sixfold in a given family, pull a cycle back to $X\times X_2$ and push it to X after cutting with a divisor on X_2. The cutting and pushing is done in Chapter 13. What is needed here is the isogeny, and the point is that its degree can be made prime to p, so that pull-back and push-forward change Weil coefficients only by units at p. Recall that the polarized abelian sixfolds of Weil type $(3,3)$ with a given lattice $H_1(X_6,\mathbb{Z})$, action of O_K and Riemann form form a connected family: they correspond to the complex structures on $H_1(X_6,\mathbb{R})$ that commute with K and for which the form is a Riemann form, and by the proof of Proposition 10.5 these correspond to the 3-dimensional complex subspaces on which h is positive definite. In a basis in which $h=\mathrm{diag}(1,1,1,-1,-1,-1)$ these subspaces are the graphs of the 3×3 complex matrices γ with $1-\gamma^*\gamma$ positive definite, a convex and hence connected set.

Proposition 10.9 (Schoen's step). *Let p be an odd prime inert in K. Let X_6 be a polarized complex abelian sixfold of Weil type $(3,3)$ for K, and X a polarized complex abelian fourfold of Weil type $(2,2)$ for K, both with polarizations compatible with K, such that $O_{K,(p)}$ acts on $H_1(X_6,\mathbb{Z}_{(p)})$ and on $H_1(X,\mathbb{Z}_{(p)})$ and both are unimodular Hermitian lattices. Then there are*

(a) a polarized abelian surface X_2 of Weil type $(1,1)$ for K, with $H_1(X_2,\mathbb{Z}_{(p)})$ a unimodular Hermitian $O_{K,(p)}$-lattice,

(b) a member X_6' of the family of X_6, with $H_1(X_6',\mathbb{Z})=H_1(X_6,\mathbb{Z})$ as a lattice with action of $O_K\cap\mathrm{End}(X_6)$ and Riemann form, and

(c) an isogeny $\vartheta\colon X\times X_2\to X_6'$ of degree prime to p, compatible with the actions of K.

Proof. Let $(\mathcal{V}_6,h_6)$ and $(\mathcal{V}_4,h_4)$ be the Hermitian spaces $H_1(X_6,\mathbb{Q})$ and $H_1(X,\mathbb{Q})$ over K. By Proposition 10.5 their signatures are $(3,3)$ and $(2,2)$, so $\det h_6<0<\det h_4$, and computing the determinants in $O_{K,(p)}$-bases of the unimodular lattices shows that both are units at p. So the ratio $\det h_6/\det h_4$ is a negative rational number that is a unit at p. Let $\mathcal{V}'=K^2$ with the Hermitian form $h'=n_1\mathrm{diag}(1,\det h_6/\det h_4)$, where n_1 is a positive integer prime to p chosen so that the Riemann form $\psi'=\mathrm{Tr}_{K/\mathbb{Q}}(\theta^{-1}h')$ is integral on $\mathcal{V}'_{\mathbb{Z}}=O_K^2$. Then $\mathcal{V}'$ has signature $(1,1)$, $\mathcal{V}'_{\mathbb{Z}}\otimes\mathbb{Z}_{(p)}$ is unimodular, and $\mathcal{V}_4\oplus\mathcal{V}'$ has dimension 6, signature $(3,3)$ and determinant $n_1^2\det h_6\equiv\det h_6$ modulo norms. By the classification of Hermitian spaces over K there is a K-linear isometry $\Psi_0\colon\mathcal{V}_4\oplus\mathcal{V}'\to\mathcal{V}_6$.

The surface. Let $\mathcal{V}'_{\mathbb{R}} = \mathcal{V}'_+ \oplus \mathcal{V}'_-$ be an h'-orthogonal splitting into a positive and a negative line, and define $\mathcal{J}'$ by $\theta = \sqrt{d_0}\mathcal{J}'$ on $\mathcal{V}'_+$ and $\theta = -\sqrt{d_0}\mathcal{J}'$ on $\mathcal{V}'_-$. The computation in the proof of Proposition 10.5, read backwards, shows that ψ' is a Riemann form for $\mathcal{J}'$. So $X_2 = \mathcal{V}'_{\mathbb{R}}/\mathcal{V}'_{\mathbb{Z}}$ with complex structure $\mathcal{J}'$ is a polarized abelian surface on which O_K acts, of type $(1,1)$; this is (a).

The isometry at p. The lattices $L = (H_1(X,\mathbb{Z}) \oplus \mathcal{V}'_{\mathbb{Z}}) \otimes \mathbb{Z}_p$ and $L_6 = H_1(X_6,\mathbb{Z}) \otimes \mathbb{Z}_p$ are unimodular Hermitian $O_{K,p}$-lattices of rank 6, so by Fact 10.7(a) there is an isometry $\Psi_p\colon L \to L_6$. The set of $\gamma \in \mathrm{U}(\mathcal{V}_4 \oplus \mathcal{V}')(\mathbb{Q}_p)$ with $\Psi_0\gamma(L) = L_6$ is the coset $\gamma_p \mathsf{S}_p$ of the stabilizer S_p of L, with $\gamma_p = \Psi_0^{-1}\Psi_p$; the stabilizer is an open subgroup and contains the scalars of norm 1 in $O_{K,p}^\times$. By Lemma 10.8 the coset contains an element γ of $\mathrm{U}(\mathcal{V}_4 \oplus \mathcal{V}')(\mathbb{Q})$. Then $\Psi = \Psi_0\gamma$ is a K-linear isometry $\mathcal{V}_4 \oplus \mathcal{V}' \to \mathcal{V}_6$ with $\Psi(L) = L_6$, and hence $\Psi\big((H_1(X,\mathbb{Z}) \oplus \mathcal{V}'_{\mathbb{Z}}) \otimes \mathbb{Z}_{(p)}\big) = H_1(X_6,\mathbb{Z}_{(p)})$, because a $\mathbb{Z}_{(p)}$-lattice is the intersection of its p-adic completion with the rational space.

The isogeny. The lattices $\Psi(H_1(X,\mathbb{Z}) \oplus \mathcal{V}'_{\mathbb{Z}})$ and $H_1(X_6,\mathbb{Z})$ in $\mathcal{V}_6$ agree after localization at p, so there is a positive integer n_2 prime to p with $n_2\Psi(H_1(X,\mathbb{Z}) \oplus \mathcal{V}'_{\mathbb{Z}}) \subseteq H_1(X_6,\mathbb{Z})$, of index prime to p. Give $H_1(X_6,\mathbb{R})$ the complex structure $\mathcal{J}'_6 = \Psi(\mathcal{J}_X \oplus \mathcal{J}')\Psi^{-1}$. It commutes with K because Ψ is K-linear, and the Riemann form of X_6 is positive for it because Ψ is an isometry for h, hence for $\psi = \mathrm{Tr} \circ \theta^{-1}h$. So $X'_6 = H_1(X_6,\mathbb{R})/H_1(X_6,\mathbb{Z})$ with complex structure $\mathcal{J}'_6$ is a member of the family of X_6, which is (b), and $n_2\Psi$ induces an isogeny $\vartheta\colon X \times X_2 \to X'_6$, compatible with K, of degree $[H_1(X_6,\mathbb{Z}) : n_2\Psi(H_1(X,\mathbb{Z}) \oplus \mathcal{V}'_{\mathbb{Z}})]$, which is prime to p. This is (c). □

What just happened. The fourfold's Hermitian space, plus a plane of signature $(1,1)$ with the right determinant, is isometric to the sixfold's, by the classification of Hermitian spaces. At p both lattices are unimodular, so they are isometric there as well (Fact 10.7), and the Cayley transform produces one global isometry that does both (Lemma 10.8). Transporting complex structures along it puts $X \times X_2$ into the sixfold's family up to an isogeny whose degree is prime to p.

Where this is used. Definitions 10.2 and 10.3 and the K-types are used throughout Part IV, starting with Markman's sixfolds in Chapter 11. Proposition 10.5 and Exercise 10.6 are the last step of the unimodularity lemma Lemma 12.6. Proposition 10.9 is the Schoen step in the construction of the Weil cycle, Proposition 13.2.

CHAPTER 11

Markman's classes and Hypothesis (M)

Where we are. The proof needs one algebraic cycle with integer coefficients on an abelian variety of Weil type whose Weil component has a coefficient that is a unit at p. This chapter says exactly what is assumed to get one, and what is proved from the assumption. Hypothesis (M) (Hypothesis (M)) is that three statements made in the proof of a theorem of a preprint of Markman hold, together with the other statements of the preprint that the chapter cites. From them, Proposition 11.5 derives that an explicit integral class $2(8d)^{8d}\kappa_3(\mathcal{E})$ is the class of an algebraic cycle with integer coefficients on every member of a family of abelian sixfolds of Weil type. The chapter then computes, also under Hypothesis (M), the Weil coefficient of this class, $\frac{d+1}{2d}$ times a primitive Weil class (Lemma 11.8), which is a unit at every prime p that the proof uses. It is the only place in the companion that discusses the status of the dependency on the preprint (Section 11.7). It needs the Weil classes of Chapter 10. Derived categories and twisted sheaves enter only through statements of the preprint, Chern classes of complexes of analytic sheaves and their relation to algebraic cycles are explained in Section 11.4, and the proof of Proposition 11.5 uses arithmetic groups, families of abelian varieties over arithmetic quotients and Hilbert schemes, which are explained where they are used.

11.1. Markman's classes in two pages

A preprint of Markman claims that the Weil classes of every polarized abelian sixfold of Weil type for $\mathbb{Q}(\sqrt{-d})$ whose Hermitian form has discriminant -1 are algebraic [Mar25, Theorem 1.5.1], that is, classes of cycles with rational coefficients. The construction behind the claim is explicit. On the Jacobian X_3 of a curve of genus 3, two ideal sheaves of unions of translates of the curve, twisted by the theta divisor, have Chern characters on a line spanned by two conjugate exponentials $\exp(\pm\sqrt{-d}\Theta)$. Markman states that Orlov's derived equivalence carries their product to a sheaf $\mathcal{E}$ of rank $8d$ on the sixfold $X_6 = X_3 \times \hat{X}_3$, and that the class $\kappa_3(\mathcal{E})$, the degree-6 part of $\mathrm{ch}(\mathcal{E})\exp(-c_1(\mathcal{E})/8d)$, stays a Hodge class on every deformation of X_6 as a polarized abelian sixfold of Weil type.

The proof in this companion needs more than algebraicity with rational coefficients. It needs an algebraic cycle with *integer* coefficients whose class is an explicitly known integral class, and it needs the Weil component of that class modulo p. For the first need, Hypothesis (M) assumes three statements that Markman makes in his proof: a twisted sheaf $\mathcal{B}$ of rank $8d$ on a quotient Y_6 of X_6 exists and is semiregular, and such sheaves deform with the sixfold, as long as their Chern character stays of Hodge type. It also assumes the other statements of the preprint that this chapter cites. From these, Proposition 11.5 proves the integral statement in three steps. Near X_6, the derived tensor power $\mathcal{B}^{\otimes 8d}$ is an untwisted complex whose third Chern class pulls back to $2(8d)^{8d}\kappa_3(\mathcal{E})$; integrality comes from the fact that Chern classes of honest complexes are integral. The deformation statement carries this to every sixfold in a neighborhood of X_6. A countable-union argument over relative Hilbert schemes of a family over an arithmetic quotient, together with Baire's theorem, carries it from the neighborhood to the whole family. This adapts Markman's argument to integer coefficients, and Section 11.5 explains it.

The second need is a computation: the Weil component of $\kappa_3(\mathcal{E})$ is $\pm\frac{d+1}{2d}$ times a primitive integral Weil class (Lemma 11.8). It starts from statements of the preprint, so it is also stated

under Hypothesis (M). If $K=\mathbb{Q}(\sqrt{-d_0})$ is inert at p and $d=4d_0$, then p divides none of 2, d and $d+1$, so the coefficient is a unit at p and the Weil component of the algebraic class is $\nu\omega+\bar\nu\bar\omega$ with ν a unit.

Example 11.1 ($d=4$ and $d=8$). For $d=4$, $\sqrt{-d}=2\mathrm{i}$ and the coefficient that appears in the Chern character of the ideal sheaves below is $\varpi_4=\frac12(1+\frac{1}{2\mathrm{i}})=\frac12-\frac{\mathrm{i}}{4}$, with norm $\mathrm{Nm}(\varpi_4)=\frac14+\frac{1}{16}=\frac{5}{16}=\frac{d+1}{4d}$. The Weil coefficient is $2\,\mathrm{Nm}(\varpi_4)=\frac58=\frac{d+1}{2d}$. For $K=\mathbb{Q}(\sqrt{-2})$, $d_0=2$ and $d=8$, the coefficient is $\frac{9}{16}$, a unit at $p=5$, where K is inert (Example 10.1); here $2d(d+1)=144$ is prime to 5.

11.2. The construction

Let $d\geq 3$ be even and $K_d=\mathbb{Q}(\sqrt{-d})$. Let C be a generic non-hyperelliptic curve of genus 3, $X_3=\mathrm{Pic}^2(C)$ with its principal theta divisor Θ, so that $\int_{X_3}\Theta^3=3!=6$, $\hat X_3$ the dual abelian threefold, and $X_6=X_3\times\hat X_3$. Translates of the Abel–Jacobi curve $\mathrm{AJ}(C)\subset X_3$ have class $\Theta^2/2$ by Poincaré's formula.

The sheaf. Let $\mathcal{I}_1$ be the ideal sheaf of a union of $d+1$ generic translates of $\mathrm{AJ}(C)$, twisted by Θ, and $\mathcal{I}_2$ the same for translates of $-\mathrm{AJ}(C)$. Let $\mathrm{FM}\colon \mathrm{D}^b(X_3\times X_3)\to\mathrm{D}^b(X_6)$ be Orlov's derived equivalence, as Markman uses it [Mar25, Section 1.3]. Markman states that the dual of $\mathrm{FM}(\mathcal{I}_2\boxtimes\mathcal{I}_1)$ is, up to shift, a simple reflexive sheaf $\mathcal{E}$ of rank $8d$ on X_6 [Mar25, Theorem 1.4.1(2) and Proposition 9.2.2].

For a sheaf or a complex $\mathcal{F}$ of nonzero rank $\mathrm{rk}\,\mathcal{F}$ put

$$\kappa(\mathcal{F})=\exp\bigl(-c_1(\mathcal{F})/\mathrm{rk}\,\mathcal{F}\bigr)\,\mathrm{ch}(\mathcal{F}),$$

and let $\kappa_i(\mathcal{F})$ be its component in H^{2i}. Tensoring $\mathcal{F}$ with a line bundle does not change $\kappa(\mathcal{F})$; more generally κ does not change when the Chern character is multiplied by the exponential of a class of degree 2. Also $\kappa_0(\mathcal{F})=\mathrm{rk}\,\mathcal{F}$ and $\kappa_1(\mathcal{F})=0$.

The lattice and the action of $\sqrt{-d}$. Write $H^1(X_6,\mathbb{Z})=H^1(X_3,\mathbb{Z})\oplus H^1(\hat X_3,\mathbb{Z})$, with elements (w,y), and let $(\cdot,\cdot)$ be the symmetric pairing for which both summands are isotropic and which pairs them by duality [Mar25, (1.2.2)]. Let $\Theta^\sharp\colon H^1(\hat X_3,\mathbb{Z})\to H^1(X_3,\mathbb{Z})$ be the contraction with Θ [Mar25, (2.4.3)]; it is an isomorphism because Θ is principal. Markman defines an endomorphism η of $H^1(X_6,\mathbb{Q})$ with $\eta^2=-d$ (his $f=\eta_{\sqrt{-d}}$, [Mar25, (2.4.1)]), and the form

$$\psi_6(x,y)=(\eta x,y)$$

[Mar25, (2.4.2)]. With them X_6 is a polarized abelian sixfold of Weil type for K_d [Mar25, Section 1.2 and Proposition 2.4.4], whose Hermitian form, in Markman's normalization, has signature $(3,3)$ and discriminant -1 [Mar25, Lemmas 3.1.2 and 3.1.3]. On $H^1(X_6,K_d)$ the endomorphism η acts by $\sqrt{-d}$ on

$$\mathcal{W}_1=\{(-\sqrt{-d}\Theta^\sharp y,y)\},$$

and by $-\sqrt{-d}$ on $\mathcal{W}_2=\{(\sqrt{-d}\Theta^\sharp y,y)\}$, with y running over $H^1(\hat X_3,K_d)$ [Mar25, Section 1.2 and (2.4.6)]. Decomposing $(w,0)$ and $(0,y)$ into these two eigenspaces gives

$$\eta(w,0)=\bigl(0,-(\Theta^\sharp)^{-1}w\bigr),\qquad \eta(0,y)=(d\Theta^\sharp y,0)$$

(Exercise 11.2). So η preserves $H^1(X_6,\mathbb{Z})$, and ψ_6 is an integral alternating form on it of determinant d^6 (Exercise 11.2). A class in $\bigwedge^{i+j}H^1(X_6,K_d)$ has *K_d-type* (i,j) if it lies in $\bigwedge^i\mathcal{W}_1\wedge\bigwedge^j\mathcal{W}_2$; this agrees with Section 10.2 with $\mathcal{W}_1$ the ι-eigenspace.

The family. The complex structures on $H^1(X_6,\mathbb{R})$ that commute with η and for which ψ_6 is a polarization form a connected complex manifold $\mathscr{D}$, the Hermitian symmetric domain of the special unitary group of the Hermitian form of ψ_6, a group whose real points are isomorphic to $\mathrm{SU}(3,3)$; by the proof of Proposition 10.5, as in Section 10.5, its points correspond to the 3-dimensional complex subspaces on which the Hermitian form is positive definite. We call the polarized abelian sixfolds $X_{6,t}$, $t\in\mathscr{D}$, with $H^1(X_{6,t},\mathbb{Z})=H^1(X_6,\mathbb{Z})$, the action η and the polarization ψ_6, the *family of* $(H^1(X_6,\mathbb{Z}),\eta,\psi_6)$, and we identify the cohomology of

each member with $\bigwedge^\bullet H^1(X_6,\mathbb{Z})$. A class on X_6 then gives a class on every member, its *flat continuation*.

Integral Weil classes. Let $\mathcal{W}_{1,\mathbb{Z}} = \mathcal{W}_1 \cap (H^1(X_6,\mathbb{Z}) \otimes O_{K_d})$ and $\mathcal{W}_{2,\mathbb{Z}} = \overline{\mathcal{W}_{1,\mathbb{Z}}}$. For a $\mathbb{Z}$-basis (y_i) of $H^1(\hat{X}_3,\mathbb{Z})$, the vectors $(-\sqrt{-d}\Theta^\sharp y_i, y_i)$ form an O_{K_d}-basis of $\mathcal{W}_{1,\mathbb{Z}}$, since an element of $\mathcal{W}_1$ is integral exactly when its second component is. Let ω_{X_6} be their wedge product and $\bar\omega_{X_6}$ its conjugate. If $p \nmid 2d$, then $O_{K_d,(p)} = \mathbb{Z}_{(p)}[\sqrt{-d}]$, $H^1(X_6,\mathbb{Z}_{(p)}) \otimes O_{K_d,(p)} = (\mathcal{W}_{1,\mathbb{Z}} \oplus \mathcal{W}_{2,\mathbb{Z}}) \otimes_{O_{K_d}} O_{K_d,(p)}$, these are the eigenlattices of (10.1), and the integral Weil classes at p are the $\nu\omega_{X_6} + \bar\nu\bar\omega_{X_6}$, $\nu \in O_{K_d,(p)}$ (Definition 10.3).

The class is integral on X_6. Assume Hypothesis (M), which covers Markman's statements on $\mathcal{E}$. In the Grothendieck group of X_6, the class $\mathcal{E}^{\otimes 8d} \otimes (\det\mathcal{E})^{-1}$ has Chern character $\operatorname{ch}(\mathcal{E})^{8d}\exp(-c_1(\mathcal{E})) = \kappa(\mathcal{E})^{8d}$. Its first Chern class vanishes, and by Exercise 11.1 its third Chern class, an integral class, is $2(8d)^{8d}\kappa_3(\mathcal{E})$. So $2(8d)^{8d}\kappa_3(\mathcal{E})$ lies in $H^6(X_6,\mathbb{Z})$, and hence, by flat continuation, in $H^6(X_{6,t},\mathbb{Z})$ for every member of the family.

Exercise 11.1. Let $\mathcal{F}$ be a sheaf with $c_1(\mathcal{F}) = 0$. Using $\operatorname{ch}_3 = \frac{1}{6}(c_1^3 - 3c_1c_2 + 3c_3)$, show that $c_3(\mathcal{F}) = 2\operatorname{ch}_3(\mathcal{F})$. If moreover $\mathcal{F}$ has rank $n_\mathcal{F}$, so that $\kappa(\mathcal{F}) = n_\mathcal{F} + \kappa_2 + \kappa_3 + \dots$, show that the degree-6 part of $\kappa(\mathcal{F})^{n_\mathcal{F}}$ is $n_\mathcal{F}^{n_\mathcal{F}}\kappa_3$. Both statements hold verbatim for classes in the Grothendieck group and for complexes.

Exercise 11.2. Write $(w,0) = a + b$ with $a \in \mathcal{W}_1$, $b \in \mathcal{W}_2$, and use $\eta a = \sqrt{-d}a$, $\eta b = -\sqrt{-d}b$ to derive $\eta(w,0) = (0, -(\Theta^\sharp)^{-1}w)$; do the same for $(0,y)$. Check $\eta^2 = -d$. Then show that the determinant of ψ_6 on $H^1(X_6,\mathbb{Z})$ is d^6: the pairing $(\cdot,\cdot)$ is perfect, so the determinant of ψ_6 is $\pm\det\eta$; $(\det\eta)^2 = \det(\eta^2) = d^{12}$; and the determinant of an alternating form is a square.

11.3. Hypothesis (M)

Hypothesis (M). *For every even $d \geq 3$, [Mar25, Lemmas 9.3.6 and 9.3.11] and [Mar25, Conjecture 7.3.9], in the form claimed for families of abelian varieties in [Mar25, Section 7.4.2], hold, and so do the other statements of [Mar25] cited in this chapter.*

Here is what these statements say. In them, the translates in $\mathcal{I}_1$ and $\mathcal{I}_2$ are taken to be the orbits of two cyclic subgroups of X_3 of order $d+1$ that meet trivially, which exist for generic C [Mar25, Section 1.5 and Lemma 9.3.1]; this choice changes neither $\operatorname{ch}(\mathcal{I}_1)$, $\operatorname{ch}(\mathcal{I}_2)$ nor $\kappa(\mathcal{E})$. The two subgroups induce a group of translations of X_6 of order $(d+1)^2$, and $\varrho\colon X_6 \to Y_6$ is the quotient by it, an isogeny of degree $(d+1)^2$ [Mar25, Section 1.5 and Lemma 9.3.3].

(M1) [Mar25, Lemma 9.3.6]: Y_6 carries a reflexive sheaf $\mathcal{B}$ of rank $8d$, twisted by a Čech 2-cocycle with values in the group $\boldsymbol{\mu}_{8d}$ of roots of unity, with trivial determinant.

(M2) [Mar25, Lemma 9.3.11]: $\mathcal{B}$ is semiregular.

(M3) [Mar25, Conjecture 7.3.9], for sheaves of rank $8d$: if $\mathcal{Y}$ is a deformation of a smooth complex projective variety $\mathcal{Y}_0$ over a smooth germ $(\Sigma,0)$, and $\mathcal{B}$ is a semiregular coherent sheaf of rank $8d$ on $\mathcal{Y}_0$, twisted by a cocycle with values in $\boldsymbol{\mu}_{8d}$, whose Chern character extends to a horizontal section of Hodge type, then $\mathcal{B}$ extends to a twisted coherent sheaf over the part of $\mathcal{Y}$ above an open neighborhood of 0. For families of abelian varieties and $\det\mathcal{B}$ trivial, the extension constructed in [Mar25, Section 7.4.2] is flat over that neighborhood and twisted by a cocycle with values in $\boldsymbol{\mu}_{8d}$ that restricts to the cocycle of $\mathcal{B}$ after a change of the gluing of $\mathcal{B}$ by a cochain with values in $\boldsymbol{\mu}_{8d}$ [Mar25, Remark 7.3.2]. Such a change does not affect $\mathcal{B}^{\otimes 8d}$.

These are the statements specific to Markman's proof of [Mar25, Theorem 1.5.1]. Hypothesis (M) also covers the other statements of the preprint cited in this chapter, and what depends on Hypothesis (M) is conditional on all of them. Every statement in the companion that depends on Hypothesis (M) says so.

Intuition 11.2 (a twisted sheaf). A twisted sheaf is glued from sheaves on the open sets of a cover by isomorphisms that agree on triple overlaps only up to scalars, here roots of unity of order r; the scalars form a Čech 2-cocycle. Such an object has no Chern classes with integer coefficients of its own, but its tensor power of order r multiplies the scalars to 1 and is an honest complex, with integral Chern classes. This is why the multiplier $(8d)^{8d}$ appears: it is the price of passing from $\mathcal{B}$ to its tensor power $\mathcal{B}^{\otimes 8d}$.

11.4. Chern classes of complexes and of cycles

The proof of Proposition 11.5 needs two kinds of Chern classes and a bridge between them. Markman's statements concern a complex of sheaves on a complex manifold that moves in a family, and the conclusion concerns algebraic cycles with integer coefficients. Lemma 11.4 provides what is needed: integral Chern classes of complexes of coherent analytic sheaves, which are additive and stay constant in proper smooth families, and the statement that on a projective variety these classes are classes of algebraic cycles with integer coefficients, with an explicit formula for the class of a subscheme. It is proved below from results of Atiyah and Hirzebruch, of Borel and Haefliger, and of Grothendieck.

Intuition 11.3 (why real-analytic functions). A coherent analytic sheaf on a complex manifold need not have a resolution by holomorphic vector bundles, so its Chern classes cannot simply be read off from a resolution, as one does in algebraic geometry. Atiyah and Hirzebruch observed that after tensoring with real-analytic functions such resolutions exist, at least near compact sets; the resulting real-analytic vector bundles are in particular topological vector bundles, whose Chern classes are integral. Tensoring with real-analytic functions does not change the homological algebra, because it is a flat operation; this is what makes the classes compatible with restriction to fibers.

The classes. Let $\mathscr{N}$ be a complex manifold with countable topology, $\mathcal{O}$ its sheaf of holomorphic functions and $\mathcal{C}^\omega$ its sheaf of complex-valued real-analytic functions. For a coherent $\mathcal{O}$-module $\mathcal{F}$, $\mathcal{F}\otimes\mathcal{C}^\omega$ is a coherent $\mathcal{C}^\omega$-module [AH62, Proposition 2.9], and every compact subset of $\mathscr{N}$ has an open neighborhood on which $\mathcal{F}\otimes\mathcal{C}^\omega$ has a finite resolution by locally free $\mathcal{C}^\omega$-modules, that is, by real-analytic vector bundles [AH62, Proposition 2.6 and Section 4]; Atiyah and Hirzebruch assume that manifolds have countable topology. Let $\mathscr{N}$ be compact. Then the K-theory and cohomology of [AH62] are the usual ones [AH62, Section 1 and remark after Proposition 6.2], and the alternating sum $[\mathcal{F}]_{\mathrm{top}}$ of the classes of the bundles in such a resolution, in topological K-theory, does not depend on the resolution [AH62, Section 4]. For a bounded complex $\mathcal{F}$ of $\mathcal{O}$-modules with coherent cohomology put $[\mathcal{F}]_{\mathrm{top}}=\sum_j(-1)^j[H^j(\mathcal{F})]_{\mathrm{top}}$, and let $c(\mathcal{F})\in H^{\mathrm{ev}}(\mathscr{N},\mathbb{Z})$ and $\mathrm{ch}(\mathcal{F})\in H^{\mathrm{ev}}(\mathscr{N},\mathbb{Q})$ be the total Chern class and the Chern character of $[\mathcal{F}]_{\mathrm{top}}$.

On the algebraic side, for a nonsingular quasi-projective complex variety Y let $\mathrm{cl}\colon \mathrm{CH}^\bullet(Y)\to H^{2\bullet}(Y,\mathbb{Z})$ be the cycle class map, a ring homomorphism compatible with pull-backs [BH61, p. 4.15]. For algebraic coherent sheaves and complexes on a nonsingular projective Y, c and ch denote the classes just defined of their analytifications. A closed subscheme $Z'\subseteq Y$ of dimension at most n has an n-cycle $[Z']_n=\sum m_{Y'}Y'$, the sum of its irreducible components Y' of dimension n with their multiplicities [The, Tag 02QU].

LEMMA 11.4 (Chern classes in families). *(a) Let $\mathscr{N}$ be compact. Then $\mathcal{F}\mapsto[\mathcal{F}]_{\mathrm{top}}$ is additive on distinguished triangles of bounded complexes of $\mathcal{O}$-modules with coherent cohomology, in particular on short exact sequences of coherent sheaves.*

(b) Let $\mathfrak{f}\colon\mathscr{N}\to\mathscr{T}$ be a proper holomorphic submersion with fibers $\mathscr{N}_t$, $t\in\mathscr{T}$, let Li_t^* be the derived restriction to $\mathscr{N}_t$, and let $\mathcal{F}$ be a bounded complex of $\mathcal{O}_{\mathscr{N}}$-modules with coherent cohomology. Then $t\mapsto c(Li_t^*\mathcal{F})$ and $t\mapsto\mathrm{ch}(Li_t^*\mathcal{F})$ are flat sections over $\mathscr{T}$ of $t\mapsto\bigoplus_i H^{2i}(\mathscr{N}_t,\mathbb{Z})$ and of $t\mapsto\bigoplus_i H^{2i}(\mathscr{N}_t,\mathbb{Q})$.

(c) *Let Y be a nonsingular projective complex variety and $\mathcal{G}$ a bounded complex of $\mathcal{O}_{Y^{\mathrm{an}}}$-modules with coherent cohomology. Then $c(\mathcal{G})$ is* cl *of an element of* $\mathrm{CH}^\bullet(Y)$*; in particular the Chern classes of $\mathcal{G}$ are classes of algebraic cycles with integer coefficients.*

(d) *Let Y be as in (c) and $Z' \subseteq Y$ a closed subscheme of dimension at most $n = \dim Y - l$. Then $\mathrm{ch}_l(\mathcal{O}_{Z'}) = \mathrm{cl}([Z']_n)$.*

Proof. (a) First, $\mathcal{C}^\omega$ is flat over $\mathcal{O}$. At a point with holomorphic coordinates z, the stalk $\mathbb{C}\{z,\bar z\}$ of $\mathcal{C}^\omega$ has the completion $\mathbb{C}[[z,\bar z]]$, which is faithfully flat over $\mathbb{C}\{z,\bar z\}$ and flat over the stalk $\mathbb{C}\{z\}$ of $\mathcal{O}$ (see e.g. [The, Tags 00MB and 00MC]); so $\mathbb{C}\{z,\bar z\}$ is flat over $\mathbb{C}\{z\}$ (Exercise 11.3). Locally free $\mathcal{C}^\omega$-modules are projective among coherent ones [AH62, Lemma 2.7], so by the horseshoe lemma $[\cdot]_{\mathrm{top}}$ is additive on short exact sequences of coherent $\mathcal{C}^\omega$-modules. Hence the alternating sum of the classes of the terms of a bounded complex of locally free $\mathcal{C}^\omega$-modules with coherent homology is the alternating sum of the classes of its homology modules, and, by the long exact cohomology sequence and the flatness of $\mathcal{C}^\omega$, $[\cdot]_{\mathrm{top}}$ is additive on distinguished triangles.

(b) As $\mathfrak{f}$ is proper, every point of $\mathscr{T}$ has an open neighborhood $\mathscr{T}'$ such that the $H^j(\mathcal{F})\otimes\mathcal{C}^\omega$ have finite locally free resolutions on $\mathfrak{f}^{-1}(\mathscr{T}')$. These give one class $\sum_j(-1)^j[H^j(\mathcal{F})]_{\mathrm{top}}$ in the K-theory of $\mathfrak{f}^{-1}(\mathscr{T}')$, and the restrictions of its Chern classes to the fibers over $\mathscr{T}'$ form a flat section, because the family of fibers is topologically locally trivial over a ball. It remains to see that the restriction of this class to a fiber $\mathscr{N}_t$ is $[Li_t^*\mathcal{F}]_{\mathrm{top}}$. Near a point of $\mathscr{N}_t$ choose holomorphic coordinates (z,w) on $\mathscr{N}$ such that w is the pull-back of a coordinate system on $\mathscr{T}$ centered at t. Then the sheaf of complex-valued real-analytic functions on $\mathscr{N}_t$ is $\mathcal{C}^\omega/(w,\bar w)$, and by the flatness of $\mathcal{C}^\omega$ over $\mathcal{O}$ on $\mathscr{N}$ and on $\mathscr{N}_t$, a locally free resolution of $\mathcal{F}\otimes\mathcal{C}^\omega$, for a coherent sheaf $\mathcal{F}$, restricted to $\mathscr{N}_t$, has homology $\mathrm{Tor}_i^{\mathcal{O}_{\mathscr{N}}}(\mathcal{F},\mathcal{O}_{\mathscr{N}_t})\otimes\mathcal{C}^\omega$. So the restriction of $[\mathcal{F}]_{\mathrm{top}}$ is $[Li_t^*\mathcal{F}]_{\mathrm{top}}$. For a complex, apply Li_t^* to the truncation triangles $\tau_{\le j-1}\mathcal{F}\to\tau_{\le j}\mathcal{F}\to H^j(\mathcal{F})[-j]$ and use (a).

(c) For an algebraic vector bundle $\mathscr{E}$ on Y, the topological Chern class of its analytification is cl of its Chern class in the Chow ring. Indeed, both are functorial and additive, the latter by [Gro58, Théorème 1]. For a line bundle with a rational section of divisor D, the topological first Chern class is $\mathrm{cl}(D)$ by [BH61, p. 4.13] and linearity, and the Chow-ring one is $[D]$ by [Gro58, Section 2, example 1°, and Théorème 1]. So the two agree by the uniqueness in [Gro58, Théorème 1], applied to example 3° of [Gro58, Section 2] on nonsingular quasi-projective varieties. Now the cohomology sheaves of $\mathcal{G}$ are analytifications of algebraic coherent sheaves [Gro03, Exposé XII, Théorème 4.4] (GAGA), each of which is quasi-isomorphic to a bounded complex of algebraic vector bundles (see e.g. [The, Tags 0FDC, 0F87 and 0F8E]), and analytification is exact [Gro03, Exposé XII, Proposition 1.3.1]. So by (a), $[\mathcal{G}]_{\mathrm{top}}$ is an alternating sum of classes of analytified algebraic vector bundles, and $c(\mathcal{G})$ is cl of an element of $\mathrm{CH}^\bullet(Y)$. Its coefficients are integers because the total Chern class of a vector bundle in the Chow ring is 1 plus classes with integer coefficients, and so is its inverse.

(d) Let first $Y'\subseteq Y$ be a closed subvariety of codimension l. Its analytification is reduced and irreducible of codimension l [Gro03, Exposé XII, Propositions 2.1 and 2.4], and $\mathrm{ch}(\mathcal{O}_{Y'})$ is the class of Y'^{an} defined in [AH62, Proposition 5.4] plus terms of degree greater than $2l$ [AH62, Propositions 3.4 and 6.2 and Lemma 5.6]. That class is $\mathrm{cl}(Y')$: both restrict to the class of the submanifold $Y'\smallsetminus Y'_{\mathrm{sing}}$ on the complement of the singular locus Y'_{sing} [BH61, proof of 4.5], and this restriction is injective in degree $2l$ [AH62, Lemma 5.3]. For the subscheme Z', [The, Tags 02MX and 02S9] and induction on the dimension show that $[\mathcal{O}_{Z'}]-\sum m_{Y'}[\mathcal{O}_{Y'}]$ is, in the Grothendieck group of coherent sheaves on Y, an integral combination of classes $[\mathcal{O}_{Y''}]$ of subvarieties of dimension less than n, whose Chern characters vanish in degrees up to $2l$. As $[\cdot]_{\mathrm{top}}$ is additive on coherent sheaves on Y by (a), $\mathrm{ch}_l(\mathcal{O}_{Z'})=\mathrm{cl}([Z']_n)$. □

Exercise 11.3. Let $A\to B\to\hat B$ be ring homomorphisms with $\hat B$ faithfully flat over B and flat over A. Show that B is flat over A: for an injection $M'\to M$ of A-modules, the kernel of $M'\otimes_A B\to M\otimes_A B$ becomes 0 after $\otimes_B\hat B$.

EXERCISE 11.4. Let R be a ring, $t \in R$ a non-zero-divisor, and $\mathcal{Z}$ an R-module on which t is a non-zero-divisor. Using the resolution $0 \to R \xrightarrow{t} R \to R/t \to 0$, show that $\operatorname{Tor}_1^R(\mathcal{Z}, R/t) = 0$, so that the derived tensor product $\mathcal{Z} \otimes_R^L R/t$ is $\mathcal{Z}/t\mathcal{Z}$. Why is a local coordinate of a smooth curve a non-zero-divisor on a module that is flat over the curve?

11.5. The integral Weil cycle on the sixfolds

PROPOSITION 11.5 (integral cycles on the family). *Assume Hypothesis (M) and let $d \geq 3$ be even. On every member of the family of $(H^1(X_6, \mathbb{Z}), \eta, \psi_6)$, the class $2(8d)^{8d}\kappa_3(\mathcal{E}) \in \bigwedge^6 H^1(X_6, \mathbb{Q})$ is the class of an algebraic cycle with integer coefficients.*

Markman deduces the algebraicity with rational coefficients [Mar25, proof of Theorem 1.5.1], and the argument below adapts his argument to integer coefficients. It has three steps: near X_6, near-by members, and the whole family.

PROOF. *Step 1: near X_6.* Markman states that $\operatorname{ch}(\mathcal{B}) = \kappa(\mathcal{B})$ because $\det \mathcal{B}$ is trivial [Mar25, Section 7.3, after Lemma 7.3.7] and that $\varrho^*\kappa(\mathcal{B}) = \kappa(\mathcal{E})$ [Mar25, Section 9.3, after Remark 9.3.7]. His Chern character is defined through the Atiyah class, and for coherent sheaves such as $\mathcal{E}$ it is the usual one (see e.g. [BF03, Section 1]). He also states that the derived tensor power $\mathcal{B}^{\otimes 8d}$ is untwisted with $\operatorname{ch}(\mathcal{B}^{\otimes 8d}) = \operatorname{ch}(\mathcal{B})^{8d}$ [Mar25, (7.3.4) and Section 7.3, after Definition 7.3.6], and we use, as he does there, that this is the rational Chern character of $\mathcal{B}^{\otimes 8d}$, the one of Lemma 11.4. As $\kappa_0(\mathcal{B}) = 8d$ and $\kappa_1(\mathcal{B}) = 0$, the class $\operatorname{ch}(\mathcal{B}^{\otimes 8d}) = \kappa(\mathcal{B})^{8d}$ has $\operatorname{ch}_1 = 0$, so $c_1(\mathcal{B}^{\otimes 8d}) = 0$, and by Exercise 11.1 $\operatorname{ch}_3(\mathcal{B}^{\otimes 8d}) = (8d)^{8d}\kappa_3(\mathcal{B})$ and

$$c_3(\mathcal{B}^{\otimes 8d}) = 2\operatorname{ch}_3(\mathcal{B}^{\otimes 8d}) = 2(8d)^{8d}\kappa_3(\mathcal{B}) \qquad \text{in } H^6(Y_6, \mathbb{Z}),$$

which is torsion-free, Y_6 being an abelian variety. The left-hand side is a Chern class of a complex with coherent cohomology on the projective variety Y_6, so it is the class of an algebraic cycle with integer coefficients (Lemma 11.4(c)), and pulling back along ϱ, which is compatible with cl [BH61, p. 4.15], gives $\varrho^* c_3(\mathcal{B}^{\otimes 8d}) = 2(8d)^{8d}\kappa_3(\mathcal{E})$.

Step 2: deformation. The group of translations defining ϱ consists of torsion points, which are determined by the lattice $H^1(X_6, \mathbb{Z})$, so it acts on every $X_{6,t}$, $t \in \mathscr{D}$, and gives isogenies $\varrho_t \colon X_{6,t} \to Y_{6,t}$. The class $\kappa(\mathcal{E})$ is of Hodge type on every $X_{6,t}$ [Mar25, Theorem 1.4.1(3) and Corollary 1.3.2], and ϱ_t^* is an isomorphism of rational Hodge structures, so the flat continuation of $\operatorname{ch}(\mathcal{B}) = \kappa(\mathcal{B})$ is of Hodge type on every $Y_{6,t}$. By Hypothesis (M), $\mathcal{B}$ extends to a twisted coherent sheaf $\mathcal{B}_{\mathscr{U}}$ on the family of the $Y_{6,t}$ over a contractible open neighborhood $\mathscr{U} \subseteq \mathscr{D}$ of the point of X_6, flat over $\mathscr{U}$ and twisted by a cocycle with values in $\boldsymbol{\mu}_{8d}$. Its derived tensor power $\mathcal{F} = \mathcal{B}_{\mathscr{U}}^{\otimes 8d}$ is untwisted, a bounded complex with coherent cohomology on the total space of the family, and by flatness its derived restriction to $Y_{6,t}$ is $\mathcal{B}_t^{\otimes 8d}$, where $\mathcal{B}_t$ is the restriction of $\mathcal{B}_{\mathscr{U}}$. The family of the $Y_{6,t}$ is a proper holomorphic submersion over $\mathscr{U}$, so by Lemma 11.4(b) the Chern classes of $\mathcal{B}_t^{\otimes 8d}$ form a flat section over $\mathscr{U}$; as $\mathscr{U}$ is contractible, they are the flat continuations of those of $\mathcal{B}^{\otimes 8d}$. As $Y_{6,t}$ is projective, they are classes of algebraic cycles with integer coefficients by Lemma 11.4(c). Pulling back along ϱ_t [BH61, p. 4.15] shows that $2(8d)^{8d}\kappa_3(\mathcal{E})$ is the class of an algebraic cycle with integer coefficients on $X_{6,t}$ for every $t \in \mathscr{U}$.

Step 3: spreading out. The idea is to put all members of the family into one algebraic family over a variety $\mathscr{M}$, to show that the set of points where the class is algebraic with integer coefficients is a countable union of closed algebraic subsets of $\mathscr{M}$, and to use that this set contains the non-empty open set $\mathscr{U}$.

(a) An arithmetic group. Let A_0 be the group of elements of $\mathrm{GL}(H^1(X_6, \mathbb{Z}))$ that lie in the group of [Mar25, (3.1.1)]: the elements of $\mathrm{SO}^+(H^1(X_6, \mathbb{Q}), (\cdot,\cdot))$ that commute with η and have determinant 1 on $\mathcal{W}_1$ and on $\mathcal{W}_2$, where SO^+ is the image of $\mathrm{Spin}(H^1(X_6, \mathbb{Q}), (\cdot,\cdot))$ in $\mathrm{SO}(H^1(X_6, \mathbb{Q}), (\cdot,\cdot))$. Its elements fix $\kappa(\mathcal{E})$ [Mar25, Corollary 1.3.2 and Lemma 3.1.1]. Let SU_6 be the special unitary group of the Hermitian form of ψ_6 (Definition 10.4): the K_d-linear automorphisms of $(H^1(X_6, \mathbb{Q}), \eta)$ that preserve ψ_6 and have K_d-linear determinant 1. A

subgroup of $\mathrm{SU}_6(\mathbb{Q})$ is *arithmetic* if it is commensurable with $\mathrm{SU}_6(\mathbb{Q}) \cap \mathrm{GL}_n(\mathbb{Z})$ for some embedding $\mathrm{SU}_6 \hookrightarrow \mathrm{GL}_n$, that is, if the intersection of the two has finite index in both. We show that A_0 is arithmetic. An element g of $\mathrm{GL}(H^1(X_6, \mathbb{Q}))$ that commutes with η preserves $(\cdot,\cdot)$ if and only if it preserves $\psi_6(x,y) = (\eta x, y)$, and then, by the uniqueness in Definition 10.4, it preserves the Hermitian form of ψ_6; its K_d-linear determinant on $(H^1(X_6,\mathbb{Q}), \eta)$ is its determinant on $\mathcal{W}_1$, the ι-eigenspace. So

$$\mathsf{A}_0 \subseteq \mathsf{D}_6 = \mathrm{SU}_6(\mathbb{Q}) \cap \mathrm{GL}(H^1(X_6, \mathbb{Z})),$$

and A_0 contains the intersection of D_6 with the image of $\mathrm{Spin}(H^1(X_6,\mathbb{Q}),(\cdot,\cdot))$. Let $\tilde{G}_6$ be the inverse image of SU_6 in the spin group. The covering map restricts to a surjective homomorphism $\tilde{G}_6 \to \mathrm{SU}_6$, so it maps an arithmetic subgroup of $\tilde{G}_6(\mathbb{Q})$ to an arithmetic subgroup D_6' of $\mathrm{SU}_6(\mathbb{Q})$ (see e.g. [Mil05, Proposition 3.2]). Two arithmetic subgroups are commensurable, so $\mathsf{D}_6' \cap \mathsf{D}_6$ has finite index in D_6; it lies in A_0, so A_0 has finite index in D_6 and is arithmetic. Let $\mathsf{A} \subseteq \mathsf{A}_0$ be a neat subgroup of finite index (see e.g. [Mil05, Proposition 3.5]); neat implies torsion-free, which is what the next step needs.

(b) The family over the quotient. The group A acts on $\mathscr{D}$, and $\mathscr{M} = \mathsf{A}\backslash\mathscr{D}$ is a nonsingular quasi-projective variety (see e.g. [Mil05, Proposition 3.1 and Theorem 3.12]). The polarized variation of Hodge structure given by $H^1(X_6,\mathbb{Z})$ over $\mathscr{D}$ descends to $\mathscr{M}$, because A preserves the lattice, η and ψ_6. Its dual, of type $(-1,0),(0,-1)$, comes from a polarized, hence projective, family of abelian varieties $\pi\colon \mathfrak{X} \to \mathscr{M}$ whose first cohomology groups form the local system $H^1(X_6,\mathbb{Z})$ (see e.g. [Mil05, Theorem 14.8], and for projectivity [Ge26, Section 2.1] and [The, Tag 0B45]). Every member of the family of $(H^1(X_6,\mathbb{Z}),\eta,\psi_6)$ is a fiber of π.

(c) Where the class is algebraic. The class $2(8d)^{8d}\kappa_3(\mathcal{E})$ is fixed by A, so it defines a flat section of $R^6\pi_*\mathbb{Q}$ over $\mathscr{M}$. Let $\mathscr{M}^{\mathrm{alg}} \subseteq \mathscr{M}(\mathbb{C})$ be the set of points at which it is the class of an algebraic cycle with integer coefficients. For finitely many irreducible components $\mathfrak{H}_1,\dots,\mathfrak{H}_m$ of the relative Hilbert scheme of $\mathfrak{X}/\mathscr{M}$ whose points are subschemes of dimension at most 3, each projective over $\mathscr{M}$ (see e.g. [Nit05, Section 1 and Theorem 5.1]), and integers $n_1,\dots,n_m$, let $\mathscr{Q}$ be a connected component of $\mathfrak{H}_1 \times_{\mathscr{M}} \cdots \times_{\mathscr{M}} \mathfrak{H}_m$, and let $Z_{i,\mathfrak{q}}$ be the fiber at $\mathfrak{q} \in \mathscr{Q}$ of the i-th universal subscheme $\mathcal{Z}_i$, a subscheme of the fiber of π over the image of $\mathfrak{q}$. By Lemma 11.4(d),

$$\mathfrak{b}(\mathfrak{q}) = \sum_i n_i \,\mathrm{ch}_3(\mathcal{O}_{Z_{i,\mathfrak{q}}})$$

is the class of the algebraic cycle $\sum_i n_i [Z_{i,\mathfrak{q}}]_3$ with integer coefficients, and every algebraic cycle of codimension 3 with integer coefficients on a fiber of π is of this form, with integral $Z_{i,\mathfrak{q}}$.

The point is that $\mathfrak{b}$ moves flatly on $\mathscr{Q}$: for $\mathfrak{q},\mathfrak{q}' \in \mathscr{Q}$, $\mathfrak{b}(\mathfrak{q}')$ is the parallel transport of $\mathfrak{b}(\mathfrak{q})$ along a path in $\mathscr{Q}$. Indeed, $\mathscr{Q}$ is connected and has finitely many irreducible components, so $\mathfrak{q}$ and $\mathfrak{q}'$ are joined by a chain of irreducible components, consecutive ones meeting, and two points of an irreducible component lie on an irreducible curve in it (see e.g. [Mil08, Chapter I, Lemma 5.20], applied to the closure of the component in a projective space). For such a curve, let $\mathfrak{n}\colon \tilde{C} \to \mathscr{Q}$ be its normalization, a connected nonsingular curve (see e.g. [The, Tag 0B8Y]). The pull-back of $\mathfrak{X}$ to $\tilde{C}$ is analytically a proper submersion over $\tilde{C}$, and the pull-backs $\tilde{\mathcal{Z}}_i$ of the $\mathcal{Z}_i$ are flat over $\tilde{C}$, also analytically [Gro03, Exposé XII, Propositions 3.1 and 3.2]. So a local coordinate of $\tilde{C}$ vanishing at a point $x \in \tilde{C}$ is a non-zero-divisor on $\mathcal{O}_{\tilde{\mathcal{Z}}_i}$, and the derived restriction of $\mathcal{O}_{\tilde{\mathcal{Z}}_i}$ to the fiber over x is $\mathcal{O}_{Z_{i,\mathfrak{n}(x)}}$ (Exercise 11.4). By Lemma 11.4(b), $\mathfrak{b}\circ\mathfrak{n}$ is a flat section over $\tilde{C}$.

So $\mathfrak{b}$ equals the given class either at every point of $\mathscr{Q}$ or at none, and in the first case the image of $\mathscr{Q}$ in $\mathscr{M}$, a closed algebraic subset because $\mathscr{Q}$ is projective over $\mathscr{M}$, lies in $\mathscr{M}^{\mathrm{alg}}$. There are countably many choices of components, integers and connected components. Hence $\mathscr{M}^{\mathrm{alg}}$ is a countable union of closed algebraic subsets of $\mathscr{M}$. By Step 2 it contains the image of $\mathscr{U}$, a non-empty open subset of $\mathscr{M}(\mathbb{C})$. This is the standard argument for Hodge loci, see e.g. [Voi16, Section 4.2].

(d) Baire and the identity theorem. By Baire's theorem (see e.g. [The, Tag 0CQN]), one of these closed subsets, say $\mathscr{Z}$, has non-empty interior $\mathscr{Z}^\circ$ in $\mathscr{M}(\mathbb{C})$. Then $\mathscr{Z} = \mathscr{M}$. Indeed, $\mathscr{M}(\mathbb{C})$ is a connected complex manifold, being the image of $\mathscr{D}$, and $\mathscr{Z}^\circ$ is open and also closed in it: a point x of the closure of $\mathscr{Z}^\circ$ lies in $\mathscr{Z}$, which is closed, and near x the set $\mathscr{Z}$ is the common zero set of finitely many regular functions on a connected coordinate ball $\mathscr{V} \ni x$; each of them vanishes on the non-empty open set $\mathscr{V} \cap \mathscr{Z}^\circ$, hence on $\mathscr{V}$ by the identity theorem for holomorphic functions, so $\mathscr{V} \subseteq \mathscr{Z}$ and $x \in \mathscr{Z}^\circ$. So $\mathscr{Z}^\circ = \mathscr{M}(\mathbb{C})$, and $\mathscr{M}^{\mathrm{alg}} = \mathscr{M}(\mathbb{C})$. Since every member of the family is a fiber of π, this proves the proposition. □

What just happened. On one sixfold, the twisted sheaf $\mathcal{B}$ of Hypothesis (M) becomes an honest complex after taking its tensor power of order $8d$, whose third Chern class is integral and algebraic and pulls back to $2(8d)^{8d}\kappa_3(\mathcal{E})$. The deformation statement of Hypothesis (M) moves this to a neighborhood. An arithmetic quotient puts all members of the family into one algebraic family, the locus where a fixed integral class is algebraic with integer coefficients is a countable union of closed algebraic subsets, and a countable union that contains an open set contains everything, by Baire's theorem and the identity theorem.

Intuition 11.6 (why the countable union is needed). A family of cycles moves in a Hilbert scheme, and over a component of it the class of the moving cycle is constant. So the locus where a given class is algebraic is a union of images of components. There are countably many components, and in general none of them is enough; Baire's theorem says that one of them has interior, and the identity theorem upgrades interior to everything.

11.6. Why integer coefficients matter

It is worth seeing exactly where an integer multiple would break the argument. Suppose only $n \cdot 2(8d)^{8d}\kappa_3(\mathcal{E})$ were known to be algebraic with integer coefficients, for some integer n. The construction of Chapter 13 would then produce a cycle Z on the CM fourfold whose Weil coefficient is $n\nu_Z$ instead of ν_Z, and the two cycles built from it have Gram determinant $-\big(\int \omega \wedge \bar{\omega}\big)^2 \operatorname{Nm}(n\nu_Z)^2(b^4 - \bar{b}^4)^2$, which is the unit of (13.2) times n^4. If $p \nmid n$ nothing changes. If $p \mid n$, the specialized classes span a sublattice $\mathcal{L}'$ of the Weil lattice with $[\mathcal{L} : \mathcal{L}']^2 = n^4 \cdot (\text{unit})$, so $[\mathcal{L} : \mathcal{L}'] = p^{2v_p(n)}$, and the argument shows only $p^{v_p(n)}\mathcal{L} \subseteq \mathrm{Alg}^2$, which is already known: $p\mathcal{L} \subseteq S$ by Proposition 8.2. So a rational statement, which allows an unknown n, gives nothing at p, and the proof needs both the integrality of Proposition 11.5 and the exact value of the Weil coefficient.

Example 11.7 (the full multiplier at $d = 8$, $p = 5$). For $K = \mathbb{Q}(\sqrt{-2})$ and $d = 8$ the class of Proposition 11.5 is $2 \cdot 64^{64}\kappa_3(\mathcal{E})$, and $2 \cdot 64^{64} = 2^{385}$ is prime to 5. Its Weil component is $\mp 2^{385} \cdot \frac{9}{16}\Upsilon$. At $p = 5$ both factors are units, so the Weil component is $\nu\omega_{X_6} + \bar{\nu}\bar{\omega}_{X_6}$ with $\nu \in O_{K,(5)}^\times$. The degree $(d+1)^2 = 81$ of the isogeny ϱ is also prime to 5, although the argument does not need this.

Exercise 11.5. Let L be a free $\mathbb{Z}_p$-module of rank 2 with a symmetric bilinear form, and $x_1, x_2 \in L$ with a Gram determinant that is a unit. Show that nx_1, nx_2 span a sublattice of index $p^{2v_p(n)}$ in L, and that it contains pL only if $v_p(n) \le 1$.

11.7. The status of the dependency

The preprint. The note and this companion use statements of Markman's preprint [Mar25] whose proofs they have not verified. The preprint claims [Mar25, Theorem 1.5.1] that for every positive integer d the Weil classes of polarized abelian sixfolds of Weil type for $\mathbb{Q}(\sqrt{-d})$ with discriminant -1 are algebraic, a statement with rational coefficients.

What is assumed and what is proved. Hypothesis (M) consists of three statements made in the preprint's proof of that theorem, (M1)–(M3) of Section 11.3: the existence of the twisted sheaf $\mathcal{B}$, its semiregularity, and the deformation statement for semiregular twisted sheaves, in the form the preprint claims for families of abelian varieties. It also covers the other statements of the preprint cited in this chapter: the construction of $\mathcal{E}$ and its rank, the action η and the polarization, the Hodge type of $\kappa(\mathcal{E})$ and its invariance under the group of [Mar25, (3.1.1)], the Chern character of the ideal sheaves, and the spin formalism used in Lemma 11.8. The integral statement Proposition 11.5 is proved from Hypothesis (M) in Section 11.5. The proof explained here needs it with integer coefficients: if the class $2(8d)^{8d}\kappa_3(\mathcal{E})$ were known to be algebraic only after multiplication by an integer divisible by p, the argument of Chapter 13 would give nothing at p (Section 11.6).

Where (M) enters. Hypothesis (M) is used through Proposition 11.5 and Lemma 11.8, at exactly one point, the construction of the Weil cycle on the fourfold with complex multiplication (Proposition 13.2). Everything that depends on that construction is stated under "Assume Hypothesis (M)": Proposition 11.5, Lemma 11.8, Propositions 13.2 and 13.4, Theorem A(b) and Theorem C(b), and the conditional row of Table 15.1. Theorem A(a), Theorem B, Theorem C(a) and the nine unconditional classes of Chapter 15 do not use it.

11.8. The Weil coefficient

The following lemma computes the Weil component of $\kappa_3(\mathcal{E})$. Let $\rho_1 = \exp(\sqrt{-d}\Theta)$ and its conjugate $\rho_2 = \exp(-\sqrt{-d}\Theta)$ in $H^{\mathrm{ev}}(X_3, K_d)$, and

$$\varpi_d = \tfrac{1}{2}(1 + 1/\sqrt{-d}), \qquad \mathrm{Nm}(\varpi_d) = \tfrac{1}{4} + \tfrac{1}{4d} = \tfrac{d+1}{4d}.$$

Lemma 11.8 (the Weil coefficient). *Assume Hypothesis (M). For even $d \geq 3$, $\kappa_3(\mathcal{E})$ has components only of K_d-types $(6,0)$, $(0,6)$ and $(3,3)$, and its component of types $(6,0)\oplus(0,6)$ is $\mp\frac{d+1}{2d}\Upsilon$ with $\Upsilon = \frac{1}{2}(\omega_{X_6} + \bar\omega_{X_6})$, which is primitive in $H^6(X_6,\mathbb{Z})$ and hence in the lattice of integral Weil classes. In particular, for p inert in K_d with $p \nmid 2d(d+1)$, it is $\nu\omega_{X_6} + \bar\nu\bar\omega_{X_6}$ with $\nu = \mp\frac{d+1}{4d} \in O^\times_{K_d,(p)}$.*

Proof. *The input.* Markman's preprint states that $\mathrm{ch}(\mathcal{I}_1) = 1 + \Theta - \frac{d}{2}\Theta^2 - d[\mathrm{pt}]$ [Mar25, Lemma 8.2.1]; this follows from Grothendieck–Riemann–Roch for the $d+1$ curves, each of class $\Theta^2/2$ and genus 3, and the twist by Θ (Exercise 11.6). Expanding $\rho_1 = 1 + \sqrt{-d}\Theta - \frac{d}{2}\Theta^2 - d\sqrt{-d}[\mathrm{pt}]$, using $\Theta^3 = 6[\mathrm{pt}]$, one checks

$$\mathrm{ch}(\mathcal{I}_1) = \varpi_d\rho_1 + \bar\varpi_d\rho_2$$

term by term (Example 11.9). Moreover $\mathrm{ch}(\mathcal{I}_2) = \mathrm{ch}(\mathcal{I}_1)$, because a translate of $-\mathrm{AJ}(C)$ has the same class $\Theta^2/2$ and the same genus as a translate of $\mathrm{AJ}(C)$.

The spin formalism. Let $x \mapsto x^\star$ be the involution of $H^\bullet(X_3)$ of [Mar25, (1.2.3)]; it exchanges ρ_1 and ρ_2. Let $\mathfrak{s}$ be the linear map that Markman calls ϕ' [Mar25, Proposition 6.4.1], so that

$$\mathrm{ch}\,\mathrm{FM}(\mathcal{I}_2 \boxtimes \mathcal{I}_1) = \mathfrak{s}\big(\mathrm{ch}(\mathcal{I}_1)\otimes \mathrm{ch}(\mathcal{I}_1)^\star\big)$$

[Mar25, proof of Lemma 8.3.1]. Put $\tilde{\mathfrak{s}} = \exp(-c_1(\mathcal{P})/2)\cup\mathfrak{s}$, with $\mathcal{P}$ the Poincaré bundle on X_6. By [Mar25, (6.1.4) and Proposition 6.1.2], $\tilde{\mathfrak{s}}$ is equivariant: $\tilde{\mathfrak{s}}(gc\otimes gc') = \bar g(\tilde{\mathfrak{s}}(c\otimes c'))$ for g in the spin group $\mathrm{Spin}(H^1(X_6,K_d))$ of the pairing $(\cdot,\cdot)$, where g acts on $H^\bullet(X_3,K_d)$ by the spin representation and $\bar g$, its image in the special orthogonal group, acts on $H^\bullet(X_6,K_d) = \bigwedge^\bullet H^1(X_6,K_d)$. Since κ does not change when a class is multiplied by the exponential of a class of degree 2, $\kappa(\mathrm{FM}(\mathcal{I}_2\boxtimes\mathcal{I}_1)) = \kappa(\mathfrak{c})$ with

$$\mathfrak{c} = \tilde{\mathfrak{s}}\big(\mathrm{ch}(\mathcal{I}_1)\otimes\mathrm{ch}(\mathcal{I}_1)^\star\big) = \tfrac{d+1}{4d}\big(\tilde{\mathfrak{s}}(\rho_1\otimes\rho_1) + \tilde{\mathfrak{s}}(\rho_2\otimes\rho_2)\big) + \varpi_d^2\tilde{\mathfrak{s}}(\rho_1\otimes\rho_2) + \bar\varpi_d^2\tilde{\mathfrak{s}}(\rho_2\otimes\rho_1),$$

by expanding $(\varpi_d\rho_1 + \bar\varpi_d\rho_2)\otimes(\varpi_d\rho_2 + \bar\varpi_d\rho_1)$ and using $\varpi_d\bar\varpi_d = \frac{d+1}{4d}$.

The types. The stabilizer in the spin group of the two lines $K_d\rho_1$ and $K_d\rho_2$ acts on $\rho_1\otimes\rho_1$ and on $\rho_2\otimes\rho_2$ through the determinants of its actions on $\mathcal{W}_1$ and on $\mathcal{W}_2$, and trivially on $\rho_1\otimes\rho_2$ and $\rho_2\otimes\rho_1$ [Mar25, Section 6.4]. It contains an element that acts on $\mathcal{W}_1$ by 4 and on

$\mathcal{W}_2$ by $1/4$ [Mar25, Remark 2.4.3]; this element acts on classes of K_d-type (i,j) by 4^{i-j}, on $\rho_1\otimes\rho_1$ by 4^6, on $\rho_2\otimes\rho_2$ by 4^{-6} and trivially on the mixed terms. By the equivariance of $\tilde{\mathfrak{s}}$, $\tilde{\mathfrak{s}}(\rho_1\otimes\rho_1)$ lies in the eigenspace of 4^6, so it has type $(6,0)$; likewise $\tilde{\mathfrak{s}}(\rho_2\otimes\rho_2)$ has type $(0,6)$, and the mixed terms have only types (j,j). Hence $c_1(\mathfrak{c})$ has type $(1,1)$, the parts of $\mathfrak{c}$ of degree less than 6 have types (j,j), and in $\kappa_3(\mathfrak{c})$, which is the degree-6 part of $\exp(-c_1(\mathfrak{c})/8d)\,\mathfrak{c}$, the parts of types $(6,0)$ and $(0,6)$ come only from the degree-6 part of $\mathfrak{c}$ multiplied by 1. So $\kappa_3(\mathfrak{c})$ has only types $(6,0)$, $(0,6)$ and $(3,3)$, with $(6,0)$-part $\frac{d+1}{4d}\tilde{\mathfrak{s}}(\rho_1\otimes\rho_1)$. Without the normalization by κ this fails: the degree-6 part of $\operatorname{ch}\mathrm{FM}(\mathcal{I}_2\boxtimes\mathcal{I}_1)$ has components of every K_d-type.

The $(6,0)$-part. The element $g=\exp(\sqrt{-d}\Theta)$ of the spin group acts on $H^\bullet(X_3,K_d)$ as cup product with ρ_1, and $\bar g(w,y)=(w-\sqrt{-d}\Theta^\sharp y,y)$ [Mar25, (2.4.4)]. Since $\rho_1\otimes\rho_1=g1\otimes g1$, $\tilde{\mathfrak{s}}(\rho_1\otimes\rho_1)=\bar g(\tilde{\mathfrak{s}}(1\otimes 1))$. By [Mar25, Section 1.3], FM is the inverse of the composite of the equivalence $\mathrm{id}\times\Phi_{\mathcal{P}}\colon \mathrm{D}^b(X_6)\to\mathrm{D}^b(X_3\times X_3)$, whose kernel is the exterior product of the structure sheaf of the diagonal of $X_3\times X_3$ and $\mathcal{P}$, with the push-forward along the automorphism $(x_1,x_2)\mapsto(x_1+x_2,x_2)$ of $X_3\times X_3$. The former maps $\mathcal{O}_{X_3\times\{0\}}$ to $\mathcal{O}_{X_3}\boxtimes\mathcal{P}|_{X_3\times\{0\}}=\mathcal{O}_{X_3\times X_3}$, as the Poincaré bundle is trivial on $X_3\times\{0\}$ (see e.g. [Mil08, Chapter III, Section 1 and Summary 6.11], X_3 being a Jacobian), and the push-forward fixes $\mathcal{O}_{X_3\times X_3}$. Hence $\mathrm{FM}(\mathcal{O}_{X_3\times X_3})=\mathcal{O}_{X_3\times\{0\}}$, so $\mathfrak{s}(1\otimes 1)=\pm[X_3\times\{0\}]$, which $c_1(\mathcal{P})$ annihilates; so $\tilde{\mathfrak{s}}(1\otimes 1)=\pm y_1\wedge\cdots\wedge y_6$ for a $\mathbb{Z}$-basis (y_i) of $H^1(\hat X_3,\mathbb{Z})$, and $\bar g$ maps it to $\pm\bigwedge_i(-\sqrt{-d}\Theta^\sharp y_i,y_i)=\pm\omega_{X_6}$. Thus the Weil component of $\kappa_3(\mathrm{FM}(\mathcal{I}_2\boxtimes\mathcal{I}_1))$ is $\pm\frac{d+1}{4d}(\omega_{X_6}+\bar\omega_{X_6})=\pm\frac{d+1}{2d}\Upsilon$. Dualizing changes the sign of κ_3, and $\mathcal{E}$ is, up to an even shift, the dual of $\mathrm{FM}(\mathcal{I}_2\boxtimes\mathcal{I}_1)$ [Mar25, Theorem 1.4.1(2)], which gives the stated component.

Primitivity. Write (w,y) as $w+y$. Then $\omega_{X_6}=\bigwedge_i(y_i-\sqrt{-d}\Theta^\sharp y_i)$. Expanding the product, each wedge product of some of the y_i and of the $\Theta^\sharp y_j$ for the complementary indices appears with coefficient $(-\sqrt{-d})^k$, k the number of factors $\Theta^\sharp y_j$, and in $\Upsilon=\frac12(\omega_{X_6}+\bar\omega_{X_6})$ the terms with odd k cancel and those with even k have coefficient $(-d)^{k/2}$. Since the y_i and the $\Theta^\sharp y_i$ form a $\mathbb{Z}$-basis of $H^1(X_6,\mathbb{Z})$, these wedge products form part of a $\mathbb{Z}$-basis of $H^6(X_6,\mathbb{Z})$, so Υ is integral, and its coefficient 1 on $y_1\wedge\cdots\wedge y_6$ makes it primitive. Finally, $\Upsilon=\frac12\omega_{X_6}+\frac12\bar\omega_{X_6}$, so the Weil component is $\nu\omega_{X_6}+\bar\nu\bar\omega_{X_6}$ with $\nu=\mp\frac{d+1}{4d}$, a unit at p when $p\nmid 2d(d+1)$. □

Example 11.9 (the term-by-term check). Identify K_d with a subfield of $\mathbb{C}$ through ι, so that $\sqrt{-d}=\mathrm{i}\sqrt{d}$, $(\sqrt{-d})^2=-d$ and $(\sqrt{-d})^3=-d\sqrt{-d}$. Then $\varpi_d=\frac12+\frac{1}{2\sqrt{-d}}$ and $\varpi_d\sqrt{-d}=\frac{\sqrt{-d}}{2}+\frac12$. The degree-6 term of ρ_1 is $(\sqrt{-d})^3\Theta^3/6=-d\sqrt{-d}[\mathrm{pt}]$. Since ρ_2 is the complex conjugate of ρ_1, $\varpi_d\rho_1+\bar\varpi_d\rho_2$ is twice the real part of $\varpi_d\rho_1$, and degree by degree:

$$\begin{aligned}
H^0:&\quad 2\operatorname{Re}(\varpi_d)=1,\\
H^2:&\quad 2\operatorname{Re}(\varpi_d\sqrt{-d})\Theta=\Theta,\\
H^4:&\quad 2\operatorname{Re}(\varpi_d)\cdot(-\tfrac{d}{2})\Theta^2=-\tfrac{d}{2}\Theta^2,\\
H^6:&\quad 2\operatorname{Re}\left(\varpi_d\cdot(-d\sqrt{-d})\right)[\mathrm{pt}]=-d\cdot 2\operatorname{Re}(\varpi_d\sqrt{-d})[\mathrm{pt}]=-d[\mathrm{pt}].
\end{aligned}$$

This is $1+\Theta-\frac{d}{2}\Theta^2-d[\mathrm{pt}]=\operatorname{ch}(\mathcal{I}_1)$. For $d=4$, $\varpi_4=\frac12-\frac{\mathrm{i}}{4}$ and $2\operatorname{Re}(\varpi_4\cdot 2\mathrm{i})=2\operatorname{Re}(\mathrm{i}+\frac12)=1$.

Remark on the proof 11.1: what carries the lemma. The derivation for general d rests on Markman's spin formalism, in particular on the equivariance of $\tilde{\mathfrak{s}}$, which is taken from [Mar25, Proposition 6.1.2] and not re-derived here. Independently of that formalism, an exact computation confirms the content $\frac{d+1}{2d}$ and the types for $d=4,6,8,10,12,28$, and only for these values: the cohomological Fourier–Mukai transform of Orlov's equivalence is written out on explicit integral bases of $H^\bullet(X_3\times X_3)$ and $H^\bullet(X_3\times\hat X_3)$, the image of $\operatorname{ch}(\mathcal{I}_1)\boxtimes\operatorname{ch}(\mathcal{I}_1)$ is computed exactly over $\mathbb{Q}(\sqrt{-d})$ and normalized by $\exp(-c_1/\operatorname{rk})$, the eigenlattice $\mathcal{W}_{1,\mathbb{Z}}$ is determined as the annihilator of the decomposable degree-6 part

of the image of $\rho_1 \boxtimes \rho_2$, κ_3 is decomposed by K_d-types, and the content of its Weil component in the saturated lattice of integral Weil classes is computed by Hermite normal form. The results are rank $8d$, components only of types $(6,0)$, $(0,6)$, $(3,3)$, and contents $\frac{5}{8}, \frac{7}{12}, \frac{9}{16}, \frac{11}{20}, \frac{13}{24}, \frac{29}{56}$, which are $\frac{d+1}{2d}$. The same computation finds that the primitive integral alternating form attached to η has Pfaffian d^3, in agreement with the determinant d^6 of ψ_6 (Exercise 11.2).

EXERCISE 11.6. Let $C_1, \dots, C_{d+1} \subset X_3$ be disjoint translates of $\mathrm{AJ}(C)$. Using $[C_i] = \Theta^2/2$ and $\mathrm{ch}(\mathcal{O}_{C_i}) = [C_i] + (1 - \mathrm{genus}(C))[\mathrm{pt}]$, which is Grothendieck–Riemann–Roch for a curve in an abelian variety, compute ch of the ideal sheaf of $\bigcup C_i$ and then of its twist by Θ, and recover $\mathrm{ch}(\mathcal{I}_1) = 1 + \Theta - \frac{d}{2}\Theta^2 - d[\mathrm{pt}]$.

EXERCISE 11.7. Show that $\mathrm{Nm}(\varpi_d) = \frac{d+1}{4d}$ for every $d > 0$. For which d is $\frac{d+1}{2d}$ a unit at $p = 5$, at $p = 7$?

EXERCISE 11.8. Let $K = \mathbb{Q}(\sqrt{-d_0})$ with d_0 squarefree, p an odd prime inert in K, and $d = 4d_0$. Show that $K_d = K$, that $p \nmid 2d$, and that $p \nmid d+1$: if $p \mid d+1$ then $-d \equiv 1$ is a square modulo p, hence so is $-d_0$.

EXERCISE 11.9. Let $K = \mathbb{Q}(\mathrm{i})$ act on $\mathbb{Z}^2$ by $\mathrm{i} \mapsto \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Find a generator ω of the i-eigenlattice of $\mathbb{Z}^2 \otimes \mathbb{Z}[\mathrm{i}]$, show that $\omega + \bar{\omega}$ has content 2 in $\mathbb{Z}^2$, and show that $\{\nu\omega + \bar{\nu}\bar{\omega} : \nu \in \mathbb{Z}[\mathrm{i}]\}$ has index 4 in $\mathbb{Z}^2$. Why does the factor 2 not matter at an odd prime p?

Where this is used. Proposition 11.5 and Lemma 11.8 are combined with Schoen's step in Proposition 13.2, with $d = 4d_0$ for the field $K = \mathbb{Q}(\sqrt{-d_0})$ of the fourfold with complex multiplication of Chapter 12. The determinant d^6 of ψ_6 shows that $H^1(X_6, \mathbb{Z})$ is unimodular at p, which is a hypothesis of Proposition 10.9. Section 11.7 is the reference for every later "Assume Hypothesis (M)", and Section 14.7 lists it among what the proof rests on.

CHAPTER 12

A fourfold with complex multiplication

Where we are. Under Hypothesis (M), the Weil cycle of Chapter 13 is built in characteristic 0 on one fourfold X_{CM} of Mumford's family and then specialized to a supersingular point. This chapter constructs X_{CM} with the four properties the construction needs: an imaginary quadratic field K, inert at p, acts on X_{CM} with type $(2,2)$; the action is integral at p; the reduction X_{t_0} is supersingular; and at the reduction the action is diagonal in the cube basis of $\mathbb{M}$, with eigenset T_+ or T_- (Proposition 12.2). It then shows that $H_1(X_{\mathrm{CM}}, \mathbb{Z}_{(p)})$ is a unimodular Hermitian lattice (Lemma 12.6), which is the hypothesis of Schoen's step. It needs Chapters 6 and 7, the eigenset lemma Lemma 8.4 of Chapter 8, and Chapter 10.

12.1. The CM fourfold in two pages

Points of a Shimura variety with complex multiplication come from maximal tori. Choose an imaginary quadratic field K in which p is inert and which satisfies finitely many local conditions at the primes where B ramifies, so that the CM field $K' = kK$ embeds into B. The norm-one elements of K' over k, together with the scalars, form a torus $\mathbb{T} \subset G$ that is compact modulo the center over $\mathbb{R}$, and some point $\mathbf{h}$ of $\mathbb{X}$ factors through it, by the Skolem–Noether theorem applied at the non-compact real place (Section 12.3). The abelian fourfold X_{CM} at such a point has complex multiplication by the algebra $R = \mathbb{Q}[\mathbb{T}(\mathbb{Q})]$, which is $K \times K'$, as Section 12.4 shows.

Everything is read off from the eight weight lines of $\mathbb{T}$ on $U_1 \otimes U_2 \otimes U_3$, indexed by sign vectors $\epsilon \in \{\pm\}^3$ (Example 6.2). The Galois group permutes the slots and flips all signs, which gives two orbits, of sizes 2 and 6, and hence $R \cong K \times K'$. An embedding of K into R must respect this symmetry, and there are exactly two ways: by the product of the signs, which gives type $(2,2)$, and by the majority sign, which gives type $(1,3)$. The rest is bookkeeping at p. The lattice spanned by the integral weight lines is a tensor induction, hence a translate of the hyperspecial lattice, which gives integrality. The reduction is not μ-ordinary because $R \otimes \mathbb{Q}_p = \mathbb{Q}_{p^2} \times \mathbb{Q}_{p^6}$ has no homomorphism to $\mathbb{Q}_p$, so it is supersingular by Proposition 7.4. And the action at the reduction can be made diagonal in the cube basis by the Skolem–Noether theorem in a quaternion division algebra over $\mathbb{Q}_{p^3}$.

Example 12.1 (the sign vectors). The group generated by the permutations of the three slots and the simultaneous change of all signs acts on $\{\pm\}^3$ with two orbits:

$$\{+++, ---\} \qquad \text{and} \qquad \{++-, +-+, -++, --+, -+-, +--\}.$$

On the first orbit the product of the signs and the majority sign agree; on the second they disagree. The two K-structures of Section 12.4 have ι-eigensets $\{\epsilon : \epsilon_1\epsilon_2\epsilon_3 = +\}$ and $\{\epsilon : \text{majority of } \epsilon = +\}$, up to complement. Fixing the sign in slot 1, say $\epsilon_1 = +$, picks out four vectors $+++, ++-, +-+, +--$. Two of them, $+++$ and $+--$, have product $+$, so the product structure has type $(2,2)$; three of them have majority $+$, so the majority structure has type $(3,1)$, or $(1,3)$ for the complementary choice. In the cube basis of the model, the four eigensets are the four sets $\mathsf{T}_+, \mathsf{T}_-, \mathsf{M}_+, \mathsf{M}_-$ of Chapter 8; Example 12.5 gives the dictionary.

12.2. The statement

Assume (h1)–(h4) of (6.2). Write $\mathrm{Ram}_f(B)$ for the set of finite places of k at which B ramifies. For $\iota, \bar{\iota}$ and the types we use the conventions of Definition 10.2.

PROPOSITION 12.2 (the CM fourfold). *There are an imaginary quadratic field K in which p is inert, a point $t_{\mathrm{CM}} \in \mathrm{Sh}_{\mathsf{K}}(G,\mathbb{X})(\overline{\mathbb{Q}})$ with abelian fourfold X_{CM}, and a commutative algebra $R \cong K \times K' \subseteq \mathrm{End}(X_{\mathrm{CM}}) \otimes \mathbb{Q}$, $K' = kK$, such that:*

(a) $O_R \otimes \mathbb{Z}_p$ preserves $H_1(X_{\mathrm{CM}}, \mathbb{Z}_p)$;
(b) an embedding $K \hookrightarrow R$ makes X_{CM} of Weil type $(2,2)$ for K;
(c) t_{CM} reduces to a point $t_0 \in \mathscr{S}(\overline{\mathbb{F}}_p)$ with $X_{t_0} = \mathcal{A}_{t_0}$ supersingular, and R acts on X_{t_0};
(d) after an automorphism of $(M(X_{t_0}), F)$ and the identification of Proposition 7.4, $O_R \otimes \mathbb{Z}_p$ acts diagonally on the cube basis (e_s), and the ι-eigenset of $O_K \otimes \mathbb{Z}_p$ is T_+ or T_-.

The proof occupies Sections 12.3 to 12.6.

12.3. The field K and the torus

Choice of K. By (h3), p lies below no place of $\mathrm{Ram}_f(B)$. For each prime ℓ below a place of $\mathrm{Ram}_f(B)$, choose a quadratic field extension K_ℓ of $\mathbb{Q}_\ell$ that is contained in none of the completions k_v, $v \mid \ell$, $v \in \mathrm{Ram}_f(B)$. This is possible: since $[k:\mathbb{Q}] = 3$, at most one k_v with $v \mid \ell$ is quadratic over $\mathbb{Q}_\ell$, and $\mathbb{Q}_\ell$ has at least three quadratic extensions (Exercise 12.1). Choose K imaginary quadratic, inert at p and with completion K_ℓ at each such ℓ. These are finitely many local conditions on the square class of a negative integer, and they can be met simultaneously.

Then $K' \otimes_k k_v$ is a field at every place v where B ramifies: at the finite ones by the choice of K_ℓ, and at the two ramified real places because $K' \otimes_{k,\infty_i} \mathbb{R} = K \otimes \mathbb{R} = \mathbb{C}$. A quadratic extension of k embeds into the quaternion algebra B if and only if it is a field at every place where B ramifies (see e.g. [Voi21, Proposition 14.6.7]). So K' embeds into B, and we fix an embedding.

EXAMPLE 12.3 (the data at $p = 5$). For the data of Example 6.1, B ramifies only at two real places, so $\mathrm{Ram}_f(B) = \emptyset$ and the only condition on K is that 5 be inert. By Example 10.1, $K = \mathbb{Q}(\sqrt{-2})$ will do. Then $K' = kK$ is a CM field of degree 6 with $K' \otimes \mathbb{Q}_5 = \mathbb{Q}_{5^3} \otimes_{\mathbb{Q}_5} \mathbb{Q}_{5^2} \cong \mathbb{Q}_{5^6}$, because $\gcd(2,3) = 1$ (Exercise 12.2), and $R \otimes \mathbb{Q}_5 \cong \mathbb{Q}_{5^2} \times \mathbb{Q}_{5^6}$.

EXERCISE 12.1. Show that for an odd prime ℓ the group $\mathbb{Q}_\ell^\times / (\mathbb{Q}_\ell^\times)^2$ has order 4, with representatives $1, \xi, \ell, \xi\ell$ for a non-square unit ξ, so that $\mathbb{Q}_\ell$ has exactly three quadratic extensions. For $\ell = 2$ the group has order 8. Deduce that a quadratic extension of $\mathbb{Q}_\ell$ avoiding one given quadratic extension always exists.

EXERCISE 12.2. Let p be inert in k and in K. Show that $K' \otimes \mathbb{Q}_p \cong \mathbb{Q}_{p^3} \otimes_{\mathbb{Q}_p} \mathbb{Q}_{p^2} \cong \mathbb{Q}_{p^6}$. (Unramified extensions of $\mathbb{Q}_p$ are determined by their degree, and the compositum of those of degrees 3 and 2 has degree 6.) Deduce that K' has a single prime above p.

The torus. Let K'^1 be the kernel of the norm $K'^\times \to k^\times$, as an algebraic group over k. For $x \in K' \subset B$ the reduced norm of x in B is its norm to k, so $\mathrm{Res}_{k/\mathbb{Q}} K'^1 \subset B^1$, and we put

$$\mathbb{T} = \mathbb{G}_m \cdot \mathrm{Cor}\left(\mathrm{Res}_{k/\mathbb{Q}} K'^1\right) \subset G.$$

It is a torus of dimension $1 + 3 = 4$, which is the rank of G, so it is a maximal torus. Over $\mathbb{R}$, $K' \otimes_{k,\infty_i} \mathbb{R} = \mathbb{C}$ for each i, so $\mathrm{Res}_{k/\mathbb{Q}} K'^1(\mathbb{R}) = (\mathbb{C}^1)^3$ is compact and $\mathbb{T}_{\mathbb{R}}$ is compact modulo the center.

A point of $\mathbb{X}$ through the torus. We show that some $\mathbf{h} \in \mathbb{X}$ factors through $\mathbb{T}_{\mathbb{R}}$. Recall from Section 6.2 that $\mathbb{X}$ is the $G(\mathbb{R})$-conjugacy class of $\mathbf{h}_0$, which is induced by $(r,z) \mapsto (r, u_0(z))$, where $u_0(z) \in B^1(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R}) \times \mathrm{SU}(2)^2$ is 1 at the two ramified real places and, at ∞_1, the restriction to the circle S^1 of the embedding $\mathbb{C} \to \mathrm{Mat}_2(\mathbb{R})$, $x + \mathrm{i}y \mapsto \left(\begin{smallmatrix} x & y \\ -y & x \end{smallmatrix}\right)$. We use the following theorem.

FACT 12.4 (Skolem–Noether). *Two homomorphisms from a simple algebra over a field F to a central simple F-algebra Δ are conjugate by an element of $\Delta^\times$.*

For this see e.g. [Voi21, Main Theorem 7.7.1]. Apply it with $F = \mathbb{R}$ to the embedding of $K' \otimes_{k,\infty_1} \mathbb{R} \cong \mathbb{C}$ into $B \otimes_{k,\infty_1} \mathbb{R} \cong \mathrm{Mat}_2(\mathbb{R})$ given by the fixed embedding $K' \subset B$, and to the embedding above: they are conjugate by some $b \in \mathrm{GL}_2(\mathbb{R})$. The element $\mathrm{diag}(1,-1)$ normalizes the image of the second one, since it conjugates $x+\mathrm{i}y$ to $x-\mathrm{i}y$, so b can be taken in $\mathrm{SL}_2(\mathbb{R})$. Conjugating $\mathbf{h}_0$ by the image in $G(\mathbb{R})$ of $(1,b,1,1) \in \mathbb{R}^\times \times B^1(\mathbb{R})$ gives $\mathbf{h} \in \mathbb{X}$ with $\mathbf{h}(S^1)$ in the image of $(K' \otimes_{k,\infty_1} \mathbb{R})^1 \times \{1\} \times \{1\}$. Together with the scalars, this shows that $\mathbf{h}$ factors through $\mathbb{T}_\mathbb{R}$. Fix such an $\mathbf{h}$.

12.4. The algebra of complex multiplication

Over $\overline{\mathbb{Q}}$, $K' \otimes_{k,\tau} \overline{\mathbb{Q}} \cong \overline{\mathbb{Q}} \times \overline{\mathbb{Q}}$ for each embedding τ of k, the two factors corresponding to the two extensions of τ to K', which restrict to K as ι and as $\bar\iota$. Through $B \otimes_{k,\tau} \overline{\mathbb{Q}} = \mathrm{End}(U_i)$, K' splits each U_i into two eigenlines, and we label them $+$ and $-$ according to whether K' acts on them through the extension that restricts to ι or to $\bar\iota$ on K. So $\mathbb{T}$ acts on $U_1 \otimes U_2 \otimes U_3$ through eight characters on the eight lines indexed by $\epsilon \in \{\pm\}^3$, as in Example 6.2.

Galois orbits. The absolute Galois group of $\mathbb{Q}$ permutes these lines, because the characters are permuted. An automorphism permutes the slots as it permutes the three embeddings of k, and it changes all signs at once exactly when it acts non-trivially on K. The Galois closure of k is totally real and K is imaginary, so these two actions are independent, and the Galois group of the Galois closure of k contains a 3-cycle because it acts transitively on the three embeddings. So the orbits are those of Example 12.1: $\{+++, ---\}$, whose stabilizer is $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$, and the six others, each with stabilizer a conjugate of $\mathrm{Gal}(\overline{\mathbb{Q}}/K')$. The $\mathbb{Q}$-algebra $R = \mathbb{Q}[\mathbb{T}(\mathbb{Q})] \subset \mathrm{End}(\mathbb{V})$ generated by $\mathbb{T}(\mathbb{Q})$ is therefore the product of the fields of the two orbits:

$$R \cong K \times K'.$$

Since $\mathbf{h}$ factors through $\mathbb{T}_\mathbb{R}$ and $\mathbb{T}$ is commutative, R commutes with the Hodge structure, so $R \subseteq \mathrm{End}(X_{\mathrm{CM}}) \otimes \mathbb{Q}$ for every abelian variety X_{CM} in the isogeny class of the point.

The two K-structures. An embedding $K \hookrightarrow R$ acts on the line of ϵ through ι or $\bar\iota$, and Galois equivariance says that the rule $\epsilon \mapsto \iota$ or $\bar\iota$ is invariant under permutations of the slots and is reversed when all signs change. On the six-element orbit, $++-$, $+-+$, $-++$ are permuted transitively by the slots, so the rule is constant on them, and the opposite on their negatives: it is given by the majority sign. On $\{+++, ---\}$ there are two choices. So up to exchanging ι and $\bar\iota$ there are exactly two K-structures, with ι-eigensets

$$\{\epsilon : \epsilon_1\epsilon_2\epsilon_3 = +\} \qquad \text{and} \qquad \{\epsilon : \text{majority of } \epsilon = +\}.$$

Types. The Hodge cocharacter is non-trivial only in the slot of ∞_1, which we take to be slot 1 (Exercise 6.3), so $H^{1,0}$ is spanned by the four weight lines with a fixed sign in slot 1. By the count in Example 12.1, the product structure has type $(2,2)$ and the majority structure type $(1,3)$ or $(3,1)$. We use the product structure. This proves (b) of Proposition 12.2.

EXERCISE 12.3. Let a group act on $\{\pm\}^3$ by all permutations of the coordinates and by the simultaneous sign change. Find the orbits and their stabilizers. Repeat with only the cyclic permutations; do the orbits change?

EXERCISE 12.4. List the four ι-eigensets $\{\epsilon_1\epsilon_2\epsilon_3 = \pm\}$ and $\{\text{majority} = \pm\}$, and for each count how many elements have $\epsilon_1 = +$ and how many have $\epsilon_1 = -$. Which of the four give type $(2,2)$?

12.5. Integrality and supersingular reduction

Integrality, (a). Since p is inert in k and in K, $K'_p = K' \otimes \mathbb{Q}_p \cong \mathbb{Q}_{p^6}$ (Exercise 12.2). It embeds into $B \otimes_k k_p = \mathrm{End}_{k_p}(U_p)$ as a maximal subfield, so U_p is a one-dimensional K'_p-vector space. Choose $0 \neq x_0 \in U_p$ and put $\Lambda_{R,0} = O_{K'_p} x_0$, a $\mathbb{Z}_{p^3}$-lattice in U_p, and $\Lambda_R = \mathrm{Cor}(\Lambda_{R,0})$

(Definition 6.6). Since K_p'/k_p is unramified, $O_{K_p'} \otimes_{\mathbb{Z}_{p^3},\tau_i} W \cong W \times W$ compatibly with the two eigenlines in each slot, so

$$\Lambda_R \otimes W = \bigotimes_{i=1}^{3} (We_i^+ \oplus We_i^-) = \bigoplus_{\epsilon} We_1^{\epsilon_1} \otimes e_2^{\epsilon_2} \otimes e_3^{\epsilon_3}$$

is the sum of integral generators of the eight weight lines. On each of them an element of $O_R \otimes \mathbb{Z}_p$ acts by a scalar in W, so $O_R \otimes \mathbb{Z}_p$ preserves $\Lambda_R \otimes W$, hence Λ_R.

By (h4), $\Lambda \otimes \mathbb{Z}_p = p^j \operatorname{Cor}(\Lambda_0)$. The group $\mathrm{GL}_2(k_p) = \mathrm{GL}(U_p)$ acts transitively on the $\mathbb{Z}_{p^3}$-lattices of U_p, so there is $\gamma \in \mathrm{GL}_2(k_p)$ with $\gamma\Lambda_0 = \Lambda_{R,0}$. Then $\operatorname{Cor}(\gamma)$, which lies in $G(\mathbb{Q}_p)$ (Section 6.5) and commutes with ς, maps $\operatorname{Cor}(\Lambda_0)$ onto $\operatorname{Cor}(\Lambda_{R,0})$. So $\Lambda_R = \gamma_p(\Lambda \otimes \mathbb{Z}_p)$ with $\gamma_p = p^{-j}\operatorname{Cor}(\gamma) \in G(\mathbb{Q}_p)$. In the moduli description of the points of $\mathrm{Sh}_{\mathsf{K}}(G,\mathbb{X})$, the point $t_{\mathrm{CM}} = [\mathbf{h}, (\gamma_p, 1)]$ has an abelian fourfold X_{CM} with $H_1(X_{\mathrm{CM}}, \mathbb{Z}_p) = \Lambda_R$ and $H_1(X_{\mathrm{CM}}, \mathbb{Z}_\ell) = \Lambda \otimes \mathbb{Z}_\ell$ for $\ell \neq p$. This proves (a).

The same transitivity holds already for the elements of $\mathrm{GL}_2(k_p)$ with determinant in $\mathbb{Q}_p^\times$: multiplying γ by $\mathrm{diag}(\lambda^{-1}, 1)$, which preserves Λ_0 in a suitable basis, removes a unit λ from the determinant. The subgroup $\mathrm{SL}_2(k_p)$ alone is not transitive, even up to homothety, and Exercise 12.5 explains why.

Exercise 12.5. For a $\mathbb{Z}_{p^3}$-lattice $\Lambda_0' \subset U_p$ write $\Lambda_0' = \gamma'\Lambda_0$ and define its *parity* as $v_p(\det\gamma')$ modulo 2. Show that the parity is well defined on homothety classes of lattices, that $\mathrm{SL}_2(k_p)$ preserves it, and that an element of determinant p changes it. (In the language of the Bruhat–Tits tree of $\mathrm{PGL}_2(k_p)$, whose vertices are the homothety classes, the parity is the parity of the distance to the vertex of Λ_0.)

Reduction, (c). The abelian fourfold X_{CM} has complex multiplication by R, so by Fact 6.4(e) it has good reduction after a finite extension of its field of definition, and by Fact 6.4(d) t_{CM} extends to a point of $\mathscr{S}$ with special point t_0. The endomorphisms extend to the abelian scheme and reduce to endomorphisms of $X_{t_0} = \mathcal{A}_{t_0}$, by the Néron property (Fact 2.9), so R acts on X_{t_0}. If t_0 were μ-ordinary, the slope-0 part of $M(X_{t_0}) \otimes \mathbb{Q}$ would be an F-isocrystal of rank 1 (Proposition 7.4), preserved by R because endomorphisms commute with F. Its endomorphism algebra is $\{\lambda \in W[1/p] : \sigma\lambda = \lambda\} = \mathbb{Q}_p$, so $R \otimes \mathbb{Q}_p \cong \mathbb{Q}_{p^2} \times \mathbb{Q}_{p^6}$ would have a ring homomorphism to $\mathbb{Q}_p$. It has none: such a homomorphism would restrict to one of the two field factors as an embedding of $\mathbb{Q}_{p^2}$ or $\mathbb{Q}_{p^6}$ into $\mathbb{Q}_p$. By Proposition 7.4, t_0 is supersingular. This proves (c).

12.6. The diagonal action

Identify $M(X_{t_0})$ with the model $\mathbb{M}$ by Proposition 7.4. The elements of $\mathbb{T}(\mathbb{Q})$ fix the étale tensors, because they lie in $G(\mathbb{Q})$, so by Fact 6.4(c) they act on $M(X_{t_0}) \otimes \mathbb{Q}$ through the group

$$G^F = \{\gamma \in G(W[1/p]) : \ \gamma F = F\gamma\}.$$

The group G^F in the model. Write $\gamma = \gamma_1 \otimes \gamma_2 \otimes \gamma_3$ and compare γF with $F\gamma$ for $F(x_1 \otimes x_2 \otimes x_3) = \sigma x_3 \otimes A\sigma x_1 \otimes \sigma x_2$: up to scalars, $\gamma_1 = \sigma(\gamma_3)$, $\gamma_3 = \sigma(\gamma_2)$ and $\gamma_2 A = A\sigma(\gamma_1) = A\sigma^3(\gamma_2)$. After rescaling, every $\gamma \in G^F$ is a scalar times

$$\sigma^2(\gamma') \otimes \gamma' \otimes \sigma(\gamma'), \qquad \gamma' \in \Delta^\times,$$

where Δ is the centralizer of $A\sigma^3$ in $\mathrm{Mat}_2(W[1/p])$, that is, the set of γ' with $\gamma' A = A\sigma^3(\gamma')$. Comparing entries in this equation (Exercise 12.6) shows that Δ consists of the matrices

$$\begin{pmatrix} \lambda & p\lambda' \\ \sigma^3(\lambda') & \sigma^3(\lambda) \end{pmatrix}, \qquad \lambda, \lambda' \in \mathbb{Q}_{p^6},$$

so it is the quaternion division algebra over $\mathbb{Q}_{p^3}$, the center $\{\lambda : \sigma^3\lambda = \lambda\} \cap \mathbb{Q}_{p^6}$ (see e.g. [Voi21, Corollary 13.3.14], with the unramified quadratic extension $\mathbb{Q}_{p^6}$ of $\mathbb{Q}_{p^3}$ and the uniformizer p). The element A is the case $\lambda = 0$, $\lambda' = 1$, and $A^2 = p$; its valuation ring O_Δ is the set

of these matrices with $\lambda, \lambda' \in \mathbb{Z}_{p^6}$, and $\Delta^\times = A^{\mathbb{Z}} O_\Delta^\times$ (see e.g. [Voi21, Theorem 13.3.11]). In particular $O_\Delta \subset \mathrm{Mat}_2(W)$.

The slot-2 components of $\mathbb{T}(\mathbb{Q})$. Let $\Delta_\mathbb{T} \subseteq \Delta$ be the $\mathbb{Q}_{p^3}$-span of the slot-2 components γ' of the elements $\gamma \in \mathbb{T}(\mathbb{Q})$, written as above. It is commutative. Indeed, if $\gamma, \tilde\gamma \in \mathbb{T}(\mathbb{Q})$, which commute, have slot-2 components $\gamma', \tilde\gamma'$, then $\gamma'\tilde\gamma' = c\tilde\gamma'\gamma'$ for a scalar c with $c^2 = 1$, by determinants. As $c = \pm 1$ is fixed by σ, the same c appears in each of the three slots, so $\gamma\tilde\gamma = c^3\tilde\gamma\gamma$; thus $c^3 = 1$, as the kernel of $\mathrm{GL}_2^3 \to \mathrm{GL}_8$ consists of the triples of scalars with product 1 (Proposition 6.7, Step 1), and $c = 1$. As Δ is a division algebra, $\Delta_\mathbb{T}$ is a field, and its degree over the center $\mathbb{Q}_{p^3}$ divides $\dim_{\mathbb{Q}_{p^3}} \Delta = 4$ and is not 4, since Δ is not commutative.

To see that this degree is 2, count dimensions over $W[1/p]$. The $W[1/p]$-span of the action of $\mathbb{T}(\mathbb{Q})$ on $\mathbb{M} \otimes \mathbb{Q}$ is the image of $R \otimes_\mathbb{Q} W[1/p] \cong W[1/p]^8$, which acts faithfully, as R does on X_{t_0}, by Fact 4.10 and because $\mathrm{End}(\mathbb{M}, F) \otimes W$ is a lattice in $\mathrm{End}_W(\mathbb{M})$ (Section 5.7). Each $\gamma \in \mathbb{T}(\mathbb{Q})$ is a scalar times $\sigma^2(\gamma') \otimes \gamma' \otimes \sigma(\gamma')$, so this image lies in the tensor product of the $W[1/p]$-spans of $\sigma^2(\Delta_\mathbb{T})$, $\Delta_\mathbb{T}$ and $\sigma(\Delta_\mathbb{T})$ in $\mathrm{Mat}_2(W[1/p])$. These spans are commutative, so each has dimension at most 2, and their tensor product has dimension at most 8. Hence each of them has dimension 2, their tensor product is the image of $R \otimes W[1/p]$, and the $W[1/p]$-span of $\Delta_\mathbb{T}$, being a subalgebra of an algebra isomorphic to $W[1/p]^8$, is isomorphic to $W[1/p] \times W[1/p]$. So $\Delta_\mathbb{T}$ has degree 2 over $\mathbb{Q}_{p^3}$, and $\Delta_\mathbb{T} \otimes_{\mathbb{Q}_{p^3}} W[1/p]$ is not a field. A quadratic extension of $\mathbb{Q}_{p^3}$ fails to stay a field over $W[1/p]$ exactly when it embeds into $W[1/p]$, which is unramified over $\mathbb{Q}_p$; so only the unramified one does, and $\Delta_\mathbb{T}$ is a maximal subfield of Δ isomorphic to $\mathbb{Q}_{p^6}$. Another maximal subfield isomorphic to $\mathbb{Q}_{p^6}$ is the diagonal one,

$$\Delta_0 = \{\mathrm{diag}(\lambda, \sigma^3\lambda) : \lambda \in \mathbb{Q}_{p^6}\},$$

which commutes with $A\sigma^3$ because $A\,\mathrm{diag}(\sigma^3\lambda, \lambda) = \mathrm{diag}(\lambda, \sigma^3\lambda)A$.

By Fact 12.4, applied over the center $\mathbb{Q}_{p^3}$ of Δ to the two embeddings of $\mathbb{Q}_{p^6}$, $\Delta_\mathbb{T}$ is conjugate to Δ_0 by an element of $\Delta^\times = A^{\mathbb{Z}} O_\Delta^\times$. Conjugation by A maps Δ_0 to itself, $A\,\mathrm{diag}(\lambda, \sigma^3\lambda)A^{-1} = \mathrm{diag}(\sigma^3\lambda, \lambda)$, so the conjugating element can be taken in $O_\Delta^\times$; call it γ_0'. The automorphism $\sigma^2(\gamma_0') \otimes \gamma_0' \otimes \sigma(\gamma_0')$ of $(\mathbb{M}, F)$ is integral, and after applying it the slot components of the elements of $\mathbb{T}(\mathbb{Q})$ are diagonal: $\mathrm{diag}(\lambda, \sigma^3\lambda)$ in slot 2 and its conjugates $\mathrm{diag}(\sigma^2\lambda, \sigma^5\lambda)$ and $\mathrm{diag}(\sigma\lambda, \sigma^4\lambda)$ in slots 1 and 3. So $\mathbb{T}(\mathbb{Q})$, and with it its $\mathbb{Q}$-span R, $R \otimes \mathbb{Q}_p$ and $O_R \otimes \mathbb{Z}_p$, act diagonally on the cube basis e_s. By (a), the order $\mathrm{End}(X_{\mathrm{CM}}) \cap K$ has conductor prime to p (first step of the proof of Lemma 12.6, which uses only (a)), so $O_K \otimes \mathbb{Z}_{(p)}$ acts on the abelian scheme and Lemma 8.4(ii) applies. By (b) the K-structure has type $(2, 2)$ on the generic fiber, so by Lemma 8.4(ii) its ι-eigenset is T_+ or T_-. This proves (d) and completes the proof of Proposition 12.2.

Remark on the proof 12.1: the slot components. Two steps here are terse. The rescaling that puts an element of G^F in the form $\sigma^2(\gamma') \otimes \gamma' \otimes \sigma(\gamma')$ uses that the scalar λ with $\gamma' A = \lambda A \sigma^3(\gamma')$ is a unit, which follows from determinants, and that every unit of W is $\lambda'/\sigma^3(\lambda')$ for some unit λ', by Lang's lemma in rank 1. The identification of $\Delta_\mathbb{T}$ with $\mathbb{Q}_{p^6}$ rests on the dimension count over $W[1/p]$, which uses that $R \otimes W[1/p]$ acts faithfully on $\mathbb{M} \otimes \mathbb{Q}$; without it, the slot-2 components could a priori span only the center.

Exercise 12.6. Write $\gamma' = \left(\begin{smallmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{smallmatrix}\right)$ and compare the entries of $\gamma' A$ and $A\sigma^3(\gamma')$. Show that $x_{12} = p\sigma^3(x_{21})$ and $x_{11} = \sigma^3(x_{22})$, $x_{22} = \sigma^3(x_{11})$, so that x_{11} and x_{12} are fixed by σ^6, and deduce the description of Δ. Show directly that Δ is a division algebra: the determinant $\lambda\sigma^3(\lambda) - p\lambda'\sigma^3(\lambda')$ has valuation $\min(2v_p(\lambda), 2v_p(\lambda') + 1)$, so it vanishes only at 0.

Example 12.5 (the dictionary with the four sets). In the diagonal form, an element of $R \otimes \mathbb{Q}_p$ that lies in $G(\mathbb{Q}_p)$, with slot-2 component $\mathrm{diag}(\lambda, \sigma^3\lambda)$ acts on e_s, up to a common scalar, by $\sigma^{j_1}(\lambda)\sigma^{j_2}(\lambda)\sigma^{j_3}(\lambda)$ with $j_1 = 2 + 3s_1$, $j_2 = 3s_2$, $j_3 = 1 + 3s_3$, exponents modulo 6. For a general λ, the lines e_{001} and e_{110} have the characters $\lambda\sigma^2(\lambda)\sigma^4(\lambda)$ and its conjugate, which take values in $\mathbb{Q}_{p^2}$: these are the two lines on which $\mathbb{T}$ acts through K. To separate the

other six, take the element $b/\bar{b}$ of $K_p'^1$ for $b \in K_p^\times = \mathbb{Q}_{p^2}^\times$; its slot-2 component is $\mathrm{diag}(\lambda, \sigma^3\lambda)$ with $\lambda = b/\bar{b}$, up to replacing λ by λ^{-1}. Then $\sigma^j(\lambda)$ is λ for even j and λ^{-1} for odd j, and counting even minus odd exponents gives the character λ^{n_s}:

s	000	011	101	010	111	100	001	110
$\{j_1, j_2, j_3\}$	$\{2,0,1\}$	$\{2,3,4\}$	$\{5,0,4\}$	$\{2,3,1\}$	$\{5,3,4\}$	$\{5,0,1\}$	$\{2,0,4\}$	$\{5,3,1\}$
n_s	1	1	1	-1	-1	-1	3	-3

The six lines with $n_s = \pm 1$ split into the alternate vertices $\{000, 011, 101\}$ and $\{010, 111, 100\}$ of the six-cycle of Frobenius (Example 7.1), and by the Galois symmetry of Section 12.4 they play the roles of the majority-$+$ and majority-$-$ vectors, in some order. A K-structure acts through one embedding on one triple and through the other on the other triple, and attaches one of the two K-lines to each triple. Attaching e_{110} to $\{000, 011, 101\}$ gives the eigensets

$$\mathsf{T}_+ = \{000, 011, 101, 110\}, \qquad \mathsf{T}_- = \{001, 010, 100, 111\},$$

and attaching e_{001} gives

$$\mathsf{M}_+ = \{000, 001, 011, 101\}, \qquad \mathsf{M}_- = \{010, 100, 110, 111\},$$

which are the four sets of Chapter 8. The kernel of F modulo p is spanned by the e_s with $s_1 = 1$, and it meets T_+, T_-, M_+, M_- in $2, 2, 1, 3$ elements. So the first pair has type $(2,2)$ and is the product structure, and the second pair has types $(1,3)$ and $(3,1)$ and is the majority structure; this is Lemma 8.4 seen from the torus. The two-element orbit $\{+++, ---\}$ corresponds to $\{e_{001}, e_{110}\}$.

12.7. Unimodularity at p

LEMMA 12.6 (unimodularity). *In Proposition 12.2, $H_1(X_{\mathrm{CM}}, \mathbb{Z}_{(p)})$ is an $O_{K,(p)}$-module, and for a suitable polarization of X_{CM} it is a unimodular Hermitian $O_{K,(p)}$-lattice.*

PROOF. *The module structure.* $\mathrm{End}(X_{\mathrm{CM}})$ consists of the endomorphisms of $H_1(X_{\mathrm{CM}}, \mathbb{Q})$ that preserve the Hodge structure and the lattice $H_1(X_{\mathrm{CM}}, \mathbb{Z})$, so $\mathrm{End}(X_{\mathrm{CM}}) \otimes \mathbb{Z}_p$ consists of the elements of $\mathrm{End}(X_{\mathrm{CM}}) \otimes \mathbb{Q}_p$ that preserve $H_1(X_{\mathrm{CM}}, \mathbb{Z}_p)$. By Proposition 12.2(a) this contains $O_K \otimes \mathbb{Z}_p$. So the order $\mathrm{End}(X_{\mathrm{CM}}) \cap K$ has conductor prime to p, and $O_{K,(p)}$ acts on $H_1(X_{\mathrm{CM}}, \mathbb{Z}_{(p)})$.

A polarization perfect at p. Let ψ_{CM} be the Riemann form of a polarization of X_{CM} whose class is a multiple of the polarization ψ of the Shimura datum. The group $G(W)$ acts on $\Lambda \otimes W$ by similitudes with unit multipliers, so the ψ_{CM}-dual of $\Lambda \otimes W$ is again $G(W)$-stable, and since the W-lattices stable under $G(W)$ are the $p^{j'}\Lambda \otimes W$ (Proposition 6.7(d)), it is $p^{j'}\Lambda \otimes W$ for some j'; the same holds for $\Lambda \otimes \mathbb{Z}_p$. The element γ_p is a similitude, so the ψ_{CM}-dual of $\Lambda_R = \gamma_p(\Lambda \otimes \mathbb{Z}_p)$ is $p^{j''}\Lambda_R$ for some j''. Since ψ_{CM} is integral on Λ_R, the dual contains Λ_R, so $j'' \le 0$, and $\psi_{\mathrm{CM}}(\Lambda_R, \Lambda_R) \subseteq p^{|j''|}\mathbb{Z}_p$. The form $p^{-|j''|}\psi_{\mathrm{CM}}$ is integral on Λ_R, and the dual of Λ_R for it is $p^{|j''|} \cdot p^{j''}\Lambda_R = \Lambda_R$, so it is perfect on Λ_R. It is still integral on $H_1(X_{\mathrm{CM}}, \mathbb{Z})$, because it is integral at p and differs from ψ_{CM} by a unit at every prime $\ell \neq p$, and it is still positive. We replace ψ_{CM} by it.

The Hermitian form. The Rosati involution of ψ_{CM} preserves $R = \mathbb{Q}[\mathbb{T}(\mathbb{Q})]$: for $\gamma \in \mathbb{T}(\mathbb{Q})$, $\psi_{\mathrm{CM}}(\gamma x, \gamma y) = \lambda_\gamma \psi_{\mathrm{CM}}(x, y)$ with a multiplier $\lambda_\gamma \in \mathbb{Q}^\times$, so $\gamma^\dagger = \lambda_\gamma \gamma^{-1} \in R$. The Rosati involution is positive, and the only positive involution of an imaginary quadratic field is complex conjugation, so it restricts to complex conjugation on K. Hence ψ_{CM} is compatible with K and $\psi_{\mathrm{CM}} = \mathrm{Tr}_{K/\mathbb{Q}} \circ \mathcal{H}$ for a unique skew-Hermitian form $\mathcal{H}$ (Definition 10.4). Since p is unramified in K, the ψ_{CM}-dual and the $\mathcal{H}$-dual of Λ_R coincide (Exercise 10.6), so $\mathcal{H}$, and with it $h = \theta\mathcal{H}$, is unimodular on $\Lambda_R = H_1(X_{\mathrm{CM}}, \mathbb{Z}_p)$, hence on $H_1(X_{\mathrm{CM}}, \mathbb{Z}_{(p)})$. □

What just happened. The CM fourfold is a point of Mumford's family whose torus is built from $K' = kK$ with K inert at p. The Galois symmetry of the eight weight lines gives $R = K \times K'$ and exactly two K-structures, of types $(2,2)$ and $(1,3)$. At p

the weight lines span a tensor-induced lattice, a translate of the hyperspecial one, which gives integrality and, after rescaling the polarization, unimodularity. The reduction is supersingular because $R \otimes \mathbb{Q}_p$ has no homomorphism to $\mathbb{Q}_p$, and Skolem–Noether in the quaternion division algebra Δ diagonalizes the action on the cube basis, where the type $(2,2)$ structure has eigenset T_+ or T_-.

Where this is used. Proposition 12.2 and Lemma 12.6 are the input of Chapter 13: (b) and Lemma 12.6 feed Schoen's step in Proposition 13.2, (c) provides the abelian scheme along which the Weil cycle is specialized, and (d) puts the specialized classes into the Weil lattice $\mathcal{L}$ in Proposition 13.4.

CHAPTER 13

A p-integral Weil cycle and its specialization

Where we are. This chapter produces the one algebraic class that the gap needs. Under Hypothesis (M) it constructs an algebraic cycle Z on the CM fourfold X_{CM} whose Weil component $\nu_Z\omega + \bar{\nu}_Z\bar{\omega}$ has a coefficient ν_Z that is a unit at p (Proposition 13.2), and then shows that the specializations to the supersingular point t_0 of two cycles built from Z span the whole Weil lattice $\mathcal{L}(X_{t_0})$ (Proposition 13.4). The second step uses only intersection numbers, not a p-adic comparison theorem. It needs the discriminant lemma Lemma 4.13, the Weil lattice of Chapter 8, and Chapters 10 to 12.

13.1. The specialization argument in two pages

Let $K = \mathbb{Q}(\sqrt{-d_0})$, X_{CM} and t_0 be as in Proposition 12.2. Assume Hypothesis (M). With $d = 4d_0$, Markman's sixfold X_6 has a Weil-type lattice that is unimodular at p, Schoen's step (Proposition 10.9) gives an isogeny $X_{\mathrm{CM}} \times X_2 \to X_6'$ of degree prime to p onto a member of its family, and Proposition 11.5, which is proved from Hypothesis (M), gives an algebraic cycle on X_6' with integer coefficients whose Weil coefficient is a unit at p (Lemma 11.8). Pulling back to $X_{\mathrm{CM}} \times X_2$, cutting with a divisor on X_2 and pushing to X_{CM} gives a cycle Z on X_{CM} whose Weil component is $\nu_Z\omega + \bar{\nu}_Z\bar{\omega}$ with $\nu_Z \in O_{K,(p)}^{\times}$.

The task is to carry this unit to the supersingular point. The classes on X_{t_0} live in crystalline cohomology, and the Weil component of Z lives in Betti cohomology; comparing the two directly would need integral p-adic Hodge theory. The one idea of the chapter is that intersection numbers do the comparison. Choose $b \in O_K$ whose reduction generates $\mathbb{F}_{p^2}^{\times}$. A polynomial Q_P with coefficients in $\mathbb{Z}_{(p)}$, evaluated at $[b]^*$, is the projector P onto the Weil part in Betti cohomology of X_{CM} and, by Proposition 12.2(d), in crystalline cohomology of X_{t_0}, because it is defined by the eigenvalues of $[b]^*$. The cycles $Z_1 = PZ$ and $Z_2 = [b]^*Z_1$ have the Gram determinant

$$\det\big(\deg(Z_i \cdot Z_j)\big) = -\langle\omega,\bar{\omega}\rangle^2 \,\mathrm{Nm}(\nu_Z)^2 (b^4 - \bar{b}^4)^2,$$

with $\langle\omega,\bar{\omega}\rangle = \int \omega\wedge\bar{\omega}$ a unit at p, and this is a unit at p. Specialization preserves intersection numbers, so the crystalline classes of the specialized cycles, which are integral and lie in the Weil lattice $\mathcal{L}$ of rank 2, span a sublattice of unit discriminant; by the discriminant formula it is all of $\mathcal{L}$.

Example 13.1 (the Gram determinant at $p = 5$). For $K = \mathbb{Q}(\sqrt{-2})$ and $b = 1 + \sqrt{-2}$: $b^2 = -1 + 2\sqrt{-2}$ and $b^4 = -7 - 4\sqrt{-2}$, so $b^4 - \bar{b}^4 = -8\sqrt{-2}$ and $(b^4 - \bar{b}^4)^2 = -128$. The Gram determinant is $128\langle\omega,\bar{\omega}\rangle^2 \,\mathrm{Nm}(\nu_Z)^2$, and $128 = 2^7$ is prime to 5. The reduction of b modulo 5 generates $\mathbb{F}_{25}^{\times}$, a group of order 24 (Example 13.3).

13.2. The Weil cycle on the CM fourfold

In this section X_{CM} carries the polarization of Lemma 12.6, so that $H_1(X_{\mathrm{CM}}, \mathbb{Z}_{(p)})$ is a unimodular Hermitian $O_{K,(p)}$-lattice, K acts with type $(2,2)$, and ω is the exterior product of an $O_{K,(p)}$-basis of the eigenlattice $H^1_\iota(X_{\mathrm{CM}})$ (Definition 10.3).

Proposition 13.2 (the Weil cycle). *Assume Hypothesis (M). Let X_{CM} and $K = \mathbb{Q}(\sqrt{-d_0})$, d_0 squarefree, be as in Proposition 12.2, with the polarization of Lemma 12.6. Then there*

is an algebraic cycle Z on X_{CM} with integer coefficients whose class has Weil component $\nu_Z\omega+\bar\nu_Z\bar\omega$ with $\nu_Z\in O_{K,(p)}^\times$, and whose other components have K-types $(i,4-i)$ with $i\neq 0,4$.

PROOF. *The parameter.* Put $d=4d_0$. Then $d\geq 4$ is even and $K_d=\mathbb{Q}(\sqrt{-4d_0})=K$. Since p is odd and inert in K, $p\nmid 2d$, and $p\nmid d+1$ by Exercise 11.8.

The sixfold is unimodular at p. The polarization of X_6 is $\psi_6(x,y)=(\eta x,y)$ on $H^1(X_6,\mathbb{Z})$, where $(\cdot,\cdot)$ is the perfect pairing between $H^1(X_3,\mathbb{Z})$ and $H^1(\hat X_3,\mathbb{Z})$, and its determinant is d^6 (Exercise 11.2), a unit at p. So ψ_6 is perfect on $H^1(X_6,\mathbb{Z}_{(p)})$, and by Exercise 10.6 $H^1(X_6,\mathbb{Z}_{(p)})$, and its dual $H_1(X_6,\mathbb{Z}_{(p)})$, are unimodular Hermitian lattices over $O_{K,(p)}=\mathbb{Z}_{(p)}[\sqrt{-d}]$ for the Hermitian form of ψ_6.

Homology and cohomology. Proposition 10.9 works with first homology, on which K acts by push-forward, while Markman's data $(H^1(X_6,\mathbb{Z}),\eta,\psi_6)$ live in first cohomology. For every member $X_{6,t}$ of the family, $x\mapsto\psi_6(x,\cdot)$ maps $H^1(X_6,\mathbb{Z})$ into $H_1(X_{6,t},\mathbb{Z})=\mathrm{Hom}(H^1(X_6,\mathbb{Z}),\mathbb{Z})$ with cokernel of order d^6, prime to p. It is a morphism of Hodge structures up to a Tate twist, as ψ_6 is a polarization, and it carries ψ_6 to the dual form, the Riemann form of the polarization. Since η is skew-adjoint for $(\cdot,\cdot)$ [Mar25, Section 2.4], it is skew-adjoint for ψ_6, and this map carries $-\eta$ to the push-forward by the endomorphism of $X_{6,t}$ whose pull-back is η (Exercise 13.1). So, in this proof, when $H_1(X_6,\mathbb{Z}_{(p)})$ with its action of K is compared with $H_1(X_{\mathrm{CM}},\mathbb{Z}_{(p)})$, $\sqrt{-d}$ acts on $H^1(X_6,\mathbb{Q})$ by $-\eta$, and the Hermitian form of ψ_6 (Definition 10.4) for this action is $-\bar h$, where h is its Hermitian form for the action η. Like h, it is unimodular on $H^1(X_6,\mathbb{Z}_{(p)})$ and has signature $(3,3)$, and $\det(-\bar h)=(-1)^6\overline{\det h}=\det h$, as $\det h$ is rational. This change of K-structure exchanges the K-types (i,j) and (j,i), so it maps Weil classes to Weil classes. The K-types of classes on the members of the family, in Lemma 11.8 and below, refer to the action by pull-back, that is, to η.

Schoen's step. By Proposition 10.9, applied to X_6 and $X=X_{\mathrm{CM}}$, there are a polarized abelian surface X_2 of Weil type $(1,1)$ with $H_1(X_2,\mathbb{Z}_{(p)})$ unimodular, a member X_6' of the family of $(H^1(X_6,\mathbb{Z}),\eta,\psi_6)$, and an isogeny $\vartheta\colon X_{\mathrm{CM}}\times X_2\to X_6'$ of degree prime to p, compatible with K. By Proposition 11.5 there is an algebraic cycle Z_6 on X_6' with integer coefficients and class $2(8d)^{8d}\kappa_3$, the flat continuation of $2(8d)^{8d}\kappa_3(\mathcal{E})$. The class ω_{X_6} is defined by the lattice and η, so it continues flatly to the class $\omega_{X_6'}$ of X_6'. By Lemma 11.8 the Weil component of $[Z_6]$ is $\nu\omega_{X_6'}+\bar\nu\bar\omega_{X_6'}$ with $\nu\in O_{K,(p)}^\times$, because $2(8d)^{8d}$ is prime to p, and the other components of $[Z_6]$ have K-type $(3,3)$.

Pull-back. The pull-back ϑ^* is an isomorphism on $H^1(\cdot,\mathbb{Z}_{(p)})$, since the degree of ϑ is prime to p, and it commutes with the actions of $O_{K,(p)}$ by pull-back. So it maps $H^1_\iota(X_6')=\mathcal{W}_{1,\mathbb{Z}}\otimes\mathbb{Z}_{(p)}$, on which η acts by $\sqrt{-d}$, onto $H^1_\iota(X_{\mathrm{CM}})\oplus H^1_\iota(X_2)$, and on top exterior powers

$$\vartheta^*\omega_{X_6'}=\det{}_K(\vartheta^*)\cdot\omega\wedge\omega',$$

where ω' is the exterior product of an $O_{K,(p)}$-basis of $H^1_\iota(X_2)$ and $\det_K(\vartheta^*)\in O_{K,(p)}^\times$ is the determinant of ϑ^* in the chosen bases. The other components of $\vartheta^*[Z_6]$ have K-type $(3,3)$.

Cutting and pushing. Since X_2 has type $(1,1)$, ω' and $\bar\omega'$ have Hodge type $(1,1)$ (as in Exercise 10.1), so $\omega'+\bar\omega'\in H^2(X_2,\mathbb{Z}_{(p)})$ is a rational class of Hodge type $(1,1)$, and $n_1(\omega'+\bar\omega')$ is integral for some positive integer n_1 prime to p. By the Lefschetz theorem on $(1,1)$-classes (see e.g. [Voi16, Theorem 2]), $n_1(\omega'+\bar\omega')$ is the class of a divisor y on X_2. Put

$$Z=\mathrm{pr}_{X_{\mathrm{CM}}*}\left(\vartheta^*Z_6\cdot\mathrm{pr}_{X_2}^*\,y\right),$$

a cycle on X_{CM} with integer coefficients. The push-forward $\mathrm{pr}_{X_{\mathrm{CM}}*}$ keeps only the part of top degree $(2,2)$ on X_2. So a component of $\vartheta^*[Z_6]$ of K-type (i,j) on $X_{\mathrm{CM}}\times X_2$ contributes to the K-type $(4,0)$ on X_{CM} only if its X_{CM}-part has type $(4,0)$ and its X_2-part has type $(2,0)$, to be completed by $\bar\omega'$, or type $(0,2)$, to be completed by ω'; that is, only if (i,j) is

$(6,0)$ or $(4,2)$. Only $(6,0)$ occurs. Its contribution is

$$\mathrm{pr}_{X_{\mathrm{CM}*}}\left(\nu \det{}_K(\vartheta^*)\omega\wedge\omega'\wedge n_1\bar\omega'\right)=\nu_Z\omega,\qquad \nu_Z=\pm n_1\nu\det{}_K(\vartheta^*)\int_{X_2}\omega'\wedge\bar\omega'.$$

The integral is a unit of $O_{K,(p)}$, because $H^1(X_2,\mathbb{Z}_{(p)})\otimes O_{K,(p)}$ is the sum of the two eigenlattices, so $\omega'\wedge\bar\omega'$ generates $H^4(X_2,O_{K,(p)})$. So ν_Z is a unit. The $(0,4)$-component is the conjugate $\bar\nu_Z\bar\omega$, and the components of K-type $(3,3)$ of $\vartheta^*[Z_6]$ contribute only to K-types $(i,4-i)$ with $i\neq 0,4$. □

Exercise 13.1. Let Γ be a free $\mathbb{Z}$-module of finite rank with a symmetric bilinear form $(\cdot,\cdot)$ and an endomorphism η that is skew-adjoint for it, $(\eta x,y)=-(x,\eta y)$, and put $\psi(x,y)=(\eta x,y)$. Show that η is skew-adjoint for ψ. Let $\delta\colon\Gamma\to\Gamma^\vee=\mathrm{Hom}(\Gamma,\mathbb{Z})$ be $x\mapsto\psi(x,\cdot)$ and $\eta^\vee(f)=f\circ\eta$ the transpose. Show that $\delta\circ(-\eta)=\eta^\vee\circ\delta$. Why does this say that $x\mapsto\psi_6(x,\cdot)$ carries $-\eta$ to the push-forward by the endomorphism whose pull-back is η?

What just happened. Unimodularity of X_{CM} at p (Lemma 12.6) and of X_6 at p (determinant d^6) is what makes Schoen's isogeny of degree prime to p. Proposition 11.5, proved from Hypothesis (M), gives an integral cycle on the sixfold, and Lemma 11.8 says its Weil coefficient is a unit at p. Pull-back along an isogeny of degree prime to p, cutting with a divisor whose Weil coefficient is a unit, and push-forward multiply this coefficient by units at p, and the K-type bookkeeping shows that nothing else lands in the Weil part of X_{CM}.

13.3. The projector

The cycle Z is a priori defined over $\mathbb{C}$. Since X_{CM} is defined over $\overline{\mathbb{Q}}$, Z is algebraically equivalent to a cycle defined over $\overline{\mathbb{Q}}$ (see e.g. [Del82]): spread Z out over a smooth variety over $\overline{\mathbb{Q}}$ and specialize to a $\overline{\mathbb{Q}}$-point. Algebraically equivalent cycles have the same class, and we replace Z by this cycle from now on.

By Lemma 12.6, $\mathrm{End}(X_{\mathrm{CM}})\cap K$ is an order of conductor prime to p, so its reduction modulo p is all of $O_K/p\cong\mathbb{F}_{p^2}$. Choose $b\in O_K\cap\mathrm{End}(X_{\mathrm{CM}})$ whose reduction $\zeta=b \bmod p$ generates the cyclic group $\mathbb{F}_{p^2}^\times$ of order p^2-1. On the component of K-type $(i,4-i)$ of $H^4(X_{\mathrm{CM}})$, $[b]^*$ acts by

$$\mu_i=b^i\bar b^{4-i},\qquad i=0,\dots,4.$$

Since p is inert in K, conjugation induces the Frobenius $x\mapsto x^p$ on O_K/p, so $\bar b\equiv\zeta^p$ and $\mu_i\equiv\zeta^{i+p(4-i)} \bmod p$. For $0\le i<j\le 4$, $\mu_i\equiv\mu_j$ would mean $\zeta^{(j-i)(1-p)}=1$, that is, $(p^2-1)\mid(j-i)(p-1)$, that is, $(p+1)\mid(j-i)$, which is impossible for $p\ge 5$ because $0<j-i\le 4<p+1$. So the five values μ_i are distinct modulo p. Let Q_P be the Lagrange interpolation polynomial of degree at most 4 with

$$Q_P(\mu_0)=Q_P(\mu_4)=1,\qquad Q_P(\mu_1)=Q_P(\mu_2)=Q_P(\mu_3)=0,\qquad P=Q_P([b]^*).\tag{13.1}$$

Its coefficients are sums of products of the μ_i divided by products of differences $\mu_i-\mu_j$, which are units at p; so they lie in $O_{K,(p)}$. Complex conjugation exchanges μ_i and μ_{4-i} and so permutes the interpolation conditions among themselves, so the conjugate of Q_P satisfies the same conditions and equals Q_P. Hence the coefficients lie in $O_{K,(p)}\cap\mathbb{Q}=\mathbb{Z}_{(p)}$.

On cycles, P is a $\mathbb{Z}_{(p)}$-combination of the pull-backs $[b^j]^*$, $0\le j\le 4$. In Betti cohomology it is the projector onto the Weil part, the sum of the K-types $(4,0)$ and $(0,4)$, because $[b]^*$ acts on the K-type $(i,4-i)$ by μ_i. In crystalline cohomology of X_{t_0} it is the same: by Proposition 12.2(d), $O_K\otimes\mathbb{Z}_p$ acts diagonally on the cube basis with ι-eigenset T_+, say, so $[b]^*$ acts on e_J, $|J|=4$, by $\iota(\mu_i)$ with $i=|J\cap\mathsf{T}_+|$, and P is the coordinate projection onto $We_{\mathsf{T}_+}\oplus We_{\mathsf{T}_-}$, the Weil part of Lemma 8.4(iii).

EXAMPLE 13.3 (the projector at $p=5$). Let $K=\mathbb{Q}(\sqrt{-2})$, $p=5$ and $b=1+\sqrt{-2}$, with $\mathrm{Nm}(b)=3$. The powers of b modulo 5 first return to 1 at the 24th power, so b generates $\mathbb{F}_{25}^{\times}$. The five eigenvalues are

$$\mu_0=\bar b^4=-7+4\sqrt{-2},\qquad \mu_1=3\bar b^2=-3-6\sqrt{-2},\qquad \mu_2=9,$$
$$\mu_3=3b^2=-3+6\sqrt{-2},\qquad \mu_4=b^4=-7-4\sqrt{-2},$$

and modulo 5 they are $3+4\sqrt{-2}$, $2+4\sqrt{-2}$, 4, $2+\sqrt{-2}$, $3+\sqrt{-2}$, pairwise distinct. The interpolation polynomial is

$$Q_P(x)=\tfrac{241}{256}+\tfrac{95}{1728}x+\tfrac{17}{31104}x^2-\tfrac{43}{46656}x^3-\tfrac{23}{186624}x^4,$$

with denominators 2^8, $2^6 3^3$, $2^7 3^5$, $2^6 3^6$, $2^8 3^6$, all prime to 5, and rational coefficients, as the conjugation argument predicts. Modulo 5 it is $Q_P(x)\equiv 1+3x^2+2x^3+3x^4$; for instance $Q_P(\mu_2)\equiv 1+3\cdot 16+2\cdot 64+3\cdot 256=945\equiv 0$.

EXERCISE 13.2. Show that $(p+1)\nmid(j-i)$ for $0<j-i\le 4$ when $p\ge 5$, and find the pairs $i<j$ with $\mu_i\equiv\mu_j \bmod 3$ for an inert $p=3$. Show also that $b^4\not\equiv\bar b^4 \bmod p$ for $p\ge 5$, while for $p=3$ always $b^4\equiv\bar b^4$.

EXERCISE 13.3. Let $Q(x)=\sum_l \lambda_l x^l$ be the unique polynomial of degree at most 4 with prescribed values at five distinct points $\mu_0,\dots,\mu_4$ of K. Show that if the set of points is stable under complex conjugation, with $\bar\mu_i=\mu_{4-i}$, and the prescribed values at μ_i and μ_{4-i} are equal and rational, then all λ_l are rational.

13.4. The Gram determinant

Let O be the localization at a prime above p of the ring of integers of a number field over which X_{CM}, Z and b are defined, with an abelian scheme $\mathcal{X}$ over O whose generic fiber is X_{CM} and whose special fiber is X_{t_0} (Proposition 12.2(c)). By the Néron property (Fact 2.9) b extends to an endomorphism of $\mathcal{X}$. We replace O by its completion, as Fact 2.9(b) requires; this changes neither the special fiber nor the intersection numbers. Put

$$Z_1=PZ,\qquad Z_2=[b]^*Z_1,$$

cycles on X_{CM} with coefficients in $\mathbb{Z}_{(p)}$. Their Betti classes are

$$[Z_1]=\nu_Z\omega+\bar\nu_Z\bar\omega,\qquad [Z_2]=b^4\nu_Z\omega+\overline{b^4\nu_Z}\bar\omega,$$

because $[b]^*$ acts on ω by b^4 and on $\bar\omega$ by $\bar b^4$. Write $\nu_{Z_1}=\nu_Z$ and $\nu_{Z_2}=b^4\nu_Z$, and $\langle\omega,\bar\omega\rangle=\int_{X_{\mathrm{CM}}}\omega\wedge\bar\omega$. Since $\omega\wedge\omega$ lies in $\bigwedge^8 H^1_\iota=0$, H^1_ι having rank 4,

$$\deg(Z_i\cdot Z_j)=\int(\nu_{Z_i}\omega+\bar\nu_{Z_i}\bar\omega)(\nu_{Z_j}\omega+\bar\nu_{Z_j}\bar\omega)=\langle\omega,\bar\omega\rangle\,\mathrm{Tr}_{K/\mathbb{Q}}\left(\nu_{Z_i}\bar\nu_{Z_j}\right).$$

The number $\langle\omega,\bar\omega\rangle$ is rational, being equal to its conjugate, and it is a unit of $O_{K,(p)}$, because $H^1(X_{\mathrm{CM}},\mathbb{Z}_{(p)})\otimes O_K=H^1_\iota\oplus H^1_{\bar\iota}$ and so $\omega\wedge\bar\omega$ generates $H^8(X_{\mathrm{CM}},O_{K,(p)})$. Hence $\langle\omega,\bar\omega\rangle\in\mathbb{Z}_{(p)}^{\times}$. The Gram matrix is

$$\begin{pmatrix}2\langle\omega,\bar\omega\rangle\,\mathrm{Nm}(\nu_Z) & \langle\omega,\bar\omega\rangle\,\mathrm{Nm}(\nu_Z)\,\mathrm{Tr}(\bar b^4)\\ \langle\omega,\bar\omega\rangle\,\mathrm{Nm}(\nu_Z)\,\mathrm{Tr}(b^4) & 2\langle\omega,\bar\omega\rangle\,\mathrm{Nm}(\nu_Z)\,\mathrm{Nm}(b)^4\end{pmatrix},$$

and its determinant is $\langle\omega,\bar\omega\rangle^2\,\mathrm{Nm}(\nu_Z)^2(4b^4\bar b^4-(b^4+\bar b^4)^2)$, that is,

$$\det\left(\deg(Z_i\cdot Z_j)\right)=-\langle\omega,\bar\omega\rangle^2\,\mathrm{Nm}(\nu_Z)^2(b^4-\bar b^4)^2. \tag{13.2}$$

It is a unit at p: $\langle\omega,\bar\omega\rangle$ and ν_Z are units, and $b^4-\bar b^4\equiv\zeta^4-\zeta^{4p}\not\equiv 0$, since $\zeta^{4(p-1)}=1$ would need $(p+1)\mid 4$.

For $p=5$, $K=\mathbb{Q}(\sqrt{-2})$ and $b=1+\sqrt{-2}$ (Example 13.3), $\mathrm{Tr}(b^4)=-14$ and $\mathrm{Nm}(b)^4=81$, so the Gram matrix is $\langle\omega,\bar\omega\rangle\,\mathrm{Nm}(\nu_Z)\left(\begin{smallmatrix}2&-14\\-14&162\end{smallmatrix}\right)$, with determinant $\langle\omega,\bar\omega\rangle^2\,\mathrm{Nm}(\nu_Z)^2(324-196)=128\langle\omega,\bar\omega\rangle^2\,\mathrm{Nm}(\nu_Z)^2$, in agreement with Example 13.1.

EXERCISE 13.4. Derive (13.2) from the entries $\langle\omega,\bar\omega\rangle\,\mathrm{Tr}(\nu_{Z_i}\bar\nu_{Z_j})$: show that the determinant of $\big(\mathrm{Tr}(x_i\bar x_j)\big)_{i,j=1,2}$ for $x_1,x_2\in K$ is $-(x_1\bar x_2-\bar x_1x_2)^2$, and specialize to $x_1=\nu_Z$, $x_2=b^4\nu_Z$.

13.5. The specialized classes span the Weil lattice

PROPOSITION 13.4 (the Gram proposition). *Assume Hypothesis (M). In the situation of Proposition 12.2,* $\mathcal{L}(X_{t_0})\subseteq\mathrm{Alg}^2(X_{t_0})$.

PROOF. The specializations $\mathrm{sp}\,Z_i$ to X_{t_0} are cycles with coefficients in $\mathbb{Z}_{(p)}$. By Fact 4.6, $\mathrm{cl}(\mathrm{sp}\,Z_i)\in T^4(X_{t_0})$. Specialization commutes with pull-backs by endomorphisms of $\mathcal{X}$ (Fact 2.9), so $\mathrm{cl}(\mathrm{sp}\,Z_1)=P\,\mathrm{cl}(\mathrm{sp}\,Z)$, where P now acts on crystalline cohomology. The endomorphism P is a $\mathbb{Z}_{(p)}$-combination of pull-backs and preserves T^4, and by Section 13.3 it projects onto $We_{\mathsf{T}_+}\oplus We_{\mathsf{T}_-}$; so $\mathrm{cl}(\mathrm{sp}\,Z_1)\in T^4\cap(We_{\mathsf{T}_+}\oplus We_{\mathsf{T}_-})=\mathcal{L}$ (Definition 8.6). The same holds for $\mathrm{cl}(\mathrm{sp}\,Z_2)=[b]^*\,\mathrm{cl}(\mathrm{sp}\,Z_1)$. By Facts 4.6 and 2.9,

$$\int\mathrm{cl}(\mathrm{sp}\,Z_i)\,\mathrm{cl}(\mathrm{sp}\,Z_j)=\deg(\mathrm{sp}\,Z_i\cdot\mathrm{sp}\,Z_j)=\deg(Z_i\cdot Z_j).$$

The cup product pairs T^4 with itself into $T^8=\mathbb{Z}_p[\mathrm{pt}]$, so $\mathcal{L}$ carries a $\mathbb{Z}_p$-valued symmetric bilinear form, and the sublattice $\mathcal{L}'$ spanned by $\mathrm{cl}(\mathrm{sp}\,Z_1),\mathrm{cl}(\mathrm{sp}\,Z_2)$ has Gram determinant (13.2), a unit. In particular $\mathcal{L}'$ has rank 2, and by Lemma 4.13, $\mathrm{disc}\,\mathcal{L}'=[\mathcal{L}:\mathcal{L}']^2\,\mathrm{disc}\,\mathcal{L}$ with $\mathrm{disc}\,\mathcal{L}\in\mathbb{Z}_p$. So $[\mathcal{L}:\mathcal{L}']=1$, that is, $\mathcal{L}'=\mathcal{L}$, and $\mathcal{L}$ is spanned by classes of algebraic cycles with coefficients in $\mathbb{Z}_{(p)}$, hence lies in $\mathrm{Alg}^2(X_{t_0})$. □

EXERCISE 13.5. Let L be a free $\mathbb{Z}_p$-module of rank 2 with a symmetric bilinear form with values in $\mathbb{Z}_p$, and $L'\subseteq L$ a sublattice of rank 2 whose Gram determinant is a unit. Show that $L'=L$, and that L' need not equal L if the Gram determinant of L' is only nonzero. Give an example with $[L:L']=p$.

EXERCISE 13.6. For $p=5$, $K=\mathbb{Q}(\sqrt{-2})$ and $b=1+\sqrt{-2}$, verify the values of $\mu_0,\dots,\mu_4$ and their reductions in Example 13.3, and check that $Q_P(\mu_4)\equiv1$ and $Q_P(\mu_3)\equiv0$ modulo 5, computing in $\mathbb{F}_{25}=\mathbb{F}_5[\sqrt{-2}]$.

Why no comparison theorem is needed. A p-adic comparison theorem would identify the crystalline class of $\mathrm{sp}\,Z$ with the image of its Betti class, integrally, and read off its Weil coefficient directly. The argument above avoids this. It needs only three properties of the specialized classes: they are integral and Tate (Fact 4.6), they lie in the Weil part, because P is the same polynomial in $[b]^*$ in both theories and $[b]^*$ has the same eigenvalue pattern on both sides (Proposition 12.2(d)), and their intersection numbers are those computed in characteristic 0 (Fact 2.9). Given these, the intersection numbers fix the p-adic normalization.

What just happened. The projector $P=Q_P([b]^*)$ is a polynomial with $\mathbb{Z}_{(p)}$-coefficients in one endomorphism, so it acts on cycles and is the projector onto the Weil part both in Betti cohomology of X_{CM} and in crystalline cohomology of X_{t_0}. The two cycles PZ and $[b]^*PZ$ have a Gram determinant $-\langle\omega,\bar\omega\rangle^2\,\mathrm{Nm}(\nu_Z)^2(b^4-\bar b^4)^2$ that is a unit at p when $p\geq5$. After specialization their classes lie in $\mathcal{L}$, a lattice of rank 2, and span a sublattice of unit discriminant, which is $\mathcal{L}$ itself.

Where this is used. Proposition 13.4 is the input of the proof of Theorem A(b) in Chapter 14: together with the endomorphism proposition Proposition 9.4 it gives, under Hypothesis (M), $\mathrm{Alg}^2(X_{t_0})=T^4(X_{t_0})$ at the point t_0, and the transport lemma carries this to every supersingular point and to every fourfold with p-divisible group $\mathscr{G}_p$.

Part V

The theorems and beyond

CHAPTER 14

The theorems, and what they rest on

Where we are. This chapter assembles the proofs of Theorem A(b), Theorem B and Theorem C; the proof of Theorem A(a) is in Section 9.4. The one ingredient not met in earlier chapters is the transport lemma (Lemma 14.2), which carries the result from one supersingular point to every abelian fourfold with the same p-divisible group. The chapter then says what the theorems imply for the exceptional Hodge classes of Mumford's fourfolds (Remark 14.3), and lists everything the proof rests on (Section 14.7). It needs all earlier chapters.

14.1. The whole proof in two pages

Fix $p \geq 5$. By Lemma 6.10 there are a Mumford family and data satisfying (6.2) at p. At every supersingular point t of its integral model, the Dieudonné module is the model $\mathbb{M}$ (Proposition 7.4), so all of them have the same p-divisible group $\mathscr{G}_p$. In $\mathbb{M}$, Frobenius maps the cube basis to multiples of basis vectors, every lattice the proof needs is monomial, and its exponents are min-plus expressions independent of p (Chapter 5). Their exact evaluation shows that $T^4/S \cong (\mathbb{Z}/p)^4$, carried by four sets of the cube (Proposition 8.2), and that S together with the pull-backs by endomorphisms of any primitive element of the Weil lattice $\mathcal{L}$ is all of T^4 (Proposition 9.4 and Section 9.4). So one algebraic class in $\mathcal{L} \setminus p\mathcal{L}$ is all that is missing, which gives Theorem A(a) and the reduction of Theorem A(b) to the inclusion $\mathcal{L} \subseteq \mathrm{Alg}^2$.

That inclusion is proved at one point. The fourfold X_{CM} with complex multiplication by $K \times kK$, K inert at p, reduces to a supersingular point t_0 and has a unimodular Hermitian lattice at p (Proposition 12.2 and Lemma 12.6). Under Hypothesis (M), the integral cycles on Markman's sixfolds (Proposition 11.5) and Schoen's step give a cycle Z on X_{CM} whose Weil coefficient is a unit at p (Proposition 13.2), and a projector and a unit Gram determinant show that the specialized classes span $\mathcal{L}(X_{t_0})$ (Proposition 13.4). So, under Hypothesis (M), $\mathrm{Alg}^2(X_{t_0}) = T^4(X_{t_0})$.

What remains is the observation that isogenies of degree prime to p see only p-divisible groups, as far as integral crystalline classes are concerned. Two supersingular abelian varieties with isomorphic p-divisible groups are related by an isogeny of degree prime to p, and its pull-back identifies T^{2i}, S and Alg^i (Lemma 14.2). Under Hypothesis (M), this carries $\mathrm{Alg}^2 = T^4$ from X_{t_0} to every supersingular point of the family, which is Theorem A(b), and to every abelian fourfold over $\bar{\mathbb{F}}_p$ with p-divisible group $\mathscr{G}_p$, which is Theorem C(b). The Künneth statements on $X \times X$ follow in the same way from the endomorphism proposition on $X \times X$, by extracting bihomogeneous components with a Vandermonde matrix. At primes that are unramified and not inert in k, with B split at every place of k above p and the lattice at p a tensor induction as in (h4), the same method shows that the supersingular points have $T^4 = S$ (Theorem B), without any cycle beyond divisors.

Example 14.1 (the Vandermonde determinant). The Vandermonde matrix $(j^i)_{0 \leq i,j \leq 4}$ of the points $0, 1, 2, 3, 4$ has determinant $\prod_{0 \leq j < j' \leq 4}(j' - j) = (1 \cdot 2 \cdot 3 \cdot 4)(1 \cdot 2 \cdot 3)(1 \cdot 2) \cdot 1 = 24 \cdot 6 \cdot 2 = 288 = 2^5 \cdot 3^2$. So it is invertible modulo every prime $p \geq 5$ and singular modulo 2 and 3. This is one of several places where the proof uses $p \geq 5$ rather than p odd. The others are the polarization step of Chapter 5, where 4! must be a unit; the projector and the Gram

determinant of Chapter 13, where $(p+1)\nmid(j-i)$ for $0<j-i\le 4$ and $b^4\not\equiv\bar{b}^4$ modulo p are needed (Exercise 13.2); and the proof of Lemma 6.10, where 3 must be invertible modulo p.

14.2. The transport lemma

LEMMA 14.2 (transport). *Let X, X' be supersingular abelian varieties over $\bar{\mathbb{F}}_p$ with $X[p^\infty]\cong X'[p^\infty]$. Then there is an isogeny $f\colon X'\to X$ of degree prime to p, and f^* maps $T^{2i}(X)$, $\mathrm{Alg}^i(X)$ and $S(X)$ isomorphically onto $T^{2i}(X')$, $\mathrm{Alg}^i(X')$ and $S(X')$.*

PROOF. *Existence.* By Fact 4.10, $\mathrm{Hom}(X',X)\otimes\mathbb{Z}_p=\mathrm{Hom}(X'[p^\infty],X[p^\infty])$. Let γ be an isomorphism of p-divisible groups. Since $\mathrm{Hom}(X',X)$ is dense in $\mathrm{Hom}(X',X)\otimes\mathbb{Z}_p$, there is $f\in\mathrm{Hom}(X',X)$ with $f=\gamma+p\gamma_1$ for some $\gamma_1\in\mathrm{Hom}(X'[p^\infty],X[p^\infty])$. Then $f[p^\infty]=\gamma(1+p\gamma^{-1}\gamma_1)$ is an isomorphism, because $1+p\gamma^{-1}\gamma_1$ has the inverse $\sum_l(-p\gamma^{-1}\gamma_1)^l$.

f is an isogeny of degree prime to p. The varieties X and X' have the same dimension, since their p-divisible groups have the same height $2\dim$. The reduced identity component X'' of $\ker f$ is an abelian subvariety of X', and $f[p^\infty]$ vanishes on $X''[p^\infty]\subseteq X'[p^\infty]$, which has height $2\dim X''$. As $f[p^\infty]$ is injective, $X''=0$. So $\ker f$ is finite, and its p-primary part, which lies in $X'[p^\infty]$ and is killed by $f[p^\infty]$, is trivial. Hence f is an isogeny and $\deg f=|\ker f|$ is prime to p.

The lattices. By Dieudonné theory $f^*\colon M(X)\to M(X')$ is an isomorphism compatible with F, so $f^*=\bigwedge^{2i}f^*$ maps $T^{2i}(X)$ isomorphically onto $T^{2i}(X')$. In particular it maps $T^2(X)$ onto $T^2(X')$, and since it is a ring homomorphism, $S(X)$ onto $S(X')$. Pull-back of cycles gives $f^*\,\mathrm{Alg}^i(X)\subseteq\mathrm{Alg}^i(X')$. On cohomology $f_*f^*=f^*f_*=\deg f$ (Exercise 14.2), and $\deg f\in\mathbb{Z}_p^\times$. So every $y\in\mathrm{Alg}^i(X')$ is $f^*((\deg f)^{-1}f_*y)$ with $f_*y\in\mathrm{Alg}^i(X)$, and $f^*\,\mathrm{Alg}^i(X)=\mathrm{Alg}^i(X')$. □

EXERCISE 14.1. Let $f\colon X'\to X$ be a homomorphism of abelian varieties of the same dimension such that $f[p^\infty]$ is an isomorphism. Explain why $\ker f$ cannot contain an elliptic curve, and why its order is prime to p. Give an example of an endomorphism f of E_0 with $f[p^\infty]$ an isomorphism and $\deg f=7$ for some p.

EXERCISE 14.2. Let $f\colon X'\to X$ be an isogeny of degree prime to p, so that $\ker f$ is étale. Show that $f_*f^*x=(\deg f)x$ for x in the cohomology of X, using the projection formula, and that $f^*f_*y=(\deg f)y$ for y in the cohomology of X', using that f^*f_*y is the sum of the translates of y by the points of $\ker f$ and that translations act trivially on cohomology. Why does the second identity fail on Chow groups?

14.3. Proof of Theorem A

Part (a) is proved in Section 9.4. For part (b), assume (6.2) and Hypothesis (M), and let t_0 be the point of Proposition 12.2.

$\mathrm{Alg}^2=T^4$ at t_0. By Proposition 13.4, $\mathcal{L}(X_{t_0})\subseteq\mathrm{Alg}^2(X_{t_0})$. By Fact 4.10, $T^2=\mathrm{NS}\otimes\mathbb{Z}_p$, so $S\subseteq\mathrm{Alg}^2$. Pull-backs of cycles by endomorphisms are cycles, so Alg^2 is stable under $\mathrm{End}(X_{t_0})^*$, and since the $\mathbb{Z}_p$-span of the α^*x over $\alpha\in\mathrm{End}(X_{t_0})$ equals the span over $\mathrm{End}(X_{t_0})\otimes\mathbb{Z}_p=\mathrm{End}(M,F)$ (Chapter 9), it contains $S+\mathrm{End}^*\mathcal{L}$. By Proposition 9.4, $S+\mathrm{End}^*\mathcal{L}=T^4$. So $\mathrm{Alg}^2(X_{t_0})=T^4(X_{t_0})$.

The Künneth component at t_0. Write $X=X_{t_0}$ and let $\alpha_1,\alpha_2\in\mathrm{End}(X)$, with $(\alpha_1,\alpha_2)\colon X\times X\to X$, $(y_1,y_2)\mapsto\alpha_1y_1+\alpha_2y_2$. For $x\in T^4(X)$ the class $(\alpha_1,\alpha_2)^*x$ has Künneth components $z_i\in\bigwedge^iM\otimes\bigwedge^{4-i}M$, $i=0,\dots,4$. Replacing α_1 by $j\alpha_1$ multiplies z_i by j^i, so

$$(j\alpha_1,\alpha_2)^*x=\sum_{i=0}^{4}j^iz_i,\qquad j=0,1,2,3,4.$$

The Vandermonde matrix (j^i) is invertible over $\mathbb{Z}_{(p)}$ (Example 14.1), so each z_i, in particular z_2, is a $\mathbb{Z}_{(p)}$-combination of the five classes $(j\alpha_1,\alpha_2)^*x$. If x is algebraic, so are these, and hence so is z_2. The Künneth $(2,2)$-components of products of divisor classes on $X\times X$ are

products of Künneth components of divisor classes, and those are again divisor classes by Fact 4.10, since Frobenius respects the Künneth decomposition. By Proposition 9.4(iv), T_{22} (Definition 9.3) is spanned by the $(2,2)$-components of $S(X\times X)$ and of the classes $(\alpha_1,\alpha_2)^*x$, $x\in\mathcal{L}$. All of these are algebraic, so the Künneth component in $H^2_{\mathrm{cris}}(X/W)\otimes H^2_{\mathrm{cris}}(X/W)$ of every class in $T^4(X\times X)$ lies in $\mathrm{Alg}^2(X\times X)$.

Every supersingular point. For a supersingular $t\in\mathscr{S}(\bar{\mathbb{F}}_p)$, Proposition 7.4 gives $\mathcal{A}_t[p^\infty]\cong X_{t_0}[p^\infty]$. Lemma 14.2, applied to $\mathcal{A}_t$ and to $\mathcal{A}_t\times\mathcal{A}_t$, transports both statements, because the pull-back by an isogeny $f\times f$ respects Künneth components. This proves Theorem A(b). □

Exercise 14.3. Compute the determinant of the Vandermonde matrix of $0,1,2,3,4$ and reduce it modulo 5 and 7. For $p=5$, write z_2 explicitly as an $\mathbb{F}_5$-combination of $\sum_i j^i z_i$, $j=0,\dots,4$, by inverting the matrix modulo 5, or at least find its middle row.

14.4. Proof of Theorem B

Let $p\geq 5$ be unramified and not inert in k, with B split at every place of k above p and (h4) read with $k_p=k\otimes\mathbb{Q}_p$, and let $t\in\mathscr{S}(\bar{\mathbb{F}}_p)$ be supersingular. Proposition 6.7 holds with the same proof for p unramified in k: now $k\otimes\mathbb{Q}_p$ is a product of unramified extensions of $\mathbb{Q}_p$, the slot lattices $\Lambda_i=\Lambda_0\otimes_{\tau_i}W$ are indexed by the three embeddings $\tau_i\colon O_k\otimes\mathbb{Z}_p\to W$, and σ permutes the τ_i within each place of k above p. So the argument of Section 7.2 applies with this permutation of the slots in place of the cyclic one, and again exactly one slot component of Frobenius is not a scalar times an element of $\mathrm{GL}_2(W)$.

p splits completely. Then σ fixes each slot. The two slots with invertible slot components form a crystal of rank 4 on which Frobenius is a σ-semilinear bijection, which has a basis of fixed vectors by Lang's lemma. The third is a crystal of rank 2 with elementary divisors $1,p$ and, t being supersingular, slopes $\frac{1}{2}$, so Lemma 7.2 with $r=1$ applies. Hence $(M,F)\cong(W^2,A\sigma)\otimes(W^4,\sigma)$, the Dieudonné module of E_0^4, with words $01+01+01+01$.

$p=\mathfrak{p}_1\mathfrak{p}_2$ with residue degrees 1 and 2. If the non-scalar slot is the one of $\mathfrak{p}_1$, the same argument gives $M(E_0^4)$. If it is one of the two slots of $\mathfrak{p}_2$, the slot of $\mathfrak{p}_1$ is a unit-root crystal of rank 2, isomorphic to (W^2,σ) by Lang's lemma, and the other two form a crystal $(W^2\otimes W^2,(A\otimes 1)\varsigma')$ with $\varsigma'(x\otimes y)=\sigma y\otimes\sigma x$, by Lemma 7.2 with $r=2$ applied to F^2 on one slot. On the basis $e_i\otimes e_j$ this crystal acts by $e_i\otimes e_j\mapsto p^j e_{1-j}\otimes e_i$, which is the cycle $e_{00}\mapsto e_{10}\mapsto e_{11}\mapsto pe_{01}\mapsto p^2e_{00}$ with word 0011. So (M,F) has words $0011+0011$.

Exercise 14.4. For the crystal $(W^2\otimes W^2,(A\otimes 1)\varsigma')$ with $\varsigma'(x\otimes y)=\sigma y\otimes\sigma x$, compute Frobenius on the four vectors $e_i\otimes e_j$, verify the cycle $e_{00}\mapsto e_{10}\mapsto e_{11}\mapsto pe_{01}\mapsto p^2e_{00}$, and read off its word. Show that $F^4=p^2\sigma^4$ on this crystal, so that it is supersingular.

In each case (M,F) is monomial, and the exact computation of the min-plus exponents, as in Chapter 5, gives $[T^4:S]=1$ and that the Künneth $(2,2)$-component of $T^4(X\times X)$ is spanned by the corresponding components of $S(X\times X)$; both models give p^0 for both indices. By Fact 4.10, $S\subseteq\mathrm{Alg}^2$, and no algebraicity input beyond it is used. This proves Theorem B. □

14.5. Proof of Theorem C

Let X be an abelian fourfold over $\bar{\mathbb{F}}_p$ with $X[p^\infty]\cong\mathscr{G}_p$. By Dieudonné theory, $M(X)\cong\mathbb{M}$ compatibly with F. The lattices $T^4(X)$ and $S(X)$ are defined from $(M(X),F)$ alone, and $\mathrm{End}(X)\otimes\mathbb{Z}_p=\mathrm{End}(M(X),F)$ by Fact 4.10. The proof of Theorem A(a) in Section 9.4 uses nothing else, so it applies to X; this is Theorem C(a).

For (b), assume Hypothesis (M). Lemma 6.10 gives data satisfying (6.2) at p, Proposition 12.2 a supersingular point t_0, and Section 14.3 gives $\mathrm{Alg}^2(X_{t_0})=T^4(X_{t_0})$ and the Künneth statement on $X_{t_0}\times X_{t_0}$. By Proposition 7.4, $X_{t_0}[p^\infty]\cong\mathscr{G}_p\cong X[p^\infty]$. Lemma 14.2 uses no structure of Mumford's families, so it gives an isogeny $f\colon X\to X_{t_0}$ of degree prime to p, and

$$\mathrm{Alg}^2(X)=f^*\,\mathrm{Alg}^2(X_{t_0})=f^*T^4(X_{t_0})=T^4(X).$$

The same argument with $f \times f$ gives the Künneth statement. □

Exercise 14.5. Which parts of Theorems A to C hold without Hypothesis (M)? Show moreover, using only Theorem A(a), that for a supersingular point t at an inert prime either $\mathrm{Alg}^2(\mathcal{A}_t) = T^4(\mathcal{A}_t)$ or $\mathrm{Alg}^2(\mathcal{A}_t) \subseteq N = S + \mathcal{N}$.

14.6. The exceptional Hodge classes

Remark 14.3 (what the theorems say about $X_{\mathrm{gen}} \times X_{\mathrm{gen}}$). For a very general complex fiber X_{gen} of Mumford's family, $H^4(X_{\mathrm{gen}} \times X_{\mathrm{gen}}, \mathbb{Q})$ contains Hodge classes that are not in the span of products of divisor classes [MZ99]; modulo that span they form a space of dimension 2 in the Künneth $(2,2)$-component (Section 6.3). Let δ be such a class. If an integer multiple $n\delta$ were algebraic, the cycles would specialize, and for primes $p \nmid n$ outside a finite set the integral crystalline class δ_t at a point t of characteristic p would be algebraic. Conversely, non-algebraic classes δ_t at infinitely many primes would show that δ is not algebraic. Making these two statements precise needs, besides Fact 2.9, a comparison between the Betti cohomology of the complex fibers and the crystalline cohomology of the special fibers that carries δ to an integral class δ_t, which the companion does not discuss. Theorem A(b), under Hypothesis (M), and Theorem B, unconditionally, show that no such δ_t exists at supersingular points at primes satisfying their hypotheses: the whole Künneth $(2,2)$-component of $T^4(X_t \times X_t)$ is algebraic there, and at non-inert primes it is spanned by products of divisor classes. This removes one possible route to proving that δ is not algebraic. It says nothing about the algebraicity of δ in characteristic 0.

14.7. What the proof rests on

Hypothesis (M). Theorem A(b) and Theorem C(b) assume Hypothesis (M): that three statements made in the proof of a theorem of a preprint of Markman hold, together with the other statements of the preprint cited in Chapter 11. From them Proposition 11.5 derives that an explicit integral class is the class of an algebraic cycle with integer coefficients on every member of a family of abelian sixfolds of Weil type, and Lemma 11.8 computes the Weil component of that class. Their exact form, their relation to the preprint and their status are in Section 11.7. The proposition and the lemma are used once, in Proposition 13.2.

Cited facts. The following inputs are cited with references and not proved in this companion, except that Lemma 11.4 on Chern classes in families is proved there from the results it cites. The table gives, for each, where it is stated and the source, with the place in the source where the statement used can be found. Where the source is not the original, the citation in the text says "see e.g.".

input	stated in	source
Dieudonné theory, $M(X) = H^1_{\mathrm{cris}}(X/W)$, $VM/pM \cong H^0(\Omega^1)$	Fact 3.10	[Oda69; Lie16; Hai05], at the places given after the Fact
Lang's theorem modulo p; Dieudonné–Manin; positive slopes force nilpotence	Lemma 3.5, Fact 3.11	[Oor01], [Lie16, Theorem 3.4, Proposition 3.7], [Jon98, Section 4.5]
supersingular varieties are isogenous to E_0^g	Fact 2.6	[Oor74, Theorem 4.2], [Lie16, Section 3.4.1]
homomorphisms and Dieudonné modules; $\mathrm{NS} \otimes \mathbb{Z}_p = T^2$	Fact 4.10	[Jon98, proof of Theorem 2.6], [Oor74, Theorem 4.2]
crystalline cycle class and trace	Fact 4.6	[GM87; Pet03; Lie16], at the places given after the Fact
specialization of cycles and Néron property	Fact 2.9	[GM87, Appendix B, B.3], [The, Tag 0H4H], [Mil08, Chapter I, Remark 17.2]

input	stated in	source
Kisin's integral model	Fact 6.4	[Kis10; KP18; Mad19; Mil08; Mil05; The], at the places given after the Fact
closed-immersion criterion; closure and flat base change	Proposition 6.7	[DG70, Exp. XVI, Corollaire 1.5(a)], [The, Tag 081I]
quaternion algebras with given ramification; $\mathrm{Cor}_{k/\mathbb{Q}} B \cong \mathrm{Mat}_8(\mathbb{Q})$	Lemma 6.10	[Voi21, Main Theorem 14.6.1], [Che25, Section 2.1.2]
Mumford's Hodge morphism	Section 6.2	[SZ16, Section 2]
embedding of K' into B; the division algebra Δ	Sections 12.3 and 12.6	[Voi21, Proposition 14.6.7, Corollary 13.3.14, Theorem 13.3.11]
Skolem–Noether	Fact 12.4	[Voi21, Main Theorem 7.7.1]
unimodular Hermitian lattices at an inert prime	Fact 10.7	[Yu12, Section 2], [Voi21, p. 13.2.5]
classification of Hermitian spaces over K	Section 10.4	[Sch98, Section 7]
Schoen's degeneration step	Proposition 10.9	follows the proof of [Sch98, Proposition 10]
Markman's construction and statements	Chapter 11	[Mar25], a preprint, at the places given there
arithmetic groups, quotients and families of abelian varieties; Hilbert schemes; Baire	Proposition 11.5	[Mil05, Propositions 3.1, 3.2, 3.5, Theorems 3.12, 14.8], [Ge26, Section 2.1], [Nit05, Section 1 and Theorem 5.1], [The, Tags 0B45, 0CQN]
Chern classes of complexes in families and algebraic cycles: results of Atiyah–Hirzebruch, Borel–Haefliger and Grothendieck, GAGA; Atiyah-class Chern character	Lemma 11.4, Proposition 11.5	[AH62], [BH61], [Gro58], [Gro03, Exposé XII], [BF03, Section 1], [The], at the places given in the proof of the Lemma and in the Proposition
Hilbert schemes and Hodge loci; curves through two points	Proposition 11.5	[Voi16, Section 4.2], [Mil08, Chapter I, Lemma 5.20], [The, Tag 0B8Y]
a cycle over $\mathbb{C}$ on a variety over $\overline{\mathbb{Q}}$	Section 13.3	[Del82]
Kraft's classification	Fact 15.2	[Oor01, Section 9]
$\chi(\mathcal{P})^2 = 1$; Rosati involution and NS	Section 15.4, Section 1.2	[Mil08, Chapter I, Theorems 11.1 and 8.9, Proposition 14.2]

The computations. The proofs of Theorems A to C use three exact computations, each evaluating min-plus exponents of monomial lattices in integer arithmetic: the exponents n_J and n_J^S of the model for all 2-sets, 4-sets and 6-sets of the cube (Proposition 8.2); the exponents of $\mathrm{End}(M, F)$ and the spans of pull-backs, including on $X \times X$ (Proposition 9.4); and the same for the two models of Section 14.4. All exponents are independent of $p \geq 5$. Two further exact computations are not used by these proofs: the lattices of Proposition 15.7 for the twenty cycle decompositions, and the Fourier–Mukai computation in $\mathbb{Q}(\sqrt{-d})$ that confirms Lemma 11.8 for six values of d.

The least secure steps. The step regarded as least secure is the dependence of Theorem A(b) and Theorem C(b) on the statements of Markman's preprint whose proofs were not verified in the note or in this companion (Section 11.7). Besides, the Weil coefficient $\frac{d+1}{2d}$ of Lemma 11.8 is derived for general d through Markman's spin formalism and confirmed by exact computation only for $d = 4, 6, 8, 10, 12, 28$.

What is left undecided. Theorems A and C concern one isomorphism class of p-divisible groups for each $p \geq 5$, and Theorem B the two classes $01 + 01 + 01 + 01$ and $0011 + 0011$.

Among the fourteen isomorphism classes of monomial supersingular Dieudonné modules of height 8 and dimension 4, four are left undecided, and nothing is proved here about non-monomial ones; Chapter 15 describes what is known and what would be needed.

CHAPTER 15

Other supersingular fourfolds

Where we are. The model $\mathbb{M}$ is one of several *monomial* supersingular Dieudonné modules of height 8 and dimension 4, those on which Frobenius maps a basis to multiples of basis vectors. This chapter compares them. The min-plus calculus applies to all of them, and together with one further unconditional source of algebraic classes, the Fourier transform of divisor products on the dual (Definition 15.4), it decides the integral crystalline Tate conjecture in codimension 2 for nine of their fourteen isomorphism classes; the class of $\mathbb{M}$ is decided under Hypothesis (M), and the methods explained here leave four undecided (Proposition 15.7). Nothing in this chapter is used in the proofs of Theorems A to C. It needs Chapters 3, 5 and 9.

15.1. Other monomial modules in two pages

A monomial supersingular Dieudonné module of height 8 and dimension 4 is named by a multiset of binary words with as many 0s as 1s and total length 8, each word up to rotation (Definition 3.17). There are twenty such multisets, the *cycle decompositions*. Some of them give isomorphic modules: a word that is a power of a shorter word, such as $0101 = (01)^2$, gives the same module as copies of the shorter word, by Lang's lemma. Once these coincidences are removed the twenty decompositions form fourteen isomorphism classes, distinguished by their reductions modulo p through Kraft's classification (Fact 15.2). Each of them is the Dieudonné module of some abelian fourfold, a quotient of E_0^4, and T^4 and S depend only on the module.

For each of them, the min-plus calculus of Chapter 5 computes $[T^4 : S]$ exactly, independently of p. Six classes have $T^4 = S$. For the others, the one idea of the chapter is a second source of algebraic classes that needs no hypothesis: the *Fourier source* $\widehat{S}(X)$, the image of the divisor products on the dual abelian variety $X^\vee$ under the cohomological Fourier transform given by the Poincaré bundle (Definition 15.4). Its classes are algebraic for $p \geq 5$ (Lemma 15.5), and in a monomial basis it is again a monomial lattice with min-plus exponents. Divisor products and the Fourier source together give T^4 for three more classes, so nine classes are settled unconditionally. The class of $\mathbb{M}$, with gap $(\mathbb{Z}/p)^4$, is settled by Theorem C under Hypothesis (M). Four classes, two dual pairs, are left undecided, with gaps p^2 and p^{26}.

Example 15.1 (a word and its square). The word 0101 gives the module with basis e_0, e_1, e_2, e_3 and $Fe_0 = e_1$, $Fe_1 = pe_2$, $Fe_2 = e_3$, $Fe_3 = pe_0$. The vector $x_1 = e_0 + e_2$ satisfies $Fx_1 = e_1 + e_3$ and $F^2x_1 = pe_2 + pe_0 = px_1$, so x_1, Fx_1 span a copy of the module 01 of a supersingular elliptic curve. A second copy comes from $x_2 = \lambda e_0 + \sigma^2(\lambda)e_2$ with $\lambda \in \mathbb{Z}_{p^4}$: then $F^2x_2 = p\sigma^2(\lambda)e_2 + p\sigma^4(\lambda)e_0 = px_2$, because $\sigma^4(\lambda) = \lambda$. If the reduction of λ lies in $\mathbb{F}_{p^4} \setminus \mathbb{F}_{p^2}$, the determinant $\sigma^2(\lambda) - \lambda$ of x_1, x_2 in the basis e_0, e_2 is a unit, and x_1, Fx_1, x_2, Fx_2 is a basis of the module. So $0101 \cong 01 + 01$.

15.2. Monomial modules and their cycle decompositions

Let $\mathbf{w}$ be a multiset of binary words $w^{(j)}$, each with as many 0s as 1s, of total length 8, each considered up to cyclic rotation. The module $M_{\mathbf{w}}$ has a basis $e_{j,i}$, one for each word $w^{(j)}$ of $\mathbf{w}$ and each $i \in \mathbb{Z}/|w^{(j)}|$, and

$$Fe_{j,i} = p^{w_i^{(j)}} e_{j,i+1},$$

where $w_i^{(j)} \in \{0,1\}$ is the i-th letter of $w^{(j)}$. We write $M_{\mathbf{w}}$ by the sum of its words; for example $01+01+01+01$ is the Dieudonné module of E_0^4, and $01+000111$ is $\mathbb{M}$ (Remark 7.6). Each cycle has as many 1s as 0s, so a power F^n of F is $p^{n/2}\sigma^n$ on the basis and $M_{\mathbf{w}}$ is supersingular. Each $M_{\mathbf{w}}$ is the Dieudonné module of an abelian fourfold that is a quotient of E_0^4 by a finite subgroup scheme. Indeed, for a word w of length $2m$, let (e'_i) be the basis of the module of the word $0101\cdots01$ of length $2m$, which is isomorphic to $M(E_0^m)$ by Section 15.3. Then $e_i \mapsto p^{c_i}e'_i$ with $c_{i+1} = c_i + \frac{1-(-1)^i}{2} - w_i$ is well defined, because w has m letters 1, and commutes with F and V (Exercise 15.2). So, after scaling, $M_{\mathbf{w}}$ is a sublattice of finite index in $M(E_0^4)$ stable under F and V, and by Dieudonné theory (Fact 3.10) it is $M(E_0^4/H)$ for the finite subgroup scheme $H \subset E_0^4[p^\infty]$ whose Dieudonné module is the quotient $M(E_0^4)/M_{\mathbf{w}}$ (see e.g. [Oda69, Corollary 3.16]). The min-plus calculus of Chapter 5 applies to it.

The multisets are counted as follows. The balanced binary necklaces, words up to rotation with as many 0s as 1s, number 1, 2, 4, 10 in lengths 2, 4, 6, 8. The partitions of 8 into even parts are 8, $6+2$, $4+4$, $4+2+2$ and $2+2+2+2$, which contribute 10, $4\cdot 1$, 3 (multisets of two necklaces out of two), $2\cdot 1$ and 1 multisets. So there are $10+4+3+2+1 = 20$ cycle decompositions.

Exercise 15.1. List the balanced binary necklaces of lengths 2, 4, 6 and 8, and among them the *primitive* ones, those that are not a power of a shorter word. (There are 1, 1, 3 and 8 primitive ones.)

15.3. Isomorphisms between decompositions

Let w be a word of length $|w|$ and consider the single word $w^n = w\cdots w$ of length $n|w|$, with basis e_i, $i \in \mathbb{Z}/n|w|$. Since w has $|w|/2$ letters 1, the map $\Phi = p^{-|w|/2}F^{|w|}$ sends $e_{j|w|}$ to $e_{(j+1)|w|}$ and is a $\sigma^{|w|}$-semilinear bijection of $M' = \bigoplus_{0\le j<n} We_{j|w|}$. By Lang's lemma (Lemma 3.5) M' has a basis $x_1,\dots,x_n$ of Φ-fixed vectors. Let l_i be the number of 1s among the first i letters of w. In the basis $p^{-l_i}F^i x_j$, $0 \le i < |w|$, $1 \le j \le n$, Frobenius has the matrix of the module $w + w + \cdots + w$ with n summands. So

$$w^n \cong w + \cdots + w \quad (n \text{ times}).$$

Applied to the twenty decompositions this gives three families of coincidences: $01+01+01+01$, $01+01+0101$, $0101+0101$, $01+010101$ and 01010101 are isomorphic; so are $01+01+0011$ and $0011+0101$; and so are $0011+0011$ and 00110011. Modules whose multisets of primitive words differ are not isomorphic, by the following classification.

Fact 15.2 (Kraft's classification). *Dieudonné modules over $\bar{\mathbb{F}}_p$ killed by p with $\ker F = \operatorname{im} V$, which are the reductions modulo p of Dieudonné modules of p-divisible groups, are classified by multisets of primitive cyclic words, in such a way that the reduction modulo p of a monomial module $M_{\mathbf{w}}$ corresponds to the multiset of primitive words underlying $\mathbf{w}$, a word w^n being counted as n copies of w.*

For Kraft's classification see e.g. [Oor01, Section 9]. With it, the twenty cycle decompositions form $20-4-1-1 = 14$ isomorphism classes.

Duality and a-numbers. The dual of $M_{\mathbf{w}}$, the Dieudonné module of the dual p-divisible group, is the monomial module whose words are the complementary words, with 0 and 1 exchanged. A module is *self-dual* if it is isomorphic to its dual. A polarization of degree prime to p induces an isomorphism $X[p^\infty] \cong X^\vee[p^\infty]$, and $M(X^\vee)$ is the dual module [Oda69, Definition 3.6 and Proposition 3.23], so self-duality is necessary for its existence (Exercise 15.5). The a-number of $M_{\mathbf{w}}$ is the number of cyclic transitions from 1 to 0 in its words (Definition 3.15).

Example 15.3 (a dual pair). The word 00100111 has cyclic $1\to 0$ transitions at positions $3\to 4$ and $8\to 1$, so $a = 2$. Its complement is 11011000, which rotated to start with its three 0s is 00011011. Since 00011011 is not a rotation of 00100111, the module 00100111 is not

self-dual, and 00100111, 00011011 is a dual pair. In the same way 00110101 and 00101011 are dual to each other, while 0011, 000111 and 00001111 are self-dual.

EXERCISE 15.2. Let w be a word of length $2m$ with letters w_i, and $M_{(01)^m}$ the module with basis e'_i and $Fe'_i = p^{[i \text{ odd}]}e'_{i+1}$, where $[i \text{ odd}] = \frac{1-(-1)^i}{2}$. Show that $e_i \mapsto p^{c_i}e'_i$, with $c_0 = 0$ and $c_{i+1} = c_i + [i \text{ odd}] - w_i$, is well defined modulo $2m$ because the sum of $[i \text{ odd}] - w_i$ over a cycle is $m - m = 0$, and that it commutes with F. Why does it then commute with $V = pF^{-1}$?

EXERCISE 15.3. Compute the a-numbers of 00100111, 00101101, 00001111 and 01+001011 directly from $\dim M/(FM + VM)$, using $Fe_i = p^{w_i}e_{i+1}$ and $Ve_{i+1} = p^{1-w_i}e_i$, and compare with the count of $1 \to 0$ transitions.

EXERCISE 15.4. Find the dual of 00100111 up to rotation, and decide which of the eight primitive words of length 8 are self-dual.

EXERCISE 15.5. Let $\mathrm{pol}_{\mathscr{L}} \colon X \to X^\vee$ be a polarization of degree prime to p. Show that $\mathrm{pol}_{\mathscr{L}}[p^\infty]$ is an isomorphism and deduce that $M(X)$ is isomorphic to its dual. Conclude that the abelian fourfolds with Dieudonné module 00100111 have no polarization of degree prime to p.

15.4. The Fourier source

Let X be a supersingular abelian fourfold over $\bar{\mathbb{F}}_p$, $X^\vee$ its dual, and $\mathcal{P}$ the Poincaré bundle on $X \times X^\vee$.

DEFINITION 15.4 (the Fourier source). The *Fourier source* of X is

$$\widehat{S}(X) = \mathbb{Z}_p\text{-span of } \tfrac{1}{24}\,\mathrm{pr}_{X*}\big(\mathrm{pr}_{X^\vee}^* y \cdot c_1(\mathcal{P})^4\big), \qquad y \in S(X^\vee).$$

It is the degree-4 part of the cohomological Fourier transform applied to the divisor products of the dual (compare [Bea83]).

LEMMA 15.5 (the Fourier lemma). *For $p \geq 5$, $\widehat{S}(X) \subseteq \mathrm{Alg}^2(X)$.*

PROOF. By Fact 4.10, $S(X^\vee) \subseteq \mathrm{Alg}^2(X^\vee)$. The class $c_1(\mathcal{P})$ is the class of a divisor, 24 is a unit in $\mathbb{Z}_p$, and the cycle class is compatible with products, pull-backs and push-forwards (Fact 4.6). □

Computing $\widehat{S}$. Let (e_i) be a basis of $M(X)$ and (e'_j) one of $M(X^\vee)$. The bundle $\mathcal{P}$ is trivial on $X \times \{0\}$ and on $\{0\} \times X^\vee$, so $c_1(\mathcal{P})$ has no Künneth components of types $(2,0)$ and $(0,2)$, and $c_1(\mathcal{P}) = \sum_{i,j} \lambda_{ij} e_i \otimes e'_j$ with $\lambda_{ij} \in W$. By Fact 4.6, $\int c_1(\mathcal{P})^8$ is $\pm 8! \det(\lambda_{ij})$ times a unit of W. By Riemann–Roch on $X \times X^\vee$ it is $\deg(c_1(\mathcal{P})^8) = 8!\chi(\mathcal{P})$, and $\chi(\mathcal{P}) = \pm 1$. Indeed $\chi(\mathcal{P})^2$ is the degree of the homomorphism $X \times X^\vee \to X^\vee \times X^{\vee\vee}$ attached to $\mathcal{P}$, which is $(x, x^\vee) \mapsto (x^\vee, x)$ with x viewed in $X^{\vee\vee}$, an isomorphism because biduality is one (see e.g. [Mil08, Chapter I, Theorems 11.1 and 8.9]). So $\det(\lambda_{ij}) \in W^\times$, the vectors $\check{e}_i = \sum_j \lambda_{ij} e'_j$ form a basis of $M(X^\vee)$, and

$$\frac{c_1(\mathcal{P})^n}{n!} = \sum_{|J|=n} \pm e_J \otimes \check{e}_J$$

is integral for every n. Hence the Fourier transform

$$\mathfrak{F}(y) = \mathrm{pr}_{X*}\Big(\mathrm{pr}_{X^\vee}^* y \cdot \frac{c_1(\mathcal{P})^{8-n}}{(8-n)!}\Big), \qquad y \in \textstyle\bigwedge^n M(X^\vee),$$

maps $\check{e}_J$, $|J| = n$, to a unit multiple of e_{J^c}, where J^c is the complement of J, and is an isomorphism $\bigwedge^n M(X^\vee) \to \bigwedge^{8-n} M(X)$. Since $c_1(\mathcal{P})$ is the class of a divisor, $Fc_1(\mathcal{P}) = pc_1(\mathcal{P})$, and with $\int Fz = p^4\sigma(\int z)$ on $X^\vee$ this gives $F\mathfrak{F}(y) = p^{4-n}\mathfrak{F}(Fy)$ (Exercise 15.6). So $\mathfrak{F}$ maps $T^n(X^\vee)$ onto $T^{8-n}(X)$.

Now let (e_i) be the monomial basis of $M(X)$. For $n = 2$, $T^2(X^\vee) \otimes W$ is monomial in the basis $(\check{e}_J)$, with the exponent of $T^6(X)$ at e_{J^c}. A product of two classes of $T^2(X^\vee)$ is mapped by $\mathfrak{F}$ to a product of the Pontryagin kind, which on the monomial basis sends e_{J_1} and e_{J_2}, for 6-sets J_1, J_2, to $\pm e_{J_1 \cap J_2}$ if $J_1 \cup J_2$ is the whole index set and to 0 otherwise. So $\widehat{S}(X) \otimes W$ is the monomial lattice whose exponent at e_J, $|J| = 4$, is

$$n_J^{\widehat{S}} = \min\{n_{J_1} + n_{J_2} : \ J_1, J_2 \text{ 6-sets}, \ J_1 \cap J_2 = J, \ J_1 \cup J_2 \text{ the whole index set}\},$$

with n_{J_1}, n_{J_2} the exponents of $T^6(X)$.

Exercise 15.6. Check the degrees in $\mathfrak{F}$: $\mathrm{pr}_{X^\vee}^* y \cdot c_1(\mathcal{P})^{8-n}$ has degree $16 - n$ on $X \times X^\vee$, and pr_{X*} lowers degrees by 8. Then derive $F\mathfrak{F}(y) = p^{4-n}\mathfrak{F}(Fy)$ from $Fc_1(\mathcal{P}) = pc_1(\mathcal{P})$ and $\mathrm{pr}_{X*} F = p^4 F \,\mathrm{pr}_{X*}$, and deduce that $\mathfrak{F}(T^n(X^\vee)) \subseteq T^{8-n}(X)$.

Fourier symmetry. For $n = 4$ the transform $\mathfrak{F}$ is an isomorphism $T^4(X^\vee) \to T^4(X)$, and by definition it maps $S(X^\vee)$ onto $\widehat{S}(X)$. Hence

$$[T^4(X) : \widehat{S}(X)] = [T^4(X^\vee) : S(X^\vee)]. \tag{15.1}$$

The Fourier source of X is as large as the divisor products of the dual. Since the Dieudonné module of $X^\vee$ is the dual module, whose words are the complementary words, (15.1) can be read off a list of the indices $[T^4 : S]$ alone.

Example 15.6 (the Fourier source closes a gap). The module 00101011 has $[T^4 : S] = p^2$, and its dual 00110101 has $[T^4 : S] = 1$ (Table 15.1). By (15.1), $\widehat{S} = T^4$ for 00101011: the Fourier source alone fills the gap that divisor products leave. For the dual pair 00011101, 00010111, with $[T^4 : S] = p^2$ and p^{16}, the Fourier source has index p^{16} and p^2 respectively, so neither source suffices alone; the computation shows that together they span T^4, because the two sources miss different monomials. For the undecided pair 00100111, 00011011 both indices are p^{26}, and $S + \widehat{S}$ still has index p^{26}. For $\mathbb{M} = 01 + 000111$, which is self-dual, $[T^4 : \widehat{S}] = [T^4 : S] = p^4$, and $S + \widehat{S} = S$.

Exercise 15.7. Using (15.1) and Table 15.1, find $[T^4 : \widehat{S}]$ for each of the four undecided modules and for 00110101. Why can the Fourier source not help for a self-dual module with $\widehat{S} = S$? Is $\widehat{S} = S$ automatic for self-dual modules, or only $[T^4 : \widehat{S}] = [T^4 : S]$?

15.5. The monomial-module proposition

Proposition 15.7 (monomial modules). *Let $p \geq 5$. For the twenty cycle decompositions, the indices $[T^4 : S]$ and $[T^4 : S + \widehat{S}]$ are as in Table 15.1. Consequently the integral crystalline Tate conjecture holds in codimension 2, without Hypothesis (M), for every abelian fourfold over $\overline{\mathbb{F}}_p$ whose Dieudonné module is isomorphic to one of the fifteen decompositions with $S + \widehat{S} = T^4$, which form nine isomorphism classes. It holds under Hypothesis (M) for $01 + 000111$ (Theorem C). For the remaining four modules the index $[T^4 : S + \widehat{S}]$ does not change when $S + \widehat{S}$ is enlarged by the push-forwards and pull-backs of T^4 along homomorphisms to and from the abelian fourfolds whose Dieudonné modules are among the fifteen with $S + \widehat{S} = T^4$, and then closed under pull-backs and push-forwards by endomorphisms. Nor does it change when the same is done with T^4 of the fourfolds with p-divisible group $\mathscr{G}_p$, which is algebraic under Hypothesis (M).*

Proof. All lattices involved are monomial with min-plus exponents: T^4 and S by the descent lemma (Lemma 5.3), $\widehat{S}$ by Section 15.4. Push-forward along a homomorphism f acts on $\bigwedge^4$ through the complementary 4×4 minors of f^*, by Poincaré duality. The Hom-lattices are monomial in the matrix units, and since 4! is a unit, polarization reduces the spans over all homomorphisms to spans over monomial multiples of matrix units (Chapter 5). The exponents are then an exact integer computation, described below. The consequences follow from $S \subseteq \mathrm{Alg}^2$, Lemma 15.5, and the fact that T^4 and S depend only on the Dieudonné module. □

module	a-number	self-dual	$\log_p[T^4 : S]$	$\log_p[T^4 : S + \widehat{S}]$
$01+01+01+01$, $01+01+0101$, $0101+0101$, $01+010101$, 01010101	4	yes	0	0
$01+01+0011$, $0011+0101$, 00101101	3	yes	0	0
00110101	3	no	0	0
$0011+0011$, 00110011	2	yes	0	0
00001111	1	yes	0	0
00101011	3	no	2	0
00011101, 00010111	2	no	2, 16	0
$01+000111$	2	yes	4	4
$01+001101$, $01+001011$	3	no	2, 10	2
00100111, 00011011	2	no	26	26

TABLE 15.1. The twenty cycle decompositions of monomial supersingular Dieudonné modules of height 8 and dimension 4, named by their words. They form fourteen isomorphism classes: the five decompositions of the first row give isomorphic modules, as do $01+01+0011$ and $0011+0101$, and $0011+0011$ and 00110011. "Self-dual" means isomorphic to the dual module, whose words are the complementary words; it is necessary for a polarization of degree prime to p, because such a polarization induces an isomorphism $X[p^\infty] \cong X^\vee[p^\infty]$ and $M(X^\vee)$ is the dual module [Oda69, Definition 3.6 and Proposition 3.23]. The indices are powers of p whose exponents are exact and independent of $p \geq 5$.

The computation, in words. For each of the twenty decompositions the computation lists the cycles of Frobenius, evaluates the orbit rule (5.1) for all 2-, 4- and 6-subsets of the basis, takes the minima over splittings for S and the minima of $n_{J_1} + n_{J_2}$ for $\widehat{S}$, and compares exponents. For the enlargements it computes the monomial Hom-lattices between the modules, the spans of pull-backs through 4×4 minors and of push-forwards through complementary minors, and closes under endomorphisms. It also determines the duals and the a-numbers. Every number is an exact integer and none depends on p; the arithmetic is in exponents, not in p-adic numbers.

What just happened. Divisor products alone give T^4 for six of the fourteen classes. The Fourier transform of divisor products on the dual is a second unconditional source, algebraic for $p \geq 5$ because 24 is then a unit, so that $c_1(\mathcal{P})^4/24$ is a p-adic unit multiple of an algebraic class, and it closes the gap for three more classes, including 00010111, where divisor products miss a factor p^{16}. The class of $\mathbb{M}$ is closed by the Weil cycle of Part IV under Hypothesis (M), and four classes are left undecided.

15.6. The four undecided modules

For each of the four undecided modules, $01+001101$, $01+001011$, 00100111 and 00011011, the computation finds exactly one pair of complementary eigensets of a diagonal action of an inert imaginary quadratic field of type $(2, 2)$, alternating along every cycle of Frobenius as in Lemma 8.4, and the corresponding lattice of integral Weil classes, together with its translates under endomorphisms, would span T^4 with S. For the two modules of a-number 3 the Weil lattice and $S + \widehat{S}$ already span T^4, without endomorphisms; for the two of a-number 2 they leave index p^{24}, and the endomorphism translates are needed. So each gap would be closed by one algebraic Weil class with a unit coefficient, exactly as for $\mathbb{M}$.

None of the four modules is self-dual, so the abelian fourfolds that carry them have no polarization of degree prime to p (Exercise 15.5). The unimodularity lemma Lemma 12.6 and Schoen's step Proposition 10.9 need a unimodular Hermitian lattice at p, which comes from such a polarization, so they do not apply as written. The Gram step of Proposition 13.4 itself does not use a polarization: the pairing on the Weil lattice is the intersection form. What is missing is a p-integral Weil cycle with a unit Weil coefficient on a lift whose first homology is not a unimodular Hermitian lattice at p.

The pair 00100111, 00011011 keeps the index p^{26} under all the enlargements of Proposition 15.7, the largest gap among the monomial modules. It is the natural test case, both for a new source of algebraic classes and for a possible failure of the integral crystalline Tate conjecture, and the computations decide neither.

Where this is used. Nothing in the proofs of the main theorems uses this chapter. Proposition 15.7 is the summary of the monomial cases quoted in Chapter 1, and Section 15.6 is what Section 14.7 refers to as left undecided.

APPENDIX A

Glossary of symbols

Each symbol in the table has the one meaning given there, everywhere in the companion: in the text, the examples, the exercises and the solutions. Decorations (primes, indices, bars) do not change the meaning of a letter; they distinguish several objects of the same kind. A few letters are used throughout as variables with a fixed kind and are not listed below: i, j, l and n are integers (indices, counts and exponents), x, y and z are elements of modules, classes, cycles, points or variables of polynomials, λ is a scalar, and γ is a matrix, a linear map or an element of a group. Fonts are part of a symbol: S and $\mathscr{S}$, or L and $\mathcal{L}$, are different symbols. The last column names the place where the symbol is defined or first explained.

symbol	meaning	defined in
p	a prime, $p \geq 5$ unless a statement says otherwise	Chapter 1
W, σ	the Witt vectors $W(\bar{\mathbb{F}}_p)$ and their Frobenius	Chapter 3
r, $\mathbb{Z}_{p^r}$, $\mathbb{Q}_{p^r}$, $W[1/p]$	a residue degree, $W(\mathbb{F}_{p^r})$, its fraction field, the fraction field of W	Section 3.2
v_p	the p-adic valuation	Chapter 3
X, g, $X^\vee$	an abelian variety, its dimension, its dual	Chapter 2
f	a morphism of varieties, mostly an isogeny or a homomorphism of abelian varieties	Section 2.3
E, E_0	an elliptic curve, a supersingular elliptic curve over $\bar{\mathbb{F}}_p$	Chapter 2
$\mathcal{P}$	the Poincaré bundle on $X \times X^\vee$	Chapter 2, Section 15.4
$\mathscr{L}$, $\mathrm{pol}_{\mathscr{L}}$	a line bundle, the homomorphism $X \to X^\vee$ it defines	Section 2.3
$\boldsymbol{\alpha}_p$, $\boldsymbol{\mu}_p$, $\boldsymbol{\mu}_{p^\infty}$	the kernel of $x \mapsto x^p$ on the additive group, the group schemes of p-th and of p-power roots of unity	Section 2.4
Γ_α	the graph of an endomorphism α	Example 2.8
Y, $\mathrm{CH}^i(Y)$	a smooth projective variety, its Chow groups	Section 2.6
O, $\mathcal{X}$, $\mathcal{Y}$	a discrete valuation ring, an abelian scheme and a smooth projective scheme over it	Section 2.7
$X[p^\infty]$, $\mathscr{G}$	the p-divisible group of X, a p-divisible group	Definition 2.7, Fact 3.10
H^n, H_1, $H^{1,0}$, Ω^1, $\mathcal{O}$	cohomology, homology, holomorphic 1-forms, the sheaf of 1-forms, the structure sheaf	Section 2.2
M, $M(X)$, F, V	a Dieudonné module or a module, the Dieudonné module $H^1_{\mathrm{cris}}(X/W)$, Frobenius, Verschiebung	Fact 3.10
Φ, Π	a σ^r-semilinear map, a bijection $p^{-1}F^2$ or $p^{-1}\Phi^2$	Section 3.3, Proposition 3.16
ξ	a unit that is not a square	Example 3.3
I, $I_{l/n}$	an F-isocrystal, the simple isocrystal of slope l/n	Section 3.6
u	a Newton slope	Section 3.6, Section 7.4
$a(X)$	the a-number	Definition 3.15
w, w_i, $\lvert w\rvert$	a binary word, its letters, its length	Definition 3.17
A	the matrix $\left(\begin{smallmatrix} 0 & p \\ 1 & 0 \end{smallmatrix}\right)$, $Ae_0 = e_1$, $Ae_1 = pe_0$	Equation (3.1)
e	a basis vector: e_0, e_1, e_s, e_J, the matrix units $e_{ss'}$, a second basis e'_j, the dual basis $\check{e}_j$	Section 3.8

symbol	meaning	defined in
$T^n(X)$	integral crystalline Tate classes of degree n, X supersingular	Definition 4.3
$S(X)$, S^n	products of two classes of T^2; products in degree n	Definition 4.9, Chapter 5
$\mathrm{Alg}^i(X)$	$\mathbb{Z}_p$-span of classes of codimension-i cycles	Definition 4.8
cl, $\int$	crystalline cycle class, trace	Fact 4.6
c_1, c_2, c_3, ch	Chern classes, Chern character	Fact 4.6, Section 11.2
χ	the Euler characteristic	Section 2.3
L, $\operatorname{disc} L$, $\langle\ ,\ \rangle$	a lattice, its discriminant, a bilinear form	Section 4.7
α, α^*	an endomorphism or homomorphism, its pull-back	Chapter 4
J	a subset of the index set of a basis	Section 4.2
$\mathcal{C}$, s, s'	the index set of a monomial basis (for $\mathbb{M}$ the cube $\{0,1\}^3$), its elements (for $\mathbb{M}$ the vertices $s=(s_1,s_2,s_3)$)	Section 5.1, Equation (1.1)
$w(s)$, $w(J)$	the weight of an index and of a subset	Section 5.3
φ, q, π, π'	$p^{-n/2}\bigwedge^n F$, the order of π, a permutation of a basis, another permutation or bijection	Lemma 5.3
n_J, n_J^S	the exponents of T^n and of S^n at e_J	Lemma 5.3
$L(n)$	the monomial lattice with exponent vector n	Section 5.2
$m_{ss'}$	the exponents of $\mathrm{End}(M,F)\otimes W$ in the matrix units	Section 5.7, Section 9.2
Ad_F, D	conjugation by F on $\mathrm{End}_W(M)$, the polarized form $D(\alpha_1,\dots,\alpha_4)$ of $\alpha\mapsto\bigwedge^4\alpha$ and its components D_i	Chapter 5
$\mathcal{R}$, Ξ, $\mathrm{End}^*\,\Xi$	a ring or module of endomorphisms, a set of classes, the span of their pull-backs	Section 5.7
$\mathbb{M}$	the model, $F(x_1\otimes x_2\otimes x_3)=\sigma x_3\otimes A\sigma x_1\otimes\sigma x_2$	Equation (1.1)
T_+, T_-, M_+, M_-	the four sets: tetrahedra and majority sets	Equation (8.2)
ι_s, J_ι, M_ι	the character on e_s of a diagonal action of $\mathbb{Z}_{p^2}$, its ι-eigenset, the ι-eigenspace	Section 8.5
$\mathcal{L}$, $\mathcal{N}$, N	the Weil lattice, the majority lattice, $N=S+\mathcal{N}$	Definition 8.6, Definition 8.8
pr_J	the coordinate projection onto the span of the e_s, $s\in J$	Example 9.1
T_{22}	Künneth $(2,2)$-component of $T^4(X\times X)$	Definition 9.3
$\mathscr{G}_p$, $\mathscr{G}'_p$	the p-divisible group of $\mathbb{M}$, its factor of height 6	Chapter 1, Remark 7.6
k, $\infty_1,\infty_2,\infty_3$	the totally real cubic field, its real embeddings	Section 6.2
B, G, $\mathbb{V}$, ψ	the quaternion algebra, Mumford's group, $\mathbb{Q}^8$, a Riemann form (the symplectic form of the datum)	Section 6.2
$\mathrm{Ram}(B)$	the set of places of k where B ramifies	Exercise 6.2
v	a place of a number field	Section 6.2
$\mathfrak{p}_1$, $\mathfrak{p}_2$	primes of k above p	Section 14.4
$\mathfrak{S}_n$	the symmetric group	Section 5.7
Mat_n	the algebra of $n\times n$ matrices	Section 3.3
U, U_1, U_2, U_3	a plane (a module of rank 2), the three planes with $\mathbb{V}\otimes\overline{\mathbb{Q}}=U_1\otimes U_2\otimes U_3$	Section 6.2
ϵ, e^ϵ	a sign vector in $\{\pm\}^3$, the weight vector it indexes	Example 6.2
$\mathbf{h}$, $\mathbb{X}$, $\mathcal{J}$	a Hodge morphism, its conjugacy class, a complex structure	Section 6.2
X_{gen}	a very general complex fiber of Mumford's family	Section 6.3
Λ, $\mathsf{K}=\mathsf{K}_p\mathsf{K}^p$, $\mathscr{S}$, $\mathcal{A}$	the lattice, the level, Kisin's integral model, the abelian scheme	Section 6.4
t	a point of $\mathscr{S}$	Section 6.4
$\mathfrak{t}_i$	Kisin's crystalline tensors	Section 6.4

symbol	meaning	defined in
(h1)–(h4)	the hypotheses at p	Equation (6.2)
U_p, τ, τ_i	the plane over k_p, an embedding of k, the embeddings $\mathbb{Z}_{p^3} \to W$	Section 6.5
Λ_0, Λ_i, Cor, ς	a lattice in U_p, its slot lattices, tensor induction, the slot permutation	Definition 6.6
$\mathbb{T}'$, $\mathcal{G}$	the kernel torus of $\mathrm{GL}_2^3 \to \mathrm{GL}_8$, the closure of G in $\mathrm{GL}(\Lambda \otimes \mathbb{Z}_{(p)})$	Proposition 6.7
u_0, $\mathbf{h}_0$, S^1	the homomorphism defining Mumford's Hodge morphism, that morphism, the circle group	Section 6.2
N_i	a nilpotent map in one slot	Exercise 6.4
$\mathcal{U}$	an auxiliary vector space or subspace	Exercise 6.4
β_1, β_2, β_3	slot components of Frobenius	Equation (7.1)
K, d_0, θ	an imaginary quadratic field $\mathbb{Q}(\sqrt{-d_0})$, $\theta = \sqrt{-d_0}$	Section 10.2
ι, $\bar{\iota}$	the two embeddings of K, with $\operatorname{Im}\iota(\theta) > 0$	Section 10.2
b	an element of K, of O_K or of K_p	Section 10.2
(g_+, g_-)	the type of a K-action	Definition 10.2
H^1_ι, $H^1_{\bar{\iota}}$	eigenlattices of $H^1(\cdot, \mathbb{Z}_{(p)}) \otimes O_K$	Equation (10.1)
ω, $\bar{\omega}$	exterior products of bases of H^1_ι, $H^1_{\bar{\iota}}$	Definition 10.3
ν	a Weil coefficient, $\nu\omega + \bar{\nu}\bar{\omega}$	Definition 10.3
$\mathcal{H}$, h	skew-Hermitian form of a polarization, the Hermitian form $h = \theta\mathcal{H}$	Definition 10.4
$\mathcal{V}$	a Hermitian space, or a real subspace of one	Proposition 10.5
X_2, $\mathcal{V}'$, $\mathcal{V}'_{\mathbb{Z}}$	the Weil surface of Schoen's step, its Hermitian space and lattice	Proposition 10.9
Ψ, ϑ	the isometry, the isogeny of Schoen's step	Proposition 10.9
$\mathrm{U}(\mathcal{V})$, $\mathfrak{u}_{\mathcal{V}}$, S_p	a unitary group, its skew-Hermitian maps, an open subgroup of $\mathrm{U}(\mathcal{V})(\mathbb{Q}_p)$	Lemma 10.8
d, K_d	Markman's even integer $d \geq 3$, $\mathbb{Q}(\sqrt{-d})$	Section 11.2
C, X_3, Θ	a curve of genus 3, $\mathrm{Pic}^2(C)$, its theta divisor	Section 11.2
X_6, $\mathcal{E}$, $\mathcal{I}_1$, $\mathcal{I}_2$	Markman's sixfold, his sheaf, the ideal sheaves	Section 11.2
$\mathcal{F}$, $\mathcal{B}$	a sheaf or complex, the twisted sheaf of Hypothesis (M)	Section 11.2, Section 11.3
ϱ, Y_6	the quotient isogeny of Hypothesis (M), its target	Section 11.3
$\Theta^\sharp$, $(\cdot,\cdot)$, ψ_6	contraction with Θ, the symmetric pairing on $H^1(X_6, \mathbb{Z})$, the polarization $(\eta x, y)$	Section 11.2
$\mathcal{W}_1$, $\mathcal{W}_2$, $\mathcal{W}_{1,\mathbb{Z}}$, $\mathcal{W}_{2,\mathbb{Z}}$	the eigenspaces of η in $H^1(X_6, K_d)$, their integral parts	Section 11.2
$\mathscr{D}$, $X_{6,t}$	the period domain of the family of $(H^1(X_6,\mathbb{Z}), \eta, \psi_6)$, its members	Section 11.2
SU_6, A_0, A, D_6, D'_6, $\tilde{G}_6$	the special unitary group of ψ_6, Markman's arithmetic group, a neat subgroup, two arithmetic subgroups, the inverse image in the spin group	Section 11.5
$\mathscr{N}$, $\mathcal{C}^\omega$, $[\mathcal{F}]_{\mathrm{top}}$, $\mathfrak{f}\colon \mathscr{N} \to \mathscr{T}$, $\mathscr{N}_t$	a complex manifold, its sheaf of real-analytic functions, the topological K-theory class of a complex, a proper holomorphic submersion, a fiber	Section 11.4
$\mathscr{E}$, Y', Y'', Z', $[Z']_n$	an algebraic vector bundle, subvarieties, a subscheme, its cycle of dimension n	Section 11.4, Lemma 11.4
$\mathcal{Z}_i$, $Z_{i,\mathfrak{q}}$, $\mathfrak{b}$, $\tilde{C}$, $\mathfrak{n}$	universal subschemes, their fibers, the class $\sum_i n_i \operatorname{ch}_3(\mathcal{O}_{Z_{i,\mathfrak{q}}})$, a nonsingular curve, its map to $\mathscr{Q}$	Section 11.5
$\mathscr{M}$, $\mathfrak{X}$, $\mathscr{U}$, $\mathfrak{H}_i$, $\mathscr{Q}$, $\mathscr{Z}$, $\mathscr{V}$	the arithmetic quotient, its family of sixfolds, a neighborhood, Hilbert scheme components, a component of their product, a closed subset, a coordinate ball	Section 11.5
η, FM, D^b	the action of $\sqrt{-d}$, Orlov's equivalence, the bounded derived category	Section 11.2

symbol	meaning	defined in
κ, κ_3	$\exp(-c_1/\operatorname{rk})\operatorname{ch}$ and its degree-6 part	Section 11.2
ρ_1, ρ_2, ϖ_d	$\exp(\pm\sqrt{-d}\Theta)$, the coefficient $\frac{1}{2}(1+1/\sqrt{-d})$	Section 11.8
Υ	the primitive Weil class $\frac{1}{2}(\omega_{X_6}+\bar{\omega}_{X_6})$ of X_6	Lemma 11.8
$\mathfrak{s}$, $\tilde{\mathfrak{s}}$, $\mathfrak{c}$	the linear map of Markman's spin argument, its twist by $\exp(-c_1(\mathcal{P})/2)$, the image of $\operatorname{ch}(\mathcal{I}_1)\otimes\operatorname{ch}(\mathcal{I}_1)^\star$	Lemma 11.8
(M)	Hypothesis (M)	Hypothesis (M)
K', K'^1, $\mathbb{T}$	the CM field kK, its norm-one torus over k, the torus of G	Section 12.3
R	the algebra $\mathbb{Q}[\mathbb{T}(\mathbb{Q})]\cong K\times K'$	Section 12.4
t_{CM}, X_{CM}, t_0, Λ_R	the CM point, the CM fourfold, its reduction point, the lattice $H_1(X_{\mathrm{CM}},\mathbb{Z}_p)$	Proposition 12.2, Section 12.5
Δ, G^F	the quaternion division algebra centralizing $A\sigma^3$, the centralizer of F	Section 12.6
Z, ν_Z, Z_6	the Weil cycle on X_{CM}, its unit Weil coefficient, the cycle on X_6' given by Proposition 11.5	Proposition 13.2
ζ, μ_i	the reduction of b modulo p, the eigenvalues $b^i\bar{b}^{4-i}$	Section 13.3
Q, Q_P, P	a polynomial, the interpolation polynomial, the projector $Q_P([b]^*)$	Equation (13.1)
Z_1, Z_2, sp	the two cycles PZ and $[b]^*PZ$, specialization	Section 13.4, Fact 2.9
δ	an exceptional Hodge class on $X_{\mathrm{gen}}\times X_{\mathrm{gen}}$	Remark 14.3
$\mathbf{w}$, $M_{\mathbf{w}}$	a multiset of words, its monomial module	Section 15.2
$\widehat{S}(X)$, $n_J^{\widehat{S}}$	the Fourier source, its exponents	Definition 15.4, Section 15.4
$\mathfrak{F}$	the Fourier transform	Section 15.4

APPENDIX B

Hints and solutions

For each exercise a hint comes first and the full solution after it, so that the hint can be read on its own.

Chapter 1

Hint for Exercise 1.1. The rank of $\bigwedge^n M$ is $\binom{8}{n}$. A pair $\{J, J'\}$ is determined by its union and by a splitting of the union into two halves.

Solution to Exercise 1.1. The ranks are $\binom{8}{n}$: $1, 8, 28, 56, 70, 56, 28, 8, 1$ for $n = 0, \dots, 8$. An unordered pair $\{J, J'\}$ of disjoint 2-sets is determined by its union $J \cup J'$, a 4-set, together with the splitting of $J \cup J'$ into J and J'; a 4-set has $\frac{1}{2}\binom{4}{2} = 3$ splittings. So there are $3 \cdot 70 = 210$ pairs, which agrees with $\frac{1}{2}\binom{8}{2}\binom{6}{2} = \frac{1}{2} \cdot 28 \cdot 15 = 210$, and each 4-set is the union of exactly 3 of them. So the 210 products $e_J \wedge e_{J'}$ give, up to sign, each of the 70 basis vectors $e_{J \cup J'}$ of $\bigwedge^4 M$ three times. In particular the products of 2-forms span $\bigwedge^4 M$, which is the rational statement in degree 4 in its simplest form. □

Hint for Exercise 1.2. Compute F on the basis $e_1 \wedge e_2$, $e_i \wedge e_j$ $(i \le 2 < j)$, $e_3 \wedge e_4$, and compare p-adic valuations of coefficients on the outer parts.

Solution to Exercise 1.2. In the basis given, $F(e_1 \wedge e_2) = e_1 \wedge e_2$, $F(e_i \wedge e_j) = p e_i \wedge e_j$ for $i \le 2 < j$, and $F(e_3 \wedge e_4) = p^2 e_3 \wedge e_4$, with F acting σ-semilinearly on coefficients. Write $x = \lambda_1 e_1 \wedge e_2 + \sum_{i \le 2 < j} \lambda_{ij} e_i \wedge e_j + \lambda_2 e_3 \wedge e_4$ with coefficients in W. Then $Fx = px$ means $\sigma(\lambda_1) = p\lambda_1$, $\sigma(\lambda_{ij}) = \lambda_{ij}$ and $p\sigma(\lambda_2) = \lambda_2$. Since σ preserves p-adic valuations, $\sigma(\lambda_1) = p\lambda_1$ is impossible unless $\lambda_1 = 0$, and likewise $\lambda_2 = 0$. The equations $\sigma(\lambda_{ij}) = \lambda_{ij}$ mean $\lambda_{ij} \in W^\sigma = \mathbb{Z}_p$ (Chapter 3). So the solutions are the $\mathbb{Z}_p$-span of the four $e_i \wedge e_j$, of rank 4, and no nonzero vector of $\bigwedge^2 M_{\text{et}} \oplus \bigwedge^2 M_{\text{mult}}$ is a solution. □

Hint for Exercise 1.3. The map $L''/L \to L''/L'$, $x + L \mapsto x + L'$, is well defined and surjective.

Solution to Exercise 1.3. Since $L \subseteq L'$, the map $L''/L \to L''/L'$, $x + L \mapsto x + L'$, is well defined and surjective, with kernel L'/L. So L''/L' is a quotient of L''/L, and $|L''/L| = |L''/L'| \cdot |L'/L|$; all three groups are finite because the modules have the same rank. In the application $L = S(X)$, $L' = \mathrm{Alg}^2(X)$, $L'' = T^4(X)$: if divisor products span T^4, so do algebraic classes. □

Hint for Exercise 1.4. A finite $\mathbb{Z}_p$-module killed by p is a vector space over $\mathbb{F}_p$.

Solution to Exercise 1.4. The finite group L/L' is a $\mathbb{Z}_p$-module killed by p, hence a vector space over $\mathbb{Z}/p$. Its order is $[L : L'] = p^4$, so its dimension is 4 and $L/L' \cong (\mathbb{Z}/p)^4$. □

Hint for Exercise 1.5. Frobenius maps $x_1 \otimes x_2 \otimes x_3$ to $\sigma x_3 \otimes A\sigma x_1 \otimes \sigma x_2$, and σ is bijective.

Solution to Exercise 1.5. Since σ is bijective on W^2, the image of F is spanned by the vectors $x \otimes Ay \otimes z$ with $x, y, z \in W^2$, that is $F(\mathbb{M}) = W^2 \otimes AW^2 \otimes W^2$. As $AW^2 = \{(p\lambda, \lambda')\}$ contains pW^2, $F(\mathbb{M})$ contains $p\mathbb{M}$, so $V = pF^{-1}$ is defined on $\mathbb{M}$ and $(\mathbb{M}, F, V)$ is a Dieudonné module, of height $\operatorname{rk} \mathbb{M} = 8$. The quotient $\mathbb{M}/F(\mathbb{M}) \cong W^2 \otimes (W^2/AW^2) \otimes W^2$ has length $2 \cdot 1 \cdot 2 = 4$, which is the dimension. The vectors e_s not in $F(\mathbb{M})$ are those with $e_{s_2} \notin AW^2$,

that is with $s_2 = 0$: $e_{000}, e_{001}, e_{100}, e_{101}$. In terms of the formula, e_s with $s_2 = 0$ is F of $p^{-1}e_{\pi^{-1}(s)}$, where $\pi^{-1}(s) = (1 - s_2, s_3, s_1)$ has first coordinate 1. □

Chapter 2

Hint for Exercise 2.2. Use the product polarization on E_0^g; the Rosati involution is the conjugate transpose with quaternion conjugation.

Solution to Exercise 2.2. With the product of the principal polarizations, $\mathrm{End}(E_0^g) \otimes \mathbb{Q}$ is the algebra of $g \times g$ matrices with entries in the quaternion algebra $\mathrm{End}(E_0) \otimes \mathbb{Q}$, and the Rosati involution is $(\alpha_{ij}) \mapsto (\bar{\alpha}_{ji})$. A fixed matrix has diagonal entries with $\bar{\alpha}_{ii} = \alpha_{ii}$, that is $\alpha_{ii} \in \mathbb{Q}$, giving g dimensions, and for each of the $\binom{g}{2}$ pairs $i < j$ an arbitrary quaternion α_{ij}, which determines $\alpha_{ji} = \bar{\alpha}_{ij}$, giving 4 dimensions each. So $\mathrm{NS}(E_0^g) \otimes \mathbb{Q}$ has dimension $g + 4\binom{g}{2} = g + 2g(g-1) = g(2g-1)$, which is 28 for $g = 4$. This equals $\binom{2g}{2}$, the rank of $T^2(E_0^g)$, as it must by Fact 4.10. □

Hint for Exercise 2.3. Composition with isogenies $E_0^{g'} \to X'$ and $X \to E_0^g$ and their quasi-inverses identifies the rational Hom-spaces.

Solution to Exercise 2.3. By Fact 2.6(a) there are isogenies $f_1 \colon E_0^{g'} \to X'$ and $f_2 \colon X \to E_0^g$, with quasi-inverses f_1', f_2' such that $f_1 f_1' = [\deg f_1]$ and so on. The maps $\alpha \mapsto f_2 \alpha f_1$ and $\alpha' \mapsto f_2' \alpha' f_1' / (\deg f_1 \deg f_2)$ are inverse to each other after tensoring with $\mathbb{Q}$, so $\mathrm{Hom}(X', X) \otimes \mathbb{Q} \cong \mathrm{Hom}(E_0^{g'}, E_0^g) \otimes \mathbb{Q}$. A homomorphism $E_0^{g'} \to E_0^g$ is a $g \times g'$ matrix of endomorphisms of E_0, so this is $\mathrm{Mat}_{g \times g'}(\mathrm{End}(E_0) \otimes \mathbb{Q})$, of dimension $4gg'$ because $\mathrm{End}(E_0) \otimes \mathbb{Q}$ is a quaternion algebra. □

Hint for Exercise 2.4. Compute $(([n]^* \mathscr{L})^g)$ in two ways.

Solution to Exercise 2.4. On the one hand $(([n]^* \mathscr{L})^g) = \deg[n] \cdot (\mathscr{L}^g)$, by the stated property of finite surjective morphisms. On the other hand $[n]^* \mathscr{L} \cong \mathscr{L}^{\otimes n^2}$, so $(([n]^* \mathscr{L})^g) = (n^2)^g (\mathscr{L}^g)$. Since $(\mathscr{L}^g) > 0$ for ample $\mathscr{L}$, $\deg[n] = n^{2g}$. □

Hint for Exercise 2.5. Since $3 \nmid 11 - 1$, cubing is a bijection of $\mathbb{F}_{11}^\times$, hence of $\mathbb{F}_{11}$.

Solution to Exercise 2.5. As x runs over $\mathbb{F}_{11}$, $z = x^3 + 1$ runs over every element of $\mathbb{F}_{11}$ exactly once. The number of y with $y^2 = z$ is $1 + \left(\frac{z}{11}\right)$, with the Legendre symbol $\left(\frac{z}{11}\right)$, which is 0 for $z = 0$, and $\sum_z \left(\frac{z}{11}\right) = 0$. So there are $\sum_z \left(1 + \left(\frac{z}{11}\right)\right) = 11$ affine points, and $\#E(\mathbb{F}_{11}) = 12 = p + 1$. The trace of Frobenius is 0, so the curve is supersingular at $p = 11$, as it is at $p = 5$ (Example 2.1). □

Hint for Exercise 2.6. On a group scheme killed by p^n, multiplication by an integer prime to p is invertible.

Solution to Exercise 2.6. Let $l = \deg f$, prime to p, and f' with $f \circ f' = [l]$ and $f' \circ f = [l]$. Since $X'[p^n]$ and $X[p^n]$ are killed by p^n and l is invertible modulo p^n, $[l]$ is an automorphism of both, with inverse $[l']$ for $ll' \equiv 1 \bmod p^n$. So $f[p^n] \colon X'[p^n] \to X[p^n]$ has the left inverse $[l]^{-1} \circ f'[p^n]$ and the right inverse $f'[p^n] \circ [l]^{-1}$, and is an isomorphism. These isomorphisms are compatible with the inclusions $X[p^n] \subseteq X[p^{n+1}]$, so $f[p^\infty]$ is an isomorphism. □

Hint for Exercise 2.7. Apply the ring homomorphism property to the product $x \cdot y$, a 0-cycle.

Solution to Exercise 2.7. Since sp is a ring homomorphism, $\mathrm{sp}\, x \cdot \mathrm{sp}\, y = \mathrm{sp}(x \cdot y)$, and since it preserves degrees of 0-cycles, $\deg(\mathrm{sp}\, x \cdot \mathrm{sp}\, y) = \deg \mathrm{sp}(x \cdot y) = \deg(x \cdot y)$. The compatibility with pull-backs is part of Fact 2.9(b); combined with the first statement it gives $\deg(\alpha_{\mathrm{sp}}^* \mathrm{sp}\, x \cdot \mathrm{sp}\, y) = \deg(\alpha^* x \cdot y)$, which is the form in which the specialization step uses it: intersection numbers of cycles and their translates by endomorphisms are the same on both fibers. □

Hint for Exercise 2.1. Compute $\alpha\alpha^\dagger$ from $\alpha^\dagger = \lambda - \alpha$.

Solution to Exercise 2.1. For $\alpha \in \mathbb{Q}$ there is nothing to show. For $\alpha \notin \mathbb{Q}$, $\lambda = \alpha + \alpha^\dagger$ and $\lambda' = \alpha\alpha^\dagger$ are fixed by $\dagger$ (for λ' because $(\alpha\alpha^\dagger)^\dagger = \alpha^{\dagger\dagger}\alpha^\dagger = \alpha\alpha^\dagger$), so they are rational. Then $\alpha^\dagger = \lambda - \alpha$ and $\lambda' = \alpha(\lambda - \alpha)$, so $\alpha^2 - \lambda\alpha + \lambda' = 0$. Since $\alpha \notin \mathbb{Q}$ and α is quadratic over $\mathbb{Q}$, its minimal polynomial over $\mathbb{Q}$ has degree 2, so every monic quadratic polynomial over $\mathbb{Q}$ that vanishes at α equals it; it is the reduced characteristic polynomial $x^2 - \mathrm{trd}(\alpha)x + \mathrm{nrd}(\alpha)$. So $\lambda = \mathrm{trd}(\alpha)$ and $\alpha^\dagger = \mathrm{trd}(\alpha) - \alpha = \bar{\alpha}$. □

Chapter 3

Hint for Exercise 3.1. Modulo p, σ is the p-th power map. For the correction, expand $\sigma(x_1 + pz)$ and compare the coefficients of p.

Solution to Exercise 3.1. Modulo p the equation reads $\bar{x}^p = \bar{\lambda}\bar{x}$, with the solution $\bar{x} = 0$ and the $p-1$ solutions of $\bar{x}^{p-1} = \bar{\lambda}$ in $\bar{\mathbb{F}}_p$. Let $x_1 \in W$ reduce to one of the nonzero solutions, and write $\sigma(x_1) = \lambda x_1 + py$. For $x = x_1 + pz$,

$$\sigma(x) - \lambda x = p\big(y + \sigma(z) - \lambda z\big),$$

so x solves the equation modulo p^2 if and only if $\bar{z}^p - \bar{\lambda}\bar{z} + \bar{y} = 0$, an equation of degree p in $\bar{z}$ with p solutions in $\bar{\mathbb{F}}_p$ (it is separable, its derivative being $-\bar{\lambda} \neq 0$). Repeating the step gives a solution in W, as in the rank-1 case of Lemma 3.5. For $\lambda = -1$ the nonzero solutions modulo p are the $\bar{x}$ with $\bar{x}^{p-1} = -1$; one of them is the reduction of $\sqrt{\xi}$, since $\sqrt{\xi}^{p-1} = \xi^{(p-1)/2} \equiv -1$, and the others are its multiples by $\mathbb{F}_p^\times$. The solutions in W are the $\lambda'\sqrt{\xi}$ with $\lambda' \in \mathbb{Z}_p$, as in Example 3.3. □

Hint for Exercise 3.2. The map σ^{-1} fixes p, and $p\gamma^{-1}$ is integral by assumption. For the dimension, use the elementary divisors of γ.

Solution to Exercise 3.2. From $F(x) = \gamma\sigma(x)$ we get $F^{-1}(y) = \sigma^{-1}(\gamma^{-1}y)$ on $M \otimes \mathbb{Q}$, so $V(y) = pF^{-1}(y) = \sigma^{-1}(p\gamma^{-1}y)$, which maps M into M because $p\gamma^{-1}$ is integral. Then $FV(y) = \gamma\sigma\sigma^{-1}(p\gamma^{-1}y) = py$ and $VF(x) = \sigma^{-1}(p\gamma^{-1}\gamma\sigma(x)) = px$. Since σ is bijective, $FM = \gamma M$, and $M/\gamma M$ has length $v_p(\det\gamma)$ by the elementary divisor theorem; this is the dimension. For $\gamma = A$ see Example 3.4. For $\gamma = \mathrm{diag}(1, p)$: $F(\lambda e_0 + \lambda' e_1) = \sigma(\lambda)e_0 + p\sigma(\lambda')e_1$, so $\ker(F \bmod p)$ is spanned by e_1; and $V(\lambda e_0 + \lambda' e_1) = p\sigma^{-1}(\lambda)e_0 + \sigma^{-1}(\lambda')e_1$, so VM/pM is spanned by e_1 as well. □

Hint for Exercise 3.3. Every maximal block of 1s, read cyclically, ends with exactly one transition 10.

Solution to Exercise 3.3. A balanced word contains a 0, so every maximal cyclic block of 1s is followed by a 0, and each occurrence of 10 is the end of exactly one block. So the a-number is the number of blocks. The words 00101011, 00100111, 00011011 and 01010101 have 3, 2, 2 and 4 blocks of 1s: for the first, the blocks are the single 1s at the third and fifth positions and the pair 11 at the end, which is followed cyclically by the initial 0. □

Hint for Exercise 3.4. Exchange 0 and 1, then rotate. Rotations preserve the multiset of lengths of blocks of 0s.

Solution to Exercise 3.4. The complement of 00101011 is 11010100; its longest block of 0s is the final 00, and the rotation starting there is 00110101. The complement of 00100111 is 11011000, whose rotation starting with the block 000 is 00011011. Neither word is isomorphic to its dual by a rotation: 00100111 has no block of three 0s while 00011011 has one; and 00101011 and 00110101 both have a single block 00, but the rotations beginning with it are the different words 00101011 and 00110101. Both pairs reappear in Chapter 15, among the four dual pairs of non-self-dual modules there. □

Hint for Exercise 3.5. Follow a basis vector around its cycle. For the slopes, compare the growth of the p-adic valuation of $F^j x$ with that on a simple isocrystal $I_{l/n}$.

Solution to Exercise 3.5. Going once around the cycle, $F^n e_i = p^{w_i+w_{i+1}+\cdots+w_{i+n-1}} e_i = p^l e_i$, and F^n is σ^n-semilinear, so $F^n = p^l\sigma^n$ in the basis (e_i). Let $L = M_w$ and, for $x \neq 0$ in $M_w \otimes \mathbb{Q}$, let $\operatorname{ord}_L(x)$ be the largest j with $x \in p^j L$. Then $\operatorname{ord}_L(F^{nj}x) = \operatorname{ord}_L(x) + lj$ exactly, so $\operatorname{ord}_L(F^i x)/i \to l/n$ for every $x \neq 0$. On a summand $I_{l'/n'}$ of the Dieudonné–Manin decomposition the same ratio tends to l'/n', because $F^{n'} = p^{l'}\sigma^{n'}$ there and any two lattices are commensurable. So every slope equals l/n; for a balanced word $l/n = \frac{1}{2}$. □

Hint for Exercise 3.6. As in Example 3.6, a fixed vector is determined by its first coordinate, which must be fixed by σ^3.

Solution to Exercise 3.6. Here $\Phi(x_1, x_2, x_3) = (\sigma x_3, \sigma x_1, \sigma x_2)$, so a fixed vector satisfies $x_2 = \sigma(x_1)$, $x_3 = \sigma(x_2) = \sigma^2(x_1)$ and $x_1 = \sigma(x_3) = \sigma^3(x_1)$. Hence $(W^3)^\Phi = \{(x, \sigma x, \sigma^2 x) : x \in \mathbb{Z}_{p^3}\}$, a free $\mathbb{Z}_p$-module of rank 3; a basis is given by $(\lambda_j, \sigma\lambda_j, \sigma^2\lambda_j)$ for a $\mathbb{Z}_p$-basis $\lambda_1, \lambda_2, \lambda_3$ of $\mathbb{Z}_{p^3}$. These vectors form a basis of W^3 for every p: the determinant $\det(\sigma^i\lambda_j)$ squared is the discriminant of $\mathbb{Z}_{p^3}$ over $\mathbb{Z}_p$, which is a unit because $\mathbb{Z}_{p^3}$ is unramified. By Lemma 3.5 this had to happen. □

Hint for Exercise 3.7. On (W, σ), $V = p\sigma^{-1}$; on $(W, p\sigma)$, $V = \sigma^{-1}$. Compute $F^\vee = \sigma \circ (\cdot) \circ V$ on the dual basis.

Solution to Exercise 3.7. Let $M = We$ with $Fe = e$, so $Ve = pe$, and let $e^\vee$ be the dual basis vector. Then $(F^\vee e^\vee)(e) = \sigma(e^\vee(Ve)) = p$, so $F^\vee e^\vee = pe^\vee$ and $M^\vee \cong (W, p\sigma)$. In the same way the dual of $(W, p\sigma)$, where $Ve = e$, has $F^\vee e^\vee = e^\vee$. The module $(W, \sigma) \oplus (W, p\sigma)$ is therefore isomorphic to its dual, the two summands being exchanged. Its a-number is $\dim M/(FM + VM) = 0$, since FM contains the first basis vector and VM the second. □

Chapter 4

Hint for Exercise 4.1. Two non-squares modulo p differ by a square. For the trace, apply $\int Fz = p\sigma(\int z)$ to $z = e_0 \wedge e_1$.

Solution to Exercise 4.1. If ξ' is another unit that is not a square modulo p, then ξ'/ξ is a square modulo p, hence, by Hensel's lemma, the square of a unit $\lambda \in \mathbb{Z}_p^\times$. So $\sqrt{\xi'} = \pm\lambda\sqrt{\xi}$, and $\mathbb{Z}_p\sqrt{\xi'}e_0 \wedge e_1 = \mathbb{Z}_p\sqrt{\xi}e_0 \wedge e_1$. Let $\lambda' = \int e_0 \wedge e_1$, a unit of W because $\int$ is an isomorphism $\bigwedge^2 M(E_0) \to W$. From $F(e_0 \wedge e_1) = -pe_0 \wedge e_1$ and $\int Fz = p\sigma(\int z)$ we get $-p\lambda' = p\sigma(\lambda')$, so $\sigma(\lambda') = -\lambda'$ and $\lambda' = \lambda_0\sqrt{\xi}$ with $\lambda_0 \in \mathbb{Z}_p$, a unit since λ' is. Then $\int \sqrt{\xi}e_0 \wedge e_1 = \lambda_0\xi \in \mathbb{Z}_p^\times$. The class of a point lies in $T^2(E_0)$ by Fact 4.6 and has trace 1, so it is a unit multiple of the generator. □

Hint for Exercise 4.2. Use Proposition 4.4, and for T^8 the identity $\int Fz = p^4\sigma(\int z)$.

Solution to Exercise 4.2. The ranks are $\binom{8}{2} = 28$, $\binom{8}{4} = 70$, $\binom{8}{6} = 28$ and $\binom{8}{8} = 1$. The trace is an isomorphism $\bigwedge^8 M \to W$, and $z \in \bigwedge^8 M$ satisfies $Fz = p^4 z$ if and only if $p^4\sigma(\int z) = p^4 \int z$, that is, $\int z \in W^\sigma = \mathbb{Z}_p$. So $\int$ maps $T^8(X)$ bijectively onto $\mathbb{Z}_p$. □

Hint for Exercise 4.3. Look at what Fact 4.10(c) identifies T^2 with.

Solution to Exercise 4.3. By Fact 4.6, $\mathrm{Alg}^1(X) \subseteq T^2(X)$, and by Fact 4.10(c) the cycle class map $\mathrm{NS}(X) \otimes \mathbb{Z}_p \to T^2(X)$ is surjective, so $\mathrm{Alg}^1(X) = T^2(X)$. The algebraicity comes for free because classes of degree 2 are, through the identification of $\bigwedge^2 M(X)$ with alternating maps between Dieudonné modules, the same as symmetric homomorphisms between the Dieudonné modules of $X^\vee$ and X. Fact 4.10 says that these come from homomorphisms $X \to X^\vee$ of abelian varieties, and the symmetric homomorphisms $X \to X^\vee$ are exactly the $\mathrm{pol}_{\mathscr{L}}$ of line bundles. In degree 4 nothing of this kind is available: a class in $\bigwedge^4 M(X)$ is not a homomorphism between Dieudonné modules of abelian varieties, and the products of degree-2 classes only give $S(X)$, which can be strictly smaller than $T^4(X)$, as it is for the model (Proposition 8.2). □

Hint for Exercise 4.4. A basis vector of degree $2i$ is a product of i basis vectors of degree 2.

Solution to Exercise 4.4. For a basis $e_1, \dots, e_n$, $e_{j_1} \wedge \cdots \wedge e_{j_{2i}} = (e_{j_1} \wedge e_{j_2}) \wedge \cdots \wedge (e_{j_{2i-1}} \wedge e_{j_{2i}})$, so the products of degree-2 elements span every even degree. For $x = e_1 \wedge e_2 + e_3 \wedge e_4$, $x \wedge x = e_1 \wedge e_2 \wedge e_3 \wedge e_4 + e_3 \wedge e_4 \wedge e_1 \wedge e_2 = 2e_1 \wedge e_2 \wedge e_3 \wedge e_4$, since moving $e_3 \wedge e_4$ past $e_1 \wedge e_2$ is an even permutation; the squares $(e_1 \wedge e_2)^{\wedge 2}$ vanish. □

Hint for Exercise 4.5. The index of the span of $(1,0)$ and $(1,p)$ is the absolute value of the determinant of the matrix with these columns.

Solution to Exercise 4.5. The matrix with columns $(1,0)$, $(1,p)$ has determinant p, so $[L : L'] = p$. With $\langle x, y\rangle = x_1y_2 + x_2y_1$: $\langle (1,0),(1,0)\rangle = 0$, $\langle (1,0),(1,p)\rangle = p$, $\langle (1,p),(1,p)\rangle = 2p$. So $\operatorname{disc} L' = \det \left(\begin{smallmatrix} 0 & p \\ p & 2p \end{smallmatrix}\right) = -p^2$, while $\operatorname{disc} L = -1$, and $-p^2 = p^2 \cdot (-1)$, as Lemma 4.13 says. In general $v_p(\operatorname{disc} L') = 2 + v_p(\operatorname{disc} L) \geq 2$ for a sublattice of index p, since $v_p(\operatorname{disc} L) \geq 0$ for a $\mathbb{Z}_p$-valued form; so no such sublattice has unit discriminant. □

Chapter 5

Hint for Exercise 5.1. Intersections take componentwise maxima of exponents, sums take minima.

Solution to Exercise 5.1. The exponent vectors are $(1,0,2)$ and $(0,3,1)$. So $L_1 \cap L_2 = pW \oplus p^3W \oplus p^2W$, with exponents $(1,3,2)$, and $L_1 + L_2 = W \oplus W \oplus pW$, with exponents $(0,0,1)$. The length of $(L_1+L_2)/L_1$ is $(1-0)+(0-0)+(2-1) = 2$, and that of $L_2/(L_1 \cap L_2)$ is $(1-0)+(3-3)+(2-1) = 2$. In general both lengths equal $\sum_s \max(0, n_s - n'_s)$ for exponent vectors n of L_1 and n' of L_2: the first is $\sum_s (n_s - \min(n_s, n'_s))$ and the second $\sum_s (\max(n_s, n'_s) - n'_s)$. □

Hint for Exercise 5.2. The sum $\sum_{i=1}^{j} (w(\pi^{-i}J_{i'}) - \frac{n}{2})$ is a difference of two partial sums $\widetilde{n}$.

Solution to Exercise 5.2. Extend $\widetilde{n}_{i'}$ to all integers i' by periodicity, which is consistent because $\widetilde{n}_l = 0$. Then $\sum_{i=1}^{j} (w(J_{i'-i}) - \frac{n}{2}) = \widetilde{n}_{i'} - \widetilde{n}_{i'-j}$, and as j runs over $0, \dots, q-1$, which contains a full period since $l \mid q$, $i'-j$ runs over all residues modulo l. So (5.1) gives $n_{J_{i'}} = \max_{j'}(\widetilde{n}_{i'} - \widetilde{n}_{j'}) = \widetilde{n}_{i'} - \min_{j'} \widetilde{n}_{j'}$. Then $n_{J_{i'+1}} - n_{J_{i'}} = \widetilde{n}_{i'+1} - \widetilde{n}_{i'} = w(J_{i'}) - \frac{n}{2}$. □

Hint for Exercise 5.3. There are two orbits of 2-sets, one of length 4 and one of length 2.

Solution to Exercise 5.3. The orbit $\{0,1\} \to \{1,2\} \to \{2,3\} \to \{3,0\}$ was treated in Example 5.5: exponents $1,0,0,1$. The other orbit is $\{0,2\} \to \{1,3\} \to \{0,2\}$, with $w(\{0,2\}) = w(\{1,3\}) = 1$, so both steps are 0 and both exponents are 0. The six exponents are $n_{\{0,1\}} = 1$, $n_{\{1,2\}} = 0$, $n_{\{2,3\}} = 0$, $n_{\{0,3\}} = 1$, $n_{\{0,2\}} = 0$, $n_{\{1,3\}} = 0$, with sum 2, and each orbit contains an exponent 0. □

Hint for Exercise 5.4. List the predecessors $\pi^{-1}J', \pi^{-2}J', \dots$ of each 2-set J', write down $w-1$ for each, and take the largest partial sum.

Solution to Exercise 5.4. The word is $w = (0,0,1,0,1,1)$ and $\pi(i) = i+1$ modulo 6. For $J = \{0,1,2,4\}$ the predecessors $\pi^{-1}J, \dots, \pi^{-5}J$ are $\{5,0,1,3\}$, $\{4,5,0,2\}$, $\{3,4,5,1\}$, $\{2,3,4,0\}$, $\{1,2,3,5\}$, with weights $1,3,2,2,2$, so the steps $w-2$ are $-1,+1,0,0,0$, the partial sums are $-1,0,0,0,0$, and $n_J = 0$. For the 2-sets, the steps $w-1$ along the predecessors are:

J'	steps $w(\pi^{-i}J') - 1$, $i = 1, \dots, 5$	$n_{J'}$
$\{0,1\}$	$0,+1,0,0,0$	1
$\{2,4\}$	$-1,0,0,0,0$	0
$\{0,2\}$	$0,0,0,+1,-1$	1
$\{1,4\}$	$-1,+1,0,-1,+1$	0
$\{0,4\}$	$0,+1,-1,0,0$	1
$\{1,2\}$	$-1,0,+1,0,0$	0

For instance the predecessors of $\{0,1\}$ are $\{5,0\}$, $\{4,5\}$, $\{3,4\}$, $\{2,3\}$, $\{1,2\}$, with weights $1,2,1,1,1$. So each of the three splittings has $n_{J_1}+n_{J_2}=1$, and $n_J^S=1>0=n_J$. □

Hint for Exercise 5.5. Use Lemma 5.2 for the index, and for the second statement compare $p(L\otimes W)$ with $L'\otimes W$.

Solution to Exercise 5.5. By Lemma 5.2, $[L:L']$ is p to the length of $L(n)/L(n')$, which is $\sum_s(n'_s-n_s)$. If all differences are at most 1, then $pL(n)=L(n+1)\subseteq L(n')$, so $pL\subseteq L\cap(L'\otimes W)=L'$, again by Lemma 5.2. □

Hint for Exercise 5.6. Take a single endomorphism and its integer multiples.

Solution to Exercise 5.6. Expanding, $\bigwedge^2(\alpha_1+\alpha_2)(x_1\wedge x_2)=(\alpha_1+\alpha_2)x_1\wedge(\alpha_1+\alpha_2)x_2$ is the sum of $\alpha_1x_1\wedge\alpha_1x_2$, $\alpha_2x_1\wedge\alpha_2x_2$ and $\alpha_1x_1\wedge\alpha_2x_2+\alpha_2x_1\wedge\alpha_1x_2=D(\alpha_1,\alpha_2)(x_1\wedge x_2)$, and $D(\alpha,\alpha)=2\bigwedge^2\alpha$. Let $\mathcal{R}=\mathbb{Z}\cdot\mathrm{id}$ on $\mathbb{Z}^2$ and $x=e_1\wedge e_2$. Then $\bigwedge^2(n\,\mathrm{id})(x)=n^2x$, whose span over $n\in\mathbb{Z}$ is $\mathbb{Z}x$, while $D(n\,\mathrm{id},n'\,\mathrm{id})(x)=2nn'x$ spans only $2\mathbb{Z}x$. Over $\mathbb{Z}_p$ with p odd, $\bigwedge^2\alpha(x)=\frac{1}{2}D(\alpha,\alpha)(x)$ lies in the span of the D-values, and the D-values lie in the span of the $\bigwedge^2$-values by the first identity, so the spans agree. □

Chapter 6

Hint for Exercise 6.1. Apply $\gamma_1\otimes\gamma_2\otimes\gamma_3$ to decomposable tensors $x_1\otimes x_2\otimes x_3$.

Solution to Exercise 6.1. If $\gamma_i=\lambda_i\cdot 1$ with $\lambda_1\lambda_2\lambda_3=1$, then $\gamma_1\otimes\gamma_2\otimes\gamma_3=\lambda_1\lambda_2\lambda_3=1$. Conversely, suppose $\gamma_1\otimes\gamma_2\otimes\gamma_3=1$. For nonzero $x_i\in U_i$, $\gamma_1x_1\otimes\gamma_2x_2\otimes\gamma_3x_3=x_1\otimes x_2\otimes x_3$, and two nonzero decomposable tensors are equal only if their factors are proportional, so γ_1x_1 is a multiple of x_1 for every x_1. A linear map for which every vector is an eigenvector is a scalar, so $\gamma_1=\lambda_1$, and likewise $\gamma_2=\lambda_2$, $\gamma_3=\lambda_3$, with $\lambda_1\lambda_2\lambda_3=1$. The kernel is $\{(\lambda_1,\lambda_2,\lambda_3)\in\mathbb{G}_m^3:\lambda_1\lambda_2\lambda_3=1\}$, isomorphic to $\mathbb{G}_m^2$ by $(\lambda_1,\lambda_2)\mapsto(\lambda_1,\lambda_2,(\lambda_1\lambda_2)^{-1})$, a split torus of dimension 2. □

Hint for Exercise 6.2. A central simple algebra over $\mathbb{Q}$ is a matrix algebra exactly when all its local invariants vanish.

Solution to Exercise 6.2. The invariant of B at a place v' of k is $\frac{1}{2}$ for $v'\in\mathrm{Ram}(B)$ and 0 otherwise, so the invariant of $\mathrm{Cor}_{k/\mathbb{Q}}B$ at v is $\frac{1}{2}$ times the number of places of $\mathrm{Ram}(B)$ above v, modulo 1. It vanishes exactly when that number is even, and $\mathrm{Cor}_{k/\mathbb{Q}}B\cong\mathrm{Mat}_8(\mathbb{Q})$ exactly when it vanishes at every v. For $\mathrm{Ram}(B)=\{\infty_2,\infty_3\}$ there are two places above ∞ and none above any prime. For an example with finite places, take a prime ℓ that has at least two places v_1,v_2 of k above it of which no third lies in $\mathrm{Ram}(B)$, for instance a prime with $\ell=\mathfrak{p}_1\mathfrak{p}_2$, and $\mathrm{Ram}(B)=\{\infty_2,\infty_3,v_1,v_2\}$; it has even cardinality, so B exists (see e.g. [Voi21, Main Theorem 14.6.1]). □

Hint for Exercise 6.3. The weights are $n_0+\epsilon_1n_1+\epsilon_2n_2+\epsilon_3n_3$, $\epsilon_i=\pm1$. If two of the n_i are positive, find three distinct values.

Solution to Exercise 6.3. If $n_1=n_2=n_3=0$ there is one value. If exactly one, say n_1, is positive, the values are $n_0\pm n_1$, four times each, and they differ by 1 exactly when $n_1=\frac{1}{2}$. If $n_1,n_2>0$, put $x=n_1+n_2+n_3$ and $z=n_1-n_2+n_3$. Then n_0+x, n_0-x and n_0+z are values, with $z<x$ because $n_2>0$ and $z>-x$ because $z+x=2n_1+2n_3>0$; three values are too many. For Mumford's $\mathbf{h}$ the non-trivial factor is the one of ∞_1, since $\mathbf{h}$ is trivial in the two compact factors. □

Hint for Exercise 6.4. In slot i the upper unipotent matrix acts as $1+x^{p^{i-1}}\mathsf{N}_i$; expand the product of the three. For (c), O_k/p is a product of finite fields.

Solution to Exercise 6.4. (a) In slot i, $\left(\begin{smallmatrix}1&x\\0&1\end{smallmatrix}\right)^{(p^{i-1})}=1+x^{p^{i-1}}\mathsf{N}_i$, and the tensor product of the three is $\prod_i(1+x^{p^{i-1}}\mathsf{N}_i)=\sum_J x^{l_J}\mathsf{N}_J$. The l_J are sums of distinct elements of $\{1,p,p^2\}$, so they are distinct by uniqueness of base-p expansions, and $l_J\le 1+p+p^2<p^3$. (b) For $y\in\mathcal{U}$ the vectors $\sum_J x^{l_J}\mathsf{N}_Jy$, $x\in\mathbb{F}_{p^3}$, lie in $\mathcal{U}$. The eight functions $x\mapsto x^{l_J}$ on $\mathbb{F}_{p^3}$ are linearly

independent, since a nontrivial combination is a nonzero polynomial of degree less than p^3. So for each J_0 there are coefficients λ_x with $\sum_x \lambda_x x^{l_J} = 1$ for $J = J_0$ and 0 otherwise, and $\mathsf{N}_{J_0} y = \sum_x \lambda_x \sum_J x^{l_J} \mathsf{N}_J y \in \mathcal{U}$. If $y \in \mathcal{U}$ is nonzero, choose J maximal with $\mathsf{N}_J y \neq 0$. Then $y' = \mathsf{N}_J y \in \mathcal{U}$ is nonzero and $\mathsf{N}_i y' = 0$ for every i, for $i \in J$ because $\mathsf{N}_i^2 = 0$ and for $i \notin J$ by maximality. The common kernel of $\mathsf{N}_1, \mathsf{N}_2, \mathsf{N}_3$ is the line of e^{+++}, so $e^{+++} \in \mathcal{U}$. The lower unipotent matrices give in the same way the maps N_J^-, with $\mathsf{N}_i^- : e^+ \mapsto e^-$ in slot i, and $\mathsf{N}_J^- e^{+++}$ is the e^ϵ with $\epsilon_i = -$ exactly for $i \in J$. So $\mathcal{U}$ contains every e^ϵ. (c) The upper unipotent matrix with entry $x \in O_k/p$ acts as $\sum_J \left(\prod_{i\in J} \bar{\tau}_i(x)\right)\mathsf{N}_J$, with $\bar{\tau}_i$ the reductions of the τ_i, and the argument of (b) needs only that the eight functions $x \mapsto \prod_{i\in J} \bar{\tau}_i(x)$ are linearly independent. If p splits completely, $O_k/p = \mathbb{F}_p^3$, $\bar{\tau}_i(x) = x_i$, and the functions are the monomials $\prod_{i\in J} x_i$. If $p = \mathfrak{p}_1\mathfrak{p}_2$ with residue degrees 1 and 2, $O_k/p = \mathbb{F}_p \times \mathbb{F}_{p^2}$, and with $\bar{\tau}_1$ factoring through $\mathbb{F}_p$ the functions are $x_1^i y^{j+pl}$, $i, j, l \in \{0, 1\}$, with distinct exponents. In both cases they are distinct monomials of degree less than p in the variables over $\mathbb{F}_p$ and less than p^2 in the variable over $\mathbb{F}_{p^2}$, and a nonzero polynomial with these degree bounds does not vanish on all of O_k/p. So they are linearly independent. □

Hint for Exercise 6.5. The eight characters $\lambda_1^{\pm1}\lambda_2^{\pm1}\lambda_3^{\pm1}$ of $(\bar{\mathbb{F}}_p^\times)^3$ are distinct, so a torus-stable subspace is a sum of weight lines. Unipotent elements move one sign at a time.

Solution to Exercise 6.5. Let $\mathcal{U}$ be a nonzero invariant subspace. It is stable under the diagonal torus, whose eight characters on the lines $\bar{\mathbb{F}}_p e^\epsilon$ are distinct, so $\mathcal{U}$ is the sum of the lines it contains, and it contains some e^ϵ. Write $e_i^+ = (1, 0)$, $e_i^- = (0, 1)$. The matrix $\left(\begin{smallmatrix} 1 & 0 \\ x & 1 \end{smallmatrix}\right)$ in slot i maps e_i^+ to $e_i^+ + xe_i^-$ and fixes e_i^-; applied to e^ϵ with $\epsilon_i = +$ it gives $e^\epsilon + xe^{\epsilon'}$, where ϵ' differs from ϵ in slot i. Since $\mathcal{U}$ is a sum of weight lines, $e^{\epsilon'} \in \mathcal{U}$. Repeating, $e^{---} \in \mathcal{U}$, and with the upper unipotent matrices in the same way every $e^\epsilon \in \mathcal{U}$. So $\mathcal{U}$ is everything. □

Hint for Exercise 6.7. Evaluate the cubics at all residues and use the discriminant formula $-4\lambda_1^3 - 27\lambda_0^2$.

Solution to Exercise 6.7. For $x^3 - 4x + 1$ the values at $0, \dots, 4$ are $1, 3, 1, 1, 4$ modulo 5, the discriminant is $229 > 0$, and $5 \nmid 229$. For $x^3 - 3x + 1$ the discriminant is $-4(-27) - 27 = 81 > 0$, so it has three real roots, and its values at $0, \dots, 6$ are $1, 6, 3, 5, 4, 6, 3$ modulo 7, none zero; since $7 \nmid 81$, 7 is inert in $\mathbb{Q}[x]/(x^3 - 3x + 1)$. The cubic $x^3 - 4x + 1$ does not work at 7 because $4^3 - 16 + 1 = 49 \equiv 0$, so it has a root modulo 7 and 7 is not inert. □

Hint for Exercise 6.6. Expand $N(u + v + w)$ into the 27 products $a_1 \otimes a_2 \otimes a_3$ with each $a_i \in \{u_i, v_i, w_i\}$.

Solution to Exercise 6.6. Expanding as in the hint and doing the same for the other six terms, inclusion and exclusion leaves exactly the products in which each of u, v, w contributes one factor: $T(u, v, w) = \sum_\pi a_1^\pi \otimes a_2^\pi \otimes a_3^\pi$, the sum over the six bijections π from $\{u, v, w\}$ to the three slots. This is W-linear in each argument and symmetric, and for $u = v = w$ it is $6N(u)$. For $u = (x_1, 0, 0)$, $v = (0, x_2, 0)$, $w = (0, 0, x_3)$ only the bijection that puts u in slot 1, v in slot 2 and w in slot 3 gives a nonzero term, namely $x_1 \otimes x_2 \otimes x_3$. By the defining formula, $T(\mathcal{O}, \mathcal{O}, \mathcal{O})$ lies in the $\mathbb{Z}$-span of $N(\mathcal{O})$. By trilinearity, the W-span of $T(\mathcal{O}, \mathcal{O}, \mathcal{O})$ contains $T(u, v, w)$ for all u, v, w in the W-span $\mathrm{Mat}_2(W)^3$ of $\mathcal{O}$, in particular every $x_1 \otimes x_2 \otimes x_3$. □

Chapter 7

Hint for Exercise 7.1. A tensor product of diagonal matrices is diagonal, and multiplying by invertible matrices over W does not change elementary divisors.

Solution to Exercise 7.1. On $e_{s_1} \otimes e_{s_2} \otimes e_{s_3}$ the matrix $\bigotimes_i \mathrm{diag}(p^{n_i}, p^{n_i'})$ acts by $p^{l_1+l_2+l_3}$ with $l_i = n_i$ if $s_i = 0$ and $l_i = n_i'$ if $s_i = 1$, so its elementary divisors are these eight powers of p. Since $\beta_1 \otimes \beta_2 \otimes \beta_3 = (\gamma_1' \otimes \gamma_2' \otimes \gamma_3')(\bigotimes_i \mathrm{diag}(p^{n_i}, p^{n_i'}))(\gamma_1'' \otimes \gamma_2'' \otimes \gamma_3'')$ and $\gamma_1' \otimes \gamma_2' \otimes \gamma_3'$, $\gamma_1'' \otimes \gamma_2'' \otimes \gamma_3''$ lie in $\mathrm{GL}_8(W)$, the elementary divisors are the same. □

Hint for Exercise 7.2. $\varsigma^{-1}(y_1 \otimes y_2 \otimes y_3) = \sigma^{-1}y_2 \otimes \sigma^{-1}y_3 \otimes \sigma^{-1}y_1$.

Solution to Exercise 7.2. Applying ς^{-1}, then γ, then ς to $y_1 \otimes y_2 \otimes y_3$ gives $\gamma_1\sigma^{-1}y_2 \otimes \gamma_2\sigma^{-1}y_3 \otimes \gamma_3\sigma^{-1}y_1$ and then $\sigma(\gamma_3)y_1 \otimes \sigma(\gamma_1)y_2 \otimes \sigma(\gamma_2)y_3$. So $\varsigma\gamma\varsigma^{-1} = \sigma(\gamma_3) \otimes \sigma(\gamma_1) \otimes \sigma(\gamma_2)$, and $\gamma F\gamma^{-1} = \gamma\beta\varsigma\gamma^{-1}\varsigma^{-1}\varsigma = \gamma\beta(\varsigma\gamma\varsigma^{-1})^{-1}\varsigma$, whose slot components are $\gamma_i\beta_i\sigma(\gamma_{i-1})^{-1}$. □

Hint for Exercise 7.3. Apply $F(x \otimes y \otimes z) = \sigma z \otimes \beta_2\sigma x \otimes \sigma y$ three times. For $\beta_2 = A$, $\sigma^j(A) = A$.

Solution to Exercise 7.3. $F^2(x) = \sigma^2 x_2 \otimes \beta_2\sigma^2 x_3 \otimes \sigma(\beta_2)\sigma^2 x_1$, and applying F once more gives $\sigma^2(\beta_2)\sigma^3 x_1 \otimes \beta_2\sigma^3 x_2 \otimes \sigma(\beta_2)\sigma^3 x_3$, which is (7.3). For $\beta_2 = A$ this is $F^3 = (A \otimes A \otimes A)\sigma^3$, and $Ae_s = p^s e_{1-s}$, so $F^3 e_s = p^{s_1+s_2+s_3} e_{(1-s_1,1-s_2,1-s_3)}$. In Example 7.1, $F^3 e_{000} = e_{111}$ and $F^3 e_{111} = p^3 e_{000}$, as predicted. □

Hint for Exercise 7.4. The slopes of F^3 are the sums of one slope per slot; count how many slots carry $1-u$.

Solution to Exercise 7.4. If j slots carry $1-u$ and $3-j$ carry u, the sum is $3u + j(1-2u)$, which is $3u$, $1+u$, $2-u$, $3-3u$ for $j = 0, 1, 2, 3$, with $\binom{3}{j} = 1, 3, 3, 1$ choices. Dividing by 3 gives (7.4). The sum of all eight slopes is $\frac{1}{3}(3u + 3(1+u) + 3(2-u) + 3 - 3u) = 4$. □

Hint for Exercise 7.5. Here $Fe_s = p^{s_3} e_{(1-s_3,s_1,s_2)}$. Relabel the slots cyclically.

Solution to Exercise 7.5. Starting from e_{000}: $e_{000} \mapsto e_{100} \mapsto e_{110} \mapsto e_{111} \mapsto pe_{011} \mapsto p^2 e_{001} \mapsto p^3 e_{000}$, with letters 000111, and $e_{010} \mapsto e_{101} \mapsto pe_{010}$, with word 01. The cyclic relabeling $x_1 \otimes x_2 \otimes x_3 \mapsto x_3 \otimes x_1 \otimes x_2$ conjugates this Frobenius into $\sigma y_3 \otimes A\sigma y_1 \otimes \sigma y_2$, so the module is isomorphic to $\mathbb{M}$. As for $\mathbb{M}$, F modulo p has image spanned by the e_s with $s_1 = 1$, V modulo p has image spanned by the e_s with $s_3 = 1$, two vectors e_{000}, e_{010} are missing, and the a-number is 2. □

Chapter 8

Hint for Exercise 8.1. Apply $\pi(s_1, s_2, s_3) = (s_3, 1 - s_1, s_2)$ three times to a general vertex.

Solution to Exercise 8.1. For instance $\pi(000) = (0, 1, 0) = 010$, $\pi(010) = 011$, $\pi(011) = 111$, $\pi(111) = 101$, $\pi(101) = 100$, $\pi(100) = 000$, and $\pi(001) = 110$, $\pi(110) = 001$, which is the table and the two orbits; reading s_1 along them gives 000111 and 01. Since $F^6 e_s$ is e_s times p to the sum of s_1 over six steps of π, which is 3 on the orbit of length 6 and $3 \cdot 1$ on the orbit of length 2, $F^6 = p^3\sigma^6$. The orbits have lengths 6 and 2, so no vertex is fixed. Finally $\pi^2(s) = \pi(s_3, 1 - s_1, s_2) = (s_2, 1 - s_3, 1 - s_1)$ and $\pi^3(s) = \pi(s_2, 1 - s_3, 1 - s_1) = (1 - s_1, 1 - s_2, 1 - s_3)$ for every s. □

Hint for Exercise 8.2. Use the table of π.

Solution to Exercise 8.2. By the table of π, the images of the vertices $000, 011, 101, 110$ of T_+ are $010, 111, 100, 001$, so $\pi(\mathsf{T}_+) = \mathsf{T}_-$, and the images of $001, 010, 100, 111$ are $110, 011, 000, 101$, so $\pi(\mathsf{T}_-) = \mathsf{T}_+$. Likewise π maps $000, 001, 011, 101$ to $010, 110, 111, 100$, so $\pi(\mathsf{M}_+) = \mathsf{M}_-$, and $010, 100, 110, 111$ to $011, 000, 001, 101$, so $\pi(\mathsf{M}_-) = \mathsf{M}_+$. The weights count the vertices with $s_1 = 1$: $w(\mathsf{T}_+) = |\{101, 110\}| = 2$, $w(\mathsf{T}_-) = |\{100, 111\}| = 2$, $w(\mathsf{M}_+) = |\{101\}| = 1$, $w(\mathsf{M}_-) = |\{100, 110, 111\}| = 3$. □

Hint for Exercise 8.3. All three 2-sets lie in the orbit of $\{000, 001\}$.

Solution to Exercise 8.3. The orbit is $\{000, 001\} \to \{010, 110\} \to \{011, 001\} \to \{111, 110\} \to \{101, 001\} \to \{100, 110\} \to \{000, 001\}$, with weights $0, 1, 0, 2, 1, 2$, steps $-1, 0, -1, +1, 0, +1$, partial sums $0, -1, -1, -2, -1, -1$ and minimum -2. So the exponents are $2, 1, 1, 0, 1, 1$; in particular $n_{\{000,001\}} = 2$, $n_{\{001,011\}} = 1$ and $n_{\{001,101\}} = 1$. The orbit of M_+ is $\{\mathsf{M}_+, \mathsf{M}_-\}$ with weights $1, 3$ (Exercise 8.2), steps $-1, +1$, partial sums $0, -1$, so $n_{\mathsf{M}_+} = 1$ and $n_{\mathsf{M}_-} = 0$. The three splittings of $\mathsf{M}_+ = \{000, 001, 011, 101\}$ give $n_{\{000,001\}} + n_{\{011,101\}} = 2 + 0$, $n_{\{000,011\}} + n_{\{001,101\}} = 1 + 1$ and $n_{\{000,101\}} + n_{\{001,011\}} = 1 + 1$, using the exponents computed in Section 8.4. So $n^S_{\mathsf{M}_+} = 2$, a defect of 1. □

Hint for Exercise 8.4. Compare $p(T^4 \otimes W)$ with $S \otimes W$ exponent by exponent, and use that a finite $\mathbb{Z}_p$-module is determined by its base change to W.

Solution to Exercise 8.4. If $n_J^S \le n_J + 1$ for all J, then $p(T^4 \otimes W)$, with exponents $n_J + 1$, lies in $S \otimes W$, so $pT^4 \subseteq S$ by Lemma 5.2. If the defects were $2, 1, 1, 0$, then $(T^4/S) \otimes W \cong W/p^2 \oplus W/p \oplus W/p$. Writing $T^4/S \cong \bigoplus_i \mathbb{Z}/p^{n_i}$ gives $(T^4/S) \otimes W \cong \bigoplus_i W/p^{n_i}$, and the elementary divisors of a finite W-module are unique, so $T^4/S \cong \mathbb{Z}/p^2 \oplus (\mathbb{Z}/p)^2$, of order p^4 but not killed by p. □

Hint for Exercise 8.5. The vertices with $s_1 = 1$ are $100, 101, 110, 111$.

Solution to Exercise 8.5. $\mathsf{T}_+ \cap \{s_1 = 1\} = \{101, 110\}$, $\mathsf{T}_- \cap \{s_1 = 1\} = \{100, 111\}$, $\mathsf{M}_+ \cap \{s_1 = 1\} = \{101\}$ and $\mathsf{M}_- \cap \{s_1 = 1\} = \{100, 110, 111\}$, so the counts are $2, 2, 1, 3$. The action with eigenset T_- has characters ι on T_- and $\bar{\iota}$ on T_+, which are the characters of the action with eigenset T_+ composed with the nontrivial automorphism of $\mathbb{Z}_{p^2}$; so it is that action precomposed with complex conjugation of K, and both have type $(2, 2)$. □

Hint for Exercise 8.6. Apply φ to $\lambda e_{\mathsf{T}_+} + \lambda' e_{\mathsf{T}_-}$ and compare coefficients.

Solution to Exercise 8.6. $\varphi(\lambda e_{\mathsf{T}_+} + \lambda' e_{\mathsf{T}_-}) = (-1)^{j_2}\sigma(\lambda')e_{\mathsf{T}_+} + (-1)^{j_1}\sigma(\lambda)e_{\mathsf{T}_-}$, so the vector is fixed if and only if $\lambda' = (-1)^{j_1}\sigma(\lambda)$ and $\lambda = (-1)^{j_2}\sigma(\lambda') = (-1)^{j_1+j_2}\sigma^2(\lambda)$. If $j_1 + j_2$ is even, the solutions are $\lambda \in W^{\sigma^2} = \mathbb{Z}_{p^2}$, a free $\mathbb{Z}_p$-module of rank 2. If it is odd, let $\xi' \in \mathbb{Z}_{p^2}$ be a unit that is not a square modulo p; its square root $\sqrt{\xi'}$ is a unit of $\mathbb{Z}_{p^4}$ with $\sigma^2(\sqrt{\xi'}) = -\sqrt{\xi'}$, and λ is a solution if and only if $\lambda/\sqrt{\xi'} \in \mathbb{Z}_{p^2}$, again a free module of rank 2. For the model, $F^6 = p^3\sigma^6$ in the cube basis (Section 8.2) gives $\varphi^6 = \sigma^6$, and since $\varphi^6(e_{\mathsf{T}_+}) = (-1)^{3(j_1+j_2)}e_{\mathsf{T}_+}$, this forces $j_1 + j_2$ to be even. So $\mathcal{L} = \{\lambda e_{\mathsf{T}_+} + (-1)^{j_1}\sigma(\lambda)e_{\mathsf{T}_-} : \lambda \in \mathbb{Z}_{p^2}\}$. □

Chapter 9

Hint for Exercise 9.1. Expand $(j\alpha_1 + \alpha_2)x_1 \wedge \cdots \wedge (j\alpha_1 + \alpha_2)x_4$ and sort the terms by the number of factors α_1.

Solution to Exercise 9.1. Each of the four factors contributes either $j\alpha_1 x_l$ or $\alpha_2 x_l$; the terms with α_1 in exactly i places carry j^i, and their sum is $D_i(\alpha_1, \alpha_2)(x_1 \wedge \cdots \wedge x_4)$. So $\bigwedge^4(j\alpha_1 + \alpha_2) = \sum_{i=0}^4 j^i D_i$. For $j = 0, \dots, 4$ this is a linear system with the Vandermonde matrix (j^i), whose determinant is $\prod_{0 \le j < j' \le 4}(j' - j) = (1\cdot2\cdot3\cdot4)(1\cdot2\cdot3)(1\cdot2)\cdot1 = 288 = 2^5 \cdot 3^2$. For $p \ge 5$ this is a unit at p, so each D_i is a $\mathbb{Z}_{(p)}$-combination of the five maps $\bigwedge^4(j\alpha_1 + \alpha_2)$. □

Hint for Exercise 9.2. Compare F applied to $\iota_s(\lambda)e_s$ with λ applied to Fe_s.

Solution to Exercise 9.2. For $\lambda \in \mathbb{Z}_{p^2}$, $F(\iota_s(\lambda)e_s) = \sigma(\iota_s(\lambda))p^{w(s)}e_{\pi(s)}$, while λ applied to Fe_s gives $\iota_{\pi(s)}(\lambda)p^{w(s)}e_{\pi(s)}$. So the action commutes with F if and only if $\iota_{\pi(s)} = \sigma \circ \iota_s = \bar{\iota}_s$ for all s, as in the proof of Lemma 8.4(i). Along an orbit the characters must then alternate, which is possible exactly when the orbit has even length; since every orbit of a monomial Dieudonné module is balanced, its length is even, and there are $2^{(\text{number of orbits})}$ such actions. □

Hint for Exercise 9.3. For $x = (y_0, y)$ with $y \ne 0$, first choose λ to fix the second coordinate, then γ to fix the first.

Solution to Exercise 9.3. Composing (λ', γ') after (λ, γ) gives $(y_0, y) \mapsto (\lambda'\lambda y_0 + (\lambda'\gamma + \gamma'\lambda)(y), \lambda'\lambda y)$, of the same form, and sums are of the same form too, so $\mathcal{R}$ is a ring. Clearly $\mathcal{R}$ maps $\mathcal{U}_0 = \{(y_0, 0)\}$ into itself. Let $x = (y_0, y)$ with $y \ne 0$ and let $(y_0', y') \in \mathcal{U}$. Choose $\lambda = y'/y \in \mathbb{F}_{p^2}$, and then an $\mathbb{F}_p$-linear γ with $\gamma(y) = y_0' - \lambda y_0$, which exists because $y \ne 0$. Then (λ, γ) maps x to (y_0', y'), so $\mathcal{R}x = \mathcal{U}$. If $\mathcal{U} = \mathcal{U}_0 \oplus \mathcal{U}_1$ with $\mathcal{U}_1$ stable under $\mathcal{R}$, then $\mathcal{U}_1 \ne 0$ contains some $x \notin \mathcal{U}_0$, so $\mathcal{U}_1 \supseteq \mathcal{R}x = \mathcal{U}$, a contradiction; so the extension does not split. Multiplication by $\lambda \in \mathbb{F}_{p^2}$ imitates the diagonal action of $\mathbb{Z}_{p^2}$, which moves within the

Weil coordinates, and γ imitates the endomorphisms that carry the Weil lattice $\mathcal{L}$ into the bottom layer N/S (Proposition 9.4(ii)). □

Hint for Exercise 9.4. The vector $\bigwedge^4 \mathrm{pr}_J(e_{J'})$ is the wedge of the $\mathrm{pr}_J e_s$, $s \in J'$.

Solution to Exercise 9.4. By definition $\bigwedge^4 \mathrm{pr}_J(e_{J'}) = \mathrm{pr}_J e_{s_1} \wedge \cdots \wedge \mathrm{pr}_J e_{s_4}$ for $J' = \{s_1, \dots, s_4\}$, which is $e_{J'}$ if every s_i lies in J, that is $J' = J$, and 0 otherwise because some factor vanishes. In the same way $\bigwedge^2 \mathrm{pr}_J$ is the coordinate projection of $\bigwedge^2 M$ onto the span of the six vectors $e_{J'}$ with $J' \subseteq J$, $|J'| = 2$. □

Hint for Exercise 9.5. The $(i, 4-i)$-component is $\bigwedge^i M \otimes \bigwedge^{4-i} M$.

Solution to Exercise 9.5. The ranks are $\binom{8}{i}\binom{8}{4-i}$: 70, $8 \cdot 56 = 448$, $28 \cdot 28 = 784$, 448, 70 for $i = 0, \dots, 4$, with sum $1820 = \binom{16}{4}$. □

Chapter 10

Hint for Exercise 10.1. The action of K preserves the Hodge decomposition, and complex conjugation on $H^1(X, \mathbb{C})$ exchanges the ι- and $\bar{\iota}$-eigenspaces.

Solution to Exercise 10.1. The space $H^1_\iota \otimes_{O_K, \iota} \mathbb{C}$ is the subspace of $H^1(X, \mathbb{C})$ on which $\lambda \in K$ acts by $\iota(\lambda)$. Since K acts by endomorphisms, it preserves $H^{1,0}$ and $H^{0,1}$, so this subspace is $H^{1,0}_\iota \oplus H^{0,1}_\iota$. Complex conjugation maps $H^{1,0}$ to $H^{0,1}$ and, K acting through rational endomorphisms, the $\bar{\iota}$-eigenspace to the ι-eigenspace; so $H^{0,1}_\iota$ is the conjugate of $H^{1,0}_{\bar{\iota}}$. For type $(2,2)$ both have dimension 2, and ω spans $\bigwedge^4(H^{1,0}_\iota \oplus H^{0,1}_\iota) = \bigwedge^2 H^{1,0}_\iota \otimes \bigwedge^2 H^{0,1}_\iota \subset H^{2,2}$. For type $(1,3)$ the dimensions are 1 and 3, and ω has type $(1,3)$, so it is not a Hodge class. □

Hint for Exercise 10.2. Use $\theta^2 = -d_0$, $\bar{\theta} = -\theta$ and $\psi(x, \theta y) = \psi(\bar{\theta} x, y) = -\psi(\theta x, y)$.

Solution to Exercise 10.2. From (10.2), $\mathcal{H}(\theta x, y) = \frac{1}{2}\psi(\theta x, y) + \frac{\theta}{2}\psi(x, y) = \theta \mathcal{H}(x, y)$, so $\mathcal{H}$ is K-linear in x. Next $\mathcal{H}(y, x) = -\frac{1}{2}\psi(x, y) + \frac{\theta}{2d_0}\psi(x, \theta y) = -\frac{1}{2}\psi(x, y) - \frac{\theta}{2d_0}\psi(\theta x, y) = -\overline{\mathcal{H}(x, y)}$. Since $\operatorname{Tr}\theta = 0$, $\operatorname{Tr}\mathcal{H} = \psi$. Finally $h(y, x) = \theta \mathcal{H}(y, x) = -\theta\overline{\mathcal{H}(x, y)} = \overline{\theta \mathcal{H}(x, y)} = \overline{h(x, y)}$. □

Hint for Exercise 10.3. The norm of a unit reduces to $\bar{\lambda}^{p+1}$ in $\mathbb{F}_{p^2}$.

Solution to Exercise 10.3. Write $x = p^n \lambda$ with $\lambda \in O^\times_{K,p}$. Then $\mathrm{Nm}(x) = p^{2n} \mathrm{Nm}(\lambda)$, and $\mathrm{Nm}(\lambda) = \lambda\sigma(\lambda)$ reduces to $\bar{\lambda}^{1+p} \neq 0$ in $\mathbb{F}_{p^2}$, so it is a unit and $v_p(\mathrm{Nm}\, x) = 2n$. For $K = \mathbb{Q}(\sqrt{-2})$ at 5: if $x^2 + 2y^2 \equiv 0$ with $y \not\equiv 0$, then $(x/y)^2 \equiv -2 \equiv 3$, but the squares modulo 5 are $0, 1, 4$. So $y \equiv 0$ and then $x \equiv 0$. □

Hint for Exercise 10.4. A change of basis multiplies the determinant by a norm. A hyperbolic plane scaled by 5 still contains a unimodular lattice.

Solution to Exercise 10.4. The Gram matrix of $O^n_{K,p}$ is $\mathrm{diag}(\lambda_1, \dots, \lambda_n)$, which has entries in $O_{K,p}$ and a unit determinant exactly when every λ_i is a unit. Changing the basis by γ multiplies $\det h$ by $\mathrm{Nm}(\det \gamma)$, of even valuation, so $v_p(\det h)$ modulo 2 is an invariant. The space $\mathrm{diag}(1, -1)$ has a unimodular lattice, the standard one. The space $\mathrm{diag}(5, -5)$ has determinant -25, of even valuation, and indeed $e'_1 = e_1 + e_2$, $e'_2 = (e_1 - e_2)/10$ have Gram matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, unimodular. The space $\mathrm{diag}(1, -5)$ has determinant of odd valuation and contains no unimodular lattice. □

Hint for Exercise 10.6. For x fixed, $\mathcal{H}(x, L)$ is an $O_{K,p}$-submodule of K_p.

Solution to Exercise 10.6. For $x \in L \otimes \mathbb{Q}$, $\mathcal{H}(x, L)$ is an $O_{K,p}$-submodule of K_p, because $\mathcal{H}(x, \lambda y) = \bar{\lambda}\mathcal{H}(x, y)$. Then $\psi(x, L) = \operatorname{Tr}(\mathcal{H}(x, L)) \subseteq \mathbb{Z}_p$ if and only if $\mathcal{H}(x, L) \subseteq \{z : \operatorname{Tr}(z O_{K,p}) \subseteq \mathbb{Z}_p\}$, the inverse different, which is $O_{K,p}$ when p is unramified. So x lies in the ψ-dual exactly when $\mathcal{H}(x, L) \subseteq O_{K,p}$, that is, when it lies in the $\mathcal{H}$-dual. □

Chapter 11

Hint for Exercise 11.1. Set $c_1 = 0$ in the formula for ch_3. In $(n_{\mathcal{F}} + \kappa_2 + \kappa_3 + \cdots)^{n_{\mathcal{F}}}$ only one factor can contribute κ_3 in degree 6.

Solution to Exercise 11.1. With $c_1 = 0$, $\mathrm{ch}_3 = \frac{1}{6} \cdot 3c_3 = \frac{1}{2}c_3$, so $c_3 = 2\,\mathrm{ch}_3$. Write $n = n_{\mathcal{F}}$. In $\kappa^n = (n + \kappa_2 + \kappa_3 + \cdots)^n$ a product of terms has degree 6 only if it is κ_3 times n^{n-1}, because $\kappa_1 = 0$ and κ_2 has degree 4; there are n ways to choose the factor, so the degree-6 part is $n \cdot n^{n-1}\kappa_3 = n^n\kappa_3$. □

Hint for Exercise 11.2. Solve $(w, 0) = (-\sqrt{-d}\Theta^\sharp y_a, y_a) + (\sqrt{-d}\Theta^\sharp y_b, y_b)$ for y_a, y_b.

Solution to Exercise 11.2. From the second components $y_b = -y_a$, and from the first $w = -2\sqrt{-d}\Theta^\sharp y_a$, so $y_a = -(\Theta^\sharp)^{-1}w/(2\sqrt{-d})$. Then $\eta(w, 0) = \sqrt{-d}(-\sqrt{-d}\Theta^\sharp y_a, y_a) - \sqrt{-d}(\sqrt{-d}\Theta^\sharp y_b, y_b) = (0, 2\sqrt{-d}y_a) = (0, -(\Theta^\sharp)^{-1}w)$. Similarly $(0, y) = a + b$ with $a = \frac{1}{2}(-\sqrt{-d}\Theta^\sharp y, y)$, $b = \frac{1}{2}(\sqrt{-d}\Theta^\sharp y, y)$, and $\eta(0, y) = \sqrt{-d}a - \sqrt{-d}b = (d\Theta^\sharp y, 0)$. Hence $\eta^2(w, 0) = \eta(0, -(\Theta^\sharp)^{-1}w) = (-dw, 0)$ and $\eta^2(0, y) = \eta(d\Theta^\sharp y, 0) = (0, -dy)$. In a $\mathbb{Z}$-basis adapted to the two summands, $(\cdot, \cdot)$ has Gram matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ in blocks, of determinant ± 1, and the Gram matrix of ψ_6 is that of $(\cdot, \cdot)$ times the matrix of η, so its determinant is $\pm \det \eta$. From $\eta^2 = -d$ on a lattice of rank 12, $(\det \eta)^2 = (-d)^{12} = d^{12}$, so $\det \eta = \pm d^6$, and the determinant of the alternating form ψ_6, a square, is d^6. □

Hint for Exercise 11.3. Use that $M' \otimes_A \hat{B} \to M \otimes_A \hat{B}$ is injective.

Solution to Exercise 11.3. Let $\mathcal{K}$ be the kernel of $M' \otimes_A B \to M \otimes_A B$. Since $\hat{B}$ is flat over B, $\mathcal{K} \otimes_B \hat{B}$ is the kernel of $M' \otimes_A \hat{B} \to M \otimes_A \hat{B}$, which is 0 because $\hat{B}$ is flat over A. Since $\hat{B}$ is faithfully flat over B, $\mathcal{K} \otimes_B \hat{B} = 0$ implies $\mathcal{K} = 0$. □

Hint for Exercise 11.4. Tensor the resolution with $\mathcal{Z}$.

Solution to Exercise 11.4. Tensoring $0 \to R \xrightarrow{t} R \to R/t \to 0$ with $\mathcal{Z}$ gives the complex $\mathcal{Z} \xrightarrow{t} \mathcal{Z}$, whose homology is $\mathrm{Tor}_1^R(\mathcal{Z}, R/t) = \ker(t\colon \mathcal{Z} \to \mathcal{Z}) = 0$ and $\mathrm{Tor}_0^R(\mathcal{Z}, R/t) = \mathcal{Z}/t\mathcal{Z}$. So $\mathcal{Z} \otimes_R^L R/t \cong \mathcal{Z}/t\mathcal{Z}$. For the last question: the local ring of a smooth curve at a point is a discrete valuation ring with uniformizer t, and a flat module over it is torsion-free, so t is a non-zero-divisor on it; this passes to a module over a ring flat over that local ring. □

Hint for Exercise 11.5. By Exercise 13.5, x_1, x_2 span L.

Solution to Exercise 11.5. A sublattice of rank 2 with unit Gram determinant is all of L, so x_1, x_2 span L and nx_1, nx_2 span $nL = p^{v_p(n)}L$, of index $p^{2v_p(n)}$. It contains pL exactly when $v_p(n) \leq 1$. □

Hint for Exercise 11.6. Use that $\mathrm{ch}(\mathcal{O}_X(\Theta)) = 1 + \Theta + \frac{1}{2}\Theta^2 + [\mathrm{pt}]$, because $\Theta^3 = 6[\mathrm{pt}]$.

Solution to Exercise 11.6. Each C_i has genus 3, so $\mathrm{ch}(\mathcal{O}_{C_i}) = \frac{1}{2}\Theta^2 - 2[\mathrm{pt}]$, and the ideal sheaf $\mathcal{I}$ of the disjoint union has $\mathrm{ch}(\mathcal{I}) = 1 - \sum_i \mathrm{ch}(\mathcal{O}_{C_i}) = 1 - \frac{d+1}{2}\Theta^2 + 2(d+1)[\mathrm{pt}]$. Multiplying by $1 + \Theta + \frac{1}{2}\Theta^2 + [\mathrm{pt}]$ and using $\Theta^3 = 6[\mathrm{pt}]$,

$$\mathrm{ch}(\mathcal{I}(\Theta)) = 1 + \Theta + (\tfrac{1}{2} - \tfrac{d+1}{2})\Theta^2 + (1 - 3(d+1) + 2(d+1))[\mathrm{pt}] = 1 + \Theta - \tfrac{d}{2}\Theta^2 - d[\mathrm{pt}].$$

□

Hint for Exercise 11.7. Under ι, $\varpi_d = \frac{1}{2} - \frac{\mathrm{i}}{2\sqrt{d}}$.

Solution to Exercise 11.7. The norm is $\mathrm{Nm}(\varpi_d) = \frac{1}{4} + \frac{1}{4d} = \frac{d+1}{4d}$. The number $\frac{d+1}{2d}$ is a unit at an odd prime p exactly when $p \nmid d(d+1)$: at $p = 5$ when $d \not\equiv 0, 4 \bmod 5$, at $p = 7$ when $d \not\equiv 0, 6 \bmod 7$. □

Hint for Exercise 11.8. Note that $\sqrt{-4d_0} = 2\sqrt{-d_0}$. An odd prime $p \nmid d_0$ splits in $\mathbb{Q}(\sqrt{-d_0})$ exactly when $-d_0$ is a square modulo p.

Solution to Exercise 11.8. Here $K_d = \mathbb{Q}(2\sqrt{-d_0}) = K$. Since p is odd and unramified in K, $p \nmid d_0$ and so $p \nmid 2d$. If $p \mid d + 1$, then $-d \equiv 1 = 1^2$, so $-4d_0$ and hence $-d_0$ is a square modulo p, and p would split in K. □

Hint for Exercise 11.9. Solve $\gamma\omega = \mathrm{i}\omega$ in $\mathbb{Z}[\mathrm{i}]^2$.

Solution to Exercise 11.9. With $\gamma = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, $\gamma(x_1, x_2) = (-x_2, x_1) = \mathrm{i}(x_1, x_2)$ means $x_2 = -\mathrm{i}x_1$, so the eigenlattice is $\mathbb{Z}[\mathrm{i}]\omega$ with $\omega = e_1 - \mathrm{i}e_2$, and $\omega + \bar{\omega} = 2e_1$ has content 2. For $\nu = x + y\mathrm{i}$, $\nu\omega + \bar{\nu}\bar{\omega} = 2(xe_1 + ye_2)$, so these classes form $2\mathbb{Z}^2$, of index 4. At an odd prime p the factor 2 is a unit: $e_1 = \nu\omega + \bar{\nu}\bar{\omega}$ with $\nu = \frac{1}{2} \in O_{K,(p)}$. □

Chapter 12

Hint for Exercise 12.1. Write $\mathbb{Q}_\ell^\times = \ell^{\mathbb{Z}} \times \boldsymbol{\mu}_{\ell-1} \times (1 + \ell\mathbb{Z}_\ell)$ and use Hensel's lemma on $1 + \ell\mathbb{Z}_\ell$.

Solution to Exercise 12.1. For odd ℓ, every element of $1 + \ell\mathbb{Z}_\ell$ is a square by Hensel's lemma, and the squares in the cyclic group $\boldsymbol{\mu}_{\ell-1}$ have index 2. So $\mathbb{Q}_\ell^\times/(\mathbb{Q}_\ell^\times)^2 \cong (\mathbb{Z}/2)^2$ with representatives $1, \xi, \ell, \xi\ell$, and the three nontrivial classes give the three quadratic extensions. For $\ell = 2$, $\mathbb{Z}_2^\times = \{\pm 1\} \times (1 + 4\mathbb{Z}_2)$ and the squares are $1 + 8\mathbb{Z}_2$, so $\mathbb{Z}_2^\times/(\mathbb{Z}_2^\times)^2$ has order 4 and $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$ order 8, with seven quadratic extensions. In both cases at least two quadratic extensions avoid a given one. □

Hint for Exercise 12.2. $\mathbb{Q}_{p^3} \cap \mathbb{Q}_{p^2} = \mathbb{Q}_p$ inside an algebraic closure.

Solution to Exercise 12.2. $K' \otimes \mathbb{Q}_p = (k \otimes_{\mathbb{Q}} \mathbb{Q}_p) \otimes_{\mathbb{Q}_p} (K \otimes_{\mathbb{Q}} \mathbb{Q}_p) = \mathbb{Q}_{p^3} \otimes_{\mathbb{Q}_p} \mathbb{Q}_{p^2}$. The minimal polynomial over $\mathbb{Q}_p$ of a generator of $\mathbb{Q}_{p^2}$ stays irreducible over $\mathbb{Q}_{p^3}$, because $\mathbb{Q}_{p^3}$ contains no quadratic extension of $\mathbb{Q}_p$, its degree being 3. So the tensor product is a field of degree 6, unramified, hence $\mathbb{Q}_{p^6}$. A field has one maximal ideal, so K' has a single prime above p. □

Hint for Exercise 12.3. The orbit of $+++$ is $\{+++, ---\}$; for $++-$ use the cyclic permutations and the sign change.

Solution to Exercise 12.3. The group $\mathfrak{S}_3 \times \{\pm\}$ has order 12. The vectors $+++$ and $---$ form an orbit with stabilizer $\mathfrak{S}_3$. The stabilizer of $++-$ is generated by the transposition of the first two slots, so its orbit has $12/2 = 6$ elements: the three vectors with two $+$ and the three with two $-$. With only the cyclic permutations the group has order 6, the orbit of $++-$ is still $\{++-, +-+, -++\}$ together with their negatives, and the orbits do not change. □

Hint for Exercise 12.4. List the four sets and count $\epsilon_1 = +$.

Solution to Exercise 12.4. $\{\epsilon_1\epsilon_2\epsilon_3 = +\} = \{+++, +--, -+-, --+\}$ has two elements with $\epsilon_1 = +$ and two with $\epsilon_1 = -$: type $(2,2)$, and so has its complement. $\{\text{majority} = +\} = \{+++, ++-, +-+, -++\}$ has three with $\epsilon_1 = +$: type $(3,1)$, and its complement $(1,3)$. So the product sets give type $(2,2)$. □

Hint for Exercise 12.5. Two matrices γ', γ'' with $\gamma'\Lambda_0 = \gamma''\Lambda_0$ differ by an element of $\mathrm{GL}_2(\mathbb{Z}_{p^3})$, which has a unit determinant.

Solution to Exercise 12.5. If $\gamma'\Lambda_0 = \gamma''\Lambda_0$, then $\gamma''^{-1}\gamma'$ preserves Λ_0, so it lies in $\mathrm{GL}_2(\mathbb{Z}_{p^3})$ in a basis of Λ_0 and has a unit determinant; $v_p(\det\gamma')$ is well defined. Replacing Λ_0' by $\lambda\Lambda_0'$, $\lambda \in k_p^\times$, replaces γ' by $\lambda\gamma'$ and the determinant by $\lambda^2 \det\gamma'$, of the same parity of valuation. Elements of $\mathrm{SL}_2(k_p)$ do not change the determinant, and an element of determinant p changes its valuation by 1. □

Chapter 13

Hint for Exercise 13.1. Apply skew-adjointness twice, and evaluate both sides of the second identity at $y \in \Gamma$.

Solution to Exercise 13.1. First, $\psi(\eta x, y) = (\eta^2 x, y) = -(\eta x, \eta y)$ and $\psi(x, \eta y) = (\eta x, \eta y)$, so $\psi(\eta x, y) = -\psi(x, \eta y)$. Next, for $y \in \Gamma$, $\delta(-\eta x)(y) = -\psi(\eta x, y) = \psi(x, \eta y) = \delta(x)(\eta y) = (\eta^\vee\delta(x))(y)$. On a member $X_{6,t}$ take $\Gamma = H^1(X_{6,t}, \mathbb{Z})$, so that $\Gamma^\vee = H_1(X_{6,t}, \mathbb{Z})$. For an

endomorphism e, the push-forward e_* on H_1 and the pull-back e^* on H^1 are transposes of each other for the pairing between homology and cohomology. So if $e^* = \eta$, then $e_* = \eta^\vee$, and the identity says that δ carries $-\eta$ to e_*. □

Hint for Exercise 13.2. Modulo p, $\mu_i \equiv \mu_j$ if and only if $(p+1) \mid (j-i)$, and $b^4 \equiv \bar{b}^4$ if and only if $(p+1) \mid 4$.

Solution to Exercise 13.2. For $p \geq 5$, $0 < j - i \leq 4 < 6 \leq p+1$, so $p+1 \nmid j-i$. For an inert $p = 3$, $p+1 = 4$ divides $j-i$ only for $(i,j) = (0,4)$, so $\mu_0 \equiv \mu_4$ modulo 3. Next, $b^4 \equiv \bar{b}^4$ means $\zeta^4 = \zeta^{4p}$, that is $\zeta^{4(p-1)} = 1$, which for a generator ζ of $\mathbb{F}_{p^2}^\times$ means $(p^2-1) \mid 4(p-1)$, that is $(p+1) \mid 4$. This fails for $p \geq 5$ and holds for $p = 3$, where $\zeta^8 = 1$ for every $\zeta \in \mathbb{F}_9^\times$. □

Hint for Exercise 13.3. The conjugate polynomial $\bar{Q}$ interpolates the conjugate data at the conjugate points.

Solution to Exercise 13.3. Let $\bar{Q}$ be Q with conjugated coefficients. Then $\bar{Q}(\bar{\mu}_i) = \overline{Q(\mu_i)}$, which is the prescribed value at μ_i, and since $\bar{\mu}_i = \mu_{4-i}$ and the values at μ_i and μ_{4-i} agree, $\bar{Q}$ takes the prescribed values at all five points. By uniqueness $\bar{Q} = Q$, so the coefficients are fixed by conjugation and rational. □

Hint for Exercise 13.4. Put $z = x_1\bar{x}_2$; then $\operatorname{Tr}(x_1\bar{x}_1)\operatorname{Tr}(x_2\bar{x}_2) = 4z\bar{z}$.

Solution to Exercise 13.4. The determinant is $4\operatorname{Nm}(x_1)\operatorname{Nm}(x_2) - \operatorname{Tr}(x_1\bar{x}_2)^2 = 4z\bar{z} - (z+\bar{z})^2 = -(z-\bar{z})^2$ with $z = x_1\bar{x}_2$. For $x_1 = \nu_Z$, $x_2 = b^4\nu_Z$, $z = \operatorname{Nm}(\nu_Z)\bar{b}^4$, so $-(z-\bar{z})^2 = -\operatorname{Nm}(\nu_Z)^2(b^4 - \bar{b}^4)^2$, and multiplying by $\langle\omega,\bar{\omega}\rangle^2$ gives (13.2). □

Hint for Exercise 13.5. Use $\operatorname{disc} L' = [L : L']^2 \operatorname{disc} L$.

Solution to Exercise 13.5. Since $\operatorname{disc} L \in \mathbb{Z}_p$ and $\operatorname{disc} L'$ is a unit, $[L : L']^2$ is a unit, so $[L : L'] = 1$. For $L = \mathbb{Z}_p^2$ with the form $\operatorname{diag}(1,1)$ and L' spanned by e_1 and pe_2, the Gram determinant of L' is $p^2 \neq 0$ and $[L : L'] = p$. □

Hint for Exercise 13.6. Compute in $\mathbb{F}_{25} = \mathbb{F}_5[\theta]$, $\theta^2 = 3$.

Solution to Exercise 13.6. Here $b^2 = -1 + 2\sqrt{-2}$ and $b^4 = -7 - 4\sqrt{-2}$; $\mu_1 = \operatorname{Nm}(b)\bar{b}^2 = -3 - 6\sqrt{-2}$, $\mu_2 = \operatorname{Nm}(b)^2 = 9$, $\mu_3 = 3b^2$, $\mu_0 = \bar{b}^4$. Modulo 5, with $\theta = \sqrt{-2}$ and $\theta^2 = 3$: $\mu_4 \equiv 3+\theta$, $\mu_4^2 \equiv 2+\theta$, $\mu_4^3 \equiv 4$, $\mu_4^4 \equiv 2+4\theta$, so $Q_P(\mu_4) \equiv 1+3(2+\theta)+2\cdot 4+3(2+4\theta) = 21+15\theta \equiv 1$. And $\mu_3 \equiv 2+\theta$, $\mu_3^2 \equiv 2+4\theta$, $\mu_3^3 \equiv 1$, $\mu_3^4 \equiv 2+\theta$, so $Q_P(\mu_3) \equiv 1+3(2+4\theta)+2+3(2+\theta) = 15+15\theta \equiv 0$. □

Chapter 14

Hint for Exercise 14.1. A supersingular elliptic curve has a nontrivial p-divisible group. For the example take $E_0\colon y^2 = x^3 + 1$ over $\mathbb{F}_5$, which has an automorphism of order 3.

Solution to Exercise 14.1. If $\ker f$ contained an elliptic curve E, then $f[p^\infty]$ would vanish on $E[p^\infty]$, which has height 2, contradicting injectivity. So $\ker f$ is finite, and its p-primary part lies in $X'[p^\infty]$ and is killed by the injective $f[p^\infty]$, so it is trivial and $|\ker f|$ is prime to p. For an example, let $p = 5$ and $E_0\colon y^2 = x^3 + 1$, supersingular by Example 2.1, with the automorphism $\alpha_\lambda(x,y) = (\lambda x, y)$, $\lambda \in \mathbb{F}_{25}$ a primitive cube root of unity. The endomorphism $f = 3 + \alpha_\lambda$ has degree $\operatorname{Nm}(3+\alpha_\lambda) = 9 - 3 + 1 = 7$, prime to 5, so $f[5^\infty]$ is an isomorphism by Exercise 2.6. □

Hint for Exercise 14.2. Projection formula: $f_*(f^*x \cdot 1) = x \cdot f_*1$.

Solution to Exercise 14.2. By the projection formula $f_*f^*x = x \cdot f_*(1) = (\deg f)x$. For the other identity, f^*f_*y is the sum of the pull-backs of y by the translations by the points of $\ker f$, and translations form a connected family containing the identity, so they act trivially on cohomology; the sum is $(\deg f)y$ when $\ker f$ is étale, which is the case for $\deg f$ prime to p. On Chow groups translations act nontrivially, for instance the pull-back of [0] by the

translation by a point $x' \neq 0$ of an elliptic curve is $[-x'] \neq [0]$ in CH_0, so the identity fails there. □

Hint for Exercise 14.3. Over $\mathbb{F}_5$, $\sum_{j\in\mathbb{F}_5} j^l$ is -1 if $l > 0$ and $4 \mid l$, and 0 otherwise.

Solution to Exercise 14.3. The determinant is 288, which is 3 modulo 5 and 1 modulo 7. Over $\mathbb{F}_5$ the points $0, \dots, 4$ are all of $\mathbb{F}_5$. For $\lambda_j = -j^2$, $\sum_j \lambda_j j^i = -\sum_j j^{i+2}$, which for $i = 0, \dots, 4$ is $-1 \cdot (-1) = 1$ when $i = 2$ and 0 otherwise. So $z_2 \equiv -\sum_{j=0}^4 j^2 (j\alpha_1, \alpha_2)^* x$, with weights $(0, -1, -4, -9, -16) \equiv (0, 4, 1, 1, 4)$ modulo 5, the middle row of the inverse matrix. □

Hint for Exercise 14.4. Compute $F(e_i \otimes e_j) = Ae_j \otimes e_i = p^j e_{1-j} \otimes e_i$.

Solution to Exercise 14.4. On the basis vectors, $F(e_i \otimes e_j) = A\sigma e_j \otimes \sigma e_i = p^j e_{1-j} \otimes e_i$. So $e_{00} \mapsto e_{10} \mapsto e_{11} \mapsto pe_{01} \mapsto p^2 e_{00}$, with letters $0, 0, 1, 1$: the word 0011. Going once around the cycle multiplies by p^2, so $F^4 = p^2\sigma^4$ on this basis, and the crystal is isoclinic of slope $\frac{1}{2}$. □

Hint for Exercise 14.5. The lattice Alg^2 contains S and is stable under End^*; use the last statement of Theorem A(a).

Solution to Exercise 14.5. Without Hypothesis (M): Theorem A(a), Theorem B, Theorem C(a), and the nine unconditional classes of Proposition 15.7. For the second part, if $\mathrm{Alg}^2(\mathcal{A}_t) \not\subseteq N$, choose $x \in \mathrm{Alg}^2 \setminus N$. By Theorem A(a), S and the $\alpha^* x$ span T^4, and all of them lie in Alg^2, so $\mathrm{Alg}^2 = T^4$. □

Chapter 15

Hint for Exercise 15.1. Count balanced words up to rotation; a word is non-primitive if it is a power of a shorter word.

Solution to Exercise 15.1. Length 2: 01. Length 4: 0011 and $0101 = (01)^2$. Length 6: 000111, 001011, 001101 and $010101 = (01)^3$. Length 8: 00001111, 00010111, 00011011, 00011101, 00100111, 00101011, 00101101, 00110101, and the non-primitive $00110011 = (0011)^2$ and $01010101 = (01)^4$. So the primitive ones number 1, 1, 3, 8. □

Hint for Exercise 15.3. A basis vector e_i satisfies $e_i \notin FM + VM$ modulo p exactly when $w_{i-1} = 1$ and $w_i = 0$.

Solution to Exercise 15.3. Modulo p, FM contains e_{i+1} when $w_i = 0$, and VM contains e_i when $w_i = 1$. So e_i is missing from $FM + VM$ exactly when $w_{i-1} = 1$ and $w_i = 0$, a cyclic $1 \to 0$ transition. This gives $a = 2$ for 00100111, 3 for 00101101, 1 for 00001111, and $1 + 2 = 3$ for $01 + 001011$. □

Hint for Exercise 15.4. Complement and rotate to a word that starts with the longest run of 0s.

Solution to Exercise 15.4. The complement of 00100111 is 11011000, which rotated is 00011011. Among the eight primitive words of length 8, the complements give the pairs $00010111 \leftrightarrow 00011101$, $00011011 \leftrightarrow 00100111$ and $00101011 \leftrightarrow 00110101$, while 00001111 and 00101101 are their own duals. So two of the eight are self-dual. □

Hint for Exercise 15.5. Use Exercise 2.6 and the fact that the Dieudonné module of $X^\vee[p^\infty]$ is the dual of that of $X[p^\infty]$.

Solution to Exercise 15.5. A polarization $\mathrm{pol}_{\mathscr{L}}$ of degree prime to p is an isogeny of degree prime to p, so $\mathrm{pol}_{\mathscr{L}}[p^\infty] \colon X[p^\infty] \to X^\vee[p^\infty]$ is an isomorphism (Exercise 2.6). By Dieudonné theory, $M(X^\vee)$ is the dual of $M(X)$, so $M(X)$ is isomorphic to its dual. The module 00100111 has dual 00011011, a different primitive word, so by Fact 15.2 it is not isomorphic to its dual, and a fourfold with this Dieudonné module has no polarization of degree prime to p. □

Hint for Exercise 15.6. Frobenius is multiplicative, $F(\operatorname{pr}_{X^\vee}^* y) = \operatorname{pr}_{X^\vee}^* Fy$, and $\operatorname{pr}_{X*} F = p^4 F \operatorname{pr}_{X*}$ because the fibers have dimension 4.

Solution to Exercise 15.6. The class $\operatorname{pr}_{X^\vee}^* y \cdot c_1(\mathcal{P})^{8-n}$ has degree $n + 2(8-n) = 16 - n$, and pushing forward along fibers of dimension 4 lowers degrees by 8, to $8 - n$. Next $F\big(\operatorname{pr}_{X^\vee}^* y \cdot c_1(\mathcal{P})^{8-n}\big) = p^{8-n} \operatorname{pr}_{X^\vee}^*(Fy) \cdot c_1(\mathcal{P})^{8-n}$, and $F \operatorname{pr}_{X*} = p^{-4} \operatorname{pr}_{X*} F$, so $F\mathfrak{F}(y) = p^{4-n}\mathfrak{F}(Fy)$. If $Fy = p^{n/2}y$, then $F\mathfrak{F}(y) = p^{(8-n)/2}\mathfrak{F}(y)$, so $\mathfrak{F}(y) \in T^{8-n}(X)$. □

Hint for Exercise 15.7. Read off $[T^4 : S]$ of the dual module from the table.

Solution to Exercise 15.7. The dual of $01 + 001101$ is $01 + 001011$ and conversely, so $[T^4 : \widehat{S}]$ is p^{10} for $01 + 001101$ and p^2 for $01 + 001011$. For 00100111 and 00011011 it is p^{26}. For 00110101 the dual is 00101011, so $[T^4 : \widehat{S}] = p^2$, while $[T^4 : S] = 1$. For a self-dual module, (15.1) gives only $[T^4 : \widehat{S}] = [T^4 : S]$; the two lattices have the same index but need not be equal, since an isomorphism with the dual need not carry the monomial basis to itself. For $\mathbb{M}$ the computation finds $S + \widehat{S} = S$, so there the Fourier source adds nothing, and in general whether it adds something has to be computed. □

Hint for Exercise 15.2. Compare F of both sides on e_i.

Solution to Exercise 15.2. The map sends $Fe_i = p^{w_i} e_{i+1}$ to $p^{w_i + c_{i+1}} e'_{i+1}$, and $F(p^{c_i} e'_i) = p^{c_i + [i \text{ odd}]} e'_{i+1}$. These agree exactly when $c_{i+1} = c_i + [i \text{ odd}] - w_i$. Going once around the cycle adds $\sum_i [i \text{ odd}] - \sum_i w_i = m - m = 0$, so the c_i are well defined modulo $2m$. Both modules are free of the same rank and the map is injective after inverting p, so $V = pF^{-1}$ is determined by F on both sides, and a map commuting with F commutes with V. □

Bibliography

[AH62] M. F. Atiyah and F. Hirzebruch. "Analytic cycles on complex manifolds". In: *Topology* 1 (1962), pp. 25–45. DOI: 10.1016/0040-9383(62)90094-0.

[Bea83] A. Beauville. "Quelques remarques sur la transformation de Fourier dans l'anneau de Chow d'une variété abélienne". In: *Algebraic Geometry (Tokyo/Kyoto, 1982)*. Vol. 1016. Lecture Notes in Mathematics. Berlin: Springer, 1983, pp. 238–260. DOI: 10.1007/BFb0099965.

[BF03] R.-O. Buchweitz and H. Flenner. "A semiregularity map for modules and applications to deformations". In: *Compositio Mathematica* 137 (2003), pp. 135–210. DOI: 10.1023/A:1023999012081. arXiv: math/9912245.

[BH61] A. Borel and A. Haefliger. "La classe d'homologie fondamentale d'un espace analytique". In: *Bulletin de la Société Mathématique de France* 89 (1961), pp. 461–513. DOI: 10.24033/bsmf.1571.

[Bro26] M. Broe. *The Tate conjecture for abelian fourfolds over finite fields*. preprint. 2026. arXiv: 2608.28651.

[Che25] F. Chen. *Infinitely many supersingular primes for some Mumford's abelian fourfolds*. preprint. 2025. arXiv: 2511.06654.

[CP26] A. Cadoret and A. Pirutka. "Uniform bounds for obstructions to the integral Tate conjecture". In: *Journal of Algebraic Geometry* 35 (2026), pp. 615–641. DOI: 10.1090/jag/861. arXiv: 2410.21010.

[Del82] P. Deligne. "Hodge cycles on abelian varieties (notes by J. S. Milne)". In: *Hodge Cycles, Motives, and Shimura Varieties*. Vol. 900. Lecture Notes in Mathematics. Berlin: Springer, 1982, pp. 9–100. DOI: 10.1007/978-3-540-38955-2_3.

[DG70] M. Demazure and A. Grothendieck, eds. *Schémas en groupes II (SGA 3)*. Vol. 152. Lecture Notes in Mathematics. Berlin: Springer, 1970.

[EGS25] P. Engel, O. de Gaay Fortman, and S. Schreieder. *Matroids and the integral Hodge conjecture for abelian varieties*. preprint. 2025. arXiv: 2507.15704.

[Ge26] T. Ge. "Intersecting subvarieties of abelian schemes with group subschemes I". In: *Compositio Mathematica* 162 (2026), pp. 231–275. DOI: 10.1017/S0010437X26103066. arXiv: 2411.16108.

[GM87] H. Gillet and W. Messing. "Cycle classes and Riemann–Roch for crystalline cohomology". In: *Duke Mathematical Journal* 55 (1987), pp. 501–538. DOI: 10.1215/S0012-7094-87-05527-X.

[Gre23] O. Gregory. "Torsion codimension 2 cycles on supersingular abelian varieties". In: *Canadian Mathematical Bulletin* 66 (2023), pp. 458–466. DOI: 10.4153/S0008439522000431.

[Gro03] A. Grothendieck, ed. *Revêtements étales et groupe fondamental (SGA 1)*. Vol. 3. Documents Mathématiques. Paris: Société Mathématique de France, 2003. arXiv: math/0206203.

[Gro58] A. Grothendieck. "La théorie des classes de Chern". In: *Bulletin de la Société Mathématique de France* 86 (1958), pp. 137–154. DOI: 10.24033/bsmf.1501.

[Hai05] T. J. Haines. "Introduction to Shimura varieties with bad reduction of parahoric type". In: *Harmonic Analysis, the Trace Formula, and Shimura Varieties*. Vol. 4. Clay Mathematics Proceedings. Providence, RI: American Mathematical Society, 2005, pp. 583–642. arXiv: math/0409482.

[Jac62] R. Jacobowitz. "Hermitian forms over local fields". In: *American Journal of Mathematics* 84 (1962), pp. 441–465. DOI: 10.2307/2372982.

[Jon98] A. J. de Jong. "Homomorphisms of Barsotti–Tate groups and crystals in positive characteristic". In: *Inventiones Mathematicae* 134 (1998), pp. 301–333. DOI: 10.1007/s002220050266.

[Kis10] M. Kisin. "Integral models for Shimura varieties of abelian type". In: *Journal of the American Mathematical Society* 23 (2010), pp. 967–1012. DOI: 10.1090/S0894-0347-10-00667-3.

[KP18] M. Kisin and G. Pappas. "Integral models of Shimura varieties with parahoric level structure". In: *Publications Mathématiques de l'IHÉS* 128 (2018), pp. 121–218. DOI: 10.1007/s10240-018-0100-0.

[Lie16] C. Liedtke. "Lectures on supersingular K3 surfaces and the crystalline Torelli theorem". In: *K3 Surfaces and Their Moduli*. Vol. 315. Progress in Mathematics. Birkhäuser, 2016, pp. 171–235. DOI: 10.1007/978-3-319-29959-4_8. arXiv: 1403.2538.

[Mad19] K. Madapusi Pera. "Toroidal compactifications of integral models of Shimura varieties of Hodge type". In: *Annales scientifiques de l'École Normale Supérieure (4)* 52 (2019), pp. 393–514. DOI: 10.24033/asens.2391. arXiv: 1211.1731.

[Mar25] E. Markman. *Cycles on abelian 2n-folds of Weil type from secant sheaves on abelian n-folds*. preprint. 2025. arXiv: 2502.03415.

[Mil05] J. S. Milne. "Introduction to Shimura varieties". In: *Harmonic Analysis, the Trace Formula, and Shimura Varieties*. Vol. 4. Clay Mathematics Proceedings. Providence, RI: American Mathematical Society, 2005, pp. 265–378.

[Mil08] J. S. Milne. *Abelian varieties*. course notes. 2008. URL: https://www.jmilne.org/math/.

[Mil25] J. S. Milne. *On the integral Tate conjecture for abelian varieties*. preprint. 2025. arXiv: 2509.06707.

[Mum69] D. Mumford. "A note of Shimura's paper "Discontinuous groups and abelian varieties"". In: *Mathematische Annalen* 181 (1969), pp. 345–351. DOI: 10.1007/BF01350672.

[MZ99] B. J. J. Moonen and Y. G. Zarhin. "Hodge classes on abelian varieties of low dimension". In: *Mathematische Annalen* 315 (1999), pp. 711–733. DOI: 10.1007/s002080050333.

[Nit05] N. Nitsure. "Construction of Hilbert and Quot schemes". In: *Fundamental Algebraic Geometry*. Vol. 123. Mathematical Surveys and Monographs. Providence, RI: American Mathematical Society, 2005, pp. 107–137. DOI: 10.1090/surv/123/05. arXiv: math/0504590.

[Oda69] T. Oda. "The first de Rham cohomology group and Dieudonné modules". In: *Annales scientifiques de l'École Normale Supérieure (4)* 2 (1969), pp. 63–135. DOI: 10.24033/asens.1175.

[Oor01] F. Oort. "A stratification of a moduli space of abelian varieties". In: *Moduli of Abelian Varieties (Texel Island, 1999)*. Vol. 195. Progress in Mathematics. Basel: Birkhäuser, 2001, pp. 345–416. DOI: 10.1007/978-3-0348-8303-0_13.

[Oor74] F. Oort. "Subvarieties of moduli spaces". In: *Inventiones Mathematicae* 24 (1974), pp. 95–119. DOI: 10.1007/BF01404301.

[Pet03] D. Petrequin. "Classes de Chern et classes de cycles en cohomologie rigide". In: *Bulletin de la Société Mathématique de France* 131 (2003), pp. 59–121. DOI: 10.24033/bsmf.2437.

[Sch98] C. Schoen. "Addendum to: Hodge classes on self-products of a variety with an automorphism". In: *Compositio Mathematica* 114 (1998), pp. 329–336. DOI: 10.1023/A:1000566205021.

[SS24] F. Scavia and F. Suzuki. "Non-algebraic geometrically trivial cohomology classes over finite fields". In: *Advances in Mathematics* 458 (2024), p. 109964. DOI: 10.1016/j.aim.2024.109964.

[SS25] F. Scavia and F. Suzuki. *On direct summands of products of Jacobians over arbitrary fields*. preprint. 2025. arXiv: 2507.09821.

[SZ16] M. Sheng and K. Zuo. "Deuring's mass formula of a Mumford family". In: *Transactions of the American Mathematical Society* 368 (2016), pp. 169–207. DOI: 10.1090/s0002-9947-2015-06312-0.

[The] The Stacks Project Authors. *The Stacks Project*. URL: https://stacks.math.columbia.edu.

[Voi16] C. Voisin. "The Hodge conjecture". In: *Open Problems in Mathematics*. Cham: Springer, 2016, pp. 521–543. DOI: 10.1007/978-3-319-32162-2_17.

[Voi21] J. Voight. *Quaternion Algebras*. Vol. 288. Graduate Texts in Mathematics. Cham: Springer, 2021. DOI: 10.1007/978-3-030-56694-4.

[Yu12] C.-F. Yu. "On Hermitian forms over dyadic non-maximal local orders". In: *Pure and Applied Mathematics Quarterly* 8 (2012), pp. 1117–1146. DOI: 10.4310/PAMQ.2012.v8.n4.a14. arXiv: 1005.4825.