Chapter XI. Polarizations and Weil pairings.

In the study of higher dimensional varieties and their moduli, one often considers polarized varieties. Here a polarization is usually defined as the class of an ample line bundle modulo a suitable equivalence relation, such as algebraic or homological equivalence. If X is an abelian variety then, as we have seen in (7.24), the class of an ample bundle L modulo algebraic equivalence carries the same information as the associated homomorphism $\lambda = \varphi_L \colon X \to X^t$. And it is in fact this homomorphism that we shall put in the foreground. One reason for this is that λ usually has somewhat better arithmetic properties; for instance, it may be defined over a smaller field than any line bundle representing it. The positivity of an ample bundle shall later be translated into the positivity of the Rosati involution associated to λ; this is an important result that shall be given in the next chapter.

The first Chern class of L only depends on L modulo algebraic equivalence, and we therefore expect that it can be expressed directly in terms of the associated homomorphism $\lambda = \varphi_L$. This is indeed the case. As we have seen before (cf. ??), the ℓ-adic cohomology of X can be described in more elementary terms via the Tate-ℓ-module. The class $c_1(L)$ then takes the form of an alternating pairing $E^\lambda_\ell \colon T_\ell X \times T_\ell X \to \mathbb{Z}_\ell(1)$, usually referred to as the Riemann form of L (or of λ). It is obtained, by a limit procedure, from pairings $e^\lambda_n \colon X[n] \times X[n] \to \mu_n$, called the Weil pairing.

§ 1. *Polarizations.*

(11.1) Proposition. *Let X be an abelian variety. Let $\lambda \colon X \to X^t$ be a homomorphism, and consider the line bundle $M := (\mathrm{id}, \lambda)^* \mathscr{P}_X$ on X. Then $\varphi_M = \lambda + \lambda^t$. In particular, if λ is symmetric then $\varphi_M = 2\lambda$.*

Proof. Immediate from Proposition (7.6) together with Exercise (7.5). □

(11.2) Proposition. *Let X be an abelian variety over a field k. Let $\lambda \colon X \to X^t$ be a homomorphism. Then the following properties are equivalent:*

(a) *λ is symmetric;*

(b) *there exists a field extension $k \subset K$ and a line bundle L on X_K such that $\lambda_K = \varphi_L$;*

(c) *there exists a finite separable field extension $k \subset K$ and a line bundle L on X_K such that $\lambda_K = \varphi_L$.*

Proof. Assume (a) holds. Let $M := (\mathrm{id}, \lambda)^* \mathscr{P}_X$ and $N := M^2$. By the previous proposition we know that $\varphi_M = 2\lambda$, so $\varphi_N = 4\lambda$. In particular, $X[4] \subset K(N) = \mathrm{Ker}(\varphi_N)$. We claim that $X[2] \subset X[4]$ is totally isotropic with respect to the commutator pairing e^N. Indeed, if x, $x' \in X[2]\big(T\big)$ for some k-scheme T then possibly after passing to an fppf covering of T we can write $x = 2y$ and $x' = 2y'$ for some y, $y' \in X[4]\big(T\big)$. Our claim now follows by noting that the restriction of e^N to $X[4] \times X[4]$ takes values in μ_4. By Corollary (8.11) we can find a line bundle

PolWp, 15 september, 2011 (812)

L on $X_{\overline{k}}$ such that $N \cong [2]^*L$ on $X_{\overline{k}}$. But then $4\lambda_{\overline{k}} = \varphi_{[2]^*L} = 4\varphi_L$, using Corollary (7.25). As $[4]_X$ is an epimorphism, it follows that $\lambda_{\overline{k}} = \varphi_L$. So (b) holds with $K = \overline{k}$.

To see that the apparently stronger condition (c) holds, view λ as a k-valued point of $\mathit{Hom}_{\mathsf{AV}}(X, X^t)$. Let $P(\lambda) \subset \mathrm{Pic}_{X/k}$ be the inverse image of λ under the homomorphism $\varphi\colon \mathrm{Pic}_{X/k} \to \mathit{Hom}_{\mathsf{AV}}(X, X^t)$. As $P(\lambda)$ is a closed subscheme of $\mathrm{Pic}_{X/k}$, it is locally of finite type. If T is a k-scheme then the T-valued points of $P(\lambda)$ are the classes of line bundles M on X_T such that $\varphi_M = \lambda$. Note that $P(\lambda)$ inherits a natural action of $X^t = \mathrm{Pic}^0_{X/k}$ by translations. The exact sequence of (7.22) tells us that for every k-scheme T the set $P(\lambda)(T)$ is either empty or it is a principal homogeneous space under $X^t(T)$. Hence if L is a line bundle on $X_{\overline{k}}$ with $\varphi_L = \lambda_{\overline{k}}$ then $x \mapsto [t_x^*L]$ defines an isomorphism of $\overline{k}$-schemes $(X^t)_{\overline{k}} \xrightarrow{\sim} P(\lambda)_{\overline{k}}$. In particular, $P(\lambda)$ is a geometrically integral k-scheme, so it has points with values in some finite separable extension $k \subset K$.

Finally, it is clear that (c) implies both (a) and (b). $\square$

(11.3) Corollary. *Let X/k be an abelian variety. Then the homomorphism $\psi\colon \mathrm{NS}_{X/k} \to \mathit{Hom}^{\mathrm{symm}}(X, X^t)$ of (7.26) is an isomorphism.*

Proof. Both group schemes are étale and we already know that ψ is injective. Hence it suffices to show that ψ is surjective on k_s-valued points, and this follows from the preceding Proposition. $\square$

(11.4) Proposition. *Let X/k be an abelian variety. Let $\lambda\colon X \to X^t$ be a symmetric homomorphism, and write $M := (\mathrm{id}, \lambda)^*\mathscr{P}_X$. Let $k \subset K$ be a field extension and let L be a line bundle on X_K with $\lambda_K = \varphi_L$.*

(i) *We have: λ is an isogeny $\Leftrightarrow$ L is non-degenerate $\Leftrightarrow$ M is non-degenerate.*

(ii) *If λ is an isogeny then L is effective if and only if M is effective.*

(iii) *We have: L is ample $\Leftrightarrow$ M is ample.*

Proof. By Proposition (11.1) $\varphi_{M_K} = 2\varphi_L = \varphi_{L^2}$, so M_K and L^2 are algebraically equivalent. Now (i) is clear, and (ii) follows from Corollary (9.23) and part (ii) of Proposition (9.18). For (iii), recall that a line bundle N on X is ample if and only if N is non-degenerate and effective; this is just Proposition (2.22). $\square$

Putting Propositions (2.22), (11.2) and (11.4) together we obtain the following corollary.

(11.5) Corollary. *Let X/k be an abelian variety. Let $\lambda\colon X \to X^t$ be a homomorphism. Then the following properties are equivalent:*

(a1) *λ is a symmetric isogeny and the line bundle $(\mathrm{id}, \lambda)^*\mathscr{P}$ on X is ample;*

(a2) *λ is a symmetric isogeny and the line bundle $(\mathrm{id}, \lambda)^*\mathscr{P}$ on X is effective;*

(b1) *there exists a field extension $k \subset K$ and an ample line bundle L on X_K such that $\lambda_K = \varphi_L$;*

(b2) *there exists a finite separable field extension $k \subset K$ and an ample line bundle L on X_K such that $\lambda_K = \varphi_L$.*

(11.6) Definition. Let X be an abelian variety over a field k. A *polarization* of X is an isogeny $\lambda\colon X \to X^t$ that satisfies the equivalent conditions in (11.5).

By the Riemann-Roch Theorem (9.11) the degree of a polarization is always a square: $\deg(\lambda) = d^2$ with $d = \chi(L)$ if $\lambda_{\overline{k}} = \varphi_L$. If λ is an isomorphism (equivalent: λ has degree 1) then we call it a *principal polarization.*

It is clear that the sum of two polarizations is again a polarization. But of course the polarizations do not form a subgroup of $\mathrm{Hom}_{\mathsf{AV}}(X, X^t)$.

We also remark that if λ is a polarization, then for any line bundle L on X_K with $\lambda_K = \varphi_L$ we have that L is ample. In fact, ampleness of a line bundle N on an abelian variety only depends on the associated homomorphism φ_N, as is clear for instance from Proposition (11.4).

(11.7) Let X be an abelian variety over a field k. We have an exact sequence of fppf sheaves

$$0 \longrightarrow X^t \longrightarrow \mathrm{Pic}_{X/k} \longrightarrow \mathit{Hom}^{\mathrm{symm}}(X, X^t) \longrightarrow 0$$

which gives a long exact sequence in fppf cohomology

$$0 \longrightarrow X^t(k) \longrightarrow \mathrm{Pic}(X) \longrightarrow \mathrm{Hom}^{\mathrm{symm}}(X, X^t) \xrightarrow{\partial} H^1_{\mathrm{fppf}}(k, X^t) \longrightarrow \cdots \quad .$$

For $\lambda\colon X \to X^t$ a symmetric homomorphism, $\partial(\lambda)$ is the obstruction for finding a line bundle L on X (over k) with $\varphi_L = \lambda$. Now we know from Proposition (11.2) that $\partial(2\lambda) = 0$; hence $\partial(\lambda)$ lies in the image of

$$H^1_{\mathrm{fppf}}\big(k, X^t[2]\big) \to H^1_{\mathrm{fppf}}(k, X^t)\,.$$

(NOG VERDERE OPM OVER MAKEN, BV VGL MET GALOIS COHOM?)

(11.8) Proposition. *Let $f\colon X \to Y$ be an isogeny. If $\mu\colon Y \to Y^t$ is a polarization of Y, then $f^*\mu := f^t \circ \mu \circ f$ is a polarization of X of degree* $\deg(f^*\mu) = \deg(f)^2 \cdot \deg(\mu)$.

Proof. It is clear that $f^*\mu$ is an isogeny of the given degree. By assumption there is a field extension $k \subset K$ and an ample line bundle M on Y_K such that $\mu_K = \varphi_M$. Then $f^*\mu_K = \varphi_{f^*M}$ and because f is finite f^*M is an ample line bundle on X_K. $\square$

See Exercise (11.1) for a generalization.

(11.9) Definition. Let X and Y be abelian varieties over k. A *(divisorial) correspondence* between X and Y is a line bundle L on $X \times Y$ together with rigidifications $\alpha\colon L_{|\{0\}\times Y} \xrightarrow{\sim} O_Y$ and $\beta\colon L_{|X\times\{0\}} \xrightarrow{\sim} O_X$ that coincide on the fibre over $(0,0)$.

Correspondences between X and Y form a group $\mathrm{Corr}_k(X, Y)$, with group structure obtained by taking tensor products of line bundles. (Cf. the definition of $P_{X/S,\varepsilon}$ in Section (6.2).)

Note that the multiplicative groep $\mathbb{G}_m$ acts (transitively) on the choices of the rigidifications (α, β). Moreover, if $Y = X$ we can speak of symmetric correspondences.

The Poincaré bundle $\mathscr{P} = \mathscr{P}_X$ on $X \times X^t$ comes equipped with a rigidification along $\{0\} \times X^t$. There is a unique rigidification along $X \times \{0\}$ such that the two rigidifications agree at the origin $(0,0)$. We thus obtain an element

$$[\mathscr{P}_X] = (\mathscr{P}_X, \alpha_{\mathscr{P}}, \beta_{\mathscr{P}}) \in \mathrm{Corr}_k(X, X^t)\,.$$

The following proposition makes an alternative definition of the notion of polarization possible.

(11.10) Proposition. *Let X/k be an abelian variety. Then we have a bijection*

$$\{\textit{polarizations } \lambda\colon X \to X^t\} \xrightarrow{\sim} \left\{\begin{matrix} \textit{symmetric divisorial correspondences} \\ (L, \alpha, \beta) \textit{ on } X \times X \textit{ such that } \Delta_X^* L \textit{ is ample}\end{matrix}\right\}$$

by associating to a polarization λ the divisorial correspondence (L,α,β) with $L = (\mathrm{id}_X \times \lambda)^*\mathscr{P}_X$ and α and β the pull-backs under $\mathrm{id}_X \times \lambda$ of the rigidifications $\alpha_{\mathscr{P}}$ and $\beta_{\mathscr{P}}$.

Proof. This is essentially contained in Corollary (11.5). The inverse map is obtained by associating to (L,α,β) the unique homomorphism $\lambda\colon X \to X^t$ such that $(L,\alpha) = (\mathrm{id}_X \times \lambda)^*(\mathscr{P}_X, \alpha_{\mathscr{P}})$ as rigidified line bundles on $X \times X$. The assumption that (L,α,β) is symmetric implies that λ_X is symmetric, and because $(\mathrm{id}_X,\lambda)^*\mathscr{P}_X = \Delta_X^*(\mathrm{id}_X \times \lambda)^*\mathscr{P}_X = \Delta_X^* L$ is ample, λ is a polarization. This establishes the correspondence. □

The alternative definition of a polarization suggested by Proposition (11.10) as "a symmetric self-correspondence such that restriction to the diagonal is ample" is evidently similar in appearance to the definition of a positive definite symmetric bilinear form in linear algebra. But, whereas in linear algebra one dominantly views a bilinear form b as a map $V \times V \to k$ rather than as a map $V \to V^*$ given by $v \mapsto \bigl(w \mapsto b(v,w)\bigr)$, in the theory of abelian varieties the latter point of view dominates. Note further that the role of the evaluation map $V \times V^* \to k$ with $(v,w) \mapsto w(v)$ is played in our context by the Poincaré bundle $\mathscr{P}$.

§ 2. *Pairings.*

We now turn to the study of some bilinear forms attached to isogenies. In its most general form, any isogeny f gives a pairing e_f between $\mathrm{Ker}(f)$ and $\mathrm{Ker}(f^t)$; this is an application of the duality result Theorem (7.5). Of particular interest is the case $f = [n]_X$. If we choose a polarization λ we can map $X[n]$ to $X^t[n]$, and we obtain a bilinear form e_n^λ on $X[n]$, called the Weil pairing. The pairings that we consider satisfy a number of compatibilities, which, for instance, allow us to take the limit of the pairings $e_{\ell^m}^\lambda$, obtaining a bilinear form E^λ with values in $\mathbb{Z}_\ell(1)$ on the Tate module $T_\ell X$. In cohomological terms this pairing is the first Chern class of λ (or rather, of any line bundle representing it). It is the ℓ-adic analogue of what over $\mathbb{C}$ is called the Riemann form associated to a polarization. (See also ???)

(11.11) Definition. Let $f\colon X \to Y$ be an isogeny of abelian varieties over a field k. Write $\beta\colon \mathrm{Ker}(f^t) \xrightarrow{\sim} \mathrm{Ker}(f)^D$ for the isomorphism of Theorem (7.5).

(i) Define

$$e_f\colon \mathrm{Ker}(f) \times \mathrm{Ker}(f^t) \longrightarrow \mathbb{G}_{m,k}$$

to be the perfect bilinear pairing given (on points) by $e_f(x,y) = \beta(y)(x)$. Note that if $\mathrm{Ker}(f)$ is killed by $n \in \mathbb{Z}_{\geqslant 1}$ then e_f takes values in $\mu_n \subset \mathbb{G}_m$. In the particular case that $f = n_X\colon X \to X$ we obtain a pairing

$$e_n\colon X[n] \times X^t[n] \to \mu_n$$

which we call the *Weil pairing*.

(ii) Let $\lambda\colon X \to X^t$ be a homomorphism. We write

$$e_n^\lambda\colon X[n] \times X[n] \to \mu_n$$

for the bilinear pairing given by $e_n^\lambda(x_1,x_2) = e_n\bigl(x_1,\lambda(x_2)\bigr)$. If $\lambda = \varphi_L$ for some line bundle L then we also write e_n^L instead of e_n^λ.

Recall that if A and B are finite commutative group schemes (written additively), a pairing $e\colon A \times B \to \mathbb{G}_m$ is said to be bilinear if $e(a+a',b) = e(a,b)\cdot e(a',b)$ and $e(a,b+b') = e(a,b)\cdot e(a,b')$ for all points a and a' of A and b and b' of B. (Points with values in an arbitrary k-scheme.) The pairing e is said to be perfect if sending a to $e(a,-)\colon B \to \mathbb{G}_m$ gives an isomorphism $A \xrightarrow{\sim} B^D$. This is equivalent to the condition that $b \mapsto e(-,b)$ gives an isomorphism $B \xrightarrow{\sim} A^D$. It is clear from the construction that the pairings e_f, in particular also the Weil pairings, are perfect bilinear pairings. If n is relatively prime to the degree of λ then the pairing e_n^λ is perfect, too.

There are various ways in which we can make the pairings defined above more explicit. We shall give a couple of different points of view.

(11.12) Let us first try to unravel the definition of e_f by going back to the proof of (7.5). This leads to the following description. Let T be a k-scheme. Let L be a rigidified line bundle on Y_T that represents a class $\eta \in \mathrm{Ker}(f^t)(T)$. Then $f^*L \cong O_{X_T}$. Hence the geometric line bundle $\mathbb{L}$ corresponding to L can be described as a quotient of $X_T \times_T \mathbb{A}^1_T$ by an action of $\mathrm{Ker}(f)_T$. More precisely, by what was explained in (7.3) there exists a character $\chi\colon \mathrm{Ker}(f)_T \to \mathbb{G}_{m,T}$ such that the action of a point x of $\mathrm{Ker}(f)$ on $X_T \times_T \mathbb{A}^1_T$ is given (on points) by

$$(z,a) \mapsto \big(z+x, \chi(x)\cdot a\big)\,.$$

The isomorphism $\mathrm{Ker}(f^t) \xrightarrow{\sim} \mathrm{Ker}(f)^D$ of Theorem (7.5) sends η to χ. Hence the pairing e_f is given by $e_f(x,\eta) = \chi(x)$.

(11.13) Next let us give a more geometric description of the Weil pairings e_n. Suppose D is a divisor on X such that nD is linearly equivalent to zero. Write $L = O_X(D)$. As $n^*L \cong O_X$ (cf. Exercise (7.2)), there exists a rational function g on X with divisor $(g) = n^*D$. But also $L^n \cong O_X$, so there exists a rational function f with divisor $(f) = nD$. Then n^*f and g^n both have divisor $n\cdot n^*D = n^*(nD)$, so there is a constant $c \in k^*$ with $g^n = c\cdot (n^*f)$.

Let $x \in X[n](k)$ be a k-rational n-torsion point. We find that

$$g(\xi)^n = c\cdot f(n\xi) = c\cdot f\big(n(\xi+x)\big) = g(\xi+x)^n = \big((t_x^*g)(\xi)\big)^n$$

for all $\xi \in X(\bar{k})$. So $g/t_x^*(g)$ is an n-th root of unity. We claim that in fact $e_n\big(x,[D]\big) = g/t_x^*(g)$.

To see this, note that we have an isomorphism of line bundles $n^*L \xrightarrow{\sim} O_X$ given by $g \mapsto 1$. As described in (11.12), there is a character $\chi\colon X[n] \to \mathbb{G}_m$ such that the natural action of $X[n]$ on n^*L becomes the action of $X[n]$ on O_X given by the character χ. Note that $x \in X[n](k)$ acts on the identity section $1 \in \Gamma(X,O_X)$ as multiplication by $\chi(x)^{-1}$. Hence $g/t_x^*(g) = \chi(x) = e_n\big(x,[D]\big)$, as claimed.

(11.14) Example. We calculate the Weil pairing e_3 on the elliptic curve E over $\mathbb{F}_2$ given by the affine equation $y^2+y = x^3$. This curve has 9 points over $\mathbb{F}_4$ which realise an isomorphism $E[3]\big(\mathbb{F}_4\big) \cong \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$. Let $O = P_\infty$ be the point at ∞, which we take as the identity element on E. The bundle $L = O_E(P_\infty)$ is ample. The associated principal polarization $\lambda\colon E \xrightarrow{\sim} E^t = \mathrm{Pic}^0_{E/\mathbb{F}_2}$ is given on points by $R \mapsto O_E(O-R)$. (Note that this is *minus* the map given by $R \mapsto O_E(R-O)$; see Remark (2.11).)

Let us calculate $e_3^\lambda(Q,P)$ for $P = (0,0)$ and $Q = (1,\alpha)$, where α is an element of $\mathbb{F}_4$ not in $\mathbb{F}_2$. First we note that the function y has divisor $(y) = 3\cdot(P-O)$. Next we compute a function g with divisor $[3]^*(O-P)$. For this we compute the "triplication formula" on E which expresses for a point $R = (\xi,\eta)$ on E the coordinates of $3R$ in those of R. As we have seen in Example (5.26), E is supersingular. The relative Frobenius $\pi = F_{E/\mathbb{F}_2}\colon E \to E$ is an endomorphism of E. One can show that it satisfies $\pi^2 = -2$, for example by verifying that for $T \in E$ the point $\pi^2(T)$ lies on the tangent line to E in T. As -1 on E is given by $(x,y) \mapsto (x, y+1)$ we find that $2R$ has coordinates (ξ^4, η^4+1). Next one calculates that the coordinates of $3R$ are $\big((\xi^9+\xi^3+1)/(\xi+\xi^4)^2, (\eta\xi^3+1)^3/(\xi+\xi^4)^3\big)$. Hence the function

$$g = \frac{x^4+x}{yx^3+1}$$

has divisor $(g) = [3]^*(O-P)$. (Use that $3 \cdot (g) = [3]^*(y) = 3 \cdot [3]^*(O-P)$.)

Now we know that g/t_Q^*g is constant and this constant can be computed by evaluating g and t_Q^*g at a suitable point T; so

$$g/t_Q^*g = g(T)/g(T+Q)\,.$$

For T we take a point rational over $\mathbb{F}_{64}$. Let γ be a generator of $\mathbb{F}_{64}^*$ with $\gamma^{21} = \alpha$ and such that $\delta := \gamma^9 \in \mathbb{F}_8^*$ satisfies $\delta^3+\delta = 1$. Then the point $T = (\gamma^3, \gamma^{18})$ is in $E(\mathbb{F}_{64})$. One easily verifies that $(\gamma^{24}, \gamma^{18}+1)$ is again a point of E, and that it lies on the line through T and Q; hence $T+Q = (\gamma^{24}, \gamma^{18})$. By (11.13) we conclude that $e_3^\lambda(Q,P) = e_3\big(Q,(O-P)\big)$ equals $(\gamma^{12}+\gamma^3)/(\gamma^{33}+\gamma^{24}) = 1/\gamma^{21} = 1/\alpha = \alpha^2$.

The value of $e_3^\lambda(P',Q')$ for any pair $(P',Q') \in E[3]\times E[3]$ can be computed from this using the fact that e_3 is bilinear and alternating; see Cor. (11.22) below.

(11.15) Let $f\colon X \to Y$ be an isogeny of abelian varieties over a field k. By definition, $f^t\colon Y^t \to X^t$ is the unique map such that $(f\times \mathrm{id}_{Y^t})^*\mathscr{P}_Y \cong (\mathrm{id}_X \times f^t)^*\mathscr{P}_X$ as line bundles on $X \times Y^t$ with rigidification along $\{0\}\times Y^t$. Note that this isomorphism is unique, so without ambiguity we can define $\mathscr{Q} := (f\times \mathrm{id}_{Y^t})^*\mathscr{P}_Y = (\mathrm{id}_X \times f^t)^*\mathscr{P}_X$. The diagram to keep in mind is

$$\begin{array}{ccccc} \mathscr{P}_X & & \mathscr{Q} & & \mathscr{P}_Y \\ X\times X^t & \xleftarrow{\mathrm{id}\times f^t} & X\times Y^t & \xrightarrow{f\times \mathrm{id}} & Y\times Y^t \end{array} \tag{1}$$

On the line bundle $\mathscr{Q}$ we have an action of $\mathrm{Ker}(f)\times\{0\}$, lifting the action on $X\times Y^t$ by translations. This action is given by isomorphisms $\sigma_x\colon \mathscr{Q}_T \xrightarrow{\sim} t_{(x,0)}^*\mathscr{Q}_T$, for any k-scheme T and $x \in \mathrm{Ker}(f)\big(T\big)$. Likewise, we have an action of $\{0\}\times\mathrm{Ker}(f^t)$, given by isomorphisms $\tau_q\colon \mathscr{Q}_T \xrightarrow{\sim} t_{(0,q)}^*\mathscr{Q}_T$ for $q \in \mathrm{Ker}(f^t)\big(T\big)$. Unless f is an isomorphism, these two group scheme actions on $\mathscr{Q}$ do not commute, for if they did it would give us an action of $\mathrm{Ker}(f)\times\mathrm{Ker}(f^t)$ and $\mathscr{Q}$ would descend to a line bundle L on $(X\times Y^t)/\mathrm{Ker}(f)\times\mathrm{Ker}(f^t) = Y\times X^t$. But then we had $(-1)^g = \chi(\mathscr{P}_X) = \deg(f)\cdot\chi(L)$, which is possible only if $\deg(f) = 1$. We shall prove that the extent to which the two actions fail to commute is measured by the pairing e_f.

Let $\mathscr{Q}'$ be the restriction of $\mathscr{Q}$ to $X\times\mathrm{Ker}(f^t)$. We have $\mathscr{Q}' = (\mathrm{id}_X\times f^t)^*\big((\mathscr{P}_X)_{|X\times\{0\}}\big)$, so the natural rigidification of $\mathscr{P}_X$ along $X\times\{0\}$ (see (7.7)) gives us a trivialisation $\mathscr{Q}' \xrightarrow{\sim} O_{X\times\mathrm{Ker}(f^t)}$. The action of $\{0\}\times\mathrm{Ker}(f^t)$ on $\mathscr{Q}$ restricts to the trivial action on $\mathscr{Q}'$. It will be useful to think of $\mathscr{Q}'$ as being the sheaf of sections of $\mathbb{A}^1$ over $X\times\mathrm{Ker}(f^t)$. Writing $\mathbb{A}^1_{X\times\mathrm{Ker}(f^t)} = X\times\mathrm{Ker}(f^t)\times\mathbb{A}^1$, the action of a point $(0,q)\in\{0\}\times\mathrm{Ker}(f^t)$ on $\mathscr{Q}'$ corresponds to the action on $X\times\mathrm{Ker}(f^t)\times\mathbb{A}^1$ given by $\tau_q\colon (t,u,a)\mapsto(t,u+q,a)$.

Note that also the action of $\mathrm{Ker}(f)\times\{0\}$ restricts to an action on $\mathscr{Q}'$. To describe this action we apply what was explained in (11.12) in the "universal case", i.e., with $T = \mathrm{Ker}(f^t)$ and $\eta = \mathrm{id}_T$. The corresponding line bundle L on $Y_T = Y\times\mathrm{Ker}(f^t)$ is just the restriction of $\mathscr{P}_Y$ to $Y\times\mathrm{Ker}(f^t)$, so f^*L is precisely our bundle $\mathscr{Q}'$. If we write a point of $\mathrm{Ker}(f)_T =$

$\mathrm{Ker}(f)\times_k\mathrm{Ker}(f^t)$ as a pair (x,u) then the conclusion of (11.12) is that the character $\chi\colon \mathrm{Ker}(f)\times_k \mathrm{Ker}(f^t) \to \mathbb{G}_{m,k}\times_k \mathrm{Ker}(f^t)$ is given by $(x,u)\mapsto \bigl(e_f(x,u),u\bigr)$. Hence the action of a point $(x,0)\in\mathrm{Ker}(f)\times\{0\}$ on $\mathscr{Q}'$ corresponds to the action on $X\times\mathrm{Ker}(f^t)\times\mathbb{A}^1$ given by $\sigma_x\colon (t,u,a)\mapsto \bigl(t+x,u,e_f(x,u)\cdot a\bigr)$.

Now we can start drawing some conclusions. The first result is an interpretation of the pairing e_f as a measure for the extent to which the two group scheme actions on $\mathscr{Q}$ fail to commute.

(11.16) Proposition. *Let $f\colon X\to Y$ be an isogeny of abelian varieties over a field k, and consider the line bundle $\mathscr{Q} := (f\times\mathrm{id}_{Y^t})^*\mathscr{P}_Y = (\mathrm{id}_X\times f^t)^*\mathscr{P}_X$ on $X\times Y^t$. Let T be a k-scheme, $x\in\mathrm{Ker}(f)\bigl(T\bigr)$ and $q\in\mathrm{Ker}(f^t)\bigl(T\bigr)$. Let $\sigma_x\colon \mathscr{Q}_T\xrightarrow{\sim} t^*_{(x,0)}\mathscr{Q}_T$ be the isomorphism that gives the action of $(x,0)\in\mathrm{Ker}(f)\times\{0\}$ on $\mathscr{Q}_T$, and let $\tau_q\colon \mathscr{Q}_T\xrightarrow{\sim} t^*_{(0,q)}\mathscr{Q}_T$ be the isomorphism that gives the action of $(0,q)\in\{0\}\times\mathrm{Ker}(f^t)$. Then we have a commutative diagram*

$$\begin{array}{ccccc}
\mathscr{Q}_T & \xrightarrow{\sigma_x} & t^*_{(x,0)}\mathscr{Q}_T & \xrightarrow{t^*_{(x,0)}\tau_q} & t^*_{(x,q)}\mathscr{Q}_T \\
\| & & & & \big\downarrow{\scriptstyle \text{multiplication by } e_f(x,q)} \\
\mathscr{Q}_T & \xrightarrow{\tau_q} & t^*_{(0,q)}\mathscr{Q}_T & \xrightarrow{t^*_{(0,q)}\sigma_x} & t^*_{(x,q)}\mathscr{Q}_T
\end{array}$$

Proof. A priori it is clear that there exists a constant $c\in\mathbb{G}_m(T)$ such that $(t^*_{(0,q)}\sigma_x)\circ\tau_q = c\cdot(t^*_{(x,0)}\tau_q)\circ\sigma_x$, so all we need to show is that $c=e_f(x,q)$. For this we may restrict everything to $X\times\mathrm{Ker}(f^t)$. As in the above discussion, we think of $\mathscr{Q}'$ as the sheaf of sections of $\mathbb{A}^1$ over $X\times\mathrm{Ker}(f^t)$. We have seen that $(t^*_{(x,0)}\tau_q)\circ\sigma_x$ is given on points by $(t,u,a)\mapsto\bigl(t+x,u+q,e_f(x,u)\cdot a\bigr)$, whereas $(t^*_{(0,q)}\sigma_x)\circ\tau_q$ is given by $(t,u,a)\mapsto\bigl(t+x,u+q,e_f(x,u+q)\cdot a\bigr)$. Because e_f is bilinear, the result follows. $\square$

Next we prove a compatibility result among the two main duality theorems that we have proved in Chapter 7.

(11.17) Proposition. *Let $f\colon X\to Y$ be an isogeny of abelian varieties. Let $\kappa_X\colon X\to X^{tt}$ be the canonical isomorphism.*

(i) *For any k-scheme T and points $x\in\mathrm{Ker}(f)\bigl(T\bigr)$ and $\eta\in\mathrm{Ker}(f^t)\bigl(T\bigr)$ we have the relation $e_{f^t}\bigl(\eta,\kappa_X(x)\bigr) = e_f(x,\eta)^{-1}$.*

(ii) *Let $\beta_1\colon \mathrm{Ker}(f^t)\xrightarrow{\sim}\mathrm{Ker}(f)^D$ and $\beta_2\colon \mathrm{Ker}(f^{tt})\xrightarrow{\sim}\mathrm{Ker}(f^t)^D$ be the canonical isomorphisms as in* Theorem (7.5), *and let $\gamma\colon \mathrm{Ker}(f)^{DD}\xrightarrow{\sim}\mathrm{Ker}(f)$ be the isomophism of* Theorem (3.22). *Then the isomorphism $\mathrm{Ker}(f)\xrightarrow{\sim}\mathrm{Ker}(f^{tt})$ induced by κ_X equals $-\beta_2^{-1}\circ\beta_1^D\circ\gamma^{-1}$.*

Proof. (i) Consider the commutative diagram

$$\begin{array}{ccccc}
X\times X^t & \xleftarrow{\mathrm{id}\times f^t} & X\times Y^t & \xrightarrow{f\times\mathrm{id}} & Y\times Y^t \\
{\scriptstyle \kappa_X\times\mathrm{id}}\big\downarrow & & {\scriptstyle \kappa_X\times\mathrm{id}}\big\downarrow & & \big\downarrow{\scriptstyle \kappa_Y\times\mathrm{id}} \\
X^{tt}\times X^t & \xleftarrow{\mathrm{id}\times f^t} & X^{tt}\times Y^t & \xrightarrow{f^{tt}\times\mathrm{id}} & Y^{tt}\times Y^t
\end{array} \qquad (2)$$

If we read the lower row from right to left (term by term!), we get the row

$$Y^t\times Y^{tt} \xleftarrow{\mathrm{id}\times f^{tt}} Y^t\times X^{tt} \xrightarrow{f^t\times\mathrm{id}} X^t\times X^{tt}$$

which is precisely (1) for the morphism $f^t\colon Y^t \to X^t$. Now the result follows from the previous proposition, with the -1 in the exponent coming from the fact that we are reading the lower row in (2) from right to left, thereby switching factors.

(ii) This follows from (i) using the relations $e_f(x,\eta) = \beta_1(\eta)\bigl(x\bigr) = (\beta_1^D\circ\gamma^{-1})(x)\bigl(\eta\bigr)$ and $e_{f^t}\bigl(\eta,\kappa_X(x)\bigr) = \beta_2\bigl(\kappa_X(x)\bigr)\bigl(\eta\bigr)$. □

(11.18) Example. Let X be an abelian variety over k. Let $\mathscr{P} = \mathscr{P}_X$ be its Poincaré bundle. Let n be a positive integer, and let $e_n\colon X[n]\times X^t[n] \to \mu_n$ be the Weil pairing.

The geometric line bundle on $X\times X^t[n]$ that corresponds to $\mathscr{P}_{|X\times X^t[n]}$ is the quotient of $\mathbb{A}^1_{X\times X^t[n]} = X\times X^t[n]\times\mathbb{A}^1$ under the action of $X[n]\times\{0\}$, with $x\in X[n]$ acting on $X\times X^t[n]\times\mathbb{A}^1$ by $\sigma_x\colon (t,u,a)\mapsto \bigl(t+x,u,e_n(x,u)\cdot a\bigr)$.

To make this completely explicit, suppose $k=\overline{k}$ and $\mathrm{char}(k)\nmid n$, so that $X[n]$ and $X^t[n]$ are constant group schemes, each consisting of n^{2g} distinct points. Then for $\xi\in X^t[n](k)$, the restriction of the Poincaré bundle to $X\times\{\xi\}$ is given by

$$\mathscr{P}_{|X\times\{\xi\}}\bigl(U\bigr) = \bigl\{f\in O_X(n^{-1}U)\bigm| f(v+x) = e_n(x,\xi)\cdot f(v) \text{ for all } v\in n^{-1}U \text{ and } x\in X[n]\bigr\}\,.$$

For the restriction of $\mathscr{P}_X$ to $X[n]\times X^t$ we have an analogous description; namely, the corresponding geometric line bundle is the quotient of $\mathbb{A}^1_{X[n]\times X^t} = X[n]\times X^t\times\mathbb{A}^1$ under the action of $\{0\}\times X^t[n]$, with $\xi\in X^t[n]$ acting on $X[n]\times X^t\times\mathbb{A}^1$ by $\tau_\xi\colon (t,u,a)\mapsto \bigl(t,u+\xi,e_n(t,\xi)^{-1}\cdot a\bigr)$. Note, however, that whereas our description of $\mathscr{P}_{|X\times X^t[n]}$ is essentially a reformulation of the definition of the Weil pairing, to arrive at our description of $\mathscr{P}_{|X[n]\times X^t}$ we use (i) of Proposition (11.17).

(11.19) Let L be a non-degenerate line bundle on an abelian variety X. As the associated isogeny $\varphi_L\colon X\to X^t$ is symmetric, we have $K(L) = \mathrm{Ker}(\varphi_L) = \mathrm{Ker}(\varphi_L^t)$, and we obtain a pairing

$$e_{\varphi_L}\colon K(L)\times K(L)\to\mathbb{G}_m\,.$$

On the other hand we have the theta group $1\longrightarrow\mathbb{G}_m\longrightarrow\mathscr{G}(L)\longrightarrow K(L)\longrightarrow 0$, and this, too, gives a pairing

$$e^L\colon K(L)\times K(L)\to\mathbb{G}_m\,.$$

(11.20) Proposition. *We have* $e_{\varphi_L} = e^L$.

Proof. We apply what was explained in (11.15) to the isogeny $\varphi_L\colon X\to X^t$. We identify $X\times X^{tt}$ with $X\times X$ via the isomorphism $\mathrm{id}\times\kappa_X\colon X\times X\xrightarrow{\sim} X\times X^{tt}$. The line bundle $\mathscr{Q} := (\varphi_L\times\kappa_X)^*\mathscr{P}_{X^t} = (\mathrm{id}\times\varphi_L)^*\mathscr{P}_X$ is none other than the Mumford bundle $\Lambda(L)$ associated to L. Let $\mathscr{Q}' := \mathscr{Q}_{|X\times K(L)} = \Lambda(L)_{|X\times K(L)}$ which, as we already knew from Lemma (2.17), is trivial.

Let T be a k-scheme, and consider T-valued points x, $y\in K(L)\bigl(T\bigr)$. Possibly after replacing T by a covering we can choose isomorphisms $\varphi\colon L_T\xrightarrow{\sim} t_x^*L_T$ and $\psi\colon L_T\xrightarrow{\sim} t_y^*L_T$. Then (x,φ) and (y,ψ) are T-valued points of $\mathscr{G}(L)$, and by definition of the pairing e^L we have the relation

$$(t_y^*\varphi)\circ\psi = e^L(x,y)\cdot(t_x^*\psi)\circ\varphi\,. \tag{3}$$

We can also view ψ as the trivialisation

$$\psi\colon O_{X_T\times\{y\}}\xrightarrow{\sim}\Lambda(L_T)_{X_T\times\{y\}} = t_y^*L_T\otimes L_T^{-1}$$

that sends $1 \in \Gamma(X_T, O_{X_T\times\{y\}})$ to the global section ψ of $t_y^*L_T \otimes L_T^{-1}$. If $\sigma_x\colon \mathscr{Q}_T \to t_{(x,0)}^*\mathscr{Q}_T$ is the isomorphism that gives the action of $(x,0) \in K(L)\times\{0\}$ on $\mathscr{Q}$ then it follows from what we have seen in (11.15) that we have a commutative diagram

$$\begin{array}{ccc} \Lambda(L)_{X_T\times\{y\}} & \xrightarrow{(\sigma_x)_{|X_T\times\{y\}}} & t_{(x,0)}^*\Lambda(L)_{|X_T\times\{y\}} \\ {\scriptstyle\psi}\uparrow & & \uparrow{\scriptstyle e_{\varphi_L}(x,y)\cdot\left(t_{(x,0)}^*\psi\right)} \\ O_{X_T\times\{y\}} & \xrightarrow{\text{can}} & t_{(x,0)}^*O_{X_T\times\{y\}} \end{array}.$$

We have $t_{(x,0)}^*\Lambda(L_T) = m^*(t_x^*L_T\otimes L_T^{-1})\otimes p_1^*(t_x^*L_T\otimes L_T^{-1})^{-1}\otimes\Lambda(L_T)$. Taking this as an identification, σ_x is given on sections by $s \mapsto m^*\varphi\otimes p_2^*\varphi^{-1}\otimes s$. (Note that this does not depend on the choice of φ.) Now restrict to $X_T\times\{y\}$ and use the natural identification

$$t_{(x,0)}^*\Lambda(L_T)_{|X_T\times\{y\}} = t_{x+y}^*L_T\otimes t_x^*L_T^{-1} = \mathit{Hom}(t_x^*L_T, t_{x+y}^*L_T)\,.$$

we find that $\sigma_x\circ\psi$ maps $1 \in \Gamma(X_T, O_{X_T\times\{y\}})$ to the homomorphism $t_y^*\varphi\circ\psi\circ\varphi^{-1}\colon t_x^*L_T \to t_{x+y}^*L_T$. On the other hand, the composition $(t_{(x,0)}^*\psi)\circ\text{can}$ sends 1 to $t_x^*\psi$. Hence we have

$$t_y^*\varphi\circ\psi\circ\varphi^{-1} = e_{\varphi_L}(x,y)\cdot t_x^*\psi$$

and comparison with (3) now gives the result. □

(11.21) Proposition. (i) *Let $f\colon X\to Y$ be a homomorphism of abelian varieties over k. Then for any integer $n \geqslant 1$ the diagram*

$$\begin{array}{ccc} X[n]\times Y^t[n] & \xrightarrow{1\times f^t} & X[n]\times X^t[n] \\ {\scriptstyle f\times 1}\downarrow & & \downarrow{\scriptstyle e_n} \\ Y[n]\times Y^t[n] & \xrightarrow{e_n} & \mu_n \end{array}$$

is commutative. In other words: if T is a k-scheme, $x \in X[n](T)$ and $\eta \in Y^t[n](T)$ then $e_n\big(f(x),\eta\big) = e_n\big(x, f^t(\eta)\big)$.

(ii) *Let $f\colon X\to Y$ and $g\colon Y\to Z$ be isogenies, and write $h := g\circ f\colon X\to Z$. Then we have "commutative diagrams"*

$$\begin{array}{ccccc} \mathrm{Ker}(f) & \times & \mathrm{Ker}(f^t) & \xrightarrow{e_f} & \mathbb{G}_m \\ {\scriptstyle i}\downarrow & & \uparrow{\scriptstyle g^t} & & \| \\ \mathrm{Ker}(h) & \times & \mathrm{Ker}(h^t) & \xrightarrow{e_h} & \mathbb{G}_m \end{array} \quad \textit{and} \quad \begin{array}{ccccc} \mathrm{Ker}(g) & \times & \mathrm{Ker}(g^t) & \xrightarrow{e_g} & \mathbb{G}_m \\ {\scriptstyle f}\uparrow & & \downarrow{\scriptstyle i} & & \| \\ \mathrm{Ker}(h) & \times & \mathrm{Ker}(h^t) & \xrightarrow{e_h} & \mathbb{G}_m \end{array}$$

where the maps labelled "i" are the natural inclusion homomorphisms. By our assertion that the first diagram is commutative we mean that if T is a k-scheme, $x \in \mathrm{Ker}(f)(T)$ and $\eta \in \mathrm{Ker}(h^t)(T)$ then $e_f\big(x, g^t(\eta)\big) = e_h\big(i(x),\eta\big)$; similarly for the second diagram.

Proof. (i) Let $\chi\colon Y[n]_T \to \mathbb{G}_{m,T}$ be the character corresponding to η, as in (11.12). Then the character corresponding to $h^t(\eta)$ is $\chi\circ h\colon X[n]_T\to\mathbb{G}_{m,T}$. By (11.12) we find

$$e_n\big(h(x),\eta\big) = \chi\big(h(x)\big) = \chi\circ h(x) = e_n\big(x, h^t(\eta)\big)\,.$$

(ii) Let $\chi\colon \mathrm{Ker}(h)_T \to \mathbb{G}_{m,T}$ be the character corresponding to η. Then the character $\mathrm{Ker}(f)_T\to\mathbb{G}_{m,T}$ corresponding to $g^t(\eta)$ is simply $\chi\circ i$. Hence by what was explained in (11.12),

$e_h\big(i(x),\eta\big) = \chi\big(i(x)\big) = \chi\circ i(x) = e_f\big(x, g^t(\eta)\big)$. This gives the first commutative diagram. For the second, apply the first diagram to the composition $f^t\circ g^t\colon Z^t \to Y^t \to X^t$; then apply (i) of Proposition (11.17). □

(11.22) Corollary. *Let $\lambda\colon X \to X^t$ be a polarization, and let n be a positive integer. Then the pairing $e_n^\lambda\colon X[n]\times X[n] \to \mu_n$ is alternating: for any $x \in X[n]\big(T\big)$ with T a k-scheme we have $e_n^\lambda(x,x) = 1$.*

Proof. Without loss of generality we may assume that $k = \overline{k}$ and write $\lambda = \varphi_L$ for some ample L. Consider the composition $n\lambda = \lambda\circ[n]_X$. Applying (ii) of Proposition (11.21) we find a commutative diagram

$$\begin{array}{ccc} X[n]\times X^t[n] & \xrightarrow{e_n} & \mathbb{G}_m \\ {\scriptstyle i}\big\downarrow \qquad \big\uparrow{\scriptstyle\lambda} & & \big\| \\ \mathrm{Ker}(n\lambda)\times\mathrm{Ker}(n\lambda) & \xrightarrow{e_{n\lambda}} & \mathbb{G}_m \end{array}$$

This gives $e_n^\lambda(x,x) = e_n\big(x,\lambda\circ i(x)\big) = e_{n\lambda}\big(i(x),i(x)\big) = 1$, where in the last step we use Proposition (11.20) together with the remark that $n\lambda = \varphi_{L^n}$. □

In particular, we find that the pairing e_n^λ is skew-symmetric: $e_n^\lambda(x,y) = e_n^\lambda(y,x)^{-1}$. Note, however, that skew-symmetry is weaker in general than the property of being alternating.

(11.23) Let X be an abelian variety over a field k. Fix a separable closure $k\subset k_s$. As usual, ℓ denotes a prime number different from char(k). Let $x = (0,x_1,x_2,\ldots)$ be an element of $T_\ell X$ and $\xi = (0,\xi_1,\xi_2,\ldots)$ and element of $T_\ell X^t$. Applying (ii) of Proposition (11.21) we find that

$$e_{\ell^m}(x_m,\xi_m) = e_{\ell^{m+1}}(\ell\cdot x_{m+1},\xi_{m+1}) = e_{\ell^{m+1}}(x_{m+1},\xi_{m+1})^\ell\,.$$

This means precisely that

$$E(x,\xi) = \big(1, e_\ell(x_1,\xi_1), e_{\ell^2}(x_2,\xi_2),\ldots\big)$$

is a well-defined element of $\mathbb{Z}_\ell(1) = T_\ell\mathbb{G}_m$. The map $(x,\xi)\mapsto E(x,\xi)$ defines a perfect bilinear pairing

$$E\colon T_\ell X\times T_\ell X^t \to \mathbb{Z}_\ell(1)\,.$$

If $\beta\colon T_\ell X^t \xrightarrow{\sim} (T_\ell X)^\vee(1)$ is the canonical isomorphism as in Proposition (10.9) then the pairing E is nothing else but the composition

$$T_\ell X\times T_\ell X^t \xrightarrow{\mathrm{id}\times\beta} T_\ell X\times (T_\ell X)^\vee(1) \xrightarrow{\mathrm{ev}} \mathbb{Z}_\ell(1)$$

where the map “ev” is the canonical pairing, or “evaluation pairing”. Note that the pairing E is equivariant with respect to the natural action of $\mathrm{Gal}(k_s/k)$ on all the terms involved.

If $\lambda\colon X\to X^t$ is a polarization, we obtain a pairing

$$E^\lambda\colon T_\ell X\times T_\ell X \to \mathbb{Z}_\ell(1) \qquad \text{by} \qquad E^\lambda(x,x') := E\big(x, T_\ell\lambda(x')\big)\,.$$

If $\lambda = \varphi_L$ we also write E^L for E^λ. It readily follows from Corollary (11.22) that the pairing E^λ is alternating.

Putting everything together, E^λ is a $\mathrm{Gal}(k_s/k)$-invariant element in $\big(\wedge^2(T_\ell X)^\vee\big)(1)$. The cohomological interpretation is that E^λ is the first Chern class of λ, or rather of any line bundle representing λ. Note that $\big(\wedge^2(T_\ell X)^\vee\big)(1) = H^2\big(X_{k_s},\mathbb{Z}_\ell(1)\big)$, see Corollary (10.39).

§ 3. *Existence of polarizations, and Zarhin's trick.*

(11.24) Suppose we have an abelian variety X of dimension g over a field k. If $g = 1$ then X is an elliptic curve, and the origin O (as a divisor on X) gives a principal polarization (via $Q \mapsto O - Q$). If $g \geqslant 2$ then in general X does not carry a principal polarization, not even if we allow an extension of the base field. Let us explain why this is so.

Fix $g \geqslant 2$. We shall use the fact that there exists an algebraically closed field k and an abelian variety Y of dimension g over k such that $\mathrm{End}(Y) = \mathbb{Z}$. A proof of this shall be given later; see ??. Note that this does not work for arbitrary k; for instance, every abelian variety over $\overline{\mathbb{F}}_p$ has $\mathbb{Z} \subsetneq \mathrm{End}(Y)$, as we shall see in ??.

If Y carries no principal polarization then we have the desired example. Hence we may assume there is a principal polarization $\lambda\colon Y \to Y^t$. As $k = \overline{k}$ there is a line bundle L with $\lambda = \varphi_L$. Because λ is principal and $\mathrm{End}(X) = \mathbb{Z}$ the only polarizations of Y are those of the form $\varphi_{L^n} = n \cdot \lambda$, of degree n^{2g}.

On the other hand, if ℓ is any prime number different from $\mathrm{char}(k)$ then $Y[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^{2g}$ as group schemes. Hence Y has a subgroup scheme H of order ℓ. Let $q\colon Y \to X := Y/H$ be the quotient. If $\mu\colon X \to X^t$ is a polarization then $q^*\mu$ is a polarization of Y, with $\deg(q^*\mu) = \ell^2 \cdot \deg(\mu)$. But as just explained, any polarization of Y has degree equal to n^{2g} for some $n \in \mathbb{N}$. Hence μ cannot be principal.

With a similar construction we shall see later that an abelian variety of dimension $g \geqslant 2$ over a field of characteristic p in general does not even carry a separable polarization; see ??.

To arrive at some positive results, we shall now first give a very useful criterion for when a polarization $\lambda\colon X \to X^t$ descends over an isogeny $f\colon X \to Y$. If L is a line bundle on X then by Theorem (8.10) there exists a line bundle M on Y with $L \cong f^*M$ if and only if the following conditions are satisfied:

(a) $\mathrm{Ker}(f)$ is contained in $K(L)$ and is totally isotropic with respect to the pairing $e_{\mathscr{G}(L)} = e_{\varphi_L}$;
(b) the inclusion map $\mathrm{Ker}(f) \hookrightarrow K(L)$ can be lifted to a homomorphism $\mathrm{Ker}(f) \hookrightarrow \mathscr{G}(L)$.

(The second condition in (a) is in fact implied by (b).) As we shall prove now, in order for a polarization to descend, it suffices that the analogue of condition (a) holds.

(11.25) Proposition. *Let $\lambda\colon X \to X^t$ be a symmetric isogeny, and let $f\colon X \to Y$ be an isogeny.*

(i) *There exists a symmetric isogeny $\mu\colon Y \to Y^t$ such that $\lambda = f^*\mu := f^t \circ \mu \circ f$ if and only if* $\mathrm{Ker}(f)$ *is contained in* $\mathrm{Ker}(\lambda)$ *and is totally isotropic with respect to the pairing* $e_\lambda\colon \mathrm{Ker}(\lambda) \times \mathrm{Ker}(\lambda) \to \mathbb{G}_m$. *If such an isogeny μ exists then it is unique.*

(ii) *Assume that an isogeny μ as in* (i) *exists. Then μ is a polarization if and only if λ is a polarization.*

Note that the "only if" in (ii) was already proven in Proposition (11.8). For this implication the assumption that f is an isogeny can be weakened; see Exercise (11.1).

Proof. (i) If $\lambda = f^t \circ \mu \circ f$ then $\mathrm{Ker}(f) \subset \mathrm{Ker}(\lambda)$ and it follows from (ii) of Proposition (11.21), applied with $g = (f^t \circ \mu)$ and $h = \lambda$, that $\mathrm{Ker}(f)$ is totally isotropic for the pairing e_λ.

For the converse, assume $\mathrm{Ker}(f)$ is contained in $\mathrm{Ker}(\lambda)$ and is totally isotropic with respect to e_λ. Consider the line bundle $M := (1 \times \lambda)^*\mathscr{P}_X$ on $X \times X$. Recall from Example (8.26) that the theta group $\mathscr{G}(M)$ is naturally isomorphic to the Heisenberg group associated to the group scheme $\mathrm{Ker}(\lambda)$. We have natural actions of $\mathrm{Ker}(\lambda) \times \{0\}$ and $\{0\} \times \mathrm{Ker}(\lambda)$ on M; for the first action note that M can also be written as $(\lambda \times 1)^*\mathscr{P}_{X^t}$. The assumption that $\mathrm{Ker}(f) \subset \mathrm{Ker}(\lambda)$

is totally isotropic for e_λ means precisely that the actions of $\mathrm{Ker}(f) \times \{0\}$ and of $\{0\} \times \mathrm{Ker}(f)$ commute, and therefore define an action of $\mathrm{Ker}(f)\times\mathrm{Ker}(f)$ on M. This gives us a line bundle N on $Y \times Y$ such that $M \cong (f \times f)^*N$. If $\mu\colon Y \to Y^t$ is the (unique) homomorphism such that $N = (1\times\mu)^*\mathscr{P}_Y$ then we get the desired relation $\lambda = f^t\circ\mu\circ f$. The uniqueness of μ is immediate from Lemma (5.4). But we also have $\lambda = \lambda^t = (f^t\circ\mu\circ f)^t = f^t\circ\mu^t\circ f$. Hence $\mu = \mu^t$.

(ii) By Proposition (11.2) there exists a field extension $k \subset K$ and a line bundle L on Y_K with $\mu_K = \varphi_L$, and then $\lambda_K = \varphi_{f^*L}$. Because f is finite, L is effective if and only if f^*L is effective. □

(11.26) Corollary. *Let X be an abelian variety over an algebraically closed field. Then X is isogenous to an abelian variety that admits a principal polarization.*

Proof. Start with any polarization $\lambda\colon X \to X^t$. By Lemma (8.22) there exists a Lagrangian subgroup $H \subset \mathrm{Ker}(\lambda)$. (There clearly exists a subgroup $H \subset \mathrm{Ker}(\lambda)$ satisfying condition (i) of that Lemma.) By the previous Proposition, λ descends to a principal polarization on X/H. □

The conclusion of the Corollary no longer holds in general if we drop the assumption that the ground field is algebraically closed. For examples, see e.g. Howe [1], [2] and Silverberg-Zarhin [1].

(11.27) Before we turn to Zarhin's trick, we recall from Exercise (7.8) some notation.

Suppose X is an abelian variety and $\alpha = (a_{ij})$ is an $r \times s$ matrix with integral coefficients. Then we denote by $[\alpha]_X\colon X^s \to X^r$ the homomorphism given by

$$[\alpha]_X\big(x_1,\dots,x_s\big) = \Big(a_{11}x_1 + a_{12}x_2 + \cdots + a_{1s}x_s, \dots, \sum_{j=1}^{s} a_{ij}x_j, \dots, a_{r1}x_1 + a_{r2}x_2 + \cdots + a_{rs}x_s\Big)\,.$$

For $r = s = 1$ this just gives our usual notation $[n]_X$ for the "multiplication by n" maps. As another example, the 1×2 matrix $(1\,1)$ gives the group law on X while the 2×1 matrix $\begin{pmatrix}1\\1\end{pmatrix}$ gives the diagonal.

If β is a $q \times r$ matrix with integral coefficients then $[\beta\cdot\alpha]_X = [\beta]_X\circ[\alpha]_X\colon X^s \to X^q$. It follows that if α is an invertible $r \times r$ matrix then $[\alpha]_X$ is an automorphism of X^r. Further, if $f\colon X \to Y$ is a homomorphism of abelian varieties then for any integral $r \times s$ matrix α,

$$[\alpha]_Y\circ\underbrace{(f,\dots,f)}_{s} = \underbrace{(f,\dots,f)}_{r}\circ[\alpha]_X\colon X^s \to Y^r\,.$$

(11.28) Proposition. *Let X be an abelian variety of dimension g.*

(i) *If $\alpha \in M_r(\mathbb{Z})$ then $[\alpha]_X\colon X^r \to X^r$ has degree $\det(\alpha)^{2g}$.*

(ii) *Let β be an $r \times s$ matrix with integral coefficients. Then $\big([\beta]_X\big)^t = \big[{}^{\mathrm{t}}\beta\big]_{X^t}$, where ${}^{\mathrm{t}}\beta$ is the transposed matrix.*

Proof. (i) If $\det(\alpha) = 0$ then it is readily seen that $[\alpha]_X$ has infinite kernel, so by convention we have $\deg\big([\alpha_X]\big) = 0$. Now assume $\det(\alpha) \neq 0$, and let $\{e_1,\dots,e_r\}$ be the standard ordered basis of $\mathbb{Z}^r$. By the theory of elementary divisors, there is an ordered basis $\{f_1,\dots,f_r\}$ for $\mathbb{Z}^r$ and a sequence of nonzero integers $(n_1,\dots,n_r)$ such that $\alpha(e_i) = n_i\cdot f_i$. Let $\beta \in \mathrm{GL}_r(\mathbb{Z})$ be the matrix with $\beta(e_i) = f_i$, and let $\gamma = \mathrm{diag}(n_1,\dots,n_r)$ be the diagonal matrix with coefficients n_i. Then $[\beta]_X$ is an automorphism of X^r and it is clear that $[\gamma]_X\colon X^r \to X^r$, which is given by

$(x_1, \ldots, x_r) \mapsto (n_1x_1, \ldots, n_rx_r)$, has degree $(n_1 \cdots n_r)^{2g} = \det(\alpha)^{2g}$. As $[\alpha]_X = [\gamma]_X \circ [\beta]_X$ the claim follows.

(ii) Write $\beta = (b_{ij})$. Any line bundle L on X^r with class in Pic^0 can be written as $L = p_1^*L_1 \otimes \cdots \otimes p_r^*L_r$, where the $p_i\colon X^r \to X$ are the projection maps and the L_i are line bundles on X with class in Pic^0. Because $(X^s)^t \cong (X^t)^s$ (cf. Exercise (6.2)) it suffices to know the restriction of $[\beta]_X^*L$ to each of the coordinate axes $\{0\} \times \cdots \times \{0\} \times X \times \{0\} \times \cdots \times \{0\}$. But the restriction of $[\beta]_X$ to the j-th coordinate axis is the map $X \to X^r$ given by $x \mapsto (b_{1j}x, b_{2j}x, \ldots, b_{rj}x)$ and the pull-back of L under this map is

$$b_{1j}^*L_1 \otimes \cdots \otimes b_{rj}^*L_r = L_1^{\otimes b_{1j}} \otimes \cdots \otimes L_r^{\otimes b_{rj}} .$$

This means precisely that $[\beta]_X^t\colon (X^r)^t = (X^t)^r \to (X^s)^t = (X^t)^s$ is the map given by the matrix

$$\begin{pmatrix} b_{11} & \cdots & b_{i1} & \cdots & b_{r1} \\ \vdots & & \vdots & & \vdots \\ b_{1j} & \cdots & b_{ij} & \cdots & b_{rj} \\ \vdots & & \vdots & & \vdots \\ b_{1s} & \cdots & b_{is} & \cdots & b_{rs} \end{pmatrix} = {}^{\mathrm{t}}\beta ,$$

as claimed. □

(11.29) Theorem. (Zarhin's trick) *Let X be an abelian variety over a field k. Then $X^4 \times (X^t)^4$ carries a principal polarization.*

Proof. Suppose we have an abelian variety Y, a polarization $\mu\colon Y \to Y^t$, and an endomorphism $\alpha\colon Y \to Y$. Consider the isogeny $f\colon Y \times Y \to Y \times Y^t$ given by $(y_1, y_2) \mapsto \big(y_1 - \alpha(y_2), \mu(y_2)\big)$. The kernel is given by $\mathrm{Ker}(f) = \big\{(\alpha(y), y) \bigm| y \in \mathrm{Ker}(\mu)\big\}$. In particular, $\deg(f) = \deg(\mu)$. Proposition (11.25) tells us under what conditions the polarization $\mu \times \mu\colon (Y \times Y) \to (Y^t \times Y^t)$ descends to a polarization on $Y \times Y^t$ via the isogeny f. Namely: there exists a polarization ν on $Y \times Y^t$ with $f^*\nu = (\mu \times \mu)$ if and only if
(a) $\alpha\big(\mathrm{Ker}(\mu)\big) \subseteq \mathrm{Ker}(\mu)$, and
(b) $e_\mu\big(\alpha(y_1), \alpha(y_2)\big) \cdot e_\mu(y_1, y_2) = 1$ for all (scheme valued) points y_1, y_2 of $\mathrm{Ker}(\mu)$.
Note that if such a descended polarization ν exists then it is principal.

Condition (a) means that there exists an endomorphism $\beta\colon Y^t \to Y^t$ such that $\beta \circ \mu = \mu \circ \alpha$. By (ii) of Proposition (11.21),

$$e_\mu\big(\alpha(y_1), \alpha(y_2)\big) = e_{\mu \circ \alpha}\big(y_1, \alpha(y_2)\big) = e_{\beta \circ \mu}\big(y_1, \alpha(y_2)\big) = e_\mu\big(y_1, \beta^t\alpha(y_2)\big) ,$$

so (b) is equivalent to the condition that $e_\mu\big(y_1, (1 + \beta^t\alpha)(y_2)\big) = 1$ for all y_1, y_2 in $\mathrm{Ker}(\mu)$. As e_μ is a pefect pairing on $\mathrm{Ker}(\mu)$, this is equivalent to the condition that $(1 + \beta^t\alpha) \in \mathrm{End}(Y)$ kills $\mathrm{Ker}(\mu)$.

We now apply this with $Y = X^4$. Choose any polarization λ on X, and take $\mu = \lambda^4$ (so $\mu = \lambda \times \lambda \times \lambda \times \lambda$). For α we take the endomorphism $[\alpha]_X$ given by a 4×4 matrix α with integral coefficients. As $\lambda^4 \circ [\alpha]_X = [\alpha]_{X^t} \circ \lambda^4$, condition (a) is automatically satisfied, and we have $\beta = [\alpha]_{X^t}$ in the above. Using (ii) of Proposition (11.28) we find that the only condition that remains is that $[\mathrm{id}_4 + {}^{\mathrm{t}}\alpha\alpha]_X$ kills $\mathrm{Ker}(\mu) = \mathrm{Ker}(\lambda)^4$, where id_4 is the 4×4 identity matrix.

Choose an integer m such that $\mathrm{Ker}(\lambda) \subset X[m]$. We are done if we can find an integral 4×4 matrix α such that $\mathrm{id}_4 + {}^{\mathrm{t}}\alpha\alpha \equiv 0 \bmod m$. To see that such a matrix can be found we use the fact that every integer can be written as a sum of four squares. In particular there exist integers a, b, c, d with $a^2 + b^2 + c^2 + d^2 = m - 1$. Now take

$$\alpha = \begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix}, \tag{4}$$

for which we have $\mathrm{id}_4 + {}^{\mathrm{t}}\alpha\alpha = m \cdot \mathrm{id}_4$. □

(11.30) Remarks. (i) The choice of the matrix α can be explained as follows. Consider the Hamiltonian quaternion algebra $\mathbb{H} = \mathbb{R}\cdot 1 + \mathbb{R}\cdot i + \mathbb{R}\cdot j + \mathbb{R}\cdot k$, which is a central simple algebra over $\mathbb{R}$. For $x = a\cdot 1 + b\cdot i + c\cdot j + d\cdot k$ we define its complex conjugate by $\bar{x} = a\cdot 1 - b\cdot i - c\cdot j - d\cdot k$. The reduced trace and norm of $\mathbb{H}$ over $\mathbb{R}$ are given by

$$\mathrm{Trd}_{\mathbb{H}/\mathbb{R}}(x) = x + \bar{x} = 2a \qquad \text{and} \qquad \mathrm{Nrd}_{\mathbb{H}/\mathbb{R}}(x) = x\bar{x} = a^2 + b^2 + c^2 + d^2\,.$$

Further, taking $\{1, i, j, k\}$ as a basis of $\mathbb{H}$, left multiplication by x is given precisely by the matrix (4). The map $h\colon \mathbb{H} \to M_4(\mathbb{R})$ sending x to this matrix is an injective homomorphism of $\mathbb{R}$-algebras, and we have $h(\bar{x}) = {}^{\mathrm{t}}h(x)$ and $\mathrm{Nrd}_{\mathbb{H}/\mathbb{R}}(x) = \det\bigl(h(x)\bigr)$. Further it is clear that h maps the subring $\mathbb{Z}\cdot 1 + \mathbb{Z}\cdot i + \mathbb{Z}\cdot j + \mathbb{Z}\cdot k$ into $M_4(\mathbb{Z})$. In sum, we can think of α as being the (left) multiplication by $a\cdot 1 + b\cdot i + c\cdot j + d\cdot k$, where a, b, c, d are chosen such that $a^2 + b^2 + c^2 + d^2 = m - 1$.

(ii) In general there is no positive n such that for any abelian variety X the nth power X^n admits a principal polarization. To see this we go back to the example in (11.24). We start with an abelian variety Y of dimension $g \geqslant 2$ over a field $k = \overline{k}$ such that $\mathrm{End}(Y) = \mathbb{Z}$ and such that Y does admit a principal polarization; see ?? for the existence. Any homomorphism $Y^n \to (Y^t)^n$ is of the form $\lambda^n \circ [\alpha]_Y = [\alpha]_{Y^t} \circ \lambda^n$ for some $\alpha \in M_n(\mathbb{Z})$, and it easily follows from (ii) of Proposition (11.28) that this homomorphism is symmetric if and only if $\alpha = {}^{\mathrm{t}}\alpha$. Now choose a prime number ℓ different from $\mathrm{char}(k)$, and choose a subgroup $H \subset Y$ of order ℓ, generated by a point of order ℓ. Let $\pi\colon Y \to X := Y/H$ be the quotient.

Let μ be any polarization on X^n. By what was just explained we have $(\pi^n)^*\mu = \lambda^n \circ [\alpha]_Y$ for some $\alpha \in M_n(\mathbb{Z})$. Moreover, $H \times \cdots \times H \subset \mathrm{Ker}\bigl([\alpha]_Y\bigr)$, which readily implies that α is divisible by ℓ, say $\alpha = \ell \cdot \beta$. Further we have $\deg(\mu)\cdot \ell^{2n} = \deg\bigl([\alpha]_Y\bigr) = \ell^{2ng}\cdot \det(\beta)^{2g}$, so $\deg(\mu) = \ell^{2n(g-1)}\cdot \det(\beta)^{2g}$. In particular, X^n does not carry a principal polarization.

Exercises.

(11.1) Let $f\colon X \to Y$ be a homomorphism of abelian varieties with finite kernel. If $\mu\colon Y \to Y^t$ is a polarization, show that $f^*\mu := f^t \circ \mu \circ f$ is a polarization of X.

(11.2) Let X be an abelian variety over a field k. Suppose there exists a polarization $\lambda\colon X \to X^t$ with $\deg(\lambda) = m$ odd.

(i) Show that there exist integers a and b with $1 + a^2 + b^2 \equiv 0 \bmod m$. [*Hint:* Use the Chinese remainder theorem. First find a solution modulo p for any prime p dividing m. Then use the fact that the curve $C \subset \mathbb{A}^2$ given by $1 + x^2 + y^2 = 0$ is smooth over $\mathbb{Z}_p$ $(p \neq 2\ !)$ to see that the solutions can be lifted to solutions modulo arbitrarily high powers of p.]

(ii) Adapting the proof of Zarhin's trick, show that $X^2 \times (X^t)^2$ admits a principal polarization.

(11.3) Let L be a line bundle on an abelian variety X over a perfect field k. Write $Y := K(L)^0_{\mathrm{red}}$, which is an abelian subvariety of X, and let $q\colon X \to Z := X/Y$ be the quotient.

(i) Show that $\varphi_L\colon X \to X^t$ factors as $\varphi_L = q^t \circ \psi \circ q$ for some homomorphism $\psi\colon Z \to Z^t$.

(ii) Show that there is a finite separable field extension $k \subset K$ and a line bundle M on Z_K such that $\psi_K = \varphi_M$.

(iii) With K and M as in (ii), conclude that the class of $L \otimes q^*M^{-1}$ lies in $\mathrm{Pic}^0_{X/k}(K)$.