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 \( \lambda = \varphi_L : X \to X^t \). And it is in fact this homomorphism that we shall put in the foreground. One reason for this is that \( \lambda \) 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 \( \lambda \); 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 \( \ell \)-adic cohomology of \( X \) can be described in more elementary terms via the Tate-\( \ell \)-module. The class \( c_1(L) \) then takes the form of an alternating pairing \( E^\lambda : T_\ell X \times T_\ell X \to \mathbb{Z}_\ell(1) \), usually referred to as the Riemann form of \( L \) (or of \( \lambda \)). It is obtained, by a limit procedure, from pairings \( e_n^\lambda : X[n] \times X[n] \to \mu_n \), called the Weil pairing.

§ 1. Polarizations.

**(11.1) Proposition.** Let \( X \) be an abelian variety. Let \( \lambda : X \to X^t \) be a homomorphism, and consider the line bundle \( M := (\text{id}, \lambda)^* \mathcal{P}_X \) on \( X \). Then \( \varphi_M = \lambda + \lambda^t \). In particular, if \( \lambda \) 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 \( \lambda : X \to X^t \) be a homomorphism. Then the following properties are equivalent:

(a) \( \lambda \) 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 \( M := (\text{id}, \lambda)^* \mathcal{P}_X \) and \( N := M^2 \). By the previous proposition we know that \( \varphi_M = 2\lambda \), so \( \varphi_N = 4\lambda \). In particular, \( X[4] \subset K(N) = \text{Ker}(\varphi_N) \). We claim that \( X[2] \subset X[4] \) is totally isotropic with respect to the commutator pairing \( e^N \). Indeed, if \( x, x' \in X[2](T) \) for some \( k \)-scheme \( T \) then possibly after passing to an fpf covering of \( T \) we can write \( x = 2y \) and \( x' = 2y' \) for some \( y, y' \in X[4](T) \). Our claim now follows by noting that the restriction of \( e^N \) to \( X[4] \times X[4] \) takes values in \( \mu_4 \). By Corollary (8.11) we can find a line bundle...
Let $X/k$ be a symmetric isogeny and the line bundle $(id, \lambda)^*\mathcal{P}$ on $X$ is ample;
(a2) $\lambda$ is a symmetric isogeny and the line bundle $(id, \lambda)^*\mathcal{P}$ 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 $\lambda: X \to X^t$ 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 $\lambda_K = \varphi_L$. If $\lambda$ is an isomorphism (equivalent: $\lambda$ 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 \( \text{Hom}_X(X, X^t) \).

We also remark that if \( \lambda \) 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 \( \varphi_N \), 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

\[
0 \rightarrow X^t \rightarrow \text{Pic}_{X/k} \rightarrow \text{Hom}^{\text{symm}}(X, X^t) \rightarrow 0
\]

which gives a long exact sequence in fppf cohomology

\[
0 \rightarrow X^t(k) \rightarrow \text{Pic}(X) \rightarrow \text{Hom}^{\text{symm}}(X, X^t) \xrightarrow{\partial} H^1_{\text{fppf}}(k, X^t) \rightarrow \cdots.
\]

For \( \lambda: X \rightarrow X^t \) 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

\[
H^1_{\text{fppf}}(k, X^t[2]) \rightarrow H^1_{\text{fppf}}(k, X^t).
\]

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

(11.8) Proposition. Let \( f: X \rightarrow Y \) be an isogeny. If \( \mu: Y \rightarrow Y' \) is a polarization of \( Y \), then \( f^*\mu := f^* \circ \mu \circ f \) 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 \( \alpha: L|_{\{0\} \times Y} \sim \rightarrow O_Y \) and \( \beta: L|_{X \times \{0\}} \sim \rightarrow O_X \) that coincide on the fibre over \( (0,0) \).

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

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

The Poincaré bundle \( \mathcal{P} = \mathcal{P}_X \) 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

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

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

\[
\{ \text{polarizations } \lambda: X \rightarrow X^t \} \sim \rightarrow \left\{ \text{symmetric divisorial correspondences } \right\}
\]

\[
\left( L, \alpha, \beta \right) \text{ on } X \times X \text{ such that } \Delta_X^* L \text{ is ample}
\]

– 161 –
by associating to a polarization $\lambda$ the divisorial correspondence $(L, \alpha, \beta)$ with $L = (\id_X \times \lambda)^* \mathcal{P}_X$ and $\alpha$ and $\beta$ the pull-backs under $\id_X \times \lambda$ 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 $(L, \alpha, \beta)$ the unique homomorphism $\lambda: X \to X^t$ such that $(L, \alpha) = (\id_X \times \lambda)^*(\mathcal{P}_X, \alpha_{\mathscr{P}})$ as rigidified line bundles on $X \times X$. The assumption that $(L, \alpha, \beta)$ is symmetric implies that $\lambda_X$ is symmetric, and because $(\id_X, \lambda)^* \mathcal{P}_X = \Delta_X^*(\id_X \times \lambda)^* \mathcal{P}_X = \Delta_X^* L$ is ample, $\lambda$ is a polarization. This establishes the correspondence. $\Box$

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 as a map $V \times V \to k$ rather than as a map $V \to V^*$ given by $v \mapsto (w \mapsto b(v, w))$, 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 $\Ker(f)$ and $\Ker(f^t)$; 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 $\lambda$ we can map $X[n]$ to $X^t[n]$, and we obtain a bilinear form $e^\lambda_n$ 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 $e^\lambda_n$, obtaining a bilinear form $E^\lambda$ with values in $\mathbb{Z}_l(1)$ on the Tate module $T_l X$. In cohomological terms this pairing is the first Chern class of $\lambda$ (or rather, of any line bundle representing it). It is the $\ell$-adic analogue of what over $\mathbb{C}$ is called the Riemann form associated to a polarization. (See also ???)

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

(i) Define $e_f: \Ker(f) \times \Ker(f^t) \to \mathbb{G}_{m,k}$ to be the perfect bilinear pairing given (on points) by $e_f(x, y) = \beta(y)(x)$. Note that if $\Ker(f)$ is killed by $n \in \mathbb{Z}_{\geq 1}$ then $e_f$ takes values in $\mu_n \subset \mathbb{G}_m$. In the particular case that $f = n_X: X \to X$ we obtain a pairing $e_n: X[n] \times X^t[n] \to \mu_n$, which we call the Weil pairing.

(ii) Let $\lambda: X \to X^t$ be a homomorphism. We write $e^\lambda_n: X[n] \times X[n] \to \mu_n$ for the bilinear pairing given by $e^\lambda_n(x_1, x_2) = e_n(x_1, \lambda(x_2))$. If $\lambda = \varphi_L$ for some line bundle $L$ then we also write $e^L_n$ instead of $e^\lambda_n$.

Recall that if $A$ and $B$ are finite commutative group schemes (written additively), a pairing $e: A \times B \to \mathbb{G}_m$ 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 $e(a, -): B \to \mathbb{G}_m$ gives an isomorphism $A \cong B^D$. This is equivalent to the condition that $b \mapsto e(-, b)$ gives an isomorphism $B \cong A^D$. It is clear from the construction that the pairings $e_f$, in particular the Weil pairings, are perfect bilinear pairings. If $n$ is relatively prime to the degree of $\lambda$ then the pairing $e^n_f$ 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 $\eta \in \text{Ker}(f^i)(T)$. Then $f^*L \cong O_{X_T}$. Hence the geometric line bundle $\mathbb{L}$ corresponding to $L$ can be described as a quotient of $X_T \times_T \mathbb{A}_T^1$ by an action of $\text{Ker}(f)_T$. More precisely, by what was explained in (7.3) there exists a character $\chi: \text{Ker}(f)_T \to \mathbb{G}_m, T$ such that the action of a point $x$ of $\text{Ker}(f)$ on $X_T \times_T \mathbb{A}_T^1$ is given (on points) by

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

The isomorphism $\text{Ker}(f^i) \cong \text{Ker}(f)^D$ of Theorem (7.5) sends $\eta$ to $\chi$. 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

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

The isomorphism $\text{Ker}(f^i) \cong \text{Ker}(f)^D$ of Theorem (7.5) sends $\eta$ to $\chi$. Hence the pairing $e_f$ is given by $e_f(x, \eta) = \chi(x)$.

(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 $E[3](\mathbb{F}_4) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Let $O = P_\infty$ be the point at $\infty$, which we take as the identity element on $E$. The bundle $L = O_E(P_\infty)$ is ample. The associated principal polarization $\lambda: E \cong E^t = \text{Pic}^0_E/\mathbb{F}_2$ 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 $e_3^3(Q, P)$ for $P = (0, 0)$ and $Q = (1, \alpha)$, where $\alpha$ 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 $\pi = F_{E/\mathbb{F}_2}: E \to E$ 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 $(\xi^4,\eta^4+1)$. Next one calculates that the coordinates of $3R$ are $((6\xi^4+\xi^2+1)/(\xi^4+1), (7\xi^4+1)/(\xi^4+1))$. 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 $F_{64}$. Let $\gamma$ be a generator of $F_{64}^*$ with $\gamma^21 = \alpha$ and such that $\delta := \gamma^9 \in F_{64}$ satisfies $\delta^3 + \delta = 1$. Then the point $T = (\gamma^3, \gamma^{18})$ is in $E(F_{64})$. One easily verifies that $(\gamma^21, \gamma^{18}+1)$ 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 $e_3(Q,P) = e_3(Q,(O-P))$ equals $(\gamma^{12} + \gamma^3)/(\gamma^{33} + \gamma^{24}) = 1/\gamma^{21} = 1/\alpha = \alpha^2$.

The value of $e_3(P',Q')$ 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 $f : X \to Y$ be an isogeny of abelian varieties over a field $k$. By definition, $f^t : Y^t \to X^t$ is the unique map such that $(f \times \id_Y)^t_* \mathcal{P}_X \cong (\id_X \times f^{t*})^* \mathcal{P}_X$ 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 $\mathcal{D} := (f \times \id_Y)^t_* \mathcal{P}_Y = (\id_X \times f^{t*})^* \mathcal{P}_Y$. The diagram to keep in mind is

\[ \begin{array}{ccc}
\mathcal{P}_X & \xrightarrow{\text{id} \times f^t} & \mathcal{P}_Y \\
X \times X^t & \xleftarrow{\text{id} \times f^t} & X \times Y^t \\
& \xrightarrow{f \times \id} & Y \times Y^t
\end{array} \]

On the line bundle $\mathcal{D}$ we have an action of $\Ker(f) \times \{0\}$, lifting the action on $X \times Y^t$ by translations. This action is given by isomorphisms $\sigma_x : \mathcal{D}_T \sim \to t^*_{(x,0)} \mathcal{D}_T$, for any $k$-scheme $T$ and $x \in \Ker(f)(T)$. Likewise, we have an action of $\{0\} \times \Ker(f^t)$, given by isomorphisms $\tau_q : \mathcal{D}_T \sim \to t^*_{(0,q)} \mathcal{D}_T$ for $q \in \Ker(f^t)(T)$. Unless $f$ is an isomorphism, these two group scheme actions on $\mathcal{D}$ do not commute, for if they did it would give us an action of $\Ker(f) \times \Ker(f^t)$ and $\mathcal{D}$ would descend to a line bundle $L$ on $(X \times Y^t)/\Ker(f) \times \Ker(f^t) = Y \times X^t$. But then we had $(-1)^9 = \chi(\mathcal{P}_X) = \deg(f) \cdot \chi(L)$, 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 $\mathcal{D}'$ be the restriction of $\mathcal{D}$ to $X \times \Ker(f^t)$. We have $\mathcal{D}' = (\id_X \times f^{t*})^* ((\mathcal{P}_X)|_{X \times \{0\}})$, so the natural rigidification of $\mathcal{P}_X$ along $X \times \{0\}$ (see (7.7)) gives us a trivialisation $\mathcal{D}' \sim \to O_{X \times \Ker(f^t)}$. The action of $\{0\} \times \Ker(f^t)$ on $\mathcal{D}$ restricts to the trivial action on $\mathcal{D}'$. It will be useful to think of $\mathcal{D}'$ as being the sheaf of sections of $\mathbb{A}^1$ over $X \times \Ker(f^t)$. Writing $\mathbb{A}^1_{X \times \Ker(f^t)} = X \times \Ker(f^t) \times \mathbb{A}^1$, the action of a point $(0,q) \in \{0\} \times \Ker(f^t)$ on $\mathcal{D}'$ corresponds to the action on $X \times \Ker(f^t) \times \mathbb{A}^1$ given by $\tau_q : (t,u,a) \mapsto (t,u+q,a)$.

Note that also the action of $\Ker(f) \times \{0\}$ restricts to an action on $\mathcal{D}'$. To describe this action we apply what was explained in (11.12) in the “universal case”, i.e., with $T = \Ker(f^t)$ and $\eta = \id_Y$. The corresponding line bundle $L$ on $Y_T = Y \times \Ker(f^t)$ is just the restriction of $\mathcal{P}_Y$ to $Y \times \Ker(f^t)$, so $f^*L$ is precisely our bundle $\mathcal{D}'$. If we write a point of $\Ker(f)_T = \cdots - 164 -
Ker(\(f\)) \times_k Ker(\(f^t\)) as a pair \((x, u)\) then the conclusion of (11.12) is that the character \(\chi: \text{Ker}(f) \times_k \text{Ker}(f^t) \rightarrow G_{m,k} \times_k \text{Ker}(f^t)\) is given by \((x, u) \mapsto (\epsilon_f(x,u),u)\). Hence the action of a point \((x, 0) \in \text{Ker}(f) \times \{0\}\) on \(\mathcal{D}\) corresponds to the action on \(X \times \text{Ker}(f^t) \times k^1\) given by \(\sigma_x:\ (t,u,a) \mapsto (t + x, u, \epsilon_f(x,u) \cdot a)\).

Now we can start drawing some conclusions. The first result is an interpretation of the pairing \(\epsilon_f\) as a measure for the extent to which the two group scheme actions on \(\mathcal{D}\) fail to commute.

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

\[
\begin{array}{ccc}
\mathcal{D}_T & \xrightarrow{\sigma_x} & t^*(x,0)\mathcal{D}_T \\
\downarrow & & \downarrow \\
\mathcal{D}_T & \xrightarrow{\tau_q} & t^*(0,q)\mathcal{D}_T \\
\end{array}
\]

Proof. A priori it is clear that there exists a constant \(c \in G_m(T)\) such that \((t^*(x,0)\sigma_x) \circ \tau_q = c \cdot (t^*(0,q)\tau_q) \circ \sigma_x\), so all we need to show is that \(c = \epsilon_f(x,q)\). For this we may restrict everything to \(X \times \text{Ker}(f^t)\). As in the above discussion, we think of \(\mathcal{D}\) as the sheaf of sections of \(k^1\) over \(X \times \text{Ker}(f^t)\). We have seen that \((t^*(x,0)\tau_q) \circ \sigma_x\) is given on points by \((t,u,a) \mapsto (t + x, u + q, \epsilon_f(x,u) \cdot a)\), whereas \((t^*(0,q)\tau_q) \circ \sigma_x\) is given by \((t,u,a) \mapsto (t + x, u + q, \epsilon_f(x,u+q) \cdot a)\). Because \(\epsilon_f\) 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 \(f: X \rightarrow Y\) be an isogeny of abelian varieties. Let \(\kappa_X: X \rightarrow X^{\text{tt}}\) be the canonical isomorphism.

(i) For any \(k\)-scheme \(T\) and points \(x \in \text{Ker}(f)(T)\) and \(\eta \in \text{Ker}(f^t)(T)\) we have the relation \(\epsilon_f(\eta, \kappa_X(x)) = \epsilon_f(x,\eta)^{-1}\).

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

Proof. (i) Consider the commutative diagram

\[
\begin{array}{ccc}
X \times X^t & \xleftarrow{\text{id} \times f^t} & X \times Y^t \\
\downarrow{\kappa_X \times \text{id}} & & \downarrow{\kappa_X \times \text{id}} \\
X^{tt} \times X^t & \xleftarrow{\text{id} \times f^t} & X^{tt} \times Y^t \\
\end{array}
\]

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

\[
\begin{array}{ccc}
Y^t \times Y^{tt} & \xleftarrow{\text{id} \times f^{tt}} & Y^t \times X^{tt} \\
\downarrow{\kappa_Y \times \text{id}} & & \downarrow{\kappa_Y \times \text{id}} \\
Y^t \times X^t & \xleftarrow{\text{id} \times f^t} & X^t \times X^t
\end{array}
\]
which is precisely (1) for the morphism $f^t: Y^t \to X^t$. 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 $e_f(x, \eta) = \beta_1(\eta)(x) = (\beta_1 D \circ \gamma^{-1})(x)(\eta)$ and $e_{f^t}(\eta, k_X(x)) = \beta_2(k_X(x))(\eta)$.

\(\square\)

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

The geometric line bundle on $X \times X^t[n]$ that corresponds to $\mathcal{P}|_{X \times X^t[n]}$ 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 $\sigma_x: (t, u, a) \mapsto (t + x, u, e_n(x, u) \cdot a)$.

To make this completely explicit, suppose $k = \overline{k}$ and 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

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

For the restriction of $\mathcal{P}_X$ 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 $\tau_\xi: (t, u, a) \mapsto (t, u + \xi, e_n(t, \xi^{-1} \cdot a)$. Note, however, that whereas our description of $\mathcal{P}|_{X[n] \times X^t}$ is essentially a reformulation of the definition of the Weil pairing, to arrive at our description of $\mathcal{P}|_{X[n] \times X^t}$ 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 $\varphi_L: X \to X^t$ is symmetric, we have $K(L) = \text{Ker}(\varphi_L) = \text{Ker}(\varphi_L^t)$, and we obtain a pairing

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

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

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

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

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

Let $T$ be a $k$-scheme, and consider $T$-valued points $x, y \in K(L)(T)$. Possibly after replacing $T$ by a covering we can choose isomorphisms $\varphi: L_T \xrightarrow{\sim} t^*_x L_T$ and $\psi: L_T \xrightarrow{\sim} t^*_y L_T$. Then $(x, \varphi)$ and $(y, \psi)$ are $T$-valued points of $\mathcal{G}(L)$, and by definition of the pairing $e^L$ we have the relation

$$(t^*_y \varphi) \circ \psi = e^L(x, y) \cdot (t^*_y \psi) \circ \varphi. \quad (3)$$

We can also view $\psi$ as the trivialisation

$$\psi: O_{X_T \times \{y\}} \xrightarrow{\sim} \Lambda(L_T)|_{X_T \times \{y\}} = t^*_y L_T \otimes L_T^{-1}$$

- 166 -
that sends $1 \in \Gamma(X_T, O_{X_T \times \{y\}})$ to the global section $\psi$ of $t^*_y L_T \otimes L_T^{-1}$. If $\sigma_x : \mathcal{O}_T \to t^*_{(x,0)} \mathcal{O}_T$ is the isomorphism that gives the action of $(x,0) \in K(L) \times \{0\}$ on $\mathcal{O}$ then it follows from what we have seen in (11.15) that we have a commutative diagram

$$
\begin{array}{ccc}
\Lambda(L)_{X_T \times \{y\}} & \xrightarrow{(\sigma_x)_{|X_T \times \{y\}}} & t^*_{(x,0)} \Lambda(L)_{X_T \times \{y\}} \\
\psi & & \uparrow \psi_{x,y} \circ (t^*_{(x,0)} \psi) \\
O_{X_T \times \{y\}} & \xrightarrow{\text{can}} & t^*_{(x,0)} O_{X_T \times \{y\}}.
\end{array}
$$

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

$$
t^*_{(x,0)} \Lambda(L_T)_{X_T \times \{y\}} = t^*_{x+y} L_T \otimes t^*_x L_T^{-1} = \text{Hom}(t^*_x L_T, t^*_{x+y} L_T),
$$

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

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

and comparison with (3) now gives the result. \hfill \Box

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

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

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

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

$$
\begin{array}{ccc}
\text{Ker}(f) \times \text{Ker}(f^t) & \xrightarrow{\text{can}} & \mathbb{G}_m \\
\downarrow i & & \Downarrow g^* \\
\text{Ker}(h) \times \text{Ker}(h^t) & \xrightarrow{\text{can}} & \mathbb{G}_m
\end{array}
\quad \text{and} \quad
\begin{array}{ccc}
\text{Ker}(g) \times \text{Ker}(g^t) & \xrightarrow{\text{can}} & \mathbb{G}_m \\
\downarrow f & & \Downarrow i \\
\text{Ker}(h) \times \text{Ker}(h^t) & \xrightarrow{\text{can}} & \mathbb{G}_m
\end{array}
$$

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, $x \in \text{Ker}(f)(T)$ and $\eta \in \text{Ker}(h^t)(T)$ then $e_f(x,g^t(\eta)) = e_h(i(x),\eta)$; similarly for the second diagram.

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

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

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

\hfill \Box
\(e_k(i(x), \eta) = \chi(i(x)) = \chi \circ i(x) = e_f(x, g'(\eta)).\) This gives the first commutative diagram. For the second, apply the first diagram to the composition \(f^* \circ g^* : Z^t \to Y^t \to X^t;\) then apply (i) of Proposition (11.17). \(\square\)

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

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

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

This gives \(e^\lambda_n(x, x) = e_n(x, \lambda \circ i(x)) = e_n\lambda(i(x), i(x)) = 1,\) where in the last step we use Proposition (11.20) together with the remark that \(n\lambda = \varphi_L^n.\) \(\square\)

In particular, we find that the pairing \(e^\lambda_n\) is skew-symmetric: \(e^\lambda_n(x, y) = e^\lambda_n(y, x)^{-1}.\) 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, \(\ell\) denotes a prime number different from \(\text{char}(k).\) 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

\[E(x, \xi) := (1, e_\ell(x_1, \xi_1), e_\ell^2(x_2, \xi_2), \ldots)\]

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

\[E : T_\ell X \times T_\ell X^t \to \mathbb{Z}_\ell(1).\]

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

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

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 \(\text{Gal}(k_s/k)\) on all the terms involved.

If \(\lambda : X \to X^t\) is a polarization, we obtain a pairing

\[E^\lambda : T_\ell X \times T_\ell X \to \mathbb{Z}_\ell(1) \quad \text{by} \quad E^\lambda(x, x') := E(x, T_\ell \lambda(x')).\]

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

Putting everything together, \(E^\lambda\) is a \(\text{Gal}(k_s/k)\)-invariant element in \(\bigwedge^2(T_\ell X)^\vee(1).\) The cohomological interpretation is that \(E^\lambda\) is the first Chern class of \(\lambda,\) or rather of any line bundle representing \(\lambda.\) Note that \(\bigwedge^2(T_\ell X)^\vee(1) = H^2\left(X_{\overline{k}}, \mathbb{Z}_\ell(1)\right),\) 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 $g \geq 2$ 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 $g \geq 2$. 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 $\text{End}(Y) = \mathbb{Z}$. 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 $\mathbb{Z} \subset \text{End}(Y)$, 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 $\lambda: Y \to Y^t$. As $k = \overline{k}$ there is a line bundle $L$ with $\lambda = \varphi_L$. Because $\lambda$ is principal and $\text{End}(X) = \mathbb{Z}$ the only polarizations of $Y$ are those of the form $\varphi_L^m = n \cdot \lambda$, of degree $n^{2g}$.

On the other hand, if $\ell$ is any prime number different from $\text{char}(k)$ then $Y|\ell \cong (\mathbb{Z}/\ell \mathbb{Z})^{2g}$ as group schemes. Hence $Y$ has a subgroup scheme $H$ of order $\ell$. Let $q: Y \to X := Y/H$ be the quotient. If $\mu: X \to X^t$ 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 $\mu$ cannot be principal.

With a similar construction we shall see later that an abelian variety of dimension $g \geq 2$ 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 $\lambda: X \to X^t$ descends over an isogeny $f: X \to Y$. 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) $\text{Ker}(f)$ is contained in $K(L)$ and is totally isotropic with respect to the pairing $e_{\varphi(L)} = e_{\varphi_L}$;
(b) the inclusion map $\text{Ker}(f) \hookrightarrow K(L)$ can be lifted to a homomorphism $\text{Ker}(f) \hookrightarrow \mathcal{G}(L)$.

(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 $\lambda: X \to X^t$ be a symmetric isogeny, and let $f: X \to Y$ be an isogeny.

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

(ii) Assume that an isogeny $\mu$ as in (i) exists. Then $\mu$ is a polarization if and only if $\lambda$ 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 $\lambda = f^* \circ \mu \circ f$ then $\text{Ker}(f) \subset \text{Ker}(\lambda)$ and it follows from (ii) of Proposition (11.21), applied with $q = (f^* \circ \mu)$ and $h = \lambda$, that $\text{Ker}(f)$ is totally isotropic for the pairing $e_{\lambda}$.

For the converse, assume $\text{Ker}(f)$ is contained in $\text{Ker}(\lambda)$ and is totally isotropic with respect to $e_{\lambda}$. Consider the line bundle $M := (1 \times \lambda)^* \mathcal{P}_X$ on $X \times X$. Recall from Example (8.26) that the theta group $\mathcal{G}(M)$ is naturally isomorphic to the Heisenberg group associated to the group scheme $\text{Ker}(\lambda)$. We have natural actions of $\text{Ker}(\lambda) \times \{0\}$ and $\{0\} \times \text{Ker}(\lambda)$ on $M$; for the first action note that $M$ can also be written as $(\lambda \times 1)^* \mathcal{P}_X$. The assumption that $\text{Ker}(f) \subset \text{Ker}(\lambda)$
is totally isotropic for $e_\lambda$ means precisely that the actions of $\text{Ker}(f) \times \{0\}$ and of $\{0\} \times \text{Ker}(f)$ commute, and therefore define an action of $\text{Ker}(f) \times \text{Ker}(f)$ on $M$. This gives us a line bundle $\mathcal{N}$ on $Y \times Y$ such that $M \cong (f \times f)^* \mathcal{N}$. If $\mu: Y \to Y$ is the (unique) homomorphism such that

$\mathcal{N} = (1 \times \mu)^* \mathcal{P}_Y$ then we get the desired relation $\lambda = f^t \cdot \mu \cdot f$. The uniqueness of $\mu$ is immediate from Lemma (5.4). But we also have $\lambda = \lambda^t = (f^t \cdot \mu \cdot f)^t = f^t \cdot \mu^t \cdot f$. 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. $\square$

**Corollary (11.26).** 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 $\lambda: X \to X^t$. By Lemma (8.22) there exists a Lagrangian subgroup $H \subset \text{Ker}(\lambda)$. (There clearly exists a subgroup $H \subset \text{Ker}(\lambda)$ satisfying condition (i) of that Lemma.) By the previous Proposition, $\lambda$ descends to a principal polarization on $X/H$. $\square$

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].

**Exercise (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 $[\alpha]_X: X^s \to X^r$ the homomorphism given by

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

For $r = s = 1$ this just gives our usual notation $[n]_X$ for the “multiplication by $n$” maps. As another example, the $1 \times 2$ matrix (11) gives the group law on $X$ while the $2 \times 1$ matrix $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ gives the diagonal.

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

$$[\alpha]^t_{Y^s \circ (f_{r^s}, \ldots, f)}, \ldots, f X^s \circ (f_{r^s}, \ldots, f) \cdot [\alpha]_X: X^s \to Y^r.$$ 

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

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

(ii) Let $\beta$ be an $r \times s$ matrix with integral coefficients. Then $([\beta]_X)^t = [\beta^t]_X$, where $\beta^t$ 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 $\deg([\alpha]_X) = 0$. Now assume $\det(\alpha) \neq 0$, and let $\{e_1, \ldots, e_r\}$ be the standard ordered basis of $\mathbb{Z}^r$. By the theory of elementary divisors, there is an ordered basis $\{f_1, \ldots, f_r\}$ for $\mathbb{Z}^r$ and a sequence of nonzero integers $(n_1, \ldots, n_r)$ such that $\alpha(e_i) = n_i \cdot f_i$. Let $\beta \in \text{GL}_r(\mathbb{Z})$ be the matrix with $\beta(e_i) = f_i$, and let $\gamma = \text{diag}(n_1, \ldots, n_r)$ be the diagonal matrix with coefficients $n_i$. Then $[\beta]_X$ is an automorphism of $X^r$ and it is clear that $[\gamma]_X: X^r \to X^r$, which is given by
(x_1, \ldots, x_r) \mapsto (n_1 x_1, \ldots, n_r x_r), has degree \((n_1 \cdots n_r)^2 = \det(\alpha)^2\). As \([\alpha]_X = [\gamma]_X \cdot [\beta]_X\) the claim follows.

(ii) Write \(\beta = (b_{ij})\). Any line bundle \(L\) on \(X^\ell\) with class \(\in \text{Pic}^0\) can be written as \(L = p_1^* L_1 \otimes \cdots \otimes p_r^* L_r\), where the \(p_i: X^\ell \to X\) are the projection maps and the \(L_i\) are line bundles on \(X\) with class \(\in \text{Pic}^0\). Because \((X^\ell)^s \simeq (X^s)^r\) (cf. Exercise (6.2)) it suffices to know the restriction of \([\beta]_X\) 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 \(X \to X^\ell\) 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 \([\beta]_X^t: (X^t)^s \to (X^s)^r = (X^s)^r\) is the map given by the matrix

\[
\left( \begin{array}{cccc}
 b_{11} & \cdots & b_{11} & \cdots & b_{1r_1} \\
 \vdots & \ddots & \vdots & \ddots & \vdots \\
 b_{1j} & \cdots & b_{ij} & \cdots & b_{ir_j} \\
 \vdots & \ddots & \vdots & \ddots & \vdots \\
 b_{1n} & \cdots & b_{i_1} & \cdots & b_{r_1}
\end{array} \right) = y^t \beta,
\]

as claimed. \(\square\)

**11.29 Theorem.** (Zarhin’s trick) Let \(X\) be an abelian variety over a field \(k\). Then \(X^4 \times (X^s)^4\) carries a principal polarization.

**Proof.** Suppose we have an abelian variety \(Y\), a polarization \(\mu: Y \to Y^t\), and an endomorphism \(\alpha: Y \to Y\). Consider the isogeny \(f: Y \times Y \to Y \times Y^t\) given by \((y_1, y_2) \mapsto (y_1 - \alpha(y_2), \mu(y_2))\). The kernel is given by \(\text{Ker}(f) = \{(\alpha(y), y) \mid y \in \text{Ker}(\mu)\}\). In particular, \(\deg(f) = \deg(\mu)\). Proposition (11.25) tells us under what conditions the polarization \(\mu \times \mu: (Y \times Y) \to (Y^t \times Y^t)\) descends to a polarization on \(Y \times Y^t\) via the isogeny \(f\). Namely: there exists a polarization \(\nu\) on \(Y \times Y^t\) with \(f^* \nu = (\mu \times \mu)\) if and only if

(a) \(\alpha(\text{Ker}(\mu)) \subseteq \text{Ker}(\mu)\), and

(b) \(e_\mu(\alpha(y_1), \alpha(y_2)) \cdot e_\mu(y_1, y_2) = 1\) for all (scheme valued) points \(y_1, y_2\) of \(\text{Ker}(\mu)\).

Note that if such a descended polarization \(\nu\) exists then it is principal.

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

\[
e_\mu(\alpha(y_1), \alpha(y_2)) = e_\mu(\alpha(y_1), \alpha(y_2)) = e_\beta(\nu_1, \alpha(y_2)) = e_\beta(\nu_1, \beta^t \alpha(y_2)),
\]

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

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

Choose an integer \(m\) such that \(\text{Ker}(\lambda) \subseteq X[m]\). We are done if we can find an integral \(4 \times 4\) matrix \(\alpha\) such that \(\text{id}_4 + \beta \alpha \equiv 0 \mod m\). 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

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

(4)

for which we have $id_4 + 4\alpha = m \cdot id_4$. 

(11.30) Remarks. (i) The choice of the matrix $\alpha$ 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

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

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 $h: \mathbb{H} \to M_4(\mathbb{R})$ sending $x$ to this matrix is an injective homomorphism of $\mathbb{R}$-algebras, and we have $h(\bar{x}) = h(x)$ and $\text{Nrd}_{\mathbb{H}/\mathbb{R}}(x) = \det(h(x))$. 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 $\alpha$ 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 $n$th 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 $g \geq 2$ over a field $k = \bar{k}$ such that $\text{End}(Y) = \mathbb{Z}$ and such that $Y$ does admit a principal polarization; see ?? for the existence. Any homomorphism $Y^n \to (Y^\ell)^n$ is of the form $\lambda^n \cdot [\alpha]_Y = [\alpha]_Y \cdot \lambda^n$ 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 $\alpha = \bar{\lambda}$. Now choose a prime number $\ell$ different from $\text{char}(k)$, and choose a subgroup $H \subset Y$ of order $\ell$, generated by a point of order $\ell$. Let $\pi: Y \to X := Y/H$ be the quotient.

Let $\mu$ be any polarization on $X^n$. By what was just explained we have $(\pi^n)^* \mu = \lambda^n \cdot [\alpha]_Y$ for some $\alpha \in M_n(\mathbb{Z})$. Moreover, $H \times \cdots \times H \subset \text{Ker}([\alpha]_Y)$, which readily implies that $\alpha$ is divisible by $\ell$, say $\alpha = \ell \cdot \beta$. Further we have $\deg(\mu) \cdot \ell^{2n} = \deg([\alpha]_Y) = \ell^{2ng} \cdot \det(\beta)^{2g}$, 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 $f: X \to Y$ be a homomorphism of abelian varieties with finite kernel. If $\mu: Y \to Y^\ell$ is a polarization, show that $f^* \mu := f^\ell \cdot \mu \cdot f$ is a polarization of $X$.

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

(i) Show that there exist integers $a$ and $b$ with $1 + a^2 + b^2 \equiv 0 \mod m$. [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 $C \subset k^2$ 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 \( Y := K(L)^0_{\text{red}} \), 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 \( \text{Pic}^0_{X/k}(K) \).