Chapter V. Isogenies.

In this chapter we define the notion of an isogeny, and we discuss some basic examples, including the multiplication by an integer $n \neq 0$ and the relative Frobenius homomorphism in characteristic p. As applications we obtain results about the group of n-torsion points on an abelian variety. If the ground field has positive characteristic p this leads to the introduction of an invariant, the p-rank of the abelian variety.

§ 1. *Definition of an isogeny, and basic properties.*

(5.1) Lemma. (i) *Let X and Y be irreducible noetherian schemes which are both regular and with $\dim(X) = \dim(Y)$. Let $f\colon X \to Y$ be a quasi-finite morphism. Then f is flat.*

(ii) *Let $f\colon X \to Y$ be a morphism of finite type between noetherian schemes, with Y reduced and irreducible. Then there is a non-empty open subset $U \subseteq Y$ such that either $f^{-1}(U) = \emptyset$ or the restricted morphism $f\colon f^{-1}(U) \to U$ is flat.*

A proof of (i) can be found in Altman-Kleiman [1], Chap. V, Cor. 3.6 or Matsumura [1], Thm. 23.1. For (ii) we refer to Mumford [2], Lecture 8.

(5.2) Proposition. *Let $f\colon X \to Y$ be a homomorphism of abelian varieties. Then the following conditions are equivalent:*

(a) *f is surjective and $\dim(X) = \dim(Y)$;*

(b) *$\mathrm{Ker}(f)$ is a finite group scheme and $\dim(X) = \dim(Y)$;*

(c) *f is a finite, flat and surjective morphism.*

Proof. We shall use that if $h\colon Z_1 \to Z_2$ is a flat morphism of k-varieties and $F \subset Z_1$ is the fibre of h over a closed point of Z_2 then F is equidimensional and

$$\dim(Z_1) = \dim(Z_2) + \dim(F)\,. \tag{1}$$

(This is a special case of HAG, Chap. III, Prop. 9.5.)

Let us first assume that (b) holds. As f is proper and all fibres are translates of $\mathrm{Ker}(f)$ it follows that f is finite. Hence $f(X)$ is closed in Y, of dimension equal to $\dim(X) = \dim(Y)$. Hence f is surjective. Further, by (i) of the lemma, f is flat. This shows that (a) and (c) hold.

Next suppose that (a) holds. By (ii) of the lemma, f is flat over a non-empty open subset $U \subseteq Y$. As all fibres of f are translates of $\mathrm{Ker}(f)$, (b) follows from (1). That (c) implies (b) again readily follows from (1). □

By making use of the results about quotients that were discussed in the previous chapter, we could do without Lemma (5.1). We leave such an alternative proof of the proposition to the reader.

(5.3) Definition. A homomorphism $f\colon X \to Y$ of abelian varieties is called an *isogeny* if f satisfies the three equivalent conditions (a), (b) and (c) in (5.2). The *degree* of an isogeny f is

the degree of the function field extension $[k(X)\colon k(Y)]$. (Note that we have a homomorphism $k(Y) \to k(X)$, since an isogeny is surjective.)

If $f\colon X \to Y$ is an isogeny then f induces an isomorphism $X/\mathrm{Ker}(f) \xrightarrow{\sim} Y$. Because all fibres of f are translates of $\mathrm{Ker}(f)$ the sheaf f_*O_X is a locally free O_Y-module of finite rank. Computing this rank at the generic point of Y, respectively the closed point $0 \in Y$, gives

$$\deg(f) = \mathrm{rank}_{O_Y}(f_*O_X) = \mathrm{rank}\big(\mathrm{Ker}(f)\big)\,.$$

(Here $\mathrm{rank}\big(\mathrm{Ker}(f)\big)$ denotes the rank of the finite group scheme $\mathrm{Ker}(f)$.) If $f\colon X \to Y$ and $g\colon Y \to Z$ are isogenies then so is $g \circ f$, and $\deg(g \circ f) = \deg(g) \cdot \deg(f)$.

(5.4) Lemma. *Let $f\colon W \to X$ and $h\colon Y \to Z$ be isogenies of abelian varieties over k. If g_1, $g_2\colon X \to Y$ are homomorphisms such that $h \circ g_1 \circ f = h \circ g_2 \circ f$ then $g_1 = g_2$.*

Proof. We may assume that $k = \overline{k}$. Suppose $h \circ g_1 \circ f = h \circ g_2 \circ f$. Because f is faithfully flat, it is an epimorphism of schemes, so it follows that $h \circ g_1 = h \circ g_2$. Hence $g_1 - g_2$ maps X into the finite group scheme $\mathrm{Ker}(h)$. As X is connected and reduced, $g_1 - g_2$ factors through $\mathrm{Ker}(h)^0_{\mathrm{red}}$, which is trivial. □

(5.5) We recall the notion of a purely inseparable morphism (French: morphisme radiciel). In EGA I$^{\mathrm{new}}$, Prop. 3.7.1 it is shown that the following conditions on a morphism of schemes $f\colon X \to Y$ are equivalent:

(a) f is universally injective; this means that for every $Y' \to Y$ the morphism $f'\colon X' \to Y'$ obtained from f by base change is injective;

(b) f is injective and for every $x \in X$ the residue field $k(x)$ is a purely inseparable extension of $k\big(f(x)\big)$;

(c) for every field K, the map $X(K) \to Y(K)$ induced by f is injective.

A morphism that satisfies these conditions is called a *purely inseparable morphism*.

(5.6) Proposition. *Let $f\colon X \to Y$ be an isogeny.*

(i) *The following conditions are equivalent.*
- (a) *The function field $k(X)$ is a separable field extension of $k(Y)$;*
- (b) *f is an étale morphism;*
- (c) *$\mathrm{Ker}(f)$ is an étale group scheme.*

(ii) *The following conditions are equivalent.*
- (a) *The function field $k(X)$ is a purely inseparable field extension of $k(Y)$;*
- (b) *f is a purely inseparable morphism;*
- (c) *$\mathrm{Ker}(f)$ is a connected group scheme.*

Proof. (i) That (b) and (c) are equivalent is clear from (4.33). If f is étale then for every $x \in X$, writing $y = f(x) \in Y$, the residue field $k(x)$ is a finite separable extension of $k(y)$. If we apply this with x the generic point of X, we see that (b) implies (a).

Now assume that $k(X)$ is a finite separable extension of $k(Y)$. As f is a finite flat morphism, it is étale at a point $x \in X$ if and only if $(\Omega^1_{X/Y})_x = 0$. But $\Omega^1_{X/Y}$ is a coherent O_X-module, hence its support is closed, and it follows that the locus where f is étale is an open subset $U \subset X$. The assumption that $k(X)$ is finite separable over $k(Y)$ means that the generic point of X is in U, so U is non-empty. As f is proper it follows that there is an open subset $V \subset Y$ such that $f^{-1}(V)$ is étale over V. But V is the quotient of $f^{-1}(V)$ under $\mathrm{Ker}(f)$, so it follows from (4.33) that $\mathrm{Ker}(f)$ is étale.

(ii) We can factor f as a composition of two isogenies: $X \to X/\mathrm{Ker}(f)^0 \to Y$. The kernel of the second isogeny is $\mathrm{Ker}(f)/\mathrm{Ker}(f)^0$, which is étale. (See also Prop. (4.45).) Using (i) it follows that (a) implies (c).

That (b) implies (a) is immediate from property (b) in (5.5), applied to the generic point of X.

Finally suppose that $N := \mathrm{Ker}(f)$ is a connected group scheme. Let $k \subset K$ be a field extension. Let A be the affine algebra of N and write $A_K = A \otimes_k K$. If y: $\mathrm{Spec}(K) \to Y$ is a K-valued point then the scheme-theoretic fibre $f^{-1}(y) := X \times_{Y,y} \mathrm{Spec}(K)$ is isomorphic to $N_K = \mathrm{Spec}(A_K)$. As A_K has finite K-dimension it is an artinian ring. Any artinian ring is a product of artinian local rings; this corresponds to the decomposition of $f^{-1}(y)$ as a union of connected components. But we know from (i) of (3.17) that N_K is a connected scheme. Hence A_K is artinian local and $|f^{-1}(y)|$ consists of a single point. This shows that f satisfies condition (c) of (5.5) and is therefore purely inseparable. □

(5.7) Definition. An isogeny f: $X \to Y$ is called *separable* if it satisfies the three equivalent conditions in (5.6)(i). It is called a *(purely) inseparable isogeny* if it satisfies the equivalent conditions of (5.6)(ii).

(5.8) Corollary. *Every isogeny f: $X \to Y$ can be factorized as $f = h \circ g$, where g: $X \to Z$ is an inseparable isogeny and h: $Z \to Y$ is a separable isogeny. This factorization is unique up to isomorphism, in the sense that if $f = h' \circ g'$: $X \to Z' \to Y$ is a second such factorization then there is an isomorphism α: $Z \xrightarrow{\sim} Z'$ with $g' = \alpha \circ g$ and $h = h' \circ \alpha$.*

Proof. Immediate from the above and Prop. (4.45). □

An important example of an isogeny is the multiplication $[n]_X$: $X \to X$ by an integer $n \neq 0$. We write $X[n] := \mathrm{Ker}([n]_X) \subset X$.

(5.9) Proposition. *For $n \neq 0$, the morphism $[n]_X$ is an isogeny. If $g = \dim(X)$, we have $\deg([n]_X) = n^{2g}$. If $(\mathrm{char}(k), n) = 1$ then $[n]_X$ is separable.*

Proof. Choose an ample and symmetric line bundle L on X. (Recall that L is said to be symmetric if $(-1)^*L \cong L$, and note that if L is ample then $L \otimes (-1)^*L$ is ample and symmetric.) By (2.12) we know that $n_X^*L \cong L^{\otimes n^2}$. The restiction of n_X^*L to $\mathrm{Ker}(f)$ is a trivial bundle which is ample. (Here we use that $n \neq 0$.) This implies that $\mathrm{Ker}(f)$ is finite, hence $[n]_X$ is an isogeny.

To compute the degree we use intersection theory on smooth varieties. Choose an ample symmetric divisor D. Then $\deg([n]_X) \cdot (D)^g = ([n]_X^*D)^g$. But $[n]_X^*D$ is linearly equivalent to $n^2 \cdot D$, so $([n]_X^*D)^g = n^{2g} \cdot (D)^g$, and we find that $\deg([n]_X) = n^{2g}$.

If $\mathrm{char}(k) = 0$ then the last assertion is trivial. If $\mathrm{char}(k) = p > 0$ with $p \nmid n$ then also $p \nmid n^{2g} = \mathrm{rank}(X[n])$, and the result follows from Cor. (4.48). Alternatively, as p does not divide $n^{2g} = \big[k(X_1) : k(X_2)\big]$, the field extension $k(X_2) \subset k(X_1)$ given by f is separable. □

(5.10) Corollary. *If X is an abelian variety over an algebraically closed field k then $X(k)$ is a divisible group. That is, for every $P \in X(k)$ and $n \in \mathbb{Z}\backslash\{0\}$ there exists a point $Q \in X(k)$ with $n \cdot Q = P$.*

Note that if the ground field k is only assumed to be separably closed then it is *not* true in general that $X(k)$ is a divisible group. See ?? for an example.

(5.11) Corollary. *If* $(\mathrm{char}(k), n) = 1$ *then* $X[n](k_s) = X[n](\overline{k}) \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$.

Proof. We know that $X[n]$ is an étale group scheme of rank n^{2g}. Hence $X[n](k_s) = X[n](\overline{k})$ is an abelian group of order n^{2g}, killed by n. Further, for every divisor d of n the subgroup of elements killed by d is just $X[d](k_s)$ and has order d^{2g}. It now readily follows from the structure theorem for finite abelian groups that we must have $X[n](k_s) \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$. □

(5.12) Proposition. *If* $f\colon X \to Y$ *is an isogeny of degree* d *then there exists an isogeny* $g\colon Y \to X$ *with* $g \circ f = [d]_X$ *and* $f \circ g = [d]_Y$.

Proof. If $\deg(f) = d$ then $\mathrm{Ker}(f)$ is a finite group scheme of rank d and is therefore annihilated by multiplication by d; see Exercise (4.4). It follows that $[d]_X$ factors as

$$[d]_X = (X \xrightarrow{f} Y \xrightarrow{g} X)$$

for some isogeny $g\colon Y \to X$. Then $g \circ [d]_Y = [d]_X \circ g = (g \circ f) \circ g = g \circ (f \circ g)$, and by Lemma (5.4) it follows that $f \circ g = [d]_Y$. □

(5.13) Corollary. *The relation*

$$X \sim_k Y \quad \stackrel{\text{def}}{=} \quad \text{there exists an isogeny } f\colon X \to Y$$

is an equivalence relation on the set of abelian varieties over k.

If there is no risk of confusion we shall use the notation $X \sim Y$ instead of $X \sim_k Y$. Note, however, that the ground field plays a role: if $k \subset K$ is a field extension then $X \sim_k Y$ implies that $X_K \sim_K Y_K$, but the converse does not hold in general.

If there exists an isogeny $f\colon X \to Y$ then we say that X and Y are *isogenous*. Again this notion is relative to a given ground field; if necessary we may specify that X and Y are isogenous over the given field k.

(5.14) Example. Suppose we work over the field $\mathbb{C}$ of complex numbers. If X is an abelian variety over $\mathbb{C}$, the associated analytic manifold X^{an} is a complex torus; see also (1.10). So we can write $X^{\mathrm{an}} = V/L$, where V is a complex vector space and $L \subset V$ is a lattice. More intrinsically, V can be identified with the tangent space of X^{an} at the origin, and the projection map $V \to X$ is then the exponential map in the sense of Lie theory. We shall come back to this in more detail in Chapter ??.

Let X_1 and X_2 be complex abelian varieties; write $X_i^{\mathrm{an}} = V_i/L_i$. Let $f\colon X_1 \to X_2$ be a homomorphism. It follows from the previous remarks that the associated analytic map $f^{\mathrm{an}}\colon X_1^{\mathrm{an}} \to X_2^{\mathrm{an}}$ is given by a $\mathbb{C}$-linear map $\varphi\colon V_1 \to V_2$ such that $\varphi(L_1) \subseteq L_2$. Conversely, any such φ gives an analytic map $\bar{\varphi}\colon X_1^{\mathrm{an}} \to X_2^{\mathrm{an}}$, and it can be shown (using a result of Chow, see HAG, Appendix B, Thm. 2.2) that there exists a unique algebraic homomorphism $f\colon X_1 \to X_2$ with $\bar{\varphi} = f^{\mathrm{an}}$.

As an example, multiplication by n on X corresponds to $\varphi = n \cdot \mathrm{id}_V$, which obviously maps L into itself. We find that the group of n-torsion points $X[n](\mathbb{C})$ is isomorphic to $n^{-1}L/L \subset V/L$, and if $g = \dim(X)$ then indeed $n^{-1}L/L \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$.

As an application we find that $X_1 \sim X_2$ if and only if there exists a $\mathbb{C}$-linear isomorphism $\alpha\colon V_1 \xrightarrow{\sim} V_2$ such that $\alpha(L_1 \otimes \mathbb{Q}) = L_2 \otimes \mathbb{Q}$; in other words, there should exist positive integers m and n with $m \cdot L_2 \subseteq \alpha(L_1) \subseteq n^{-1} \cdot L_2$.

§ 2. *Frobenius and Verschiebung.*

As the next example of an isogeny, we look at Frobenius in characteristic $p > 0$.

(5.15) Proposition. *Let X be a g-dimensional abelian variety over a field k with* $\mathrm{char}(k) = p > 0$. *Then the relative Frobenius homomorphism $F_{X/k}\colon X \to X^{(p)}$ is a purely inseparable isogeny of degree p^g.*

Proof. Write $X[F] := \mathrm{Ker}(F_{X/k})$. On underlying topological spaces, the absolute Frobenius $\mathrm{Frob}_X\colon X \to X$ is the identity. It follows that the topological space underlying $X[F]$ is the singleton $\{e\}$. Let now $U = \mathrm{Spec}(A)$, with $A = k[x_1, \ldots, x_r]/(f_1, \ldots, f_n)$, be an affine open neigbourhood of e in X such that e corresponds to the maximal ideal $\mathfrak{m} = (x_1, \ldots, x_r) \subset A$. Write $f_i^{(p)} \in k[x_1, \ldots, x_r]$ for the polynomial obtained from f_i by raising all coefficients to the pth power. Then $U^{(p)} = \mathrm{Spec}(A^{(p)})$, with $A^{(p)} = k[x_1, \ldots, x_r]/(f_1^{(p)}, \ldots, f_n^{(p)})$, and $F_{U/k}\colon U \to U^{(p)}$, the restriction of $F_{X/k}$ to U, is given on rings by

$$\begin{aligned} A = k[x_1, \ldots, x_r]/(f_1, \ldots, f_n) &\longleftarrow A^{(p)} = k[x_1, \ldots, x_r]/(f_1^{(p)}, \ldots, f_n^{(p)}) \\ x_i^p &\longleftarrow\!\shortmid\ x_i\,. \end{aligned}$$

It follows that $X[F] = \mathrm{Spec}(B)$, with $B = k[x_1, \ldots, x_r]/(x_1^p, \ldots, x_r^p, f_1, \ldots, f_n)$. In particular, $X[F]$ is finite, hence $F_{X/k}$ is an isogeny.

Write $\hat{A}$ for the $\mathfrak{m}$-adic completion of A. Without loss of generality we may assume that $x_1, \ldots, x_g$ form a basis of $\mathfrak{m}/\mathfrak{m}^2 = T^\vee_{X,e}$. The structure theory for complete regular local rings tells us that there is an isomorphism

$$k[\![t_1, \ldots, t_g]\!] \xrightarrow{\sim} \hat{A}$$

sending t_i to x_i. (See Bourbaki [2], Chap. VIII, § 5, n° 2.) Since $(x_1^p, \ldots, x_r^p) \subset \mathfrak{m}$, we find that

$$\begin{aligned} B = A/(x_1^p, \ldots, x_r^p)A &\cong \hat{A}/(x_1^p, \ldots, x_r^p)\hat{A} \\ &\cong \hat{A}/(x_1^p, \ldots, x_g^p)\hat{A} \\ &\cong k[\![t_1, \ldots, t_g]\!]/(t_1^p, \ldots, t_g^p) \\ &\cong k[t_1, \ldots, t_g]/(t_1^p, \ldots, t_g^p)\,. \end{aligned}$$

In particular this shows that $\deg(F_{X/k}) = \mathrm{rank}(X[F]) = p^g$ and that $X[F]$ is a connected group scheme. □

Our next goal is to define the *Verschiebung* isogeny for abelian varieties in characteristic p. In fact, under a suitable flatness assumption the Verschiebung can be defined for arbitrary commutative group schemes over a basis S with $\mathrm{char}(S) = p$; we shall give the construction in this generality. First we need some preparations.

(5.16) Let R be a ring with $\mathrm{char}(R) = p > 0$. Let A be an R-algebra. Write $T^p(A) := A \otimes_R \otimes_R \cdots \otimes_R A$ for the p-fold tensor product of A over R. The symmetric group $\mathfrak{S}_p$ on p letters naturally acts on $T^p(A)$ by ring automorphisms. Write $S^p(A) \subset T^p(A)$ for the subalgebra of $\mathfrak{S}_p$-invariants, i.e., the subalgebra of symmetric tensors.

Let $N\colon T^p(A) \to S^p(A)$ be the "symmetrizer" map, i.e., the map given by

$$N(a_1 \otimes \cdots \otimes a_p) = \sum_{\sigma \in \mathfrak{S}_p} a_{\sigma(1)} \otimes \cdots \otimes a_{\sigma(p)}\,.$$

If $s \in S^p(A)$ is a symmetric tensor and $t \in T^p(A)$ then $N(st) = sN(t)$. It follows that $J := N\big(T^p(A)\big)$ is an ideal of $S^p(A)$.

Write $U := \mathrm{Spec}(A) \to T := \mathrm{Spec}(R)$. Applying Thm. (4.8) we find that the quotient $S^p(U)$ of $U_T^p := U \times_T U \times_T \cdots \times_T U$ (p factors) under the natural action of $\mathfrak{S}_p$ exists and is given by $S^p(U) = \mathrm{Spec}\,\big(S^p(A)\big)$. The scheme $S^p(U)$ is called the p-th symmetric power of U over T. Note that $S^p(U/T)$ would be a better notation, as the base scheme is important in the construction. We trust, however, that the simpler notation $S^p(U)$ will not cause any confusion. Let $U^{[p/T]} \hookrightarrow S^p(U)$ be the closed subscheme defined by the ideal J. If $\eta\colon T^p(A) \to A$ is the multiplication map, given by $a_1 \otimes \cdots \otimes a_p \mapsto a_1 \cdots a_p$, then $\eta\big(N(a_1 \otimes \cdots \otimes a_p)\big) = p! \cdot (a_1 \cdots a_p) = 0$. This means that the morphism

$$U \xrightarrow{\Delta^p_{U/T}} U_T^p \longrightarrow S^p(U)$$

factors through $U^{[p/T]} \subset S^p(U)$. Write $F'_{U/T}\colon U \to U^{[p/T]}$ for the morphism thus obtained.

Write $A^{(p/R)} := A \otimes_{R,F} R$, where $F = \mathrm{Frob}_R\colon R \to R$ is the Frobenius homomorphism, given by $r \mapsto r^p$. We view $A^{(p/R)}$ as an R-algebra via $r \mapsto 1 \otimes r$; so for $a \in A$ and $r \in R$ we have the relations $r^p \cdot (a \otimes 1) = a \otimes r^p = (ra) \otimes 1$. By definition, $U^{(p/T)} = \mathrm{Spec}\,\big(A^{(p/R)}\big)$. Now observe that we have a well-defined map

$$\varphi_{A/R}\colon A^{(p/R)} \to S^p(A)/J$$

sending $a \otimes r \in A^{(p/R)}$ to $(ra \otimes a \otimes \cdots \otimes a) \bmod J$. Note that $(ra \otimes a \otimes \cdots \otimes a)$ is an element of $S^p(A)$ because all tensors are taken over the ring R. Also note that $\varphi_{A/R}$ is well-defined precisely because we use p-tensors. (Check this yourself!) Write $\varphi_{U/T}\colon U^{[p/T]} \to U^{(p/T)}$ for the morphism of schemes induced by $\varphi_{A/R}$. It is clear from the definitions that $F_{U/T} = \varphi_{U/T} \circ F'_{U/T}$.

We now globalize these constructions. For this, consider a base scheme S of characteristic p and an S-scheme $\pi\colon X \to S$. Define $S^p(X)$, the pth symmetric power of X over S, to be the quotient of X_S^p under the natural action of $\mathfrak{S}_p$. If $U \subset X$ and $T \subset S$ are affine open subsets with $\pi(U) \subseteq T$ then $S^p(U)$ is an affine open subset of $S^p(X)$. The closed subschemes $U^{[p/T]} \hookrightarrow S^p(U)$ glue to a locally closed subscheme $X^{[p/S]} \hookrightarrow S^p(X)$. Also, the morphisms $F'_{U/T}$ and $\varphi_{U/T}$ glue and give a factorization of the relative Frobenius morphism $F_{X/S}$ as

$$F_{X/S} = \big(X \xrightarrow{F'_{X/S}} X^{[p/S]} \xrightarrow{\varphi_{X/S}} X^{(p/S)}\big)\,.$$

By construction, the composition of $F'_{X/S}$ and the inclusion $X^{[p/S]} \hookrightarrow S^p(X)$ is the same as the composition of the diagonal $\Delta^p_{X/S}\colon X \to X_S^p$ and the natural projection $X_S^p \to S^p(X)$. Summing up, we have a commutative diagram

$$\begin{array}{ccc} X & \xrightarrow{\Delta_{X/S}} & X_S^p \\ \big\downarrow{\scriptstyle F'_{X/S}} & & \big\downarrow \\ X^{[p/S]} & \hookrightarrow & S^p(X) \\ \big\downarrow{\scriptstyle \varphi_{X/S}} & & \\ X^{(p/S)} & & \end{array} \qquad F_{X/S}$$

(5.17) Lemma. (i) *The construction of $X^{[p/S]}$, as well as the formation of $F'_{X/S}$ and $\varphi_{X/S}$, is functorial in X and compatible with flat base change $T \to S$.*

(ii) *If X is flat over S then $\varphi_{X/S}\colon X^{[p/S]} \to X^{(p/S)}$ is an isomorphism of S-schemes.*

Proof. Part (i) of the lemma is a straightforward verification. For (ii), it suffices to treat the case that $X = U = \operatorname{Spec}(A)$ and $S = T = \operatorname{Spec}(R)$. Let M be an R-module. Just as before we can form the p-fold tensor product $T^p(M)$ of M over R and the submodule $S^p(M) \subset T^p(M)$ of symmetric tensors, and there is a symmetrizer map $N\colon T^p(M) \to S^p(M)$. We have a well-defined map

$$\varphi_{M/R}\colon M^{(p/R)} \longrightarrow S^p(M)/N\big(T^p(M)\big) \quad \text{given by} \quad m \otimes r \mapsto [rm \otimes m \otimes \cdots \otimes m]\,.$$

Suppose M is a free R-module with a basis $\{e_i\}_{i\in I}$. The tensors $e_{\underline{i}} := e_{i_1} \otimes e_{i_2} \otimes \cdots \otimes e_{i_p}$ with $\underline{i} = (i_1, \ldots, i_p) \in I^p$, form a basis of $T^p(M)$. Such a tensor $e_{\underline{i}}$ can be symmetrized in a minimal way. Namely, if $H \subset \mathfrak{S}_p$ is the stabilizer of $(i_1, \ldots, i_p)$ in the natural action of $\mathfrak{S}_p$ on I^p then for $\bar\sigma \in H\backslash\mathfrak{S}_p$ the element $e_{i_{\bar\sigma(1)}} \otimes e_{i_{\bar\sigma(2)}} \otimes \cdots \otimes e_{i_{\bar\sigma(p)}}$ is well-defined; now set

$$s_{\underline{i}} := \sum_{\bar\sigma \in H\backslash\mathfrak{S}_p} e_{i_{\bar\sigma(1)}} \otimes e_{i_{\bar\sigma(2)}} \otimes \cdots \otimes e_{i_{\bar\sigma(p)}}\,.$$

The symmetric tensors $s_{\underline{i}}$ obtained in this way span $S^p(M)$; note however that different sequences $\underline{i}$ may give the same tensor $s_{\underline{i}}$. If $i_1 = i_2 = \cdots = i_p$ then $N(e_{\underline{i}}) = p! \cdot s_{\underline{i}} = 0$; if not all i_j are equal then $N(e_{\underline{i}})$ is a unit times $s_{\underline{i}}$. (Recall that R is an $\mathbb{F}_p$-algebra.) We conclude that the tensors $e_i \otimes e_i \otimes \cdots \otimes e_i$ form a basis of $S^p(M)/N\big(T^p(M)\big)$, and it follows that $\varphi_{M/R}$ is an isomorphism if M is free over R.

Now we use a non-trivial result from commutative algebra. Namely, if M is flat over R then it can be written as a filtered direct limit, say $M = \varinjlim M_\alpha$, of free R-modules. For a proof see [??]. Since $\varinjlim$ is right exact and commutes with tensor products, $\varphi_{M/R}$ can be identified with $\varinjlim \varphi_{M_\alpha/R}$ and is therefore again an isomorphism. Applying this to $M = A$ the lemma follows. □

We now consider a commutative S-group scheme G. The morphism $m^{(p)}\colon G_S^p \to G$ given on sections by $(g_1, g_2, \ldots, g_p) \mapsto g_1 g_2 \cdots g_p$ factors through $S^p(G)$, say via $\bar m^{(p)}\colon S^p(G) \to G$. It follows that $[p]\colon G \to G$, which is equal to $m^{(p)} \circ \Delta^p_{G/S}$, factors as

$$[p] = \big(G \xrightarrow{F'_{G/S}} G^{[p/S]} \hookrightarrow S^p(G) \xrightarrow{\bar m^{(p)}} G\big)\,. \tag{2}$$

(5.18) Definition. If G is a commutative flat group scheme over a basis S of characteristic p then we define the Verschiebung homomorphism

$$V_{G/S}\colon G^{(p/S)} \longrightarrow G$$

to be the composition

$$V_{G/S} = \big(G^{(p/S)} \xrightarrow{\varphi^{-1}_{G/S}} G^{[p/S]} \hookrightarrow S^p(G) \xrightarrow{\bar m^{(p)}} G\big)\,.$$

That $V_{G/S}$ is indeed a homomorphism of group schemes follows from (i) of the lemma.

(5.19) Proposition. *Let S be a scheme with $\operatorname{char}(S) = p > 0$. Let G be a flat S-group scheme.*

(i) *We have* $V_{G/S} \circ F_{G/S} = [p]_G \colon G \longrightarrow G$.

(ii) *If* G *is finite locally free over* S *then the Verschiebung is Cartier dual to the Frobenius homomorphism; more precisely, we have* $(V_{G/S})^D = F_{G^D/S}$ *and* $V_{G/S} = (F_{G^D/S})^D$.

Proof. Statement (i) follows from the definitions; indeed, if we write $j \colon G^{[p/S]} \hookrightarrow S^p(G)$ for the inclusion morphism then

$$V_{G/S} \circ F_{G/S} = (\bar{m}^{(p)} \circ j \circ \varphi_{G/S}^{-1}) \circ (\varphi_{G/S} \circ F'_{G/S}) = \bar{m}^{(p)} \circ j \circ F'_{G/S} = [p]_G$$

by (2).

For (ii), suppose G is finite locally free over S. Without loss of generality we may assume that $S = \mathrm{Spec}(R)$ is affine, so that G is given by an R-algebra A. Possibly after further localization on S we may assume that A is free as a module over R, say with basis $\{e_1, \ldots, e_n\}$. Recall from the proof of Lemma (5.17) that given a sequence $\underline{i} = (i_1, i_2, \ldots, i_p) \in \{1, 2, \ldots, n\}^p$, we can symmetrize the tensor $e_{i_1} \otimes e_{i_2} \otimes \cdots \otimes e_{i_p}$ in a minimal way. The resulting collection of tensors

$$\{s_{\underline{i}}\}_{1 \leqslant i_1 \leqslant i_2 \leqslant \cdots \leqslant i_p \leqslant n}$$

is a basis of $S^p(A)$. It follows from the proof of Lemma (5.17) that the Verschiebung $V_{G/S}$ is given on rings by the composition

$$A \xrightarrow{\bar{m}^{(p)}} S^p(A) \longrightarrow A^{(p/R)}\,,$$

where $\bar{m}^{(p)}$ is the homomorphism that corresponds to the morphism $\bar{m}^{(p)} \colon S^p(G) \to G$, and where the homomorphism $S^p(A) \to A^{(p/R)}$ is given by

$$s_{\underline{i}} \mapsto \begin{cases} 0, & \text{if } i_j < i_{j+1} \text{ for some } j; \\ e_i \otimes 1 & \text{if } \underline{i} = (i, i, \ldots, i). \end{cases}.$$

Now we apply the functor $(\ )^D = \mathrm{Hom}_R(-, R)$. We have an isomorphism

$$\big(A^D\big)^{(p/R)} \xrightarrow{\sim} \big(A^{(p/R)}\big)^D$$

by sending $\varphi \otimes \rho \in A^D \otimes_{R,F} R$ to the map $a \otimes r \mapsto r\rho\varphi(a)^p$. Further there is a canonical isomorphism $\big(S^p(A)\big)^D \cong \mathrm{Sym}^p(A^D)$; here we note that by our general conventions in (??), $\mathrm{Sym}^p(A^D)$ is a *quotient* of the p-fold tensor product $T^p(A^D)$, whereas $S^p(A)$ is a *sub-algebra* of $T^p(A)$. Using these identifications, and writing $\{\varepsilon_1, \ldots, \varepsilon_n\}$ for the R-basis of A^D dual to $\{e_1, \ldots, e_n\}$, the dual of the map $S^p(A) \to A^{(p/R)}$ is the map

$$\big(A^D\big)^{(p/R)} \longrightarrow \mathrm{Sym}^p(A^D) \quad \text{given by} \quad \varepsilon_i \otimes \rho \mapsto [\rho\varepsilon_i \otimes \varepsilon_i \otimes \cdots \otimes \varepsilon_i]\,.$$

Furthermore, by definition of the ring structure on A^D, the dual of the map $\bar{m}^{(p)} \colon A \to S^p(A)$ is the multiplication map $\mathrm{Sym}^p(A^D) \to A^D$ given by $[\varphi_1 \otimes \cdots \otimes \varphi_p] \mapsto \varphi_1 \cdots \varphi_p$. Combining this we see that the Cartier dual of $V_{G/S}$ is given on rings by the map

$$\big(A^D\big)^{(p/R)} \to A \quad \text{sending} \quad \varphi \otimes r \quad \text{to} \quad r \cdot \varphi^p\,.$$

This shows that $(V_{G/S})^D = F_{G^D/S}$. By Cartier duality then also $V_{G/S} = (F_{G^D/S})^D$. □

Now we apply this to abelian varieties.

(5.20) Proposition. *Let X be an abelian variety over a field k with $\mathrm{char}(k) = p$. Then the Verschiebung homomorphism $V_{X/k}\colon X^{(p)} \to X$ is an isogeny of degree p^g. We have $V_{X/k} \circ F_{X/k} = [p]_X$ and $F_{X/k} \circ V_{X/k} = [p]_{X^{(p)}}$.*

Proof. Write $F = F_{X/k}$ and $V = V_{X/k}$. We have already seen that $V \circ F = [p]_X$. It follows that V satisfies (a) of Proposition (5.2); hence it is an isogeny. That V has degree p^g follows from the relation $p^{2g} = \deg\bigl([p]\bigr) = \deg(V) \cdot \deg(F) = \deg(V) \cdot p^g$. Finally, $F \circ V \circ F = F \circ [p] = [p] \circ F$, and because F is an epimorphism this implies that $F \circ V = [p]$. □

(5.21) Let X be a k-scheme, where k is a field of characteristic p. For $m \geqslant 1$ we write $X^{(p^m)}$ for the base change of X over the mth power Frobenius homomorphism $\mathrm{Frob}_k^m\colon k \to k$. By a slight abuse of notation we write

$$F_{X/k}^m = F_{X^{(p^{m-1})}/k} \circ \cdots \circ F_{X^{(p)}/k} \circ F_{X/k}\colon X \to X^{(p)} \to X^{(p^2)} \to \cdots \to X^{(p^m)}$$

for the "mth power" of Frobenius, or "iterated Frobenius". Similarly, we can define an "mth iterated Verschiebung" $V_{X/k}^m\colon X^{(p^m)} \to X$ by

$$V_{X/k}^m = V_{X/k} \circ V_{X^{(p)}/k} \circ \cdots \circ V_{X^{(p^{m-1})}/k}\,.$$

By an easy induction on m we find that $[p^m]_X = V_{X/k}^m \circ F_{X/k}^m$ and $[p^m]_{X^{(p^m)}} = F_{X/k}^m \circ V_{X/k}^m$. Indeed, for $m = 1$ this is just Proposition (5.20), and to make the induction we note that

$$\begin{aligned} V_{X/k}^{m+1} \circ F_{X/k}^{m+1} &= V_{X/k} \circ V_{X^{(p)}/k}^m \circ F_{X^{(p)}/k}^m \circ F_{X/k} \\ &= V_{X/k} \circ [p^m]_{X^{(p)}} \circ F_{X/k} \\ &= [p^m]_X \circ V_{X/k} \circ F_{X/k} = [p^{m+1}]_X\,. \end{aligned}$$

(Likewise for the relation $[p^m]_{X^{(p^m)}} = F_{X/k}^m \circ V_{X/k}^m$.)

Let us now look what is the analogue of (5.11) in case $\mathrm{char}(k) \mid n$. In fact, since all $X[n](\overline{k})$ are finite abelian, it suffices to consider the case that $n = p^m$, where $p = \mathrm{char}(k) > 0$.

(5.22) Proposition. *Suppose $\mathrm{char}(k) = p > 0$. There is an integer $f = f(X)$, with $0 \leqslant f \leqslant g = \dim(X)$, such that $X[p^m](\overline{k}) \cong (\mathbb{Z}/p^m\mathbb{Z})^f$ for all $m \geqslant 0$. If Y is isogenous to X then $f(Y) = f(X)$.*

Proof. We can factor $p^m\colon X \to X$ as

$$[p^m]_X = \left(X \xrightarrow{F_{X/k}^m} X^{(p^m)} \xrightarrow{h_1} Y \xrightarrow{h_2} X \right),$$

where $h_1 \circ F_{X/k}^m$ is purely inseparable and h_2 is a separable isogeny. Looking at the degrees we find that $X[p^m](\overline{k})$ is an abelian group of rank $\deg(h_2) = p^{d(m)}$, where $d(m)$ is an integer with $0 \leqslant d(m) \leqslant gm$. Write $f = d(1)$, so that $X[p](\overline{k}) \cong (\mathbb{Z}/p\mathbb{Z})^f$. It follows from Corollary (5.10) that we have exact sequences of (abstract) groups

$$0 \longrightarrow X[p^{m-1}](\overline{k}) \longrightarrow X[p^m](\overline{k}) \xrightarrow{p^{m-1}} X[p](\overline{k}) \longrightarrow 0\,.$$

The claim that $X[p^m](\overline{k}) \cong (\mathbb{Z}/p^m\mathbb{Z})^f$ for all $m \geqslant 0$ follows by induction on m.

Finally, suppose $h\colon X \to Y$ is an isogeny, say of degree d. Then $X[p^m](\overline{k})$ maps to $Y[p^m](\overline{k})$, and the kernel has order at most d. Taking m large enough, it follows that $f(Y) \geqslant f(X)$. As $X \sim Y$ is a symmetric relation, we conclude that $f(X) = f(Y)$. □

(5.23) Definition. The integer $f = f(X)$, which lies in the range $0 \leqslant f \leqslant g := \dim(X)$, is called the *p-rank* of X.

(5.24) Caution. Let X be an abelian variety of p-rank $f > 0$ over a non-perfect field k, and let $k \subset k_s \subset \overline{k}$ be respectively a separable closure and an algebraic closure of k. Then we have natural injective maps $X[p^m](k_s) \to X[p^m](\overline{k})$, but these are not, in general, isomorphisms. In other words, in order to see all p^{mf} distinct physical points of order p^m, in general we need an inseparable extension of the ground field.

At first sight this may seem to contradict the fact that an étale k-group scheme becomes constant over k_s. For instance, taking $m = 1$ we have a short exact sequence of k-group schemes

$$1 \longrightarrow X[p]_{\mathrm{loc}} \longrightarrow X[p] \longrightarrow X[p]_{\text{ét}} \longrightarrow 1\,,$$

(see Prop. (4.45)) and $X[p]_{\text{ét}} \otimes_k k_s$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^f$. However, in order to split the exact sequence, and hence to be able to lift the points of $X[p]_{\text{ét}}$ to points of $X[p]$, we in general need to pass to an inseparable extension. See also the examples in (5.26) and (5.27) below for a concrete illustration of this point.

(5.25) Remarks. (i) The p-rank does not depend on the ground field. More precisely, if $k \subset K$ is a field extension and X is an abelian variety over k then $f(X) = f(X_K)$. To see this we may assume that k and K are both algebraically closed. By (4.45) the group scheme $X[p]$ is a product of its local and étale parts, i.e., $X[p] \cong X[p]_{\mathrm{loc}} \times X[p]_{\text{ét}}$. Over $k = \overline{k}$ the étale part becomes a constant group scheme, i.e., $X[p]_{\text{ét}} = \Gamma_k$ with $\Gamma = X[p](\overline{k})$. But after extension of scalars to K the local and étale parts of $X[p]$ remain local and étale, respectively; see ??. Therefore $X[p](K) = \Gamma_k(K) = \Gamma$, so indeed $f(X) = f(X_K)$.

(ii) Later we shall prove that the p-rank may take any value between 0 and $\dim(X)$: given a field k with $\mathrm{char}(k) = p > 0$ and integers $0 \leqslant f \leqslant g$, there exists an abelian variety X over k with $\dim(X) = g$ and $f(X) = f$. In fact, as clearly $f(X_1 \times X_2) = f(X_1) + f(X_2)$, it suffices to show that there exist elliptic curves X_0 and X_1 over k with $f(X_i) = i$.

(iii) An elliptic curve X is said to be *ordinary* if $f(X) = 1$ and *supersingular* if $f(X) = 0$. In the examples below we shall use this terminology. In Chapter ??, we shall define the notions "ordinary" and "supersingular" for abelian varieties of arbitrary dimension. It should be noted that for $\dim(X) > 2$, "supersingular" is *not* equivalent to "p-rank = 0".

(5.26) Example. Let X be an elliptic curve over a field k with $\mathrm{char}(k) = 2$. Then X can be given by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\,, \tag{3}$$

such that the origin is the "point at infinity" $\infty = (0 : 1 : 0)$. A point $P \in X(k)$ with affine coordinates (ξ, η) is a 2-torsion point precisely if the tangent line at P passes through ∞. An easy calculation shows that this happens if and only if $a_1\xi + a_3 = 0$. We cannot have $a_1 = a_3$, because X then would be singular. We conclude:

$$f(X) = \begin{cases} 0 & \text{if } a_1 = 0; \\ 1 & \text{if } a_1 \neq 0. \end{cases}$$

It should be noted that if $a_1 = 0$ and $k = \overline{k}$ then there is a linear change of coordinates such that the equation for X becomes $y^2 + y = x^3$. So, up to isomorphism this is the only supersingular elliptic curve in characteristic 2 (over $k = \overline{k}$).

In the ordinary case, $a_1 \neq 0$, we find that the non-trivial point of order 2 in $X(\overline{k})$ is the point with affine coordinates $(a_3/a_1, \eta)$, where $\eta \in \overline{k}$ satisfies

$$\eta^2 = (a_3/a_1)^3 + a_2(a_3/a_1)^2 + a_4(a_3/a_1) + a_6\,.$$

In particular, we see illustrated here the point made in (5.24) that in general we need to pass to an inseparable extension of the ground field in order to have all p-torsion points rational.

(5.27) Example. Let X be an elliptic curve given by a Weierstrass equation (3), this time over a field k with $\mathrm{char}(k) = 3$. Then $P \in X(k) \setminus \{0\}$ is a 3-torsion point if and only if P is a flex point, i.e., a point at which the tangent line $T_{X,P}$ intersects X with multiplicity 3. (As X is a nonsingular cubic curve the intersection multiplicity cannot be bigger.) Again this allows to compute the p-rank by hand. To simplify, let us assume that $a_1 = a_3 = 0$; this is achieved after a linear change of variables. Then $P = (\xi, \eta) \in X(k)$ is a flex point if and only if

$$4a_2\eta^2 = 4a_2^2\xi^2 + 4a_2a_4\xi + a_4^2\,. \tag{4}$$

Combined with the equation for X this is equivalent to

$$4a_2\xi^3 + (4a_2a_6 - a_4^2) = 0\,. \tag{5}$$

As X is nonsingular we cannot have $a_2 = a_4 = 0$. Hence

$$X \text{ is ordinary} \quad \overset{\text{def}}{\iff} \quad X[3](\overline{k}) \cong \mathbb{Z}/3\mathbb{Z} \quad \iff \quad a_2 \neq 0\,.$$

Note that if $a_2 \neq 0$ then (5) has a unique solution for $\xi \in \overline{k}$, and if $\pm\eta$ are the corresponding solutions of (5.27.1) then $(\xi, \pm\eta)$ are the only two non-trivial 3-torsion points in $X(\overline{k})$. So indeed $X[3](\overline{k}) \cong \mathbb{Z}/3\mathbb{Z}$ and $f = 1$. Further note that solving (4) in general requires passing to an inseparable extension of k.

(5.28) Example. Let k be a field of characteristic 2. Consider the elliptic curve $X \subset \mathbb{P}^2_k$ given by the homogeneous equation $x_1^2x_2 + x_1x_2^2 = x_0^3$, with $\infty = (0 : 1 : 0)$ as origin. As we have seen above, X is supersingular, which for an elliptic curve is the same as saying that X has p-rank zero.

Recall that the group scheme $\alpha_2 = \alpha_{2,k}$ is given by $\alpha_2 = \mathrm{Spec}\,\big(k[\varepsilon]/(\varepsilon^2)\big)$, with co-multiplication $\varepsilon \mapsto \varepsilon \otimes 1 + 1 \otimes \varepsilon$. We are going to give an action $\rho\colon \alpha_2 \times X \to X$ of α_2 on X. For this, write X as the union of two affine open subsets: $X = U_1 \cup U_2$, with

$$U_1 = X \setminus \{(0 : 1 : 0)\} = \mathrm{Spec}\,\big(k[x, y]/(x^3 - y^2 - y)\big)$$

and

$$U_2 = X \setminus \{(0 : 0 : 1)\} = \mathrm{Spec}\,\big(k[x, z]/(x^3 - z^2 - z)\big)\,.$$

Now we can give the action ρ on rings: let $\rho_1\colon \alpha_2 \times U_1 \to U_1$ be given by the homomorphism

$$k[x, y]/(x^3 - y^2 - y) \longrightarrow k[x, y, \varepsilon]/(x^3 - y^2 - y, \varepsilon^2) \qquad \text{with} \quad x \mapsto x + \varepsilon\,, \quad y \mapsto y + \varepsilon x^2\,,$$

and, similarly, let $\rho_2\colon \alpha_2 \times U_2 \to U_2$ be given on rings by $x \mapsto x + \varepsilon$ and $z \mapsto z + \varepsilon x^2$. It is not hard to verify that these homomorphisms are well-defined, that ρ_1 and ρ_2 agree on $U_1 \cap U_2$, and that the resulting morphism ρ is indeed a group scheme action. Note that the points $(0:1:0)$ and $(0:0:1)$ are α_2-stable when viewed as points in the underlying topological space $|X|$, but that they are *not* fixed points of the action. In fact, the action is strictly free.

On U_1 the functions $\xi := x^2$ and $\eta := y^2$ are α_2-invariant. They generate a subring of $O(U_1)$ of index 2; as the functions x and y themselves are clearly not invariant we conclude that

$$O(U_1)^{\alpha_2} \cong k[\xi,\eta]/(\xi^3 - \eta^2 - \eta) \hookrightarrow O(U_1) = k[x,y]/(x^3 - y^2 - y)\,.$$

Similarly, the algebra of α_2-invariants in $O(U_2)$ is generated by x^2 and z^2. We find that the quotient $\alpha_2\backslash X$ is isomorphic to X itself, where the quotient map $X \to X$ is just the Frobenius endomorpism, given on points by $(x,y) \mapsto (x^2, y^2)$.

It can be shown that there is an isomorphism $X[F] \cong \alpha_2$ such that the action ρ described above becomes precisely the action of $X[F]$ on X by translations. As Exercise (??) shows, this does not immediately follow from the fact that the quotient map for the α_2-action is the Frobenius morphism. Note that from the given definition of the action ρ it is not clear that this is an action of a subgroup scheme by translations. We shall return to this later; see (??).

(5.29) Example. Let X be an elliptic curve over a field k with $\mathrm{char}(k) = p$, such that $X[F] \cong \alpha_{p,k}$. It is not hard to verify that $k \xrightarrow{\sim} \mathrm{End}_k(\alpha_{p,k})$, where the map sends $\lambda \in k$ to the endomorphism of $\alpha_{p,k} = \mathrm{Spec}\big(k[t]/(t^p)\big)$ given on rings by $t \mapsto \lambda \cdot t$. For $(\lambda,\mu) \in \mathbb{A}^2(k)$ we obtain an embedding $\varphi_{(\lambda,\mu)}\colon \alpha_{p,k} \hookrightarrow X \times X$ by taking the composition

$$\alpha_{p,k} \xrightarrow{(\lambda,\mu)} \alpha_{p,k} \times \alpha_{p,k} \cong X[F] \times X[F] \subset X \times X\,.$$

The image of $\varphi_{(\lambda,\mu)}$ only depends on $(\lambda:\mu) \in \mathbb{P}^1(k)$.

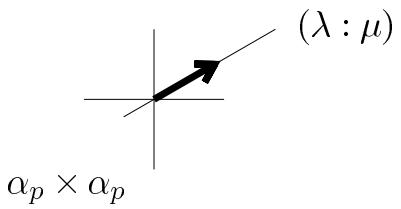

Figure ??.

We get a family of abelian surfaces over $\mathbb{P}^1$ by considering $Y_{(\lambda:\mu)} := (X \times X)/\varphi_{(\lambda,\mu)}(\alpha_p)$. It can be shown that given $(\lambda_0:\mu_0) \in \mathbb{P}^1(k)$, there are only finitely many $(\lambda:\mu)$ with $Y_{(\lambda:\mu)} \cong Y_{(\lambda_0:\mu_0)}$. The conclusion is that we have a non-trivial "continuous" family of isogenies $X \times X \to Y_{(\lambda:\mu)}$. As we shall see later, such examples only exist in characteristic $p > 0$.

§ 3. *Density of torsion points.*

(5.30) Theorem. *Let X be an abelian variety over a field k and let p be a prime number. Then the collection of subschemes $X[p^m]$ for $m \geqslant 0$ is scheme-theoretically dense in X.*

Let $i_m\colon X[p^m] \hookrightarrow X$ be the inclusion homomorphism. By definition, saying that the collection of subschemes $X[p^m] \subset X$ is scheme-theoretically dense in X means that there does not exist a proper closed subscheme $Y \subsetneq X$ such that all i_m factor through Y. If $p \neq \mathrm{char}(k)$ we can express the density of the torsion points of p-power order in a more elementary way. Namely, in that case the following statements hold, as we shall see in the proof.

(1) *Topological density:* the union of the subspaces $\big|X[p^m]\big| \subset |X|$ is dense in $|X|$;

(2) *Function-theoretic density:* the homomorphism of sheaves $O_X \to \prod_{m\geqslant 0} O_{X[p^m]}$ that is induced by the homomorphisms i_m is injective.

Because X is reduced, properties (1) and (2) are equivalent, and (1) immediately implies that the collection of subschemes $X[p^n]$ is scheme-theoretically dense in X.

By contrast, if $p = \mathrm{char}(k)$ then (1) and (2) do not hold, in general. Indeed, if the p-rank of X is zero then the group schemes $X[p^m]$ are local, which means that the underlying topological space is reduced to the single point 0. So in this case we can only interprete the density statement scheme-theoretically.

Proof. We give separate proofs for the cases $p = \mathrm{char}(k)$ and $p \neq \mathrm{char}(k)$.

First assume that $p \neq \mathrm{char}(k)$. It suffices to prove the assertion for $k = \overline{k}$, which from now on we assume. In this case we know that $X[p^m]$ is étale and consists of p^{2gm} distinct closed points. Let $T \subset X(k)$ be the union of all $X[p^m](k)$, and let $Y \subset X$ be the smallest closed subscheme such that all i_m factor through Y. Note that Y is reduced; it is in fact just the reduced closed subscheme of X whose underlying space is the Zariski closure of T. We shall first prove that Y is a subgroup scheme of X.

If $x \in T$ then the translation $t_x\colon X \to X$ maps T into itself; hence $t_x(Y) \subseteq Y$. This holds for all $x \in T$, so it follows that for all $y \in Y(k)$ also the translation t_y maps T into itself, and hence $t_y(Y) \subset Y$. Because Y and $Y \times_k Y$ are reduced, this implies that under the group law $m\colon X \times X \to X$ we have $m(Y \times Y) \subset Y$. As further it is clear that also Y is mapped into itself under the inverse $\iota\colon X \to X$, we conclude that Y is indeed a subgroup scheme of X.

The identity component Y^0 is an abelian subvariety of X. Let N be the number of connected components of Y. Further, let $g = \dim(X)$ and $h = \dim(Y^0)$. By Prop. (5.9) we have $\#Y^0[p^m](k) = p^{2mh}$ for all $m \geqslant 0$, and it follows that $\#Y[p^m](k) \leqslant N \cdot p^{2mh}$. (If $W \subset Y$ is a connected component that contains a torsion point w with $p^m \cdot w = 0$ then translation by w gives an isomorphism $Y^0[p^m] \xrightarrow{\sim} W \cap X[p^m]$.) But by construction, Y contains all torsion points of X of p-power order; so $\#Y[p^m](k) = p^{2mg}$. Taking m very large we see that we must have $h = g$, which gives that $Y^0 = X$.

Next we deal with the case $p = \mathrm{char}(k)$. Let $F^m = F^m_{X/k}\colon X \to X^{(p^m)}$ be the mth power of the Frobenius homomorphism, and let $X[F^m] \subset X$ be the kernel. Because $[p^m] = V^m \circ F^m$ (with $V^m = V^m_{X/k}$ the iterated Verschiebung; see (5.21)) we have $X[F^m] \subset X[p^m]$. So we are done if we can prove that the collection of group schemes $X[F^m]$ is scheme-theoretically dense in X. As in the proof of Prop. (5.15), let $U = \mathrm{Spec}(A)$ with $A = k[x_1, \ldots, x_r]/(f_1, \ldots, f_n)$ be an affine open neigbourhood of the origin e in X such that e corresponds to the maximal ideal $\mathfrak{m} = (x_1, \ldots, x_r) \subset A$. Write $f_i^{(p^m)} \in k[x_1, \ldots, x_r]$ for the polynomial obtained from f_i by raising all coefficients to the power p^m, and write $A^{(p^m)} = k[x_1, \ldots, x_r]/(f_1^{(p^m)}, \ldots, f_n^{(p^m)})$. The restriction of F^m to U is given on rings by the homomorphism $A^{(p^m)} \to A$ that sends x_j to $x_j^{p^m}$. It follows that $X[F^m]$ is the closed subscheme of U defined by the ideal $(x_1^{p^m}, \ldots, x_r^{p^m}, f_1, \ldots, f_n) \subset A$.

Suppose $Y \subset X$ is a closed subscheme such that all inclusion homomorphisms $X[F^m] \hookrightarrow X$ factor through Y. Let $J \subset A$ be the ideal of $Y \cap U$. As in the proof of Prop. (5.15), let $\hat{A}$ be the $\mathfrak{m}$-adic completion of A and choose the coordinates x_i in such a way that $x_1, \ldots, x_g$

(with $g = \dim(X)$) form a basis of $\mathfrak{m}/\mathfrak{m}^2$. We then have an isomorphism $k[\![t_1, \ldots, t_g]\!] \xrightarrow{\sim} \hat{A}$ via $t_i \mapsto x_i$, and we shall identify $\hat{A}$ with $k[\![t_1, \ldots, t_g]\!]$ via this isomorphism. The assumption that $X[F^m]$ is a subscheme of Y means that $J\hat{A}$ is contained in the ideal $(t_1^{p^m}, \ldots, t_g^{p^m})$. The intersection of the ideals $(t_1^{p^m}, \ldots, t_g^{p^m}) \subset \hat{A}$ for all $m \geqslant 0$ is the zero ideal, so we conclude that $J\hat{A} = (0)$. But then the complete local ring $\hat{O}_{Y,e} = \hat{A}/J\hat{A}$ of Y at the origin has Krull dimension g, and consequently $Y = X$. □

We now prove the fact stated in Remark (2.14) that the results in (2.13) are true over an arbitrary, not necessarily perfect, ground field.

(5.31) Proposition. *Let X be an abelian variety over a field k. If $Y \hookrightarrow X$ is a closed subgroup scheme then the connected component $Y^0 \subset Y$ that contains the origin is an open and closed subgroup scheme of Y that is geometrically irreducible. The reduced underlying scheme $Y^0_{\mathrm{red}} \hookrightarrow X$ is an abelian subvariety of X.*

Proof. The assertion that Y^0 is open and closed in Y and is geometrically irreducible, was proven in Prop. (3.17). To prove that Y^0_{red} is an abelian subvariety of X we may assume, to simplify notation, that $Y = Y^0$. We are going to prove that Y_{red} is geometrically reduced. Before we give the argument, let us explain how the desired conclusion follows. If Y_{red} is geometrically reduced then we have, with $k \subset \overline{k}$ an algebraic closure, that $Y_{\mathrm{red},\overline{k}} = (Y_{\overline{k}})_{\mathrm{red}}$ is a closed subgroup scheme of $Y_{\overline{k}}$; see Exercise (3.2). But then also Y_{red} is a closed subgroup scheme of Y. Indeed, the assertion that Y_{red} is a subgroup scheme just means that the morphism $Y_{\mathrm{red}} \times Y_{\mathrm{red}} \to Y$ given on points by $(y_1, y_2) \mapsto y_1 - y_2$ factors through $Y_{\mathrm{red}} \subset Y$. If this holds after extension of scalars to $\overline{k}$ then it also holds over k. So the conclusion is that Y_{red} is a subgroup scheme of X that is geometrically integral; hence it is an abelian subvariety.

We now prove that Y_{red} is geometrically reduced. If $\mathrm{char}(k) = 0$ then $Y = Y_{\mathrm{red}}$ by Thm. (3.20) and we are done by Prop. (3.17). Assume then that $\mathrm{char}(k) = p > 0$. For all positive integers n with $p \nmid n$ the subgroup scheme $Y[n] \subset Y$ is étale; hence we have $Y[n] \subset Y_{\mathrm{red}} \subset Y$. This gives us a homomorphism of sheaves $h_n\colon O_{Y_{\mathrm{red}}} \to O_{Y[n]}$ on $|Y_{\mathrm{red}}| = |Y|$, and we define

$$h\colon O_{Y_{\mathrm{red}}} \to \prod_{p \nmid n} O_{Y[n]}$$

by $h(f) = \prod_n h_n(f)$. Further we know that $(Y_{\overline{k}})_{\mathrm{red}} \subset X_{\overline{k}}$ is an abelian subvariety. By Thm. (5.30) the collection of $Y[n]_{\overline{k}}$, for $n \geqslant 1$ with $p \nmid n$, is topologically dense in $|Y_{\overline{k}}| = |(Y_{\overline{k}})_{\mathrm{red}}|$. This implies that also the collection of all $Y[n]$ is topologically dense in $|Y| = |Y_{\mathrm{red}}|$, and because Y_{red} is reduced, the homomorphism h is injective.

Suppose that Y_{red} is not geometrically reduced. Then there is a finite, purely inseparable field extension $k \subset K$ such that $(Y_{\mathrm{red}})_K$ is not reduced. (See EGA IV, Prop. 4.6.1.) As $k \subset K$ is purely inseparable, we have $|(Y_{\mathrm{red}})_K| = |Y_{\mathrm{red}}|$ and $|Y[n]_K| = |Y[n]|$ for all n. The structure sheaves of $(Y_{\mathrm{red}})_K$ and $Y[n]_K$ are just $O_{Y_{\mathrm{red}}} \otimes_k K$ and $O_{Y[n]} \otimes_k K$, respectively, and the homomorphism

$$h \otimes \mathrm{id}\colon O_{Y_{\mathrm{red}}} \otimes_k K \to \big(\prod_{p \nmid n} O_{Y[n]}\big) \otimes_k K$$

can be identified with the map

$$h_K\colon O_{(Y_{\mathrm{red}})_K} \to \prod_{p \nmid n} O_{Y[n]_K}$$

induced by the inclusions $Y[n]_K \hookrightarrow (Y_{\mathrm{red}})_K$. By our assumptions, $(Y_{\mathrm{red}})_K$ is not reduced, whereas all $Y[n]_K$ are reduced schemes. Hence $h \otimes \mathrm{id} = h_K$ must have a non-trivial kernel. But then also h has a non-trivial kernel ($k \subset K$ being faithfully flat), which contradicts our earlier conclusion that it is injective. □

Exercises.

(5.1) Let $f\colon X \to Y$ be a surjective homomorphism of abelian varieties. Show that f is flat.

(5.2) Let $k = \mathbb{F}_p$. By definition, α_p is a subgroup scheme of $\mathbb{G}_a$, so that we get a natural action $\rho\colon \alpha_p \times \mathbb{G}_a \to \mathbb{G}_a$. Similarly, μ_p is a subgroup scheme of $\mathbb{G}_m$, which gives an action $\sigma\colon \mu_p \times \mathbb{G}_m \to \mathbb{G}_m$.

(i) Identify $\mathbb{G}_m$ with the open subscheme of $\mathbb{G}_a$ given by $x \neq 0$. Show that the action ρ restricts to a free action ρ' of α_p on $\mathbb{G}_m$, and that the Frobenius endomorphism $F\colon \mathbb{G}_m \to \mathbb{G}_m$, given on points by $x \mapsto x^p$, is a quotient morphism for ρ'.

(ii) Conclude that σ and ρ' give rise to the same quotient morphism, even though $\alpha_p \ncong \mu_p$.