SELF DUALITY OF ELLIPTIC CURVES

1. Preliminaries

All schemes and varieties are over a fixed field k. A variety is a reduced, irreducible and *separated* k-scheme X of finite type. The first two conditions, taken together are equivalent to saying that every affine open subscheme of a variety is the spectrum of an integral domain, and the third condition says that the diagonal $\Delta \subset X \times_k X$ is closed. Some comments (especially the scheme theoretic ones) are to clarify issues for the more sophisticated reader (since a scheme is much more than a topological space, and two non-isomorphic schemes could well have the same underlying topology. This especially creates confusion when one says that a map of schems is constant, for a closed "point" z on a scheme Z is repesented by many different closed subschemes of Z, namely by each subscheme $\mathrm{Spec}\,\mathscr{O}_{Z,z}/\mathfrak{m}_z^n$, as n varies over positive integers. Here, as elsewhere, $\mathfrak{m}_z$ is the maximal ideal of the local ring $\mathscr{O}_{Z,z}$. By the image of a map of noetherian schemes $f\colon W \to Z$ one means the subscheme of Z defined by the (necessarily coherent) ideal sheaf of $\mathscr{O}_Z$ given by the kernel of the natural map of sheaves $\mathscr{O}_Z \to f_*\mathscr{O}_W$.

My apologies for being pedantic. Actually, most of my scheme-theory colleagues would say I am being very cavalier.

We will need the following facts:

1) If $f\colon X \to U$ is a map of k-varieties, with X connected and *complete*, and U affine, then f is a constant. Indeed $f(X)$ is a closed, complete connected subscheme of U and U is affine, which forces $f(X)$ to be supported in a point (the only complete and affine schemes are finite sets of points, and any closed subscheme of an affine scheme is again affine) . If we further insist that X is geometrically reduced and geometrically irreducible (comes with the turf for elliptic curves X or even abelian varieties X), then actually $f(X)$ is a k-valued point, rather than an L-valued point, where L is a non-trivial finite extension of k. The idea is that any any map from X to an affine scheme must factor through the canonical map $X \to \mathrm{Spec}\,\Gamma(X,\,\mathscr{O}_X)$ (this is a universal property). If X is geometrically reduced and geometrically irreducible, then $\Gamma(X,\,\mathscr{O}_X) = k$.

2) Let X, Y and U be k-varieties with X complete and $X \times_k Y$ geometrically irreducible and geometrically reduced, $x_0 \in X$, $y_0 \in Y$ and $u_0 \in U$, k-rational points. If

$$\psi\colon X \times_k Y \to U$$

a map of varieties, such that $\psi(\{x_0\} \times Y) = \{u_0\}$ and $\psi(X \times \{y_0\}) = \{u_0\}$ then $\psi(X \times_k Y) = \{u_0\}$. I mean this in the strong sense, namely that the hypothesis is that the images of the "co-ordinate axes" are isomorphic to $\mathrm{Spec}\,k$ (and not $\mathrm{Spec}\,L$ for a non-trivial k-extension L) and the conclusion is that the image of the product is isomorphic to $\mathrm{Spec}\,k$. In other words, this is really a scheme theoretic statement and not merely a topological space statement. The correct way of thinking about the k-rational point x_0, for example, is as a k-scheme map (necessarily a closed

Date: July 19, 2019.

immersion) $x_0\colon \operatorname{Spec} k \hookrightarrow X$. So when we say the image of $\psi\colon X \times_k Y \to U$ is the k-rational point x_0 (i.e. it is "constantly x_0"), we mean that ψ factors as $X \times_k Y \to \operatorname{Spec} k \xrightarrow{x_0} U$, where the first map is the structure map, coming from the fact that $X \times_k Y$ is a k-scheme. Ditto for other statements.

The proof of the statement 2) follows from 1). Without loss of generality (by making a base change to the algebraic closure of k). Pick an affine neighbourhood U' of u_0 in U, and consider $W = U \setminus U'$. W is closed in U, whence its inverse-image $\psi^{-1}(W)$ in $X \times_k Y$ is closed. Since X is complete the natural projection map $p_Y\colon X \times_k Y \to Y$ is proper, whence $p_Y(\psi^{-1}(W))$ is closed in Y. Let $Y' := Y \setminus p_Y(\psi^{-1}(W))$. In set theoretic terms, Y' consists of those points y such that there is a point on $p_Y^{-1}(y)$ which maps into U' under ψ. Since $\psi(x, y_0) = u_0 \in U'$, clearly we have, $y_0 \in Y'$, whence Y' is non-empty. We can work with closed points, since we are dealing with varieties over an algebraically closed field. For each (closed point) $y \in Y$, let $X_y := p_Y^{-1}(y) = X \times_k \operatorname{Spec} k(y) = X$. Note that each X_y is connected, (in fact it is geometrically reduced and irreducible) for otherwise $X \times_k Y$ would not be connected (and hence not irreducible). If $y \in Y'$, then clearly X_y maps into U' under ψ. By 1., $\psi|_{X_y}\colon X_y \to U'$ is a constant, since U' is affine. In fact, since $(x_0,\, y) \in X_y$, and $\psi(x_0,\, y) = u_0$, the constant is actually u_0. It follows that ψ is constant on $X \times_k Y'$. Since $X \times_k Y$ is irreducible, the non-empty open subscheme $X \times_k Y'$ must be dense in $X \times_k Y$. In the ordinary way, we would then conclude that ψ is constant on $X \times_k Y$ (since it so on a dense open subset). But our topologies are not Hausdorff. This is where our hypothesis that our varieties are separated comes in. Since $X \times_k Y$ is separated, this means ψ is constant.

The statement in 2) goes under the name of rigidity.

2. Consequences of rigidity

By an abelian variety, we mean a group variety, which is *complete*. By Proposition 2.1.2 below, such a variety is commutative.

Proposition 2.1.1. *Let A and B be abelian varieties. Let $f\colon A \to B$ be a map of varieties such that $f(0) = 0$. Then f is a map of abelian varieties (i.e. it is a homomorphism of group schemes).*

Proof. Let $m_A\colon A \times_k \to A$ and $m_B\colon B \times_k B \to B$ be the maps maps giving "addition" in A and B. We have to show that the diagram of varieties

$$\begin{array}{ccc} A \times_k A & \xrightarrow{m_A} & A \\ {\scriptstyle f\times f}\downarrow & & \downarrow{\scriptstyle f} \\ B \times_k B & \xrightarrow[m_B]{} & B \end{array}$$

commutes. Let $\varphi_1\colon A \times_k A \to B$ be the composite obtained by following the downward arrow on the left followed by the horizontal arrow at the bottom, and let $\varphi_2\colon A \times_k A \to B$ be the other composite, i.e. "first go right and then south" (a truer political axiom, I do not know of). Consider the map

$$\psi := \varphi_1 - \varphi_2.$$

All the hypotheses of 2) of the previous section (i.e. of rigidity) are satisfied by ψ by taking $X = A$, $Y = A$, $U = B$, $x_0 = y_0 = 0$ and $u_0 = 0$. It follows that ψ is the zero map, whence the diagram commutes. ∎

Proposition 2.1.2. *If A is an abelian variety then $m_A \circ \mathrm{sw} = m_A$, where*

$$\mathrm{sw}\colon A \times_k A \to A \times_k A$$

is the automorphism of varieties obtained by switching factors.

Proof. Same idea. The difference between the two maps has to be constantly zero. □

3. Elliptic curves

Let E be a complete smooth curve, of genus g such that E is a group variety (necessarily with a rational point, namely $0 \in E$). Then sheaf of differentials $\omega_{E/k}$ is free (an argument using translations for example), whence, $2g-2 = \deg \omega_{X/k} = 0$. This means $g = 1$. Conversely, as we shall see, if X is a genus one smooth complete curve with a rational point x_0, then one can impose a group variety structure on X with $x_0 = 0$. From Proposition 2.1.1 this group variety structure is actually unique.

Now forget group structures temporarily. Suppose X is a complete smooth curve. Very obviously X is the variety of effective degree one divisors on X, with the universal family of degree one divisors being the diagonal embedding of X in $X \times_k X$. (We are lucky we are with working with curves, so that the diagonal is a divisor). In other words X is the Hilbert scheme of effective degree one divisors on X, and Δ is the universal family of such divisors, where $\Delta \subset X \times_k X$ is the diagonal embedding.

In the event you are wondering, here is how one would prove that (X, Δ) is $H_1(X)$, where $H_d(X)$ is the Hilbert scheme of *effective* degree d divisors on X. Let q_1 and q_2 be the two projections on $X \times_k X$ and p_1 and p_2 their restrictions to Δ. Let S be a k-scheme, and let q_S (resp. q_X) be the projection $X \times_k S \to S$ (resp. $X \times_k S \to X$). Suppose $\mathscr{D} \subset X \times_k S$ is a divisor such that the resulting map $\mathscr{D} \xrightarrow{p_S} S$ is flat, and gives a family of effective degree one divisors on X. The second half of the last sentence means that, with $X_s := X \times_k k(s)$, for $s \in S$, we have $\mathscr{D}|_{X_s}$ is a (clearly effective) degree one divisor on X_s for every $s \in S$. We have to produce a unique classifying map of k-schemes $g\colon S \to X$ such that $\mathscr{D}$ is the pull-pack of Δ. But clearly $p_S\colon \mathscr{D} \to S$ is an isomorphism of schemes. Well, let me elaborate just a bit. The map p_S is quasi-finite (i.e. the fibres are finite, in fact singletons) and proper. It is therefore finite and hence an affine map. Pick an affine open subscheme $U = \operatorname{Spec} A$ of S. Since p_S is an affine map, $p_S^{-1}(U)$ is also affine, equal to (say) $\operatorname{Spec} B$. We have to show $A \to B$ is an isomorphism. Now, $A \to B$ is a finite flat map. Moreover, for every maximal ideal $\mathfrak{m}$ of A, $A/\mathfrak{m} \to B \otimes_A A/\mathfrak{m}$ is an isomorphism (because, for every $s \in S$, the fibre $p_S^{-1}(s)$ is an effective degree one divisor on X_s, it is isomorphic (as a *scheme*!!) to $\operatorname{Spec} k(s)$). By Nakayama $A_{\mathfrak{m}} \to B_{\mathfrak{m}}$ is an isomorphism for every maximal ideal $\mathfrak{m}$ of A, whence $A \to B$ is an isomorphism. The map $g\colon S \to X$ is then the composite

$$S \xrightarrow{p_S^{-1}} \mathscr{D} \subset X \times_k S \xrightarrow{q_X} X.$$

It is easy to check that the above map fits the requirements.

Now suppose X has genus $g = 1$ as well as a rational point x_0. I want to say that in this case, if $\mathcal{L}$ is a line bundle on X such that $\deg \mathcal{L} = 1$, then there is exactly one effective divisor of degree one which gives rise to $\mathcal{L}$. Since effective divisors of degree one are necessarily of the form $D_p = \{p\}$, where $p \in X$, this would mean that for each such line bundle $\mathcal{L}$ there is associated exactly one point p in X. The correspondence $\mathcal{L} \mapsto p$ would then give the isomorphism between degree one line bundles and X. One obtains the same for degree 0, by translation. (I am sweeping issues of k-rationality etc, temporarily, under the rug.) Here is the idea for showing that a degree one line bundle on X arises from exactly one degree one effective divisor. Let K be any canonical divisor on X. Let D be any divisor of degree 1. We claim there is exactly one effective divisor linearly equivalent to it. Then $\deg K - D = -1$ (we are using $g = 1$, and $\deg K = 2g - 2$ here). We conclude that $l(K - D) = 0$. This means, by Riemann-Roch, that $l(D) = 1$ (this uses $g = 1$). This means that that if $D + (f)$ and $D + (h)$ are effective, then f is a non-zero scalar multiple of (h), whence $(f) = (h)$. Thus there is a unique effective degree one divisor linearly equivalent to D. Since this is effective divisor is of degree one it must be of the form $D_p = \{p\}$ where p is a point of X.

Here is how one would say it properly, in terms of universal properties. Let D_0 be the degree one effective divisor supported with multiplicity one at our rational point x_0, i.e., $D_0 = D_{x_0}$. Let L_0 be the line bundle on X arising from D_0. Let $\mathcal{L}'_1$ be the line bundle on $X \times_k X$ which arises from the divisor Δ and set $\mathcal{L}_1 := \mathcal{L}'_1 \otimes q_2^* L_0^{-1}$. Then $\mathcal{L}_1$ is a family of degree one line bundles on X, parameterized by X (the parameter space is the second factor, and the ambient space on which line bundles vary is the first factor). The pair $(X, \mathcal{L}_1)$ enjoys the following universal property (as we will prove):

If $\mathcal{L}_S$ is any line bundle on a scheme $S \times_k X$ such that $\mathcal{L}_S$ restricted to each fibre X_s of $S \times_k X \to S$ is of degree one, with $\mathcal{L}_S|_{S\times x_0}$ a trivial line bundle, then there is a unique map $g\colon S \to X$ such that $\mathcal{L}_S$ is isomorphic to the pull-back of $\mathcal{L}_1$.

One has to make the argument relative when one works over S. First, semi-continuity shows that $R^1 q_{S*}(\mathcal{L}_S) = 0$, whence $q_{S*}\mathcal{L}_S$ is actually a line bundle on S (need semi-continuity here too). Write $\mathcal{M} = q_{S*}\mathcal{L}_S$. We have a natural map $q_S^*\mathcal{M} \to \mathcal{L}_S$. This gives a map $\mathscr{O}_{X\times_k S} \to \mathcal{L}_S \otimes q_s^*\mathcal{M}^{-1}$, and this is the same as section σ of $F_S = \mathcal{L}_S \otimes {q_S}^*\mathcal{M}^{-1}$. Clearly the family of line bundles on X given by F_S is the same as the family given by $\mathcal{L}_S$. Let $\mathscr{D} \subset X \times_k S$ be the divisor arising from the zero locus of σ. We claim that *$\mathscr{D}$ is flat over S and gives a family of effective degree one divisors on X parametrized by S*. Firstly note that σ behaves well with respect to base changes on S. More precisely, if $S' \to S$ is a k-map and $\mathcal{L}_{S'}$ the pull back of $\mathcal{L}_S$ to $X \times_k S'$, and if $\mathcal{M}'$, $F_{S'}$, σ' etc are obtained from $\mathcal{L}_{S'}$, the way $\mathcal{M}$, F_S, and σ etc were obtained from $\mathcal{L}_S$, then the "primed-objects" are the pull-backs of "un-primed objects". In particular the section σ' of $F_{S'}$ is the pull-back of the section σ of F_S.[1] Specializing to the canonical maps $S' = \operatorname{Spec} k(s) \to S$, where $s \in S$, we see, for each $s \in S$, that $\sigma \otimes k(s)$ is a non-zero section of the degree one line bundle $\mathcal{L}_S|_{X\times_k\{s\}}$ and its zero locus is precisely the unique effective degree one divisor (i.e. a $k(s)$-rational point) D_s of $X_s := X \times_k \operatorname{Spec} k(s)$, and this shows that the fibre of $\mathscr{D} \to S$ over s is the $k(s)$-rational point D_s.

To complete our proof that $\mathscr{D} \to S$ is flat, we appeal to the following standard (and easy) fact from commutative algebra (see [M, (2) $\Rightarrow$ (1), Corollary to Thm. 22.5, p.177]).

[1] This is an aside, loosely related to what was just said. Since $\Gamma(X \times_k S, F_S) = \Gamma(S, q_{S*}F_S)$, the section σ is a section of $q_{S*}F_S$. But $q_{S*}F_S = q_{S*}\mathcal{L}_S \otimes \mathcal{M}^{-1}$ by the projection formula, i.e., $q_{S*}F_S = \mathcal{M} \otimes \mathcal{M}^{-1} = \mathscr{O}_S$, and a little thought shows that σ is the canonical section 1 of $q_{S*}F_S = \mathscr{O}_S$. Note that this means that the "zero-locus" of σ (thought of as a section of F_S) in $X \times_k S$ could never contain an entire fiber X_s of $X \times_k S \to S$. This is the same as saying that $\mathscr{D} \cap X_s$ is at most zero-dimensional. In fact it is always a $k(s)$-rational point.

Let $A \to R$ be a local homomorphism of local rings (i.e. $\mathfrak{m}_A R \subset \mathfrak{m}_R$), such that R is flat over A, and $t \in \mathfrak{m}_R$ is such that the image of t in $R/(\mathfrak{m}_A R) = R \otimes_A (A/\mathfrak{m})$ is a non-zero divisor in $R/(\mathfrak{m}_A R)$. Then $B = R/tR$ is flat over A.

The proof that $\mathscr{D}$ is flat over S is along the following lines. We have to take a local trivialization of $\mathcal{L}_S$ over an open affine subscheme $\operatorname{Spec} R$ of $X \times_k S$. Then the section σ is the same as a map of R-algebras, $R[T] \to R$, which amounts to giving an element $t \in R$. By definition, the closed subscheme $\mathscr{D} \cap \operatorname{Spec} R$ of $\operatorname{Spec} R$ is given by the vanishing of t, i.e., $\mathscr{D} \cap \operatorname{Spec} R = \operatorname{Spec} R/tR$, and the just cited result from [M] applies. Now (X, Δ) is the Hilbert scheme $H_1(X)$, whence we have a unique map $g\colon S \to X$ such that $\mathscr{D}$ is the pull back of Δ under the base change g. This means the pull back of $\mathcal{L}'$ is F_S, and the pull back of $\mathcal{L}$ is $\mathcal{L}_S$. Clearly, g is the unique map which does this.

Anyway, the upshot is that $(X, \mathcal{L}_1)$ is $\operatorname{Pic}^1_{X/k}$. Reminding ourselves that $D_0 = D_{x_0}$ and L_0 the line bundle corresponding to D_0. Setting $\mathscr{L} := \mathcal{L}_1 \otimes p_1^* L_0^{-1}$, we see that $(X, \mathscr{L})$ is the Jacobian of X, denoted either $\operatorname{Pic}^\circ_{X/k}$ or $J(X)$.

Recall we did not worry about the group structure on X to begin with. We have obtained one on it now from $J(X)$. If X started with a group structure such that x_0 is its identity element, then the two group structures on X, one from $J(X)$ and the other, the one we started with, would have to be the same by Proposition 2.1.1. Indeed, apply the Proposition to the identity map $X \to J(X) = X$, the left side having the original group structure, and the right side the one from X's role as the Jacobian.

References

[M] H. Matsumura, *Commutative Ring theory*, Cambridge studies in advanced mathematics 8, Cambridge University Press, Cambridge, 1980.