Reprinted from JOURNAL OF ALGEBRA
All Rights Reserved by Academic Press, New York and London

Vol. 54, No. 2, October 1978
Printed in Belgium

Poncelet Correspondences: Finite Correspondences; Ritt's Theorem; and the Griffiths–Harris Configuration for Quadrics

MICHAEL D. FRIED*

University of California at Irvine, Irvine, California 92717

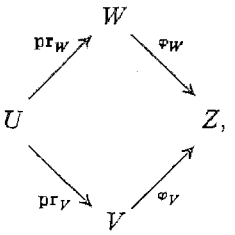
Communicated by Walter Feit

Received August 24, 1977

A geometrically interpretable condition on a correspondence between two algebraic varieties of the same dimension is considered and gives rise to the name *finite correspondence*. After an algebraic characterization of finite correspondences the paper considers many contexts in which the concept appears to be very attractive and historically motivated.

0. INTRODUCTION AND EXAMPLES OF CLASSICAL CORRESPONDENCES

Suppose that V and W are algebraic varieties of the same dimension which are Z-schemes where the structure morphisms $V \to^{\varphi_V} Z$ and $W \to^{\varphi_W} Z$ are finite morphisms. If U is a correspondence between V and W fitting into a commutative diagram,



(0.1)

we say that U is a *finite correspondence* on V and W. In Section 1 we start with an apparently weaker correspondence theoretic definition of finite correspondence. In Theorem 1 these two definitions are shown to be equivalent. The main problem may be phrased in the following way: Given varieties V and W, explicitly describe the finite correspondences between them, or (alternatively) given an explicit set of correspondences between them describe the subset of correspondences which are finite.

* This research partially supported by a 1975 Summer NSF Grant and by a visiting professorship at the University of Tel-Aviv (Spring 1977).

0021-8693/78/0542-0467$02.00/0

A plethora of influences have shaped this paper. McConnell and Berkson [2] starting from [8] gave a suggestion toward a useful characterization of finite correspondences in the category of compact Riemann surfaces. They left as an unsolved problem the production of an algebraic proof of this and their other results. We respond to their preprint with the sought for algebraic generalizations of their results (Section 1). In their simplicity these results fairly begged for illuminating illustration. This too we provided (Section 2). Our motivation for these examples was some infinished business in ongoing arithmetic investigations of the fibers of the Picard bundles of algebraic curves [6]: work parallel to investigations by MacRae [12] and MacRae and Samuel [13].

Much of this might have remained private except that we heard a lecture given by P. Griffiths at UCLA on a "modern" treatment of a classical problem solved by Poncelet. Since Griffiths' lecture inspired the name Poncelet correspondence for the examples of Section 2, we explain in some detail.

Poncelet considered the problem of the inscription of a polygon between two (real) nonintersecting plane conics. Let $\mathscr{C}_{\mathbb{R}}{}^1$ and $\mathscr{C}_{\mathbb{R}}{}^2$ be the real points of these plane conics, where $\mathscr{C}_{\mathbb{R}}{}^1$ "surrounds" $\mathscr{C}_{\mathbb{R}}{}^2$ in $\mathbb{R}^2$. There is a natural correspondence between $\mathscr{C}_{\mathbb{R}}{}^1$ and $\mathscr{C}_{\mathbb{R}}{}^2$ given by $\mathfrak{p} \in \mathscr{C}_{\mathbb{R}}{}^1$ corresponds to the points φ_1 and $\varphi_2 \in \mathscr{C}_{\mathbb{R}}{}^2$, where the lines from $\mathfrak{p}$ to φ_1 and φ_2 are tangent to $\mathscr{C}_{\mathbb{R}}{}^2$. Also, $\varphi \bullet \mathscr{C}_{\mathbb{R}}{}^2$ corresponds to $\mathfrak{p}_1$ and $\mathfrak{p}_2 \in \mathscr{C}_{\mathbb{R}}{}^1$, where $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are the points of intersection of $C_{\mathbb{R}}{}^1$ and the tangent to $\mathscr{C}_{\mathbb{R}}{}^2$ at φ. Let $\mathscr{D}$ be this correspondence on $\mathscr{C}^1 \times \mathscr{C}^2$. Then $\mathscr{D}$ is of degree 2 over $\mathscr{C}^1$ and $\mathscr{C}^2$. The existence of the inscribed polygon is immediately (from Theorem 1 of Section 1) seen to be equivalent to the property: $\mathscr{D}$ is a finite correspondence. To compute the genus of $\mathscr{D}$ we count the ramification points of the cover $\mathscr{D} \to \mathscr{C}^1$: the points $\mathfrak{p} \in \mathscr{C}^1$ such that the two tangents to $\mathscr{C}^2$ from $\mathfrak{p}$ are coincident. Since there are four such points, the Riemann–Hurwitz formula implies that the genus of $\mathscr{D}$ is 1, and the situation is exactly that of Section 2. We have treated the investigation of the conditions that characterize such a Poncelet correspondence and the further conditions that guarantee that the correspondence is finite, over an arbitrary field. Such generality is compatible with the arithmetic considerations of [6, 12, 13].

There are several immediate directions of investigation suggested by the completeness of these characterizations of Poncelet correspondences. A nonobvious generalization arises when we consider the transversal intersection of two nonsingular quadrics $\mathscr{S}_1$ and $\mathscr{S}_2$ in $\mathbb{P}^3$. Over an algebraically closed field each of these quadrics is isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$, and the intersection $\mathscr{E} = \mathscr{S}_1 \cap \mathscr{S}_2$ is an elliptic curve. The projection morphisms of $\mathscr{E}$ on the various copies of $\mathbb{P}^1$ provided by the isomorphisms of $\mathscr{S}_i$ with $\mathbb{P}^1 \times \mathbb{P}^1$ $(i = 1, 2)$ are all of degree 2 and thereby give rise to 4 involutions whose properties are described in Section 4.B. Indeed, these involutions give rise to the same geometric involutions to which Griffiths and Harris [10] associated a polyhedral figure inscribed between the real points of $\mathscr{S}_1$ and $\mathscr{S}_2$. This polyhedral figure is finite if and only if the four associated involutions generate a finite group of automorphisms of $\mathscr{E}$.

We observe the connection between the transversal intersection of quadrics in $\mathbb{P}^3$ and the theory of "2-descent of elliptic curves in Weierstrass normal form" in order to obtain generalization of the results of [10]. These results are presented both in geometric form (i.e., over an algebraically closed field in Section 4.B) for simplicity, and then in arithmetic form for the sake of completeness of the relationship of this problem to the arithmetic of elliptic curves (in Section 4.C).

The discussion of Section 4 concludes with further problems. We mention one suggested by Griffiths in private correspondence. Consider possible analogs of the situations above for two quadrics in $\mathbb{P}^n$ ($n \geqslant 4$). In this connection Griffiths pointed out that the intersection of two transversal quadrics in $\mathbb{P}^5$ is a *quadric line complex*: a variety with doubly infinite families of lines, each family indexed by a point of the Jacobian variety of a hyperelliptic curve of genus 2 (see [20] for this and other interesting facts on intersections of quadrics).

Surprisingly, there are few situations where it is easy to explicitly characterize the finite correspondences even on algebraic curves. In fact, an explicit description of the finite correspondences of *genus* 0 on a pair of genus 0 curves would appear to be extremely difficult. Diophantine problems suggest the usefulness of such a description (as in [5]). In Section 3 we take the opportunity to interpret a very deep theorem due to Ritt [16] that may suggest a route to further characterizations. We have tried to make as explicit as possible the relationship between the material of Section 3, formal groups, and the theory of Complex Multiplication. Indeed, all the correspondences considered in this paper are in some way related to group laws; most coming from the group law on an elliptic curve or an Abelian variety. Still, we would predict that it is naive to think that all interesting examples will arise in this way. See for instance, the comments and example of Section 2.B.

Our last motivation for this paper comes from a lecture presented by William Messing (in one of the 1975 meetings of the Southern California Algebraic Geometry Seminar) on Grothendieck's conjectural theory of motives. Naively put, the theory conjectures that all reasonable cohomology theories on algebraic varieties can be obtained from the theory of algebraic correspondences. Although Grothendieck's theory is *not* conjectural in the case of curves, many interesting results and problems about curves (and higher-dimensional varieties) suggest consideration of a motivic fundamental group. We were especially interested in the extent to which finite correspondences might be viewed as generators of other correspondences.

There are important unsolved problems listed at the end of Sections 1, 3, and 4. Although the description of quadrics given in Section 4.A may well be classical, we know of no reference. Much of this description we learned from B. Bennett. The reader need not read Section 4.A except to see, most clearly, how the author sees that the ideas of Section 4.B should be generalized to higher-dimensional quadrics in Section 4.C.

1. Finite Correspondences

1.A. *Definitions and Proof of the Main Theorem*

Let F be an arbitrary field. For any field L we let $\bar{L}$ be a fixed algebraic closure of L. For V an (irreducible and reduced) algebraic variety defined over F we let $F(V)$ be the field of F-rational functions on V. Let U, V, W be normal algebraic varieties of dimension n where: $U \subset V \times W$, and; the projections $\mathrm{pr}_V: V \times W \to V$, $\mathrm{pr}_W: V \times W \to W$ are finite morphisms when restricted to U. We regard U as a correspondence between V and W.

For $\mathfrak{p} \in V$, define $U(\mathfrak{p}) = \mathrm{pr}_W(U \cdot (\mathfrak{p} \times W))$. Similarly, for $\mathfrak{q} \in W$ define ${}^{\mathrm{tr}}U(\mathfrak{q}) = \mathrm{pr}_V(U \cdot (V \times \mathfrak{q}))$. If $V = W$ we denote by $U^{(n)}$ the nth iterate of the correspondence U. All field extensions of this section are to be regarded as contained in a fixed algebraic closure of the function field $F(U)$.

The correspondence U is said to be a *finite correspondence* if there exists an integer $n > 0$ such that

$$({}^{\mathrm{tr}}U \circ U)^{(n)} \equiv ({}^{\mathrm{tr}}U \circ U)^{(n+1)}. \tag{1.1}$$

For v^{gen} a (Weil) generic point of V this expression is equivalent to $({}^{\mathrm{tr}}U \circ U)^{(n)}(v^{\mathrm{gen}}) = ({}^{\mathrm{tr}}U \circ U)^{(n+1)}(v^{\mathrm{gen}})$. The minimal integer n for which expression (1.1) holds is called the *period of* U, denoted $\mathrm{Per}(U)$.

In this section we compare the following field theoretic properties.

(H.1) $F(V)$ (and therefore $F(W)$) is a finite extension of $F(V) \cap F(W)$;

(H.2) there exists a finite extension M of $F(V)$ and $F(W)$ such that M is a normal extension of both $F(V)$ and $F(W)$, and;

(H.3) the statement (H.2) holds and $\mathrm{Aut}(M/F(V))$ and $\mathrm{Aut}(M/F(W))$ together generate a finite group of automorphisms of M.

It is clear that for the consideration of each of (H.1), (H.2), and (H.3) we may assume (with no loss) that $F(U) = F(V) \cdot F(W)$. *In the main theorem of this section we show that U is a finite correspondence if and only if property* (H.1) *holds.*

Lemma. *The properties* (H.1) *and* (H.3) *are equivalent.*

Proof. We show that (H.1) implies (H.3). Under the hypothesis (H.1) we consider Ω_V (resp. Ω_W) the normal closure of $F(V)/F(V) \cap F(W)$ (resp. $F(W)/F(V) \cap F(W)$). Then $M = \Omega_V \cdot \Omega_W$ is a normal extension of $F(V) \cap F(W)$ containing $F(V)$ and $F(W)$ and so M is a normal extension of both $F(V)$ and $F(W)$. Since M is a finite extension of $F(V) \cap F(W)$, $\mathrm{Aut}(M/F(V) \cap F(W))$ is a finite group. Therefore the subgroups $\mathrm{Aut}(M/F(V))$ and $\mathrm{Aut}(M/F(W))$ generate a finite group of automorphisms of M, and (H.3) holds.

Conversely, we assume that (H.3) holds. The fixed field of $\mathrm{Aut}(M/F(V))$ (resp. $\mathrm{Aut}(M/F(W))$) is a purely inseparable extension L_V (resp. L_W) of $F(V)$

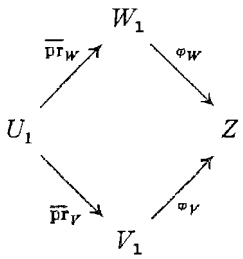
(resp. $F(W)$). Also, the group generated by $\mathrm{Aut}(M/F(V))$ and $\mathrm{Aut}(M/F(W))$ is a finite group G with fixed field $L_V \cap L_W$. Thus L_V (resp. L_W) is a finite extension of $L_V \cap L_W$. We have only to demonstrate that this implies that $F(V)$ (resp. $F(W)$) is a finite extension of $F(V) \cap F(W)$.

Let p be the characteristic of F, and let p^e (resp. p^f) be the exponent of the inseparable extension $L_V/F(V)$ (resp. $L_W/F(W)$). Then $[F(V): F \cdot (L_V)^{p^e}]$ (resp. $[F(W): F \cdot (L_W)^{p^f}]$) is finite, since $F(V)$ (resp. $F(W)$) is a finitely generated extension of F. Let m be the maximum of p^e and p^f. Then,

$$\begin{aligned}
&[F(V) : F(V) \cap F(W)] \\
&\quad \leqslant [F(V) : F \cdot (L_V)^m \cap F \cdot (L_W)^m] \\
&\quad \leqslant [F(V) : F \cdot (L_V)^m] \cdot [F \cdot (L_V)^m : F \cdot (L_V)^m \cap F \cdot (L_W)^m] \\
&\quad \leqslant [F(V) : F \cdot (L_V)^m] \cdot [L_V : L_V \cap L_W].
\end{aligned}$$

The terms in the last expression are finite, so $[F(V) : F(V) \cap F(W)]$ is finite, and (H.1) holds. ∎

THEOREM 1. *Let U, V, W be normal F-varieties of dimension n, as at the beginning of this section. Then U is a finite correspondence on $V \times W$ if and only if there exists an F-variety Z such that*



(1.2)

is a commutative diagram where φ_V and φ_W are finite morphisms, V_1 (resp. W_1 and U_1) is a Zariski F-open subset of V (resp. W and U), and $\overline{\mathrm{pr}}_V$ (resp. $\overline{\mathrm{pr}}_W$) is the restriction of pr_V (resp. pr_W) to U_1.

If U is a finite correspondence, then we may choose Z so that $F(Z) = F(V) \cap F(W)$ where $F(V)$ and $F(W)$ are regarded as subfields of $F(U)$. With this choice, U is a separable correspondence (i.e. pr_V *and* pr_W *are separable morphisms*) *if and only if φ_V and φ_W are separable morphisms. In addition, $\mathrm{Per}(U) = 1$ if and only if $U(\mathfrak{p}) = \varphi_W^{-1}(\varphi_V(\mathfrak{p}))$ for all $\mathfrak{p}$ for which both sides are defined.*

Proof. The existence of the commutative diagram of expression (1.2) is merely a geometric restatement of the field theoretic property (H.1), where $F(Z)$ is taken to be $F(V) \cap F(W)$. In order to facilitate our field theoretic proof, we let u^{gen} be a (Weil) generic point of U. Then $v^{\mathrm{gen}} = \mathrm{pr}_V(u^{\mathrm{gen}})$ (resp. $w^{\mathrm{gen}} =$

$\mathrm{pr}_W(u^{\mathrm{gen}})$) is a generic point of V (resp. W). Then, with no loss, we may identify $F(u^{\mathrm{gen}})$ with $F(U)$.

Let $\widehat{F(u^{\mathrm{gen}})}_{v^{\mathrm{gen}}}$ (resp. $\widehat{F(u^{\mathrm{gen}})}_{w^{\mathrm{gen}}}$) be the normal closure of $F(u^{\mathrm{gen}})/F(v^{\mathrm{gen}})$ (resp. $F(u^{\mathrm{gen}})/F(w^{\mathrm{gen}})$). Let $w^{(1)} = w^{\mathrm{gen}},\ldots, w^{(s)}$ (resp. $v^{(1)} = v^{\mathrm{gen}},\ldots, v^{(r)}$) be the conjugates of w^{gen} (resp. v^{gen}) under the action of $\mathrm{Aut}(\widehat{F(u^{\mathrm{gen}})}_{v^{\mathrm{gen}}}/F(v^{\mathrm{gen}}))$ (resp. $\mathrm{Aut}(\widehat{F(u^{\mathrm{gen}})}_{w^{\mathrm{gen}}}/F(w^{\mathrm{gen}}))$. Then the collection $\{w^{(1)},\ldots, w^{(s)}\}$ is identified with $U(v^{\mathrm{gen}})$, and the collection $\{v^{(1)},\ldots, v^{(r)}\}$ is identified with ${}^{\mathrm{tr}}U(w^{\mathrm{gen}})$. With the obvious continuation of our notation $\bigcup_{i=1}^{s} {}^{\mathrm{tr}}U(w^{(i)})$ is identified with ${}^{\mathrm{tr}}U \circ U(v^{\mathrm{gen}})$. Successively we form the tth iterate $({}^{\mathrm{tr}}U \circ U)^{(t)}$ applied to v^{gen}.

From the previous lemma we must show the equivalence of property (H.3) and the condition that U is a finite correspondence.

First we assume that U is a finite correspondence. Let M be the composite of the fields

$$M^{(t)}(v^{\mathrm{gen}}) = F(v^*;\ v^* \in ({}^{\mathrm{tr}}U \circ U)^{(t)}(v^{\mathrm{gen}}))$$

and

$$M^{(t)}(w^{\mathrm{gen}}) = F(w^*;\ w^* \in (U \circ {}^{\mathrm{tr}}U)^{(t)}(w^{\mathrm{gen}})),$$

where t is the period of U. These are finite extensions of both $F(v^{\mathrm{gen}})$ and $F(w^{\mathrm{gen}})$.

Step 1. *We show that M is a normal extension of $F(v^{\mathrm{gen}})$ and $F(w^{\mathrm{gen}})$.*

Define $V(v^{\mathrm{gen}})$ (resp. $W(w^{\mathrm{gen}})$) to be $({}^{\mathrm{tr}}U \circ U)^{(t)}(v^{\mathrm{gen}})$ (resp. $(U \circ {}^{\mathrm{tr}}U)^{(t)}(w^{\mathrm{gen}})$). Since M is generated by the coordinates of the elements of $V(v^{\mathrm{gen}}) \cup W(w^{\mathrm{gen}})$, we have only to show that the conjugates of each element of $V(v^{\mathrm{gen}}) \cup W(w^{\mathrm{gen}})$ over $F(v^{\mathrm{gen}})$ (resp. $F(w^{\mathrm{gen}})$) are in $V(v^{\mathrm{gen}}) \cup W(w^{\mathrm{gen}})$.

In order to be specific, consider the conjugates of $w^* \in W(w^{\mathrm{gen}})$ and $v^* \in V(v^{\mathrm{gen}})$ over $F(v^{\mathrm{gen}})$. We do an induction on i (resp. j), where i (resp. j) is the minimal integer such that $w^* \in (U \circ {}^{\mathrm{tr}}U)^{(i)}(w^{\mathrm{gen}})$ (resp. $v^* \in ({}^{\mathrm{tr}}U \circ U)^{(j)}(v^{\mathrm{gen}})$). There exists $w^{**} \in (U \circ {}^{\mathrm{tr}}U)^{(i-1)}(w^{\mathrm{gen}})$ such that $w^* \in (U \circ {}^{\mathrm{tr}}U)(w^{**})$. Let w' be a conjugate of w^* over $F(v^{\mathrm{gen}})$. Thus w' corresponds to an embedding of $F(v^{\mathrm{gen}}, w^*)$ into the algebraic closure of $F(v^{\mathrm{gen}})$. This embedding extends to an embedding of $F(v^{\mathrm{gen}}, w^*, w^{**})$ into the algebraic closure. We let w'' be the conjugate of w^{**} corresponding to this embedding. By the induction assumption $w'' \in W(w^{\mathrm{gen}})$. Since $w' \in (U \circ {}^{\mathrm{tr}}U)(w'')$, $w' \in W(w^{\mathrm{gen}})$. Thus, every conjugate of w^* is in $W(w^{\mathrm{gen}})$. The argument for v^* is similar.

Thus M is a normal extension of $F(v^{\mathrm{gen}})$ and of $F(w^{\mathrm{gen}})$, and the argument above easily shows that it is the *smallest* normal extension of both $F(v^{\mathrm{gen}})$ and of $F(w^{\mathrm{gen}})$.

Step 2. *We show that* $\mathrm{Aut}(M/F(v^{\mathrm{gen}}))$ *and* $\mathrm{Aut}(M/F(w^{\mathrm{gen}}))$ *generate a finite group of automorphisms of M.*

Indeed, the groups $\mathrm{Aut}(M/F(v^{\mathrm{gen}}))$ and $\mathrm{Aut}(M/F(w^{\mathrm{gen}}))$ act faithfully and transitively on the finite set of elements of $V(v^{\mathrm{gen}}) \cup W(w^{\mathrm{gen}})$. Thus we obtain

an embedding of the group generated by $\mathrm{Aut}(M/F(v^{\mathrm{gen}}))$ and $\mathrm{Aut}(M/F(w^{\mathrm{gen}}))$ into the finite group of permutations of $V(v^{\mathrm{gen}}) \cup W(w^{\mathrm{gen}})$. This shows that the group generated by $\mathrm{Aut}(M/F(v^{\mathrm{gen}}))$ and $\mathrm{Aut}(M/F(w^{\mathrm{gen}}))$ is a finite group. We conclude that property (H.3) holds.

Conversely, let M^* be a normal extension of $F(v^{\mathrm{gen}})$ and of $F(w^{\mathrm{gen}})$ such that $\mathrm{Aut}(M^*/F(v^{\mathrm{gen}}))$ and $\mathrm{Aut}(M^*/F(w^{\mathrm{gen}}))$ generate a finite group. From the last comment of Step 1 (above) we see that for each integer t', $M^{(t')}(v^{\mathrm{gen}}) \cdot M^{(t')}(w^{\mathrm{gen}})$ is contained in M^*. Note that, in no essential way did we use the fact that $t = \mathrm{Per}(U)$ in Step 1 is a finite number, until the final conclusions of the argument. We now can conclude that $M' = \bigcup_{t'=1}^{\infty} M^{(t')}(v^{\mathrm{gen}}) \cdot M^{(t')}(w^{\mathrm{gen}})$ is a finite normal extension of both $F(v^{\mathrm{gen}})$ and $F(w^{\mathrm{gen}})$. The group $\mathrm{Aut}(M'/F(v^{\mathrm{gen}}))$ (resp. $\mathrm{Aut}(M'/F(w^{\mathrm{gen}}))$) is a quotient of the group $\mathrm{Aut}(M^*/F(v^{\mathrm{gen}}))$ (resp. $\mathrm{Aut}(M^*/F(w^{\mathrm{gen}}))$). Therefore, the hypotheses imply that the group G' generated by $\mathrm{Aut}(M'/F(v^{\mathrm{gen}}))$ and $\mathrm{Aut}(M'/F(w^{\mathrm{gen}}))$ is a finite group.

From the argument of Step 2 above, G' acts transitively on the elements of $W(w^{\mathrm{gen}}) = \bigcup_{t'=1}^{\infty}(U \circ {}^{\mathrm{tr}}U)^{(t')}(w^{\mathrm{gen}})$ and on the elements of $V(v^{\mathrm{gen}}) = \bigcup_{t'=1}^{\infty}({}^{\mathrm{tr}}U \circ U)^{(t')}(v^{\mathrm{gen}})$. A group acting transitively on an infinite number of elements must be infinite. Therefore $W(w^{\mathrm{gen}})$ and $V(v^{\mathrm{gen}})$ are finite sets, and U is a finite correspondence.

In the case that U is a *separable* finite correspondence we conclude in the above argument that $M'/F(v^{\mathrm{gen}})$ and $M'/F(w^{\mathrm{gen}})$ are Galois extensions. Therefore the fixed field of the group generated by $\mathrm{Aut}(M'/F(v^{\mathrm{gen}}))$ and $\mathrm{Aut}(M'/F(w^{\mathrm{gen}}))$ is exactly $F(v^{\mathrm{gen}}) \cap F(w^{\mathrm{gen}})$. Thus $F(v^{\mathrm{gen}})$ (resp. $F(w^{\mathrm{gen}})$) is a separable extension of $F(v^{\mathrm{gen}}) \cap F(w^{\mathrm{gen}})$. This shows that the morphisms $\overline{\mathrm{pr}}_V$ and $\overline{\mathrm{pr}}_W$, in the statement of the theorem, are separable.

In order to conclude the proof of the theorem we have only to characterize the conditions under which a finite correspondence U has period equal to 1. It is clear that if t is the period of U, then $({}^{\mathrm{tr}}U \circ U)^{(t)}(v^{\mathrm{gen}})$ consists of the points of $\varphi_W^{-1}(\varphi_V(v^{\mathrm{gen}}))$. In the case that $t = 1$, this is clearly equivalent to $U(v^{\mathrm{gen}}) = \varphi_W^{-1}(\varphi_V(v^{\mathrm{gen}}))$. The specialization of v^{gen} to any point p of V gives the result. ∎

1.B. *Galois Correspondences and Comments*

Let U, V, W be normal F-varieties of dimension n, where $U \subset V \times W$ and the projections $\mathrm{pr}_V\colon U \to V$ and $\mathrm{pr}_W\colon U \to W$ are finite morphisms. Suppose that there exists a finite extension M of $F(U)$ such that property (H.2) holds: M is a *normal* extension of $F(V)$ and of $F(W)$.

DEFINITION 1.1. Assume the hypotheses above hold. Then we say that U is a *normal correspondence.*

DEFINITION 1.2. Assume in addition to the hypotheses above that M is a Galois extension of $F(V)$ and of $F(W)$. Then we say that U is a *Galois correspondence.*

There does not seem to be such a nice characterization of normal (or Galois) correspondences as the characterization of finite correspondences provided by Theorem 1. However, some simple observations serve to make the relationship between normal correspondences and finite correspondences less mysterious. The lemma of Section 1.A shows that a finite correspondence is a normal correspondence.

Conversely, suppose that U is a *Galois correspondence* between two *curves* V and W. For simplicity's sake we assume that the field F is of characteristic zero (or just that it is a perfect field). Denote by $g(U)$ the *genus* of the nonsingular (i.e., normal) curve U. Then $g(U) \geqslant g(V)$ with equality if and only if either $g(U) = 0$ or, $q(U) = 1$ and, $\mathrm{pr}_V: U \to V$ is an unramified cover. Also, as is well known, a curve of genus greater than 1 has only finitely many automorphisms. Therefore, if U is *not* a finite correspondence, we must have $g(U) = 0$ or 1. Indeed, the problem of finding Galois correspondences U between nonsingular curves V and W which are *not* finite correspondences is equivalent to finding function fields $M, F(V)$, and $F(W)$ in one variable such that:

(1.3) M is of genus 0 or 1 and M is a Galois extension of both $F(V)$ and $F(W)$, and;

(1.4) the Galois groups $G(M/F(V))$ and $G(M/F(W))$ generate an infinite group of automorphisms of M.

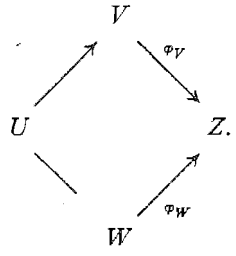
Although we have never seen it written down explicitly, it is not hard to classify the set of function fields satisfying (1.3) and (1.4) since the finite subgroups of automorphisms of a genus 0 or genus 1 curve are well known.

When M and $F(V)$ are of genus 1, the description follows from the isogeny theory of elliptic curves as in [3]; so that when M, $F(V)$, and $F(W)$ are all of genus 1 any Galois (more generally, normal) correspondence is automatically a finite correspondence. When M is of genus 1 and $F(V)$ is of genus 0 the description is started with the ideas that appear in Sections 2 and 3 of this paper. In Section 2, in particular, we are provided with Galois correspondences that are not finite correspondences. When M is of genus 0, the description can be obtained from the explicit list of finite groups of automorphisms of a genus 0 curve given in [4, p. 133]. The nonexceptional groups of [4, p. 133] also provide many examples of Galois correspondences that are not finite correspondences. In [9] some other examples are discussed explicitly in the case that M is of genus 0.

Our next comment also is related to the topics of [9]. Again let us assume that U is a finite correspondence between nonsingular curves V and W, where V and W are of genus 0. Assume also that V and W have F-rational points so that $F(V) = F(x)$, $F(W) = F(y)$, and (by Luroth's theorem) $F(V) \cap F(W) = F(z)$ where x (resp. y) is a uniforming parameter for V (resp. W), and $f(x) = z = h(y)$ for some rational functions $f(X)$, $h(X) \in F(X)$, where X is an indeterminate. In this case, the curve U corresponds to a divisor of $f(x) - h(y)$, a rational function of two variables with the variables separated. The period of U is 1 if and only if

$f(x) - h(y)$ is irreducible as a rational function in two variables (i.e., cannot be written as a product of two rational functions in two variables, both of lower degree). The reducibility of special rational functions in two separated variables occurs as a phenomena related to many interesting Diophantine problems (as in [5]). Only in the case that f and h are polynomials is there a good theory of such reducibility (see [7]).

From the uniqueness of a complete normal model of an algebraic curve, in the case that U, V, W are complete normal curves, the birational character of the conclusion of Theorem 1 can be strengthened to: There is a complete normal curve Z fitting in a commutative diagram



One last concept is of special value and still is not well understood, even in the case of curves. For simplicity assume that U is a separable correspondence, but is *not* a finite correspondence. We say that $\mathfrak{p} \in V$ is an *exceptional point for the integer* n if the cardinality of the support of $({}^{\mathrm{tr}}U \circ U)^{(n)}(\mathfrak{p})$ is less than the cardinality of the support of $({}^{\mathrm{tr}}U \circ U)^{(n)}(v^{\mathrm{gen}})$, where v^{gen} is a generic point of V. The coordinates of the points of the set $({}^{\mathrm{tr}}U \circ U)^{(n)}(v^{\mathrm{gen}})$ generate a finite extension of $F(v^{\mathrm{gen}})$ which we denote by $F(v^{\mathrm{gen}})^{(n)}$. Clearly, $\mathfrak{p}$ *is an exceptional point for the integer* n *if and only if* $\mathfrak{p}$ *corresponds to a place of* $F(v^{\mathrm{gen}})$ *ramified in the extension* $F(v^{\mathrm{gen}})^{(n)}$. We say that the exceptional point $\mathfrak{p} \in V$ is *finite* if for *some* positive integer n the support of $({}^{\mathrm{tr}}U \circ U)^{(n)}(\mathfrak{p})$ is equal to the support of $({}^{\mathrm{tr}}U \circ U)^{(n+1)}(\mathfrak{p})$.

PROBLEM 1. *For* U, V, W *normal varieties of dimension* n *(with special attention to dimension* 1*) give an explicit characterization of the points* $\mathfrak{p} \in V$ *that are finite with respect to the correspondence* U *on* $V \times W$.

2. PONCELET CORRESPONDENCES AND SPECIAL GENUS 2 CURVES

2.A. *Poncelet Correspondences*

We retain previous notation except that we assume that F is a perfect field of characteristic different from 2. For $\mathfrak{p}$ a point on a projective variety V let $F(\mathfrak{p})$ be the field generated by inhomogeneous coordinates of $\mathfrak{p}$.

In the introduction we considered Poncelet's problem. Compatible with that discussion we say that a correspondence U on $V \times W$ is a *Poncelet correspondence* if U, V, W are complete nonsingular curves defined over F, and:

(a) U is of genus 1;

(b) V and W are of genus 0;

(c) $\mathrm{pr}_V: U \to V$ and $\mathrm{pr}_W: U \to W$ are degree 2 morphisms (defined over F), and; (2.1)

(d) V and W have F-rational points.

Our emphasis is on the curve U, and the constructions of this section can be stated entirely in terms of properties of U. We do *not* assume that U is an elliptic curve (i.e., U has a F-rational point). We use the phrase *the inscription problem of Poncelet has an affirmative answer* if the Poncelet correspondence U is a finite correspondence and if V and W are represented by plane conics (as explained in Part C of the proposition below) having no common F-rational points. In the discussion of Poncelet's problem in the introduction, the field F was $\mathbb{R}$.

Basic Problem. For a given U of genus 1, describe explicitly all pairs (V, W) for which the inscription problem of Poncelet has an affirmative answer.

Let $J(U)^{[n]}$ (resp. $J(U)_F^{[n]}$) be the component of the Picard variety of U corresponding to divisor classes (resp. F-rational divisor classes) of degree n on U. Denote by $U^{(n)}$ the *symmetric* product of U with itself n times. There is a natural morphism

$$U^{(n)} \xrightarrow{\Phi^{(n)}} J(U)^{[n]} \tag{2.2}$$

such that for $\mathfrak{p} \in J(U)^{[n]}$ the fiber $(U^{(n)})_{\mathfrak{p}}$ over $\mathfrak{p}$ consists of the positive divisors in the linear system represented by $\mathfrak{p}$. From the Riemann–Roch theorem $(U^{(n)})_{\mathfrak{p}}$ is a complete projective algebraic variety defined over $F(\mathfrak{p})$ and $(U^{(n)})_{\mathfrak{p}} \otimes \bar{F}$ is isomorphic to $\mathbb{P}^N(\bar{F})$ for some integer N. Indeed, for U of genus g and for $n \geqslant 2g - 1$, $N = n - g$ (independent of $\mathfrak{p}$). In our case U is assumed to be of genus 1, so $N = n - 1$.

Now we consider a functorial way in which to obtain covers $U \to^{\mathrm{pr}_V} V$, where V is of genus 0 and the degree of the finite morphism pr_V is n. Consider the diagram

$$\begin{array}{ccccc} U \times U^{(n-1)} & \xrightarrow{\Psi^{(n)}} & U^{(n)} & \xrightarrow{\Phi^{(n)}} & J(U)^{[n]}, \\ \downarrow{\scriptstyle \mathrm{pr}_1} & & & & \\ U & & & & \end{array} \tag{2.3}$$

where pr_1 is the projection of $U \times U^{(n-1)}$ onto its first factor, and; for $\mathfrak{q} \in U$, D a positive divisor of degree $n - 1$ on U, $\Psi^{(n)}$ maps $(\mathfrak{q}, D)$ to $\mathfrak{q} + D \in U^{(n)}$.

For $\mathfrak{p} \in J(U)_F^{[n]}$ consider a closed subscheme V of the fiber $(U^{(n)})_{\mathfrak{p}}$ for which: *$V \otimes \bar{F}$ is a line in the projective space $(U^{(n)})_{\mathfrak{p}} \otimes \bar{F}$, and; the linear system corresponding to $V \otimes \bar{F}$* (of dimension 1) *is free of base points.* From (2.3) we obtain the diagrams

$$\text{(a)} \qquad \begin{array}{ccc} (U \times U^{(n-1)})_{\mathfrak{p}} & \xrightarrow{\Psi_{\mathfrak{p}}^{(n)}} & (U^{(n)})_{\mathfrak{p}} \\ \downarrow{\scriptstyle \overline{\mathrm{pr}}_1} & & \\ U & & \end{array} \tag{2.4}$$

and;

$$\text{(b)} \qquad \begin{array}{ccc} V' & \xrightarrow{\Psi_{\mathfrak{p}}^{(n)}} & V, \\ \downarrow{\scriptstyle \overline{\mathrm{pr}}_1} & & \\ U & & \end{array}$$

where $\overline{\mathrm{pr}}_1$ is the restriction of pr_1 to the fiber over $\mathfrak{p}$, and; V' is the pullback of V under $\Psi_{\mathfrak{p}}^{(n)}$. From the above remarks we easily conclude that $\overline{\mathrm{pr}}_1 \colon V' \to U$ is an isomorphism, and we define $U \to^{\mathrm{pr}_V} V$ to be the morphism obtained from $\Psi_{\mathfrak{p}}^{(n)} \circ (\overline{\mathrm{pr}}_1)^{-1}$.

THEOREM 2. Part A. *Let U be a complete normal curve of genus 1 defined over F. The pairs (V, W) for which* (2.1)(a), (b), (c) *hold are in one–one correspondence with distinct pairs of points on $J(U)_F^{[2]}$. In addition, (V, W) gives a Poncelet correspondence* (*i.e.* (2.1)(d) *holds*) *if (V, W) corresponds to $(\mathfrak{p}_1, \mathfrak{p}_2) \in J(U)_F^{[2]} \times J(U)_F^{[2]}$, where $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are both represented by F-rational divisors of degree 2.*

Part B. *Let $J(U)^{[2]} \times J(U)^{[2]} \to^{\alpha} J(U)^{[0]}$ be defined by $\alpha(\mathfrak{p}_1, \mathfrak{p}_2) = \mathfrak{p}_1 - \mathfrak{p}_2$ (regarded as a divisor of degree 0). If $(\mathfrak{p}_1, \mathfrak{p}_2) \in J(U)_F^{[2]} \times J(U)_F^{[2]}$ corresponds to (V, W) satisfying* (2.1)(a), (b), *and* (c), *then U is a finite correspondence on $V \times W$ if and only if $\alpha(\mathfrak{p}_1, \mathfrak{p}_2)$ is a point of finite order in the elliptic curve structure on $J(U)^{[0]}$.*

Part C. *Suppose $(\mathfrak{p}_1, \mathfrak{p}_2) \in J(U)_F^{[2]} \times J(U)_F^{[2]}$ corresponds to a pair (V, W) satisfying* (2.1)(a), (b), (c), *and* (d). *Then V (resp. W) is represented by a plane conic from the linear system associated to the divisor $\mathrm{pr}_V(D_2)$ (resp. $\mathrm{pr}_W(D_1)$) on V (resp. W), where D_1 (resp. D_2) is a positive F-rational divisor of degree 2 representing $\mathfrak{p}_1$ (resp. $\mathfrak{p}_2$). If these plane conics have no common F-rational points, then $(\mathfrak{p}_1, \mathfrak{p}_2)$ provides an affirmative answer to the inscription problem of Poncelet.*

Proof of Part A. If $(\mathfrak{p}_1, \mathfrak{p}_2) \in J(U)_F^{[2]} \times J(U)_F^{[2]}$, we obtain the pair (V, W) from the discussion preceeding the statement of the proposition in the case $n = 2$. Conversely, assume that $U \to^{\varphi} V$ is a degree 2 morphism of nonsingular curves with V of genus 0. Then the fibers of φ give a one-dimensional linear system of divisors such that the divisor class (of degree 2) is defined over F. Thus φ

corresponds to a point of $J(U)^{[2]}_F$. This divisor class is represented by a F-rational divisor if and only if V has an F-rational point.

Proof of Part B. Assume $(\mathfrak{p}_1, \mathfrak{p}_2)$ and (V, W) correspond as hypothesized in the statement of Part B. The morphisms $U \to^{\mathrm{pr}_V} V$ and $U \to^{\mathrm{pr}_W} W$ (since they are of degree 2) correspond to automorphisms σ_V and σ_W of U. From the proof of Theorem 1, U is a finite correspondence if and only if σ_V and σ_W generate a finite group of automorphisms of U. In order to check the condition that σ_V and σ_W generate a finite group of automorphisms of U we may (with no loss) extend scalars to $\bar{F}$. Over $\bar{F}$, $J(U)^{[0]}$ and U are isomorphic so that we may assume that U has the group structure of an elliptic curve. For $a \in U_{\bar{F}}$ let T_a denote translation by a and let τ be the canonical involution on $U_{\bar{F}}$. Then we may write σ_V (resp. σ_W) as the composition of automorphisms $T_{-a(V)} \circ \tau \circ T_{a(V)}$ (resp. $T_{-a(W)} \circ \tau \circ T_{a(W)}$) for $a(V) \in U_{\bar{F}}$ (resp. $a(W) \in U_{\bar{F}}$). Consider $\sigma_V \circ \sigma_W^{-1} = \sigma_V \circ \sigma_W$. This can be written as $T_{2 \cdot a(W) - 2 \cdot a(V)} = \gamma$. Clearly γ and σ_V generate the same group as in generated by σ_V and σ_W. Also, the group generated by γ and σ_V is easily seen to be of finite order if and only if γ is of finite order (in which case the group is of order 2 times the order of γ). Also, γ is of finite order if and only if the point on $U_{\bar{F}}$ represented by $2 \cdot a(W) - 2 \cdot a(V)$ is of finite order. We conclude the proof of Part B by noticing that, in the identification of $J(U)^{[0]}_F$ and $U_{\bar{F}}$, $\alpha(\mathfrak{p}_1, \mathfrak{p}_2)$ represents the point $2 \cdot a(W) - 2 \cdot a(V)$.

Proof of Part C. The Riemann–Roch theorem demonstrates that V (resp. W) is represented as a plane conic from the projective embedding associated to the divisor $\mathrm{pr}_V(D_2)$ (resp. $\mathrm{pr}_W(D_1)$). The remainder of the assertion of Part C is clear once we have demonstrated that the correspondence induced on V and W as plane conics (the Poncelet correspondence as described in the introduction) is the same as the correspondence given by U. Actually, this need not quite be the case since if U' is the Poncelet correspondence (as in the introduction) then we obtain new correspondences on V and W (as plane conics) by composing U' with an automorphism of V (on the left) or an automorphism of W (on the right). Modulo this inexactitude, however, it is clear that U is unique. ∎

In [6] it is shown that the $\mathbb{P}^1$-bundle

$$U^{(2)} \otimes \bar{F} \to J(U)^{[2]} \otimes \bar{F}$$

over the elliptic curve $J(U)^{[2]} \otimes \bar{F}$ may be identified with the $\mathbb{P}^1$-bundle denoted A_{-1} in Atiyah's classification [1]. The classification over F of such surfaces is also considered through explicit identifications within the Brauer group over $J(U)^{[\,]}$. As an example of the kind of results obtained, we remark that if F is a number field and if $J(U)^{[\,]}$ has an F-rational point, then the essential obstruction to this bundle being locally trivial in the Zariski topology over F lies in the quotient of the *Weil–Chatelet group* of $J(U)^{[2]}$ by the *Tate–Shafarevich group* of $J(U)^{[2]}$ (see [3] for definitions).

It is only reasonable to point out that even though the proposition is very explicit in its classification of Poncelet correspondences, there is no definitive theory of F-rational points on an elliptic curve over an arbitrary field. Therefore the proposition throws the classification back to unsolved problems in Diophantine analysis. However, in the case considered by Poncelet (and Griffiths, see the Introduction) $F = \mathbb{R}$. In this case (or the case where the field is a p-adic field) the Diophantine analysis can be made quite explicit (see [11] or [3]).

2.B. *Curves Whose Jacobian is Isogeneous to a Product of Two Elliptic Curves*

In this subsection we merely want to indicate an interesting example that is also related to elliptic curves. Therefore we will not be as arithmetically precise as we were in Section 1.A.

Let $\bar{F}$ be an algebraically closed field of characteristic different from 2. Let $\lambda_1, \lambda_2 \in \bar{F} - \{0, 1\}$ *be distinct* elements of $\bar{F}$, and consider the elliptic curves in Legendre normal form given by

$$E_i : y_i^2 = x(x - 1)(x - \lambda_i), \qquad i = 1, 2.$$

Let E_i^* be the completion of E_i in $\mathbb{P}^2$ (coordinates given by (X_i, Y_i, Z), where $Y_i^2 \cdot Z = X(X - Z)(X - \lambda_i Z)$), $i = 1, 2$. Consider the complete nonsingular curve U whose function field over $\bar{F}$ is given by $\bar{F}(x, (x(x - 1)(x - \lambda_1)^{1/2}), (x(x - 1)(x - \lambda_2))^{1/2})$. An affine model for U is described by the coordinates (x, y_1, y_2). There are two natural projections:

$$\mathrm{pr}_i : U \to E_i^* \quad \text{corresponding to} \quad (x, y_1, y_2) \to (x, y_i), \quad i = 1, 2. \tag{2.5}$$

In this way we have presented U as a correspondence on $E_1^* \times E_2^*$. Since the degree of pr_i is 2, $i = 1, 2$, $\bar{F}(U)$ is a Galois extension of $\bar{F}(E_i^*)$, $i = 1, 2$. Thus, U is a Galois correspondence on $E_1^* \times E_2^*$ (as in Section 1.B), and therefore, by the remarks of Section 1.B, U is a finite correspondence. Indeed, E_1^* and E_2^* are both degree 2 covers of the x-sphere, and U is a cover of the x-sphere ramified of order 2 at two places each over $x = 0, 1, \infty, \lambda_1$, and λ_2. By the Riemann–Hurwitz formula the genus $g(U)$ of U is given by: $2(4 + g(U) - 1) = \sum_{\mathfrak{p} \in U} (e(\mathfrak{p}) - 1) = 10$, where $e(\mathfrak{p})$ is the order of ramification of the place $\mathfrak{p}$ in the cover of the x-sphere by U. *Thus* $g(U)$ *is* 2.

The canonical involution τ on U is induced by multiplication by -1 on $E_1^* \times E_2^*$, and the quotient of U by the group generated by τ is a 2-sheeted cover of the x-sphere ramified at $x = \lambda_1$ and at $x = \lambda_2$. This situation might be regarded as the analog of the Poncelet correspondences for genus 2 curves. The point of the example is, however, that in a lot of ways these analogs are much simpler than are the Poncelet correspondences.

3. Ritt's Theorem, Complex Multiplication, and Formal Groups

Let F be a field of zero characteristic. Let $\mathscr{C}$ be a nonsingular projective curve over F of genus 0. Since $\mathscr{C}$ is a Brauer–Severi variety of dimension 1, $\mathscr{C}$ is determined up to isomorphism by its class in the Brauer group $H^2(F)$. We denote this class by $[\mathscr{C}]$. Let $\mathscr{C} \to^{\varphi} \mathscr{C}'$ be a finite morphism of nonsingular, projective F-curves. The following proposition appears in [6] (but it is not needed for the main discussion of this section).

Proposition. *In the notation above:* $[\mathscr{C}']$ *is the* 0*-class of* $H^2(F)$ *if* $\deg(\varphi)$ *is even, and;* $[\mathscr{C}'] = [\mathscr{C}]$ *if odd. In addition, if* $\mathscr{C}$ *and* n $(=\deg(\varphi))$ *are regarded as given, then a morphism* $\mathscr{C} \to^{\varphi} \mathscr{C}'$ *(as above) exists, with* $\deg(\varphi) = n$. *In fact, such morphisms correspond to the* F*-rational points on an* F*-form of a Grassmanian.*

One of the most intriguing problems considered in [6] is the description of the *Poncelet correspondences* between two genus 0 curves V and W for which $[V]$, $[W] \in H^2(F)$ are given a priori.

In this section we consider U, V, W, where U is an irreducible *genus* 0 correspondence between V and W (as in Section 1). From the proposition above, the class $[U] \in H^2(F)$ determines $[V]$ and $[W]$ from the degree of the morphisms $\mathrm{pr}_V\colon U \to V$ and $\mathrm{pr}_W\colon U \to W$. It would appear feasible to consider versions of the results of this section in the case that $[U]$ is any element of $H^2(F)$. However, for the sake of clarity of presentation of our version of Ritt's theorem, we attempt only the case where $[U] = 0$ (i.e., U is isomorphic to $\mathbb{P}^1$).

Let t be a uniformizing parameter for $\mathbb{P}^1$. Since the function fields $F(U), F(V)$, and $F(W)$ are all isomorphic to $F(t)$, by explicitly choosing these isomorphisms we may assume that U is given by a pair (f_V, f_W), where $f_V, f_W \in F(t)$. Such a pair gives a (not necessarily irreducible) correspondence on $\mathbb{P}^1 \times \mathbb{P}^1$ by: for $x_0 \in \bar{F}$, $x_0 \to f_W(f_V^{-1}(x_0))$, where $f_V^{-1}(x_0)$ is the collection of values t_0 in $\bar{F}$ such that $f_V(t_0) = x_0$.

Definition 3.1. Let $C_f = (f_1, f_2)$ and $C_g = (g_1, g_2)$ be pairs of elements of $F(t)$. We say that C_f and C_g are *equivalent* if there exist linear fractional transformations (i.e., degree 1 elements of $F(t)$) l_1, l_2, l such that $l_1(f_1(l(t))) = g_1(t)$ and $l_2(f_2(l(t))) = g_2(t)$.

Note that C_f gives a finite correspondence if and only if there exists $f_3, f_4 \in F(t)$ such that $f_3(f_1(t)) = f_4(f_2(t))$. Also, if C_f and C_g (as in the definition) are equivalent, then C_f gives a finite correspondence if and only if C_g gives a finite correspondence.

Definition 3.2. We say that $C_f = (f_1, f_2)$ is a *commutative correspondence* if $f_1(f_2(t)) = f_2(f_1(t))$. Note that if C_f is equivalent to a commutative correspondence then it is a finite correspondence. However, C_f may be equivalent to a commutative correspondence and not be commutative itself.

For two correspondences C_f, C_g we introduce a multiplication $C_f * C_g = (f_1(g_1(t)), f_2(g_2(t)))$. Note that this multiplication is *not* related in any simple-minded way to the usual multiplication of correspondences that comes from intersection theory. However, we have the formula

$$C_f = (f_1(t), t) * (t, f_2(t)). \tag{3.1}$$

DEFINITION 3.3. For $C_f = (f_1, f_2)$ we let $\mathcal{A}(C_f)$ be the set of $C_g = (g_1, g_2)$ such that $f_i(g_i(t)) = g_i(f_i(t))$ for $i = 1, 2$. Then, for $C_g \in \mathcal{A}(C_f)$ we have $C_g * C_f = C_f * C_g$.

Consider the free Abelian group $\overline{\mathcal{A}(C_f)}$ on the elements of $\mathcal{A}(C_f)$ equipped with a multiplication given by $*$. The identity for multiplication is (t, t), and $\overline{\mathcal{A}(C_f)}$ is easily seen to have an associative ring structure.

Our translation of Ritt's theorem [16] to this context amounts to an explicit description of the ring $\overline{\mathcal{A}(C_f)}$ when C_f is an *irreducible commutative correspondence*. First we list the relevant examples of commutative correspondences. Let $h \in F(t)$, and let $h^{(n)}(t)$ denote the functional composition of h, n times. We regard as trivial the commutative correspondence C_f, where $f_i(t) = h^{(n_i)}(t)$, $i = 1, 2$. The hypotheses of Theorem 3 (below) have been contrived to exclude this case (i.e., if n_1, n_2 are positive and degree h is at least 2, then $(h^{(n_1)}(t), h^{(n_2)}(t)) = C_f$ is not an irreducible correspondence).

Let $\mathbb{G}_m(F)$ be the affine multiplicative group regarded as an F-scheme. We write the coordinate ring of $\mathbb{G}_m(F)$ as $F[t, 1/t]$. The automorphism group $\mathrm{Aut}(\mathbb{G}_m(F))$ is generated by α_m, which is induced on the coordinate ring level by the substitution $t \to 1/t$. An isogony ψ_n of $\mathbb{G}_m(F)$ of degree n is induced on the coordinate ring level by the substitution $t \to t^n$. We obtain a commutative diagram

$$\begin{array}{ccc} \mathbb{G}_m(F) & \xrightarrow{\psi_n} & \mathbb{G}_m(F) \\ \downarrow & & \downarrow \\ \mathbb{G}_m(F)/\{\alpha_m\} & \xrightarrow{\bar{\psi}_n} & \mathbb{G}_m(F)/\{\alpha_m\}, \end{array} \tag{3.2}$$

where $\bar{\psi}_n$ is the effect of ψ_n induced on the quotient of $\mathbb{G}_m(F)$ by the group generated by α_m. Consider the upper row of (3.2). A geometric point t^0 of $\mathbb{G}_m(\bar{F})$ goes to $(t^0)^n \in \mathbb{G}(\bar{F})$. Consider the lower row in (3.2). A geometric point $\mathfrak{p}$ of $\mathbb{G}_m(\bar{F})/\{\alpha_m\}$ corresponds to the value $t^0 + 1/t^0$ if $t^0 \in \mathbb{G}_m(\bar{F})$ lies above $\mathfrak{p}$. Then $\bar{\psi}_n(\mathfrak{p})$ corresponds to $(t^0)^n + 1/(t^0)^n$. Therefore $\bar{\psi}_n$ is a map from the affine line to the affine line corresponding to the polynomial (nth Chebychev polynomial of first kind) $T_n(X)$ for which: $T_n(t + 1/t) = t^n + 1/t^n$.

If n_1 and n_2 are relatively prime integers we obtain irreducible commutative correspondences from

$$\begin{array}{lll} \text{(a)} & C_f = (t^{n_1}, t^{n_2}) & (\textit{cyclic} \text{ case}), \\ \text{(b)} & C_f = (T_{n_1}(t), T_{n_2}(t)) & (\textit{Chebychev} \text{ case}). \end{array} \tag{3.3}$$

Consider now an elliptic curve E defined over F. Consider also: $\theta(E)$, a nontrivial subgroup of the automorphisms of E fixing the origin, and; H, a finite subgroup of points of $E_{\bar{F}}$ such that H is both $\theta(E)$ and $G(\bar{F}/F)$ invariant, and E/H is isomorphic to E. From this data we obtain a commutative diagram

$$\begin{array}{ccc} E & \xrightarrow{\psi_H} & E/H \simeq E \\ \downarrow & & \downarrow \\ E/\theta(E) & \xrightarrow{\bar{\psi}_H} & E/\theta(E). \end{array} \tag{3.4}$$

Since $\theta(E)$ is a nontrivial group, $E/\theta(E)$ is isomorphic to $\mathbb{P}^1$. If $\theta(E)$ (which is of order 2, 4, 3, or 6) is the *full* subgroup of automorphisms of E fixing the origin, then $\bar{\psi}_H$ is uniquely determined, independently of the choice of the isomorphism of E/H with E. Write E in Weierstrass normal form:

$$y^2 = x^3 + ax + b.$$

For details on these and further comments see [3]. In each of the cases for $\theta(E)$ the function field $F(E/\theta(E))$ has a preferred generator: $F(E/\theta(E)) = F(x)$ if $\theta(E)$ is of order 2; $F(E/\theta(E)) = F(x^2)$ if $\theta(E)$ is of order 4; $F(E/\theta(E)) = F(y)$ if $\theta(E)$ is of order 3, and; $F(E/\theta(E)) = F(x^3)$ if $\theta(E)$ is of order 6. We let this preferred generator be $t = t(\theta(E))$. Thus the diagram (3.4) results in a rational function f_H such that $f_H(t)$ is the preferred generator of the image of $F((E/H)/\theta(E))$ in $F(E/\theta(E))$ coming from the lower row of (3.4).

If H_1, H_2, are nonintersecting subgroups of E, where E and $\theta(E)$ are fixed then we obtain an irreducible commutative correspondence from

$$C_f = (f_{H_1}(t), f_{H_2}(t)). \tag{3.5}$$

THEOREM 3. *In each of the cases* (3.3a), (3.3b) *or* (3.5) *above the ring* $\overline{\mathcal{O}(C_f)}$ *is a commutative ring. In fact, we describe explicit generators* C_g, *as follows*:

(i) *In case* (3.3a), $C_g = (t^{\bar{n}_1}, t^{\bar{n}_2})$, *where* $\bar{n}_1$ *and* $\bar{n}_2$ *run over all pairs of integers*;

(ii) *In case* (3.3b), $C_g = (T_{\bar{n}_1}(t), T_{\bar{n}_2}(t))$, *where* $\bar{n}_1$ *and* $\bar{n}_2$ *run over all pairs of positive integers, and*;

(iii) *In case* (3.5), $C_g = (f_{\bar{H}_1}(t), f_{\bar{H}_2}(t))$, *where* $\bar{H}_1$ *and* $\bar{H}_2$ *run over all pairs of finite subgroups of* $E_{\bar{F}}$ *that are* $G(\bar{F}/F)$ *and* $\theta(H)$ *invariant and for which* $E_{\bar{F}}/\bar{H}_i$, $i = 1, 2$ *is isomorphic to* $E_{\bar{F}}$.

Conversely, if we are given an irreducible commutative correspondence C_f, *there exists a linear fractional transformation* $l(t)$ *such that* $\overline{\mathcal{O}(C_f)}$ *is obtained from one of the rings* $\overline{\mathcal{O}(C_f)}$ *described in* (i), (ii), *or* (iii) *by*: $\overline{\mathcal{O}(C_f)}$ *is generated by* $C_{l\circ g\circ l^{-1}} = (l(g_1(l^{-1}(t)), l(g_2(l^{-1}(t)))$ *where* C_g *runs over elements generating* $\overline{\mathcal{O}(C_f)}$.

Comments on the Proof. Ritt computed explicitly (in terms of special functions such as the Weierstrass $\mathscr{P}$-function) the pairs of rational functions f_1 and f_2 such that $f_1(f_2(t)) = f_2(f_1(t))$. We have merely rephrased his results to suit our more arithmetico-geometrical context. However, the proof of Ritt's results are unbelievably complicated. Our rephrasing suggests that to each commutative correspondence there ought to be a natural way to associate a formal group.

We describe a naive approach to simplifying the proof of Ritt's results. For $x = f(t)$, $f(t) \in \bar{F}(t)$, let $\Omega_{f(t)-x}$ be the Galois closure of the field extension $\bar{F}(t)/\bar{F}(x)$. Let $f_1, f_2 \in \bar{F}(t)$ be such that $C_f = (f_1, f_2)$ is an irreducible commutative correspondence. Suppose it could be established that $\Omega_{f_1(f_2(t))-x}$ is isomorphic (as a function field) to $\Omega_{f_1(t)-x}$ (resp. $\Omega_{f_2(t))-x}$). Then, since $\Omega_{f_i(t)-x} \subseteq \Omega_{f_i(f_2(t))-x}$ for $i = 1, 2$ we deduce that the genus of $\Omega_{f_1(f_2(t))-x}$ is 0 or 1, and the results above can be easily deduced.

One last comment for those unfamiliar with the theory of complex multiplication (see [18, 19]). For "most" elliptic curves E, the only subgroups H for which E/H is isomorphic to E are the congruence subgroups $H_n = \{\mathfrak{p} \in E_{\bar{F}} \mid n \cdot \mathfrak{p} = 0 \text{ on the elliptic curve}\}$. Those elliptic curves for which there are additional subgroups are the elliptic curves with *complex multiplications*. Each of these (up to isomorphism) corresponds to some divisor class of the ring of integers $\mathcal{O}_L$ of a complex quadratic extension field L of the rational numbers. In order to explicitly describe the ring $\overline{\mathcal{O}(C_f)}$ in this case, one must refer back to the concepts of algebraic number theory and an explicit description of the Abelian extensions of the field L via Artin's reciprocity law. ∎

PROBLEM 2. *Give a proof of Theorem* 3 (*Ritt's Theorem*) *based on the comments above.*

PROBLEM 3. *Let U, V, W be nonsingular complete curves over a field F, where $U \subset V \times W$ gives a correspondence on $V \times W$. Assume that V and W are genus* 0 *curves* (*not necessarily having an F-rational point*). *Describe explicitly the possible U, V, W such that $U \otimes \bar{F}$, $V \otimes \bar{F}$, $W \otimes \bar{F}$ give one of the correspondences as described in* (3.3a), (3.3b), *or* (3.5).

4. QUADRICS IN $\mathbb{P}^n$

4.A. *Descriptions of Quadrics in* $\mathbb{P}^n$

We sketch an inductive description of the nonsingular quadrics in $\mathbb{P}^n$ whereby they are obtained from nonsingular quadrics in $\mathbb{P}^{n-2}$. The nonsingularity assumption is not severe, and with the aid of the opening remarks of [20], the reader could put together an analogous construction for all quadrics. For simplicity's sake we assume that all construction takes place over an algebraically closed field $\bar{K}$ (but see comments at the end of the subsection).

Let $Z \subseteq \mathbb{P}^n$ be a nonsingular quadric, and let P be a point of Z. Let $\mathbb{P}_\infty^{n-1}$ be a hyperplane of $\mathbb{P}^n$ not containing P and meeting Z transversally. We may identify $\mathbb{P}_\infty^{n-1}$ with the projectivized tangent one to P in $\mathbb{P}^n$, denoted $\mathbb{P}(\mathbb{T}_{\mathbb{P}^n,P})$. Projection from P gives a correspondence between Z and $\mathbb{P}_\infty^{n-1}$ given by $\pi\colon Z - \{P\} \to \mathbb{P}_\infty^{n-1}$, where $\pi(Q)$ is the intersection of the line l_Q from P to Q and $\mathbb{P}_\infty^{n-1}$ for Q in $Z - \{P\}$.

Extend this to a map $\tilde{\pi}\colon \tilde{Z} \to \mathbb{P}_\infty^{n-1}$, where $\tilde{Z}$ is Z with P *blown up* (see [14, Chap. 3]). That is, Z is obtained by replacing P by all of its tangent directions in Z. Let V be the locus of those Q in Z such that l_Q is *contained* in Z. Then $\pi|_{Z-V}$ is an isomorphism onto its image.

Assume that $X_0, \ldots, X_n$ are the coordinates of the ambient projective space $\mathbb{P}^n$, and let P be the origin in the affine subspace $D_+(X_0)$ (complement in $\mathbb{P}^n$ of the hyperplane $X_0 = 0$), so that the coordinates of P are given by $X_i/X_0 = x_i = 0$. Then, in a neighborhood of P, Z is defined by

$$\sum_{i=1}^{n} a_i x_i + \sum_{i,j} b_{i,j} x_i \cdot x_j = 0.$$

The condition that a line l_Q through P lie entirely in Z is equivalent to $l_Q \cap Z$ contains three points (counting multiplicity), since Z is of degree 2. Thus l_Q lies entirely in Z if and only if l_Q lies in the tangent plane to Z at P, and l_Q contains another point, say Q, of Z. The tangent plane to Z at P is defined by $\sum a_i X_i = 0$, and we conclude *that the set* $V \cap D_+(X_0)$ *consists of* $Z \cap D_+(X_0) \cap (\sum a_i X_i = 0)$. If we change coordinates so that $\sum a_i x_i = x_1$, then $V|_{D_+(X_0)}$ is the affine quadric cone given by $\sum_{i,j \geqslant 2}^{n} b_{i,j} x_i \cdot x_j = 0$ in affine n-space thus $\pi\colon V \to C \subseteq \mathbb{P}^{n-2} = \mathbb{P}(\mathbb{T}_{Z,P})$, where C is a quadric in $\mathbb{P}^{n-2}$. Indeed, C is then easily shown to be nonsingular from the fact that Z is nonsingular. Thus we obtain the following conclusion from these computations.

Let C be a nonsingular quadric in $\mathbb{P}^{n-2}$, where $\mathbb{P}^{n-2}$ is regarded as a hyperplane of $\mathbb{P}^{n-1}$. Let Y be the blow-up of C in $\mathbb{P}^{n-1}$, and let $\pi'\colon Y \to \mathbb{P}^{n-1}$ be the natural map. Let Y' be obtained from Y by blowing down the closure of $(\pi')^{-1}(\mathbb{P}^{n-2} - C)$ in Y.

LEMMA 4.1. *Let Z be a nonsingular quadric in $\mathbb{P}^n$. Then there is a nonsingular quadric C in $\mathbb{P}^{n-2}$, where $\mathbb{P}^{n-2}$ is regarded as a hyperplane in $\mathbb{P}^{n-1}$ such that Z is isomorphic to the variety Y described above.*

Conversely, suppose we are given a quadric C in $\mathbb{P}^{n-2}$, where $\mathbb{P}^{n-2}$ is regarded as a hyperplane in $\mathbb{P}^{n-1}$. Let $X_0, \ldots, X_{n-1}$ be homogeneous coordinates for $\mathbb{P}^{n-1}$, and assume that the hyperplane $\mathbb{P}^{n-2}$ is described by $X_0 = 0$, and that the quadric C is given by the intersection of $X_0 = 0$ with $G(X_0, \ldots, X_{n-1}) = 0$, where G is a homogeneous form of degree 2.

Consider the space of homogeneous polynomials $\mathcal{M} = \{H \in \bar{K}[X_0, \ldots, X_{n-1}] \mid \deg H = 2$, and $H = 0$ contains the quadric $C\}$. Then it is easy to see that

$\mathscr{M}$ is spanned by the $n+1$ polynomials: G, X_0^2, $X_0 \cdot X_1$,..., $X_0 \cdot X_{n-1}$, which we denote by Y_0, Y_1,..., Y_n, respectively. There is a map ψ: $\mathbb{P}^{n-1} - C \to \mathbb{P}^n$ given by,

$$\psi(\mathfrak{p}) = (Y_0(\mathfrak{p}),..., Y_n(\mathfrak{p})) \qquad \text{for} \quad \mathfrak{p} \in \mathbb{P}^{n-1} - C. \tag{4.1}$$

The map ψ extends to a map

$$\Psi\colon Y \to \mathbb{P}^n, \qquad \text{where } Y \text{ is the blow-up of } \mathbb{P}^{n-1} \text{ along } C. \tag{4.2}$$

It is also clear that the locus of $X_0 = 0$ in Y gets mapped by Ψ to a point, so that Ψ factors through $\Psi'\colon Y' \to \mathbb{P}^n$, where Y' is the blow-down of Y along the locus $X_0 = 0$. Now it is clear that the image of Y' by Ψ' is a hypersurface of degree equal to the number of points of intersection of $G = 0$,

$$X_0 \cdot X_1 = 0,...,X_0 \cdot X_{n-2} = 0$$

lying off of the locus $X_0 = 0$. Thus, the degree of the image of Y' is the number of points of intersection of $G = 0$, $X_1 = 0$,..., $X_{n-2} = 0$, which is 2. Indeed, it is easy to give a degree 2 polynomial in Y_0,..., Y_n which generates the ideal of the image of Y' under Ψ'. Merely notice that some quadratic polynomial in Y_1,..., Y_n is equal to X_0^2 times G (i.e., some quadratic in Y_1,..., Y_n, say $Q(Y_1,..., Y_n)$ is equal to $Y_0 \cdot Y_1$).

We conclude this subsection with comments about the case where we do *not* assume that all our computations are done over an algebraically closed field. *In fact, if we started with a quadric $Z \subseteq \mathbb{P}^n$ with Z defined over a field K (not necessarily algebraically closed), and if we selected a point P satisfying*

$$P \text{ is defined over } K, \tag{4.3}$$

then, the quadric $C \subseteq \mathbb{P}^{n-2}$, where $\mathbb{P}^{n-2}$ is regarded as a hyperplane in $\mathbb{P}^{n-1}$ (as in Lemma 4.1) *can be defined over K.*

Apparently, however, there is no obvious converse to this observation. Suppose we are given the following data:

$$\text{A quadric } C \text{ in } \mathbb{P}^{n-2}, \text{ defined over } K, \tag{4.4}$$

where $\mathbb{P}^{n-2}$ is regarded as a K-subspace of $\mathbb{P}^{n-1}$.

PROBLEM 4. Give a biregular (resp. birational) classification over K of the data in (4.4).

PROBLEM 5. Give a biregular (resp. birational) classification over K of the quadrics in $\mathbb{P}^n$. Recall that for $n = 2$ the usual classification of the quadrics in $\mathbb{P}^2$ defined over K is via the correspondence with a subset of the elements of order 2 of the Brauer group $H^1(K)$.

4.B. *Intersections of Quadrics in $\mathbb{P}^3$ and the Griffiths–Harris Configuration*

In this subsection we assume that $\bar{K}$ is an algebraically closed field of characteristic different from 2 in order that the reader may easily compare our interpretation of the significance of the "canonical" involutions on an intersection of two quadrics in $\mathbb{P}^3$ with [10]. In Section 4.C we consider the arithmetic case and make special note of the relationship of this problem with the theory of 2-descent on an elliptic curve.

With no loss we may assume that $\mathbb{Y} = (Y_0, Y_1, Y_2, Y_3)$ are homogeneous coordinates for $\mathbb{P}^3$, and that we have chosen these coordinates so that, relative to the discussion below, the intersection of two quadrics $\mathscr{S}_1$ and $\mathscr{S}_2$ contains the point (1, 0, 0, 0). When we make this assumption we then also assume that

$$\text{*Linear projection from* } (1, 0, 0, 0) \text{ *maps either of these quadrics to the plane* } Y_0 = 0 \text{ (*with homogeneous coordinates* } (Y_1, Y_2, Y_3)). \tag{4.5}$$

The general form of a quadric through (1, 0, 0, 0) is

$$\sum_{1 \leqslant i \leqslant j \leqslant 3} b_{ij} Y_i \cdot Y_j + l \cdot Y_0 = H(\mathbb{Y}),$$

where l any linear form in Y_0, Y_1, Y_2, Y_3.

OBSERVATION 1. *Let $\mathscr{S}$ be a nonsingular quadric containing* (1, 0, 0, 0). *The linear projection from* (1, 0, 0, 0) *determines two points $P_1(\mathscr{S})$ and $P_2(\mathscr{S})$ in $Y_0 = 0$; the images of the lines of intersection of the tangent plane to $\mathscr{S}$ and $\mathscr{S}$ itself. In addition, the tangent plane to $\mathscr{S}$ at* (1, 0, 0, 0) *has equation $l = 0$.*

Let two quadrics $\mathscr{S}_1$ and $\mathscr{S}_2$ be represented by the quadric polynomials $H_1(\mathbb{Y})$ and $H_2(\mathbb{Y})$, respectively. Then $\{P_1(\mathscr{S}_1), P_2(\mathscr{S}_1)\} = \{P_1(\mathscr{S}_2), P_2(\mathscr{S}_2)\}$ if and only if $H_1(\mathbb{Y}) \equiv \alpha \cdot H_2(\mathbb{Y}) \bmod l$, where $l = 0$ represents the common tangent plane to the two quadrics at (1, 0, 0, 0) *and α is a nonzero constant.*

Argument. The tangent plane to $\mathscr{S}$ is computed by evaluating the partial derivatives of $H(\mathbb{Y})$ with respect to the variables $\mathbb{Y}$ at (1, 0, 0, 0). Since $\partial H(\mathbb{Y})/\partial Y_i \,|_{(1,0,0,0)}$ is equal to the coefficient of Y_i in l for $i = 1, 2, 3$ (see notation above), and $\partial H(\mathbb{Y})/\partial Y_0 \,|_{(1,0,0,0)}$ is equal to $l \,|_{(1,0,0,0)} = 0$, the tangent plane is given by $l = 0$. The remainder of the observation follows from Section 4.A. ∎

The reader should find no difficulty in generalizing Observation 1 to a general quadric.

OBSERVATION 2. *Let $\mathscr{S}$ be a nonsingular quadric in $\mathbb{P}^3$ and let $l = 0$ be the tangent plane to $\mathscr{S}$ at* (1, 0, 0, 0) *and let $P_1(\mathscr{S})$, $P_2(\mathscr{S})$ be the points of projection in the plane $Y_0 = 0$, as in Observation* 1. *Let $l_1(\mathscr{S})$ (resp. $l_2(\mathscr{S})$) be lines in the plane $Y_0 = 0$ such that $P_1(\mathscr{S})$ (resp. $P_2(\mathscr{S})$) is not contained in $l_1(\mathscr{S})$ (resp. $l_2(\mathscr{S})$). Then we can identify $l_i(\mathscr{S})$ with the projectivized tangent plane at $P_i(\mathscr{S})$, $i = 1, 2$*

through projection from $P_i(\mathscr{S})$ onto $l_i(\mathscr{S})$. Then $\mathscr{S}$ is isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$, where we identify $\mathbb{P}^1 \times \mathbb{P}^1$ with $l_1(\mathscr{S}) \times l_2(\mathscr{S})$.

Proof. Let π be the plane $Y_0 = 0$, and let $P \in \pi - P_1(\mathscr{S}) - P_2(\mathscr{S}) - l'$, where l' represents the points of the line, excluding P_1 and P_2, joining P_1 and P_2. Then P determines two lines, $L_1(P)$ and $L_2(P)$ from $P_1(\mathscr{S})$ and $P_2(\mathscr{S})$ to P. We define:

$$\varphi: \pi - P_1(\mathscr{S}) - P_2(\mathscr{S}) - l' \to l_1(\mathscr{S}) \times l_2(\mathscr{S}) \tag{4.6}$$

by

$$\varphi(P) = (L_1(P) \cap l_1(\mathscr{S})) \times (L_2(P) \cap l_2(\mathscr{S})).$$

The natural extension of φ to $\pi - P_1(\mathscr{S}) - P_2(\mathscr{S})$ maps all the points of l' to the point $(l \cap l_1(\mathscr{S})) \times (l \cap l_2(\mathscr{S}))$. Then the blowup of π at $P_1(\mathscr{S})$ (resp. $P_2(\mathscr{S})$) gets mapped to the points of $l_1(\mathscr{S}) \times (l \cap l_2(\mathscr{S}))$ (resp. the points of $(l \cap l_1(\mathscr{S})) \times l_2(\mathscr{S})$). ∎

There is a natural embedding, the Segre embedding, $\Phi_{\text{Seg}}: \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3$. To describe this, let W_0, W_1 (resp. Z_0, Z_1) be homogeneous coordinates for two copies of $\mathbb{P}^1$, and let $Y_0 = W_0 \cdot Z_0$, $Y_1 = W_0 \cdot Z_1$, $Y_2 = W_1 \cdot Z_0$, and $Y_3 = W_1 \cdot Z_1$. Then Φ_{Seg} maps $\mathbb{P}^1 \times \mathbb{P}^1$ isomorphically to the quadric $Y_0 \cdot Y_3 - Y_1 \cdot Y_2 = 0$.

OBSERVATION 3. *By a projective linear change of coordinates each nonsingular quadric is the image of the Segre embedding of $\mathbb{P}^1 \times \mathbb{P}^1$. Let $\mathscr{C}$ be a curve on $\mathbb{P}^1 \times \mathbb{P}^1$ with bidegree (d_1, d_2)* (i.e., $\text{pr}_i: \mathscr{C} \to \mathbb{P}^1$, *projection on the ith copy of $\mathbb{P}^1$, is of degree d_i, $i = 1, 2$). Then $\mathscr{C}$ is the zero set of a polynomial, homogeneous and of degree d_1 in (W_0, W_1) and homogeneous and of degree d_2 in (Z_0, Z_1). Since the restriction of a hyperplane meets a nonsingular quadric $\mathscr{S}$ in a curve of bidegree* (1, 1), *the transversal intersection* (i.e., *nonsingular intersection*) *of two nonsingular quadrics is a curve of bidegree* (2, 2) *on both quadrics. In addition this transversal intersection is an elliptic curve.*

Argument. Let the nonsingular quadric $\mathscr{S}$ be described by the equation $H(\mathbb{Y}) = 0$. By projective linear change of coordinates we may assume that $H(\mathbb{Y}) = \sum_{i=0}^{3} Y_i^2$. Let $Y_0' = Y_0 + (-1)^{1/2} Y_1$, $Y_1' = Y_0 - (-1)^{1/2} Y_1$, etc. Then it is clear that $\mathscr{S}$ can be described as the zero set of $Y_0' \cdot Y_1' + Y_2' \cdot Y_3' = 0$. From here a very simple change of coordinates gives $\mathscr{S}$ as the image of $\mathbb{P}^1 \times \mathbb{P}^1$ under the Segre embedding. Since the Segre embedding can now be seen to correspond to the same linear system as given by the description of a quadric as obtained from the blowup of $\mathbb{P}^2$ at two points, the remainder of Observation 3, excluding the last sentence, follows easily.

In order to conclude that the transversal intersection of two nonsingular quadrics is an elliptic curve we use a deformation argument, as such an argument is compatible with our later discussion of 2-descent.

Let $\mathscr{P}$ be the pairs of quadrics (not necessarily nonsingular) in $\mathbb{P}^3$, and let $\mathscr{P}^{(0)}$ be the open subset consisting of the pairs of quadrics which intersect in a one-dimensional set. We have a total space $\mathscr{E}$ and a natural morphism

$$\mathscr{E} \xrightarrow{\Psi} \mathscr{P}^{(0)}, \tag{4.7}$$

where, if $p \in \mathscr{P}^{(0)}$ corresponds to the pair of quadrics $\mathscr{S}_1$, $\mathscr{S}_2$ then the fiber $\mathscr{E}_p$ is isomorphic to $\mathscr{S}_1 \cap \mathscr{S}_2$. We note first that Ψ is a *flat morphism* (see [12, Chap. 3]) since the fibers of Ψ are a continuously varying family of complete intersections. We leave the proof of this to the reader. From [12, Chap. 2, p. 83] the Euler characteristic of the structure sheaves of the geometric fibers of (4.7) is constant. The Euler characteristic of a nonsingular curve is 0 if and only if the curve is an elliptic curve. Therefore, in order to conclude Observation 3 we have only to compute the arithmetic genus of some special fiber of (4.7). We compute the arithmetic genus of the fiber $\mathscr{S}_1 \cap \mathscr{S}_2$, where $\mathscr{S}_1$ is the zero set of the equation $(\alpha Y_0 - Y_1) \cdot (\beta Y_0 - Y_2) = 0$ and $\mathscr{D}_2$ is the zero set of the equation $(\gamma Y_0 - Y_3) \cdot Y_0 = 0$ and α, β, γ are nonzero distinct elements of $\bar{K}$. Then $\mathscr{S}_1 \cap \mathscr{S}_2$ consists of 4 lines which we list as:

$$\begin{aligned}
&\text{(a)} \quad (\alpha Y_0 - Y_1 = 0) \cap (Y_0 = 0);\\
&\text{(b)} \quad (\beta Y_0 - Y_2 = 0) \cap (Y_0 = 0);\\
&\text{(c)} \quad (\alpha Y_0 - Y_1 = 0) \cap (\gamma Y_0 - Y_3 = 0), \text{ and;}\\
&\text{(d)} \quad (\beta Y_0 - Y_2 = 0) \cap (\gamma Y_0 - Y_3 = 0).
\end{aligned} \tag{4.8}$$

Thus the intersection of $\mathscr{S}_1$ and $\mathscr{S}_2$ consists of four lines meeting at four points, the four points defined by any three of the hyperplanes. We label these lines as l_1, l_2, l_3, l_4 where l_i and l_{i+1} meet at p_i, $i = 1, 2, 3, 4$ and we make the usual convention of regarding the subscripts as reduced modulo 4. The Euler characteristic $\chi(\mathscr{O}_{\mathscr{S}_1 \cap \mathscr{S}_2})$ is given by

$$\dim(H^0(\mathscr{O}_{\mathscr{S}_1 \cap \mathscr{S}_2})) - \dim(H^1(\mathscr{O}_{\mathscr{S}_1 \cap \mathscr{S}_2})), \tag{4.9}$$

where $\mathscr{O}_{\mathscr{S}_1 \cap \mathscr{S}_2}$ is the structure sheaf of $\mathscr{S}_1 \cap \mathscr{S}_2$ and $H^i(\mathscr{O}_{\mathscr{S}_1 \cap \mathscr{S}_2})$ is the ith Čech cohomology group of this sheaf. From Serre duality $H^1(\mathscr{O}_{\mathscr{S}_1 \cap \mathscr{S}_2})$ is isomorphic to $H^0(\kappa_{\mathscr{S}_1 \cap \mathscr{S}_2})$, where $\kappa_{\mathscr{S}_1 \cap \mathscr{S}_2}$ is the sheaf of differentials with poles of order at most one at the points p_i, $i = 1, 2, 3, 4$ and whose sum of residues is 0. Thus the Euler characteristic $\chi(\mathscr{O}_{\mathscr{S}_1 \cap \mathscr{S}_2})$ is easily computed to be 0. ∎

Griffiths and Harris [10] describe four involutions on an elliptic curve $\mathscr{E}$ presented as an intersection of two nonsingular quadrics $\mathscr{S}_1$ and $\mathscr{S}_2$ in $\mathbb{P}^3$. Their description is geometric. *We show that these involutions arise from the various degree 2 projection morphisms of $\mathscr{E}$ coming from the isomorphisms of $\mathscr{S}_i$ with* $\mathbb{P}^1 \times \mathbb{P}^1$, $i = 1, 2$ (i.e., Observation 4).

To fix the ideas, consider $\mathrm{pr}_{11}\colon \mathscr{S}_1 \to \mathbb{P}^1$ by projecting $\mathscr{S}_1$ onto the first factor in the isomorphism $\mathscr{S}_1 \simeq \mathbb{P}^1 \times \mathbb{P}^1$. Let $\mathrm{pr}_{12}\colon \mathscr{S}_1 \to \mathbb{P}^1$ be projection on the second factor.

Before giving Observation 4 we make a few relevant remarks about dual varieties. The points of projective n-space are noncanonically in one–one correspondence with the hyperplanes of projective n-space, which we denote by $(\mathbb{P}^n)^*$. Let V be a nonsingular quadric of $\mathbb{P}^n$. To $\mathfrak{p} \in V$ we associate, $T_{\mathfrak{p}} \in (\mathbb{P}^n)^*$, the tangent plane to V at $\mathfrak{p}$. We let the image of V be denoted by V^*. If V is represented by the polynomial equation $f(\mathbf{Y}) = 0$, then the point $T_{\mathfrak{p}} \in (\mathbb{P}^n)^*$ is represented by the coordinates $(\partial f/\partial Y_0 \mid_{\mathfrak{p}}, \ldots, \partial f/\partial Y_n \mid_{\mathfrak{p}}) \in \mathbb{P}^n$, so that there is a map, which we denote by a * superscript from V to V^*.

Now apply the concepts above to $\mathscr{S}_1$ and $\mathscr{S}_2$, so that the intersection of $\mathscr{S}_1^*$ and $\mathscr{S}_2^*$ consists of the bitangents to $\mathscr{S}_1$ and $\mathscr{S}_2$, and $\mathscr{S}_1^* \cap \mathscr{S}_2^*$ is the dual $\mathscr{E}^*$ to the elliptic curve $\mathscr{E}$.

OBSERVATION 4. *Given a line l not contained in $\mathscr{S}_2$, there are two tangents to $\mathscr{S}_2$ through l.*

Let $\eta \in \mathscr{E}$ so that $\mathrm{pr}_{12}^{-1}(\mathrm{pr}_{11}(\eta)) = l_A$ and $\mathrm{pr}_{11}^{-1}(\mathrm{pr}_{12}(\eta)) = l_B$ are lines on $\mathscr{S}_1$. Then, if $\eta^* \in \mathscr{E}^*$ corresponds to η we have $\eta^* \cap \mathscr{S}_1 = l_A \cup l_B$. We obtain an involution, denoted τ_A, given by:

$$\tau_A(\eta) = \eta', \tag{4.10}$$

where $(\eta')^*$ and η^* are the two bitangents to $\mathscr{S}_1$ and $\mathscr{S}_2$ through l_A. In addition, τ_A is the involution of $\mathscr{E}$ corresponding to pr_{11}.

Proof. Consider the line l not contained in $\mathscr{S}_2$. The statement that "there are two planes through l tangent to $\mathscr{S}_2$" is the dual to the statement "there are two points of intersection of a line l with a quadric not containing l". If π is a plane containing l, where l lies on $\mathscr{S}_1$, and π is tangent to $\mathscr{S}_2$ then π is also tangent to $\mathscr{S}_1$ since the intersection of π and $\mathscr{S}_1$ consists of two lines.

Now consider the lines l_A and l_B corresponding to $\eta \in \mathscr{E}$. Then $l_A \cap l_B = \eta$, and the tangent to $\mathscr{S}_1$ at η meets $\mathscr{S}_1$ in $l_A \cup l_B$ from Observation 3. This is equivalent to the statement $\eta^* \cap \mathscr{S}_1 = l_A \cup l_B$.

Let $\bar{\eta}$ be a generic point of $\mathscr{E}$. In order to show that τ_A is the involution of $\mathscr{E}$ corresponding to pr_{11} we have only to show that the involution induced by τ_A on the function field $\bar{K}(\eta)$ (i.e., $\bar{K}$ with the coordinates of $\bar{\eta}$ adjoined) leaves the subfield $\bar{K}(\mathrm{pr}_{11}(\bar{\eta}))$ fixed. That is, we must show that $\mathrm{pr}_{11}(\bar{\eta})$ and $\mathrm{pr}_{11}(\tau_A(\bar{\eta}))$ are the same. However we recover $\mathrm{pr}_{11}(\tau_A(\bar{\eta}))$ by knowing the lines of intersection of $(\tau_A(\bar{\eta}))^*$ with $\mathscr{S}_1$, and we know that l_A is one of these lines of intersection by the definition of τ_A. Therefore the result follows, and we conclude the observation. ∎

Lastly, we consider the main problem suggested by Observation 4. Let $\mathscr{E}$, as above, be the elliptic curve obtained as a transversal intersection of two non-

singular quadrics $\mathscr{S}_1$ and $\mathscr{S}_2$. From $\mathscr{S}_1$ (resp. $\mathscr{S}_2$) we obtain two involutions $\tau_{A,1}$ and $\tau_{B,1}$ (resp. $\tau_{A,2}$ and $\tau_{B,2}$), and we want to know the nature of the groups.

(a) $G(\mathscr{E}, \mathscr{S}_1) = \{$group of automorphisms of $\mathscr{E}$ generated by $\tau_{A,1}$ and $\tau_{B,1}\}$;

(b) $G(\mathscr{E}, \mathscr{S}_2) = \{$group generated by $\tau_{A,2}$ and $\tau_{B,2}\}$, and; (4.11)

(c) $G(\mathscr{E}, \mathscr{S}_1, \mathscr{S}_2) = \{$group generated by $\tau_{A,1}, \tau_{B,1}, \tau_{A,2}$, and $\tau_{B,2}\}$.

In the case that $\mathscr{S}_1$ and $\mathscr{S}_2$ are real quadrics with $\mathbb{R}$-rational points, Griffiths and Harris [10] show how to associate a polygonal figure inscribed between the real points if and only if the group of (4.11c) is a finite group. *In order to make clear the nature of the groups obtained we assume that $\mathscr{E}$ is fixed, and we vary the quadrics $\mathscr{S}_1$ and $\mathscr{S}_2$ whose intersections give $\mathscr{E}$.*

Let the original quadrics $\mathscr{S}_1$ and $\mathscr{S}_2$ be represented by the equations $H_1(\mathbf{Y}) = 0$ and $H_2(\mathbf{Y}) = 0$, respectively, in $\mathbb{P}^3$. Then the quadrics containing $\mathscr{E}$ are represented by the pencil

$$t_1(H_1(\mathbf{Y})) + t_2(H_2(\mathbf{Y})) = 0, \tag{4.12}$$

where (t_1, t_2) represents homogeneous coordinates for a copy of $\mathbb{P}^1$.

Thus, for $\alpha = (t_1, t_2) = \mathbb{P}^1$, we obtain a pair of involutions $\tau_{A,\alpha}$ and $\tau_{B,\alpha}$ from the observations above. From Section 2, $\tau_{A,\alpha}$ (resp. $\tau_{B,\alpha}$) is given by conjugation of the canonical involution of $\mathscr{E}$ by translation by a point $\mathfrak{p}(A, \alpha)$ (resp. $\mathfrak{p}(B, \alpha)$) of $\mathscr{E}$. Therefore, in a natural way $\tau_{A,\alpha}$ (resp. $\tau_{B,\alpha}$) corresponds (uniquely) to the image in $\mathscr{E}/\mathscr{E}_2$ of $\mathfrak{p}(A, \alpha)$ (resp. $\mathfrak{p}(B, \alpha)$), where $\mathscr{E}_2$ consists of the points of order 2 on $\mathscr{E}$. Although $\mathscr{E}/\mathscr{E}_2$ is isomorphic to $\mathscr{E}$, in our later discussion of 2-descent, it can be important to distinguish between $\mathscr{E}$ and $\mathscr{E}/\mathscr{E}_2$.

At this point the reader might benefit from part of the discussion in [20, pp. 57–58]. To the pencil (4.12) we associate an elliptic curve $\mathscr{C}$ represented as a double cover of $\mathbb{P}^1$ (the same copy of $\mathbb{P}^1$ that appears in (4.12)). Indeed, let $\mathscr{Q}$ be the space of all quadrics (including singular quadrics) in $\mathbb{P}^3$. Then $\mathscr{Q}$ is isomorphic to $\mathbb{P}^{10}$ and the singular quadrics Δ form a hypersurface of degree 4 (i.e., the locus of Δ is described by the condition that the determinant of the symmetric matrix associated to a quadratic form is zero). The pencil of (4.12) meets Δ in four points, and $\mathscr{C}$ is the double cover of $\mathbb{P}^1$ branched at these four points. Conversely, if $\mathscr{C}$ is a double cover of $\mathbb{P}^1$ branched at four points, say $\lambda_1, \lambda_2, \lambda_3$, and λ_4, then the pencil generated by the pair of quadrics $H_1' = \sum_{i=0}^{3} Y_i^2$ and $H_2' = \sum_{i=0}^{3} - \lambda_i Y_i^2$ "results" in the double cover of $\mathbb{P}^1$ given by $\mathscr{C}$. In this way [20] explains (roughly) that the moduli space of intersections of quadrics in $\mathbb{P}^3$ (resp. $\mathbb{P}^{n+2}$) is the same as the moduli space of elliptic curves (resp. hyperelliptic curves of genus $\frac{1}{2} \cdot (n+1)$, for n odd). *What most interests us is the precise relation between the elliptic curve $\mathscr{E}$ common to the members of the pencil* (4.12) *and the elliptic curve $\mathscr{C}$.*

THEOREM 4. *The curve $\mathscr{C}$ is isomorphic to $\mathscr{E}/\mathscr{E}_2$ by a map that associates to the pair of points of $\mathscr{C}$ over $\alpha = (t_1, t_2) \in \mathbb{P}^1$ the points that are the images of $\mathfrak{p}(A, \alpha)$ and $\mathfrak{p}(B, \alpha)$ in $\mathscr{E}/\mathscr{E}_2$.*

Let $\alpha, \alpha' \in \mathbb{P}^1$. In the notation above we obtain the relation (between involutions on $\mathscr{E}$) $\tau_{A,\alpha} \circ \tau_{A,\alpha'} \circ \tau_{B,\alpha} \circ \tau_{B,\alpha'}$ is equal to the identity. Also, we may pick α and α' so that $\tau_{A,\alpha} \circ \tau_{B,\alpha}$ and $\tau_{A,\alpha'} \circ \tau_{B,\alpha'}$ have whatever pair of finite orders we may desire, thus generalizing the results of [10] *attributed to Steinberg.*

Proof. We start by considering the argument of [20, p. 58]. Let T be the variety of lines in $\mathbb{P}^3$ that are contained in one of the quadrics of the pencil (4.12), and let $\mathrm{Alb}(T)$ be the Albanese variety of T. We have a natural map $\psi\colon T \to \mathbb{P}^1$ since each line lying on one of the quadrics lies on *just* one of the quadrics. In addition, if $\alpha \in \mathbb{P}^1$ corresponds to a nonsingular quadric then $\psi^{-1}(\alpha) = \mathbb{P}^1 \cup \mathbb{P}^1$, and if α corresponds to a singular quadric then $\psi^{-1}(\alpha)$ is $\mathbb{P}^2$. Thus, from the basic properties of $\mathrm{Alb}(T)$, $\mathrm{Alb}(T)$ is a double cover of $\mathbb{P}^1$ branched over exactly the points of $\mathbb{P}^1$ corresponding to singular quadrics in the pencil (4.12) (i.e., $\mathrm{Alb}(T) \simeq \mathscr{C}$). On the other hand, from our previous observations, for $\alpha \in \mathbb{P}^1$ corresponding to a nonsingular quadric, each of the copies of $\mathbb{P}^1$ in $\psi^{-1}(\alpha)$ corresponds to an involution of $\mathscr{E}$, and thereby to a point of $\mathscr{E}/\mathscr{E}_2$. This establishes the first part of the theorem.

The identity $\tau_{A,\alpha} \circ \tau_{A,\alpha'} \circ \tau_{B,\alpha} \circ \tau_{B,\alpha'} = \mathrm{Id}$. is equivalent to: The addition of the images of $\mathfrak{p}(A, \alpha) + \mathfrak{p}(B, \alpha)$ in $\mathscr{E}/\mathscr{E}_2$ is independent of $\alpha \in \mathbb{P}^1$. However, we may assume (with no loss) that the isomorphism of $\mathscr{E}/\mathscr{E}_2$ with $\mathscr{C}$ takes the origin to the origin, and that the double cover of $\mathbb{P}^1$ given by $\mathscr{C}$ is in Weierstrass normal form, so that the images of $\mathfrak{p}(A, \alpha)$ and $\mathfrak{p}(B, \alpha)$ in $\mathscr{E}/\mathscr{E}_2$ are *inverse* to each other. Thus the identity follows. In order to conclude the theorem we have only to show that $\tau_{A,\alpha} \circ \tau_{B,\alpha}$ can have arbitrary order. However $\tau_{A,\alpha} \circ \tau_{B,\alpha}$ corresponds to the image of $\mathfrak{p}(A, \alpha) - \mathfrak{p}(B, \alpha)$ in $\mathscr{E}/\mathscr{E}_2$. Since this is arbitrary, and therefore can have arbitrary order, we conclude the theorem. ∎

4.C. *Comments On The Arithmetic Case and Higher-Dimensional Quadrics*

This subsection consists entirely of short comments on Section 4.B. We start with a review of 2-descent (as in [3, p. 269–272]). Let K be a (not necessarily algebraically closed) field. Let $(\mathscr{C}, \mathfrak{p}_0)$ be an elliptic curve defined over K (i.e., $\mathfrak{p}_0$ is the origin for a multiplication structure on $\mathscr{C}$). By an m-covering (where m is a positive integer) we mean a commutative diagram

$$\begin{array}{ccc} \mathscr{C} & \xrightarrow{\text{mult by } m} & \mathscr{C}, \\ {\scriptstyle\theta}\downarrow & \nearrow_{M} & \\ \mathscr{D} & & \end{array} \tag{4.13}$$

where $\mathscr{D}$ is a curve defined over K; θ is an isomorphism defined over $\bar{K}$ and; the morphism M is defined over K.

The case when $K = \mathbb{Q}$, $m = 2$ is of special interest and has been used (endlessly!) to help decide the nature of the $\mathbb{Q}$-rational points on $\mathscr{C}$. Indeed this classical case usually starts by assuming that $\mathscr{C}$ is in Weierstrass normal form: $Y^2 = \prod_1^3 (X - e_i)$ with $e_i \in \mathbb{Z}$. The idea of the Diophantine analysis is to let (x, y) be a $\mathbb{Q}$-rational point, change variables to $x = r/t^2, y = s/t^3, (r, t) = 1$, and $r, s, t \in \mathbb{Z}$ to obtain the equation $s^2 = \prod_1^3 (r - e_i t)$. Excluding the case $s = 0$, the only common factor of $(r - e_1 t^2)$ and $(r - e_2 t^2)$ divides $e_1 - e_2$, so $r - e_j t^2 = d_j v_j^2$, where d_1, d_2, d_3 are squarefree and include only a finite number of possibilities. Corresponding to any one such triplet d_1, d_2, d_3, upon eliminating r we obtain a pair of (singular) quadrics

$$(e_2 - e_1)t^2 = d_1 v_1^2 - d_2 v_2^2 \tag{4.14}$$

and

$$(e_3 - e_1)t^2 = d_1 v_1^2 - d_3 v_3^2$$

in $\mathbb{P}^3$ with homogeneous coordinates given by (t, v_1, v_2, v_3). The intersection of the quadrics of (4.14) give the possible $\mathscr{D}$'s, and the map M is given by $(t, v_1, v_2, v_3) \to (r/t^2, s/t^3)$ where $r = e_j t^2 + d_j v_j^2$ and $s = (d_1 d_2 d_3)^{1/2} v_1 v_2 v_3$.

If we return to the discussion preceeding Theorem 4 we notice that these are definitely not the same pair of quadrics that occurred in the discussion of [20] despite the fact that the argument was clearly also related to 2-decent. Indeed, of course, when we take the pencil of quadrics corresponding to Eqs. (4.14) we do not recover $\mathscr{C}$ as the double cover of $\mathbb{P}^1$ branched at four points. That is to say, arithmetic versions of Theorem 4 could well touch on very deep considerations. Part of these considerations has to do with a nice description of the coordinates over which a pencil of quadrics in $\mathbb{P}^3$ trivializes to a pencil of varieties isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$.

Also, in higher dimensions, as outlined in Observations 1 and 2, pencils of quadrics trivialize to varieties in a more standard form (the form given by Section 4A) if the "right coordinates are used".

PROBLEM 6. *Use the Albanese argument of Theorem 4 to find coordinates over which a pencil of quadrics in $\mathbb{P}^n$ trivializes to the "standard form" of Section 4.A, by incorporating the structure of the Jacobian of the corresponding hyperelliptic curve.*

REFERENCES

1. M. F. ATIYAH, Complex fibre bundles and ruled surfaces, *Proc. London Math. Soc.* (3) 5 (1955), 407–434; Vector bundles over an elliptic curve, *Proc. London Math. Soc.* (3) (1957), 414–452.

2. A. J. Berkson and A. McConnell, "Using Categorical Constructions in the Category of Compact Riemann Surfaces," preprint.
3. J. W. S. Cassels, Diophantine equations with special reference to elliptic curves, *J. London Math. Soc.*, **41** (1966), 193–291.
4. L. R. Ford, "Automorphic Functions," Chelsea, New York, 1951.
5. M. Fried, On a theorem of Ritt and related Diophantine problems, *Crelles J.* **264** (1973), 40–55.
6. M. Fried, "Brauer Groups and Jacobians," preprint.
7. M. Fried, The field of definition of function fields and a problem in the reducibility of polynomials in two variables, *Illinois J. Math.* **17** (1973), 128–146.
8. M. Fried and R. E. MacRae, On the invariance of chains of fields, *Illinois J. Math.* **13** (1969), 165–171.
9. M. Fried and R. E. MacRae, On curves with separated variables, *Math. Ann.* **182** (1969), 220–226.
10. P. Griffiths and J. Harris, "A Poncelet Theorem in Space," preprint.
11. N. Jacobson, The theory of fields and Galois theory, *in* "Lectures in Abstract Algebra," Nostrand (1964).
12. R. MacRae, "Conic Subfields of Genus 1 Curves," preprint.
13. R. MacRae and P. Samuel, Subfields of index 2 of elliptic fields (Conference in Comm. Algebra, Lawrence Kansas, 1972), Lecture Notes in Mathematics No. 311, Springer-Verlag, Berlin/New York.
14. D. Mumford, "Introduction to Algebraic Geometry," Harvard Notes, 1968.
15. D. Mumford, Lectures on curves on an algebraic surface, *Ann. Math. Stud.* **59** (1965).
16. J. F. Ritt, Permutable rational functions, *Trans. Amer. Math. Soc.* **25** (1923), 399–448.
17. M. Reid, "The Complete Intersection of Two or More Quadrics," Ph.D. dissertation, Cambridge Univ., 1972.
18. G. Shimura and Y. Taniyama, Complex multiplication of Abelian varieties and its application to number theory, *J. Math. Soc. Japan*, 1961.
19. H. P. F. Swinnerton-Dyer, Applications of algebraic geometry to number theory (No. Theory Institute, 1969, Proc. Sympos, Pure Math.), Vol. 20, pp. 1–52, State Univ. New York, Stony Brook, Amer. Math. Soc., Providence, R.I., 1971.
20. A. N. Tyurin, On intersections of quadrics, *Russian Math. Surveys* **30** (1975), 51–105; *Uspekhi Mat. Nauk.* **30** (1975), 51–99.

Printed by the St Catherine Press Ltd., Tempelhof 37, Bruges, Belgium