TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 211, 1975

ON THE TWO SHEETED COVERINGS OF CONICS BY ELLIPTIC CURVES

BY

R. E. MACRAE

ABSTRACT. Let K be the field of algebraic functions on an elliptic curve that can be described by an equation of the form $y^2 = f(x)$ where $f(x)$ is a quartic polynomial over a field k. Moreover, assume that the Riemann surface for K contains no points rational over k. When k is the field of real numbers it is well known that K may also be expressed as a quadratic extension of a function field $L = k(u, v)$ of algebraic functions on a conic whose Riemann surface also contains no points rational over k. We extend this result to p-adic ground fields k. Moreover, we describe the various subfields of index two and genus zero (conic subfields) in terms of the k-rational points on the Jacobian of K. This is done for arbitrary ground fields. In particular, the embedding of the projective class group of K (over k) is seen to describe exactly those conic subfields that possess k-rational points.

1. **Introduction.** Function fields of genus one are very often given as quadratic extensions of function fields of genus zero. Geometrically this situation is that described in the title. In order for this to obtain it suffices that the elliptic curve (over k) have a k-rational or quadratic point. We consider, therefore, the following situation: (1) a field k and a fixed quadratic extension k_1 are given, (2) a function field K_1 in one variable of genus one over k with a k_1-rational point but no k-rational point is given. We wish to describe the various subfields of index 2 and genus 0 in K_1 (conic subfields). We prove the following facts (among others): (1) There is an explicit one-to-one correspondence between the k-rational points, J_k, in the Jacobian variety and the conic subfields of K_1. (2) If $j(\bar{D}_0^{K_1/k})$ is the usual embedding of the class group of divisors of degree zero on K_1 into J_k, then a conic subfield corresponds to a point in $j(\bar{D}_0^{K_1/k})$ iff that conic subfield has a k-rational point. (3) If NJ_{k_1} is the subgroup of norms of k_1-rational points on the Jacobian, then a conic subfield corresponds to a point in NJ_{k_1} iff the conic subfield has a k-rational point that lies under a quadratic point with coordinates in k_1. (4) $NJ_{k_1} \leq j(\bar{D}_0^{K_1/k})$ and (5) if k is a p-adic field then K_1 contains a conic subfield without k-rational points. A variety of

Received by the editors April 1, 1974.
AMS (MOS) subject classifications (1970). Primary 14H05; Secondary 12B99.
Copyright © 1975, American Mathematical Society

other information is derived—particularly in the case that k is p-adic (see §4). Moreover, it is shown, using the techniques developed, that the Jacobian of the so-called Reichardt equation $y^2 = 2(x^4 - 17)$ is given by $y^2 = x(x^2 + 17)$ over Q.

Several comments and a caution of a technical nature should be made at this point. A cursory reading of the succeeding sections of this paper may suggest that we are playing formal games with the standard cohomology of groups. This is, however, not the case as in analysis of the statements and scope of Theorem 3.7 and Theorem 4.6 will readily show. The technical caution concerns the perverse habit of the author to take his group action on the right and to compute his cocycles consistent with this convention. This makes the form of the equation for a 1-cocycle somewhat different from the standard one. However, the reader should have no difficulty in understanding the proofs.

The author wishes to express his gratitude to various persons and agencies that provided both intellectual and financial support during the period of time that this paper was written. In part this was the National Science Foundation and the University of Paris at Orsay for research grants. The University of Colorado provided me with a Faculty Fellowship during the academic year 1972–1973 that permitted me time to engage in research activities at the University of Paris. Finally I am greatly appreciative of many helpful conversations with P. Samuel and G. Poitou.

2. **Preliminaries.** We begin with a brief review of some known results simply in order to establish a convenient notation. Details may be found in [1]. We let k be a completely arbitrary field and let K be an elliptic function field over k. By this we mean that K is a finitely, separably generated extension of k such that k is algebraically closed in K and genus $(k_1 \otimes_k K/k_1) = 1$ for all algebraic extensions k_1 of k. Now let k_1 be a Galois extension of k and set $L = k_1 \otimes_k K$. The following short exact sequence of Galois groups is easy to verify:

$$1 \longrightarrow \mathrm{Aut}(L/k_1) \longrightarrow \mathrm{Aut}(L/k) \longrightarrow \mathrm{Aut}(k_1/k) \longrightarrow 1. \tag{2.1}$$

In the language of group extensions this is a split extension since $\mathrm{Aut}(L/K)$ is a complete set of coset representatives that forms a group. By pairing each such group of representatives with the subfield it leaves pointwise fixed we establish a one-to-one correspondence between the various groups of representatives and the subfields K_1 of L that contain k, are linearly disjoint from k_1 and such that $k_1K_1 = L$.

Now let us assume further that L has a k_1-rational point. We arbitrarily

distinguish such a point and call it $\mathfrak{P}_\infty$. In the usual way, the set J_{k_1} of k_1-rational points of L has the structure of an abelian group with $\mathfrak{P}_\infty$ as the neutral element. Indeed one sets up a correspondence between J_{k_1} and the group $\bar{D}_0^{L/k_1}$ of divisor classes of degree zero. We now let $F(\mathfrak{P}_\infty)$ consist of all automorphisms in $\mathrm{Aut}(L/k_1)$ that leave $\mathfrak{P}_\infty$ fixed and $T(L/k_1)$ denote the subgroup of $\mathrm{Aut}(L/k_1)$ consisting of translations. Now $T(L/k_1)$ is isomorphic to J_{k_1} and is a normal subgroup of $\mathrm{Aut}(L/k_1)$. Moreover $\mathrm{Aut}(L/k_1)$ is the subdirect product of $T(L/k_1)$ and $F(\mathfrak{P}_\infty)$ or, equivalently, the short exact sequence

$$1 \longrightarrow T(L/k_1) \longrightarrow \mathrm{Aut}(L/k_1) \longrightarrow \mathrm{Aut}(L/k_1)/T(L/k_1) \longrightarrow 1$$

is split and $F(\mathfrak{P}_\infty)$ is a group of representatives. All details may be found in [2, Chapter IV, §2].

Now let $\mathfrak{G}_1 = \{A_\sigma \mid \sigma \in \mathrm{Aut}(k_1/k)\}$ and $\mathfrak{G}_2 = \{B_\sigma \mid \sigma \in \mathrm{Aut}(k_1/k)\}$ be two groups of representatives with respect to the sequence (2.1). We assume that $A_\sigma \to \sigma$ and $B_\sigma \to \sigma$. It is always the case that $A_\sigma^{-1}B_\sigma \in \mathrm{Aut}(L/k_1)$ for all $\sigma \in \mathrm{Aut}(k_1/k)$.

Definition 2.2. $\mathfrak{G}_1$ and $\mathfrak{G}_2$ are said to be *translation equivalent* if $A_\sigma^{-1}B_\sigma$ is in $T(L/k_1)$ for all σ.

It is not difficult to see that this is in fact an equivalence relation. The following lemma follows immediately from various definitions while its corollary requires the remark that an automorphism is determined uniquely by its effect on prime divisors.

Lemma 2.3. *Let* $\mathfrak{P}_1, \mathfrak{P}_2$ *be in* J_{k_1} *and* A *be in* $\mathrm{Aut}(L/k)$. *Then* (i) $(\mathfrak{P}_1 + \mathfrak{P}_2)^A = \mathfrak{P}_1^A + \mathfrak{P}_2^A - \mathfrak{P}_\infty^A$ *and* (ii) $(-\mathfrak{P}_1)^A = -\mathfrak{P}_1^A + 2\mathfrak{P}_\infty^A$.

Corollary 2.4. *Let* $T_{\mathfrak{P}}$ *be the translation by the point* $\mathfrak{P}$ *of* J_{k_1}. *Then* $A^{-1}T_{\mathfrak{P}}A = T_{(\mathfrak{P}^A - \mathfrak{P}_\infty^A)}$ *for every* A *in* $\mathrm{Aut}(L/k)$.

We will customarily write $T_{\mathfrak{P}}^A = A^{-1}T_{\mathfrak{P}}A$.

The following result is fundamental to the entire theory.

Theorem 2.5 (Chatalet). *In each equivalence class of translation equivalent groups of representatives of* (2.1) *there is precisely one all of whose elements fix* $\mathfrak{P}_\infty$.

Proof. To show uniqueness we let $\mathfrak{G}_1 = \{A_\sigma, \dots\}$ and $\mathfrak{G}_2 = \{B_\sigma, \dots\}$ be two groups satisfying the conclusion of the theorem. Then $A_\sigma^{-1}B_\sigma = T_{\mathfrak{P}_\sigma}$ by hypothesis and $\mathfrak{P}_\infty = \mathfrak{P}_\infty^{A_\sigma^{-1}B_\sigma} = \mathfrak{P}_\infty + \mathfrak{P}_\sigma = \mathfrak{P}_\sigma$ for all σ again by hypothesis.

Thus $A_\sigma = B_\sigma$ for all σ. To show existence we let $\mathfrak{G}_1 = \{A_\sigma, \dots\}$ be any member of a translation equivalent class. Let $B_\sigma = A_\sigma T_{-\mathfrak{P}_\infty^{A_\sigma}}$. Since $\mathfrak{P}_\infty^{B_\sigma} = \mathfrak{P}_\infty$ for all σ, it suffices to show that $\mathfrak{G}_2 = \{B_\sigma, \dots\}$ is in fact a group. But by Corollaries 2.3 and 2.4 we see that

$$B_\sigma B_\tau = A_\sigma T_{-\mathfrak{P}_\infty^{A_\sigma}} A_\tau T_{-\mathfrak{P}_\infty^{A_\tau}} = A_\sigma A_\tau T^{A_\tau}_{-\mathfrak{P}_\infty^{A_\sigma}} T_{-\mathfrak{P}_\infty^{A_\tau}}$$

$$= A_{\sigma\tau} T_{(-\mathfrak{P}_\infty^{A_\sigma})^{A_\tau} - \mathfrak{P}_\infty^{A_\tau}} = A_{\sigma\tau} T_{-\mathfrak{P}_\infty^{A_\sigma A_\tau}} = B_{\sigma\tau}.$$

Also $B_\sigma B_{\sigma^{-1}} = A_1$ so $\mathfrak{G}_2$ is closed under inverses as well.

From now on we will assume a class of translation equivalent groups has been selected and that $\mathfrak{G}_0$ is the unique member whose elements fix $\mathfrak{P}_\infty$. By an abuse of notation the elements of $\mathfrak{G}_0$ will be denoted by $\sigma, \tau, \dots$ as are the elements of $\mathrm{Aut}(k_1/k)$. We regard $T(L/k_1)$ as a right $\mathrm{Aut}(k_1/k)$-module by utilizing its natural structure as a right $\mathfrak{G}_0$-module. We have

Theorem 2.6. *There is a one-to-one correspondence between the members of the translation equivalent class and the cocycles of* $Z^1(\mathrm{Aut}(k_1/k); T(L/k_1))$ *and* $\mathfrak{G}_0$ *corresponds to the trivial cocycle.*

The proof is immediate.

We now consider the various subfields $K_0, K_1, \dots$ left pointwise fixed by the groups $\mathfrak{G}_0, \mathfrak{G}_1, \dots$ in a translation equivalent class. As we know, each is an elliptic function field over k.

Definition 2.7. We say that two of these fields K_i, K_j are k_1-*translates* if there is a translation $T_{\mathfrak{P}}$ in $T(L/k_1)$ such that $K_i^{T_{\mathfrak{P}}} = K_j$.

This is clearly an equivalence relation.

Theorem 2.8. K_i *is a* k_1-*translate of* K_0 *if and only if* K_i *has a* k-*rational point.*

Proof. Let $\mathfrak{G}_i = \{\sigma T_{\mathfrak{P}_\sigma}, \dots\}$ be the group associated with K_i and $\{T_{\mathfrak{P}_\sigma}, \dots\}$ the associated cocycle. Clearly K_i has a k-rational point if and only if there is a k_1-rational point $\mathfrak{P}$ in L such that $\mathfrak{P}^{\sigma T_{\mathfrak{P}_\sigma}} = \mathfrak{P}$. That is, $\mathfrak{P}^\sigma + \mathfrak{P}_\sigma = \mathfrak{P}$. On the other hand a quick computation shows that $K_i = K_0^{T_{\mathfrak{P}}}$ if and only if $\mathfrak{P}^\sigma + \mathfrak{P}_\sigma = \mathfrak{P}$.

Another way of looking at Theorem 2.8 is

Theorem 2.9. K_i *is a* k_1-*translate of* K_j *if and only if their associated cocycles differ by a coboundary in* $B^1(\mathrm{Aut}(k_1/k); T(L/k_1))$. *Thus there is a one-to-one correspondence between the elements of* $H^1(\mathrm{Aut}(k_1/k); T(L/k_1))$

and the equivalence classes of k_1-translates with the trivial member of H^1 being associated with the class of K_0.

We remark at this point that in dealing with the various group cohomologies we will use $T(L/k_1)$ and J_{k1} interchangeably with no further warning.

Now let $D_0^{K_i/k}$ be the group of divisors of degree zero for K_i. In an obvious way there is a homomorphism of $D_0^{K_i/k}$ into $D_0^{L/k1}$ and hence into $J_{k1} = \bar{D}_0^{L/k1}$, the group of divisor classes of degree zero. Now it is an easy consequence of "Hilbert's Theorem 90" that the kernel of this homomorphism is the group of principal divisors of K_i. Hence we have a monomorphism $j: \bar{D}_0^{K_i/k} \to J_{k1}$.

Theorem 2.10. $j(\bar{D}_0^{K_i/k}) \leq J_k$.

Proof. It is clear that $J_k = \{\mathfrak{P} \in J_{k1} \mid \mathfrak{P}^\sigma = \mathfrak{P} \text{ for all } \sigma\}$. Now if $\mathfrak{P} \in j(\bar{D}_0^{K_i/k})$ there is a divisor $\mathfrak{A}$ of degree zero on K_i such that $\mathfrak{A}$ is linearly equivalent to $\mathfrak{P}/\mathfrak{P}_\infty$. Thus if $\mathfrak{E}_i = \{\sigma T_{\mathfrak{P}\sigma}, \dots\}$ we see that $\mathfrak{P}^{\sigma T_{\mathfrak{P}\sigma}}/\mathfrak{P}_\infty^{\sigma T_{\mathfrak{P}\sigma}}$ is linearly equivalent to $\mathfrak{P}/\mathfrak{P}_\infty$. That is $\mathfrak{P} = \mathfrak{P}^\sigma$.

3. **Conic subfields.** Our notation and conventions remain as in §2 except that k_1 will now be a fixed quadratic extension of k and $\mathrm{Aut}(k_1/k) = \{1, \sigma\}$.

Definition 3.1. A subfield K_{i1} of K_i is said to be *conic* if (i) $k \leq K_{i1}$, (ii) $\mathrm{genus}(K_{i1}/k) = 0$ and (iii) $[K_i : K_{i1}] = 2$.

Theorem 3.2. *There is a one-to-one correspondence between the conic subfields of K_i and the points of J_k.*

Proof. Since L has the k_1-rational point $\mathfrak{P}_\infty$ there is a one-to-one correspondence between the conic subfields of L and the points of J_{k1} given by associating the point $\mathfrak{P}$ to the fixed field of the automorphism $\mu T_{\mathfrak{P}}$ where μ is the reflexion automorphism (i.e., $\mathfrak{P}^\mu = -\mathfrak{P}$). Now K_i is the fixed field of $\sigma T_{\mathfrak{P}\sigma}$. Thus if $\sigma T_{\mathfrak{P}\sigma}$ and $\mu T_{\mathfrak{P}}$ commute they generate a group of order 4 and the fixed field of this group is clearly a conic subfield of K_i. Conversely if K_{i1} is a conic subfield of K_i then $k_1 K_{i1}$ is a conic subfield of L and the point $\mathfrak{P}$ is associated and $\mu T_{\mathfrak{P}}$ and $\sigma T_{\mathfrak{P}\sigma}$ commute. Finally $\mu T_{\mathfrak{P}} \sigma T_{\mathfrak{P}\sigma} = \sigma T_{\mathfrak{P}\sigma} \mu T_{\mathfrak{P}}$ if and only if $\mu\sigma T_{\mathfrak{P}^\sigma + \mathfrak{P}_\sigma} = \sigma\mu T_{\mathfrak{P}-\mathfrak{P}_\sigma}$ if and only if $\mathfrak{P}^\sigma + \mathfrak{P}_\sigma = \mathfrak{P} - \mathfrak{P}_\sigma$ (since $\mu\sigma = \sigma\mu$). Now write $\mathfrak{P} = \mathfrak{P}_1 + \mathfrak{P}_\sigma$. Since $\mathfrak{P}_\sigma^\sigma + \mathfrak{P}_\sigma = \mathfrak{P}_\infty$ the equation $\mathfrak{P}^\sigma + \mathfrak{P}_\sigma = \mathfrak{P} - \mathfrak{P}_\sigma$ translates into $\mathfrak{P}_1^\sigma = \mathfrak{P}_1$. That is to say $\mathfrak{P}_1 \in J_k$.

Definition 3.3. Let K_{im} and K_{in} be conic subfields of K_i associated with the points $\mathfrak{P}_m$ and $\mathfrak{P}_n$, respectively, of J_k. We say that K_{im} is a k_1-translate of K_{in} if there is a k_1-translate $K_j = K_i^{T\mathfrak{P}}$ of K_i such that the conic subfield $K_{in}^{T\mathfrak{P}}$ is associated with the point $\mathfrak{P}_m$.

In order to see that this relation is in fact an equivalence relation it suffices to verify the following proposition.

Proposition 3.4. *K_{im} is a k_1-translate of K_{in} if and only if $\mathfrak{P}_m = \mathfrak{P}_n + \mathfrak{P} + \mathfrak{P}^\sigma$ where $\mathfrak{P}$ is some point in J_{k_1}.*

Proof. We note that if $\mathfrak{P}_\sigma$ is the cocycle associated with K_i then $\mathfrak{P}_\sigma + \mathfrak{P} - \mathfrak{P}^\sigma$ is the cocycle associated with $K_j = K_i^{T\mathfrak{P}}$. Likewise the point of J_k associated with $K_{in}^{T\mathfrak{P}}$ is $\mathfrak{P}_n + \mathfrak{P} + \mathfrak{P}^\sigma$.

We thus have an interpretation of $H^2(\mathrm{Aut}(k_1/k); J_{k_1})$.

Theorem 3.5. *There is a one-to-one correspondence between the equivalence classes of k_1-translate conic subfields of K_i and the elements of $H^2(\mathrm{Aut}(k_1/k); J_{k_1})$.*

Proof. Since k_1 is a cyclic extension of k we have $H^2(\mathrm{Aut}(k_1/k); J_{k_1}) = J_k/NJ_{k_1}$ where $NJ_{k_1} = \{\mathfrak{P} + \mathfrak{P}^\sigma \mid \mathfrak{P} \in J_{k_1}\}$. Now apply Proposition 3.4.

We also have an interpretation of the trivial class.

Theorem 3.6. *Let K_{i1} be the conic subfield of K_i associated with the point $\mathfrak{P}_1$. Moreover assume K_i is not itself in the trivial class. Then $\mathfrak{P}_1 \in NJ_{k_1}$ if and only if K_{i1} has a k-rational point that lies under a quadratic point of K_i that splits in L.*

Proof. Suppose $\mathfrak{P}_1 = \mathfrak{P} + \mathfrak{P}^\sigma$. Since $\mathfrak{P}_\sigma$ is not the trivial cocycle, the points $\mathfrak{P}$ and $\mathfrak{P}^{\sigma T\mathfrak{P}\sigma} = \mathfrak{P}^\sigma + \mathfrak{P}_\sigma$ are distinct. Thus they lie over a quadratic point of K_i that splits in L. On the other hand, $\mathfrak{P}^{\mu T_{\mathfrak{P}+\mathfrak{P}^\sigma+\mathfrak{P}_\sigma}} = \mathfrak{P}^\sigma + \mathfrak{P}_\sigma = \mathfrak{P}^{\sigma T\mathfrak{P}\sigma}$ so this quadratic point lies over a k-rational point of K_{i1}. This argument can be reversed in order to prove the converse.

Perhaps the most interesting interpretation is contained in the following result.

Theorem 3.7. *Let K_{i1} be the conic subfield associated with the point $\mathfrak{P}_1$. Then $\mathfrak{P}_1 \in j(\bar{D}_0^{K_i/k})$ if and only if K_{i1} has a k-rational point.*

Proof. First of all let us parametrize K_0 by a nonsingular plane cubic so that $K_0 = k(x, y)$ and $L = k_1(x, y)$. Now k_1K_{i1} is the fixed field of

$\mu T_{\mathfrak{P}_1+\mathfrak{P}_\sigma}$. Thus if we let t be the slope of the line through $-\mathfrak{P}_1-\mathfrak{P}_\sigma$ we have $k_1K_{i1}=k_1(t)$. Since $\sigma T_{\mathfrak{P}_\sigma}$ and $\mu T_{\mathfrak{P}_1+\mathfrak{P}_\sigma}$ commute, $t^{\sigma T_{\mathfrak{P}_\sigma}}=(at+b)/(ct+d)$ for suitable a, b, c, d in k_1 with $ad-bc\neq 0$. Now let the x and y coordinates of $-\mathfrak{P}_1-\mathfrak{P}_\sigma$ be α and β, respectively. Then $t=(y-\beta)/(x-\alpha)$. Thus $t^{\sigma T_{\mathfrak{P}_\sigma}}=(y^{T_{\mathfrak{P}_\sigma}}-\beta^\sigma)/(x^{T_{\mathfrak{P}_\sigma}}-\alpha^\sigma)$ (recall that $y^\sigma=y$, $x^\sigma=x$, $\alpha^{T_{\mathfrak{P}_\sigma}}=\alpha$ and $\beta^{T_{\mathfrak{P}_\sigma}}=\beta$). Now let $\mathfrak{P}_2\in J_{k_1}$. We see from the above remarks that $t(\mathfrak{P}_2)$ is the slope of the line through $\mathfrak{P}_2$ and $-\mathfrak{P}_1-\mathfrak{P}_\sigma$ while $t^{\sigma T_{\mathfrak{P}_\sigma}}(\mathfrak{P}_2)$ is the slope of the line through $\mathfrak{P}_2-\mathfrak{P}_\sigma$ and $(-\mathfrak{P}_1-\mathfrak{P}_\sigma)^\sigma=-\mathfrak{P}_1+\mathfrak{P}_\sigma$. We distinguish two cases. *Case* 1: $c=0$. We claim that this occurs if and only if $\mathfrak{P}_1=\mathfrak{P}_\infty$. Indeed $t(\mathfrak{P}_\infty)=\infty$ so $c=0$ if and only if $t^{\sigma T_{\mathfrak{P}_\sigma}}(\mathfrak{P}_\infty)=\infty$. Since the latter is the slope of the line through $\mathfrak{P}_\infty-\mathfrak{P}_\sigma=-\mathfrak{P}_\sigma$ and $-\mathfrak{P}_1+\mathfrak{P}_\sigma$, we see that the third point on the line must be $\mathfrak{P}_\infty$ (note that $\mathfrak{P}_\sigma\neq\mathfrak{P}_\infty$ since $\mathfrak{P}_\sigma$ is assumed nontrivial). Thus $c=0$ if and only if $\mathfrak{P}_1=\mathfrak{P}_\infty$. Continuing with this case, it suffices to set $d=1$ so $t^{\sigma T_{\mathfrak{P}_\sigma}}=at+b$. We claim $a=-1$ and $b=0$. To see this we let $\bar{k}$ be the separable closure of k and extend σ to an automorphism of $\bar{k}$ over k in any of the possible ways. We extend $T_{\mathfrak{P}_\sigma}$ to $\bar{L}=\bar{k}\otimes_{k_1}L$ in the obvious way as the translation by $\mathfrak{P}_\sigma$. We see that if $\mathfrak{P}_2$ is any point in $J_{\bar{k}}$ then $t(\mathfrak{P}_2)$ is the slope of the line through $\mathfrak{P}_2$ and $-\mathfrak{P}_1-\mathfrak{P}_\sigma$ while $t^{\sigma T_{\mathfrak{P}_\sigma}}(\mathfrak{P}_2)=at(\mathfrak{P}_2)+b$ is the slope of the line through $\mathfrak{P}_2-\mathfrak{P}_\sigma$ and $-\mathfrak{P}_1+\mathfrak{P}_\sigma$. Now let $\mathfrak{P}_2, \mathfrak{P}_2', \mathfrak{P}_2'', \mathfrak{P}_2'''$ be the four (necessarily distinct) points of tangency to the line through $-\mathfrak{P}_\sigma$. Moreover let $t_2=t(\mathfrak{P}_2),\ldots, t_2'''=t(\mathfrak{P}_2''')$. Since $\mathfrak{P}_2-\mathfrak{P}_\sigma=-\mathfrak{P}_2$ we have $-t_2=at_2+b,\ldots,-t_2'''=at_2'''+b$. Since these slopes are distinct, one must have $a=-1, b=0$. Finally let $k_1=k(\sqrt{d}_0)$ and $t'=\sqrt{d}_0 t$. Clearly $k_1(t)=k_1(t')$ while $(t')^{\sigma T_{\mathfrak{P}_\sigma}}=t'$ implies that $k(t')\leq K_{i1}$. But the containment cannot be proper since $k_1(t')=k_1K_{i1}$. Hence K_{i1} has a k-rational point. *Case* 2: $c\neq 0$. It is no loss of generality to take $c=1$ so $t^{\sigma T_{\mathfrak{P}_\sigma}}=(at+b)/(t+d)$. Now $(\sigma T_{\mathfrak{P}_\sigma})^2=1$ so

$$t=((aa^\sigma+b^\sigma)t+(a^\sigma b+b^\sigma d))/((a+d^\sigma)t+(b+d^\sigma d)).$$

Thus $aa^\sigma+b^\sigma=b+d^\sigma d\neq 0$ while $a^\sigma b+b^\sigma d=a+d^\sigma=0$. Hence $d=-a^\sigma$ and $b=b^\sigma$. Let $\Delta=aa^\sigma+b$ and note that $\Delta\in k^*$. Moreover $(t-a^\sigma)^{\sigma T_{\mathfrak{P}_\sigma}}=\Delta/(t-a^\sigma)$. Again let $k_1=k(\sqrt{d}_0)$ and write $t-a^\sigma=u+\sqrt{d}_0 v$ with $u, v\in K_{i1}$. Thus

$$\Delta=(t-a^\sigma)(t-a^\sigma)^{\sigma T_{\mathfrak{P}_\sigma}}=(u+\sqrt{d}_0 v)(u-\sqrt{d}_0 v)=u^2-d_0v^2.$$

Since $k_1(t-a^\sigma)=k_1(u, v)=k_1K_{i1}$ we have $K_{i1}=k(u, v)$. Consequently K_{i1} has a k-rational point if and only if $u^2-d_0v^2=\Delta$ has a solution in k. In other words, if and only if $\Delta\in Nk_1^*$. Let us look now at the principal

divisor $(t - a^\sigma)$. We have $(t - a^\sigma) = \mathfrak{P}_1\mathfrak{P}_\sigma/\mathfrak{P}_\infty(\mathfrak{P}_1 + \mathfrak{P}_\sigma)$. Indeed, the poles of $t^{\sigma T\mathfrak{P}}$ are exactly the zeros of $t - a^\sigma$. Hence $(t - a^\sigma) = (\mathfrak{P}_1/\mathfrak{P}_\infty)^{1-\sigma T\mathfrak{P}\sigma}$. From this equation it follows easily that $\Delta \in Nk_1^*$ if and only if there is an element ω in L^* such that $(\omega\mathfrak{P}_1/\mathfrak{P}_\infty) = (\omega\mathfrak{P}_1/\mathfrak{P}_\infty)^{\sigma T\mathfrak{P}\sigma}$. In other words $\mathfrak{P}_1 \in j(\overline{D}_0^{K} i1^{/k})$.

Corollary 3.8. $NJ_{k1} \leq j(\overline{D}_0^{K} i1^{/k})$.

4. **The local case.** The results of this section will mostly pertain to the case in which k is a p-adic field. We begin, however, with a construction which is general. Our notation and assumptions remain as in §3.

We let K_0' be the fixed field for the involution $\sigma\mu$. It is easy to see that K_0' is an elliptic extension of k with $\mathfrak{P}_\infty$ as a k-rational point and $k_1K_0' = L$. Let J_k' denote the group of k-rational points of K_0'. ($\mathfrak{P}_\infty$ is the neutral element.) Moreover, we will write J_{k1}' instead of J_{k1} when we regard L as k_1K_0'. Now $\mathrm{Aut}(k_1/k)$ acts on J_{k1}' by $\mathfrak{P} \to \mathfrak{P}^{\sigma\mu}$. Thus we obtain the following duality relations:

$$J_k = Z^1(\mathrm{Aut}(k_1/k);\ J_{k_1}') \quad \text{and} \quad J_k' = Z^1(\mathrm{Aut}(k_1/k);\ J_{k_1}).$$

Next let us denote the Tate-Shafaravich maps reduced to the cyclic layer determined by k_1 as follows:

$$\phi\colon J_k \times Z^1(\mathrm{Aut}(k_1/k);\ J_{k_1}) \to H^2(\mathrm{Aut}(k_1/k);\ k_1^*)$$

and

$$\phi'\colon Z^1(\mathrm{Aut}(k_1/k);\ J_{k_1}') \times J_k' \to H^2(\mathrm{Aut}(k_1/k);\ k_1^*).$$

See [4] for explicit details of the pairing.

Proposition 4.1. *Let $\mathfrak{P}_1$ be in J_k and $\mathfrak{P}_\sigma$ be in $Z^1(\mathrm{Aut}(k_1/k);\ J_{k1})$. Then $\phi(\mathfrak{P}_1, \mathfrak{P}_\sigma) = \phi'(\mathfrak{P}_1, \mathfrak{P}_\sigma)$.*

Proof. Let ρ be a generator for the fixed field of $\mu T\mathfrak{P}_1 + \mathfrak{P}_\sigma$ such that the principal divisor $(\rho) = \mathfrak{P}_1\mathfrak{P}_\sigma/\mathfrak{P}_\infty(\mathfrak{P}_1 + \mathfrak{P}_\sigma)$. Since $\rho^{\mu T\mathfrak{P}_1 + \mathfrak{P}\sigma} = \rho$ it follows that $\rho^{\sigma T\mathfrak{P}\sigma} = \rho^{\sigma\mu T\mathfrak{P}1}$. Moreover, $(\rho) = (\mathfrak{P}_1/\mathfrak{P}_\infty)^{1-\sigma T\mathfrak{P}\sigma} = (\mathfrak{P}_\sigma/\mathfrak{P}_\infty)^{1-\sigma\mu T\mathfrak{P}1}$. Hence, $\phi(\mathfrak{P}_1, \mathfrak{P}_\sigma) = \rho^{1+\sigma T\mathfrak{P}\sigma Nk_1^*} = \phi'(\mathfrak{P}_1, \mathfrak{P}_\sigma)$.

From now on, k will be a p-adic field. We assume known the exactness of the Tate-Shafaravich pairing. See [1], for example. Using this fact and Proposition 4.1 we obtain with no difficulty the following

Corollary 4.2. *The pairing induces a nonsingular pairing*

$\bar{\phi}$: $H^2(\mathrm{Aut}(k_1/k); J_{k_1}) \times H^1(\mathrm{Aut}(k_1/k); J_{k_1}) \to H^2(\mathrm{Aut}(k_1/k); k_1^*)$.

The next three corollaries depend on the fact that when k is p-adic then J_k contains a subgroup $\mathfrak{D}$ isomorphic to the additive group of integers of k and of finite index in J_k. See [1, Theorem 17.1].

Corollary 4.3. $H^1(\mathrm{Aut}(k_1/k); J_{k_1}) \cong H^2(\mathrm{Aut}(k_1/k); J_{k_1})$.

Proof. It suffices to show that either of these groups is finite. But $J_k/2J_k \to H^2(\mathrm{Aut}(k_1/k); J_{k_1}) \to 0$ and $J_k/2J_k$ is finite since $2\mathfrak{D}$ is of finite index in $\mathfrak{D}$ for all primes p.

Corollary 4.4. *If $p \neq 2$ then the order of $H^1(\mathrm{Aut}(k_1/k); J_{k_1})$ is 1, 2 or 4.*

Proof. Let $J_{k,2}$ be the 2-primary component of J_k and $(J_k/\mathfrak{D})_2$ the 2-primary component of $J_k/\mathfrak{D}$. It is easily seen that $J_{k,2} \to (J_k/\mathfrak{D})_2 \to 0$. Next, $(J_k/\mathfrak{D})_2 \to J_k/2J_k \to 0$ since $\mathfrak{D} = 2\mathfrak{D}$. The proof is completed by observing that $J_k/2J_k \to H^2(\mathrm{Aut}(k_1/k); J_{k_1}) \to 0$.

Corollary 4.5. *If $p \neq 2$ and K_0 is given by $y^2 = P_3(x)$ with $P_3(x)$ an irreducible cubic, then $H^1(\mathrm{Aut}(k_1/k); J_{k_1}) = 0$.*

Proof. $J_{k,2} = 0$.

Our final result is an easy consequence of Theorem 3.7 and Proposition 4.1 and Corollary 4.2.

Theorem 4.6. *If K_1 is an elliptic function field without rational points over the p-adic field k, then K_1 contains a conic subfield K_{11} without k-rational points.*

5. **Special computations.** We begin with the general cubic $y^2 = x^3 + Ax^2 + Bx + C$ over the field k (characteristic not 2). Set $k_1 = k(\sqrt{d})$. Let $\mathfrak{P}_\sigma = (\alpha, \beta) \neq \mathfrak{P}_\infty$ be an arbitrary nonzero cocycle. In other words $\mathfrak{P}_\infty = \mathfrak{P}_\sigma + \mathfrak{P}_\sigma^\sigma$ and so $\alpha \in k$ and $\beta^\sigma = -\beta$. Let $t = (y + \beta)/(x - \alpha)$ be the slope of the line through $-\mathfrak{P}_\sigma = -\mathfrak{P}_\infty - \mathfrak{P}_\sigma$. As we have seen, $t^{\sigma T_{\mathfrak{P}_\sigma}} = -t$. Now $y^2 = t^2(x - \alpha)^2 - 2\beta t(x - \alpha) + \beta^2$ implies $t^2(x - \alpha) - 2\beta t = x^2 + \alpha x + \alpha^2 + A(x + \alpha) + B$ or $x^2 + (\alpha + A - t^2)x + (\alpha^2 + \alpha A + B + \alpha t^2 + 2\beta t) = 0$. Hence $x = [-(\alpha + A - t^2) + \omega]/2$ where $\omega^2 = (\alpha + A - t^2)^2 - 4(\alpha^2 + \alpha A + B + \alpha t^2 + 2\beta t)$. Since $t^{\sigma T_{\mathfrak{P}_\sigma}} = -t$, $\beta^{\sigma T_{\mathfrak{P}_\sigma}} = \beta^\sigma = -\beta$ and $\alpha^{\sigma T_{\mathfrak{P}_\sigma}} = \alpha^\sigma = \alpha$, it follows that $\omega^{\sigma T_{\mathfrak{P}_\sigma}} = \pm\sigma$. We claim that the minus sign prevails. Indeed if $\omega^{\sigma T_{\mathfrak{P}_\sigma}} = \omega$ then $x^{\sigma T_{\mathfrak{P}_\sigma}} = x$. Moreover, since $\mathfrak{P}_\sigma \neq \mathfrak{P}_\infty$ it is clear that $x^{\sigma T_{\mathfrak{P}_\sigma}} \neq x$. We have therefore shown

Proposition 5.1. *With the notation as above, a quartic equation for the principal homogeneous space, K_1, associated with $\mathfrak{P}_\sigma$ is given by* $d\bar{\omega}^2 = (\alpha + A - d\bar{t}^2)^2 - 4(\alpha^2 + \alpha A + B + \alpha d\bar{t}^2 + 2\beta\sqrt{d}\bar{t})$.

Let us now consider several special cases. Let $y^2 = x(x^2 + bx + c)$ and $\mathfrak{P}_\sigma = (0, 0)$. Specializing Proposition 5.1 we see that K_1 is given by $d\bar{\omega}^2 = d^2\bar{t}^4 - 2bd\bar{t}^2 + b^2 - 4c$. Next set $\mathfrak{P}_1 = (0, 0)$ and let us compute the conic subfield K_{11}. The slope of the line through $-\mathfrak{P}_1 - \mathfrak{P}_\sigma = \mathfrak{P}_\infty$ is the variable x. Since the slope of the line through $\mathfrak{P}_1$ and $\mathfrak{P}_\sigma$ is 0 in this case it follows that $x^{\sigma_T\mathfrak{P}_\sigma} = \Delta/x$. Now if $\mathfrak{P}_2 = \frac{1}{2}\mathfrak{P}_\sigma$ we know that $\mathfrak{P}_2^{\sigma_T\mathfrak{P}_\sigma} = -\mathfrak{P}_2$. Thus if $\mathfrak{P}_2 = (x_2, y_2)$ we see that $\Delta = x_2^2$. To compute $\mathfrak{P}_2$ let $r = y/x$ be the slope through $\mathfrak{P}_\sigma$. Hence $y^2 = r^2x^2 = x(x^2 + bx + c)$ or $x^2 + (b - r^2)x + c = 0$. Thus $x_2 = [-(b - r_2^2)/2]$ where $r_2^4 - 2br_2^2 + b^2 - 4c = 0$. Now $r_2^2 = b \pm 2\sqrt{c}$ so $x_2 = \pm\sqrt{c}$. We have proved

Proposition 5.2. *With $\mathfrak{P}_1$ and $\mathfrak{P}_\sigma$ as above we have $\phi(\mathfrak{P}_1, \mathfrak{P}_\sigma) = cNk_1^*$.*

Continuing, we set $x = u + \sqrt{d}v$ with u, v in K_{11}. Then $K_1 = k(u, v)$ and $u^2 - dv^2 = c$. Moreover, since $t^2 = (y/x)^2 = (x + (c/x) + b) = 2u + b$ and $t^{\sigma_T\mathfrak{P}_\sigma} = -t$, we have $d\bar{t}^2 = 2u + b$ where $\sqrt{d}\bar{t} = t$. Thus we have

Proposition 5.3. *With all notation as above, K_{11} is given by the equation $u^2 - dv^2 = c$ and K_1 is given by the pair of equations $u^2 - dv^2 = c$ and $d\bar{t}^2 = 2u + b$.*

It is, perhaps, of interest to specialize all of this for the equation $y^2 = x(x^2 + 17)$ over $k = Q$. We let $k_1 = Q(\sqrt{2})$ and $\mathfrak{P}_\sigma = (0, 0)$. Then the equation for the principal homogeneous space is given by $\bar{\omega}^2 = 2(\bar{t}^4 - 17)$. This latter equation is well known as the so-called Reichardt equation and is an example of an elliptic curve defined over Q which has no rational points but which has points in every completion of Q. See [1, §26] for details. We have

Proposition 5.4. *The equation for the Jacobian variety of the Reichardt equation $y^2 = 2(x^4 - 17)$ over Q is $y^2 = x(x^2 + 17)$.*

Finally we consider the case of a cubic of the form $y^2 = x(x - a)(x - c)$ and $\mathfrak{P}_\sigma = (0, 0)$ and $\mathfrak{P}_1 = (a, 0)$. Clearly $-\mathfrak{P}_1 - \mathfrak{P}_\sigma = (c, 0)$. Let $t = y/(x - c)$ be the slope of the line through $-\mathfrak{P}_1 - \mathfrak{P}_\sigma$. Thus $y^2 = t^2(x - c)^2 = x(x - a)\cdot(x - c)$ or $x^2 - (z + t^2)x + ct^2 = 0$. Hence $x = [(a + t^2) + \omega]/2$ where $\omega^2 = t^4 + 2(a - 2c)t^2 + a^2$. Now since the slope of the line through $\mathfrak{P}_1$ and $\mathfrak{P}_\sigma$ is zero we know that $t^{\sigma_T\mathfrak{P}_\sigma} = \Delta/t$. In order to compute Δ we first find $\frac{1}{2}\mathfrak{P}_\sigma$.

Indeed let $r = y/x$ be the slope of the line through $\mathfrak{P}_\sigma$. We have $y^2 = r^2x^2 = x(x-a)(x-c)$ so $x^2 - (a + c + r^2)x + ac = 0$. Hence if $\frac{1}{2}\mathfrak{P}_\sigma = (x_2, y_2)$ we have $x_2 = (a + c + r_2^2)/2$ where $0 = (a + c + r_2^2)^2 - 4ac = r_2^4 + 2(a + c)r_2^2 + (a - c)^2$. In other words, $r_2^2 = -(a + c) \pm 2\sqrt{ac}$. Hence $x_2 = \pm\sqrt{ac}$ and $y_2 = x_2 r_2$. Since $(\frac{1}{2}\mathfrak{P}_\sigma)^{\sigma T\mathfrak{P}\sigma} = -(\frac{1}{2}\mathfrak{P}_\sigma)$ it follows that $-y_2/(x_2 - c) = \Delta/(y_2/(x_2 - c))$ so $\Delta = -y_2^2/(x_2 - c)^2 = a$. Now set $t = u + \sqrt{d}v$ so that $u^2 - dv^2 = a$ is the equation for the conic subfield K_{11}. Finally $(\omega/t)^2 = t^2 + a^2/t^2 + 2(a - 2c)$ or $(\omega/t)^2 = 2(u^2 + dv^2) + 2(a - 2c)$. Hence $(\omega/t)^{\sigma T\mathfrak{P}\sigma} = \pm(\omega/t)$. We claim that the minus sign prevails. Indeed if $(\omega/t)^{\sigma T\mathfrak{P}\sigma} = (\omega/t)$ it follows that $(x/t) = u + (\omega/2t)$ is fixed under $\sigma T_{\mathfrak{P}\sigma}$. But $(x/t)^{\sigma T\mathfrak{P}\sigma} = x^{\sigma T\mathfrak{P}\sigma}t/a$, so $x^{\sigma T\mathfrak{P}\sigma}t^2/a = x$ or $x^{\sigma T\mathfrak{P}\sigma}(x - a) = a(x - c)$. However computing this equation at $(a, 0)$ or $(c, 0)$ yields a contradiction. Let $\sqrt{d}\,\eta = \omega/t$. Then $\eta^{\sigma T\mathfrak{P}\sigma} = \eta$ and $d\eta^2 = 2(u^2 + dv^2) + 2(a - 2c)$. Combining these equations shows that $d\eta^2 = 2(2u^2 - a) + 2(a - 2c) = 4u^2 - 4c$. Thus we have proved

Proposition 5.5. *With notation as above, K_{11} is described by $u^2 - dv^2 = a$ while K_1 is described by the pair of equations $u^2 - dv^2 = a$ and $(2u)^2 - d\eta^2 = 4c$.*

As a simple example of these techniques, consider the equation $2\omega^2 = 4t^4 + 36t^2 + 9$ or, equivalently, $\omega^2 - 2(t^2 + (9/2))^2 = -36$. This has no points in Q. Indeed its Jacobian is $y^2 = x(x - 3)(x - 6)$ and 3 is not a norm from $Q(\sqrt{2})$.

BIBLIOGRAPHY

1. J. W. S. Cassels, *Diophantine equations with special reference to elliptic curves*, J. London Math. Soc. 41 (1966), 193–291; corrigenda, ibid. 42 (1967), 183. MR 33 #7299; 34 #2523.

2. M. Eichler, *Einführung in die Theorie der algebraischen Zahlen und Funktionen*, Lehrbücher und Monographien aus dem Gebiete der exakten Wissenschaften, Mathematische Reihe, Band 27, Birkhäuser Verlag, Basel-Stuttgart, 1963; English transl., Pure and Appl. Math., vol. 23, Academic Press, New York, 1966. MR 29 #5821; 35 #160.

3. R. E. MacRae and P. Samuel, *Subfields of index 2 of elliptic function fields*, Lecture Notes in Math., vol. 311, Springer-Verlag, New York, 1972, pp. 171–193.

4. G. Poitou, *Dans les pas de François Chatalet*, Journées Arithmétiques, 1965, Faculté des Science de Besancon.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF COLORADO, BOULDER, COLORADO 80302 (Current address)

DÉPARTEMENT DE MATHÉMATIQUE, UNIVERSITÉ DE PARIS, SUD XI, ORSAY, FRANCE