Arithmetic on curves of genus 1

VIII. On conjectures of Birch and Swinnerton-Dyer

By *J. W. S. Cassels* at Cambridge (England)

---

1. Introduction

Birch and Swinnerton-Dyer [1] have recently produced convincing evidence that some analogue of the Tamagawa Number, which has been defined for linear algebraic groups [7, 14, 15, 16], must also exists for abelian varieties. In the present state of knowledge it is difficult to see how these conjectures can be proved. In this paper I show, however, that certain results can be proved which would (conjecturally) follow from the comparison of the (conjectural) Tamagawa Numbers of a pair of isogenous abelian varieties of dimension 1. My results thus corroborate the Birch-Swinnerton-Dyer conjectures and, in particular, they confirm a part of them for which the numerical evidence was not particularly strong. It turns out that my results are equivalent to a conjecture of Birch and Swinnerton-Dyer about the number of "first descents" for a pair of conjugate isogenies which was at first thought to be independent of their other conjecture.

For this work it is necessary to study the behaviour under isogeny of the bilinear form on the Tate-Šafarevič group, whose existence was proved in Paper IV of this series.

I suspect that it would be possible to extend the results of this paper to abelian varieties of arbitrary dimension by the techniques outlined by Tate in his Stockholm address [13].

I must express here my heartfelt gratitude to Birch and Swinnerton-Dyer for keeping me informed of the progress of their work and of their conjectures. They have shown great insight in choosing the right questions to ask the computer and in drawing the correct conclusions from its sometimes surprising replies. Their conjectures were the

starting point of all the work described here. Proofs of a particular case of one of the conjectures were obtained independently by Mr E. Forrest [17] by a different argument.

In the rest of this introduction we enunciate the main results of the paper and discuss them in more detail. The rest of the paper contains only proofs. There is a discussion of the background to this paper in my Stockholm address [3].

An abelian variety of dimension 1 defined over a field k is an elliptic curve $\mathcal{C}$ together with a point $\mathfrak{o}$ on it, both defined over k. There is then a uniquely defined abelian group structure defined over k on the points of $\mathcal{C}$ for which $\mathfrak{o}$ is the zero element (see e. g. [3], [6]). An isogeny ν_1 of $(\mathcal{C}_1, \mathfrak{o}_1)$ onto $(\mathcal{C}_2, \mathfrak{o}_2)$ is a rational map

$$(1.\ 1) \qquad \mathcal{C}_1 \xrightarrow{\nu_1} \mathcal{C}_2$$

defined over k such that $\nu_1(\mathfrak{o}_1) = \mathfrak{o}_2$ and having a finite kernel Δ_1 (say). Let $\mathfrak{G}_j$, $\bar{\mathfrak{G}}_j$ be the groups of points on $\mathcal{C}_j (j = 1, 2)$ defined over k and over its algebraic closure $\bar{k}$ respectively. Then there is an exact sequence

$$(1.\ 2) \qquad 0 \longrightarrow \Delta_1 \longrightarrow \bar{\mathfrak{G}}_1 \xrightarrow{\nu_1} \bar{\mathfrak{G}}_2 \to 0$$

from which and the usual cohomology sequence one obtains the exact sequence (cf. [6], [8], [9], [10]),

$$(1.\ 3) \qquad 0 \to \mathfrak{G}_2 / \mathfrak{G}_1 \to H^1(\Gamma, \Delta_1) \to (WC_1)_{\nu_1} \to 0$$

provided that k is perfect (and so, in particular, if it is of characteristic 0). Here Γ is the galois group of $\bar{k}/k$,

$$(1.\ 4) \qquad WC_j = H^1(\Gamma, \bar{\mathfrak{G}}_j)$$

is the Weil-Châtelet group and $(WC_1)_{\nu_1}$ is the kernel of the map

$$(1.\ 5) \qquad WC_1 \xrightarrow{\nu_1} WC_2$$

induced by ν_1 in an obvious way. More generally we shall denote by ν_1 a host of maps derived from ν_1 in an obvious way and if $G \xrightarrow{\lambda} H$ is any group homomorphism we shall denote[1]) by $(G)_\lambda$ the kernel of λ.

Let K be any field containing k. Then everything defined over k is also defined over K and it is easy to see that there is a sequence of maps from the terms of (1. 3) into the corresponding terms when K is taken as the groundfield, so that the result is an exact and commutative diagram. In particular this is the case when k is an algebraic numberfield (a finite extension of the rationals) and $K = k_\mathfrak{p}$ is its completion with respect to a valuation $\mathfrak{p}$. Then we have the diagram

$$(1.\ 6) \qquad \begin{array}{ccccccc} 0 \to \mathfrak{G}_2/\nu_1\mathfrak{G}_1 & \to & H^1(\Gamma, \Delta_1) & \to & (WC_1)_{\nu_1} & \to 0 \\ \downarrow j_\mathfrak{p} & & \downarrow j_\mathfrak{p} & & \downarrow j_\mathfrak{p} & \\ 0 \to \mathfrak{G}_{2\mathfrak{p}}/\nu_1\mathfrak{G}_{1\mathfrak{p}} & \to & H^1(\Gamma_\mathfrak{p}, \Delta_1) & \to & (WC_{1\mathfrak{p}})_{\nu_1} & \to 0 \end{array}$$

where a suffix $\mathfrak{p}$ denotes the corresponding thing for the groundfield $k_\mathfrak{p}$ and where the $j_\mathfrak{p}$ are "localization maps". The Selmer group S^1 by definition consists of those elements ξ of $H^1(\Gamma, \Delta_1)$ for which $j_\mathfrak{p}\xi$ is in the image of $\mathfrak{G}_{2\mathfrak{p}}/\nu_1\mathfrak{G}_{1\mathfrak{p}}$ for every valuation $\mathfrak{p}$ of k. There is then an exact sequence

$$(1.\ 7) \qquad 0 \to \mathfrak{G}_2/\nu_1\mathfrak{G}_1 \to S^1 \to (Ш_1)_{\nu_1} \to 0$$

[1]) In particular if m is a natural number $(G)_m$ denotes the group of elements of G of order dividing m, i. e. the kernel of $G \xrightarrow{m} G$.

where Ш_j is the Tate-Šafarevič group of $(\mathcal{C}_j, \mathfrak{o}_j)$ i. e. the intersection of the kernels of all the localizations

$$(1.8) \qquad WC_j \xrightarrow{j_\mathfrak{p}} WC_{j_\mathfrak{p}} \qquad (j = 1, 2)$$

and, in accordance with our general notational conventions, $(\text{Ш})_{\nu_1}$ is the kernel of the map

$$(1.9) \qquad \text{Ш}_1 \xrightarrow{\nu_1} \text{Ш}_2$$

induced by ν_1.

To the isogeny ν_1 there corresponds a conjugate (or dual) isogeny

$$(1.10) \qquad \mathcal{C}_2 \xrightarrow{\nu_2} \mathcal{C}_1.$$

If $\mathfrak{x}_2$ is a generic point of $\mathcal{C}_2$ then $\nu_2(\mathfrak{x}_2)$ is defined to be the sum on $\mathcal{C}_1$ of the points of the inverse image $\nu_1^{-1}(\mathfrak{x}_2)$ less the corresponding sum for $\nu_1^{-1}(\mathfrak{o}_2)$. This is a symmetric relationship (i. e. the conjugate of ν_2 is again ν_1) and ν_2 has the same degree as ν_1. Let S^2 be the Selmer group for ν_2, so that there is an exact sequence

$$(1.11) \qquad 0 \to \mathfrak{G}_1 / \nu_2 \mathfrak{G}_2 \to S^2 \to (\text{Ш}_2)_{\nu_2} \to 0.$$

As is well-known (cf. [6]) the Selmer groups are finite. On the basis of extensive numerical investigations Birch and Swinnerton-Dyer were led to an interesting contectural formula $|S^1|/|S^2|$ in the particular case where $\mathcal{C}_1$, $\mathcal{C}_2$ are the curves

$$(1.12) \qquad y^2 = x^3 - Dx, \ y^2 = x^3 + 4Dx$$

respectively (D, a rational integer), k is the rational field and ν_1, ν_2 are the well-known isogenies of degree 2. Here $|M|$ for any set M will denote the number of elements of M. Their conjecture in this special case was proved independently and simultaneously by E. Forrest, but his method seems incapable of generalization.

Birch and Swinnerton-Dyer were in part led to the form of their conjecture by their conjecture about the existence of an analogue of the Tamagawa Number. In order to enunciate it we must first therefore discuss Tamagawa Numbers.

For any $\mathfrak{p}$ let $d_\mathfrak{p}^+ x$ denote the additive Haar measure so normalised that the measure of the $\mathfrak{p}$-adic integers is 1 if $\mathfrak{p}$ is non-archimedean, that $d_\mathfrak{p}^+ x$ is the ordinary Lebesgue measure if $k_\mathfrak{p}$ is the real field and so that is twice the ordinary 2-dimensional Lebesgue measure if $k_\mathfrak{p}$ is the complex field. Let $(\mathcal{C}, \mathfrak{o})$ be an abelian variety (of dimension 1) defined over k and let $\omega = f(\mathfrak{x})\, dx(\mathfrak{x})$ be a differential of the first kind on $\mathcal{C}$ defined over k, where $x(\mathfrak{x})$ is one of the co-ordinates of the generic point $\mathfrak{x}$. For example if $\mathcal{C}$ is in Weierstrass Normal Form

$$(1.13) \qquad y^2 = x^3 - Ax - B$$

one can take $\omega = y^{-1} dx$. In any case ω is uniquely defined by $\mathcal{C}$ up to a multiplicative nonzero constant in k. The differential ω defines a normalization of the Haar measure on the group $G_\mathfrak{p}$ of points of C defined over $k_\mathfrak{p}$ by putting

$$(1.14) \qquad \mu_\mathfrak{p}(\omega, E) = \int_{\mathfrak{a} \in E} |f(\mathfrak{a})|_\mathfrak{p}\, d_\mathfrak{p}^+ x(\mathfrak{a})$$

for any measurable subset E of $G_\mathfrak{p}$. Here $|\ |_\mathfrak{p}$ is the $\mathfrak{p}$-adic valuation with the usual normalisation[2]). It is readily verified that $\mu_\mathfrak{p}(\omega, E)$ is independent of the particular

[2]) i. e. $|\pi|_\mathfrak{p}$ for a prime element π of $k_\mathfrak{p}$ is q^{-1}, where q is the number of elements in the residue class field when $k_\mathfrak{p}$ is-non archimedean: and $|\ |_\mathfrak{p}$ is the ordinary absolute value otherwise.

expression fdx chosen for the differential ω and that it is a Haar measure (i. e. invariant under translation by elements of $\mathfrak{G}_\mathfrak{p}$). For all this cf. [15] for the corresponding results for linear algebraic groups.

Now let ω' be another differential of the first kind defined over k, so that

$$\omega' = \alpha\omega \tag{1.15}$$

for some $\alpha \in k^*$. Then

$$\mu_\mathfrak{p}(\omega', E) = |\alpha|_\mathfrak{p}\mu_\mathfrak{p}(\omega, E) \tag{1.16}$$

by (1. 14). In particular

$$\prod_\mathfrak{p} \frac{\mu_\mathfrak{p}(\omega', \mathfrak{G}_\mathfrak{p})}{\mu_\mathfrak{p}(\omega, \mathfrak{G}_\mathfrak{p})} = \prod |\alpha|_\mathfrak{p} = 1. \tag{1.17}$$

Hence

$$\{T(C)\}^{-1}(\text{say}) = \prod_\mathfrak{p} \mu_\mathfrak{p}(\omega, \mathfrak{G}_\mathfrak{p}), \tag{1.18}$$

if it converges, is independent of the choice of ω and so depends only on C and k. It is not known whether the infinite product (1. 18) ever converges, but when C has complex multiplication Birch and Swinnerton-Dyer have produced a heuristic substitute, say $\{t(C)\}^{-1}$, for it. For the definition of $t(C)$ and the justification for taking it as a substitute for $T(C)$ see their memoirs [1] or my Stockholm address [3]. They have proved that $t(C)$ is always rational and on the basis of extensive numerical work put forward the

Conjecture.

$$\begin{aligned} t(C) &= 0 \qquad \textit{if } |\mathfrak{G}| = \infty \\ t(C) &= \frac{|\text{Ш}|}{|\mathfrak{G}|^2} \quad \textit{if } |\mathfrak{G}| < \infty. \end{aligned} \tag{1.19}$$

We remark in passing that it has not been proved that $|\text{Ш}|$ is finite, indeed no method has been found for finding the complete group Ш although its various primary components can often be computed. The factor $|\text{Ш}|$ in (1. 19) appears to be analogous to the factor $i(\tau)$ in Ono's formula for the Tamagawa numbers of tori [7]. On the other hand, the factor $|\mathfrak{G}|^2$ in (1. 19) is rather unexpected because $\{t(C)\}^{-1}$ is a heuristic substitute for the Tamagawa measure of the whole adele group and the analogue wirth the case of linear groups would have suggested $|\mathfrak{G}|$ instead.

The curve C has a "good reduction" modulo $\mathfrak{p}$ for almost all $\mathfrak{p}$ and it is easy to see that

$$\mu_\mathfrak{p}(\omega, \mathfrak{G}_\mathfrak{p}) = N_\mathfrak{p}/\text{Norm } \mathfrak{p} \tag{1.20}$$

for almost all $\mathfrak{p}$, where Norm is the absolute norm, and $N_\mathfrak{p}$ is the number of points on the mod $\mathfrak{p}$ curve[3]). (cf. [15] for the proofs in the linear group case, which is more complicated). Now Lang has proved [5] that two isogenous algebraic groups defined over a finite field have the same number of points. Hence if C_1, C_2 are isogenous curves and ω_j is a differential of the first kind on C_j ($j = 1, 2$) everything being defined over k, then

$$\mu_\mathfrak{p}(\omega_1, \mathfrak{G}_{1\mathfrak{p}}) = \mu_\mathfrak{p}(\omega_2, \mathfrak{G}_{2\mathfrak{p}}) \tag{1.21}$$

[3]) "Almost all" means "with only a finite number of exceptions". If C is in Weierstrass Normal form (1.13) and $\omega = y^{-1}dx$ then the stated result holds for all nonarchimedean $\mathfrak{p}$ for which there is a good reduction and 2 is a unit.

for almost all $\mathfrak{p}$, in an obvious notation. In particular, the product

$$T(C_2/C_1) = \prod_{\mathfrak{p}} \frac{\mu_{\mathfrak{p}}(\omega_1, \mathfrak{G}_{1\mathfrak{p}})}{\mu_{\mathfrak{p}}(\omega_2, \mathfrak{G}_{2\mathfrak{p}})} \tag{1.22}$$

is well-defined. By (1. 16) $T(C_2/C_1)$ depends only on C_1, C_2 and k, not on the choice of the differentials ω_j. By (1. 18) we have

$$T(C_2/C_1) = T(C_2)/T(C_1) \tag{1.23}$$

when (if ever) the right hand side is defined. In any case (1. 22) shows that $T(C_2/C_1)$ has the formal property

$$T(C_3/C_1) = T(C_3/C_2)\, T(C_2/C_1) \tag{1.24}$$

of a quotient for three isogenous varieties C_1, C_2, C_3.

The principal theorem of this paper is

Theorem 1. 1. Let

$$C_1 \xrightarrow{\nu_1} C_2, \quad C_2 \xrightarrow{\nu_2} C_1 \tag{1.25}$$

be conjugate isogenies defined over an algebraic numberfield k. Then

$$T(C_1/C_2) = \frac{|S^1|\,|(\mathfrak{G}_2)_{\nu_2}|}{|S^2|\,|(\mathfrak{G}_1)_{\nu_1}|} \tag{1.26}$$

where S^j are the Selmer groups of the isogenies ν_j $(j = 1, 2)$ and where (in accordance with our usual conventions) $|(\mathfrak{G}_j)_{\nu_j}|$ is the number of points defined over k in the kernel Δ_j of ν_j.

In order to relate this theorem to the the other Birch-Swinnerton-Dyer conjectures we shall need the following result which has independent interest.

Theorem 1. 2. *Let C_j, ν_j be as in Theorem 1. 1 and let l_j be the bilinear form on the corresponding Tate-Šafarevič group Ш_j $(j = 1, 2)$ whose existence was proved in Paper IV of this series. Then*

$$l_1(\xi_1, \nu_2\xi_2) = l_2(\nu_1\xi_1, \xi_2) \tag{1.27}$$

for

$$\xi_1 \in \text{Ш}_1, \quad \xi_2 \in \text{Ш}_2. \tag{1.28}$$

Theorem 1. 2 will be proved in Section 2 and the later Sections will be devoted to the proof of Theorem 1. 1. In the rest of this Introduction we shall deduce consequences of these two theorems. We shall need not Theorem 1. 2 itself but the

Corollary to Theorem 1. 2. *Let n be the degree of the isogenies ν_1, ν_2 and suppose that the only divisible element of Ш_1 whose order divides n is 0. Then the same is true for Ш_2; and l_2 sets $\text{Ш}_2/\nu_1\text{Ш}_1$ in duality with $(\text{Ш}_2)_{\nu_2}$.*

Proof. The first statement follows from the well known fact that

$$\begin{aligned} \nu_1\nu_2 &= n \cdot \text{identity on } C_2 \\ \nu_2\nu_1 &= n \cdot \text{identity on } C_1. \end{aligned} \tag{1.29}$$

The second is then an immediate consequence of the fact proved in Paper IV that l_2 is a duality on the torsion group Ш_2 modulo its divisible part.

As an almost immediate consequence of what precedes we have

Theorem 1. 3. *Suppose that either* $Ш_1$ *or* $Ш_2$ *is finite. Then so is the other and*

$$T(C_1/C_2) = \frac{|\mathfrak{G}_2/\nu_1\mathfrak{G}_1|}{|(\mathfrak{G}_1)_{\nu_1}|}\cdot\frac{|(\mathfrak{G}_2)_{\nu_2}|}{|\mathfrak{G}_1/\nu_2\mathfrak{G}_2|}\cdot\frac{|Ш_1|}{|Ш_2|}. \tag{1. 30}$$

Proof. We have the exact sequence

$$0 \longrightarrow (Ш_1)_{\nu_1} \longrightarrow Ш_1 \xrightarrow{\nu_1} Ш_2 \longrightarrow Ш_2/\nu_1 Ш_1 \longrightarrow 0. \tag{1. 31}$$

By Theorem 1. 2 Corollary we have

$$|Ш_2/\nu_1Ш_1| = |(Ш_2)_{\nu_2}| \tag{1. 32}$$

and so, since $(Ш_1)_{\nu_1}$ and $(Ш_2)_{\nu_2}$ are finite, if one of $Ш_1$, $Ш_2$ is finite so is the other and

$$\frac{|Ш_1|}{|Ш_2|} = \frac{|(Ш_1)_{\nu_1}|}{|(Ш_2)_{\nu_2}|}. \tag{1. 33}$$

By the exact sequence (1. 7) we have

$$|S'| = |\mathfrak{G}_2/\nu_1\mathfrak{G}_1|\ |(Ш_1)_{\nu_1}| \tag{1. 34}$$

Theorem 1. 3 now follows at once from (1. 26), (1. 33) and (1. 34) and the analogue of (1. 34) for S^2.

Corollary to Theorem 1. 3. *Suppose, further, that one of* $\mathfrak{G}_1$, $\mathfrak{G}_2$ *is finite. Then so is the other and*

$$T(C_1/C_2) = \frac{|\mathfrak{G}_2|^2\,|Ш_1|}{|\mathfrak{G}_1|^2\,|Ш_2|}. \tag{1. 35}$$

This is, of course, in agrement with the Birch-Swinnerton-Dyer conjecture (1. 19) in view of the heuristic equality (1. 23). For the proof it is enough to note that the exact sequence

$$0 \longrightarrow (\mathfrak{G}_1)_{\nu_1} \longrightarrow \mathfrak{G}_1 \xrightarrow{\nu_1} \mathfrak{G}_2 \longrightarrow \mathfrak{G}_2/\nu_1\mathfrak{G}_1 \longrightarrow 0 \tag{1. 36}$$

implies that

$$\frac{|\mathfrak{G}_1|}{|\mathfrak{G}_2|} = \frac{|(\mathfrak{G}_1)_{\nu_1}|}{|\mathfrak{G}_2/\nu_1\mathfrak{G}_1|}. \tag{1. 37}$$

Now (1. 35) follows from (1. 30), (1. 37) and the corresponding inequality in which 1 and 2 are interchanged.

Although it is widely conjectured, the finiteness of the Tate-Šafarevič group has never been proved even for any single curve. On the other hand the q-primary component for any prime q is finite it there are no divisible elements of order q, since $Ш/qШ$ is trivially finite. The non-existence of such divisible elements has been checked in a large number of cases. Consequently the hypotheses of Theorem 1. 3 have never been checked in any individual case while the hypotheses of the following rather more complicated variant are known to hold in many cases.

Theorem 1. 4. *Let* $Ш_j^{(n)}$ *denote the subgroup of* $Ш_j$ *the orders of whose elements divide some power of the degree* n *of the* v_j $(j = 1, 2)$. *If one of the* $Ш_j^{(n)}$ *is finite then so is the other and*

$$T(C_1/C_2) = \frac{|\mathfrak{G}_2/\nu_1\mathfrak{G}_1|}{|(\mathfrak{G}_1)_{\nu_1}|}\cdot\frac{|(\mathfrak{G}_2)_{\nu_2}|}{|\mathfrak{G}_1/\nu_2\mathfrak{G}_2|}\cdot\frac{|Ш_1^{(n)}|}{|Ш_2^{(n)}|}. \tag{1. 38}$$

For (1. 29) *shows that the* ν_j *are isomorphisms of the parts of the* $Ш_j$ *whose order is prime to* n. *The proof of Theorem* 1. 4 *is then completely analogous to that of Theorem* 1. 3.

Birch pointed out to me that Theorem 1. 4 implies

Theorem 1. 5. *Suppose that the hypotheses of Theorem* 1. 4 *hold and let*

$$g = \text{rank } \mathfrak{G}_j \qquad (j = 1, 2) \tag{1. 39}$$

(*i. e. the number of generators of infinite order*). *Then*

$$n^g T(C_1/C_2) = \text{square.} \tag{1. 40}$$

Note. Of course the ranks of $\mathfrak{G}_1$ and $\mathfrak{G}_2$ are the same. Theorem 1. 5 can be of practical use in estimating g because $T(C_1/C_2)$ is quite easy to compute. The estimate depends on the hypothesis that the $Ш_j$ contains no divisible elements of order dividing n, but it is conjectured that this is always true.

Proof. Let $\mathfrak{F}_j$ be the subgroup of $\mathfrak{G}_j$ consisting of elements of finite order. Then $\mathfrak{F}_j$ is a finite group by the Mordell-Weil theorem and there is an exact sequence

$$0 \to \mathfrak{F}_j \to \mathfrak{G}_j \to \mathfrak{H}_j \to 0, \tag{1. 41}$$

where $\mathfrak{H}_j$ is a free group on g generators. Then ν_1 induces a term-by-term map of the exact sequence (1. 41) with $j = 1$ into the corresponding exact sequence with $j = 2$ and so

$$\frac{|\mathfrak{G}_2/\nu_1\mathfrak{G}_1|}{|(\mathfrak{G}_1)_{\nu_1}|} = \frac{|\mathfrak{F}_2/\nu_1\mathfrak{F}_1|}{|(\mathfrak{F}_1)_{\nu_1}|} \cdot \frac{|\mathfrak{H}_2/\nu_1\mathfrak{H}_1|}{|(\mathfrak{H}_1)_{\nu_1}|}. \tag{1. 42}$$

Since the $\mathfrak{F}_j$ are finite groups we have

$$\frac{|\mathfrak{F}_2/\nu_1\mathfrak{F}_1|}{|(\mathfrak{F}_1)_{\nu_1}|} = \frac{|\mathfrak{F}_2|}{|\mathfrak{F}_1|}, \tag{1. 43}$$

and since the $\mathfrak{H}_j$ are free we have

$$|(\mathfrak{H}_1)_{\nu_1}| = 1 \tag{1. 44}$$

From (1. 38), (1. 42), (1. 43), (1. 44) and the corresponding equations with 1 and 2 interchanged we have

$$T(C_1/C_2) = \frac{|\mathfrak{H}_2/\nu_1\mathfrak{H}_1|}{|\mathfrak{H}_1/\nu_2\mathfrak{H}_2|} \cdot \frac{|\mathfrak{F}_2|^2}{|\mathfrak{F}_1|^2} \cdot \frac{|Ш_1^{(n)}|}{|Ш_2^{(n)}|}. \tag{1. 45}$$

By (1. 29) we have

$$|\mathfrak{H}_2/\nu_1\mathfrak{H}_1| \cdot |\mathfrak{H}_1/\nu_2\mathfrak{H}_2| = n^g \tag{1. 46}$$

since the $\mathfrak{H}_j$ are free on g generators. Finally, because the skew-symmetric form l defined in Paper IV of the series is skew-symmetric we have

$$|Ш_j^{(n)}| = \text{square} \qquad (j = 1, 2). \tag{1. 47}$$

The truth of Theorem 1. 5 is an immediate consequence of (1. 45), (1. 46) and (1. 47).

2. The behaviour of Ш under isogenies

Let

$$C_1 \xrightarrow{\nu_1} C_2, \quad C_2 \xrightarrow{\nu_2} C_1 \tag{2.1}$$

be a pair of conjugate isogenies of abelian varietes of dimension 1 over an algebraic numberfield k and let $Ш_j$ be the Tate-Šafarevič group of $C_j (j = 1, 2)$. In this section we prove Theorem 1. 2, i. e. we show that

$$l_1(\nu_2 \xi, \eta) = l_2(\xi, \nu_1 \eta) \tag{2.2}$$

for

$$\xi \in Ш_2, \quad \eta \in Ш_1 \tag{2.3}$$

where we have put ξ, η instead of the ξ_2, ξ_1 of the enunciation so as to make the notation agree more closely with that of Paper IV. The proof is, in fact, an almost immediate consequence of the construction of the l-pairing on page 101 of Paper IV.

As in Paper IV let $\mathcal{D}_2$ be a curve of genus 1 defined over k realizing $\xi \in Ш_2$ so that there is a map[4])

$$\mathcal{D}_2 \times \mathcal{D}_2 \xrightarrow{\lambda_2} C_2 \tag{2.4}$$

making C_2 the jacobian of $\mathcal{D}_2$. The isogeny ν_2 induces a map

$$\mathcal{D}_2 \xrightarrow{\vartheta} \mathcal{D}_1 \tag{2.5}$$

into a curve $\mathcal{D}_1$ which has C_1 as its jacobian and corresponds to to the element $\nu_2 \xi$ of $Ш_1$, and there is a commutative diagram

$$\begin{array}{ccc} \mathcal{D}_2 \times \mathcal{D}_2 & \xrightarrow{\lambda_2} & C_2 \\ \downarrow{\scriptstyle \vartheta \times \vartheta} & & \downarrow{\scriptstyle \nu_2} \\ \mathcal{D}_1 \times \mathcal{D}_1 & \xrightarrow{\lambda_1} & C_1 \end{array} \tag{2.6}$$

where λ_1 corresponds to $\nu_2 \xi$ as λ_2 does to ξ. All the foregoing is obvious from the definitions.

Now, again as in Paper IV, let $\mathfrak{a}_\sigma (\sigma \in \Gamma, \mathfrak{a}_\sigma \in \overline{\mathfrak{G}}_1)$ be a cocycle for η and let $\mathfrak{A}_\sigma$ be a divisor on $\mathcal{D}_1$ of degree 0 mapped into $\mathfrak{a}_\sigma$ by the jacobian map λ_1. Then, as in Paper IV, $\sigma \mathfrak{A}_{\sigma^{-1}\tau} - \mathfrak{A}_\tau + \mathfrak{A}_\sigma$ is the divisor of a function, say $f_{\sigma,\tau}(X_1)$, where X_1 is a generic point on $\mathcal{D}_1$

We now define functions $f'_{\sigma,\tau}$ on $\mathcal{D}_2$ by

$$f'_{\sigma,\tau}(\mathfrak{X}_2) = f_{\sigma,\tau}(\vartheta \mathfrak{X}_2), \tag{2.7}$$

where $\mathfrak{X}_2$ is a generic point on $\mathcal{D}_2$. The divisor of $f'_{\sigma,\tau}$ is clearly $\vartheta^{-1}\{\sigma \mathfrak{A}_{\sigma^{-1}\tau} - \mathfrak{A}_\tau + \mathfrak{A}_\sigma\}$ and by the definition of conjugate isogenies (cf. Introduction) and the commutativity of (2. 6) this in mapped onto $\nu_1(\sigma \mathfrak{a}_{\sigma^{-1}\tau} - \mathfrak{a}_\tau + \mathfrak{a}_\sigma)$ by the Jacobian map λ_2. Thus the $f'_{\sigma,\tau}$ are just the functions on $\mathcal{D}_2$ which are needed to construct $l_2(\xi, \nu_1 \eta)$.

By the definition of the Tate-Šafarevič group, for every valuation $\mathfrak{p}$ of k there is a point on $\mathcal{D}_2$ defined over $k_\mathfrak{p}$. Then

$$\mathfrak{B}_{1\mathfrak{p}} = \vartheta \mathfrak{B}_{2\mathfrak{p}} \tag{2.8}$$

---

[4]) Designated by ν in Paper IV.

is defined over k also and

$$f_{\sigma,\tau}(\mathfrak{B}_{1\mathfrak{p}}) = f'_{\sigma,\tau}(\mathfrak{B}_{2\mathfrak{p}}) \tag{2.9}$$

by (2. 7). Since the left and right hand sides of (2. 2) are defined in terms of the left and right hand sides of (2. 9) respectively, the truth of (2. 2) follows.

3. Expression of $T(C_2/C_1)$ as a local product

In this section we prove

Lemma 3. 1. *Under the hypotheses of Theorem* 1. 1 *we have*

$$T(C_2/C_1) = \prod_{\mathfrak{p}} \frac{|(\mathfrak{G}_{1\mathfrak{p}})_{\nu_1}|}{|(WC_{2\mathfrak{p}})_{\nu_2}|} \tag{3.1}$$

where all but a finite number of factors are 1.

Let ω_2 be any differential of the first kind on C_2 defined over k and put

$$\omega_1 = \nu_1^{-1}\omega_2, \tag{3.2}$$

so that ω_1 is a differential of the first kind on C_1 defined over k. For each $\mathfrak{p}$, as in the Introduction, we use ω_1 and ω_2 to normalise the Haar measure on $\mathfrak{G}_{1\mathfrak{p}}$ and $\mathfrak{G}_{2\mathfrak{p}}$ respectively. The map ν_1 is locally $1 - 1$ on $\mathfrak{G}_{1\mathfrak{p}}$ and by (3. 2) the corresponding Haar measures are so normalized that

$$\mu_{\mathfrak{p}}(\omega_1, E) = \mu_{\mathfrak{p}}(\omega_2, \nu_1 E) \tag{3.3}$$

or any set $E < \mathfrak{G}_{1\mathfrak{p}}$ which is mapped $1 - 1$ into $\mathfrak{G}_{2\mathfrak{p}}$. Hence

$$\frac{\mu_{\mathfrak{p}}(\omega_1, \mathfrak{G}_{1\mathfrak{p}})}{\mu_{\mathfrak{p}}(\omega_2, \mathfrak{G}_{2\mathfrak{p}})} = \frac{|(\mathfrak{G}_{1\mathfrak{p}})_{\nu_1}|}{|\mathfrak{G}_{2\mathfrak{p}}/\nu_1\mathfrak{G}_{1\mathfrak{p}}|}. \tag{3.4}$$

But now, by Tate's local duality $WC_{\mathfrak{p}}$ is dual to $\mathfrak{G}_{\mathfrak{p}}/\mathfrak{U}_{\mathfrak{p}}$ where $\mathfrak{U}_{\mathfrak{p}}$ is the connected (i. e. the divisible) component of $\mathfrak{G}_{\mathfrak{p}}$. In an obvious notation there is an isomorphism

$$\mathfrak{G}_{2\mathfrak{p}}/\nu_1\mathfrak{G}_{1\mathfrak{p}} \cong (\mathfrak{G}_{2\mathfrak{p}}/\mathfrak{U}_{2\mathfrak{p}})/\nu_1(\mathfrak{G}_{1\mathfrak{p}}/\mathfrak{U}_{1\mathfrak{p}}), \tag{3.5}$$

and so the finite group $\mathfrak{G}_{2\mathfrak{p}}/\nu_1\mathfrak{G}_{1\mathfrak{p}}$ is dual to $|(WC_{2\mathfrak{p}})_{\nu_2}|$. Hence

$$|\mathfrak{G}_{2\mathfrak{p}}/\nu_1\mathfrak{G}_{1\mathfrak{p}}| = |(WC_{2\mathfrak{p}})_{\nu_2}|. \tag{3.6}$$

Lemma 3. 1 now follows at once from (3. 4), (3. 6), the definition (1. 22) of $T(C_2/C_1)$, and the fact that (1. 21) holds for almost all $\mathfrak{p}$.

4. Characterization of unramified element of $H^1(\Gamma_{\mathfrak{p}}, \Delta_1)$

The following Lemma may have independent interest. I should not be surprised to learn that it is already in the literature but have been unable to find it (but cf. e. g. Lang-Tate [6]).

Lemma 4. 1. *Let $k_{\mathfrak{p}}$ be a local field, where $\mathfrak{p}$ is nonarchimedean with finite residue class field. Let C_1 be an abelian variety of dimension* 1 *defined over $k_{\mathfrak{p}}$ and with a "good reduction" modulo $\mathfrak{p}$. Let*

$$C_1 \xrightarrow{\nu_1} C_2 \tag{4.1}$$

be an isogeny defined over $k_{\mathfrak{p}}$ whose degree n is prime to $\mathfrak{p}$, and with kernel Δ_1. Then the image of $\mathfrak{G}_{2\mathfrak{p}} / \nu_1 \mathfrak{G}_{1\mathfrak{p}}$ in the corresponding exact sequence

$$(4.2) \qquad 0 \to \mathfrak{G}_{2\mathfrak{p}} / \nu_1 \mathfrak{G}_{1\mathfrak{p}} \to H^1(\Gamma_{\mathfrak{p}}, \Delta_1) \to (WC_{1\mathfrak{p}})_{\nu_1} \to 0$$

consists of precisely the unramified elements of $H^1(\Gamma_{\mathfrak{p}}, \Delta_1)$.

Let $\varkappa$ be the residue class field of $k_{\mathfrak{p}}$ and let $\bar{\varkappa}$ be its separable closure. Let $\mathfrak{g}_1$ and $\bar{\mathfrak{g}}_1$ be the points of C_1' defined over $\varkappa$ and $\bar{\varkappa}$ respectively. Under the conditions of the theorem the points of the reduction δ_1 of Δ_1 are in $\bar{\mathfrak{g}}$ and there is a separable isogeny

$$(4.3) \qquad C_1' \xrightarrow{\nu_1'} C_2'$$

with kernel δ_1 defined over $\varkappa$ such that C_2' is a good reduction of C_2 and the diagram

$$(4.4) \qquad \begin{array}{ccc} C_1 & \xrightarrow{\nu_1} & C_2 \\ \downarrow & & \downarrow \\ C_1' & \xrightarrow{\nu_1'} & C_2' \end{array}$$

is commutative.

But now, by an old theorem of F. K. Schmidt [11] (cf. Lang [5]), every elliptic curve defined over a finite field has a point on it defined over the field, and so

$$(4.5) \qquad H^1(\Gamma_s, \bar{\mathfrak{g}}_j) = 0 \qquad (j = 1, 2)$$

where Γ_s is the galois group of $\bar{\varkappa} / \varkappa$. Hence

$$(4.6) \qquad \mathfrak{g}_2 / \nu_1 \mathfrak{g}_1 \cong H^1(\Gamma_s, \delta_1)$$

by the exact cohomology sequence associated with the exact sequence

$$(4.7) \qquad 0 \longrightarrow \delta_1 \longrightarrow \bar{\mathfrak{g}}_1 \xrightarrow{\nu_1'} \bar{\mathfrak{g}} \longrightarrow 0.$$

But now, by Hensel's Lemma the maps

$$(4.8) \qquad \mathfrak{G}_j \to \mathfrak{g}_j \qquad (j = 1, 2)$$

are both surjections and

$$(4.9) \qquad \operatorname{Ker} \{\mathfrak{G}_2 \to \mathfrak{g}_2\} < \nu_1 \mathfrak{G}_1$$

because ν_1' is separable. Hence there is an isomorphism

$$(4.10) \qquad \mathfrak{G}_2 / \nu_1 \mathfrak{G}_1 \cong \mathfrak{g}_2 / \nu_1' \mathfrak{g}_1.$$

The required result now follows from (4. 6) and (4. 10) because $H^1(\Gamma_s, \delta_1)$ is isomorphic to the separable part of $H^1(\Gamma, \Delta_1)$ and the various isomorphisms clearly commute with one another.

5. A reduction step

In this section we prove

Lemma 5. 1. *Suppose that Theorem 1. 1 is true for all isogenies of prime degree. Then it is universally true.*

We may write the assertion of Theorem 1. 1 in the shape

$$(5.1) \qquad T(C_1/C_2) = T^*(C_1/C_2)$$

where $T^*(C_1/C_2)$ is the right hand side of (1. 26) and so, by (1. 34)

$$(5.2) \qquad T^*(C_1/C_2) = \frac{|\mathfrak{G}_2/\nu_1\mathfrak{G}_1| \cdot |(\mathfrak{G}_2)_{\nu_2}| \cdot |(\text{Ш}_1)_{\nu_1}|}{|\mathfrak{G}_1/\nu_2\mathfrak{G}_2| \cdot |(\mathfrak{G}_1)_{\nu_1}| \cdot |(\text{Ш}_2)_{\nu_2}|}.$$

The assertion (5. 1) is certainly true when ν_1 is multiplication by a natural number, since then $C_1 = C_2$, $\nu_1 = \nu_2$ and trivially both sides are unity. It is well-known (and easy to see) that every isogeny can be expressed in the form

$$\nu_1 = \nu^{(1)} \nu^{(2)} \cdots \nu^{(r)} \tag{5. 3}$$

where the isogenies $\nu^{(j)}$ are defined over k and either of prime degree or are multiplications by natural numbers.

We have already seen (equation 1. 23) that

$$T(C_1/C_3) = T(C_1/C_2)\, T(C_2/C_3). \tag{5. 4}$$

To prove Lemma 5. 1 it will thus be enough to show that

$$T^*(C_1/C_3) = T^*(C_1/C_2)\, T^*(C_2/C_3) \tag{5. 5}$$

in an obvious notation, where

$$\begin{tikzcd} & C_2 \arrow[dr, "\beta_1"] & \\ C_1 \arrow[ur, "\alpha_1"] \arrow[rr, "\gamma_1"'] & & C_3 \end{tikzcd} \tag{5. 6}$$

is a commutative triangle of isogenies and

$$\begin{tikzcd} & C_2 \arrow[dl, "\alpha_2"'] & \\ C_1 & & C_3 \arrow[ul, "\beta_2"'] \arrow[ll, "\gamma_2"] \end{tikzcd} \tag{5. 7}$$

is the conjugate triangle.

The diagram (5. 6) gives a commutative triangle

$$\begin{tikzcd} & \mathfrak{G}_2 \arrow[dr, "\beta_1"] & \\ \mathfrak{G}_1 \arrow[ur, "\alpha_1"] \arrow[rr, "\gamma_1"'] & & \mathfrak{G}_3 \end{tikzcd} \tag{5. 8}$$

of commutative groups and so

$$\frac{|\mathfrak{G}_3/\gamma_1\mathfrak{G}_1|}{|(\mathfrak{G}_1)_{\gamma_1}|} = \frac{|\mathfrak{G}_3/\beta_1\mathfrak{G}_2|}{|(\mathfrak{G}_2)_{\beta_1}|} \cdot \frac{|\mathfrak{G}_2/\alpha_1\mathfrak{G}_1|}{|(\mathfrak{G}_1)_{\alpha_1}|} \tag{5. 9}$$

as is readily verified. Similarly we have

$$\frac{|Ш_3/\gamma_1 Ш_1|}{|(Ш_1)_{\gamma_1}|} = \frac{|Ш_3/\beta_1 Ш_2|}{|(Ш_2)_{\beta_1}|} \cdot \frac{|Ш_2/\alpha_1 Ш_1|}{|(Ш_2)_{\alpha_1}|} \tag{5. 10}$$

and so

$$\frac{|(Ш_3)_{\gamma_2}|}{|(Ш_1)_{\gamma_1}|} = \frac{|(Ш_3)_{\beta_2}|}{|(Ш_2)_{\beta_1}|} \cdot \frac{|(Ш_2)_{\alpha_2}|}{|(Ш_1)_{\alpha_1}|} \tag{5. 11}$$

by (1. 32). The required equation (5. 5) now follows from (5. 2), (5. 9), (5. 11) and the equation similar to (5. 9) obtained from (5. 7) instead of (5. 6).

6. Some counting

We shall later need the following

Lemma 6. 1. *Let Γ be the galois group of $\bar{k}/k$, where $\bar{k}$ is the algebraic closure of the algebraic numberfield k and let M be a Γ-module of prime order q. Denote by q^η, q^ε respectively the number of elements of M and of*

(6. 1) $$M^* = \operatorname{Hom}(M, \Omega)$$

which are fixed under Γ, where $\Omega < \bar{k}^*$ is the group of q-th roots of unity and Γ acts on M^* in the usual way. Let Π be a finite set of valuations of k which includes all the non-archimedean ones and denote by $H^1_\Pi(\Gamma, M)$ the group of elements of $H^1(\Gamma, M)$ which do not ramify outside Π. Then

(6. 2) $$| H^1_\Pi(\Gamma, M) | = q^{P+\eta-\varepsilon}$$

where P is the number of $\mathfrak{p} \in \Pi$ such that the splitting field[5] $\Gamma_\mathfrak{p}$ acts trivially on M^*, provided that the set Π is large enough in the following sense:

(i) *Π contains all $\mathfrak{p}$ such that $|q|_\mathfrak{p} \neq 1$.*

(ii) *Let $\Gamma' < \Gamma$ be the subgroup which leaves M^* elementwise fixed and let K be the corresponding algebraic extension of k. Then every divisor class (i. e. ideal class) of K contains a prime divisor $\mathfrak{P}$ which is the extension to K of one of the $\mathfrak{p} \in \Pi$.*

Let

(6. 3) $$\gamma = \Gamma/\Gamma'$$

be the quotient group and let σ be a generator of γ fixed in all that follows. We define an integer g modulo q by

(6. 4) $$\sigma m^* = g m^*.$$

Clearly the order of g in the multiplicative group of integers mod q is the order of γ. (All this makes sense also when $\Gamma' = \Gamma$, so $g \equiv 1 \pmod{q}$).

It is convenient to enunciate two preliminary results as lemmas.

Lemma 6. 2. *Γ acts trivially on M if and only if $\Omega < K$ and*

(6. 5) $$\sigma\omega = g\omega \qquad (\omega \in \Omega).$$

Proof. Let m_0^* be a generator of M^*. It induces a Γ'-isomorphism

(6. 6) $$M \xrightarrow{m_0^*} \Omega$$

so that, in particular, Γ' acts trivially on M precisely when $\Omega < K$. If this is so, we can regard M, M^* and Ω as γ modules. Applying σ to (6. 6) and remembering (6. 4) we have

(6. 7) $$\sigma(m_0^*(m)) = (\sigma m_0^*)(\sigma m) = g m_0^*(\sigma m).$$

Hence $\sigma m = m$ for all $m \in M$ if and only if (6. 5) holds, because $m^*(m)$ runs through Ω when m runs through M.

Lemma 6. 3. *There is a canonical isomorphism*

(6. 8) $$H^1(\Gamma, M) \cong L/(K^*)^q$$

where L consists of those elements $\alpha \in K^*$ such that

(6. 9) $$\alpha^{\sigma-g} \in (K^*)^q.$$

[5]) $\Gamma_\mathfrak{p}$ is, of course, defined only up to an inner automorphism as a subgroup of Γ, but that does not affect the definition of P.

Proof. The Γ'-isomorphism (6.6) induces the isomorphism

$$H^1(\Gamma', M) \xrightarrow{m_0^*} H^1(\Gamma', \Omega). \tag{6.10}$$

There is the well-known canonical isomorphism

$$H^1(\Gamma', \Omega) \xrightarrow{\iota} K^*/(K^*)^q \tag{6.11}$$

arising from the cohomology sequence of the exact sequence

$$0 \longrightarrow \Omega \longrightarrow \bar{K}^* \xrightarrow{q} \bar{K}^* \longrightarrow 0. \tag{6.12}$$

Let $(H^1(\Gamma', M))^\gamma$ denote the subgroup of $H^1(\Gamma', M)$ left invariant by γ. Then

$$H^1(\Gamma, M) \cong (H^1(\Gamma', M))^\gamma \tag{6.13}$$

by the Hochschild-Serre exact sequence [4]

$$0 \to H^1(\gamma, M') \to H^1(\Gamma, M) \to (H^1(\Gamma', M))^\gamma \to H^2(\gamma, M'), \tag{6.14}$$

where M' is the portion of M left invariant by Γ' and since M' has trivial cohomology for γ, the orders being coprime. Let

$$\xi \in H^1(\Gamma', M). \tag{6.15}$$

Then, as in the proof of Lemma 6.2 we have $\xi \in (H^1(\Gamma', M))^\gamma$ i. e. $\sigma\xi = \xi$ precisely when

$$\sigma(m_0^*(\xi)) = g m_0^*(\xi), \tag{6.16}$$

and so, since ι in (6.11) is canonical, precisely when

$$\sigma\eta = g\eta \tag{6.17}$$

where

$$\eta = \iota m_0(\xi) \in K^*/(K^*)^q. \tag{6.18}$$

Since (6.10) and (6.11) are bijections, this completes the proof of the Lemma on recollecting the definition (6.9) of L.

Corollary. *Under the conditions at the end of the enunciation of Lemma* 6.1 *there is an isomorphism*

$$H^1_\Pi(\Gamma, M) \cong L_\Pi / K_\Pi^q \tag{6.19}$$

where K_Π consists of the elements of K^* which are units outside of Π and where $L_\Pi < K_\Pi$ consists of those α such that

$$\alpha^{\sigma - g} \in K_\Pi^q. \tag{6.20}$$

Proof. For we can make the isomorphism of Lemma 6.3 explicit. Let m_0 be a generator of M and put

$$\omega_0 = m_0^*(m), \tag{6.21}$$

so that ω_0 is a generator of Ω. Let $\alpha \in L$ and take $\beta \in \bar{K}^*$ so that $\beta^q = \alpha$. Then α corresponds to the element of $H^1(\Gamma, M)$ given by the cocycle

$$\tau \to n(\tau)\, m_0 \qquad (\tau \in \Gamma) \tag{6.22}$$

where $n(\tau)$ is given by

$$\beta^{\tau - 1} = \omega_0^{n(\tau)}. \tag{6.23}$$

Under condition (i) of Lemma 6. 1, this element of $H^1(\Gamma, M)$ is unramified outside Π precisely when α is a q-th power outside Π. By condition (ii) of Lemma 6. 1 this is so precisely when $\alpha = \alpha_0 \alpha_1^q$, $\alpha_0 \in L_\Pi$, $\alpha_1 \in K^*$: and this completes the proof of the Corollary.

After Lemma 6. 3 it will be enough to show that the order of L_Π / K_Π^q is given by (6. 2).

It is convenient to complete K_Π (multiplicatively) with respect to the q-adic topology, i. e. to consider

$$\widetilde{K}_\Pi = \varprojlim_n K_\Pi / K_\Pi^{q^n} \tag{6. 24}$$

and

$$\widetilde{L}_\Pi = \varprojlim_n L_\Pi / K_\Pi^{q^n} < \widetilde{K}_\Pi. \tag{6. 25}$$

Clearly

$$| L_\Pi / K_\Pi^q | = | \widetilde{L}_\Pi / \widetilde{K}_\Pi^q | . \tag{6. 26}$$

We can regard $\widetilde{K}_\Pi$ and $\widetilde{L}_\Pi$ as $\boldsymbol{Z}_q$-modules, where $\boldsymbol{Z}_q$ is the ring of q-adic integers. The number g in (6. 4) is defined only modulo q and it is convenient to take it as the q-adic integer which satisfies the equation

$$g^u = 1 - q, \tag{6. 27}$$

where u is the order of γ, and for which (6. 4) is true in an obvious sense.

We define an element ϑ of the group ring $\boldsymbol{Z}_q[\gamma]$ by

$$\vartheta = \begin{cases} \sigma^{u-1} + g\sigma^{u-2} + \cdots + g^{u-1} & (u \neq 1), \\ 1 & (u = 1), \end{cases} \tag{6. 28}$$

so

$$(\sigma - g)\, \vartheta = \sigma^u - g^u = 1 - g^u = q. \tag{6. 29}$$

Hence

$$\widetilde{L}_\Pi = (\widetilde{K}_\Pi)^\vartheta, \tag{6. 30}$$

and so

$$| \widetilde{L}_\Pi | \widetilde{K}_\Pi^q | = \frac{| \widetilde{K}_\Pi / \widetilde{K}_\Pi^q |}{| \widetilde{K}_\Pi / \widetilde{K}_\Pi^\vartheta |}. \tag{6. 31}$$

We compute these indexes in the traditional way by considering a subgroup of $\widetilde{K}_\Pi$ of finite index. Let S denote the set of infinite valuations of K and let Π' denote the set of valuations of K which extend those of Π on k, so $S < \Pi'$. Then it is well-known and easy to verify that K_Π has a subgroup N of finite index with generators $\alpha_{\mathfrak{P}} \in K_\Pi$ ($\mathfrak{P} \in \Pi'$) such that

(i)

$$\tau \alpha_{\mathfrak{P}} = \alpha_{\tau\mathfrak{P}} \quad (\tau \in \Gamma). \tag{6. 32}$$

(ii) If $\mathfrak{P} \in S$ then $| \alpha_{\mathfrak{P}} |_{\mathfrak{P}} < 1$, $| \alpha_{\mathfrak{P}} |_{\mathfrak{Q}} > 1$ for $\mathfrak{Q} \in S$, $\mathfrak{Q} \neq \mathfrak{P}$ and $| \alpha_{\mathfrak{P}} |_{\mathfrak{Q}} = 1$ for $\mathfrak{Q} \notin S$.

(iii) If $\mathfrak{P} \in \Pi' - S$ then $| \alpha_{\mathfrak{P}} |_{\mathfrak{P}} < 1$ and $| \alpha_{\mathfrak{P}} |_{\mathfrak{Q}} = 1$ for $\mathfrak{Q} \neq \mathfrak{P}$, $\mathfrak{Q} \notin S$.

(iv) The only multiplicative relation between the $\alpha_{\mathfrak{P}}$ is

$$\prod_{\mathfrak{P} \in S} \alpha_{\mathfrak{P}} = 1. \tag{6. 33}$$

Then

$$\tilde{N} = \varprojlim_{n} N / K_{\Pi}^{q^n} \tag{6.34}$$

is of finite index in $\tilde{K}_{\Pi}$. Hence

$$\frac{|\tilde{K}_{\Pi} / \tilde{K}_{\Pi}^{q}|}{|(\tilde{K}_{\Pi})_q|} = \frac{|\tilde{N} / \tilde{N}^q|}{|(\tilde{N})_q|} \tag{6.35}$$

and

$$\frac{|\tilde{K}_{\Pi} / \tilde{K}_{\Pi}^{\vartheta}|}{|(K_{\Pi})_\vartheta|} = \frac{|\tilde{N} / \tilde{N}^\vartheta|}{|(\tilde{N})_\vartheta|} \tag{6.36}$$

where, in accordance with our usual convention, the subscript q or ϑ denotes the kernel.

Clearly

$$|(\tilde{N})_\vartheta| = |(\tilde{N})_q| = 1 \tag{6.37}$$

by (6. 29), and

$$|(\tilde{K}_{\Pi})_q| = \begin{cases} q & \text{if } \Omega \subset K \\ 1 & \text{otherwise.} \end{cases} \tag{6.38}$$

Further

$$(\tilde{K}_{\Pi})_\vartheta \subset (K_{\Pi})_q \tag{6.39}$$

by (6. 29), and so

$$|(K_{\Pi})_\vartheta| = \begin{cases} q & \text{if } \Omega \subset (\tilde{K}_{\Pi})_\vartheta \\ 1 & \text{otherwise.} \end{cases} \tag{6.40}$$

We must examine the condition in (6. 40) further. Suppose that $\Omega \subset K$. Then there is an integer h such that

$$\sigma\omega = h\omega \qquad (\omega \in \Omega) \tag{6.41}$$

and

$$h^u \equiv 1 \pmod{q} \tag{6.42}$$

where, as before, u is the order of γ. By (6. 28), (6. 40) and (6. 41) we have

$$\begin{aligned} (\Omega)_\vartheta &= \Omega \text{ if } h \equiv g \ (q), \\ (\Omega)_\vartheta &= 1 \ \text{ if } h \not\equiv g \ (q), \end{aligned} \tag{6.43}$$

since

$$h^{u-1} + h^{u-2}g + \cdots + g^{u-1} \equiv \begin{cases} ug^{u-1} \not\equiv 0 & \text{if } h \equiv g \\ 0 & \text{if } h \equiv g. \end{cases} \tag{6.44}$$

To sum up, by (6. 35), (6. 36) (6. 37) (6. 38), (6.40) and (6. 43) we have

$$|\tilde{K}_{\Pi}^{\vartheta} / \tilde{K}_{\Pi}^{q}| = q^\eta \, |\tilde{N}^\vartheta / \tilde{N}^q| \tag{6.45}$$

where, by Lemma 6. 2, η has the meaning given in the enunciation of Lemma 6. 1.

Now let $\tilde{P}$ be a free $\boldsymbol{Z}_q$-module on generators $\beta_{\mathfrak{P}}$ ($\mathfrak{P} \in \Pi'$) and made into a $\boldsymbol{Z}_q[\gamma]$-module by putting $\sigma\beta_{\mathfrak{P}} = \beta_{\sigma P}$. By the definition of $\tilde{N}$ there is an exact sequence

$$0 \longrightarrow \boldsymbol{Z}_q \xrightarrow{i} \tilde{P} \xrightarrow{p} \tilde{N} \longrightarrow 0 \tag{6.46}$$

of $\boldsymbol{Z}_q[\gamma]$-modules, where i maps 1 into $\sum_{\mathfrak{P} \in S} \beta_{\mathfrak{P}}$ and p maps $\beta_{\mathfrak{P}}$ into $\alpha_{\mathfrak{P}}$. Then

$$|\tilde{P}^{\vartheta}/\tilde{P}^{q}| = |\boldsymbol{Z}_q^{\vartheta}/q\boldsymbol{Z}_q|\,|\tilde{N}^{\vartheta}/\tilde{N}^{q}| \tag{6.47}$$

since all three modules in (6. 46) are torsion-free.

But now, by (6. 29), $\boldsymbol{Z}_q^{\vartheta}$ is just the set of elements of $\boldsymbol{Z}_q$ which are mapped into $q\boldsymbol{Z}_q$ by $\sigma - g$. Since γ acts trivially on $\boldsymbol{Z}_q$ we have

$$\boldsymbol{Z}_q^{\vartheta} = \begin{cases} \boldsymbol{Z}_q \text{ if } g \equiv 1 \ (q), \\ q\boldsymbol{Z}_q \text{ if } g \not\equiv 1 \ (q), \end{cases} \tag{6.48}$$

i. e.

$$|\boldsymbol{Z}_q^{\vartheta}/q\boldsymbol{Z}_q| = q^{\varepsilon} \tag{6.49}$$

where ε has the meaning given it in the enunciation of Lemma 6. 1.

Further $\tilde{P}$ is the direct sum, as a $\boldsymbol{Z}_q[\gamma]$-module, of modules $\tilde{P}_{\mathfrak{p}}$ $(\mathfrak{p} \in \Pi)$, where $\tilde{P}_{\mathfrak{p}}$ is generated by the $\beta_{\mathfrak{P}}$ $(\mathfrak{P}|\mathfrak{p})$. As before, $\tilde{P}_{\mathfrak{p}}^{\vartheta}$, consists of those $\beta \in \tilde{P}_{\mathfrak{p}}$ such that[6])

$$(\sigma - g)\,\beta \in q\tilde{\mathfrak{P}}_{\mathfrak{p}}. \tag{6.50}$$

Write

$$\beta = \sum_{\mathfrak{P}|\mathfrak{p}} h_{\mathfrak{P}}\beta_{\mathfrak{P}} \qquad (h_{\mathfrak{P}} \in \boldsymbol{Z}_q). \tag{6.51}$$

Then (6. 50) is equivalent to

$$h_{\sigma^{-1}\mathfrak{P}} \equiv g h_{\mathfrak{P}} \ (q). \tag{6.52}$$

Since the order of g modulo q is the same as the order of σ, this is equivalent to

$$h_{\mathfrak{P}} \equiv g h_{\sigma\mathfrak{P}} \equiv \cdots \equiv g^{u-1} h_{\sigma^{u-1}\mathfrak{P}} \ (q) \tag{6.53}$$

if $\mathfrak{P}, \ldots, \sigma^{u-1}\mathfrak{P}$ are distinct, and to

$$h_{\mathfrak{P}} \equiv 0 \ (q) \tag{6.54}$$

otherwise. Hence

$$|\tilde{P}_{\mathfrak{p}}^{\vartheta}/\tilde{P}_{\mathfrak{p}}^{q}| = \begin{cases} q \text{ if } \mathfrak{p} \text{ splits completely in } K/k, \\ 1 \text{ otherwise,} \end{cases} \tag{6.55}$$

and so

$$|\tilde{P}^{\vartheta}/\tilde{P}^{q}| = q^{P}, \tag{6.56}$$

where P has the meaning given to it in the enunciation of Lemma 6. 1. Finally the assertion (6. 2) of that Lemma follows from (6. 19), (6. 26), (6. 30), (6. 45), (6. 47), (6. 49) and (6. 56).

7. Completion of the proofs

After Lemma 5. 1 all that we need to do to complete the proof of Theorem 1. 1, and so of all the results enunciated in the Introduction is to prove the following

Lemma 7. 1. *Let*

$$C_1 \xrightarrow{\nu_1} C_2, \quad C_2 \xrightarrow{\nu_2} C_1 \tag{7.1}$$

[6]) We now write $\tilde{P}$ additively instead of multiplicatively as heretofore.

be conjugate isogenies of prime degree q defined over an algebraic numberfield k. Then

(7. 2)
$$T(C_1/C_2) = \frac{|S'|\;|(\mathfrak{G}_2)_{\nu_2}|}{|S^2|\;|(\mathfrak{G}_1)_{\nu_1}|}$$

where $T(C_1/C_2)$ is the Tamagawa Ratio and S^1, S^2 are the Selmer groups.

We shall require Lemma 6. 1 and it is convenient first to enunciate it in the form in which we shall actually use it:

Lemma 7. 2. *Suppose that the hypotheses of Lemma 7. 1 hold. Then there is a finite set Π_0 of valuations of k such that*

(7. 3)
$$|H^1_\Pi(\Gamma, \Delta_2)| = \frac{q^P\,|(\mathfrak{G}_2)_{\nu_2}|}{|(\mathfrak{G}_1)_{\nu_1}|}$$

for any finite set Π of valuations containing Π_0, where, as usual Δ_j is the kernel of ν_j $(j = 1, 2)$ and where P is the number of $\mathfrak{p} \in \Pi$ such that every point of Δ_1 is defined over $k_\mathfrak{p}$.

Proof. We put

(7. 4)
$$M = \Delta_2$$

in Lemma 6. 1. There is a wellknown[7]) pairing of Δ_1 and Δ_2 with values in Ω, so we may put

(7. 5)
$$M^* = \Delta_1.$$

Then

(7. 6)
$$q^\eta = |(\mathfrak{G}_2)_{\nu_2}|, \; q^\varepsilon = |(\mathfrak{G}_1)_{\nu_1}|$$

by the definitions in the enunciation of Lemma 6. 1, and so (7. 3) is just (6. 2).

We shall also need

Lemma 7. 3. *Under the conditions of Lemma 7. 1 there is a finite set of valuations Π_1 of k such that the obvious maps*

(7. 7)
$$H^1_\Pi(\Gamma, \Delta_j) \to \prod_{\mathfrak{p}\in\Pi} H^1(\Gamma_\mathfrak{p}, \Delta_j) \qquad (j = 1, 2)$$

are injections for any finite set Π of valuations containing Π_1.

Proof. Since Δ_1, Δ_2 have order q, the usual argument using the restriction map shows that if Lemma 7. 3 is true for a field $K > k$ of relative degree prime to q instead of k then it is true also for k. Hence we may suppose that Δ_1, Δ_2, Ω are all defined over k. Then if Π is large enough we have the isomorphisms

(7. 8)
$$H^1_\Pi(\Gamma, \Delta_j) \cong H^1_\Pi(\Gamma, \Omega) \cong k_\Pi/k^q_\Pi,$$

and

(7. 9)
$$H^1(\Gamma_\mathfrak{p}, \Delta_j) \cong H^1(\Gamma_\mathfrak{p}, \Omega) \cong k^*_\mathfrak{p}/(k^*_\mathfrak{p})^q.$$

But it is well-known that

(7. 10)
$$k_\Pi/k^q_\Pi \to \prod_{\mathfrak{p}\in\Pi} k^*_\mathfrak{p}/(k^*_\mathfrak{p})^q$$

for prime q is an injection if only the set Π is large enough.

---

[7]) For let $\mathfrak{b}_2 \in \Delta_1$. Then there is a $f(\mathfrak{x}) \in \bar{k}(\mathfrak{x})$, where $\mathfrak{x}$ is a generic point on C_1, whose divisor of poles is $\nu_1^{-1}\mathfrak{o}_2$ and divisor of zeros is $\nu_1^{-1}\mathfrak{b}_2$. Then

$$\frac{f(\mathfrak{x} + \mathfrak{b}_1)}{f(\mathfrak{x})} = \psi(\mathfrak{b}_1, \mathfrak{b}_2) \in \Omega$$

for $\mathfrak{b}_1 \in \Delta_1$. This is the required pairing. It can be shown, though that is irrelevant to our purpose, that under the hypotheses of Lemma 7.1 one gets the same pairing on interchanging the roles of the two curves.

We now revert to the proof of Lemma 7. 1 which resembles the proof of e. g. Theorem 7. 1 of Paper III of this series but requires an additional twist.

Let Π be a finite set of valuations of k which contains all the infinite valuations, all the valuations where either $\mathfrak{C}_1$ or $\mathfrak{C}_2$ or the isogenies ν_1, ν_2 have a bad reduction, and which is so large that the conclusions of Lemmas 7. 2 and 7. 3 apply. Let

(7. 11) $$\boldsymbol{I}_j = \prod_{\mathfrak{p}\in\Pi} H^1(\Gamma_\mathfrak{p}, \Delta_j) \qquad (j = 1, 2)$$

and let $\boldsymbol{L}_j$ be the image of $H^1_\Pi(\Gamma, \Delta_j)$ under the map (7. 7). Then

(7. 12) $$\boldsymbol{L}_j \cong H^1_\Pi(\Gamma, \Delta_j)$$

by Lemma 7. 3. Let

(7. 13) $$\boldsymbol{N}_j = \prod_{\mathfrak{p}\in\Pi} M^j_\mathfrak{p} < \boldsymbol{I}_j$$

where, as usual, $M^1_\mathfrak{p}$ resp. $M^2_\mathfrak{p}$ is the image of $\mathfrak{G}_{2\mathfrak{p}}/\nu_1\mathfrak{G}_{1\mathfrak{p}}$ resp. $\mathfrak{G}_{1\mathfrak{p}}/\nu_2\mathfrak{G}_{2\mathfrak{p}}$ in $H^1(\Gamma_\mathfrak{p}, \Delta_1)$ resp. $H^1(\Gamma_\mathfrak{p}, \Delta_2)$ (cf. e. g. (4. 2)). By Lemma 4. 1 and the definition of the S^j we have

(7. 14) $$S^i \cong \boldsymbol{L}_j \cap \boldsymbol{N}_j \qquad (j = 1, 2),$$

the isomorphism being that of (7. 12).

We now recall that the canonical pairing of Δ_1, Δ_2 with values in Ω gives rise to a duality

(7. 15) $$H^1(\Gamma_\mathfrak{p}, \Delta_1) \otimes H^1(\Gamma_\mathfrak{p}, \Delta_2) \to H^2(\Gamma_\mathfrak{p}, \Omega) \to \boldsymbol{Q}/\boldsymbol{Z},$$

say

(7. 16) $$\xi_\mathfrak{p} \otimes \eta_\mathfrak{p} \to \lambda_\mathfrak{p}(\xi_\mathfrak{p}, \eta_\mathfrak{p}) \in \boldsymbol{Q}/\boldsymbol{Z},$$

where the first map is a cup-product and the second[8]) is taking the "invariant". Further

(7. 17) $$\lambda_\mathfrak{p}(\xi_\mathfrak{p}, \eta_\mathfrak{p}) = 1 \ (\xi_\mathfrak{p} \in M^1_\mathfrak{p},\ \eta_\mathfrak{p} \in M^2_\mathfrak{p})$$

(Tate [12], [13] or e. g. Lemma 3. 1 of Paper III of this series).

We note that the existence of the duality (7. 15) implies that

(7. 18) $$| H^1(\Gamma_\mathfrak{p}, \Delta_1) | = | H^1(\Gamma_\mathfrak{p}, \Delta_2) |$$

and so

(7. 19) $$| \boldsymbol{I}_1 | = | \boldsymbol{I}_2 |.$$

We now define a duality between $\boldsymbol{I}_1$ and $\boldsymbol{I}_2$ by putting

(7. 20) $$\Lambda(\mathfrak{J}_1, \mathfrak{J}_2) = \sum_{\mathfrak{p}\in\Pi} \lambda_\mathfrak{p}(\xi_p, \eta_p)$$

where

(7. 21) $$\mathfrak{J}_1 = \{\xi_\mathfrak{p}\}_{\mathfrak{p}\in\Pi} \in \boldsymbol{I}_1,\ \mathfrak{J}_2 = \{\eta_\mathfrak{p}\}_{\mathfrak{p}\in\Pi} \in \boldsymbol{I}_2.$$

This is a duality because the (7. 16) are. Further

(7. 22) $$\Lambda(\mathfrak{J}_1, \mathfrak{J}_2) = 0 \qquad (\mathfrak{J}_j \in \boldsymbol{N}_j,\ j = 1, 2)$$

by (7. 17), and

(7. 23) $$\Lambda(\mathfrak{J}_1, \mathfrak{J}_2) = 0 \qquad (\mathfrak{J}_j \in \boldsymbol{L}_j,\ j = 1, 2)$$

because then the local cup-products in (7. 15) are the localizations of a global cup-product, and the sum of the local invariants of an element of the global $H^2(\Gamma, \Omega)$ is zero.

8) $\boldsymbol{Q}$, $\boldsymbol{Z}$ are the rationals and the rational integers respectively.

By (7. 22) and (7. 23) we have

$$\Lambda(\mathfrak{J}_1, \mathfrak{J}_2) = 0, \ \mathfrak{J}_1 \in \boldsymbol{N}_1 \cap \boldsymbol{L}_1, \ \mathfrak{J}_2 \in \boldsymbol{N}_2 \cup \boldsymbol{L}_2, \tag{7.24}$$

where $\boldsymbol{N}_2 \cup \boldsymbol{L}_2$ is the subgroup of $\boldsymbol{I}_2$ generated by $\boldsymbol{N}_2$ and $\boldsymbol{L}_2$, and so

$$| \boldsymbol{N}_1 \cap \boldsymbol{L}_1 | \ | \boldsymbol{N}_2 \cup \boldsymbol{L}_2 | \leqq | \boldsymbol{I}_1 | = | \boldsymbol{I}_2 | \tag{7.25}$$

because Λ is nondegenerate. But now

$$| \boldsymbol{N}_2 \cap \boldsymbol{L}_2 | \ | \boldsymbol{N}_2 \cup \boldsymbol{L}_2 | = | \boldsymbol{N}_2 | \ | \boldsymbol{L}_2 | \tag{7.26}$$

and so

$$\frac{| S^1 |}{| S^2 |} \leqq \frac{| \boldsymbol{I}_2 |}{| \boldsymbol{N}_2 | \boldsymbol{L}_2 |} \tag{7.27}$$

by (7. 14).

But now

$$\frac{| \boldsymbol{I}_2 |}{| \boldsymbol{N}_2 |} = \prod_{\mathfrak{p} \in \Pi} \frac{| H^1(\Gamma_{\mathfrak{p}}, \Delta_2) |}{M_{\mathfrak{p}}^2} = \prod_{\mathfrak{p} \in \Pi} | (WC_{2\mathfrak{p}})_{\nu_2} | \tag{7.28}$$

by the exactness of the sequence (4. 2) (or more precisely the one obtained from it by interchanging 1 and 2) and the definition of $M_{\mathfrak{p}}^2$. Also

$$| \boldsymbol{L}_2 | = | H_\Pi^1(\Gamma, \Delta_2) | = \frac{| (G_2)_{\nu_2} |}{| (G_1)_{\nu_1} |} \prod_{\mathfrak{p} \in \Pi} | (G_{1\mathfrak{p}})_{\nu_1} | \tag{7.29}$$

by Lemma 7. 2 because $| (G_{1\mathfrak{p}})_{\nu_1} |$ is 1 or q according as Δ_1 is defined elementwise over $k_{\mathfrak{p}}$ or not. Hence finally

$$\frac{| (\mathfrak{G}_1)_{\nu_1} | \ | S^2 |}{| (\mathfrak{G}_2)_{\nu_2} | \ | S^1 |} \geqq \prod_{\mathfrak{p} \in \Pi} \frac{| (G_{1\mathfrak{p}})_{\nu_1} |}{| (WC_{2\mathfrak{p}})_{\nu_2} |} \tag{7.30}$$

by (7. 27), (7. 28) and (7. 29).

By Lemma 3. 1 the right hand side of (7. 30) is precisely $T(C_2/C_1)$, at least if the set Π was initially chosen large enough. Since $T(C_2/C_1)\ T(C_1/C_2) = 1$, this shows that the left hand side of (7. 2) is greater than or equal to the right hand side. Similarly, on interchanging the indexes 1 and 2, the left hand side of (7. 2) is less than or equal to the right hand side. Hence (7. 2) holds. This concludes the proof of Lemma 7. 1 and so of Theorem 1. 1.

There is one little result which follows readily from the above arguments and which has not so far been mentioned:

Corollary to Lemma 7. 1. *Define* Ж^1 *by the exactness of the sequence*

$$(WC_1)_{\nu_1} \to \sum_{\mathfrak{p}} (WC_{1\mathfrak{p}})_{\nu_1} \to Ж^1 \to 0. \tag{7.31}$$

Then there is a natural duality between Ж^1 *and* S^2.

For this compare the reformulation of Theorem 7. 1 of Paper III given in Section 2 of Paper VII. Let Ж$^1_\Pi$ arise from $\sum_{\mathfrak{p} \in \Pi} (WC_{1\mathfrak{p}})_{\nu_1}$ in (7. 31). Then

$$Ж^1_\Pi \cong \boldsymbol{I}_2 / \boldsymbol{N}_2 \cup \boldsymbol{L}_2 \tag{7.32}$$

by the arguments leading to (7. 28). The proof of Lemma 7. 1 shows that there is, in fact, equality in (7. 30) and so also equality in (7. 26). Hence Λ sets up a duality between Ж$^1_\Pi$ and $S^2 \cong \boldsymbol{N}_2 \cap \boldsymbol{L}_2$. It follows that Ж$^1_\Pi$ is independent of Π if it is large enough, and so then Ж$^1_\Pi$ = Ж^1.

References

[1] *B. J. Birch* and *H. P. F. Swinnerton-Dyer*. Notes on elliptic curves. I. J. reine angew. Math. **212** (1963), 7—25. and subsequent papers, to appear.

[2] *J. W. S. Cassels*, Arithmetic on curves of genus 1. III. The Tate-Šafarevič and Selmer groups. Proc. London Math. Soc. (3) **12** (1962), 259—296. IV. Proof of the Hauptvermutung. J. reine angew. Math. **211** (1962), 95—112. VII. The dual exact sequence. J. reine angew. Math. **216** (1964), 150—158.

[3] *J. W. S. Cassels*, Arithmetic on an elliptic curve. Proc. Intern. Congress Math., Stockholm 1962, 234—246.

[4] *G. Hochschild* and *J.-P. Serre*, Cohomology of group extensions. Trans. Amer. Math. Soc. **74** (1953), 110—134.

[5] *S. Lang*, Algebraic groups over finite fileds. Amer. J. Math. **78** (1956), 555—563.

[6] *S. Lang* and *J. Tate*, Principal homogeneous spaces over abelian varieties. Amer. J. Math. **80** (1958), 659—684

[7] *T. Ono*, On the Tamagawa number of algebraic tori. Annals of Math. **78** (1963), 47—72.

[8] И. Р. Шафаревич. О бирациональной эквивалентиости эллиптических кривых. Доклады Акад. Наук СССР **114** (1957), 267—270.

[9] И. Р. Шафаревич. Показатели эллиптических кривых. Доклады Акад. Наук СССР **114** (1957), 714—716.

[10] И. Р. Шафаревич. Группа главных однородных алгебраических многообразий. Доклады Акад. Наук СССР **124** (1959), 42—43.

[11] *F. K. Schmidt*, Analytische Zahlentheorie in Körpern der Charakteristik p. Math. Z. **35** (1931), 1—32.

[12] *J. Tate*, *WC*-groups over $\mathfrak{p}$-adic fields. Séminaire Bourbaki 1957/8, Exposé 156.

[13] *J. Tate*, Duality theorems in galois cohomology over number-fields. Proc. Intern. Congress. Math., Stockholm, 1962, 288—295.

[14] *A. Weil*, Adèles et groupes algébriques. Séminaire Bourbaki 1958/9, Exposé 186.

[15] *A. Weil*, Adeles and algebraic groups. (Mimeographed). Institute for Advanced Study, Princeton, 1961.

[16] *A. Weil*, Sur la théorie des formes quadratiques. Colloque sur la théorie des groupes algébriques, Bruxelles, 1962 (Gauthier-Villars).

[17] *E. Forrest*, Cambridge M. Sc. thesis (1964).

Eingegangen 15. Februar 1964