ISRAEL JOURNAL OF MATHEMATICS, Vol. 31, Nos. 3-4, 1978

TORSION POINTS OF ELLIPTIC CURVES OVER LARGE ALGEBRAIC EXTENSIONS OF FINITELY GENERATED FIELDS

BY

WULF-DIETER GEYER AND MOSHE JARDEN

ABSTRACT

The following Theorem is proved: *Let K be a finitely generated field over its prime field. Then, for almost all e-tuples $(\sigma) = (\sigma_1, \cdots, \sigma_e)$ of elements of the abstract Galois group $G(K)$ of K we have*:

(a) *If $e = 1$, then $E_{tor}(\tilde{K}(\sigma))$ is infinite. Morover, there exist infinitely many primes l such that $E(\tilde{K}(\sigma))$ contains points of order l.*

(b) *If $e \geqq 2$, then $E_{tor}(\tilde{K}(\sigma))$ is finite.*

(c) *If $e \geqq 1$, then for every prime l, the group $E(\tilde{K}(\sigma))$ contains only finitely many points of an l-power order.*

Here $\tilde{K}(\sigma)$ is the fixed field in the algebraic closure $\tilde{K}$ of K, of $\sigma_1, \cdots, \sigma_e$, and "almost all" is meant in the sense of the Haar measure of $G(K)$.

§ 1. Presentation of the problem

1.1. *Introduction*

By an *elliptic curve E defined over a field K* we mean a projective absolutely irreducible curve E of genus 1 defined over K and equipped with a distinguished K-rational point 0. An addition law is defined on the set of all points of E (in some universal field that contains K) such that E becomes an abelian variety with 0 as the zero point. If $\mathrm{char}(K) \neq 2, 3$, then E can be presented by the affine Weierstrass canonical form $Y^2 = 4X^3 - g_2X - g_3$, where $g_2, g_3 \in K$ (see Roquette [23, p. 70]). Here 0 is the point at infinity of the curve. The K-rational points of E form a subgroup, $E(K)$, of E whose torsion part is denoted by $E_{tor}(K)$. The main interest in the theory of elliptic curves lies in the exploration of the properties of the groups $E(K)$ and $E_{tor}(K)$ for various K's. The most important result is given by the Mordell–Weil Theorem, that handles the case

Received November 14, 1977 and in revised form May 20, 1978

where K is finitely generated over its prime field (K is then said to be *finitely generated*).

MORDELL–WEIL THEOREM. *If E is an elliptic curve defined over a finitely generated field, then the group $E(K)$ is finitely generated.*

For a proof of this theorem see e.g. Lang [12, p. 92]. One can split the theorem into two parts.

(a) The rank of $E(K)$ is finite.

(b) The torsion group, $E_{\mathrm{tor}}(K)$, is finite.

Recently Mazur gave a bound for the order of $E_{\mathrm{tor}}(\mathbf{Q})$ that depends only on $\mathbf{Q}$ (see [19]). Whether there exists a bound for rank$(E(K))$ that depends only on K, is still an open question. If L is a finite extension of K, then L is also finitely generated, hence both rank$(E(L))$ and $E_{\mathrm{tor}}(L)$ remain finite, but they are possibly larger. If L is an infinite extension of K, then rank$(E(L))$ and $E_{\mathrm{tor}}(L)$ may but must not be finite (cf. [19] and [11]). More precise statements about the behaviour of these quantities can be made in the case where L is "close" to the algebraic closure, $\tilde{K}$, of K. By "close" we mean that the absolute Galois group, $G(L) = \mathcal{G}(L_s/L)$ of L (L_s is the separable closure of L) is finitely generated (in the topological sense).

To be precise, consider the absolute Galois group, $G(K)$, of K. For every $(\sigma) = (\sigma_1, \cdots, \sigma_e) \in G(K)^e$ let $K_s(\sigma)$ be the fixed field in K_s of $\sigma_1, \cdots, \sigma_e$. The maximal purely inseparable extension of $K_s(\sigma)$ is denoted by $\tilde{K}(\sigma)$. It is the fixed field in $\tilde{K}$ of the unique extensions of $\sigma_1, \cdots, \sigma_e$ to $\tilde{K}$.

In [5, p. 124] Frey and Jarden proved the following

THEOREM. *Let K be an infinite finitely generated field. Then for almost all $(\sigma) \in G(K)^e$ and for every elliptic curve E defined over $K_s(\sigma)$, the rank of $E(K_s(\sigma))$ is infinite.*

Here "almost all" is meant in the sense of the Haar measure of $G(K)$. (See section 1.2 for details.)

Certainly the Frey–Jarden theorem remains valid if the fields $K_s(\sigma)$ are replaced by the fields $\tilde{K}(\sigma)$. It remains therefore to consider the torsion part of the groups $E(\tilde{K}(\sigma))$. The situation here can be compared with the question of the torsion groups of $\tilde{K}(\sigma)^\times$. These are the groups of all roots of unity that are contained in $\tilde{K}(\sigma)$. In [10, p. 124] Jarden proved the following

THEOREM. *Let K be a field of a finite type. Then almost all $(\sigma) \in G(K)^e$ have the following property:*

(a) *If $e = 1$, then $K_s(\sigma)$ contains infinitely many roots of unity.*

(b) *If $e \geqq 2$, then $K_s(\sigma)$ contains only finitely many roots of unity.*

One observes that unlike in Frey–Jarden's theorem, there is a distinction here between the case $e = 1$ and $e \geqq 2$. This distinction extends also to elliptic curves, where we prove the analogous

THEOREM 1.1. *Let K be a finitely generated field. Then, for almost all $(\sigma) \in G(K)^e$ and for every elliptic curve E defined over $\tilde{K}(\sigma)$ we have:*

(a) *If $e = 1$, then $E_{\text{tor}}(\tilde{K}(\sigma))$ is infinite. Moreover, there exist infinitely many primes l such that $E(\tilde{K}(\sigma))$ contains points of order l.*

(b) *If $e \geqq 2$, then $E_{\text{tor}}(\tilde{K}(\sigma))$ is finite.*

(c) *If $e \geqq 1$, then for every prime l, the group $E(\tilde{K}(\sigma))$ contains only finitely many points of an l-power order.*

Theorem 1.1 is our main theorem and the whole work is devoted to its proof. It turns out that in order to prove the theorem it suffices to prove the following seemingly weaker

PROPOSITION 1.2. *Let E be an elliptic curve with an absolute invariant j defined over a finitely generated field. Suppose that j is contained in a finite field or $K = \mathbf{F}_p(j)$ or $K = \mathbf{Q}(j)$. Then for almost all $(\sigma) \in G(K)^e$ we have*

(A) *If $e = 1$, then there exist infinitely many primes l such that $E(\tilde{K}(\sigma))$ contains points of order l.*

(B) *If $e \geqq 2$, then there exist only finitely many primes l such that $E(\tilde{K}(\sigma))$ contains a point of order l.*

(C) *If $e = 1$ and l is a prime, then $E(\tilde{K}(\sigma))$ contains only finitely many points of an l-power order.*

In the proof of Proposition 1.2 we distinguish between several cases. We consider the n-torsion group E_n of an elliptic curve E defined over K. Let $p = \operatorname{char} K$. It is well known that if $p \nmid n$, then $E_n = \mathbf{Z}/nZ \oplus \mathbf{Z}/n\mathbf{Z}$ (cf. Cassels [2, p. 219]). In this case $K_n = K(E_n)$ is a Galois extension of K and $G_n = \mathcal{G}(K_n/K)$ is isomorphic to a subgroup $G(n)$ of $\mathrm{GL}(2, n) = \mathrm{GL}(2, \mathbf{Z}/n\mathbf{Z})$; the action of G_n on E_n is transferred by this isomorphism to the action of $\mathrm{GL}(2, n)$ on $Z/nA \oplus Z/nZ$. Our proof of Proposition 1.2 is based on a good knowledge of $G(n)$. It turns out that there are four completely distinct cases.

Case I. $p = 0$ and E has no complex multiplication. Then $G(n)$ is "almost" equal to $\mathrm{GL}(2, n)$. This follows from classical results of Weber (cf. Lang [16, p. 68]) as well as new results of Serre (see [25, p. 260]).

Case II. $K = \mathbf{F}_p(j)$ and j is transcendental over $\mathbf{F}_p$. If $p \mid n$, then $G(n) = \{A \in \mathrm{GL}(2,n) \mid \det A$ is a power of $p\}$, by Igusa [8, p. 469].

Case III. K is a number field and E has a complex multiplication. Here $G(n)$ is "almost" abelian and $|G(n)|$ has the order of magnitude n^2. To prove this we apply classical results of Weber that use class field theory.

Case IV. The invariant j is contained in a finite field and thus E is isomorphic (over a finite separable extension of K) to an elliptic curve E' defined over a finite field. $G(n)$ is "almost" cyclic. We prove a somewhat stronger theorem and use the Riemann Hypotheses for elliptic curves.

The fact that Theorem 1.1 is true in all the possible cases makes the following generalization plausible.

CONJECTURE. *Theorem* 1.1 *remains valid even if one replaces E by an arbitrary abelian variety A.*

Notation

$\mathbf{Z}$ = the ring of integers.
$\mathbf{Q}$ = the field of rational numbers.
$\mathbf{F}_q$ = the field with q elements.
l = a variable for prime numbers.
$\mathbf{Z}_l$ = the ring of l-adic integers.
$\mathbf{Q}_l$ = the field of l-adic numbers.
K = a finitely generated field.
L = an extension field of K.
$\tilde{K}$ = the algebraic closure of K.
K_s = the separable closure of K.
$G(K) = \mathcal{G}(K_s/K)$ = the absolute Galois group of K.
$\tilde{K}(\sigma)$ = the fixed field of $(\sigma) = (\sigma_1, \cdots, \sigma_e) \in G(K)^e$ in $\tilde{K}$.
p = the characteristic of K.
$\mathrm{ord}_n p$ = the order of p modulo n (n is relatively prime to p).
$|A|$ = the cardinality of a set A.
$\mathrm{SL}(2,n) = \mathrm{SL}(2, \mathbf{Z}/n\mathbf{Z})$.
$\mathrm{GL}(2,n) = \mathrm{GL}(2, \mathbf{Z}/n\mathbf{Z})$.
E = an elliptic curve defined over K.
$E(L)$ = the group of L-rational points of E.
$E_n = \{P \in E(\tilde{K}) \mid nP = 0\}$.
$E_{l^\infty} = \bigcup_{i \geqq 1} E_{l^i}$.

E_{tor} = the torsion part of E.
$K_n = K(E_n)$.
$G_n = \mathcal{G}(K_n/K)$.
$K_{l^\infty} = \bigcup_{i \geq 1} K(E_{l^\infty})$.
$G_{l^\infty} = \mathcal{G}(K_{l^\infty}/K) = \varprojlim G_{l^i}$.
$T_l = \lim E_{l^i}$ = the Tate module of E at l.

1.2. *The Haar measure of a profinite group*

Every profinite group G has a canonical topology that makes it a compact group. There is therefore a unique way to define a Haar measure $\mu = \mu_G$ on G such that $\mu(G) = 1$. We complete μ by adjoining to the Borel field all the subsets of zero sets and denote the completion also by μ.

The fundamental property of the Haar measure is that it is invariant under translations. This means that if A is a measurable subset of G, and $g \in G$, then gA and Ag are also measurable and $\mu(gA) = \mu(Ag) = \mu(A)$. In particular it follows that $\mu(H) = (G : H)^{-1}$ for every closed subgroup H of a finite index, and $\mu(H) = 0$ if $(G : H) = \infty$. If a measurable set A has infinitely many translations g_iA, for $i = 1, 2, 3, \cdots$, such that $\mu(g_iA \cap g_jA) = 0$ for every $i \neq j$, then $\mu(A) = 0$. The intersection of countably many subsets of measure 1 is again a subset of measure 1.

We recall that a sequence $\{A_i\}_{i=1}^\infty$ of measurable sets is said to be μ-*independent*, if $\mu(\bigcap_{j \in J} A_j) = \prod_{j \in J} \mu(A_j)$ for every finite subset J of positive integers.

Borel–Cantelli Lemma. *Let $\{A_i\}_{i=1}^\infty$ be a sequence of measurable sets in a probability space (X, μ). Then*

(a) *If the sequence $\{A_i\}_{i=1}^\infty$ is μ-independent and if $\Sigma_{i=1}\,\mu(A_i) = \infty$, then almost every $x \in X$ belongs to infinitely many of the A_i's.*

(b) *If $\Sigma_{i=1}^\infty\,\mu(A_i) < \infty$, then almost every $x \in X$ belongs, at most, to finitely many of the A_i's.*

A proof of this lemma can be found in [10, p. 111].

Let H be a closed subgroup with a finite index of a profinite group G. Then H is also a profinite group. If A is a measurable subset of H, then it is measurable in G and $\mu_H(A) = (G : H)\mu_G(A)$. In particular $\mu_G(A) = 0$ is equivalent to $\mu_H(A) = 0$. If B is a measurable subset of G, then $B \cap H$ is measurable in H and $\mu_G(B) = 1$ implies $\mu_H(B \cap H) = 1$.

Let $r : G \to G'$ be a continuous epimorphism of profinite groups. Let $\mu = \mu_G$

and $\mu' = \mu_{G'}$. A subset B of G' is measurable if and only if $r^{-1}(B)$ is measurable, and in this case $\mu'(B) = \mu(r^{-1}(B))$. In particular it follows that if $\mu(A) = 1$, then $\mu'(rA) = 1$, since $A \subseteq r^{-1}r(A)$.

The cartesian power G^e of a profinite group G is also a profinite group and the completion of the Haar measure of G^e coincides with the completion of the power measure of μ_G.

Let now M be a Galois extension of a field K. Then $\mathcal{G}(M/K)$ is a profinite group and has therefore a Haar measure $\mu = \mu_{M/K} = \mu(M/K)$ as described above. The following statements about fields are therefore the translations of the corresponding statements about profinite groups.

If $L \subseteq M$ is a finite extension of K, then $\mu(\mathcal{G}(M/L)) = [L:K]^{-1}$. If $[L:K] = \infty$, then $\mu(\mathcal{G}(M/L)) = 0$.

A sequence $\{K_i\}_{i=1}^{\infty}$ of intermediate fields of M/K is said to be linearly disjoint over K, if K_{i+1} is linearly disjoint from $K_1 \cdots K_i$ over K for every positive integer i. This happens to be the case if and only if the sequence $\{\mathcal{G}(M/K_i)\}_{i=1}^{\infty}$ is μ-independent. In this case, $\mu\left(\bigcup_{i=1}^{\infty} \mathcal{G}(M/K_i)\right) = 1$, if $\Sigma_{i=1}^{\infty}[K_i:K]^{-1} = \infty$.

Let $\{K_i/K\}_{i=1}^{\infty}$ be a linearly disjoint sequence of finite Galois subextensions of J/K. For every $i \geqq 1$ let A'_i be a subset of $\mathcal{G}(K_i/K)$, and let A_i be the lifting of A'_i to $\mathcal{G}(M/K)$. Then $\mu(A_i) = |A_i|[K_i:K]^{-1}$ and the sequence $\{A_i\}_{i=1}^{\infty}$ is μ-independent.

Let K_1 be an extension of K which is linearly disjoint from M and let M_1 be a Galois extension of K_1 that contains M. Then the restriction map $r: \mathcal{G}(M_1/K_1)^e \to \mathcal{G}(M/K)^e$ is a continuous map, for every $e \geqq 1$. In particular we have the formula $\mu_{M/K}(A) = \mu_{M_1/K_1}(r^{-1}(A))$ for every measurable subset A of $\mathcal{G}(M/K)^e$.

Let K'' be a purely inseparable extension of K, let $\mu = \mu_{K_s/K}$ and $\mu'' = \mu_{K''_s/K''}$. The restriction map of $G(K'')^e$ into $G(K)^e$ is an isomorphism. Hence, if A is the image of a measurable subset A'' of $G(K'')^e$, then A is μ-measurable and $\mu(A) = \mu''(A'')$. Note that if $(\sigma'') \in G(K'')^e$ and (σ) is the restriction of (σ'') to K_s, then $\tilde{K}(\sigma) = \tilde{K}(\sigma'')$.

1.3. *Reduction steps*

We show in this section that Theorem 1.1 follows from Proposition 1.2.

Step 1. Proposition 1.2 implies

LEMMA 1.3. *Let* $\tilde{K}(\sigma) = \tilde{K}(\sigma'')$.
be an elliptic curve with an absolute invariant j defined over a field K. Suppose that j belongs to a finite field or $K = \mathbf{F}_p(j)$ or $K = \mathbf{Q}(j)$. Then for almost all $(\sigma) \in G(K)^e$ we have:

(a) *If $e = 1$, then there exist infinitely many primes l such that $E_l(\tilde{K}(\sigma)) \neq 0$.*

(b) *If $e \geqq 2$, then $E_{\mathrm{tor}}(\tilde{K}(\sigma))$ is finite.*

(c) *If $e \geqq 1$, then $E_{l^\infty}(\tilde{K}(\sigma))$ is finite for every prime l.*

PROOF. Statement (a) is just a repetition of (A). We continue with the proof of (c). Let $A_e = \{(\sigma) \in G(K)^e \mid E_{l^\infty}(\tilde{K}(\sigma))$ is finite for every $l\}$. Then $A_1^e \subseteq A^e$, since $\tilde{K}(\sigma_1, \cdots, \sigma_e) \subseteq \tilde{K}(\sigma_1)$. By (C), $\mu_1(A_1) = 1$, hence $\mu_e(A_e) = 1$.

Statement (b) follows now from (B) and from (c).

Step 2. Lemma 1.3 implies:

LEMMA 1.4. *Let E be an elliptic curve defined over a finitely generated field K. Then for almost all $(\sigma) \in G(K)^e$ we have:*

(a) *If $e = 1$, then there exist infinitely many primes l such that $E_l(\tilde{K}(\sigma)) \neq 0$.*

(b) *If $e \geqq 2$, then $E_{\mathrm{tor}}(K(\sigma))$ is finite.*

(c) *If $e \geqq 1$, then $E_{l^\infty}(K(\sigma))$ is finite for every prime l.*

PROOF. We start the proof with a lemma on Hilbertian fields. Let L be a field, let $f_1, \cdots, f_m$ be irreducible polynomials in $L(T_1, \cdots, T_r)[X_1, \cdots, X_s]$ and let $f'_1, \cdots, f'_m$ be arbitrary polynomials there. The *Hilbertian set* in L^r defined by $f_1, \cdots, f_m, f'_1, \cdots, f'_n$ is the set H of all (a) in L^r such that $f_i(a, X)$ and $f'_j(a, X)$ are defined, and $f_i(a, X)$ are irreducible in $L[X]$. The field L is said to be *Hilbertian*, if all its Hilbertian sets are non empty (cf. Lang [12, p. 141]). It is known that every infinite finitely generated field is Hilbertian (cf. [12, p. 155]). It is also known that if M is a finitely separable extension of a field L, then every Hilbertian set of M^r contains a Hilbertian set of L^r (cf. [12, p. 152]). The following lemma is less known, but it is still true (cf. Roquette [24, corol. 4.5]).

LEMMA 1.5. *Let M/L be a finitely generated separable extension. Then every Hilbertian set of M^r contains a Hilbertian set of L^r.*

Next we prove the following

LEMMA 1.6. *Let E be an elliptic curve with an absolute invariant j defined over a finitely generated field K. Let F be the prime field of K and suppose that $F(j)$ is an infinite field. Then for almost all $(\sigma) \in G(K)^e$ there exists an elliptic curve E' defined over $F(j)$ and isomorphic to E over $\tilde{K}(\sigma)$.*

PROOF. It is well known that E is isomorphic over K to a curve $E_{(j,\gamma)}$ given in affine coordinates by the equation

$$\begin{aligned} &Y^2 = 4X^3 - g_2X - g_3, && \text{if } p \neq 2,3,\\ &Y^2 = X^3 + \gamma X^2 - \frac{\gamma^3}{j}, && \text{if } p = 3,\\ &Y^2 + XY = X^3 + \gamma X^2 + \frac{1}{j}, && \text{if } p = 2. \end{aligned}$$

Note that if $p = 2$ or $p = 3$, then $j \neq 0, 12^3$. On the case $p \neq 2,3$ we have

$$j = 12^3 \frac{g_2^3}{g_2^3 - 27g_3^2} \qquad \text{and} \qquad \gamma = \begin{cases} -\frac{1}{2}\frac{g_2}{g_3}, & \text{if } j \neq 0, 12^3,\\ g_2, & \text{if } j = 12^3,\\ g_3, & \text{if } j = 0, \end{cases}$$

for the Haase invariant γ. In this case we also have $F(j, \gamma) = F(g_2, g_3)$.

Further, let $c \neq 0$ and let γ' be the new Haase invariant defined by

$$\gamma' = \begin{cases} \gamma c^2, & \text{if } p \neq 2 \quad \text{and} \quad j \neq 0, 12^3;\\ \gamma c^4, & \text{if } p \neq 2 \quad \text{and} \quad j = 12^3;\\ \gamma c^6, & \text{if } p \neq 2 \quad \text{and} \quad j = 0;\\ c^2 + c + \gamma, & \text{if } p = 2. \end{cases}$$

Then the curve $E_{(j,\gamma')}$ is defined over $F(j, \gamma')$ and is isomorphic to $E = E_{(j,\gamma)}$ over $F(j, \gamma, c)$ (cf. Roquette [23, pp. 69–79]).

Let now $K_1 = F(j, \gamma)$. Then $K_1 \subseteq K$ and E is defined over K_1. Let $K_2 = K \cap K_{1,s}$. Then K_2 is a finite separable extension of K_1 and K is linearly disjoint from $K_{1,s}$ over K_2. The restriction map $\rho : G(K)^e \to G(K_2)^e$ is an epimorphism. Suppose Lemma 1.6 is true for K_2. Let S_2 be the set of all $(\sigma) \in G(K_2)^e$ for which there exists an elliptic curve E' over $F(j)$ and isomorphic to E over $\tilde{K}(\sigma)$ and let S_1, S be the corresponding sets for K_1, K, respectively. Then $\mu_{K_2}(S_2) = 1$ and $\rho^{-1}(S_2) \subseteq S$; hence $\mu_K(S) = 1$. It follows that it suffices to prove Lemma 1.6 for the case where K is a finite separable extension of K_1.

Suppose next that Lemma 1.6 is true for K_1, i.e. $\mu_{K_1}(S_1) = 1$. Then $\mu_K(S) = 1$, since $S = S_1 \cap G(K)^e$. It follows that it suffices to prove Lemma 2.4 in the case where $K = K_1$.

If $p \neq 0$ and γ is algebraic over $F(j)$, then $j \neq 0, 12^3$ and γ must not be separable over $F(j)$. Let

$$c = \begin{cases} \gamma^{(p-1)/2}, & \text{if } p \neq 2, \\ \gamma, & \text{if } p = 2. \end{cases}$$

Then $\gamma' = \gamma^p$ and E is isomorphic over K to $E_{(j,\gamma^p)}$. Now, there exists a power q of p such that γ^q is separable over $F(j)$. Applying the above process a finite number of times we conclude that E is isomorphic over K to $E_{(j,\gamma^q)}$. It follows that we can assume that either γ is separable algebraic or transcendental over $F(j)$.

Define now an integer n and a polynomial $f \in K[T, X]$ as follows:

$$\begin{array}{llll} p \neq 2 \text{ and } j \neq 0, 12^3 & \Rightarrow n = 2 & \text{and} & f(T,X) = \gamma X^2 - T; \\ p \neq 2 \text{ and } j = 12^3 & \Rightarrow n = 4 & \text{and} & f(T,X) = \gamma X^4 - T; \\ p \neq 2 \text{ and } j = 0 & \Rightarrow n = 6 & \text{and} & f(T,X) = \gamma X^6 - T; \\ p = 2 & \Rightarrow n = 2 & \text{and} & f(T,X) = X^2 + X + T + \gamma. \end{array}$$

Further, define by induction a linearly disjoint sequence, $\{L_i/K\}_{i=1}^{\infty}$, of separable field extensions of degree n, and a sequence, $\{E_i\}_{i=1}^{\infty}$, of elliptic curves which are defined over $F(j)$, such that E_i is isomorphic to E over L_i. Suppose that $L_1, \cdots, L_{i-1}$ and $E_1, \cdots, E_{i-1}$ have already been defined. The field L generated by $L_1, \cdots, L_{i-1}$ is a finite separable extension of K. Moreover $F(j)$ is a Hilbertian field, since it is infinite, and $f(T, X)$ is absolutely irreducible and separable in X. Hence, by Lemma 1.4, there exists a γ' in $F(j)$ such that $f(\gamma', X)$ is irreducible in $L[X]$, of degree n and separable. Let c be an element in $\tilde{K}$ such that $f(\gamma', c) = 0$ and let $L_i = L(c)$. Then L_i is a separable extension of degree n of K which is linearly disjoint from L over K. The curve $E_i = E_{(j,\gamma')}$ is defined over $F(j)$ and isomorphic to E over L_i. Our induction is thus completed.

If $(\sigma) \in G(K_i)^e$, then $\tilde{K}(\sigma)$ contains L_i and hence E_i is isomorphic to E over $\tilde{K}(\sigma)$. This ends the proof of Lemma 1.6, since almost all $(\sigma) \in G(K)^e$ belong to one of the $G(L_i)^e$, by section 1.2.

END OF PROOF OF LEMMA 1.3 $\Rightarrow$ LEMMA 1.4. Let E be an elliptic curve with an absolute invariant j defined over a finitely generated field K. We have to consider only the case where $F(j)$ is an infinite field. Then, by Lemma 1.6, the set S_0 of all $(\sigma) \in G(K)^e$ for which there exists an elliptic curve E' over $K_0 = F(j)$ and isomorphic to E over $\tilde{K}(\sigma)$, is of measure 1. Order all these E' in a sequence: $E'_1, E'_2, E'_3, \cdots$. For every $i \geqq 1$ let S_i be the set of all $(\sigma) \in G(K_0)^e$

such that (a), (b) and (c) are true with respect to E'_i, and let $S' = \bigcap_{i=1}^{\infty} S'_i$. Then $\mu_{K_0}(S') = 1$, by Lemma 1.3.

Let $K'_1 = K \cap K_{0,s}$. Then K is linearly disjoint from $K_{0,s}$ over K'_1 and hence the restriction map $r : G(K)^e \to G(K'_1)^e$ is surjective. Moreover, K'_1 is a finite separable extension of K_0. Hence $\mu_{K'_1}(S' \cap G(K'_1)^e) = 1$. Let $S = r^{-1}(S' \cap G(K'_1)^e)$, then $\mu_K(S) = 1$, hence $\mu_K(S_0 \cap S) = 1$.

Let now $(\sigma) \in S_0 \cap S$ and let $(\sigma') = r(\sigma)$. Then there exists an E' over K_0 and (a), (b), (c) are true for E' and $\tilde{K}(\sigma) \cap \tilde{K}_0 = \tilde{K}_0(\sigma')$. If $e = 1$, then there exist infinitely many l such that $E'_l(\tilde{K}(\sigma)) \neq 0$, hence also $E_l(\tilde{K}(\sigma)) \neq 0$, since E and E' are isomorphic over $\tilde{K}(\sigma)$. If $e \geqq 2$, then $E'_{\mathrm{tor}}(\tilde{K}_0(\sigma'))$ is finite. Hence $E'_{\mathrm{tor}}(\tilde{K}(\sigma))$ is finite, since $E'_{\mathrm{tor}} \subseteq E'(\tilde{K}_0)$. It follows that $E_{\mathrm{tor}}(\tilde{K}(\sigma))$ is finite. The same argument implies that if $e \geqq 1$ and l is a prime, then $E_{l^\infty}(\tilde{K}(\sigma))$ is finite.

The second reduction step is therefore completed.

Step 3. Lemma 1.4 implies Theorem 1.1.

Let K be a finitely generated field. Let L be a finite extension of K and let L_0 be the separable closure of K in L. For every elliptic curve E defined over L, define $S(L,E)$ to be the set of all $(\sigma) \in G(L)^e$ such that (a), (b) and (c) are satisfied. By Lemma 1.5, $\mu_L(S(L,E)) = 1$. Let $S_0(L,E)$ be the restriction of $S(L,E)$ to K_s. Then $\mu_{L_0}(S_0(L,E)) = 1$. Hence $\mu_K(G(L_0)^e - S_0(L,E)) = 0$. There are only countably many pairs (L,E). Hence the union $\bigcup (G(L_0)^e - S_0(L,E))$, where (L,E) runs over all possible pairs, is a zero set in $G(K)^e$.

Suppose that $(\sigma) \in S_0(L,E)$. Hence (a), (b), and (c) are satisfied for (σ) and E.

1.4. *Permutation groups*

By a permutation group we mean a pair (G,A), where A is an additive abelian group and G is a multiplicative group that operates faithfully (and continuously, if A and G have topologies) on A.

A pair (G_1,A) is said to be a *subgroup* of (G,A) if $G_1 \leqq G$ and if the operation of an element $g_1 \in G_1$ on A coincides with its operation on A as an element of G.

A *homomorphism* of a permutation group (G,A) into another one (H,B) is a pair (θ,α), where $\theta : G \to H$ and $\alpha : A \to B$ are homomorphisms, and $\theta(g)\alpha a = \alpha g a$ for every $a \in A$ and $g \in G$.

The pair (θ,α) is said to be surjective, if both θ and α are surjective. It is called an *embedding* if α is an isomorphism. In this case θ is injective. It is called an *isomorphism*, if both α and θ are isomorphisms.

Let (G_1,A) be a subgroup of (G,A) and let $(\theta,\alpha):(G_1,A) \to (H,B)$ be an embedding. Then (θ, α) can be uniquely extended to an embedding of (G, A) into $(\operatorname{Aut} B, B)$ by the following definition:

$$\theta(g)b = \alpha g \alpha^{-1} b \qquad \text{for } b \in B \text{ and } g \in G.$$

Suppose that we are given an inverse system $\{(G_i, A_i), (\theta^i_j, \alpha^i_j) \mid i, j \in I\}$ of finite permutation groups. Then its inverse limit $(G, A) = \varprojlim (G_i, A_i)$ is also a permutation group, taking into account now also the topologies of G and A.

Given a permutation group (G, A) and a positive integer e, we define

$$S_e(G, A) = \{(g_1, \cdots, g_e) \in G^e \mid \exists a \in A : a \neq 0 \text{ and } g_i a = a \text{ for } i = 1, \cdots, e\}.$$

This is a subset of G^e that contains $(1, 1, \cdots, 1)$. We also write

$$S(G, A) = S_1(G, A) = \{g \in G \mid \exists a \in A : a \neq 0 \quad \text{and} \quad ga = a\}.$$

Then $S_e(G, A) \subseteq S(G, A)^e$.

1.5. *Examples of permutation groups*

We bring in this section examples of permutation groups which we shall meet in this work.

(1) (G, R^2). Here R is a commutative ring with 1 and G is a subgroup of $\mathrm{GL}(2, R)$, with the usual operation. A matrix B belongs to $S(G, R^2)$ if and only if 1 is a characteristic value of B.

(2) $(R^\times, R)$. Here R is a commutative ring with 1 and $R^\times$ is the multiplicative group of all invertible elements. An element $u \in R^\times$ operates on an element $r \in R$ by multiplication. In particular we shall consider the case where $R = R_1^2$ and R_1 is an integral domain. In this case

$$S(R^\times, R) = \{(u_1, u_2) \in R_1^{\times 2} \mid u_1 = 1 \quad \text{or} \quad u_2 = 1\}.$$

(3) (G_n, E_n). Here E is an elliptic curve defined over a field K of characteristic p that does not divide n and $G_n = \mathcal{G}(K(E_n)/K)$. The elements of G_n operate on E_n, since the law of addition of E is defined over K. E_n is isomorphic to $(\mathbf{Z}/n\mathbf{Z})^2$. One can therefore choose P, Q in E such that $E_n = \{xP + yQ \mid x, y \in \mathbf{Z}\}$.

A specific isomorphism of E_n onto $(\mathbf{Z}/n\mathbf{Z})^2$ can now be defined by mapping the point $xP + yQ$ onto the pair (x, y) modulo n. Also, one maps an element $\sigma \in G_n$ onto the matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ of } \mathrm{GL}(2, n) \text{ defined by } \begin{array}{l} \sigma P = aP + cQ, \\ \sigma Q = bP + dQ. \end{array}$$

This gives an embedding of (G_n, E_n) into $(\mathrm{GL}(2, n), (\mathbf{Z}/n\mathbf{Z})^2)$ which is, however, not canonical, and depends on the choice of P and Q. Note that every embedding $(G_n, E_n) \to (\mathrm{GL}(2, n), (\mathbf{Z}/n\mathbf{Z})^2)$ is induced by a certain pair (P, Q). Indeed, P is the point of E_n which is mapped on $(1, 0)$ and Q is the one mapped on $(0, 1)$.

Using the fact that an inverse limit of non-void finite sets is not empty, one can prove that for every n which is prime to p there exist points P_n, Q_n that generate E_n such that if $n = km$, then $kP_n = P_m$ and $kQ_n = Q_m$. Denote by $G(n)$ the image of G_n in $\mathrm{GL}(2, n)$ by the canonical embedding induced by (P_n, Q_n).

In particular consider a prime $l \neq p$. Let

$$K_{l^\infty} = \bigcup_{i=1}^{\infty} K_{l^i} \quad \text{and} \quad G_{l^\infty} = \mathcal{G}(K_{l^\infty}/K).$$

Then we have a sequence of canonical commutative diagrams

$$\begin{tikzcd}
(G_{l^{i+1}}, E_{l^{i+1}}) \arrow[r] \arrow[d] & (G(l^{i+1}), (\mathbf{Z}/l^{i+1}\mathbf{Z})^2) \arrow[d] \\
(G_{l^i}, E_{l^i}) \arrow[r] & (G(l^i), (\mathbf{Z}/l^i\mathbf{Z})^2).
\end{tikzcd}$$

Taking the inverse limit of this sequence we get an isomorphism

$$(G_{l^\infty}, T_l) \longrightarrow (G(l^\infty), \mathbf{Z}_l^2),$$

where $T = \varprojlim E_{l^i}$ is the *Tate-module.*

(4) Occasionally we shall consider pairs (G, A), where G is a multiplicative group operating non-faithfully on A. We shall keep the notation $S(G, A)$ for the set of all $g \in G$ that fix a non-zero element of A. In particular we shall consider the pairs $(G(K), E_n)$. An element σ of $G(K)$ belongs to $S(G(K), E_n)$ if and only if $E_n(\tilde{K}(\sigma)) \neq 0$, i.e. if the restriction of σ to K_n belongs to $S(G_n, E_n)$.

1.6. *Further reduction*

The case where j belongs to a finite field needs special treatment. In all other cases it is more convenient to prove the following Proposition 1.7 rather than Proposition 1.2. Indeed, Proposition 1.2 follows from Proposition 1.7 in these cases.

PROPOSITION 1.7. *Let E be an elliptic curve with an absolute invariant j defined over a field K. Suppose that $K = \mathbf{F}_p(j)$ and j is transcendental over $\mathbf{F}_p$, or $K = \mathbf{Q}(j)$. Then the following statements are true:*

(A′) *There exists an infinite set of primes Λ, and for every $l \in \Lambda$ there exists a non-empty subset $S'(G_l, E_l)$ of $S(G_l, E_l)$ such that*

(A′1) $$\sum_{l\in\Lambda}\frac{|S'(G_l,E_l)|}{|G_l|}=\infty,\quad \textit{and}$$

(A′2) *for every* $l_1,\cdots,l_r\in\Lambda$ *we have*

$$\frac{|S'_n|}{|G_n|}=\prod_{j=1}^{r}\frac{|S'(G_{l_j},E_{l_j})|}{|G_{l_j}|},$$

where $n=l_1\cdots l_r$ *and* $S'_n=\{\sigma\in G_n\mid \sigma\mid K_{l_j}\in S'(G_{l_j},E_{l_j})\ \textit{for}\ j=1,\cdots,r\}$.

(B′) *There exists a positive constant c such that*

$$\frac{|S(G_l,E_l)|}{|G_l|}\leqq\frac{c}{l}$$

for all but finitely many primes l.

(C′) *If* $l\neq p$, *then* $S(G_{l^\infty},T_l)$ *is a zero set in* G_{l^∞}. *For almost all* $\sigma\in G(K)$, *the set* $E_{p^\infty}(\tilde K(\sigma))$ *is finite.*

Lemma 1.8. *Proposition* 1.7 *implies Proposition* 1.2 *in the cases where* $K=\mathbf{F}_p(j)$ *and* j *transcendental over* $\mathbf{F}_p$, *or* $K=\mathbf{Q}(j)$.

Proof. (A′) ⇒ (A). Let $S'(G(K),E_l)$ be the lifting of $S'(G_l,E_l)$ to $G(K)$. Then

$$\mu(S'(G(K),E_l)=\frac{|S'(G_l,E_l)|}{|G_l|}.\tag{1}$$

Hence, by (A′1), $\Sigma_{l\in\Lambda}\mu(S'(G(K),E_l))=\infty$.

Next, let $l_1,\cdots,l_r\in\Lambda$. Then $\bigcap_{j=1}^{r}S'(G(K),E_{l_j})$ is the lifting of S'_n to $G(K)$. (We are using here the notation of (A′2).) Hence, by (A′2) and (1), we have

$$\mu\Big(\bigcap_{j=1}^{r}S'(G(K),E_{l_j})\Big)=\prod_{j=1}^{r}\mu\,(S'(G(K),E_{l_j})).$$

It follows that the set $\{S'(G(K),E_l)\,|\,l\in\Lambda\}$ is μ-independent. By the Borel–Cantelli Lemma, the set S of all $\sigma\in G(K)$ that belong to infinitely many $S'(G(K),E_l)$ is of measure 1. For every σ in S there are infinitely many l's such that $E_l(\tilde K(\sigma))\neq 0$. This is (A) of Proposition 1.2.

(B′) ⇒ (B). By (B′) we have $\mu(S(G(K),E_l))\leqq c/l$ for all but finitely many l's. We also know that $S_e(G(K),E_l)\subseteq(S(G(K),E_l))^e$. Hence

$$\mu(S_e(G(K),E_l))\leqq\Big(\frac{c}{l}\Big)^e,\qquad\text{for all but finitely many } l\text{'s.}$$

Hence $\Sigma_l\mu(S_e(G(K),E_l))$ converges, since $e\geqq 2$. It follows, by the

Borel–Cantelli Lemma, that the set T of all $(\sigma) \in G(K)^e$ that belong to at most finitely many $S_e(G(K), E_l)$ is of measure 1. For every $(\sigma) \in T$ there are only finitely many primes l such that $E_l(\tilde{K}(\sigma)) \neq 0$. This proves (B) of Proposition 1.2.

(C′) $\Rightarrow$ (C). Let $l \neq p$ be a prime. Denote by $S(G(K), T_l)$ the lifting of $S(G_{l^\infty}, T_l)$ to $G(K)$. Then $\mu\,(S(G(K), T_l)) = 0$. We have therefore to prove that if $\sigma \in G(K) - S(G(K), T_l)$, then $E_{l^\infty}(\tilde{K}(\sigma))$ is finite.

Assume that $E_{l^\infty}(\tilde{K}(\sigma))$ is infinite. Then there exist infinitely many i's such that $E_{l^{i+1}}(\tilde{K}(\sigma)) - E_{l^i}(\tilde{K}(\sigma))$ is not empty, since each of the sets $E_{l^i}(\tilde{K}(\sigma))$ is finite. Further, if $P \in E_{l^{i+1}}(\tilde{K}(\sigma)) - E_{l^i}(\tilde{K}(\sigma))$, then $lP \in E_{l^i}(\tilde{K}(\sigma)) - E_{i-1}(\tilde{K}(\sigma))$ (where E_{l^0} means 0). It follows that $E_{l^{i+1}}(\tilde{K}(\sigma)) - E_{l^i}(\tilde{K}(\sigma))$ is not empty, for every $i \geqq 1$. Thus, these sets form an inverse system of finite non-empty sets. The inverse limit of such a system is not empty. It follows that there exists a sequence $\{P_i\}_{i=1}^\infty$ of points such that $P_i \in E_{l^{i+1}} - E_{l^i}$, $\sigma P_i = P_i$ and $lP_{i+1} = P_i$ for every $i \geqq 1$. This sequence defines a non-zero point P of T_l which is fixed by σ. Hence $\sigma \in S(G(K), T_l)$, which is a contradiction.

Actually, we shall not prove Proposition 1.7 directly, but rather its matrix counterpart. This is

Proposition 1.9. *Let E be an elliptic curve with an absolute invariant j defined over a field K. Suppose that $K = \mathbf{F}_p(j)$ and j is transcendental over $\mathbf{F}_p$, or $K = \mathbf{Q}(j)$. Then the following statements are true*:

(A″) *There exists an infinite set of primes Λ, and for every $l \in \Lambda$ there exists a non-empty subset $S'(G(l), (\mathbf{Z}/l\mathbf{Z})^2)$ of $S(G(l), (\mathbf{Z}/l\mathbf{Z})^2)$ such that*

$$\text{(A″1)} \qquad \sum_{l \in \Lambda} \frac{|S'(G(l), (\mathbf{Z}/l\mathbf{Z})^2)|}{|G(l)|} = \infty, \text{ and}$$

(A″2) *for every $l_1, \cdots, l_r \in \Lambda$ we have*

$$\frac{|S'(n)|}{|G(n)|} = \prod_{j=1}^{r} \frac{|S'(G(l_j), (\mathbf{Z}/l_j\mathbf{Z})^2)|}{|G(l)|},$$

where $n = l_1 \cdots l_r$ and $S'(n)$ is the set of all matrices A in $G(n)$ that, when reduced modulo l_j, belong to $S'(G(l_j), (\mathbf{Z}/l_j\mathbf{Z})^2)$, for $j = 1, \cdots, r$.

(B″) *There exists a positive constant c such that*

$$\frac{|S(G(l), (\mathbf{Z}/l\mathbf{Z}^2))|}{|G(l)|} \leqq \frac{c}{l} \quad \textit{for all but finitely many primes } l.$$

(C″) *If $l \neq p$, then $S(G(l^\infty), \mathbf{Z}_l^2)$ is a zero set in $G(l^\infty)$. For almost all $\sigma \in G(K)$, the set $E_{p^\infty}(\tilde{K}(\sigma))$ is finite.*

Proposition 1.9 is equivalent to Proposition 1.7, by section 1.5. The sets $S'(G(l),(\mathbf{Z}/l\mathbf{Z})^2)$ of (A″) are the images of the sets $S'(G_l, E_l)$ of (A′).

Remarks. (1) In some of the cases we shall choose for Λ of (A″) the set of all primes $l = ax + b$, where a, b are some fixed relatively prime positive integers. In these cases we shall also find a $c' > 0$ such that

$$\frac{|S(G(l),(\mathbf{Z}/l\mathbf{Z})^2)|}{|G(l)|} \geqq \frac{c'}{l}$$

for every $l \in \Lambda$. Then (A″1) is satisfied, since $\Sigma_{l\in\Lambda} 1/l = \infty$, by the Dirichlet Theorem.

(2) If one proves that

(A‴2) The sequence $\{K_l/K \mid l \in L\}$ is linearly disjoint, then conditions (A′2) and (A″2) are certainly satisfied. We shall however have occasions on which we shall have to prove (A″2) directly, since (A‴2) will be false.

§2. Elliptic curves without complex multiplication over a field of characteristic 0

2.1. *Axiomatization of the problem*

In this Section we consider an elliptic curve E with an absolute invariant j defined over $\mathbf{Q}(j)$ and has no complex multiplication. We prove Proposition 1.2 via Proposition 1.9 for E and for $K = \mathbf{Q}(j)$.

If j is transcendental over $\mathbf{Q}$, then $G(n) = \mathrm{GL}(2, n)$ for every positive integer n. This is a classical result of Weber (see e.g. Lang [16, p. 68]). If j is algebraic over $\mathbf{Q}$, then $(\mathrm{GL}(2, n) : G(n))$ is bounded by a constant that depends only on K and E but not on n. This statement is equivalent to the conjunction of the following two statements:

(I). There exists a positive integer m such that $G(n) = \mathrm{GL}(2, n)$ for every n which is relatively prime to m.

II. $(\mathrm{GL}(2, \mathbf{Z}_l) : G(l^\infty)) < \infty$ for every prime l.

(Compare Serre [25, p. 260].) Of course, this result is valid also in the case where j is transcendental over $\mathbf{Q}$. We shall therefore assume in this chapter that the curve E satisfies I and II.

2.2. *Calculation of $S(G(l),(\mathbf{Z}/l\mathbf{Z})^2)$*

Lemma 2.1. $|S(\mathrm{GL}(2, l),(\mathbf{Z}/l\mathbf{Z})^2)| = l(l^2 - 2)$ *for every prime* l.

Proof. The group $(\mathbf{Z}/l\mathbf{Z})^2$ can be presented as a union of $l + 1$ cyclic groups $Z_1, \cdots, Z_{l+1}$ of order l such that $Z_1 \cap Z_j = \{(0,0)\}$ if $i \neq j$.

If a matrix in $\mathrm{GL}(2,l)$ fixes a non-zero element of Z_i, then it fixes all the elements of Z_i. Denote the set of all matrices that fix the elements of Z_i by S_i. It is not difficult to see that $|S_i| = l(l-1)$. Further, if $i \neq j$ and if $A \in S_i \cap S_j$, then A has two independent fix-points, hence A is the unit matrix. It follows that

$$|S(\mathrm{GL}(2,l),(\mathbf{Z}/l\mathbf{Z})^2)| = \left|\bigcup_{i=1}^{l+1} S_i\right| = \sum_{i=1}^{l+1} |S_i| - l = l(l^2-2).$$

2.3. *Proof of* (A″) *and* (B″)

It is well known that $|\mathrm{GL}(2,l)| = (l^2-1)(l^2-l)$ for a prime l (cf. Huppert [7, p. 178]). If $l > m$, then $G(l) = \mathrm{GL}(2,l)$, by I. Hence $|S(G(l),(\mathbf{Z}/l\mathbf{Z})^2)| = l(l^2-2)$, by Lemma 2.1. It follows that there exist positive constants c_1, c_2 such that

$$\frac{c_1}{l} \leq \frac{|S(G(l),(\mathbf{Z}/l\mathbf{Z})^2)|}{|G(l)|} \leq \frac{c_2}{l}$$

for every prime l. This already proves (A″1) and (B″). We proceed to prove (A‴2) by proving that the sequence $\{K_l/K \mid l > m\}$ is linearly disjoint.

It suffices to prove that if k, n, m are pairwise relatively prime, then K_k and K_n are linearly disjoint over K. Indeed, $K_{kn} = K_k K_n$. Also $\mathrm{GL}(2,kn) \cong \mathrm{GL}(2,k) \times \mathrm{GL}(2,n)$. Hence $[K_k K_n : K] = [K_k : K] \cdot [K_n : K]$, by I.

2.4. *Proof of* (C″)

Let l be a prime. We have to prove that $S(G(l^\infty),\mathbf{Z}_l^2)$ is a zero set in $G(l^\infty)$. Clearly $S(G(l^\infty),\mathbf{Z}_l^2) \subseteq S(\mathrm{GL}(2,\mathbf{Z}_l),\mathbf{Z}_l^2)$ and by II, $(\mathrm{GL}(2,\mathbf{Z}_l) : G(l^\infty)) < \infty$. Hence it suffices to prove

Lemma 2.2. *$S(\mathrm{GL}(2,\mathbf{Z}_l),\mathbf{Z}_l^2)$ is a zero set in* $\mathrm{GL}(2,\mathbf{Z}_l)$.

Proof. We have already mentioned that the set $S = S(G(2,\mathbf{Z}_l),\mathbf{Z}_l^2)$ consists exactly of all the matrices in $\mathrm{GL}(2,\mathbf{Z}_l)$ having the characteristic value 1. In particular S is a closed subset of $\mathrm{GL}(2,\mathbf{Z}_l)$. If $u \in \mathbf{Z}_l^\times$, then uS consists of all the matrices in $\mathrm{GL}(2,\mathbf{Z}_l)$ having the characteristic value u. Our proof will be completed if we show that if $u' \in \mathbf{Z}_l^\times$ and $u' \neq u$, then $uS \cap u'S$ is a zero set in $\mathrm{GL}(2,\mathbf{Z}_l)$. Indeed, if $w, w' \in \mathbf{Z}_l^\times$ and $w \neq \pm w'$, then $w(uS \cap u'S) \cap w'(uS \cap u'S) = \emptyset$, since a 2×2 matrix can have at most two characteristic values. Hence, if we let w run over a set of representatives of $\mathbf{Z}_l^\times/\{\pm 1\}$, then we obtain infinitely many disjoint translations $w(uS \cap u'S)$ of $uS \cap u'S$. This implies that $uS \cap u'S$ is a zero set in $\mathrm{GL}(2,\mathbf{Z}_l)$. □

The proof of Proposition 1.2 is completed in Case I.

§3. Elliptic curves with a transcendental j-invariant over $\mathbf{F}_p$

3.1. *The theorem of Igusa*

We consider in this section a fixed prime p, a transcendental element j over $\mathbf{F}_p$ and an elliptic curve E with the absolute invariant j defined over $K = \mathbf{F}_p(j)$. Let ζ_n be a primitive n-th root of 1, and let $G(n) = \{A \in \mathrm{GL}(2,n) \mid \det A \text{ is a } p\text{-power}\}$. Then the following theorem is a reformulation of theorem 3 of Igusa [8, p. 469].

IGUSA'S THEOREM. *Suppose that $p \nmid n$. Then*

(a) $\mathbf{F}_p(\zeta_n) \subseteq K_n$,

(b) K_n *is Galois over* K,

(c) $(G_n, E_n) \cong (G(n), (\mathbf{Z}/n\mathbf{Z})^2)$,

(d) $\mathcal{G}(K_n/K(\zeta_n))$ *is mapped under the above isomorphism onto* $\mathrm{SL}(2,n)$,

(e) $[K(\zeta_n):K] = \mathrm{ord}_n p$.

3.2. *Proof of* (A″) *and* (B″)

An immediate consequence from Igusa's theorem and from the well-known formula for $|\mathrm{SL}(2,n)|$ (e.g. Igusa [9, p. 458]) is:

LEMMA 3.1. *If $p \nmid n$, then*

$$|G(n)| = n^3 \mathrm{ord}_n p \prod_{l \mid n} (1 - l^{-2}). \tag{1}$$

In particular we have for $l \neq p$ that

$$|G(l)| = l(l^2 - 1)\mathrm{ord}_l p. \tag{2}$$

LEMMA 3.2. $|S(G(l), (\mathbf{Z}/l\mathbf{Z})^2)| = l((l+1)\mathrm{ord}_l p - 1)$.

PROOF. We use the notation of the proof of Lemma 2.1.

A matrix of $G(l)$ fixes the point $(0,1)$ if and only if it has form

$$\begin{pmatrix} p^i & 0 \\ c & 1 \end{pmatrix},$$

where $c \in \mathbf{Z}/l\mathbf{Z}$. The number of these matrices is $l \cdot \mathrm{ord}_l p$. Moreover, $\mathrm{SL}(2,l)$ operates transitively on $(\mathbf{Z}/l\mathbf{Z})^2$, hence $G(l)$ also does. It follows that $|S_i| = l \cdot \mathrm{ord}_l p$ for $i = 1, \cdots, l+1$. Our formula follows as in the proof of Lemma 2.1. □

It follows from Lemmas 3.1 and 3.2 that

$$\frac{|S(G(l), (\mathbf{Z}/l\mathbf{Z})^2)|}{|G(l)|} = \frac{(l+1)\mathrm{ord}_l p - 1}{(l^2-1)\mathrm{ord}_l p} \leqq \frac{2}{l} \tag{3}$$

for every l. This proves (B″).

One observes that the arithmetic function $|G(n)|$ is not multiplicative, since $\mathrm{ord}_n p$ is not. Hence we cannot achieve here linear disjointness for the fields K_l, as we did in section 2.3. Moreover, the quotients (3) have the order of magnitude l^{-1}, but the factor $\mathrm{ord}_l p$ still prevents the sets $S(G(K), E_l)$ being μ-independent. We therefore define $S'(G(l), (\mathbf{Z}/l\mathbf{Z})^2)$ as a proper subset of $S(G(l), (\mathbf{Z}/l\mathbf{Z})^2)$ such that the factor $\mathrm{ord}_n p$ disappears from the quotients corresponding to (3) and such that (A″) is satisfied.

Indeed, let $S'(l, i)$ be the subset of $\mathrm{GL}(2, l)$ consisting of all matrices of the form

$$\begin{pmatrix} 1-cx & x \\ c-cp^i-c^2x & p^i+cx \end{pmatrix} \tag{4}$$

where $c \in \mathbf{Z}/l\mathbf{Z}$ and $x \in (\mathbf{Z}/l\mathbf{Z})^\times$. Then $|S'(l,i)| = l(l-1)$. Note that the determinant of (4) is p^i. Also, (4) fixes the point $(1, c)$ of $(\mathbf{Z}/l\mathbf{Z})^2$. Hence $S'(l,i) \subset S(G(l), (\mathbf{Z}/l\mathbf{Z})^2)$. It follows also that if $i \not\equiv j \bmod \mathrm{ord}_l p$, then $S'(l,i) \cap S'(l,j) = \varnothing$. Hence, if we define

$$S'(l) = S'(G(l), (\mathbf{Z}/l\mathbf{Z})^2) = \bigcup_{i=1}^{\mathrm{ord}_n p} S'(l,i)$$

we get that $|S'(l)| = l(l-1)\mathrm{ord}_l p$. This together with (2) implies

$$\frac{|S'(l)|}{|G(l)|} = \frac{1}{l+1} \geqq \frac{1}{2l}. \tag{5}$$

Thus statement (A″1) is also satisfied.

We prove now statement (A″2). Let $l_1, \cdots, l_r$ be r primes, different from p, let $n = l_1 \cdots l_r$, and let

$$S' = \{A \in G(n) \mid A \text{ modulo } l_j \text{ belongs to } S'(l_j) \quad \text{for } j = 1, \cdots, r\}.$$

By the Chinese Remainder Theorem there exists for every i a canonical bijection of the cartesian product $S'(l_1, i) \times \cdots \times S'(l_r, i)$ onto the set $S'_i = \{A \in S' \mid \det A = p^i\}$. Hence $|S'_i| = \prod_{j=1}^r l_j(l_j - 1)$. Further S' is the disjoint union of the sets S'_i for $i = 1, \cdots, \mathrm{ord}_n p$. Hence

$$|S'| = \mathrm{ord}_n p \prod_{j=1}^r l_j(l_j - 1).$$

This, together with (1) and (5) implies

$$\frac{|S'|}{|G(n)|} = \prod_{j=1}^r \frac{1}{l_{j+1}} = \prod_{j=1}^r \frac{|S'(l_j)|}{|G(l_j)|}.$$

Statement (A″2) is thus also proved.

3.3. *Proof of* (C″) *for* $l \neq p$

LEMMA 3.2. *If $l \neq p$, then $(\mathbf{Z}_l^\times : \langle p \rangle) < \infty$. Here $\langle p \rangle$ denotes the closed subgroup of $\mathbf{Z}_l^\times$ generated by p.*

PROOF. One can write $\mathbf{Z}_l^\times$ as a direct product $\mathbf{Z}_l^\times = G \times H$, where $G \cong \mathbf{Z}_l$, and $H \cong \mathbf{Z}/(l-1)\mathbf{Z}$ if $l \neq 2$; $H \cong \mathbf{Z}/r\mathbf{Z}$ if $l = 2$. Then $p^k \in G$, where $k = |H|$. Clearly $p^k \neq 1$, hence $(G : \langle p^k \rangle) < \infty$ (cf. Ribes [27, p. 57]). It follows that $(\mathbf{Z}_l^\times : \langle p \rangle) < \infty$. □

By Igusa's theorem we have now that $G(l^i) = \{A \in \mathrm{GL}(2, l^i) \mid \det A \in \langle p \rangle\}$. Taking the inverse limit we get $G(l^\infty) = \{A \in \mathrm{GL}(2, \mathbf{Z}_l) \mid \det A \in \langle p \rangle\}$. It follows that $\mathrm{GL}(2, \mathbf{Z}_l)/G(l^\infty) \cong \mathbf{Z}_l^\times/\langle p \rangle$.

This together with Lemma 3.2 implies that $G(l^\infty)$ is a closed subgroup of $\mathrm{GL}(2, \mathbf{Z}_l)$ of a finite index. Now, $S(G(l^\infty), \mathbf{Z}_l^2)$ is contained in $S(\mathrm{GL}(2, \mathbf{Z}_l), \mathbf{Z}_l^2)$, which is a zero set in $\mathrm{GL}(2, \mathbf{Z}_l)$, by Lemma 2.2. Therefore $S(G(l^\infty), \mathbf{Z}_l^2)$, hence also in $G(l^\infty)$. □

3.4. *Proof of* (C″) *for* $l = p$

We have to prove that $E_{p^\infty}(\tilde{K}(\sigma))$ is finite for almost all $\sigma \in G(K)$. Indeed, by a well known result of Hasse $E_{p^i} \cong \mathbf{Z}/p^i\mathbf{Z}$ for every $i \geqq 1$ (cf. Robert [22, p. 123]; note that E is not super singular, since j is not algebraic over $\mathbf{F}_p$). The field $K_{p^i} = K(E_{p^i})$ is now not Galois over K but it is still normal over K. Denote by K'_{p^i} the maximal separable extension of K contained in K_{p^i}. Igusa proved in [9] that $[K'_{p^i} : K] \geqq \frac{1}{2}p^i(p-1)$. Hence, the maximal separable extension K'_{p^∞} of K contained in K_{p^∞} is of infinite degree. In particular it follows that $G(K'_{p^\infty})$ is a zero set in $G(K)$.

Let now σ be an element of $G(K)$ such that $E_{p^\infty}(\tilde{K}(\sigma))$ is infinite. It suffices to prove that $\sigma \in G(K'_{p^\infty})$. Indeed, the unique extension σ' of σ to $\tilde{K}$ fixes infinitely many points of E_{l^∞}. If σ' fixes a point in $E_{p^i} - E_{p^{i+1}}$, then σ' fixes all the points in E_{p^i}, since E_{p^i} is cyclic. It follows that σ' fixes all the points of E_{l^∞}. Hence $\sigma \in (K'_{p^\infty})$.

The proof of Proposition 1.2 is completed in case II.

§4. Elliptic curves with complex multiplication over a number field

4.1. *The endomorphism ring*

We consider in this chapter an elliptic curve E defined over a number field $K = \mathbf{Q}(j)$. We assume that E *has a complex multiplication.* Then its endomorphism ring, $\mathrm{End}\, E$, is isomorphic to an order S of an imaginary quadratic extension L_0 of $\mathbf{Q}$. The curve E itself has an analytic representation $E \cong \mathbf{C}/\mathfrak{a}$, where $\mathfrak{a}$ is a lattice of $\mathbf{C}$ which is contained in L_0 and $S = \{s \in L_0 \mid s\mathfrak{a} \subseteq \mathfrak{a}\}$. Moreover, if a point P of E corresponds to a coset $z + \mathfrak{a}$ and the endomorphism λ corresponds to the element s of S, then the point $\lambda(P)$ corresponds to the coset $sz + \mathfrak{a}$ (cf. Shimura [26, p. 104]).

The ring S is contained in the ring of integers S_0 of L_0. Indeed it has the form $S = Z + fS_0$, where the positive integer f is the *conductor* of S. The ring S_0 can be represented as $S_0 = \mathbf{Z}[w_0]$. Hence S has the form $S = \mathbf{Z}[w]$, where $w = fw_0$, and w satisfies an irreducible equation $X^2 - gX - h = 0$, where $g, h \in \mathbf{Z}$. Further, if δ_0 is the discriminant of S_0, then $\delta = f^2\delta_0$ is the discriminant of S.

For every prime l consider the quotients ring

$$S_{(l)} = \left\{\frac{s}{n}\,\middle|\, s \in S \quad \text{and} \quad n \in \mathbf{Z} - l\mathbf{Z}\right\} \quad \text{and the } S_{(l)}\text{-module}$$

$$\mathfrak{a}_{(l)} = \left\{\frac{a}{n}\,\middle|\, a \in \mathfrak{a} \quad \text{and} \quad n \in \mathbf{Z} - l\mathbf{Z}\right\}.$$

It is known that there exists an element $c_l \in \mathfrak{a}_{(l)}$ such that

$$\mathfrak{a}_{(l)} = c_l S_{(l)} \tag{1}$$

(cf. Lang [16, p. 98]). This implies that

$$\mathfrak{a}/n\mathfrak{a} \cong_S S/nS \tag{2}$$

for every positive integer n.

For odd primes l that do not divide the discriminant δ of S, the ring $S_{(l)}$ coincides with the localization of S_0 with respect to l. There are therefore two types of such l's:

(i) $(\delta/l) = 1$. Then there are in S two prime ideals over l, each of degree 1 and

$$((S/lS)^\times, S/lS) \cong (\mathbf{F}_l^{\times 2}, \mathbf{F}_l^2). \tag{3}$$

In particular $|S/lS)^\times| = (l-1)^2$.

(ii) $(\delta/l) = -1$. Then there is only one prime ideal over l, its degree is 2, and $((S/lS)^\times, S/lS) \cong (\mathbf{F}_{l^2}^\times, \mathbf{F}_{l^2})$. In particular

$$|(S/lS)^\times| = l^2 - 1.$$

Moreover, the polynomial $X^2 - gX - h$ remains irreducible modulo l and $\mathbf{F}_{l^2} = \mathbf{F}_l[\bar{w}]$, where $\bar{w}^2 - g\bar{w} - h = 0$.

4.2. *Embedding of H_n in $(S/nS)^\times$*

Let $L = L_0K$ and for every n let $L_n = LK_n = L(E_n)$. Write $G_n = \mathcal{G}(K_n/K)$ and $H_n = \mathcal{G}(L_n/L)$. If $L \subseteq K_n$, then $K_n = L_n$ and H_n is a subgroup of G_n of index $[L : K]$, i.e. 1 or 2. If $L \not\subseteq K_n$, then L is linearly disjoint from K_n over K and the restriction map induces an isomorphism $(H_n, E_n) \cong (G_n, E_n)$. We shall first examine the permutation groups (H_n, E_n) and then imply the accumulated information on the permutation groups (G_n, E_n).

We note first that the analytic presentation $E = \mathbf{C}/\mathfrak{a}$ induces the analytic presentation $E_n = (1/n)\mathfrak{a}/\mathfrak{a}$. The elements of H_n fix the elements of $\operatorname{End} E = S$. Moreover, they operate faithfully on E_n. Hence there is an embedding $(H_n, E_n) \to (\mathrm{Aut}_{\mathrm{End}\,E}\, E_n, E_n)$. Further

$$\begin{aligned}(\mathrm{Aut}_{\mathrm{End}\,E}\, E_n, E_n) &\cong (\mathrm{Aut}_S\, (\tfrac{1}{n}\mathfrak{a}/\mathfrak{a}), \tfrac{1}{n}\mathfrak{a}/\mathfrak{a})\\ &\cong (\mathrm{Aut}_S\, S/nS, S/nS) \cong ((S/nS)^\times, S/nS),\end{aligned}$$

by (2). Hence we get an embedding

$$(H_n, E_n) \to ((S/nS)^\times, S/nS). \tag{4}$$

We write $((S/nS)^\times : H_n)$ for the index of the image of H_n in $(S/nS)^\times$. This index will be proved to be bounded in the next two sections.

4.3. *Class field theory*

Consider the Weierstrass normal form of $E : Y^2 = 4X^3 - g_2X - g_3$. Then the discriminant of E is given by $\Delta = g_2^3 - 27g_3^2$. The *Weber function* of E is defined on a point (x, y) of E by

$$h(x, y) = \begin{cases} \Delta^{-1} g_2 g_3 x, & \text{if } g_2 g_3 \neq 0,\\ \Delta^{-1} g_2^2 x^2, & \text{if } g_3 = 0,\\ \Delta^{-1} g_3 x^3, & \text{if } g_2 = 0.\end{cases}$$

This function is independent of the selected Weierstrass normal form of E. It obtains the same value on points which are obtained from one another by $\operatorname{Aut} E$. Let $L'_n = L(hE_n)$. The L'_n are shown to be class fields over L_0 of certain open subgroups of the idèle group of L_0. In this section we describe these subgroups and deduce some of their properties.

For every prime l let $L_{0,l} = L_0 \otimes_{\mathbf{Q}} \mathbf{Q}_l$,

$$\begin{aligned} S_l &= S_{(l)} \otimes \mathbf{Z}_l = S \otimes \mathbf{Z}_l = \varprojlim S/l^i S, \qquad \text{and}\\ \mathfrak{a}_l &= \mathfrak{a}_{(l)} \otimes \mathbf{Z}_l = \mathfrak{a} \otimes \mathbf{Z}_l = \lim \mathfrak{a}/l^i \mathfrak{a}.\end{aligned}$$

Then $\mathfrak{a}_l = c_l S_l$ by (1), hence $S_l = \{s \in L_{0,l} \mid s\mathfrak{a}_l \subseteq \mathfrak{a}_l\}$.

Consider now the *adèle* ring $\mathbf{Q}_A$ of $\mathbf{Q}$ defined as the restricted product $\mathbf{Q}_A = \mathbf{R} \times \Pi(\mathbf{Q}_l, \mathbf{Z}_l)$. The *adèle* ring of L_0 can be then written as $L_{0,A} = L_0 \otimes_{\mathbf{Q}} \mathbf{Q}_A = \mathbf{C} \times \Pi(L_{0,l}, S_l)$. It contains L_0 as a discrete subring. The group of units $L_{0,A}^\times$ is the *idèle* group of L_0; $J = L_{0,A}^\times = \mathbf{C}^\times \times \Pi(L_{0,l}^\times, S_l^\times)$.

Let further $S_A = \mathbf{C}^\times \times \Pi S_l$. Then $L_0 \cap S_A = S$ and hence $S \cap nS_A = nS$ for every n. Moreover $S_A = S + nS_A$. Hence

$$S_A / nS_A \cong S/nS. \tag{5}$$

Denote the group of unites of S_A by $W = S_A^\times = \mathbf{C}^\times \times \Pi S_l^\times$. It is an open subgroup of J. Then $S_A = \{s \in L_{0,A} \mid s\mathfrak{a} \subseteq \mathfrak{a}\}$ and $W = \{s \in S_A \mid s\mathfrak{a} = \mathfrak{a}\}$, where $s\mathfrak{a} \subseteq \mathfrak{a}$ and $s\mathfrak{a} = \mathfrak{a}$ mean that $s_l\mathfrak{a}_l \subseteq \mathfrak{a}_l$ and $s_l\mathfrak{a}_l = \mathfrak{a}_l$, respectively, for every l. The group W contains for every positive integer n the open subgroup $W_n = \{s \in W \mid s \equiv 1 \bmod nS_A\}$.

Attached to this subgroup is the following exact sequence:

$$1 \to W \cap L_0^\times / W_n \cap L_0^\times \to W/W_n \to WL_0^\times / W_nL_0^\times \to 1. \tag{6}$$

We shall identify the components of this short sequence with some familiar groups.

We start from $WL_0^\times / W_nL_0^\times$ and note that the proof of the corollary on page 135 of Lang [16], together with theorem 5.5 on page 122 of Shimura [26], can be used to prove:

Lemma 4.1. *$L'_n = L_0(W_n)$ is the class field of the idèle group W_n over L_0. In particular $L = L_0(W)$ is the class field of W over L_0.*

It follows from Lemma 4.1 and from class field theory that

$$WL_0^\times / W_nL_0^\times \cong \mathcal{G}(L'_n/L) = H'_n. \tag{7}$$

Next note that if $a, b \in S_l$ and $ab \equiv 1 \bmod lS_l$, then $a, b \in S_l^\times$. It follows that $W/W_n \cong (S_A/nS_A)^\times$ and by (5) we obtain that

$$W/W_n \cong (S/nS)^\times. \tag{8}$$

Observe also that $S^\times = W \cap L_0^\times$. Therefore, taking into account (6), (7) and (8) we obtain an exact sequence $S^\times \to (S/nS)^\times \to H'_n \to 1$. Thus, a quotient group of H_n has been represented as a quotient group of $(S/nS)^\times$ with a bounded kernel. Indeed, $S^\times$ is contained in the ring of unites $S_0^\times$ of S_0 and

$$|S_0^\times| = \begin{cases} 2, & \text{if } L_0 \neq \mathbf{Q}(\sqrt{-1}), \mathbf{Q}(\sqrt{-3}), \quad \text{i.e. if } j \neq 0, 12^3, \\ 4, & \text{if } L_0 = \mathbf{Q}(\sqrt{-1}), \quad \text{i.e. if } j = 12^3, \\ 6, & \text{if } L_0 = \mathbf{Q}(\sqrt{-3}), \quad \text{i.e. if } j = 0 \end{cases}$$

(cf. Shimura [26, p. 106]). Hence $|S^\times|$ is equal to 1, 2, 3, 4 or 6. If one adds to this result the fact that H_n was embedded in $(S/nS)^\times$ (see (4) of section 4.2), one can easily deduce the following

Proposition 4.2. *Let E be an elliptic curve with complex multiplication defined over $K = \mathbf{Q}(j)$. Let $S = \operatorname{End} E$, let L_0 be the quotient field of S and let $L = L_0(j)$. For every n let $L'_n = L(hE_n)$, $L_n = L(E_n)$, $H'_n = \mathcal{G}(L'_n/L)$ and $H_n = \mathcal{G}(L_n/L)$. Then (H_n, E_n) can be embedded in $((S/nS)^\times, (S/nS))$ and*

$$[L_n : L'_n] \cdot ((S/nS)^\times : H_n) = \begin{cases} 1 \text{ or } 2, & \text{if } j \neq 0, 12^3, \\ 1, 2 \text{ or } 4, & \text{if } j = 12^3, \\ 1, 2, 3 \text{ or } 6, & \text{if } j = 0. \end{cases}$$

4.4. *Linearly disjoint fields*

Lemma 4.3. *If n and m are relatively prime positive integers, then L'_n and L'_m are linearly disjoint over L.*

Proof. Observe that $W_n W_m = W$. Hence $L_0(W_n) \cap L(W_m) = L_0(W) = L$, by class field theory, i.e. L'_n and L'_m are linearly disjoint over L. □

In order to deduce the linear disjointness of the L_n from that of the L'_n we need the concept of the Frattini group $\Phi(G)$ of a finite group G and the following

Lemma 4.4. *For $i = 1, 2, \cdots, n$ let $N_i \supseteq N'_i$ be finite Galois extensions of a field M such that $\mathcal{G}(N_i/N'_i) \subseteq \Phi(\mathcal{G}(N_i/M))$. If $N'_1, \cdots, N'_n$ are linearly disjoint over M, then $N_1, \cdots, N_n$ are also linearly disjoint over M.*

Proof. Let $J_i = \mathcal{G}(N_i/M)$, $\bar{J}_i = \mathcal{G}(N'_i/M)$ and $A_i = \mathcal{G}(N_i/N'_i)$. Denote by N and N' the fields generated by $N_1, \cdots, N_n$ and $N'_1, \cdots, N'_n$ respectively and let $J = \mathcal{G}(N/M)$ and $\bar{J} = \mathcal{G}(N'/M)$. Then J can be considered as a subgroup of the direct product $\prod_{i=1}^n J_i$, and $\bar{J} = \prod_{i=1}^n \bar{J}_i$, since $N'_1, \cdots, N'_n$ are linearly disjoint over M. It follows that $J \cdot \prod_{i=1}^n A_i = \prod_{i=1}^n J_i$. Next we have $\prod_{i=1}^n A_i \subseteq \prod_{i=1}^n \Phi(J_i) = \Phi(\prod_{i=1}^n J_i)$ (see Huppert [7, p. 275]). Hence $J = \prod_{i=1}^n J_i$, by the fundamental property of Frattini groups (see [7, p. 268]). Hence $N_1, \cdots, N_n$ are linearly disjoint over M. □

Lemma 4.5. *If $l \equiv 1 \bmod 72\delta$, then $\mathcal{G}(L_l/L'_l) \subseteq \Phi(H_l)$.*

Proof. Our assumption implies that $(l/\delta) = 1$. Hence, by section 4.1 we have $(S/lS)^\times \cong (\mathbf{Z}/(l-1)\mathbf{Z})^2$. If $L'_l = L_{l'}$ there is nothing to prove. Suppose therefore that $[L_l : L'_l] > 1$.

If $j \neq 0, 12^3$ then $[L_l : L'_l] = 2$ and $H_l \cong (S/lS)^\times$, by Proposition 4.2. Hence $H_l \cong (\mathbf{Z}/2^r\mathbf{Z})^2 \oplus C$, where $r \geqq 3$ and C has an odd order. It follows that $\Phi(H_l) \cong (\mathbf{Z}/2^{r-1}\mathbf{Z})^2 \oplus \Phi(C)$, hence $\mathscr{G}(L_l/L'_l) \subseteq \Phi(H_l)$.

If $j = 12^3$, then $[L_l : L'_l] = 2$ and $((S/lS)^\times : H_l) \leqq 2$, or $[L_l : L'_l] = 4$ and $H_l \cong (S/lS)$. In the first case H_l is isomorphic to $\mathbf{Z}/2^{r'}\mathbf{Z} \oplus \mathbf{Z}/2^{r''}\mathbf{Z} \oplus C$, where $r', r'' \geqq 2$ and we still have that $\mathscr{G}(L/L'_l) \subseteq \Phi(H_l)$. The second case is treated as the case $j \neq 0, 12^3$.

The case $j = 0$ is proved analogously. One treats the 2-factors and the 3-factors separately. □

Combining Lemmas 4.3, 4.4 and 4.5 together we get:

Lemma 4.6. *The sequence of fields* $\{L_l \mid l \equiv 1 \bmod 72\delta\}$ *is linearly disjoint over* L.

Lemma 4.7. *There exist at most two primes* l_i *such that*

(9) $$l_i \equiv 1 \bmod 72\delta \quad \textit{and} \quad ((S/l_iS)^\times : H_{l_i}) \geqq 2.$$

Proof. Indeed, assume that there were three primes l_i, for $i = 1, 2, 3$, satisfying (9). Let $n = l_1l_2l_3$. By Lemma 4.6 we have $H_n \cong \prod_{i=1}^3 H_{l_i}$. Also $(S/nS)^\times \cong \prod_{i=1}^3 (S/l_iS)^\times$. Hence, by Proposition 4.2

$$8 \leqq \prod_{i=1}^{3} \frac{|S/l_iS)^\times|}{|H_{l_i}|} = \frac{|(S/nS)^\times|}{|H_n|} \leqq 6,$$

which is a contradiction. □

By Lemma 4.7 and by (3) we have for all primes $l \equiv 1 \bmod 72\delta$, except possibly for two, that

(10) $$(H_l, E_l) = (\mathbf{F}_l^{\times 2}, \mathbf{F}_l^2).$$

We split these primes into a set Λ' with $L \not\subseteq K$ or $L_0 \subseteq K_l$, and a set Λ'' with $L \subseteq K_l$ and $L_0 \not\subseteq K$. Then (i) $\sum_{l \in \Lambda'} 1/l = \infty$ or (ii) $\sum_{l \in \Lambda''} 1/l = \infty$, by Dirichlet's Theorem.

4.5. *Proof of* (A′) *in case* (i)

In this case $\sum_{l \in \Lambda'} 1/l = \infty$. Let $l \in \Lambda'$. Then L is linearly disjoint from K_l over K. Hence $(G_l, E_l) \cong (H_l, E_l) = (\mathbf{F}_l^{\times 2}, \mathbf{F}_l^2)$, by (10). Hence $|S(G_l, E_l)| = 2l - 3$ (see example 2 in section 1.5). It follows that for $l \in \Lambda'$

$$\frac{|S(G_l, E_l)|}{|G_l|} = \frac{2l - 3}{(l-1)^2} > \frac{2}{l}.$$

Condition (A′1) follows.

In order to prove (A′2) it suffices to prove that the set of fields $\{K_l \mid l \in \Lambda'\}$ is linearly disjoint over K. Note that by Lemma 4.6 the set of fields $\{L_l \mid l \in \Lambda'\}$ is linearly disjoint over L. Hence it suffices to prove

LEMMA 4.8. *Let L be a finite extension of a field K. Let $K_i, \cdots, K_r$ be finite extensions of K and let $L_i = K_iL$. Suppose that K_i is linearly disjoint from L over K for $i = 1, \cdots, r$, and $L_i, \cdots, L_r$ are linearly disjoint over L. Then $K_1, \cdots, K_r$ are linearly disjoint over K.*

PROOF.

$$[K_1 \cdots K_r : K] \geqq [L_1 \cdots L_r : L] = \prod_{i=1}^{r} [L_i : L] = \prod_{i=1}^{r} [K_i : K] \geqq [K_1 \cdots K_r : K]$$

$$\Rightarrow [K_1 \cdots K_r : K] = \prod_{i=1}^{r} [K_i : K]$$

$$\Rightarrow K_1, \cdots, K_r \text{ are linearly disjoint over } K.$$

4.6. *Some matrices computations*

Let R be an integral domain. Then

$$(R^{\times 2}, R^2) \cong (D, R^2), \tag{11}$$

where $D = D(R)$ is the group of all diagonal matrices in $\mathrm{GL}(2, R)$. Consider the set $C = C(R)$ that consists of D and all the antidiagonal matrices

$$\begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} \qquad b, c \in R^{\times}. \tag{12}$$

It is easy to see that C is a subgroup of $\mathrm{GL}(2, R)$ and $(C : D) = 2$.

LEMMA 4.9. *Let H be a subgroup of D and let G be a subgroup of* $\mathrm{GL}(2, R)$ *that contains H such that $(G : H) \leqq 2$. If $|R^{\times}| > (D : H)$, then G is contained in C. In particular, if $|R^{\times}| \geqq 2$, then C is the unique subgroup of* $\mathrm{GL}(2, R)$ *that contains D as a subgroup of index* 2.

PROOF. It suffices to consider a matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

in $G - D$ and to prove that $a = d = 0$. Indeed, $A^2 \in D$. Hence $b(a + d) = 0$ and $c(a + d) = 0$.

Next we have that

$$(13) \qquad b \neq 0 \quad \text{or} \quad c \neq 0.$$

Hence $a = -d$.

Next observe that the condition $|R^\times| > (D:H)$ implies that H contains a matrix of the form

$$\begin{pmatrix} u & 0 \\ 0 & v \end{pmatrix} \qquad u, v \in R^\times, \quad u \neq v.$$

The matrix A acts on H. Hence there exist $u', v' \in R^\times$ such that

$$A^{-1}\begin{pmatrix} u & 0 \\ 0 & v \end{pmatrix} A = \begin{pmatrix} u' & 0 \\ 0 & v' \end{pmatrix}$$

$\Rightarrow$

$$(14) \qquad ua = u'a \quad \text{and} \quad va = v'a \quad \text{and} \quad vc = u'c \quad \text{and} \quad ub = v'b.$$

If $a \neq 0$, then $u = u'$ and $v = v'$. Hence, by (13) and (14), $u = v$, which is a contradiction. Hence $a = 0$ and A has the form (12.) □

A matrix A of C belongs to $S(C, R^2)$ if and only if it has the characteristic value 1. Hence

LEMMA 4.10. *The set $S(C, R^2)$ consists of the matrices having one of the forms*:

$$\begin{pmatrix} u & 0 \\ 0 & 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 1 & 0 \\ 0 & u \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 0 & u \\ u^{-1} & 0 \end{pmatrix},$$

where $u \in R^\times$.

4.7. *Proof of* (A″) *in case* (ii)

In this case $\Sigma_{l \in \Lambda''} 1/l = \infty$. Let $l \in \Lambda''$. Then $[L : K] = 2$ and $K_l = L_l$. Hence H_l is a subgroup of G_l of index 2. Also, we have by (10) and (11) that $(H_l, E_l) \cong (D(l), \mathbf{F}_l^2)$, where $D(l) = D(\mathbf{F}_l)$ is the subgroup of $\mathrm{GL}(2, l)$ consisting of all diagonal matrices. This isomorphism can be uniquely extended to an isomorphism $(G_l, E_l) \cong (G(l), \mathbf{F}_l^2)$, where $G(l)$ is a subgroup of $G(2, l)$ (see section 1.4). Clearly $G(l)$ contains $D(l)$ as a subgroup of index 2. Hence $G(l) = C(l) = C(\mathbf{F}_l)$, by Lemma 5.9.

Define now the set $S'(G(l), \mathbf{F}_l^2)$ to be the set consisting of all matrices in $G(l)$ of the form

$$\begin{pmatrix} 1 & 0 \\ 0 & v \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 0 & b \\ b^{-1} & 0 \end{pmatrix}.$$

Then $S'(G(l),\mathbf{F}_l^2) \subseteq S(G(l),\mathbf{F}^2)$, by Lemma 4.10. Further we have $|S'(G(l),\mathbf{F}_l^2)| = 2(l-1)$. Hence

$$\frac{|S'(G(l),\mathbf{F}_l^2)|}{|G(l)|} = \frac{1}{l-1} > \frac{1}{l}. \tag{15}$$

Statement (A″1) follows. We proceed now with the proof of (A″2). Consider $l_1,\cdots,l_r \in \Lambda''$ and let $n = l_1\cdots l_r$.

Lemma 4.11. *$(G_n,E_n)\cong(G(n),(\mathbf{Z}/n\mathbf{Z})^2)$, where $G(n)$ is the subgroup of $G(2,n)$ consisting of the diagonal matrices and all the matrices of the form*

$$\begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} \tag{16}$$

Proof. For every $1 \leqq j \leqq r$ we have the isomorphism

$$(G_{l_j},E_{l_j})\cong(C(l_j),(\mathbf{Z}/l_j\mathbf{Z})^2). \tag{17}$$

Let P_j and Q_j be the points of E_{l_j} which are mapped on $(1,0)$ and $(0,1)$ respectively. Then (17) is induced by (P_j,Q_j). We know that $E_n = \bigoplus_{j=1}^r E_{l_j}$, where the projection $E_n \to E_{l_j}$ is induced by multiplication by n/l_j. It follows that one can choose generators P,Q for E_n such that

$$\frac{n}{l_j}P = P_j \quad\text{and}\quad \frac{n}{l_j}Q = Q_j \qquad \text{for } j = 1,\cdots,r.$$

Thus we obtain the following commutative diagrams:

$$\begin{tikzcd}
(G_n,E_n) \arrow[rr, "\cong"] \arrow[dd] & & (G_1(n),(\mathbf{Z}/n\mathbf{Z})^2) \arrow[dd] & \\
& (H_n,E_n) \arrow[ul, hook'] \arrow[rr, "\cong"] \arrow[dd] & & (D_1(n),(\mathbf{Z}/n\mathbf{Z})^2) \arrow[ul, hook'] \arrow[dd] \\
(G_{l_j},E_{l_j}) \arrow[rr, "\cong"] & & (C(l_j),(\mathbf{Z}/l_j\mathbf{Z})^2) & \\
& (H_{l_j},E_{l_j}) \arrow[ul, hook'] \arrow[rr, "\cong"] & & (D(l_j),(\mathbf{Z}/l_j\mathbf{Z})^2) \arrow[ul, hook']
\end{tikzcd}$$

where $D_1(n) \subseteq G_1(n)$ are subgroups of $\mathrm{GL}(2,n)$. Now, $K_{l_1},\cdots,K_{l_r}$ are linearly disjoint over L, by Lemma 4.6. Hence $D_1(n)$ is equal to $D(n)$, the group of all diagonal matrices in $\mathrm{GL}(2,n)$.

Let now $\sigma \in G_n - H_n$ and let

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

be the matrix in $G_1'(n)$ that corresponds to σ under the above isomorphism. Then $\sigma \mid K_{l_j} \in G_{l_j} - H_{l_j}$ for $j = 1, \cdots, r$. Hence if we denote by A_j the matrix A modulo l_j we get that

$$\begin{aligned} & A_j \in C(l_j) - D(l_j) && \text{for } j = 1, \cdots, r. \\ & \Rightarrow a \equiv d \equiv 0 \bmod l_j && \text{for } j = 1, \cdots, r. \\ & \Rightarrow a \equiv d \equiv 0 \bmod n. \end{aligned}$$

This means that A has the form (16).

We have thus proved that $D(n) \subset G_1(n) \subseteq G(n)$. One observes that the elements b and c appearing in (16) must be invertible in $\mathbf{Z}/n\mathbf{Z}$. It follows that $(G(n):D(n)) = 2$. Hence $G_1(n) = G(n)$. □

We consider now the set $S'(n)$ consisting of all matrices A in $G(n)$ that, when reduced modulo l_j, belong to $S'(G(l_j), (\mathbf{Z}/l_j\mathbf{Z})^2)$, for $j = 1, \cdots, r$. By Lemma 4.11, and by the Chinese Remainder Theorem, $S'(n)$ consists of all the matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & v \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & b \\ b^{-1} & 0 \end{pmatrix} \quad \text{where } v, b \in (\mathbf{Z}/n\mathbf{Z})^\times.$$

Hence

$$|S'(n)| = 2\prod_{j=1}^{r} (l_j - 1). \tag{18}$$

Moreover,

$$[K_n : K] = [L : K][K_n : L] = 2\prod_{j=1}^{r} (l_j - 1)^2, \tag{19}$$

by Lemma 4.6. Hence, by (15), (18) and (19) we get

$$\frac{|S'(n)|}{|G(n)|} = \prod_{j=1}^{r} \frac{|S'(G(l_j), (\mathbf{Z}/l_j\mathbf{Z})^2)|}{|G(l_j)|}.$$

This is exactly statement (A″2).

The proof of (A″) is thus completed.

4.8. *More matrices computations*

Let R be an integral domain and let w be an element of a field extension of R satisfying an equation $w^2 - gw - h = 0$, where g and h are elements of R such that $X^2 - gX - h$ is irreducible over the quotient field of R. Every element of $R[w]$ can be uniquely represented in the form $x + yw$, where $x, y \in R$. The map $x + yw \rightarrow (x, y)$ is therefore an additive group isomorphism of $R[w]$ onto R^2. Using the formula $(a + bw)(x + yw) = (ax + byh) + (bx + ay + byg)w$ one can prove directly that

$$(R[w]^{\times}, R[w]) = (I, R^2), \tag{20}$$

where $I = I(R)$ is the subgroup of $\mathrm{GL}(2, R)$ consisting of all the matrices

$$B = \begin{pmatrix} a & bh \\ b & a + bg \end{pmatrix}. \tag{21}$$

In this isomorphism an element $a + bw$ of $R[w]^{\times}$ is mapped onto the matrix B.

Define now $J = J(R)$ to be the subgroup of $\mathrm{GL}(2, R)$ consisting of I and all the matrices

$$\begin{pmatrix} x & xg - zh \\ z & -x \end{pmatrix}.$$

Note that $J - I$ is not empty since it contains the matrix with $z = 0$ and $x = 1$.

LEMMA 4.12. *Let H be a subgroup of I and let G be a subgroup of* $\mathrm{GL}(2, R)$ *that contains H such that $(G : H) \leqq 2$. If $(R[w]^{\times} : R^{\times}) > (I : H)$, then G is contained in J. In particular, if $(R[w]^{\times} : R^{\times}) \geqq 2$, then J is the unique subgroup of* $\mathrm{GL}(2, R)$ *that contains I as a subgroup of index* 2.

PROOF. It suffices to consider a matrix

$$A = \begin{pmatrix} x & y \\ z & u \end{pmatrix}$$

in $G - I$ and to prove that it belongs to J. Indeed, $A^2 \in I$, hence

$$(x + u)(y - zh) = 0 \qquad \text{and} \qquad (x + u)(x - u + zg) = 0. \tag{22}$$

If $x + u \neq 0$, then (22) implies that $y = zh$ and $u = x + zg$, hence $A \in I$, against our assumption. It follows that $x = -u$, i.e.

$$A = \begin{pmatrix} x & y \\ z & -x \end{pmatrix}.$$

Next note that the assumption $(R[w]^{\times} : R^{\times}) > (I : H)$ implies that H contains a non-scalar matrix, i.e. a matrix B of the form (21) in which $b \neq 0$. The matrix A acts on H. Hence, there exists a matrix $B_1 \in H$ such that $A^{-1}BA = B_1$. Hence $ABA = A^2B_1 \in I$.

Now

$$ABA = \begin{pmatrix} x^2a + xyb + xzbh + yza + yzbg & xya + y^2b - x^2bh - xya - xybg \\ xza - x^2b + z^2bh - xza - xzbg & yza - xyb - xzbh + x^2a + x^2bg \end{pmatrix}.$$

Hence

$$xya + y^2b - x^2bh - xya - xybg = xzah - x^2bh + z^2bh^2 - xzah - xzbgh, \tag{23}$$

$$x^2a + xyb + xzbh + yza + yzbg + xzag - x^2bg + z^2bgh - xzag - xzbg^2 \tag{24}$$
$$= yza - xyb - xzbh + x^2a + x^2bg.$$

The condition $b \neq 0$ implies that (23) and (24) can be rewritten as

$$(y - zh)(y + zh - xg) = 0, \qquad \text{and} \qquad (2x + zg)(y + zh - xg) = 0.$$

If $y + zh - xg \neq 0$, then $y = zh$ and $2x + zg = 0$, hence $A \in I$, against our assumption. It follows that $y = xg - zh$. □

LEMMA 4.13. *In the above notation, $S(J, R^2)$ consists of the unit matrix and the subset W of $J - I$, of all matrices with determinant -1. Moreover, if u runs over a set of representatives in $R^\times$ modulo $\{\pm 1\}$, then uW is a disjoint union and it is contained in $J - I$.*

PROOF. Clearly $S(J, R^2) = S(I, R^2) \cup S(J - 1, R^2)$. Also $S(R[w]^\times, R[w])$ consists of 1 only, since $R[w]$ is an integral domain. Hence $S(I, R^2)$ consists of the unit matrix only, by (20).

Now, a matrix

$$A = \begin{pmatrix} x & xg - zh \\ z & -x \end{pmatrix}$$

of $J - I$ belongs to $S(J - I, R^2)$ if and only if it has the characteristic value 1. This happens exactly if $\det A = -1$.

If $u \in R^\times$ and $A \in J - I$, then $uA \in J - I$ and $\det(uA) = -u^2$. It follows that if $v \in R^\times$ and $v \neq \pm u$, then $uA \cap vA = \varnothing$. This proves our second assertion. □

4.9. *Proof of* (B″)

We consider only primes $l > 7$ that do not divide the discriminant δ of S and distinguish between two cases:

Case i. $(\delta/l) = 1$. By Lemma 4.2, (H_l, E_l) can be embedded in $((S/lS)^\times, S/lS)$ such that $((S/lS)^\times : H_l) \leqq 6$. Further $((S/lS)^\times, S/lS) \cong (D(l), \mathbf{F}_l^2)$, by (3) and (11). Here $D(l) = D(\mathbf{F}_l)$, in the notation of section 4.6. It follows that

$$(H_l, E_l) \cong (H(l), \mathbf{F}_l^2), \tag{25}$$

where $H(l)$ is a subgroup of $D(l)$ of index $\leqq 6$. Further, (H_l, E_l) can be considered as a subgroup of (G_l, E_l) of index $\leqq 2$. The isomorphism (25) can be therefore extended to an isomorphism $(G_l, E_l) \cong (G(l), \mathbf{F}_l^2)$, where $H(l) \subseteq G(l) \subset \mathrm{GL}(2, l)$ and $(G(l) : H(l)) \leqq 2$. Also $|\mathbf{F}_l^\times| = l - 1 > 6 \geqq (D(l) : H(l))$. It follows from Lemma 4.9 that $G(l) \subseteq C(l)$, where $C(l) = C(\mathbf{F}_l)$, in the notation of section 4.6. The index of $G(l)$ in $C(l)$ is certainly not greater than 12. Hence

$$|G(l)| \geqq \tfrac{1}{6}(l-1)^2. \tag{26}$$

Moreover $S(G(l), \mathbf{F}_l^2) \subseteq S(C(l), \mathbf{F}_l^2)$ and the last set consists, by Lemma 4.10, of all the matrices

$$\begin{pmatrix} u & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & u \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & u \\ u^{-1} & 0 \end{pmatrix},$$

where $u \in \mathbf{F}_l^\times$. Their number is $3(l-1) - 1$. Hence

$$\frac{|S(G(l), \mathbf{F}_l^2)|}{|G(l)|} \leqq \frac{6(3(l-1)-1)}{(l-1)^2} < \frac{20}{l}$$

by (26). This is the desired inequality in (B″) for case i.

Case ii. $(\delta / l) = -1$. As in case i, one proves, by the end of section 4.1, Lemma 4.2 and Lemma 4.12, that the following diagram of groups holds in $\mathrm{GL}(2, l)$:

$$\begin{tikzcd}
G(l) \arrow[r, dash, "\leqq 12"] \arrow[d, dash, "\leqq 2"'] & J(l) \arrow[d, dash, "2"'] \\
H(l) \arrow[r, dash, "\leqq 6"'] & I(l)
\end{tikzcd}$$

Here $H(l)$ and $G(l)$ are, as above, the images of H_l and G_l, respectively, $I(l) = I(\mathbf{F}_l)$ and $J(l) = J(\mathbf{F}_l)$, in the notation of Section 4.8. Now $|J(l)| = 2|I(l)| = 2|\mathbf{F}_{l^2}^\times| = 2(l^2 - 1)$. Hence

$$|G(l)| \geqq \frac{l^2 - 1}{6}. \tag{27}$$

Next we know, by Lemma 4.13, that $S(J(l), \mathbf{F}_l^2)$ consists of the unit matrix and the subset $W(l)$ of $J(l) - I(l)$ of all matrices with determinant -1. Moreover, if we let u run over a set of representatives of $\mathbf{F}_l^\times / \{\pm 1\}$, then $\bigcup uW(l)$ is a disjoint union in $J(l) - I(l)$. Since $|\mathbf{F}_l^\times / \{\pm 1\}| = \frac{1}{2}(l-1)$, we obtain that

$$\frac{l-1}{2}\,|W(l)|\leqq l^2-1.$$

Hence $|W(l)|\leqq 2(l+1)$, hence

$$|S(J(l),\mathbf{F}_l^2)|\leqq 2(l+1)+1. \tag{28}$$

It follows from (27) and (28) that

$$\frac{|S(G(l),\mathbf{F}_l^2)|}{|G(l)|}\leqq\frac{6(2(l+1)+1)}{l^2-1}<\frac{20}{l}.$$

This is the desired inequality for the case ii. The proof of (B″) is now completed.

4.10. *Proof of* (C″)

Let l be a prime. We embed (G_{l^∞},T_l) in $(\mathrm{GL}(2,\mathbf{Z}_l),\mathbf{Z}_l^2)$ and show that $S(G(l^\infty),\mathbf{Z}_l^2)$ is a zero set in $G(l^\infty)$.

Let $L_{l^\infty}=L(E_{l^\infty})$ and let $H_{l^\infty}=\mathcal{G}(L_{l^\infty}/L)$. Then H_{l^∞} can be considered as a subgroup of G_{l^∞} of index $\leqq 2$.

Lemma 4.14. *There exists an embedding*

$$(H_{l^\infty},T_l)\longrightarrow(S_l^\times,S_l) \tag{29}$$

such that $(S_l^\times:H_{l^\infty})\leqq 6$.

Proof. By Lemma 4.2, there exists for every $i\geqq 1$ an embedding

$$(H_{l^i},E_{l^i})\longrightarrow((S/l^iS)^\times,S/l^iS) \tag{30}$$

such that $((S/l^iS)^\times,H_{l^i})\leqq 6$. Consider the diagram

$$\begin{tikzcd}
(H_{l^i},E_{l^i}) \arrow[r] \arrow[d, "{(\rho,l)}"'] & ((S/l^iS)^\times,S/l^iS) \arrow[d, "{(r,r)}"] \\
(H_{l^{i-1}},E_{l^{i-1}}) & ((S/l^{i-1}S)^\times,S/l^{i-1})
\end{tikzcd}$$

where ρ is the restriction map and r is reduction modulo $l^{i-1}S$. One observes that the kernel of (ρ,l) is embedded into the kernel of (r,r). Hence the diagram (39) can be completed in a canonical way to a commulatative diagram, by an embedding.

This argument shows that if one denotes by I_i the non-empty finite set of embeddings (30), then there is a canonical map of I_i into I_{i-1}. The I_i's together with this map form an inverse system. The inverse limit of this system is not empty. Every element of it induces the desired embedding (29). □

We proceed by embedding S_l in $\mathrm{GL}(2, \mathbf{Z}_l)$ and distinguish between two cases:

Case i. l decomposes in L_0. We recall that $S_0 = \mathbf{Z}[w_0]$ and w_0 satisfies an irreducible equation $X^2 - g_0 X - h_0 = 0$ over $\mathbf{Z}$. Let w_0' be the other root of this equation. Then $w_0, w_0' \in \mathbf{Z}_l$ and $l \nmid (w - w_0')$ (e.g. by Dedekind Theorem, cf. Lang [15, p. 27]), i.e. $w_0 - w_0'$ is a unit in $\mathbf{Z}_l$. Now $S_{0l} = \mathbf{Z}_l \otimes S_0 \cong \mathbf{Z}_l[\bar{w}_0]$, where $1, \bar{w}_0$ are linearly independent elements over $\mathbf{Q}_l$ and $\bar{w}_0^2 - g_0 \bar{w}_0 - h_0 = 0$. One easily checks that the map

$$a + b\bar{w}_0 \rightarrow (a + bw_0, a + bw_0') \qquad (a, b \in \mathbf{Z}_l)$$

is a ring isomorphism $\mathbf{Z}_l[\bar{w}_0] \cong \mathbf{Z}_l^2$. Further $S_l \cong \mathbf{Z}_l[f\bar{w}_0]$. Hence S_l is isomorphic to the subring $\mathbf{Z}_{l,f}^2 = \{(a,b) \in \mathbf{Z}_l^2 \mid a \equiv b \bmod f\mathbf{Z}_l\}$ of $\mathbf{Z}_l^2$. Denote by $D_f(l^\infty)$ the group of all diagonal matrices in $\mathrm{GL}(2, \mathbf{Z}_l)$ with $(a\,b)$ as the principal diagonal for which $a \equiv b \bmod f\mathbf{Z}_l$. Then we have $(S_l^\times, S_l) = (D_f(l^\infty), \mathbf{Z}_{l,f}^2)$. Let also $D(l_\infty) = D_1(l^\infty) = D(\mathbf{Z}_l)$ (in the notation of section 4.6). Then, noting that $(D(l^\infty) : D_f(l^\infty)) \leqq f$, we have, by Lemma 4.14, that $(H_{l^\infty}, T_l) \cong (H(l^\infty), \mathbf{Z}_{l,f}^2)$, where $H(l^\infty)$ is a closed subgroup of $D(l^\infty)$ of index $\leqq 6f$. This isomorphism can be extended to an isomorphism $(G_{l^\infty}, T_l) \cong (G(l^\infty), \mathbf{Z}_{l,f}^2)$, where $G(l^\infty)$ is a closed subgroup of $\mathrm{GL}(2, \mathbf{Z}_l)$ that contains $H(l^\infty)$ and $(G(l^\infty) : H(l^\infty)) \leqq 2$. Clearly $|\mathbf{Z}_l^\times| > 6f \geqq (D(l^\infty) : H(l^\infty))$. It follows from Lemma 4.9 that $G(l^\infty) \leqq C(l^\infty)$, where $C(l^\infty) = C(\mathbf{Z}_l)$, in the notation of Section 4.6, and we have $(C(l^\infty) : G(l^\infty)) \leqq 12f$. Also $S(G(l^\infty), \mathbf{Z}_{l,f}^2) \subseteq S(C(l^\infty), \mathbf{Z}_l^2)$. Hence, in order to prove that $S(G(l^\infty), \mathbf{Z}_{l,f}^2)$ is a zero set in $G(l^\infty)$, it suffices to prove that $S(C(l^\infty), \mathbf{Z}_l^2)$ is a zero set in $C(l^\infty)$.

Indeed, $S(C(l^\infty), \mathbf{Z}_l^2)$ is, by Lemma 4.10, the union of three subsets

$$V_1 = \left\{ \begin{pmatrix} u & 0 \\ 0 & 1 \end{pmatrix} \middle| \, u \in \mathbf{Z}_l^\times \right\} \quad \text{and} \quad V_2 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & u \end{pmatrix} \middle| \, u \in \mathbf{Z}_l^\times \right\} \quad \text{and}$$

$$V_3 = \left\{ \begin{pmatrix} 0 & u \\ u^{-1} & 0 \end{pmatrix} \middle| \, u \in \mathbf{Z}_l^\times \right\}.$$

V_1 and V_2 are clearly closed subgroups of $D(l^\infty)$, hence of $C(l^\infty)$, of an infinite index. Hence they are zero sets in $C(l^\infty)$. V_3 is a coset of the subgroup

$$V_3' = \left\{ \begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix} \middle| \, u \in \mathbf{Z}_l^\times \right\}$$

of $D(l^\infty)$. Since the index of V_3' in $D(l^\infty)$ is infinite, V_3 is also a zero set in $C(l^\infty)$. Thus $S(C(l^\infty), \mathbf{Z}_l^2)$ is a zero set in $C(l^\infty)$.

Case ii. l remains prime in L_0 or l ramifies in L_0. In this case L_{0l} is a quadratic extension of $\mathbf{Q}_l$. Hence the irreducible equation $X^2 - gX - h = 0$ for w over $\mathbf{Q}$ remains irreducible over $\mathbf{Q}_l$. It follows that $S_l \cong \mathbf{Z}_l[w]$ is an integral domain and $(S_l^\times, S_l) \cong (\mathbf{Z}_l[w]^\times, \mathbf{Z}_l[w\})$.

The elements $1 + l'w$, $i = 1, 2, 3, \cdots$ represent distinct cosets of $\mathbf{Z}_l[w]^\times$ modulo $\mathbf{Z}_l^\times$. Hence $(\mathbf{Z}_l[w]^\times : \mathbf{Z}_l^\times) > 6 \geqq (I(l^\infty) : H(l^\infty))$, by Lemma 4.14, and Lemma 4.12 is thus applicable. As in case i, we have only to prove that $S(J(l^\infty), \mathbf{Z}_l^2)$ is a zero set in $J(l^\infty)$. Here $I(l^\infty) = I(\mathbf{Z}_l)$ and $J(l^\infty) = J(\mathbf{Z}_l)$ in the notation of Section 4.8. Indeed, by Lemma 4.13, $S(J(l^\infty), \mathbf{Z}_l^2)$ consists of the unit matrix and a subset W of $J(l^\infty) - I(l^\infty)$ of all matrices having determinant -1. W is therefore a closed subset. Moreover, if u runs over a set of representatives of $\mathbf{Z}_l^\times / \{\pm 1\}$, then $\bigcup uW$ is a disjoint union in $J(l^\infty)$. It follows that W is a zero set in $J(l^\infty)$, since $\mathbf{Z}_l^\times / \{\pm 1\}$ is certainly infinite. Thus $S(J(l^\infty), \mathbf{Z}^2)$ is a zero set in $J(l^\infty)$.

The proof of (C″) is completed and with it the proof of Proposition 1.2 in case III is also completed.

§5. The absolute invariant j is contained in a finite field

An elliptic curve E defined over a field K whose j-invariant belongs to a finite field K' is isomorphic, over a finite extension of K, to a curve E' defined over K'. We first prove a stronger theorem for E' than Proposition 1.2 and then deduce Proposition 1.2 for E from the stronger theorem for E'.

5.1. *The stronger theorem for elliptic curves over finite fields*

We consider in this section an elliptic curve E defined over a finite field K of characteristic p. It is well known that the group of all algebraic automorphisms, $\operatorname{Aut} E$, of E is a finite group, the order of which divides 24. If $\varepsilon \in \operatorname{Aut} E$, then $\operatorname{ord} \varepsilon$ .is equal to 1, 2, 3, 4, or 6 (cf. Lang [16, pp. 301–304]).

THEOREM 5.1. *Let E be an elliptic curve defined over a finite field K. Then for almost all $(\sigma) \in G(K)^e$ we have:*

(A‴) *If $e = 1$, then for every finite $\varepsilon \in \operatorname{Aut} E$ there exist infinitely many $P \in E(\tilde{K})$ such that $\sigma P = \varepsilon P$.*

(B‴) *If $e \geqq 2$, then there exist only finitely many $P \in E(\tilde{K})$ for which there exist $\varepsilon_1, \cdots, \varepsilon_e \in \operatorname{Aut} E$ such that $\sigma_i P = \varepsilon_i P$ for $i = 1, \cdots, e$.*

(C‴) *If $e = 1$ and l is a prime, then there exist only finitely many $P \in E_{l^\infty}(\tilde{K})$ for which there exists an $\varepsilon \in \operatorname{Aut} E$ such that $\sigma P = \varepsilon P$.*

5.2. *A generalization of Riemann Hypothesis for elliptic curves*

We shall imitate Hasse's proof of the Riemann Hypothesis for elliptic curves (see Hasse [6] or Cassels [2, p. 241]).

Let λ be a non-zero endomorphism of E which is defined over an extension L of K and let P be a generic point of E over L. Then the *degree* of λ is defined as $\deg \lambda = [L(P): L(\lambda(P)]$. It is a positive integer that does not depend on P and on L. The endomorphism λ is said to be *separable* if $L(P)/L(\lambda P)$ is a separable extension. In this case

$$|\operatorname{Ker} \lambda| = \deg \lambda \tag{1}$$

(cf. Cassels [2, p. 217]). One knows also that there corresponds to λ an element $\bar{\lambda} \in \operatorname{End} E$ such that

$$\lambda\bar{\lambda} = \bar{\lambda}\lambda = \deg \lambda. \tag{2}$$

The map $\lambda \to \bar{\lambda}$ of $\operatorname{End} E$ into itself satisfies the following rules:

$$\overline{\lambda + \mu} = \bar{\lambda} + \bar{\mu} \quad \text{and} \quad \overline{m\lambda} = m\bar{\lambda} \qquad \text{for } m \in Z$$

(cf. [2, p. 220]). It follows from (2) that if $\lambda, \mu \in \operatorname{End} E$ and $\lambda, \mu \neq 0$, then $\deg(\lambda + \mu) = \deg \lambda + \deg \mu + \lambda\bar{\mu} + \mu\bar{\lambda}$. Define therefore $(\lambda, \mu) = \frac{1}{2}(\lambda\bar{\mu} + \mu\bar{\lambda})$. Define also $(\lambda, 0) = (0, \mu) = 0$. In this way one obtains a **Q**-valued symmetric **Z**-bilinear form on $\operatorname{End} E$. Clearly $(\lambda, \lambda) = \deg \lambda > 0$ for $\lambda \neq 0$. Hence if we define $|\lambda| = \sqrt{(\lambda, \lambda)}$, we obtain the usual Cauchy-Schwartz inequality

$$|(\lambda, \mu)| \leqq |\lambda| \cdot |\mu|. \tag{3}$$

We consider now certain special endomorphisms. First let ε be an automorphism of E. It is defined over a finite extension L of K. If P is a generic point of E over L, then $L(\varepsilon P) = L(P)$ and hence $\deg \varepsilon = 1$.

Suppose that the order of L is q and denote by $\pi = \pi_q$ the Frobenius endomorphism defined by $\pi(x) = x^q$. Then π induces an endomorphism of E which we also denote by π. If (x, y) is an affine representative of P, then $L(\pi P) = L(x^q, y^q) = L(x, y)^q$, hence $\deg \pi = [L(P): L(\pi P)] = q$ (see also Lang [16, p. 118]) and π is a purely inseparable endomorphism. Also

$$L(P) = L(\varepsilon P) \subseteq L(\pi P)L((\varepsilon - \pi)P) \subseteq L(P).$$

Hence $L(P)^q L((\varepsilon - \pi)P) = L(P)$. It follows that $L(P)$ is a separable extension of $L((\varepsilon - \pi)P)$ (see Lang [14, p. 188]), hence $\varepsilon - \pi$ is a separable endomorphism.[†] In particular we obtain that $|\operatorname{Ker}(\varepsilon - \pi)| = (\varepsilon - \pi, \varepsilon - \pi)$, by (1). Now $(\varepsilon - \pi, \varepsilon - \pi) = 1 - q - 2(\varepsilon, \pi)$ and $|(\varepsilon, \pi)| \leqq \sqrt{q}$, by (3). Therefore the following lemma has been proved.

[†] This argument was suggested by Peter Roquette.

LEMMA 5.2. *Let q be a power of p. Denote by $N(q,\varepsilon)$ the number of points P of $E(\tilde{K})$ for which $\pi_q(P)=\varepsilon P$. Then*

$$|N(q,\varepsilon)-q-1|\leqq 2\sqrt{q}.$$

For $\varepsilon = 1$, one obtains the usual Riemann Hypothesis for elliptic curves. A similar result for curves of arbitrary genus can be found in Bombieri [1, p. 430].

5.3. *The operation of $G(K)$ on* Aut E

The points that occur in Lemma 5.2 are algebraic over K. We show in this section that their degrees over K are bounded.

The smallest field of definition for the elements of Aut E is obtained from K by adjoining roots of equations of degrees 2, 3 and 4 with coefficients in K (see Deuring [4, section 2]). It follows that the elements of Aut E are defined over the unique extension L of K of degree 12. Hence

$$\text{(4)} \qquad \sigma\in G(L) \quad \text{and} \quad \alpha\in \operatorname{Aut}E \Rightarrow \sigma\alpha\sigma^{-1}=\alpha.$$

If $\sigma\in G(L)$, then $\sigma\alpha\sigma^{-1}$ is in general not equal to α, but it is still an element of Aut E. We therefore define $\sigma(\alpha)=\sigma\alpha\sigma^{-1}$. This is a representation of $G(K)$ as an automorphism group of Aut E. The order of every σ, as an automorphism of Aut E, divides 12, by (4).

More generally we consider a finite (multiplicative) group B and denote the set of all maps of B into itself by $T(B)$. We introduce addition and multiplication to $T(B)$ by $(f+g)(\beta)=f(\beta)g(\beta)$ and $(f\cdot g)(\beta)=f(g(\beta))$. Define also $(-f)(\beta)=f(\beta)^{-1}$ and $0(\beta)=1$ and $1(\beta)=\beta$.

These operations satisfy the following rules: (i) Addition is associative (but not necessarily commutative). (ii) $0+g=g+0=g$. (iii) $f+(-f)=(-f)+f=0$. (iv) Multiplication is associative. (v) $1\cdot g=g\cdot 1=g$. (vi) $f\cdot g=1$ implies f and g are bijective. (vii) $(f+g)h=fg+gh$ for $h\in T(B)$. (viii) $0\cdot f=0$. (ix) If $f\in \operatorname{End}B$, then $f(g+h)=fg+fh$ and $f\cdot 0=0$. If $\sigma\in \operatorname{Aut}B$ and n is a positive integer we define $s_m(\sigma)=\sum_{i=1}^{m}\sigma^{m-i}=\sigma^{m-i}+\sigma^{m-2}+\cdots+1$.

This is an element of $T(B)$. Using the above rules one finds that

$$\text{(5)} \qquad s_{mn}(\sigma)=s_m(\sigma^n)s_n(\sigma).$$

LEMMA 5.3. *If B is a finite group, k is a multiple of the exponent of B, σ is an element of* Aut B, *l is a multiple of* ord σ *and $m=kl$, then*

(a) $s_m(\sigma)=0$, *and*

(b) *if n is relatively prime to m, then $s_n(\sigma)$ is bijective.*

PROOF. Note first that $s_k(1)(\beta) = \beta^k = 1$ for every $\beta \in B$. Hence $s_k(1) = 0$. It follows, by (5), that

$$s_m(\sigma) = s_k(\sigma^l)s_l(\sigma) = s_k(1)s(\sigma) = 0 \cdot s_l(\sigma) = 0.$$

In order to prove (b) take positive integers u, v such that $un = mv + 1$. Then

$$s_u(\sigma^n)s_n(\sigma) = s_{un}(\sigma) = \sigma^{mv} + s_{mv}(\sigma) = 1 + s_m(\sigma^v)s_v(\sigma) = 1 + 0 \cdot s_v(\sigma) = 1,$$

by (5) and by (a). It follows that $s_n(\sigma)$ is indeed bijective. □

We return now to our elliptic curve E and prove:

LEMMA 5.4. *Let $\sigma \in G(K)$, $\alpha \in \operatorname{Aut} E$ and $P \in E(K)$. Suppose that $\sigma P = \alpha P$. Then $\sigma^i p = (s_i(\sigma)(\alpha))P$ for every $i \geqq 1$ and $\sigma^{144}p = p$.*

PROOF. The first formula can be rewritten as

$$\sigma^i p = (\sigma^{i-1}\alpha\sigma^{1-i})(\sigma^{i-2}\alpha\sigma^{2-i})\cdots(\sigma\alpha\sigma^{-1})\alpha P$$

and this can be easily proved by induction on i. For the proof of the second statement recall that $\alpha^{12} = 1$ and that σ^{12} operates trivially on $\operatorname{Aut} E$. Hence we have, by Lemma 5.3, that $\sigma^{144}P = (0(\alpha)P) = P$. □

5.4. *Proof of* (A‴)

Denote by $K^{(2)}$ and $K^{(3)}$ the maximal 2 and 3 extensions of K, respectively. These are infinite extensions and $\mathcal{G}(K^{(2)}/K) \cong \mathbf{Z}_2$, $\mathcal{G}(K^{(3)}/K) \cong \mathbf{Z}_3$. It follows that $G(K^{(2)})$ and $G(K^{(3)})$ are zero sets of $G(K)$. Let S be the set of all $\sigma \in (G(K) - G(K^{(2)})) \cap (G(K) - G(K^{(3)}))$ such that $\tilde{K}(\sigma)$ is an infinite field. Then $\mu(S) = 1$, by lemma 7.1 of [10]. We prove that every $\sigma \in S$ satisfies (A‴).

Indeed, let $M = \tilde{K}(\sigma)$. Then $K^{(2)} \nsubseteq M$, and hence $K^{(2)} \cap M$ is a finite extension of K (cf. Ribes [21, p. 57]). Similarly $K^{(3)} \cap M$ is a finite extension of K. Let $\varepsilon \in \operatorname{Aut} E$ and let m be a positive integer. By Lemma 5.2 there exists a q_0 such that $N(q, \alpha) \geqq m$ for every p-power $q \geqq q_0$ and every $\alpha \in \operatorname{Aut} E$. The field M is an infinite extension of K. Hence one can find a subfield L of M of order $q \geqq q_0$ that contains both $K^{(2)} \cap M$ and $K^{(3)} \cap M$. For every $\alpha \in \operatorname{Aut} E$ there exist then points $P_{\alpha 1}, \cdots, P_{\alpha m}$ in $E(\tilde{K})$ such that

$$\pi_q P_{\alpha i} = \alpha P_{\alpha i} \qquad \text{for } i = 1, \cdots, m. \tag{6}$$

It follows from Lemma 5.4 that $\pi_q^{144} P_{\alpha i} = P_{\alpha i}$ for $i = 1, \cdots, m$. The points $P_{\alpha i}$ belong therefore to $E(L')$, where L' is the unique extension of L of degree 144. The degree $[M : L]$ is relatively prime to 144, since $K^{(2)} \cap M$ and $K^{(3)} \cap M$ are contained in L. It follows that M is linearly disjoint from L' over L. In particular

$\sigma \mid L'$ generates the cyclic group $\mathcal{G}(L'/L)$. Hence there exists a positive integer n which is relatively prime to 12 such that $\sigma \mid L' = \pi_q^n \mid L'$. By Lemma 5.3, $s_n(\pi_q)$ is a bijective map of Aut E onto itself. Hence there exists an $\alpha \in \operatorname{Aut} E$ such that $s_n(\pi_q)(\alpha) = \varepsilon$. It follows from Lemma 5.4 and from (6) that $\sigma P_{\alpha i} = \pi_q^n P_{\alpha i} = (s_n(\pi_q)\alpha)P_{\alpha i} = \varepsilon P_{\alpha i}$ for $i = 1, \cdots, m$.

Since m is arbitrary, there exist infinitely many points $P \in E(\tilde{K})$ such that $\sigma P = \varepsilon P$.

5.5. *Proof of* (B‴)

Let $e \geqq 2$ and denote by S the set of all $(\sigma) \in G(K)^e$ such that $\tilde{K}(\sigma)$ is a finite field. By lemma 7.2 of [10], S has the measure 1. We prove that every $(\sigma) \in S$ satisfies (B‴).

Indeed, the field $M = \tilde{K}(\sigma)$ is finite with, say, q elements. The group $G(M)$ is therefore generated by the Frobenius automorphism $\pi = \pi_q$. In particular there exist $u_1, \cdots, u_e \in \hat{\mathbf{Z}}$ such that

$$(7) \qquad \sigma_i = \pi^{u_i} \qquad \text{for } i = 1, \cdots, e.$$

On the other hand, the group $G(M)$ is generated also by $\sigma_1, \cdots, \sigma_e$. Hence there exist $v_1, \cdots, v_e \in \mathbf{Z}$ such that

$$(8) \qquad \pi = \sigma_1^{v_1} \cdots \sigma_e^{v_e}.$$

Raising equalities (7) and (8) to the 144-th power, one sees that $M' = \tilde{K}(\sigma_1^{144}, \cdots, \sigma_e^{144}) = \tilde{K}(\pi^{144})$ is the unique extension of M of degree 144.

Let now P be a point of $E(\tilde{K})$ for which there exist $\varepsilon_1, \cdots, \varepsilon_e \in \operatorname{Aut} E$ such that $\sigma_i P = \varepsilon_i P$ for $i = 1, \cdots, e$. By Lemma 5.4, $\sigma_i^{144} P = P$ for $i = 1, \cdots, e$. It follows that $P \in E(M')$. But M' is a finite field, hence $E(M')$ is a finite group. It follows that there are only finitely many such P's.

5.6. *Proof of* (C‴)

Recall that an elliptic curve E defined over a field K of characteristic p is said to be *super singular* if End E is a non-commutative ring. In this case $T_p = E_{p^\infty} = 0$. If E is not super singular, then $T_p \cong \mathbf{Z}_p$ and G_{p^∞} is isomorphic to a subgroup $G(p^\infty)$ of $\mathbf{Z}_p^\times$ (cf. Robert [22, p. 123]).

LEMMA 5.5. *Let K be a finite field and let E be an elliptic curve defined over K. Let l be a prime such that $T_l \neq 0$. Then $G_{l^\infty} = \mathbf{Z}_l \times H$, where H is a finite cyclic group whose order is prime to l.*

PROOF. The group $G_{l^\infty} = \mathcal{G}(K_{l^\infty}/K)$ is an infinite subgroup of $\hat{\mathbf{Z}}$. Hence it is pro-cyclic. Suppose first that $l \neq p$. Then $G(l^\infty)$ is an infinite pro-cyclic subgroup of $\mathrm{GL}(2,\mathbf{Z}_l)$. We prove that $G(l^\infty) \cong \mathbf{Z}_l \times H$, where H is as above.

For $i \geqq 1$, let $N_i = \{A \in \mathrm{GL}(2,\mathbf{Z}_l) \mid A \equiv I \bmod l^i\}$, where I is the 2×2 unit matrix. Then N_i are open normal subgroups of $\mathrm{GL}(2,\mathbf{Z}_l)$. Let $A = I + l^iA'$ and $B = I + l^iB'$ be two elements of N_i. Then $AB \equiv I + l^i(A' + B') \bmod l^{i+1}$. It follows that the map $A \mapsto A'$ induces an isomorphism $N_i/N_{i+1} \cong (\mathbf{Z}/l\mathbf{Z})^4$.

Hence, for $N = N_1$, we have that $(N : N_{i+1}) = l^{4i}$. Also $N \cong \varprojlim N/N_i$, hence N is a pro-l group.

Let now $r = (\mathrm{GL}(2,\mathbf{Z}_l) : N)$ and let A be a generator of $G(l^\infty)$. Then $A^r \in N$ and hence $\operatorname{ord} A^r$ must be a power of l, which is necessarily l^∞, since $G(l^\infty)$ is infinite. It follows that $\operatorname{ord} A = kl^\infty$, where k is relatively prime to l. This means that $G(l^\infty) \cong \mathbf{Z}_l \times H$, where H is a cyclic group of order k.

If $l = p$, then $G(p^\infty)$ is an infinite pro-cyclic subgroup of $\mathbf{Z}_p^\times$. Now $\mathbf{Z}_p^\times \cong \mathbf{Z}_p \times \mathbf{Z}/(p-1)\mathbf{Z}$ if $p \neq 2$, and $\mathbf{Z}_2^\times \cong \mathbf{Z}_2 \times \mathbf{Z}/2\mathbf{Z}$. The proof can be carried on as above, replacing N by $\mathbf{Z}_p$. □

End of Proof of (C'''). By Lemma 5.5 there exists a field K' such that $K \subset K' \subseteq K_{l^\infty}$ and $[K_{l^\infty} : K'] < \infty$ and $\mathcal{G}(K'/K) \cong \mathbf{Z}_l$. If L is an infinite extension of K which is contained in K', then $L = K$, since $\mathbf{Z}_l$ has no closed finite subgroups except 1. Also $G(K')$ is a zero set in $G(K)$. We show that every $\sigma \in G(K) - G(K')$ satisfies (C''').

Indeed, suppose that $\sigma \in G(K) - G(K')$ and that there exist infinitely many $P \in E_{l^\infty}$ for which there exists an $\varepsilon \in \operatorname{Aut} E$ such that $\sigma P = \varepsilon P$. For every such P we have $\sigma^{144}P = P$, by Lemma 5.4. It follows that $K_{l^\infty} \cap \tilde{K}(\sigma^{144})$ is an infinite field, since $E(K_{l^\infty} \cap \tilde{K}(\sigma^{144}))$ is an infinite set. Hence also $K' \cap \tilde{K}(\sigma^{144})$ is an infinite field, since $[K_{l^\infty} : K'] < \infty$. It follows that $K' \subseteq \tilde{K}(\sigma^{144})$. Hence $[K' : K' \cap \tilde{K}(\sigma)] \leqq [\tilde{K}(\sigma^{144}) : \tilde{K}(\sigma)] \leqq 144$. Thus $K' \cap \tilde{K}(\sigma)$ is also an infinite field and hence $K' \subseteq \tilde{K}(\sigma)$. This however contradicts the assumption that $\sigma \notin G(K')$.

5.7. *Proof of Proposition* 1.2 *in Case* IV

We return now to the case where the elliptic curve E is defined over a field K which is finitely generated over $\mathbf{F}_p$ and such that $\mathbf{F}_p(j)$ is a finite field. Then there exists an elliptic curve E' defined over $\mathbf{F}_p(j)$ which is isomorphic to E over a finite extension L of K. Let $\phi : E \to E'$ be an isomorphism. Then ϕ induces an isomorphism of groups $\phi : E_{\mathrm{tor}} \to \mathrm{E}'(\tilde{\mathbf{F}}_p)$. If $\sigma \in G(K)$, then $\sigma \circ \phi \circ \sigma^{-1}$ is also an isomorphism from E to E'. Therefore there exists an automorphism $\varepsilon = \varepsilon_\sigma$ of E' such that $\sigma \circ \phi \circ \sigma^{-1} = \varepsilon \circ \phi$. It follows that if $P \in F_{\mathrm{tor}}$ and $P' = \phi(P)$, then

$$(9) \qquad \sigma P = P \Leftrightarrow \sigma P' = \varepsilon P'.$$

Let now $K' = \tilde{\mathbf{F}}_p \cap K$. Then $\mathbf{F}_p(j) \subset K'$, and the lifting of every subset of $G(K')^e$ of measure 1 to $G(K)^e$ is again a set of measure 1. Parts (B) and (C) of Proposition 1.2 follow therefore from Theorem 5.1 for E' and K', by (9). It follows also that $E_{\mathrm{tor}}(\tilde{K}(\sigma))$ is infinite for almost all $\sigma \in G(K)$. If we combine this result with (C) we get that almost all $\sigma \in G(K)$ have the property that $E_{\mathrm{tor}}(\tilde{K}(\sigma))$ is infinite and that $E_{l^\infty}(\tilde{K}(\sigma))$ is finite for every l. Hence, by Lemma 1.3, there exist infinitely many l such that $E_l(\tilde{K}(\sigma)) \neq 0$.

The proof of Proposition 1.2 is completed.

Acknowledgement

The authors are indebted to Peter Roquette and Gerhard Frey for several valuable discussions.

References

1. E. Bombieri, *Counting points on curves over finite fields*, Seminar Bourbaki, 25e année, no. 430, 1972/73.
2. J. W. S. Cassels, *Diophantine equations with special reference to elliptic curves*, J. London Math. Soc. **41** (1966), 193–291.
3. J. W. S. Cassels and A. Fröhlich, *Algebraic Number Theory*, Academic Press, London, 1967.
4. M. Deuring, *Zur Theorie der elliptischen Funktionenkörper*, Hamb. Abh. **15** (1942), 211–261.
5. G. Frey and M. Jarden, *Approximation theory and the rank of abelian varieties over large algebraic fields*, Proc. London Math. Soc. **28** (1974), 112–128.
6. H. Hasse, *Abstrakte Begründung der komplex Multiplikation und Riemannsche Vermutung in Funktionenkörpern*, Abh. Math. Sem. Univ. Hamburg **10** (1934), 325–348.
7. B. Huppert, *Endliche Gruppen I*, Springer, Berlin, 1967.
8. J. I. Igusa, *Fibre systems of Jacobian varieties* (*III. Fibre systems of elliptic curves*), Amer. J. Math. **81** (1959), 454–475.
9. J. I. Igusa, *On the algebraic theory of elliptic modular functions*, J. Math. Soc. Japan **20** (1968), 98–106.
10. M. Jarden, *Roots of unity over large algebraic fields*, Math. Ann. **213** (1975), 109–127.
11. P. F. Kurčanov, *Elliptische Kurven unendlichen Ranges über* Γ*-Erweiterungen*, Mat. Sb. **19** (1973), 320–324.
12. S. Lang, *Diophantine Geometry*, Interscience Publishers, New York, 1962.
13. S. Lang, *Introduction to Algebraic Geometry*, Interscience Publishers, New York, 1964.
14. S. Lang, *Algebra*, Addison-Wesley, Reading, Mass., 1965.
15. S. Lang, *Algebraic Number Theory*, Addison-Wesley, Reading, 1970.
16. S. Lang, *Elliptic Functions*, Addison-Wesley, Reading, 1973.
17. W. J. LeVeque, *Topics in Number Theory*, Vol. I, Addison-Wesley, Reading, Mass., 1958.
18. W. J. LeVeque, *Topics in Number Theory*, Vol. II, Addison-Wesley, Reading, Mass., 1961.
19. B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266.
20. B. Mazur, *Modular curves and the Eisenstein ideal*, to appear.
21. L. Ribes, *Introduction to Profinite Groups and Galois Cohomology*, Queen's University, Kingston, 1970.

22. A. Robert, *Elliptic Curves*, Lecture Notes in Math. **326**, Springer, Berlin, 1973.

23. P. Roquette, *Analytic Theory of Elliptic Functions over Local Fields*, Vandenhaeck & Ruprecht, Göttingen, 1970.

24. P. Roquette, *Non-standard aspects of Hilbert's Irreducibility Theorem*, in *Model Theory and Algebra*, A memorial tribute to Abraham Robinson, Lecture Notes in Math. **498**, Springer, Berlin, 1975.

25. J. P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes élliptiques*, Invent. Math. **15** (1972), 259–331.

26. C. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press, 1971.

27. A. Weil, *Foundation of Algebraic Geometry*, Amer. Math. Soc., Providence, 1964.

MATHEMATISCHES INSTITUT
UNIVERSITÄT ERLANGEN-NÜRNBERG
BISMARCKSTR. $1\frac{1}{2}$, 852 ERLANGEN, BRD

AND

DEPARTMENT OF MATHEMATICS
TEL AVIV UNIVERSITY
RAMAT AVIV, TEL AVIV, ISRAEL