Stat.

Netherlands school of economics

ECONOMETRIC INSTITUTE

# ASPECTS OF ELLIPTIC CURVES: AN INTRODUCTION

R.J. STROEKER

Erasmus

REPORT 7808/M

ERASMUS UNIVERSITY ROTTERDAM, P.O. BOX 1738, ROTTERDAM, THE NETHERLANDS

# ASPECTS OF ELLIPTIC CURVES

## AN INTRODUCTION

by

R.J. Stroeker

## PREFACE

This exposition is meant to give a bird's eye view on the theory of elliptic curves at an elementary level. So as to introduce the various aspects of the theory within a framework both brief and simple, we have avoided wantonly the technical language of schemes and the like. Also, in order to keep a close eye on the number of pages, we could not be too ambitious. Thus important topics like complex multiplication and the Galois action on the points of finite order one will look for in vain, while we only briefly touched on the connection with modular functions.

December 1977

To make this treatise at least to some extent self contained, the first section covers the relevant notions of algebraic geometry which are needed in the sequel. In section 2 plane cubic curves are discussed and the next section gives the connection with elliptic functions. Not until section 4 a general definition of elliptic curves is given. The last section is mainly devoted to the Mordell-Weil group (e.g. Mazur's recent result on the torsion group of an elliptic curve over $\mathbb{Q}$) and some outstanding conjectures, like those of Birch and Swinnerton-Dyer and of Weil.

Textbooks which are especially useful in connection with the more fundamental concepts are: Fulton [17], Lang [21], Mumford [30], Robert [42] and Shafarevich [49].

Finally the author wishes to express his sincere gratitude to F. Oort for his advise and valuable suggestions. It goes without saying that the author remains solely responsible for the remaining errors and misconceptions.

CONTENTS

## 1. PLANE ALGEBRAIC CURVES. BASIC CONCEPTS.

Throughout this section k will be an arbitrary field with algebraic closure $K = \overline{k}$.

A *plane affine algebraic curve* C is the set of all zero's, contained in the affine plane $\mathbb{A}_K^2$, of a polynomial $f \in k[x,y]$, irreducible in $K[x,y]$. Thus

$$C = \{(x,y) \in \mathbb{A}_K^2 \mid f(x,y) = 0\}.$$

The affine plane $\mathbb{A}_K^2$ may be embedded in the projective plane $\mathbb{P}_K^2$ by means of the identification $(x,y) = (x:y:1)$. We define a *plane projective algebraic curve* $\tilde{C}$ as the set of all zero's of a homogeneous polunomial $\tilde{f} \in k[x,y,z]$, irreducible in $K[x,y,z]$ :

$$\tilde{C} = \{(x:y:z) \in \mathbb{P}_K^2 \mid \tilde{f}(x,y,z) = 0\}.$$

In this first section, we shall generally consider affine curves only. All concepts being discussed here for affine curves may be extended in a more or less natural way to projective curves. Since we can not give more than the bare minimum of information, necessary to understand at least the principles of algebraic geometry, in connection with the (arithmetical) theory of elliptic curves, we feel justified to do so. A textbook which contains all we need here (and far more) is Shafarevich's book [49].

The degree of the polynomial f is called the *degree* of C. Algebraic curves, as defined above, are also called *absolutely* *irreducible*.

Let C be an algebraic curve, given by the equation $f = 0$, $f \in k[x,y]$. The ideal $(f)$ in $k[x,y]$, generated by f, is a prime ideal. Hence

$$k[C] := {}^{k[x,y]}/_{(f)}$$

is an integral domain. Let $k(C)$ be the quotient field of $k[C]$. This field is called the *function field of* C and its elements are the *rational functions defined on* C. Clearly, the field $k(C)$ has transcendence degree 1 over k.

An important notion in the theory of algebraic curves is that of *birational transformations*. Such a transformation is a device which puts the points on a curve C in one-to-one correspondence with the points on another curve C', which is possibly of a simpler form (e.g. its degree may be lower). To be more precise, let C and C' be two algebraic curves given by the equations $f = 0$ and $f' = 0$ respectively. A *rational transformation* $\rho\colon C \to C'$ is a mapping, defined in all but a finite number of points on C, which is given by a pair $\phi_1$, $\phi_2$ of rational functions defined on C. A rational transformation $\rho\colon C \to C'$ is called *birational* if it has a rational inverse. In that case C and C' are *birationally equivalent*.

The function fields $k(C)$ and $k(C')$ of two birationally equivalent curves are isomorphic. For, if the birational transformation $\rho\colon C \to C'$ is given by $\phi_1, \phi_2 \in k(C)$, then the homomorphism $\tau\colon k[x',y'] \to k(C)$, defined by $\tau(x') = \phi_1$ and $\tau(y') = \phi_2$, has kernel $\mathrm{Ker}(\tau) = (f)$, where f is the defining polynomial of C'. Hence we have an injective homomorphism

$$k[C'] = {}^{k[x',y']}/_{(f)} \to k(C),$$

which can be extended to an injective homomorphism

$$k(C') \to k(C).$$

Similarly, there is an injective homomorphism

$$k(C) \to k(C'),$$

which is inverse to the former. Conversely, if $k(C) \cong k(C')$, then C and C' are birationally equivalent (over k). So we may alternatively define: the curves C and C' are birationally equivalent iff $k(C) \cong k(C')$.

As an example, consider the curves

$$C : x^3 + y^3 - 1 = 0 \text{ and } C' : Y^2 = X^3 - 2$$

defined over $k = \mathbb{R}$. The transformation given by

$$X = 2 \cdot \frac{x}{1-y} \quad , \quad Y = \sqrt{6} \cdot \frac{1+y}{1-y}$$

shows that C and C' are birationally equivalent over $\mathbb{R}$.

For an algebraic curve C, we define the *local ring* $\mathcal{O}_P(C)$ *of a point* $P \in C$ as follows:

$$\mathcal{O}_P(C) := \{ \frac{F}{G} \in k(C) \mid F,G \in k[C],\ G(P) \neq 0\}.$$

The defing rational functions $\phi_1, \phi_2 \in k(C)$ of a rational transformation $\rho: C \to C'$ belong to $\mathcal{O}_P(C)$ for every $P \in C$ at which $\rho$ is defined. The unique maximal ideal $\mathfrak{M}_P(C)$ of $\mathcal{O}_P(C)$ contains information on the multiplicity of the point P as a zero of the defing polynomial of C. To see this, we first explain what is meant by *simple point* and *singular point*.

Let P be a point on a curve C, given by the polynomial $f \in k[x,y]$ of degree n. Every line through P intersects C in exactly n points, counting multiplicities. If such a line L intersects C in P r ($\geq$ 1) times, i.e. (f=0,L=0) has an r-fold root in P, we call r the *intersection multiplicity of* L *at* P, notation: r = i(C L,P). Then P is a point on C with *multiplicity* r, iff $\min_{L \ni P} i(C\ L,P) = r$. If r = 1, then P is a *simple point* (or *non-singular point*) and if r > 1, then P is called a *singular point* of C. It follows that C has a unique tangent at P iff P is simple. If $P = (p_1,p_2)$, then the tangent at P is

$$\left(\frac{\partial f}{\partial x}\right)_P (x-p_1) + \left(\frac{\partial f}{\partial y}\right)_P (y-p_2) = 0.$$

By definition, at a singular point, $\frac{\partial f}{\partial x}$ and $\frac{\partial f}{\partial y}$ must vanish simultaneously. A curve C with no singular points is called *non-singular*. Note that the rational transformation $\rho: C \to \mathbb{P}^2_K$ is defined in each non-singular point of C.We say that ρ is *regular* in such a point. A birational transformation which is *biregular* everywhere (this is the case when both curves concerned are non-singular) is a *birational isomorphism*.

Now let P be a non-singular point on C with coordinates in k. Then the maximal ideal $\mathfrak{M}_P(C)$ of the local ring at P is a principal ideal. The converse is also true. A generator for $\mathfrak{M}_P(C)$ is called a *local* (or *uniformizing*) *parameter at* P; $\mathfrak{M}_P(C) = (\tau)$ with local parameter τ at P. Clearly, if P is simple and $0 \neq \phi \in \mathcal{O}_P(C)$, then there is a unique $m \in \mathbb{Z}$, $m \geq 0$ and a unit $u \in \mathcal{O}_P(C)$ such that $\phi = u\tau^m$. More over, this integer m does not depend on the choice of τ. This means, since P is rational over k, that for each $\phi \in \mathcal{O}_P(C)$ and for each $\ell \in \mathbb{N}$, there exist unique elements $a_0, a_1, \ldots, a_{\ell-1}$ of k such that

$$\phi - (a_0 + a_1\tau + \ldots + a_{\ell-1}\tau^{\ell-1}) \in \mathfrak{m}_P^{\ell}(C).$$

This gives rise to an embedding of $\mathcal{O}_P(C)$ in the ring of formal power series $k[[\tau]]$. Hence every rational function $\phi$ defined on C and regular at the simple point $P \in C$ (i.e. $\varphi \in \mathcal{O}_P(C)$), can be uniquely expressed as a formal power series in the local parameter $\tau$ at P.

Another essential concept in the theory of algebraic curves is that of *divisor*. Let P be a simple point with coordinates in k, $P \in C$. For any $\phi \in k(C)$, we define the integer $\mathrm{ord}_P(\varphi)$ as follows: if $\phi = 0$, then $\mathrm{ord}_P(\phi) = \infty$. If $0 \neq \phi \in \mathcal{O}_P(C)$, then $\mathrm{ord}_P(\phi) = m$, where m is defined by $\phi = u\tau^m$. Finally, if $0 \neq \phi \in k(C)$ then $\varphi = \psi_1/\psi_2$ with $\psi_1, \psi_2 \in \mathcal{O}_P(C)$ and $\mathrm{ord}_P(\phi) = \mathrm{ord}_P(\psi_1) - \mathrm{ord}_P(\psi_2)$. Then $\mathrm{ord}_P$ becomes a valuation on the field k(C), i.e.

$$\mathrm{ord}_P(\phi_1+\phi_2) \geqq \min(\mathrm{ord}_P(\phi_1), \mathrm{ord}_P(\phi_2)) \quad \text{and}$$

$$\mathrm{ord}_P(\phi_1 \cdot \phi_2) = \mathrm{ord}_P(\phi_1) + \mathrm{ord}_P(\phi_2).$$

Clearly, $\mathrm{ord}_P(k(C)-\{0\}) = \mathbb{Z}$. If $\mathrm{ord}_P(\phi) = m > 0$, then $\phi$ has a *zero of order* m *at* P and if $\mathrm{ord}_P(\phi) = -m < 0$, then $\phi$ has a *pole of order* m *at* P.

Assume that C is non-singular, so that all points on C are simple points (defined over K). We also assume that C is a projective curve. A *divisor* D on C is defined to be a formal finite sum

$$\sum_{P \in C}^{<\infty} n_P(P) ,$$

where $n_P \in \mathbb{Z}$. The set of divisors on C can be made into an abelian group with respect to the following addition: if $D = \Sigma\, n_P(P)$ and $D' = \Sigma\, n'_P(P)$, then $D + D' := \Sigma\, (n_P+n'_P)(P)$. We write $D \geqq 0$ if $n_P \geqq 0$ for all $P \in C$ in the divisor $D = \Sigma\, n_P(P)$; if $n_P > 0$ for at least one P, then we write $D > 0$. If $D = \Sigma\, n_P(P)$, the finite sum $\Sigma\, n_P$ is called the *degree of* D, notation: deg(D).

A special class of divisors is that of the *principal divisors*:

$$(\phi) = \sum_{P\in C} \mathrm{ord}_P(\phi)(P) \quad , \; 0 \neq \phi \in K(C).$$

These principal divisors form a subgroup P(C) of the group of all divisors Div(C) on C. In fact P(C) is already a subgroup of the group $\mathrm{Div}^o(C)$ of all divisors of degree zero. Indeed, it follows from Bézout's theorem ([49], p.199), that $\deg(\phi) = = \Sigma\, \mathrm{ord}_P(\phi)$ = (number of zero's) - (number of poles) = 0. The factor group

$$C\ell(C) := {}^{\mathrm{Div}(C)}/_{P(C)}$$

is called the *group of divisor classes*. Two divisors $D_1$ and $D_2$ are *equivalent*, in notation $D_1 \sim D_2$, iff $D_1 - D_2 = (\phi)$ for some $\phi \in K(C)$. Because of the fact that $\deg(\phi) = 0$, all divisors in the same divisor class have the same degree. This is the *degree* of the divisor class.

Let D be a divisor on C. Consider the set of all $\phi \in K(C)$ that make D *effective*, that is to say: $(\phi) + D \geqq 0$. Thus we define

$$L(D) := \{\varphi \in K(C) \mid (\phi) + D \geqq 0\}.$$

We also include the zero element of K(C) in L(D). Then it is easy to see that L(D) is a vectorspace over K. More over, if

$\ell(D) := \dim_K L(D)$, then $\ell(D) = 0$ if $\deg(D) < 0$ and $\ell(D) \leqq$ $\leqq \deg(D) + 1$ if $\deg(D) \geqq 0$. Consequently, $L(D)$ is finite dimensional. An important property of $L(D)$ is, that equivalent divisors determine the same vectorspace, up to isomorphism.

A divisor $D = \sum_{P \in C} n_P(P)$ is *defined over* k if it is invariant under the action of the Galois group $\mathrm{Gal}({}^K/_k)$. By this we mean that for all $P \in C$ and $\sigma \in \mathrm{Gal}({}^K/_k)$ we have $n_{\sigma P} = n_P$. When this is so, the space $L(D)$ has a basis consisting of functions of $k(C)$ (cf. [7], p. 210).

Beside the principal divisors, another type of divisor plays an important role, namely the divisors of (linear) differential forms on C. An algebraic definition of these differential forms may be given as follows: consider the set $V_C$ of all mappings $d: K(C) \to K(C)$, with the following properties:

(i) $d(a) = 0$ for all $a \in K$,

(ii) $d(\phi + \psi) = d(\phi) + d(\psi)$ for all $\phi, \psi \in K(C)$ and

(iii) $d(\phi \cdot \psi) = \phi d(\psi) + \psi d(\phi)$ for all $\phi, \psi \in K(C)$.

The functions d are called *derivations*. The set $V_C$ can be made into a vectorspace (of dimension 1 over $K(C)$) in the natural way. From (i) and (iii) it follows easily that a derivation is linear over K. Let $\Omega(C) := V_C^*$ be the dual space of $V_C$ (over $K(C)$) i.e. the 1-dimensional vectorspace over $K(C)$ of linear maps $\omega: V_C \to K(C)$. This vectorspace $\Omega(C)$ is the space of *differential forms of* $K(C)$. Now every $\phi \in K(C)$ defines a differential form $d\phi: d \mapsto d(\phi)$. Let $\tau$ be a local parameter at a point P of C. Considering the differential form $\omega = \phi d\tau$ ($\phi \neq 0$), we define

$\mathrm{ord}_P(\omega) := \mathrm{ord}_P(\phi)$. Note that this definition does not depend on the choice of $\tau$. Then

$$(\omega) := \sum_{P \in C} \mathrm{ord}_P(\omega)(P)$$

is an element of Div(C). From the definition it follows easily that $(\phi\omega) = (\phi) + (\omega)$ for all $\phi \in K(C)$. Since $\Omega(C)$ is a one-dimensional vector space over K(C), we see that the divisors of all the forms $\omega \in \Omega(C)$ are equivalent to each other. Thus, they form a single divisor class, the *canonical class*, denoted by $K_C$.

A differential form $\omega \in \Omega(C)$ with no poles, i.e. $(\omega) \geqq 0$, is called a *differential form of the first kind*. The space of all such forms, we denote it by $\Omega[C]$, is a vector space over K. It's dimension is the *genus* g of the curve C:

$$g = g(C) = \dim_K \Omega[C].$$

Both the genus and the degree of the canonical class are birational invariants of the curve C. In fact we have

$$\deg(K_C) = 2g - 2.$$

This is a consequence of a very deep result, namely the Riemann-Roch theorem (cf. [8], chapter II). It asserts (for algebraic curves) that

$$\ell(D) - \ell(K_C-D) = \deg(D) - g + 1,$$

for any divisor D of C. Indeed, set $D = (\omega)$ in the above formula, then $\deg(\omega) = \ell(\omega) - \ell(0) + g - 1 = 2g - 2$ since $\ell(\omega) = g$ and $\ell(0) = 1$.

## 2. PLANE CUBIC CURVES.

In this section we assume that $k$ is a field of characteristic $\neq 2$ or 3, with algebraic closure $K = \overline{k}$.

A plane algebraic absolutely irreducible projective cubic curve $C$ over $k$ is given by an equation

$$F(X,Y,Z) = 0,$$

where $F \in k[X,Y,Z]$ is homogeneous, absolutely irreducible and of degree 3. Such a curve can have at most one singular point, because a line intersects $C$ in exactly three points (counting multiplicities). A simple point $P \in C$ is called a *flex* (*point of inflection*) if its tangent at $P$ intersects $C$ exactly three times in $P$. The flexes and the singular point (if in existence) lie on the curve with equation

$$H(X,Y,Z) = 0,$$

where $H$ is the *Hessian of* $F$, given by

$$H(X_1,X_2,X_3) = \det\left(\frac{\partial^2 F(X_1,X_2,X_3)}{\partial X_i \partial X_j}\right).$$

The Hessian $H$ is of degree 3 and consequently $H$ intersects $C$ in precisely 9 points (counting multiplicities). If each of those points has intersection multiplicity one, then $C$ has nine different flexes. This is exactly the case when $C$ is non-singular.

The following two theorems give a standard form for a plane cubic curve (in characteristic $\neq 2$ or 3).

THEOREM 1. *Let* C *be an absolutely irreducible non-singular cubic curve defined over* k. *More over, let* P *be a flex on* C *with coordinates in* k. *Then* C *is birationally isomorphic over* k *to a curve given by an equation (in* Weierstrass normal form*)*

$$Y^2Z = X^3 + AXZ^2 + BZ^3$$

*with* $A, B \in k$ *and* $4A^3 + 27B^2 \neq 0$. *The flex* P *then corresponds with the point* (0:1:0) *on the line* Z = 0.

The proof exhibites suitable coordinate transformations (transform P to the point (0:1:0) and then make Z = 0 tangent at this point, and so on) so as to obtain a birational transformation defined over k. The fact that C is non-singular can be seen from $4A^3 + 27B^2 \neq 0$.

For singular cubic curves we have

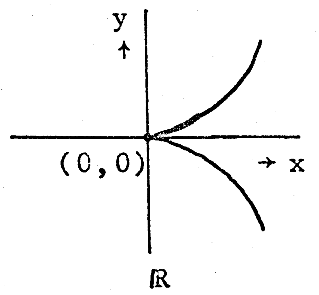
THEOREM 2. *If* C *is an absolutely irreducible singular cubic curve defined over* k *with a flex defined over* k, *then* C *is birationally equivalent to a curve, given by an equation*

$$Y^2Z = X^2(X - AZ),$$

*with* $A \in k$. *On this curve* (0:1:0) *is the flex and* (0:0:1) *the singular point.*

We distinguish two cases:

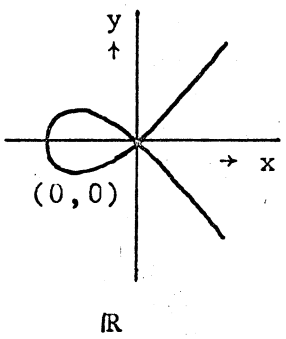
1) A = 0. Then $Y^2Z = X^3$, or in affine coordinates $y^2 = x^3$. There is a "double tangent" at the singular point (0,0) - in fact, every line $x = \alpha y$ is a tangent at (0,0) and y = 0 is the *tangent cone*. The singular point is called a *cusp*. Let $C_{ns}$ denote the set of non-



singular points on the curve C. It is easy to see that the map $C_{ns} \to \mathbb{A}^1_K \overset{\sim}{=} K^+$, $(x,y) \mapsto x/y$ and flex $\mapsto 0$, is a bijection. All finite points on C may be given by the parametrization

$$(x,y) = (t^2,t^3).$$

2) $A \neq 0$. The equation becomes $y^2 = x^2(x + A)$ in affine coordinates.



There are two "distinct tangents" at the singular point (0,0): they form the *tangent cone*. The singular point is called a *node*. Choose $\alpha \in K$ such that $\alpha^2 = A$. The map $C_{ns} \to \mathbb{A}^1_K - \{0\} \overset{\sim}{=} K^\times$, given by $(x,y) \mapsto \frac{y-\alpha x}{y+\alpha x}$ and flex $\mapsto 1$, is again a bijection. The finite points $(x,y) \neq (0,0)$ on C are given by the parametrization

$$(x,y) = (t^2-A, t(t^2-A)).$$

This shows that in both cases C is a *rational curve* i.e. C may be parametrized by rational functions or, equivalently, $k(C) \overset{\sim}{=} k(t)$ is a pure transcendental extension of k. We shall now show that a plane absolutely irreducible non-singular cubic curve C is not rational. That is to say that the curve C is not birationally isomorphic (over K) to $\mathbb{P}^1_K$.

First we observe that $\Omega[\mathbb{P}^1_K] = 0$, since a differential of the first kind on $\mathbb{P}^1_K$ can only be zero. It then follows that the genus of $\mathbb{P}^1_K$ equals zero.

Now if C is a plane absolutely irreducible non-singular cubic, then C may be given by the affine equation

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

Consider the differential form $\omega = \frac{1}{y}dx$. For any point $P \in C$, $P \in \mathbb{A}^2_K$

with $y_P \neq 0$, we see that x is a local parameter at P and $\mathrm{ord}_P(\omega) = 0$. If $y_P = 0$, then y is a local parameter at P and again $\mathrm{ord}_P(\omega) = 0$. Let $P_\infty \in C$ be the point at infinity. Then z is a local parameter at $P_\infty$ and

$$x = uz^{-2},\ y = vz^{-3},$$

where u and v are units in the local ring of $P_\infty$. This shows that

$$\mathrm{ord}_{P_\infty}(\omega) = \mathrm{ord}_{P_\infty}(dx) - \mathrm{ord}_{P_\infty}(y) = \mathrm{ord}_{P_\infty}(x) - 1 - \mathrm{ord}_{P_\infty}(y) = 0$$

and thus $(\omega) = 0$. Now every differential form in $\Omega[C]$ can be written as

$$\phi\omega \quad \text{with } \phi \in K[C].$$

Hence $\phi = f(x) + g(x)y$, where $f,g \in K[x]$. Then

$$0 \leqq \mathrm{ord}_{P_\infty}(\phi) \leqq \min(\mathrm{ord}_{P_\infty}(f(x)), \mathrm{ord}_{P_\infty}(g(x)y)).$$

If $g \neq 0$, then it follows that $\mathrm{ord}_{P_\infty}(\phi) \leqq -3$, a contradiction. Hence $g = 0$ and $\phi = f(x)$. More over, if f is not a constant ($\neq 0$), then $\mathrm{ord}_{P_\infty}(\phi) \geqq 0$ again gives a contradiction. We deduce that $\phi \in K$. But then $\dim_K \Omega[C] = 1$ and this means that the genus of C equals 1. Since the genus is birationally invariant, it follows that $C \not\simeq \mathbb{P}^1_K$. We also observe that the canonical class $K_C$ is zero and this verifies $\deg(K_C) = g(C) - 1$ in this particular case. We have shown

THEOREM 3. *A plane absolutely irreducible non-singular curve* C *has genus* 1. *This means in particular that* C *can not be parametrized by rational functions.*

We return for a moment to singular plane cubics. As was shown, the non-singular points on a singular cubic are in one-to-one correspondence with the elements of the additive algebraic group $\mathbb{A}^1_K \cong K^+$ or of the multiplicative algebraic group $\mathbb{A}^1_K - \{0\} \cong K^\times$. This hints at the existence of a group-structure on the set of non-singular points of a plane singular cubic curve. We shall see that such an algebraic group structure also exists on plane non-singular cubics.

Let C be a plane absolutely irreducible non-singular cubic curve. Then C may be given by an affine equation

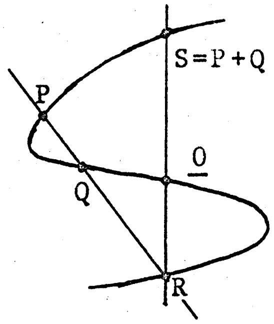
$$y^2 = x^3 + ax + b \qquad \text{with } a,b \in K$$

and the flex, which we shall denote by $\underline{0}$, lies on the line at infinity $z = 0$.

For any two points P and Q on C, let R be the third intersection point of C and the line through P and Q (this line is the tangent to C at P if P = Q). The line through R and $\underline{0}$ intersects C at a third point S. We define

$$P + Q := S,$$

the *sum* of the points P and Q (not to be confused with the sum of the divisors (P) + (Q)). Clearly, P + Q = Q + P and $P + \underline{0} = P$. For any $P \in C$, the line joining P and $\underline{0}$ intersects C also in the inverse of P, -P (this is, because $\underline{0}$ is a flex). Observe, that in case one takes a point $\underline{0}'$ on C which is not a flex as the neutral element, the inverse of P can be constructed by joining the third intersection of the tangent to C at $\underline{0}'$ with P. So far, this shows that the choice of neutral element is immaterial. Explicit addition formulae may easily be given. For instance, if P = (x,y), then -P = (x,-y)



in case $\underline{0}$ is the neutral element: $(x,y) + (x,-y) = \underline{0}$.

We are left to show that point addition, as defined above, is associative. To prove this, we proceed as follows. For any line L, we define the divisor

$$(L) = \sum_{P\in C} n_P(P),$$

where $n_P = 0$ if $P \notin C$ and $n_P$ is the intersection multiplicity of L at P in case $P \in C$. Then $\deg(L) = 3$ for any line L. Consequently, the divisors of any two lines $L_1$ and $L_2$ are equivalent, $(L_1) \sim (L_2)$. Now take three points P,Q and R on C. Let $L_1$ be the line through P and Q and $L_2$ the line through $\underline{0}$ and $P + Q$. Then $L_1$ intersects $L_2$ in S say, and $S \in C$. Thus

$$(L_1) = (P) + (Q) + (S) \text{ and } (L_2) = (S) + (\underline{0}) + (P+Q).$$

Since $(L_1) \sim (L_2)$ we deduce

(i) $$(P) + (Q) \sim (\underline{0}) + (P+Q).$$

Similarly, let $L_3$ be the line through $P + Q$ and R and let $L_4$ join $(P+Q) + R$ and $\underline{0}$. Suppose that $L_3$ intersects $L_4$ in $T \in C$. Then

$$(L_3) = (P+Q) + (R) + (T) \text{ and } (L_4) = (T) + (\underline{0}) + ((P+Q)+R).$$

This gives as before

(ii) $$(P+Q) + (R) \sim (\underline{0}) + ((P+Q)+R).$$

Combining (i) and (ii), we see that

$$(P) + (Q) + (R) \sim 2(\underline{0}) + ((P+Q)+R).$$

In an analogous fashion, we construct a point $P + (Q+R) \in C$ such that

$$(P) + (Q) + (R) \sim 2(\underline{0}) + (P+(Q+R)).$$

Consequently,

$$((P+Q)+R) \sim (P+(Q+R)).$$

Now suppose that $(P+Q) + R \neq P + (Q+R)$. Then there is a function $\phi \in K(C)$, such that

$$((P+Q)+R) - (P+(Q+R)) = (\phi).$$

Considering $\phi$ as a function $\phi\colon C \to \mathbb{P}^1_K$, it follows from the fact that $\phi$ has precisely one pole and one zero, that $K(C) \cong K(\phi)$. This means that $\phi$ is a biregular birational isomorphism. Hence $C \cong \mathbb{P}^1_K$. This is contradictory, as we have seen before. Thus

$$(P+Q) + R = P + (Q+R).$$

To show that the group law on C is algebraic, we have to prove that the mappings

$$f\colon C \to C \quad , \ f(P) = -P \ \text{ and}$$
$$g\colon C\times C \to C \quad , \ g(P,Q) = P + Q$$

are regular. This follows easily from the explicit formulae one can obtain in the coordinates of P and Q, working with the equation $y^2 = x^3 + ax + b$. Note that the group law on the set of non-singular points of a singular cubic is also given by lines.

We indicate the group on C by C(K). If the curve C and the flex $\underline{0}$ (or another neutral element) are defined over k, then the points on the (non-singular) curve C with coordinates in k form a subgroup C(k) of C(K). This follows simply from the observation that a line joining two points defined over k, intersects C in a third point with coordinates in k (note that

$a,b \in k$). This group $C(k)$ is called *the group of* k-*rational points on* C. In case k is an algebraic number field, the group $C(k)$ is finitely generated. This theorem, known as the Mordell-Weil theorem, will be discussed in a later section.

A more precise statement on the algebraic group of points on a non-singular cubic, is given in the following

THEOREM 4. *Let* C *be a plane absolutely irreducible non-singular cubic curve with a point* $P_0 \in C$. *Let* $\mathrm{Div}^o(C)$ *be the group of divisors of degree zero on* C *and let* $P(C)$ *be the subgroup of principal divisors, then*

$$C(K) \cong \mathrm{Div}^o(C)/_{P(C)} ,$$

*where the isomorphism is given by* $P \mapsto \mathrm{Class}_P$ *with* $(P) - (P_0) \in \mathrm{Class}_P$ . *In particular, the group law on* C *is independent (up to translation) of the choice of the point* $P_0$.

We shall prove the following theorem, which is contained in theorem 4.

THEOREM 5. *Let* C *and* C' *be two plane absolutely irreducible non-singular cubics and suppose* $\underline{0}$ *and* $\underline{0}'$ *are the zero elements of the groups* $C(K)$ *and* $C'(K)$ *respectively. Then every* K-*birational isomorphism* $\rho: C \overset{\sim}{\to} C'$ *which sends* $\underline{0}$ *to* $\underline{0}'$ *is a group isomorphism:* $C(K) \overset{\sim}{\to} C'(K)$.

*Proof*. For any two points $P,Q \in C$, we have

$$(P-\underline{0}) + (Q-\underline{0}) \sim ((P+Q)-\underline{0}).$$

Since C and C' are absolutely irreducible, we know that $\rho$ is biregular. It then follows from $K(C') \overset{\sim}{\to} K(C)$, that

$$(\rho(P)-\underline{0}') + (\rho(Q)-\underline{0}') \sim (\rho(P+Q)-\underline{0}'),$$

because of $\rho(\underline{0}) = \underline{0}'$. This gives $\rho(P+Q) = \rho(P) + \rho(Q)$ as required.

Note that, if $\underline{0}$ and $\underline{0}'$ have coordinates in k and C, C' and $\rho$ are defined over k, then also $C(k) \overset{\sim}{=} C'(k)$.

A natural question is: what does such an isomorphism look like in terms of the coordinates? The answer is given in the following theorem.

THEOREM 6. *We consider two plane absolutely irreducible non-singular cubic curves* C *and* C' *, given by the equations*

$$Y^2Z = X^3 - AXZ^2 - BZ^3 \quad , \quad Y'^2Z = X'^3 - A'X'Z'^2 - B'Z'^3$$

*respectively, with* $A,B,A',B' \in k$. *Suppose* $\underline{0} = \underline{0}' = (0:1:0)$ *gives the zero elements of* $C(K)$ *and* $C'(K)$. *Then every birational isomorphism* $\rho\colon C \overset{\sim}{\to} C'$ *, defined over* k *with* $\rho(\underline{0}) = \underline{0}'$ *is of the form*

$$\begin{aligned} X' &= c^2X \\ Y' &= c^3Y \qquad A' = c^4A \ , \ B' = c^6B \textit{ and } \ c \in k^*. \\ Z' &= Z \end{aligned}$$

*Proof.* We give only a sketch. Put $\tau = \frac{X}{Y}$ , $\phi = \frac{X}{Z}$ and $\psi = \frac{Y}{Z}$. Then $\tau$ is a local parameter at $\underline{0}$ (we consider $\tau,\phi$ and $\psi$ as elements of $k(C)$). It is easy to see that

$$\mathrm{ord}_{\underline{0}}(\phi) = -2 \text{ and } \mathrm{ord}_{\underline{0}}(\psi) = -3.$$

From the theorem of Riemann-Roch it follows that

$$\ell(2\underline{0}) := \dim_k L(2\underline{0}) = 2 \text{ and } \ell(3\underline{0}) = 3.$$

Then clearly, $\{1,\phi\}$ is a basis of $L(2\underline{0})$ and $\{1,\phi,\psi\}$ is a basis of $L(3\underline{0})$.

Similarly, if $\tau' = \frac{X'}{Y'}$, $\phi' = \frac{X'}{Z'}$ and $\psi' = \frac{Y'}{Z'}$ then $\{1,\phi'\}$ is a basis of $L'(2\underline{O}')$ and $\{1,\phi',\psi'\}$ is a basis of $L'(3\underline{O}')$. The birational isomorphism $\rho$ induces an isomorphism $k(C') \overset{\sim}{\to} k(C)$. Consequently, $L(2\underline{O}) \cong L'(2\underline{O}')$ and $L(3\underline{O}) \cong L'(3\underline{O}')$. Identifying $k(C)$ and $k(C')$, it is clear that

$\phi' \in L(2\underline{O})$ implies that $\phi' = a\phi + b$ with $a,b \in k$ and

$\psi' \in L(3\underline{O})$ implies that $\psi' = r\phi + s\psi + t$ with $r,s,t \in k$.

To arrive at the required result is now just a matter of arithmetic.

Note that if $\Delta$ and $\Delta'$ are the discriminants of the equations for C and C' respectively, then $\Delta' = c^{12}\Delta$. Since $\Delta = 16(4A^3-27B^2) \neq 0$, the expression $A^3/\Delta$ makes sense and $A'^3/\Delta' = A^3/\Delta$. For any plane absolutely irreducible non-singular cubic curve C, we define *the modular invariant* as the expression

$$j(C) = (48)^3A^3/\Delta \ ,$$

if C is birationally isomorphic to the curve C' with equation

$$Y^2Z = X^3 - AXZ^2 - BZ^3$$

in normal form with discriminant $\Delta$. The constant appearing in the definition of j(C) is a traditional one. It follows from the above that two birationally isomorphic non-singular cubic curves have the same modular invariant. Also, if k is algebraically closed and $j(C) = j(C')$, then there exists a k-isomorphism between C and C'.

THEOREM 7. *For each* $j \in K$ , *there is an absolutely irreducible non-singular cubic curve* C , *defined over* k(j) *such that* $j(C) = j$.

*Proof*. If $j = 0$, such a curve is $Y^2Z = X^3 - Z^3$. If $j = 12^3$, then $Y^2Z = X^3 - XZ^2$ satisfies the requirement and if $j \neq 0$ or $12^3$ then $Y^2Z = X^3 - AXZ^2 - BZ^3$, with $A = \frac{3}{4}j(j-12^3)$ and $B = \frac{1}{4}j(j-12^3)^2$ is a curve with modular invariant $j$.

## 3. ELLIPTIC FUNCTIONS.

Throughout this section we shall work in $\mathbb{C}$, the field of complex numbers.

A *lattice* in the complex plane $\mathbb{C}$ is a free subgroup of rank 2 over $\mathbb{Z}$, which generates $\mathbb{C}$ considered as a vectorspace over $\mathbb{R}$. Thus a lattice $L$ in $\mathbb{C}$ is a subgroup of the form

$$L = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$$

for two complex numbers $\omega_1$ and $\omega_2$, such that $\mathbb{C} = \mathbb{R}\omega_1 \oplus \mathbb{R}\omega_2$; clearly this is so iff $\omega_2 \neq 0$ and $\omega_1/\omega_2 \notin \mathbb{R}$. It is customary to select a basis $\{\omega_1, \omega_2\}$ for $L$ for which $\mathrm{Im}(\omega_1/\omega_2) > 0$ i.e. $\omega_1/\omega_2$ lies in the upper half plane $H := \{x+iy \mid y > 0\}$.

An *elliptic function* $f$ (with respect to the lattice $L$; we denote $f$ also by $f_L$) is a meromorphic function on $\mathbb{C}$, which is $L$-periodic. Thus

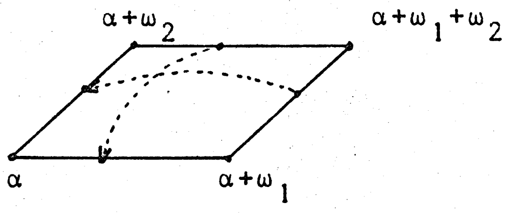
$$f(z+\omega) = f(z) \quad \text{for all } z \in \mathbb{C} \text{ and } \omega \in L.$$

Consequently, an $L$-elliptic function may be viewed as a function defined on the factor group ${}^{\mathbb{C}}/_{L}$. Since $f$ is $L$-periodic, the values it takes are already determined on the set of points

$$z = \alpha + t_1\omega_1 + t_2\omega_2 \text{ , } 0 \leqq t_1, t_2 < 1$$

for any $\alpha \in \mathbb{C}$. Let $P_\alpha$ be the *fundamental parallellogram*

$$P_\alpha := \{z \in \mathbb{C} \mid z = \alpha + t_1\omega_1 + t_2\omega_2, \; 0 \leqq t_1, t_2 \leqq 1\}.$$



By a proper identification of the points of $\partial P_\alpha$, the boundary of $P_\alpha$, it is easy to see that ${}^{\mathbb{C}}/_{L}$ is (topologically) homeomorphic, as a real manifold, to a torus, i.e. to $S^1 \times S^1$. Hence ${}^{\mathbb{C}}/_{L}$ is a compact group. This shows that a non-constant L-elliptic function (viewed as a meromorphic function on ${}^{\mathbb{C}}/_{L}$) must have a pole, because of Liouville's theorem.

For any L-elliptic function $f \neq 0$, we can use the Laurent expansion of f at a point $a \in \mathbb{C}$, to define the integer $\text{ord}_a(f)$, the *order of* f *at* a. Thus, if $\text{ord}_a(f) = -n$ , $n \in \mathbb{N}$ then f has a pole of order n at a and if $\text{ord}_a(f) = n \in \mathbb{N}$, then f has a zero of order n at a. Since f is L-periodic, we have

$$\text{ord}_{a+\omega}(f) = \text{ord}_a(f) \quad \text{for any } \omega \in L.$$

Hence, in writing $\text{ord}_a(f)$, we may consider a as an element of ${}^{\mathbb{C}}/_{L}$. The formal sum

$$\text{div}(f) = \Sigma \ \text{ord}_a(f)(a),$$

the *divisor* of f at $a \in {}^{\mathbb{C}}/_{L}$, has only finitely many non-zero coefficients, because the zero's and poles of f are isolated. They form a subgroup, the group of *principal divisors* $P({}^{\mathbb{C}}/_{L})$, of the additive group of all divisors $\text{Div}({}^{\mathbb{C}}/_{L})$. This group $\text{Div}({}^{\mathbb{C}}/_{L})$ is, as before, defined as the group of all finite formal sums

$$\overset{<\infty}{\Sigma} n_a(a) \qquad , \ n_a \in \mathbb{N},$$

with respect to the usual addition.

Before going into the question of the existence of L-elliptic functions, we state the following theorem (a proof of which may be found in [21]).

THEOREM 8. *Let f be a non-constant L-elliptic function. Then*

*(1) f is not entire*

*(2)* $\Sigma\ \mathrm{Res}_a(f) = 0$

*(3)* $\Sigma\ \mathrm{ord}_a(f) = 0$

*(4)* $\Sigma\ \mathrm{ord}_a(f)a = 0$ *(addition in* $\mathbb{C}/_L$*)*

Now (1) and (2) show that an elliptic function must have at least two poles (counting multiplicities). The fact that an elliptic function f has as many zero's as poles (this is the contents of (3)), implies that f takes all complex values the same number of times. Indeed, for any $a \in \mathbb{C}$, f and $f - a$ have the same poles, and consequently also the same zero's.

The existence of L-elliptic functions may be proved by exhibiting the *Weierstrass* $\wp$*-function*:

$$\wp_L(z) := z^{-2} + \sum_{\substack{\omega\in L\\ \omega\neq 0}} \left((z-\omega)^{-2} - \omega^{-2}\right) .$$

The series entering in the above formula is absolutely convergent for all $z \notin L$ and converges uniformly on compact sets $C \subset \mathbb{C}$ with $C \cap L = \phi$. Hence $\wp_L$ is meromorphic with a double pole (i.e. of order two) at each lattice point and with no other poles. So $\wp_L$ has only one double pole on the torus $\mathbb{C}/_L$. It is not difficult to show that $\wp_L$ is an even elliptic function. The derivative $\wp_L'$ can be computed by termwise differentiation, and thus we obtain

$$\wp_L'(z) = -2 \sum_{\omega\in L} (z-\omega)^{-3}.$$

This function is an odd elliptic function with one pole of order three at $0 \in \mathbb{C}/_L$.

By considering the Laurent expansion of $\wp_L$ and $\wp'_L$ at the origin, it is a straightforward exercise to show that

$$\wp'^2_L(z) = 4\wp^3_L(z) - g_2\wp_L(z) - g_3$$

identically in z, where $g_2 = g_2(L) := 60 \sum_{\substack{\omega\in L\\ \omega\neq 0}} \omega^{-4}$ and $g_3 = g_3(L) :=$ $= 140 \sum_{\substack{\omega\in L\\ \omega\neq 0}} \omega^{-6}$.

We claim that $g_2^3 - 27g_3^2 \neq 0$. To prove this, we consider the zero's of $\wp'_L(z)$. Since $\wp'_L$ has a treble pole (at 0), this function must also have three zero's, counting multiplicities. On the torus $\mathbb{C}/_L$ there are exactly four points a, such that $2a = 0$ (i.e. $2a \equiv 0 \bmod L$ in $\mathbb{C}$). They are represented by

$$0, \tfrac{1}{2}\omega_1, \tfrac{1}{2}\omega_2, \tfrac{1}{2}\omega_3$$

where $\omega_3 := \omega_1 + \omega_2$ in the fundamental parallellogram $P_0$. Since $\wp'_L$ is an odd function, we find that

$$\wp'_L(\tfrac{1}{2}\omega_i) = -\wp'_L(\tfrac{1}{2}\omega_i) \text{ for } i = 1,2,3.$$

Hence $\frac{1}{2}\omega_1$, $\frac{1}{2}\omega_2$ and $\frac{1}{2}\omega_3$ are precisely the three (simple) zero's of $\wp'_L$. Now put $e_i := \wp_L(\frac{1}{2}\omega_i)$ for $i = 1,2,3$. Comparing zero's and poles, we see that

$$\wp'^2_L(z) = 4(\wp_L(z)-e_1)(\wp_L(z)-e_2)(\wp_L(z)-e_3)$$

identically in z. Because $\wp_L$ takes on the value $e_i$ exactly twice, we have $e_i \neq e_j$ for $i \neq j$. Then the discriminant $\Delta$ of the polynomial $4x^3 - g_2x - g_3$ does not vanish, i.e.

$$0 \neq \Delta = \prod_{i<j} (e_i - e_j)^2 = 2^{-4}(g_2^3 - 27g_3^2).$$

Clearly, the set of all L-elliptic functions forms a field, whose constant field is $\mathbb{C}$. It turns out that this field is generated by $\wp_L$ and $\wp_L'$.

THEOREM 9. *The field of* L-*elliptic functions is generated by* $\wp_L$ *and* $\wp_L'$. *In particular, the field of even* L-*elliptic functions is the field* $\mathbb{C}(\wp_L)$. *The functions* $\wp_L$ *and* $\wp_L'$ *satisfy the functional equation*

$$\wp_L'^{\,2}(z) = 4\wp_L^3(z) - g_2\wp_L(z) - g_3.$$

*More over* $g_2^3 - 27g_3^2 \neq 0$.

We now turn our attention to the relation between elliptic functions and non-singular cubic curves defined over $\mathbb{C}$ (elliptic curves!).

Let C be the irreducible cubic curve given by the equation

$$Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3.$$

This curve is non-singular iff $g_2^3 - 27g_3^2 \neq 0$. If so, the map

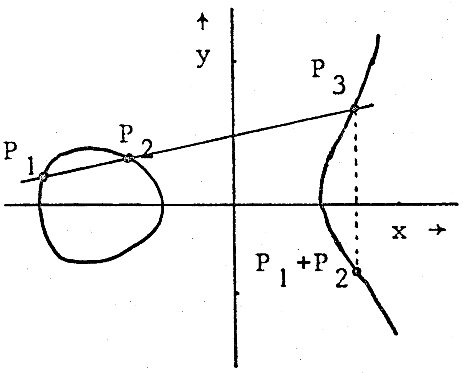
$$\rho\colon \mathbb{C} \to C \subset \mathbb{P}^2_{\mathbb{C}}\text{ , given by}$$

$$\rho\colon z \mapsto (z^3\wp_L(z), z^3\wp_L'(z), z^3)$$

factorizes through ${}^{\mathbb{C}}/_{L}$ : consider the diagram

$$\begin{tikzcd}
\mathbb{C} \arrow[rr, "\rho"] \arrow[dr, "\pi"'] & & C \subset \mathbb{P}^2_{\mathbb{C}} \\
& {}^{\mathbb{C}}/_{L} \arrow[ur, dotted, "\hat\rho"'] &
\end{tikzcd}$$

where $\pi\colon z \mapsto z \pmod L$. Then $\hat\rho$ is the map given by $\hat\rho\pi = \rho$. It is not difficult to see that $\hat\rho$ is a bijection: $\hat\rho$ is onto since $\rho$ is onto and $\hat\rho$ is injective because $\wp_L$ is an even function and $\wp_L'$ is an odd one. As we know, the points on the torus ${}^{\mathbb{C}}/_{L}$ form a group with respect to ordinary addition and the points on the curve C form a group $C(\mathbb{C})$ with respect to point addition. The bijection $\hat{\rho}$ is a group isomorphism! To prove this, we observe that the addition on C is given by: three points have sum zero whenever they are collinear. Suppose $\hat{\rho}(z_1) = P_1 \in C$ and $\hat{\rho}(z_2) = P_2 \in C$. Thus we have to show that $\hat{\rho}(z_1+z_2) = P_1 + P_2$. Suppose $P_1 = (x_1,y_1)$ and $P_2 = (x_2,y_2)$. If $x_1 = x_2$, then $y_2 = -y_1$ and $P_1 + P_2 = \underline{0}$. Also $\wp_L(z_1) = \wp_L(z_2)$ and hence $z_1 + z_2 \equiv 0 \pmod{L}$. This shows that $\hat{\rho}(0) = \underline{0}$. Assume $x_1 \neq x_2$. Then $\wp_L(z_1) \neq \wp_L(z_2)$. This means that we can find $a,b \in \mathbb{C}$ such that $\wp_L'(z_1) = a\wp_L(z_1) + b$ and $\wp_L'(z_2) = $ $= a\wp_L(z_2) + b$, or geometrically, $P_1$ and $P_2$ lie on the line $y = ax + b$. The function $f(z) := \wp_L'(z) - a\wp_L(z) - b$ is L-elliptic with a pole of order 3 at 0. Thus f must have three zero's, two of which are known to be $z_1$ and $z_2$. Let $z_3$ be the third zero of f. Then, since $\Sigma \operatorname{ord}_a(f)a = 0$, we deduce that $z_1 + z_2 + z_3 \equiv 0 \pmod{L}$. The points $P_1$, $P_2$ and $P_3 = \hat{\rho}(z_3)$ are collinear. Because $P_3 = (x_3,y_3)$ implies $-P_3 = (x_3,-y_3)$, we find that $\hat{\rho}(z_1+z_2) = \hat{\rho}(-z_3) = -P_3 = P_1 + P_2$.



We have proved

THEOREM 10. *For any lattice* L *of* $\mathbb{C}$, *let* $C_L$ *be the non-singular cubic curve given by the functional equation of* $\wp_L(z)$. *Then the map* $\rho\colon \mathbb{C} \to C \subset \mathbb{P}^2_{\mathbb{C}}$, $\rho(z) = (z^3\wp_L(z), z^3\wp_L'(z), z^3)$ *induces a group isomorphism between* $\mathbb{C}/_L$ *and* $C_L(\mathbb{C})$.

All we have done so far depends on the lattice L. A natural question may be asked: what relation should exist between two lattices $L_1$ and $L_2$ (or two toruses $\mathbb{C}/_{L_1}$ and $\mathbb{C}/_{L_2}$) to be birationally isomorphic?

First we observe that for any lattices L and M the toruses $\mathbb{C}/_L$ and $\mathbb{C}/_M$ are topologically the same. This is also true for the groups on $\mathbb{C}/_L$ and $\mathbb{C}/_M$ with respect to ordinary complex addition. So we need extra structure. Consider the torus $\mathbb{C}/_L$ as a Riemann-surface (i.e. a Hausdorff space with an analytic structure). Note that the isomorphism given in theorem 10 is an *analytic isomorphism*. Now let L and M be two lattices and let $\phi: \mathbb{C}/_L \to \mathbb{C}/_M$ be an analytic isomorphism such that $\phi(0) = 0$. Consider the commutative diagram:

$$\begin{tikzcd}
\mathbb{C}/_L \arrow[r, "\phi"] & \mathbb{C}/_M \\
\mathbb{C} \arrow[u, "\pi_L"] \arrow[r, "\hat{\phi}"] & \mathbb{C} \arrow[u, "\pi_M"']
\end{tikzcd} \qquad \pi_M\hat{\phi} = \phi\pi_L$$

Then for any $z \in \mathbb{C}$ and $\omega \in L$, we must have $\hat{\phi}(z+\omega) - \hat{\phi}(z) \in M$. More over $\hat{\phi}(z+\omega) - \hat{\phi}(z)$ is independent of z. Consequently, $\hat{\phi}'(z+\omega) = \hat{\phi}'(z)$ and this shows that $\hat{\phi}'$ is an entire L-elliptic function. Thus $\hat{\phi}(z) = \alpha z + \beta$. Clearly $\beta = 0$, since $\phi(0) = 0$ and $\alpha \neq 0$. This means that $\alpha L = M$ (we call such lattices *homothetic*). The converse is also true i.e. homothetic lattices induce an analytic isomorphism between their toruses.

Obviously, homothety is an equivalence relation. Let us denote it by $L \sim_h M$. Thus $L \sim_h M$ iff there is an $\alpha \in C^*$ such that $\alpha L = M$. Now for each lattice L there is at least one $\tau \in H = \{ z \in \mathbb{C} \mid \mathrm{Im}(z) > 0 \}$ such that $L \sim_h L_\tau := \mathbb{Z} \oplus \mathbb{Z}\tau$. For instance, if $\{\omega_1,\omega_2\}$ is a basis for L with $\mathrm{Im}(\omega_1/\omega_2) > 0$, put $\tau = \omega_1/\omega_2$. Then $L \sim_h M$ iff $L_\tau \sim_h M_{\tau'}$.

Suppose $L_\tau = \alpha L_{\tau'}$ with $\alpha \neq 0$. Then there are integers a,a',b,b',c,c',d and d' such that

$$\begin{matrix} \alpha\tau' = a\tau + b \\ \alpha = c\tau + d \end{matrix} \quad \text{and} \quad \begin{matrix} \alpha^{-1}\tau = a'\tau' + b' \\ \alpha^{-1} = c'\tau' + d' \end{matrix} \quad \text{or}$$

$$\tau' = \frac{a\tau+b}{c\tau+d} \quad \text{and} \quad \tau = \frac{a'\tau'+b'}{c'\tau'+d'} .$$

The matrices $S = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $S' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ must be inverse to one another. Since their entries are integral, it follows that $\det S = \pm 1$. More over $\mathrm{Im}(\tau) > 0$ and $\mathrm{Im}(\tau') > 0$ and thus $\det S = +1$. Conversely, if there is an $S \in SL_2(\mathbb{Z}) :=$ $= \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in \mathbb{Z},\ ad - bc = 1\}$ such that $\begin{pmatrix} \tau' \\ 1 \end{pmatrix} = S\begin{pmatrix} \tau \\ 1 \end{pmatrix}$, then $L_\tau \sim_h L_{\tau'}$, as is easy to see. Since the matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$ have the same effect, we consider them equal. The resulting group we denote by $\Gamma := SL_2(\mathbb{Z})/\{\pm 1\}$. This group is called the *modular group* and an element of $\Gamma$ is a *modular transformation*. Two elements $\tau,\tau' \in H$ are called *congruent modulo* $\Gamma$ if they can be transformed into each other by means of a modular transformation. It can be seen that the set of congruence classes $^H/_\Gamma$ is in one-to-one correspondence with the *fundamental domain* (cf. [47], ch. VII):

$$D := \{\tau \in H : |\tau| > 1, -\tfrac{1}{2} \leq \mathrm{Re}(\tau) < \tfrac{1}{2}\} \cup \{\tau \in H : |\tau| = 1, -\tfrac{1}{2} \leq \mathrm{Re}(\tau) < 0\}.$$

All this leads to

THEOREM 11. *There is a one-to-one correspondence between the elements of* ${}^{H}/_{\Gamma}$ *and the isomorphism classes of plane non-singular cubic curves defined over* $\mathbb{C}$.

It remains to show that every plane non-singular cubic curve is isomorphic to such a curve given by the torus ${}^{\mathbb{C}}/_{L}$ for a lattice $L \subset \mathbb{C}$.

Let L be a lattice and C the cubic curve with equation

$$Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3$$

with $g_2 = g_2(L) = 60 \sum_{\substack{\omega\in L\\ \omega\neq 0}} \omega^{-4}$ and $g_3 = g_3(L) = 140 \sum_{\substack{\omega\in L\\ \omega\neq 0}} \omega^{-6}$.

If we put $\tau = \omega_1/\omega_2$, then clearly $g_2(L) = \omega_2^{-4} g_2(L_\tau)$ and $g_3(L) = \omega_2^{-6} g_3(L_\tau)$. This shows that the modular invariant $j(C) = 1728g_2^3(L)/(g_2^3(L) - 27g_3^2(L)) = 1728g_2^3(L_\tau)/(g_2^3(L_\tau)-27g_3^2(L_\tau)) = {}$ $=: J(\tau)$ is a function of $\tau$. This function is a *modular function*; it is invariant under the modular group.

It can be shown that J gives a bijection between the fundamental domain D and $\mathbb{C}$ (cf.[22], ch. I).

Thus, if C is a plane non-singular cubic curve with modular invariant j(C), then a $\tau \in D$ may be found such that $j(C) = J(\tau)$. In turn this gives a lattice $L_\tau$ and a cubic curve $C_\tau = {}^{\mathbb{C}}/_{L_\tau}$. Since C and $C_\tau$ have the same modular invariant, they are birationally isomorphic.

To conclude this section, we like to comment briefly on the concept of genus of a cubic curve. Consider the Weierstrass function $\wp_L$ as a function on ${}^{\mathbb{C}}/_{L}$. Then $\wp_L\colon {}^{\mathbb{C}}/_{L} \to \tilde{\mathbb{C}} = S^2$ is an analytic map onto the extended complex plane $\tilde{\mathbb{C}}$ (by $S^2$ we mean the Riemann sphere). Now $\wp_L$ takes on all complex values exactly twice, with the exception of $e_1$, $e_2$, $e_3$ and $\infty$ in $S^2$. Thus we have a double sheeted covering with four ramification points $e_1$, $e_2$, $e_3$ and $\infty$. On the curve $C(\mathbb{C}) \cong \mathbb{C}/_L$ this mapping coincides with

$$C(\mathbb{C}) \to \mathbb{P}^1_{\mathbb{C}} = S^2 \;, \quad (x,y) \mapsto x \;, \; \underline{0} \mapsto \infty = (0:1:0).$$

We can visualize the Riemann surface $\mathbb{C}/_L$ as the surface constructed by sticking together (in the proper way) two Riemann spheres, each with two slits from $e_1$ to $e_2$ and from $e_3$ to $\infty$. This gives us a torus, or equivalently, a Riemann sphere with one handle. The *topological genus* of a Riemann surface homeomorphic to a Riemann sphere with g handles is precisely this number g. So we see that the algebraic genus and the topological genus coincide (this is also true for $g \neq 1$;cf.[30], p. 132). Also, by the Zeuthen-Hurwitz formula we have (the map given above has degree 2):

$$2g(C) - 2 = 2(2g(\mathbb{P}^1_{\mathbb{C}})-2) + (2-1)(\#\text{ramification points}) =$$
$$= -4 + 4 = 0.$$

## 4. ELLIPTIC CURVES.

We shall give (finally) a general definition of what is known as an elliptic curve. Again, we fix a field k with an algebraic closure $K = \overline{k}$ .

An algebraic curve is defined (as was done in the first section for a plane algebraic curve) as the set of zero's, contained in the projective space $\mathbb{P}^{\ell}_{K}$ ($\ell \geqq 2$), of a polynomial $f(x_1,\ldots,x_\ell)$ with coefficients in k. All concepts, discussed in section 1 apply in this case. For instance, the genus of an algebraic curve C is essentially the transcendence degree of its function field K(C) over K.

DEFINITION. *An elliptic curve* E *is an absolutely irreducible non-singular algebraic curve of genus 1, furnished with a point* P. *The curve* E *is defined over* k, *in notation* $E|k$, *if the point* P *has coordinates in* k*(and if the defing equation has coefficients in* k, *which was already assumed).*

An elliptic curve $E|k$ is birationally isomorphic (over k) to a plane cubic curve, given by an equation (in *generalized Weierstrass normal form*):

$$(\ast) \qquad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (a_i \in k),$$

where x and y are coordinates in the affine plane. The point P (see definition) is transformed into the flex $\underline{0} = (0:1:0) \in \mathbb{P}^2_K$, the neutral element for the group law on the curve. The extra terms in the equation are due to the fact that nothing was assumed on char(k). If char(k) ≠ 2, then an equation for $E|k$ may be given in the form ($\ast$) with $a_1 = a_3 = 0$, and in case char(k) ≠ 2 or 3, one may also assume that $a_2 = 0$ (see theorem 1).

Given an equation ($\ast$) for $E|k$, we define (cf.[11]and [21], Appendix 1):

$$b_2 = a_1^2 + 4a_2 \qquad c_4 = b_2^2 - 24b_4$$
$$b_4 = a_1a_3 + 2a_4 \qquad c_6 = -b_2^3 + 36b_2b_4 - 216b_6$$
$$b_6 = a_3^2 + 4a_6$$
$$b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2$$

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \quad \text{(the discriminant)}$$
$$j = c_4^3 / \Delta \quad \text{(the modular invariant)}$$

The connection with $y^2 = 4x^3 - g_2x - g_3$ (see section 3) in char(k) $\neq$ 2 or 3, is given by

$$c_4 = 12g_2 \text{ , } c_6 = 216g_3 \text{ , } \Delta = g_2^3 - 27g_3^2 \text{ , } j = 1728J.$$

It is easy to check that

$$4b_8 = b_2b_6 - b_4^2 \quad \text{and} \quad c_4^3 - c_6^2 = 2^6 3^3 \Delta.$$

A differential of the first kind on (✲) is

$$\omega = \frac{dx}{2y+a_1x+a_3} \text{ .}$$

Two elliptic curves $E|k$ and $E'|k$ with weierstrass models $y^2 + a_1xy$ ... and $y'^2 + a_1'x'y'$ ... are birationally isomorphic iff there are $r,s,t,u \in k$ with $u \neq 0$, such that

$$x = u^2x' + r \quad \text{and} \quad y = u^3y' + u^2sx' + t.$$

In particular, we see that under such a transformation

$$u^4c_4' = c_4 \text{ , } u^6c_6' = c_6 \text{ , } u^{12}\Delta' = \Delta \text{ , } j' = j \text{ , } \omega' = u\omega.$$

Also $E(k) \cong E'(k)$ implies that $j = j'$ and conversely if $j = j'$ then $E(K) \cong E'(K)$.

For all these facts we refer to section 2.

As an example, consider the "generic" curve $E|k(j)$, given by the Weierstrass equation

$$y^2 + xy = x^3 - \frac{36}{j-1728}x - \frac{1}{j-1728} \qquad j \neq 0 \text{ or } 1728.$$

The discriminant $\Delta = j^2/(j-1728)^3$ and $j$ is the modular invariant (this explains the term "generic"). See also theorem 7.

A further example is furnished by the curve $E|k$ given by

$$x_1^3 + x_2^3 - x_3^3 = 0.$$

If $\mathrm{char}(k) \neq 2$ or $3$, then the birational transformation

$$x = 3x_3/(x_1+x_2) \ , \ 2y = 9(x_1-x_2)/(x_1+x_2) + 1$$

maps the equation into

$$y^2 - y = x^3 - 7 \qquad \Delta = -3^9 \text{ and } j = 0.$$

(cf. section 1).

Amongst all the Weierstrass equations an elliptic curve may possess, it is sometimes possible to select one with a certain "minimality" condition. For instance, for the curve $E|\mathbb{Q}$ (take $k = \mathbb{Q}$) given in the last example, the equation $y^2 - y = x^3 - 7$ is minimal in the sense that any other equation for $E|\mathbb{Q}$ of weierstrass type has discriminant $\Delta' = -u^{12}3^9$ with $u \in \mathbb{Z}$, $u \neq 0$.

The precise definition runs as follows. A Weierstrass equation (✻) for $E|k$ is called *minimal with respect to a discrete valuation* $\nu$ of $k$ iff $\nu(a_i) \geqq 0$ for all $i$ and $\nu(\Delta)$ is minimal, subject to that condition.

Let $R_\nu$ be the valuation ring of $\nu$ in k. It can be shown that there is always a minimal equation for $E|k$ with respect to $\nu$. More over, such a minimal equation is unique up to a transformation of the form $x = u^2x' + r$, $y = u^3y' + su^2x' + t$ with $r,s,t \in R_\nu$ and u invertible in $R_\nu$. Further the differential $\omega$ associated with a minimal Weierstrass equation is unique.

If $a_i \in R_\nu$ and $\nu(\Delta) < 12$, then the equation (✱) is apparently minimal. On the other hand, if the modular invariant j of a minimal equation belongs to $R_\nu$, then $\nu(\Delta) < 12 + 12\nu(2) + 6\nu(3)$ provided that $\mathrm{char}(k) \neq 2$ or 3. An algorithm for reducing to minimal form is given by Tate in [56].

Let k be an algebraic number field with class number 1 (or, equivalently, the ring of integers $O_k$ is a principal ideal domain). Then any elliptic curve $E|k$ has a Weierstrass equation which is simultaneously minimal for all discrete valuations $\nu$ of k (cf. [51]). Such an equation is called a *global minimal Weierstrass equation for* $E|k$. It follows, that a global minimal Weierstrass equation has coefficients in $O_k$ and that the discriminant of such an equation is unique as an (integral) ideal of k.

Let $f(x,y) = y^2 + a_1xy + \ldots = 0$ be a minimal equation for the curve $E|k$ with respect to a valuation $\nu$. Let $R_\nu$ be the valuation ring with prime ideal $P_\nu$ and residue class field $k_\nu = {}^{R}\nu/_{P_\nu}$. Reducing the coefficients $a_i$ of $f = 0$ modulo $P_\nu$, one obtains an equation $\tilde{f} = 0$ for a plane cubic curve $\tilde{E}|k_\nu$. Clearly, the curve $\tilde{E}|k_\nu$ is uniquely determined up to a transformation of type $x = u^2x' + r$ , $y = u^3y' + su^2x' + t$ with

$r,s,t,u \in k_\nu$ and $u \neq 0$. If $\tilde{E}|k_\nu$ has no singular points, then $\tilde{E}|k_\nu$ is elliptic and $\tilde{f} = 0$ is an equation for $\tilde{E}|k_\nu$. In that case $\tilde{\Delta} \neq 0$ or, equivalently $\nu(\Delta) = 0$. We say that $E|k$ has *good (or stable or non-degenerate) reduction at* $\nu$. In that case $j \in R_\nu$ and $\tilde{j}$ is the modular invariant of $\tilde{E}|k_\nu$. If $\tilde{\Delta} = 0$ i.e. $\nu(\Delta) > 0$, then $\tilde{E}|k_\nu$ is a rational curve and $E|k$ has *bad (or degenerate) reduction at* $\nu$. In particular, if $\nu(\Delta) > 0$ and $\nu(c_4) = 0$, then $\tilde{E}|k_\nu$ has a node and we say that $E|k$ has *multiplicative (or semistable) reduction at* $\nu$. Now $j \notin R_\nu$. If the singular point is defined over $k_\nu$ (for instance, if $k_\nu$ is perfect), then $\tilde{E}_{ns}(\overline{k}_\nu)$ is a multiplicative algebraic group (here $\tilde{E}_{ns}$ is the non-singular part of $\tilde{E}$). If $\tilde{E}|k_\nu$ has a cusp, which occurs only if $\nu(\Delta) > 0$ and $\nu(c_4) > 0$, then $E|k$ is said to have *additive (or unstable) reduction at* $\nu$. In that case we have that $\tilde{E}_{ns}(\overline{k}_\nu)$ is an additive algebraic group (see also section 2).

If we define

$$E_0(k) := \{P \in E(k) | \quad \tilde{P} \in \tilde{E}_{ns}(k_\nu)\}$$

and if we denote by $\rho$ the reduction map $\rho \colon E(k) \to \tilde{E}(k_\nu)$, then we have

THEOREM 12. *The set* $E_0(k)$ *is a sub-group of finite index in* $E(k)$ *and* $\rho|E_0(k)$ *is a homomorphism of groups.*

That $E_0(k)$ is a sub-group of $E(k)$ and that $\rho|E_0(k)$ (the restriction of $\rho$ to $E_0(k)$) is a homomorphism follows from the fact that reduction carries lines into lines (by which the group law is given). The finiteness of the index depends on the minimality of the equation $f = 0$. It is a consequence of Tate's minimality algorithm (cf. [56]). More information on the index may be found in [55].

If we assume that k is an algebraic number field, then it is easy to see that an elliptic curve $E|k$ must have good reduction at all but a finite number of places. For, consider a Weierstrass equation for $E|k$ with coefficients in the ring of integers $O_k$. Then the ideal, generated by the discriminant $\Delta$ of the equation can be written as a finite product of prime ideals of $O_k$, because of the unique factorization of ideals in $O_k$. Hence $\nu(\Delta) = 0$ for almost all discrete valuations $\nu$ of k.

It is natural to ask whether, given an algebraic number field k, there are any curves $E|k$ with good reduction at all places of k. In particular, if k has class number 1, the question becomes: are there any Weierstrass equations (✻) with $a_i \in O_k$ and with unit discriminant? Tate has shown that this is not the case if $k = \mathbb{Q}$.

THEOREM 13. *An elliptic curve* $E|\mathbb{Q}$ *has bad reduction at* $\nu$ *for at least one place* $\nu$ *of* $\mathbb{Q}$.

*Proof*. Assuming the statement to be false, there must be a curve $E|\mathbb{Q}$ having a global minimal model (✻) with coefficients in $\mathbb{Z}$ and unit discriminant. In particular

$$c_4^3 - c_6^2 = 2^6 3^3 \Delta = \pm 2^6 3^3.$$

Knowing that the diophantine equation $x^3 - y^2 = a$, $a \in \mathbb{Z}$ $a \neq 0$, has at most a finite number of solutions $(x,y) \in \mathbb{Z}^2$ (this was first shown by A. Thue in [57]), we find that $(c_4, c_6) = (\pm 12, 0)$ is the only possibility (see also [10]). Then $b_2 \equiv 0 (\mathrm{mod}\ 2)$

and this implies that $a_1 \equiv 0 \pmod 2$. Hence $b_2 \equiv 0 \pmod 4$ and $b_4 \equiv 0 \pmod 2$. We arrive at a contradiction, because it would follow that $c_4 = b_2^2 - 24b_4 \equiv 0 \pmod{16}$. For different proofs see [33] and [51].

In [51] this result is generalized to elliptic curves defined over imaginary quadratic number fields having a global minimal model. That there are nevertheless curves defined over certain imaginary quadratic number fields having good reduction everywhere, was shown by Tate (cf. [54] and [51]): he proves that the generic curve (see page 32), defined over $\mathbb{Q}(j)$, where $j$ is given by $j^2 - 1728j \pm n^{12} = 0$ for a rational integer $n$ prime to 6, has good reduction everywhere.

Another example of a curve with good reduction everywhere, is the curve given by the equation

$$y^2 + xy = x^3 - 2\varepsilon x^2 + \varepsilon^2 x \qquad \Delta = -\varepsilon^6 ,$$

defined over $\mathbb{Q}(\sqrt{7})$, where $\varepsilon = 8 + 3\sqrt{7}$ is a fundamental unit of $\mathbb{Z}[\sqrt{7}]$.

An important result, due to Shafarevich is given in the following theorem.

THEOREM 14. *Let* $k$ *be an algebraic number field and* $\Pi$ *a finite set of places of* $k$. *Then there is only a finite number of elliptic curves* $E|k$ *(up to isomorphism) with good reduction everywhere outside* $\Pi$.

In the proof of this theorem (cf. [41]) use is made of a famous theorem of C.L. Siegel to the effect that on any affine equation for an elliptic curve $E|k$ there are only finitely many points with coordinates in $O_k$. The method of proof is ineffective. However, not so long ago, A. Baker [2] has given an explicit upperbound for $\max(\|x\|,\|y\|)$, where $(x,y)$ is a solution with coordinates in $O_k$ of the diophantine equation

$y^2 = P(x)$ with $P \in O_k[x]$ , $\deg(P) \geqq 3$ and P has three simple zero's. This shows that for a given set $\Pi$ , all curves $E|k$ with good reduction outside $\Pi$ may be, at least in principle, effectively found.

F.B. Coghlan ([10]) has determined global minimal equations for all curves $E|\mathbb{Q}$ with good reduction outside the set $\{2,3\}$ and in [51] this was carried out for all curves $E|\mathbb{Q}(i)$ and $E|\mathbb{Q}\sqrt{-2})$ with good reduction outside $\{2\}$.

Let k be a field with discrete valuation $\nu$ and let $E|k$ be an elliptic curve. The *exponent of the conductor of* E *at* $\nu$ is a certain integer $f_\nu \geqq 0$, which is a finer measure of the reduction of E at $\nu$ then "degenerate" versus "non-degenerate". The integer $f_\nu$ equals zero for good reduction at $\nu$, one for multiplicative reduction and $2+\delta$ for additive reduction, where $\delta \geqq 0$ is a certain "measure of wild ramification" (cf. [34] and [45]). It was shown by Tate that $\delta = 0$ in case $\mathrm{char}(k) \neq 2$ or 3. Tate also devised an algorithm for finding the exponent $f_\nu$ in general (cf. [56]). In it he analyses the reduction of the minimal model for E in the sense of Néron ([31]). Néron's minimal model is in general not a plane cubic. If n is the total number of irreducible components, not counting multiplicities, of Néron's reduction of E over K, then

$$f_\nu = \nu(\Delta) + 1 - n ,$$

as was shown by Ogg (cf. [34]). Here $\Delta$ is the discriminant of a minimal (Weierstrass) equation for E with respect to $\nu$.

If k is an algebraic number field and $E|k$ has a global minimal Weierstrass equation over k with discriminant $\Delta$, then

$$N = \prod_{\mathfrak{p}|\Delta} \mathfrak{p}^{f_{\mathfrak{p}}}$$

is the *conductor of* $E|k$; the product runs over all prime ideal divisors $\mathfrak{p}$ of $\Delta$.

To conclude this section, we mention the concept of *potentially good reduction*. The curve $E|k$ has potentially good reduction at the discrete valuation $\nu$ of k if there exists a finite extension k' of k and a prolongation $\nu'$ of $\nu$ to k' such that $E|k'$ has good reduction at $\nu'$. It was shown by M. Deuring [14], that $E|k$ has potentially good reduction at $\nu$ iff the modular invariant j belongs to the valuation ring $R_\nu$ (i.e. $\nu(j) \geqq 0$). See also [45].

We finally mention the good reduction "criterion of Ogg-Néron-Shafarevich", see [45] and [55], a discussion of which goes beyond the scope of this exposition.

## 5. THE GROUP E(k). SOME CONJECTURES.

In this final section we shall briefly comment on some outstanding problems in the theory of elliptic curves.

About 55 years ago, L.J. Mordell proved the following theorem (cf. [27]).

THEOREM 15. *If* E *is an elliptic curve defined over* $\mathbb{Q}$, *then the group* $E(\mathbb{Q})$ *is finitely generated.*

Not long after Mordell obtained his result, A. Weil generalized it to elliptic curves defined over algebraic number fields (In fact his generalization reached further: he proved a similar result for abelian varieties defined over number fields - elliptic curves are abelian varieties of dimension 1). Since then, the theorem in its more general form has become known as the Mordell-Weil theorem. Also, A. Néron and S. Lang extended the theorem for abelian varieties over function fields of one variable with finite constant field (cf. [19]). Proofs of the Mordell-Weil theorem can be found in Cassels' survey article [7] and Mordell's book [28].

If we denote the torsion subgroup of $E(\mathbb{Q})$ by $E(\mathbb{Q})_{tors}$ (i.e. the subgroup of points of finite order), then theorem 15 says that there is a non-negative integer r such that

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \times \mathbb{Z}^r .$$

The integer r is called the *rank* of $E|\mathbb{Q}$.

Let us first investigate the group of points of finite order. To that end we introduce the concept of *isogeny*. Let k be an algebraic number field with algebraic closure K, and let $E_1|k$ and $E_2|k$ be two elliptic curves. Consider a rational map $\lambda : E_1 \rightarrow E_2$, defined (everywhere) over k. More over, suppose that $\lambda$ is surjective and that $\lambda(\underline{0}_1) = \underline{0}_2$. Then $\lambda$ induces a homomorphism

$$\Sigma\ n_P(P) \rightarrow \Sigma\ n_P(\lambda(P))$$

of the group of divisor classes of degree zero on $E_1(k)$ into the corresponding group on $E_2(k)$, taking principal divisors into principal divisors. The kernel of $\lambda$ is finite and the *degree* of $\lambda$ is the number of points in $\mathrm{Ker}(\lambda)$ counting their multiplicities. (In fact the degree of $\lambda$ is the degree of the corresponding function field extension $k(E_1)/k(E_2)$). Such a rational map is called an *isogeny*.

An isogeny $\lambda: E_1 \to E_2$ induces a *dual isogeny* $\hat{\lambda} : E_2 \to E_1$ with the property that $\lambda\cdot\hat{\lambda} : E_2 \to E_2$ and $\hat{\lambda}\cdot\lambda : E_1 \to E_1$ is multiplication by $m = \deg(\lambda) = \deg(\hat{\lambda})$ on $E_2$, $E_1$ respectively (cf. [7], p.216 and [21], ch. II). In particular, multiplication by $m \in \mathbb{N}$ on the curve E (i.e. the map $m(id)_E$) is an isogeny of degree $m^2$.

THEOREM 16. *Let* $E|k$ *be an elliptic curve. If the positive integer* m *is prime to the characteristic of* k, *then the group* $E_m(K)$ *of elements of order dividing* m *is isomorphic to* $\mathbb{Z}/_{m\mathbb{Z}} \times \mathbb{Z}/_{m\mathbb{Z}}$. *If* $m = p^a$ *for a prime* $p = \mathrm{char}(k)$ , *then* $E_m(K)$ *is a cyclic group of order* m *or of order* 1, *depending on the value of the so-called Hasse invariant.*

(The Hasse invariant equals 1 and E is said to be *ordinary* in the first case; E is *supersingular* if the Hasse invariant equals zero and then $E_m(K) = 0$. See [55]).

If k is of characteristic zero and $K = \mathbb{C}$, then the statement of the theorem follows immediately from $E(\mathbb{C}) \cong \mathbb{C}/_L$, because the kernel of the mapping $E(\mathbb{C}) \to E(\mathbb{C})$, $t \mapsto mt$ equals

$$E_m(\mathbb{C}) = \tfrac{1}{m}L/_L \cong L/_{mL} \cong \mathbb{Z}/_{m\mathbb{Z}} \times \mathbb{Z}/_{m\mathbb{Z}} .$$

Next, let k be a field of characteristic $p > 0$ with $q = p^a$ elements. The elements of k are characterized in K by the equation $\alpha^q = \alpha$. Hence if the curve $E|k$ is given by $f(x_1,\dots,x_\ell) = 0$, the map $(x_1,\dots,x_\ell) \mapsto (x_1^q,\dots,x_\ell^q)$ induces a rational map $\pi_{E|k} : E \to E$, the *Frobenius endomorphism relative to* k (An endomorphism is an isogeny or the zero map), whose fixed point set is precisely the set E(k) of k-rational points on E. Now $\pi_{E|k}$ is a purely inseparable isogeny of degree q, i.e. the points of the kernel occur with multiplicity one. E. Artin conjectured and H. Hasse proved (cf. [14])

THEOREM 17. *If* k *is a finite field with* $q = p^a$ *elements, then the order of the group* E(k) *of an elliptic curve* $E|k$ *is*

$$|E(k)| = 1 + q - a \quad \textit{with} \quad |a| \leqq 2q^{\frac{1}{2}}.$$

An immediate consequence of this theorem is that two isogenous curves defined over a finite field k have the same number of k-rational points.

We return to the case $k = \mathbb{Q}$. But first, we mention an important result due to Lutz (cf. [23]). Let $E|\mathbb{Q}$ be an elliptic curve and let p be a prime number. If $\mathbb{Q}_p$ denotes the p-adic completion of $\mathbb{Q}$, then

THEOREM 18. *For any prime* p, *the group* $E(\mathbb{Q}_p)$ *contains only finitely many points of finite order. More over, the subgroup of points of finite order is effectively computable.*

So, if $E(\mathbb{Q})_{tors}$ is the group of points of finite order on $E|\mathbb{Q}$, the theorem shows that $E(\mathbb{Q})_{tors}$ is finite and computable.

Indeed, $E(\mathbb{Q}) \subset E(\mathbb{Q}_p)$ for any fixed prime number p. One may derive from Lutz's result the explicit

THEOREM 19. *If* $P = (p_1, p_2)$ *is a point of finite order defined over* $\mathbb{Q}$ *on the curve given by*

$$y^2 = x^3 + Ax + B \qquad \textit{with } A, B \in \mathbb{Z},$$

*then* $p_1, p_2 \in \mathbb{Z}$ *and either* $p_2 = 0$ *or* $p_2^2$ *divides* $4A^3 + 27B^2$.

Information on $E(\mathbb{Q})_{tors}$ for an elliptic curve $E|\mathbb{Q}$ can be obtained by considering the curves one gets by means of reduction modulo p for various primes p. For example, if $E|\mathbb{Q}$ is given by a Weierstrass equation with integer coefficients, we select a prime p for which $E|\mathbb{Q}$ has good reduction at p. The reduction map sends $E(\mathbb{Q})_{tors}$ into $\tilde{E}(\mathbb{Z}/_{p\mathbb{Z}})$. This mapping is injective if p is odd and the kernel is of order 1 or 2 if p = 2 (see theorem 16).

Recently, B. Mazur has settled the problem of the structure of $E(\mathbb{Q})_{tors}$. He proved (cf. [26])

THEOREM 20. *Let* $E|\mathbb{Q}$ *be an elliptic curve. Then the torsion subgroup* $E(\mathbb{Q})_{tors}$ *is isomorphic to one of the following 15 groups:*

$\mathbb{Z}/_{m\mathbb{Z}}$ *for* $m \leqq 10$ *or* $m = 12$ ; $\mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2n\mathbb{Z}}$ *for* $n \leqq 4$.

*More over, all of these 15 groups do indeed occur.*

In his proof he uses techniques attributed to Demjanenko [12], [13] and Kubert [18] of associating to a point of $E(\mathbb{Q})_{tors}$ on any elliptic curve $E|\mathbb{Q}$ (under certain conditions) $\mathbb{Q}$-rational points of some specific algebraic curves $C|\mathbb{Q}$, so-called modular curves. Besides [26] mentioned above, an excellent account of the problem is given by Ogg in [36] and [38], where the connection between the curve $E|\mathbb{Q}$ together with a point P of order m and the modular curve $X_1(m)$ is given. In connection with theorem 20 we also refer to [4].

In this context, we have the

CONJECTURE 1. *If* k *is an algebraic number field, the order of* $E(k)_{\mathrm{tors}}$ *is bounded by a positive integer* B(k) *depending only on* k *(if* E *ranges through all curves* $E|k$*).*

See Cassels [7], Manin [24], Demjanenko [13]. For no $k \neq \mathbb{Q}$ the conjecture is proved; one does not even know what a reasonable value for the bound B(k) should be.

For many curves $E|\mathbb{Q}$ the rank r has been computed. See for instance the account in Zimmer [62], section 11. In all these cases r is quite small. There is however no definite reason why this should always be the case. Néron has shown in [32] that there must be curves $E|\mathbb{Q}$ with $r \geq 11$. Very interesting numerical investigations have been carried out by Birch and Swinnerton-Dyer (cf. [5]). They were led by their results to state several conjectures, some of which relate the rank r of $E|\mathbb{Q}$ to the behaviour of the so-called L-*function* of $E|\mathbb{Q}$ near the point s = 1. To be more precise, let $y^2 + a_1xy + ..$ be a global minimal Weierstrass equation for $E|\mathbb{Q}$ with discriminant $\Delta$. For any prime p, the reduced curve $\tilde{E}_p|\mathbb{F}_p$ is defined over the finite field $\mathbb{F}_p$ of p elements. Denote by $N_p$ the number of points on $\tilde{E}_p$, rational over $\mathbb{F}_p$. Then $N_p$ is one more (because of the point $\underline{0}$ at infinity) than the number of distinct solutions of the congruence $y^2 + a_1xy + \ldots \equiv 0 \pmod p$. If $\alpha_p$ and $\overline{\alpha}_p$ are the characteristic roots of the Frobenius endomorphism of $\tilde{E}_p|\mathbb{F}_p$, then $\alpha_p\overline{\alpha}_p = p$ and thus $|\alpha_p| = p^{\frac{1}{2}}$. More over (see also theorem 17)

$$N_p = 1 + p - \alpha_p - \overline{\alpha}_p .$$

All this is only true in case $\tilde{E}_p$ is elliptic, i.e. $p \nmid \Delta$, or equivalently, $E|\mathbb{Q}$ has good reduction at p. The *local* L-*function for* $E|\mathbb{Q}$ is then defined as

$$L_{\tilde{E}_p}(s) = \Big((1-\alpha_p p^{-s})(1-\overline{\alpha}_p p^{-s})\Big)^{-1}.$$

On the other hand, if $E|\mathbb{Q}$ has bad reduction at p, thus $p|\Delta$, then $\tilde{E}_p|\mathbb{F}_p$ has a singular point which is necessarily defined over $\mathbb{F}_p$. If this singular point is a cusp, then $N_p = 1 + p$. If it is a node, we distinguish the two cases

(i) the tangent directions at the singular point are defined over $\mathbb{F}_p$, and

(ii) the tangent directions are not defined over $\mathbb{F}_p$ and hence conjugate over $\mathbb{F}_p$.

In case (i) we have $N_p = p$ and $N_p = 2 + p$ in the second case (ii). If we set $t_p := 1 + p - N_p$, then the *local* L-*function for* $E|\mathbb{Q}$ at the bad prime p is defined to be

$$L_{\tilde{E}_p}(s) = (1-t_p p^{-s})^{-1}.$$

The *global* L-*function for* $E|\mathbb{Q}$ is now defined by

$$L_E(s) = \prod_p L_{\tilde{E}_p}(s) ,$$

where the product runs over all primes p. This product certainly converges for $\mathrm{Re}(s) > \frac{3}{2}$. In fact it is a Dirichlet series $\Sigma c_n n^{-s}$ with $c_p = 1 + p - N_p$ at the prime p.

For every prime p not dividing $\Delta$ (a good prime), we have

$$L_{\tilde{E}_p}(1) = \left(\frac{N_p}{p}\right)^{-1} .$$

This suggests that, in order to obtain information on the behaviour of $L_E(s)$ near $s = 1$, one should look at

$$\prod_p \left(\frac{N_p}{p}\right) .$$

Now $|N_p - p| \leqq 2p^{\frac{1}{2}}$ and $\prod_{p\leqq x} (1 + \frac{1}{p}) \sim c\log x \quad (x \to \infty)$ for a certain constant c. This, together with their numerical results, led Birch and Swinnerton-Dyer to the following

CONJECTURE 2. *If* r *is the rank of the curve* $E|\mathbb{Q}$*, then there are constants* $c_1$ *and* $c_2$ *(depending on* E*), such that*

$$c_1 \leqq (\log x)^{-r} \prod_{p\leqq x} \left(\frac{N_p}{p}\right) \leqq c_2$$

*for all sufficiently large* x*. More over the* L*-function* $L_E(s)$ *has a zero of order* r *at* $s = 1$.

On examining the values of $\prod_{p\leqq x}\left(\frac{N_p}{p}\right)$, Birch and Swinnerton-Dyer were able to predict and verify the value of r for quite a number of curves.

Let N be the conductor of $E|\mathbb{Q}$ i.e. $N = \prod_{p|\Delta} p^{f_p}$ (see section 4). We define the function

$$Z_E(s) := N^{\frac{1}{2}s}(2\pi)^{-s}\Gamma(s)L_E(s).$$

CONJECTURE 3. *The function* $Z_E(s)$ *can be analytically continued to the entire* s*-plane as a holomorphic function. Further more it satisfies the functional equation*

$$Z_E(s) = \pm Z_E(2-s)$$

*for one or the other sign.*

This conjecture is known to be true for some special cases, such as curves with complex multiplication (cf. [15]). For general information on curves with complex multiplication, one should consult [43].

In connection with this last conjecture, we would like to mention another remarkable conjecture, due to A. Weil (cf. [60]). Since the setting in which this conjecture plays an important role is quite involved, we shall merely give a superficial outline. A full account may be found in [53].

CONJECTURE 4. *All elliptic curves* $E|\mathbb{Q}$ *of conductor* $N$ *are parametrized by modular functions for the congruence subgroup* $\Gamma_0(N)$ *of the modular group* $\Gamma$.

This needs clarification. First of all, $\Gamma_0(N)$ is defined as

$$\Gamma_0(N) := \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \mid c \equiv 0 \pmod N \}.$$

If $H = \{ z \in \mathbb{C} \mid \mathrm{Im}(z) > 0 \}$, the upper half plane, let $Y_0(N)$ denote the quotient of $H$ and $\Gamma_0(N)$. See also section 3. Now let $X_0(N)$ be the compactification of $Y_0(N)$ by adjoining the cusps (for an explanation of this and other facts concerning modular functions, see [37], [22] and [35]). Then $X_0(N)$

becomes a compact Riemann surface and thus may be viewed as an algebraic curve defined over $\mathbb{C}$ (by means of an embedding in projective space). In fact, $X_0(N)$ is even a curve defined over $\mathbb{Q}$. Now conjecture 4 says that for any curve $E|\mathbb{Q}$ of conductor N, there is a rational map

$$\varphi : X_0(N) \to E$$

defined over $\mathbb{Q}$. This gives the parametrization of $E|\mathbb{Q}$ mentioned in the conjecture, because $\phi$ is given in terms of a special modular function (which corresponds to $L_E(s)$) for the congruence subgroup $\Gamma_0(N)$. Consequently, the number of these particular modular functions should be equal to the number of isogeny classes of elliptic curves $E|\mathbb{Q}$ of conductor N. Note that the conductor is invariant under isogeny.

As an example, consider the first non trivial case N = 11. In [58] it is shown that the only curves $E|\mathbb{Q}$ of conductor 11 are (up to isomorphism):

(i) $y^2 - y = x^3 - x^2 - 10x - 20$

(ii) $y^2 - y = x^3 - x^2$

(iii) $y^2 - y = x^3 - x^2 - 7820x - 263580$ (See also [59])

Observe that for any given N it is possible, in principle, to construct all curves $E|\mathbb{Q}$ of conductor N. See theorem 14. Now the curves (ii) and (iii) are isogenous over $\mathbb{Q}$ to (i) and up to isomorphism there are no others isogenous to (i). More over equation (i) is a Weierstrass equation for the modular curve $X_0(11)$. This shows the truth of the conjecture in case N = 11.

Conjecture 4 has been checked for many values of N, and all the information thus obtained points to the truth of it. See for instance [48].

# REFERENCES.

This bibliography is not meant to be complete. Extensive lists of additional references may be found in [7],[46] and [55].

[1] Atkin, A.O.L. & Lehner, J. - Hecke operators on $\Gamma_0(m)$. Math. Ann. 185 (1970), 134-160.

[2] Baker, A. - Bounds for the solutions of the hyperelliptic equation. Proc. Cam. Phil. Soc. 65 (1969), 439-444.

[3] Baker, A. & Coates, J. - Integer points on curves of genus 1. Proc. Cam. Phil. Soc. 67 (1970), 595-602.

[4] Billing, G. & Mahler, K. - On exceptional points on cubic curves. J. London Math. Soc. 15 (1940), 32-43.

[5] Birch, B.J. & Swinnerton-Dyer, H.P.F. - Notes on elliptic curves I,II. J. reine u. angew. Math. (Crelle) 212 (1963), 7-25; 218 (1965), 79-108.

[6] Borel, A. a.o. - Seminar on complex multiplication. Lecture Notes in Math. 21. Berlin-Heidelberg-New York, Springer, 1966.

[7] Cassels, J.W.S. - Diophantine equations with special reference to elliptic curves. J. London Math. Soc. 41 (1966),193-291.

[8] Chevalley, C. Introduction to the theory of algebraic functions of one variable. Math. Surveys VI, AMS, Providence, 1951.

[9] Coates, J. - Verification of Weil's conjecture on elliptic curves over $\mathbb{Q}$ in some special cases. Proc. Number Theory Conf. Univ. of Colorado, Boulder (1972), 43-48.

[10] Coghlan, F.B. - Elliptic curves with conductor $N = 2^m 3^n$. Ph.D. thesis. Manchester, 1967.

[11] Déligne, P. - Courbes elliptiques: Formulaire (d'après J.Tate). In: Modular functions of one variable IV. Lecture Notes in Math. 476. Berlin-Heidelberg-New York. Springer, 1975, 53-73.

[12] Demjanenko, V.A. - On the torsion of elliptic curves (in Russian). Izv. Akad. Nauk. SSSR 35 (1971), 280-307.

[13] Demjanenko, V.A. - On the uniform boundness of the torsion of elliptic curves over algebraic number fields.(in Russian). Proc. Steklov Inst. Math. CXXXII (1973), 82-87. (English translation AMS 1975), 93-99.

[14] Deuring, M. - Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Abh. Math. Sem. Hamburg 14 (1941), 197-272.

[15] Deuring, M. - Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins. Nachr. Akad. Wiss. Göttingen Math.-Phys. (1953), 85-94; (1955), 13-42; (1956), 37-76; (1957), 55-80.

[16] Frey, G. - Some remarks concerning points of finite order on elliptic curves over global fields. Arkiv för Math. 15 (1977), 1-19.

[17] Fulton, W. - Algebraic curves. Amsterdam-New York, Benjamin, 1969.

[18] Kubert, D. - Universal bounds on the torsion and isogenies of elliptic curves. Ph.D. thesis, Harvard, 1973.

[19] Lang, S. & Néron, A. - Rational points of abelian varieties over function fields. Am. J. Math. (1959), 95-118.

[20] Lang, S. - Diophantine geometry. New York, Interscience, 1962.

[21] Lang, S. - Elliptic functions. Addison-Wesley, Reading, 1973.

[22] Lang, S. - Introduction to modular forms. Grundlehren der Math. Wiss. 222. Berlin-Heidelberg-New York, Springer, 1976.

[23] Lutz, E. - Sur l'équation $y^2 = x^3-Ax-B$ dans les corps p-adiques. J. reine u. angew. Math. (Crelle), 177 (1937), 238-247.

[24] Manin, Y.I. - A uniform bound for p-torsion in elliptic curves. (in Russian). Izv. Akad. Nauk. SSSR, 33 (1969), 459-465.

[25] Mazur, B. & Tate, J. - Points of order 13 on elliptic curves. Invent. Math. 22 (1973), 41-49.

[26] Mazur, B. - Rational points on modular curves. In: Modular functions of one variable V. Lecture Notes in Math. 601, Berlin-Heidelberg-New York, Springer, 1977, 107-148.

[27] Mordell, L.J. - On the rational solutions of the indeterminate equations of the third and fourth degrees. Proc. Cam. Phil. Soc. 21 (1922), 179-192.

[28] Mordell, L.J. - Diophantine equations. Pure & Appl. Math. 30, Academic Press, London-New York, 1969.

[29] Mumford, D. - Abelian varieties. Tata Inst. Fund. Res. Studies 5. Oxford Univ. Press, 1974.

[30] Mumford, D. - Algebraic geometry I. Complex projective varieties. Grundlehren der Math. Wiss. 221, Berlin-Heidelberg-New York, Springer, 1976.

[31] Néron, A. - Modèles minimaux des variétés abéliennes sur les corps locaux et globaux. Publ. Math. IHES 21, Paris, 1964.

[32] Néron, A. - Propriétés arithmétiques de certaines familles de courbes algébriques. Proc. Int. Congress Amsterdam III, (1954), 481-488.

[33] Ogg, A.P. - Abelian curves of 2-power conductor. Proc. Cam. Phil. Soc. 62 (1966), 143-148.

[34] Ogg, A.P. - Elliptic curves and wild ramification. Amer. J. Math. 89 (1967), 1-21.

[35] Ogg, A.P. - Modular forms and Dirichlet series. New York-Amsterdam, Benjamin, 1969.

[36] Ogg, A.P. - Rational points of finite order on elliptic curves. Invent. Math. 12 (1971), 105-111.

[37] Ogg, A.P. - Survey of modular functions of one variable. In: Modular functions of one variable I. Lecture Notes in Math. 320. Berlin-Heidelberg-New York, Springer, 1973, 1-35.

[38] Ogg, A.P. - Rational points on certain elliptic modular curves. Analytic Number Theory. Proc. Symp. Pure Math. XXIV, AMS, Providence (1973), 221-231.

[39] Olson, L.D. - Torsion points on elliptic curves with given j-invariant. Manusc. Math. 16 (1975), 145-150.

[40] Oort, F. - Elliptic curves: Diophantine torsion solutions and singular j-invariants. Math. Ann. 207 (1974), 139-162.

[41] Oort, F. - Hyperelliptic curves over number fields. In: Lecture Notes in Math. 412. Berlin-Heidelberg-New York, Springer, 1974, 211-219.

[42] Robert, A. - Elliptic curves. Lecture Notes in Math. 326. Berlin-Heidelberg-New York, Springer, 1973.

[43] Serre, J.-P. - Complex multiplication. In: J.W.S. Cassels & A. Fröhlich - Algebraic number theory. Washington D.C. Thompson Book Co., 1967.

[44] Serre, J.-P. - Abelian $\ell$-adic representations and elliptic curves. Amsterdam-New York, Benjamin, 1968.

[45] Serre, J.-P. & Tate, J. - Good reduction of abelian varieties. Ann. of Math. (1968), 492-517.

[46] Serre, J.-P. - Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Invent. Math. 15 (1972), 259-331.

[47] Serre, J.-P. - A course in arithmetic. Graduate Texts in Math. 7. Berlin-Heidelberg-New York, Springer, 1973,

[48] Setzer, C.B. - Elliptic curves of prime conductor. Ph.D. thesis Harvard, 1972.

[49] Shafarevich, I.R. - Basic algebraic geometry. Springer, 1977. (reprinted from Grundlehren der Math. Wiss. 213, 1974).

[50] Shimura, G. - Introduction to the arithmetic theory of automorphic functions. Publ. Math. Soc. Japan 11, Iwanomi Shoten Publ. & Princeton Univ. Press, 1971.

[51] Stroeker, R.J. - Elliptic curves defined over imaginary quadratic number fields. A Diophantine approach. Ph.D. thesis, Amsterdam, 1975

[52] Swinnerton-Dyer, H.P.F. - The conjectures of Birch and Swinnerton-Dyer and of Tate. Proc. Conf. Local Fields. Driebergen (1966), 132-157.

[53] Swinnerton-Dyer, H.P.F. & Birch, B.J. - Elliptic curves and modular functions. In: Modular functions of one variable IV. Lecture Notes in Math. 476. Berlin-Heidelberg-New York, Springer, 1975, 2-32.

[54] Tate, J.T. - Letter to Serre, dated July 24th, 1971.

[55] Tate, J.T. - The arithmetic of elliptic curves. Invent. Math. 23 (1974), 179-206.

[56] Tate, J.T. - Algorithm for finding the type of a singular fibre in an elliptic pencil. In: Modular functions of one variable IV. Lecture Notes in Math. 476. Berlin-Heidelberg-New York, Springer, 1975, 33-52.

[57] Thue, A. - Ueber Annäherungswerte algebraischer Zahlen. J. reine u. angew. Math. 135 (1909), 284-305.

[58] Van der Poorten, A.J. - The polynomial $x^3+x^2+x-1$ and elliptic curves of conductor 11. Séminaire Delange-Pisot-Poitou (Théorie des nombres) 18e année (1977), 1-8.

[59] Vélu, J. - Courbes elliptiques sur $\mathbb{Q}$ ayant bonne réduction en dehors de {11}. Comptes Rend. Acad. Sc. Paris, 273 Série A (1971), 73-75.

[60] Weil, A. Ueber die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen. Math. Ann. 168 (1967), 149-156.

[61] Weil, A. - Dirichlet series and automorphic forms. Lecture Notes in Math. 189. Berlin-Heidelberg-New York, Springer, 1971.

[62] Zimmer, H.G. - Computational problems, methods and results in algebraic number theory. Lecture Notes in Math. 262. Berlin-Heidelberg-New York, Springer, 1972.

Econometric Institute
ERASMUS University
Burg. Oudlaan 50
Rotterdam - 3016.
The Netherlands

## LIST OF REPORTS 1978

7800 "List of Reprints, nos 200-208; Abstracts of Reports Second Half 1977".

7801/S "Conjugate $\Pi$-Variation and Process Inversion", by L. de Haan and S.J. Resnick.

7802/S "General Quadratic Forms in Normal Variates", by C. Dubbelman.

7803/S "On Bahadur's Representation of Sample Quantiles", by L. de Haan and E. Taconis-Haantjes.

7804/O "Experiments with a Reduction Method for Nonlinear Programming Based on a Restricted Lagrangian", by G. v.d. Hoek.

7805/S "Derivatives of Regularly Varying Functions in IR$^{d}$ and Domains of Attraction of Stable Distributions", by L. de Haan and S.I. Resnick.

7806/E "Estimation and Testing of Alternative Production Function Models", by S. Schim van der Loeff and R. Harkema.

7807/E "Money Illusion and Aggregation Bias", by J. van Daal.

7808/M "Aspects of Elliptic Curves: An Introduction", by R.J . Stroeker.