A LEISURELY INTRODUCTION TO FORMAL GROUPS AND ELLIPTIC CURVES

Antonia W. Bluher

The purpose of this paper is twofold: to explain in an elementary way how to associate a formal group law to an elliptic curve (in Parts I and II) and to discuss some theorems related to work of Couveignes [C] (in Part III). The subject of formal groups is enormous, and the subject of elliptic curves is even larger. In Parts I and II we content ourselves with presenting just enough background to see how the two subjects are interconnected. Many (in fact, most) interesting topics relating elliptic curves and formal groups are not mentioned, for instance the connections of formal groups and elliptic curves with L-functions and the applications of formal groups to lifting ordinary abelian varieties from characteristic p to characteristic zero. The reader who is interested in these topics can consult the bibliography of [H]. This exposition should be accessible to people with no background in elliptic curves or formal groups.

We treat curves defined over arbitrary fields, including fields of characteristic two or three. Some standard theorems are stated without proof; in those cases precise references are given. For instance, it is not proved that the group law for an elliptic curve is associative. The paper is divided into three parts: (I) Formal group laws; (II) Elliptic curves and their associated formal group laws; and (III) Further results on formal group laws. Each part is divided into several sections. Cross references to theorems, propositions, lemmas, examples, equations within a part are given in parentheses, for example (3.2). Cross references from within one part to another part are preceded by the appropriate roman numeral, for example (I.3.2). Apart from some results in §III.3, none of the material is original. I would like to thank Al Laing for a very careful reading of the original manuscript and many suggestions for improvement.

Contents

PART I: FORMAL GROUPS

1. Definition and construction of formal group laws
2. A formal semigroup law is automatically a formal group law
3. Homomorphisms of formal group laws
4. Heights

PART II. ELLIPTIC CURVES AND THEIR ASSOCIATED FORMAL GROUPS

1. Background on elliptic curves
2. The affine plane $Y \neq 0$
3. Function fields, local rings, and uniformizers
4. Power series expansions
5. Isogenies
6. Constructing the formal group law of an elliptic curve
7. Homomorphisms of formal group laws arising from isogenies
8. Height of an elliptic curve

PART III. FURTHER RESULTS ON FORMAL GROUPS

1. Some theorems of Couveignes
2. $\mathrm{Hom}(F, F')$ as a $\mathbf{Z}$-module or $\mathbf{Z}_p$-module
3. Consequences of Couveignes' theorems

PART I: FORMAL GROUPS

§I.1. Definition and construction of formal group laws

Let R be a commutative ring with a multiplicative identity 1. A **formal power series over** R is a symbol $\sum_{n=0}^{\infty} a_n \tau^n$, where $a_n \in R$ and τ is a dummy variable. The set of power series can be made into a ring $R[[\tau]]$ by defining

$$\sum a_i \tau^i + \sum b_i \tau^i = \sum (a_i + b_i)\tau^i$$

$$(\sum a_i \tau^i)(\sum b_i \tau^i) = \sum c_i \tau^i, \qquad \text{where } c_i = \sum_{j=0}^{i} a_j b_{i-j}.$$

In other words, addition and multiplication are defined by extending the usual addition and multiplication rules for polynomials. One can recursively define $R[[X,Y]] = R[[X]][[Y]]$, $R[[X,Y,Z]] = R[[X,Y]][[Z]]$, and so on.

In general it is not possible to compose two power series in a meaningful way. For example, if we tried to form the composition $f \circ g$ with $f = 1 + \tau + \tau^2 + \tau^3 + \cdots$ and $g = 1 + \tau$ we would get

$$f \circ g = 1 + (1+\tau) + (1+\tau)^2 + (1+\tau)^3 + \cdots$$

The constant term is $1 + 1 + 1 + \cdots$, which makes no sense. But there are some cases where $f \circ g$ does make sense, namely when f is a polynomial *or* when the constant term of g is zero. Let $R[[X,Y]] = R[[X]][[Y]]$, the ring of formal power series in two variables. If $F \in R[[X,Y]]$ and $g, h \in \tau R[[\tau]]$ then

$$F(g,h) \quad \text{makes sense and belongs to } R[[\tau]].$$

To see this, we must show that only finitely many terms of $F(X,Y)$ contribute to the nth coefficient of $F(g,h)$. Let $F(X,Y) = \sum f_{ij} X^i Y^j$. If $g = \sum_{i=1}^{\infty} g_i \tau^i$ and $h = \sum_{i=1}^{\infty} h_i \tau^i$ then $g^i h^j = g_1 h_1 \tau^{i+j} +$ higher order terms, so if $i + j > n$ then $f_{ij} g^i h^j$ does not contribute to the nth coefficient of $F(g,h)$. Since there are a finite number of terms $X^i Y^j$ with $i + j \leq n$, it follows that $F(g,h)$ is defined. Notice that if the constant term of F vanishes then $F(g,h) \in \tau R[[\tau]]$.

A one dimensional (commutative) **formal group law** over R is a power series $F \in R[[X,Y]]$ with zero constant term such that the "addition" rule on $\tau R[[\tau]]$ given by

$$g \oplus_F h = F(g,h)$$

makes $\tau R[[\tau]]$ into an abelian group with identity 0. In other words, for every g, h we must have $(f \oplus_F g) \oplus_F h = f \oplus_F (g \oplus_F h)$ (associative law), $f \oplus_F g = g \oplus_F f$ (commutative law), $f \oplus_F 0 = f$ (0 is identity), and for each $f \in \tau R[[\tau]]$ there exists $g \in \tau R[[\tau]]$ such that $f \oplus_F g = 0$ (inverses). Denote this group by $\mathcal{C}(F)$.

The following proposition gives a general method to construct formal group laws.

Proposition 1.1. *Let G be an abelian group, 0_G its identity element, and write its multiplication law additively. Suppose there is a one-to-one map $T : \tau R[[\tau]] \to G$ such that $T(0) = 0_G$, and a power series $F \in R[[X,Y]]$ with zero constant term such that*

$$T(g) + T(h) = T(F(g,h)) \tag{1.1}$$

for all $g, h \in \tau R[[\tau]]$. Then F defines a formal group law.

The nontrivial part of the proof is the existence of inverses. The proof will be given in the next section. Here we give three examples of the construction. The first two are warm-up examples, and the third is the construction of the formal group law associated to an elliptic curve.

Example 1.2. Let $G = R[[\tau]]$ under usual addition. Let $T : \tau R[[\tau]] \to R[[\tau]]$ be the inclusion. Then the equation (1.1) may be written as $g + h = F(g, h)$. Thus $X \oplus_F Y = F(X, Y) = X + Y$. This is called the **additive formal group law**.

Example 1.3. Assume R is a ring with a unit. The units of $R[[\tau]]$ are the power series whose constant term is a unit in R; see Lemma 1.4 below.

Let $T : \tau R[[\tau]] \to R[[\tau]]^\times$ be given by

$$T(g) = 1 + g.$$

Then

$$T(g)T(h) = (1 + g)(1 + h) = 1 + g + h + gh = T(g + h + gh).$$

Thus we are led to the **multiplicative formal group law**

$$X \oplus_F Y = F(X, Y) = X + Y + XY.$$

Lemma 1.4. *The units of the ring $R[[X_1, \ldots, X_n]]$ are the power series whose constant term is a unit in R.*

Proof. Let $R_j = R[[X_1, \ldots, X_j]]$ for $1 \le j \le n$, and let $R_0 = R$. If $j > 0$ then $R_j = R_{j-1}[X_j]$ by definition. Let M_j denote the ideal of R_j generated by $X_1, X_2, \ldots, X_j$ when $j > 0$, and let $M_0 = \{0\}$. We make the inductive hypothesis that $R_j^\times = R^\times + M_j$ for all $j < n$. This holds trivially when $n = 1$. Let $n > 1$, and let $\sum a_i X_n^i \in R_n$ be a power series whose inverse we wish to compute, where $a_i \in R_{n-1}$. Then $\sum a_i X_n^i \sum b_i X_n^i = 1$ iff

$$a_0 b_0 = 1$$

$$a_0 b_1 + a_1 b_0 = 0$$

$$\cdots$$

$$a_0 b_m + a_1 b_{m-1} + \cdots + a_{m-1} b_1 + a_m b_0 = 0$$

$$\cdots$$

This infinite system of equations has a solution with b_i in R_{n-1} iff a_0 is a unit in R_{n-1}. Thus

$$R_n^\times = R_{n-1}^\times + X_n R_n.$$

By induction hypothesis, $R_{n-1}^\times + X_n R_n = R^\times + M_{n-1} + X_n R_n$, and this equals $R^\times + M_n$, since $M_n = M_{n-1} + X_n R_n$. □

Example 1.5. Those not familiar with elliptic curves should read this example after reading §II.1. Let R be a domain and let L be the quotient field of $R[[\tau]]$. Let E be an elliptic curve with equation of the form

$$Y^2 Z + a_1 XYZ + a_3 YZ^2 = X^3 + a_2 X^2 Z + a_4 XZ^2 + a_6 Z^3,$$

where the a_i belong to R. Since $R \subset L$, one can consider $E(L)$, the solutions to the above equation which lie in $\mathbf{P}^2(L)$. In Part II we will show that $E(L)$ is a group (provided the projective curve is nonsingular), explicitly give a one-to-one map $T : \tau R[[\tau]] \to E(L)$, and find a power series F such that $T(g) + T(h) = T(F(g, h))$. F will be called the **formal group law associated to the elliptic curve** E.

§I.2. A formal semigroup law is automatically a formal group law

Let R be a commutative ring with a multiplicative identity which we denote by 1. In the preceding section we defined a commutative formal group law to be a power series in two variables which makes $\tau R[[\tau]]$ into an abelian group with identity 0. The more customary definition is as follows: a (commutative) **formal group law over** R is a power series $F(X, Y) \in R[[X, Y]]$ such that

$$\begin{array}{lll} (i) & F(X,0) = X; & \text{(Additive Identity)} \\ (ii) & F(X,Y) = F(Y,X) & \text{(Commutative Law)} \\ (iii) & F(F(X,Y),Z) = F(X,F(Y,Z)) & \text{(Associative Law).} \end{array} \tag{2.1}$$

We will show in Proposition 2.3 that this definition is equivalent to our earlier one. The first property implies that F has the form $X + YH(X, Y)$. By symmetry in X and Y, it must therefore be of the form

$$F(X,Y) = X + Y + XYG(X,Y), \qquad G \in R[[X,Y]]. \tag{2.2}$$

First we should check that (*iii*) makes sense; that is, that $F(F(X, Y), Z)$ and $F(X, F(Y, Z))$ are well defined power series in X, Y, and Z. This follows from the following lemma.

Lemma 2.1. *Let F, g be power series in two variables and let h be a power series in one variable. Suppose that g and h have zero constant term. Then $F(g(X, Y), h(Z))$ is a well defined power series in $R[[X, Y, Z]]$.*

Proof. If F is a polynomial then the result is clear. Let $F = \sum F_{ab} X^a Y^b$. Observe that $g(X, Y)^a h(Z)^b$ consists only of terms $c_{ijk} X^i Y^j Z^k$ such that $i + j + k \geq a + b$. In other words, if $i + j + k = N$ then only the terms of F with $a + b \leq N$ contribute to the coefficient of $X^i Y^j Z^k$ in $F(g, h)$. The important point is that there are only finitely many such a and b. This proves that $F(g, h)$ is well defined. □

Lemma 2.2. *Let F be a power series satisfying the three conditions above. There exists a power series $\iota(\tau) \in \tau R[[\tau]]$ such that*

$$F(g, \iota \circ g) = 0 \qquad \text{for all } g \in \tau R[[\tau]].$$

Proof. Let $\iota^{(1)} = -\tau$. By (2.2)

$$F(\tau, \iota^{(1)}) \equiv \tau - \tau \equiv 0 \bmod \tau^2.$$

Now assume inductively that $\iota^{(N)} \in \tau R[[\tau]]$ satisfies $F(\tau, \iota^{(N)}) \equiv 0 \bmod \tau^{N+1}$ and $\iota^{(N)} \equiv \iota^{(N-1)} \bmod \tau^N$. Then there is $a \in R$ such that

$$F(\tau, \iota^{(N)}) \equiv a\tau^{N+1} \bmod \tau^{N+2}.$$

Let $\iota^{(N+1)} = \iota^{(N)} - a\tau^{N+1}$. By (2.2)

$$F(\iota^{(N)}, -a\tau^{N+1}) \equiv \iota^{(N)} - a\tau^{N+1} = \iota^{(N+1)} \bmod \tau^{N+2}.$$

Thus

$$\begin{aligned} F(\tau, \iota^{(N+1)}) &\equiv F(\tau, F(\iota^{(N)}, -a\tau^{N+1})) = F(F(\tau, \iota^{(N)}), -a\tau^{N+1}) \\ &\equiv F(\tau, \iota^{(N)}) - a\tau^{N+1} \equiv 0 \bmod \tau^{N+2}. \end{aligned}$$

This completes the induction. Let $\iota \in \tau R[[\tau]]$ be the power series such that $\iota \equiv \iota^{(N)} \bmod \tau^{N+1}$ for all N. Then $F(\tau, \iota(\tau)) = 0$, and hence $F(x, \iota(x)) = 0$ for all $x \in \tau R[[\tau]]$. □

Proposition 2.3. *Let F be a power series in two variables with coefficients in R such that $F(0, 0) = 0$. The following are equivalent.*
(1) The three conditions in (2.1) hold;
(2) The binary operation on $\tau R[[\tau]]$ defined by $f \oplus_F g = F(f, g)$ makes $\tau R[[\tau]]$ into an abelian group with identity 0;

(3) The binary operation on $\tau R[[\tau]]$ defined by $f \oplus_F g = F(f,g)$ makes $\tau R[[\tau]]$ into an abelian semigroup with identity 0.

Proof. We will show (1) ⇒ (2) ⇒ (3) ⇒ (1). Assume (1) holds. Define a binary operation on $\tau R[[\tau]]$ by $f \oplus_F g = F(f,g)$ for $f, g \in \tau R[[\tau]]$. The three conditions immediately imply $f \oplus_F 0 = f$, $f \oplus_F g = g \oplus_F f$, and $(f \oplus_F g) \oplus_F h = f \oplus_F (g \oplus_F h)$ for $f, g, h \in \tau R[[\tau]]$. Lemma 2.2 implies $f \oplus_F \iota(f) = 0$. This proves (2). It is obvious that (2) implies (3).

Now assume (3) holds. We will prove condition (*iii*) of (2.1) holds; the other conditions in (2.1) can be proved similarly. Let $G(X,Y,Z) = F(F(X,Y),Z) - F(X,F(Y,Z))$. We must show $G = 0$. By hypothesis, if a, b, c are any positive integers then

$$G(\tau^a,\tau^b,\tau^c) = (\tau^a \oplus_F \tau^b) \oplus_F \tau^c - \tau^a \oplus_F (\tau^b \oplus_F \tau^c) = 0$$

as an element of $R[[\tau]]$. We must show that every coefficient of G is zero. Write

$$G = \sum_{i,j,k \geq 0} g_{ijk} X^i Y^j Z^k.$$

Since the Nth coefficient of $G(\tau^a,\tau^b,\tau^c)$ is zero we have

$$\sum_{\{\, i,j,k \in \mathbf{Z}_{\geq 0} \mid (a,b,c)\cdot(i,j,k) = N \,\}} g_{ijk} = 0 \tag{2.3}$$

for all positive integers a, b, c, N. We need to show each $g_{ijk} = 0$. Suppose not. Among all i, j, k for which g_{ijk} is nonzero, consider those for which $N_1 = i + j + k$ is minimal. Among all i, j, k with $g_{ijk} \neq 0$ and $i + j + k = N_1$, consider those for which $N_2 = i + j$ is minimal. Finally, among all i, j, k with $g_{ijk} \neq 0$, $i + j + k = N_1$, and $i + j = N_2$ select the one for which $N_3 = i$ is minimal. Call this triple (i_0, j_0, k_0); that is, $i_0 + j_0 + k_0 = N_1$, $i_0 + j_0 = N_2$, $i_0 = N_3$. Choose integers M_1, M_2, M_3 such that

$$M_3 \geq 1, \quad M_2 > M_3 N_3, \quad M_1 > M_2 N_2 + M_3 N_3.$$

Let

$$(a,b,c) = (M_1 + M_2 + M_3, M_1 + M_2, M_1), \qquad N = M_1 N_1 + M_2 N_2 + M_3 N_3.$$

We will obtain a contradiction by showing that

$$\sum_{\{\, i,j,k \in \mathbf{Z}_{\geq 0} \mid (a,b,c)\cdot(i,j,k) = N \,\}} g_{ijk} = g_{i_0,j_0,k_0} \neq 0. \tag{2.4}$$

Suppose $g_{ijk} \neq 0$ and $(a,b,c)\cdot(i,j,k) = N$. The equality can be written

$$M_1(i + j + k) + M_2(i + j) + M_3 i = N. \tag{2.5}$$

Now $i + j + k \geq N_1$ by the minimality of N_1. Strict inequality cannot hold, since otherwise

$$M_1(i + j + k) + M_2(i + j) + M_3 i \geq M_1(N_1 + 1) > N.$$

Thus $i + j + k = N_1$. By minimality of N_2 we know $i + j \geq N_2$. Again strict inequality cannot hold, since otherwise

$$M_1(i + j + k) + M_2(i + j) + M_3 i \geq M_1 N_1 + M_2(N_2 + 1) > N.$$

Thus $i + j = N_2$. Now the equality (2.5) shows $i = N_3$. This establishes (2.4) and completes the proof. □

Proof of Proposition 1.1: The hypothesis of Proposition 1.1 is that there is an injective map T from $\tau R[[\tau]]$ into an abelian group G such that $T(0) = 0_G$, and there is a power series $F(X,Y)$ with zero constant term such that

$$T(g) + T(h) = T(F(g,h))$$

for all $g, h \in \tau R[[\tau]]$. We need to show that F gives an abelian group law on $\tau R[[\tau]]$. By the preceding proposition, it suffices to show F makes $\tau R[[\tau]]$ into an abelian semigroup with identity 0; that is, if $f, g, h \in \tau R[[\tau]]$ then

$$f \oplus_F (g \oplus_F h) = (f \oplus_F g) \oplus_F h, \qquad f \oplus_F g = g \oplus_F h, \qquad f \oplus_F 0 = f.$$

Now $T(f \oplus_F (g \oplus_F h)) = T(f) + T(g \oplus_F h) = T(f) + T(g) + T(h)$ and similarly $T((f \oplus_F g) \oplus_F h) = T(f) + T(g) + T(h)$. This proves the first identity, since T is one-to-one. The other two identities are proved similarly. □

§I.3. Homomorphisms of formal group laws

If F is a formal group law then write $\mathcal{C}(F)$ for the group it determines. That is, $\mathcal{C}(F) = \tau R[[\tau]]$ as a set, and the group law is given by $g \oplus_F h = F(g,h)$. If F, F' are two formal group laws then a **homomorphism** from F to F' is defined as a power series $U(\tau) \in \tau R[[\tau]]$ with zero constant term such that $g \mapsto U(g)$ defines a *homomorphism* from $\mathcal{C}(F)$ into $\mathcal{C}(F')$. Explicitly,

$$U \circ (x \oplus_F y) = (U \circ x) \oplus_{F'} (U \circ y)$$

for all $x, y \in \tau R[[\tau]]$. In terms of power series this can be written

$$U(F(X,Y)) = F'(U(X), U(Y)). \tag{3.1}$$

The reason that U has zero constant term is that U must take $\tau R[[\tau]]$ into itself. An example of a homomorphism from F to itself is the multiplication by n map, denoted $[n]$ or $[n]_F$, which is defined by the rules:

$$[0] = 0, \quad [1] = \tau, \quad [n+1]\tau = [n]\tau \oplus_F \tau = F([n]\tau, \tau) \text{ if } n > 0, \quad [n] = \iota \circ [-n] \text{ if } n < 0. \tag{3.2}$$

Let G_1, G_2 be abelian groups, and let $T_i : \tau R[[\tau]] \to G_i$ $(i = 1, 2)$ be one-to-one maps such that $T_i(0)$ is the identity element of G_i. Let F_i be power series with zero constant term such that

$$T_i(g) \oplus_{G_i} T_i(h) = T_i(g \oplus_{F_i} h), \qquad i = 1, 2,$$

where $\oplus_{G_i}$ denotes addition on the group G_i and $g \oplus_{F_i} h = F_i(g,h)$. We showed that F_i is a formal group law, and the above equation simply states that T_i is a group homomorphism from $\mathcal{C}(F_i)$ into G_i.

Lemma 3.1. *Let G_i, T_i, F_i, $\mathcal{C}(F_i)$ be as above. Suppose there is a group homomorphism $\psi : G_1 \to G_2$ and a power series U with zero constant term such that*

$$\psi(T_1(g)) = T_2(U(g)) \tag{3.3}$$

for all $g \in \tau R[[\tau]]$. Then U is a homomorphism between the formal group laws defined by F_1 and F_2.

Proof. It suffices to show that U is a homomorphism from $\mathcal{C}(F_1)$ to $\mathcal{C}(F_2)$. By hypothesis there is a commutative diagram

$$\begin{tikzcd}
\mathcal{C}(F_1) \arrow[r, hook, "T_1"] \arrow[d, "U"'] & G_1 \arrow[d, "\psi"] \\
\mathcal{C}(F_2) \arrow[r, hook, "T_2"] & G_2
\end{tikzcd}$$

Here T_1, T_2, ψ are homomorphisms and T_1, T_2 are injective. It follows by diagram chasing that U is a homomorphism, as claimed. □

As a special case, let $G_1 = G_2 = G$, $T_1 = T_2 = T$, $F_1 = F_2 = F$, and $\psi(g) = ng$, where $n \in \mathbf{Z}$. Then $U = [n]$, which was defined by (3.2). The power series for $[n]$ may either be computed from the recursion (3.2) or from the formula (3.3), which in this context reads

$$nT(g) = T([n](g)) \qquad \text{for } g \in \tau R[[\tau]]. \tag{3.4}$$

For the additive formal group law we have T = inclusion of $\tau R[[\tau]]$ into $R[[\tau]]$ and the formula reads $ng = [n](g)$. So in that case,

$$[n](\tau) = n\tau \qquad \text{(Additive Formal Group)}$$

For the multiplicative formal group law we have $G = R[[\tau]]^\times$ and $T(g) = 1 + g$, so the formula reads $(1+g)^n = 1 + [n](g)$. Thus for the multiplicative formal group law the coefficients of $[n]$ are given by the binomial coefficients:

$$[n](g) = \sum_{i=1}^{n} \binom{n}{i} \tau^i \qquad \text{(Multiplicative Formal Group).}$$

In the special case where $n = p =$ the characteristic of R with $p > 0$ we have $(1+g)^p = 1 + g^p$, and therefore

$$[p](\tau) = \tau^p \qquad \text{(Multiplicative Formal Group).}$$

§I.4. Heights

If R has characteristic p then the **height of a homomorphism** U, written $\mathrm{ht}(U)$, is the largest integer h such that $U(\tau) = V(\tau^{p^h})$ for some power series V, or ∞ if $U = 0$. The **height of the formal group law** is defined as the height of the homomorphism $[p]$. For the additive formal group law of Example 2.2 defined by $F(X,Y) = X + Y$ we have $[p](\tau) = p\tau = 0$, so the height of F is ∞. For the multiplicative formal group law of Example 2.3 given by $F(X,Y) = X + Y + XY$ we have $[p](\tau) = \tau^p$, therefore the multiplicative formal group law has height one.

Example 4.1. Let $F = \sum f_{ij} X^i Y^j$ be a formal group law over an integral domain R of characteristic $p > 0$. Let $F^{(p)} = \sum f_{ij}^p X^i Y^j$. We claim that $F^{(p)}$ is a formal group law, and $\phi = X^p$ is a homomorphism (evidently of height 1) from F to $F^{(p)}$. For the first assertion, replace X, Y, Z by $X^{1/p}$, $Y^{1/p}$, $Z^{1/p}$ in the relation (2.1) then take the pth power. This yields the corresponding relations for $F^{(p)}$. For the second assertion, note that

$$F^{(p)}\big(\phi(X), \phi(Y)\big) = F(X,Y)^p = \phi\big(F(X,Y)\big).$$

Observe that $\phi^k : F \to F^{(p^k)}$.

Proposition 4.2. *Let F_1, F_2 be formal group laws over an integral domain R of characteristic p. Let $U(\tau) = \sum u_i \tau^i$ be a homomorphism from F_1 to F_2 of height k. Then the first nonzero coefficient of U is u_{p^k}. Moreover, there is a homomorphism $V : F_1^{(p^k)} \to F_2$ such that $U = V \circ \phi^k$.*

Proof. If $k = 0$ then $u_j \neq 0$ for some j which is prime to p, therefore $U'(\tau) = \sum_m m u_m \tau^{m-1}$ is nonzero. Differentiate the equation $U(F_1(X,Y)) = F_2(U(X), U(Y))$ with respect to Y and then set $Y = 0$. We obtain

$$U'\big(F_1(X,0)\big) \frac{\partial F_1}{\partial Y}(X,0) = \frac{\partial F_2}{\partial Y}\big(U(X), U(0)\big)\, U'(0).$$

Since $F_i(X,Y) = X + Y + XYG_i(X,Y)$ for $i = 1, 2$, this becomes

$$U'(X)\big(1 + XG_1(X,0)\big) = \big(1 + G_2(U(X),0)\big)\, u_1.$$

The left side is nonzero, therefore $u_1 \neq 0$.

Now let $k \geq 1$ and set $q = p^k$. By definition of height, there is a power series $V(\tau) \in \tau R[[\tau]]$ such that $U(\tau) = V(\tau^q)$. Now V' is nonzero, since otherwise V would be a function of τ^p, so that q could be replaced by pq. We claim V is a homomorphism from $F_1^{(q)}$ to F_2. We have to show $V\big(F_1^{(q)}(X,Y)\big) = F_2\big(V(X), V(Y)\big)$. The left side is $V(F_1(X^{1/q}, Y^{1/q})^q) = U\big(F_1(X^{1/q}, Y^{1/q})\big)$. The right side is $F_2\big(U(X^{1/q}), U(Y^{1/q})\big)$. These two are equal because U is a homomorphism from F_1 to F_2. Since $V' \neq 0$, V has height zero. It follows from the case $k = 0$ that the first coefficient of V is nonzero. Thus the coefficient of τ^q in U is nonzero. □

Example 4.3 Suppose $F = \sum f_{ij} X^i Y^j$ is a formal group law over an integral domain R of characteristic two. Then

$$[2]_F = [1]_F \oplus_F [1]_F = F(\tau, \tau) = \sum_{n=1}^{\infty} \tau^n \sum_{i+j=n} f_{ij}.$$

Since F is symmetric, $f_{ij} + f_{ji} = 0$. Thus the terms in $\sum f_{ij}$ with $i < j$ cancel the terms with $i > j$. The only surviving terms are f_{ii}, where $2i = n$. Thus

$$[2] = \sum_{n=1}^{\infty} f_{nn}\tau^{2n}.$$

Proposition 4.2 asserts that the smallest n for which $f_{nn} \neq 0$ is a power of two, say 2^k, and the height of F is $k + 1$.

Corollary 4.4. *If F, F', F'' are formal group laws over an integral domain R, $U : F \to F'$, and $V : F' \to F''$, then*

$$\mathrm{ht}(V \circ U) = \mathrm{ht}(V) + \mathrm{ht}(U).$$

PROOF. Define the degree of a nonzero power series $\sum a_i\tau^i$ to be the smallest i such that $a_i \neq 0$. Proposition 4.2 asserts that if U is a nonzero homomorphism of formal group laws then $\deg(U) = p^{\mathrm{ht}(U)}$. The degrees of power series multiply when they are composed, therefore $p^{\mathrm{ht}(V\circ U)} = p^{\mathrm{ht}(V)}p^{\mathrm{ht}(U)} = p^{\mathrm{ht}(V)+\mathrm{ht}(U)}$. □

If F, F' are formal group laws over an integral domain R and $U_1, U_2 : F \to F'$, define $U_1 \oplus_{F'} U_2 = F'(U_1, U_2)$. $U_1 \oplus_{F'} U_2$ is a homomorphism from F to F'.

Corollary 4.5. $\mathrm{ht}(U_1 \oplus_{F'} U_2) \geq \inf\{\,\mathrm{ht}(U_1), \mathrm{ht}(U_2)\,\}$. *If* $\mathrm{ht}(U_1) < \mathrm{ht}(U_2)$ *then* $ht(U_1 \oplus_{F'} U_2) = \mathrm{ht}(U_1)$.

PROOF. Write $F'(X, Y) = X+Y+XYG'(X, Y)$. Then $U_1 \oplus_{F'} U_2 = F'(U_1, U_2) = U_1+U_2+U_1U_2G'(U_1, U_2)$. The corollary is therefore true when the word "degree" is substituted for the word "height". Since $\mathrm{ht}(U_i) = \log_p(\deg(U_i))$, the corollary follows. □

Corollary 4.6. *If F, F' are formal group laws defined over an integral domain R and if there is a nonzero homomorphism U from F to F' then F and F' have the same height.*

PROOF. Certainly $[p]_{F'} \circ U = U \circ [p]_F$, so $[p]_F$ and $[p]_{F'}$ have the same height by Corollary 4.4. □

It is a theorem of M. Lazard ([F], [H]) that if R is a separably closed field of characteristic p then two formal group laws F, F' defined over R are isomorphic iff they have the same height; this gives a partial converse to Corollary 4.6. We will see that the height of the formal group law associated to an elliptic curve E defined over a field R of characteristic p is one or two according as E is ordinary or supersingular. Thus Lazard's Theorem implies that the formal group laws of any two ordinary elliptic curves (or any two supersingular elliptic curves) are isomorphic over the algebraic closure of R. On the other hand, the condition that two elliptic curves over R be isomorphic is much more restrictive (the two curves must have the same j-invariant; see [S, p. 47-50]) This means that isomorphisms of formal group laws are far more abundant than isomorphisms of elliptic curves.

Corollary 4.7. *Every formal group F over a ring of characteristic p has height at least one.*

PROOF. We claim that for any $n \in \mathbf{Z}$,

$$[n]_F = n\tau + \tau^2(\cdots). \tag{4.1}$$

This is true if $n = 0$ or 1 since $[0]_F = 0$ and $[1]_F = \tau$. Let $n > 1$, and assume the claim is true for $n - 1$. Then it is true for n also, since

$$[n]_F = F([n-1]_F, \tau) = [n-1]_F + \tau + \tau^2(\cdots).$$

The claim is true for negative integers because $[-n]_F = \iota \circ [n]_F$ where $\iota = [-1]_F$, and the first term of ι is $-\tau$ by the proof of Lemma 2.2. This proves the claim. Now $[p]_F = p\tau + \cdots$, and $p\tau = 0$. Thus $[p]_F$ cannot have height zero by Proposition 4.2. □

Corollary 4.8. *Suppose R is an integral domain of characteristic $p > 0$ and F is a formal group law over R. If $n = ap^t$ with $(a,p) = 1$ then $\mathrm{ht}([n]_F) = t\ \mathrm{ht}(F)$.*

Proof. $\mathrm{ht}([n]_F) = \mathrm{ht}([a]_F) + t\ \mathrm{ht}([p]_F)$ by Corollary 4.4. The height of $[a]_F$ is zero by (4.1), and $\mathrm{ht}([p]_F) = \mathrm{ht}(F)$ by definition. □

Proposition 4.9. *Let F, F' be formal group laws of finite height h over a finite field K of characteristic p and let v, v' be the first nonzero coefficient of the power series $[p]_F, [p]_{F'}$, respectively. Let L be the compositum of K and $\mathbf{F}_q$, where $q = p^h$. If there is a nonzero homomorphism U from F into F' then $\mathrm{N}_{L/\mathbf{F}_q}(v) = \mathrm{N}_{L/\mathbf{F}_q}(v')$.*

Proof. Let K have cardinality p^n. Write $n = n'd$, $h = h'd$, where $(n', h') = 1$. Then L has cardinality $p^{n'h'd} = q^{n'}$. By Proposition 4.2, $[p]_F = V \circ \phi^h$, $[p]_{F'} = V' \circ \phi^h$. Here V is a homomorphism of height zero from $F^{(q)}$ into F, and similarly for V'. The first term of V is $v\tau$. Now $\phi^k \circ V = V^{(p^k)} \circ \phi^k$, where $V^{(p^k)}$ is the homomorphism from $F^{(p^{k+h})}$ into $F^{(p^k)}$ obtained by raising the coefficients of V to the p^kth power. Thus

$$[p^{n'}]_F = (V \circ \phi^h)^{n'} = V \circ V^{(q)} \circ V^{(q^2)} \circ \cdots \circ V^{(q^{n'-1})} \circ \phi^{hn'}. \tag{4.2}$$

Denote $V \circ V^{(q)} \circ \cdots \circ V^{(q^{n'-1})}$ by $\mathrm{N}(V)$. The first term of $\mathrm{N}(V)$ is

$$\Big(\prod_{i=0}^{n'-1} v^{q^i}\Big)\tau = \mathrm{N}_{L/\mathbf{F}_q}(v)\tau.$$

Since U, V, V' have coefficients in K and $a^{p^n} = a$ for $a \in K$, $\phi^{hn'} = \phi^{nh'}$ commutes with U, V, and V'. Thus the equality $[p^{n'}]_{F'} \circ U = U \circ [p^{n'}]_F$ implies $\mathrm{N}(V') \circ U = U \circ \mathrm{N}(V)$. If U has height j then the coefficient of τ^{p^j} in the above equality is $\mathrm{N}_{L/\mathbf{F}_q}(v')u_{p^j} = u_{p^j}\mathrm{N}_{L/\mathbf{F}_q}(v)$, and $u_{p^j} \neq 0$ by Proposition 4.2. Thus $\mathrm{N}_{L/\mathbf{F}_q}(v) = \mathrm{N}_{L/\mathbf{F}_q}(v')$. □

PART II. ELLIPTIC CURVES AND THEIR ASSOCIATED FORMAL GROUPS

§II.1. Background on elliptic curves

If K is a field then the 2-dimensional projective space $\mathbb{P}^2(K)$ is the set of triples $(X, Y, Z) \in K \times K \times K$ such that X, Y, Z are not all zero, modulo the equivalence $(X, Y, Z) \cong (\lambda X, \lambda Y, \lambda Z)$ for all $0 \neq \lambda \in K$. Three points (X_i, Y_i, Z_i) $(i = 1, 2, 3)$ in $\mathbb{P}^2(K)$ are said to be **colinear** if there exist $\lambda, \mu, \nu \in K$, not all zero, such that $\lambda X_i + \mu Y_i + \nu Z_i = 0$ for $i = 1, 2, 3$. In particular, if $Z_i \neq 0$ for all i then the colinearity of the three points (X_i, Y_i, Z_i) in $\mathbb{P}^2(K)$ is equivalent to the colinearity of the points (x_i, y_i) in the affine plane, where $x_i = X_i/Z_i$ and $y_i = Y_i/Z_i$. This follows from the equation $\lambda x_i + \mu y_i + \nu = 0$ for all i.

A **Weierstrass equation** is a cubic equation $W(X, Y, Z) = 0$, where

$$W(X, Y, Z) = Y^2 Z + a_1 XYZ + a_3 YZ^2 - (X^3 + a_2 X^2 Z + a_4 XZ^2 + a_6 Z^3), \tag{1.1}$$

$a_i \in K$. Since this equation is homogeneous, we can think of its solutions as lying in $\mathbb{P}^2(K)$. A **singular point** is a point $P \in \mathbb{P}^2(\overline{K})$ such that $W(P) = \partial W/\partial X(P) = \partial W/\partial Y(P) = \partial W/\partial Z(P) = 0$, where $\overline{K}$ denotes the algebraic closure of K. It can be shown that the Weierstrass equation has no singular points iff $\Delta \neq 0$, where Δ is a certain polynomial in the a_i; see [S, p. 46]. Let us assume $\Delta \neq 0$. Then the set of solutions to (1.1) in $\mathbb{P}^2(\overline{K})$ is called an **elliptic curve**. The elements of the elliptic curve are called **points**. If L is any field containing all the Weierstrass coefficients a_i then $E(L)$ is defined to be the set of solutions to (1.1) in $\mathbb{P}^2(L)$. The Weierstrass equation can often be simplified. For example, in characteristic zero a linear change of coordinates puts the Weierstrass equation into the form $Y^2 Z = X^3 + a_4 XZ^2 + a_6 Z^3$. See [S, Appendix A].

The only point on the elliptic curve which intersects the line $Z = 0$ is the point $(0, 1, 0)$. This is called the **point at infinity** and is often denoted by O_E. In contrast, the "finite" points of $E(K)$ are the points $(X, Y, 1)$ which satisfy the above equation, and it is customary to identify these points with the points (X, Y) in the affine plane $K \times K$ such that

$$Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6. \tag{1.2}$$

$E(K)$ can be made into an abelian group with additive identity equal to O_E by insisting that any three colinear points on $E(K)$ (counting multiplicities) sum to O_E. The proof that this group law is associative can be found in [K] using Bézout's Theorem or in [S] using the Picard group. In this context, the phrase "counting multiplicities" means to count the multiplicities of the roots of the cubic which results when one variable is eliminated from the Weierstrass equation by using the equation of the intersecting line. We give several examples which should make this clear.

Example 1.1: Lines through the origin. The equation of a line through $(0, 1, 0)$ has the form $\lambda X + \nu Z = 0$, where $\lambda, \nu \in K$ are not both zero. If $\lambda = 0$ then the line is $Z = 0$, and the Weierstrass equation becomes simply $0 = W(X, Y, 0) = X^3$. This has one solution $X = 0$ with multiplicity three. Thus $(0, 1, 0)$ intersects $Z = 0$ with multiplicity three. This gives $3(0, 1, 0) = (0, 1, 0)$, which is consistent with the fact that $(0, 1, 0)$ is the identity. If $\lambda \neq 0$ then $X = cZ$, where $c = -\nu/\lambda$. The Weierstrass equation becomes

$$W(cZ, Y, Z) = Y^2 Z + (a_1 c + a_3) YZ^2 - (c^3 + a_2 c^2 + a_4 c + a_6) Z^3 = 0.$$

This factors as

$$Z(Y^2 + (a_1 c + a_3) YZ - (c^3 + a_2 c^2 + a_4 c + a_6) Z^2) = Z(Y - y_1 Z)(Y - y_2 Z)$$

where y_1, y_2 belong to a quadratic extension of K and satisfy $y_1 + y_2 = -(a_1 c + a_3)$, $y_1 y_2 = -(c^3 + a_2 c^2 + a_4 c + a_6)$. The intersection of E with the line is $\{(0, 1, 0), (c, y_1, 1), (c, y_2, 1)\}$, hence $(0, 1, 0) + (c, y_1, 1) + (c, y_2, 1) = (0, 1, 0)$. In other words, if $(c, y_1, 1)$ lies on E then $-(c, y_1, 1) = (c, y_2, 1)$, where $y_1 + y_2 = -(a_1 c + a_3)$. This gives the inversion formula:

$$-(x, y, 1) = (x, -(y + a_1 x + a_3), 1). \tag{1.3}$$

If it happens that $y = -(y + a_1x + a_3)$, that is, $2y = -(a_1x + a_3)$, then $(x, y, 1)$ is a two-torsion point.

Example 1.2: Lines which miss the origin. The equation of a line which misses $(0, 1, 0)$ is $\lambda X + \mu Y + \nu Z = 0$, where $\mu \neq 0$. Since $(0, 1, 0)$ is the only point on E which intersects $Z = 0$, the intersection points of the line with the elliptic curve all have a nonzero Z-coordinate. Let $m = -\lambda/\mu$, $b = -\nu/\mu$, $y = Y/Z$, $x = X/Z$. Then the three intersection points $(x_i, y_i, 1)$, $i = 1, 2, 3$, satisfy the Weierstrass equation and $y_i = mx_i + b$. Another way to view this is: suppose $(x_1, y_1, 1)$ and $(x_2, y_2, 1)$ are two points on the elliptic curve such that $x_1 \neq x_2$, and define $m = (y_1 - y_2)/(x_1 - x_2)$, $b = y_1 - mx_1$. Substitute $y = mx + b$ into the affine form of the Weierstrass equation to get a cubic equation in x of the form $x^3 + Bx^2 + Cx + D = 0$, where the coefficients explicitly depend on the a_i and on m and b. Explicitly, $B = -m^2 - a_1m + a_2$. Two roots of this cubic equation are x_1 and x_2. Let x_3 denote the third root. Then

$$x^3 + Bx^2 + Cx + D = (x - x_1)(x - x_2)(x - x_3) = x^3 - (x_1 + x_2 + x_3)x^2 + (\cdots)x + (\cdots),$$

so that $x_3 = -x_1 - x_2 - B$. This yields the addition formula

$$(x_1, y_1, 1) + (x_2, y_2, 1) = (x_3, -(y_3 + a_1x_3 + a_3), 1) \qquad \text{if } x_1 \neq x_2,$$

$$x_3 = -x_1 - x_2 + m^2 + a_1m - a_2, \qquad m = (y_1 - y_2)/(x_1 - x_2),$$

$$y_3 = mx_3 + y_1 - mx_1.$$

Example 1.3: Duplication formula. How do we compute $P + P$? Assume $P = (x_1, y_1, 1)$ is not a two-torsion point, that is, $2y_1 \neq -(a_1x + a_3)$. Then $-(P + P)$ is the point $(x_2, y_2, 1)$ on the curve such that $2(x_1, y_1, 1) + (x_2, y_2, 1) = (0, 1, 0)$. Let $\lambda X + \mu Y + \nu Z$ be the line which passes through these points with correct multiplicity. It misses the origin, so $\mu \neq 0$. Thus the line has the form $y - y_1 = m(x - x_1)$, where $y = Y/Z$, $x = X/Z$. First we will find m, then we will find x_2, y_2. When y is replaced by $m(x - x_1) + y_1$ in the Weierstrass equation, we get a cubic $x^3 + Bx^2 + Cx + D$, and it should equal $(x - x_1)^2(x - x_2)$. Here $B = a_2 - m^2 - a_1m$, $C = m^2(2x_1) + m(-2y_1 + a_1x_1 - a_3) + (a_4 - a_1y_1)$. If we differentiate the cubic and set $x = x_1$ we are supposed to get zero. Hence $3x_1^2 + 2Bx_1 + C = 0$. We can solve for m in this relation; in fact m will just be the slope of the tangent line to the curve E at P, namely $m = (dy/dx)(P)$. It turns out

$$m = (3x_1^2 + 2a_2x_1 + a_4 - a_1y_1)/(a_1x_1 + 2y_1 + a_3).$$

Since $(x - x_1)^2(x - x_2) = x^3 + Bx^2 + Cx + D$,

$$x_2 = -2x_1 - B = -2x_1 - a_2 + m^2 + a_1m, \qquad y_2 = m(x_2 - x_1) + y_1.$$

Finally,

$$2(x_1, y_1, 1) = -(x_2, y_2, 1) = (x_2, -(y_2 + a_1x_2 + a_3), 1).$$

§II.2. The affine plane $Y \neq 0$

It turns out that the image of the map $T : \tau R[[\tau]] \to E(L)$ which was alluded to in Example I.1.4 will be contained in the set of points (X, Y, Z) for which $Y \neq 0$. For this reason we will need some addition formulas for points in this region. In principle, such addition formulas could be deduced from formulas in the preceding section by using a change of variables, however this method is cumbersome to the point that it will crash Mathematica on a workstation. The better method is to introduce new affine coordinates $(X, Y, Z) = (t, -1, s)$ and calculate addition by intersecting the curve with various lines.

There are three points (X, Y, Z) on E (counting multiplicities) such that $Y = 0$. Suppose $\lambda X + \mu Y + \nu Z$ is a line which misses these three points. Then λ and ν are not both zero. If $\nu \neq 0$ then the line misses the three points iff $(-\lambda/\nu, 0, 1) \notin E$; that is, iff $-\lambda/\nu$ is not a root of the equation $X^3 + a_2X^2 + a_4X + a_6 = 0$. If $\lambda \neq 0$ then the line misses the three points iff $(1, 0, -\nu/\lambda) \notin E$ iff $-\nu/\lambda$ is not a root of the equation $1 + a_2Z + a_4Z^2 + a_6Z^3 = 0$.

If $Y \neq 0$ then $(X, Y, Z) = (t, -1, s)$, where $s = -Z/Y$, $t = -X/Y$. The point $(t, -1, s)$ lies on the line $\lambda X + \mu Y + \nu Z = 0$ iff $\lambda t + \nu s = \mu$. The Weierstrass equation can be written as

$$s = t^3 + a_1 ts + a_2 t^2 s + a_3 s^2 + a_4 ts^2 + a_6 s^3. \tag{2.1}$$

The next proposition summarizes addition formulas of the form $(t_1, -1, s_1) + (t_2, -1, s_2) + (t_3, -1, s_3) = (0, 1, 0)$.

Proposition 2.1. *Let $P_i = (t_i, -1, s_i)$ for $i = 1, 2$.*
(a) Suppose $t_1 \neq 0$ and let $m = s_1/t_1$. If $1 + a_2 m + a_4 m^2 + a_6 m^3 \neq 0$ then

$$-P_1 = \left(\frac{-t_1}{1 - a_1 t_1 - a_3 s_1}, -1, \frac{-s_1}{1 - a_1 t_1 - a_3 s_1} \right). \tag{2.2}$$

(b) Suppose $t_1 \neq t_2$ and let $m = (s_1 - s_2)/(t_1 - t_2)$, $b = s_1 - mt_1$, $A = 1 + a_2 m + a_4 m^2 + a_6 m^3$. If $A \neq 0$ then

$$\begin{aligned} P_1 + P_2 &= -(t_3, -1, mt_3 + b), \\ t_3 &= -t_1 - t_2 - \frac{a_1 m + a_2 b + a_3 m^2 + 2a_4 mb + 3a_6 m^2 b}{A}. \end{aligned} \tag{2.3}$$

(c) Suppose $1 - a_1 t_1 - 2a_3 s_1 - a_2 t_1^2 - 2a_4 t_1 s_1 - 3a_6 s_1^2 \neq 0$. Let

$$m = \frac{a_1 s_1 + 3t_1^2 + 2a_2 s_1 t_1 + a_4 s_1^2}{1 - a_1 t_1 - 2a_3 s_1 - a_2 t_1^2 - 2a_4 t_1 s_1 - 3a_6 s_1^2}.$$

Suppose $1 + a_2 m + a_4 m^2 + a_6 m^3 \neq 0$. Then

$$\begin{aligned} [2]P_1 = P_1 + P_1 &= -(t_3, -1, mt_3 - mt_1 + s_1), \\ t_3 = -2t_1 &- \frac{a_1 m + a_3 m^2 + (a_2 + 2a_4 m + 3a_6 m^2)(s_1 - mt_1)}{1 + a_2 m + a_4 m^2 + a_6 m^3}. \end{aligned}$$

Proof. (b) P_1, P_2 lie on the line $mX - bY - Z = 0$. Let P_3 be the third point of intersection of this line with the elliptic curve. Write $P_3 = (x_3, y_3, z_3)$. If $y_3 = 0$ then $P_3 = (1, 0, m)$. From the Weierstrass equation (1.1), $1 + a_2 m + a_4 m^2 + a_6 m^3 = 0$, contrary to the hypothesis. Thus $y_3 \neq 0$, and hence P_3 can be written $P_3 = (t_3, -1, mt_3 + b)$. Likewise $P_i = (t_i, -1, mt_i + b)$ for $i = 1, 2$. When $(t, -1, mt + b)$ is substituted for (X, Y, Z) in the Weierstrass equation, the result must be of the form $A(t - t_1)(t - t_2)(t - t_3)$ with $A \neq 0$. Hence

$$\begin{aligned} -(mt + b) + a_1 t(mt + b) + a_3(mt + b)^2 + t^3 + a_2 t^2(mt + b) + a_4 t(mt + b)^2 + a_6(mt + b)^3 \\ = A(t - t_1)(t - t_2)(t - t_3). \end{aligned}$$

The left side is of the form

$$(1 + a_2 m + a_4 m^2 + a_6 m^3)t^3 + (a_1 m + a_3 m^2 + a_2 b + 2a_4 mb + 3a_6 m^2 b)t^2 + (\cdots)t + (\cdots)$$

and the right side is of the form $At^3 - A(t_1 + t_2 + t_3)t^2 + \cdots$. Now (b) follows immediately.

(a) Let $P_2 = (0, 1, 0)$, $m = s_1/t_1$, $A = 1 + a_2 m + a_4 m^2 + a_6 m^3$. Since $A \neq 0$, (b) implies that $P_1 + (0, 1, 0) + (t_3, -1, mt_3) = (0, 1, 0)$, where $t_3 = -t_1 - (a_1 m + a_3 m^2)/A$. Thus $-P_1 = (t_3, -1, mt_3)$. Now

$$t_1^3 A = t_1^3 + a_2 t_1^2 s_1 + a_4 t_1 s_1^2 + a_6 s_1^3 = s_1 - a_1 t_1 s_1 - a_3 s_1^2,$$

thus

$$\begin{aligned} t_3 = -t_1 - \frac{a_1 m + a_3 m^2}{A} &= \frac{-t_1(t_1^3 A) - (a_1 t_1^2 s_1 + a_3 t_1 s_1^2)}{t_1^3 A} \\ = \frac{-t_1 s_1}{s_1 - a_1 t_1 s_1 - a_3 s_1^2} &= \frac{-t_1}{1 - a_1 t_1 - a_3 s_1}. \end{aligned}$$

(c) From equation (2.1) one computes that $(ds/dt)(P_1) = m$. Thus $s = mt + (s_1 - mt_1)$ is the line which is tangent to the elliptic curve at P_1. In (X, Y, Z)-coordinates this line has the equation $mX + (mt_1 - s_1)Y - Z$. Let $P_3 = (x_3, y_3, z_3)$ be the other point on the curve which intersects this line. The only point on the line with $y = 0$ is $(1, 0, m)$. Since we assume $1 + a_2m + a_4m^2 + a_6m^3 \neq 0$, $(1, 0, m)$ does not lie on the curve. Thus $y_3 \neq 0$, so $P_3 = (t_3, -1, s_3)$. Substitute $(t, -1, mt + b)$ with $b = s_1 - mt_1$ into the Weierstrass equation to get

$$\begin{aligned}(1 + a_2m + a_4m^2 + a_6m^3)t^3 + (a_1m + a_3m^2 + a_2b + 2a_4mb + 3a_6m^2b)t^2 + (\cdots)t + (\cdots)\\ = (\text{constant})(t - t_1)^2(t - t_3).\end{aligned}$$

Now solve for t_3 to get the result. □

§II.3. Function fields, local rings, and uniformizers

Let K be any field, and let $C = C(X, Y, Z)$ be a curve in $\mathbb{P}^2(\overline{K})$. This means that C is an irreducible homogeneous polynomial with coordinates in $\overline{K}$. Assume the coefficients of C belong to K, and let $C(K) = \{\, P \in \mathbb{P}^2(K) \mid C(P) = 0 \,\}$. A point in $C(\overline{K})$ is called **nonsingular** if $\nabla_P C \neq 0$, where

$$\nabla_P C = \left(\frac{\partial}{\partial X}C(P), \frac{\partial}{\partial Y}C(P), \frac{\partial}{\partial Z}C(P)\right).$$

The **function field** $K(C)$ of C over K is the set of all quotients $p(X, Y, Z)/q(X, Y, Z)$, where p and q are homogeneous polynomials of the same degree with coefficients in K such that C does not divide q, modulo the equivalence: $p/q \cong p'/q'$ iff $pq' - qp'$ is divisible by C. The addition and multiplication in $K(C)$ are defined in the same way as for rational functions. Equivalently, if we set $x = X/Z$ and $y = Y/Z$ then $K(C)$ is the quotient field of the integral domain

$$K[x, y]/(C(x, y, 1)).$$

This field has transcendence degree 1, thus any two elements of the function field satisfy some algebraic relation. Notice that $p(\lambda X, \lambda Y, \lambda Z)/q(\lambda X, \lambda Y, \lambda Z) = p(X, Y, Z)/q(X, Y, Z)$ because of the homogeneity, so $p(P)/q(P)$ makes sense for $P \in C(\overline{K})$ provided $q(P) \neq 0$. A function $f \in K(C)$ is said to be **defined** at a point $P \in C(\overline{K})$ if there exists p/q in the equivalence class of f such that $q(P) \neq 0$. If f is defined at P then the **value** of f at P, denoted $f(P)$, is defined as $p(P)/q(P)$ for any (hence every) p/q which is in the equivalence class of f and for which $q(P) \neq 0$. If $P \in C(K)$ and $f \in K(C)$ is defined at P then $f(P) \in K$.

As an example, let us show that for the Weierstrass equation, Z/X is defined at $(0, 1, 0)$. Since $Z(Y^2 + a_3YZ - a_6Z^2) = X(-a_1YZ + X^2 + a_2XZ + a_4Z^2)$,

$$Z/X = \frac{-a_1YZ + X^2 + a_2XZ + a_4Z^2}{Y^2 + a_3YZ - a_6Z^2}.$$

Now $Y^2 + a_3YZ - a_6Z^2$ does not vanish at $(0, 1, 0)$, so Z/X is indeed defined at $(0, 1, 0)$.

For the remainder of this section assume $P \in C(K)$. Let Ω_P be the ring of functions in $K(C)$ which are defined at P, and let M_P be the ideal of Ω_P consisting of functions which take the value zero at P. Ω_P is called the **local ring of C at P**. If we identify the set of constant functions with K then

$$\Omega_P = K \oplus M_P \tag{3.1}$$

(internal direct sum) because $f = f(P) + (f - f(P))$.

Lemma 3.1. *$\Omega_P - M_P = \Omega_P^\times$. M_P is the unique maximal ideal of Ω_P.*

Proof. If $f \in \Omega_P - M_P$ then f can be written as $F(X, Y, Z)/G(X, Y, Z)$, where F, G are homogeneous polynomials of the same degree and F, G do not vanish at P. Since $1/f$ can be written G/F, $1/f \in \Omega_P$.

This shows that $\Omega_P - M_P \subset \Omega_P^\times$. The reverse inclusion is also true, for if $f \in \Omega_P^\times$ then there is $g \in \Omega_P$ with $fg = 1$. Then $f(P)g(P) = 1$, so $f(P)$ is a unit in K. In particular, f is not in M_P. We have proved the first statement. For the second statement, let I be any proper ideal of Ω_P. Then $I \cap \Omega_P^\times = \emptyset$; otherwise I would equal Ω_P. Thus I misses the complement of M_P completely; equivalently, $I \subset M_P$. □

Our next goal is to show that if P is a nonsingular point (that is, $\nabla_P C \neq 0$) then M_P is principal. First we need some lemmas. These lemmas are true in more generality than we state them.

Lemma 3.2 (Nakayama's Lemma). *If A is a finitely generated Ω_P-module and $M_P A = A$ then $A = \{0\}$.*

Proof. Let $u_1, \ldots, u_n$ be a set of generators for A with n as small as possible. Since $u_1 \in A = M_P A$, there exist $\mu_i \in M_P$ such that $u_1 = \sum \mu_i u_i$. Now $1 - \mu_1 \in \Omega_P^\times$, so we can solve for u_1 in terms of $u_2, \ldots, u_n$. This contradicts the minimality of n. □

Corollary 3.3. $\cap_{n=1}^\infty M_P^n = \{0\}$. *Thus* $M_P \supsetneq M_P^2$.

Proof. Let $A = \cap M_P^n$. A is finitiely generated by the Hilbert Basis Theorem [Fu, p. 13], so $A = \{0\}$ by Nakayama's Lemma. □

Lemma 3.4. *If P is a nonsingular point of C then M_P/M_P^2 is isomorphic to K.*

Proof. Observe that M_P/M_P^2 is an Ω_P/M_P-vector space, and Ω_P/M_P is canonically isomorphic to K by (3.1). We just have to prove this vector space is one-dimensional, or equivalently that its dual is one-dimensional. So let $\lambda : M_P/M_P^2 \to K$ be a K-linear map. Since $\Omega_P = K + M_P$, we can think of λ as a K-linear map from Ω_P into K which is trivial on $M_P^2 + K$.

We will construct a K-linear map $\vartheta : \Omega_P \to K$ which is trivial on $K + M_P^2$, and we will prove that λ is proportional to ϑ. Fix coordinates for P: $P = (X_0, Y_0, Z_0)$. Fix $R \in K^3$ such that $R \cdot P = 1$. Let $C(X,Y,Z) = 0$ be the equation of the curve. Let $\nabla_P C = (\partial C/\partial X(P), \partial C/\partial Y(P), \partial C/\partial Z(P))$, the gradient of C at P. We claim $\nabla_P C$ and R are linearly independent. First observe $\nabla_P C \neq 0$ since the curve is nonsingular at P by hypothesis. By Euler's identity $(X\partial/\partial X + Y\partial/\partial Y + Z\partial/\partial Z)C = \deg(C)C$. (The proof of Euler's identity is that for any monomial $X^aY^bZ^c$, we have $(X\partial/\partial X + Y\partial/\partial Y + Z\partial/\partial Z)(X^aY^bZ^c) = (a+b+c)X^aY^bZ^c$.) Evaluating Euler's identity at P gives $P \cdot \nabla_P C = dec(C)\, C(P) = 0$. Since $P \cdot R \neq 0$, this shows $\nabla_P C$ is linearly independent from R. It follows that the space of vectors which are orthogonal to R and $\nabla_P C$ is one-dimensional, spanned by a vector T.

Define $\vartheta : \Omega_P \to K$ by

$$\vartheta(f) = T \cdot \nabla_P(f).$$

We claim ϑ is well-defined, K-linear, and surjective. To prove it is well-defined, it suffices to show $T \cdot \nabla_P(F/G) = 0$ if F vanishes identically on the curve and $G(P) \neq 0$. In that case, C divides F. Let $h = F/(CG)$. Then

$$T \cdot \nabla_P(F/G) = C(P) T \cdot \nabla_P h + h(P) T \cdot \nabla_P C = 0 + 0$$

as required. The map ϑ is certainly K-linear. If S is any vector in K^3 such that $S \cdot P = 0$ but $S \cdot T \neq 0$ then

$$T \cdot \nabla_P(S \cdot (X,Y,Z)/R \cdot (X,Y,Z)) = \frac{T \cdot S}{R \cdot P} - \frac{(T \cdot R)(S \cdot P)}{(R \cdot P)^2} = \frac{T \cdot S}{R \cdot P} \neq 0, \tag{3.1}$$

so the map is nontrivial. Any nontrivial K-linear map into K is surjective. Let us show that the kernel contains $K + M_P^2$. Certainly $T \cdot \nabla_P$ annihilates the constants K. If $f, g \in M_P$ then $\nabla_P(fg) = 0$ by the product rule, so M_P^2 is in the kernel also.

It remains to show that an arbitrary linear map $\lambda : \Omega_P \to K$ which is trivial on $K + M_P^2$ coincides with a multiple of ϑ. The map λ obeys a product rule, for if $f = f(P) + f_1$, $g = g(P) + g_1$ where $f, g \in \Omega_P$ then $f_1, g_1 \in M_P$, and $fg = f(P)g + g(P)f - f(P)g(P) + f_1 g_1$, so

$$\lambda(fg) = f(P)\lambda(g) + g(P)\lambda(f).$$

It follows that λ is completely determined by its values at X/ρ, Y/ρ, and Z/ρ, where $\rho = R \cdot (X, Y, Z)$. Denote these by values by α, β, γ. We claim (α, β, γ) is proportional to T. This will imply there is a one-dimensional space of such λ; in particular λ must be proportional to ϑ. We must show (α, β, γ) is orthogonal to both R and $\nabla_P C$. Let $R = (R_1, R_2, R_3)$ and $\rho = R_1 X + R_2 Y + R_3 Z$. Then

$$\begin{aligned} R \cdot (\alpha, \beta, \gamma) &= R_1 \lambda(X/\rho) + R_2 \lambda(Y/\rho) + R_3 \lambda(Z/\rho) \\ &= \lambda((R_1 X + R_2 Y + R_3 Z)/\rho) = \lambda(1) = 0, \end{aligned}$$

$$\nabla_P C \cdot (\alpha, \beta, \gamma) = \lambda(C(X/\rho, Y/\rho, Z/\rho)) = \lambda(C(X, Y, Z)/\rho^{\deg(C)}) = 0.$$

□

Corollary 3.5. *Supose P is nonsingular. Let $u \in M_P$, and let R, T be nonzero vectors in K^3 such that $R \cdot P \neq 0$, $T \cdot R = 0$, and $T \cdot \nabla_P C = 0$. Then $u \in M_P - M_P^2$ iff $T \cdot \nabla_P u \neq 0$. Also, if $S \cdot P = 0$ but $S \cdot T \neq 0$ then $S \cdot (X, Y, Z)/R \cdot (X, Y, Z)$ belongs to $M_P - M_P^2$.*

PROOF. In the notation of the preceding proof, the hypothesis states that $\vartheta(u) \neq 0$. Since ϑ induces an isomorphism of M_P/M_P^2 with K, we know $u \notin M_P^2$ iff $\vartheta(u) \neq 0$. The last statement follows from (3.1). □

Proposition 3.6. *Suppose P is nonsingular. Then M_P is a principal ideal of Ω_P. In fact, if $u \in M_P$ then $M_P = u\Omega_P \iff u \notin M_P^2$.*

PROOF. $M_P \neq M_P^2$ by Lemma 3.2. Let $u \in M_P - M_P^2$. Then

$$K \cong \frac{\Omega_P}{M_P} \cong \frac{u\Omega_P}{uM_P} \to \frac{u\Omega_P}{M_P^2}.$$

The image of 1 in this composite map is $u \bmod M_P^2$, which is nonzero. Thus the kernel of the projection map from $u\Omega_P/uM_P$ into $u\Omega_P/M_P^2$ has to be trivial. This shows $uM_P = M_P^2$.

Also, $M_P = uK + M_P^2$ because M_P/M_P^2 is a one-dimensional K-vector space by Lemma 3.4. Thus

$$u\Omega_P = u(K + M_P) = uK + uM_P = uK + M_P^2 = M_P.$$

□

Corollary 3.7. *Suppose P is nonsingular. Let $0 \neq f \in K(C)$, $u \in M_P - M_P^2$. There is a unique integer $v(f)$ such that $f = u^{v(f)} g$ with $g \in \Omega_P^\times$. This integer does not depend on the choice of u.*

PROOF. Write $f = F/G$ with F, G homogeneous of degree m. Choose $R \in K^3$ so that $P \cdot R \neq 0$. Let ρ be the homogeneous polynomial $\rho = R \cdot (X, Y, Z)$. Then $f = f_1/f_2$, where $f_1 = F/\rho^m$ and $f_2 = G/\rho^m$. Note that $f_1, f_2 \in \Omega_P$. By Corollary 3.3,

$$\Omega_P - \{0\} = \sqcup_{n=0}^{\infty} (M_P^n - M_P^{n+1}),$$

where $M_P^0 = \Omega_P$. Clearly $M_P^n - M_P^{n+1} = u^n \Omega_P^\times$, since $M = u\Omega_P$. Define n_1, n_2 by $f_i \in M_P^{n_i} - M_P^{n_i+1}$, and let $n = n_1 - n_2$. Then $fu^{-n} = f_1 u^{-n_1}/(f_2 u^{-n_2}) \in \Omega_P^\times$. □

Ω_P is called the **local ring** at P. If P is nonsingular, then a **uniformizer** is an element of M_P such that $M_P = u\Omega_P$; equivalently it is an element of $M_P - M_P^2$. The integer $v(f)$ is called the **valuation** of f at P. If $v(f) > 0$, f has a **zero of order** $v(f)$ **at** P; if $v(f) < 0$, f has a **pole of order** $-v(f)$ **at** P. If $v(f) = 0$, we say f is **finite and nonvanishing at** P.

Example 3.8 Let $C = W$ be given by the Weierstrass equation (1.1). Let us show that X/Y is a uniformizer at $(0, 1, 0)$. In Corollary 3.5 we take $R = P = (0, 1, 0)$ and compute from (1.1) that $\nabla_P W = (0, 0, 1)$. Thus

$T = (1, 0, 0)$. Now X/Y vanishes at P, and $T \cdot \nabla_P(X/Y) = \partial/\partial X(X/Y)|_P = 1 \neq 0$. So X/Y is a uniformizer by Corollary 3.5.

Example 3.9 Let us compute $v(Z/X)$ at the point $P = (0, 1, 0)$ on an elliptic curve. By (1.1), $ZV = X^3$, with

$$V = Y^2 + a_1XY + a_3YZ - a_2X^2 - a_4XZ - a_6Z^2.$$

Then $Z/X = X^2/V = (X/Y)^2(Y^2/V)$. Since $Y^2/V \in \Omega_P^\times$ and X/Y is a uniformizer, we see that $v(Z/X) = 2$. Thus $x = X/Z$ has a pole of order 2 at the origin. Since $Y/Z = (Y/X)(X/Z)$, $y = Y/Z$ has a pole of order 3 at the origin.

§II.4. Power series expansions

Lemma 4.1. *Let $C = C(X, Y, Z)$ be a projective curve over $\overline{K}$ which is nonsingular at P. Suppose C has coefficients in K and $P \in C(K)$. Let $u \in K(C)$ be a uniformizer at P. If f is a nonzero function in $K(C)$ and $v(f) = a$ then there exist unique constants $f_j \in K$ for $j \geq a$ such that for any $N \geq a$,*

$$f - \sum_{j=a}^{N} f_j u^j \qquad \text{has a zero of order at least } N + 1.$$

Moreover, $f_a \neq 0$.

Proof. Let $g = u^{-a}f \in \Omega_P^\times$, $f_a = g(P)$. This is the only constant for which $g - f_a \in M_P$, so it is the only constant for which $v(f - u^a f_a) = v(u^a(g - f_a)) > a$. From this observation, the lemma may be easily proved by induction. □

Corollary 4.2. *A choice of uniformizer u at P determines a one to one homomorphism of rings*

$$\Psi_u : \Omega_P \hookrightarrow K[[\tau]].$$

If $0 \neq V = \sum v_i \tau^i \in K[[\tau]]$, define $\deg(V)$ to be the smallest integer n such that $v_n \neq 0$, and define $\deg(0) = \infty$. If one puts metrics on Ω_P and on $K[[\tau]]$ by the rules $|f| = c^{v_P(f)}$ for $f \in \Omega_P$, $|V| = c^{\deg(V)}$ for $V \in K[[\tau]]$, where $0 < c < 1$, then Ψ_u is an isometry. In particular, Ψ_u is continuous with respect to the topologies on Ω_P, $K[[\tau]]$ which are induced by the above metrics. The image of Ψ_u is dense in $K[[\tau]]$.

Proof. The homomorphism Ψ_u is defined by: $\Psi_u(f) = \sum f_j \tau^j$, where the f_j are as in Lemma 4.1. It is easy to see (using the uniqueness of the coefficients f_j) that Ψ_u is a ring homomorphism. Ψ_u is an isometry because $v_P(f) = a$ implies f_a is the first nonzero coefficient. If $\Psi_u(f) = 0$ then $|f| = |\Psi_u(f)| = |0| = 0$, so $f \in \cap M_P^n$. By Corollary 3.3, f must be zero; thus Ψ_u is one to one. If g is any polynomial with coefficients in K then $g(u) \in \Omega_P$ and $\Psi_u(g(u)) = g(\tau)$. This shows $\Psi_u(\Omega_P)$ is dense in $K[[\tau]]$. □

Let E be an elliptic curve determined by a nonsingular Weierstrass equation (1.1). Define functions $s, t \in K(E)$ by the formulas: $s = -Z/Y$, $t = -X/Y$, as in §2. These have zeroes at the identity of orders 3 and 1, respectively, by Examples 3.8 and 3.9. By dividing through the Weierstrass equation by Y^3 we see that s and t satisfy the equation (2.1). If O is the additive identity of E then $s(O) = t(O) = 0$. Moreover, t is a uniformizer at O since it has a simple zero there, thus we can formally express s as a power series in t in the sense that we can find an infinite power series

$$S(\tau) = \sum_{i=3}^{\infty} s_i \tau^i$$

with the property that for any $N \geq 3$, the function $s - \sum_3^N s_i t^i$ has a zero of order at least $N + 1$ at the additive identity. The series S can be computed by recursively substituting approximations for s into the right hand side of (2.1) and expanding to get improved approximations. We start with the approximation $s = O(t^3)$ to obtain

$$\begin{aligned} s &= t^3 + a_1 t\, O(t^3) + a_2 t^2 O(t^3) + a_3 (O(t^3))^2 + a_4 t (O(t^3))^2 + a_6 (O(t^3))^3 \\ &= t^3 + O(t^4). \end{aligned}$$

On the next round substitute $t^3 + O(t^4)$ for s in the right side of the equation to obtain

$$s = t^3 + a_1 t (t^3 + O(t^4)) + O(t^5) = t^3 + a_1 t^4 + O(t^5).$$

The next round yields

$$\begin{aligned} s &= t^3 + a_1 t (t^3 + a_1 t^4 + O(t^5)) + a_2 t^2 (t^3 + O(t^4)) + O(t^6) \\ &= t^3 + a_1 t^4 + (a_1^2 + a_2) t^5 + O(t^6). \end{aligned}$$

This procedure yields the general rule:

$$s_0 = s_1 = s_2 = 0, \qquad s_3 = 1, \qquad \text{and if } n \geq 4 \text{ then}$$

$$s_n = a_1 s_{n-1} + a_2 s_{n-2} + a_3 \sum_{i+j=n} s_i s_j + a_4 \sum_{i+j=n-1} s_i s_j + a_6 \sum_{i+j+k=n} s_i s_j s_k. \tag{4.1}$$

Lemma 4.3. *Let W be the Weierstrass equation (1.1), where $a_i \in R$ and R is an integral domain. Let $s_i \in R$ be defined by the recursion (4.1) and let $S = \sum s_i \tau^i \in \tau R[[\tau]]$. Then $W(\tau, -1, S) = 0$ in $R[[\tau]]$. If $f, g \in \tau R[[\tau]]$ and $W(f, -1, g) = 0$ then $g = S \circ f$.*

Remark. Since the Weierstrass equation is cubic in the variable Z, it follows that for fixed $f \in \tau R[[\tau]]$, the equation $W(f, -1, g) = 0$ has three solutions for g in the algebraic closure of the quotient field of $R[[\tau]]$. The lemma asserts that exactly one of these solutions lies in $\tau R[[\tau]]$.

Proof. Let K be the quotient ring of R and let E be the elliptic curve over K with equation W. As usual, let $t = -X/Y$, $s = -Z/Y \in K(E)$. Then t is a uniformizer at the origin, so $\Psi_t : \Omega_O \to K[[\tau]]$ can be defined. Moreover, $\psi_t(t) = \tau$, $\Psi_t(s) = S$. Now $W(t, -1, s) = 0$, so

$$0 = \Psi_t \left(W(t, -1, s) \right) = W(\tau, -1, S).$$

From this it follows that $W(f, -1, S \circ f) = 0$ for any $f \in \tau K[[\tau]]$.

Now suppose $f, g \in \tau R[[\tau]]$ and $W(f, -1, g) = 0$. Let $h = S \circ f$. Then

$$\begin{aligned} 0 &= W(f, -1, h) - W(f, -1, g) \\ &= (g - h) \left(-1 + a_1 f + a_2 f^2 + a_3 (g + h) + a_4 f (g + h) + a_6 (g^2 + gh + h^2) \right). \end{aligned}$$

Since $-1 + a_1 f + \cdots$ is a unit in $R[[\tau]]$ by Lemma I.1.4, $g - h$ must be zero. □

§II.5. Isogenies

A reference for this section is [S]. Let E, E' be two elliptic curves defined over the same field K. An **algebraic map** from E to E' is a function $\alpha : E(\overline{K}) \to E'(\overline{K})$ such that for each $P \in E$ there exist homogeneous polynomials f_1, f_2, f_3 of the same degree and not all vanishing at P such that for all but finitely many $Q \in E(\overline{K})$,

$$\alpha(Q) = (f_1(Q), f_2(Q), f_3(Q)).$$

An example of an algebraic map from E to itself is the **translation by** P **map** $\tau_P(Q) = P+Q$ for $P, Q \in E$. The algebraic map is said to be **defined** over a field K if E, E' are defined over K and if all the coefficients of f_1, f_2, f_3 can be chosen to belong to K. It is a theorem [S, p. 75] that every nonconstant algebraic map from E into E' which takes the origin to the origin is a group homomorphism. Such an algebraic map is called an **isogeny**. If $\tau : E \to E'$ and $-Q = \tau(0,1,0) \in E'$ then $\tau_Q \circ \tau$ takes the origin of E into the origin of E'. Thus every nonconstant algebraic map is the composition of an isogeny with a translation. Two curves E, E' are called **isogenous** over K if there exists an isogeny defined over K from E into E'. The **endomorphism ring** of E, written $\mathrm{End}_K(E)$, is the set of isogenies over K from E to itself, together with the constant zero map, with the addition and multiplication laws:

$$(\alpha + \beta)(P) = \alpha(P) + \beta(P), \qquad \alpha\beta = \alpha \circ \beta.$$

Note that $\mathbf{Z} \subset \mathrm{End}_K(E)$. If K is the finite field with q elements then the **Frobenius endomorphism** φ_q, is defined by $\varphi_q(X,Y,Z) = (X^q, Y^q, Z^q)$. Since φ_q coincides with the Galois action, it commutes with any endomorphism of E which is defined over K. In particular, φ_q commutes with $\mathbf{Z}$.

If $\alpha : E \to E'$ is an isogeny, define $\alpha^* K(E') = \{\, f \circ \alpha \,|\, f \in K(E')\,\}$; this is a subfield of $K(E)$. The **degree** of an isogeny $\alpha : E \to E'$ is the index of $\alpha^* K(E')$ in $K(E)$. This number is finite because both fields have transcendence degree 1 and α is a nonconstant map. If K has characteristic p then the Frobenius isogeny $\varphi_p(X,Y,Z) = (X^p, Y^p, Z^p)$ from E into $E^{(p)}$ has degree p. Here $E^{(p)}$ is the curve whose Weierstrass equation is obtained from that of E by raising the coefficients to the pth power.

Every isogeny $\alpha : E \to E'$ has a **dual isogeny** $\hat{\alpha} : E' \to E$. The dual isogeny is characterized by the property that $\alpha \circ \hat{\alpha} = [\deg(\alpha)]_{E'}$ and $\hat{\alpha} \circ \alpha = [\deg(\alpha)]_E$, where $[n]_E$ denotes multiplication by n. If $E = E'$, then there is an integer $a(\alpha)$, called the **trace of** α, such that $\alpha + \hat{\alpha} = [a(\alpha)]_E$. The endomorphism α satisfies the quadratic equation

$$\alpha^2 - [a(\alpha)]\alpha + [\deg(\alpha)] = 0 \qquad \text{in } \mathrm{End}(E).$$

In particular, if K has q elements then there is $t \in \mathbf{Z}$ such that

$$\varphi_q^2 - [t]\varphi_q + [q] = 0.$$

The integer t is called the **trace of Frobenius**. It is well known ([S, Ch. 5]) that $|t| \le 2\sqrt{q}$ and the cardinality of $E(K)$ is $q + 1 - t$.

§II.6. Constructing the formal group law of an elliptic curve

Consider an elliptic curve E with Weierstrass equation given by equation (1.1) over an arbitrary field K. Let L be the quotient field of $K[[\tau]]$. Since $K \subset L$, we can consider the points in $E(L)$. Let R be a subring of K (possibly $R = K$) containing 1 and all the Weierstrass coefficients a_i. We will construct a formal group law by embedding $\tau R[[\tau]]$ into $E(L)$ and "stealing" the group law from $E(L)$.

Consider points of the form $(t, -1, s)$ in $E(K)$. Then t can be regarded as the function $-X/Y \in K(E)$, and it is a uniformizer at the origin. Let S be the formal power series constructed in §4. If $f \in \tau R[[\tau]]$ then $(f, -1, S(f)) \in E(L)$ by Lemma 4.3, so there is an embedding $T : \tau R[[\tau]] \to E(L)$ given by

$$T(f) = (f, -1, S(f)). \tag{6.1}$$

Recall Proposition I.1.1, which guarantees that if we can find a power series F in two variables with the properties that $F(0,0)=0$ and $T(f)+T(g)=T(F(f,g))$ then F will be a formal group law. We now show such an F can be found.

Theorem 6.1. *There is a power series $F(t_1,t_2)\in R[[X,Y]]$ with zero constant term such that for $f,g\in\tau R[[\tau]]$,*

$$T(f)+T(g)=T(F(f,g)). \tag{6.2}$$

Therefore F is a formal group law.

Proof. Consider Proposition 2.1, but treat t_1,t_2 as indeterminates and substitute $S(t_1)$, $S(t_2)$ for s_1,s_2. In other words, we are working over the field L' = the quotient field of $R[[t_1,t_2]]$. We need to show t_3 of equation (2.3) is a power series in t_1,t_2. Let M be the ideal of $R[[t_1,t_2]]$ generated by t_1 and t_2. In other words, M is the set of elements $\mu\in R[[t_1,t_2]]$ for which $\mu(0,0)=0$. If $\mu\in M$ and u is a unit of R then $u+\mu$ is a unit in $R[[t_1,t_2]]$ by Lemma I.1.4. Now

$$\begin{aligned} m=\frac{S(t_1)-S(t_2)}{t_1-t_2}&=\sum_{i=3}^{\infty}\frac{s_i(t_1^i-t_2^i)}{t_1-t_2}\\ &=\sum_{i=3}^{\infty}s_i(t_1^{i-1}+t_1^{i-2}t_2+\cdots+t_1t_2^{i-1}+t_2^{i-1})\\ &=s_3(t_1^2+t_1t_2+t_2^2)+s_4(t_1^3+t_1^2t_2+t_1t_2^2+t_2^3)+\cdots \end{aligned}$$

so m belongs to M^2. Then $A=1+a_2m+a_4m^2+a_6m^3$ is a unit in $R[[t_1,t_2]]$, since A is the sum of a unit in R and an element of M. In particular, $A\neq 0$, so Proposition 2.1(b) applies. Also $b=S(t_1)-mt_1\in M^3$. Now (2.3) shows that $t_3\in M$. Thus we can write $t_3=G(t_1,t_2)$, $G\in M$. Certainly $t_3\neq 0$, because $G\equiv -t_1-t_2 \bmod M^2$. We have $(t_1,-1,S(t_1))+(t_2,-1,S(t_2))=-(t_3,-1,s_3)$ in $E(L')$, where $s_3=mt_3+b\in M^3$. By Proposition 2.1(a), the right side is

$$\left(\frac{-t_3}{1-a_1t_3-a_3s_3},-1,\frac{-s_3}{1-a_1t_3-a_3s_3}\right).$$

Let

$$F(t_1,t_2)=\frac{-t_3}{1-a_1t_3-a_3s_3}\in M.$$

If we substitute $t_1=f(\tau)$, $t_2=g(\tau)$ for $f,g\in\tau R[[\tau]]$ we get a homomorphism $R[[t_1,t_2]]\to R[[\tau]]$, which induces a homomorphism $E(L')\to E(L)$. It follows that

$$(f,-1,S(f))+(g,-1,S(g))=(F(f,g),-1,(**)),$$

where $(**)$ is the result of substituting f,g into the power series $s_3\in M^3$. In particular, $(**)\in\tau R[[\tau]]$, so by Lemma 4.3 $(**)=S(F(f,g))$. This proves (6.2). The fact that F is a formal group law follows from Proposition I.1.1. □

The first few terms of F are:

$$F(X,Y)=X+Y-a_1XY-a_2(X^2Y+XY^2)-(2a_3X^3Y+(3a_3-a_1a_2)X^2Y^2+2a_3XY^3)+\cdots$$

§II.7. Homomorphisms of formal group laws arising from isogenies

We claim that an isogeny of elliptic curves over K gives rise to a homomorphism of the corresponding formal group laws over K. Indeed, let

$$I(X,Y,Z) = (f_1(X,Y,Z), f_2(X,Y,Z), f_3(X,Y,Z))$$

be an isogeny between elliptic curves E, E' over K. Here f_1, f_2, f_3 are homogeneous polynomials of the same degree, say d, and f_1, f_2, f_3 do not simultaneously vanish at the origin. Since the origin of E is carried to the origin of E', f_1 and f_3 vanish at $(0,1,0)$ but $f_2(0,1,0) \neq 0$. Thus $f_1/Y^d \in M$ and $f_2/Y^d \in \Omega^\times$, where $M = M_{(0,1,0)}$ and $\Omega = \Omega_{(0,1,0)}$. Now $f_1/Y^d = f_1(X/Y, 1, Z/Y) = f_1(-t,1,-s) = (-1)^d f_1(t,-1,s) \in M$ and similarly $f_2/Y^d = (-1)^d f_2(t,-1,s) \in \Omega^\times$. Thus

$$f_1(X,Y,Z)/f_2(X,Y,Z) = f_1(t,-1,s)/f_2(t,-1,s) \in M.$$

Let $U(\tau) = \sum_{i=1}^\infty u_i \tau^i$ denote the expansion of f_1/f_2 with respect to t. Practically speaking, U can be obtained by expanding s as a power series S and then computing

$$f_1(\tau,-1,S(\tau))/f_2(\tau,-1,S(\tau))$$

in the ring $K[[\tau]]$. Note that $f_2(\tau,-1,S(\tau))$ is invertible since its constant term is nonzero.

Proposition 7.1. *Let E, E', E'' be elliptic curves over K and let F, F', F'' denote the associated formal group laws over K. If $I : E \to E'$ is an isogeny then the power series U constructed above belongs to* $\mathrm{Hom}(F,F')$. *The map $I \mapsto U$ is a one to one group homomorphism from* $\mathrm{Isog}(E,E') \hookrightarrow \mathrm{Hom}(F,F')$. *If $I' : E' \to E''$ and I' corresponds to $U' \in \mathrm{Hom}(F',F'')$ then $I' \circ I$ corresponds to $U' \circ U \in \mathrm{Hom}(F,F'')$.*

Proof. Let L be the quotient field of $K[[\tau]]$. Since I is defined over K, it is a priori defined over L. As usual, let $t = -X/Y$, $s = -Z/Y$. The discussion above shows that I can be written in a neighborhood of the origin as

$$I(X,Y,Z) = \left(\frac{f_1(t,-1,s)}{f_2(t,-1,s)}, -1, \frac{f_3(t,-1,s)}{f_2(t,-1,s)}\right).$$

Let $T : \tau K[[\tau]] \to E(L)$ and $T' : \tau K[[\tau]] \to E'(L)$ be the embeddings (6.1). Substitute $(X,Y,Z) \to T(f) = (f,-1,S(f)) \in E(L)$, where $f \in \tau K[[\tau]]$. Then $t = -X/Y$ changes to f and $s = -Z/Y$ changes to $S \circ f$. Thus

$$I(T(f)) = (U(f), -1, V(f)),$$

where

$$U(\tau) = f_1(\tau,-1,S(\tau))/f_2(\tau,-1,S(\tau)) \in \tau K[[\tau]]$$

and $V(\tau) = f_3(\tau,-1,S(\tau))/f_2(\tau,-1,S(\tau)) \in \tau K[[\tau]]$. By Lemma 4.3, $V = S' \circ U$, where $S'(t)$ is the power series expansion for $-Z/Y$ in the curve E'. Thus

$$I(T(f)) = T'(U(f)). \tag{7.1}$$

By Lemma I.3.1, this equation proves that U is a homomorphism of formal group laws.

If $I_1, I_2 \in \mathrm{Isog}(E,E')$, and if $U_1, U_2 \in \mathrm{Hom}(F,F')$ are the corresponding homomorphisms of formal group laws then on the elliptic curve $E(L)$,

$$\begin{aligned}(I_1+I_2)(\tau,-1,S(\tau)) &= I_1(\tau,-1,S) + I_2(\tau,-1,S) && \text{by definition of } I_1+I_2\\ &= T'(U_1) + T'(U_2) && \text{by (7.1)}\\ &= T'(F'(U_1,U_2)) && \text{by (6.2).}\end{aligned}$$

On the other hand, if $I_1 + I_2$ corresponds to U_3 then

$$(I_1+I_2)(\tau,-1,S) = T'(U_3)$$

by (6.2). Since T' is one to one, $U_3 = F'(U_1, U_2) = U_1 \oplus_{F'} U_2$. This shows that the map $I \mapsto U$ is a group homomorphism.

Finally, if $I : E \to E'$, $I' : E' \to E''$ correspond to U, U', respectively, then since U is the unique solution in $\tau K[[\tau]]$ to $I \circ T = T' \circ U$,

$$I' \circ I \circ T = I' \circ T' \circ U = T'' \circ U' \circ U,$$

whence $I' \circ I$ corresponds to $U' \circ U$. □

Example 7.2: Let F be the formal group law over R associated to an elliptic curve E with Weierstrass equation (1.1), where the coefficients $a_i \in R$, and R is an integral domain. We will compute $[-1]_F$ and $[-2]_F$. Let $g \in \tau R[[\tau]]$. By Proposition 2.1(a),

$$[-1]_E T(g) = [-1]_E(g, -1, S \circ g) = \left(\frac{-g}{1 - a_1 g - a_3 S \circ g}, -1, \frac{-S \circ g}{1 - a_1 g - a_3 S \circ g} \right)$$

The right side is $T\big(-g/(1 - a_1 g - a_3 S \circ g)\big)$ by Lemma 4.3. Now Lemma I.3.1 implies

$$[-1]_F = \frac{-\tau}{1 - a_1\tau - a_3 S} = -\tau \sum_{n=0}^{\infty} (a_1\tau + a_3 S)^n.$$

The calculation of $[-2]_E$ is similar. By Proposition 2.1(c),

$$[-2]_E T(g) = [-2]_E(g, -1, S \circ g) = (t_3(g), -1, m(g)t_3(g) - gm(g) + S \circ g),$$

where

$$\begin{aligned} m(\tau) &= (a_1 S(\tau) + 3\tau^2 + 2a_2\tau S(\tau) + a_4 S(\tau)^2) \\ &\quad \cdot \sum_{n=0}^{\infty} \left(a_1\tau + 2a_3 S(\tau) + a_2\tau^2 + 2a_4\tau S(\tau) + 3a_6 S(\tau)^2\right)^n, \\ t_3(\tau) &= -2\tau - (a_1 m(\tau) + a_3 m(\tau)^2 + (a_2 + 2a_4 m(\tau) + 3a_6 m(\tau)^2)\big(S(\tau) - \tau m(\tau)\big) \\ &\quad \cdot \sum_{n=0}^{\infty} (-1)^n \left(a_2 m(\tau) + a_4 m(\tau)^2 + a_6 m(\tau)^3\right)^n. \end{aligned}$$

Again, Lemma 4.3 implies $[2]_E T(g) = T\big(t_3(g)\big)$ and Lemma I.3.1 implies

$$[-2]_F = t_3(\tau).$$

Obviously $[2]_F = [-1]_F \circ [-2]_F$. □

An isogeny $I : E \to E'$ is called **separable** if it has the property: if t' is a uniformizer at the origin of E' then $I \circ t'$ is a uniformizer at the origin of E. This definition does not depend on the choice of uniformizer t'. An isogeny which is not separable is called **inseparable**. In characteristic zero, all isogenies are separable. In characteristic p, the Frobenius is not separable, since it carries uniformizers into pth powers of uniformizers. It is a theorem [S, II.2.12] that every isogeny can be factored as φ_p^k from E into $E^{(q)}$ ($q = p^k$) composed with a separable isogeny from $E^{(q)}$ into E'.

Lemma 7.3. *Let I be an isogeny from E to E' and let $U(\tau) = \sum u_i\tau^i$ be the corresponding homomorphism between the formal group laws. I is separable iff $u_1 \neq 0$.*

Proof. Let t' be the function $-X/Y \in K(E')$. U is the power series expansion of $t' \circ I$. Thus $t' \circ I$ is not a uniformizer iff $t' \circ I \in M^2_{(0,1,0)}$ iff $u_1 = 0$. □

Example 7.4. Let E be an elliptic curve over a field K of characteristic $p > 0$, and let F be its associated formal group law. Then $\varphi_p : E \to E^{(p)}$ corresponds to the homomorphism of formal group laws $\phi = \tau^p : F \to F^{(p)}$.

§II.8. Height of an elliptic curve

The height of a formal group law was defined in §I.4. Naturally, the height of an elliptic curve is defined to be the height of the associated formal group law.

Proposition 8.1. *An elliptic curve over a field of characteristic p has height one or two.*

Proof. Let $\varphi_p : E \to E^{(p)}$ be the pth power Frobenius and $\hat{\varphi}_p : E^{(p)} \to E$ its dual. Let F be the formal group law associated to E, and let $V(\tau) = \sum v_i \tau^i : F^{(p)} \to F$ be the homomorphism of formal group laws associated to $\hat{\varphi}_p$. Then $[p]_F = V(\tau^p)$. If $\hat{\varphi}_p$ is separable then $v_1 \neq 0$, so E has height one. If $\hat{\varphi}_p$ is inseparable, it can be written as a composition of a power of φ_p and a separable isogeny ([S, Corollary II.2.12]). Since the degree of $\hat{\varphi}_p$ equals the degree of φ_p, only one power of φ_p can occur in this decomposition. Thus $\hat{\varphi}_p = \alpha \circ \varphi_p$ with α an isomorphism. Let $A = \sum a_i \tau^i$ be the power series corresponding to α and let A' be the power series corresponding to α^{-1}. Then $[p]_E = A(\tau^{p^2}) = a_1 \tau^{p^2} + \cdots$, and $a_1 \neq 0$ because $A \circ A'(\tau) = \tau$. In this case E has height two. □

An elliptic curve in characteristic p of height one is called **ordinary**. An elliptic curve in characteristic p of height 2 is called **supersingular**. The next lemma gives another characterization of supersingular and ordinary curves when the underlying field is finite. Recall that the trace of Frobenius was defined in §5.

Proposition 8.2. *An elliptic curve E over a finite field K with $q = p^n$ elements is supersingular iff p divides the trace of Frobenius iff $|E(K)| \equiv 1 \bmod p$. If E is supersingular and n is even then $|E(K)| = q + 1 + m\sqrt{q}$, $m \in \{ -2, -1, 0, 1, 2 \}$. If E is supersingular, n is odd, and $p \geq 5$, then $|E(K)| = q + 1$. If E is supersingular, n is odd, and $p \leq 3$ then $|E(K)| = q + 1 + m\sqrt{pq}$, where $m \in \{ -1, 0, 1 \}$.*

For a more precise statement about which values of $|E(K)|$ can occur, the reader may consult [W, Theorem 4.1].

Proof. As above, let F be the formal group law corresponding to E and $V : F^{(p)} \to F$ the homomorphism of formal group laws corresponding to $\hat{\varphi}_p$. In other words, V is defined by $[p]_F = V(\tau^p)$. Recall that $E^{(p)}$ denotes the elliptic curve whose Weierstrass equation is obtained by taking the pth powers of the Weierstrass coefficients for E, and we use similar notation for isogenies. Now $\hat{\varphi}^{(p^k)} : E^{(p^{k+1})} \to E^{(p^k)}$ is the dual of the map $\varphi_p : E^{(p^k)} \to E^{(p^{k+1})}$, so

$$\hat{\varphi}_p \circ \hat{\varphi}_p^{(p)} \circ \cdots \circ \hat{\varphi}_p^{(p^{n-1})}$$

is the dual of φ_p^n. The corresponding formal group law homomorphism is

$$N(V) = V \circ V^{(p)} \circ \cdots \circ V^{(p^{n-1})}.$$

Let t be the trace of Frobenius (§5), so that $|E(K)| = q + 1 - t$. Since $[t]_E$ is the sum of φ_p^n and its dual in $\mathrm{End}(E)$, it follows that

$$[t]_F = N(V) \oplus_F \tau^{p^n} = F(N(V), \tau^{p^n}).$$

If E is supersingular then V has height one, so $\mathrm{N}(V)$ has height n. In that case, $[t]_F$ has height at least n, so $[t^2]_F$ has height at least $2n$. Since the height of F is two in this case, Corollary I.4.8 implies t^2 is divisible by p^n. Since $|t| \leq 2\sqrt{q}$ (see §5) and $q|t^2$, we deduce that $t^2 \in \{ 0, q, 2q, 3q, 4q \}$. Since $t \in \mathbf{Z}$, we find $t \in \{ 0, \pm q^{1/2}, \pm 2q^{1/2} \}$ if n is even; $t = 0$ if n is odd and $p > 3$; $t \in \{ 0, \pm\sqrt{2q} \}$ if n is odd and $p = 2$, $t \in \{ 0, \pm\sqrt{3q} \}$ if n is odd and $p = 3$. Since $|E(K)| = q + 1 - t$, the cardinality of $E(K)$ must be of the form stated.

Next suppose E is ordinary. Then $\mathrm{N}(V)$ has height zero, so $[t]_F$ has height zero. In that case Corollary I.4.8 implies t is prime to p. □

Proposition 8.3. *If E is an ordinary elliptic curve defined over a field K of cardinality p^n and F is its associated formal group law then the trace of the Frobenius endomorphism is equal mod p to the norm from K to $\mathbf{F}_p$ of the first nonzero coefficient of $[p]_F$.*

PROOF. Let $|K| = p^n = q$. The homomorphism of F associated to $\varphi_q^2 + [-t]_E\varphi_q + [q]_E$ is zero, thus each of its coefficients is zero. Now φ_q corresponds to the power series τ^q, and $[-t]_E$ corresponds to a power series of the form $-t\tau + \tau^2(\cdots)$, therefore $\varphi_q^2 + [-t]_E \circ \varphi_q$ corresponds to $F(\tau^{q^2}, -t\tau^q + \tau^{2q}(\cdots))$, which is of the form $-t\tau^q + \tau^{2q}(\cdots)$. Finally, we evaluate $[q]_F$. Equation (I.4.2) reads

$$[q]_F = (V \circ \phi)^n = V \circ V^{(p)} \circ \cdots \circ V^{(p^{n-1})} \circ \phi^n = (\mathrm{N}_{K/\mathbf{F}_p}(v)\tau + (\cdots)\tau^2) \circ \tau^q,$$

so $[q]_F = \mathrm{N}_{K/\mathbf{F}_p}(v)\tau^q + (\tau^{2q})(\cdots)$. Thus

$$0 = F\left(-t\tau^q + \tau^{2q}(\cdots), \mathrm{N}_{K/\mathbf{F}_p}(v)\tau^q + \tau^{2q}(\cdots)\right) = (-t + \mathrm{N}_{K/\mathbf{F}_p}(v))\tau^q + \tau^{2q}(\cdots).$$

□

PART III. FURTHER RESULTS ON FORMAL GROUPS

§III.1. Some theorems of Couveignes

Let R be an integral domain of characteristic p. Let $\mathbf{F}_p \subset \mathbf{R}$ be the field with p elements if p is prime, and $\mathbf{F}_p = \mathbf{Z}$ if $p = 0$. Let $F = \sum_{i,j} f_{ij} X^i Y^j$, $F' = \sum_{i,j} f'_{ij} X^i Y^j$ be two formal group laws over R, and let $U(\tau) = \sum_{i=1}^{\infty} u_i \tau^i \in \tau R[[\tau]]$ be a homomorphism from F to F'. Couveignes proved with an elementary argument in his PhD thesis that the coefficients u_i satisfy some simple relations over R.

Theorem 1.1. *Let i be a positive integer which is not a power of p. If $p = 0$ assume $\binom{i}{m}$ is a unit in R for some $1 \leq m < i$. There is a polynomial C_i in several variables with coefficients in $\mathbf{F}_p$ such that for each F, F', U as above we have*

$$u_i = C_i(u_j, f_{kl}, f'_{kl} \,|\, 1 \leq j < i, 1 \leq k + \ell \leq i\,).$$

Proof. Let A be transcendental and work in the integral domain $R[A]$. Since U is a homomorphism,

$$U(F(\tau, A\tau)) = F'(U(\tau), U(A\tau)).$$

By (I.2.2) there are power series $G, G' \in R[[X, Y]]$ such that $F(X, Y) = X + Y + XYG(X, Y)$ and $F'(X, Y) = X + Y + XYG'(X, Y)$. Therefore

$$\sum u_j(\tau + A\tau + A\tau^2 G(\tau, A\tau))^j = \sum u_j \tau^j + \sum u_j (A\tau)^j + U(\tau)U(A\tau)G'(U(\tau), U(A\tau)).$$

This can be rewritten

$$\begin{aligned} 0 = &\sum u_j \tau^j \{(1 + A + A\tau G(\tau, A\tau))^j - (1 + A^j)\} \\ &- A\tau^2 (\sum_{j=0}^{\infty} u_{j+1}\tau^j)(\sum_{j=0}^{\infty} u_{j+1}(A\tau)^j) G'(\sum_{j=1}^{\infty} u_j \tau^j, \sum_{j=1}^{\infty} u_j (A\tau)^j). \end{aligned}$$

The coefficient of τ^i is of the form $u_i\{(1+A)^i - (1+A^i)\} + M_i$, where M_i is a polynomial in $A, u_1, u_2, \ldots, u_{i-1}$ and in some of the coefficients of G, G'. This gives the relation

$$u_i\{(1 + A)^i - (1 + A^i)\} - M_i = 0.$$

The hypothesis that i is not a power of p implies $(1+A)^i \neq 1 + A^i$. If $p = 0$ choose m such that $\binom{i}{m}$ is a unit in R, and if $p > 0$ let m be a positive integer such that the coefficient of A^m is nonzero in the polynomial $(1 + A)^i - (1 + A^i)$. In characteristic p this coefficient is a unit in R because it is a nonzero element of the prime field $\mathbf{F}_p$. Since A is transcendental, the coefficient of A^m in our relation must be identically zero. This coefficient gives our desired formula for u_i in terms of the u_j and the coefficients of F and F'. □

The next theorem accounts for the u_i when i is a power of p. It was proved by Couveignes for formal group laws associated to ordinary elliptic curves, but his argument generalizes easily to formal group laws of any height.

Theorem 1.2. *Let i be a power of a prime p and let $h > 0$. There is a polynomial C_i in several variables with coefficients in $\mathbf{F}_p$ such that: if $F = \sum f_{k\ell} X^k Y^\ell$ and $F' = \sum f'_{j\ell} X^j Y^\ell$ are formal group laws of height h over a domain R of characteristic p and $U = \sum u_j \tau^j : F \to F'$ a homomorphism then*

$$v'_1 u_i^q - v_1^i u_i = C_i(u_j, f_{k\ell}, f'_{k\ell} \,|\, j < i, k + \ell \leq qi\,)$$

where $q = p^h$ and v_1, v'_1 are the first nonzero coefficients of the power series $[p]_F$, $[p]_{F'}$, respectively.

Proof. By Proposition I.4.2 we can write $[p]_F(\tau) = V \circ \phi^h(\tau) = V(\tau^q)$, where $V(\tau) = \sum v_j \tau^j$ is a homomorphism of height zero from $F^{(q)}$ to F'. It is easy to show by induction on n that for $n > 0$ the jth coefficient of $[n]_F$ is a polynomial in the $f_{k\ell}$ with $k + \ell \le j$. Since v_j is the jqth coefficient of $[p]_F$, v_j is a polynomial in the $f_{k\ell}$ with $k + \ell \le jq$. Similarly $[p]_{F'} = V' \circ \phi^h$, $V'(\tau) = \sum v'_j \tau^j$, and v'_j is a polynomial in the $f'_{k\ell}$ with $k + \ell \le jq$. Since $[p]_{F'} \circ U = U \circ [p]_F$,

$$V'(U(\tau)^q) = U\big(V(\tau^q)\big).$$

Let $\sigma = \tau^q$. The left side is

$$v'_1(\sum_{j=1}^{\infty} u_j^q \sigma^j) + v'_2(\sum_{j=1}^{\infty} u_j^q \sigma^j)^2 + \cdots,$$

and the coefficient of σ^i is of the form $v'_1 u_i^q$ plus terms involving u_j for $j < i$ and v'_j for $j \le i$. The right side is

$$u_1(\sum_j v_j \sigma^j) + u_2(\sum_j v_j \sigma^j)^2 + \cdots + u_i(\sum_j v_j \sigma^j)^i + \cdots.$$

This time the coefficient of σ^i is of the form $u_i(v_1)^i$ plus terms involving u_j for $j < i$ and v_j for $j \le i$. By equating the two sides we get $v'_1 u_i^q - v_1^i u_i$ equals a polynomial in the u_j for $1 \le j < i$ and the v_j, v'_j for $1 \le j \le i$. □

Example 1.3. When $i = p^0$ Couveignes' relation is simply

$$v'_1 u_1^q - v_1 u_1 = 0.$$

If $p = 2$ and $i = 2$ then

$$v'_1 u_2^q - v_1^2 u_2 = v_2 u_1 + v'_2 u_1^{2q}.$$

§III.2. Hom(F, F') as a Z-module or $\mathbf{Z}_p$-module

Let F, F' be two formal group laws over an integral domain R of characteristic p. Let $\operatorname{Hom}(F, F')$ denote the group of homomorphisms from F to F', where the addition is defined as in Corollary I.4.5. Write $\operatorname{End}(F) = \operatorname{Hom}(F, F)$. If $\lambda \in \operatorname{End}(F)$, $\mu \in \operatorname{End}(F')$, $U, V \in \operatorname{Hom}(F, F')$ then $\mu \circ U \circ \lambda \in \operatorname{Hom}(F, F')$. In particular, $\mathbf{Z}$ acts on $\operatorname{Hom}(F, F')$ by

$$n \cdot U = [n]_{F'} \circ U = U \circ [n]_F \qquad (n \in \mathbf{Z}).$$

We will show that if $p > 0$ then the action of $\mathbf{Z}$ can be extended to an action of $\mathbf{Z}_p$, the p-adic integers. By definition, $\mathbf{Z}_p$ is the completion of $\mathbf{Z}$ with respect to the p-adic metric $|ap^r|_p = p^{-r}$ for $ap^r \in \mathbf{Z}$, $(p, a) = 1$. For nonzero $a \in \mathbf{Z}_p$ we define $v_p(a) = r$, where r is the integer such that $a = p^r b$, $b \in \mathbf{Z}_p^\times$; thus $|a|_p = p^{-v(a)}$.

Lemma 2.1. *If $U \in \operatorname{Hom}(F, F')$ and the height of F' is not ∞ then $n \cdot U = 0$ only if $n = 0$ or $U = 0$.*

Proof. $n \cdot U = [n]_{F'} \circ U$. Since R is a domain, the composition of two power series $A, B \in \tau R[[\tau]]$ is zero iff $A = 0$ or $B = 0$. Thus $n \cdot U = 0$ iff $U = 0$ or $[n]_{F'} = 0$. Now $[n]_{F'} = 0$ iff $n = 0$ by Corollaries I.4.8 and I.4.7. □

We put a topology on $\operatorname{Hom}(F, F')$ by decreeing that U and V are close iff $U \ominus_{F'} V$ has a large height. In other words, the topology on $\operatorname{Hom}(F, F')$ is induced from the **height metric** $|U| = c^{\operatorname{ht}(U)}$, where $0 < c < 1$.

Proposition 2.2. *If R is a domain of characteristic $p > 0$ and $U \in \operatorname{Hom}(F, F')$ then the map $\mathbf{Z} \times \operatorname{Hom}(F, F') \to \operatorname{Hom}(F, F')$ given by $(n, U) \mapsto n \cdot U$ is continuous with respect to the p-adic metric on $\mathbf{Z}$ and the height metric on $\operatorname{Hom}(F, F')$.*

Proof. We must show that if $n = m + ap^t$ with t large and if $U, V \in \operatorname{Hom}(F, F')$ are close then $n \cdot U$ is close to $m \cdot V$. But

$$n \cdot U \ominus_{F'} m \cdot V = [n]_{F'} \circ (U \ominus_{F'} V) \oplus_{F'} [ap^t]_{F'} \circ V.$$

The height of $[n]_{F'} \circ (U \ominus_{F'} V)$ is $\geq \mathrm{ht}(U \ominus_{F'} V)$. The height of $[ap^t]_{F'} \circ V$ is $\geq t$. Both these heights are large, so the height of the sum is large by Corollary I.4.5. □

Corollary 2.3. *If R is an integral domain of characteristic $p > 0$ then $\mathrm{Hom}(F, F')$ is a $\mathbf{Z}_p$-module. If the height of F' is finite and $a \in \mathbf{Z}_p$, $U \in \mathrm{Hom}(F, F')$ then $a \cdot U = 0$ only if $a = 0$ or $U = 0$.*

Proof. The first sentence is immediate from Proposition 2.2. Since in particular $\mathrm{End}(F')$ is a $\mathbf{Z}_p$-module, we can define $[a]_{F'} = a \cdot [1]_{F'} \in \mathrm{End}(F')$ when $a \in \mathbf{Z}_p$. Then $a \cdot U = [a]_{F'} \circ U$. This can equal zero only if $[a]_{F'} = 0$ or $U = 0$. Suppose $[a]_{F'} = 0$. Let n be an integer such that $|a - n|_p < |a|_p$, thus $n = a + p^k b$, $b \in \mathbf{Z}_p$, and p^k does not divide a. Then $\mathrm{ht}([n]_{F'}) < k\ \mathrm{ht}(F')$, $\mathrm{ht}([p^k b]_{F'}) \geq k\ \mathrm{ht}(F')$, so by Corollary I.4.5, $\mathrm{ht}([a]_{F'}) = \mathrm{ht}([n]_{F'}) < \infty$. This shows $[a]_{F'} \neq 0$, as required. □

§III.3. Consequences of Couveignes' theorems

Fix the following notation throughout this section. Let R be an integral domain of characteristic $p > 0$, F and F' formal group laws of height h over R, and $q = p^h$. Let $C_1, C_2, \ldots$ denote Couveignes' relations given in §1 evaluated at the coefficients of F, F' but leaving the u_i as indeterminates; thus $C_i \in R[X_1, \ldots, X_i]$ and $C_i = X_i +$ a certain polynomial in $X_1, \ldots, X_{i-1}$ if i is not a power of p; $C_i = v_1' X_i^q - v_1^i X_i +$ a certain polynomial in $X_1, \ldots, X_{i-1}$ if i is a power of p. Here the v_i and v_i' lie in R, since they are polynomials in the coefficients of F and F', respectively. Couveignes' theorems assert that if $\sum u_i \tau^i \in \mathrm{Hom}(F, F')$ then $C_i(u_1, \ldots, u_i) = 0$ for all i. Let K denote the separable algebraic closure of the quotient field of R.

Lemma 3.1. *There are exactly q^n solutions $(u_1, \ldots, u_{p^n - 1})$ with $u_i \in K$ to the first $p^n - 1$ of Couveignes' relations.*

Proof. For each solution $(v_1, \ldots, v_{i-1})$ to the first $i - 1$ of Couveignes' equations over K there are q values or 1 value of v_i such that $(v_1, \ldots, v_i)$ is a solution to the ith relation, according as i is or is not a power of p. (To see that the q solutions for v_i are distinct when i is a power of p, note that the derivative with respect to X_i of C_i is v_1^i, which is nonzero.) The lemma now follows easily by induction on n. □

Theorem 3.2. *If $u_1, u_2, \ldots$ is a solution to Couveignes' relations then $\sum u_i \tau^i \in \mathrm{Hom}(F, F')$.*

Proof. Without loss of generality we can replace R by K. In [F, III, §2] it is shown that $\mathrm{Hom}(F, F')$ is free over $\mathbf{Z}_p$ of rank h^2 and $p^n \mathrm{Hom}(F, F')$ is the set of homomorphisms with height $\geq nh$. (In fact, it is shown that $\mathrm{Hom}(F, F')$ is the maximal order of a central division algebra over $\mathbf{Q}_p$ of rank h^2 and invarianat $1/h$, but we do not need this here.) It follows that a complete set of $\mathbf{Z}_p$-module generators $U_1, \ldots, U_{h^2}$ can be found such that the height of each generator is less than h, and if $\sum c_i U_i$ has height $\geq nh$ for some $c_i \in \mathbf{Z}_p$ then each c_i is divisible by p^n. If $U, U' \in \mathrm{Hom}(F, F')$ and $U \equiv U' \bmod \deg q^n$ (meaning that the ith coefficient of U and U' coincide for all $i \leq q^n$) then

$$0 = F'(U', [-1]_{F'} \circ U') \equiv F'(U, [-1]_{F'} \circ U') = U \ominus_{F'} U' \bmod \deg q^n,$$

so $U \ominus_{F'} U'$ has height $\geq nh$, and it is therefore divisible by p^n. Thus $\sum c_i U_i \equiv \sum c_i' U_i \bmod \deg q^n$ $(c_i, c_i' \in \mathbf{Z}_p)$ implies $c_i \equiv c_i' \bmod p^n$. This shows that the number of distinct elements $\sum_{i=1}^{q^n - 1} u_i \tau^i$ which are truncations of power series in $\mathrm{Hom}(F, F')$ is the cardinality of $(\mathbf{Z}/p^n\mathbf{Z})^{h^2}$, which is q^{nh}. Each truncation gives rise to a solution $(u_1, \ldots, u_{q^n - 1})$ of the first $q^n - 1$ of Couveignes' relations. Since this coincides with the total number of solutions, each solution of Couveignes' relation arises from $\mathrm{Hom}(F, F')$. □

Corollary 3.3. *If $h = 1$ and if $\mathrm{Hom}(F, F')$ contains a homomorphism (with coefficients in R) of height k then all the solutions $(v_1, v_2, \ldots)$ in K to Couveignes' relations for which $v_i = 0$ for $i < p^k$ actually lie in R.*

Proof. Let U be the homomorphism of height k and $\mathbf{Z}_p \cdot U = \{\, c \cdot U \mid c \in \mathbf{Z}_p \,\}$. As mentioned in the previous proof, $\mathrm{Hom}(F, F') \cong \mathbf{Z}_p$, and it is generated by a homomorphism U_0 of height zero. Find $a \in \mathbf{Z}_p$

such that $U = a \cdot U_0$. Since $\mathrm{ht}(a \cdot U_0) = v_p(a)$, $v_p(a) = k$. Thus $\mathbf{Z}_p \cdot U = \mathbf{Z}_p a \cdot U_0 = p^k \mathbf{Z}_p \cdot U_0$. Since U is defined over R, so is $c \cdot U$ for each $c \in \mathbf{Z}_p$. Thus every element of $p^k \mathbf{Z}_p \cdot U_0$ has coefficients in R. The coefficients of such elements are precisely the solutions $(v_1, v_2, \ldots)$ to Couveignes' relations which have $v_i = 0$ for all $i < p^k - 1$. □

Bibliography

[C] J. P. Couveignes, Quelques calculs en theorie des nombres, Ph.D. thesis, Bourdeaux, 1995

[F] A. Frohlich, *Formal Groups*, *Lect. Notes in Math.* **74**, Springer-Verlag, 1968

[Fu] W. Fulton, *Algebraic Curves*, Addison-Wesley, 1969

[H] M. Hazewinkel, *Formal Groups and Applications*, Academic Press, New York, 1978

[K] A. W. Knapp, *Elliptic Curves*, *Math. Notes* **40**, Princeton University Press, Princeton, New Jersey, 1992

[LM] R. Lercier and F. Morain, Counting the number of points on elliptic curves over F_{p^n} using Couveignes' algorithm, Research report LIX/RR/95/09, Ecole Polytechnique-LIX, September 1995

[S] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986

[W] W. C. Waterhouse, Abelian varieties over finite fields, *Ann. scient. Éc. Norm. Sup.* **2** 1969, 521-560