Formal groups

Peter Bruin
2 March 2006

0. Introduction

The topic of formal groups becomes important when we want to deal with *reduction* of elliptic curves. Let R be a discrete valuation ring with field of fractions K and residue class field k, and suppose we are given a Weierstraß equation

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in R.$$

If the discriminant of E is not in the maximal ideal $\mathfrak{m}$ of R, it makes sense to look at the solutions of the *reduced curve* $\tilde{E}$ over k obtained by reducing the a_i modulo $\mathfrak{m}$. It turns out that there are natural group homomorphisms

$$E(K) \cong E(R) \to \tilde{E}(k),$$

and that the situation is relatively simple if we assume that R is a *complete* discrete valuation ring. We recall the definition of completeness of a ring with respect to an ideal.

Definition. Let A be a ring and I an ideal of A. Consider A as a topological ring by defining the sets $I \supseteq I^2 \supseteq I^3 \supseteq \cdots$ to be a basis of open neighbourhoods of 0. Then A is called *complete with respect to* I if A is Hausdorff (equivalently, $\bigcap_{n=1}^{\infty} I^n = 0$) and complete with respect to this topology. It amounts to the same to say that A is complete with respect to I if the natural homomorphism of topological rings

$$A \to \varprojlim A/I^n,$$

where each A/I^n has the discrete topology, is an isomorphism.

If we assume that R is complete with respect to its maximal ideal, it turns out that we can construct a short exact sequence

$$0 \longrightarrow \hat{E}(\mathfrak{m}) \longrightarrow E(K) \longrightarrow \tilde{E}(k) \longrightarrow 0,$$

where $\hat{E}(\mathfrak{m})$ is a group that will be defined in the next section.

1. Parametrisation of an elliptic curve

Let (E, O) be an elliptic curve over a field k. We embed E in $\mathbf{P}^2_k$ as a Weierstraß curve

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

with $O = (0 : 1 : 0)$. We choose affine coordinates (z, w) on the open part $D(Y)$ of $\mathbf{P}^2_k$, placing O at the origin of our coordinate system:

$$z = -X/Y, \quad w = -Z/Y;$$

after dividing by Y^3, the equation of the curve becomes

$$-w + a_1zw + a_3w^2 = -z^3 - a_2z^2w - a_4zw^2 - a_6w^3.$$

We put

$$f = z^3 + a_1zw + a_2z^2w + a_3w^2 + a_4zw^2 + a_6w^3 \in k[z, w]$$

and write the Weierstraß equation as

$$w = f(z, w).$$

We want to 'solve' this equation for w as a power series in z. To do this, we generalise things a bit by considering the above equation as a polynomial equation in the variable w over the ring

$$A = \mathbf{Z}[a_1, a_2, a_3, a_4, a_6][[z]],$$

which is the completion of the polynomial ring $\mathbf{Z}[a_1, a_2, a_3, a_4, a_6, z]$ with respect to the ideal (z). We put

$$F = -z^3 + (1 - a_1z - a_2z^2)w - (a_3 + a_4z)w^2 - a_6w^3 \in A[w]$$

and apply the following version of Hensel's lemma to find a zero of F.

Hensel's lemma. *Let A be a ring which is complete with respect to an ideal I, and let $F \in A[w]$ be a polynomial. If for some $m \geq 1$ we have*

$$F(0) \in I^m \quad \textit{and} \quad F'(0) \equiv 1 \pmod{I},$$

then there is an element $\alpha \in I^m$ with $F(\alpha) = 0$, and the recursion

$$w_0 = 0, \quad w_{n+1} = w_n - F(w_n) \text{ for } n \geq 0$$

converges to α. If moreover A is a domain, α is the unique zero of F in I.

Proof. We first note that the assumption $F(0) \in I^m$ implies that $F(x) \in I^m$ for all $x \in I^m$, and by induction on n it follows immediately that $w_n \in I^m$ for all $n \geq 0$. Next we prove by induction on n that

$$w_{n+1} \equiv w_n \pmod{I^{m+n}} \quad \text{for } n \geq 0.$$

For $n = 0$, this is just the assumption $F(0) \in I^m$. Now suppose that the congruence holds for $n - 1$, and write

$$F(x) - F(y) = (x - y)(F'(0) + xG(x, y) + yH(x, y))$$

where $G, H \in A[x, y]$ are certain polynomials. Then

$$\begin{aligned} w_{n+1} - w_n &= (w_n - F(w_n)) - (w_{n-1} - F(w_{n-1})) \\ &= (w_n - w_{n-1}) - (F(w_n) - F(w_{n-1})) \\ &= (w_n - w_{n-1}) - (w_n - w_{n-1})(F'(0) + w_nG(w_n, w_{n-1}) + w_{n-1}H(w_n, w_{n-1})) \\ &= (w_n - w_{n-1})(1 - F'(0) - w_nG(w_n, w_{n-1}) - w_{n-1}H(w_n, w_{n-1})). \end{aligned}$$

This is in I^{m+n} because $w_n - w_{n-1} \in I^{m+n-1}$ by the induction hypothesis and because the second factor is in I. The completeness of A with respect to I implies that the sequence $\{w_n\}_{n \geq 0}$ converges to a unique element $\alpha \in A$, which is in I^m because all the w_n are. The sequence $\{F(w_n)\}_{n \geq 0}$ converges to $F(\alpha)$, and taking the limit of the relation $w_{n+1} = w_n - F(w_n)$ as $n \to \infty$ shows that $F(\alpha) = 0$.

If A is a domain and $\alpha, \beta \in I$ are zeros of F, then the equality

$$0 = F(\alpha) - F(\beta) = (\alpha - \beta)(F'(0) + \alpha G(\alpha, \beta) + \beta H(\alpha, \beta))$$

shows that either $\alpha = \beta$ or $F'(0) = -\alpha G(\alpha, \beta) - \beta H(\alpha, \beta) \in I$. The second possibility contradicts our assumption $F'(0) - 1 \in I$, so $\alpha = \beta$, and we conclude that α is the unique zero of F in I. □

Carrying out the first few steps of the recursion gives us the following power series expansion of w in terms of z:

$$w = z^3(1 + a_1 z + (a_1^2 + a_2)z^2 + (a_1^3 + 2a_1 a_2 + a_3)z^3 + \cdots).$$

Now let K be the field of fractions of an integral local k-algebra A which is complete with respect to its maximal ideal $\mathfrak{m}$. Then the power series $w(z)$ (or any power series with coefficients in A, for that matter) converges for all $z \in \mathfrak{m}$. This gives us an injective map

$$\begin{aligned} \mathfrak{m} &\to E(K) \\ z &\mapsto (z : -1 : w(z)), \end{aligned}$$

or (in terms of the coordinates z and w)

$$\begin{aligned} \mathfrak{m} &\to E(K) \\ z &\mapsto (z, w(z)). \end{aligned}$$

The above version of Hensel's lemma shows that the image of this map is equal to the set of points (z, w) in $E(K)$ with $z, w \in \mathfrak{m}$.

For $z \in \mathfrak{m}$, it is also possible to express the usual coordinates (x, y) of the point $(z, w(z))$ in terms of formal Laurent series in z. Since $x = X/Z = z/w(z)$ and $y = Y/Z = -1/w(z)$, we get

$$\begin{aligned} x &= z^{-2}(1 - a_1 z - a_2 z^2 - a_3 z^3 + \cdots) \\ y &= -z^{-3}(1 - a_1 z - a_2 z^2 - a_3 z^3 + \cdots). \end{aligned}$$

Our next goal is to express the group operation of E in terms of the parameter z. The group operation will then give us a map

$$\Sigma\colon \mathfrak{m} \times \mathfrak{m} \to \mathfrak{m}.$$

Computing Σ is a matter of writing down the formulas for the "chord and tangent" algorithm in the coordinates (z, w). Recall that if E is embedded into $\mathbf{P}^2_k$ via a Weierstraß equation, then the points of E lying on any line in $\mathbf{P}^2$ add to zero. If z_1, z_2 are in $\mathfrak{m}$, then the slope of the line through the points $(z_1, w(z_1))$ and $(z_2, w(z_2))$ is

$$\begin{aligned} \lambda &= \frac{w(z_1) - w(z_2)}{z_1 - z_2} \\ &= (z_1^2 + z_1 z_2 + z_2^2) + a_1(z_1^3 + z_1^2 z_2 + z_1 z_2^2 + z_2^3) + (a_1^2 + a_2)(z_1^4 + z_1^3 z_2 + z_1^2 z_2^2 + z_1 z_2^3 + z_2^4) + \cdots; \end{aligned}$$

the last expression is valid also when $z_1 = z_2$. The equation of this line is

$$w = \lambda z + v \quad \text{with } v = w_1 - \lambda z_1 = w_2 - \lambda z_2;$$

substituting this into the equation for the elliptic curve, we obtain a cubic equation in z whose three roots are z_1, z_2 and the z-coordinate of a third point, say z_3. The coefficient of the quadratic term of this equation gives us $-(z_1 + z_2 + z_3)$, and we obtain

$$z_3 = -z_1 - z_2 - \frac{a_1\lambda + a_2 v + a_3\lambda^2 + 2a_4\lambda v + 3a_6\lambda^2 v}{1 + a_2\lambda + a_4\lambda^2 + a_6\lambda^3}.$$

We first consider the special case where $z_1 = z$, $z_2 = 0$. Making use of $\lambda = w(z)/z$ and $v = 0$, we find the following formula for $i(z)$, the z-coordinate of the inverse of the point $(z, w(z))$:

$$\begin{aligned} i(z) &= -z - \frac{a_1 w(z)/z + a_3(w(z)/z)^2}{1 + a_2 w(z)/z + a_4(w(z)/z)^2 + a_6(w(z)/z)^3} \\ &= -z - a_1 z^2 - a_1^2 z^3 - (a_1^3 + a_3)z^4 - a_1(a_1^3 + 3a_3)z^5 + \cdots. \end{aligned}$$

The z-coordinate of the sum of the two points $(z_1, w(z_1))$ and $(z_2, w(z_2))$ is now

$$\begin{aligned} \Sigma(z_1, z_2) &= i(z_3) \\ &= z_1 + z_2 - a_1 z_1 z_2 - a_2(z_1^2 z_2 + z_1 z_2^2) - (2a_3 z_1^3 z_2 - (a_1 a_2 - 3a_3)z_1^2 z_2^2 + 2a_3 z_1 z_2^3) + \cdots. \end{aligned}$$

The binary operation Σ makes $\mathfrak{m}$ into an Abelian group with neutral element 0 and inverse operation i. We denote this group by $\hat{E}(\mathfrak{m})$. As the power series Σ defining the group structure does not depend on $\mathfrak{m}$, it makes sense to study it on its own, for example as a power series over $\mathbf{Z}[a_1, a_2, a_3, a_4, a_6]$. It is an instance of a *formal group law*.

2. Formal groups

We fix a ring R.

Definition. A *formal group law* over R is a power series

$$F \in R[[x, y]]$$

satisfying the following axioms:
(1) $F \equiv x + y \pmod{(x, y)^2}$.
(2) Associativity: $F(x, F(y, z)) = F(F(x, y), z)$.
(3) Neutral element: $F(x, 0) = x$ and $F(0, y) = y$.
(4) Commutativity: $F(x, y) = F(y, x)$.
(5) Existence of inverse: $F(x, i(x)) = 0$ for some unique power series

$$i = -x + \cdots \in R[[x]].$$

The *formal group* $\mathfrak{F}$ defined by F is the rule that associates to an R-algebra which is complete with respect to an ideal I the group $\mathfrak{F}(I)$ with underlying set I and whose group operation is given by the power series I.

Implicit function theorem. *Let $F \in R[[x, y]]$ be a power series of the form*

$$F = ax + by + \cdots \quad \text{with } b \in R^\times.$$

Then there exists a unique power series $g \in R[[x]]$ such that $F(x, g(x)) = 0$.

Proof. We have to show that there exists a unique sequence of polynomials $g_n \in R[x]$, with g_n of degree at most n, such that

$$g_{n+1} \equiv g_n \pmod{(x)^{n+1}}$$

and

$$F(x, g_n(x)) \equiv 0 \pmod{(x)^{n+1}}.$$

For $n = 1$ it is clear that we must take $g_1 = -x$. To define g_n for $n \geq 2$, we note that g_n has to be of the form $g_{n-1} + \lambda x^n$ with $\lambda \in R$. Since

$$\begin{aligned} F(x, g_{n-1}(x) + \lambda x^n) &\equiv F(x, g_{n-1}(x)) + b\lambda x^n \\ &\equiv c_n x^n + b\lambda x^n \pmod{(x)^{n+1}} \end{aligned}$$

for some $c_n \in R$. From this we see that the only possibility is $\lambda = -b^{-1} c_n$. We conclude that

$$g = -x - c_2 x^2 - c_3 x^3 - \cdots$$

is the unique solution of $F(x, g(x)) = 0$. □

Corollary. (Inversion of series) *Let R be a ring, and let*

$$f = ax + \cdots \in R[[x]]$$

be a power series. If $a \in R^\times$, there is a unique power series $g \in R[[x]]$ such that $f(g(x)) = x$, and it also satisfies $g(f(x)) = x$.

Proof. We apply the inverse function theorem to $F(x, y) = x - f(y)$ to obtain a unique power series $g(x)$ with $F(x, g(x)) = x - f(g(x)) = 0$. We do the same for g instead of f to get a unique power series h with $g(h(x)) = x$; now

$$g(f(x)) = g(f(g(h(x)))) = g(h(x)) = x.$$ □

Proposition. *Let $F \in R[[x, y]]$ be a power series satisfying the axioms (1) and (2) above. Then F also satisfies (3) and (5).*

Proof. We will show that $F(x, 0) = x$; the proof that $F(0, y) = y$ is completely similar. Write $F(x, 0) = x + a_2x^2 + a_3x^3 + \cdots$; we will prove by complete induction on n that $a_2 = a_3 = \cdots = a_n = 0$. For $n = 1$, there is nothing to prove. Assuming the statement for some $n \geq 1$, we have

$$F(x, F(0, 0)) = F(x, 0) = x + a_{n+1}x^{n+1} + \cdots,$$

while

$$F(F(x, 0), 0) = F(x + a_nx^{n+1} + \cdots, 0) = (x + a_nx^{n+1}) + a_{n+1}x^{n+1} + \cdots;$$

since the two must be equal because of associativity, we conclude that $a_{n+1} = 0$.

The existence of a unique inverse follows directly from the implicit function theorem applied to $F(x, y)$. □

It can be shown that if R contains no torsion nilpotents (elements $x \neq 0$ such that $x^m = 0$ and $nx = 0$ for some $m, n > 0$), then (4) also follows from the first two axioms. The properties (1) and (3) are equivalent to saying that

$$F = x + y + xy \cdot (\text{power series in } x \text{ and } y).$$

Some important examples of formal group laws are:

(i) The additive formal group law over $\mathbf{Z}$: $G_\mathrm{a} = x + y$.

(ii) The multiplicative formal group law over $\mathbf{Z}$: $G_\mathrm{m} = (1 + x)(1 + y) - 1 = x + y + xy$.

(iii) The formal group law Σ associated to addition of points on an elliptic curve.

Definition. A *homomorphism of formal groups* from $\mathfrak{F}$ to $\mathfrak{G}$ over R is a power series $f \in R[[x]]$, without constant term, such that

$$f(F(x, y)) = G(f(x), f(y)).$$

Important examples of homomorphisms are the endomorphisms $[m]$ of a formal group $\mathfrak{F}$, defined recursively for all $m \in \mathbf{Z}$ in the following way:

$$\begin{aligned} [0](x) &= 0, \\ [m + 1](x) &= F([m](x), x) \quad (m \geq 0), \\ [m - 1](x) &= F([m](x), i(x)) \quad (m \leq 0). \end{aligned}$$

In particular, we see that $[1](x) = x$ and $[-1](x) = i(x)$.

Proposition. *For all $m \in \mathbf{Z}$, we have*

$$[m](x) = mx + \cdots.$$

Proof. We use induction on m. The case $m = 0$ is trivial; for $m > 0$ we have

$$[m](x) = F([m - 1](x), x) = (m - 1)x + x + \cdots = mx + \cdots,$$

and the case $m < 0$ is similar.

3. Groups associated to a formal group law

Let S be an R-algebra which is complete with respect to an ideal I. Then, because F has no constant term, the power series $F(x, y)$ converges to an element of I for all $x, y \in I$. It follows immediately from the properties (2)–(5) that the set I equipped with the operation $(x, y) \mapsto F(x, y)$ is an Abelian group; we denote it by $\mathfrak{F}(I)$.

If S is complete with respect to I, then it is also complete with respect to I^n for all $n \geq 1$, and the ideals $I \supseteq I^2 \supseteq I^3 \supseteq \cdots$ gives rise to a chain of subgroups

$$\mathfrak{F}(I) \supseteq \mathfrak{F}(I^2) \supseteq \mathfrak{F}(I^3) \supseteq \cdots.$$

We make $\mathfrak{F}(I)$ into a topological group by declaring these subgroups to be a basis for the open neighbourhoods of 0.

Let S and T be two R-algebras which are complete with respect to ideals I and J, and let $f\colon S \to T$ be an R-algebra homomorphism with $f(I) \subseteq J$. Then it is straightforward to check that f is continuous, and that the map

$$\mathfrak{F}(f)\colon \mathfrak{F}(I) \to \mathfrak{F}(J)$$

which is equal to f on the underlying sets is a continuous group homomorphism. This makes $\mathfrak{F}$ into a functor from a suitable "category of ideals of complete R-algebras" to the category of Abelian topological groups.

Proposition. *Let F be a formal group over law R, and let S be an R-algebra which is complete with respect to an ideal I. Then for each $n \geq 1$, the map*

$$\mathfrak{F}(I^n)/\mathfrak{F}(I^{n+1}) \to I^n/I^{n+1}$$

defined as the identity on the underlying sets is a group isomorphism. Furthermore, if S is a local ring with maximal ideal I, then the order of any torsion element of $\mathfrak{F}(I)$ is a power of p, where p is the residue characteristic of S. (If $p = 0$, this means that $\mathfrak{F}(I)$ is torsion-free.)

Proof. We know that the map in the first assertion is bijective, so it suffices to show that it is a homomorphism. This is clear because

$$F(x, y) \equiv x + y \pmod{I}^{2n}$$

for all $x, y \in I^n$.

For the second assertion, we have to show that there are no torsion elements of order m for any m not divisible by p, i.e. for any m not in the maximal ideal of S. We view $[m]$ as a power series with coefficients in S; because

$$[m] = mx + \cdots$$

and $m \in S^\times$, the lemma on inversion of series shows that there exists a power series $g \in S[[x]]$ without constant term such that $g([m](x)) = x$. Therefore the map $[m]$ is injective on $\mathfrak{F}(I)$, which was to be proved.