Introduction to Formal Group Laws
GRK Retreat 2024

Pengcheng Zhang

September 16, 2024

Heinrich Heine Universität Düsseldorf

BERGISCHE UNIVERSITÄT WUPPERTAL

RUHR UNIVERSITÄT BOCHUM

Definition

Let R be a commutative ring with identity.

Definition

A (one-dimensional) formal group $\mathscr{F}$ over R is given by a power series $F(x, y) \in R[[x, y]]$ satisfying the following axioms:

(1) $F(x, 0) = X, F(0, Y) = Y$(Identity).

(2) $F(x, F(y, z)) = F(F(x, y), z)$(Associativity).

If $F(x, y) = F(y, x)$ is also satisfied, the formal group $\mathscr{F}$ is said to be commutative.

Definition

Let R be a commutative ring with identity.

Definition

A (one-dimensional) formal group $\mathscr{F}$ over R is given by a power series $F(x, y) \in R[[x, y]]$ satisfying the following axioms:

(1) $F(x, 0) = X, F(0, Y) = Y$(Identity).

(2) $F(x, F(y, z)) = F(F(x, y), z)$(Associativity).

If $F(x, y) = F(y, x)$ is also satisfied, the formal group $\mathscr{F}$ is said to be commutative.

The existence of inverses is automatic. For a formal group law $F(x, y)$, the inverse $i(x)$ of x is determined by the equation $F(x, i(x)) = 0$.

Examples

•: The formal additive group, denoted by $\hat{\mathbb{G}}_a$, is given by the formal group law $F(x, y) = x + y$.

•: The formal multiplicative group, denoted by $\hat{\mathbb{G}}_m$, is given by $F(x, y) = x + y + xy$.

Examples

•: The formal additive group, denoted by $\hat{\mathbb{G}}_a$, is given by the formal group law $F(x, y) = x + y$.
•: The formal multiplicative group, denoted by $\hat{\mathbb{G}}_m$, is given by $F(x, y) = x + y + xy$.

Theorem

If $F(x, y)$ is a formal group law over R and $F(x, y) \in R[x, y]$, then $F(x, y) = x + y + cxy$ for some $c \in R$.

Examples

•: The formal additive group, denoted by $\hat{\mathbb{G}}_a$, is given by the formal group law $F(x, y) = x + y$.
•: The formal multiplicative group, denoted by $\hat{\mathbb{G}}_m$, is given by $F(x, y) = x + y + xy$.

Theorem

If $F(x, y)$ is a formal group law over R and $F(x, y) \in R[x, y]$, then $F(x, y) = x + y + cxy$ for some $c \in R$.

Theorem (Commutativity theorem)

Every one dimensional formal group law over a ring A is commutative if and only if A contains no element $a \neq 0$ that is both torsion and nilpotent.

Homomorphisms

Definition

Let $F(x, y), G(x, y)$ be two formal group laws over R. A homomorphism between them is a power series $f(T) \in R[[T]]$ such that

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

Homomorphisms

Definition

Let $F(x, y), G(x, y)$ be two formal group laws over R. A homomorphism between them is a power series $f(T) \in R[[T]]$ such that

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

Definition

A homomorphism $f(T)$ between two formal groups $F(x, y)$ and $G(x, y)$ over R is an isomorphism if there exists another power series $g(T)$ such that

$$f(g(T)) = g(f(T)) = T.$$

Examples of isomorphisms

Let $E(x)$ and $log(1+x)$ be the following power series

$$E(x) = \sum_{n=1}^{\infty} \frac{x^n}{n!}, log(1+x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n}.$$

Then they are isomorphisms between the additive formal group $\hat{\mathbb{G}}_a$ and the multiplicative formal group $\hat{\mathbb{G}}_m$ over $\mathbb{Q}$ and inverse to each other.

Examples of isomorphisms

Let $E(x)$ and $log(1+x)$ be the following power series

$$E(x) = \sum_{n=1}^{\infty} \frac{x^n}{n!}, log(1+x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n}.$$

Then they are isomorphisms between the additive formal group $\hat{\mathbb{G}}_a$ and the multiplicative formal group $\hat{\mathbb{G}}_m$ over $\mathbb{Q}$ and inverse to each other.

An interesting fact is, they are no longer isomorphisms when we replace $\mathbb{Q}$ with a field k of characteristic $p > 0$. To see this, we need the notion of $[n]$-series.

n-series

Definition

For each integer n and a given formal group law $F(x, y)$, the n-series is defined by

$$\begin{aligned} [1](x) &= x \\ [n](x) &= F(x, [n-1](x)), n > 1 \\ [-n](x) &= i([n](x)). \end{aligned}$$

Moreover, they satisfy

$$\begin{aligned} [n](x) &\equiv nx \mod x^2 \\ [m+n](x) &= F([m](x), [n](x)) \\ [mn](x) &= [m]([n](x)) \end{aligned}$$

Example

For the formal group $\hat{\mathbb{G}}_a$, one can easily check that $[n]_{\hat{\mathbb{G}}_a}(x) = nx$, for $n \geq 0$.

Example

For the formal group $\hat{\mathbb{G}}_a$, one can easily check that $[n]_{\hat{\mathbb{G}}_a}(x) = nx$, for $n \geq 0$.

Example

For the formal group $\hat{\mathbb{G}}_m$, one can easily check that $[n]_{\hat{\mathbb{G}}_m}(x) = (1+x)^n - 1$.

n-series

Example

For the formal group $\hat{\mathbb{G}}_a$, one can easily check that $[n]_{\hat{\mathbb{G}}_a}(x) = nx$, for $n \geq 0$.

Example

For the formal group $\hat{\mathbb{G}}_m$, one can easily check that $[n]_{\hat{\mathbb{G}}_m}(x) = (1+x)^n - 1$.

Suppose $\hat{\mathbb{G}}_a$ and $\hat{\mathbb{G}}_m$ are isomorphic over a field k of characteristic $p > 0$. Then there exists a power series $\alpha(x) = b_1 x + b_2 x^2 + \cdots \in k[[x]]$ with $b_1 \neq 0$ such that $[p]_{\hat{\mathbb{G}}_a}(\alpha(x)) = \alpha([p]_{\hat{\mathbb{G}}}(x)) = \alpha(x^p)$ because all the coefficients of x^a with $1 \leq a < p$ are 0 modulo p.

Groups associated to formal groups

Let Γ be the set of power series $\gamma(t) \in R[[t]]$ that don't have constant terms, i.e. $\gamma(t) = b_1 t + b_2 t^2 + \cdots$. Given two such power series $\gamma_1(t), \gamma_2(t)$, the power series $F(\gamma_1(t), \gamma_2(t))$ is in Γ. Define the addition on Γ to be $\gamma_1(t) + \gamma_2(t) = F(\gamma_1(t), \gamma_2(t))$. Then Γ becomes a group, denoted by $\mathscr{C}(F)$.

Groups associated to formal groups

Let Γ be the set of power series $\gamma(t) \in R[[t]]$ that don't have constant terms, i.e. $\gamma(t) = b_1 t + b_2 t^2 + \cdots$. Given two such power series $\gamma_1(t), \gamma_2(t)$, the power series $F(\gamma_1(t), \gamma_2(t))$ is in Γ. Define the addition on Γ to be $\gamma_1(t) + \gamma_2(t) = F(\gamma_1(t), \gamma_2(t))$. Then Γ becomes a group, denoted by $\mathscr{C}(F)$.

If $F(x, y)$ is commutative, so is Γ.

Groups associated to formal groups

Let Γ be the set of power series $\gamma(t) \in R[[t]]$ that don't have constant terms, i.e. $\gamma(t) = b_1 t + b_2 t^2 + \cdots$. Given two such power series $\gamma_1(t), \gamma_2(t)$, the power series $F(\gamma_1(t), \gamma_2(t))$ is in Γ. Define the addition on Γ to be $\gamma_1(t) + \gamma_2(t) = F(\gamma_1(t), \gamma_2(t))$. Then Γ becomes a group, denoted by $\mathscr{C}(F)$.

If $F(x, y)$ is commutative, so is Γ.

Example

We take F to be the multiplicative formal group law. Then $\mathscr{C}(F)$ is the underlying additive group of the ring of Witt vectors $W(R)$.

Universal formal group law

Let A, B be two rings and $\phi : A \to B$ be a ring homomorphism. Then given a formal group law $F(x, y) = x + y + \sum_{(i,j) \gneqq (1,1)} c_{i,j} x^i y^j$ over A, we can construct another formal group law over B:

$$\phi_* F(x, y) = x + y + \sum_{(i,j) \gneqq (1,1)} \phi(c_{i,j}) x^i y^j.$$

Universal formal group law

Let A, B be two rings and $\phi : A \to B$ be a ring homomorphism. Then given a formal group law $F(x, y) = x + y + \sum_{(i,j) \gneqq (1,1)} c_{i,j} x^i y^j$ over A, we can construct another formal group law over B:

$$\phi_* F(x, y) = x + y + \sum_{(i,j) \gneqq (1,1)} \phi(c_{i,j}) x^i y^j .$$

Q: Is there a universal formal group law over a ring from which all other formal group laws over a ring can be derived?

Universal formal group law

Let A, B be two rings and $\phi : A \to B$ be a ring homomorphism. Then given a formal group law $F(x,y) = x + y + \sum_{(i,j)\gneqq(1,1)} c_{i,j}x^i y^j$ over A, we can construct another formal group law over B:

$$\phi_* F(x,y) = x + y + \sum_{(i,j)\gneqq(1,1)} \phi(c_{i,j})x^i y^j.$$

Q: Is there a universal formal group law over a ring from which all other formal group laws over a ring can be derived?
A: Such a universal formal group law exists over a certain ring L called the Lazard ring!

n-dimensional formal group law

Definition

An n-dimensional formal group law over a ring A is an n-tuple of power series $F(X, Y) = (F_1(X, Y), F_2(X, Y), \ldots, F_n(X, Y))$ in $2n$ variables $X = (X_1, \ldots, X_n)$, $Y = (Y_1, \ldots, Y_n)$ such that

- $F_k(X, Y) = X_k + Y_k \mod \deg 2 \text{ terms}.$
- $F_k(F(X, Y), Z) = F_k(X, F(Y, Z)).$

As in the one-dimensional case, there exists an n-tuple of power series $i(X) = (i_1(X), \ldots, i_n(X))$ such that $F(X, i(X)) = 0$.

n-dimensional formal group law

Definition

An n-dimensional formal group law over a ring A is an n-tuple of power series $F(X, Y) = (F_1(X, Y), F_2(X, Y), \ldots, F_n(X, Y))$ in $2n$ variables $X = (X_1, \ldots, X_n)$, $Y = (Y_1, \ldots, Y_n)$ such that

- $F_k(X, Y) = X_k + Y_k \mod \deg 2 \text{ terms.}$
- $F_k(F(X, Y), Z) = F_k(X, F(Y, Z))$.

As in the one-dimensional case, there exists an n-tuple of power series $i(X) = (i_1(X), \ldots, i_n(X))$ such that $F(X, i(X)) = 0$.

Again, we can expect a universal n-dimensional formal group law, and it indeed exists.

Example

The *n*-dimensional additive formal group law $\hat{\mathbb{G}}_a^n(X, Y) = X + Y$.

Examples

Example

The n-dimensional additive formal group law $\hat{\mathbb{G}}_a^n(X, Y) = X + Y$.

Example

An anonymous 4-dimensional formal group law:

$$
\begin{aligned}
F_1(X, Y) &= X_1 + Y_1 + X_1 Y_1 + X_2 Y_3 \\
F_2(X, Y) &= X_2 + Y_2 + X_1 Y_2 + X_2 Y_4 \\
F_3(X, Y) &= X_3 + Y_3 + X_3 Y_1 + X_4 Y_3 \\
F_4(X, Y) &= X_4 + Y_4 + X_3 Y_2 + X_4 Y_4
\end{aligned}
$$

Infinite dimensional formal group laws

Definition

An (infinite) dimensional formal group law with (possibly infinite) index set I over a ring A consists of power series $F_i(X,Y) = \sum_{\mathbf{m},\mathbf{n}} c^i_{\mathbf{m},\mathbf{n}} X^{\mathbf{m}} Y^{\mathbf{n}} \in A[[X_i, Y_i; i \in I]]$ one for each $i \in I$, such that

- $F_i(X,Y) \equiv X_i + Y_i, \mod \deg 2 \text{ terms}, \forall i \in I$.
- For every $\mathbf{m}, \mathbf{n}$ there are only finitely many $i \in I$ such that $c^i_{\mathbf{m},\mathbf{n}} \neq 0$.
- $F_i(F(X,Y),Z) = F_i(X, F(Y,Z)), \forall i \in I$.

Infinite dimensional formal group laws

Definition

An (infinite) dimensional formal group law with (possibly infinite) index set I over a ring A consists of power series $F_i(X,Y) = \sum_{\mathbf{m},\mathbf{n}} c^i_{\mathbf{m},\mathbf{n}} X^{\mathbf{m}} Y^{\mathbf{n}} \in A[[X_i, Y_i; i \in I]]$ one for each $i \in I$, such that

- $F_i(X,Y) \equiv X_i + Y_i, \mod \deg 2 \text{ terms}, \forall i \in I$.
- For every $\mathbf{m}, \mathbf{n}$ there are only finitely many $i \in I$ such that $c^i_{\mathbf{m},\mathbf{n}} \neq 0$.
- $F_i(F(X,Y),Z) = F_i(X, F(Y,Z)), \forall i \in I$.

Unfortunately, there doesn't exist a universal infinite dimensional formal group law, because there's no way to predict which finitely many $c^i_{\mathbf{m},\mathbf{n}}$ are non-zero.

Construction of formal group laws

There are many ways to construct a formal group law. Below is an example of it that is quite different from the "trivial" ones discussed below.

Construction of formal group laws

There are many ways to construct a formal group law. Below is an example of it that is quite different from the "trivial" ones discussed below.

Let R be a ring of characteristic 0. Let $f(x) \in R \otimes \mathbb{Q}$ be a power series of the form $f(x) = x + a_2x^2 + \cdots$. Then it has an inverse power series $f^{-1}(x)$. Now define

$$F(x, y) = f^{-1}(f(x) + f(y)).$$

Construction of formal group laws

There are many ways to construct a formal group law. Below is an example of it that is quite different from the "trivial" ones discussed below.

Let R be a ring of characteristic 0. Let $f(x) \in R \otimes \mathbb{Q}$ be a power series of the form $f(x) = x + a_2 x^2 + \cdots$. Then it has an inverse power series $f^{-1}(x)$. Now define

$$F(x, y) = f^{-1}(f(x) + f(y)).$$

One can easily verify that it satisfies commutativity, associativity, and the inverse is given by $i(x) = f^{-1}(-f(x))$. Such a power series $f(x)$ is called the logarithm of $F(x, y)$.

Construction of formal group laws

The formal group law constructed above is not an interesting one because it's always isomorphic (via $f(x)$) to the additive formal group law $\hat{\mathbb{G}}_a$ over the ring $R \otimes \mathbb{Q}$.

Construction of formal group laws

The formal group law constructed above is not an interesting one because it's always isomorphic (via $f(x)$) to the additive formal group law $\hat{\mathbb{G}}_a$ over the ring $R \otimes \mathbb{Q}$.
However, if $f(x)$ satisfies a collection of functional equations(one for each prime p), the associated $F(x, y)$ has coefficients in $R \subset R \otimes \mathbb{Q}$.

Construction of formal group laws

The formal group law constructed above is not an interesting one because it's always isomorphic (via $f(x)$) to the additive formal group law $\hat{\mathbb{G}}_a$ over the ring $R \otimes \mathbb{Q}$.
However, if $f(x)$ satisfies a collection of functional equations(one for each prime p), the associated $F(x, y)$ has coefficients in $R \subset R \otimes \mathbb{Q}$.

Given a power series $g(x) = \sum_{i=1}^{\infty} b_i x^i$ with b_1 invertible in R, we have a new power series depending on $g(x)$:

$$f_g(x) = g(x) + \sum_{i=1}^{\infty} s_i \sigma_*^i f_g(x^{q^i}) \in R \otimes \mathbb{Q}[[x]]$$

which makes $F_g(x, y) = f_g^{-1}(f_g(x) + f_g(y))$ a formal group law over R.

Construction of formal group laws

The setup for this procedure is as follows:
A is a subring of K, $\sigma : K \to K$ is a ring homomorphism, $\mathfrak{a}$ is an ideal of A, p is a prime number, q is a power of p, $s_1, s_2, \ldots$ are elements in K.
These ingredients are required to satisfy the following relations:

$$\sigma(A) \subset A, \sigma(a) \equiv a^q \mod \mathfrak{a}, \forall a \in A, p \in \mathfrak{a}, s_i\mathfrak{a} \subset A, i = 1, 2, \ldots.$$

In addition, we require

$$\mathfrak{a}^r b \subset \mathfrak{a} \Rightarrow \mathfrak{a}^r \sigma(b) \subset \mathfrak{a}$$

for all positive integer r and $b \in K$.

Construction of formal group laws

Functional equation-integrality lemma: Assume all the conditions in the previous page, and in addition let $g(x) = \sum_{i=1}^{\infty} b_i x^i, \bar{g}(x) = \sum_{i=1}^{\infty} \bar{b}_i x^i$ be two power series over A. Then we have

(i) the formal group law $F_g(x, y) = f_g^{-1}(f_g(x) + f_g(y))$ has its coefficients in A.

(ii) the power series $f_g^{-1}(f_{\bar{g}}(x))$ has its coefficients in A.

(iii) if $h(X) = \sum_{n=1}^{\infty} c_n x^n$ is a power series with coefficients in A, then there is a power series $\hat{h}(x) = \sum_{n=1}^{\infty} \hat{c}_n x^n$ with $\hat{c}_n \in A$ such that $f_g(h(x)) = f_{\hat{h}}(x)$.

(iv) if $\alpha(x) \in A[[x]], \beta(x) \in K[[x]]$ are two power series with coefficients in A and K respectively and r is a positive integer, then we have

$$\alpha(x) \equiv \beta(x) \mod \mathfrak{a}^r A[[x]] \Leftrightarrow f_g(\alpha(x)) \equiv f_g(\beta(x)) \mod \mathfrak{a}^r A[[x]].$$

For example, a set of ingredients can be

$$A = \mathbb{Z}_{(p)}, K = \mathbb{Q}, \sigma = id, \mathfrak{a} = p\mathbb{Z}_{(p)},$$
$$q = p, s_1 = p^{-1}, s_2 = s_3 = \cdots = 0.$$

We set $g(x) = x$, and $\bar{g}(x) = \sum_{(n,2)=1} n^{-1}(x^n - x^{2n})$ if $p = 2$ and $\bar{g}(x) = \sum_{(n,p)=1}(-1)^{n+1}n^{-1}x^n$ if $p > 2$. Then we have

$$f_g(x) = x + p^{-1}x^p + p^{-2}x^{p^2} + \cdots := H(x)$$
$$f_{\bar{g}}(x) = \log(1+x) = \sum_{n=1}^{\infty}(-1)^{n+1}\frac{x^n}{n} := l(x)$$

By Functional equation-integrality lemma, the power series $Exp(H(x))$ has coefficients in A.

Construction of formal group laws

By giving different sets of ingredients, we can produce many non-isomorphic formal group laws. Some other options are:

$$A = \mathbb{Z}, K = \mathbb{Q}, \sigma = id, q = p, \mathfrak{a} = p\mathbb{Z}, s_i \in p\mathbb{Z}$$

Construction of formal group laws

By giving different sets of ingredients, we can produce many non-isomorphic formal group laws. Some other options are:

$$A = \mathbb{Z}, K = \mathbb{Q}, \sigma = id, q = p, \mathfrak{a} = p\mathbb{Z}, s_i \in p\mathbb{Z}$$

$$A = \mathbb{Z}[V_1, V_2, \dots; W_1, W_2, \dots] = \mathbb{Z}[\mathbf{V}, \mathbf{W}], K = \mathbb{Q}[\mathbf{V}, \mathbf{W}]$$
$$\sigma/\mathbb{Q} : K \to K, V_i \mapsto V_i^p, W_i \mapsto W_i^p, q = p, \mathfrak{a} = pA,$$
$$s_i = p^{-1} V_i, g(X) = X, \bar{g}(X) = X + \sum_{i=1}^{\infty} W_i X^{q^i}$$