FORMAL GROUPS OVER DISCRETE VALUATION RINGS

CHRIS HURLBURT

Abstract. This white paper contains some supplementary material to the theory of formal groups over discrete valuation rings. The material contained is without doubt common knowledge, though not necessarily explicitly written in the texts in the references. The approach is exactly that found in chapter four of [2].

1

Let R be a discrete valuation ring with residue field k of characteristic p for p a prime number. An n-dimensional commutative formal group law over R is an n-tuple of power series

$$F(X,Y) = (F_1(X,Y), \ldots, F_n(X,Y))$$

where $F_i(X,Y) \in R[[X,Y]]$, $X = (X_1, \ldots X_n)$, $Y = (Y_1, \ldots, Y_n)$, and

$$\begin{aligned} F_i(X,Y) &\equiv X_i + Y_i \mod \deg 2 \\ F_i(F(X,Y),Z) &= F_i(X,F(Y,Z)) \\ F_i(X,Y) &= F_i(Y,X) \end{aligned}$$

as defined on page 51 in [1]. Then as an exercise analogous to those in [2], we can show

$$\begin{aligned} F(X,0) &= X \\ F(0,Y) &= Y \end{aligned}$$

This implies that $F_i(X,0) = X_i$ which in turn implies that every term of degree 2 or higher contains at least one Y_k. Similarly $F_i(0,Y) = Y_i$ and so every term of degree 2 or higher in the power series F_i contains at X_k element. We will refer the formal group associated to the formal group law by $\mathcal{F}$ or by $F(X,Y)$ itself.

A morphism of formal groups from an n-dimensional formal group with n-tuple of power series denoted by F to an m-dimensional formal group with m-tuple of power series denoted by G is an m-tuple of power series $\theta_i \in R[T]$ where T is a n-tuple such that

$$G(\theta(X), \theta(Y)) = \theta(F(X,Y))$$

Date: January, 2003.
1991 *Mathematics Subject Classification.* 11,14.

for X, Y m-tuples and $\theta = (\theta_1, \ldots, \theta_m)$. Let $[m]_F : F(X,Y) \to F(X,Y)$ for $n \in \mathbb{N}$ be the endomorphism defined by

$$\begin{aligned}[0]_F(X) &= 0\\ [1]_F(X) &= X\\ [m]_F(X) &= F(X, [m-1]_F(X)) \text{ if } m \geq 2\end{aligned}$$

In cases when the formal group clearly implied, we will refer to the this endomorphism by $[m]$.

Proposition 1.1. *Let $F(X,Y)$ be an n-dimensional formal group over R and let $m \in \mathbb{Z}$, $m \geq 0$. Then*

$$[m](X) = (mX_1, mX_2, \ldots, mX_n) \mod \deg 2$$

Proof. Induction. □

Definition 1.2. An invariant differential of an n-dimensional formal group $F(X,Y)$ is the 'differential form'

$$\omega = P(T)DT$$

where $P(T)$ is an $n \times n$ matrix of power series in n variables and DT is the total derivative of T (also an $n \times n$ matrix) that satisfies the condition

$$\omega(F(T,Y)) = \omega(T).$$

Remark 1.3. The last condition is equivalent to

$$P(F(T,Y))DF_T(T,Y) = P(T) \tag{1.1}$$

where DF_T is the $n \times n$ derivative matrix of F with respect to T.

If we substitute $T = 0$ into equation 1.1, then we get

$$P(Y)DF_T(0,Y) = P(0) \tag{1.2}$$

where

$$DF_T(0,Y) = \begin{bmatrix} \frac{\partial F_1}{\partial T_1}(0,Y) & \cdots & \frac{\partial F_1}{\partial T_n}(0,Y) \\ \vdots & \ddots & \vdots \\ \frac{\partial F_n}{\partial T_1}(0,Y) & \cdots & \frac{\partial F_n}{\partial T_n}(0,Y) \end{bmatrix}.$$

Note that modulo degree 1, the matrix $DF_T(0,Y)$ is the identity and hence is invertible. Therefore it is possible to solve equation 1.2 for $P(Y)$.

$$P(Y) = P(0)\left[DF_X(0,Y)\right]^{-1} \tag{1.3}$$

Now we note that any two functions ω differ by at most an $n \times n$ constant matrix.

Next we verify that the function $P(Y)$ given by equation 1.3 when used in the invariant differential satisfies the invariant differential condition of $\omega(F(T,Y)) = \omega(T)$. If we differentiate

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

with respect to X we have

$$\begin{bmatrix} \frac{\partial F_1}{\partial X_1}(X, F(Y,Z)) & \dots & \frac{\partial F_1}{\partial X_n}(X, F(Y,Z)) \\ \vdots & \ddots & \vdots \\ \frac{\partial F_n}{\partial X_1}(X, F(Y,Z)) & \dots & \frac{\partial F_n}{\partial X_n}(X, F(Y,Z)) \end{bmatrix}$$
$$= \begin{bmatrix} \frac{\partial F_1}{\partial X_1}(Y,Z) & \dots & \frac{\partial F_1}{\partial X_n}(Y,Z) \\ \vdots & \ddots & \vdots \\ \frac{\partial F_n}{\partial X_1}(Y,Z) & \dots & \frac{\partial F_n}{\partial X_n}(Y,Z) \end{bmatrix} \begin{bmatrix} \frac{\partial F_1}{\partial X_1}(X,Y) & \dots & \frac{\partial F_1}{\partial X_n}(X,Y) \\ \vdots & \ddots & \vdots \\ \frac{\partial F_n}{\partial X_1}(X,Y) & \dots & \frac{\partial F_n}{\partial X_n}(X,Y) \end{bmatrix}$$

More succinctly if DF_X is the operator

$$DF_X = \begin{bmatrix} \frac{\partial F_1}{\partial X_1} & \dots & \frac{\partial F_1}{\partial X_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial F_n}{\partial X_1} & \dots & \frac{\partial F_n}{\partial X_n} \end{bmatrix}$$

then applying this operator to the associative law gives

$$DF_X(F(X,Y),Z)DF_X(X,Y) = DF_X(X, F(Y,Z)).$$

So when $X = 0$, this becomes

$$DF_X(Y,Z)DF_X(0,Y) = DF_X(0, F(Y,Z)).$$

Therefore

$$[DF_X(0, F(Y,Z))]^{-1} DF_X(Y,Z) = [DF_X(0,Y)]^{-1}.$$

Substituting equation 1.3 into each side of equation 1.1 we have

$$P(0)[DF_X(0, F(T,Y))]^{-1} DF_X(T,Y)$$

and

$$P(0)[DF_X(0,T)]^{-1}$$

which are equal by our computations with the associative law and hence the invariant differential condition $\omega(F(T,Y)) = \omega(T)$ is satisfied.

Definition 1.4. We say an invariant differential is normalized if $P(0) = I$ where I is the $n \times n$ identity matrix.

Corollary 1.5. *The normalized invariant differential of an n-dimensional formal group $F(X,Y)$ is unique. Any other invariant differential of $F(X,Y)$ differs from the normalized invariant differential by an $n \times n$ matrix with coefficients in R.*

Corollary 1.6. *Let $F(X,Y)$, $G(X,Y)$ be n-dimensional formal groups and let ω_F, ω_G be the respective normalized invariant differentials. Let $f : F(X,Y) \to G(X,Y)$ be a homomorphism. Then $\omega_G \circ f = Df(0)\omega_F$ where Df is the $n \times n$ derivative matrix of f.*

Proof.

$$\begin{aligned} \omega_G(f(F(T,X))) &= \omega_G(G(f(T), f(S)) \\ &= \omega_G(f(T)) \end{aligned}$$

Hence $\omega_G \circ f$ satisfies the property of an invariant differential of F. So $\omega_G \circ f = A\omega_F$ where A is an $n \times n$ matrix. This means

$$[DG_X(0, f(T))]^{-1} Df(T) = A[DF_X(0, T)]^{-1}$$

and so

$$A = [DG_X(0, f(T))]^{-1} Df(T) DF_X(0, T).$$

Substituting $T = 0$, we get $A = Df(0)$.

□

Corollary 1.7. *Let $F(X, Y)$ be an n-dimensional formal group. Let $p \in \mathbb{Z}$ be prime. Then*

$$[p](T) = (pf_1(T) + g_1(T^P), \ldots, pf_n(T) + g_n(T^p))$$

where f_i, g_i are all power series in n-variables and $T^p \overset{def}{=} (T_1^p, T_2^p, \ldots, T_n^p)$ (by abuse of notation). Moreover for each $1 \leq i \leq n$, $f_i(0) = 0 = g_i(0)$.

Proof. Let ω be the normalized invariant differential of $F(X, Y)$. We know $[p](X) = (pX_1, pX_2, \ldots pX_n) \mod \deg 2$. So

$$D[p] = \begin{bmatrix} p & 0 & \ldots & 0 \\ 0 & p & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & p \end{bmatrix} \mod \deg 1$$

Hence $D[p](0) = pI$ where I is the $n \times n$ identity matrix. By the previous corollary $\omega_F \circ [p] = pI\omega_F$ or $[DF_X(0, [p](T))]^{-1} D[p](T) = pI[DF_X(0, T)]^{-1}$. Therefore

$$\begin{aligned} D[p](T) &= p[DF_X(0, [p](T))][DF_X(0, T)]^{-1} \\ &= pM \end{aligned}$$

where M is some matrix. So for any pair ij

$$\frac{\partial [p]_i}{\partial T_j} = ph(T)$$

for some power series in n-variables $h(T)$. Let $aT_1^{k_1} T_n^{k_2} \ldots T_n^{k_n}$ be a term in $[p]_i$ such that it is the only term with exponent $(k_1, k_2, \ldots, k_n)$. We look at what happens to this term under partial derivatives

partial of $[p]_i$ w.r.t.	term resulting from $aT_1^{k_1} T_n^{k_2} \ldots T_n^{k_n}$
T_1	$ak_1 T_1^{k_1 - 1} T_n^{k_2} \ldots T_n^{k_n}$
T_2	$ak_2 T_1^{k_1} T_n^{k_2 - 1} \ldots T_n^{k_n}$
$\vdots$	
T_n	$ak_n T_1^{k_1} T_n^{k_2} \ldots T_n^{k_n - 1}$

In each of these cases we note that p must divide the coefficient in the second column. So if $p|a$, we are done. Otherwise p must divide all of $k_1, \ldots, k_n$. Hence we can split $[p]_i$ into two parts:

$$[p]_i = pf_i(T) + g_i(T^p).$$

We note that by our sorting method, g_i does not contain a constant term so $g_i(0) = 0$. However, $[p]_i(0) = 0$ so $f_i = 0$. We can do this for $1 \leq i \leq n$ completing the proof. □

Corollary 1.8. *Let $F(X, Y)$ be an n-dimensional formal group. Let $p \in \mathbb{Z}$ be prime and let k be a positive integer. Then*

$$[p^k]_i(X) = p^k\phi_{ik}(X)+p^{k-1}\phi_{ik-1}(X_1^p, \ldots, X_n^p)+p^{k-2}\phi_{ik-2}(X_1^{p^2}, \ldots, X_n^{p^2})+\ldots+\phi_{i0}(X_1^{p^k}, \ldots, X_k^{p^k})$$

where ϕ_{ij} are all power series in n-variables with $\phi_{ij}(0) = 0$.

Proof. We proceed by induction. For the case $k = 1$, we refer to corollary 1.7. For ease of notation we define $X^{p^j} \stackrel{def}{=} (X_1^{p^j}, X_2^{p^j}, \ldots, X_n^{p^j})$. Suppose $[p^k]_i(X) = p^k\psi_{ik}(X)+p^{k-1}\psi_{ik-1}(X^p)+ p^{k-2}\psi_{ik-2}(X^{p^2}) + \ldots + \psi_{i0}(X^{p^k})$ for $1 \leq i \leq n$. Consider

$$\begin{aligned}
[p^{k+1}](X) &= [p] \circ [p^{k+1}](X) \\
&= [p]\left(p^k\psi_{1k}(X) + \ldots + \psi_{10}(X^{p^k}), \ldots, p^k\psi_{nk}(X) + \ldots + \psi_{n0}(X^{p^k})\right) \\
&= \Bigg(pf_1\left(p^k\psi_{1k}(X) + \ldots + \psi_{10}(X^{p^k}), \ldots, p^k\psi_{nk}(X) + \ldots + \psi_{n0}(X^{p^k})\right) \\
&\quad + g_1\left((p^k\psi_{1k}(X) + \ldots + \psi_{10}(X^{p^k}))^p, \ldots, (p^k\psi_{nk}(X) + \ldots + \psi_{n0}(X^{p^k})^p)\right), \\
&\quad \ldots, \\
&\quad + pf_n\left(p^k\psi_{1k}(X) + \ldots + \psi_{10}(X^{p^k}), \ldots, p^k\psi_{nk}(X) + \ldots + \psi_{n0}(X^{p^k})\right) \\
&\quad + g_n\left((p^k\psi_{1k}(X) + \ldots + \psi_{10}(X^{p^k}))^p, \ldots, (p^k\psi_{nk}(X) + \ldots + \psi_{n0}(X^{p^k})^p)\right)\Bigg)
\end{aligned}$$

The induction follows by rearrangement and then by noting that none of the resulting power series could have a constant term, we have $\phi_{ij}(0) = 0$. □

2

Let $\mathfrak{m}$ be the maximal ideal of R. An n-dimensional commutative formal group when applied to n-tuples of elements in $\mathfrak{m}R$ forms a group. For the rest of this section, whenever we refer to an n-tuple X, we will assume that it is an n-tuple of elements in $\mathfrak{m}R$ and for this section we will fix the non-zero n-tuple x throughout.

Let $\nu : R \to R$ be the valuation. Let j be the index such that

$$\nu(x_j) = \min\{\nu(x_i) | 1 \leq i \leq n\}$$

Proposition 2.1. *Suppose there exists an integer m such that $[p^m](x) = 0$ but $[p^{m-1}](x) \neq 0$. Then*

$$\nu(x_j) \leq \frac{\nu(p)}{p-1}.$$

Proof. Using corollary 1.8,

$$[p^m]_j(x) = p^m\phi_{jm}(x) + p^{m-1}\phi_{jm-1}(x^p) + \ldots + \phi_{j0}(x^{p^m}) = 0.$$

In addition $[p^m]_j(x) \equiv p^m x_j \mod \deg 2$. Now we note that every term in $\phi_{jm}(x)$ of $\deg 2$ or higher will have valuation higher than the valuation of x_j. So for the term $p^m x_j$ to cancel, its valuation must be equal to the valuation of a term from some ϕji for $1 \leq i < m$. The minimum possible valuation for any term in ϕ_{ji} is $\nu(x_j^{p^{m-i}})$. So

$$\nu(p^m x_j) \geq \min\{\nu(p^{m-1}x_j^p), \nu(p^{m-2}x_j^{p^2}), \ldots, \nu(px_j^{p^{m-1}}), \nu(x_j^{p^m})\}.$$

Suppose i is the index of the minimum value on the right. Then

$$\nu(p^m x_j) \geq \nu(p^{m-i}x_j^{p^i})$$

implying

$$\frac{i\nu(p)}{p^i - 1} \geq \nu(x_j).$$

Lastly note

$$\frac{\nu(p)}{p-1} \geq \frac{i\nu(p)}{p^i-1} \geq \nu(x_j).$$

□

The following are immediate consequences of the proposition.

Corollary 2.2. *Suppose there exists an integer m such that $[p^m](x) = 0$ but $[p^{m-1}](x) \neq 0$. Then*

$$\min\{\nu(px_j), \nu(x_j^p)\} = \nu(x_j^p)$$

or

$$p\nu(x_j) \leq \nu(p) + \nu(x_j) = \nu(px_j).$$

Corollary 2.3. *Suppose there exists an integer m such that $[p^m](x) = 0$ but $[p^{m-1}](x) \neq 0$. Then for all $1 \leq i \leq n$,*

$$\nu([p]_i(x) \geq \nu(x_j^p) = p\nu(x_j).$$

Proof.

$$[p]_i(x) = pf_i(x) + g_i(x^p)$$

implying

$$\nu([p]_i(x)) = \nu\left(pf_i(x) + g_i(x^p)\right)$$
$$\nu([p]_i(x)) \geq \min\{\nu(px_j), \nu(x_j^p)\} = \nu(x_j^p)$$

□

Using corollary 2.3, we can induct to show

Proposition 2.4. *Suppose there exists an integer m such that $[p^m](x) = 0$ but $[p^{m-1}](x) \neq 0$. Then for all $1 \leq i \leq n$,*

$$\nu\left([p^k]_i(x)\right) \geq p^k \nu(x_j).$$

Proof. Induction. Case $k = 1$ follows from corollary 2.3. Suppose $k = 2$. For $1 \leq i \leq n$,

$$[p^2]_i(x) = [p]_i([p](x)).$$

So we can choose l such that

$$\nu([p]_l(x)) = \min\{\nu([p]_i(x)) : 1 \leq i \leq n\}.$$

Then

$$\begin{aligned} \nu\left([p]_i([p](x))\right) &\geq p\nu([p]_l(x)) \\ \nu\left([p^2]_i(x)\right) &\geq p\nu([p]_l(x)) \geq p(p\nu(x_j)) \\ \nu\left([p^2]_i(x)\right) &\geq p^2\nu(x_j). \end{aligned}$$

Suppose that for all $1 \leq i \leq n$, $\nu\left([p^{k-1}]_i(x)\right) \geq p^{k-1}\nu(x_j)$. Then

$$[p^k]_i(x) = [p]_i([p^{k-1}](x)).$$

Let l be such that

$$\nu([p^{k-1}]_l(x)) = \min\{\nu([p^{k-1}]_i(x)) : 1 \leq i \leq n\}.$$

Then

$$\begin{aligned} \nu\left([p]_i([p^{k-1}](x))\right) &\geq p\nu([p^{k-1}]_l(x)) \\ \nu\left([p^k]_i(x)\right) &\geq p\nu([p^{k-1}]_l(x)) \geq p(p^{k-1}\nu(x_j)) \\ \nu\left([p^k]_i(x)\right) &\geq p^k\nu(x_j). \end{aligned}$$

The proposition follows from induction. □

We can now prove the following theorem.

Theorem 2.5. *Suppose there exists an integer m such that $[p^m](x) = 0$ but $[p^{m-1}](x) \neq 0$. Then*

$$p^{m-1}\nu(x_j) \leq \frac{\nu(p)}{p-1}.$$

Proof. Choose l such that

$$\nu\left([p^{m-1}]_l(x)\right) = \min\{\nu([p^{m-1}]_i(x)) : 1 \leq i \leq n\}.$$

(Note: This means $[p^{m-1}]_l(x) \neq 0$.) Now

$$\begin{aligned} 0 = [p]_i\left([p^{m-1}]_l(x)\right) &= pf_i([p^{m-1}](x)) + g_i(([p^{m-1}](x))^p) \\ &= p[p^{m-1}]_l(x) \mod \deg 2 \text{ considering } [p^{m-1}]_l(x) \text{ as the variables.} \end{aligned}$$

In order for the element $p[p^{m-1}]_l(x)$ to be cancelled in a discrete valuation ring

$$\nu(p[p^{m-1}]_l(x)) \geq \nu\left(([p^{m-1}]_l(x))^p\right)$$

implying

$$[p^{m-1}]_l(x) \leq \frac{\nu(p)}{p-1}.$$

Combining this inequality with the inequality from the previous proposition

$$p^{m-1}\nu(x_j) \leq \frac{\nu(p)}{p-1}.$$

□

References

1. M. Hazewinkel, *Formal Groups and Applications*, Pure and Applied Mathematics, vol. 78, Academic Press, 1978.
2. J. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, vol. 106, Springer Verlag, 1986.

Department of Mathematical Sciences, Northern Illinois University, DeKalb, Illinois 60115

E-mail address: hurlburt@math.niu.edu