ONE-DIMENSIONAL FORMAL GROUPS

CARL ERICKSON

In this Wednesday night section for Algebraic Number Theory, we will go through basic facts about one dimensional formal groups and hopefully get to see how they might be useful and interesting. All rings are commutative with identity.

The sources of this material are my notes from Elliptic Curves, a course taught by Tom Fisher at Cambridge last year, J. Silverman's Elliptic Curves Book. A few things I worked out myself though they're surely out there somewhere.

1. Definitions and Basic Properties

Formal groups may look a bit, well, formal, and not particularly interesting at first, but that's not true. In the next section I'll give some intuition for how to think of them and a few hints of their usefulness. For now, just the facts.

Definition 1.1. Let A be a ring. A *one dimensional formal group law* over A is a power series $F(X,Y) \in A[\![X,Y]\!]$ with the following properties

- $F(X,Y) = X + Y +$ higher degree terms
- $F(X,F(Y,Z)) = F(F(X,Y),Z)$ (associativity).

If in addition $F(X,Y) = F(Y,X)$, then F is called *commutative*.

From now on we will omit "one-dimensional" and work only with one-dimensional formal group laws. If you're interested in seeing an interesting formal group law that's more than one dimensional, look at the Witt vectors defined in class.

One often expresses the first property in the definition by saying that

$$F(X,Y) \equiv X + Y \pmod{\deg 2}.$$

The formal group law axioms imply the following properties of formal groups, namely the identity and inverse axioms.

Proposition 1.2. *Let F be a formal group law over a ring A. Then the identity and inverse axioms hold, that is, $F(X,0) = X$ and $F(0,Y) = Y$, and there is a unique power series $\iota(T) \in A[\![T]\!]$ such that $F(X,\iota(X)) = F(\iota(Y),Y) = 0$.*

Proof. Say that $F(X,0) = f(X)$ and $g(Y) = F(0,Y)$ for some $f, g \in A[\![X]\!]$. We aim to show that $f(X) = g(X) = X$. It suffices to assume that $f(X) \equiv X + a_m X^m \pmod{\deg m+1}$ for some $a_m \in A$ and prove that $a_m = 0$, and likewise $g(Y) \equiv Y + b_n Y^n \pmod{\deg n+1}$. Without loss of generality, $m \geq n$. We also fix notation

$$F(X,Y) = X + Y + \sum_{i+j \geq 2} c_{ij} X^i Y^j.$$

By the definition of a formal group law, we have

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

Date: October 29, 2008.

Writing this out, we find that

$$X + g(Y) + \sum_{i+j\geq 2} c_{ij} X^i g(Y)^j = f(X) + Y + \sum_{i+j\geq 2} c_{ij} f(X)^i Y^j,$$

and so

$$X + Y + b_m Y^m + \sum_{2\leq i+j\leq m} c_{ij} X^i Y^j \equiv X + a_m X^m + Y + \sum_{i+j\geq 2} c_{ij} X^i Y^j \pmod{\deg m + 1},$$

hence $a_m = b_m = 0$ as desired.

The inverse axiom may be verified by (term-by-term) construction. □

Remark 1.3. In fact, all formal group laws are commutative as long as A has no elements that are both nilpotent and torsion. However, we will simply assume that a "formal group law" is commutative (and one-dimensional) from now on.

With formal group laws defined, we should now discuss maps between them.

Definition 1.4. Let F, G be formal group laws over a ring A. A *homomorphism* $f : F \to G$ *over* A is a power series with no constant term $f(T) \in A[\![T]\!]$ satisfying

$$f(F(X, Y) = G(f(X), f(Y)).$$

If given such f there exists a homomorphism $g \in A[\![T]\!], g : G \to F$ such that

$$f(g(T)) = g(f(T)) = T,$$

then we say that F and G are *isomorphic over* A and f is an *isomorphism over* A.

With these definitions in place, here are the most basic examples of formal group laws, which will occupy all of our time this evening.

Example 1.5. The *additive group* $\hat{\mathbb{G}}_a$ over $\mathbb{Z}$ is given by

$$F(X, Y) = X + Y.$$

Example 1.6. The *multiplicative group* $\hat{\mathbb{G}}_m$ over $\mathbb{Z}$ is given by

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

These examples are certainly not typical, because (exercise:) if A has no nilpotents, then any polynomial $F(X, Y) \in A[X, Y]$ satisfying the associativity axiom of the group law is of the form

$$F(X, Y) = X + Y + cXY, \quad \text{some } c \in A.$$

Scalar multiplication maps, which correspond to the power map in the group, provide the most basic example of group homomorphisms.

Example 1.7. Let F be a formal group law over the ring A. Define the power series $[n]_F(T) \in A[\![T]\!]$ by

$$[0]_F(T) = 0, [n]_F(T) = F(T, [n-1]_F(T)) \text{ for } n \geq 1;$$
$$[-n]_F(T) = \iota([n]_F(T)) \text{ for } n \geq 1.$$

One can check by induction that $[\cdot]_F$ is a homomorphism, and that $[\cdot]_F$ defines a homomorphism $[\cdot]_F : \mathbb{Z} \to \mathrm{End}_A(F)$.

The following important fact allows us to characterize isomorphisms.

Lemma 1.8. *Let $f(T) \in A[\![T]\!]$, $f(T) = aT + \cdots$. Then $f(T)$ has an inverse $g(T) = a^{-1}T + \cdots \in A[\![T]\!]$ if an only if $a \in A^\times$. This inverse g is unique if it exists.*

Remark 1.9. One may quickly check that if $f \in A[\![T]\!]$ is a homomorphism $f : F \to G$ and there exists $g \in A[\![T]\!]$ such that $f(g(T)) = g(f(T)) = T$, then g is a homomorphism $g : G \to F$. This is quite useful, because then we can take an inverse power series of a morphism to be itself a morphism in the opposite direction, without having to perform an extra check.

Proof. (Lemma 1.8) We can readily see that the inverse g of f cannot exist when $a \notin A^\times$.

This is the main example that we will write out here of how one constructs a power series as a limit of polynomials to fit a certain requirement. Naturally, we do this by induction. We wish to find polynomials $g_n(T) \in A[T]$ such that

$$f(g_n(T)) \equiv T \pmod{T^{n+1}} \quad \text{and} \quad g_{n+1}(T) \equiv g_n(T) \pmod{T^{n+1}}$$

Setting $g_1(T) = a^{-1}T$ takes care of the base case. Assume that we have found g_{n-1}, so that

$$f(g_{n-1}(T)) = a^{-1}T + bT^n \pmod{T^{n-1}}, \quad \text{some } b \in A$$

Set $g_n(T) = g_{n-1}(T) + \lambda T^n$ for some $\lambda \in A$ be chosen later. Then

$$\begin{aligned} f(g_n(T)) &= f(g_{n-1}(T) + \lambda T^n) \\ &= f(g_{n-1}(T)) + \lambda a T^n \pmod{T^{n+1}} \\ &= T + (b + \lambda a)T^n \pmod{T^{n+1}}. \end{aligned}$$

Thus pick $\lambda = -a^{-1}b$, and we have that $f(g(T)) = T$ where $g(T) = \lim_{n\to\infty} g_n(T) = a^{-1}T + \cdots \in A[\![T]\!]$. Uniqueness is clear from the process of picking coefficients of g.

It remains to show that $g(f(T)) = T$. Apply the work above to g to get $h(T) \in A[\![T]\!]$ such that $g(h(T)) = T$. Then $f(T) = f(g(h(T))) = h(T)$, so we're done. □

Because the leading coefficient of the multiplication by m map $[m]_F$ is m, we have this useful corollary.

Corollary 1.10. *Given a formal group F over A, the multiplcation by m map $[m]_F : F \to F$ is an automorphism (i.e. invertible) if and only if $m \in A^\times$.*

Proof. First we notice that by the definition and basic properties of formal groups that

$$[n]_F(X) \equiv nX \pmod{\deg 2}.$$

Then we apply Lemma 1.8 and the Remark after it to get that $[n]_F$ is an isomorphism. □

We conclude our basic properties with a statement that says in some way that formal groups over characteristic 0 rings are relatively boring. It is easy to see how the proof below doesn't work in non-zero characteristic rings.

Theorem 1.11. *Let F be a formal group over a characteristic 0 ring A. Then F is isomorphic to $\hat{\mathbb{G}}_a$ over $A \otimes \mathbb{Q}$.*

Theorem 1.11 follows from this much more explicit theorem, which we will (mostly) prove.

Theorem 1.12. *Let F and A be as above. Then there is a unique power series*

$$\log_F(T) = T + \frac{a_2}{2}T^2 + \frac{a_3}{3} + \cdots$$

with $a_i \in A$ such that

$$\log_F(F(X, Y)) = \log_F(X) + \log_F(Y).$$

Likewise, there exists a unique power series

$$\exp_F(T) = T + \frac{b_2}{2!}T^2 + \frac{b_3}{3!}T^3 + \cdots$$

with $b_i \in R$ such that $\exp_F(\log_F(T)) = \log_F(\exp_F(T)) = T$.

Proof. Fix notation and constants $a_2, a_3, \ldots \in A$ such that

$$F_1(X,Y) = \frac{d}{dX}F(X,Y), \qquad p(T) = F_1(0,T)^{-1} = 1 + a_2T + a_3T^2 + \cdots$$

and define $\log_F(T)$ by

$$\log_F(T) = T + \frac{a_2}{2}T^2 + \frac{a_3}{3}T^3 + \cdots .$$

Differentiate the associative law with respect to X to get

$$F_1(X, F(Y,Z)) = F_1(F(X,Y),Z) \cdot F_1(X,Y).$$

Set $X = 0$ to get

$$F_1(0, F(Y,Z)) = F_1(Y,Z)F_1(0,Y).$$

Hence by definition of p,

$$p(F(Y,Z))^{-1} = F_1(Y,Z) \cdot p(Y)^{-1},$$

which we rewrite as

$$p(Y) = F_1(Y,Z) \cdot p(F(Y,Z)).$$

Then apply inverse chain rule to get

$$\frac{d}{dY}(\log(Y)) = \frac{d}{dY}(\log(F(Y,Z))).$$

Therefore $\log(F(Y,Z)) = \log(Y) + h(Z)$ for some $h(Z) \in A[\![Z]\!]$. By symmetry, what we've done applies equally well to Z and we're done. To check uniqueness, differentiate the identity defining $\log_F$.

Now since the linear term of our homomorphism is a unit, there is an inverse over $A \otimes \mathbb{Q}$ which we'll call $\exp_F$. With some more work, we can show that $b_i \in A$. □

Remark 1.13. Actually, the proof above can be much more handily executed with the "invariant differential" in hand. If you are familiar with elliptic curves, for example, this differential of the formal group is the same one (in the case of the formal group of an elliptic curve) as the algebraic geometry invariant differential.

2. Some Intuition for Formal Groups

So far I've been droning on about abstract formal groups. But actually, I think that formal groups are pretty cool and useful. Their incarnations in scheme theory (formal group schemes) are the foundation of the theory of algebraic groups. Certain formal groups correspond to certain multiplicative generalized cohomology theories. The functor from Lie groups to Lie algebras factors through formal group laws – this is not something that I have experience with, but this is how formal groups came to be in the first place. The following examples illustrate how this Lie perspective gives rise to formal group laws.

This is the basic idea of how to get a formal group from a Lie group G with identity e and operation $m : G \times G \to G$. Say our Lie group is n-dimensional over a ring R, where R has natural smooth structure, e.g. $R = \mathbb{R}$ and $R = \mathbb{Z}_p$. Let V be a neighborhood of the identity with a chart $\Phi : V \to R^n$ such that $V(e) = 0$, and let $V_0 \subseteq V$ such that $m(V_0 \times V_0) \subseteq V$. Let $U \subset R^n$ be the image of V_0 under Φ. We then get a map on the coordinates,

$$F : U \times U \to R^n; \quad F = \Phi \circ m \circ (\Phi^{-1} \times \Phi^{-1}).$$

That is, we are expressing our group law on the coordinate charts. Taking the power series development of F around $0 \in R^n \times R^n$ gives us a formal group law. Doing this with a one-dimensional Lie group gets us a one-dimensional formal group law, and the formalities that we discussed in the previous section. Thinking about this construction should make the definition and most basic properties of a formal group law appear more natural, for example, the fact that $F(X,0) = X$.

Let's do a couple examples.

The additive group corresponds to the trivial chart on the trivial Lie group over R, namely R itself.

Next, consider our example from class that got me started with this in the first place: $G = \{1 + p\mathbb{Z}_p\} \subset \mathbb{Z}_p^\times$ with the chart

$$\Phi : G \to p\mathbb{Z}_p, \quad \Phi(1+X) = X$$

as we have $m(1+X, 1+Y) = 1+X+Y+XY$, the expression on the coordinates is $F(X,Y) = X+Y+XY$.

We'll have an eye toward the multiplicative group over a p-adic ring for most of our time here, but let's look at a more non-trivial example before moving on.

Let the homogenous Weierstrass equation

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

define an elliptic curve over some domain of characteristic 0, so we'll just say it's over $A = \mathbb{Z}[a_1, \ldots, a_6]$. The identity in this equation is $O_E = (0:1:0)$. The typical affine piece of $\P^2$ comes from setting $x = X/Z, y = Y/Z$. But this time, set $w = -X/Y$ and $t = -Z/Y$ to get the affine piece of E with O_E at the origin. The equation for this piece may be written

$$w = t^3 + a_1tw + a_2t^2w + a_3w^2 + a_4tw^2 + a_6w^3.$$

Letting $(t) = I \subset A[\![t]\!]$ define the I-adic topology on $A[\![t]\!]$, by Hensel's lemma applied to the equation above we can express w in terms of t, i.e. $w(t) = t^3 + \cdots \in A[\![t]\!]$.

Now note that $O_E = (0,0)$ in (w,t)-coordinates, and consider w as the inverse to a coordinate chart in some neighborhood of O_E. By using the group law for the elliptic curve and Hensel's lemma with $I \subset A[\![T]\!]$, we can find a formal group law $\hat{E}$ expressing E around O_E. The first few terms are

$$\hat{E}(X,Y) = X + Y - a_1XY - a_2(X^2Y + XY^2) + \cdots$$

3. Formal Groups over Complete DVRs

So far we've avoided talking about actual formal groups. Above, we've only spoken of axioms about group operations and what we can prove about those. Now we'll move on to evaluating our formal group laws at appropriate elements of our ring, yielding a group.

There are significant barriers in the way of doing this for a general ring A and formal group F. A general formal group law is a power series, and in a general ring there is no such thing as a value of a power series $F(a_1, a_2)$, $a_i \in A$. One way to get around this is to let B be any A-algebra and let the nilpotent elements of B form the elements of the group. This then gives us a functor $(A-\text{alg}) \to (\text{Groups})$, but it's not that nice.

Even if we do have a sense of what convergence is, say in $A = \mathbb{R}$, then we have to deal with convergence issues, and choosing proper V, V_0 in the general Lie group example above. The nicest and most general case is to work with B, a topological algebra over A equipped with an ideal I defining an I-adic topology. Then for all elements $x, y \in I$, we have $F(x,y) \in I$. There are no convergence issues! Polynomials and power series serve as our smooth functions. We will specify to rings of integers of ultrametric local fields, since this is what interests us.

From now on we'll use the usual notation from class: let A be a complete noetherian local ring with maximal ideal $\mathfrak{m}$, finite residue field $k = R/\mathfrak{m}$ of characteristic p, fraction field K, normalized valuation $\text{ord}_K : K \to \mathbb{Z}$, and choice of uniformizer π. Let $U = A^\times$ and let

$$U = U^{(0)} \supset U^{(1)} = \{1 + \mathfrak{m}\} \supset U^{(2)} = \{1 + \mathfrak{m}^2\} \supset \cdots$$

Soon we will limit ourselves to A being characteristic 0, so that it is a p-adic ring.

Definition 3.1. Let F be a formal group over A. Then the *group associated to F/A*, written $F(\mathfrak{m})$, is the set $\mathfrak{m}$ with group operation

$$x \oplus_F y = F(x, y) \quad \text{for } x, y \in \mathfrak{m},$$

and inverse operation

$$\ominus_F x = \iota(X) \quad \text{for } x \in \mathfrak{m}.$$

Check from the definition and properties of a formal group law that the operations indeed converge and give us a group. Also, check that homomorphisms (resp. isomorphisms) of formal group laws induce homomorphisms (resp. isomorphisms) on the groups $F(\mathfrak{m})$.

Example 3.2. The additive group $\hat{\mathbb{G}}_a(\mathfrak{m})$ is just the usual $\mathfrak{m}$. We can an exact sequence of additive groups

$$0 \to \hat{\mathbb{G}}_a(\mathfrak{m}) \to A \to k \to 0.$$

Example 3.3. Notice that $\hat{\mathbb{G}}_m(\mathfrak{m})$ is precisely $U^{(1)}$. We have an exact sequence

$$0 \to \hat{\mathbb{G}}_m(\mathfrak{m}) \to A^\times \to k^\times \to 0.$$

The existence of this sort of exact sequence often occurs for formal groups, and is quite useful because of the structure theorems we can prove about the formal groups. The following statement shows that any torsion in our formal group is p-power torsion. This generalizes what we know about $U^{(1)}$ from class.

Proposition 3.4. *Let F be a formal group over A then any torsion element of $F(\mathfrak{m})$ has order a power of p.*

Proof. Let $x \in \mathfrak{m}$ be a torsion element with respect to $\oplus_F$. Without loss of generality the order m of x is prime to p (just take a p^n power of x). Then $[m]_F(x) = 0$. By Corollary 1.10, $[m]_F$ is an isomorphism of $F(\mathfrak{m})$. Therefore $x = 0$. □

Also, just as with the filtration of $U^{(1)}$, successive quotients factor into $\mathfrak{m}^r/\mathfrak{m}^{r+1}$.

Lemma 3.5. *Let F be a formal group law over A. Then*

$$\frac{F(\mathfrak{m}^r)}{F(\mathfrak{m}^{r+1})} \cong (k, +).$$

Proof. Since $F(X, Y) = X + Y + XY \cdot G(X, Y)$ for some $G \in A[\![X, Y]\!]$, we have for $x, y \in \mathfrak{m}^r$ that $F(x, y) \equiv x + y \pmod{\mathfrak{m}^{2r}}$. Therefore

$$\begin{aligned} F(\pi^r A) &\to k \\ \pi^r x &\mapsto x \pmod{\pi} \end{aligned}$$

is a group homomorphism with kernel precisely $F(\mathfrak{m}^{r+1})$. □

Now we assume from now on that A has characteristic 0. Thus by Theorem 1.12, we have an isomorphism over $A \otimes \mathbb{Q}$ from any given formal group law F over A to $\hat{\mathbb{G}}_a$. The following theorem proves that this this isomorphism of formal group laws descends to the groups $F(\mathfrak{m}^r)$ and $\hat{\mathbb{G}}_a(\mathfrak{m}^r)$ for certain r.

Theorem 3.6. *Let A be a ring as above, with characteristic 0, and let F be a formal group over A. If*

$$r > \frac{\operatorname{ord}_K(p)}{p-1},$$

then $\log_F$ induces an isomorphism $F(\mathfrak{m}^r) \xrightarrow{\sim} \hat{\mathbb{G}}_a(\mathfrak{m}^r)$ with inverse map $\exp_F$.

Theorem 3.6 will follow if we can show with the restrictions on r, the logarithmic series

$$\log_F(T) = T + \frac{a_2}{2}T^2 + \frac{a_3}{3} + \cdots$$

sends $\mathfrak{m}^r$ to $\mathfrak{m}^r$, i.e $\log_F(\mathfrak{m}^r) \subseteq \mathfrak{m}^r$. Likewise, we must show the same of the exponential series

$$\exp_F(T) = T + \frac{b_2}{2!}T^2 + \frac{b_3}{3!}T^3 + \cdots$$

Thus we will establish Theorem 3.6 by proving the following

Proposition 3.7. *Let $f(T) \in A[\![T]\!]$ be a power series of the form*

$$f(T) = \sum_{n=1}^{\infty} \frac{b_n}{n!}T^n \qquad \text{with } b_1 \in U.$$

If $x \in A$ satisfies

$$\mathrm{ord}_K(x) > \frac{\mathrm{ord}_K(p)}{p-1},$$

then the series $f(x)$ converges and

$$\mathrm{ord}_K(f(x)) = \mathrm{ord}_K(x).$$

Note that both $\exp_F(T)$ and $\log_F(T)$ are of this form. One might suspect that we could place a looser requirement on $\log_F(T)$ than $\exp_F(T)$ to get a homomorphism in one direction, but actually this is not the case in general.

Proof. (Proposition 3.7) We will use the inequality

$$\mathrm{ord}_K(n!) \leq \frac{(n-1)\mathrm{ord}_K(p)}{p-1}.$$

For a general term of $f(x)$ we have

$$\begin{aligned}
\mathrm{ord}_K(b_n x^n/n!) &\geq n\mathrm{ord}_K(x) - \mathrm{ord}_K(n!) \\
&\geq n\mathrm{ord}_K(x) - \frac{(n-1)\mathrm{ord}_K(p)}{p-1} \\
&= \mathrm{ord}_K(x) + (n-1)\left(\mathrm{ord}_K(x) - \frac{\mathrm{ord}_K(p)}{p-1}\right).
\end{aligned}$$

Therefore, as the term in big parentheses is positive, the sequence of terms converges to 0. Consequently, the series converges since the topology is ultrametric. Moreover, every term has valuation strictly greater than the first term, and consequently $\mathrm{ord}_K(f(x)) = \mathrm{ord}_K(b_1 x) = \mathrm{ord}_K(x)$ as desired. □

Before getting to how the bound on r above is best possible even for the logarithmic function, here are some corollaries.

Corollary 3.8. *$F(\mathfrak{m})$ contains a subgroup of finite index isomorphic to $(A, +)$.*

Proof. By Theorem 3.6, there exists r such that $F(\mathfrak{m}^r) \cong \hat{\mathbb{G}}_a(\mathfrak{m}^r)$. By Lemma 3.5, each quotient in the series

$$F(\mathfrak{m}) \supset F(\mathfrak{m}^2) \supset \cdots \supset F(\mathfrak{m}^r) = \hat{\mathbb{G}}_a(\mathfrak{m}^r)$$

is of finite index since the residue field k is finite, so we're done. □

Corollary 3.9. *For any formal group law F over A, the group $F(\mathfrak{m})$ is pro-p.*

With these generalities in mind, we'll conclude by thinking about the multiplicative group $\hat{\mathbb{G}}_m$ and what we can say about the functions $\log_{\hat{\mathbb{G}}_m}$ and $\exp_{\hat{\mathbb{G}}_m}$, which we'll just write as log and exp for now.

By uniqueness of Taylor series, we have that

$$\log(T) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} T^n, \qquad \exp(T) = \sum_{n=1}^{\infty} \frac{1}{n!} T^n.$$

If we evaluate exp at $x \in \mathfrak{m}$, we find that for prime power order terms, our lower bound on the valuation is exactly the valuation of the term, because

$$\mathrm{ord}_K((p^n)!) = \mathrm{ord}_K(p) \sum_{i=1}^{\infty} \left\lfloor \frac{p^n}{p^i} \right\rfloor = \mathrm{ord}_K(p) p^n \sum_{i=1}^{n} p^{-i} = \mathrm{ord}_K(p) p^n \frac{1 - p^{-n}}{p-1} = \mathrm{ord}_K(p) \frac{p^n - 1}{p-1}.$$

With this fact, and the fact that all coefficients of exp have valuation 0, we have that all of the inequalities in the proof of Proposition 3.7 are equalities for pth power terms.

Now, as far as the log series, we start by noting that for any $x \in \mathfrak{m}$, $\log(x)$ converges. This is the case for any series of the form $\log_F$, i.e. $\log_F(T) = T + (a_2/2)T^2 + \dots$. This is because the valuation of the nth term is

$$\mathrm{ord}_K(a_n x^n / n) \geq n \mathrm{ord}_K(x) - \mathrm{ord}_K(n) \geq n \mathrm{ord}_K(x) - \mathrm{ord}_K(p) \log_p x,$$

which is unbounded when $x \in \mathfrak{m}$. However, this convergence is convergence in K, and not necessarily in R or $\mathfrak{m}$. In fact, if we want $\log_F(x) \in \mathfrak{m}$ when $x \in \mathfrak{m}$ or $\log_F(x) \in \mathfrak{m}^r$ when $x \in \mathfrak{m}^r$, we'll need a bound that is just as stringent as that needed to deal with $\exp_F$. The reason is that the pth term in either case is the same. Let's deal with the pth term of log, i.e. $\log = \log_{\hat{\mathbb{G}}_m}$. Say that $x \in \mathfrak{m}^r$ (or more precisely $\mathrm{ord}_K(x) = r$) and we want $\log(x)$ to be in $\mathfrak{m}^r$. We find that

$$\mathrm{ord}_K((-1)^p x^p / p) = pr - \mathrm{ord}_K(p),$$

so we want that

$$pr - \mathrm{ord}_K(p) \geq r,$$

that is,

$$r \geq \frac{\mathrm{ord}_K(p)}{p-1}.$$

Given that we satisfy this property, the subsequent powers of p will not be a problem. Therefore if we set $c = \mathrm{ord}_K(p)/(p-1)$, the lower bound of r such that log and exp converge on $\mathfrak{m}^r$ and map it into $\mathfrak{m}^r$ are

$$\mathfrak{m}^{\lfloor c \rfloor} \quad \text{and} \quad \mathfrak{m}^{\lfloor c \rfloor + 1}, \text{ respectively.}$$

As an example of how we can then get a logarithm that is not an isomorphism, simply consider $A = \mathbb{Z}_2, K = \mathbb{Q}_2, \pi = 2$. Then $\mathrm{ord}_K(2) = 1$ and $c = \mathrm{ord}_K(2)/(2-1) = 1$. Therefore

$$\log : \hat{\mathbb{G}}_m((2)) \to \hat{\mathbb{G}}_a((2))$$

is well defined, but we can quickly compute that $\mathrm{ord}(\log(x)) \geq 2$ for all $x \in \mathbb{Z}_2$, i.e. $\log(\hat{\mathbb{G}}_m((2))) \subset \hat{\mathbb{G}}_a((4))$. Therefore since by our main theorem log induces an isomorphism of $\hat{\mathbb{G}}_m((4))$ onto $\hat{\mathbb{G}}_a((4))$, we know that log is not injective on $\hat{\mathbb{G}}_m((2))$. Moreover, we know that

$$\mathbb{Z}_2^{\times} \cong \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}.$$

If you chose a case where $A \neq \mathbb{Z}_p$ and a prime ramifies sufficiently, perhaps you could find something interesting by playing around with this stuff.