Selmer Group Estimates Arising from the Existence of Canonical Subgroups

A. Klapper
Northeastern University

Abstract

Generalizing the work of Lubin in the one dimensional case, conditions are found for the existence of canonical subgroups of finite height commutative formal groups of arbitrary dimension over local rings of mixed characteristic $(0, p)$. These are p-torsion subgroups which are optimally close to being kernels of Frobenius homomorphisms. The $\mathbf{F}_p$ ranks of the first flat cohomology groups of these canonical subgroups are found. These results are applied to the estimation of the $\mathbf{F}_p$ rank of the Selmer group of an Abelian variety over a global number field of characteristic zero, and the lim sup of these ranks as the Abelian variety varies in an isogeny class.

1 Introduction

The purpose of this paper is to study the p-torsion subgroup Π_F of a commutative formal group F over a local field of mixed characteristic. Sufficient conditions are found for the the existence of a canonical subgroup in F. Such a subgroup is both the kernel of a homomorphism reducing to the (absolute) Frobenius homomorphism over the residue field, and a congruence subgroup of Π_F. Thus it is closer to being the kernel of the Frobenius homomorphism than any other subgroup. The discriminants of these groups are computable and, using a result of Mazur and Roberts [9], the $\mathbf{F}_p$ ranks of their first flat cohomology groups can be found. We apply this result to an estimate of the $\mathbf{F}_p$ rank of the p-Selmer group of an Abelian variety A.

All formal groups studied in this paper will be assumed to be commutative. For this introduction, let K be a global number field, R its ring of integers, η a prime ideal of R dividing p, K_η the completion of K at η, and R_η its ring of integers. Let A be defined over R and let F be the formal group associated with A. Consider the exact sequence

$$0 \longrightarrow \Pi_F \longrightarrow F \xrightarrow{[p]} F \longrightarrow 0.$$

Taking flat cohomology H^*_{Fl} over R and R_η, and truncating the long exact sequences on either side of $H^1_{Fl}(\Pi_F, -)$, we get a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & F(R)/pF(R) & \longrightarrow & H^1_{Fl}(\Pi_F, R) & \longrightarrow & H^1_{Fl}(F, R)_p & \longrightarrow & 0 \\ & & \downarrow & & \downarrow r_{\eta,p} & & \downarrow & & \\ 0 & \longrightarrow & F(R_\eta)/pF(R_\eta) & \xrightarrow{i_{\eta,p}} & H^1_{Fl}(\Pi_F, R_\eta) & \longrightarrow & H^1_{Fl}(F, R_\eta)_p & \longrightarrow & 0 \end{array}$$

The p-Selmer group of F (over R) is defined to be

$$S^p(F, R) = \bigcap_{\eta | p} r^{-1}_{\eta,p}(i_{\eta,p}(F(R_\eta)/pF(R_\eta)))$$

and similarly for $S^p(A,K)$, the p-Selmer group of A over K. We have $S^p(F,R) \subset S^p(A,K)$. By [10], $H^1_{Fl}(F,R_\eta) = 0$, so

$$S^p(F,R) = \bigcap r^{-1}_{\eta,p}(H^1_{Fl}(\Pi_F, R_\eta)).$$

Thus if we understand how the $r^{-1}_{\eta,p}(H^1_{Fl}(\Pi_F, R_\eta))$ intersect, then we can compute $S^p(F,R)$ and obtain lower bounds for $S^p(A,K)$.

Our results show that for certain Abelian varieties a canonical subgroup exists which is stable as η varies and forces the intersection of the $r^{-1}_{\eta,p}(H^1_{Fl}(\Pi_F, R_\eta))$ to be large enough to obtain a significant lower bound. Letting A move in an isogeny class, we show that for such Abelian varieties, the lim sup of the $\mathbf{F}_p$ ranks of the Selmer groups is at least $nd/2$, where $n = [K : \mathbf{Q}]$ and d is the dimension of A. This result generalizes Lubin's result in [5] for elliptic curves.

The first section contains results on the existence of canonical subgroups of formal groups over local fields of mixed characteristic. We present a condition on what can loosely be thought of as moduli for formal groups that implies such existence. The valuation of the set of points of this group is expressed in terms of these "moduli". In certain cases, this allows us to compute the $\mathbf{F}_p$ rank of the first flat cohomology group of the canonical subgroup using Mazur and Roberts' [9] local Euler characteristic. With an additional restriction (one that applies to formal groups associated to Abelian varieties) we determine necessary and sufficient conditions for the image of F under a homomorphism to have a canonical subgroup when F has one.

The last section contains the application of these results to estimating the rank of the Selmer group of an Abelian variety, as described above. The main result expresses this bound in terms of the canonicity of a p-torsion subgroup of A. This is a number that can be thought of as measuring how far away such a subgroup is from being étale. A key step is showing that if canonical subgroups exist over the localizations of R at several primes dividing p, then a subgroup exists over the localization at the union of these primes reducing to each of the canonical subgroups when localized.

This work has been heavily influenced by the work of Hazewinkel [4], Ditters [2], Mazur and Roberts [8, 9, 10, 11], and Lubin and Tate [5, 6, 7]. I would like to especially thank Jonathan Lubin for the help and encouragement he has given me.

2 Canonical Subgroups of Formal Groups

In this section we work entirely locally.

2.1 Notation and Constructions

Let (K, R, η, k, ν) be a local number field of (mixed) characteristic $(0,p)$, it's ring of integers, maximal ideal, residue field, and valuation, normalized so $\nu(p) = 1$. Reduction modulo η will often be denoted by a subscript 0. Also, let $(\overline{K}, \overline{R}, \overline{\eta}, \overline{k}, \overline{\nu})$ be the corresponding objects for the algebraic closure $\overline{K}$ of K.

Let F be a commutative finite height formal group over R of dimension d, and $\overline{x} = (x_1, \dots, x_d)$ be coordinates on F. We denote by $[i](\overline{x})$ the endomorphism "multiplication by i", i an integer. The kernel of $[p]_F$ will be denoted Π_F. If F_0 is the reduction modulo η of F, then there is a homomorphism $f_0 : F_0 \to F_0^{(p)}$, $f_0(\overline{x}) = (x_0^p, \dots, x_0^p)$ $(= \overline{x}^p)$, where $F_0^{(p)}$ is F_0 with each coefficient raised to the pth power. f_0 is called the (absolute) Frobenius homomorphism. There is also a homomorphism $g_0 : F_0^{(p)} \to F_0$, called the Verschiebung homomorphism, such that $g_0(f_0(\overline{x})) = [p](\overline{x})$. See [4].

Definition 2.1 *A homomorphism $f' : F \to G$ of formal groups over R is pre-Frobenius if $f'_0 = f_0$ (and $G_0 = F_0^{(p)}$). The kernel of a pre-Frobenius homomorphism is said to be a pre-canonical subgroup of F.*

We will need to construct subgroup schemes of formal groups from groups of points.

Proposition 2.2 *Let F be a formal group of dimension d over a complete d.v.r. S, with maximal ideal η. Let $T = \{\overline{\alpha_1}, \ldots, \overline{\alpha_r}\}$ be a set of (distinct) d-tuples from η, and $I = \{h(\overline{x}) \in S[[\overline{x}]] | \forall i, h(\overline{\alpha_i}) = 0\}$. Suppose that, for $1 \leq i, j \leq r$,*

1. $\overline{0} \in T$,
2. $[-1](\overline{\alpha_i}) \in T$,
3. $F(\overline{\alpha_i}, \overline{\alpha_j}) \in T$.

(In other words, T is a finite subgroup of $F(S)$, the group of formal S-points in F.) Then $\Gamma =$ $\mathrm{Spec}(S[[\overline{x}]]/I)$ is a finite free formal subgroup scheme of F of order r, and is in fact an affine group scheme.

Proof: We need to show that $I \subset (\overline{x})$, $[-1](I) \subset I$, and, if $A = S[[\overline{x}]]$, $B = A \hat{\otimes} A \cong S[[\overline{x}, \overline{y}]]$, $J = I \otimes A + A \otimes I$, and J' = closure of J in B, that $F(I) = \{h(F(\overline{x}, \overline{y})) | h(\overline{x}) \in I\} \subset J'$.

The first two assertions are clear. Let $J'' = \{h(\overline{x}, \overline{y}) | h(\overline{\alpha_i}, \overline{\alpha_j}) = 0, 1 \leq i, j \leq r\}$. Then $F(I) \subset J''$, and $J' \subset J''$. B/J is free of rank r^2 and

$$B/J' = A/I \hat{\otimes} A/I = A/I \otimes A/I \tag{1}$$

(since A/I is finite and free over S) is free of rank r^2. Thus $B/J = B/J'$ and $J = J'$. That Γ is affine follows from 1. □

We will also need homomorphisms with prescribed kernels.

Proposition 2.3 *Let F be a commutative formal group of finite height over a ring S which is either complete, local, Noetherian, and of residue charcteristic $p > 0$, or satisfies $p^n S = 0$ for some n. Let Γ be a finite free formal subgroup scheme of F, $\Gamma \subset ker([p^m])$ for some m. Then there are a formal group F' over S and homomorphisms $h_1 : F \to F'$, $h_2 : F' \to F$ such that $\Gamma = ker(h_1)$ and $h_2 \circ h_1 = [p^m]_F$.*

Proof: Over such an S the finite height formal groups are equivalent to certain Barsotti-Tate groups by way of $F \mapsto (ker([p^n]))_n$ (see [12]). Then F' is the formal group corresponding to the Barsotti-Tate group $([p^n]^{-1}(H)/(H))_n$. □

Some notation is necessary before defining canonical subgroups. We extend ν to matrices over $\overline{K}$. What we get is no longer a valuation, but does have enough structure to be useful. It would be interesting to study rings satisfying the first four conditions in lemma 2.5.

Definition 2.4 *Let $M = (m_{ij})$ be a matrix over $\overline{K}$. We denote $min\{\nu(m_{ij})\}$ by $\nu(M)$.*

For M and N matrices of the same dimensions, and P a matrix with same number of rows as M has columns,

Lemma 2.5 *1. $\nu(M+N) \geq min(\nu(M), \nu(N))$, with equality if $\nu(M) \neq \nu(N)$.*

2. $\nu(MP) \geq \nu(M) + \nu(P)$.

3. $\nu(aM) = \nu(a) + \nu(M)$, for $a \in \overline{K}$.

4. $\nu(M) = \infty$ iff $M = (0)$.

5. If M and N are square and have coefficients in $\overline{R}$, M is $\overline{K}$-invertible, $\nu(M) + \nu(M^{-1}) = 0$, and $\nu(M) = \nu(N) + \nu(M-N)$, then N is $\overline{K}$-invertible and $\nu(N) + \nu(N^{-1}) = 0$.

Proof: The first four assertions are obvious.

To prove the last assertion, we note that the field $K(M,N)$ generated over K by the matrix entries of M and N is complete. $\nu(I - M^{-1}N) = \nu(M^{-1}(M-N)) \geq \nu(M^{-1}) + \nu(M-N) \geq \nu(M^{-1}) + \nu(M) > 0$. It follows that $N^{-1} = \sum (I - M^{-1}N)^i M^{-1}$ converges. □

Let Γ be a finite subgroup scheme of F and let r be a positive real number.

Definition 2.6 *The rth congruence subgroup of Γ, denoted by Γ_r is the subgroup scheme defined by the set of $\bar{R}$ points T of Γ with valuation at least r. Γ_r is defined over the ring of integers S of $K(T)$. We denote $(\Pi_F)_r$ by F_r.*

Definition 2.7 *If Γ is a finite free subgroup scheme of F which is both pre-canonical and a congruence subgroup of Π_F, then we say Γ is canonical. If f is a pre-Frobenius homomorphism whose kernel is Γ, then we say f is a Frobenius homomorphism.*

A priori, Γ_r is only defined over S, but T is acted upon by the Galois group of $K[T]$ over K. A Galois descent argument, as in [3], shows that Γ_r is in fact defined over R. In particular, a canonical subgroup is always defined over R.

A formal group will generally have many pre-canonical subgroups over finite extensions of R (the number of subgroups of Π_F of order p^d is the number of $GF(p)$ subspaces of dimension d in $GF(p)^h$, where h is the height of F, though not all are pre-canonical), but may not have a canonical subgroup. The F_r can be thought of as giving a filtration of Π_F. A canonical subgroup exists only if some stage of this filtration has order p^d.

2.2 A Conguence for Formal Homomorphisms

Our analysis of formal homomorphisms depends upon the pure pth power coefficients and their valuations. These coefficients dominate all others, as is made precise by proposition 2.8. More precise statements can often be made by considering the functional equation defining a p-typical curve.

Underlying proposition 2.8 is much of the Cartier-Dieudonné theory of formal groups, as described in [4]. The main results we use here are 3 and the universality of the p-typical formal groups. The reader should keep in mind that theorem 2.9 was discovered from the point of view of Cartier-Dieudonné theory.

Proposition 2.8 *Let $h : F \to G$ be a homomorphism of formal groups over a $\mathbf{Z}_{(p)}$-algebra S. Let I_j be the ideal in $S[[\bar{x}]]$ generated by the homogeneous degree j terms of h. Then there are matrices $\{A_j\}$ with coefficients in S such that*

$$h(\bar{x}) \equiv \sum_{j=0}^{\infty} \bar{x}^{p^j} A_j \pmod{\sum_{j=0}^{\infty} I_{p^j}(\bar{x})^{p^j+1}}. \tag{2}$$

Proof: Assume first that F and G are p-typical, so also curvilinear. Let F have dimension d and G have dimension e, and let $\gamma_1, \ldots, \gamma_d$ and $\delta_1, \ldots, \delta_e$ be the standard $\mathbf{V}$-bases for the modules of p-typical curves in F and G respectively. By [4], p. 332,

$$h(\bar{x}) = \sum_i {}^G h(\gamma_i)(x_i). \tag{3}$$

$G(\bar{x}, \bar{y}) \equiv \bar{x} + \bar{y}$ mod degree 2, so

$$h(\bar{x}) \equiv \sum h(\gamma_i)(x_i) \pmod{\sum I_\ell(\bar{x})^{\ell+1}}, \tag{4}$$

and there are elements $\{a_k(i,j) \in S : 1 \le i \le d, 1 \le j \le e\}$ such that for $1 \le i \le d$,

$$h(\gamma_i) = \sum_k {}^G V^k \langle a_k(i,j) \rangle \delta_j, \tag{5}$$

where $\langle a_k(i,j) \rangle$ is the homothety operator associated with $a_k(i,j)$. Letting A_k be the matrix whose i,jth entry is $a_k(i,j)$, equations 4 and 5 imply that

$$h(\bar{x}) \equiv \sum \bar{x}^{p^k} A_k \pmod{\sum I_\ell(\bar{x})^{\ell+1}}. \tag{6}$$

By induction, the same holds modulo $\sum I_{p^k}(\bar{x})^{p^k+1}$.

If F and G are arbitrary, we can find strict homomorphisms $u : F \to F'$ and $w : G \to G'$, with F' and G' p-typical. Then equation 6 for $whu^{-1} : F \to G$ and the strictness of w and u gives equation 2. □

Proposition 2.8 applies in particular to $[p](\bar{x})$. In this case the $\{A_k\}$ in equation 5 are moduli for the set of p-typical formal groups of fixed dimension d. Thus the coefficients of the pure pth power terms of $[p](\bar{x})$ can be thought of as parametrizing the dimension d formal groups over S. They are not, strictly speaking, moduli, for distinct p-typical formal groups may be isomorphic (even strictly.)

2.3 The Existence of Canonical Subgroups

In theorem 2.9 we give a set of sufficient conditions for the existence of a canonical subgroup in F. These conditions generalize the conditions given by Lubin [6], though the form is different. In the one dimensional case, these conditions are necessary as well, as seen in theorem 2.13. If t is a real number, we denote the set of $a \in R$ such that $\nu(a) \ge t$ by (p^t).

Theorem 2.9 *Let F be a formal group over R and $\{A_i\}$ be matrices such that*

$$[p]_F(\bar{x}) \equiv \sum_{i=0}^{\infty} \bar{x}^{p^i} A_i \pmod{\sum (p^{\nu(A_i)})(\bar{x})^{p^i+1}},$$

A_1 is invertible over K, and, for $i \geq 2$,

$$r \stackrel{\text{def}}{=} \frac{1+\nu(A_1^{-1})}{p-1} > \frac{1-\nu(A_i)}{p^i-1}. \tag{7}$$

Then F_r is canonical.

Note that the restriction on the invertibility of A_1 is not a restriction on F. $A_0 = pI$, so A_1 is only determined modulo (p). Hence, A_1 can always be chosen so it is K invertible. Note also that we may have $F_r = F_s$ for some $s > r$.

Proof: It suffices to show F_r is pre-canonical. We may assume that F is p-typical, since congruence subgroups, pre-Frobenius homomorphisms, and the above inequalities are preserved under strict isomorphisms. By examining the logarithm of F, defined by the functional equation lemma of [4], we see that in fact

$$[p](\bar{x}) \equiv M(\bar{x}^p A_1) + \sum_{i \neq 1} \bar{x}^{p^i} A_i \pmod{\sum_{i\neq 1} (p^{\nu(A_i)})(\bar{x}^{p^i+1})},$$

where $M(\bar{x})$ is a d-tuple (d the dimension of F) of power series over R, congruent to $\bar{x}$ modulo degree two terms. Thus there is an invertible d by d matrix of power series $N(\bar{x})$ over R such that $M(\bar{x})N(\bar{x}) = \bar{x}$, and $N(0) = I$. Let $p(\bar{x}) = [p](\bar{x})N(\bar{x}^p A_1)$. Then

$$p(\bar{x}) \equiv \sum_{i=0}^{\infty} \bar{x}^{p^i} A_i \equiv [p]_F(\bar{x}) \pmod{\sum_{i \neq 1} (p^{\nu(A_i)})(\bar{x})^{p^i+1}}$$

and $R[[\bar{x}]]/([p](\bar{x})) = R[[\bar{x}]]/(p(\bar{x}))$. Thus $[p](\bar{x})$ and $p(\bar{x})$ define the same subscheme of F.

Let $a \in \bar{R}$ satisfy $\nu(a) = r$, and let

$$h(\bar{x}) = \frac{1}{a^p} p(a\bar{x}) A_1^{-1}.$$

Then $h(\bar{x})$ has integral coefficients by equation 7 and

$$h(\bar{x}) \equiv \bar{x} p a^{1-p} A_1^{-1} + \bar{x}^p \pmod{\bar{\eta}}.$$

Let $Y = \operatorname{Spec}(R[[\bar{x}]]/(h(\bar{x})))$. Then Y is a finite free R-scheme of order p^d. The injection $Y \to F$ defined by $\bar{x} \to a\bar{x}$ induces an isomorphism $Y(\bar{R}) \to F_r(\bar{R})$. Moreover, $\ker([p]_F)$ is smooth, so Y is smooth, so $|F_r(\bar{R})| = |Y(\bar{R})| = p^d$ and F_r has order p^d.

By proposition 2.3 there is a homomorphism $f' : F \to F'$, for some F', defined over R, whose kernel is F_r. By proposition 2.8 we can find matrices B and B_1 over R such that

$$f'(\bar{x}) \equiv \bar{x}B + \bar{x}^p B_1 \pmod{(p^{\nu(B)})(\bar{x})^2 + (\bar{x})^{p+1}}.$$

We claim that $\nu(B) > 0$. Let $b \in \bar{R}$ satisfy

$$r > \nu(b) > \frac{1-\nu(A_i)}{p^i - 1}$$

for all $i \geq 2$, and set $h'(\bar{x}) = b^{-p} p(b\bar{x}) A_1^{-1}$. Then $h'(\bar{x})$ has integral coefficients, and $h'(\bar{x}) \equiv \bar{x}^p \bmod \bar{\eta}$. The same arguments as above show that $F_{\nu(b)}$ has order p^d. $F_r \subset F_{\nu(b)}$, so $F_r = F_{\nu(b)}$. Now, $b^{-1}f'(b\bar{x})$ is integral and vanishes on the smooth scheme $\operatorname{Spec}(R[[\bar{x}]]/(h'(\bar{x})))$, so $b^{-1}f'(b\bar{x})$ is contained in $(h'(\bar{x}))$. There must be a d by d matrix of power series $M(\bar{x})$ such that $b^{-1}f'(b\bar{x}) = h'(\bar{x})M(\bar{x})$. In particular, $B = pb^{1-p}A_1^{-1}M(0) \equiv 0 \pmod{\bar{\eta}}$, so $\nu(B) > 0$, as claimed.

The fact that $\ker(f') = F_r$ has order p^d implies that B_1 is invertible over R. In particular, we can find an invertible d-tuple of power series $u(\bar{x}) \equiv \bar{x}B_1$ modulo degree two terms such that $f'(\bar{x}) \equiv u(\bar{x}^p) \pmod{\eta}$. Let $G(\bar{x},\bar{y}) = u^{-1}(F'(u(\bar{x}),u(\bar{y})))$, and $f(\bar{x}) = u^{-1}(f'(\bar{x}))$. Then G is a formal group over R, $u : G \to F'$ is an isomorphism, and $f : F \to G$ is a homomorphism with kernel F_r. Moreover, $f(\bar{x}) \equiv \bar{x}^p \bmod \eta$, and it follows that $G(\bar{x},\bar{y}) \equiv F^{(p)}(\bar{x},\bar{y}) \bmod \eta$. □

Corollary 2.10 *If, moreover, $\nu(A_1) + \nu(A_1^{-1}) = 0$, then $F_s = (0)$ for every $s > r$, and $\nu(B) = \nu(pA_1^{-1}) < \nu(B - pA_1^{-1})$ (so $\nu(B) + \nu(B^{-1}) = 0$ by proposition 2.5.)*

Proof: Let Y be as in the proof of theorem 2.9. Then $u = pa^{1-p}A_1^{-1}$ is $\bar{R}$-invertible, so Y_0 is a smooth finite $\bar{k}$-scheme of order p^d. If F_s is nontrivial, then $F_s(\bar{R}) \neq (0)$, so Y has a subscheme of order at least p whose reduction modulo η is not smooth. This proves the first assertion.

We claim that $Y_0(\bar{k})$ linearly spans $\bar{k}^d$. If not, then $Y_0(\bar{k})$ lies in a hyperplane. Thus there is a $d-1$ by d matrix M_0 over $\bar{k}$, which we may take to be of rank $d-1$, such that $Y_0(\bar{k})$ lies in $\bar{k}^{d-1}M_0$. Letting $\bar{y} = (y_1, \ldots, y_{d-1})$, $\bar{y}M_0u_0 + (\bar{y}M_0)^p$ has p^d distinct $\bar{k}$-points, which is not possible.

It follows that $Y(\bar{R})$ spans $\bar{R}^d$, so $F_r(\bar{R})$ spans $a\bar{R}^d$. Hence $a\bar{R}^dB = a^p\bar{R}^d$ and $\bar{R}^dB = a^{p-1}\bar{R}^d$. This proves the identity.

Finally, $h(\bar{x}) - a^{-p}f(a\bar{x}) \equiv \bar{x}(u - a^{1-p}B) \bmod \eta$ has roots spanning $\bar{R}^d$, so $\nu(u - a^{1-p}B) > 0$, and this proves the inequality. □

This in turn gives

Corollary 2.11 *With hypotheses as in theorem 2.9, suppose $F_r(R) = F_r(\bar{R})$ and $\nu(A_1)+\nu(A_1^{-1}) = 0$. Then the first flat cohomology group of F_r over R, $H^1_{Fl}(F_r, R)$, has rank $d(1 + n(1 - \nu(A_1)))$ over $\mathbf{Z}/p\mathbf{Z}$, where $n = [K : \mathbf{Q}_p]$.*

Proof: By [9],

$$\begin{aligned}
\mathrm{rank}(H^1_{Fl}(F_r, R)) &= d + \nu(\mathrm{discriminant}(F_r/R))/p^d \\
&= d + n\nu(\det(B)) \\
&= d + n\nu(\det(pA_1^{-1})) \\
&= d + n(d - \nu(\det(A_1))) \\
&= d(1 + n(1 - \nu(A_1))).
\end{aligned}$$

□

Proposition 2.3 implies that in general we can find $g : G \to F$ such that

$$[p]_F(\bar{x}) = g(f(\bar{x})) \text{ and } [p]_G(\bar{x}) = f(g(\bar{x})) \tag{8}$$

(the second equation holding because f is an isomorphism over K). There exist matrices $\{A'_i\}$ and $\{C_i\}$ such that

$$[p]_G(\bar{x}) \equiv \sum_{i=0}^{\infty} \bar{x}^{p^i} A'_i \text{ and } g(\bar{x}) \equiv \sum_{i=0}^{\infty} \bar{x}^{p^i} C_i$$

modulo appropriate ideals. Using these in equation 8 gives

$$\begin{aligned} C_0 B &= pI \\ C_0 + B^{(p)} C_1 &\equiv A_1 \pmod{p^{\nu(C_0)+2\nu(B)}} \\ C_1 + C_0^{(p)} &\equiv A_1' \pmod{p^{2\nu(C_0)+\nu(B)}}. \end{aligned}$$

Thus B is K-invertible, $C_0 = pB^{-1}$, and

$$pB^{-1} + B^{(p)} C_1 \equiv A_1 \pmod{p^{\nu(pB^{-1})+2\nu(B)}} \tag{9}$$

$$C_1 B + (pB^{-1})^{(p)} \equiv A_1' \pmod{p^{2\nu(pB^{-1})+\nu(B)}}. \tag{10}$$

Suppose the hypotheses of corollary 2.10 hold. Then equation 9 holds modulo $p^{1+\nu(B)}$, while equation 10 holds modulo $p^{1+\nu(A_1)}$.

If $\nu(A_1) = 0$, then $\nu(B) = 1$, so $A_1' \equiv A_1^{(p)} \bmod p$. In particular, $\nu(A_1') = \nu(A_1'^{-1}) = 0$. Thus G has a canonical subgroup. In fact, C_0 is R-invertible, so g is an isomorphism.

Corollary 2.12 *With the hypotheses of corollary 2.10, suppose moreover that A_2 is R-invertible and $\nu(A_1) > 0$. Then A_2' is R-invertible and*

1. *If $\nu(A_1) < 1/(p+1)$, then $\nu(A_1') = p\nu(A_1) < \nu(A_1' - A_1^{(p)})$ and G has a canonical subgroup.*
2. *If $\nu(A_1) = 1/(p+1)$, then $\nu(A_1') \geq p/(p+1)$ and G has no canonical subgroup.*
3. *If $1/(p+1) < \nu(A_1) < p/(p+1)$, then $\nu(A_1') = 1 - \nu(A_1) < \nu(A_1' - pA_1^{-1})$, and G has a canonical subgroup.*

Proof: Comparing coefficients of $\bar{x}^{p^2}$ in equation 8, we see that $\nu(C_1) = \nu(A_2)$ and $\nu(A_2') = \nu(C_1^{(p)}) = 0 < \nu(A_2' - A_2^{(p)})$, so A_2 is R-invertible.

Next note that the hypotheses of theorem 2.9, in this case, amount to $\nu(A_1) < p/(p+1)$. Equation 10 implies that

$$pA_2 A_1^{-1} + A_1^{(p)} \equiv A_1' \pmod{p\bar{\eta}}. \tag{11}$$

The breakdown of cases follows from a consideration of which term on the lefthand side of equation 11 dominates in valuation. The existence of a canonical subgroup follows from theorem 2.9 and the nonexistence from theorem 2.13 below. $\square$

Theorem 2.13 is as close as we have come to a converse to theorem 2.9.

Theorem 2.13 *If $[p]_F(\bar{x}) \equiv \sum \bar{x}^{p^i} A_i \bmod \sum (p^{\nu(A_i)})(\bar{x})^{p^i+1}$, $A_j = aU$ for some $j \geq 2$, $a \in R$, and U a R-invertible matrix, and if*

$$s \stackrel{\text{def}}{=} \frac{1-\nu(A_j)}{p^j - 1} \geq \frac{1-\nu(A_i)}{p^i - 1}$$

for all $i \geq 1$, then F does not have a canonical subgroup.

Proof: Let $ac^{p^j-1} = p$, for some $c \in \bar{K}$, so $\nu(c) = s$. Let

$$\begin{aligned} h''(\bar{x}) &= \frac{1}{cp}[p](c\bar{x}) \\ &\equiv \bar{x} + \cdots + \bar{x}^{p^j}U + \cdots \pmod{\eta} \end{aligned}$$

If $Z = \mathrm{Spec}(\bar{R}[[\bar{x}]]/(h''(\bar{x})))$ then Z is free of rank at least $p^{dj} > p^d$, so Z has more than p^d points. Z_0 is smooth so all of Z's points have valuation zero. Thus s is maximal such that $F_s \neq (0)$, and must be contained in any canonical subgroup. On the other hand, F_s has too large a rank to be a subgroup scheme of a canonical subgroup. □

Thus, for example, if A_2 is R-invertible and $\nu(A_1) + \nu(A_1^{-1}) = 0$, then F has a canonical subgroup if and only if $\nu(A_1) < p/(p+1)$. It seems that not much more can be said about the existence or nonexistence of canonical subgroups by this approach.

2.4 Products

The product of two formal groups that have canonical subgroups may not have a canonical subgroup, except in special cases. A canonical subgroup in a product, however, is always the product of canonical subgroups in the factors.

Proposition 2.14 *If F_1 and F_2 are formal groups over R, and Γ is a canonical subgroup of $F = F_1 \times F_2$, then $\Gamma = \Gamma_1 \times \Gamma_2$, with Γ_i canonical in F_i, $i = 1, 2$.*

Proof: Let $d_i = \dim(F_i)$, so H has order $p^{d_1+d_2}$. $H = F_r$ for some real number r. Let $T_1 = \{\bar{\alpha} | (\bar{\alpha}, \bar{\beta}) \in \Gamma(\bar{R})$ for some $\bar{\beta}\}$, and $T_2 = \{\bar{\beta} | (\bar{\alpha}, \bar{\beta}) \in \Gamma(\bar{R})$ for some $\bar{\alpha}\}$, and let Γ_i be the subgroup of F_i generated as in proposition 2.2 by T_i, $i = 1, 2$. Then

$$\Gamma_1 \times \Gamma_2 \subset F_r = \Gamma \subset \Gamma_1 \times \Gamma_2,$$

so $\Gamma_1 \times \Gamma_2 = \Gamma$.

If $f_i : F_i \to F_i'$ has kernel Γ_i, $i = 1, 2$, then $f = f_1 \times f_2 : F \to F_1' \times F_2'$ has kernel Γ. Γ is canonical so $f(\bar{x}) \equiv 0$ modulo η and degree two terms. The same must hold for for f_i, $i = 1, 2$. It follows that Γ_i has order p^{d_i}, and hence is pre-canonical. $\Gamma_i = (F_i)_r$, and thus is canonical. □

As a partial converse, we have

Proposition 2.15 *Let F_1 and F_2 be formal groups over R, and suppose that for $i = 1, 2$*

$$[p]_{F_i}(\bar{x}) \equiv p\bar{x} + \bar{x}^p A_{i,1} + \bar{x}^{p^2} A_{i,2} \pmod{p(\bar{x})^2 + (p^{\nu(A_{i,1})})(\bar{x})^{p+1} + (\bar{x})^{p^2+1}},$$

with $A_{i,2}$ R-invertible, $A_{i,1}$ K-invertible, $\nu(A_{i,1}) + \nu(A_{i,1}^{-1}) = 0$, and $\nu(A_{i,1}) > 0$. Then the following are equivalent:

1. *$F = F_1 \times F_2$ has a canonical subgroup.*

2. *F_1 and F_2 each has a canonical subgroup.*

3. $\nu(A_{i,1}) < p/(p+1)$, $i = 1, 2$.

Note that F satisfies the hypotheses on the F_i only if $\nu(A_{1,1}) = \nu(A_{2,1})$.

Proof: 1. implies 2. by proposition 2.14.
2. implies 3. by theorem 2.13.
3. implies 1. by theorem 2.9. $\square$

The converse of proposition 2.14 fails in general, as is shown by the following example. Let F_1 be a formal group over R with $\Gamma_1 \neq \Pi_{F_1}$ canonical in F_1. $\Gamma_1 = (F_1)_r$ for some r. Let $\bar{\alpha}$ be in $\Pi_{F_1}(\bar{R})$ but not in $\Gamma_1(\bar{R})$, and choose a positive integer h and $b \in \bar{R}$ such that

$$\nu(\bar{\alpha}) > \frac{1-\nu(b)}{p-1} \stackrel{\text{def}}{=} s > \frac{1}{p^h - 1}.$$

By the functional equation lemma of [4] we can construct a (one dimensional) formal group F_2 over $R[b]$ such that

$$[p]_{F_2}(x) \equiv px + bx^p + x^{p^h} \pmod{p(x)^2 + b(x)^{p+1} + (x)^{p^h+1}}.$$

$\Gamma_2 = (F_2)_s$ is canonical in F_2 by theorem 2.9, but $(\bar{\alpha}, 0)$ is in any congruence subgroup of $\Pi_{F_1 \times F_2}$ containing $\Gamma_1 \times \Gamma_2$, so $\Gamma_1 \times \Gamma_2$ cannot be canonical.

2.5 Canonical Subgroups: A Special Case

In this subsection we assume that A_2 is R-invertible and $A_1 = bU$, with $b \in R$ and U R-invertible. F has height d if b is a unit, $2d$ otherwise. F has a canonical subgroup Γ if and only if $\nu(b) < p/(p+1)$, and, in this case, $\Gamma = F_r$ for any r satisfying

$$\frac{1-\nu(b)}{p-1} \geq r > \frac{\nu(b)}{p-p^2}.$$

In particular, $r = 1/(p^2-1)$ will do. In fact, if $\alpha \neq 0$ is a $\bar{K}$-point of Γ, then $\nu(\alpha) = (1-\nu(b))/(p-1)$, and the remaining non-zero points of the Π_F have valuation $\nu(b)/(p^2-p)$. If $\nu(b) > p/(p+1)$, then each non-zero $\bar{R}$-point of the Π_F has valuation $1/(p^2-p)$.

Let $\nu(b) < p/(p+1)$ and let Γ be the canonical subgroup of F. Let Δ be a subgroup of Π_F satisfying $\Gamma(\bar{R}) + \Delta(\bar{R}) = \Pi_F(\bar{R})$, let $g : F \to G$ be an isogeny with kernel Δ, and let Γ' be the image of Γ under g (so Γ' is also the image of Π_F).

Δ is trivial and g is an isomorphism if $\nu(b) = 0$.

Proposition 2.16 *If $\nu(b) > 0$, then Δ is precanonical.*

Proof: Choose $a \in \bar{R}$ such that $a^{p^2-p} = b$, so $\nu(a) = \nu(b)/(p^2-p)$. Let $h(\bar{x}) = a^{-p^2}[p]_F(a\bar{x}) \equiv \bar{x}^p U + \bar{x}^{p^2} A_2 \bmod \eta$. Denoting by $a^{-1}\Delta$ the R-scheme whose set of $\bar{R}$-points is $\{a^{-1}\delta | \delta \in \Delta(\bar{R})\}$, we see that $\bar{x}U + \bar{x}^p A_2 \bmod \eta$ is a regular system of generators for the ideal in $k[\bar{x}]$ of the image under Frobenius of $(a^{-1}\Delta) \times_R k$ (i.e., the ideal vanishing on $\{(a^{-1}\delta)^p \bmod \eta | \delta \in \Delta(\bar{R})\}$.) $a^{-p}g^{(p)}(a^p\bar{x}) \equiv \bar{x}D^{(p)}$ is in this ideal (where $g^{(p)(\bar{x})}$ is $g(\bar{x})$ with each coefficient raised to the pth power and D is the Jacobian of g) so $\delta D \equiv 0 \bmod \eta$ if $\delta \in a^{-1}\Delta(\bar{R})$.

As a set of vectors, $a^{-1}\Delta(k)$ spans k^d (otherwise we could produce a system $\bar{y}M + \bar{y}^p$, $\bar{y} = (y_1, \ldots, y_{d-1})$ and M a $(d-1) \times (d-1)$ matrix, with p^d roots over k.) Consequently, $k^d D = 0$, so $D \equiv 0 \bmod \eta$, i.e., Δ is pre-canonical.

If $\nu(c) = \nu(D)$ and $\nu(c) < \nu(b)/p$, then $c^{-p}a^{-p}g^{(p)}(a^p\bar{x}) \equiv \bar{x}c^{-p}D^{(p)} \bmod \eta$ and the same argument leads to a contradiction. Thus $\nu(D) \geq \nu(b)/p$. Conversely, if $\delta \in \Delta(\bar{R})$, then $\nu(\delta) = \nu(b)/(p^2-p)$ and $\nu(\delta^p) = \nu(\delta D) \geq \nu(\delta) + \nu(D)$, so $\nu(D) \geq (p-1)\nu(\delta) = \nu(b)/p$. □

To keep track of the existence of canonical subgroups under isogeny we need the following.

Proposition 2.17 *If Γ and Δ are subgroups of Π_F such that $\Gamma(\bar{R}) \oplus \Delta(\bar{R}) = \Pi(\bar{R})$ and Γ is canonical in F, then the image Γ' of Γ under an isogeny $g : F \to G$ with kernel Δ is canonical in G. If Δ is nontrivial (i.e., $\nu(b) > 0$) and $[p]_G(\bar{x}) \equiv p\bar{x} + \bar{x}^p A_1' + \bar{x}^{p^2} A_2' \bmod p(\bar{x})^2 + (A_1')(\bar{x})^{p+1} + (\bar{x})^{p^2+1}$ then $\nu(A_1') = \nu(A_1)/p$.*

Proof: First note that $[p]_G(\bar{x})$ satisfies such a congruence with A_1' or A_2' R-invertible under these hypotheses. The proposition is easily proved if $\nu(b) = 0$. If $\nu(b) > 0$, then Δ is precanonical by proposition 2.16, so $\nu(g(\gamma)) > \nu(\gamma) \geq 1/(p^2-1)$ for any $\gamma \in \Gamma(\bar{R})$. Also, $\nu(b) < p/(p+1)$.

Retaining the notation of the proof of proposition 2.16, and comparing $a^{-p^2}g^{(p)}(a^p\bar{x})$ with $\bar{x}U + \bar{x}^p A_2$ we find $D^{(p)} \equiv A_1 A_2^{-1} \bmod (A_1)\eta$. We have $g \circ [p]_F = [p]_G \circ g$, so, equating $\bar{x}^{p^2}$ terms, $A_1'^{(p)} \equiv A_2^{(p)} A_1 A_2^{-1} \bmod (A_1)\eta = b\eta$. Therefore $A_1' = cU$ with U a R-invertible matrix and $c^p = b$. G has a canonical subgroup if and only if Π_G has nonzero points with valuation greater than $1/(p^2-1)$ and these are the non-zero points of the canonical subgroup. Thus G has a canonical subgroup containing $g(\Gamma)$. The canonical subgroup and $g(\Gamma)$ both have rank d, hence are identical. □

3 Application: Selmer Group Estimates for Abelian Varieties

In this section we use the results of section 2 to derive lower bounds on the ranks of the Selmer groups of certain Abelian varieties over rational number fields. We now let K (R) be a rational number field (resp., its ring of integers). For each non-zero prime η of R let K_η be the completion of K at η.

If η is nonarchimedean, let R_η denote the ring of integers in K_η, η (by abuse of notation) its maximal ideal, k_η its residue field, p_η the characteristic of k_η, and ν_η the valuation on R_η, normalized so that $\nu_\eta(p_\eta) = 1$, and extended to K_η. Let $n = [K : \mathbf{Q}]$, and $n_\eta = [K_\eta : \mathbf{Q}_{p_\eta}]$. Observe that the results of section 2 apply to formal groups over R.

3.1 Stability

We show in this subsection that canonical subgroups are stable as η varies. Let F be a formal group over $R_{(p)}$, for some prime integer p. As in the local case, we may write

$$[p]_F(\bar{x}) \equiv \sum_{j=0}^{\infty} \bar{x}^{p^j} A_j \quad (\mathrm{mod} \ \sum_{j=0}^{\infty} (A_j)(\bar{x})^{p^j+1}). \tag{12}$$

Let η_1 and η_2 be two primes dividing p. Suppose A_2 is R_{η_i}-invertible, and $A_1 = bU$, with $\nu_{\eta_i}(b) < p/(p+1)$, and U invertible over R_{η_i}, $i = 1, 2$. Let Γ_i be the canonical subgroup of F over R_{η_i}.

Proposition 3.1 *With the above hypotheses, F has a subgroup Γ over $R_{\eta_1\cup\eta_2}$ such that*

$$\Gamma_i = \Gamma \times_{R_{(\eta_1\cup\eta_2)}} R_{\eta_i}.$$

Proof: Choose $\tau \in \bar{K}$ such that $\tau^{p-1} = pb^{-1}$. Then, by the proof of theorem 2.9, $\tau^{-1}\Gamma_i(R_{\eta_i})$ is the set of η_i-integral roots of $\tau^{-p}[p](\tau\bar{x})A_1^{-1} \overset{\text{def}}{=} h'(\bar{x})$. The coefficients of h' are integral over $R_{(\eta_1\cup\eta_2)}$ and, by descent, there is a finite $R_{(\eta_1\cup\eta_2)}$-scheme Γ such that $\tau^{-1}\Gamma(\bar{K}_{\eta_1\cup\eta_2})$ is the set of η_i-integral roots of h'. The arguments in the proof of proposition 2.2 show that Γ is a subgroup scheme of F and $\Gamma_i = \Gamma\times_{R_{(\eta_1\cup\eta_2)}} R_{\eta_i}$. $\Box$

3.2 Selmer Group Estimates

Let A be an abelian variety over K with good reduction everywhere. We recall the definition of the Selmer group of A. Let m be a positive integer and consider the exact sequence

$$0 \longrightarrow A_m \longrightarrow A \xrightarrow{\cdot m} A \longrightarrow 0. \tag{13}$$

For any prime η of R, we denote by $r_{\eta,m} : H^1_{Fl}(A_m, K) \to H^1_{Fl}(A_m, K_\eta)$ and $i_{\eta,m} : A(K_\eta)/mA(K_\eta) \to H^1_{Fl}(A_m, K_\eta)$ the localization homomorphism and connecting homormorphism for this sequence. The m-Selmer group $S^m(A,K)$ is then defined to be $\bigcap_\eta r^{-1}_{\eta,m}(\mathrm{Im}(i_{\eta,m}))$

This generalizes by replacing m by a finite subgroup scheme Γ of A and a homomorphism $f : A \to B$ with kernel Γ. There are homomorphisms $r_{\eta,\Gamma} : H^1_{Fl}(\Gamma, K) \to H^1_{Fl}(\Gamma, K_\eta)$ and $i_{\eta,\Gamma} : B(K_\eta)/fA(K_\eta) \to H^1_{Fl}(\Gamma, K_\eta)$ analogous to $r_{\eta,m}$ and $i_{\eta,m}$, and $S^\Gamma(A,K) \overset{\text{def}}{=} \bigcap_\eta r^{-1}_{\eta,\Gamma}(\mathrm{Im}(i_{\eta,\Gamma}))$. Thus $S^m(A,K) = S^{A_m}(A,K)$.

$S^\Gamma(A,K)$ fits into an exact sequence which we will use to estimate its rank:

$$0 \longrightarrow S^\Gamma(A,K) \longrightarrow H^1_{Fl}(\Gamma,K) \longrightarrow \prod_\eta H^1_{Fl}(\Gamma,K_\eta)/\mathrm{Im}(i_{\eta,\Gamma}). \tag{14}$$

We now require that $A_p(K) = A_p(\bar{K})$ (by extending K, if necessary) and assume that $\Gamma \subset A_p$ (and Γ is defined over R.) Thus Γ is étale over R_η for each nonarchimedean prime η not dividing (p). There is a homomorphism $\Gamma \to \mu_p^r$, where r is the rank of Γ, which is an isomorphism over K or R_η if $\eta \not| (p)$. This assumption on A_p means that the completions at the archimedean primes are all complex, so $H^1_{Fl}(\Gamma, K_\eta)$ is trivial for these primes. We have $H^1_{Fl}(\Gamma,K) \cong H^1_{Fl}(\mu_p^r, K)$ and $H^1_{Fl}(\Gamma, K_\eta) \cong H^1_{Fl}(\mu_p^r, K_\eta)$. If Γ is local at $\eta|(p)$, (that is, if Γ is a subgroup of the formal group F of A at η) then $H^1_{Fl}(F, R_\eta) = 0$ by [8, 10], so $\mathrm{Im}(i_{\eta,\Gamma}) = H^1_{Fl}(\Gamma, R_\eta)$. We need a theorem of Mazur and Roberts.

Theorem 3.2 *(Mazur-Roberts [9]) If Γ is a finite flat group scheme over R_η, annihilated by p, and of rank r, all of whose points are defined over R_η, then*

$$\mathrm{rank}_{\mathbf{F}_p}(H^1_{Fl}(\Gamma, R_\eta)) = r + \sum_{\gamma\in\Gamma(R_\eta)} \frac{\nu_\eta(\det(\mathrm{disc}_\gamma(\Gamma)))}{p^r}\cdot n_\eta. \tag{15}$$

In particular, $H^1_{Fl}(\mu_p, R_\eta)$ has rank $1 + n_\eta$ if $\eta|(p)$. We also know that $H^1_{Fl}(\mu_p, R) = R^*/(R^*)^p$ has rank $n/2$ by the Dirichlet unit theorem (e.g. [1].) To dispose of the primes η not dividing (p) we need

Lemma 3.3 *If $\eta \not| (p)$, then $Im(i_\eta, \Gamma) = H^1_{Fl}(\Gamma, R_\eta) \cong H^1_{Fl}(\mu_p^r, R_\eta)$.*

Proof: There is a homomorphism $g : B \to A$ such that $[p] = g \circ f$, i.e., $\ker(g) = f(A_p) \stackrel{\text{def}}{=} \Delta'$. We have $B(R_\eta)/fA(R_\eta) \subset H^1_{Fl}(\Gamma, R_\eta)$, and $A(R_\eta)/gB(R_\eta) \subset H^1_{Fl}(\Delta', R_\eta)$. These cohomology groups have ranks $r = \text{rank}(\Gamma)$ and $r' = \text{rank}(A_p) - r = \text{rank}(\Delta')$ since they are étale. Thus $\text{rank}(B(R_\eta)/fA(R_\eta)) \le r$ and $\text{rank}(A(R_\eta)/gB(R_\eta)) \le r'$.

A_p is étale, so $A(R_\eta)/pA(R_\eta) \cong A(k_\eta)/pA(k_\eta)$. $A(k_\eta)$ is finite, so the rank of $A(k_\eta)/pA(k_\eta)$ equals the rank of $A_p(k_\eta)$ which is $r + r'$.

The sequence

$$0 \longrightarrow B(R_\eta)/fA(R_\eta) \xrightarrow{g} A(R_\eta)/pA(R_\eta) \longrightarrow A(R_\eta)/gB(R_\eta) \longrightarrow 0 \tag{16}$$

is exact since $\Delta(R_\eta) = f(A_p(R_\eta))$ (thus if $g(\gamma) = p\delta = g \circ f(\delta)$ then $\gamma - f(\delta) \in \Delta(R_\eta) = f(A_p(R_\eta))$, so $\gamma \in f(A(R_\eta))$.) A count of ranks gives the desired results. □

Thus by considering only the integral cocycles in $H^1_{Fl}(\mu_p^r, K)$ we get an exact sequence

$$0 \longrightarrow C \longrightarrow H^1_{Fl}(\mu_p^r, R) \longrightarrow \Pi_{\eta|(p)} H^1_{Fl}(\mu_p^r, R_\eta)/H^1_{Fl}(\Gamma, R_\eta) \tag{17}$$

with $C \subset S^\Gamma(A, K)$ (Γ local at each $\eta|(p)$.)

Definition 3.4 *If $\Gamma \subset A_p$ is a finite flat subgroup scheme of rank d, then the local and global canonicities of Γ are*

$$c_\eta(\Gamma) = \begin{cases} \sum_{\gamma \in \Gamma(R)} \frac{\nu_\eta(det(disc_\gamma(\Gamma)))}{dp^d} & \text{if } \Gamma \text{ is canonical at } \eta, \\ 0 & \text{otherwise} \end{cases}$$

and $c(\Gamma) = \sum_{\eta|(p)} c_\eta(\Gamma) n_\eta / n$.

For example, $c(\mu_p) = 1$ in G_m, $c(\Gamma) = 0$ if Γ is étale, $c(\gamma) = 1$ if A has ordinary reduction at each $\eta|p$ and $\Gamma = A_p$, and $0 \le (\Gamma) \le 1$ for any Γ. Note that the definition used here differs slightly from that in [5].

It follows from equations 15 and 17 that

Theorem 3.5 *Let A be an Abelian variety over K with good reduction everywhere and Γ be a finite flat subgroup of A_p of rank d which is local at each $\eta|(p)$. Then*

$$rank_{F_p}(S^\Gamma(A, K)) \ge nd(c(\Gamma) - 1/2)$$

Proof: Follows from the additivity of rank and the exact sequence 17. □

Corollary 3.6 *Let A be an Abelian variety over $R_{(p)}$ with good reduction at each prime of K (when regarded as an Abelian variety over K), and let F be the associated formal group. Assume that*

$$[p]_F(\bar{x}) \equiv p\bar{x} + \bar{x}^p A_1 + \bar{x}^{p^2} A_2 \pmod{p(\bar{x})^2 + (A_1)(\bar{x})^{p+1} + (\bar{x})^{p^2+1}}$$

where $A_1 = bU$, with $b \in \eta R_{(p)}$, and U and A_2 are $d \times d$ matrices invertible over R_η for each $\eta|(p)$. If $b^{p+1}|p^p$ in $R_{(p)}$, then

$$rank_{\mathbf{F}_p}(S^{(p)}(A, K)) \ge nd(\frac{1}{2} - \sum \nu_\eta(b)\frac{n_\eta}{n}).$$

Proof: Proposition 3.1 allows us to find a subgroup Γ of A_p which is canonical at each $\eta|(p)$. By proposition 2.11,

$$\nu_\eta(\det(\mathrm{disc}_\gamma(\Gamma))) = d(1-\nu_\eta(b))$$

for any $\gamma \in \Gamma(\bar{K})$, $\eta|(p)$. Thus

$$c(\Gamma) = 1 - \sum_{\eta|(p)} \nu_\eta(b)\frac{n_\eta}{n}.$$

□

Letting A move in an isogeny class gives

Corollary 3.7 *With hypotheses as in corollary 3.6,*

$$\limsup\{rank_{\mathbf{F}_p}(S^{(p)}(A',K))\} \geq \frac{nd}{2},$$

where the limit is taken over all A' isogenous to A.

Proof: Take $\Delta \subset A_p$ of rank d over $\mathbf{F}_p$ so that $\Delta + \Gamma = A_p$. Δ is a pre-canonical subgroup of F at all primes dividing (p) by proposition 2.16. Let $A' = A/\Delta$, $g : A \to A'$ the quotient map. The $\Gamma' = g(\Gamma)$ is a canonical subgroup of the formal group F' of A' and $1 - c_\eta(\Gamma') = (1 - c_\eta(\Gamma))/p$ for $\eta|(p)$. Iterating, we see that $1 - c_\eta(\Gamma') \to 0$. □

References

[1] Z. Borevich and I. Shafarevič. *Number Theory*, Academic Press, New York, 1966.

[2] E.J. Ditters. Higher Hasse-Witt matrices, *Journées de Géometrie Algébrique de Rennes*, **1**(1978), *Astérisque, Soc. Math. de Fr.*, **63** (1979), 67-71.

[3] A. Grothendieck. Technique de descente et theoremes d'existence en géometrie algébrique, *Séminaire Bourbaki*, **190**(1959).

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

[5] J. Lubin. The canonicity of a cyclic subgroup of an elliptic curve, *Journées de Géometrie Algébrique de Rennes*, **1**(1978), *Astérisque, Soc. Math. de Fr.*, **63** (1979), 165-167.

[6] J. Lubin. Canonical subgroups of formal groups, *Trans. Am. Math. Soc.*, **251** (1979) 103-127.

[7] J. Lubin and J. Tate. Formal moduli for one parameter formal Lie groups, *Bull. Soc. Math. de Fr.*, **85** (1967) 49-60.

[8] B. Mazur. Local flat duality, *Amer. Jo. of Math.*, **92** (1970) 201-223.

[9] B. Mazur and L. Roberts. Local Euler characteristic. *Inventiones Math.*, **9** (1970) 201-234.

[10] L. Roberts. The flat cohomology of group schemes, Ph.D. Thesis, Harvard Univ., 1968.

[11] L. Roberts. The flat cohomology of group schemes of rank p, *Am. Jo. Math.*, **95** (1973) 688-702.

[12] J. Tate. p-divisible groups, *Proc. of a Conf. on Local Fields*, T.A. Springer, Ed., Springer-Verlag, Berlin and New York, 1979, 158-183.