TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 251, July 1979

CANONICAL SUBGROUPS OF FORMAL GROUPS

BY

JONATHAN LUBIN

ABSTRACT. Let R be a complete local domain of mixed characteristic. This paper gives a complete answer to the question: "If F is a one-dimensional formal group over R of finite height, when is there a canonical morphism $F \to F'$ that lifts Frobenius?" For given height h, a universal family of formal groups F with such a morphism is constructed, and the shape of F' is described for small values of h.

Let X be an Abelian variety or a divisible commutative formal group, of dimension n, defined over a p-adic integer ring R. Let k be the residue-field of R and $X' = X \times_R k$, and suppose in the Abelian variety case that X' is also an Abelian variety. Then in either case, X' has a canonical subgroupscheme of order p^n, the kernel of the Frobenius morphism frob: $X' \to X'^{(p)}$ where $X'^{(p)}$ may be thought of as the structure obtained from X' by raising the coefficients of all defining relations to the pth power, and frob is the morphism that raises each coordinate of a given point to the pth power.

The question then arises: under what circumstances may there be an X^* and a morphism $\phi: X \to X^*$, both defined over R, such that $(X^*, \phi) \times_R k = (X'^{(p)}, \text{frob})$? An equivalent formulation is: when is there a finite groupscheme Γ of X, defined over R, such that $\Gamma \times_R k = \ker(\text{frob})$? In case R is not highly-enough ramified over Z_p, there may be no lifting of the kernel of Frobenius **[10]**, but in general a finite extension of R will bring in subgroups reducing to ker(frob). The question to be attacked here is rather: under what conditions is there a canonical lifting of the kernel of Frobenius? Although I will treat only the one-dimensional formal case in this paper, I can point out here the original motivation for this question, which comes from the study of elliptic curves. If E is an elliptic curve over R with good reduction, then "reduction modulo p" sends geometric points of E to geometric points of E'. Calling $[p]_E$ the endomorphism "multiplication by p" on E, we see that if E' is ordinary, i.e. not supersingular, then $\ker[p]_E$ has exactly p points that go to identity under reduction modulo p. Thus when E' is ordinary

$$\ker(\text{reduction mod}\, p) \cap \ker[\,p\,]_E$$

Received by the editors August 9, 1977.
AMS (MOS) subject classifications (1970). Primary 14L05; Secondary 14D15; 14D20.

0002-9947/79/0000-0305/$07.25

is the subgroup of E of order p whose associated groupscheme is the lifting of ker(frob). But if E' is supersingular, everything in $\ker[p]_E$ is annihilated under reduction modulo p. A simple pair of examples that suggests the complications that arise, is the following:

(a) $y^2 + y = x^3$ defined over Z_2,

(b) $y^2 + \sqrt{2}\, xy + y = x^3$ over $Z_2[\sqrt{2}\,]$.

Since points of order two are just those where the tangent is vertical, one sees easily that in case (a), all three points (α, β) in ker[2] that are different from the neutral point at infinity have $v_2(\alpha) = -2/3$ (two-adic valuation written additively and normalized so that $v_2(2) = 1$), and in fact these three points are conjugate over Z_2, thus indistinguishable in an essential way. On the other hand, in case (b), there is one point (α, β) in ker[2] for which $v_2(\alpha) = -1$, while if (γ, δ) is either of the others (other than the neutral point), then $v_2(\gamma) = -1/2$. In this case, the group consisting of the neutral point and (α, β) is the desired canonical subgroup. In terms of the methods developed in this paper, the difference between the two examples is that in case (a), the 2-adic valuation of the "formal modulus" is $\geqslant p/(p+1)$, while in case (b), the formal modulus is $\sqrt{2}$, whose 2-adic valuation is $\frac{1}{2} < p/(p+1)$.

The question of the existence of canonical subgroups of elliptic curves began with Deligne and Tate, who analysed the p-adic properties of the classical modular equation $\Phi_p(X, Y) = 0$. The polynomial $\Phi_p(X, Y)$ has its coefficients in Z, is symmetric and of degree $p + 1$ in each variable, and has the property that for elliptic curves E and E', there is an isogeny of degree p from E to E' if and only if $\Phi_p(j(E'), j(E)) = 0$. Let K be a p-adic local field, with ring of integers R and maximal ideal $m \subset R$, and let $\{\beta_1, \ldots, \beta_n\}$ be elements of an unramified extension of Q_p representing all the j-invariants in characteristic p of supersingular elliptic curves. It is clear that if j is an element of K which is incongruent modulo m to all the β_i, then since any E defined over K with invariant j has a canonical subgroup S of order p defined over K, there is a canonical value $j' \in K$, namely the invariant of $E' = E/S$, with $\Phi_p(j', j) = 0$. The mapping $j \mapsto j'$ is p-adically analytic. Tate showed in the case $p = 2$, and Deligne proved generally, that this mapping could be extended from the set where $v_p(j - \beta_i) \leqslant 0$ for all i to the set where $v_p(j - \beta_i) < p/(p+1)$ for all i. Deligne's theorem is fully treated in [3], but from a standpoint that de-emphasizes the role of the canonical subgroup, while Katz in [4] has given a detailed theory of canonical subgroups of elliptic curves.

In this paper I will concentrate entirely on the case of formal groups of dimension one, leaving the study of higher-dimensional Abelian varieties and formal groups to later papers. The first sections are concerned with the existence of canonical subgroups of formal groups defined over rings of integers in finite field extensions of Q_p, and with the shape of the quotient-groups. The last sections describe just what local families of formal groups have canonical subgroups, and in an appendix is proved a "Local Factorization Principle" which is used throughout the paper.

As a general source of background, **[1]**, **[5]** or **[7]** may be suggested. We will be using without comment the existence, but not the explicit construction, of quotients of formal groups by finite subgroups: **[8]** works for the one-dimensional case, but a more general and more abstract way of looking at it can be found in **[11]** or **[2]**.

Standard notations used here will be: $\mathbf{R}$, the field of real numbers; Z, the ring of integers, $R[[x]]$, the ring of formal power series over the ring R, in the variable x or the set of variables denoted by x; Q_p, the field of p-adic numbers; Z_p, the ring of p-adic integers; v, the p-adic valuation on any algebraic extension of Q_p, additively written and normalized so that $v(p) = 1$; $[n]_F$, the endomorphism of multiplication by n in a commutative formal group F. All formal groups mentioned in this paper will be commutative and one-dimensional.

This paper is the result of research done over a fairly long period, and I can thank here only a few of the institutions and persons whose help I benefited from: N. Katz, the Institut Henri Poincaré, the Piscine Deligny, G. B. Winters, the National Science Foundation, K. Lønsted, and Københavns Universitets Matematiske Institut.

1. Standard generic formal groups; the Local Factorization Principle. To begin, let us recall some concepts from **[9]**.

Let (r, m) be a local ring with residue-field $k = r/m$. A homomorphism of r-formal groups, ϕ: $F \to G$, is a **-isomorphism* if $F \times_r k = G \times_r k$, and $\phi \times_r k$ is the identity. Suppose that r is complete and noetherian and that k is of characteristic $p > 0$. Given a one-dimensional commutative formal group F over r, of finite height h, the functor that associates to each complete noetherian local r-algebra (R, M) the set of *-isomorphism classes of R-formal groups G for which $G \times_R (R/M) = F \times_r (R/M)$ is representable by formal-affine $(h-1)$-space over r. To be down-to-earth, we can say that there is then a formal group $\Gamma_{t_1, \ldots, t_{h-1}}$ defined over $r[[t]] = r[[t_1, \ldots, t_{h-1}]]$, such that

(1) $\Gamma_0 = F$,

(2) If G is an R-formal group with $G \times_R (R/M) = F \times_r (R/M)$, then there is a unique $(h-1)$-tuple $(\alpha_1, \ldots, \alpha_{h-1})$ of elements of M and a unique *-isomorphism ϕ: $G \to \Gamma_\alpha$.

According to **[9]**, Γ_t may be chosen so that

$$\Gamma_{0, \ldots, 0, t_i, \ldots, t_{h-1}}(x, y) \equiv F(x, y) - u_i t_i C_{p^i}(x, y) \bmod (x, y)^{p^i+1},$$

where $C_{p^i}(x,y) = ((x+y)^{p^i} - x^{p^i} - y^{p^i})/p$, and where $(u_1, \ldots, u_{h-1})$ is any $(h-1)$-tuple of units of r. In fact, we can apply [5, Lemma 6, p. 267] to see that the choice $u_i = (1 - p^{p^i - 1})^{-1} \in r$ gives the endomorphism $[p]_t = [p]_{\Gamma_t}$ of Γ_t the form

$$[p]_{0,\ldots,0,t_i,\ldots,t_{h-1}}(x) \equiv [p]_0(x) + t_i x^{p^i} \operatorname{mod}(x^{p^i+1}).$$

In case p generates the maximal ideal m of r, $[p]_t$ necessarily has the form

$$[p]_t(x) = pxg_0(x) + \sum_{i=1}^{h-1} t_i x^{p^i} g_i(x) + x^{p^h} g_h(x),$$

where for each $i < h$, $g_i(x)$ is a unit in $r[[t_1, \ldots, t_i]][[x]]$, and g_h is a unit in $r[[t]][[x]]$. In case Γ_t is of this form, it will be called a *standard generic formal group of height h*.

Now suppose that (R, M) is a local domain, and let $f(x) = \sum_{i=0}^{\infty} a_i x^i \in R[[x]]$. Let $r > 0$. I will say that f *has a vertex at r* if for all i, j with $0 \leq i < r < j$, $a_i^{j-r} a_j^{r-i} / a_r^{j-i} \in M$.

If in addition $n > r$ is such that for all $i < r$ we have $a_i^{n-r}/a_r^{n-i} \in M$, I will say that f is *of contingent order less than n*. This will certainly be the case if a_n is a unit of R.

One sees immediately that in case R is a discrete valuation ring with additive valuation V, the condition

$$V\left(a_i^{j-r} a_j^{r-i} / a_r^{j-i}\right) > 0 \quad (\text{all } i,j \text{ with } 0 \leq i < r < j)$$

is exactly equivalent to the existence of a vertex of the Newton polygon of f at $(r, V(a_r))$. The condition

$$V\left(a_i^{n-r}/a_r^{n-i}\right) > 0 \quad (\text{all } i < r)$$

just says that the segment of the Newton polygon of f that is immediately to the left of $(r, V(a_r))$, when extended rightwards, crosses the horizontal axis at or to the left of $(n, 0)$.

The following proposition is proved in the Appendix, but will be used throughout this paper.

LOCAL FACTORIZATION PRINCIPLE. *Let (R, M) be a complete local domain which is integrally closed, and let $f(x) = \sum_{i=0}^{\infty} a_i x^i \in R[[x]]$. If f has a vertex at $r > 0$ and finite contingent order, then $f(x) = g(x) \cdot h(x)$ where $g(x)$ is a monic polynomial of degree r over R with $g(x) \equiv x^r \operatorname{mod} M$, and $h(x) \in R[[x]]$. Furthermore, if ϕ: $R \to R_0$ is a local morphism into a rank-one valuation ring with additive valuation V, and if $\phi(a_r) \neq 0$, then for every root ρ of g^{ϕ} and every root σ of h^{ϕ} in R_0, we have $V(\rho) > V(\sigma)$.*

(In the special case that a_r is a unit of R, the Local Factorization Principle is a corollary of the Weierstrass Preparation Theorem.)

2. Existence of canonical subgroups. In this section, A will denote the ring of v-integers in a field K which is complete with respect to a rank-one valuation v that extends the p-adic valuation of Q_p, $\bar{K}$ will denote a fixed algebraic closure of K, and $\bar{A}$ will be the integral closure of A in $\bar{K}$.

Let F be any one-dimensional formal group over A. The set $\{\alpha \in \bar{K}: v(\alpha) > 0\}$ becomes a group $F(\bar{A})$ under F by the rule $(\alpha, \beta) \to F(\alpha, \beta)$ since any two elements of $\bar{K}$ are in a finite extension of K, which is complete with respect to v. In fact, since $F(\alpha, \beta) = \alpha + \beta +$ terms involving both α and β, we have $v(F(\alpha, \beta)) \geqslant \min(v(\alpha), v(\beta))$, and so $F(\bar{A})$ has a natural filtration: for any positive real number λ we set $F(\bar{A})_\lambda = \{\alpha \in \bar{K}: v(\alpha) \geqslant \lambda\}$, a subgroup of $F(\bar{A})$ which in fact is independent of the coordinatization of F. That is, if $\phi: F \to F'$ is an isomorphism, $\phi(F(\bar{A})_\lambda) = F'(\bar{A})_\lambda$.

DEFINITION. If S is a finite subgroup of $F(\bar{A})$, the subgroup S' of S is a *congruence subgroup of* S if there is a positive real number λ for which $S' = S \cap F(\bar{A})_\lambda$.

DEFINITION. The subgroup S of $F(\bar{A})$ is a *congruence-torsion subgroup of* F if there is a positive real number λ for which $S = \{\alpha \in F(\bar{A})_\lambda$: there is an n such that $[p^n]_F(\alpha) = 0\}$.

It is not hard to see that a congruence-torsion subgroup must be finite.

A finite flat subgroupscheme of a formal group F over A will be $\mathrm{Spec}(A[[x]]/(f(x)))$, where f is a monic polynomial over A such that $f(x) \equiv x^n \bmod m$, where m is the maximal ideal of A, and $n > 0$ is the degree of f, and such that $f(F(x, y))$ is in the ideal $(f(x), f(y))$ of $A[[x, y]]$. Examples are the monic polynomials that come via the Weierstrass Preparation Theorem from the power series $[p^n]_F(x)$, if F is of finite height.

DEFINITION. If G is a finite flat subgroupscheme of F, then a subgroupscheme G' of G is a *congruence subgroupscheme of* G if $G'(\bar{A})$ is a congruence subgroup of $G(\bar{A})$. G is a *congruence-torsion subgroupscheme of* F if $G(\bar{A})$ is a congruence-torsion subgroup of $F(\bar{A})$.

The canonical lifting of the kernel of the Frobenius morphism that we are looking for is just a congruence subgroupscheme of order p in $\ker([p]_F)$. The questions to be answered in this paper are: when does a formal group have a congruence-torsion subgroupscheme of order p, and what is the shape of the quotient group with respect to it; is there a universal formal group with such a subgroupscheme; and some other questions formed from these by straightforward generalization.

THEOREM A. *Let A_0 be the ring of integers of a complete unramified field extension K_0 of Q_p, and let Γ_t be a standard generic formal group of height $h < \infty$ defined over $A_0[[t_1, \ldots, t_{h-1}]]$. If K is a complete field extension of K_0, and A is the ring of integers of K, with maximal ideal m, and if $(\alpha_1, \ldots, \alpha_{h-1})$ is an $(h-1)$-tuple of elements of m, then a necessary and sufficient condition* *for* Γ_α *to have a congruence-torsion subgroupscheme of order p is*

$$v(\alpha_1) < (p^h - p)/(p^h - 1)$$

and for each i with $1 < i < h$, $v(\alpha_1) < (p^i - p + (p-1)v(\alpha_i))/(p^i - 1)$.

If Γ_α *has such a subgroupscheme G, then* $G \times (A/m)$ *is the kernel of the Frobenius morphism on* $\Gamma_\alpha \times (A/m)$.

PROOF. That the stated inequalities among the $v(\alpha_i)$ are equivalent to the existence of a congruence-torsion subgroup of $F(\bar{A})$ follows from a concatenation of the formula

$$[p]_\alpha(x) = pxg_0(x) + \sum_{i=1}^{h-1} \alpha_i x^{p^i} g_i(x) + x^{p^h} g_h(x)$$

with the Local Factorization Principle.

Indeed, if we write $[p]_\alpha(x) = \sum_{i=1}^{\infty} a_i x^i$, then for $p^i \leqslant j < p^{i+1}$ and $i < h$, we have $v(a_j) \geqslant \min(1, v(\alpha_1), \ldots, v(\alpha_i))$. Thus for the inequalities $v(a_i^{j-p} a_j^{p-i} / a_p^{j-i}) > 0$ $(1 \leqslant i < p < j)$ to be satisfied, it is enough for the inequalities $v(a_1^{p^j - p} a_{p^j}^{p-1} / a_p^{p^j - 1}) > 0$ $(1 < j \leqslant h)$ to be satisfied. If they are, the Local Factorization Principle applies, and there is a monic polynomial of degree p dividing $[p]_\alpha(x)$, whose roots have greater valuation than all other roots of $[p]_\alpha$. The roots are distinct because the derivative of $[p]_\alpha(x)$ is never zero on $\Gamma_\alpha(\bar{A})$: just differentiate $[p]_\alpha(\Gamma_\alpha(x,y)) = \Gamma_\alpha([p]_\alpha x, [p]_\alpha y)$ with respect to one of the variables. Thus there is a congruence subgroup of the kernel of $[p]$ in $\Gamma_\alpha(\bar{A})$, of order p.

Conversely, if there is a congruence-torsion subgroup of $\Gamma_\alpha(\bar{A})$, of order p, then the Newton polygon of $[p]_\alpha(x)$ will have a vertex at $(p, v(\alpha_1))$ and our inequalities will be satisfied.

In case we do have a congruence-torsion subgroup S of $F(\bar{A})$ of order p, let $f(x)$ be the monic A-polynomial of degree p given to us by the Local Factorization Principle. Of course, $f(x) = \prod_{s \in S}(x - s)$. Let J be the ideal consisting of all power series $\psi(x, y) \in A[[x, y]]$ for which $\psi(s, s') = 0$ whenever $s, s' \in S$. One sees easily enough that $J = (f(x), f(y))$. The fact that S is a group under F implies that $f(F(x, y)) \in J$. Since the kernel of Frobenius in $\Gamma_\alpha \times (A/m)$ is $\mathrm{Spec}((A/m)[x]/(x^p))$, the proof is done.

In a like way, we can ask, if $1 < \nu < h$, about the existence of a congruence subgroupscheme of $\ker([p]_F)$ of order p^ν. Here there are $\nu(h - \nu)$ inequalities to be satisfied:

$$v(\alpha_\nu) < \frac{(p^\nu - p^i)v(\alpha_j) + (p^j - p^\nu)v(\alpha_i)}{p^j - p^i}$$

for all i, j with $0 \leqslant i < \nu < j \leqslant h$, where we formally write $\alpha_0 = p$ and $\alpha_h = 1$.

3. Valuation function, polytope, and copolytope. Let K be a field with an additive rank-one valuation V. By a *K-formal Laurent series* in $x_1, \ldots, x_n$, I will mean an expression of the form $\Sigma a_M M$ where each $a_M \in K$, and $M = x_1^{e_1(M)} x_2^{e_2(M)} \cdots x_n^{e_n(M)}$, $e_i(M) \in Z$. The K-formal Laurent series form a group but not a ring. The *valuation-function* associated to a K-formal Laurent series $f(x_1, \ldots, x_n)$ is the function V_f: $\mathbf{R}^n \to \overline{\mathbf{R}} = \mathbf{R} \cup \{+\infty, -\infty\}$ defined by $V_f(\xi_1, \ldots, \xi_n) = \inf_M(V(a_M) + \Sigma_{i=1}^n e_i(M)\xi_i)$. One sees that if U is a nonempty open set in $\mathbf{R}^n$ on which V_f never takes the value $-\infty$, then for all $(\beta_1, \ldots, \beta_n) \in K^n$ for which $(V(\beta_1), \ldots, V(\beta_n)) \in U$, the formal sum $f(\beta) = \Sigma a_M \beta_1^{e_1(M)} \cdots \beta_n^{e_n(M)}$ is Cauchy with respect to V, so that if K is complete, $f(\beta)$ is a well-defined element of K. Furthermore, for all $\xi \in U$ except those lying in an exceptional set with empty interior, if $\beta \in K^n$ with $(V(\beta_1), \ldots, V(\beta_n)) = \xi$, then $V(f(\beta)) = V_f(V(\beta_1), \ldots, V(\beta_n))$. For example, if K is any complete extension of Q_p and $f(x) = \mathrm{Log}(x) = \Sigma_{i=1}^{\infty}(-1)^{i+1}x^i/i$, v_f is finite on the open interval $(0, \infty)$ but on no larger interval; and $v(f(\beta)) = v_f(v(\beta))$ as long as $v(\beta) \neq 1/(p-1)p^k$ for a nonnegative integer k.

An m-tuple $f = (f_1, \ldots, f_m)$ of K-formal Laurent series in $x_1, \ldots, x_n$ will give a map V_f: $\mathbf{R}^n \to \overline{\mathbf{R}}^m$. But the association $f \to V_f$ is *not* functorial, as the example $f(x) = p + x$, $g(x) = -p + x$, $V_{f \circ g} \neq V_f \circ V_g$ shows. However, if the V_g-inverse image of the exceptional set of V_f still has empty interior, the relation $V_{f \circ g} = V_f \circ V_g$ will hold. In particular, this is the case if $g(x) \in K[[x]]$ is a power-series in one variable without constant term.

A *cone* in $\mathbf{R}^m$ is a set C with the property that whenever $a, b \in C$ and λ, μ are nonnegative real numbers, $\lambda a + \mu b \in C$. The cone *spanned by* a set X in $\mathbf{R}^n$ is the smallest closed cone containing X.

If $f(x_1, \ldots, x_n) = \Sigma a_M M$ is a K-formal Laurent series, the *Newton cone* of f is the cone spanned in $\mathbf{R}^{n+2}$ by $(0, 0, \ldots, 0, 1, 0)$ and all the points $(e_1(M), e_2(M), \ldots, e_n(M), V(a_M), 1)$; and the *Newton polytope* of f is the intersection of the Newton cone with the hyperplane of all points with last coordinate equal to 1.

The *Newton dual cone* of f is the closed cone consisting of all $(\xi_1, \xi_2, \ldots, \xi_n, \eta, \zeta) \in \mathbf{R}^{n+2}$ such that $0 \leqslant \eta$, and for every M appearing in f,

$$\zeta \leqslant \sum_{i=1}^{n} e_i(M) \cdot \xi_i + V(a_M) \cdot \eta.$$

Except for the unusual coordinatization, this is exactly the dual body of the Newton cone. The *Newton copolytope* of f is the intersection of the dual cone with the hyperplane $\eta = 1$. It is immediate that if $V_f(\xi_1, \ldots, \xi_n) \neq -\infty$, then $(\xi_1, \ldots, \xi_n, 1, V_f(\xi))$ is a boundary point of the Newton copolytope of f. Therefore two formal Laurent series have the same Newton polytope if and only if they have the same valuation function.

4. The quotient by the congruence-torsion subgroup of order p. In this section the notations and conventions are as in §2.

THEOREM B. *Let* A_0 *be the ring of integers in a complete unramified field extension* K_0 *of* Q_p, *let* A *be the ring of integers in a finite field extension* K *of* K_0, *and let* m *be the maximal ideal of* A. *Let* Γ_t *be a standard generic formal group of height* $h < \infty$ *defined over* $A_0[[t_1, \ldots, t_{h-1}]]$, *and let* $\Delta_t = (\Gamma_t)^{\phi}$, *where* $\phi\colon A_0 \to A_0$ *is the Frobenius automorphism of* A_0: $\phi(a) \equiv a^p \bmod pA_0$. *Let* $(\alpha_1, \ldots, \alpha_{h-1})$ *be an* $(h-1)$*-tuple of elements of* m.

(1) *If* $v(\alpha_1) < (p^h - p)/(p^h - 1)$ *and for every* i *with* $1 < i < h$,

$$v(\alpha_1) < \big(p^i - p + (p-1)v(\alpha_i)\big)/\,(p^i - 1),$$

then there is a unique $(h-1)$*-tuple* $(\beta_1, \ldots, \beta_{h-1})$ *of elements of* m *and a unique* $f \in \operatorname{Hom}_A(\Gamma_\alpha, \Delta_\beta)$ *such that* $f(x) \equiv x^p \bmod m$.

(2) *If, in addition, that vertex of the Newton polygon of* $[p]_{\Gamma_\alpha}(x)$ *that is immediately to the right of* $(p, v(\alpha_1))$ *is at* (p^i, c) *and*

$$v(\alpha_1) < \big(p^{i-1} - 1 + (p-1)c\big)/\,(p^i - 1),$$

then whenever (p^j, d) *is on the boundary of the Newton polygon of* $[p]_{\Gamma_\alpha}$, *for* $1 \leqslant j \leqslant h$, *the point* (p^j, pd) *is on the boundary of the Newton polygon of* $[p]_{\Delta_\beta}$.

Comments to Theorem B. In §6 we will see that in fact the β's are analytic functions of $(\alpha_1, \ldots, \alpha_{h-1})$, but throughout this section we will be interested just in $(v(\beta_1), \ldots, v(\beta_{h-1}))$.

The stronger condition on (α), of part (2), will certainly be satisfied if $v(\alpha_1) < 1/(p+1)$. The conclusion in part (2) implies that the vertices of the two Newton polygons are in one-to-one correspondence, and in particular that $v(\beta_1) = pv(\alpha_1)$.

PROOF. The hypotheses guarantee the existence of a congruence-torsion subgroup S of order p, and thus of a quotient formal group $F = \Gamma_\alpha/S$ over A, which may be coordinatized so that $F \times (A/m) = (\Gamma_\alpha \times (A/m))^{(p)} = \Delta_0 \times (A_0/pA_0)$, and so that the quotient morphism $f_0\colon \Gamma_\alpha \to F$ has $f_0(x) \equiv x^p \bmod m$. The existence of a *-isomorphism $F \to \Delta_\beta$ follows from the fact that A is noetherian and Δ_t is a standard generic formal group. Thus part (1) is proved.

Now suppose that (α) satisfies the stronger condition, and let $g\colon \Delta_\beta \to \Gamma_\alpha$ be the left complement of f in $[p]$ namely $g \circ f = [p]_\alpha\colon \Gamma_\alpha \to \Gamma_\alpha$.

The bounded segments of the Newton polygon of $[p](x)$ are in one-to-one correspondence with the vertices of the copolygon; if the slope of a segment is $-\mu$, the first coordinate of the corresponding vertex is μ. The nonzero elements of the congruence-torsion subgroup S of Γ_α correspond to the leftmost nonvertical segment of the polygon from $(1, 1)$ to $(p, v(\alpha_1))$, and thus to the vertex $((1 - v(\alpha_1))/(p-1), \cdot)$ of the copolygon. But these elements of

S are just the nonzero roots of $f(x)$. Thus we know exactly the shape of the copolygon of f: from $(0, 0)$ the first segment rises to the vertex $((1 - v(\alpha_1))/(p-1), (p - pv(\alpha_1))/(p-1))$. This is the only vertex of the copolygon of f; from it proceeds rightwards a segment of slope 1, corresponding to the vertex $(1, \cdot)$ of the polygon. Thus we have:

$$v_f(\xi) = \begin{cases} p\xi & \text{for } 0 < \xi < \dfrac{1 - v(\alpha_1)}{p-1}, \\[2ex] 1 - v(\alpha_1) + \xi & \text{for } \xi > \dfrac{1 - v(\alpha_1)}{p-1}. \end{cases}$$

Since the valuation-function v_p of $[p]_{\Gamma_\alpha}$ is equal to $v_g \circ v_f$, we can say immediately what v_g is. We know from our hypotheses that $(v(\alpha_1) - c)/(p-1) < (1 - v(\alpha_1))/(p-1)$, and that for $(v(\alpha_1) - c)/(p-1) < \xi < (1 - v(\alpha_1))/(p-1)$, $v_p(\xi) = v(\alpha_1) + p\xi$, while for $\xi > (1 - v(\alpha_1))/(p-1)$, $v_p(\xi) = 1 + \xi$. Also, $v_f^{-1}(\xi) = \xi/p$ for $0 < \xi < (p - pv(\alpha_1))/(p-1)$. It follows that

$$v_g(\xi) = \begin{cases} v_p(\xi/p) & \text{for } 0 < \xi < \dfrac{v(\alpha_1) - c}{p^{i-1} - 1}, \\[2ex] v(\alpha_1) + \xi & \text{for } \xi > \dfrac{v(\alpha_1) - c}{p^{i-1} - 1}. \end{cases}$$

But since $[p]_{\Delta_\beta} = f \circ g$, the valuation-function of this power series is just $v_f \circ v_g$. Once we know that $v_g((v(\alpha_1) - c)/(p^{i-1} - 1)) < (1 - v(\alpha_1))/(p-1)$, we can then conclude

$$v_{f \circ g}(\xi) = \begin{cases} pv_p(\xi/p) & \text{for } \xi < \dfrac{v(\alpha_1) - c}{p^{i-1} - 1}, \\[2ex] pv(\alpha_1) + p\xi & \text{for } \dfrac{v(\alpha_1) - c}{p^{i-1} - 1} < \xi < \dfrac{1 - pv(\alpha_1)}{p-1}, \\[2ex] 1 + \xi & \text{for } \xi > \dfrac{1 - pv(\alpha_1)}{p-1}. \end{cases}$$

But

$$v_g\left(\frac{v(\alpha_1) - c}{p^{i-1} - 1}\right) = v(\alpha_1) + \frac{v(\alpha_1) - c}{p^{i-1} - 1} = \frac{p^{i-1}v(\alpha_1) - c}{p^{i-1} - 1},$$

which is less than $(1 - v(\alpha_1))/(p-1)$ because of the hypothesis

$$v(\alpha_1) < \frac{p^{i-1} - 1 + (p-1)c}{p^i - 1}.$$

We now know that if the copolygon of $[p]_{\Gamma_\alpha}$ has a segment given by the formula $\zeta = d + p^j\xi$, $j \neq 0$, then $[p]_{\Delta_\beta}$ has a segment given by the formula $\zeta = pd + p^j\xi$, and conversely. Q.E.D.

Let us observe that for a subgroup S of $\Gamma(\bar{A})$ which is cyclic of order p^r, S is a congruence subgroup of $\ker[p^r]$ if and only if S is a congruence-torsion subgroup of Γ. Indeed, suppose $S = \{\alpha \in \Gamma(\bar{A}): [p^r]_\Gamma(\alpha) = 0 \text{ and } v(\alpha) \geqslant \lambda\}$; without loss of generality, we may suppose that λ is the common valuation of the generators of S. If $[p^s](\beta) = 0$, and $\beta \notin S$, then either $s < r$, when already we know that $v(\beta) < \lambda$, or else $s > r$, in which case we may suppose that $[p^{s-1}](\beta) \neq 0$. Then $[p^{s-r}](\beta) = \beta' \in \ker[p^r]$, with $v(\beta') > v(\beta)$; if $\beta' \notin S$, then $v(\beta') < \lambda$, and if $\beta' \in S$, then β' is a generator of S, so $v(\beta') = \lambda$. Thus S is a congruence-torsion subgroup of Γ. The converse is immediate.

Corollary B. *Let K_0, A_0, K, A, m, and Γ_t be as in Theorem* B. *If $k \geqslant 1$, and $(\alpha_1, \ldots, \alpha_{h-1})$ is an $(h-1)$-tuple of elements of m such that $v(\alpha_1) < 1/p^{k-2}(p+1)$, then Γ_α has a cyclic congruence-torsion subgroup of order p^k.*

Proof. The hypotheses imply that there is a sequence of formal groups, and morphisms lifting Frobenius

$$\Gamma_\alpha = \Gamma^k_{\alpha^k} \xrightarrow{f_k} \Gamma^{k-1}_{\alpha^{k-1}} \to \cdots \to \Gamma^1_{\alpha^1} \xrightarrow{f_1} \Gamma^0_{\alpha^0}$$

where $\alpha^j = (\alpha_1^{(j)}, \ldots, \alpha_{h-1}^{(j)})$, $\Gamma_t^k = \Gamma_t$, $\alpha^k = \alpha$, and $\Gamma_t^j = (\Gamma_t^{j+1})^\phi$, so that all the Γ_t^j are standard generic formal groups over $A_0[[t_1, \ldots, t_{h-1}]]$. We know that if $j \geqslant 1$,

$$v(\alpha_1^{(j)}) = pv(\alpha_1^{(j+1)}) < 1/p^{j-2}(p+1).$$

For typographical convenience, write F_j for $\Gamma^j_{\alpha^j}$, and a_j for $v(\alpha_1^{(j)})$.

We can see by induction that the copolygon of $f_1 \circ f_2 \circ \cdots \circ f_j$ has as its first segment the line $\zeta = p^j\xi$ and as its second the line $\zeta = 1 - a_1p^{j-1}\xi$: this is true for $j = 1$, and if it is true for $j - 1$, then since the copolygon of f_j has only two segments, given by $\zeta = p\xi$ and $\zeta = 1 - a_j + \xi$, and since the first segment of the copolygon of $f_1 \circ \cdots \circ f_{j-1}$ has equation $\zeta = p^{j-1}\xi$, the second segment of the copolygon of $f_1 \circ \cdots \circ f_j$ is given by the smaller of the two expressions $1 - a_1 + p^{j-1}\xi$ and $p^{j-1}(1 - a_j + \xi) = p^{j-1} - a_1 + p^{j-1}\xi$. In particular this is true for $j = k$, so that the first vertex of the copolygon of $f_1 \circ f_2 \circ \cdots \circ f_k$ is $((1 - a_1)/(p^k - p^{k-1}), \cdot)$.

Now the next-to-last vertex of the copolygon of $[p]_{F_k}$ is located at $(\lambda, \cdot)$, where $-\lambda$ is the slope of the second nonvertical segment of the polygon. This segment runs from (p, a_k) to (p^j, c) for some $j > 1$ and $c > 0$, so its slope is at least $a_k/(p - p^2)$: that is, $\lambda < a_k/(p^2 - p) = a_1/(p^{k+1} - p^k)$. But the hypothesis $a_k < 1/(p^{k-2} + p^{k-1})$ implies $a_1 < p/(p+1)$, which in turn implies $a_1/(p^{k+1} - p^k) < (1 - a_1)/(p^k - p^{k-1})$. Thus the only nonvertical segment of the polygon of $[p]_{F_k}$ of slope less than $-a_1/(p^{k+1} - p^k)$ is the first one, from (1, 1) to (p, a_k). This shows that the intersection of the kernels of $f_1 \circ f_2 \circ \cdots \circ f_k$ and $[p]_{F_k}$ is of order p. So the kernel of $f_1 \circ \cdots \circ f_k$ is cyclic, and since it is of order p^k, it is contained in $\ker([p^k])$. Now if it ever happens that $\ker[p]$ has only p elements s with $v(s) > \mu$, then for each j, $\ker[p^j]$ will have at most p^j such elements s. We apply this with $\mu = a_1/(p^{k+1} - p^k)$ to see that $\ker([p^k])$ has exactly p^k elements of value greater than $a_1/(p^{k+1} - p^k)$, namely the elements of $\ker(f_1 \circ \cdots \circ f_k)$, which is thus seen to be a congruence subgroup of $\ker[p^k]$.

5. Special results for heights 2 and 3.

THEOREM C2. *Let K_0, A_0, K, A, m, Γ_t, and Δ_t be as in Theorem* B, *but with $h = 2$. For each $\alpha \in m$ with $v(\alpha) < p/(p + 1)$, let β be the element of m for which there is a canonical morphism f: $\Gamma_\alpha \to \Delta_\beta$ which lifts Frobenius. Then*:

1. *If $v(\alpha) < 1/(p + 1)$, then $v(\beta) = pv(\alpha)$.*
2. *If $v(\alpha) = 1/(p + 1)$, then $v(\beta) \geqslant p/(p + 1)$.*
3. *If $1/(p + 1) < v(\alpha) < p(p + 1)$, then $v(\beta) = 1 - v(\alpha)$.*

PROOF. The first assertion is contained in the conclusion of Theorem B.

In case $v(\alpha) = 1/(p + 1)$, the Newton copolygon of $[p]_{\Gamma_\alpha}$ has vertices at $(1/(p^3 - p), p/(p^2 - 1))$ and $(p/(p^2 - 1), (p^2 + p - 1)/(p^2 - 1))$, so that the valuation-function of f is

$$v_f(\xi) = \begin{cases} p\xi & \text{if } \xi \leqslant p/(p^2 - 1), \\ p/(p + 1) + \xi & \text{if } \xi \geqslant p/(p^2 - 1). \end{cases}$$

If $g \circ f = [p]_{\Gamma_\alpha}$, then the valuation-function of g is

$$v_g(\xi) = \begin{cases} p\xi & \text{if } \xi \leqslant 1/(p^2 - 1), \\ 1/(p + 1) + \xi & \text{if } \xi \geqslant 1/(p^2 - 1). \end{cases}$$

But $v_f \circ v_g(\xi) = p^2\xi$ if $\xi \leqslant 1/(p^2 - 1)$ and $v_f \circ v_g(\xi) = 1 + \xi$ if $\xi \geqslant 1/(p^2 - 1)$. Thus the polygon of $[p]_{\Delta_\beta}$ has only the vertices $(p^2, 0)$ and $(1, 1)$: $v(\beta) \geqslant p/(p + 1)$.

In case $1/(p + 1) < v(\alpha) = a < p/(p + 1)$, the vertices of the Newton copolygon of $[p]_{\Gamma_\alpha}$ are at $(a/(p^2 - p), pa/(p - 1))$ and $((1 - a)/(p - 1), (p - a)/(p - 1))$, so that v_f and v_g are given as:

$$v_f(\xi) = \begin{cases} p\xi & \text{if } 0 \leqslant \xi \leqslant (1 - a)/(p - 1), \\ 1 - a + \xi & \text{if } \xi \geqslant (1 - a)/(p - 1), \end{cases}$$

$$v_g(\xi) = \begin{cases} p\xi & \text{if } 0 \leqslant \xi \leqslant a/(p - 1), \\ a + \xi & \text{if } \xi \geqslant a/(p - 1). \end{cases}$$

Again the valuation-function of $[p]_{\Delta_\beta}$ is $v_f \circ v_g$:

$$v_f \circ v_g(\xi) = \begin{cases} p^2\xi & \text{if } 0 < \xi < \dfrac{1-a}{p^2-p}, \\ 1-a+p\xi & \text{if } \dfrac{1-a}{p^2-p} < \xi < \dfrac{a}{p-1}, \\ 1+\xi & \text{if } \xi > \dfrac{a}{p-1}. \quad \text{Q.E.D.} \end{cases}$$

Thus there is a mapping π that associates to any $\alpha \in m$ with $1/(p+1) < v(\alpha) < p/(p+1)$, the element β in the same set, and according to part 3 of Theorem C2, $v(\pi(\pi(\alpha))) = v(\alpha)$. But unless $\Gamma_t = \Delta_t$, it makes no sense to compose π with itself. However, we can see that there is a natural choice of a mapping π' that will associate a $\Gamma_{\pi'(\alpha)}$ to a Δ_α.

If $F(x,y)$ is any formal group of height two over a field k of characteristic p, then $[p]_F(x) = \gamma(x^{p^2})$, with $\gamma'(0) \neq 0$, so that, in addition to frob $\in \operatorname{Hom}_k(F, F^{(p)})$, $\operatorname{frob}(x) = x^p$, we have the Verschiebung vers $\in \operatorname{Hom}_k(F^{(p)}, F)$, $\operatorname{vers}(x) = \gamma(x^p)$. And γ is an isomorphism, in $\operatorname{Hom}_k(F^{(p^2)}, F)$.

Now suppose we are given $\alpha \in m$, and wish to lift vers: $\Delta_0 \times (A_0/pA_0) \to \Gamma_0 \times (A_0/pA_0)$ to $g\colon \Delta_\alpha \to \Gamma_\beta$ for some $\beta \in m$. A routine argument shows that there is such a g if and only if $v(\alpha) < p/(p+1)$; and that the same relations between α and β hold in this case as in Theorem C2. We can call the particular $\beta \in m$ that arises, $\beta = \pi'(\alpha)$.

Theorem D2. *Let $K_0, A_0, K, A, m, \Gamma_t, \Delta_t$ be as in Theorem* B, *but with $h = 2$. For each $\alpha \in m$ with $v(\alpha) < p/(p+1)$, let $f_\alpha\colon \Gamma_\alpha \to \Delta_{\pi(\alpha)}$ be the canonical lifting of* frob, *and let $g_\alpha\colon \Delta_\alpha \to \Gamma_{\pi'(\alpha)}$ be the canonical lifting of* vers.

If $1/(p+1) < v(\alpha) < p/(p+1)$, then $\pi'(\pi(\alpha)) = \alpha$, and $g_{\pi(\alpha)} \circ f_\alpha = [p]_{\Gamma_\alpha}$.

Proof. The valuation-function of f_α is

$$v_f(\xi) = \begin{cases} p\xi & \text{if } \xi < (1-v(\alpha))/(p-1), \\ 1-v(\alpha)+\xi & \text{if } \xi > (1-v(\alpha))/(p-1). \end{cases}$$

If ρ is a root of $[p]_{\Gamma_\alpha}$, then either $f_\alpha(\rho) = 0$, or else $v(\rho) = v(\alpha)/(p^2-p) < (1-v(\alpha))/(p-1)$, in which case $v(f_\alpha(\rho)) = v(\alpha)/(p-1)$. But the congruence subgroup of $\ker([p]_{\Delta_{\pi(\alpha)}})$ consists of the elements whose valuation is

$$\frac{1-v(\pi(\alpha))}{p-1} = \frac{v(\alpha)}{p-1},$$

so that $g_{\pi(\alpha)}(f_\alpha(\rho)) = 0$. Now $g_{\pi(\alpha)} \circ f_\alpha$ has only p^2 roots, and so its kernel is the same as that of $[p]_{\Gamma_\alpha}$. Hence there is an isomorphism $\psi\colon \Gamma_\alpha \to \Gamma_{\pi'(\pi(\alpha))}$ such that $\psi \circ [p]_\alpha = g_{\pi(\alpha)} \circ f_\alpha$. But $[p]_\alpha(x) \equiv (g_{\pi(\alpha)} \circ f_\alpha)(x) \bmod m$, so that $\psi(x) \equiv x \bmod m$: ψ is a *-isomorphism, and thus $\alpha = \pi'(\pi(\alpha))$, and $\psi(x) = x$. Q.E.D.

We may look at the above phenomenon from a different angle when K_0 is the quadratic unramified extension of Q_p. Then we have not only $\Delta_t = (\Gamma_t)^\phi$, but also $\Gamma_t = (\Delta_t)^\phi$.

THEOREM D2′. *Let $K_0, A_0, K, A, m, \Gamma_t, \Delta_t$ be as in Theorem* B, *but with $[K_0 : Q_p] = h = 2$. For each $\alpha \in m$ with $v(\alpha) < p/(p+1)$, let f_α: $\Gamma_\alpha \to \Delta_{\pi(\alpha)}$ and g_α: $\Delta_\alpha \to \Gamma_{\pi'(\alpha)}$ be the canonical liftings of Frobenius. Let u be the automorphism of $\Gamma_0 \times (A_0/pA_0)$ for which $([p]_\Gamma \circ u)(x) = x^{p^2}$.*

If $1/(p+1) < v(\alpha) < p/(p+1)$, then $\pi'(\pi(\alpha)) = u^\cdot(\alpha)$, where $u^\cdot(t) \in A_0[[t]]$ is the unique power series for which there is an isomorphism $\psi(x) \in \mathrm{Hom}_{A_0[[t]]}(\Gamma_t, \Gamma_{u^\cdot(t)})$ such that $\psi(x) \times (A_0/pA_0) = u(x)$.

The proof is similar to that of Theorem D2. Later in §6, we will see that π is actually A_0-analytic; it follows then that $\pi' = \pi^\phi$. The transformations $u^\cdot$ are more fully treated in [9, §3.4].

When the height is greater than two, phenomena are more complex.

THEOREM C3. *Let $K_0, A_0, K, A, m, \Gamma_t$, and Δ_t be as in Theorem* B, *but with $h = 3$. For each pair $(\alpha_1, \alpha_2) \in m \times m$ for which Γ_α has a congruence-torsion subgroup of order p, let (β_1, β_2) be the associated pair, so that there is a canonical lifting f: $\Gamma_\alpha \to \Delta_\beta$ of Frobenius. Then*:

1. *If $v(\alpha_1) < (p^2-1)/(p^3-1)$ and $v(\alpha_2) > pv(\alpha_1)/(p+1)$, then*

$$v(\beta_1) = pv(\alpha_1) \quad \textit{and} \quad v(\beta_2) > \frac{p}{p+1} v(\beta_1).$$

2. *If $v(\alpha_1) = (p^2-1)/(p^3-1)$ and $v(\alpha_2) > (p^2-p)/(p^3-1)$, then*

$$v(\beta_1) > \frac{p^3-p}{p^3-1} \quad \textit{and} \quad v(\beta_2) > \frac{p^3-p^2}{p^3-1}.$$

3. *If $(p^2-1)/(p^3-1) < v(\alpha_1) < (p^3-p)/(p^3-1)$ and $v(\alpha_2) > pv(\alpha_1)/(p+1)$, then*

$$v(\beta_2) = 1 - v(\alpha_1) \quad \textit{and} \quad v(\beta_1) > \frac{p + v(\beta_2)}{p+1}.$$

4. *If $(p+1)v(\alpha_2)/p < v(\alpha_1) < (1 + v(\alpha_2))/(p+1)$, then*

$$v(\beta_1) = pv(\alpha_1) \quad \textit{and} \quad v(\beta_2) = pv(\alpha_2).$$

5. *If $v(\alpha_1) = (1 + v(\alpha_2))/(p+1)$ and $v(\alpha_2) < (p^2-p)/(p^3-1)$, then*

$$v(\beta_2) = pv(\alpha_2) \quad \textit{and} \quad v(\beta_1) > \frac{p + v(\beta_2)}{p+1}.$$

6. *If* $(1 + v(\alpha_2))/(p + 1) < v(\alpha_1) < (p + v(\alpha_2))/(p + 1)$ *and* $v(\alpha_1) < 1 - pv(\alpha_2)$, *then*

$$v(\beta_1) = 1 - v(\alpha_1) + v(\alpha_2) \quad \textit{and} \quad v(\beta_2) = pv(\alpha_2).$$

7. *If* $v(\alpha_1) = 1 - pv(\alpha_2)$ *and* $(p^2 - 1)/(p^3 - 1) < v(\alpha_1) < (p^3 - p^2 + p - 1)/(p^3 - 1)$, *then*

$$v(\beta_1) = 1 - v(\alpha_1) + v(\alpha_2) \quad \textit{and} \quad v(\beta_2) \geqslant \frac{p}{p+1} v(\beta_1).$$

8. *If* $(p + 1)v(\alpha_2)/p < v(\alpha_1) < (p + v(\alpha_2))/(p + 1)$ *and* $v(\alpha_1) > 1 - pv(\alpha_2)$, *then*

$$v(\beta_1) = 1 - v(\alpha_1) + v(\alpha_2) \quad \textit{and} \quad v(\beta_2) = 1 - v(\alpha_1).$$

The proof of Theorem C3 runs like that of C2. The theorem itself is really a statement about the way the Newton polygon of $[p]_{\Delta_\beta}$ compares with that of $[p]_{\Gamma_\alpha}$. The qualitative information is summarized in the table below, and the accompanying diagram shows where each of the eight kinds of behavior occurs.

The analog of the interval $(1/(p + 1), p/(p + 1))$ of Theorem D2′ is the triangle within which Case 8 holds. This triangle is stable under the transformation $(a_1, a_2) \to (1 - a_1 + a_2, 1 - a_2)$, which is in fact an automorphism of order three. The statement and proof of Theorem D3′, parallel to D2′, are left to the interested reader.

6. The universal family of formal groups with congruence-torsion subgroups of order p. In this section, K will be a field complete with respect to a discrete rank-one valuation v which extends the p-adic valuation on Q_p.

DEFINITION. Let $n \geqslant 1$, and let C be a closed cone in $\mathbf{R}^{n+1}$ that contains $(0, 0, \ldots, 0, 1)$. If $f(t_1, \ldots, t_n) = \sum_M a_M M$ is a K-formal Laurent series, f is *C-bounded* if for every $M = \prod_{i=1}^n t_i^{e_i(M)}$, $(e_1(M), e_2(M), \ldots, e_n(M), v(a_M)) \in C$. The set of C-bounded K-formal Laurent series will be denoted $L_K(C)$.

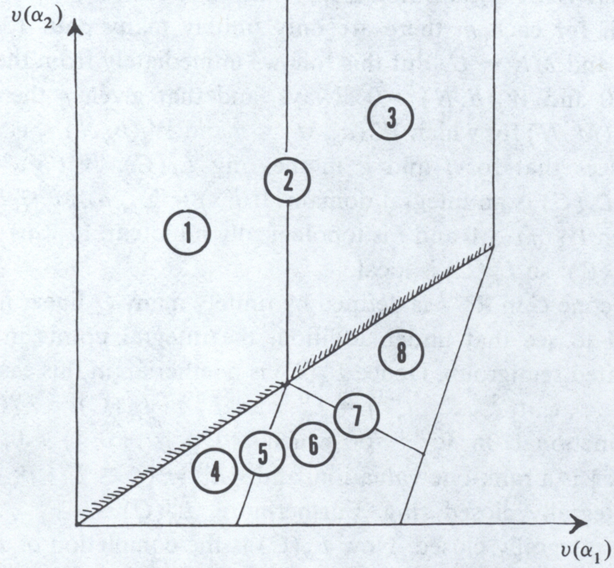
PROPOSITION α. *If C is a closed cone in* $\mathbf{R}^{n+1}$ *that contains* $(0, 0, \ldots, 0, 1)$ *but contains no lines, then $L_K(C)$ is a commutative ring, without zero-divisors, local, and integrally closed.*

If furthermore C is defined by finitely many Q-linear inequalities, then $L_K(C)$ is noetherian.

PROOF. The hypothesis that C contains no lines means exactly that the dual body C^D has nonempty interior.

The set of monomials in $K[t_1, t_2, \ldots, t_n, t_1^{-1}, \ldots, t_n^{-1}]$ can be mapped into $\mathbf{R}^{n+1}$ in a natural way:

$$at_1^{e_1} \cdots t_n^{e_n} \xrightarrow{i} (e_1, e_2, \ldots, e_n, v(a)).$$



Case	Vertices of $[p]_{\Gamma_\alpha}$	Vertices of $[p]_{\Delta_\beta}$
1	at p but not at p^2	at p only
2		at neither p nor p^2
3		at p^2 only
4	at both p and p^2	at both p and p^2
5		at p^2 only
6		at both p and p^2
7		at p only
8		at both p and p^2

Let ψ be a fixed functional in the interior of C^D; we define W_ψ: $L_K(C) \to \mathbf{R} \cup \{\infty\}$ by the rule $W_\psi(0) = +\infty$, and $W_\psi(\Sigma_M a_M M) = \inf_M(\psi(i(a_M M)))$. This infimum is actually a minimum. We have, for $f, g \in L_K(C)$: $W_\psi(f) \geqslant 0$; $W_\psi(f) = \infty$ if and only if $f = 0$; and $W_\psi(f + g) \geqslant \min(W_\psi(f), W_\psi(g))$. The group $L_K(C)$ is thus topologized by the subgroups $S_m = \{f\colon W_\psi(f) \geqslant m\}$, and is complete with respect to this topology, because of K's completeness with respect to v.

Multiplication in $L_K(C)$ is to be defined by the rule

$$\left(\sum_M a_M M\right)\left(\sum_M b_M M\right) = \sum_U \left(\sum_{MN = U} a_M b_N\right) U,$$

which will make sense if each sum $\Sigma_{MN=U}\, a_M b_N$ is convergent in K, or what is the same, if for each m there are only finitely many pairs (M, N) with $v(a_M b_N) \leqslant m$ and $MN = U$. But this follows immediately from the facts that $W_\psi(a_M M) \geqslant 0$ and $W_\psi(b_N N) \geqslant 0$ always, and that given ν there are only finitely many (M, N) for which $W_\psi(a_M M) \leqslant \nu$ and $W_\psi(b_N N) \leqslant \nu$.

One now sees that for f and g in the ring $L_K(C)$, $W_\psi(fg) = W_\psi(f) + W_\psi(g)$. Thus $L_K(C)$ is an integral domain. If $f(x) = \Sigma_M\, a_M M \in L_K(C)$, and $v(a_1) > 0$, then $W_\psi(f) > 0$ and f is topologically nilpotent. If $v(a_1) = 0$, then f is a unit in $L_K(C)$: so $L_K(C)$ is local.

In case the cone C in $\mathbf{R}^{n+1}$ is defined by finitely many Q-linear inequalities, it is not hard to see that under addition, the integral points in C form a finitely generated semigroup. Hence $L_K(C)$ is noetherian in this case.

Call $K[t_1, \ldots, t_n, t_1^{-1}, \ldots, t_n^{-1}] = L_K^0$, and $L_K^0 \cap L_K(C) = L_K^0(C)$. If ρ is any linear functional on $\mathbf{R}^{n+1}$ for which $\rho(0, 0, \ldots, 0, 1) > 0$, then W_ρ: $L_K^0 \to \mathbf{R} \cup \{\infty\}$ is a rank-one valuation, and ${}_\rho L_K^0 = \{f \in L_K^0\colon W_\rho(f) \geqslant 0\}$ is clearly an integrally closed ring. Furthermore, $L_K^0(C) = \bigcap_{\rho \in C^D}({}_\rho L_K^0)$, so that $L_K^0(C)$ is integrally closed. Now $L_K(C)$ is the completion of $L_K^0(C)$ with respect to the topology induced by the single valuation W_ψ (ψ still in the interior of C^D), and in the case that C is defined by finitely many Q-linear inequalities, $L_K^0(C)$ is of finite type over the ring of v-integers of K, so that $L_K(C)$ is also integrally closed. In the general case, $L_K(C) = \bigcap_\Gamma L_K(\Gamma)$ where Γ runs through all cones containing C such that Γ is defined by finitely many Q-linear inequalities, so that $L_K(C)$ is again integrally closed. Q.E.D.

The following is an easy exercise.

PROPOSITION β. *In $\mathbf{R}^h$, $h > 1$, let the cone C_h be defined as the set of all $(e_1, e_2, \ldots, e_{h-1}, \bar{e})$ satisfying the inequalities*

$$\sum_{k=1}^{i-1}(p^i - p^k)e_k + (p^i - 1)\bar{e} \geqslant 0, \qquad 2 \leqslant i \leqslant h,$$

$$\bar{e} \geqslant 0,$$

$$e_i \geqslant 0, \qquad 2 \leqslant i \leqslant h - 1. \qquad (N_h)$$

Then the dual cone C_h^D consists of the functionals

$$\psi\colon (e_1, \ldots, e_{h-1}, \bar{e}) \to \sum_1^{h-1} a_i e_i + \bar{a}\bar{e}$$

for which

$$(p^i - 1)a_1 \leqslant (p - 1)a_i + (p^i - p)\bar{a}, \qquad 2 \leqslant i \leqslant h - 1,$$

$$(p^h - 1)a_1 \leqslant (p^h - p)\bar{a},$$

$$0 \leqslant a_i, \qquad 1 \leqslant i \leqslant h - 1, \textit{ and } 0 \leqslant \bar{a}. \qquad (N_h^*)$$

A functional ψ which is strictly positive on all nonzero elements of C_h is necessarily in the interior of C_h^D, and so for such a ψ, the inequalities (N_h^*) will be strict.

DEFINITION. Let $h > 1$. The ring $\mathcal{Q}_h$ is $L_{Q_p}(C_h)$.

Note that C_2 is defined by only two inequalities, and that $\mathcal{Q}_2 = Z_p[[t, p/t, p^p/t^{p+1}]]$.

The following is a direct consequence of Propositions α and β.

PROPOSITION γ. *Let A be a rank-one valuation ring whose valuation function v extends the p-adic valuation on Z_p. If ϕ: $\mathcal{Q}_h \to A$ is a continuous morphism, then the h-tuple $(v(\phi(t_1)), \ldots, v(\phi(t_{h-1})), 1)$ satisfies the strict inequalities (N_h^*); conversely, if $(\alpha_1, \ldots, \alpha_{h-1})$ is an $(h-1)$-tuple of elements of A for which $(v(\alpha_1), \ldots, v(\alpha_{h-1}), 1)$ satisfies the strict inequalities (N_h^*), then there is a unique continuous morphism ϕ: $\mathcal{Q}_h \to A$ for which $\phi(t_i) = \alpha_i$.*

THEOREM E. *Let $K_0, A_0, K, A, m, \Gamma_t$, and Δ_t be as in Theorem* B, *and let $\mathcal{Q}_h' = \mathcal{Q}_h \otimes_{Z_p} A_0$. Then there is a unique $(h-1)$-tuple $\pi(t)$ of elements of the maximal ideal $\mathfrak{M}_h'$ of $\mathcal{Q}_h'$, and a unique $f \in \mathrm{Hom}_{\mathcal{Q}_h'}(\Gamma_t, \Delta_{\pi(t)})$ such that $f(x) \equiv x^p \bmod \mathfrak{M}_h'$. If F is a formal group over A, such that $F \times (A/m) = \Gamma_0 \times (A_0/pA_0)$, and such that F has a congruence-torsion subgroupscheme of order p, then there is a unique morphism of local rings $\mathcal{Q}_h' \to A$, $t_i \to \alpha_i$, such that Γ_α is $*$-isomorphic to F.*

PROOF. Unramifiedness of A_0 over Z_p implies that $\mathcal{Q}_h' = L_{K_0}(C_h)$.

Let $[p]_{\Gamma_t}(x) = \sum_{i=1}^\infty e_i x^i$. We know that if $p^{s-1} \leq i < p^s$, then $c_i \in (p, t_1, \ldots, t_{s-1})$. In particular, if $i < p$, then $c_i \in p\mathcal{Q}_h'$. Also $c_p = t_1 + pd$, but since $p/t_1 \in \mathcal{Q}_h'$, c_p is a unit times t_1.

To apply the Local Factorization Principle to $[p]_\Gamma$, we need first to verify that for $i < p$, $c_i^{p^h-p}/c_p^{p^h-i} \in \mathfrak{M}_h'$, which is true since $p^{p^h-p}/t_1^{p^h-1} \in \mathfrak{M}_h'$. Also we need to verify that if $1 \leq i \leq p < j$, then $c_i^{j-p}c_j^{p-i}/c_p^{j-i} \in \mathfrak{M}_h'$, i.e. that $\gamma_{ij} = p^{j-p}c_j^{p-i}/t_1^{j-i} \in \mathfrak{M}_h'$, but in view of the immediately preceding remarks, it is enough to show this for $j < p^h$. If $p < j < p^2$, then $c_j = \alpha p + \beta t_1$, so $p/t_1 \in \mathfrak{M}_h'$ implies immediately that $\gamma_{ij} \in \mathfrak{M}_h'$. Now let $p^s \leq j < p^{s+1}$, $1 < s < h$. Any monomial appearing in γ_{ij} will be an A_0-multiple of a monomial of form $p^{a_0+j-p}t_1^{a_1+i-j}t_2^{a_2} \cdots t_s^{a_s}$, where the a's are nonnegative, $1 \leq i < p$, and $a_0 + a_1 + \cdots + a_s = p - i$. Let us look at the mth inequality from the list (N_h): we must check that

$$(p^m - p)(a_1 + 1 - j) + \sum_{k=2}^{m-1} (p^m - p^k)a_k + (p^m - 1)(a_0 + j - p) \geq 0.$$

In case $s \geq m$, we rewrite the left-hand side as

$$\sum_{k=0}^{m-1} (p^m - p^k)a_k + (p^m - p)i + (p - 1)j - p^{m+1} + p$$

which is nonnegative, since $j \geqslant p^{m}$ and $i \geqslant 1$. In case $s < m$, the summation now runs only to s, and we write the left-hand side of our inequality as

$$p^m\left(i + \sum_{k=0}^{s} a_k\right) - pi - \sum_{k=0}^{s} p^k a_k + (p-1)j - p^{m+1} + p$$
$$\geqslant -p^s\left(i + \sum_{k=0}^{s} a_k\right) + (p^s - p)i + (p-1)j + p$$
$$= -p^{s+1} + p + (p^s - p)i + (p-1)j,$$

again nonnegative, since $j \geqslant p^s$.

Thus $[p]_{\Gamma_t}(x)$ has a monic factor of degree p, $g_t(x)$, with coefficients in $\mathcal{Q}_h'$, and in fact $g_t(x) \equiv x^p \bmod \mathfrak{M}_h'$, and $g_t(0) \geqslant 0$. g_t defines a flat subscheme of the finite $\mathcal{Q}_h'$-groupscheme $\ker([p]_{\Gamma_t})$. To show that this scheme $\operatorname{Spec}(\mathcal{Q}_h'[[x]]/(g_t(x)))$ is a subgroupscheme, we need only show that $\Gamma_t(g_t(x), g_t(y))$ is contained in the ideal $(g_t(x), g_t(y))$ of $\mathcal{Q}_h'[[x,y]]$. What we know, from the Local Factorization Principle and Proposition γ, is that whenever ϕ: $\mathcal{Q}_h' \to A'$, $\phi(t_i) = \alpha_i$, is a continuous morphism into the ring of integers in a finite field extension K' of K_0, $g_\alpha(x)$ defines a subgroupscheme of $\ker[p]_{\Gamma_\alpha}$.

Since the p^2 elements $x^i y^j$, $0 \leqslant i < p$, $0 \leqslant j < p$, form a free basis for $\mathcal{Q}_h'[[x,y]]/(g_t(x), g_t(y))$ over $\mathcal{Q}_h'$, we have

$$\Gamma_t(g_t(x), g_t(y)) \equiv \sum_{i,j=0}^{p-1} \lambda_{ij}(t) x^i y^j \quad \operatorname{mod}(g_t(x), g_t(y))$$

for suitable $\lambda_{ij}(t) \in \mathcal{Q}_h'$. But each $\lambda_{ij}(t_1, \ldots, t_{h-1})$ is a Laurent series with nonempty domain of convergence (once A' is highly-enough ramified over A_0), given in fact by the inequalities (N_h^*); and $\lambda_{ij}(t)$ is zero no matter how (t) is evaluated at an $(h-1)$-tuple (α) of elements of A' in this domain of convergence. Thus $\lambda_{ij}(t) = 0$, as a glance at the Newton copolytope shows.

That the groupscheme just constructed is the kernel of a morphism f_t: $\Gamma_t \to \Delta_{\pi(t)}$ follows from the universal property of Δ.

Finally, supposing that $F \times (A/m) = \Gamma_0 \times (A_0/pA_0)$, we have a unique *-isomorphism between Γ_α and F for some $(h-1)$-tuple of elements of m. Since Γ_α has a congruence-torsion subgroupscheme of order p, $(v(\alpha_1), \ldots, v(\alpha_{h-1}), 1)$ satisfies the strict inequalities (N_h^*), by Theorem A; by Proposition γ, the map $A_0[[t]] \to A$, $t_i \to \alpha_i$, extends to a morphism from $\mathcal{Q}_h'$ to A. Q.E.D.

Let us return to the case $h = 2$. If we have a pair Γ_t, Δ_t of formal groups of height two, as specified in Theorem C2, then over $\mathcal{Q}_2'$ there is a lifting of the Frobenius morphism, f_t: $\Gamma_t \to \Delta_{\pi(t)}$. In particular, $\pi(t)$ is a Laurent series, in $\mathcal{Q}_2' = A_0[[t, p/t, p^p/t^{p+1}]]$, whose valuation-function, v_π, we know, at least on the open interval $(0, p/(p+1))$: $v_\pi(\xi) = p\xi$ if $0 < \xi \leq 1/(p+1)$, $v_\pi(\xi) = 1 - \xi$ if $1/(p+1) \leq \xi < p/(p+1)$. This is the content of Theorem C2. Since we know the copolygon of $\pi(t)$, we also know the polygon: there is a segment running from $(-1, 1)$ to $(p, 0)$, and no other segments have negative slopes greater than $-p/(p+1)$. If now K is an overfield of K_0, complete with respect to a valuation extending the p-adic valuation on K_0, and $\beta \in K$ with $v(\beta) > 0$, we may try to solve the equation $\pi(t) = \beta$ for t. In case $v(\beta) \geq 1/(p+1)$, the polygon of $\pi(t) - \beta$ is the same as that of $\pi(t)$, and the general theory of factorization of Laurent series, e.g. [6, p. 53, Proposition 2], shows that there are $p+1$ roots α of $\pi(t) - \beta$, all with $v(\alpha) = 1/(p+1)$, corresponding to the unique monic polynomial over K which divides $\pi(t) - \beta$, and whose Newton polygon has only the two vertices $(0, 1)$ and $(p+1, 0)$. In case $1/(p+1) < v(\beta) < p/(p+1)$, the polygon of $\pi(t) - \beta$ has a vertex at $(0, v(\beta))$, and two segments with slopes between $-p/(p+1)$ and 0, while in case $0 < v(\beta) \leq 1/(p+1)$, the polygon of $\pi(t) - \beta$ has only one segment with slope between $-p/(p+1)$ and 0, that being of length p. We thus have:

THEOREM F. *Let K_0, A_0, K, A, Γ_t, and Δ_t be as in Theorem C2. There is a Laurent series $\pi(t) \in A_0[[t, p/t, p^p/t^{p+1}]]$ such that whenever $\alpha \in A$ and $0 < v(\alpha) < p/(p+1)$, there is a lifting f: $\Gamma_\alpha \to \Delta_{\pi(\alpha)}$ of the Frobenius morphism, whose kernel is a congruence-torsion subgroup of Γ_α.*

If $\beta \in A$ and $v(\beta) \geq p/(p+1)$, there are, in any large enough finite field extension of K, $p+1$ elements α such that $\pi(\alpha) = \beta$. They all satisfy $v(\alpha) = 1/(p+1)$.

If $\beta \in A$ and $1/(p+1) < v(\beta) < p/(p+1)$, there is one $\alpha \in K$ with $v(\alpha) = 1 - v(\beta)$ and $\pi(\alpha) = \beta$, and in any large enough finite field extension of K there are p elements α' with $\pi(\alpha') = \beta$, and they all satisfy $v(\alpha') = v(\beta)/p$.

If $\beta \in A$ and $0 < v(\beta) \leq 1/(p+1)$, there are, in any large enough finite field extension of K, p elements α' with $\pi(\alpha') = \beta$, and they all satisfy $v(\alpha') = v(\beta)/p$.

To see that all the α's found are distinct, we can use the derivative of $\pi(t)$. By extending the base, from $A_0[[t, p/t, p^p/t^{p+1}]]$ to $(A_0/pA_0)[[t]]$, one sees that the only unit coefficient of $\pi(t)$ is the one appearing in degree p. Because the polygon of $\pi(t)$ has a vertex at $(-1, 1)$ and no segments to the left of that point with slope greater than $-p/(p+1)$, $t^2\pi'(t)/p$ is not only in $A_0[[t, p/t, p^p/t^{p+1}]]$, but is also a unit there: so has no roots α with $0 < v(\alpha) < p/(p+1)$.

7. Appendix. Proof of the Local Factorization Principle. Throughout this section r will be a fixed positive integer, and n will be an unspecified integer greater than r. Most objects defined or constructed will depend on n, but they will be subscripted with n only when this is necessary. So, below, $A^0 = A^0_n$, $F = F_n$, etc.

We work with the ring $A^0 = Z[t_0, t_1, \ldots, t_n, t_r^{-1}]$; the *degree* of a monomial $M = t_0^{e_0} t_1^{e_1} \cdots t_n^{e_n}$ is Σe_i, and the *moment* of M is $\Sigma(i - r)e_i$. A polynomial in which all monomials have the same degree, respectively moment, is called *homogeneous*, respectively *isobaric*.

Set $I = (t_0, \ldots, t_{r-1}, t_{r+1}, \ldots, t_n)$, an ideal of A^0, and $A =$ the I-adic completion of A^0.

LEMMA Ap1. *Let* $F(x) = \Sigma_{i=0}^n t_i x^i \in A^0[x]$. *Then* $t_r F(x)$ *factors in* $A[x]$: $t_r F(x) = G(x)H(x)$, *with*

$$\begin{aligned} &\deg(G) = r, \quad \deg(H) = n - r, \\ &\textit{the highest coefficient of } G \textit{ is } t_r, \\ &G(x) \equiv t_r x^r \bmod I, \\ &H(x) \equiv t_r \bmod I. \end{aligned} \tag{a}$$

Furthermore, the coefficient of x^i *in* G *is a power series that is homogeneous of degree* 1 *and isobaric of moment* $i - r$, *while the coefficient of* x^i *in* H *is homogeneous of degree* 1 *and isobaric of moment* i.

Finally, this is the only factorization of $t_r F(x)$ *as a product of* A*-polynomials satisfying* (a).

The proof proceeds by the simplest kind of Hensel's Lemma argument.

Let T be the set of monomials in A^0 of form $t_i^{j-r} t_j^{r-i} / t_r^{j-i}$, for $0 \leq i < r < j \leq n$, and let S be the set of all nontrivial monomials in A^0 of degree and moment zero. Then $T \subset S$, and in fact a proof by induction on the number of variables appearing in the monomial M shows:

LEMMA Ap2. (a) *If* $M \in S$, *there is an integer* $N > 0$ *such that* M^N *is a product of elements of* T.

(b) *If* M *is a monomial in the ideal* $(t_0, \ldots, t_i)$ *of* A^0, *with* $\deg(M) = 1$ *and* $\text{moment}(M) = i - r < 0$, *then there is an* $N > 0$ *such that* M^N *is writable as a monomial of* $Z[t_0, \ldots, t_n]$ *times an element of* S.

(c) *If* M *is a monomial in the ideal* $(t_i, \ldots, t_n)$ *of* A^0, *with* $\deg(M) = 1$ *and* $\text{moment}(M) = i - r > 0$, *then there is an* $N > 0$ *such that* M^N *is writable as a monomial of* $Z[t_0, \ldots, t_n]$ *times an element of* S.

One sees that the coefficients of G are Z-linear combinations of monomials satisfying condition (b) of Lemma Ap2. These monomials are consequently integral over $Z[t_0, \ldots, t_n][T]$. Likewise, the coefficients of H are Z-linear combinations of monomials satisfying condition (c), so these monomials are also integral over $Z[t_0, \ldots, t_n][T] \subset A^0$.

Let us call B^0 the integral closure of $Z[t_0, \ldots, t_n][T]$, in its fraction-field.

Then $B^0 \subset A^0$. Let J be the ideal (S) of B^0. We have $J^m \subset I^m$, but the J-adic topology on B^0 is definitely stronger than the (restriction of the) I-adic topology: $t_0^m \to 0$ I-adically but not J-adically. However, it is our aim to show now that the I-adic and J-adic topologies agree on any of the spaces D_m of isobaric polynomials in $A^0[x]$ of moment m.

LEMMA Ap3. *Let M be a monomial in A^0, of moment m, contained in I^ν, where $\nu = n|m| + r^2(n-r)^2 + n(n-r)r/2$. Then $M = M_0 s$, where $s \in T$ and M_0 is a monomial in A^0 of the same degree and weight as M.*

PROOF. Set $M = t_0^{e_0} t_1^{e_1} \cdots t_n^{e_n}$, so that we have

$$e_0 + \cdots + e_{r-1} + e_{r+1} + \cdots + e_n \geqslant n|m| + r^2(n-r)^2 + \frac{nr(n-r)}{2},$$

and consequently either

(case i)

$$e_0 + \cdots + e_{r-1} \geqslant r|m| + \frac{(n-r)(n-r+1)r^2}{2}$$

or else

(case ii)

$$e_{r+1} + \cdots + e_n \geqslant (n-r)|m| + \frac{r(r+1)(n-r)^2}{2}.$$

In case i, one of $e_0, \ldots, e_{r-1}$ must be at least $|m| + (n-r)(n-r+1)r/2$, and so at least $n-r$. In case ii, one of $e_{r+1}, \ldots, e_n$ must be at least $|m| + r(r+1)(n-r)/2$, and so at least r.

If in case i all of $e_{r+1}, \ldots, e_n$ are less than r, then moment$(t_{r+1}^{e_{r+1}} \cdots t_n^{e_n})$ would be less than $r + 2r + \cdots + (n-r)r = r(n-r)(n-r+1)/2$, while moment$(t_0^{e_0} \cdots t_{r-1}^{e_{r-1}}) \leqslant -(n-r)(n-r+1)r/2 - |m|$, so that moment$(M) < -|m| \leqslant m$, a contradiction. Thus in this case we must have one $e_k \geqslant r$, $r < k \leqslant n$, and our previously found $e_i \geqslant n - r$, $0 \leqslant i < r$. In particular, $e_k \geqslant r - i$ and $e_i \geqslant k - r$, so that $M = M_0 s$, $s = t_i^{k-r} t_k^{r-i} / t_r^{k-i}$. The rest of the proof, for case ii, is similar, and since $\deg(s) = \text{moment}(s) = 0$, there is nothing else to prove.

It follows that for fixed moment, the I-adic and J-adic topologies agree. Consequently we define B to be the J-adic completion of B^0, and we see that F factors over B. It only remains to observe that B is still integrally closed. But B^0 is of finite type as a Z-algebra, so excellent, and thus its J-adic completion is integrally closed, since B^0 is.

One says that a topological ring is *linearly topologized* if it has a neighborhood base at 0 consisting of ideals.

DEFINITION. Let R be a linearly topologized ring, and $f \in R[x]$. A pair of R-polynomials (g, h) such that $gh = f$ constitutes a *Newton factorization of f* if for every rank-one valuation ring (R_0, V), every continuous morphism ϕ: $R \to R_0$ for which $f^\phi \neq 0$, every root ρ of g^ϕ in the fraction field K_0 of R_0, and every root σ of h^ϕ in K_0, we have $\infty > V(\rho) > V(\sigma)$.

DEFINITION. Let R be a linearly topologized integral domain, and let $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$. We will say that *$f$ has a vertex at r* if $a_r \neq 0$ and if for all i, j with $0 \leqslant i < r < j \leqslant n$, $a_i^{j-r} a_j^{r-i} / a_r^{j-i}$ is an analytically nilpotent element of R. If moreover $a_i / a_r \in R$ for all $i < r$, we will say that *f has a nonascending earlier segment*; or if $a_i / a_r \in R$ for all $i > r$, we will say that *f has a nondescending later segment*.

LEMMA Ap4. *If R is a linearly topologized integral domain which is separated, complete, and integrally closed, and if $f \in R[x]$ has a vertex at r, then*:

(a) *If a_r is the coefficient of x^r in f, then $a_r f$ has a Newton factorization (g, h) where $g, h \in R[x]$ and* $\deg(g) = r$.

(b) *If f has a nonascending earlier segment, then f has a Newton factorization (g, h) where $g, h \in R[x]$ and g is monic of degree r.*

(c) *If f has a nondescending later segment, then f has a Newton factorization (g, h) where $g, h \in R[x]$, $\deg(g) = r$, and $h(0) = 1$.*

PROOF. (a) Let $f(x) = \sum_{i=0}^{n} a_i x^i$. The morphism $Z[t_0, \ldots, t_n] \to R$ by $t_i \to a_i$ can be extended uniquely to ϕ: $B \to R$, and we need only verify that (G^ϕ, H^ϕ) constitutes a Newton factorization of $a_r f = (t_r F)^\phi$. To do this, we must show that (G, H) is a Newton factorization of $t_r F$.

Let ψ: $B \to R_0$ be continuous, where (R_0, V) is a rank-one valuation ring and $\psi(t_r) \neq 0$, and suppose that the smallest i for which $\psi(t_i) \neq 0$ is $i = \rho$. Consider the coefficient γ of x^ρ in G: it is homogeneous of degree 1, isobaric of moment $\rho - r \leqslant 0$. Any monomial appearing in γ contains at least one of $t_0, \ldots, t_\rho$, so that $\gamma = \delta' + \delta$, where $\psi(\delta') = 0$, and every monomial in δ has t_ρ appearing. Among these monomials is t_ρ itself, which occurs with coefficient 1. Thus by Lemma Ap2(a), δ is a unit in B times t_ρ, and $V(\psi(\gamma)) = V(\psi(t_\rho))$: the Newton polygons N_F and N_G, of F^ψ and G^ψ respectively, have their first vertex at $(\rho, V(\psi(\gamma)))$. Since G^ψ divides F^ψ, if there is a segment of N_G of slope μ and length λ, there will also be a segment of N_F of slope μ and length $\lambda' \geqslant \lambda$. Hence N_G lies nowhere below N_F. But the last vertex of N_G is $(r, V(\psi(t_r)))$, which is also a vertex of N_F. Thus the nonvertical segments of N_G coincide with segments of N_F. To the right of $(r, V(\psi(t_r)))$, then N_F coincides with a suitable translate of the Newton polygon of H^ψ. Since all slopes of N_F to the left of $(r, V(\psi(t_r)))$ are less than all slopes to the right, roots of G^ψ have greater V-value than the roots of H^ψ.

(b) We have ϕ: $B \to R$, $t_i \to a_i$, and we need only show that $G^\phi / a_r \in R[x]$.

The ideal J of B^0 is generated by finitely many elements $\{s_1, \ldots, s_N\}$ of S. Hence the ideals $\bar{J}_k = (s_1^k, \ldots, s_N^k)$ of B form a neighborhood base at zero for the J-adic topology of B. Consider the coefficient γ_i of x^i in G, where $i < r$: γ_i is a sum of monomial terms, only finitely many of which are outside $\bar{J}_k$ for any given k. A term τ of γ_i that is in $\bar{J}_k$ will be writable in the form $\tau = cMs_\nu^k$, with $c \in Z$, $1 \leqslant \nu \leqslant N$, and M a monomial that is necessarily of degree 1 and moment $i - r$. One of the variables $t_0, \ldots, t_i$ definitely appears in M; say t_λ does, $0 \leqslant \lambda \leqslant i$. Since $(M/t_r)^{r-\lambda}$ is of degree zero and moment $(i - r)(r - \lambda)$, and since $r - \lambda \geqslant r - i$, we may write $(M/t_r)^{r-\lambda} = (t_\lambda/t_r)^{r-i}M'$, where $M' \in S \subset B$, and $\phi(t_\lambda)/\phi(t_r) \in R$ by hypothesis. Thus $\phi(M)/a_r$ is integral over R, so in R, and we see not only that $\phi(\tau)/a_r$ is in R, but also that the sum of all such terms is convergent in R, i.e. $\phi(\gamma_i)/a_r \in R$.

(c) Apply part (b) to $x^n f(1/x)$.

Consider now the power series $F(x) = \sum_{i=0}^{\infty} t_i x^i$, over proj $\lim_n Z[t_0, \ldots, t_n]$, which factors over proj lim B_n. There is no possibility of there being a morphism from this last ring to a ring R of the type mentioned in Lemma Ap4, if the power series $f(x) = \sum a_i x^i$ has a vertex at r. Rather we take each coefficient of $G =$ proj lim G_n and of $H =$ proj lim H_n and use the additional hypothesis of finite contingent order to show that the infinite sum deduced from each coefficient is convergent in R.

In accordance with the definition given in §1, we will say that a power series $f(x) = \sum a_i x^i$ defined over a linearly topologized integral domain R, with a vertex at r, *has contingent order less than* n (where $n > r$) if for all $i < r$, a_i^{n-r}/a_r^{n-i} is analytically nilpotent in R. In case R is integrally closed, a_i/a_r will then be in R and analytically nilpotent.

LEMMA Ap5 (CONTINUITY OF THE ROOTS). *Let R be a linearly topologized integral domain which is separated, complete, and integrally closed, and let $f(x) = \sum a_i x^i \in R[[x]]$ be a power series with a vertex at r, and with finite contingent order. If $f_K(x) = \sum_{i=0}^{K} a_i x^i$, and (g_K, h_K) is the Newton factorization of f_K given by Lemma* Ap4(b), *then there are coefficientwise limits $h = \lim_K h_K \in R[[x]]$ and $g = \lim_K g_K \in R[x]$, a monic polynomial all of whose lower coefficients are analytically nilpotent.*

PROOF. Suppose f has contingent order less than n.

The coefficient of x^α in $G =$ proj lim G_N or in $H =$ proj lim H_N is an infinite Z-linear combination of monomials, each in B_N^0 for some N. We have a consistent family of morphisms ϕ_N: $B_N \to R$ induced by $t_i \to a_i$, so that if M is a monomial in B_N, we can simply write $\phi(M)$ instead of $\phi_N(M)$. We must show, given $\alpha \geqslant 0$ and any open ideal $\mathfrak{A}$ in R, that there is an N_0 so large that if $N \geqslant N_0$ and t_N appears in a monomial M of the coefficient of x^α in $H(x)$ or $G(x)/t_r$, then $\phi(M) \in \mathfrak{A}$. Since the a_i/a_r $(0 \leqslant i < r)$ are all analytically nilpotent elements of R, there is a k so large that any product of k of these is in $\mathfrak{A}$.

The coefficient of x^α in $H(x)$. In this case we take $N_0 = \alpha + (k+1)r$, and look at any monomial M appearing that contains $t_{N'}$ for $N' \geqslant N_0$. We have $M \in B_{N'}$ for some $N' \geqslant N$, and the degree and moment of M are 1 and α, respectively, so that $\operatorname{moment}(Mt_N^{-1}) = \alpha - (N-r) \leqslant -kr$. Thus if $M = \prod_{i=0}^{N'} t_i^{e_i}$, $\deg(\prod_{i=0}^{r-1} t_i^{e_i}) \geqslant k$, so that we may write $M = (\prod_{j=1}^{k} t_{i_j}/t_r^k)M'$ with $i_j < r$, $\deg(M') = 1$, and

$$\operatorname{moment}(M') = \alpha + \sum_{j=1}^{k} (r - i_j) \leqslant \alpha + kr \leqslant N - r.$$

Call $\rho = \operatorname{moment}(M') + r \leqslant N$. Since $\rho - r > 0$ and M' is still in the ideal $(t_\rho, \ldots, t_N, \ldots, t_{N'})$ of $A^0_{N'}$, M' is still in $B^0_{N'}$, by Lemma Ap2(c), and $\phi(M) \in \mathfrak{A}$.

The coefficient of x^α in $G(x)/t_r$. We may assume at the outset that $k > r(n-r+1)$, and we take $N_0 = \alpha + \max(kr, r(r+1)(n-r)/2)$. If M is a monomial appearing that contains t_N for $N \geqslant N_0$, then again $M \in B^0_{N'}$ for some $N' \geqslant N$, but $\deg(M) = 0$, $\operatorname{moment}(M) = \alpha - r < 0$. Now moment $(Mt_N^{-1}) = \alpha - N \leqslant -r(r+1)(n-r)/2$, and if $M = \prod_{i=0}^{N'} t_i^{e_i}$, there must be at least one $i < r$ with $e_i \geqslant n - r$, so that $M = (t_i^{n-r}/t_r^{n-i}) \cdot t_r^{r-i-1} \cdot M'$ where $\deg(M') = 1$ and $\operatorname{moment}(M') = \alpha - r + (n-r)(i-r) < \alpha - r < 0$. Since t_N appears in $M' = \prod_{j=0}^{N'} t_j^{e'_j}$, we see as before that $\operatorname{moment}(M' t_N^{-1}) \leqslant -kr$, so that we may write $M' = (\prod_{j=1}^{k} t_{i_j}/t_r^k)M''$ with $i_j < r$, $\deg(M'') = 1$, and

$$\operatorname{moment}(M') = \alpha - r + (n-r)(i-r) + \sum_{j=1}^{k} (r - i_j)$$

$$\geqslant \alpha - r + (n-r)(i-r) + k > 0$$

by the original specification of k, and also

$$\operatorname{moment}(M'') \leqslant \alpha + (k-1)r + (n-r)(i-r) < N_0 \leqslant N,$$

so that again Lemma Ap2(c) applies and $M'' \in B^0_{N'}$. As a result, $\phi(M) \in \mathfrak{A}$, and the proof is done.

For the proof of the Local Factorization Principle, everything is now done, except for verifying that if $\psi\colon R \to R_0$ is a continuous morphism into a rank-one valuation ring (R_0, V), and ρ, σ are roots of g^ψ, h^ψ respectively, in the fraction-field of R_0, then $V(\rho) > V(\sigma)$. We have $g^\psi = \lim_N g_N^\psi$ and $h^\psi = \lim_N h_N^\psi$, coefficientwise limits in $R_0[[x]]$, and we know that for each N, the first nonvertical slope of the Newton polygon of h_K^ψ is greater than the last nonvertical slope of the Newton polygon of g_N^ψ, and that this latter number is negative. Also the Newton polygon of g^ψ is the same as those of all g_N^ψ for $N \geqslant N_0$; let α be the slope of the last nonvertical segment of the Newton polygon of g^ψ, and let $\sigma \in R_0$ with $V(\sigma) \geqslant -\alpha$. Since $V(\sigma) > 0$, $h^\psi(\sigma) = \lim_N h_N^\psi(\sigma)$; for $N \geqslant N_0$, $-V(\sigma)$ is less than any slope of a nonvertical segment of the Newton polygon of h_N^ψ, so that $V(h_N^\psi(\sigma)) = V(h_N^\psi(0))$ and in particular $h^\psi(\sigma) \neq 0$.

REFERENCES

1. A. Fröhlich, *Formal groups*, Lecture Notes in Math., vol. 74, Springer, Berlin, 1968.

2. M. Demazure and A. Grothendieck, *Schémas en groupes*, Séminaire, Inst. Hautes Etudes Sci., Paris, 1963/64.

3. B. Dwork, *p-adic cycles*, Inst. Hautes Etudes Sci. Publ. Math. no. 37, Paris, 1969, pp. 27–115.

4. N. Katz, *p-adic properties of modular schemes and modular forms*, Modular Functions of One Variable. III, Lecture Notes in Math., vol. 350, Springer, Berlin, 1973, pp. 69–190.

5. M. Lazard, *Sur les groupes de Lie formels à un paramètre*, Bull. Soc. Math. France **83** (1955), 251–274.

6. ______, *Les zéros des fonctions analytiques d'une variable sur un corps valué complet*, Inst. Hautes Etudes Sci. Publ. Math. no. 14, Paris, 1962, pp. 47–75.

7. J. Lubin, *One-parameter formal Lie groups over p-adic integer rings*, Ann. of Math. (2) **80** (1964), 464–484.

8. ______, *Finite subgroups and isogenies of one-parameter formal Lie groups*, Ann. of Math. (2) **85** (1967), 296–302.

9. J. Lubin and J. Tate, *Formal moduli for one-parameter formal Lie groups*, Bull. Soc. Math. France **94** (1966), 49–60.

10. F. Oort and J. Tate, *Group schemes of prime order*, Ann. Sci. École Norm. Sup. (4) **3** (1970), 1–21.

11. J. Tate, *p-divisible groups*, Proceedings of a Conference on Local Fields, NUFFIC Summer School at Driebergen (1966), Springer, Berlin, 1967.

DEPARTMENT OF MATHEMATICS, BROWN UNIVERSITY, PROVIDENCE, RHODE ISLAND 02912