TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 267, Number 1, September 1981

THE LOCAL KRONECKER-WEBER THEOREM

BY

JONATHAN LUBIN[1]

ABSTRACT. The extension of a local field generated by adjoining the torsion points on a suitable formal group is essentially the maximal abelian extension of the field. This fact is proven by appealing to the functorial properties of the Herbrand transition function of higher ramification theory.

The theorem of the title refers to the fact that the maximal abelian extension of a local field may be generated by roots of unity (for the unramified part) and roots of endomorphisms of a certain formal group, which depends on the field, as described in [2].

This proof of the local Kronecker-Weber theorem depends not on any cohomological methods but on the functorial and geometric properties of the Herbrand transition function and on the deep but noncohomological Hasse-Arf theorem. These are fully treated in [3], in Chapters 4 and 5, and I will assume that the reader is familiar with them.

1. Review of the Newton polygon and copolygon. Let K be a field which is complete with respect to a rank-one valuation (additive), v: $K^* \to \mathbf{Q}^+$. There is a unique extension of v to any algebraic closure $\bar{K}$ of K, and this will likewise be denoted v. If $f(z) = \sum a_i z^i \in \bar{K}[z]$, the *Newton polygon of* f, $\mathcal{N}(f)$, is constructed by erecting vertical halflines on all the points of the form $(i, v(a_i))$ in the Cartesian plane, and then taking the convex hull of the union of these lines. The basic property of the Newton polygon is the following: if $\mathcal{N}(f)$ has a segment of width w and slope μ, then in $\bar{K}$ there are, counting multiplicity, w roots ρ of f with $v(\rho) = -\mu$.

Another geometric object, which contains the same information as $\mathcal{N}(f)$ but organizes it differently, is the *Newton copolygon of* f, $\mathcal{N}^*(f)$, defined to be the intersection in the Cartesian plane of all halfplanes defined by the inequalities $y \leqslant ix + v(a_i)$.

The following facts are easily verified:

1. Every vertex of $\mathcal{N}(f)$, and every segment of $\mathcal{N}^*(f)$, comes from a monomial of f; a monomial of f contributes a vertex to $\mathcal{N}(f)$ if and only if it contributes a segment to $\mathcal{N}^*(f)$.

Received by the editors May 15, 1980. Presented at a Special Session held during the Summer Meeting of the AMS in Duluth, August 22–25, 1979.

1980 *Mathematics Subject Classification.* Primary 12B25, 12B10; Secondary, 52A10.

[1]This research was supported by NSF grant #MCS 78-02313.

0002-9947/81/0000-0409/$02.50

2. The vertices of $\mathcal{N}(f)$ are in one-to-one correspondence with the segments of $\mathcal{N}^*(f)$; if (P, S^*) is a corresponding pair, the x-coordinate of P is the slope of S^* and the y-coordinate of P is the y-intercept of S^*.

3. The nonvertical segments of $\mathcal{N}(f)$ are in one-to-one correspondence with the vertices of $\mathcal{N}^*(f)$; if (S, P^*) is a corresponding pair, the x-coordinate of P^* is the negative of the slope of S and the y-coordinate of P^* is the y-intercept of S.

4. If Ψ_f is the function whose graph is the boundary of $\mathcal{N}^*(f)$, then the inequality $v(f(a)) \geqslant \Psi_f(v(a))$ is satisfied for all $a \in \bar{K}$, and equality holds if $v(a)$ is not equal to the x-coordinate of any vertex of $\mathcal{N}^*(f)$. In particular, the valuations of roots of f are the x-coordinates of the vertices of $\mathcal{N}^*(f)$. If $f, g \in \bar{K}[z]$ and g has no constant term, then $\Psi_{f \circ g} = \Psi_f \circ \Psi_g$.

5. The change in slope at a vertex of $\mathcal{N}^*(f)$ is the same (but for sign) as the width of the corresponding segment of $\mathcal{N}(f)$. Thus

$$\Psi_f(x) = \Psi_f(0) + \int_0^x (\text{number of roots } \rho \text{ of } f \text{ with } v(\rho) \geqslant t)\, dt.$$

In particular, if $f(z)$ is a monic polynomial with v-integral coefficients, so that $\Psi_f(0) = 0$, the first term on the right-hand side drops out.

It will not often be necessary to mention the dependence of the Newton polygon and copolygon on the choice of v.

2. Transition function. The reader who is familiar with Serre's description of the Herbrand transition function in Chapter 4 of [3] should be warned that the relationships arising in this paper force on us a slight modification of this function. Whereas Serre's function ${}_S\phi$ is a polygonal mapping of the halfline $\mathbf{R}^{\geqslant -1}$ into itself, we will be using the corresponding mapping ${}_L\phi$ of $\mathbf{R}^{\geqslant 0}$ into itself: ${}_L\phi(x) = 1 + {}_S\phi(x - 1)$.

To review the definition of the transition function, let L/K be a totally ramified separable extension of complete discretely valued fields, with Galois set $G_{L/K}$ of all K-morphisms of L into $\bar{K}$. Let τ be a prime element of L, and use the normalized valuation $\mathrm{ord}_\tau = v(\tau)^{-1} \cdot v$. For $t \geqslant 0$, set $G_t = \{h \in G_{L/K}\colon \mathrm{ord}_\tau(h(\tau) - \tau) \geqslant t\}$, and $\gamma_t = \mathrm{card}(G_t)$. Then the transition function is

$$\phi_{L/K}(x) = \frac{1}{[L : K]} \int_0^x \gamma_t\, dt.$$

Notice that in case L is Galois over K, the G_i, for integral $i \geqslant 1$, are just the familiar ramification subgroups of $G_{L/K} = G_1$, except for a shift of 1 in the indices. These are normal subgroups of $G_{L/K}$ with the property that G_1/G_2 is embeddable in the multiplicative group k^* of the residue field k of K, and each G_i/G_{i+1} for $i \geqslant 2$ is embeddable in the additive group of k.

We will make extensive use of the functoriality of ϕ: if $F \subset K \subset L$, then $\phi_{K/F} \circ \phi_{L/K} = \phi_{L/F}$.

The following is a restatement of a lemma of Tate, which I learned of from B. Gross [1].

LEMMA 1. *Let $K_0 \subset K \subset L$ be extensions of complete discretely valued fields with L/K separable and totally ramified. Let π be a prime element of K_0 and τ a prime element of L, and use $v = \mathrm{ord}_\pi$ for drawing Newton polygons. Let $g(z) = \mathrm{Irr}(\tau, K[z])$, and $f(z) = g(z + \tau)$. Then $\phi_{L/K}(x) = e_{K/K_0}\Psi_f(x/e_{L/K_0})$.*

The proof is immediate. What Lemma 1 says is that Ψ_f and $\phi_{L/K}$ are the same except for scale; in fact, (a, b) is a vertex of Ψ_f if and only if $(e_{L/K_0}a, e_{K/K_0}b)$ is a vertex of $\phi_{L/K}$.

Let us use Lemma 1 to determine the transition function in a particular case. Let K_0 be a local field, with prime element π and residue field $k \cong \mathbf{F}(q)$. Then we have a canonical tower of totally ramified extensions of K_0, $K_0 \subset K_1 \subset K_2 \subset \ldots$, $K_i = K_0$ (roots of $[\pi^i]$), $[\pi](z) = \pi z + z^q$, $[\pi^i] = [\pi^{i-1}] \circ [\pi]$.

These fields are all abelian over K_0, as is shown in [2], and $[K_i : K_0] = (q-1)q^{i-1}$. We define $T = \bigcup_i K_i$, when the statement of the local Kronecker-Weber theorem is just that the maximal abelian extension of K_0 is UT, where U is the maximal unramified extension of K_0.

The nonzero roots of $[\pi]$ satisfy the K_0-polynomial $[\pi](z)/z = \pi + z^{q-1} = g(z)$, and if λ_1 is one of them, $f(z) = g(z + \lambda_1)$ has form $u_1\lambda_1^{q-2}z + u_2\lambda_1^{q-3}z^2 + \cdots + u_{q-2}\lambda_1 z^{q-2} + z^{q-1}$, where $\mathrm{ord}_\pi(u_i) = 0$. Thus $\mathfrak{N}(f)$ has vertices only at $(1, (q-2)/(q-1))$ and $(q-1, 0)$, so that $\mathfrak{N}^*(f)$ has the single vertex $(1/(q-1), 1)$, and by Lemma 1, ϕ_{K_1/K_0} has the single vertex $(1, 1)$. Notice that in all cases, the slope of the rightmost (unbounded) segment of the graph of $\phi_{L/K}$ is $1/[L : K]$; in the case of K_1/K_0, this slope is $1/(q-1)$.

To compute $\phi_{K_i/K_{i-1}}$ we let λ_i be a root of $[\pi^i]$ that is not a root of $[\pi^{i-1}]$, and set $\lambda_{i-1} = [\pi](\lambda_i)$, which we know to be a prime element of K_{i-1}. Then

$$\begin{aligned} g(z) &= -\lambda_{i-1} + [\pi](z) = -\lambda_{i-1} + \pi z + z^q \\ &= \mathrm{Irr}(\lambda_i, K_{i-1}[z]). \end{aligned}$$

Now form

$$f(z) = g(z + \lambda_i) = (z + \lambda_i)^q + \pi(z + \lambda_i) - \lambda_{i-1};$$

the constant term is zero, and all intermediate binomial coefficients of $(z + \lambda_i)^q$ are divisible by p, so that the Newton polygon of $f(z)$ has its only vertices at $(1, 1)$ and $(q, 0)$. Thus $\mathfrak{N}^*(f)$ is formed from the two lines $y = qx$ and $y = x + 1$, with its only vertex at $(1/(q-1), q/(q-1))$, and by Lemma 1, $\phi_{K_i/K_{i-1}}$ has its unique vertex at (q^{i-1}, q^{i-1}) and the rightmost segment has slope $1/q$. The composition

$$\phi_{K_1/K_0} \circ \phi_{K_2/K_1} \circ \cdots \circ \phi_{K_i/K_{i-1}} = \phi_{K_i/K_0}$$

thus has the vertices (q^{j-1}, j) for $1 \leqslant j \leqslant i - 1$.

For the field $T = \bigcup_i K_i$, the transition function $\phi_{T/K_0} = \lim_i \phi_{K_i/K_0}$ (pointwise limit), and the graph of this function has vertices at all the points (i, q^{i-1}), $i \geqslant 1$, and nowhere else.

Now if L is any totally ramified Galois extension of K, finite or infinite, we can say the following about $\phi_{L/K}$:

1. Since quotients of successive ramification subgroups are injected into either k^* or k^+, the ratio of the left-hand slope at a vertex of $\phi_{L/K}$ to the right-hand slope is: a divisor of $q-1$ if the vertex is $(1, 1)$, and a divisor of q otherwise.

2. If L is also abelian over K, the Hasse-Arf theorem implies that all vertices of $\phi_{L/K}$ are at lattice points.

3. Functoriality of ϕ implies that if $K \subset L \subset L'$, totally ramified, then $\phi_{L/K} \geqslant \phi_{L'/K}$.

The transition-function ϕ_{T/K_0} described above is clearly minimal among all polygonal functions satisfying conditions 1 and 2. What remains to be shown is that any proper extension T' of T which is totally ramified and Galois over K_0 has the property that for x large enough, $\phi_{T'/K_0}(x) < \phi_{T/K_0}(x)$. Such a T' cannot be abelian over K_0, so that T is then a maximal abelian totally ramified extension of K_0, from which fact it follows that UT is the maximal abelian extension of K_0.

We will assume from now on, therefore, that T and the K_i's are the extensions gotten from the polynomials $[\pi^i]$, and that T' is an extension of T with $[T' : T] = p$, and T' abelian over K_0. The proof below will use merely the fact that T' is normal over T. Let $T' = T(w)$. Then there is i_0 such that $[K_{i_0}(w) : K_{i_0}] = p$. For $i \geqslant i_0$, put $L_i = K_i(w)$. We wish to compare

$$\phi_{T'/K_0} = \lim_i \phi_{L_i/K_0} = \lim_i \phi_{K_i/K_0} \circ \phi_{L_i/K_i}$$

with $\phi_{T/K_0} = \lim_i \phi_{K_i/K_0}$. We will soon see that for $i \gg 0$, $\phi_{L_i/K_i} = \Phi$, unchanging from i to $i+1$, so that $\phi_{T'/K_0}(x) < \phi_{T/K_0}(x)$ for $x \gg 0$, which is the desired contradiction.

Many of the extensions we will be considering, such as K_{i+1}/K_i and L_i/K_i have a transition function with only one vertex, at (a, a). In this case there is an easy arithmetic consequence $d(\mathfrak{L}/\mathfrak{K}) = a([\mathfrak{L} : \mathfrak{K}] - 1)$. Here, d is the differential exponent of $\mathfrak{L}/\mathfrak{K}$; the formula is immediate in the normal case from the formula $d = \sum_{i=1}^{\infty} (|G_i| - 1)$, and directly provable in any case.

Define g_a to be the polygonal function on $\mathbf{R}^{>0}$ defined by the rule

$$g_a(x) = \begin{cases} x & \text{if } x \leqslant a, \\ a + p^{-1}(x - a) & \text{if } x \geqslant a. \end{cases}$$

(In applications, $a \geqslant 1$ always.)

These functions commute as follows:

$$(1)\ g_{a+\varepsilon} \circ g_a = g_a \circ g_{a+p\varepsilon} \quad (\varepsilon > 0);$$
$$(2)\ g_{a+\varepsilon} \circ g_a^f = g_a^f \circ g_{a+q\varepsilon} \quad (q = p^f).$$

Here, g^f means the f-fold composition of g with itself.

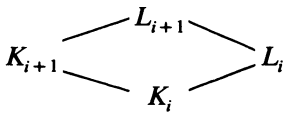
In general, suppose

$$\gamma = g_{a_1}^{e_1} \circ g_{a_1}^{e_2} \circ \cdots \circ g_{a_{m-1}}^{e_{m-1}} \circ g_{a_m}^{e_m}, \qquad e_i \in \mathbf{Z}^{\neq 0}.$$

If $a_1 < a_2 < \cdots < a_m$, say γ is *in standard form*, and if $a_1 > a_2 > \cdots > a_m$, *in antistandard form*. In the standard case, γ has vertices $(a_1, a_1), (a_2, *), \ldots, (a_m, *)$, while in the antistandard case, γ has vertices $(*, a_1), \ldots, (*, a_{m-1}), (a_m, a_m)$. It is clear from (1), or from geometric intuition, that every composition of g_*'s can be written uniquely in standard form and uniquely in antistandard form. In any case, $g_a \circ \delta$ has a vertex at $(*, a)$ and $\delta \circ g_a$ has a vertex at $(a, *)$ so long as δ is convex.

Now consider the ladder-diagram describing the lattice of the fields K_i and L_i for $i \geqslant i_0$.

We examine one cell of the ladder,



where we know

$$\phi_{K_{i+1}/K_i} = (g_{q^i})^f, \qquad \phi_{L_i/K_i} = g_{b_i}, \quad \phi_{L_{i+1}/K_{i+1}} = g_{b_{i+1}},$$

and we want to show that for $i \gg i_0$, $b_{i+1} = b_i$. Write $h = \phi_{L_{i+1}/L_i}$, so that we have the relation

$$g_{b_i} \circ h = (g_{q^i})^f \circ g_{b_{i+1}}.$$

We divide the situation into three cases:

Case 1. $b_i < q^i$. Then $q^i \leqslant b_{i+1}$ is impossible, since then $g_{b_i}^{-1} \circ (g_{q^i})^f \circ g_{b_{i+1}}$ would be standard and nonconvex. Thus $b_{i+1} < q^i$, and $(g_{q^i})^f \circ g_{b_{i+1}}$ is antistandard, so has only the vertices (b_{i+1}, b_{i+1}) and $(*, q^i)$, while it also has a vertex $(*, b_i)$. Thus $b_{i+1} = b_i$, so that we hope that Case 1 will obtain for $i \gg i_0$.

Case 2. $b_i = q^i$. This involves some arithmetic, since we use the following:

LEMMA 2. $d(L_{i+1}/K_{i+1}) \leqslant qd(L_i/K_i) - q(p-1)$.

PROOF. Let τ be a prime element of L_i; then $\tau/\lambda_{i+1}^{q/p}$ is a unit in L_{i+1} whose minimal polynomial is computed from that of τ, giving $qd(L_i/K_i) - q(p-1)$ for the exponent of the different ideal of the ring $\mathcal{O}_{L_i}[\tau/\lambda_{i+1}^{q/p}]$ as an extension of $\mathcal{O}_{K_{i+1}}$.

As a consequence of Lemma 2, $d(L_{i+1}/K_{i+1}) < qd(L_i/K_i)$, so that $(p-1)b_{i+1} < q(p-1)b_i$, and thus $b_{i+1} < q^{i+1}$ if $b_i = q^i$.

Case 3. $b_i > q^i$. Then $q^i \geqslant b_{i+1}$ is impossible, since then $h = g_{b_i}^{-1} \circ (g_{q^i})^f \circ g_{b_{i+1}}$ would be antistandard and nonconvex. Thus $b_{i+1} > q^i$, and $(g_{q^i})^f \circ g_{b_{i+1}}$ is standard, equal to $g_Q \circ (g_{q^i})^f$, which is antistandard, where $Q = q^i + ((b_{i+1} - q^i)/q)$, and this function has vertices only at $(*, Q)$ and (q^i, q^i), while we know that $g_{b_i} \circ h$ has a vertex at $(*, b)$, so that $b_i = Q$, or, solving for b_{i+1},

$$b_{i+1} = qb_i - q^i(q-1).$$

It only remains to observe that Case 3 eventually gives way to Case 1 or Case 2: if Case 3 obtains for $i, i+1, \ldots, i+k$, then

$$\begin{aligned} b_{i+k} &= q^k b_i - kq^{i+k-1}(q-1) \\ &= q^k\big[b_i - k(q^i - q^{i-1})\big]. \end{aligned}$$

Here i is fixed and $k \to \infty$, so what is in brackets must become negative, i.e. Case 3 must stop, and give way to Case 1.

References

1. B. H. Gross, *Ramification in p-adic Lie extensions* (Proc. Conf. Formal Groups and Crystalline Cohomology, Rennes, 1978), Astérisque **65** (1979), 81–202.

2. J. Lubin and J. Tate, *Formal complex multiplication in local fields*, Ann. of Math. (2) **81** (1965), 380–387.

3. J.-P. Serre, *Corps locaux*, Actualités Sci. Indust. No. 1296, Hermann, Paris, 1962.

Department of Mathematics, Brown University, Providence, Rhode Island 02912