EHUD DE SHALIT

The explicit reciprocity law of Bloch-Kato

Astérisque, tome 228 (1995), p. 197-221
<http://www.numdam.org/item?id=AST_1995__228__197_0>

The explicit reciprocity law of Bloch-Kato

Ehud de Shalit

Introduction. In §2 of their paper [B-K] Bloch and Kato proved a remarkable theorem relating the Coates-Wiles homomorphisms, which play an important role in the theory of cyclotomic fields, to the structure of Fontaine's ring B_{cris} ([F2], [F-M]). This theorem is one of the two ingredients in the proof of the "Tamagawa number conjecture" for the motive $\mathbb{Q}(r)$, r even and positive. (Cf. [B-K], §6. The other ingredient is the Main Conjecture of Iwasawa theory, proved by Mazur and Wiles.)

Starting from B_{cris}, and using the "fundamental exact sequence" (see below), one constructs, for each $r \geq 1$, a canonical class in $H^1(\mathbb{Q}_p, \mathbb{Q}_p(r))$. (We write $H^i(K,M)$ for $H^i(Gal(\overline{K}/K),M)$.) The theorem of Bloch and Kato identifies this class essentially as the r^{th} Coates-Wiles homomorphism. In §2 of [B-K] the authors reduce their theorem to the case r=1. This case, in turn, follows from more general "explicit reciprocity laws", proven in [K].

The proofs in [B-K] and [K] are difficult, and use the relation between B_{cris} and crystalline cohomology, Fontaine's syntomic cohomology, and the main results of Fontaine-Messing. In our attempt to understand them, we found a simpler proof of the case r=1, where we deduce the theorem directly from the explicit reciprocity laws of Artin-Hasse and Iwasawa. We have somewhat simplified the presentation of the general case too, although mainly in style, and not in substance. Perrin-Riou ([P], prop. 3.4(i)) found another way to reduce the general case to the case r=1.

The proof given below might cover p=2 too, which was excluded from the discussion in [B-K]. Strictly speaking, §9 relies on part III of [F-M], where p=2 causes some difficulties. (Elsewhere, e.g. in the case r=1 of the main theorem, p=2 is not a problem.) However, the results needed here should extend to p=2. In particular, lemma 8.2, which is of "qualitative" rather than "quantitative" nature (and which is the only troublesome point) should remain valid. We hope that when the details of [F-M] finally appear, they will allow us to include p=2. This should help to eliminate the unknown powers of 2 in theorem 6.1(i) of [B-K].

Chapter I (§1-§4) is devoted to a preliminary study of the ring A_{cris}. In §4 we show how to derive the "fundamental exact sequence". Despite its importance for the constructions of [B-K], the proof of the right-exactness of this sequence was unavailable in print until now. (In [F-M] the authors only say that it is done by "explicit laborious computations", but their notes on the proof were never made public[1].)

Chapter II (§5-§9) contains the proof of the theorem of Bloch and Kato along the lines discussed above.

Chapter III contains the seeds to generalizations to other Lubin-Tate formal groups (in the spirit of [W]). The author hopes to expand on this in a future paper. Recently, K. Kato kindly informed the author that he had generalized his work to any Lubin-Tate group, but in a direction that seems different than the path taken in chapter III.

Acknowledgements. Chapters I and II of this paper are based entirely on the work of others, mainly J.-M. Fontaine and K. Kato, and except for the presentation, we claim no originality on our part. This work was written while the author was visiting Princeton University. He would like to thank the department of mathematics for its support, and A. Wiles for many pleasant discussions.

I. The ring B_{cris} and the fundamental exact sequence

1. The ring R. The construction of the ring R (resp. A_{cris} and B_{cris}) reviewed below is due to Fontaine and Wintenberger (resp. Fontaine, see [F-M] ch.I, §1 and the references therein). One should think of B_{cris} as the ring of all p-adic periods of motives with good reduction over the maximal unramified extension of $\mathbb{Q}_p$.

Let p be a prime number, and $\overline{\mathbb{Q}}_p$ an algebraic closure of the p-adic numbers. Let R be the "perfection" of the ring $\mathcal{O}(\overline{\mathbb{Q}}_p)/p\mathcal{O}(\overline{\mathbb{Q}}_p)$,

$$R = \lim_{\leftarrow} \mathcal{O}(\overline{\mathbb{Q}}_p)/p\mathcal{O}(\overline{\mathbb{Q}}_p) \tag{1}$$

the inverse limit taken with respect to the Frobenius map of raising to power p. Clearly R is an integral domain in characteristic p, on which

[1] The referee has pointed out that a proof of the fundamental exact sequence will appear in [F4], and some of the ideas involved may be found also in [F3].

Frobenius ϕ is bijective. If $x=(x_0,x_1,...)\in R$, where $x_i\in\mathcal{O}(\overline{\mathbb{Q}}_p)/p\mathcal{O}(\overline{\mathbb{Q}}_p)$ and $x_i^p=x_{i-1}$, let $\hat{x}_i$ be any representative of x_i in $\mathcal{O}(\overline{\mathbb{Q}}_p)$, and define $x^{(i)}=\lim_n \hat{x}_{i+n}{}^{p^n} \in\mathcal{O}(\mathbb{C}_p)$. Here $\mathbb{C}_p$ is the completion of $\overline{\mathbb{Q}}_p$. It is easy to see that the limit exists, is independent of the choice of representatives, and that the association $x \mapsto (x^{(0)},x^{(1)},...)$ identifies R as a set (and as a multiplicative monoid) with the set of all infinite series in $\mathcal{O}(\mathbb{C}_p)$ such that $(x^{(i)})^p=x^{(i-1)}$.

For $x\in R$, define $v_R(x)=v_p(x^{(0)})$, where v_p is the p-adic valuation, normalized by $v_p(p)=1$. Then R becomes a complete valuation ring, whose residue field is $\overline{\mathbb{F}}_p$. Let ζ be an element of R such that $\zeta^{(0)}=1$, $\zeta^{(1)}\neq 1$. Then $\mathbb{F}_p[[\zeta-1]]\subseteq R$, the field of fractions of R contains a separable closure $\mathbb{F}_p((\zeta-1))^{sep}$ of $\mathbb{F}_p((\zeta-1))$, and is identified with its completion. In particular, R is integrally closed.

2. Witt vectors over R. Let W(R) be the ring of Witt vectors over R. For $a\in R$ let $[a]=(a,0,0,...)\in W(R)$ be its Teichmuller representative. Since the absolute Frobenius homomorphism ϕ is bijective on R, every element of W(R) has a unique expression in the form

$$\alpha = (a_0,a_1^p,a_2^{p^2},...) = \textstyle\sum_{0\leq n<\infty}p^n[a_n]. \tag{2}$$

Define the map $\theta : W(R) \rightarrow \mathcal{O}(\mathbb{C}_p)$ as

$$\theta(\alpha) = \textstyle\sum_{0\leq n<\infty}p^n\, a_n{}^{(0)}. \tag{3}$$

Then θ is a surjective ring homomorphism. Indeed, θ is already surjective when restricted to the set of Teichmuller representatives, because $\theta([a])=a^{(0)}$ is arbitrary, a fact that will be used below. That θ is a homomorphism follows directly from the way addition and multiplication are defined in W(R) ([S], ch. 2 §6).

Let $J = \mathrm{Ker}(\theta)$. Then J is a *principal* ideal, generated by any α as in (2), for which $\theta(\alpha)=0$ and $a_1{}^{(0)}\in\mathcal{O}(\mathbb{C}_p)^\times$. The proof is not difficult. See [F1], proposition 2.4.

The Frobenius of W(R), still denoted ϕ, is bijective. It preserves

$J+pW(R)$, but not J. The Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ acts by functoriality on R and on $W(R)$, and commutes with ϕ and θ.

Lemma 2.1 (i) The elements of $W(R)$ satisfying $\phi(\alpha)=\alpha^p$ are precisely the Teichmuller representatives $[a]$, $a\in R$.

(ii) For $a\in R$, $\theta\phi^{-n}([a])=a^{(n)}$.

Proof. The first assertion is a general and well known property of Witt vectors. The second follows from the fact that for $x\in R$, $\phi^{-n}(x)^{(m)}=x^{(m+n)}$. □

For each $n\geq 0$, let ζ_n be a primitive p^n root of 1 in $\overline{\mathbb{Q}}_p$, such that $\zeta_n{}^p=\zeta_{n-1}$. The element $\zeta\in R$ for which $\zeta^{(n)}=\zeta_n$ gives a generator $\varepsilon = [\zeta] \in W(R)$ of a "multiplicative Tate module" $\varepsilon^{\mathbb{Z}_p} \subseteq W(R)^\times$. Put $K_n=\mathbb{Q}_p(\zeta_n)$, and $K_\infty=\bigcup K_n$.

Lemma 2.2 The following sequence of multiplicative groups is exact:

$$(4) \qquad 0 \longrightarrow \varepsilon^{\mathbb{Z}_p} \longrightarrow 1+J \xrightarrow{p-\phi} 1+pW(R) \longrightarrow 0.$$

Proof. If $\beta\in W(R)^\times$, $\alpha=\beta^{p-\phi} \in 1+pW(R)$, and by successive approximations one checks that every element α of $1+pW(R)$ is of this form. Choose $r\in R$ such that $r^{(0)}=\theta(\beta)$. Then $\beta/[r] \in 1+J$, but still $\alpha=(\beta/[r])^{p-\phi}$. This proves the surjectivity of $p-\phi$. If $\beta^{p-\phi}=1$, by lemma 1(i) $\beta=[r]$, and since $r^{(0)}=\theta(\beta)=1$, r is a p-adic power of ε. □

Remark. When $p=2$, $-1\in 1+pW(R)$, so lemma 2 shows that ε has a square root $\sqrt{\varepsilon}\in 1+J$. Since -1 is not in $1+J$, this square root is unique.

3. Divided powers. Let A'_{cris} be the divided power envelope of $W(R)$ with respect to J. If γ is a generator of J, $A'_{cris} = W(R)[\gamma^2/2!,\gamma^3/3!,\ldots] \subseteq W(R)\otimes\mathbb{Q}$. Let A_{cris} be the completion of A'_{cris} in the p-adic topology (it is easy to see that A'_{cris} is separated, so it embeds in A_{cris}):

(5) $$A_{cris} = \lim_{\leftarrow} A'_{cris}/p^n A'_{cris}.$$

Since $\phi(J) \subseteq J+pW(R)$, and since (p) already admits divided powers in $W(R)$, ϕ extends to A'_{cris}. It then extends by continuity to A_{cris}. Clearly the Galois action carries over too. The map θ extends to A_{cris} easily, since $\theta(\gamma)=0$.

We denote the kernel of θ in A_{cris} by J_{cris} (it is *not* principal, nor even finitely generated). Its divided powers are the ideals $J_{cris}^{[r]}$ $(r\geq 1)$ given by

(6) $$J_{cris}^{[r]} = (\gamma^r/r!, \gamma^{r+1}/(r+1)!, \ldots)A_{cris}.$$

Obviously $J_{cris}^{[1]} = J_{cris}$. One further defines

$$J_{cris}^{\langle r\rangle} = \{ \alpha\in J_{cris}^{[r]} ;\ \phi(\alpha) \ \in \ p^r A_{cris} \}.$$

Observe that for any $\beta \in 1+J$, $\log(\beta) \in A_{cris}$ is defined by the usual power series in $\beta-1$, which converges nicely. Moreover $\log(\beta)\in J_{cris}^{\langle 1\rangle}$. In particular

(7) $$\mathbf{t} = \log(\varepsilon) \quad (\text{recall } \varepsilon=[\zeta])$$

is a generator of an "additive Tate module" $\mathbb{Z}_p(1) \subseteq J_{cris}^{\langle 1\rangle}$. We denote by $\mathbb{Z}_p(r)$ the subgroup generated by $\mathbf{t}^r$. Let

$$S^r = \{ x\in A_{cris};\ p^n x\in\mathbb{Z}_p(r) \text{ for some } n \} \subseteq J_{cris}^{\langle r\rangle}.$$

Since A_{cris} is p-torsion free, for some non-negative $c(r)$,

(8) $$S^r = p^{-c(r)}\mathbb{Z}_p(r).$$

In fact, $c(r) = \sum_{i\geq 0}[r(p-1)^{-1}p^{-i}]$, where $[x]$ denotes the largest integer $\leq x$, but we shall make no use of this exact value.

B_{cris} is defined as $A_{cris}[\mathbf{t}^{-1}]$. Our primary concern is nevertheless with

A_{cris}.

4. Proposition (The fundamental exact sequence). For every $r \geq 0$ the sequence

(9) $$0 \longrightarrow S^r \longrightarrow J_{cris}^{\langle r \rangle} \xrightarrow{1-p^{-r}\phi} A_{cris} \longrightarrow 0$$

is exact.

Remark. When $r=1$ the exact sequences (4) and (9) are related by the following diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \varepsilon^{\mathbb{Z}_p} & \longrightarrow & 1+J & \xrightarrow{p-\phi} & 1+pW(R) & \longrightarrow & 0 \\ & & \log\downarrow & & \log\downarrow & & \downarrow p^{-1}\log & & \\ 0 & \longrightarrow & S^1 & \longrightarrow & J_{cris}^{\langle 1 \rangle} & \xrightarrow{1-p^{-1}\phi} & A_{cris} & \longrightarrow & 0. \end{array}$$

If $p>2$, the vertical arrows are injective, the last one is onto $W(R)$, and the first one is an isomorphism, since $S^1=\mathbb{Z}_p(1)$. If $p=2$, the last vertical arrow has $\{\pm 1\}$ for its kernel, which is also the cokernel of the first one, since now $S^1=2^{-1}\mathbb{Z}_2(1)$ (see the remark following lemma 2.2).

Proof. That the kernel of $1-p^{-r}\phi$ on $J_{cris}^{\langle r \rangle}$ is S^r, is essentially proven in [F1], théorème 4.12. (The ring B of [F1] is *different* from B_{cris}, but the proof can be adjusted to B_{cris}.) We show the surjectivity of $1-p^{-r}\phi$ in several steps. We shall prove a little more, i.e., that for any unit $v \in A_{cris}^{\times}$

(10) $$(\phi - vp^r)J_{cris}^{[r]} \supseteq p^r A_{cris}.$$

It will be convenient to fix as a generator of $J = \gamma W(R)$ the element

(11) $$\gamma = [\pi]+p,$$

where $\pi \in R$ is some fixed element with $\pi^{(0)} = -p$.

4.1 The element $u = (\varepsilon-1)^{p-1}/p$. ([F-M] suggests the use of t^{p-1}/p, but the two elements are associates in A_{cris}.) From (11) we get

$$\gamma^p \equiv [\pi]^p \bmod pW(R),$$

and clearly

$$(\varepsilon-1)^{p-1} \equiv [\zeta-1]^{p-1} \bmod pW(R),$$

so since $(\zeta-1)^{p-1}/\pi^p \in R^\times$, there exist $\lambda \in W(R)^\times$ and $\nu \in W(R)$ such that

$$u = \lambda(\gamma^p/p)+\nu.$$

This shows that $u \in A'_{cris}$. Furthermore, $p\nu$ is divisible by γ^{p-1} in W(R), and since p is a prime in W(R), and p does not divide γ, ν is divisible by γ^{p-1}. We conclude that

$$u = \lambda(\gamma^p/p)+\mu\gamma^{p-1} \qquad \lambda \in W(R)^\times,\ \mu \in W(R). \tag{12}$$

4.2 Corollary. Inside W(R)[1/p] we have

$$A'_{cris} = W(R)[\gamma^m/m!] = W(R)[\gamma^{np}/(np)!] = W(R)[u^i/i!]. \tag{13}$$

Proof. The first equality is the definition of A'_{cris}. The second follows from the observation that if $m=np+j$, $0 \leqslant j<p$, m! and (np)! are divisible by the same power of p. Since $u \in J'_{cris} = \sum_{m\geqslant 1} W(R)(\gamma^m/m!)$, its divided powers $u^i/i! \in J'_{cris}$ as well. On the other hand, we prove by induction on n that $\gamma^{np}/(np)! \in W(R)[u^i/i!]$. If n=1 this is clear from (12). In general, we may replace $\gamma^{np}/(np)!$ by $(\gamma^p/p!)^n/n!$, since (np)! and $(p!)^n n!$ are divisible by the same power of p. So

$$(\gamma^p/p!)^n/n! = (\lambda_1 u+\mu_1\gamma^{p-1})^n/n! \in W(R)[u^i/i!]$$

since, by the induction hypothesis, $\gamma^m/m! \in W(R)[u^i/i!]$ for all $m<np$.

4.3 Claim: $(\varepsilon^p-1)/p(\varepsilon-1) \in A_{cris}^\times$.

Proof. $(\varepsilon^p-1)/p(\varepsilon-1) \equiv (\varepsilon-1)^{p-1}/p \bmod A_{cris}$, so by 4.1 it lies itself in A_{cris}.

Furthermore $\theta(\varepsilon) = 1$, so $\theta((\varepsilon^p-1)/p(\varepsilon-1)) = 1$, and $(\varepsilon^p-1)/p(\varepsilon-1) \in 1+J_{cris}$. But if $x\in J_{cris}$, $\sum_{0\leq i<\infty} x^i$ converges in A_{cris}, since $x^i/i!\in A_{cris}$ and A_{cris} is p-adically complete. It follows that $1+J_{cris}\subseteq A_{cris}^{\times}$.

4.4 Lemma. Let $v\in A_{cris}^{\times}$, $r\geq 0$, $e\geq r+1$, and consider the series

$$f(x(\varepsilon-1)^e) = \sum_{0\leq i<\infty}(v^{-1}p^{-r}\phi)^i(x(\varepsilon-1)^e), \qquad x\in A_{cris}. \tag{14}$$

Then (14) converges to an element of $J_{cris}^{\langle r\rangle}$ and

$$(1-v^{-1}p^{-r}\phi)(f(x(\varepsilon-1)^e)) = x(\varepsilon-1)^e.$$

Proof. By 4.3, $(v^{-1}p^{-r}\phi)(x(\varepsilon-1)^e) = p^{e-r}v^{-1}\phi(x)\cdot((\varepsilon^p-1)/p(\varepsilon-1))^e\cdot(\varepsilon-1)^e = p^{e-r}x_1(\varepsilon-1)^e$, with $x_1\in A_{cris}$. Iterating, the i^{th} summand in (14) will be divisible by $p^{i(e-r)}(\varepsilon-1)^e$, which guarantees convergence to an element of $J_{cris}^{\langle e\rangle}\subseteq J_{cris}^{\langle r\rangle}$, again by 4.3. The last statement follows formally.

4.5 Corollary. $(\phi-vp^r)J_{cris}^{[r]} \supseteq p^rA_{cris}\cdot u^i/i!$ if $i(p-1)>r$.

Proof. In addition to what was already said, one only has to note that if $(\varepsilon-1)^e$ is divisible by p^m in A_{cris}, so is (14).

4.6 Lemma. If $0\leq r$ and $v\in A_{cris}^{\times}$, for every $i>0$

$$(\phi-vp^r)J_{cris}^{[r]} \supseteq p^rA_{cris}\cdot u^i/i!$$

Proof. By induction on r, we may assume that (10) holds for all r's smaller than our r. When r=0, (10) follows from corollary 4.5, and lemma 4.7 below. So suppose i is such that $0<i(p-1)\leq r$ (bigger i's are taken care of by 4.5). Write $\phi(u) = p^{p-1}u\xi$, where ξ is the unit $((\varepsilon^p-1)/p(\varepsilon-1))^{p-1}$ (see 4.3). Let x be a variable. Then

$$(\phi-vp^r)(xu^i/i!) = p^{i(p-1)}\cdot\xi^i\cdot(\phi-v\xi^{-i}p^{r-i(p-1)})(x)\cdot u^i/i!,$$

and by the induction hypothesis $(\phi-v\xi^{-i}p^{r-i(p-1)})(x)$ gives everything in $p^{r-i(p-1)}A_{cris}$ as x runs over $J_{cris}^{[r-i(p-1)]}$. The claim follows, since $u^i/i!\cdot J_{cris}^{[r-i(p-1)]} \subseteq J_{cris}^{[r]}$.

4.7 To finish the proof of (10), it remains, by 4.2, and the density of A'_{cris} in A_{cris}, to prove that $(\phi-vp^r)J_{cris}^{[r]} \supseteq p^rW(R)$. We first do the case r=0. Write $v=\sum_{0\leqslant i<\infty}v_iu^i/i!$, where $v_i\in W(R)$ tend p-adically (in W(R)) to 0. This is possible by 4.2 and the density of A'_{cris} in A_{cris}. Applying θ, $\theta(v_0)=\theta(v)\in\mathcal{O}(\mathbb{C}_p)^\times$, so v_0 must be a unit in W(R). By corollary 4.5, it is enough to show that $(\phi-v_0)A_{cris} \supseteq W(R)$ (see the argument in the next paragraph), so we may assume that $v\in W(R)^\times$. In this case $(\phi-v)W(R)=W(R)$. Indeed, it is enough to prove the "mod p" version of this, i.e., that for $a\in R^\times$, $x^p-ax=b$ is solvable in $x\in R$ for every $b\in R$. This is true since R is integrally closed.

The case r=0 concludes the proof of (10) when r=0, hence we can start the induction on r, and we may assume that lemma 4.6 holds. By that lemma, the proof of (10) is reduced again to the case $v\in W(R)^\times$. Indeed, write $v=\sum_{0\leqslant i<\infty}v_iu^i/i!$ as above, let $b\in p^rA_{cris}$, and instead of solving $(\phi-vp^r)(x) = b$, solve $(\phi-v_0p^r)(x) = b$. Then $(\phi-vp^r)(x) = b-p^rx\sum_{1\leqslant i}v_iu^i/i! = b-b'$ (say). Lemma 4.6 supplies a solution of $(\phi-vp^r)(x') = b'$, and $x+x'$ is the desired element of $J_{cris}^{[r]}$.

Let therefore $v\in W(R)^\times$. We wish to show that $(\phi-vp^r)J_{cris}^{[r]} \supseteq p^rW(R)$. An easy computation shows that

$$\phi(\gamma^r) = p^r(d_0+d_1u+ \cdots +d_ru^r)$$

where $d_i\in W(R)$, and $d_0\in W(R)^\times$. To see this simply write $\phi(\gamma) = \gamma^p+pb$, and check that $b\in W(R)^\times$. Then use (12) to eliminate γ^p, and raise to power r. Now let x be a variable. Then

$$(\phi-vp^r)(x\gamma^r) = p^r((d_0+ \cdots d_ru^r)\phi(x) - vx\gamma^r).$$

By lemma 4.6 again, and by the fact that d_0 is in $W(R)^\times$, it is enough to show that every element of W(R) is of the form $\phi(x)-vx\gamma^r$, for some $x\in W(R)$. Once again, it is enough to prove the "mod p" version of this, so we have to solve $x^p-ax=b$ in R, which can be done thanks to the fact that R is integrally closed. □

4.8 Corollary (of the proof). The fundamental exact sequence splits over $(\varepsilon-1)^{r+1}A_{cris}$.

Proof. This follows from step 4.4 in the proof. □

II. The explicit reciprocity law

5. The classical explicit reciprocity law. Let $K_n=\mathbb{Q}_p(\zeta_n)$, and let U_n be the group of principal units of K_n. If α, $\beta\in K_n^\times$, we denote by σ_β the Artin symbol of β (on any abelian extension of K_n), and define $[\alpha,\beta]_n\in\mathbb{Z}/p^n\mathbb{Z}$ by

(15) $$\sigma_\beta(\alpha')/\alpha' = \zeta_n^{[\alpha,\beta]_n}$$

where α' is any p^n root of α. If $\beta = (\beta_n)$ is a norm-compatible sequence ($\beta_n\in K_n^\times$, $N_{n+1,n}(\beta_{n+1})=\beta_n$), and $\alpha\in K_n^\times$ for *some* n, then there exists a well-defined $[\alpha,\beta]\in\mathbb{Z}_p$ such that for all n large enough $[\alpha,\beta] \bmod p^n = [\alpha,\beta_n]_n$. Let

(16) $$B = \lim_{\leftarrow} K_n^\times, \qquad U = \lim_{\leftarrow} U_n$$

(inverse limits with respect to the norm).

Recall ([C], [dS]) that for any $u \in U$ Coleman associated a unique power series $g_u\in\mathbb{Z}_p[[T]]^\times$ with the property

(17) $$g_u(\zeta_n-1) = u_n \qquad \forall n\geq 1.$$

Introduce a formal variable t via $T=e^t-1$, and identify $\mathbb{Q}_p[[t]]$ with $\mathbb{Q}_p[[T]]$. Let

(18) $$\delta g = (1+T)g^{-1}dg/dT = g^{-1}dg/dt \in \mathbb{Z}_p[[T]].$$

Let $\chi : G = \mathrm{Gal}(K_\infty/\mathbb{Q}_p) \to \mathbb{Z}_p^\times$ be the cyclotomic character. For later reference we let $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ act on power series in T (or t) in a way compatible with the specialization maps sending T to ζ_n-1, i.e.

(19) $$\sigma(T) = (1+T)^{\chi(\sigma)}-1, \qquad \sigma(t)=\chi(\sigma)t.$$

The r^{th} *Coates-Wiles homomorphism* ($r\geq 1$) is the G-homomorphism $U \to \mathbb{Z}_p(r)$ given by

(20) $$\Phi^r{}_{CW}(u) = (d/dt)^r \log(g_u)(0)\cdot t^r.$$

Thus $\Phi^1{}_{CW}(u) = \delta g_u(0)\mathbf{t}$. It is easily checked that these homomorphisms are independent of the choice of ζ.

Theorem (explicit reciprocity law). Let $u\in U$, and $\alpha\in U_n$, where $n\geq 1$. Write $Tr_n=Tr_{K_n/\mathbb{Q}_p}$. Then

(21) $$[\alpha,u] = p^{-n}Tr_n(\log(\alpha)\cdot\delta g_u(\zeta_n-1)).$$

Proof. See [Iw]. Our notation follows [dS], ch.I, §4, where we give a short proof, as well as generalizations to other formal groups (due to Wiles [W]).□

6. The explicit reciprocity law of Bloch and Kato. Let $r\geq 1$, and consider

(22) $$\partial^r : \mathbb{Q}_p = H^0(\mathbb{Q}_p, A_{cris}\otimes\mathbb{Q}) \to H^1(\mathbb{Q}_p,\mathbb{Q}_p(r)),$$

the connecting homomorphism derived from (9). (Galois cohomology is always based on *continuous* cochains, and the modules are given their p-adic - or ind-p-adic, after we invert p - topologies, in which they are always complete.) Since restriction to the Galois group over K_∞ induces an isomorphism

$$(23)\qquad H^1(\mathbb{Q}_p,\mathbb{Q}_p(r)) \approx H^0(G,H^1(K_\infty,\mathbb{Q}_p(r))) = \mathrm{Hom}_G(U,\mathbb{Q}_p(r))$$

(an easy exercise), we may ask what is $\partial^r(1)$ as a G-homomorphism from U to $\mathbb{Q}_p(r)$. The answer is given in terms of the Coates-Wiles homomorphisms.

Theorem. ([B-K], theorem 2.1) For each $r\geq 1$

$$(24)\qquad \partial^r(1) = -\Phi^r{}_{CW}/(r-1)!$$

Proof. It seems better to consider, right from the beginning, cohomology over K_∞. Let $T=\varepsilon-1$ (so that $T=e^{\mathbf{t}}-1$), and observe that $\mathbb{Z}_p[[T]] \subseteq H^0(K_\infty,A_{cris})$, while $H^1(K_\infty,S^r) = \mathrm{Hom}(B,S^r)$ projects onto $\mathrm{Hom}(U,S^r)$. Restricting the map obtained from the connecting homomorphism to these subgroups, we obtain a continuous pairing of G-modules

$$(25)\qquad \partial^r : \mathbb{Z}_p[[T]] \times U \to S^r \qquad \partial^r(f,u)=\partial^r(f)(u)$$

which we wish to study. The theorem will follow from the following statement:

$$(26)\qquad \partial^r(f,u) = -\mathrm{Res}(t^{-r}f(T)\cdot d\log(g_u))\cdot \mathbf{t}^r.$$

Here f(T) is the power series obtained by substituting T (a formal variable) for **T**, and, as before, we have identified $\mathbb{Q}_p((t))$ with $\mathbb{Q}_p((T))$. Indeed, if f=1, $\mathrm{Res}(t^{-r}\cdot d\log(g)) = (d/dt)^r\log(g)(0)/(r-1)!$, so (26) and (24) coincide. The proof of (26) will be done in two steps. In §7 we do the case r=1. In §8 and §9 we reduce the general case to that of r=1.

7. Proof of (26) when r=1. Start with lemma 2.2. Let $\alpha \in H^0(K_\infty,1+pW(R))$, and pick $\beta \in 1+J$ such that $\beta^{p-\phi} = \alpha$. Then

$$\beta^{p^n-\phi^n} = \alpha^{p^{n-1}+p^{n-2}\phi+\cdots+p\phi^{n-2}+\phi^{n-1}}.$$

Now $\theta(\beta)=1$ implies

(27) $$\theta\phi^{-n}(\beta)^{p^n} = \theta\phi^{-n}(\alpha)^{p^{n-1}}\cdot\theta\phi^{1-n}(\alpha)^{p^{n-2}}\cdot\ \cdots\ \cdot\theta\phi^{-1}(\alpha).$$

In particular, take $\alpha = \alpha(T) \in 1+p\mathbb{Z}_p[[T]]$, and define

(28) $$\alpha^{(n)} = \alpha(T)^{p^{n-1}}\cdot\alpha((1+T)^p-1)^{p^{n-2}}\cdot\ \cdots\ \cdot\alpha((1+T)^{p^{n-1}}-1),$$

so that $\theta\phi^{-n}(\beta) = \alpha^{(n)}(\zeta_n-1)^{1/p^n}$, because $\theta\phi^{-i}(\alpha)=\alpha(\zeta_i-1)$. Thus, for every $\sigma\in\mathrm{Gal}(\overline{\mathbb{Q}}_p/K_\infty)$

(29) $$\theta\phi^{-n}(\beta^{\sigma-1}) = \theta\phi^{-n}(\beta)^{\sigma-1} = \{\alpha^{(n)}(\zeta_n-1)^{1/p^n}\}^{\sigma-1}.$$

By theorem 5 and lemma 2.1(ii), if $u\in U$ and

(30) $$\beta^{\sigma_u-1} = \varepsilon^{(\alpha,u)}$$

then $(\alpha,u) \equiv [\alpha^{(n)}(\zeta_n-1),u] \equiv p^{-n}\mathrm{Tr}_n\{\log(\alpha^{(n)})(\zeta_n-1)\cdot\delta g_u(\zeta_n-1)\} \bmod p^n$. However, comparing (4) and (9) (cf. remark following proposition 4), one gets $(\alpha,u)\mathbf{t} = \partial^{l}(p^{-1}\log(\alpha),u)$. We must therefore show that for $n\geq 1$

(31) $$p^{-n}\mathrm{Tr}_n\{\log(\alpha^{(n)})(\zeta_n-1)\cdot\delta g_u(\zeta_n-1)\} \equiv -\mathrm{Res}\{t^{-1}p^{-1}\log(\alpha)\cdot d\log(g_u)\} \bmod p^n.$$

7.1 Lemma. For $n\geq 1$, the following equality holds:

$$\mathrm{Tr}_n\{\log(\alpha^{(n)})(\zeta_n-1)\cdot\delta g_u(\zeta_n-1)\} = p^{n-1}\sum_{0<i<p^n}(\log(\alpha)\cdot\delta g_u)(\zeta_n{}^i-1).$$

Proof. The proof is a straightforward computation, based on the fact that for a p^n root of unity ξ,

$$\sum_{\eta^p=\xi} \delta g_u(\eta-1) = p\cdot\delta g_u(\xi-1).$$

Observe that $\log(\alpha)\in p\mathbb{Z}_p[[T]]$, and if $p=2$, $\log(\alpha)\in 4\mathbb{Z}_2[[T]]$. The proof of (31) will now be complete, provided we show

7.2 Lemma. For any $f\in\mathbb{Z}_p[[T]]$, $n\geq 1$,

(32) $$\sum_{0<i<p^n} f(\zeta_n{}^i-1) \equiv -\mathrm{Res}(t^{-1}f(T)dt) \bmod p^n$$

(if $p=2$, mod 2^{n-1}).

Proof. It is enough to check (32) with $f=(1+T)^m$, $m\geq 0$, because then it will hold for all $f\in\mathbb{Z}_p[T]$. Both sides of (32) are *continuous* homomorphisms from $\mathbb{Z}_p[[T]]$ to $\mathbb{Z}_p$, so if they agree on polynomials, they are equal. So let $f=(1+T)^m$. The left hand side is equal then to p^n-1 if $p^n|m$, and to -1 otherwise. The right hand side is computed as

$$-\mathrm{Res}\{T^{-1}(1+T/2-\cdots)(1+T)^m\cdot dT/(1+T)\} = -1.$$

This concludes the proof.

Remark. Coleman's power series are defined for any $\beta\in B$, and not only for $u\in U$, and if $\nu(\beta)=d$ (i.e. at each level n the valuation of β_n in K_n is d), the corresponding $g_\beta \in T^d\mathbb{Z}_p[[T]]^\times$. Thus $\mathrm{dlog}(g_\beta) \in T^{-1}\mathbb{Z}_p[[T]]dT$ in general. Formula (26) generalizes :

$$\partial^r(f,\beta) = -\mathrm{Res}(t^{-r}f(T)\cdot \mathrm{dlog}(g_\beta))\cdot \mathbf{t}^r$$

for all $f\in\mathbb{Z}_p[[T]]$ and $\beta\in B$. When $r=1$, the proof given above needs only minor modifications. Lemma 7.2, for example, has to be checked for f in $T^{-1}\mathbb{Z}_p[[T]]$. It is here, when one checks (32) for $f=T^{-1}$, that $p=2$ gives some trouble. The sum on the left comes out to be $(1-p^n)/2$, while the residue on the right is $1/2$. Fortunately, we only need the congruence modulo 2^{n-1} if $p=2$.

8. Reduction of the general case to the case r=1. Formula (26) is proven by reduction to the case r=1. We need two lemmas.

8.1 Lemma. If $f \in H^0(K_\infty, A_{cris})$ and $r>1$ then $\partial^r(tf) = t\partial^{r-1}(f)$.

Proof. The lemma follows immediately from the commutative diagram

$$(33)\qquad \begin{array}{ccccccccc} 0 & \longrightarrow & S^r & \longrightarrow & J_{cris}^{\langle r\rangle} & \xrightarrow{1-p^{-r}\phi} & A_{cris} & \longrightarrow & 0 \\ & & t\downarrow & & t\downarrow & & t\downarrow & & \\ 0 & \longrightarrow & S^{r+1} & \longrightarrow & J_{cris}^{\langle r+1\rangle} & \xrightarrow{1-p^{-r-1}\phi} & A_{cris} & \longrightarrow & 0. \end{array}$$

8.2 Lemma. The pairing $\mathbb{Z}_p[[T]]\times U \to S^r$ $(f,u) \mapsto \partial^r(f,u)$ factors as $\psi_r \circ \omega(f,u)$, where $\omega : \mathbb{Z}_p[[T]]\times U \to \Omega = \mathbb{Z}_p[[T]]dT$ is $\omega(f,u) = f(T)\cdot d\log(g_u)$, and $\psi_r : \Omega \to S^r$ is *some* G-homomorphism ($G=Gal(K_\infty/\mathbb{Q}_p)$).

The *proof* of this lemma, explained in full detail in §9, seems to require rather difficult concepts from syntomic cohomology, as developed by Fontaine and Messing.

8.3 Conclusion of the proof of (26). Granted lemmas 8.1 and 8.2, we proceed as follows. First, note that ω is surjective, because, for example, $1+T$ occurs as a possible g_u. Define

$$(34)\qquad \tilde{\psi}_r(\omega) = Res(t^{-r}\omega)t^r.$$

We have to check that $\tilde{\psi}_r=\psi_r$, a statement that is *equivalent* to (26) by the surjectivity of ω. For r=1 this was done in §7. By induction we may assume it to hold for r−1. Now $\tilde{\psi}_r$ annihilates $T^{r+1}\Omega$ (even $T^r\Omega$), hence extends to a homomorphism $\mathbb{Q}_p[[T]]dT/(T^{r+1}) \to \mathbb{Q}_p(r)$. The same is true for ψ_r, by corollary 4.8. Indeed, that corollary shows that $\partial^r(f,u)=0$ if $f\in T^{r+1}\mathbb{Z}_p[[T]]$, so lemma 8.2 implies $\psi_r(\omega)=0$ if $\omega\in T^{r+1}\Omega$. Having replaced $\mathbb{Z}_p$ by $\mathbb{Q}_p$, we may replace T by t, and we view ψ_r and $\tilde{\psi}_r$ as homomorphisms from $\mathbb{Q}_p[[t]]dt/(t^{r+1})$ to $\mathbb{Q}_p(r)$. By 8.1 and (34)

$$\psi_r(t\omega)=\mathbf{t}\psi_{r-1}(\omega), \qquad \tilde{\psi}_r(t\omega)=\mathbf{t}\tilde{\psi}_{r-1}(\omega),$$

so the induction hypothesis implies $\psi_r=\tilde{\psi}_r$ on $t\mathbb{Q}_p[[t]]dt/(t^{r+1})$. The difference $\psi_r-\tilde{\psi}_r$ therefore induces a G-homomorphism from $\mathbb{Q}_p$ to $\mathbb{Q}_p(r)$, which must be 0, so we conclude that $\psi_r=\tilde{\psi}_r$.

9. Proof of lemma 8.2. The proof is based on the commutative diagram of [B-K], p. 348. Here we present a slight variation of that diagram, and hopefully fill in some of the missing details. Let $\mathcal{R} = \mathbb{Z}_p[[T]] \subseteq A_{cris}$, let $A_n = A_{cris}/p^nA_{cris}$, $\mathcal{R}_n = \mathcal{R}/p^n\mathcal{R}$, $\overline{\mathcal{R}}_n$ = the image of $\mathcal{R}_n$ in A_n, $J^{\langle r\rangle}{}_n = J^{\langle r\rangle}{}_{cris}/p^nJ^{\langle r\rangle}{}_{cris}$, and $S^r{}_n=S^r/p^nS^r$. Let also U_m = the principal units of K_m. Taking coinvariants of multiplication by p^n in the fundamental exact sequence (9) we get the "mod p^n" exact sequence

$$(35) \qquad 0 \to S^r{}_n \to J^{\langle r\rangle}{}_n \to A_n \to 0,$$

which is exact also on the left because A_{cris} is p-torsion free. Take cohomology over K_m, $m\geq n$, and observe that $\overline{\mathcal{R}}_n \subseteq H^0(K_m,A_n)$ (an easy excercise; note that $\overline{\mathcal{R}}_n$ is the image of $\mathcal{R}$ in A_n and *not* $\mathcal{R}/p^n\mathcal{R}$). The connecting homomorphism will therefore give us a pairing

$$(36) \qquad \partial^r{}_n : \overline{\mathcal{R}}_n \times U_m/U_m{}^{p^n} \to S^r{}_n$$

whose composition with the natural projection $\mathcal{R}\times U \to \mathcal{R}_n\times U_m/U_m{}^{p^n}$ is simply ∂^r mod p^n. It is clearly enough to show that for every $n\geq 1$, ∂^r mod p^n factors through the homomorphism $f\otimes u \to f\cdot \mathrm{dlog}(g_u)$. In proving this we will work at the finite level m, but which m we choose is unimportant, as long as $m\geq n$.

9.1 We shall have to assume familiarity with the contents of [F2], §3.2-§3.7. It is shown there that A_n may be canonically identified with $H^0{}_{cris}(\mathcal{O}_{\overline{K},n}) = \lim_{\rightarrow} H^0{}_{cris}(\mathcal{O}_{L,n})$, L ranging over all the finite extensions of K in $\overline{K}$. Here we used the short-hand notation $H^i{}_{cris}(\mathcal{O}_{L,n}) = H^i(\mathrm{Spec}(\mathcal{O}_L/p^n\mathcal{O}_L)_{cris}, \mathcal{O}_{L/W_n})$ ($\mathcal{O}_{L/W_n}$ is the crystalline structure sheaf on the crystalline site).

Let $L = K_m$, and define $\Sigma_{L,n}$ and $D_{L,n}$ as in [F2], §3.2, where we choose $y = \zeta_m - 1$. Note that $\Sigma_{L,n} = \mathcal{R}_n = W_n[[T]]$, where $W_n = \mathbb{Z}/p^n\mathbb{Z}$. Let $f \in \mathcal{R} \subseteq W(R) \subseteq A_{cris}$, and assume $m \geqslant n$. Let $\alpha_{L,n}$ and β_n be the maps defined in [F2], §3.3 and §3.7 respectively. Then $\beta_n(f) \in W_n(\tilde{\mathcal{O}}_L) \subseteq W_n(\tilde{\mathcal{O}}_{\overline{K}})$ (it is enough to check this with $f=\varepsilon$). Furthermore, when we identify f as an element of $H^0{}_{cris}(\mathcal{O}_{L,n})$ via $\alpha_{L,n} \circ \beta_n$, we get that $\alpha_{L,n} \circ \beta_n(f)$ is the class of $\phi^n(f)$ in

(37) $$H^0{}_{cris}(\mathcal{O}_{L,n}) = \mathrm{Ker}\,(d : D_{L,n} \rightarrow D_{L,n} \otimes_{\Sigma_{L,n}} \Omega^1{}_{\Sigma_{L,n}})$$

(cf. [F2] §3.2). In (37) we mapped $\phi^n(f)$ to $\Sigma_{L,n}$ first, then to $D_{L,n}$, where it lands in the kernel of d.

We can also map, in the obvious way, $\Omega_n := \Omega^1{}_{\Sigma_{L,n}} = W_n[[T]]dT$ to

(38) $$H^1{}_{cris}(\mathcal{O}_{L,n}) = \mathrm{Coker}\,(d : D_{L,n} \rightarrow D_{L,n} \otimes_{\Sigma_{L,n}} \Omega^1{}_{\Sigma_{L,n}}).$$

Let T_p be Coleman's "trace operator" on $\mathcal{R}$ [C]. It is characterized by

(39) $$T_p \circ \phi(f) = pf,$$

its image is $p\mathcal{R}$, and the "projection formula" $T_p(\phi(f)g) = \phi(f)T_p(g)$ holds. Extend the definition of T_p to differentials in $\mathbb{Z}_p[[T]]dT$ as in [B-K], so that $T_p(f(T)dT/(1+T)) = p^{-1}T_p f(T)dT/(1+T)$. Then T_p fixes $\mathrm{dlog}(g_u)$ for $u \in U$. Now define a map

(40) $$\Omega_n \longrightarrow H^1{}_{cris}(\mathcal{O}_{L,n})$$

to be the composition of $T_p{}^n$ with the "obvious" map coming from (38). Then the discussion above may be summarized in the following lemma.

Lemma. Map $\mathcal{R}_n$ to $H^0{}_{cris}(\mathcal{O}_{L,n})$ by $\alpha_{L,n}\circ\beta_n$, and Ω_n into $H^1{}_{cris}(\mathcal{O}_{L,n})$ by (40). Then these maps are compatible with the natural action of H^0 on H^1 (and of $\mathcal{R}_n$ on Ω_n).

9.2 Recall the definition of the (small) syntomic site $(\mathrm{Spec}\ \mathcal{O}_L)_{syn}$ [F-M], and that of the sheaves $\mathcal{O}_n{}^{cris}$ and $\underline{S}^r{}_n$ on the syntomic site. In our notation, proposition II.1.3 of [F-M] states that

$$H^i{}_{cris}(\mathcal{O}_{L,n}) = H^i((\mathrm{Spec}(\mathcal{O}_L)_{syn},\mathcal{O}_n{}^{cris}) \qquad i=0,1. \tag{41}$$

Now consider the diagram

$$\begin{array}{ccc}
\mathcal{R}_n \times U/U^{p^n} & \xrightarrow{(f,u)\to f\cdot d\log(g_u)} & \Omega_n \\
\downarrow & A & \downarrow \\
H^0(\mathrm{Spec}(\mathcal{O}_L)_{syn},\mathcal{O}_n{}^{cris}) \times H^1(\mathrm{Spec}(\mathcal{O}_L)_{syn},\underline{S}^1{}_n) & \xrightarrow{\ \cup\ } & H^1(\mathrm{Spec}(\mathcal{O}_L)_{syn},\mathcal{O}_n{}^{cris}) \\
(\partial^r{}_n)_{syn}\times 1 \downarrow & B & (\partial^{r+1}{}_n)_{syn} \downarrow \\
H^1(\mathrm{Spec}(\mathcal{O}_L)_{syn},\underline{S}^r{}_n) \times H^1(\mathrm{Spec}(\mathcal{O}_L)_{syn},\underline{S}^1{}_n) & \xrightarrow{\ \cup\ } & H^2(\mathrm{Spec}(\mathcal{O}_L)_{syn},\underline{S}^{r+1}{}_n) \\
\downarrow & C & \downarrow \\
H^1(L,S^r{}_n) \times H^1(L,S^1{}_n) & \longrightarrow & H^2(L,S^{r+1}{}_n)
\end{array}$$

Explanations: The exact sequence (35) may be sheafified to produce an exact sequence of similar sheaves in the syntomic site. The vertical arrows in B are the connecting homomorphisms for that sequence. The horizontal arrows of B are cup product pairings. The commutativity of B is deduced from an analogue of (33) (lemma 8.1). The vertical arrows in C are the comparison maps between the syntomic cohomology and Galois cohomology. Just in order to define them, one needs the construction of the syntomic-étale site (cf. [F-M] §5). Square B and square C are the same as the bottom sqaures in [B-K], except that there the authors multiply the sheaves $S^r{}_n$ by some p^m to map them into $\mathbb{Z}/p^n\mathbb{Z}(r)$.

The vertical arrows in square A are constructed using (i) the maps defined in lemma 9.1 and the compatibility between them, (ii) the first Chern class map $U_m \to H^1(\mathrm{Spec}(\mathcal{O}_L)_{syn}, \underline{S}^1{}_n)$ (derived from the Kummer exact sequence in syntomic cohomology) and its relation to logarithmic differentials, and (iii) the comparison between syntomic cohomology of the sheaf $\mathcal{O}_n{}^{cris}$ and crystalline cohomology (41). In contrast with [B-K], we start with $\mathrm{Spec}(\mathcal{O}_L)$ and not with $\mathrm{Spec}(\mathcal{R})$, which allows us to map $\mathcal{R}_n$ and not just $\mathbb{Z}/p^n\mathbb{Z}$ into it. The ring $\mathcal{R}$ is (topologically) smooth, so its crystalline cohomology is dull, while that of $\mathcal{O}_L$ is rich !

The composition of the three vertical arrows on the left with the bottom horizontal arrow thus factors the way we want it to factor, since the top horizontal row is induced from ω. To conclude the proof of lemma 8.2 observe that the bottom horizontal arrow factors through $H^2(L, S^r{}_n \otimes S^1{}_n) = S^r{}_n$ (canonically!), and that the map we have constructed by following the vertical arrows on the left and then the bottom horizontal arrow (call it $\delta^r{}_n$) is the composition of $\partial^r{}_n$ with $S^r{}_n \to H^2(L, S^{r+1}{}_n)$. The latter has bounded kernel (as n increases), so from the validity of the lemma for $\delta^r{}_n$ for all n, follows its validity for $\partial^r{}_n$ as well. □

III. Other formal groups

10. Notation. From now on let K be an unramified extension of $\mathbb{Q}_p$ of degree d, π a uniformizer, $q=p^d$, and $\phi_K=\phi^d$. Fix a power series $f\in\mathcal{O}_K[[X]]$ such that

$$(42)\qquad f = \pi X + \cdots \equiv X^q \bmod \pi.$$

Let $F_f(X,Y)$ be the corresponding Lubin-Tate formal group law, and $\lambda_f(X)=X+\cdots \in K[[X]]$ its logarithm (cf. [dS], chapter I.1 for the notation used here). For $a\in\mathcal{O}_K$ let $[a]_f$ be the endomorphism of F_f whose power series expansion starts with $aX+\cdots$. Thus $f=[\pi]_f$. Let ω_n be a primitive π^n division point of F_f, such that

$$(43)\qquad f(\omega_n)=\omega_{n-1}, \qquad n\geq 1,$$

and denote by $\omega = (\omega_n)$ the corresponding generator of the *Tate module* of F_f,

$$(44)\qquad Ta(F_f) = \lim_{\leftarrow} \mathrm{Ker}\,[\pi^n] = [\mathcal{O}_K]\omega.$$

Write also $V_f = Ta(F_f)\otimes\mathbb{Q}$. Let $K_n=K(\omega_n)$ be the *Lubin-Tate tower*, analogous to the cyclotomic tower. Let $\kappa : \mathrm{Gal}(K_\infty/K) \approx \mathcal{O}_K^\times$ be the character giving the action of the Galois group on the π^n-torsion points (for all n), i.e. $\sigma(\omega_n)=[\kappa(\sigma)]_f(\omega_n)$. Then V_f is a one-dimensional vector space over K, on which the Galois group acts via κ.

10.1 Proposition. (i) There exists a unique $\mathbf{T} = T_\omega$ in W(R) such that

$$(45)\qquad \theta\phi_K^{-n}(T) = \omega_n \qquad n\geq 0.$$

(ii) For $\sigma\in G_K=\mathrm{Gal}(\bar{K}/K)$, $\sigma(T_\omega)=T_{\sigma(\omega)}=[\kappa(\sigma)]_f(T_\omega)$; $\phi_K(T_\omega)=[\pi]_f(T_\omega)$.
(iii) Let $\mathbf{t}=t_\omega$ be defined as $\lambda_f(T_\omega)$. Then $\mathbf{t}\in A_{cris}$ and

$$(46)\qquad \sigma(\mathbf{t})=\kappa(\sigma)\mathbf{t} \quad \forall\sigma\in G_K, \qquad \phi_K\mathbf{t}=\pi\mathbf{t}.$$

Remarks (i) When $K=\mathbb{Q}_p$ and $\pi=p$, so that F_f is (up to a change of variable) the multiplicative formal group, $T=\varepsilon-1$ (cf. (7)).

(ii) V_f is a crystalline representation of G_K. More generally this holds, by a theorem of Fontaine, with the Tate module of any p-divisible group over $\mathcal{O}_K$. The existence of t as in (46) is therefore not a new result (our proposition re-proves the fact that the Tate module is crystalline). What we want to emphasize is that a choice of a generator for the Tate module gives us, in a canonical way, an element of B_{cris}. In other words, $\mathrm{Hom}_{\mathbb{Q}_p[G_K]}(V_f, B_{cris})$ is not only d-dimensional over K, but has a *distinguished basis*, consisting of the homomorphisms that send ω to $\mathbf{t}_\omega$, $\phi\mathbf{t}_\omega$, ..., $\phi^{d-1}\mathbf{t}_\omega$. Note that the *line* $K\cdot\phi^i\mathbf{t}$ in $\mathrm{Hom}_{\mathbb{Q}_p[G_K]}(V_f, B_{cris})$ may be characterized as those homomorphisms that intertwine the K-action on V_f with the ϕ^i-twisted action of K on B_{cris}. In particular

$$\mathrm{Hom}_{K[G_K]}(V_f, B_{cris}) \approx \{ x\in B_{cris} \mid \sigma(x) = \kappa(\sigma)x \;\; \forall\sigma\in G_K \} = K\mathbf{t}$$

is one dimensional over K.

Proof. Everything, except the construction of $\mathbf{T}$, is easy. For example, the unicity, as well as the action of Galois and Frobenius, are deduced from the fact that $\bigcap\phi_K{}^n(J)=0$ (recall $J=\mathrm{Ker}(\theta)$). That $\mathbf{t}$ is in A_{cris} follows from the well known fact that $\lambda_f'(X)\in\mathcal{O}_K[[X]]$, while $T\in J$.

Let $\omega_{0,n}=\omega_n$. We shall define, by induction on i, $\omega_{i,n} \in \mathcal{O}(\mathbb{C}_p)$ $\forall n\geq 0$, and prove

(47) $$\omega_{i,n} \equiv \omega_{i,n+1}{}^q \mod \pi.$$

Then if we let $$x_{i,n} = \lim_{m\to\infty} \omega_{i,n+m}{}^{q^m}$$
we shall clearly have $$x_{i,n} = x_{i,n+1}{}^q.$$
We will also know that $$x_{i,n} \equiv \omega_{i,n} \mod \pi,$$
so we will be justified in setting, as the next step of the inductive definition,

$$\omega_{i+1,n} = (\omega_{i,n}-x_{i,n})/\pi.$$

Observe that $x_i = (\omega_{i,n} \mod \pi)_{n\geq 0} = (x_{i,n} \mod \pi)_{n\geq 0} \in R$, and with the notation of §1, $x_{i,n}=x_i{}^{(dn)}$. Therefore the element

(48) $$T = \sum_{i\geq 0} \pi^i [x_i] \in W(R),$$

and $\theta\phi_K^{-n}(T) = \sum_{i\geq 0}\pi^i x_{i,n} = \omega_n$. Everything now hinges on the proof of (47), which at first sight seems rather surprising. At least for i=0 it is obvious, since $\omega_{0,n}=f(\omega_{0,n+1})\equiv\omega_{0,n+1}{}^q \bmod \pi$. We need a lemma.

Lemma. If $h\in K[[X]]$ has bounded denominators, and $h(\omega_n)\in\mathcal{O}_K$ for infinitely many n, then $h\in\mathcal{O}_K[[X]]$.

The *proof* of the lemma is clear, since $|\omega_n| \to 1$ as $n \to \infty$.

We assume now that $\omega_{j,n}$ have been defined for $0\leq j\leq i$, and that they satisfy (47). We define $x_{i,n}$ and $\omega_{i+1,n}$ as above, and we wish to prove (47) with i+1.

Claim. For each $0\leq j\leq i$ and each $\nu\geq 1$ there exists a natural number $\mu(j,\nu)$ and a power series $h_{j,\nu}\in\mathcal{O}_K[[X]]$, such that

(49) $$\omega_{j,n} \equiv h_{j,\nu}(\omega_{\mu(j,\nu)+n}) \bmod \pi^\nu \qquad \forall n\geq 0.$$

The claim (with $\nu=1$ and j=i) will clearly imply (47). When j=0 it holds trivially, with $h_{0,\nu} = X$ and $\mu_{0,\nu} = 0$, so we prove the claim by induction on j. By the lemma, it is enough to find $h_{j,\nu}$ as above in K[[X]] (the proof will guarantee bounded denominators). Now

$$x_{j-1,n} = x_{j-1,n+\nu}{}^{q^\nu} \equiv \omega_{j-1,n+\nu}{}^{q^\nu} \equiv h_{j-1,1}(\omega_{\mu(j-1,1)+n+\nu})^{q^\nu} \bmod \pi^{\nu+1},$$

so $$\omega_{j,n} \equiv \{h_{j-1,\nu+1}(\omega_{\mu(j-1,\nu+1)+n}) - h_{j-1,1}(\omega_{\mu(j-1,1)+n+\nu})^{q^\nu}\}/\pi \bmod \pi^\nu.$$

Suppose that $a = \mu(j-1,\nu+1)-\mu(j-1,1)-\nu \geq 0$ (the case $a \leq 0$ being treated similarly). Define $\mu(j,\nu) = \mu(j-1,\nu+1)$, and

$$h_{j,\nu} = \{h_{j-1,\nu+1} - (h_{j-1,1}\circ f\circ f\circ \cdots \circ f)^{q^\nu}\}/\pi,$$

where f is composed with itself a times. Then (49) holds. □

10.2 Proposition. There exist exact sequences

$$(50)\qquad 0 \to [\mathcal{O}_K](T) \to F_f(J) \xrightarrow{f[-]_f\phi_K} F_f(\pi W(R)) \to 0$$

and

$$(51)\qquad 0 \to \mathcal{O}_K\mathbf{t} \to \lambda_f(J) \xrightarrow{1-\pi^{-1}\phi_K} W(R) \to 0.$$

The *proof* is left out. It is similar in principle to lemma 2.2. □

Now define

$$(52)\qquad \mathrm{Fil}^r{}_f\, A_{cris} = \{\, \alpha \in J_{cris}{}^{[r]} \mid \phi_K(\alpha) \in \pi^r A_{cris} \,\}.$$

This is a filtration similar to $J_{cris}{}^{\langle r\rangle}$. It depends on the formal group in question. Note that $\lambda_f(J) \subseteq \mathrm{Fil}^1{}_f(A_{cris})$.

11. Speculations. Propositions 10.1 and 10.2 may be viewed as the beginning of an attempt to generalize the results of this paper to other Lubin-Tate formal groups. For example, the analogue of the "fundamental exact sequence", with $Kt^r \cap A_{cris}$ replacing S^r as the left term, (52) replacing the middle term, and $1-\pi^{-r}\phi_K$ replacing $1-p^{-r}\phi$, seems to be incorrect (i.e., not exact). The reason is that A_{cris} is somehow "too big". There might be a smaller "A_{cris}" that will be the ring of p-adic periods, not for all motives with good reduction, but only for those whose p-adic realizations have *coefficients in* K, and with which the analogue of the fundamental exact sequence *will* hold. One would expect this smaller ring to be stable only under $\phi_K=\phi^d$, but not necessarily under ϕ. In particular, it should contain $\mathbf{t}$, but not $\phi^i\mathbf{t}$ for $1\leq i<d$. If so, is there a formula for the connecting homomorhpism of that sequence in terms of the Coates-Wiles homomorphisms ? The case r=1 requires only the existence of the sequence (51), and the proof given in §7 most probably generalizes, *mutatis mutandis,*

to general Lubin Tate groups. The general case needs to await analogous generalizations of the sheaves $\underline{S}^r$ and the main theorems of [F-M].

Work on p-adic periods of formal groups of abelian varieties has been done by Colmez [Cz] and by Winterberger [Win]. The first interesting non-ordinary case is the formal group of an elliptic curve with supersingular reduction. The easiest formal groups beyond the ordinary (i.e. essentially multiplicative) ones are Lubin-Tate groups of height > 1. We believe that relations between the structure of rings similar to A_{cris} and the arithmetic of Lubin-Tate groups should exist in general. In retrospect, this might be the motivation for the path taken in this paper.

Ehud de Shalit
Institute of Mathematics
Hebrew University
Giv'at Ram, Jerusalem
91904, ISRAEL
e-mail : deshalit@math.huji.ac.il

References

[B-K] Bloch, S., Kato, K. : L-functions and Tamagawa numbers of motives. In : *The Grothendieck Festschrift*, vol. I (Progress in Math. **86**), Birkhauser (1990), 333-400.

[C] Coleman, R. : Division values in local fields. Inv. Math. **53** (1979), 91-116.

[Cz] Colmez, P. : Périodes p-adiques des variétés abéliennes. Math. Ann. **292** (1992), 629-644.

[dS] de Shalit, E. : *Iwasawa theory of elliptic curves with complex multiplication*. Academic Press (1987).

[F1] Fontaine, J.-M. : Sur certains types de représentations p-adiques du groupe de Galois d'un corps local: construction d'un anneau de Barsotti-Tate. Ann. of Math., **115** (1982), 529-577.

[F2] Fontaine, J.-M. : Cohomologie de de-Rham, cohomologie cristalline, et représentations p-adiques. In : LNM **1016**, Springer-Verlag, Berlin (1983), 86-108.

[F3] Fontaine, J.-M. : Représentations p-adiques des corps locaux. In *The Grothendieck Festschrift*, vol. II (Progress in Math **87**) Birkhauser (1990), 249-309.

[F4] Fontaine, J.-M. : Séminaire de Bures, 1988. To appear in Astérisque.

[F-M] Fontaine, J.-M., Messing, W. : P-adic periods and p-adic étale cohomology. In : *Current trends in arithmetical algebraic geometry*, Cont. Math. **67** (1987) AMS, 179-207.

[Iw] Iwasawa, K. : Explicit formulas for the norm residue symbol. J. Math. Soc. Japan **20** (1968), 151-164.

[K] Kato, K. : The explicit reciprocity law and the cohomology of Fontaine-Messing. Bull. Soc. Math. France **119** (1991), 397-441.

[P] Perrin-Riou, B. : Théorie d'Iwasawa des représentations p-adiques : le cas local. C.R. Acad. Sci. Paris, **315 (Série I)** (1992), 629-632.

[S] Serre, J.-P. : *Local Fields* Springer-Verlag, Berlin (1979).

[W] Wiles, A. : Higher explicit reciprocity laws. Ann. Math. **107** (1978), 235-254.

[W] Wintenberger, J.-P. : Un scindage de la filtration de Hodge pour certaines variétés algébriques sur les corps locaux. Ann. Math. **119** (1984), 511-548.