J. COATES

A. WILES

Explicit reciprocity laws

Astérisque, tome 41-42 (1977), p. 7-17

<http://www.numdam.org/item?id=AST_1977__41-42__7_0>

Société Mathématique de France
Astérisque 41-42 (1977) p.7-17

EXPLICIT RECIPROCITY LAWS

by

J. COATES and A. WILES

-:-:-:-

Introduction

In an important paper, Iwasawa [5] proved a number of deep results about the arithmetic of cyclotomic fields. Recently, we have shown [3] that analogues of some of Iwasawa's results for fields of division points on elliptic curves with complex multiplication can be used to attack the conjecture of Birch and Swinnerton-Dyer or such curves. An essential ingredient in Iwasawa's work was the explicit reciprocity law of Artin and Hasse. Similarly, there seems little doubt that further progress on the results in [3] will depend on establishing full analogues of the Artin-Hasse law for fields of division points. In fact, this has already been done by one of us, and the detailed proofs will be appearing in [8]. The present note should be viewed as an informal, and not too technical, introduction to [8]. Throughout, we suppose that p is an odd prime number.

1. - Lubin-Tate formal groups

For the basic facts about Lubin-Tate formal groups, see [7] or Serre's article in [2]. We use the notation of [2]. Thus, if G is a one-parameter formal group defined by a power series in two variables with coefficients in $\mathbb{Z}_p$, and $\mathfrak{m}$ is the maximal ideal of the ring of integers of a finite extension of $\mathbb{Q}_p$, we write $G(\mathfrak{m})$ for the set $\mathfrak{m}$ endowed with the group law given by G. If $a \in \mathbb{Z}$, we denote by

$[a]_G$ the endomorphism of G defined by a. Addition and subtraction via G will be denoted by $\overset{*}{G}$ and $\widetilde{G}$. (The suffix G will be dropped when there is no danger of confusion.)

In this note we shall only be concerned with the special case of Lubin-Tate groups of height 1 defined over $\mathbb{Z}_p$. Recall that these arise in the following manner. Let π be any local parameter in $\mathbb{Z}_p$, and write $\mathfrak{F}_\pi$ for the set of all power series $f(X) \in \mathbb{Z}_p[[X]]$ satisfying (i) $f(X) \equiv \pi X$ mod. degree 2, and (ii) $f(X) \equiv X^p$ mod. p. To each $f \in \mathfrak{F}_\pi$, Lubin and Tate showed that there is a unique formal group G_f, defined over $\mathbb{Z}_p$, such that $[\pi]_{G_f} = f$. We call such a G_f a Lubin-Tate group (of height 1). If f and g are any two elements of $\mathfrak{F}_\pi$, the corresponding formal groups G_f and G_g are isomorphic over $\mathbb{Z}_p$. In making computations, it is often convenient to work with the Lubin-Tate group corresponding to the formal power series $f(X) = \pi X + X^p$. We always write $\mathcal{E}$ for this formal group.

We suppose now that π has been fixed, and let G be any Lubin-Tate group. The next lemma is a summary of some of the main results of Lubin-Tate theory (in the case of height 1 over $\mathbb{Z}_p$). For each $n \geq 0$, let G_{π^n} be the kernel of $[\pi^n]_G$ on G, and put $G_\infty = \bigcup_{n\geq 1} G_{\pi^n}$.

LEMMA 1. (Lubin-Tate) - (i) G_∞ <u>is isomorphic to</u> $\mathbb{Q}_p/\mathbb{Z}_p$ <u>as a</u> $\mathbb{Z}_p$-<u>module</u>.

(ii) <u>For each</u> $n \geq 0$, $\Phi_n = \mathbb{Q}_p(G_{\pi^{n+1}})$ <u>is a totally ramified abelian extension of</u> $\mathbb{Q}_p$ <u>of degree</u> $p^n(p-1)$, <u>from which</u> π <u>is a norm</u>.

(iii) <u>If</u> u <u>is a unit in</u> $\mathbb{Z}_p^\times$, <u>then the Artin symbol</u> $\sigma_u = (u, \Phi_n/\mathbb{Q}_p)$ <u>acts on</u> G_∞ <u>via</u> $[u^{-1}]_G$.

One of the simplifications introduced by the use of the special Lubin-Tate group E mentioned above is given by the following lemma.

LEMMA 2. - <u>For the formal group</u> $\mathcal{E}$, <u>we have</u> $[\zeta](w) = \zeta w$ <u>for each</u> $(p-1)$-th <u>root of unity</u> ζ <u>in</u> $\mathbb{Z}_p$. <u>Moreover if</u> $\mathcal{E}(X,Y) = X + Y + \sum_{i+j\geq 2} a_{ij} X^i Y^j$ <u>is the formal group law of</u> $\mathcal{E}$, <u>then</u> $a_{ij} = 0$ <u>unless</u> $i+j \equiv 1 \mod (p-1)$.

<u>Proof</u>. - For each $n \geq 0$ choose a generator u_n of $\mathcal{E}_{\pi^{n+1}}$ such that $[\pi](u_n) = u_{n-1}$. Let ζ be a fixed $(p-1)$-th root of unity. As the minimal polynomial for u_n over $\mathbb{Q}_p$ is a polynomial in X^{p-1}, we can find $\sigma_n \in G(\Phi_n/\mathbb{Q}_p)$ such that $\sigma_n(u_n) = \zeta u_n$. Thus there is an element σ of $G(\Phi_\infty/\mathbb{Q}_p)$, where $\Phi_\infty = \bigcup_{n=0}^{\infty} \Phi_n$, such that

$\sigma_n(u_n) = \zeta u_n$ for all n. By the last part of lemma 1 there exists $a \in \mathbb{Z}_p$ such that $\sigma(u_n) = [a](u_n)$ for all $n \geq 0$. Since $\sigma^{p-1} = 1$, a is a $(p-1)$-th root of unity. Let $\mathfrak{p}_n$ be the maximal ideal of Φ_n. Then, as

$$\zeta u_n = [a](u_n) \equiv a u_n \mod \mathfrak{p}_n^2 ,$$

$\zeta \equiv a \mod p$, whence $\zeta = a$.

The final assertion follows easily because we have

$$\rho . \mathcal{S}(X, Y) = \mathcal{S}(\rho X, \rho Y) \text{ for every } (p-1)\text{-th root of unity } \rho .$$

Let λ_G be the logarithm map of the formal group G. Thus λ_G is an isomorphism over $\mathbb{Q}_p$ of G with the formal additive group.

LEMMA 3. - <u>Let</u> $\lambda_G(w) = w + \sum_{i=x}^{\infty} a_i w^i$. <u>Then</u> $i a_i \in \mathbb{Z}_p$ <u>for all</u> $i \geq 2$. <u>For</u> $\lambda_{\mathcal{S}}$, $a_i = 0$ <u>unless</u> $i \equiv 1 \mod (p-1)$.

<u>Proof</u>. - For the first statement see [4]. The second follows from lemma 2 because $\zeta . \lambda(X) = \lambda([\zeta](X))$.

2. - <u>Norm-residue symbol</u>

As in the previous section, we suppose that we have fixed a local parameter π for $\mathbb{Z}_p$, and we take G to be any Lubin-Tate formal group associated with π. We now study an analogue of the Hilbert norm residue symbol for the fields $\Phi_n = \mathbb{Q}_p(G_{\pi^{n+1}})$. The definition of this symbol has previously been proposed by Fröhlich [4].

Fix an integer $n \geq 0$. Let $\mathfrak{p}_n$ be the maximal ideal of the ring of integers of Φ_n. The generalized norm residue symbol is a pairing

$$(\; , \;)_n^G : G(\mathfrak{p}_n) \times \Phi_n^{\times} \longrightarrow G_{\pi^{n+1}} ,$$

which is defined as follows. If $\beta \in \Phi_n$, let σ_β be the element of the Galois group over Φ_n of the maximal abelian extension of Φ_n, which is attached to β by local class field theory. If $\alpha \in G(\mathfrak{p}_n)$, choose γ in the maximal ideal of the ring of integers of the algebraic closure of $\mathbb{Q}_p$ such that $[\pi^{n+1}](\gamma) = \alpha$. Then we define $(\alpha, \beta)_n^G = \sigma_\beta \gamma \underset{G}{-} \gamma$. It is obvious that this definition is independent of the choice of γ.

Let $\Phi_\infty = \bigcup_{n \geq 0} \Phi_n$, and let $\varkappa : G(\Phi_\infty/\mathbb{Q}_p) \longrightarrow \mathbb{Z}_p^{\times}$ be the character giving the action of the Galois group of $\Phi_\infty/\mathbb{Q}_p$ on $G_\infty = \bigcup_{n \geq 0} G_{\pi^{n+1}}$, i.e. $\varkappa$ is defined by

$u^{\sigma} = [\varkappa(\sigma)](u)$ for all $u \in G_{\infty}$. Note that $\varkappa$ is independent of the choice of the Lubin-Tate group G. One verifies immediately that

$$(\alpha^{\sigma}, \beta^{\sigma})_n^G = [\varkappa(\sigma)](\alpha, \beta)_n^G \quad \text{for all} \quad \sigma \in G(\Phi_{\infty}/\mathbb{Q}_p).$$

Suppose next that G_1 and G_2 are any two Lubin-Tate groups, and take $\varphi : G_1 \xrightarrow{\sim} G_2$ to be an isomorphism defined over $\mathbb{Z}_p$. Then it is plain that

$$(1) \qquad (\alpha, \beta)_n^{G_2} = \varphi((\varphi^{-1}(\alpha), \beta)_n^{G_1}).$$

Recall that $\mathcal{S}$ is the formal group corresponding to the power series $\pi X + X^p$. From now on, we shall mainly study the symbol $(\alpha, \beta)_n^{\mathcal{S}}$. For simplicity, we write $(\alpha, \beta)_n$ for $(\alpha, \beta)_n^{\mathcal{S}}$.

LEMMA 4. - (i) $(\alpha, \beta)_n$ <u>is</u> $\mathbb{Z}_p$<u>-bilinear</u>

(ii) $(\alpha, \beta)_n = 0$ <u>if and only if</u> β <u>is a norm from</u> $\Phi_n(\gamma)$, <u>where</u> $[\pi^{n+1}](\gamma) = \alpha$

(iii) $(\alpha, \alpha)_n = 0$ <u>for all</u> $\alpha \neq 0$ <u>in</u> $\mathfrak{p}_n$.

<u>Proof</u>. - The only assertion which does not follow formally from the definition is (iii). Let $f_n(X) = [\pi^{n+1}](X)$. Then, if γ is any root of $f_n(X) = \alpha$, the extension $\Phi_n(\gamma)/\Phi_n$ is obviously independent of the choice of γ. Thus, if we factor $f_n(X) - \alpha$ into irreducible polynomials over Φ_n, say $f_n(X) - \alpha = \prod_{j \in J} f_{n,j}(X)$, then, for each j, we must obtain $\Phi_n(\gamma)$ by adjoining a single root of $f_{n,j}(X)$ to Φ_n. Therefore, if $c_{n,j}$ denotes the constant term of $f_{n,j}(X)$, then $-c_{n,j}$ is a norm from $\Phi_n(\gamma)$ for each j. Hence $\alpha = \prod_{j \in J}(-c_{n,j})$ is also a norm from $\Phi_n(\gamma)$, and so (ii) implies (iii).

One explicit reciprocity law is immediate from lemma 1. Let u_n be a generator of $\mathcal{S}_{\pi^{n+1}}$. Let N_n and T_n denote the norm and trace from Φ_n to $\mathbb{Q}_p$. Then it follows easily from assertion (iii) of lemma 1 that

$$(u_n, \beta)_n = [1/\pi^{n+1}(N_n \beta^{-1} - 1)](u_n)$$

for each unit $\beta \equiv 1 \mod \mathfrak{p}_n$ in Φ_n. Since $N_n \beta^{-1} - 1 \equiv 0 \mod p^{n+1}$, this law can be rewritten as

$$(2) \qquad (u_n, \beta)_n = [-1/\pi^{n+1}\, T_n(\log \beta)](u_n),$$

where the log is the ordinary p-adic logarithm. In the special case in which $\pi = p$, one can transfer this law to the formal multiplicative group by the general remarks made earlier.

3. - The map ψ_n

In order to go further, it is important to introduce a map ψ_n, first studied in the cyclotomic case by Iwasawa. The additive group of Φ_n is locally compact, and is self-dual under the pairing

$$(3) \qquad < \, , \, >_n \; : \; \Phi_n \times \Phi_n \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p$$

given by $<a, b>_n = T_n(ab) \bmod \mathbb{Z}_p$. Let $\lambda : \mathcal{E} \longrightarrow G_a$ be the logarithm of $\mathcal{E}$. Then λ converges for each $w \in \mathfrak{p}_n$. So $\lambda(\mathfrak{p}_n)$ is a closed subgroup of Φ_n, and we denote its orthogonal complement under the above pairing by $\mathfrak{X}_n$. Let $\Phi_n^* = N_{2n+1,n}(\Phi_{2n+1}^\times)$. The following lemma corresponds to proposition 14 of [5].

LEMMA 5. - <u>Fix a generator</u> u_n <u>of</u> $\mathcal{E}_{\pi^{n+1}}$. <u>Then there exists a unique map</u> $\psi_n : \Phi_n^* \longrightarrow \mathfrak{X}_n/\pi^{n+1}\mathfrak{X}_n$ <u>such that</u>

$$(4) \qquad (\alpha, \beta)_n = [T_n(\lambda(\alpha)\, \psi_n(\beta))](u_n)$$

<u>for all</u> $\alpha \in \mathcal{E}(\mathfrak{p}^n)$ <u>and</u> $\beta \in \Phi_n^*$. <u>This map is a group homomorphism and</u> $\psi_n(\beta^\tau) = \kappa(\tau)\, \psi_n(\beta)$ <u>for all</u> $\tau \in G(\Phi_\infty/\mathbb{Q}_p)$.

<u>Proof</u>. - The proof is essentially the same as in [5], and is a formal argument involving the dual pairing (3). Let $i : \mathcal{E}_{\pi^{n+1}} \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p$ be the unique homomorphism such that $i(u_n) = p^{-(n+1)} \bmod \mathbb{Z}_p$. Take $\beta \in \Phi_n^*$, and we proceed to define $\psi_n(\beta)$. Since β is a norm from Φ_{2n+1} by hypothesis, we have $(v, \beta)_n = 0$ for all $v \in \mathcal{E}_{\pi^{n+1}}$. Thus the map $\lambda(\alpha) \longmapsto i(\alpha, \beta)_n$ gives a well defined homomorphism from $\lambda(\mathfrak{p}_n)$ to $\mathbb{Q}_p/\mathbb{Z}_p$ (recall that the kernel of λ on $\mathcal{E}(\mathfrak{p}_n)$ is $\mathcal{E}_{\pi^{n+1}}$). As $\lambda(\mathfrak{p}_n)$ is dual to $\Phi_n/\mathfrak{X}_n$ under the pairing (3), it follows that there exists β'' in Φ_n such that $i(\alpha, \beta)_n = T_n(\beta''.\lambda(\alpha)) \bmod \mathbb{Z}_p$ for all α in $\mathcal{E}(\mathfrak{p}_n)$. If we put $\beta' = p^{n+1}\beta''$, it is plain that β' belongs to $\mathfrak{X}_n$, and that $(\alpha, \beta)_n = [T_n(\beta'.\lambda(\alpha))](u_n)$. We define $\psi_n(\beta)$ to be the coset of β' in $\mathfrak{X}_n/\pi^{n+1}\mathfrak{X}_n$. Plainly $\psi_n(\beta)$ is uniquely determined by the equation (4). In particular, this implies that ψ_n must be a group homomorphism. The final assertion follows easily from the fact that $(\alpha^\tau, \beta^\tau) = [\kappa(\tau)](\alpha, \beta)_n$ for all $\tau \in G(\Phi_\infty/\mathbb{Q}_p)$. This completes the proof.

We now investigate the non-degeneracy of the pairing $(\, , \,)_n$. We first establish a preliminary lemma. Let I be the index set consisting of p^{n+1} and all integers i with $(i, p) = 1$ and $1 \leq i < p^{n+1}$.

LEMMA 6. - Let u_n be a generator of $\mathcal{E}_{\pi^{n+1}}$, and let $A_n = \{u_n^i : i \in I\}$. Then

(i) $\mathcal{E}(\mathfrak{p}_n)$ is generated over $\mathbb{Z}_p$ by the set A_n, and

(ii) $\mathcal{E}(\mathfrak{p}_n)/[\pi^{n+1}]\,\mathcal{E}(\mathfrak{p}_n)$ is freely generated over $\mathbb{Z}_p/\pi^{n+1}\mathbb{Z}_p$ by the residue classes of the elements of A_n.

Proof. - We first prove (i). As $\mathbb{Z}_p$ is complete it suffices to show that $\mathcal{E}(\mathfrak{p}_n)/[\pi]\,\mathcal{E}(\mathfrak{p}_n)$ is generated over $\mathbb{Z}_p$ by A_n. Let β_i $(1 \le i \le p^{n+1})$ be arbitrary elements of $\mathfrak{p}_n$ such that $v_{\mathfrak{p}_n}(\beta_i) = i$ (here $v_{\mathfrak{p}_n}$ denotes the order valuation of $\mathfrak{p}_n$). If w_1, w_2 are any two elements of $\mathfrak{p}_n$, the power series giving $w_1 \sim w_2$ is $w_1 - w_2$ modulo terms of degree at least 2 in w_1 and w_2. Suppose α is any element of $\mathfrak{p}_n$. Then there exists $a_1 \in \mathbb{Z}_p$ such that $\alpha \equiv [a_1]\beta_1 \mod \mathfrak{p}_n^2$. Thus $\alpha \sim [a_1]\beta_1 \equiv 0 \mod \mathfrak{p}_n^2$. We can therefore choose $a_2 \in \mathbb{Z}_p$ such that $\alpha \sim [a_1]\beta_1 \equiv a_2\beta_2 \mod \mathfrak{p}_n^3$. Arguing recursively, we conclude that there exists $a_1, \dots, a_{p^{n+1}}$ in $\mathbb{Z}_p$ such that $\alpha \sim [a_1]\beta_1 \sim \dots \sim [a_{p^{n+1}}]\beta_{p^{n+1}}$ belongs to $\mathfrak{p}_r^{p^{n+1}+1}$. But any $\gamma \in \mathfrak{p}_r^{p^{n+1}+1}$ belongs to $[\pi]\,\mathcal{E}(\mathfrak{p}_n)$. For let u_o be a generator of $\mathcal{E}_\pi$. Dividing the equation $X^p + \pi X = \gamma$ by u_o^p, and putting $Y = X/u_o$, we obtain the equation $Y^p - Y = \rho$, where $\rho = \gamma/u_o$ belongs to $\mathfrak{p}_n$. This latter equation has a simple root mod $\mathfrak{p}_n$ at $Y = 1$, and so has a solution in Φ_n by Hensel's lemma. Hence γ itself belongs to $[\pi]\,\mathcal{E}(\mathfrak{p}_n)$, as asserted. Part (i) now follows on noting that we can take $\beta = u_n^i$ for $i \in I$, and $\beta_i = [\pi^r](u_n^{i/p^r})$ for those i with $1 \le i < p^{n+1}$ which are divisible by p; here p^r denotes the exact power of p dividing i. As for (ii), suppose that there do exist $a_i \in \mathbb{Z}_p$ $(i \in I)$, with not all $a_i \in \pi^{n+1}\mathbb{Z}_p$, such that $\sum_{i \in I} [a_i](u_n^i)$ belongs to $[\pi^{n+1}]\,\mathcal{E}(\mathfrak{p}_n)$ (here Σ denotes summation in the formal group). Dividing by the greatest common factor of the a_i $(i \in I)$, we can assume that we have a relation $\sum_{i \in I} [a_i](u_n^i) \in [\pi]\,\mathcal{E}(\mathfrak{p}_n)$, where not all a_i belong to $\pi\mathbb{Z}_p$. Let i_o be the smallest index such that $a_{i_o} \notin \pi\mathbb{Z}_p$. Suppose first that $i_o < p^{n+1}$. One deduces easily that $v_{\mathfrak{p}_n}(\sum_{i \in I} [a_i](u_n^i)) = i_o$. But this is impossible because for any $\beta \in [\pi]\,\mathcal{E}(\mathfrak{p}_n)$, we have either $v_{\mathfrak{p}_n}(\beta) \equiv 0 \mod p$ or $v_{\mathfrak{p}_n}(\beta) > p^{n+1}$. Suppose finally that $i_o = p^{n+1}$, so that $[a_{p^{n+1}}](u_n^{p^{n+1}})$, and thus also $u_n^{p^{n+1}}$, belongs to $[\pi]\,\mathcal{E}(\mathfrak{p}_n)$. This means that there exists α in $\mathfrak{p}_n$ such that $a^p + \pi\alpha = u_n^{p^{n+1}}$, or equivalently, $(\alpha/u_o)^p - (\alpha/u_o) = u_n^{p^{n+1}}/u_o^p$. As the residue field has p elements, the left hand side of this equation must lie in $\mathfrak{p}_n$, but the right hand side clearly does not. This contradiction completes the proof of the lemma.

LEMMA 7. - The norm residue symbol $(\ ,\ )_n$ gives rise to a non-degenerate pairing

$$\mathcal{E}(\mathfrak{p}_n)/[\pi^{n+1}]\,\mathcal{E}(\mathfrak{p}_n) \times \Phi_n^\times/\Phi_n^{\times\, p^{n+1}} \longrightarrow \mathcal{E}_{\pi^{n+1}} \tag{5}$$

for all $n \geq 0$ if and only if Φ_o contains no non-trivial p-th root of unity.

Proof. - Since the Artin map is surjective, it is plain that $(\alpha, \beta)_n = 0$ for all $\beta \in \Phi_n^\times$ implies that α belongs to $[\pi^{n+1}]\,\mathcal{E}(\mathfrak{p}_n)$. Thus the pairing (5) will be non-degenerate if and only if the two groups on the left of (5) have the same order. Put $q_n = p^{n+1}$. By lemma 6 the order of $\mathcal{E}(\mathfrak{p}_n)/[\pi^{n+1}]\mathcal{E}(\mathfrak{p}_n)$ is $q_n^{(p-1)p^n+1}$, and a well known computation shows that the order of $\Phi_n^\times/\Phi_n^{\times p^{n+1}}$ is $q_n^{(q-1)p^n+1}\, p^{r_n}$, where p^{r_n} is the order of the group of p-power roots of unity in Φ_n. But it easy to see that $r_n = 0$ for all $n \geq 0$ if and only if $r_o = 0$, and so the proof of the lemma is complete.

LEMMA 8. - The map ψ_n of lemma 5 is surjective.

Proof. - The pairing $(\ ,\ )_n$ gives rise to an exact sequence

$$1 \longrightarrow \mathcal{E}(\mathfrak{p}_n)/[\pi^{n+1}]\,\mathcal{E}(\mathfrak{p}_n) \longrightarrow \mathrm{Hom}(\Phi_n^\times/\Phi_n^{\times\, p^{n+1}}, \mathcal{E}_{\pi^{n+1}}) \longrightarrow \mathrm{coker} \longrightarrow 1$$

of abelian groups. Suppose that $\beta' \in \mathfrak{X}_n$. Then the map $\alpha \to [T_n(\lambda(\alpha)\beta')](u_n)$ is a homorphism from $\mathcal{E}(\mathfrak{p}_n)$ to $\mathcal{E}_{\pi^{n+1}}$ which vanishes on $[\pi^{n+1}]\,\mathcal{E}(\mathfrak{p}_n)$. By dualizing the above exact sequence with respect to $\mathcal{E}_{\pi^{n+1}}$ we see that there exists $\beta \in \Phi_n^\times$ such that $(\alpha, \beta)_n = [T_n(\lambda(\alpha)\beta')](u_n)$ for all $\alpha \in \mathcal{E}(\mathfrak{p}_n)$. In particular, we have $(u_n, \beta)_n = 0$ because $\lambda(u_n) = 0$. Thus β belongs to Φ_n^*, and by construction $\psi_n(\beta) = \beta'$.

Let $\Phi'_n = \bigcap_{m \geq n} N_{m,n}(\Phi_n^\times)$. It is shown in [3] that Φ'_n consists of all elements of $\Phi_n^\times$ whose norm is a power of π, and that $\Phi_n^\times = \Phi'_n \times V$, where V is the group of units of $\mathbb{Z}_p$ which are $\equiv 1 \bmod p$. Hence $\Phi_n^* = \Phi'_n \times V^{p^{n+1}}$ (recall that $\Phi_n^* = N_{2n+1,n}(\Phi_n^\times)$). As ψ_n is trivial on $V^{p^{n+1}}$, ψ_n induces a surjective homomorphism $\Phi'_n \to \mathfrak{X}_n/\pi^{n+1}\mathfrak{X}_n$. If Φ_o contains no non-trivial p-th root of unity, then the kernel of this induced map is $\Phi_n^{\times p^{n+1}} \cap \Phi'_n$. For then $\psi_n(\beta) = 0$ implies $\beta \in \Phi_n^{\times\, p^{n+1}}$ by the non-degeneracy of the pairing $(\ ,\ )_n$. But $\Phi_n^{\times p^{n+1}} \cap \Phi'_n = \Phi'^{\,p^{n+1}}_n$, and so we have proved the following lemma.

LEMMA 9. - If Φ_o contains no non-trivial p-th root of unity, then for all $n \geq 0$, ψ_n induces an isomorphism

$$\Phi'_n / \Phi'^{\,p^{n+1}}_n \xrightarrow{\ \sim\ } \mathfrak{X}_n / \pi^{n+1}\, \mathfrak{X}_n .$$

4. - Explicit laws

We turn now to the computation of some of the explicit reciprocity laws when $n = 0$. An alternative approach, though not quite so general, may be found in [3].

LEMMA 10. - (i) $(u_o^i, u_o)_o = 0$ for $1 \leq i < p$, and (ii) $(u_o^p, u_o)_o = u_o$.

Proof. - (i) is immediate from the fact that $(u_o^i, u_o^i)_o = 0$. The proof of (ii) is very similar to that of [1], chapter 12, theorem 8. Let γ be such that $[\pi](\gamma) = u_o^p$. Dividing the equation $X^p + \pi X = u_o^p$ by u_o^p, we see that γ / u_o satisfies the equation $Y^p - Y = 1$. As this equation has no solution mod $\mathfrak{p}_o$, there must be an extension of the residue field in $\Phi_o(\gamma)/\Phi_o$, and so $\Phi_o(\gamma)/\Phi_o$ must in fact be unramified (since it is of degree p). Thus as u_o is a local parameter for Φ_o, the action of the Artin symbol of u_o on $\Phi_o(\gamma)$ must be the same as that of the Frobenius automorphism. In particular, if we put $\beta = \gamma / u_o$, we have $\delta_{u_o}(\beta) \equiv \beta^p \mod \mathfrak{p}_o$. Now, by definition,

$$(u_o^p, u_o)_o = \delta_{u_o}(\gamma) \sim \gamma = \delta_{u_o}(\beta u_o) \sim \beta u_o = \delta_{u_o}(\beta) u_o \sim \beta u_o .$$

Substituting $\delta_{u_o}(\beta) \equiv \beta^p \mod \mathfrak{p}_o$ in the expression on the right, and then using the equation $\beta^p = \beta + 1$, we obtain

$$(u_o^p, u_o)_o \equiv \beta^p u_o \sim \beta u_o = (\beta + 1) u_o \sim \beta u_o \equiv u_o \mod \mathfrak{p}_o^2 .$$

But if two elements of $\mathcal{S}_\pi$ are congruent mod $\mathfrak{p}_o^2$, they must be equal. This is plain from the fact that u_o is a local parameter for Φ_o, and that the elements of $\mathcal{S}_\pi$ are given by 0 and the ζu_o for ζ ranging over the group of $(p-1)$-th roots of unity. This completes the proof.

LEMMA 11. - Let i, j be positive integers with $1 < i < p$. Then $(u_o^i, 1 - u_o^j)_o$ is 0 or $[-j](u_o)$, according as j does not or does divide $p - i$.

Proof. - Put $w = u_o^i (u_o^j - 1)$, and $v = u_o^i * w$. Since $i > 1$, it is clear from the second assertion of lemma 2 that $v \sim u_o^{i+j} \equiv 0 \mod \mathfrak{p}_o^{p+1}$. Hence (cf. the proof of lemma 6), we have $v = u_o^{i+j} * [\pi](\alpha)$, for some $\alpha \in \mathcal{S}(\mathfrak{p}_o)$. Recalling (iii) of lemma 4, we deduce that

$$(u_o^i, u_o^j - 1)_o = (u_o^i, w)_o = (v, w)_o = (v, u_o^j - 1)_o * (v, u_o^i)_o .$$

As $v = u_o^{i+j} * [\pi](\alpha)$, it follows that

$$(u_o^i, u_o^j - 1)_o = (u_o^{i+j}, u_o^j - 1)_o * (u_o^{i+j}, u_o^i)_o .$$

Solving recursively, we obtain

$$(u_o^i, u_o^j - 1)_o = \sum_{r=1}^{\infty} (u_o^{i+rj}, u_o^{i+(r-1)j})_o ,$$

where Σ denotes summation on the formal group. The sum on the right is finite, because the symbol is trivial when $i+rj > p$. Lemma 11 now follows from lemma 10.

5. - Computation of ψ_o

First we introduce the map δ_o. Let γ be any element of Φ_o. We may write γ in the form $\gamma = u_o^{\mathrm{ord}(\gamma)} . \rho . (1 + a_1 u_o + a_2 u_o^2 + \dots)$, where ρ is a $(p-1)$-th root of unity and the a_i are in $\mathbb{Z}_p$. Such a representation is not unique. However, for some such representation, let $\gamma(z) = z^{\mathrm{ord}(\gamma)} . (1 + a_1 z + a_2 z^2 + \dots)$. Then define

$$\delta_o(\gamma) = (1/\pi) . \frac{d}{dz} \log \gamma(z) \big|_{z = u_o} .$$

LEMMA 12. - δ_o <u>is well-defined</u> mod $\pi \mathfrak{X}_o$, <u>and thus induces a homomorphism</u>

$$\delta_o : \Phi_o^\times \longrightarrow \mathfrak{X}_o / \pi \mathfrak{X}_o .$$

<u>Proof</u>. - Recall that $\mathfrak{X}_o = \{a \in \Phi_o : T_o(a . \lambda(\alpha)) \in \mathbb{Z}_p$ for all $\alpha \in \mathscr{S}(\mathfrak{p}_o)\}$. But $\lambda(\mathfrak{p}_o) = \lambda(\mathfrak{p}_o^2) = \mathfrak{p}_o^2$ because $\lambda(u_o) = 0$, so we see that $\mathfrak{X}_o = 1/\pi . \mathfrak{p}_o^{-1}$. It is straightforward to check that δ_o is well-defined mod $\mathfrak{p}_o^{-1}$ (cf. lemma 3 of [6]) and the lemma follows.

THEOREM 13. - <u>For</u> $\alpha \in \mathscr{S}(\mathfrak{p}_o^2)$ <u>and</u> $\beta \in \Phi_o^\times$,

$$(6) \qquad (\alpha, \beta)_o = [T_o(\lambda(\alpha)\, \delta_o(\beta))](u_o) .$$

<u>In particular</u> $\psi_o = \delta_o$ <u>on</u> Φ_o^*.

<u>Proof</u>. - By lemma 12 the expression on the right of (6) is well-defined. Further, both sides are bilinear (of course linear in α means with respect to the formal group law). So we need only check the equality for $\alpha = u_o^i$, $2 \leq i < p$, and β in some generating set of $\Phi_o^\times$. It is shown in [1], chapter 12, that we may take this

generating set to consist of u_o, $1-u_o^j$ $(j\geq 1)$, and the $(p-1)$-th roots of unity.

We verify (6) when $\beta = 1-u_o^j$, the other cases being easier. By definition

$$\delta_o(1-u_o^j) = -(j/\pi)\sum_{r=1}^{\infty} u_o^{rj+1} \quad \text{mod } \pi\mathfrak{X}_o .$$

On the other hand, lemma 3 implies that $\lambda(\alpha)\equiv\alpha$ mod $\mathfrak{p}_o^{p+1}$, for all $\alpha\in\mathcal{F}(\mathfrak{p}_o^2)$. It follows easily that

$$(7) \qquad [\,T_o(\lambda(u_o^i)\,\delta_o(1-u_o^j))\,](u_o) = [\,-(j/\pi)\,T_o(\sum_{r=1}^{\infty} u_o^{rj+i-1})\,](u_o) .$$

Now $T_o(u_o^t)$ is 0 or $(p-1)(-\pi)^{t/p-1}$, according as $(p-1)$ does not or does divide t. A simple computation now shows that the right hand side of (7) agrees with the value of $(u_o^i, 1-u_o^j)_o$ given by lemma 11. To prove the final assertion of theorem 13, we note that (6) is clearly valid when $\alpha = u_o$ and $\beta\in\Phi_o^*$, whence $\psi_o = \delta_o$ by the uniqueness of ψ_o.

We may derive one of the Artin-Hasse laws immediately from theorem 13. Take $\pi = p$, and choose an isomorphism φ from the multiplicative group G_m to $\mathcal{F}$, such that $\varphi(z)\equiv z$ mod degree 2. Define $\delta_o^{G_m}$ in the same way as δ_o, except with $\zeta_o - 1 = \varphi^{-1}(u_o)$ as the local parameter in place of u_o. Then

$$\delta_o^{G_m}(\beta) = p^{-1}\,\frac{d}{dz}\log(\beta(\varphi(z)))\,\Big|_{z=\varphi^{-1}(u_o)} = \delta_o^{\mathcal{F}}(\beta)\;\varphi'(\varphi^{-1}(u_o)) ,$$

for all $\beta\in\Phi_o^{\times}$. Here $\mathcal{F}$ is the formal group law with $[p](X) = pX + X^p$ as an endomorphism. So $\varphi((1+z)^p - 1) = p.\,\varphi(z) + \varphi(z)^p$. On differentiating and evaluating at $z = \zeta_o - 1$ we find that $\varphi'(\zeta_o - 1) = \zeta_o^{p-1}/1-p$. By (1) of section 2, we have

$$\begin{aligned}(\alpha,\beta)_o^{G_m} &= \varphi^{-1}((\varphi(\alpha),\beta)_o^{\mathcal{F}})\\ &= \varphi^{-1}([T_o(\lambda_{\mathcal{F}}\circ\varphi(\alpha).\,\delta_o^{\mathcal{F}}(\beta)\,](u_o))\\ &= [T_o(\lambda_{G_m}(\alpha).\,\frac{1}{\zeta_o.\,\beta}\,.\,\frac{d\beta}{d\pi_o})](\zeta_o - 1)\end{aligned}$$

for all $\alpha\in G_m(\mathfrak{p}_o^2)$ and $\beta\in\Phi_o^{\times}$ (here $\pi_o = 1-\zeta_o$). Of course $\lambda_{G_m}(z) = \log(1+z)$, but we observe that the logarithm here plays an essentially different role from that in (2).

Final remark. - Following Iwasawa's ideas in [6], the description of ψ_o in terms of the map δ_o can be generalized so as to obtain a description of ψ_n $(n>0)$ in terms of an analogue δ_n of δ_o. This then yields all the analogues one would expect of the Artin-Hasse laws. For example, if u_n is a generator of $\mathcal{F}_{\pi^{n+1}}$, it follows from this work that

$$(\alpha, u_n)_n = [\frac{1}{\pi^{n+1}} \cdot T_n(\frac{\lambda(\alpha)}{\lambda'(u_n)} \cdot \frac{1}{u_n})](u_n)$$

for all $\alpha \in \mathcal{O}(\mathfrak{p}_n)$. For full details, see [8].

-:-:-:-

REFERENCES

[1] ARTIN E., TATE J., Class field theory, Benjamin; New-York, 1967.

[2] CASSELS J., FRÖHLICH A., Algebraic Number Theory, Academic Press, 1967.

[3] COATES J., WILES A., On the conjecture of Birch and Swinnerton-Dyer, submitted to Invent. Math.

[4] FRÖHLICH A., Formal Groups, Lecture Notes in Mathematics 74, Springer,

[5] IWASAWA K., On some modules in the theory of cyclotomic fields, Jour. Math. Soc. Japan, 16 (1964), 42-82.

[6] IWASAWA K., On explicit formulas for the norm residue symbol, Jour. Math. Soc. Japan, 20 (1968), 151-164.

[7] LUBIN J., TATE J., Formal complex multiplication in local fields, Ann. of Math., 81 (1965), 380-387.

[8] WILES A., Higher explicit reciprocity laws, to appear.

-:-:-:-

J.COATES and A.WILES
Department of Pure Mathematics
and Mathematical Statistics
University of Cambridge
16 Mill Lane
CAMBRIDGE, England.