Tôhoku Math. Journ.
29 (1977), 385-416.

THE GALOIS GROUP OF LOCAL FIELDS

SIN-ICHI WATANABE

(Received February 13, 1976)

Introduction. Let Q_p be the p-adic number field, k a finite extension of Q_p, and G the Galois group of $\bar{k}/k$. In 1968, Jakovlev [1] described the structure of the Galois group G in the case of $p \neq 2$. In his paper, he determined the number of generators of G and gave a description of the relations among the generators. But, as he recognized himself there, those relations were considerably complicated and it is difficult to look through the structure of the Galois group only by those relations. In order to determine the structure of the Galois group up to isomorphism, as we shall show later, we need not the exact description of the relations, for we can characterize the relations among the generators by more general and loose conditions.

Let K be the maximal tamely ramified extension of Q_p and let

$$A = \mathrm{Gal.}(K/Q_p)\ , \quad B = \mathrm{Gal.}(\bar{Q}_p/K)\ .$$

Then the exact sequence

$$1 \longrightarrow B \longrightarrow G \longrightarrow A \longrightarrow 1$$

splits, and G is an holomorph extension of B by A. By fixing one splitting morphism $A \longrightarrow G$, we can consider A as a subgroup of G and B as a pro-p-group with the operator domain A. In § 6, we define "the projective envelope" P of the A-pro-p-group B, and consider the relation among the generators of B as an element of P. In § 7, we define the notion of ω-regularity for the elements of P, and prove that Ker.$(P \longrightarrow B)$ is generated by an ω-regular element of P. Furthermore, we prove that for any two ω-regular elements π, π' congruent to each other modulo certain normal subgroup of P, there is an automorphism σ of PA such that $\pi^\sigma = \pi'$, where PA is the holomorph extension of P by A.

By this fact, the problem of determination of the structure of the Galois group is entirely reduced to the problem of determination of certain non-degenerate skew symmetric quadratic form corresponding to the Galois group. Though we do not show here, we can easily classify such quadratic forms, and determine the one of them which corresponds to the Galois group.

In this paper we restricted the base field to Q_p, but this is not essential and we can easily extend our results to the case of arbitrary base fields.

Finally I wish to thank Professor Ogawa for his advices and encouragements.

1. Maximal tamely ramified extension of Q_p. Let K be the maximal tamely ramified extension of Q_p, and let T be the maximal unramified extension of Q_p.

PROPOSITION 1.1. *The Galois group, $A = \mathrm{Gal.}(K/Q_p)$ is generated "as a topological group" by the two elements x, y with the unique relation,*

$$x^{-1}yx = y^p ,$$

where x is an arbitrary element of A, such that x induces the Frobenius mapping of T/Q_p, and y is an arbitrary generator of $\mathrm{Gal.}(K/T)$.

PROPOSITION 1.2. *$B = \mathrm{Gal.}(\bar{Q}_p/K)$ is a pro-p-group and the following exact sequence splits.*

$$1 \longrightarrow B \longrightarrow \mathrm{Gal.}(\bar{Q}_p/Q_p) \longrightarrow A \longrightarrow 1 .$$

In other words, $G = \mathrm{Gal.}(\bar{Q}_p/Q_p)$ is the holomorph extension of B by A. From now on, we fix a splitting morphism, $A = \mathrm{Gal.}(K/Q_p) \longrightarrow G =$ $\mathrm{Gal.}(\bar{Q}_p/Q_p)$, and by this splitting morphism we regard A as a subgroup of G.

COROLLARY 1.3. *Let $\langle x\rangle, \langle y\rangle$ be "the closures" of two subgroups of A, generated by x or y respectively.*
Then

$$\langle x\rangle \cong \varprojlim_{r} Z/p^r Z$$

$$\langle y\rangle \cong \varprojlim_{r} Z/(p^r - 1)Z$$

and A is the holomorph extension of $\langle y\rangle$ by $\langle x\rangle$.

2. Group ring of A. Let Z_p be the maximal order of Q_p.

DEFINITION 2.1. We define the "group ring", $\Lambda = Z_p\langle x, y\rangle$ of $A = \langle x, y \,|\, x^{-1}yx = y^p\rangle$, by the following formula,

$$\Lambda = \varprojlim_{r,\,U} Z/p^r Z[A/U]$$

where U runs over all normal open subgroups of A.

Let D be the set of all monic irreducible divisors with coefficients in Z_p of polynomials of type $X^{p^r-1} - 1$; $r \geqq 1$.

PROPOSITION 2.1. *Let* $F = Z_p\langle y\rangle$ *be "the closure" of the subring of* Λ, *generated by* $y \in A$.
Then

$$F = \prod_{g\in D} F_g\ ;\quad F_g \cong Z_p[Y]/g(Y)Z_p[Y]\ .$$

$\prod$ *means the direct product of topological abelian groups.*

PROOF. By Corollary 1.3, we get

$$Z_p\langle y\rangle \cong \varprojlim_r Z_p[Y]/(Y^{p^r-1}-1)Z_p[Y]\ .$$

Our assertion follows directly from this. q.e.d.

Since $x^{-1}yx = y^p$, the inner automorphism σ of Λ induced by $x \in A$ induces the Frobenius mapping on every F_g.

The unit element e_g of F_g is contained in the center of Λ, and so Λe_g is two sided ideal of Λ, and

$$\Lambda = \prod \Lambda e_g\ .$$

Put $d_g = \deg g$, then the center Γ_g of Λe_g is generated by $x^{d_g}e_g$ over $Z_pe_g \cong Z_p$.

Therefore, Γ_g is isomorphic to the group ring,

$$Z_p\langle\!\langle x^{d_g}\rangle\!\rangle \cong \varprojlim_r Z_p[X]/(X^r-1)\cdot Z_p(X)\ .$$

DEFINITION. Let $\hat{Z}$ be the completion of the ring of rational integers Z, i.e.,

$$\hat{Z} = \varprojlim_r Z/rZ \cong \prod Z_p\ .$$

In the above product, we denote by e_p the unit element of Z_p, which is regarded as an idempotent of $\hat{Z}$. For any profinite group H and for any element $h \in H$, we denote by h^{e_p} "the p-part" of h. If $a_1, a_2, \cdots$ is a sequence of integers that converges to e_p in $\hat{Z}$, then h^{e_p} is the limit of the sequence $h^{a_1}, h^{a_2}, \cdots$ in H.

We put

$$x_0 = x^{(1-e_p)d_g}\ ,\quad \text{and}\quad x_1 = x^{e_pd_g}\quad d_g = \deg g\ ,$$

then we have

$$\langle x^{d_g}\rangle = \langle x_0\rangle \times \langle x_1\rangle\quad \text{(direct product)}\ ,$$
$$\Gamma_g \cong Z_p\langle\!\langle x^{d_g}\rangle\!\rangle \cong \overline{Z_p\langle\!\langle x_0\rangle\!\rangle \otimes Z_p\langle\!\langle x_1\rangle\!\rangle}\ ,$$

and

$$Z_p\langle\!\langle x_0\rangle\!\rangle \cong \varprojlim_r Z_p[X]/(X^{p^r-1}-1)Z_p[X]$$
$$\cong \prod_{f\in D} Z_p[X]/f(X)Z_p[X]\ .$$

Since $\langle x_1 \rangle$ is a free-pro-p-group, its group ring

$$Z_p\langle\langle x_1\rangle\rangle \cong \varprojlim_r Z_p[X]/(X^{p^r}-1)Z_p[X]$$

is isomorphic to the power series ring in one variable $x_1 - 1$ over the ring Z_p.

Thus

$$\Gamma_g = \prod_{f \in D} \Gamma_{f,g}\ ; \quad g \in D$$

where $\Gamma_{f,g}$ is isomorphic to the one variable formal power series ring in one variable over the ring isomorphic to $Z_p(X)/f(X)Z_p[X]$.

Let $e_{f,g}$ be the unit element of $\Gamma_{f,g}$, then

$$\Lambda = \prod_{f,g} \Lambda_{e_{f,g}}$$

where (f, g) runs over all elements of $D \times D$. Each $\Lambda_{e_{f,g}}$ is a $\Gamma_{f,g}$-algebra which is free as a $\Gamma_{f,g}$-module, and

$$[\Lambda_{e_{f,g}} : \Gamma_{f,g}] = d^{2g}\ ; \quad d_g = \deg g\ .$$

We shall write simply $\Lambda_{f,g}$ instead of $\Lambda e_{f,g}$, then we have the following assertions.

PROPOSITION 2.2.

1) $\Lambda = \prod_{(f,g)} \Lambda_{f,g}$,

$$\Lambda_{f,g} \cong \Lambda/\mathfrak{A}_{f,g}\ ; \quad \mathfrak{A}_{f,g} = (f(x^{(1-e_p)d_g}),\ g(y))\cdot\Lambda$$

and $d_g = \deg g$.

2) $\Gamma_{f,g}$ *is isomorphic to the total matrix algebra* $(\Gamma_{f,g})d_g$ *over its center* $\Gamma_{f,g}$.

3) $\Gamma_{f,g}$ *is isomorphic to the formal power series ring in one variable over the ring isomorphic to* $Z_p[X]/f(X)\cdot Z_p[X]$.

PROOF. 1) and 3) have been already proved.

2) can be proved by means of the theory of crossed product. q.e.d.

PROPOSITION 2.3. *Let M be a $\Lambda_{f,g}$-module and put*

$$U = \{\sigma \in \Lambda = \langle x, y\rangle \mid \forall \mu \in M,\ \sigma\mu = \mu\}\ ,$$
$$\mathfrak{A} = \sum_{\sigma \in U} (\sigma - 1)\Lambda_{f,g}$$
$$\bar{A} = A/U, \quad and \quad \bar{\Lambda} = \Lambda_{f,g}/\mathfrak{A}\ .$$

We denote by x the image of x in A, then it holds that $M \cong \bar{\Lambda}$ under the following conditions 1), 2), 3):

1) *M is Z_p-free and finitely generated over Z_p.*

2) *There is a submodule* M' *of* M *such that*

$$M' \cong \bar{\Lambda}\,, \quad |M/M'|^{\#} < \infty\,.$$

3) *The subgroup* $J = \langle x^{de_p} \rangle$ *of* $\bar{\Lambda}$ *is finite and*

$$H_J^1(M) = 0$$

where $d = \deg g$.

PROOF. In the first case of $x^{de_p} = 1$, the center of $\bar{\Lambda}$ is isomorphic to $Z_p[X]/f(X)Z_p[X]$ and $\bar{\Lambda}$ is isomorphic to the total matrix algebra of rank d^2 over its center. By assumptions, M is isomorphic to a left ideal of $\bar{\Lambda}$, which satisfies

$$|\bar{\Lambda}/I|^{\#} < \infty\,.$$

But $\bar{\Lambda}$ has only one ideal class (Iwasawa [1]) and so

$$M \cong \bar{\Lambda}\,.$$

In general case, let p^r be the order of $\bar{x}$. We put

$$N = 1 + \bar{x} + \bar{x}^2 + \cdots + \bar{x}^{p^r-1}\sigma$$

and

$$\bar{\bar{\Lambda}} = \bar{\Lambda}/(1-\bar{x})\bar{\Lambda} \cong N\bar{\Lambda}\,.$$

Applicating the first case to $\bar{\bar{\Lambda}}$ and NM, we obtain $NM \cong \bar{\bar{\Lambda}}$. Therefore NM is generated by one element as a $\bar{\Lambda}$-module. On the other hand, by the assumption pertaining to H^1, we have

$$NM \cong M/(1-\bar{x})M\,.$$

Since $1-\bar{x}$ is contained in the radical of $\bar{\Lambda}$, M itself is generated by one element as a $\bar{\Lambda}$-module. By assumptions,

$$[M: Z_p] = [\bar{\Lambda}: Z_p]$$

therefore we see that

$$M \cong \bar{\Lambda} \qquad \text{q.e.d.}$$

3. Unit groups of tamely ramified extension. Let k/Q_p be a tamely ramified normal extension of Q_p of finite degree, and let U be the principal unit group that is the group consisting of all units of k congruent to 1 modulo the prime ideal of k. U can be regarded as a Λ-module, and it splits corresponding to the splitting of Λ such as

$$U = \prod_{f,g} U_{f,g}\,,$$

where almost all $U_{f,g}$ are 1.

If we put

$$A_k = \mathrm{Gal.}(K/k) \subset A$$
$$\bar{\Lambda}_{f,g} = \Lambda_{f,g} / \sum_{\sigma \in A_k} (\sigma - 1)\Lambda_{f,g} ,$$

then

$$\prod_{f,g} \bar{\Lambda}_{f,g} = \Lambda / \sum_{\sigma \in A_k} (\sigma - 1)\Lambda = Z_p[A/A_k]$$

and each $U_{f,g}$ is regarded as a $\bar{\Lambda}_{f,g}$-module.

PROPOSITION 3.1. *If $U_{f,g}$ does not contain any primitive p-th root of unity, then*

$$U_{f,g} \cong \bar{\Lambda}_{f,g} .$$

PROOF. By Proposition 2.5. q.e.d.

PROPOSITION 3.2. *Let $\theta \in K$ be a p-th primitive root of unity, then*

$$Q_p(\theta) = Q_p((-p)^{1/p-1}) .$$

If we put $\pi = (-p)^{1/p-1}$, then π is a prime element of $Q_p(\theta)$, and the principal unit group U of $Q_p(\theta)$ splits as a Λ-module, such as

$$U = U_{X-1,Y-1} \times U_{X-1,Y-\omega} \times \cdots \times U_{X-1}Y - \omega^{P-2}$$

where ω is a primitive $(p-1)$-th root of unity. And

$$U_{X-1,Y-\omega} = \theta^Z \times \exp(Z_p\pi^p)$$
$$U_{X-1,Y-\omega^i} = \exp(Z_p\pi^i) \qquad 2 \leqq i \leqq p-1 .$$

PROOF. In the case of $p = 2$, Proposition 3.2 is trivial. And so we assume that $p = 2$.

Since $X^{p-1} + \cdots + X + 1 = \prod_{i=1}^{p-1} (X - \theta^i)$, we have

$$N(1-\theta) = \prod_{i=1}^{p-1} (1 - \theta^i) = 1 + \cdots + 1 = p ; \quad N = NQ_p(\theta)/Q_p .$$

On the other hand, the chracteristic polynomial of π is $X^{p-1} + p = 0$, and so

$$N\pi = (-1)^{p-1}p = p ; \quad NQ_p(\pi)/Q_p .$$

Therefore, by class field theory, we conclude that

$$Q_p(\theta) = Q_p(\pi) .$$

We may assume that

$$\pi^y = \omega^i\pi ; \quad (i, p-1) = 1 .$$

If we put $\pi_0 = \theta - 1$, then π_0 is also a prime element of $Q_p(\theta)$, therefore

$$\pi = s\pi_0 \bmod (\pi^2) \quad \text{for some} \quad 1 \leqq s \leqq p-1 .$$

On the other hand, it is clear that

$$1 + \pi_0^y = \theta^y = \theta^\omega = (1+\pi_0)^\omega \equiv 1 + \omega\pi_0 \mod (\pi^2) ,$$

therefore $\omega^i \pi = \pi^y = s\pi_0^y = s\omega\pi_0 \equiv \omega\pi \mod (\pi^2)$. From this we have that $i = 1$ and $\pi^y = \pi$. Put $O = Z_p[\theta] = Z_p[\pi]$, then we find

$$\begin{aligned} U &= \theta^z \times \exp(O\pi^2) \\ &= \theta^Z \times \exp\left(\sum_{i=2}^{p} Z_p \pi^i\right) \\ &= \theta^Z \times \exp(Z_p\pi^2) \times \cdots \times \exp(Z_p \pi^p) , \quad O^Z \in U_{X-1,Y-\omega} , \end{aligned}$$

and

$$\exp(Z_p\pi^i) \in U_{X-1,Y-\omega} ; \quad 2 \leqq i \leqq p .$$

Since $\omega^p = \omega$ it holds that

$$\begin{aligned} U_{X-1,Y-\omega} &= \theta^Z \times \exp(Z_p \pi^p) , \\ U_{X-1,Y-\omega^i} &= \exp(Z_p\pi^i) ; \quad 2 \leqq i \leqq p-1 . \end{aligned}$$

Thus our assertion holds. q.e.d.

PROPOSITION 3.3. *Let k be the unramified extension of $Q_p(\theta)$ of degree p^r; $r \geqq 1$, and U the principal unit group of k. Then $U_{X-1,Y-\omega}$ is generated as a Λ-module by two elements α, β, which satisfy the following conditions,*

$$N_\alpha = \theta \quad N_\beta = \exp(\pi^p) ; \quad N = N^k/Q_p(\theta) , \quad \alpha^p = \beta^{x-1} ,$$

where

$$\pi = (-p)^{1/p-1} \in Q_p(\theta)$$

and

$$\theta \equiv 1 + \pi \mod (\pi^2) .$$

PROOF. Let $\langle \bar{x} \rangle$ be Gal.$(k/Q_p(\theta))$, then

$$H^0_{\langle \bar{x} \rangle}(U_{X-1,Y-\omega}) = 1 .$$

Hence, there exists such an element α_1 of $U_{X-1,Y-\omega}$ that $N_1 = 0$. Since $N\alpha_1^p = 1$ and $H'_{\langle \bar{x} \rangle}(U_{X-1,Y-\omega}) = 1$, we can find such $\beta_1 \in U_{X-1,Y-\omega}$ as $\alpha_1^p = \beta_1^{x-1}$. Now we put

$$\alpha_1 = 1 + a\pi \quad \text{and} \quad \beta_1 = 1 + b_1\pi \mod (\pi^2)$$

with integers a, b_1 of k, then

$$\alpha_1^p \equiv 1 + pa\pi + a^p\pi^p = 1 + (a^p - a)\pi^p$$
$$\beta_1^{X-1} \equiv 1 + (b_1^p - b_1)\pi \mod (\pi^{p+1}) .$$

Therefore, it holds that

$$b_1^p - b_1 \equiv 0 \mod (\pi^2) ,$$

and we may assume $b_1 \in \boldsymbol{Z}$ without loss of generality. We put $\beta_2 = \beta_1\theta^{-b_1}$, then

$$\beta_2 \in U_{X-1,Y-\omega} ,$$
$$\alpha_1^p = \beta_1^{x-1} = (\beta_2\theta^b)^{x-1} = \beta_2^{x-1} ,$$

and

$$\beta_2 = 1 \mod (\pi^2) .$$

Let k_0 be the unramified extension of Q_p of degree p^r and let 0 be the maximal order of k_0, then, similarly as Proposition 3.2, we get

$$\{u \in U_{X-1,Y-\omega} \mid u \equiv 1 \quad (\pi^2)\} = \exp(\theta\pi^p) .$$

Since

$$\alpha_1^p = 1 + (a^p - a)\pi^p \mod (\pi^{p+1})$$

we see

$$\beta_2 \equiv 1 + b\pi^p \mod (\pi^{p+1}) ,$$
$$\beta_2^{x-1} = 1 + (b^p - b)\pi^p \mod (\pi^{p+1}) ,$$

and so

$$(a - b)^p \equiv a - b \mod (\pi) .$$

On the other hand,

$$1 + \pi \equiv \theta = N\alpha_1 = 1 + \operatorname{tr} \alpha_1 \cdot \pi \mod (\pi^2) .$$

By this and the before, we get

$$\operatorname{tr} b \equiv \operatorname{tr} a \equiv 1 \mod (\pi) ,$$
$$N\beta_2 \equiv 1 + \operatorname{tr} b \cdot \pi^p \equiv 1 + \pi^p$$
$$\equiv \exp(\pi^p) \mod (\pi^{p+1}) .$$

From this and Proposition 3.2, it holds that

$$N\beta_2 = \exp(\mu^{-1}\pi^p) ; \quad \mu^{-1} \in \boldsymbol{Z}_p ,$$
$$\mu^{-1} \equiv 1 \mod (p) .$$

Now we put $\alpha = \alpha_1^\mu$ and $\beta = \beta_2^\mu$, then we have

$$N\alpha = \theta^{\mu} = \theta\ , \quad N\beta = \exp(\pi^{p})$$

and

$$\alpha^{p} = \beta^{x-1}\ .$$

Since α and β generate $U_{X-1,Y-\omega}$, this proves our assertion. q.e.d.

PROPOSITION 3.4. *Let k, U be the same that of Proposition 3.3, and let $\mathfrak{M}_1$ be the maximal ideal of*

$$\Lambda_1 = \Lambda_{X-1,Y-\omega}\ .$$

Then

$$U_{X-1,Y-\omega} \cong \mathfrak{M}_1/(x^{p^r}-1)\mathfrak{M}_1\ .$$

PROOF. Since

$$\mathfrak{M}_1 = (p, x-1)\Lambda_1\ ,$$

$\mathfrak{M}_1$ is generated as a Λ_1-module by two element $(x-1)e_1$, pe_1 with the unique relation:

$$p\cdot(x-1)e_1 = (x-1)\cdot pe_1\ ,$$

where e_1 is the unit (idempotent) of Λ_1. Therefore, we can define a Λ_1-epimorphism

$$\varphi\colon \mathfrak{M}_1 \longrightarrow U_{X-1,Y-\omega}$$

by

$$(x-1)e_1 \xrightarrow{\varphi} \alpha$$
$$pe_1 \xrightarrow{\varphi} \beta\ ,$$

using α, β in Proposition 3.3. Since Λ_1 is an integral domain, we get

$$(x^{p^r}-1)\Lambda_1/(x^{p^r}-1)\mathfrak{M}_1 \cong \Lambda_1/\mathfrak{M}_1 \cong Z/pZ\ .$$

On the other hand, we see that

$$[\mathfrak{M}_1/(x^{p^r}-1)\Lambda_1 \colon Z_p] = [\Lambda_1/(x^{p^r}-1)\Lambda_1 \colon Z_p] = [U_{X-1,Y-\omega}/\Omega \colon Z_p]$$

where Ω is the p-torsion part of $U_{X-1,Y-\omega}$ and $\Omega \cong Z/pZ$. This shows

$$\ker\varphi = (x^{p^r}-1)\mathfrak{M}_1$$

and we get

$$U_{X-1,Y-\omega} \cong \mathfrak{M}_1/(x^{p^r}-1)\mathfrak{M}_1\ . \qquad \text{q.e.d.}$$

PROPOSITION 3.5. *Let k/Q_p be a normal extension of finite degree, contained in k/Q_p and let U_k be the princial unit group of k. If we put*

$$A_k = \{\sigma \in A = \langle x, y\rangle \mid \forall \mu \in k, \mu^\sigma = \mu\} ,$$
$$\mathfrak{A}_k = \sum_{\sigma \in A_k} (\sigma - 1)\Lambda ,$$

and

$$\mathfrak{M} = (p, x - 1, y - \omega)\Lambda ,$$

then there is a Λ-left isomorphism:

$$U_k \cong \mathfrak{M}/\mathfrak{M}\mathfrak{A}_k .$$

PROOF. It is clear that the isomorphism holds except the Λ_1-parts of the both hand sides. On the Λ_1-parts, by Proposition 3.4, isomorphism holds if k is the unramified extension of $Q_p(\theta)$ of degree p^r. Therefore, by Proposition 3.1, we may assume that k contains the primitive roots of unity. Let $p^r n$ be the relative degree of k/Q_p with $(p, n) = 1$, and let $\hat{k}$ be the unramified extension of Q_p of degree p^r which is contained in k. Then the Λ_1-component of $U_{\hat{k}}$ agrees with that of U_k and the Λ_1-component of $\mathfrak{M}/\mathfrak{M}\mathfrak{A}_k$ also agrees with that of $\mathfrak{M}/\mathfrak{M}\mathfrak{A}_{\hat{k}}$, and this concludes the proof. q.e.d.

Easily we obtain the following three propositions.

PROPOSITION 3.6.

$$\varprojlim_{k} U_k \cong \mathfrak{M}$$

where the left hand side is the inverse limit with respect to the norm mappings and k moves over all tamely ramified normal extensions of Q_p of finite degree.

PROPOSITION 3.7. *Let B be* Gal.$(\bar{Q}_p/K)$ *then as the A-modules,*

$$B/[B, B] \cong \mathfrak{M} = (x - \Lambda, y - \omega)\Lambda .$$

PROPOSITION 3.8. *B is generated as a pro-p-group with the operator domain A by two elements $\tilde{Z}$, $\tilde{W}$, which admit only two relations modulo $[B, B]$:*

$$\begin{cases} \bar{Z}^{(x-1)e_1} = W^p \\ W^{e_1} = W \end{cases}$$

where e_1 is the unit (idempotent) of Λ_1.

PROPOSITION 3.9. *In Proposition 3.8, we can take such $\tilde{w}$ that admits the relations;*

$$x^e p^{-1} \tilde{w} x^{1-e} p = \tilde{w} ,$$

and $y^{-1}\tilde{w}y = \tilde{w}^\omega$.

PROOF. For $\tilde{w}$ in Proposition 3.8, it holds

$$\begin{cases} x^e p^{-1} \tilde{w} x^{1-e} p \equiv \tilde{w} , \\ y^{-1} \tilde{w} y \equiv \tilde{w}^{\omega} \mod [B, B] . \end{cases}$$

Let W be a minimal closed subgroup of B that satisfies the following conditions.

1) W is closed to the operations of x^{1-e_p} and y.

2) $\langle [B, B], \bar{W} \rangle$ contains $\tilde{w}$. Then $W' = W/[W, W]$ is indecomposable as a $\Lambda' = \boldsymbol{Z}_p\langle\langle x^{1-e}p, y\rangle\rangle$-module, and is isomorphic to $\Lambda'/(x^{1-e}p-1, y-\omega)\Lambda' \cong \boldsymbol{Z}_p$. Let $\tilde{w}_1$ be the element of W such that

$$\tilde{w}_1 \equiv \tilde{w} \mod [B, B] ,$$

then this $\tilde{w}_1$ satisfies our assertions. q.e.d.

4. Cohomology with coefficient $\boldsymbol{Z}/p\boldsymbol{Z}$. Let S be a profinite group. Following facts is well known.

PROPOSITION 4.1. *For the S-trivial module $\boldsymbol{Z}/p\boldsymbol{Z}$,*

$$H_S^1(\boldsymbol{Z}/p\boldsymbol{Z}) \cong (S/[S, S]S^p)^* .$$

The symbol $*$ in the right hand side denotes the Pontrjagin dual of the compact group.

PROPOSITION 4.2. *Let φ; $F \to S$ be a homomorphism mapping the pro-p-group F to S, such that F is free and the homomorphism*

$$F/[F, F]F^p \to S/[S, S]S^p$$

induced by φ is an isomorphism. Then,

$$H_S^2(\boldsymbol{Z}/p\boldsymbol{Z}) \cong (F_1/[F, F_1]F_1^p)^* ,$$

where $F_1 = \ker (F \to S)$. Furthermore, for any pro-p-group S, such a free group F and a homomorphism φ; $F \to S$ always exist. Let S_1 and S_2 be two (additive) pro-abelian groups. We define the tensor product $S_1 \otimes S_2$ by

$$S_1 \otimes S_2 = \varprojlim_{U_1, U_2} S_1/U_1 \otimes S_2/U_2 ,$$

where $U_1(U_2)$ runs over all open subgroups of S_1(resp. S_2). Let σ be the automorphism of $S \otimes S$ difined by

$$\sigma(a \otimes b) = b \otimes a , \quad a, b \in S .$$

We define $S \wedge S$ and $S \bigcirc\!\!\!\!\wedge\; S$ as

$$S \wedge S = \operatorname{coker}(S \otimes S \xrightarrow{1+\sigma} S \otimes S)\,,$$
$$S \textcircled{\scriptsize$\wedge$} S = \ker(S \otimes S \xrightarrow{1+\sigma} S \otimes S)\,.$$

PROPOSITION 4.3. *Let S be a pro-abelian group (additive) such that $pS=0$, and let S^* the Pontrajagin dual of S. Then $S \textcircled{\scriptsize$\wedge$} S$ is identified naturally with the Pontrjagin dual of $S^* \textcircled{\scriptsize$\wedge$} S^*$.*

PROOF.

$$\begin{aligned}\alpha \in S \textcircled{\scriptsize$\wedge$} S &\Leftrightarrow (1+\sigma)\alpha = 0 \\ &\Leftrightarrow ((1+\sigma)\alpha\,,\quad S^* \otimes S^*) = 0 \\ &\Leftrightarrow (\alpha\,,\quad (1+\sigma)(S^* \otimes S^*)) = 0\,.\end{aligned}$$

q.e.d.

PROPOSITION 4.4. *Let F be a free pro-p-group. We put*

$$F_2 = [F, F]F^p\,,\quad F_3 = [F, F_2]F_2^p$$
$$\bar{F} = F/F_2, \quad \textit{and} \quad \bar{F}_2 = F_2/F_3\,.$$

Then, we have

1) *if $p \neq 2$,*

$$\bar{F}_2 \cong (\bar{F} \textcircled{\scriptsize$\wedge$} \bar{F}) \oplus \bar{F} \cong (\bar{F} \wedge \bar{F}) \oplus \bar{F}\,.$$

2) *if $p = 2$,*

$$\bar{F}_2 \cong \bar{F} \textcircled{\scriptsize$\wedge$} \bar{F}\,.$$

PROOF. We define the mappings $\tilde{D}$; $F \times F \to \bar{F}_2$ and $\tilde{\varphi}_p$; $F \to \bar{F}_2$ by

$$\tilde{D}(a, b) = \overline{[a, b]} \in \bar{F}_2\,,$$
$$\tilde{\varphi}_p(a) = \bar{a}^p \in \bar{F}_2\,,$$

respectively. Then $\tilde{D}$ and $\tilde{\varphi}_p$ induce the mappings

$$D;\ \bar{F} \times \bar{F} \to \bar{F}_2\,,$$
$$\varphi_p;\ \bar{F} \to \bar{F}_2\,.$$

It is easily known that D is bilinear and that φ_p is linear for $p \neq 2$. Let $p \neq 2$. The homomorphism

$$\bar{F} \wedge \bar{F} \oplus \bar{F} \xrightarrow{D+\varphi_p} \bar{F}_2$$

is clearly an epimorphism. In order to show that $D + \varphi_p$ is a monomorphism, it is sufficient to construct in practice a pro-p-group S such that

$$\bar{S} = S/S_2 \cong F\,;\quad S_2 = [S, S]S^p\,,$$
$$\bar{S}_2 = S_2/S_3 \cong (\bar{F} \wedge \bar{F}) \oplus \bar{F}\,;\quad S_3 = [S, S_2]S_2^p\,.$$

Regarding $E = F/[F, F]F^p$ as a module, we put $V = E \wedge E/p\cdot E \wedge E$.

If we define the multiplication on the set $S = E \times V$ such as

$$(a, \alpha)(b, \beta) = \left(a + b, \alpha + \beta + \frac{1}{2} a \wedge b\right) \text{ for } a, b \in E, \alpha, \beta \in V$$

then S becomes a group and it satisfies our requirements. Let $p = 2$. We put

$$V = \bar{F} \otimes \bar{F}$$

and define the multiplication on the set $S = \bar{F} \times V$ such as

$$(a, \alpha)(b, \beta) = (a + b, \alpha + \beta + a \otimes b)\ , \quad \text{for} \quad a, b \in \bar{F}\ , \quad \alpha, \beta \in V\ .$$

As in the case of $p \neq 2$, S becomes a group. We identify $V = \bar{F} \otimes \bar{F}$ with the subgroup of S consisting of all elements of type $(0, \alpha)$. Then we get the following diagram with the row exact.

$$\begin{tikzcd} & F \arrow[d] & \\ S \arrow[r] & S/V \arrow[r] & 0\ ; \quad S/V \cong \bar{F}\ . \end{tikzcd}$$

Since F is free, the diagram can be extended to a commutative diagram;

$$\begin{tikzcd} & F \arrow[dl, dashed, "f"'] \arrow[d] & \\ S \arrow[r] & S/V \arrow[r] & 0\ . \end{tikzcd}$$

Since

$$(a, \alpha)^2 = (0, a \otimes a)\ ,$$
$$(a, \alpha)(b, \beta)(a, \alpha)^{-1}(b, \beta)^{-1} = (0, a \otimes b - b \otimes a)$$

the subgroup $f(F) \cap V$ agrees with the submodule $F \textcircled{\scriptsize$\wedge$} F$ of V. But clearly $f^{-1}(V) = F_2$ and $\ker f = F_3$, therefore this concludes the proof. q.e.d.

Let S be a pro-p-group. By Proposition 4.1, there exists a free pro-p-group F and a homomorphism $\varphi; F \to S$, such that φ induces an isomorphism;

$$F/[F, F]F^p \cong S/[S, S]S^p\ .$$

By Proposition 4.1 and Proposition 4.2, the following homomorphisms exist.

$$H_s^1(\boldsymbol{Z}/p\boldsymbol{Z}) \cong S^*(\cong F^*)\ .$$
$$H_s^2(\boldsymbol{Z}/p\boldsymbol{Z}) \cong \bar{N}^*\ .$$

Where $\bar{S} = S/[S, S]S^p$, $\bar{N} = N/[F, N]N^p$, and $N = \ker \varphi$.

Using the injection $N \hookrightarrow F_2$, we define the homomorphism h from

$H_s^2(Z/pZ)^*$ to $H_s^1(Z/pZ)^* \otimes H_s^1(Z/pZ)$ such as

$$\begin{aligned} H_s^2(\boldsymbol{Z}/p\boldsymbol{Z})^* &\cong \bar{N} \xrightarrow{i} \bar{F}_2 \\ &\cong (\bar{F}_1 \otimes \bar{F}_1) \oplus \bar{F}_1 \xrightarrow{\text{Proj.}} \bar{F}_1 \otimes \bar{F}_1 \\ &\cong H_s^1(\boldsymbol{Z}/p\boldsymbol{Z})^* \otimes H_s^1(\boldsymbol{Z}/p\boldsymbol{Z})^* \quad (p \neq 2)\ ; \end{aligned}$$

$$\begin{aligned} H_s^2(\boldsymbol{Z}/p\boldsymbol{Z})^* &\cong \bar{N} \xrightarrow{i} \bar{F}_2 \\ &\cong \bar{F}_1 \otimes \bar{F}_1 \cong H_s^1(\boldsymbol{Z}/p\boldsymbol{Z})^* \otimes H_s(\boldsymbol{Z}/p\boldsymbol{Z})^* \quad (p = 2)\ . \end{aligned}$$

PROPOSITION 4.5. *The cup product*

$$\cup : H_s^1(\boldsymbol{Z}/p\boldsymbol{Z}) \wedge H_s^1(\boldsymbol{Z}/p\boldsymbol{Z}) \to H_s^2(\boldsymbol{Z}/p\boldsymbol{Z})$$

is the dual of h.

DEFINITION 4.1. Let F be a free pro-p-group, and π an element of $[F, F]F^p$. We put $S = F/\langle\langle \pi \rangle\rangle$ where $\langle\langle \pi \rangle\rangle$ is the normal (closed) subgroup of F generated by π. We call π a regular element of F if the cup product

$$H_s^1(\boldsymbol{Z}/p\boldsymbol{Z}) \wedge H_s^1(\boldsymbol{Z}/p\boldsymbol{Z}) \xrightarrow{U} H_s^2(\boldsymbol{Z}/p\boldsymbol{Z})$$

is a non-degenerate bilinear form. Where "non-degenerate" means that for each non-zero-element α of $H_s^1(\boldsymbol{Z}/p\boldsymbol{Z})$ there exists at least one element β of $H_s^1(\boldsymbol{Z}/p\boldsymbol{Z})$ such that $\alpha \cup \beta \neq 0$.

5. ω-regular elements of tensor products. Put

$$\begin{aligned} A &= \langle x, y \rangle = \mathrm{Gal.}(K/Q_p)\ , \\ \Lambda &= \boldsymbol{Z}_p\langle\langle x, y \rangle\rangle = \prod_{f,g} \Lambda_{f,g},\ \Lambda_1 = \Lambda_{X-1,Y-\omega} \end{aligned}$$

be the same as in § 2.

PROPOSITION 5.1. *There is an involutive anti-automorphism* $*$ *of* Λ *determined by*

$$x^* = x^{-1}\ , \quad y^* = \omega y^{-1}\ .$$

DEFINITION 5.1. We call $\Lambda_{f,g}^*$ the ω-dual of $\Lambda_{f,g}$.

PROPOSITION 5.2. *Let* $M(N)$ *be a* $\Lambda_{f,g}$(resp. Λ_{f_1,g_1})*-non-zero module. The following two conditions are equivalent.*

1) *The* Λ_1 *component of* $M \otimes N$ *is non-zero.*

2) $\Lambda_{f,g}^* = \Lambda_{f_1,g_1}$.

We denote the number of $\Lambda_{f,g}$*-indecomposable components of a* $\Lambda_{f,g}$*-module* M *by* $[M; \Lambda_{f,g}]$.

Let A *be* Gal.(K, Q_p), *and let* M(or M^*) *be a* $\Lambda_{f,g}$(resp. $\Lambda_{f,g}^*$)*-projective* *module of finite type. The tensor product* $M \times M^*$ *is regarded as an* A *(and consequently* Λ*)-module by usual way. Thus* $M \times M^*$ *is regarded as a* $\Lambda \otimes (\mathrm{End}_\Lambda(M)) \otimes (\mathrm{End}_\Lambda(M^*))$*-module. We call* M^* *the* ω*-dual of* M *if* $[M; \Lambda_{f,g}] = [M^*; \Lambda^*_{f,g}]$.

PROPOSITION 5.3. *Let* M *be a* $\Lambda_{f,g}$*-projective module of finite type, and* M^* *its* ω*-dual. Then, we have,* $\Lambda_1 \otimes \mathrm{End}_\Lambda(M)$*-modules,*

$$e_1(M \otimes M^*) \cong \Lambda_1 \otimes \mathrm{End}_\Lambda(M) .$$

PROOF. Let $\mathfrak{N}$ be the maximal two sided ideal of $\Lambda_{f,g}$ and U an open normal subgroup of A such that

$$\forall \sigma \in U , \quad (\sigma - 1)e_{f,g} \in \mathfrak{N} .$$

We put

$$\bar{A} = A/U \quad \bar{\Lambda} = \boldsymbol{Z}p[\bar{A}] \cong \Lambda/\sum_{\sigma \in U}(\sigma - 1)\Lambda ,$$
$$\bar{\Lambda}_{f,g} = \bar{\Lambda}\cdot\Lambda_{f,g} , \quad \bar{\Lambda}^*_{f,g} = \bar{\Lambda}\cdot\Lambda^*_{f,g}$$
$$\bar{M} = \bar{\Lambda}\cdot M , \quad \text{and} \quad \bar{M}^* = \bar{\Lambda}\cdot M^* .$$

We define the right operation of Λ for $\bar{M}$ by

$$\bar{\mu}\cdot a = a^*\bar{\mu} \quad \text{for} \quad \bar{\mu} \in \bar{M} , \quad a \in \Lambda .$$

By this definition $\bar{M}$ becomes a $\Lambda^*_{f,g}$ right module, and the tensor product $\bar{M} \otimes_\Lambda \bar{M}^*$ over Λ is defined. We can easily see that as the $\mathrm{End}_\Lambda(\bar{M})$-modules,

$$e_1(\bar{M} \otimes \bar{M}^*)/(x - 1)e_1(\bar{M} \otimes \bar{M}^*) \cong \bar{M} \otimes_\Lambda \bar{M}^* .$$

Let $\bar{F}$ be the center of $\bar{\Lambda}_{f,g}$. Then $\mathrm{End}_\Lambda(\bar{M})$ is isomorphic with the total matrix algebra over $\bar{F}$ of degree $n = [\bar{M}; \bar{\Lambda}_{f,g}]$ and $\bar{M} \otimes_\Lambda \bar{M}^*$ is projective over $\mathrm{End}_\Lambda(\bar{M})$ and

$$[\bar{M} \otimes_\Lambda \bar{M}^*; \mathrm{End}_\Lambda(\bar{M})] = [\bar{M}^*; \bar{\Lambda}^*_{f,g}] = n .$$

Hence as $\mathrm{End}_\Lambda(\bar{M})$-modules it hold that

$$e_1(\bar{M} \otimes \bar{M}^*)/(x - 1)e_1(\bar{M} \otimes \bar{M}^*) \cong \mathrm{End}_\Lambda(\bar{M}) .$$

But clearly $\bar{M} \otimes \bar{M}^*$ is projective over $\bar{\Lambda}$ and consequently $\bar{\Lambda}_1(\bar{M} \otimes \bar{M}^*)$ is free over $\bar{\Lambda}_1$. This shows that

$$e_1(\bar{M} \otimes \bar{M}^*) \cong \bar{\Lambda}_1 \otimes \mathrm{End}_\Lambda(\bar{M}) .$$

Taking the inverse limits of the both hand sides, we get

$$e_1(M \otimes M^*) \cong \Lambda_1 \times \mathrm{End}_\Lambda(M) . \qquad \text{q.e.d.}$$

PROPOSITION 5.4. *Let* f, g, M, M^* *be the same as in Proposition* 5.3, *and let π be an element of $e_1(M \times M^*)$. Then the followings are equivalent to each other.*

1) *$e_1(M \otimes M^*)$ is generated by π over $\Lambda_1 \otimes \mathrm{End}_\Lambda(M)$.*

2) *$e_1(M \otimes M^*)$ is generated by π over $\Lambda_1 \otimes \mathrm{End}_\Lambda(M^*)$.*

3) *$e_1(\bar{M} \otimes \bar{M}^*)/(x-1)e_1(\bar{M} \otimes \bar{M}^*)$ is generated by $\bar{\pi}$ over $\mathrm{End}_\Lambda(\bar{M})$, where $\bar{M} = M/\mathfrak{M}M$, $M^* = \bar{M}/\mathfrak{M}M$ and $\mathfrak{M}$ is the radical of Λ,* i.e.,

$$\mathfrak{M} = p\Lambda + \prod_{(f,g)} (x^{e_p \cdot \deg \cdot g} - 1)\Lambda_{f,g} .$$

4) *For any Λ-module N and for any element α of $e_1(N \otimes M^*)$, there exists at least one Λ-morphism $f;\ M \to N$ such that*

$$(f \otimes 1)\cdot \pi \equiv \alpha \mod (x-1)e_1(N \otimes M^*) .$$

Where $f \otimes 1;\ M \otimes M^* \to N \otimes M^*$ is the Λ-morphism induced by f.

PROOF. By Proposition 5.3. q.e.d.

DEFINITION 5.2. Let f, g, M, M^* be the same as in Proposition 5.3, and $\pi \in e_1(M \times M^*)$. We call π an ω-regular element of $M \times M^*$ if π satisfies the equivalent conditions of Proposition 5.4. By the condition 3 of Proposition 5.4, the ω-regularity of π is determined only by the residue class of π in

$$e_1(\bar{M} \otimes \bar{M}^*)/(x-1)\cdot e_1(\bar{M} \otimes \bar{M}^*) .$$

6. "Projective envelope" of Gal.(Q_p/K). The notions of free, projective, essential etc. can be defined in the Category of pro-p-groups with operator domain. Namely, we have,

PROPOSITION 6.1. *Let $\tilde{A}$ a pro-finite group, and M a set. Then there exists a pro-p-group $\tilde{B}$ with the continuous operator domain $\tilde{A}$ and a map $M \to \tilde{B}$ which satisfy the following universal mapping property.*

For any $\tilde{A}$-pro-p-group $\tilde{B}_1$ and for any map $M \to \tilde{B}_1$, there exists a unique $\tilde{A}$-morphism $\tilde{B} \to \tilde{B}_1$ such that it makes the following diagram commutative.

$$\begin{tikzcd} & M \arrow[dl] \arrow[dr] & \\ \tilde{B} \arrow[rr] & & \tilde{B}_1 \end{tikzcd}$$

DEFINITION 6.1. Let $\tilde{A}$ a pro-finite group, an $\tilde{B}$ and $\tilde{A}$-pro-p-group. We call $\tilde{B}$ an $\tilde{A}$-projective group if $\tilde{B}$ satisfy the following condition:

for any $\tilde{A}$-epimorphism $\tilde{B}_1 \to \tilde{B}$, there exists a $\tilde{A}$-morphism a A-morphism $\tilde{B} \to \tilde{B}_1$ such that

$$[\tilde{B} \to \tilde{B}_1 \to \tilde{B}] = 1_{\tilde{B}} .$$

DEFINITION 6.2. Let $B_1 \xrightarrow{\varphi} B_2$ be a $\tilde{A}$-epimorphism of $\tilde{A}$-pro-p-group. We call φ a $\tilde{A}$-essential morphism if for any proper $\tilde{A}$-subgroup B'_1 of B_1, $\varphi(B'_1) \neq B_2$.

PROPOSITION 6. 2. *For any $\tilde{A}$-pro-p-group $\tilde{B}$ there exists a $\tilde{A}$-projective group $\tilde{p}$ and a $\tilde{A}$-epimorphism φ; $\tilde{p} \to \tilde{B}$ such that φ is $\tilde{A}$-essential.* (φ, p) *is uniquely determined by $\tilde{B}$ up to $\tilde{A}$-isomorphisms.*

PROOF. By Proposition 6.1, $\tilde{B}$ can be written as a residue group F/N of an $\tilde{A}$-free group F. Let N_1 be a minimal $\tilde{A}$-normal subgroup of F containing in N such that $F/N_1 \to \tilde{B}$ is essential. The existence of such N_1 can be easily proved. Next, let $\tilde{p}$ be a minimal $\tilde{A}$-subgroup of F such that $\tilde{p} \to \tilde{B}$ is onto. Such $\tilde{p}$ also exists. Then $\tilde{p} \to \tilde{B}$ is essential and $F = N_1 p$. Since F is $\tilde{A}$-free. There is a commutative diagram:

$$\begin{tikzcd} & F \arrow[dl, dashed, "\varphi"', "G"] \arrow[d] \\ \tilde{p} \arrow[r] & F/N_1 \end{tikzcd} .$$

Then, by the commutatively of the above diagram we see,

$$\ker.\ \varphi \subset \varphi^{-1}(N_1 \wedge \tilde{P}) = N_1 .$$

But for

$$F/\ker.\ \varphi \cong p \to F/N_1 \to B$$

is essential, by the minimality of N_1, therefore, we get $\ker \varphi = N_1 = \varphi^{-1}(N_1 \wedge p)$, and so

$$N_1 \wedge \tilde{p} = 1 .$$

Since F is free, this shows that p is $\tilde{A}$-projective. q.e.d.

PROPOSITION 6.3. *For any $\tilde{A}$-pro-p-group $\tilde{B}$, there exists the maximal $\tilde{A}$-normal subgroup $\tilde{B}_2$ of $\tilde{B}$ such that $\tilde{B} \to \tilde{B}/\tilde{B}_2$ is essential and this $\tilde{B}_2$ is the common part of all maximal $\tilde{A}$-normal subgroups of B.*

PROOF. Since

$$\tilde{B} \to \tilde{B}/[\tilde{B}, \tilde{B}]$$

is essential, we get Proposition 6.3 by adapting the theory of limit Artineans to the A-module $\tilde{B}/[\tilde{B}, \tilde{B}]$. q.e.d.

In the following, we put

$$A = \langle x, y \rangle = \mathrm{Gal.}(K/Q_p) ,$$
$$B = \langle\!\langle \tilde{\boldsymbol{Z}}, \tilde{w} \rangle\!\rangle = \mathrm{Gal.}(\bar{Q}_p/K) ,$$

and we shall construct the A-projective envelope of the A-pro-p-group B. Let $\mathfrak{M}$ be the "radical" of Λ, this is,

$$\mathfrak{M} = p\Lambda + \prod_{(f,g)} (x^{e_p \cdot \deg \cdot g} - 1)\Lambda_{f,g}$$

and let $B_2 = [B, B]B^{\mathfrak{M}}$ be the inverse image of $(B/[B, B])^{\mathfrak{M}}$ with respect to the A-morphism $B \longrightarrow B/[B, B]$. Then B/B_2 is essential and $B/B_2 \cong \Lambda/\mathfrak{M} \oplus \Lambda_1/\mathfrak{M}\Lambda_1$. Therefore our task is to construct the A-projective envelope of $\Lambda/\mathfrak{M} \oplus \Lambda_1/\mathfrak{M}\Lambda_1$.

Let F be a free pro-finite group generated by four elements x, y, Z_1, w_1 and let N be its normal subgroup generated by Z_1 and w_1. We denote by N_1 the normal subgroup of F generated by three elements

$$\begin{aligned} &x^{-1}yxy^{-p} \,, \\ &x^{e_p - 1}w_1 x^{1-e_p} w_1^{-1} \,; \quad \text{where} \quad e_p \in Z_p \,, \\ &y^{-1}w_1 y w_1^{-\omega} \,, \end{aligned}$$

and the all elements of type ν^{1-e_p}; $\nu \in N$, and we put

$$P = N/N_1 \wedge N \,.$$

We denote by Z, w the images of Z_1, w_1 in P respectively, and we define the A-epimorphism $P \longrightarrow B$ by $Z \longrightarrow \tilde{Z}$

$$w \longrightarrow \tilde{w} \,.$$

PROPOSITION 6.4. *$P \longrightarrow B$ is the A-projective envelope of B.*

PROOF. $P/[P, P] \cong \Lambda \oplus \Lambda_1$. q.e.d.

We denote by PA the holomorph extension of P by A.

PROPOSITION 6.5. *Let φ; $\Gamma \longrightarrow PA$ be an epimorphism from a pro-finite group Γ to PA such that* ker *φ is a pro-p-group. Then φ splits.*

PROOF. Let $N = \varphi^{-1}(p)$, then N is a pro-p-group by the assumption. The fact that the epimorphism

$$\Gamma \longrightarrow PA \longrightarrow A$$

splits is well known, and so the Γ is isomorphic with holomorph extension NA of N by A. Consequently N is regarded as an A-pro-p-group and so the A-epimorphism $N \longrightarrow P$ is splits, this concludes proof. q.e.d.

PROPOSITION 6.6. *Let $\Gamma_1 A$ and $\Gamma_2 A$ be the holomorph intensions of A-pro-p-group Γ_1, Γ_2 respectively. In the following diagram the row exact be exact.*

$$\begin{array}{ccccc} & & pA & & \\ & & \downarrow{\scriptstyle \varphi_2} & & \\ \Gamma_1 A & \xrightarrow{\varphi_1} & \Gamma_2 A & \longrightarrow & 1 . \end{array}$$

We assume that

$$\varphi_1(r_1 a) \equiv \varphi_2(ua) \equiv a \mod \Gamma_2 ,$$
$$\textit{for all} \quad r_1 \in \Gamma_1 , \quad u \in P , \quad a \in A .$$

Then there exists a morphism φ; $PA \to \Gamma_1 A$ *which makes the diagram commutative*:

$$\begin{tikzcd} & PA \arrow[dl, "\varphi"'] \arrow[d] \\ \Gamma_1 A \arrow[r] & \Gamma_2 A . \end{tikzcd}$$

PROOF. Let the diagram

$$\begin{tikzcd} C \arrow[r] \arrow[d] & PA \arrow[d, "\varphi_2"] \\ \Gamma_1 A \arrow[r, "\varphi_1"] & \Gamma_2 A \end{tikzcd}$$

be the pull back of φ_1, φ_2. Since $C \to PA$ satisfies the condition in Proposition 6.5, it splits.

Let $PA \to C$ be its splitting morphism, then φ; $PA \to C \to \Gamma_1 A$ satisfies our requirement. q.e.d.

Let N be a A-normal subgroup of P containing $p_2 = [P, P]P^{\mathfrak{m}}$, and put $N_2 = [P, N]N$. Further let φ; $P/P_2 \to N/N_2$ be a A-morphism and $\bar{\nu}(\nu \in N)$ be a A-invariant element of N/N_2. We define an automorphism $\bar{\psi}$ of PA/N_2 by

$$\begin{aligned} &\bar{\psi}(\bar{x}) = \bar{x}\bar{\nu} , \\ &\bar{\psi}(\bar{y}) = \bar{y} , \\ &\bar{\psi}(\alpha) = \bar{\alpha}\cdot\varphi(\bar{\bar{\alpha}}) \qquad \text{for} \quad \alpha \in P \end{aligned}$$

where $\bar{\bar{\alpha}}$ is residue class of $\alpha \in P$ in P/P_2. We easily see that ψ is well-defined.

PROPOSITION 6.7. *There exists an automorphism* ψ *of* PA *such that it fixes* N_2 *and induces* $\bar{\psi}$ *over* PA/N_2.

PROOF. Apply Proposition 6.6 to the diagram

$$\begin{array}{ccc} & & pA \\ & & \downarrow{\scriptstyle\bar{\psi}} \\ PA & \longrightarrow & PA/N_2 \end{array}$$ q.e.d.

PROPOSITION 6.8. *The p-cohomological dimension of PA is* 1; $Cd_p(PA)=1$ *and consequently the p-Sylow subgroup* $\langle x^{e_p}, P\rangle$ *of PA is a free pro-p-group.*

PROOF. G; free-pro-p-group $\Leftrightarrow Cd_p(G)=1$ (Tate [5]). q.e.d.

PROPOSITION 6.9. *Let* $G = BA = \mathrm{Gal.}(\bar{Q}_p/Q_p)$, *and let* Ω *be the group of all p-th roots of unity, then*

$$H_G^2(\Omega) \overset{\text{Res.}}{\cong} H_{G_p}^2(\Omega) \cong \boldsymbol{Z}/p\boldsymbol{Z}\ .$$

Where $G_p = \langle B, x^{e_p}\rangle$ *is the p-Sylow subgroup of G.*

PROOF. Since the sequence

$$1 \longrightarrow \Omega \hookrightarrow \bar{Q}_p^x \xrightarrow{p} \bar{Q}_p \longrightarrow 1$$

is exact, and

$$H_G^1(\bar{Q}_p^x) = 1\ , \quad H_G^2(\bar{Q}_p^x) \cong Q/\boldsymbol{Z}\ ,$$

we get

$$H_G^2(\Omega) \cong \ker\,(Q/\boldsymbol{Z} \xrightarrow{p} Q/\boldsymbol{Z}) \cong \boldsymbol{Z}/p\boldsymbol{Z}\ .$$

Similarly from the fact,

$$H_{G_p}^1(\bar{Q}_p) = 1$$

$$\begin{array}{ccc} H_G^2(\bar{Q}_p) & \xrightarrow{\text{Res.}} & H_{G_p}^2(\bar{Q}_p^x) \\ \wr\| & \hookrightarrow & \wr\| \\ \boldsymbol{Z}/Q\boldsymbol{Z} & \xrightarrow{\text{Proj.}} & \boldsymbol{Z}\left[\frac{1}{p}\right]\Big/\boldsymbol{Z} \end{array}$$

we get

$$H_G^2(\Omega) \overset{\text{Res.}}{\cong} H_{G_p}^2(\Omega) \cong \boldsymbol{Z}/p\boldsymbol{Z}\ .$$ q.e.d.

PROPOSITION 6.10. $N = \ker.\,(P \longrightarrow B)$ *is generated as a normal subgroup of* $\tilde{G}_p = \langle P, x^{e_p}\rangle$ *by an element* π, *that satisfies*

$$\pi = w^{-p} Z^{(x-1)e_1} \mod [P, P]\ .$$

(The notation $Z^{(x-1)e_1}$ *is explained below.) And as the A-groups*

$$N/[\tilde{G}_p, N]N^p \cong \Omega \cong \Lambda_1/\mathfrak{M}_1;\ \mathfrak{M}_1 = (p, x-1)\Lambda_1$$

and consequently we may assume that

$$x^{e_p - 1}\pi x^{1-e_p} = \pi \ ,$$
$$y^{-1}\pi y = \pi^{\omega} \ .$$

PROOF. The first half is the consequence of Proposition 6.9 and the latter half can be proved as in Proposition 3.9. q.e.d.

Here we shall give an account of the notation $Z^{(x-1)e_1}$ in Proposition 6.10.

In general for any $\alpha \in P$ we denote by α^{Λ} the Λ-subgroup of P generated by α. For any $\lambda \in \Lambda$ we denote by α^{λ} the any one of the inverse images of $\alpha^{-\lambda} \in \alpha^{\Lambda}/[\alpha^{\Lambda}, \alpha^{\Lambda}]$. Especially if e is an idempotent containing in the center of Λ, we can choose α^e such that the Λ-epimorphism $\alpha^{e\Lambda} \to (\alpha^{\Lambda}/[\alpha^{\Lambda}, \alpha^{\Lambda}])^e$ is essential where $\alpha^{e\Lambda}$ is the Λ-subgroup of α^{Λ} generated by α^e, so in the followings we shall always choose α^e as above. Similarly for any Λ-normal subgroup N of P the meaning of $[p, N]N^{\mathfrak{M}}$ etc. may be clear. Where $\mathfrak{M}$ is the "radical" of Λ, that is,

$$\mathfrak{M} = (p, \varepsilon)\Lambda \ ,$$
$$\varepsilon = \lim \sum_{(f,g)} (x^{e_p \cdot \deg \cdot g} - 1)e_{f,g} \ .$$

DEFINITION 6.3. Especially we put and fix

$$Z_0 = Z^{e_0}\ , \quad Z_1 = Z^{e_1}\ ,$$
$$Z_2 = Z^{1-e_0-e_1}\ (p \neq 2)\ ,$$

and

$$Z_0 = Z^{e_0},\ Z_2 = Z^{1-e_0}\ (p = 2)\ ,$$

where e_0, p_1 are the unit elements (which are idempotents of Λ) of $\Lambda_0 = \Lambda_{X-1,Y-1}$, $\Lambda_1 = \Lambda_{X-1,Y-\omega}$ respectively. In the case of $p = 2$, we note that $e_0 = e_1$.

PROPOSITION 6.11. *Let G_p be the p-Sylow subgroup of* Gal. $(\bar{Q}_p/Q_p)$. *The cup product*

$$H'_{G_p}(\boldsymbol{Z}/p\boldsymbol{Z}) \wedge H'_{G_p}(\boldsymbol{Z}/p\boldsymbol{Z}) \to H^2_{G_p}(\boldsymbol{Z}/p\boldsymbol{Z}) \cong \boldsymbol{Z}/p\boldsymbol{Z}$$

is a non-degenerate skew symmetric form.

PROOF. Let L/Q_p be the algebraic extension corresponding to G_p, and Ω be the group of p-th roots of unity. By taking the Kummer-character of G_p induced by the elements of L^x, we get

$$H'_{G_p}(\Omega) \cong L^x/L^{xp} .$$

On the other hand,

$$\begin{aligned} H^2_{G_p}(\Omega \otimes \Omega) &\overset{U^{-1}}{\cong} H^0_{G_p}(\Omega) \otimes H^2_{G_p}(\Omega) \\ &\cong \Omega \otimes \boldsymbol{Z}/p\boldsymbol{Z} \cong \Omega . \end{aligned}$$

Hence we have the following commutative diagram.

$$\begin{tikzcd} H'_{G_p}(\Omega) \wedge H^1_{G_p}(\Omega) \arrow[r, "U"] \arrow[d, phantom, "\wr\|"] & H^2_{G_p}(\Omega \otimes \Omega) \arrow[d, phantom, "\wr\|"] \\ (L^x/L^{xp}) \wedge (L^x/L^{xp}) \arrow[r] & \Omega \end{tikzcd}$$

We can easily prove that the second row of the diagram agrees with the Hilbert norm residue symbol of L^x, and consequently it is non-degenerate. Since Ω is trivial as G_p-module, this concludes the proof. q.e.d.

PROPOSITION 6.12. *Let π be the same as in Proposition* 6.10. *Then π is a regular element of the free pro-p-group $G_p = \langle p, x^{e_p} \rangle$ in the sense of Definition* 4.1.

7. Successive approximation.

DEFINITION 7.1.

$$\begin{aligned} p_1 &= P , \quad p_{r+1} = [P, p_r]p_r^{\mathfrak{M}} \\ \bar{p}_r &= p_r/p_{r+1} ; \quad r \geqq 1 , \\ \mathfrak{M} &= (p, \varepsilon) , \\ \varepsilon &= \lim \sum_{(f,g)} (x^{e_p \cdot \deg \cdot g} - 1)e_{f,g} . \end{aligned}$$

PROPOSITION 7.1. *The commutator mapping*

$$(a, b) \longrightarrow [a, b] = aba^{-1}b^{-1}$$

and the mappings

$$\begin{aligned} &a \longrightarrow a^{\varepsilon} , \quad \mathrm{mod}\, [a^{A}, a^{A}] \\ &a \longrightarrow a^{p} \end{aligned}$$

induce the bilinear form

$$D_{r,s};\ \bar{p}_r \otimes \bar{p}_s \longrightarrow \bar{p}_{r+s} \qquad \textit{for} \quad r, s \geqq 1 ,$$

and the linear mapping

$$\varphi_\varepsilon;\ \bar{p}_r \longrightarrow \bar{p}_{r+1} \qquad \textit{for} \quad r \geqq 1$$

and the mapping

$$\varphi_p;\ \bar{p}_r \longrightarrow \bar{p}_{r+1} \qquad \textit{for} \quad r \geqq 1 .$$

Further these mappings commutes with the operation of A, *and* φ_p *is linear except for the case of* $p = 2$, $r = 1$.

PROOF. These are easily obtained by direct computations. q.e.d.

PROPOSITION 7.2. *Except for the case of* $p = 2$, $r = 1$, *the* Λ-*homomorphism*

$$\bar{p}_1 \otimes \bar{p}_r \oplus \bar{p}_r \oplus \bar{p}_r \xrightarrow{D_{1,r}+\varphi_\varepsilon+\varphi_p} \bar{p}_{r+1}$$

is onto, and especially

$$\bar{p}_1 \wedge \bar{p}_1/\mathfrak{M}(\bar{p}_1 \wedge \bar{p}_1) \oplus \bar{p}_1 \oplus \bar{p}_1 \xrightarrow[\cong]{D_{1,1}+\varphi_\varepsilon+\varphi_p} \bar{p}_2$$

for $p \neq 2$.

PROOF. This can be proved in the same manner as in Proposition 4.4. q.e.d.

NOTE. In the followings we regard each p_r as an additive group as in Proposition 7.2.

In § 4 we have defined $S_1 \otimes S_2$, $S \wedge S$ as follows

$$S_1 \otimes S_2 = \varprojlim_{U_1,U_2} S_1/U_1 \otimes S_2/U_2 ,$$
$$S \wedge S = S \otimes S/(1+\sigma)S \otimes S ,$$
$$\sigma(a \otimes b) = b \otimes a .$$

For $p \neq 2$, the definition of $S \wedge S$ agrees with usual one but not for $p = 2$. So we define $S \mathbin{\bar{\wedge}} S$ by

$$S \mathbin{\bar{\wedge}} S = \mathrm{Im}(S \otimes S \xrightarrow{1-\sigma} S \otimes S) .$$

PROPOSITION 7.3. *Let* $\varphi_2(\bar{p}^{e_0})$ *be the subgroup of* $\bar{p}_2$ *generated by* $\{\varphi_2(\alpha) \mid \alpha \in \bar{p}_1\}$. *Then*

$$\overline{(p_1^{1-e_0} \mathbin{\bar{\wedge}} p_1^{1-e_0})^{e_0}} \oplus {}_2(\bar{p}_1^{e_0}) + p_1^{e_0} \xrightarrow[\cong]{D_{1,1}+i+\varphi_\varepsilon} \bar{p}_2^{e_0} ,$$

where i *is the injection and*

$$\overline{p_1^{1-e_0} \mathbin{\bar{\wedge}} p_1^{1-e_0}} = p_1^{1-e_0} \mathbin{\bar{\wedge}} p_1^{1-e_0}/\mathfrak{M}(p_1^{1-e_0} \mathbin{\bar{\wedge}} p_1^{1-e_0}) .$$

DEFINITION 7.2. Let M, M_1 be Λ-projective modules of finite type. We call M_1 the ω-dual of M if for any indecomposable component $\Lambda_{f,g}$ of Λ,

$$[e_{f,g}M;\ \Lambda_{f,g}] = [e^*_{f,g}M_1;\ \Lambda^*_{f,g}] .$$

We denote by M^* the ω-dual of M. Clearly M^* is uniquely determined by M up to Λ-isomorphism. Let $\tilde{\pi} \in e_1(M \otimes M^*)$. We note that

$$e_1(M \otimes M^*) = \prod_{f,g} e_1(e_{f,g}M \otimes e^*_{f,g}M^*) .$$

Let

$$\tilde{\pi} = \lim \sum_{f,g} \tilde{\pi}_{f,g} ,$$

and let

$$\tilde{\pi}_{f,g} \in e_1(e_{f,g}M \otimes e^*_{f,g}M^*)$$

be the decomposition of $\tilde{\pi}$. We call $\tilde{\pi}$ an ω-regular element of $M \otimes M^*$ if each $\pi_{f,g}$ is ω-regular in the sense of Definition 5.2. Let

$$\overline{M \otimes M} = \bar{M} \otimes \bar{M}^*/\mathfrak{M}(\bar{M} \otimes \bar{M}^*) ,$$
$$\bar{M} = M/\mathfrak{M}M , \quad \text{and} \quad \bar{M}^* = M^*/\mathfrak{M}M^* .$$

By Proposition 5.4 the ω-regularity of $\tilde{\pi}$ depend only on the residue class $\bar{\pi}$ of $\tilde{\pi}$ in $\overline{M \otimes M}$, and so we call $\bar{\pi}$ an ω-regular element of $\overline{M \otimes M^*}$ if $e_1(\overline{M \otimes M^*})$ is generated by $\bar{\pi}$ over $\mathrm{End}_\Lambda(\bar{M})$.

Further if $M = M^*$ by the natural imbedding of $M \wedge M$ into $M \otimes M$, we can define the ω-regularity of the elements of $M \wedge M$, also those of

$$\overline{M \wedge M} = \bar{M} \wedge \bar{M}/\mathfrak{M}(\bar{M} \wedge \bar{M}) .$$

Finally we note that the Λ-module

$$\begin{aligned} p_1' &= (P/[P, P])^{1-e_0-e_1} \quad (p \neq 2) , \\ &= (p/[p, p])^{1-e_0} \qquad (p = 2) \end{aligned}$$

is ω-dual with itself and

$$\overline{p_1 \wedge p_1} \cong D_{1,1}(\bar{p}_1' \wedge \bar{p}_1') ,$$

and so we can say about the ω-regularity of the elements of $D_{1,1}(\bar{p}_1' \wedge \bar{p}_1')$.

PROPOSITION 7.4. *Let π be the same as in Proposition 6.10. If we take suitable generators of AP, π is written in the form*

$$\begin{aligned} \pi &= w^p[x, Z_1][w, Z_0]\pi_1 \quad (p \neq 2) \\ &= w^2[x, Z_0]\pi_1 \qquad (p = 2) \end{aligned}$$

and

$$\bar{\pi}_1 \in D_{1,1}(\bar{p}_1' \wedge \bar{p}_1') ,$$

where $\bar{p}_1'$ is the one in Definition 7.2. Further $\bar{\pi}_1$ is an ω-regular element of $D_{1,1}(\bar{p}_1' \wedge \bar{p}_1')$ in the sense of Definition 7.2.

PROOF. We prove only in the case of $p=2$. By Proposition 6.12, we conclude that π is of the form

$$\pi = w^2[x, Z_0][x, w]^i[w, Z_0]^j\pi_1 ,$$

and

$$\bar{\pi}_1 \in D_{1,1}(\bar{p}_1' \wedge\!\!\!\wedge \bar{p}_1') \cong \overline{p_1' \wedge\!\!\!\wedge p_1'}$$

is ω-regular, where $i, j = 0$ or 1.

We put

$$Z' = Zw^i , \quad x' = xw^j .$$

Then π becomes of the form

$$\pi = w^2[Z_0', x']\pi_1$$

and

$$\bar{\pi}_1 = \bar{\pi}_1' .$$

But x', y, Z', w satisfy the same relations as x, y, Z, w in AP and generate AP, *so this completes the proof.* q.e.d.

DEFINITION 7.3. Let π be an element of p_2. We call π a standard ω-regular element of p if it satifies the following conditions.

1) $x^{e_p-1}\pi x^{1-e_p} = \pi, \quad y^{-1}\pi y = \pi.$

2) If we put

$$\begin{aligned} \pi &= w^p[x, Z_1][w, Z_0]\pi_1 \quad (p \neq 2) \\ &= w^2[x, Z_0]\pi \qquad\qquad (p = 2) \end{aligned}$$

then the residue class $\bar{\pi}_1$ of π_1 in $\bar{p}_2$ is an ω-regular element of

$$D_{1,1}(\bar{p}_1' \wedge\!\!\!\wedge \bar{p}_1') \cong \overline{p_1' \wedge\!\!\!\wedge p_1'}$$

in the sense of Definition 7.2.

DEFINITION 7.4. We denote by W_r; $r \geqq 2$ the group of all automorphisms of AP those satisfy

$$\begin{aligned} &\sigma(x^{1-e_p}) = x^{1-e_p} , \\ &\sigma(y) = y , \\ &\sigma(a) \equiv a \mod p_r \qquad \text{for} \quad a \in AP . \end{aligned}$$

PROPOSITION 7.5. *Let* $\sigma \in W_r$; $r \geqq 2$. *Then, the mapping* $\tilde{\delta}_\sigma$; $p \longrightarrow p$ *defined by*

$$\tilde{\delta}(a) = \sigma(a) \cdot a^{-1}$$

induces the A-morphism

$$\delta_\sigma^{(s)};\ \bar{p}_s \longrightarrow \bar{p}_{s+r-1} \qquad for \quad s \geqq 1\ .$$

Further $\delta_\sigma^{(s)}$ $s \geqq 1$ *is determined only by the residue class* $\bar{\sigma}$ *of* σ *in* $\bar{W}_r = W_r/W_{r+1}$.

PROPOSITION 7.6. *Let*

$$\delta_\sigma^{(0)} = \overline{\sigma(x)\cdot x^{-1}} \in \bar{p}_r\ .$$

Then $\delta^{(0)} \in p_r^{e_1}$ *and it is determined only by the residue class* $\bar{\sigma}$ *of* σ *in* $\bar{W}_r = W_r/W_{r+1}$.

PROPOSITION 7.7. *Let* $\psi;\ \bar{W}_r \longrightarrow \mathrm{Hom} \wedge (\bar{p}_1, \bar{p}_r) \bigoplus \bar{p}_r^{e_1}$ *defined by*

$$\psi(\bar{\sigma}) = \delta_\sigma^{(1)} \bigoplus \delta_\delta^{(0)} \qquad for \quad \sigma \in W_r\ .$$

Then ψ *is an isomorphism.*

PROOF. Proposition 7.5 and Proposition 7.6 can be obtained by direct computations. Proposition 7.7 is the consequence of Proposition 6.6. q.e.d.

DEFINITION 7.4. For an arbitrary $\alpha \in \bar{p}_1$, we define a Λ-homomorphism $\varphi_\alpha;\ \bar{p}_r \longrightarrow \bar{p}_{r+1};\ r \geqq 1$ by

$$\varphi_\alpha(\beta) = D_{1,r}(\alpha \otimes \beta) \in \bar{p}_{r+1}\ .$$

PROPOSITION 7.8. *Let* $\sigma \in W_r$ *and* i *the natural imbedding of* $\bar{p}_1 \mathbin{\wedge\!\!\!\wedge} \bar{p}_1$ *into* $\bar{p}_1 \otimes \bar{p}_1$. *Then the following diagram is commutative.*

$$\begin{tikzcd}
\bar{p}_1 \mathbin{\wedge\!\!\!\wedge} \bar{p}_1 \arrow[r, "i"] \arrow[d, "D_{1,1}"] & \bar{p}_1 \otimes \bar{p}_1 \arrow[r, "1\otimes\delta_\sigma^{(1)}"] & \bar{p}_1 \otimes \bar{p}_r \arrow[d, "D_{1,r}"] \\
\bar{p}_2 \arrow[rr, "\delta_\sigma^{(2)}"] & & \bar{p}_{r+1}
\end{tikzcd}$$

PROOF. By direct computations.

PROPOSITION 7.9. *Let*

$$\begin{aligned}
\pi &= w^p[x, Z_1][w, Z_0]\pi_1 \quad (p \neq 2) \\
&= w^2[x, Z_0]\pi_1 \qquad\qquad (p = 2)
\end{aligned}$$

by standard ω*-regular element of* p, *then*

$$\begin{aligned}
\delta_\sigma^{(2)}(\bar{\pi}) &= (\varphi_p - \varphi_{\bar{Z}_0})\cdot\delta_\sigma^{(1)}\bar{w} - \varphi_{\bar{Z}_1}\cdot\delta_\sigma^{(0)} + \varphi_\varepsilon\cdot\delta_\sigma^{(1)}\bar{Z}_1 \\
&\quad + \varphi_{\bar{w}}\cdot\delta_\sigma^{(1)}\bar{Z}_0 + \delta_\sigma^{(2)}\bar{\pi}_1 \quad (p \neq 2)\ , \\
\delta_\sigma^{(2)}(\bar{\pi}) &= (\varphi_2 + \varphi_{\bar{w}})\cdot\delta_\delta^{(1)}\bar{w} + \varphi_\varepsilon\cdot\delta_\sigma^{(1)}\bar{Z}_0 \\
&\quad + \varphi_{\bar{Z}_0}\cdot\delta_\sigma^{(0)} + \delta_\sigma^{(2)}\bar{\pi}_1 \qquad (p = 2)\ .
\end{aligned}$$

DEFINITION 7.5. Let

$$\mathfrak{P} = \bigoplus \sum_{r \geqq 2} \bar{p}_2 \,.$$

Then $\varphi_p, \varphi_\varepsilon, \varphi_\alpha, (\alpha \in \bar{p}_1)$, are regarded as the operators on the graded module $\mathfrak{P}$. Let Γ be the operator ring generated by $\varphi_p, \varphi_\varepsilon$ and $\{\varphi_\alpha\}$, $\alpha \in \bar{p}_1$ over $\boldsymbol{Z}/p\boldsymbol{Z}$. Let M be the right ideal of Γ generated by

$$\begin{aligned} &\varphi_p - \varphi_{\bar{Z}_0}, \varphi_{\bar{w}}, \varphi_{\bar{Z}_1}, \varphi_\varepsilon, \{\varphi_\alpha\}_\alpha \in \bar{p}_1^{1-e_0-e_1} \ (p \neq 2) \,, \\ &\varphi_2 + \varphi_{\bar{w}}, \varphi_\varepsilon, \varphi_{\bar{Z}_0}, \{\varphi_\alpha\}_\alpha \in \bar{p}_1^{1-e_0} \ (p = 2) \,. \end{aligned}$$

PROPOSITION 7.10. *Let π be a standard ω-regular element of p. Then for any $a \in M\mathfrak{P} \wedge e_1\bar{p}_{r+1}$, there exists $\sigma \in W_r$ such that*

$$\delta_\sigma^{(2)}(\bar{\pi}) = a \,, \qquad \textit{for} \quad r \geqq 2 \,.$$

PROOF. By Propositions 7.7, 7.8, 7.9, and the regularity of π. q.e.d.

PROPOSITION 7.11.

$$\begin{aligned} &M\mathfrak{P} = \sum_{r \geqq 3} \bar{p}_r \qquad \textit{for} \quad p \neq 2 \,, \\ &e_0 M\mathfrak{P} + \boldsymbol{Z}/2\boldsymbol{Z}[\varphi_2] \cdot (\varphi_2\varphi_\varepsilon\bar{w} + \varphi_2^2 \cdot \bar{Z}_0) = \sum_{r \geqq 3} e_0\bar{p}_r \qquad \textit{for} \quad p = 2 \,. \end{aligned}$$

PROOF.

CASE. $p \neq 2$. Let $\mathfrak{P}' = \sum_{r \geqq 1} \bar{p}_r$. Then the operation of Γ on $\mathfrak{P}$ can be extended to $\mathfrak{P}'$. Clearly

$$\Gamma = M \oplus \boldsymbol{Z}/p\boldsymbol{Z}[\varphi_p] \,.$$

Therefore it is sufficient to prove that $\varphi_p\bar{p}_1 \subset M\mathfrak{P}'$. If $a \in (1 - e_0 - e_1)\bar{p}_1 + \boldsymbol{Z}/p\boldsymbol{Z} \cdot (\bar{w}, \bar{Z}_1)$, we have

$$\begin{aligned} \varphi_p a &= (\varphi_p - \varphi_{Z_0})a + \varphi_{Z_0} a \\ &= (\varphi_p - \varphi_{Z_0}) - \varphi_a \bar{Z}_0 \in M\mathfrak{P}' \,. \end{aligned}$$

For $\bar{Z}_0 \in \bar{p}_1$

$$\varphi_p \bar{Z}_0 = (\varphi_p - \varphi_{\bar{Z}_0}) Z_0 \in M\mathfrak{P} \,.$$

CASE. $p = 2$. Since $\Gamma = M + \boldsymbol{Z}/2\boldsymbol{Z}[\varphi_2]$, it is sufficient to prove that

$$\varphi_2 \bar{p}_2^{e_0} \subset M\mathfrak{P} + \boldsymbol{Z}/2\boldsymbol{Z}(\varphi_2^2 Z_0, \varphi_2\varphi_\varepsilon\bar{w}) \,.$$

By Proposition 7.3, we get

$$\begin{aligned} e_0\bar{p}_2 = {} & e_0 D_{1,1}((1 - e_0)\bar{p}_1 \curlywedge (1 - e_0)\bar{p}_1) \\ & + \boldsymbol{Z}/z\boldsymbol{Z} \cdot (\varphi_2\bar{w}, \varphi_2\bar{Z}_0, \varphi_{\bar{w}}\bar{Z}_0, \varphi_\varepsilon\bar{w}, \varphi_\varepsilon\bar{Z}_0) \,. \end{aligned}$$

On the other hand for $a, b \in p_1$

$$\begin{aligned}[a, b^2] &= ab^2a^{-1}b^{-2} \\ &= [a, b]baba^{-1}b^{-2} \\ &= [a, b]b[a, b]b^{-1} \\ &= [[a, b], b]b[a, b]^2b^{-1} \\ &\equiv [[a, b], b][a, b]^2 \mod \bar{p}_4 .\end{aligned}$$

This shows that for $\alpha, \beta \in p_1$

$$\varphi_\alpha\varphi_2\beta = \varphi_\beta^2\alpha + \varphi_2\varphi_\alpha\beta .$$

Similarly, if we note that

$$\varphi_\varepsilon\bar{a} = \overline{[x, a]} \in \bar{p}_2 \qquad \text{for} \quad \bar{a} \in \bar{p}_1^{e_0} ,$$

we get

$$\varphi_\varepsilon\varphi_2\alpha = \varphi_2\varphi_\varepsilon\alpha + \varphi_\alpha\varphi_\varepsilon\alpha \qquad \text{for} \quad \alpha \in e_0\bar{p}_1 .$$

Using these formulae, we get

$$\varphi_2\varphi_\alpha\beta = \varphi_\alpha\varphi_2\beta + \varphi_\beta^2\alpha \in M\mathfrak{P} \qquad \text{for} \quad \alpha, \beta \in (1 - e_0)\bar{p}_1 ,$$

and

$$\begin{aligned}\varphi_2\varphi_{\bar{w}}\bar{Z}_0 &= \varphi_{\bar{w}}\varphi_2\bar{Z}_0 + \varphi_{\bar{Z}_0}^2\bar{w} \\ &= (\varphi_w + \varphi_2)\varphi_2\bar{Z}_0 + \bar{\varphi}_{Z_0}^2\bar{w} + \varphi_2^2\bar{Z} \in M\mathfrak{P} + \boldsymbol{Z}/z\boldsymbol{Z} \cdot \varphi_2^2\bar{Z}_0 , \\ \varphi_2^2\bar{w} &= (\varphi_2 + \varphi_{\bar{w}})\varphi_2\bar{w} \in M\mathfrak{P} , \\ \varphi_2\varphi_\varepsilon\bar{Z}_0 &= \varphi_\varepsilon\varphi_2\bar{Z}_0 + \varphi_{\bar{Z}_0}\varphi_\varepsilon\bar{Z}_0 \in M\mathfrak{P} .\end{aligned}$$

q.e.d.

THEOREM I. *Let π, π' be two standard ω-regular elements of P such that*

$$\pi \equiv \pi' \qquad \mod p_3 .$$

Then there exists an automorphism σ of AP that satisfies the following conditions.

1) $\sigma(x^{1-e_p}) = x^{1-e_p}$

$\sigma(y) = y$

$\sigma(a) = a \mod p_2$ *for* $\forall a \in AP$.

2) *If* $p \neq 2$

$$\pi^\sigma = \pi' .$$

If $p = 2$,

$$\pi^\sigma = \pi' \cdot [w, x]^{2\mu} \cdot Z_0^{4\nu} \quad \textit{for some} \quad \mu, \nu \in Z_2 .$$

PROOF. Since AP is generated by $x, y, z, w, \sigma \in W_2$ be determined by

$\sigma(x)$, $\sigma(z)$, $\sigma(w)$. And so we can define the topology on W_2 such that W_2 becomes compact and totally disconnected and it operates continuously on AP. Consequently the orbit $W_2\cdot\pi$ of π is closed in P. Therefore, it is sufficient to prove that in the case $p \neq 2$, if $\pi \equiv \pi' \bmod p_{r+1}$ $r \geqq 2$, there exists σ of W_r such that $\pi^\sigma = \pi' \bmod p_{r+2}$; and in the case $p = 2$, if $\pi \equiv \pi' \bmod p_{r+1}$ $r \geqq 2$, there exists σ of W_r such that

$$\pi^\sigma = \pi'[w, x]^{2^{r-1}\mu} Z_0^{2^r\cdot\nu} \bmod p_{r+2}\,, \quad \mu, \nu = 0 \quad \text{or} \quad 1\,.$$

But these are the immediate consequences of Propositions 7.10 and 7.11.
q.e.d.

Theorem I shows that for a standard ω-regular element π of P, the structure of the residue group $AP/\langle\!\langle\pi\rangle\!\rangle$ is determined essentially by the residue class $\bar{\pi}$ of π in $\bar{p}_2$ for $p \neq 2$. But in the case of $p = 2$, the same result as the above is not clear and so we shall discuss this case in the followings.

Let S be the normal subgroup of AP generated by x, y, z and w^2.

PROPOSITION 7.12. *Let π be the same as in Proposition 6.10. Then the normal subgroup $\langle\!\langle\pi\rangle\!\rangle = \ker(p \longrightarrow B)$ contains the generator π' such that if we take the suitable generator of AP π' is written in the form*

$$\pi' \equiv w^2[w, x]^2 \mod [S, S] \wedge P\,.$$

PROOF. Let $\tilde{S}$ be the normal subgroup of $AB = G = \mathrm{Gal.}(\bar{Q}_2/Q_2)$ generated by x, y, $\tilde{z}$ and $\tilde{w}^2$ and let 0 be the primitive root of unity of degree 4. Then $k = Q_2(\theta)$ is the field corresponding to S.

Let $k[W] = Q_2[\theta, W]$ be the Q_2-algebra generated by θ, W with relations

$$\theta W + W\theta = W^2 + 1 = 0\,.$$

Then $Q_2[\theta, W]$ is the quaternion field over Q_2, and has the invariant 1/2.

Let U be the subgroup of $k[W]^x$ generated by k^x and W, then U is isomorphic with a dense subgroup of $G/]\tilde{S}, \tilde{S}]$ by the extended norm residue mapping φ; $U \longrightarrow G/[\tilde{S}, \tilde{S}]$. By changing the generator of G if necessary, we may assume that

$$\varphi(1 + 0) = \bar{x}\,, \quad \varphi(W) = \tilde{w}$$

in $\bar{G} = G/[\tilde{S}, \tilde{S}]$.

Since

$$\begin{aligned} &W^2[W, 1 + \theta]^2 \\ &\quad = -W(1 + \theta)^2 W^{-1}(1 + \theta)^{-2} \end{aligned}$$

$$= -\left(\frac{1-\theta}{1+\theta}\right)^2 = 1 .$$

We get

$$\tilde{w}^2[\tilde{w}, x]^2 \cong 1 \mod [\tilde{S}, \tilde{S}] .$$

This conclude the proof. q.e.d.

PROPOSITION 7.13. *Let π be the same as in Proposition 6.10. Then there exists an automorphism σ of AP such that*

$$\pi^\sigma = w^2[w, x]^{2+4\mu} Z_0^{8\nu}[Z_0, x]\pi_1 ,$$
$$\pi_1 \in [Z_2^A, Z_2^A] ,$$

where $Z_2 = Z^{1-e_0}$ is defined in Definition 6.3.

PROOF. By Proposition 7.12, we get

$$\pi^\sigma = w^2[w, x]^{2+4\mu'} Z_0^{4\nu'}[Z_0, x]\pi_1', \ \pi_1' \in [Z_2^A, Z_2^A] .$$

We assume that $\nu' \equiv 1 \mod 2$.

Let τ be the automorphism defined by

$$\tau(x) = x[Z_0, w]Z_0 , \quad \tau(y) = y$$
$$\tau(w) = wZ_0^2 , \quad \tau(Z) = Z .$$

Then

$$\pi^{\sigma\tau} = w^2[w, x]^2[Z_0, x]\pi_1' \mod p_4 .$$

By Theorem I, there exists σ_1 of W_3 such that

$$\exists\sigma_1 \in W_3 \ \pi^{\sigma\tau\sigma_1} = w^2[w, x]^{2+4\mu} Z_0^{8\nu}[Z_0, x]\pi_1 , \quad \pi_1 \in [Z_2^A, Z_2^A] . \qquad \text{q.e.d.}$$

DEFINITION 7.6. In the followings we assume that any standard ω-regular element satisfies

$$\pi \equiv w^2[w, x]^2[Z_0, x]\pi_1 \mod \bar{p}_4 , \quad \pi_1 \in [Z_2^A, Z_2^A] .$$

PROPOSITION 7.14. *Let π be a standard ω-regular element of p, and $r \geqq 2$, then there exists σ of W_r such that*

$$\pi^\sigma \equiv \pi Z_0^{2^{r+1}} \mod p_{r+3} .$$

PROOF. It is sufficient to define σ such as

$$\sigma(w) = wZ_0^{2^r} ,$$
$$\sigma(x) = xZ_0^{2^{r-1}} ,$$

and

$$\sigma(z) = Z . \qquad \text{q.e.d.}$$

PROPOSITION 7.15. *Let π be a standard ω-regular element of P then there exists σ of W_2 such that*

$$\pi^\sigma = w^2[w, x]^{2+4\mu}[Z_0, x]\pi_1 , \quad \pi_1 \in [Z_2^A, Z_0^A] \qquad \textit{for some} \quad \mu \in Z_2' .$$

DEFINITION 7.7. Let N be the normal subgroup of AP generated by w^2, $[Z_0, x]$, $Z_2^A \wedge p_2$. Then, we define the groups N_r as follows.

$$\bar{N}_r = N_r/N_{r+1}, \; N_1 = N, \; N_{r+1} = [p, N_r]N_r^{\mathfrak{M}}, \; r \geqq 1 .$$

Then we can define the operations $\varphi_2, \varphi_\varepsilon, \{\varphi_\alpha\}_\alpha \in p_1$ on $\mathfrak{N} = \bigoplus \sum_{r\geqq 1} \bar{N}_r$. Let Γ be the ring generated by $\varphi_2, \varphi_\varepsilon, \{\varphi_\alpha\}_\alpha \in \bar{p}_1$ and M the right ideal of Γ generated by $\varphi_2 + \varphi_{\bar{w}}, \varphi_\varepsilon, \{\varphi_{\bar{\alpha}}\}\alpha \in Z^A$.

PROPOSITION 7.16. *Let π be an element of P such that*

$$\pi = w^2[w, x]^{2+4\mu}[Z_0, x]\pi_1 \mod N \wedge p_3; \; \pi_1 \in [\pi_2^A, \pi_2^A] .$$

Then there exists σ of W_2 such that

$$\pi^\sigma = w^2[w, x]^{2+4\mu}[Z_0, x]\pi_1 .$$

PROOF.

1) $e_0\mathfrak{N} \wedge \sum_{r\geqq 2} \bar{N}_r \subset M\mathfrak{N} + Z/2Z[\varphi_2]\cdot(\varphi_2\bar{w}, \varphi_\varepsilon Z_0)$.
Because, it is sufficient to show that

$$\varphi_2 \cdot D_{1,1}(\bar{p}_1^{1-e_0} \otimes \bar{p}_1^{1-e_0}) \subset M\mathfrak{N} .$$

This follows from that

$$\varphi_2\varphi_\alpha\beta = \varphi_\alpha\varphi_2\beta + \varphi_\beta^2\alpha \in M\mathfrak{N} .$$

This concludes the proof.

2) There exist two elements σ and τ of $\bar{W}_r$, $r \geqq 2$, such that

$$\pi^\sigma = \pi \cdot w^{2^r} ,$$

and

$$\pi^2 \equiv \pi \cdot [Z_0, x]^{2^{r-1}} \mod N \wedge P_{r+2} .$$

For, it holds that

$$\sigma(x) = x, \; \sigma(Z) = Z, \; \sigma(w) = w^{1+2^{r-1}} ,$$
$$\tau(Z) = x[Z_0, x]^{2^{r-2}}, \; \tau(Z) = Z_0^{1+2^{r-1}} ,$$

and

$$\tau(w) = w .$$

3) By Proposition 7.10, our assertion follows immediately from 1) and 2). q.e.d.

THEOREM II ($p=2$). *Let π, π' be any standard ω-regular elements in the sense of Definition* 7.6.

If $\pi \equiv \pi' \bmod p_3$ then there exist σ of W_2 and μ of Z_2 such that $\pi^{(1+2\mu)\sigma} = \pi'$.

PROOF. By Proposition 7.15, it is sufficient to prove in the case of

$$\pi = w^2[w, x]^2[Z_0, x]\pi_1 ,$$
$$\pi' = w^2[w, x]^{2+4\mu}[Z_0, x]\pi_1' ,$$
$$\pi_1, \pi_1' \in [Z_2^A, Z_2^A], \pi_1 \equiv \pi_1' \mod p_3 .$$

Since

$$\pi^2 \equiv [w, x]^4 \mod N \wedge p_3 ,$$

we get

$$\pi^{1+2\mu} \equiv w^2[w, x]^{2+4\mu}[Z_0, x]\pi_1 \equiv \pi' \mod N \wedge p_3 .$$

By Proposition 7.16 there exists σ of W_2 such that

$$\pi^{(1+2\mu)\sigma} = \pi' . \qquad \text{q.e.d.}$$

By Theorems I and II, in order to determine the structure of the total Galois group $G = AB = \mathrm{Gal.}(\bar{Q}_p/Q_p)$, it is sufficient to determine the residue class $\bar{\pi}_1$ of π_1 in

$$H = [Z_2^A, Z_2^A]/[Z_2^A, [Z_2^A Z_2^A]] \cong (Z_2^A/[Z_2^A; Z_2^A]) \curlywedge (Z_2^A/[Z_2^A, Z_2^A]) .$$

In the case of $p \neq 2$, the following fact is known by Koch
$\bar{\pi}_1$ is of the form $e_1(\alpha \wedge \beta)$ where

$$\Lambda_\alpha \oplus \Lambda_\beta = Z_2^A/[Z_2^A, Z_2^A] .$$

This is proved by investigating the Hilbert Norm residue simbol on the local fields.

REFERENCES

[1] A. V. JAKOVLEV, The Galois group of the algebraic closure of a local field, Izv. Akad. Nauk SSSR Ser. Mat., 32 (1968), 1231–1269.

[2] H. KOCH, Über Galoissche Gruppen von p-adischen Zahlkörpern, Math. Nachr., 29 (1965), 77–111.

DEPARTMENT OF MATHEMATICS
YAMAGATA UNIVERSITY
YAMAGATA, JAPAN