# *Formal groups and L functions*

By Tomoyoshi IBUKIYAMA

As Honda has shown, the structure of the formal minimal model over $Z$ of an elliptic curve defined over $Q$ is determined by its Hasse-Weil zeta function, and vice versa (cf. T. Honda [3], [4]). He has also shown similar results in the case of one dimensional tori (Honda [3]; see also Remark 1 in §2 of this paper) and certain higher dimensional Jacobian varieties (Honda [4]). In this paper, we shall show some analogous results in the case of certain higher dimensional tori. Tori that we consider here are $R_{k/Q}(G_m)$ and $R_{k/Q}(G_m)/R_{k'/Q}(G_m)$, where $k, k'$ are finite Galois extensions over $Q$ with $k' \subset k$. Now we explain briefly the case where $G = R_{k/Q}(G_m)$. For a fixed order $\mathfrak{O}$ of $k$ and a fixed $Z$-basis $\omega_1 = 1, \omega_2, \ldots, \omega_n$ of $\mathfrak{O}$, we define a formal group $F$ over $Z$ by;

$$F(x, y) = {}^t(F_1(x, y), \ldots, F_n(x, y)),$$

where

$$(1 + x_1\omega_1 + \cdots + x_n\omega_n)(1 + y_1\omega_1 + \cdots + y_n\omega_n) = 1 + F_1(x, y)\omega_1 + \cdots + F_n(x, y)\omega_n,$$

$F_i(x, y) \in Z[x, y]$. By using the same basis, we also define a matrix representation $\{A_\sigma\}$ of $\mathrm{Gal}(k/Q)$ in $GL_n(Q)$ by;

$$(\omega_1{}^\sigma, \ldots, \omega_n{}^\sigma) = (\omega_1, \ldots, \omega_n)A_\sigma.$$

By this definition, the representation $\{A_\sigma\}$ is equivalent over $Q$ to the regular representation of $\mathrm{Gal}(k/Q)$. If $k$ is an abelian extension of $Q$, we can define a *matrix* Artin $L$ function for this representation $\{A_\sigma\}$ by $\prod_p (I_n - ((1/e_p)\sum_\sigma A_\sigma)p^{-s})^{-1}$ ($\sigma$ runs over all Frobenius substitutions of a prime number $p$ and $e_p$ is the ramification index of $p$ in $k/Q$). For the sake of simplicity, we restrict ourselves here to the case where $k$ is abelian and tamely ramified over $Q$. (As for the further statements, see Proposition 2.2.3 and Theorem 4.2.8 of this paper.) Let $\mathfrak{O}_{\max}$ be the maximal order of $k$. For a fixed $Z$-basis of $\mathfrak{O}_{\max}$, define $F$ and $\{A_\sigma\}$ as above. Put

$$\prod_p \left(I_n - \left(\frac{1}{e_p}\sum_\sigma A_\sigma\right)p^{-s}\right)^{-1} = \sum_{m=1}^{\infty} \frac{A_m}{m^s} \qquad \text{and} \qquad g(x) = \sum_{m=1}^{\infty} \frac{A_m}{m^s} x^m,$$

where $x = (x_1, \ldots, x_n)$ and $x^m = (x_1{}^m, \ldots, x_n{}^m)$. Then the formal group $G$ defined by $G(x, y) = g^{-1}(g(x) + g(y))$ is a formal group over $Z_S$, where $S$ is the set of all primes

which do not divide any $e_p$ and $Z_S=\bigcap_{p\in S}(Q\cap Z_p)$. Then our results are stated as follows.

THEOREM A. *Assumptions and notations being as above, the formal group $F$ is strongly isomorphic over $Z_S$ to the formal group $G$.*

More precisely, we have;

THEOREM B. *Assumptions and notations being as above, the formal group $F$ is of type $pI_n-((1/e_p)\sum_\sigma A_\sigma)T$ for all primes $p$ in the sense of Honda* [4] *($T$ is a variable).*

Similar results are obtained in the case where $G=R_{k/Q}(G_m)/R_{k'/Q}(G_m)$, as explained in the later sections.

We get Theorem A immediately from Theorem B, using the classification theory studied by T. Honda [4]. First, we get an explicit form of the transformer of $F$ in § 3. And using this, we obtain the types of them in § 4. This proves Theorem B, therefore also proves Theorem A. In the final section, we examine briefly a weak isomorphism class of $F$.

To extend these results to general tori over $Q$, we must choose good local parameters of the tori and suitable matrix representations of the Galois groups of splitting fields of the tori over $Q$. But we do not know what are appropriate ones for general tori.

The material in this paper formed my master thesis at University of Tokyo in 1973. I would like to take the opportunity here to express my sincere thanks to my thesis advisor, Prof. Y. Ihara, who encouraged me during the preparation of this paper, and also to Prof. T. Honda who corrected my errors in the manuscript.

## § 1. General notions

Put $x={}^t(x_1,\dots,x_n)$, $x^m={}^t(x_1{}^m,\dots,x_n{}^m)$, $S$: a set of some primes, $Z_S=\bigcap_{p\in S}(Q\cap Z_p)$, $Z_S[[x]]$: the ring of formal power series over $Z_S$, $Z_S[[x]]^n$: the $n$ dimensional row vector space over $Z_S[[x]]$.

We shall consider only the commutative formal groups over $Z_S$. For given two formal groups $F$ (of dimension $n$) and $G$ (of dimension $m$), if there is $\varphi(x)\in Z_S[[x]]^m$, $\varphi(0)=0$, such that $\varphi(F(x,y))=G(\varphi(x),\varphi(y))$, $\varphi$ is called a homomorphism of $F$ to $G$ over $Z_S$. Moreover, if $m=n$ and $\varphi$ is invertible, $\varphi$ is also a homomorphism of $G$ to $F$. Such $\varphi$ is called a (weak) isomorphism. It is called a strong isomorphism if $\varphi(x)\equiv x$ mod. deg. 2 i.e. the total degrees of the terms $\varphi(x)-x$ are greater

than 2. We shall denote these relations of $F$ and $G$ as $F\sim G$ and $F\approx G$ respectively. A strong isomorphism, if it exists, is uniquely determined for $F$ and $G$. For a given $n$ dimensional commutative formal group $F(x,y)$ over $Z_S$, there exists one and only one $f(x)\in Q[[x]]^n$ called the transformer of $F$, such that $F(x,y)=f^{-1}(f(x)+f(y))$ and $f(x)\equiv x$ mod. deg. 2. This implies that all $F$ are strongly isomorphic over $Q$ to the affine group $x+y$. The problem we shall consider here is related to the strong isomorphism classes over $Z_S$. A general classification of formal groups up to strong isomorphisms over $Z_S$ was studied by T. Honda [4]. We shall adopt his theory to our special case. A formal Dirichlet series is by definition any Dirichlet series with coefficients in $M_n(Z_S)$, having the Euler product and the expansion $\sum_{m=1} A_m m^{-s}=\prod_{p\in S}(I_n+C_p p^{-s}+\cdots+C_{p^\nu}p^{\nu-1-\nu s}+\cdots)^{-1}$, assuming that $C_{p^\nu}$ and $C_{1^u}$ for different primes $p$ and 1 are commutative. The formal group attached to this series is defined by $G(x,y)=g^{-1}(g(x)+g(y))$, where

$$g(x)=\sum_{m=1}^{\infty}\frac{A_m}{m}x^m.$$

Then $pg(x)+C_pg(x^p)+\cdots+C_{p^\nu}g(x^{p^\nu})+\cdots\equiv 0 \bmod pZ_p$, that is, $G(x,y)$ is of type $pI_n+C_pT+\cdots+C_{p^\nu}T^\nu+\cdots$ in the sense of [4] and it is defined over $Z_S$ (See [4] Theorem 8.). (By an abuse of language, we say that $F(x,y)$ is of type $u$, if its transformer is of type $u$.) When we want to prove the existence of a strong isomorphism over $Z_S$ between the above $G(x,y)$ and another $F(x,y)$, we have only to prove that $F(x,y)$ is of type $pI_n+C_pT+\cdots$ at each $p\in S$ ([4] Theorem 2 and the uniqueness of strong isomorphisms) and we shall prove our theorem in that form.

## §2. $R_{k/Q}(G_m)$ and $R_{k/Q}(G_m)/R_{k'/Q}(G_m)$

Let $k$ be an algebraic number field of finite degree, $\mathfrak{O}$ an order of $k$ and $\omega_1=1,\omega_2,\ldots,\omega_n$, a $Z$-basis of $\mathfrak{O}$. Define a formal group $F$ over $Z$ by;

$$F(x,y)={}^t(F_1(x,y),\ldots,F_n(x,y)), \tag{2.1.1}$$

where

$$(1+x_1\omega_1+\cdots+x_n\omega_n)(1+y_1\omega_1+\cdots+y_n\omega_n)=1+F_1(x,y)\omega_1+\cdots+F_n(x,y)\omega_n,$$

$F_i(x,y)\in Z[x,y]$. Let $k'$ be a subfield of $k$. Suppose that $\mathfrak{O}$ has a $Z$-basis of the following form $\{\xi_i\theta_j\,|\,1\leqq i\leqq n',\ 1\leqq j\leqq(n/n')\}$ with $k=\sum_{j=1}^{n/n'}k'\theta_j$, $k'=\sum_{i=1}^{n'}Q\xi_i$ and $\xi_1=\theta_1=1$. Then a formal group $F_{k/k'}$ over $Z$ is defined by;

$$(1+(x_{n'+1}+x_{n'+2}\xi_2+\cdots)\theta_2+\cdots)(1+(y_{n'+1}+y_{n'+2}\xi_2+\cdots)\theta_2+\cdots)$$
$$=z_1(x,y)+z_2(x,y)\theta_2+\cdots+z_{n/n'}(x,y)\theta_{n/n'}, \qquad z_i(x,y)\in Z[\xi_1,\ldots,\xi_{n'},x,y],$$

$$F_{k/k',ij}(x,y)=\text{the coefficient of } \xi_j \text{ of } z_i(x,y)/z_1(x,y)$$

$$F_{k/k'}(x,y)={}^t(F_{k/k',ij}(x,y)). \tag{2.1.2}$$

$F$ (resp. $F_{k/k'}$) is a commutative formal group of dimension $n$ (resp. $n-n'$) over $Z$, and $(x_1,\ldots,x_n)$ (resp. $(x_{n'+1},\ldots,x_n)$) is one of the parameters at the origin of $R_{k/Q}(G_m)$ (resp. $R_{k/Q}(G_m)/R_{k'/Q}(G_m)$).

This is obvious for $F$. As for $F_{k/k'}$, by definition, we have, $z_1(x,y)\equiv 1$ mod. deg. 2 and $z_i(x,y)\equiv x_{(i-1)n'+1}\xi_1+\cdots+x_{in'}\xi_{n'}$ mod. deg. 2, $(i\geqq 2)$ so that we get $F_{k/k'}(x,y)\equiv x+y$ mod. deg. 2. To see the associativity, put

$$A=(1+(x_{n'+1}\xi_1+\cdots+x_{2n'}\xi_{n'})\theta_2+\cdots)(1+(y_{n'+1}\xi_1+\cdots)\theta_2+\cdots)$$
$$\times(1+(w_{n'+1}\xi_1+\cdots)\theta_2+\cdots).$$

We have

$$A=(z_1(x,y)+z_2(x,y)\theta_2+\cdots+z_{n/n'}(x,y)\theta_{n/n'})(1+(w_{n'+1}\xi_1+\cdots)\theta_2+\cdots)$$
$$=z_1(x,y)\left(1+\frac{z_2(x,y)}{z_1(x,y)}\theta_2+\cdots+\frac{z_{n/n'}(x,y)}{z_1(x,y)}\theta_{n/n'}\right)(1+(w_{n'+1}\xi_1+\cdots)\theta_2+\cdots)$$
$$=z_1(x,y)\,(z_1(F_{k'/k}(x,y),w)+z_2(F_{k'/k}(x,y),w)\theta_2+\cdots).$$

On the other hand, we have

$$A=z_1(y,w)\,(z_1(x,F_{k'/k}(y,w))+z_2(x,F_{k'/k}(y,w))\theta_2+\cdots)$$

Comparing these two equalities, we get,

$$\frac{z_i(F_{k'/k}(x,y),\omega)}{z_1(F_{k'/k}(x,y),\omega)}=\frac{z_i(x,F_{k'/k}(y,\omega))}{z_1(x,F_{k'/k}(y,\omega))}$$

and by definition, we obtain $F_{k/k'}(F_{k/k'}(x,y),\omega)=F_{k/k'}(x,F_{k/k'}(y,\omega))$.

REMARK 1: A formal group $x+y+\sqrt{D}xy$ treated in [3] is strongly isomorphic over the maximal order of $Q(\sqrt{D})$ to the formal group $F_{k/k'}$ for $k=Q(\sqrt{D})$, $k'=Q$, $\mathfrak{O}=$the maximal order of $k$.[1]

In fact, if $D$ is even,

$$F_{k/k'}(x,y)=\frac{x+y}{1+(D/4)xy} \qquad \text{for} \qquad \theta_1=1, \qquad \theta_2=\frac{\sqrt{D}}{2}$$

and the strong isomorphism to $x+y+\sqrt{D}xy$ of $F_{k/k'}$ is given by

[1] I was suggested by Y. Ihara to consider $F_{k/Q}$ instead of $x+y+\sqrt{D}xy$. This stand point is a clue to the generalization of Honda's results.

$$\varphi(x)=\frac{x}{1-(\sqrt{D}/2)x},$$

and if $D$ is odd,

$$F_{k/k'}(x,y)=\frac{x+y+xy}{1+((D-1)/4)xy}$$

for $\theta_1=1$, $\theta_2=\dfrac{(1+\sqrt{D})}{2}$ and $\varphi(x)=\dfrac{x}{1-((\sqrt{D}-1)/2)x}$.

In [3], the strong isomorphism to $x+y+\sqrt{D}xy$ of the formal group attached to $L(s,\chi)$, $(\chi(n)=(D/n))$ was obtained explicitly and globally. We shall obtain it locally for each $p$ and as a result we shall have the existence of the strong isomorphism over $Z$. There is a slight difference between two proves because in the former $L(s,\chi)$ is defined globally as Hecke's $L$-function and in the latter $L(s,\chi)$ is defined locally as Artin's $L$-function.

REMARK 2. (See [4] Theorem 3): In general, $F$ depends on the choice of orders and its $Z$-basis. But the weak isomorphism class of $F$ is well-defined if we fix an order. In fact, the base change by a unimodular matrix $V$ transforms a formal group $F$ of type $u$ into that of type $VuV^{-1}$.

LEMMA 2.1.3. *Put*

$$\frac{x_{sn'+1}\xi_1+\cdots+x_{(s+1)n'}\xi_{n'}}{1+x_1\xi_1+\cdots+x_{n'}\xi_{n'}}=\varphi_{sn'+1}(x)\xi_1+\cdots+\varphi_{(s+1)n'}(x)\xi_{n'},\ s=1\sim\frac{n}{n'}-1,\quad \varphi_i(x)\in Z[[x]],$$

*and* $\varphi(x)={}^t(\varphi_{n'+1}(x),\ldots,\varphi_n(x))$. *Then* $\varphi(x)$ *gives a homomorphism over* $Z$ *of* $F$ *to* $F_{k/k'}$.

PROOF. Put $F(x,y)={}^t(F_{ij}(x,y))$. By definition of $F$ and $z_i$, we have

$$\begin{aligned}
&(1+x_1\xi_1+\cdots x_{n'}\xi_{n'}+(x_{n'+1}\xi_1+\cdots+x_{n'}\xi_{n'})\theta_2+\cdots)\\
&\quad\times(1+y_1\xi_1+\cdots y_{n'}\xi_{n'}+(y_{n'+1}\xi_1+\cdots+y_{2n'}\xi_{n'})\theta_2+\cdots)\\
&=1+F_{11}(x,y)\xi_1+\cdots+F_{1n'}(x,y)\xi_{n'}+(F_{21}(x,y)\xi_1+\cdots+F_{2n'}(x,y)\xi_{n'})\theta_2+\cdots)\\
&=(1+x_1\xi_1+\cdots+x_{n'}\xi_{n'})(1+y_1\xi_1+\cdots+y_{n'}\xi_{n'})\\
&\quad\times(z_1(\varphi(x),\varphi(y))+z_2(\varphi(x),\varphi(y))\theta_2+\cdots+z_{n/n'}((\varphi(x),\varphi(y))\theta_{n/n'}).
\end{aligned}$$

Comparing these two equalities, we get

$$\begin{aligned}
&1+F_{11}(x,y)\xi_1+\cdots+F_{1n'}(x,y)\xi_{n'}\\
&\quad=(1+x_1\xi_1+\cdots+x_{n'}\xi_{n'})(1+y_1\xi_1+\cdots+y_{n'}\xi_{n'})z_1(\varphi(x),\varphi(y))\\
&F_{i1}(x,y)\xi_1+\cdots+F_{in'}(x,y)\xi_{n'}\\
&\quad=(1+x_1\xi_1+\cdots+x_{n'}\xi_{n'})(1+y_1\xi_1+\cdots y_{n'}\xi_{n'})z_i(\varphi(x),\varphi(y))
\end{aligned}$$

and

$$\frac{z_i(\varphi(x),\varphi(y))}{z_1(\varphi(x),\varphi(y))}=\frac{F_{i1}(x,y)\xi_1+\cdots+F_{in'}(x,y)\xi_{n'}}{1+F_{11}(x,y)\xi_1+\cdots+F_{1n'}(x,y)\xi_{n'}} \qquad (i\geqq 2).$$

The right side equals to $\varphi_{(i-1)n'+1}(F(x,y))\xi_1+\cdots+\varphi_{in'}(F(x,y))\xi_{n'}$, which implies $F_{k'lk}(\varphi(x),\varphi(y))=\varphi(F(x,y))$ and this completes the proof.

LEMMA 2.1.4. *If $f$ is the transformer of $F$, then the transformer $f_{klk'}$ of $F_{klk'}$ is given by;*

$$f_{klk'}({}^t(x_{n'+1},\ldots,x_n))=(0,I_{n-n'})f({}^t(0,\ldots,0,x_{n'+1},\ldots,x_n)),$$

*where $I_{n-n'}$ is a unit matrix.*

PROOF. Observe that $\varphi(x)\equiv(0,I_{n-n'}){}^t(x_1,\ldots,x_n)$ mod. deg. 2, then that

$$f_{klk'}{}^{-1}((0,I_{n-n'})f)=\varphi$$

(by [4] Proposition 1.6) and that

$$\varphi({}^t(0,\ldots,x_{n'+1},\ldots,x_n))={}^t(x_{n'+1},\ldots,x_n). \qquad \text{Q.E.D.}$$

Put $Z_{(p)}=Z\cap Q_p$.

LEMMA 2.1.5. *If $F$ is of type $pI_n+C_pT+C_{p^2}T^2+\cdots$ (for the valuation ring $Z_{(p)}$ and $\pi=p, q=p, \sigma=$ id. in [4] § 2) and $A_{p^\nu}=\begin{pmatrix}* & * \\ 0 & C_{p^\nu}\end{pmatrix}$, $C_{p^\nu}\in M_{n-n'}(Z_{(p)})$, then $F_{klk'}$ is of type $pI_{n-n'}+C_pT+C_{p^2}T^2+\cdots$.*

PROOF. Multiply the congruence $pf(x)+A_pf(x^p)+\cdots\equiv 0$ mod. $pZ_{(p)}$ by $(0,I_{n-n'})$ from left, and use Lemma 2.1.4.

LEMMA 2.1.6. *The multiplicative group $x+y+xy$ is of type $p-T$ (well-known and easy).*

LEMMA 2.2.1. *Let $k/Q$ be a finite Galois extension, $\mathfrak{O}$ an order of $k$, $\omega_1=1$, $\omega_2,\ldots,\omega_n$, any $Z$-basis of $\mathfrak{O}$, and $F$ the formal group defined by (2.1.1). Put $G_m{}^n(x,y)={}^t(x_1+y_1+x_1y_1,\ldots,x_n+y_n+x_ny_n)$. Then if a prime ideal $\mathfrak{p}$ of the maximal order $\mathfrak{O}_{\max}$ of $k$ does not divide the discriminant of $\mathfrak{O}$, $F$ is weakly isomorphic to $G_m{}^n$ over $\mathfrak{O}_\mathfrak{p}$, where $\mathfrak{O}_\mathfrak{p}$ is the localization of $\mathfrak{O}_{\max}$ at $\mathfrak{p}$.*

PROOF. Put $U=(w_i^{\tau_j})$, $\tau_j\in\mathrm{Gal}(k/Q)$ and $\phi(x)=Ux$. Then $(\det U)^2$ is the discriminant of $\mathfrak{O}$, which is prime to $\mathfrak{p}$ and $U^{-1}\in M_n(\mathfrak{O}_\mathfrak{p})$. By definition we have,

$$\begin{aligned}&(x_1\omega_1^{\tau_j}+\cdots+x_n\omega_n^{\tau_j})+(y_1\omega_1^{\tau_j}+\cdots+y_n\omega_n^{\tau_j})+(x_1\omega_1^{\tau_j}+\cdots+x_n\omega_n^{\tau_j})(y_1\omega_1^{\tau_j}+\cdots+y_n\omega_n^{\tau_j})\\&\quad=F_1(x,y)\omega_1^{\tau_j}+\cdots+F_n(x,y)\omega_n^{\tau_j}.\end{aligned}$$

Then we obtain $G_m{}^n(Ux,Uy)=UF(x,y)$, and $\phi$ gives a weak isomorphism of $F$ to $G_m{}^n$ over $\mathfrak{O}_\mathfrak{p}$. Q.E.D.

Assume as in Lemma 2.2.1; then $\mathfrak{p}$ is unramified in $k/Q$ and $p$ can be taken to be a prime element of $\mathfrak{O}_\mathfrak{p}$.

LEMMA 2.2.2. *$F$ is of type $pI_n - U^{-1}U^\sigma T$ for the valuation ring $\mathfrak{O}_\mathfrak{p}$ and $\pi=p$, $q=p$, where $\sigma$ is the Frobenius map of $\mathfrak{p}$ in $k$.*

PROOF. $G_m^n$ is of type $(p-T)I_n$. There exists an element $u$ of $M_n((\mathfrak{O}_\mathfrak{p})_\sigma[[T]])$ such that $F$ is of type $u$ ([4] Theorem 4), and we have $(p-T)U=tu$ where $t$ is a unit in $M_n((\mathfrak{O}_\mathfrak{p})_\sigma[[T]])$ (Lemma 2.2.1 and [4] Theorem 3). Then $pI_n - U^{-1}U^\sigma T = (U^{-1}t)u$. Therefore, $F$ is of type $pI_n - U^{-1}U^\sigma T$, for $U^{-1}t$ is also a unit. Q.E.D.

Now suppose that $p$ is a prime number which does not divide the discriminant of $\mathfrak{O}$, and $p=\mathfrak{p}_1\cdots\mathfrak{p}_g$ in $k/Q$. We denote by $\sigma_i$ the Frobenius map of $\mathfrak{p}$, and define $A_{\sigma_i}$ for $\sigma_i$ as $(\omega_1^{q^i},\ldots,\omega_n^{q^i})=(\omega_1,\ldots,\omega_n)A_{\sigma_i}$. Then, we have

PROPOSITION 2.2.3. *If $p\nmid g$, $F$ is of type $pI_n-((1/g)\sum_{i=1}^{g}A_{\sigma_i})T$ for $Z_{(p)}$, $\pi=p$, $q=p$, $\sigma=$ id.*

PROOF. There exists an element $u$ of $M_n(Z_{(p)}[[T]])$ such that $F$ is of type $u$ for $Z_{(p)}$, $\pi=p, q=p, \sigma=$ id ([4] Theorem 4), and then $F$ is also of type $u$ for $\mathfrak{O}_{\mathfrak{p}_i}$, $\pi=p, q=p, \sigma=\sigma_i$. Then by Lemma 2.2.2 and [4] Theorem 4, the following relations hold;

$$pI_n - U^{-1}U^{\sigma_i}T=t_iu \qquad (i=1\sim g) \tag{2.2.4}$$

where $t_i$ is a unit of $M_n((\mathfrak{O}_{\mathfrak{p}_i})_{\sigma_i}[[T]])$. $M_n((\mathfrak{O}_{\mathfrak{p}_i})_{\sigma_i}[[T]])$ can be naturally embedded into

$$\left\{\sum_{m=0}^{\infty}A_mT^m;\ A_m\in M_n(k)\right\}$$

as right $M_n(Z_{(p)}[[T]])$ modules. Adding both sides of (2.2.4) in this sense and dividing by $g$, we obtain

$$pI_n-\left(\frac{1}{g}\sum_{i=1}^{g}U^{-1}U^{\sigma_i}\right)T=\frac{1}{g}(t_1+\cdots+t_g)u$$

and we can easily show that $\sum_{i=1}^{g}U^{\sigma_i}=U\sum_{i=1}^{g}A_{\sigma_i}$. If $p\nmid g$ then $(t_1+\cdots+t_g)/g$ is a unit of $M_n(Z_{(p)}[[T]])$. Therefore, $F$ is of type $pI_n-((1/g)\sum_{i=1}^{g}A_{\sigma_i})T$. Q.E.D.

LEMMA 2.2.5. *If $k/Q$ is an abelian extension, $F$ is of type $pI_n-A_\sigma T$, where $A_\sigma$ is a rational matrix defined $(\omega_1^\sigma,\ldots,\omega_n^\sigma)=(\omega_1,\ldots,\omega_n)A_\sigma$, and $\sigma$ is the Frobenius automorphism of $p$.* (This time the condition $p\nmid g$ is not needed.)

PROOF. In this case, all $\sigma_i=\sigma$ and $t_1=\cdots=t_g$. Then we have

$$pI_n-U^{-1}U^\sigma T=tu \qquad \text{Q.E.D.}$$

LEMMA 2.2.6. *Assumptions being as in Lemma* 2.2.5, *we have* $A_\sigma=\begin{pmatrix} * & * \\ 0 & C_\sigma \end{pmatrix}$, $C_\sigma \in M_{n-n'}(Z_{(p)})$, *for a basis* $\{\xi_i\theta_j\}$, *and* $F_{k/k'}$ *is of type* $pI_{n-n'}-C_\sigma T$.

PROOF. Easily proved by Lemma 2.2.5 and Lemma 2.1.5. Q.E.D.

## § 3. Explicit forms of the transformers

We will obtain explicit forms of the transformers of $F$ and $F_{k/k'}$, which will make it possible to examine the types also for ramified $p$'s.

THEOREM 3.1.1. *Let* $k$ *be a finite algebraic number field,* $\mathfrak{O}$ *an order of* $k$, *and* $\omega_1=1, \omega_2, \ldots, \omega_n$ *its* $Z$*-basis. Define* $F$ *by* (2.1.1). *Then the transformer of* $F$ *is given by;*

$$f(x)=s_1(\log (I+R(\omega_1)x_1+\cdots+R(\omega_n)x_n)),$$

*where* $R$ *is the regular representation with respect to* $(\omega_1, \ldots, \omega_n)$, *"log" is the formal logarithmic expansion and* $s_1$ *is the projection to the first column of the matrix.*

PROOF. In general, a transformer $g={}^t(g_1, \ldots, g_n)$ is the unique solution, satisfying $g(x)\equiv x$ mod. deg. 2, of the differential equation $dg_i=\phi_{ij}(x)dx_j (j=1\sim n)$, where

$$(\phi_{ij}(y))=\left(\frac{\partial F_i(0, y)}{\partial x_j}\right)^{-1}$$

([4] Theorem 1). To calculate this in our case, put $\omega_l\omega_k=\sum_{i=1}^{n} a_{lk}^{(i)}\omega_i$ $(a_{lk}^{(i)}\in Q)$. Then we have

$$F_i(x, y)=x_i+y_i+\sum_{k,l=1}^{n} a_{lk}^{(i)}x_k y_l \quad \text{and} \quad \frac{\partial F_i(0, y)}{\partial x_j}=\delta_{ij}+\sum_{l=1}^{n} a_{lj}^{(i)}y_l,$$

so that we obtain, $(\phi_{ij}(x))=(I+R(\omega_1)x_1+\cdots+R(\omega_n)x_n)^{-1}$. It is clear that $f(x)\equiv x$ mod. deg. 2, and that

$$\begin{aligned}\frac{\partial f}{\partial x_j}&=s_1\left(\frac{\partial}{\partial x_j}\log (I+R(\omega_1)x_1+\cdots+R(\omega_n)x_n)\right)\\ &=s_1((I+R(\omega_1)x_1+\cdots+R(\omega_n)x_n)^{-1}R(\omega_j))\\ &=\text{the } j\text{-th column of } (I+R(\omega_1)x_1+\cdots+R(\omega_n)x_n)^{-1}.\end{aligned}$$

(Note that the first column of $R(\omega_j)$ is ${}^t(0\cdots 0\overset{j}{1}, 0\cdots 0)$). Therefore

$$\left(\frac{\partial f}{\partial x_j}\right)=(I+R(\omega_1)x_1+\cdots+R(\omega_n)x_n)^{-1}$$

and the theorem is proved.

THEOREM 3.1.2. *The transformer of* $F_{k/k'}$ *is given by;*

$$f_{k/k'}=\tilde{s}_1(\log (I+R(\xi_1\theta_2)x_{n'+1}+\cdots+R(\xi_{n'}\theta_{n/n'})x_n)),$$

*where $\tilde{s}_1$ is the projection to the $n'+1$-th to the $n$-th rows of the first column.*

PROOF. Obvious by Lemma 2.1.4 and Theorem 3.1.1.

LEMMA 3.1.3. *Assume that $F$ is a formal group over $Z_S$ and $f$, its transformer. Put $\tilde{f}(x)=f(x_1,0,\ldots,0)+f(0,x_2,0,\ldots)+\cdots+f(0,\ldots,0,x_n)$ and $\tilde{F}(x,y)=\tilde{f}^{-1}(\tilde{f}(x)+\tilde{f}(y))$. Then $\tilde{F}$ is a formal group over $Z_S$ and $\tilde{F}$ is strongly isomorphic to $F$ over $Z_S$.*

PROOF. There exists an element $u$ of $M_n(Z_{(p)}[[T]])$ such that $F$ is of type $u$ for each $p\in S$, and $f$ satisfies the congruence $pf(x)+C_pf(x^p)+\cdots\equiv 0 \bmod. pZ_{(p)}$ ([2] Theorem 4). Note that $\tilde{f}(x),\tilde{f}(x^p),\ldots$ consist only of "unmixed" terms of $f(x),f(x^p),\ldots$ (i.e. those terms $x_1^{e_1}\cdots x_n^{e_n}$ with $e_i\neq 0$ for only one i). Therefore $\tilde{f}(x)$ also satisfies

$$p\tilde{f}(x)+C_p\tilde{f}(x^p)+\cdots\equiv 0 \bmod. pZ_{(p)}.$$

Therefore the lemma follows from [4] Theorem 2 and the uniqueness of the strong isomorphism.

REMARK. Put $f(x_j)=f(0\cdots 0\ x_j\ 0\cdots 0)$. Then $f(x)$ is of type $u$ if and only if $f(x_j)$ is of type $u$ for all $j$.

## §4. The type of $F$

From now on, we assume that $k/Q$ is an *abelian* extension.

LEMMA 4.1.1. *We have the congruence,*

$$pf(x_j)-Af(x_j^p)\equiv 0 \bmod. pZ_{(p)} \quad \textit{for} \quad A\in M_n(Z_{(p)}),$$

*if and only if $s_1(R(\omega_j)^{n'p^k})\equiv As_1(R(\omega_j)^{n'p^{k-1}}) \bmod. p^kZ_{(p)}$ for all positive integers $n',k$ such that $p\nmid n'$.*

PROOF. By Theorem 3.1.1,

$$f(x_j)=\sum_{n=1}^{\infty}(-1)^{n-1}\frac{s_1(R(\omega_j)^n)}{n}x_j^n.$$

Therefore

$$pf(x_j)-Af(x_j^p)=\sum_{p\nmid n}(-1)^{n-1}\frac{ps_1(R(\omega_j)^n)}{n}x_j^n + \sum_{\substack{p\nmid n'\\ k=1}}^{\infty}\frac{x_j^{n'p^k}}{n'p^{k-1}}\{(-1)^{n'p^{k-1}}s_1(R(\omega_j)^{n'p^k}-(-1)^{n'p^{k-1}-1}As_1(R(\omega_j)^{n'p^{k-1}})\}$$

The first term is divisible by $p$. If $p=2$ and $k\geqq 2$ or $p\neq 2$ then we have

$$(-1)^{n'p^{k-1}}=(-1)^{n'p^{k-1}-1}.$$

Therefore $pf(x_j)-Af(x_j^p)\equiv 0 \bmod. pZ_{(p)}$ if and only if

$$s_1(R(\omega_j)^{n'p^k})\equiv As_1(R(\omega_j)^{n'p^{k-1}}) \bmod. p^kZ_{(p)}.$$

If $p=2$ and $k=1$, then $(-1)^{2n'-1}=-1, (-1)^{n'-1}=1$. Therefore $2f(x_j)-Af(x_j^2)\equiv 0$ mod. $2Z_{(2)}$ if and only if

$$s_1(R(\omega_j)^{2n'})\equiv -As_1(R(\omega_j)^{n'})\equiv As_1(R(\omega_j)^{n'}) \bmod. 2Z_{(2)}. \qquad \text{Q.E.D.}$$

Now, we can determine the types of $F$ also for the ramified $p$'s.

At first, we shall consider the *tamely* ramified case. Let $\mathfrak{O}$ be an order of $k$ such that $Z_{(p)}\mathfrak{O}$ equals to $Z_{(p)}\mathfrak{O}_{\max}$, where $\mathfrak{O}_{\max}$ is the maximal order of $k$. Define a rational matrix $A_\sigma$ by $(\omega_1^\sigma,\dots,\omega_n^\sigma)=(\omega_1,\dots,\omega_n)A_\sigma$. Then $R(\omega^\sigma)=A_\sigma R(\omega)A_\sigma^{-1}$. Assume that $p$ is tamely ramified in $k/Q$ with the ramification index $e$. Let $I$ be the inertia group of $p$, $k_I$ the inertia field and $\mathfrak{O}_I$ the maximal order of $k_I$. The Frobenius class mod. $I$ is defined only by $p$ (because $k/Q$ is abelian) which we denote by $\sigma I$. Suppose that $p=(\mathfrak{P}_1\cdots\mathfrak{P}_g)^e$ in $k$. For any $\omega\in Z_{(p)}\mathfrak{O}_I$, there exists $a\in Z_{(p)}\mathfrak{O}_I$ such that $\omega-a\in(\mathfrak{P}_1\cdots\mathfrak{P}_g)Z_{(p)}$, since the residue fields are the same for $k$ and $k_I$. Put $\omega=a+\theta$, then $\theta^e\in pZ_{(p)}\mathfrak{O}$, and $e\leqq p-1$ (note that $k/Q$ is abelian). Then we have $\omega^p\equiv a^p \bmod. pZ_{(p)}\mathfrak{O}$, so that

$$\omega^{p^k}\equiv a^{p^k} \bmod. p^kZ_{(p)}\mathfrak{O} \tag{4.2.1}$$

and

$$(\omega^{\sigma\tau})^{p^{k-1}}=(a^\sigma)^{p^{k-1}}+p^{k-1}\theta_1^{\sigma\tau} \tag{4.2.2}$$

$\theta_1\in(\mathfrak{P}_1\cdots\mathfrak{P}_g)Z_{(p)}\mathfrak{O}$, for all $\tau\in I$. Adding both sides of (4.2.2) over all $\tau\in I$, we obtain

$$\frac{1}{e}\sum_{\tau\in I}(\omega^{\sigma\tau})^{p^{k-1}}=(a^\sigma)^{p^{k-1}}+\frac{p^{k-1}}{e}\operatorname{tr}_{k/k_I}(\theta_1^\sigma),$$

where $\operatorname{tr}_{k/k_I}(\theta_1^\sigma)\in k_I\cap(\mathfrak{P}_1\cdots\mathfrak{P}_g)Z_{(p)}\mathfrak{O}=pZ_{(p)}\mathfrak{O}_I$ then

$$\frac{1}{e}\sum_{\tau\in I}(\omega^{\sigma\tau})^{p^{k-1}}\equiv(a^\sigma)^{p^{k-1}} \bmod. p^kZ_{(p)}\mathfrak{O}.$$

In view of (4.2.1) and the fact that $\sigma$ induces the Frobenius map on $k_I$, we have;

$$\omega^{p^k}-\frac{1}{e}\sum_{\tau\in I}(\omega^{\sigma\tau})^{p^{k-1}}\equiv a^{p^k}-(a^\sigma)^{p^{k-1}}\equiv 0 \bmod. p^kZ_{(p)}\mathfrak{O}. \tag{4.2.3}$$

Put $\omega=\omega_j^{n'}$, then from (4.2.3) we obtain the congruence

$$R(\omega_j)^{n'p^k}-\frac{1}{e}\sum_{\tau\in I}A_{\sigma\tau}R(\omega_j)^{n'p^{k-1}}A_{\sigma\tau}^{-1}\equiv 0 \bmod. p^kZ_{(p)}.$$

Noting that $A_{\sigma\tau}^{-1}=\begin{pmatrix}1 & * \\ 0 & *\end{pmatrix}$, we get

$$s_1(R(\omega_j)^{n'p^k})-\left(\frac{1}{e}\sum_{\tau\in I}A_{\sigma\tau}\right)s_1(R(\omega_j)^{n'p^{k-1}})\equiv 0 \bmod. p^kZ_{(p)}.$$

Therefore we have;

THEOREM 4.2.4. *When $p$ is tamely ramified in an abelian extension $k$ of $Q$, the formal group $F$ for an order $\mathfrak{O}$ such that $Z_{(p)}\mathfrak{O}$ equals to $Z_{(p)}\mathfrak{O}_{\max}$, is of type $pI_n-((1/e)\sum_{\tau\in I}A_{\sigma\tau})T$, where $F$ and $\{A_\sigma\}$ are defined for any common $Z$-basis of $\mathfrak{O}$.*

Corollary 4.2.5. *Put $S=\{p\,|\,p\nmid n\}$. Then the formal group attached to*

$$\prod_{p\nmid n}\left(I_n-\left(\frac{1}{e}\sum_{\tau\in I}A_{\sigma\tau}\right)p^{-s}\right)^{-1}$$

*is strongly isomorphic to $F$ over $Z_S$.*

PROOF. Easily proved by [4] Theorem 8 and the above theorem. Q.E.D.

Next, we shall consider the case of *wildly* ramified $p$'s.

LEMMA 4.3.1 *Assume that $k$ is an abelian extension of $Q$ and put $e=e_0p^{\nu-1}$ $(\nu\geqq 2, p\nmid e_0)$. Then $k$ can be embedded in a cyclotomic field $Q(\zeta_{p^\nu})Q(\zeta_m)$ $(p\nmid m)$ if $p\neq 2$, and in $K_2Q(\zeta_m)$ $(2\nmid m)$ if $p=2$, where $K_2$ is some subfield of $Q(\zeta_{2^{\nu+1}})$ with index 2.*

PROOF. By Kronecker's theorem, there exist natural integers $m$ and $\nu'$ $(p\nmid m)$ such that $k\subset Q(\zeta_{p^{\nu'}m})$. Since $Q(\zeta_m)$ is the inertia field of $p$ in $Q(\zeta_{p^{\nu'}m})$ over $Q$, we have $[k\cdot Q(\zeta_m):\ Q(\zeta_m)]=[k:\ k\cap Q(\zeta_m)]=e_0p^{\nu-1}$.

As well known, $\mathrm{Gal}(Q(\zeta_{p^{\nu'}m})/Q(\zeta_m))\cong(Z/_{p^{\nu'}z})^\times$, and we can easily verify that its subgroup with index $e_0p^{\nu-1}$ contains $\mathrm{Gal}(Q(\zeta_{p^{\nu'}m})/Q(\zeta_{p^\nu m}))$ if $p$ is odd. Therefore we have $k\cdot Q(\zeta_m)\subset Q(\zeta_{p^\nu m})$ for an odd $p$, and we obtain our lemma in this case. The proof is virtually the same for $p=2$.

LEMMA 4.3.2. *Assumptions being as in Lemma 4.3.1, the different $\mathfrak{d}_{k/Q}$ is divisible by $p^{\nu-1}$.*

PROOF. We denote the $p$-part of the different as $\mathfrak{d}^{(p)}$. Note that

$$\mathfrak{d}^{(p)}_{Q(\zeta_{p^\nu m})/Q}=\mathfrak{d}^{(p)}_{Q(\zeta_{p^\nu m})/k\cdot Q(\zeta_m)}\cdot\mathfrak{d}^{(p)}_{k\cdot Q(\zeta_m)/Q}\qquad\text{and}\qquad\mathfrak{d}^{(p)}_{k\cdot Q(\zeta_m)/Q}=\mathfrak{d}^{(p)}_{k/Q}.$$

As well known, we have $p=(\mathfrak{p}_1\cdots\mathfrak{p}_g)^{p^{\nu-1}(p-1)}$ in $Q(\zeta_{mp^\nu})/Q$ and

$$\mathfrak{d}^{(p)}_{Q(\zeta_{p^\nu m})/Q}=(\mathfrak{p}_1\cdots\mathfrak{p}_g)^{p^{\nu-1}(\nu(p-1)-1)}.$$

If $p$ is odd, $Q(\zeta_{p^\nu m})$ is a tamely ramified extension of $p$ over $k\cdot Q(\zeta_m)$ with degree $(p-1)/e_0$ so that we obtain $\mathfrak{d}^{(p)}_{Q(\zeta_{p^\nu m})/k\cdot Q(\zeta_m)}=(\mathfrak{p}_1\cdots\mathfrak{p}_g)^{(p-1)/e_0-1}$. Then we have

$$\mathfrak{d}_{k^{(p)}Q(\zeta_m)/Q}^{(p)} = (\mathfrak{p}_1 \cdots \mathfrak{p}_g)^{p^{\nu-1}(\nu(p-1)-1)-((p-1)/e_0-1)},$$

and since

$$p^{\nu-1}(\nu(p-1)-1)-\left(\frac{p-1}{e_0}-1\right) \geqq (\nu-1)p^{\nu-1}(p-1) \quad \text{and} \quad p=(\mathfrak{p}_1\cdots\mathfrak{p}_g)^{p^{\nu-1}(p-1)},$$

$\mathfrak{d}_{k/Q}$ is divisible by $p^{\nu-1}$. The proof is virtually the same for $p=2$.

LEMMA 4.3.3. *Assumptions being as in Lemma* 4.3.1, *let* $\omega$ *be an integer in* $k$. *Then* $(1/e)\,\mathrm{tr}_{k/k_I}(\omega) \in Z_{(p)}\mathfrak{O}_I$.

PROOF. By Lemma 4.3.2, we have $p^{1-\nu} \in d_{k/k_I}^{-1} = \{\alpha \in k;\ \mathrm{tr}_{k/k_I}(\alpha\mathfrak{O}_{\max}) \subset \mathfrak{O}_I\}$. Therefore we get

$$\mathrm{tr}_{k/k_I}\left(\frac{\omega}{e_0 p^{\nu-1}}\right) \in Z_{(p)}\mathfrak{O}_I$$

and this proves our lemma. Q.E.D.

Put $\mathfrak{O}^{(p)} = \mathfrak{O}_{T_p} + p\mathfrak{O}_{\max}$, where $\mathfrak{O}_{T_p}$ is the maximal order in the maximal subfield in which $p$ is tamely ramified and $\mathfrak{O}_{\max}$ is the maximal order in $k$.

THEOREM 4.3.4. *Assume that* $k$ *is an abelian extension of* $Q$ *and that* $\mathfrak{O}$ *is an order such that* $Z_{(p)}\mathfrak{O} = Z_{(p)}\mathfrak{O}^{(p)}$. *Then* $F$ *is of type* $pI_n - ((1/e)\sum_{\tau \in I} A_{\sigma\tau})T$, *where* $F$ *and* $\{A_\sigma\}$ *are defined for a common* $Z$*-basis of* $\mathfrak{O}$.

PROOF. First, $(1/e)\sum_{\tau \in I} A_{\sigma\tau} \in M_n(Z^{(p)})$ by Lemma 4.3.3. For $\omega \in Z_{(p)}\mathfrak{O}$, we can put $\omega = a + p\theta$, $a \in Z_{(p)}\mathfrak{O}_{T_p}$ and $\theta \in Z_{(p)}\mathfrak{O}_{\max}$. Then

$$\omega^{p^k} \equiv a^{p^k} \bmod p^{k+1}Z_{(p)}\mathfrak{O}_{\max}, \quad \text{and} \quad \omega^{p^{k-1}} = a^{p^{k-1}} + p^k\theta_1,\ \theta_1 \in Z_{(p)}\mathfrak{O}_{\max}, \tag{4.3.5}$$

so that

$$\frac{1}{e}\sum_{\tau \in I}(\omega^{\sigma\tau})^{p^{k-1}} \equiv \frac{1}{e}\sum_{\tau \in I}(a^{\sigma\tau})^{p^{k-1}} + p^k\frac{1}{e}\mathrm{tr}_{k/k_I}(\theta_1^{\sigma}). \tag{4.3.6}$$

Then using Lemma 4.3.3 and (4.3.5), (4.3.6), we have:

$$\omega^{p^k} - \frac{1}{e}\sum_{\tau \in I}(\omega^{p^{k-1}})^{\sigma\tau} \equiv a^{p^k} - \frac{1}{e}\sum_{\tau \in I}(a^{\sigma\tau})^{p^{k-1}} \bmod p^k Z_{(p)}\mathfrak{O}. \tag{4.3.7}$$

The right side of (4.3.7) belongs to $p^kZ_{(p)}\mathfrak{O}$ by the proof of Theorem 4.2.4. Then putting $\omega = \omega_j^{n'}$, we can prove $s_1(R(\omega)^{n'p^k}) \equiv ((1/e)\sum_{\tau \in I} A_{\sigma\tau})s_1(R(\omega)^{n'p^{k-1}}) \bmod p^kZ_{(p)}$ as in the proof of Theorem 4.2.4.

THEOREM 4.3.8. *Let* $k/Q$ *be an abelian extension,* $k_{T_p}$ *the maximal subfield of* $k$ *tamely ramified at* $p$ *and* $\mathfrak{O}_{T_p}$ *the maximal order of* $k_{T_p}$. *Put* $\mathfrak{O}^{(p)} = \mathfrak{O}_{T_p} + p\mathfrak{O}_{\max}$ *and* $\mathfrak{O} = \bigcap_p \mathfrak{O}^{(p)}$. *Then* $F$ *is of type* $pI_n - ((1/e)\sum_{\tau \in I_p} A_{\sigma\tau})T$ *for all* $p$, *where* $F$ *and* $\{A_\tau\}$ *are defined for any common* $Z$*-basis of* $\mathfrak{O}$.

PROOF. Easily proved by Theorem 4.2.4 and Theorem 4.3.4.

COROLLARY 4.3.9. *Assumptions being as above, let $S$ be the set of prime numbers which do not divide the denominators of $(1/e)\sum_{\tau\in I_p} A_{\sigma\tau}$. Then $F$ and the formal group attached to the formal Dirichlet series $\prod_{p\in S}(I_n-((1/e)\sum_{\tau\in I_p} A_{\sigma\tau})p^{-s})^{-1}$ are mutually strongly isomorphic over $Z_S$.*

PROOF. Easily proved by Theorem 4.3.8 and [4] Theorem 8. Q.E.D.

We can obtain analogous results also for $F_{k/k'}$. Now $k/Q$ is abelian, so that $k'/Q$ is also abelian. Assume that 0 is as above and has a $Z$-basis $\{\xi_i\theta_j\}$ and that $F_{k/k'}$ and $A_\sigma$ are defined for 0 and $\{\xi_i\theta_j\}$. Then $A_\sigma$ can be written as $\begin{pmatrix} * & * \\ 0 & C_\sigma \end{pmatrix}$, $C_\sigma\in M_{n-n'}(Z)$. Then by Lemma 2.1.5 and Theorem 4.3.8 we have:

COROLLARY 4.3.10. *$F_{k/k'}$ is of type $pI_{n-n'}-((1/e)\sum_{\tau\in I_p} C_{\sigma\tau})T$. The corresponding Dirichlet series is given by*

$$\det\prod_p\left(I_{n-n'}-\left(\frac{1}{e}\sum_{\tau\in I_p}C_{\sigma\tau}\right)p^{-s}\right)^{-1}=\frac{\zeta_k(s)}{\zeta_{k'}(s)}.$$

## §5. Reduction mod. $p$

Suppose that $\mathfrak{O}$ is an order of $k$, abelian over $Q$, such that $Z_{(p)}\mathfrak{O}\supset Z_{(p)}\mathfrak{O}_I$, where $\mathfrak{O}_I$ is the maximal order of the inertia field $k_I$ for $p$. Let $\mathfrak{p}$ be any extension of $p$ in $k_I$ and $\mathfrak{O}_{I,\mathfrak{p}}$, the localization of $\mathfrak{O}_I$ at $\mathfrak{p}$. Put

$$G_m{}^r\times G_a{}^{n-r}=(x_1+y_1+x_1y_1,\ldots,x_r+y_r+x_ry_r,x_{r+1}+y_{r+1},\ldots,x_n+y_n).$$

As well known, this formal group is of type $pI_n-\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}T$ for the valuation ring $Z_{(p)}$ and $\pi=p, q=p, \sigma=\mathrm{id}$.

THEOREM 5.1.1. *Notations being as in §4, assume that $F$ is of type*

$$pI_n-\left(\frac{1}{e}\sum_{\tau\in I_p}A_{\sigma\tau}\right)T.$$

*Then $F$ is weakly isomorphic to $G_m{}^r\times G_a{}^{n-r}$ over $\mathfrak{O}_{I,\mathfrak{p}}$.*

COROLLARY 5.1.2. *$F$ mod $p$ is weakly isomorphic to $G_m{}^r\times G_a{}^{n-r}$ over $F_{p^f}$.*

*($r=[k_I\colon Q]$, $f=$the relative degree of $\mathfrak{p}$ in $k_I/Q$.)*

PROOF OF THE THEOREM. As remarked in §2, the weak isomorphism class of $F$ does not depend on the choice of the basis. So we can choose $\omega_1,\ldots,\omega_r$ as a basis of $Z_{(p)}\mathfrak{O}_I$. Then

$$(5.1.2)\qquad \left(\omega_1{}^\sigma,\ldots,\omega_r{}^\sigma,\frac{1}{e}\,\mathrm{tr}_{k/k_I}(\omega_{r+1}^\sigma),\ldots,\frac{1}{e}\,\mathrm{tr}_{k/k_I}(\omega_n{}^\sigma)\right)=(\omega_1,\ldots,\omega_n)\left(\frac{1}{e}\sum_{\tau\in I_p}A_{\sigma\tau}\right).$$

All elements of the left side of (5.1.2) are in $k_I$, so that

$$\frac{1}{e}\sum A_{\sigma\tau}=\begin{pmatrix}A & B\\ 0 & 0\end{pmatrix},\ (\omega_1^{\sigma},\ldots,\omega_r^{\sigma})=(\omega_1,\ldots,\omega_r)A,\ A\in GL_r(Z_{(p)}).$$

Changing the basis by $\begin{pmatrix}I_r & A^{-1}B\\ 0 & I_{n-r}\end{pmatrix}$ we can write $(1/e)\sum A_{\sigma\tau}=\begin{pmatrix}A & 0\\ 0 & 0\end{pmatrix}$ and $U_r^{\sigma}=U_rA$, $(U_r=(\omega_i^{\tau_j}),\ i,j=1\sim r,\ \tau_j\in \mathrm{Gal}\,(KI/Q))$. Putting $U=\begin{pmatrix}U_r & 0\\ 0 & I_{n-r}\end{pmatrix}$ we obtain

$$\left(pI_n-\begin{pmatrix}I_r & 0\\ 0 & 0\end{pmatrix}T\right)U=U\left(pI_n-\begin{pmatrix}A & 0\\ 0 & 0\end{pmatrix}T\right)$$

(as an element of $M_n((\mathfrak{O}_I)\sigma[[T]])$ and $U^{-1}\in M_n(\mathfrak{O}_{I,\mathfrak{p}})$, for $p$ is unramified at $k_I/Q$. From [4] Theorem 3, $F$ is weakly isomorphic to $G_m{}^r\times G_a{}^{n-r}$. Q.E.D.

## References

[1] Artin, E., Algebraic numbers and algebraic functions I, Lecture Notes at Princeton Univ. and New York Univ. 1950-51.

[2] Dieudonné, J., Lie groups and Lie hyperalgebras over a field of characteristic $p>0$ (IV), Amer. J. Math. **77** (1955), 429-452.

[3] Honda, T., Formal groups and zeta functions, Osaka J. Math. **5** (1968), 199-213.

[4] Honda, T., On the theory of commutative formal groups, J. Math. Soc. Japan **22** (1970), 213-246.

(Received October 4, 1973)

Department of Mathematics
Faculty of Science
University of Tokyo
Hongo, Tokyo
113 Japan