83. *Group Rings and the Norm Groups*

By Shin-ichi KATAYAMA

Tokushima University

(Communicated by Shokichi IYANAGA, M. J. A., Nov. 12, 1993)

1. Introduction and preliminary lemmas. Let n be a natural number >1 and G be a cyclic group of order n generated by σ. We consider in this note the cyclic extension L/F of fields with the Galois group G. Let $a \in L^{\times}$. The well-known Hilbert theorem 90 asserts that $a^{1+\sigma+\cdots+\sigma^{n-1}}=1$ if and only if there exists $b \in L^{\times}$ such that $a=b^{1-\sigma}$. Now let t be an indeterminate and set $D_n=\{f(t) \in \boldsymbol{Z}[t] \mid f(t)$ divides $t^n-1\}$. For $f(t) \in D_n$, we shall denote $f^{\perp}(t)=(t^n-1)/f(t)$. Obviously one sees $f^{\perp}(t) \in D_n$ and $(f^{\perp})^{\perp}(t)=f(t)$. We define now:

(1. 1) $f(t) \in D_n$ is called of *H-type* if the following holds:
For any cyclic extension L/F and any $a \in L^{\times}$, $a^{f(\sigma)}=1$ if and only if there exists $b \in L^{\times}$ such that $a=b^{f^{\perp}(\sigma)}$.
If there is no fear of confusion, we shall abbreviate $f(t)$ or $f(\sigma)$ to f. It is obvious that $a=b^{f^{\perp}}$ implies $a^f=1$, so that the above definition can be simplified as follows:

(1.2) f is of *H-type,* if $a^{f(\sigma)}=1$ implies the existence of b with $a=b^{f^{\perp}(\sigma)}$.
$f=t^n-1$ is trivially of *H-type,* and Hilbert theorem 90 says that $f=1+t+\cdots+t^{n-1}$ is of *H-type.* W. Hürlimann [2] has proved an interesting result ("Cyclotomic Hilbert theorem 90") saying that the n-th cyclotomic polynomial $\Phi_n(t)$ is also of *H-type.*

The aim of this paper is to determine the set of all polynomials $(\in D_n)$ of *H-type,* which will be denoted with H_n. The result of [2] will be stated as

Lemma 1. $\Phi_n \in H_n$.
We denote the greatest common divisor and the least common multiple of f, $g \in \boldsymbol{Z}[t]$ by (f, g) and $\{f, g\}$, respectively. If $f, g \in D_n$ we have clearly $(f, g), \{f, g\} \in D_n$.

Lemma 2. *If $f, g \in D_n$ are of H-type, then (f, g) and $\{f, g\}$ are of H-type.*

Proof. We denote $f_0=(f, g)$ and $f=f_0f_1$, $g=f_0g_1$ and $t^n-1=f_0f_1g_1h$. We shall show $f_0=(f, g)$ is of *H-type.* For any $a \in L^{\times}$ such that $a^{f_0}=1$, one sees $a^f=1$. Since f is of *H-type,* there exists $b \in L^{\times}$ such that $a=b^{g_1h}$. Then $a^{f_0}=(b^h)^g=1$. Since, g is of *H-type,* there exists $c \in L^{\times}$ such that $b^h=c^{f_1h}$. Hence $a=(b^h)^{g_1}=c^{f_1g_1h}=c^{f_0^{\perp}}$. In the same way as above, one sees that $\{f, g\}$ is also of *H-type.*

For the case $m \mid n$, we define an injection $\pi_{n/m}$ from D_m to D_n by putting $\pi_{n/m}(f(t))=f(t^l)$, where $l=n/m$. We shall abbreviate $\pi_{n/m}(f(t))$ to

$\bar{f}(t)$ when no confusion is to fear. Then from the fact $(\bar{f})^{\perp} = (\overline{f^{\perp}})$, we have the following

Lemma 3. *If $f \in D_m$ is of H-type, then $\bar{f} = \pi_{n/m}(f) \in D_n$ is also of H-type.*

For a subset $\{h_1, h_2, \ldots, h_r\} \subset H_n$, $\langle h_1, h_2, \ldots, h_r\rangle$ will denote the set consisting of all the polynomials which are obtained by applying the operations $(\ ,\ )$, $\{\ ,\ \}$ on $h_1, h_2, \ldots, h_r$ finite number of times. From Lemma 2, one sees that $\langle h_1, h_2, \ldots, h_r\rangle$ is also a subset of H_n. H_n^0 will denote the set $\langle \pi_{n/d}(\Phi_d), (t^d - 1)^{\perp}\rangle$, where d runs over all $d \mid n$. Then, from Lemmas 1, 2, 3, we have $H_n^0 \subset H_n$ and the induction on the number of distinct prime factors of n yields the following proposition.

Proposition 1. *$f \in H_n^0$ if and only if f satisfies the following condition. If Φ_d divides f for some $d \mid n$, then for any d' such that $d \mid d' \mid n$, $\Phi_{d'}$ divides f.*

Our main theorem claims that $H_n^0 = H_n$.

2. A proposition on the norm group. In this section, we assume that n is a composite number and decomposes into $n = ml (m, l > 1)$ and fix l for a while. We denote the invariant field associated with $\langle \sigma^l \rangle$ by K. For any $f \in \boldsymbol{Z}[G]$, Ψ_f denotes the G-endomorphism of $L^{\times}$ defined by $\Psi_f(x) = x^{f(\sigma)}$ We denote by $q_l(t)$ (or briefly by $q(t)$) the polynomial $\Pi'_{d \mid l}\, \Phi_d(t)$. Then we have the following proposition.

Proposition 2. *With the above notation, we have*

$$Ker\ \Psi_q = \prod_{\lambda} K_{\lambda}^{\times},$$

where K_λ runs over all the maximal subfields contained in K.

Without loss of generality, we may assume $l = p_1 \cdots p_r$, where $p_1, \cdots p_r$ are distinct primes. Let l_j be the number l/p_j and K_j be the intermediate fields corresponding to $\langle \sigma^{l_j} \rangle$. Then the maximal subfields contained in K are $K_1, \ldots, K_r$. When $r = 1$, we have $q(t) = t - 1$ and $K_1 = F$ and the above proposition is obvious. Next, we recall the following elementary fact.

If $(a, b) = c$, using an analogy of the Euclidean algorithm, we see that there exist $h'(t), g'(t) \in \boldsymbol{Z}[t]$ such that

$$\left(\frac{t^a - 1}{t - 1}\right) h'(t) + \left(\frac{t^b - 1}{t - 1}\right) g'(t) = \frac{t^c - 1}{t - 1}.$$

From this fact, one can prove the following lemma using the induction on $r \geq 2$.

Lemma 4. *Let $g_i(t)$ be the polynomial $q(t)/(t^{l_i} - 1) \in D_n (1 \leq i \leq r)$. Then there exist $h_i(t) \in \boldsymbol{Z}[t]$ such that*

$$\sum_{i=1}^{r} g_i(t) h_i(t) = 1\ (r \geq 2).$$

Proof. When $r = 2$, we have $l = p_1 p_2$, $g_1(t) = \Phi_{p_1}(t) = \dfrac{t^{p_1} - 1}{t - 1}$, $g_2(t) = \Phi_{p_2}(t) = \dfrac{t^{p_2} - 1}{t - 1}$, so that there exist $h_1(t), h_2(t) \in \boldsymbol{Z}[t]$ such that $h_1 g_1 + h_2 g_2 = 1$ by the above remark.

Next, assume that the lemma holds for the case $r - 1 \geq 2$, so that for $l_r = p_1 \cdots p_{r-1}$, there exist $h_1(t), \ldots, h_{r-1}(t)$ with

$$\sum_{i=1}^{r-1} \frac{t^{l_r}-1}{\Phi_{l_r}(t)(t^{l_r/p_i}-1)} h_i(t) = 1.$$

Substituting t to t^{p_r}, we obtain

$$\sum_{i=1}^{r-1} \frac{t^{l}-1}{\Phi_{l_r}(t^{p_r})(t^{l_i}-1)} h_i(t^{p_r}) = 1.$$

Since $\Phi_{l_r}(t^{p_r}) = \Phi_l(t)\Phi_{l_r}(t)$, we obtain

$$\sum_{i=1}^{r-1} g_i(t) h_i(t^{p_r}) = \Phi_{l_r}(t).$$

Putting $h_{ir}(t) = \dfrac{h_i(t^{p_r})(t^{l_r}-1)}{\Phi_{l_r}(t)(t-1)} \in \boldsymbol{Z}[t]$, we have

$$\sum_{i=1}^{r-1} g_i(t) h_{ir}(t) = \frac{t^{l_r}-1}{t-1}.$$

In the same way as above, for any l_j, there exist $h_{ij}(t) \in \boldsymbol{Z}[t]$ such that $\sum g_i(t)h_{ij}(t) = \dfrac{t^{l_j}-1}{t-1}$. Since $(l_1, \ldots, l_r) = 1$, one can choose $h_i(t) \in \boldsymbol{Z}[t]$ such that

$$\sum_{i=1}^{r} g_i(t) h_i(t) = 1.$$

Now we shall prove Proposition 2 for the case $r \geq 2$. From the fact $(t^{l_i}-1) \mid q(t)$, it is obvious that $Ker\, \Psi_q \supset \Pi_{i=1}^{r} K_i^{\times}$. Conversely if $x \in Ker\, \Psi_q$, put $x_i = x^{g_i(\sigma)}$ $(1 \leq i \leq r)$. Then $x_i^{\sigma^{l_i}-1} = x^{q(\sigma)} = 1$. Hence we have $x_i \in K_i^{\times}$. From Lemma 4, there exist $h_i(t) \in \boldsymbol{Z}[t]$ such that $\sum g_i(t)h_i(t) = 1$. Hence we have

$$x = x^{\Sigma g_i(\sigma)h_i(\sigma)} = \prod_{i=1}^{r} x_i^{h_i(\sigma)} \in \prod_{i=1}^{r} K_i^{\times},$$

which completes the proof of Proposition 2.

Lemma 5. *Let A be an elementary abelian group $(\boldsymbol{Z}/m\boldsymbol{Z})^l$ and A_i be the subgroup $\{(x_1,\ldots,x_l) \mid x_j = x_k \in \boldsymbol{Z}/m\boldsymbol{Z}$ when $j \equiv k \bmod l_i\}$. A_0 denotes the subgroup generated by $A_1,\ldots,A_r$. Then we have $A_0 \neq A$.*

Proof. Let A' be $\boldsymbol{Z}^l$ and A'_i be the subgroup $\{(x_1,\ldots,x_l) \mid x_j = x_k \in \boldsymbol{Z}$ when $j \equiv k \bmod l_i\}$. A'_0 will denote the subgroup generated by $A'_1, \ldots, A'_r$. Then the $rank_{\boldsymbol{Z}} A'_0 = rank\, M'$. Here M' is the following matrix of $(l_1 + \cdots + l_r,\ l)$-type.

$$M' = \begin{bmatrix} E_{l_1} & \cdots & E_{l_1} \\ E_{l_2} & \cdots & E_{l_2} \\ \vdots & \cdots & \vdots \\ E_{l_r} & \cdots & E_{l_r} \end{bmatrix}, \text{ were } E_{l_i} \text{ is the } l_i \times l_i \text{ unit matrix.}$$

If $rank\, M' < l$, then it is obvious that $A'_0 \neq A'$. So we may consider only the case $l_1 + \cdots + l_r \geq l$. One can take l suitable row vectors $v_1,\ldots,v_l$ of M' such that the $l \times l$ matrix $T' = \begin{bmatrix} v_1 \\ \vdots \\ v_l \end{bmatrix}$ has the same rank $rank\, T' = rank\, M'$. Let ζ be the primitive l-th root of 1. Then one sees

$$T'\begin{pmatrix}1\\ \zeta\\ \vdots\\ \zeta^{l-1}\end{pmatrix}=\begin{pmatrix}0\\ 0\\ \vdots\\ 0\end{pmatrix}.$$

Hence the determinant $|T'|=0$. Therefore, we get $rank\ M' = rank\ T' < l$. Finally, similar argument modulo m implies $rank_{\mathbf{Z}/m\mathbf{Z}}A_0 < rank_{\mathbf{Z}/m\mathbf{Z}}A = l$, which completes the proof.

Proposition 3. *With the above notation, we have*

(i) *If L is an unramified local number field, $K^\times = (\Pi_\lambda K_\lambda^\times)\ N_{L/K}L^\times$, where K_λ runs over all the maximal subfields of K.*

(ii) *If L is a global number field, $K^\times/(\Pi_\lambda K_\lambda^\times)\ N_{L/K}L^\times$ is an infinite abelian group, where K_λ runs over all the maximal subfields of K.*

Sketch of proof. From local class field theory, one can easily verify the result (i). Let v be a place of F which is extended to l distinct places $v(K)$ in K and every $v(K)$ is inert in L/K. We denote the l extensions of v to L by $v(L)$ and the restrictions of $v(K)$ to K_λ by $v(K_\lambda)$. We note that Chebotarev's density theorem assures the existance of infinitely many places $v \in F$ which satisfy the above conditions. We denote the completions of F, K_λ, K, L by F_v, $(K_\lambda)_{v(K_\lambda)}$, $K_{v(K)}$, $L_{v(L)}$. We abbreviate

$$\prod_{v(K_\lambda)|v}(K_\lambda)^\times_{v(K_\lambda)},\ \prod_{v(K)|v}K^\times_{v(K)},\ \prod_{v(L)|v}L^\times_{v(L)}$$

to $(K_\lambda)_v^\times$, $K_v^\times$, $L_v^\times$. Then, from local class field theory, we have $K_v^\times/(\Pi_\lambda (K_\lambda)_v^\times)\ N_{L/K}L_v^\times \cong A/A_0$, where A, A_0 are those in the above lemma. Hence $K_v^\times \neq (\Pi_\lambda(K_\lambda)_v^\times)\ N_{L/K}L_v^\times$. Therefore the idele groups $K_A^\times$, $(K_\lambda)_A^\times$, $L_A^\times$ satisfies $K_A^\times \neq (\Pi_\lambda(K_\lambda)_A^\times)\ N_{L/K}L_A^\times$ and more precisely $K_A^\times/(\Pi_\lambda(K_\lambda)_A^\times)\ N_{L/K}L_A^\times$ is an infinite abelian group. Combining global class field theory and Hasse's norm theorem, one obtains that $K^\times/(\Pi_\lambda K_\lambda^\times)\ N_{L/K}L^\times$ is an infinite abelian group.

3. Proof of the main theorem. Suppose f is of *H-type* and $f \notin H_0$. Then one can choose a *H-type* polynomial $g \in \langle f, H_0\rangle (\notin H_0)$ such as $g(t) = \Phi_l(t)\ (1 < l < n)$ or $g(t) = (t^l-1)^\perp \Phi_{l_1}(t)$, where $l = l_1p_1$ (p_1 is prime).

First consider the case $g = \Phi_l$. From the assumption that g is of *H-type*, we have $Ker\Psi_g = (L^x)^{g^\perp(\sigma)}$. Since $g^\perp(\sigma) = q_l(\sigma)(\sigma^l-1)^\perp$, we have $x^{g^\perp(\sigma)} = (N_{L/K}\,x)^{q_l(\sigma)}$ for any $x \in L^\times$. Hence we have the equality $Ker\Psi_g = (L^\times)^{g^\perp(\sigma)} = (N_{L/K}L^\times)^{q_l(\sigma)}$

On the other hand, from the fact $g(t) \mid (t^l-1)$, we have $Ker\Psi_g \subset K^\times$. Hence, from Lemma 1, we have $Ker\Psi_g = \{x \in K^\times \mid x^{g(\sigma)} = 1\} = (K^\times)^{q_l(\sigma)}$. Hence we have the equality $(N_{L/K}L^\times)^{q_l(\sigma)} = (K^\times)^{q_l(\sigma)}$. Hence, from Proposition 2, we have $K^\times = (\Pi_\lambda K_\lambda^\times)\ N_{L/K}L^\times$, where K_λ runs over all the maximal subfields of K, which contradicts Proposition 3.

Next consider the case $g(t) = (t^l-1)^\perp \Phi_{l_1}(t)$ is of *H-type*. Then $g^\perp(t) = (t^l-1)/\Phi_{l_1}(t)$. From the assumption that $g(t)$ is of *H-type*, we have $Ker\Psi_g = (L^\times)^{g^\perp(\sigma)}$

On the other hand, from the fact that $x^{g(\sigma)} = N_{L/K}(x^{\Phi_{l_1}(\sigma)})$ and Hilbert theorem 90, there exists $y \in L^\times$ which satisfies $x^{\Phi_{l_1}(\sigma)} = y^{\sigma^l-1} = (y^{g^\perp(\sigma)})^{\Phi_{l_1}(\sigma)}$

for any $x \in Ker\Psi_g$. Then $x/y^{g^{\perp}(\sigma)} \in K_1^{\times}$, where K_1 is the invariant fields associated with $\langle \sigma^{l_1} \rangle$. Since $(x/y^{g^{\perp}(\sigma)})^{\Phi_{l_1}(\sigma)} = 1$, there exists $z \in K_1^{\times}$ such that $x = y^{g^{\perp}(\sigma)} z^{q_{l_1}(\sigma)}$ from Lemma 1. Conversely, if $x = y^{g^{\perp}(\sigma)} z^{q_{l_1}(\sigma)}$ for some $y \in L^{\times}$ and $z \in K_1^{\times}$ then one sees $x \in Ker\Psi_g$. Hence we have shown $Ker\Psi_g = (L^{\times})^{g^{\perp}(\sigma)} (K_1^{\times})^{q_{l_1}(\sigma)}$. Hence we have $(K_1^{\times})^{q_{l_1}(\sigma)} \subset (L^{\times})^{g^{\perp}(\sigma)}$, that is, for any $z \in K_1^{\times}$, there exists $y \in L^{\times}$ such that $z^{q_{l_1}(\sigma)} = y^{g^{\perp}(\sigma)}$. Since $y^{\sigma^l - 1} = (z^{q_{l_1}(\sigma)})^{\Phi_{l_1}(\sigma)} = z^{\sigma^{l_1} - 1} = 1$, we have $y \in K^{\times}$.

Conversely for any $y \in K^{\times}$, $y^{g^{\perp}(\sigma)} = (N_{K/K_1} y)^{q_{l_1}(\sigma)} \in (K_1^{\times})^{q_{l_1}(\sigma)}$. Hence we have shown $(K_1^{\times})^{q_{l_1}(\sigma)} = (N_{K/K_1} K^{\times})^{q_{l_1}(\sigma)}$.

From Proposition 2, we have $K_1^{\times} = (\Pi_{\lambda'} K_{\lambda'}^{\times})\, N_{K/K_1} K^{\times}$, where $K_{\lambda'}$ runs over all the maximal subfields of $K_1^{\times}$, which contradicts Proposition 3. Therefore we have shown the following theorem

Theorem. *With the above notation, we have H_n^0.*

Acknowledgement. I would express my heartly thanks to the referee for his many useful suggestions improving my first manuscript.

References

[1] S. Endo and T. Miyata: Quasi-permutation modules over finite groups. J. Math. Soc. Japan, **25**, 397–421 (1973).

[2] W. Hürlimann: A cyclotomic Hilbert 90 theorem. Arch. Math., **43**, 25–26 (1984).

[3] S. Iyanaga (ed.): The Theory of Numbers. North Holland, American Elsevier, New York (1975).