Kumamoto J. Sci. (Math.)
9 (1972), 33-40

ON THE RANK OF THE p-DIVISOR CLASS GROUP OF GALOIS EXTENSIONS OF ALGEBRAIC NUMBER FIELDS

Sunao YAMAMOTO

(Received December 2, 1971)

Let p and k be a prime number and an algebraic number field. Let K/k be a finite Galois extension which contains a primitive p-th root ζ_p of unity and we denote the Galois group of K/k by G. Corresponding to the decomposition of the group ring $Z_p[G]$ of G over the ring Z_p of p-adic integers into the direct sum of non-zero indecomposable two-sided ideals B called blocks: $Z_p[G]=\sum_B B$, the unity of G is decomposed into the sum of orthogonal primitive central idempotents η_B: $1=\sum_B \eta_B$. For any multiplicative abelian $Z_p[G]$-group A, we have its decomposition into a direct product:

(*) $$A=\prod_B A_B, \qquad A_B=A^{\eta_B}.$$

When we take as A the p-divisor class group and the unit p-class group of K, the results in [8], [7], so-called "Spiegelungssatz", will be able to be generalized to the case the order of G is divisible by p (Theorem 1). In case p is odd and K is the cyclotomic field of p^{n+1}-th roots of unity over the rational field Q, (*) becomes the Iwasawa's Δ-decomposition ([4]). In this case we shall obtain some more detailed results (Theorem 2, Theorem 3).

§1. Spiegelungssatz.

For any absolutely irreducible character χ of G in the algebraic closure of the p-adic number field Q_p, we put

$$\eta_\chi=\frac{\chi(1)}{\sharp G}\sum_{\sigma\in G}\chi(\sigma^{-1})\sigma.$$

Then η_B is a sum of several idempotents η_χ. Namely when $\eta_\chi\eta_B=\eta_\chi$, we denote $\chi\in B$ and then

$$\eta_B=\sum_{\chi\in B}\eta_\chi.$$

Next we define the linear character χ^* of G by

$$\zeta_p^\sigma=\zeta_p^{\chi^*(\sigma)} \qquad \text{for } \sigma\in G,$$

where $\chi^*(\sigma)$ is a $(p-1)$-th root of unity contained in Z_p. Moreover for any χ we put

$$\bar{\chi}(\sigma)=\chi^*(\sigma)\chi(\sigma^{-1}) \qquad \text{for } \sigma\in G.$$

Then $\bar{\chi}$ is also an absolutely irreducible character of G and $\bar{\bar{\chi}}=\chi$. For each block B, $\sum_{\chi\in B}\eta_{\bar{\chi}}$ becomes an orthogonal primitive central idempotent of $Z_p[G]$ and therefore defines a block $\bar{B}$ such that

$$\bar{B}=Z_p[G]\eta_{\bar{B}}, \qquad \eta_{\bar{B}}=\sum_{\chi\in B}\eta_{\bar{\chi}}, \qquad \bar{\bar{B}}=B.$$

Let D be the divisor group of K and H be its subgroup of all $\mathfrak{c}$ such that $\mathfrak{c}^m$ is principal for some exponent m prime to p. We denote the p-divisor class group of K by $\mathfrak{D}=D/H$. Then $\mathfrak{D}$ is a $Z_p[G]$-group. The class field N/K corresponding to H is an unramified abelian extension and N/k is a Galois extension. Let $\mathfrak{G}$ be the Galois group of N/k and $\mathfrak{A}$ be its abelian p-subgroup corresponding to K. Then

$$\mathfrak{G}/\mathfrak{A}\cong G, \qquad \mathfrak{G}=\bigcup_{\sigma\in G}\mathfrak{A}S_\sigma, \qquad S_\sigma|_K=\sigma,$$

and $\mathfrak{A}$ becomes a $Z_p[G]$-group defined by

$$S_\sigma^{-1}\alpha S_\sigma=\alpha^\sigma \qquad \text{for } \alpha\in\mathfrak{A},\ \sigma\in G.$$

By Artin's isomorphism theorem, we have a $Z_p[G]$-isomorphism:

$$\mathfrak{D}\cong\mathfrak{A}\ ;\ \mathfrak{k}\to\left(\frac{N/K}{\mathfrak{k}}\right).$$

Hence we obtain the decompositions (*) of $\mathfrak{D}$ and $\mathfrak{A}$ such that

$$\mathfrak{D}=\prod_B\mathfrak{D}_B, \qquad \mathfrak{A}=\prod_B\mathfrak{A}_B, \qquad \mathfrak{D}_B\cong\mathfrak{A}_B.$$

Let $\tilde{N}/K$ be the subextension of N/K corresponding to the subgroup $\mathfrak{A}^p$ of $\mathfrak{A}$. Then we can identify the Galois group $\tilde{\mathfrak{A}}$ of $\tilde{N}/K$ with $\mathfrak{A}/\mathfrak{A}^p$ as $Z_p[G]$-groups. By the assumption $\zeta_p\in K$, $\tilde{N}/K$ becomes a Kummer extension such that

$$\tilde{N}=K(W), \qquad W=\{\tilde{N}\ni\omega\neq 0\ ;\ \omega^p\in K\}.$$

The radical class group $\mathfrak{W}=W/K^\times$ of $\tilde{N}/K$ becomes a $Z_p[G]$-group defined by

$$\bar{\omega}^\sigma=\overline{\omega^{S_\sigma}} \qquad \text{for } \omega\in W, \sigma\in G.$$

Now we put

$$\omega^{\alpha}=\chi_{\omega}(\alpha)\omega \qquad \text{for } \omega\in W, \alpha\in\mathfrak{A},$$

where $\chi_{\omega}(\alpha)$ is a p-th root of unity independent on the choices of representatives of $\bar{\omega}\in\mathfrak{W}$ and $\bar{\alpha}\in\tilde{\mathfrak{A}}$. Therefore $\chi_{\bar{\omega}}$ defined by $\chi_{\bar{\omega}}(\bar{\alpha})=\chi_{\omega}(\alpha)$ belongs to the character group $\tilde{\mathfrak{A}}^*$ of $\tilde{\mathfrak{A}}$. Then we have an isomorphism:

$$\mathfrak{W}\cong\tilde{\mathfrak{A}}^*;\ \bar{\omega}\to\chi_{\bar{\omega}}.$$

LEMMA 1. *In the decompositions* (*) *of* $Z_p[G]$*-group* $\tilde{\mathfrak{A}}$ *and* $\mathfrak{W}$, $\tilde{\mathfrak{A}}_B$ *is isomorphic with* $\mathfrak{W}_{\bar{B}}$ *for each block* B.

PROOF. For $\omega\in W, \alpha\in\mathfrak{A}, \sigma\in G$

$$\omega\alpha^{\sigma}=\omega^{S_{\sigma}^{-1}\alpha S_{\sigma}}=(\chi_{\omega^{S_{\sigma}^{-1}}}(\alpha)\omega^{S_{\sigma}^{-1}})^{S_{\sigma}}=\chi_{\omega^{S_{\sigma}^{-1}}}(\alpha)^{\chi^*(\sigma)}\omega.$$

Hence by the definition of $\chi_{\bar{\omega}}$,

$$\chi_{\bar{\omega}}(\bar{\alpha}^{\sigma})=\chi_{\bar{\omega}^{\chi^*(\sigma)\sigma^{-1}}}(\bar{\alpha}) \qquad \text{for } \bar{\omega}\in\mathfrak{W},\ \bar{\alpha}\in\tilde{\mathfrak{A}},\ \sigma\in G.$$

For each block B if we put

$$\eta_B=\sum_{\sigma\in G}a_{\sigma}\sigma, \qquad a_{\sigma}=\frac{1}{\sharp G}\sum_{\chi\in B}\chi(1)\chi(\sigma^{-1})\in Z_p,$$

then

$$\eta_{\bar{B}}=\sum_{\sigma\in G}a_{\sigma}\chi^*(\sigma)\sigma^{-1}.$$

Hence it follows that

$$\chi_{\bar{\omega}}(\bar{\alpha}^{\eta_B})=\chi_{\bar{\omega}^{\eta_{\bar{B}}}}(\bar{\alpha}).$$

Therefore we have

$$\tilde{\mathfrak{A}}_B\cong\mathfrak{W}/\prod_{B'\neq\bar{B}}\mathfrak{W}_{B'}\cong\mathfrak{W}_{\bar{B}}.$$

Let $\mathfrak{C}$ be the p-Sylow subgroup of the divisor class group of K. Then $\mathfrak{C}$ is a $Z_p[G]$-group and is naturally $Z_p[G]$-isomorphic with $\mathfrak{D}$. Similarly the subgroup $\tilde{\mathfrak{C}}$ of $\mathfrak{C}$ generated by all elements of order p is a $Z_p[G]$-group and we have a natural $Z_p[G]$-isomorphism:

$$\tilde{\mathfrak{C}}\cong\tilde{\mathfrak{D}}=\mathfrak{D}/\mathfrak{D}^p.$$

Therefore by Lemma 1, for each block B

$$\tilde{\mathfrak{C}}_B\cong\tilde{\mathfrak{D}}_B\cong\tilde{\mathfrak{A}}_B\cong\mathfrak{W}_{\bar{B}}.$$

On the other hand, since $K(\omega)/K$ is unramified for $\omega\in W$, there is some $c\in D$

such that

$$(\omega)=\mathfrak{c} \text{ in } \tilde{N}, \quad \bar{\mathfrak{c}}\in\tilde{\mathfrak{C}}.$$

We define a $Z_p[G]$-homomorphism φ of $\mathfrak{W}$ into $\tilde{\mathfrak{C}}$ by

$$\varphi:\ \mathfrak{W}\to\tilde{\mathfrak{C}}\ ;\ \bar{\omega}\to\bar{\mathfrak{c}}.$$

For each element $\bar{\omega}_0$ in the kernel $\mathfrak{W}_0$ of φ, there is some $x\in K$ such that $(\omega_0)=(x)$ in $\tilde{N}$ and hence $\omega_0 x^{-1}$ is a unit in $\tilde{N}$. Therefore $\varepsilon=(\omega_0 x^{-1})^p$ is a unit in K and

$$\bar{\omega}_0=\overline{\sqrt[p]{\varepsilon}}, \quad \sqrt[p]{\varepsilon}\in W.$$

Now let E denote the unit group of K and E_0 denote its subgroup of all ε such that $\sqrt[p]{\varepsilon}\in W$. Then both E and E_0 are G-groups and also all the unit p-class group $\mathfrak{E}=E/E^p$, its subgroup $\mathfrak{E}_0=E_0/E^p$ and $\mathfrak{W}_0$ become $Z_p[G]$-groups. Moreover from the above argument we have $Z_p[G]$-isomorphisms:

$$\mathfrak{W}_0\cong\mathfrak{E}_0, \quad \mathfrak{W}/\mathfrak{W}_0\cong\varphi(\mathfrak{W})\subset\tilde{\mathfrak{C}}.$$

Hence in the decompositions (*) of $\mathfrak{W}_0$ and $\mathfrak{E}_0$,

$$\mathfrak{W}_{0B}\cong\mathfrak{E}_{0B}, \qquad \mathfrak{W}_B/\mathfrak{W}_{0B}\cong\varphi(\mathfrak{W}_B)\subset\tilde{\mathfrak{C}}_B.$$

Therefore we obtain the following theorem.

THEOREM 1. *For each block B let e_B and δ_B denote the ranks of $\mathfrak{T}_B$ and $\mathfrak{E}_{0B}$, respectively. Then we have*

$$e_B-\delta_{\bar{B}}\leqq e_{\bar{B}}\leqq e_B+\delta_B.$$

When the order of G is prime to p, this theorem is shown in [8], [7].

REMARK. In particular we consider the case p is odd and k is the rational field Q and the maximal real subfield K^+ of K is a Galois extension of Q with the subgroup $G^+=\{1,\sigma_\infty\}$. Then σ_∞ belongs to the center of G and hence in $Z_p[G]$ we obtain a decomposition of the unity into a sum of two orthogonal central idempotents:

$$1=\frac{1+\sigma_\infty}{2}+\frac{1-\sigma_\infty}{2}.$$

Each η_B is a summand of either $\frac{1+\sigma_\infty}{2}$ or $\frac{1-\sigma_\infty}{2}$, and we call a block B even in the former case and odd in the latter. Then immediately it follows that

$$B:\text{ even}\rightleftarrows\bar{B}:\text{ odd}.$$

Let $\mathfrak{D}^+$ denote the p-divisor class group of K^+. Then $\mathfrak{D}^+$ is a $Z_p[G]$-group and clearly

$$\mathfrak{D}^+=\prod_{B:\text{ even}} \mathfrak{D}_B^+, \qquad \mathfrak{D}_B^+ \cong \mathfrak{D}_B \quad \text{for each even block } B.$$

§2. Cyclotomic fields.

Let p be odd and k be the rational field Q and K be the cyclotomic field $Q(\zeta)$ obtained by adjoining a primitive p^{n+1}-th root ζ of unity. In this case, the Galois group G of K/Q is the direct product of the cyclic group G_0 of order $p-1$ and the cyclic group P of order p^n:

$$G=G_0\times P, \qquad G_0=\langle\rho\rangle, \qquad P=\langle\pi\rangle,$$

where ρ and π are generators of G_0 and P, respectively. Then the order of χ^* is equal to $p-1$. The number of blocks of $Z_p[G]$ is $p-1$ and

$$\eta_B=\frac{1}{p-1}\sum_{t=0}^{p-2}\chi^{*i}(\rho^{-t})\rho^t \quad \text{when } \chi^{*i}\in B.$$

By the definition of $\bar{B}$,

$$\chi^{*i}\in B \rightleftarrows \chi^{*j}\in\bar{B} \qquad \text{when } i+j=p.$$

When $\chi^{*i}\in B$, we denote η_B by η_i and A_B by A_i in the decomposition $(*)$.

Now, between unit groups of K and $K^+=Q(\zeta+\zeta^{-1})$ the following relation holds.

LEMMA 2. *Let E^+ denote the unit group of K^+ and $E_0^+=E_0\cap E^+$. Then we have*

$$E_0=E_0^+E^p.$$

PROOF. In the case of $n=0$, this lemma is shown in [9]. For general case too, it can be proved in the same manner. Namely for each unit ε in E_0 there is some $x\in K$ prime to $\mathfrak{p}=(1-\zeta)$ such that $\varepsilon\equiv x^p \pmod{\mathfrak{p}^{p^n+1}}$. Hence

$$\varepsilon-\varepsilon^p\equiv x^p(1-x^{p(p-1)})\equiv 0 \pmod{\mathfrak{p}^p}.$$

We can put $\varepsilon=\zeta^g\varepsilon^+$ for $\varepsilon^+\in E^+$, and then

$$\varepsilon-\varepsilon^p=\zeta^g\varepsilon^+(1-\zeta^{g(p-1)})+\zeta^{gp}\varepsilon^+(1-\varepsilon^{+p-1}).$$

Since ε^+ is real, $1-\varepsilon^{+p-1}\equiv 0 \pmod{\mathfrak{p}^2}$. Hence $1-\zeta^{g(p-1)}\equiv 0 \pmod{\mathfrak{p}^2}$ and then $g\equiv 0 \pmod{p}$. Therefore ε^+ is contained in E_0. This completes the proof of our lemma.

From Lemma 2 it follows that $\mathfrak{E}_0=E_0^+E^p/E^p$. In the decomposition (*) of $\mathfrak{E}_0$:

$$\mathfrak{E}_0=\prod_{i=1}^{p-1}\mathfrak{E}_{0_i},\qquad \mathfrak{E}_{0_i}=\mathfrak{E}_0^{\eta_i},$$

since units in E_0^+ are invariant under σ_∞ and $\eta_i\sigma_\infty=(-1)^i\eta_i$, then we have $\mathfrak{E}_{0_i}=1$ for all odd i. Therefore by Theorem 1 the following theorem is obtained.

THEOREM 2. *In the cyclotomic field of p^{n+1}-th roots of unity over Q, let e_i and δ_i denote the ranks of the i-components $\mathfrak{D}_i$ of $\mathfrak{D}$ and $\mathfrak{E}_{0_i}$ of $\mathfrak{E}_0$, respectively. Then we have*

$$\delta_i=0,\qquad e_j\leqq e_i\leqq e_j+\delta_j \qquad \textit{when } i \textit{ is odd and } i+j=p.$$

Let e^+ be the rank of the p-divisor class group $\mathfrak{E}^+$ of K^+. Then by the remark of the previous section,

$$e^+=\sum_{j:\text{even}} e_j.$$

From now on, we assume that the class number h^+ of K^+ is prime to p. This assumption holds for all n if it holds for $n=0$ ([3]). Then it follows that $e_j=0$ for all even j. But since representatives of the basis of $\mathfrak{E}_0$ give independent unramified Kummer extensions of K of degree p, by Theorem 2

$$e_i=\delta_j \qquad \text{when } i \text{ is odd and } i+j=p.$$

Let T denote the G-subgroup of E^+ generated by a circular unit T_0:

$$T_0=\sqrt{\frac{(1-\zeta^r)(1-\zeta^{-r})}{(1-\zeta)(1-\zeta^{-1})}},\qquad r\equiv\chi^*(\rho) \pmod{p}.$$

Then from the class number formula for K^+ ([2], [5]), h^+ is given by a group index: $h^+=[E^+:T]$. Therefore under $(h^+,p)=1$,

$$\mathfrak{E}=\mathfrak{E}_1\times E^+E^p/E^p=\mathfrak{E}_1\times TE^p/E^p,\quad \mathfrak{E}_1=\mathfrak{E}^{\eta_1}=\langle\zeta\rangle E^p/E^p,$$

where $\mathfrak{E}$ is a p-elementary abelian group of the rank $\frac{p-1}{2}p^n$ and $\mathfrak{E}_j$ for even $j\neq p-1$ is generated by $(T_0E^p)^{\eta_j\pi^s}$ $(s=0,1,\cdots,p^n-1)$ and $\mathfrak{E}_{p-1}$ is generated by $(T_0E^p)^{\eta_{p-1}\pi^s}$ $(s=0,1,\cdots,p^n-2)$. Therefore

$$\text{the rank of } \mathfrak{E}_j=\begin{cases} p^n & \text{for even } j\neq p-1.\\ p^n-1 & \text{for } j=p-1.\end{cases}$$

On the other hand, since

$$\mathfrak{E}_0 \subset \prod_{j:\mathrm{even}} \mathfrak{E}_j = TE^p/E^p,$$

finally we have

$$\delta_j \leqq \begin{cases} p^n & \text{for even } j \neq p-1. \\ p^n - 1 & \text{for } j = p-1. \end{cases}$$

Particularly in the case of $n=0$,

$\delta_{p-1}=0, \quad 0 \leqq \delta_j \leqq 1, \quad \delta_j = 1 \rightleftarrows (T_0 E^p)^{\eta_j} \in \mathfrak{E}_0$ for even $j \neq p-1$.

Making use of the method in [1], we can estimate $(T_0E^p)^{\eta_j}$ and obtain the following lemma.

LEMMA 3. *In the cyclotomic field of p-th roots of unity over Q, $(T_0E^p)^{\eta_j}$ is in $\mathfrak{E}_0$ if and only if the Bernoulli number B_j is divisible by p for $j=2,4,\cdots,p-3$.*

From this lemma, it follows immediately that:

THEOREM 3. *In the cyclotomic field of p-th roots of unity over Q under the assumption $(h^+,p)=1$, the rank e_i of the i-component $\mathfrak{D}_i$ of the p-divisor class group $\mathfrak{D}$ is given by*

$$e_1 = 0, \qquad 0 \leqq e_i \leqq 1 \qquad \text{for } i=3,5,\cdots,p-2.$$

Moreover $e_i=1$ if and only if the Bernoulli number B_j is divisible by p for even $j \leqq p-3$ such that $i+j=p$.

REMARK. For all $p \leqq 4001$, it is known ([6]) that in the cyclotomic field of p^{n+1}-th roots of unity over Q, the assumption $(h^+, p)=1$ is satisfied and when B_j is divisible by p, then $\mathfrak{D}_i$ becomes a cyclic group of order p^{n+1}.

References

[1] Z. I. Borevich and I. R. Shafarevich, Number Theory, New York and London, 1966.

[2] H. Hasse, Über die Klassenzahl abelscher Zahlkörper, Berlin, 1952.

[3] K. Iwasawa, *A note on class numbers of algebraic number fields,* Abh. Math. Sem. Univ. Hamburg, **20**(1956), 257–258.

[4] K. Iwasawa, *On the theory of cyclotomic fields,* Ann. of Math., **70**(1959), 530–561.

[5] K. Iwasawa, *A class number formula for cyclotomic fields,* Ann. of Math., **76**(1962), 171–179.

[6] K. Iwasawa and C. C. Sims, *Computation of invariants in the theory of cyclotomic fields,* J. Math. Soc. Japan, **18**(1966), 86–96.

[7] S. -N. Kuroda, *Über den allgemeinen Spiegelungssatz für Galoissche Zahlkörper,* J. Number Theory, **2**(1970), 282–297.

[8] H. W. Leopoldt, *Zur Struktur der l-Klassengruppe galoisscher Zahlkörper,* J. reine angew. Math., **199**(1958), 165–174.

[9] K. Shiratani, *Bemerkung zur Theorie der Kreiskörper*, Memoirs of Scie., Kyushu Univ., **18**(1964), 121-126.

Department of Mathematics,
Faculty of Science,
Kumamoto University