A NOTE ON IDEAL CLASS GROUPS

KENKICHI IWASAWA*

To the memory of TADASI NAKAYAMA

In the first part of the present paper, we shall make some simple observations on the ideal class groups of algebraic number fields, following the group-theoretical method of Tschebotarew[1]. The applications on cyclotomic fields (Theorems 5, 6) may be of some interest. In the last section, we shall give a proof to a theorem of Kummer on the ideal class group of a cyclotomic field.

1. For any prime numbers p and q, let

$$\begin{aligned} d(q, p) &= 2, && \text{for } p = q, \\ &= \text{the order of } p \bmod q, && \text{for } p \neq q. \end{aligned}$$

For any integer $n \geq 1$, we then define

$$d(n, p) = \text{the minimum of } d(q, p) \text{ for all prime factors } q \text{ of } n.$$

THEOREM 1. *Let G be a finite group of order n. Let M be a G-module over the prime field P with p elements, and let d be the dimension of M over P. Suppose that the action of G on M is non-trivial. Then*

$$d \geqq d(n, p).$$

Proof. Let σ be an element with minimal order in G such that the action of σ on M is non-trivial. Let q be a prime dividing the order of σ. Put $H = G_1/G_2$, where G_1 and G_2 denote the subgroups of G generated by σ and σ^q respectively. Then M is also an H-module over P, and the action of H on M is non-trivial. If $q = p$, we see immediately that $d \geqq 2 = d(p, p)$. Suppose that $q \neq p$. Then M is completely reducible, and it has an irreducible submodule on

Received June 7, 1965.

* The present research was supported in part by the National Science Foundation grant GP-4361.

[1] N. Tschebotarew, Zur Gruppentheorie des Klassenkörpers, J reine u. angew. Math., **161** (1929), pp. 179–183.

https://doi.org/10.1017/S0027763000012046 Published online by Cambridge University Press

which the action of H is again non-trivial. As is well-known, such an irreducible submodule is obtained by decomposing $P[H]$, the group ring of H over P. Let $\mathfrak{o}$ denote the maximal order of the cyclotomic field of q-th roots of unity. Identifying H with the group of q-th roots of unity in $\mathfrak{o}$, we may consider the $\mathfrak{o}$-module $\mathfrak{o}/p\mathfrak{o}$ as an H-module over P. We then see easily that

$$\begin{aligned} P[H] &\cong P \oplus (\mathfrak{o}/p\mathfrak{o}) \\ &\cong P \oplus \sum_{i=1}^{g} (\mathfrak{o}/\mathfrak{p}_i). \end{aligned}$$

Here P denotes the 1-dimensional trivial H-module, and $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ are the prime ideals of $\mathfrak{o}$ containing p. Since $\mathfrak{o}/\mathfrak{p}_i$ is a field, it is an irreducible $\mathfrak{o}$-module. Hence it is also irreducible as an H-module over P, and the action of H on it is non-trivial. It is known that the dimension of $\mathfrak{o}/\mathfrak{p}_i$ over P, namely, the degree of the extension $\mathfrak{o}/\mathfrak{p}_i$ over P, is equal to $d(q, p)$, the order of p mod q. Since M contains such a submodule $\mathfrak{o}/\mathfrak{p}_i$, we have $d \geqq d(q, p)$, *q.e.d.*

We note that if $p = 2$, then $d(q, p) \geqq 2$ for every prime q so that $d(n, p) \geqq 2$ for any integer $n \geqq 1$. Hence we also have $d \geqq 2$ in Theorem 1.

2. Let k be a finite algebraic number field, and let $\mathfrak{m}$ be an integral divisor of k, namely, a product of a finite number of prime divisors of k, archimedean or non-archimedean[2]. Let $I_{\mathfrak{m}}(k)$ denote the group of all ideals of k which are prime to $\mathfrak{m}$, and let $H_{\mathfrak{m}}(k)$ be the subgroup of all principal ideals (α) with $\alpha \equiv 1$ mod $\mathfrak{m}$. We put $C_{\mathfrak{m}}(k) = I_{\mathfrak{m}}(k)/H_{\mathfrak{m}}(k)$, and denote the order of $C_{\mathfrak{m}}(k)$ by $h_{\mathfrak{m}}(k)$. For $\mathfrak{m} = 1$, $C(k) = C_1(k)$ is the ideal class group of k, and $h(k) = h_1(k)$ is the class number of k.

Let M be a factor group of $C_{\mathfrak{m}}(k)$: $M = I_{\mathfrak{m}}(k)/H$, $H_{\mathfrak{m}}(k) \subset H \subset I_{\mathfrak{m}}(k)$. Let G be a group of automorphisms of k. If both $I_{\mathfrak{m}}(k)$ and H are invariant under the action of G, we may consider M as a G-group (or G-module). In such a case, we shall simply say that M is G-invariant.

3. Throughout this section, F will denote a finite algebraic number field, K a finite Galois extension of F with degree n, and G the Galois group of K/F.

THEOREM 2. *Let $\mathfrak{m}$ be an integral divisor of F, and let p be a prime number such that $(p, n) = (p, h_{\mathfrak{m}}(F)) = 1$. Let M be a G-invariant factor group of $C_{\mathfrak{m}}(K)$*

[2] For the classical class field theory used here and in the following, see H. Hasse's "Klassenkörperbericht" in Jahresbericht D. M.-V., **1926**, **1927**, **1930**.

with order a power of p, and let $M \neq 1$. Then the rank r of the finite abelian group M is at least equal to $d(n, p)$:

$$r \geqq d(n, p).$$

Proof. We first note that $\mathfrak{m}$ may be considered also as a divisor of K in the obvious manner so that the group $C_{\mathfrak{m}}(K)$ is well defined. Let $N = M/M^p$. Then $N \neq 1$, and it has the same rank as M. Hence, replacing M by N if necessary, we may assume that $M^p = 1$. Since M is a G-invariant factor group of $C_{\mathfrak{m}}(K)$, we may then consider M as a G-module over P. By Theorem 1, it is sufficient to show that the action of G on M is non-trivial.

Suppose that G acts trivially on M. Let L be the abelian extension of K which corresponds by class field theory to the ideal class group M. Since M is G-invariant, L/F is a Galois extension. Let A and B denote the Galois groups of L/F and L/K respectively. Then $A/B = G$, and B is canonically isomorphic to M so that G also acts trivially on B. Since the order of B is a power of p and is prime to the order n of G, the group extension A/B splits, and we have $A = B \times C$, $C \cong G$. Let E be the intermediate field of F and L such that the Galois group of L/E is C. Then E is an abelian extension of F with Galois group $A/C \cong B \cong M$. Let $\mathfrak{P}$ be a prime divisor of L, prime to $\mathfrak{m}$, and let T be the inertia group of $\mathfrak{P}$ for the extension L/F. Since L/K is the abelian extension corresponding to the factor group M of $C_{\mathfrak{m}}(K)$, $\mathfrak{P}$ is unramified by the extension L/K so that $T \cap B = 1$. Since the orders of B and C are prime to each other, it follows that T is contained in C. Therefore, if $\mathfrak{p}$ is any prime divisor of F, prime to $\mathfrak{m}$, then $\mathfrak{p}$ is unramified in K. By class field theory, the abelian extension E/F then corresponds to a factor group of $C_{\mathfrak{m}}(F)$, isomorphic to the Galois group $A/C \cong M$. Since $M \neq 1$, this implies that the order of $C_{\mathfrak{m}}(F)$ is divisible by p, and it contradicts the assumption $(p, h_{\mathfrak{m}}(F)) = 1$. Therefore the action of G on M is not trivial, and the theorem is proved.

COROLLARY. *Let p be a prime number such that $(p, n) = (p, h(F)) = 1$. Let M be a G-invariant factor group of $C(K)$ with order a power of p, and let $M \neq 1$. Then the rank r of M is at least equal to $d(n, p)$:*

$$r \geqq d(n, p).$$

In Theorem 2, suppose further that $(p-1, n) = 1$. For any prime factor q of n, we then have $p \not\equiv 1 \bmod q$ so that $d(q, p) \geqq 2$. Hence $d(n, p) \geqq 2$, and it follows from Theorem 2 that M is a non-cyclic group. Note that for $p=2$, the above assumption is always satisfied.

THEOREM 3. *Let* $\mathfrak{m}$ *and* p *be as stated in Theorem* 2: $(p, n)=(p, h_{\mathfrak{m}}(F))=1$. *If* p *divides* $h_{\mathfrak{m}}(K)$, *then the rank of the Sylow* p*-subgroup of* $C_{\mathfrak{m}}(K)$ *is at least equal to* $d(n, p)$.

Proof. This follows immediately from Theorem 2, because $C_{\mathfrak{m}}(K)$ has a G-invariant factor group isomorphic to its Sylow p-subgroup.

COROLLARY. *Let* p *be a prime number such that* $(p, n)=(p, h(F))=1$. *If* p *divides the class number* $h(K)$, *then the rank of the Sylow* p*-subgroup of the ideal class group* $C(K)$ *is at least equal to* $d(n, p)$.

Under the additional assumption $(p-1, n)=1$, we see that the Sylow p-subgroup in Theorem 3 and its corollary is non-cyclic. In particular, if $n=[K:F]$ is odd, $h(F)$ is odd, but $h(K)$ is even, then the Sylow 2-subgroup of $C(K)$ is a non-cyclic group. We can also prove by using the corollary of Theorem 2 that under the same assumption, if $h(K)$ is exactly divisible by an odd power of 2, then the rank of the Sylow 2-subgroup is at least equal to 3. For example, if $h(K)$ is exactly divisible by $8=2^3$, then the Sylow 2-subgroup is an abelian group of type $(2,2,2)$.

4. Since $h(\mathbf{Q})=1$ for the rational field $\mathbf{Q}$, we obtain the following result from the corollary of Theorem 3:

THEOREM 4. *Let* K *be a finite Galois extension of* $\mathbf{Q}$ *with degree* n, *and let* p *be a prime number, prime to* n. *Suppose that the class number* $h(K)$ *is divisible by* p. *Then the rank of the Sylow* p*-subgroup of the ideal class group* $C(K)$ *is at least equal to* $d(n, p)$.

COROLLARY. *Let* K *be a finite Galois extension of* $\mathbf{Q}$ *with an odd degree* n. *Suppose that the class number* $h(K)$ *is even. Then the Sylow* 2*-subgroup of the ideal class group* $C(K)$ *is non-cyclic, and its rank is at least equal to* $d(n, 2)$.

The assumption $(p, n)=1$ in Theorem 4 can be replaced by various other conditions on K. As a typical example, we consider the following case of cyclotomic fields.

THEOREM 5. *Let* l *be a prime number and let* K *be the cyclotomic field of* l^e*-th roots of unity* $(e \geqq 1)$. *Suppose that the class number* $h(K)$ *is divisible by* *a prime number p, and let*

$$(l-1)l^{e-1}=p^a n, \qquad (p, n)=1, \ a\geqq 0.$$

Then the rank of the Sylow p-subgroup of the ideal class group $C(K)$ is at least equal to $d(n, p)$.

Proof. Let F be the intermediate field of $\mathbf{Q}$ and K such that $[K:F]=n$, $[F:\mathbf{Q}]=p^a$. Since we know that $h(F)$ is not divisible by p[3], the theorem follows from the corollary of Theorem 3.

Corollary. *Let K be as in Theorem* 5. *Suppose that the class number $h(K)$ is even, and let*

$$(l-1)l^{e-1}=2^a n, \qquad (2, n)=1, \ a\geqq 0.$$

Then the Sylow 2-*subgroup of the ideal class group $C(K)$ is non-cyclic, and its rank is at least equal to $d(n, 2)$.*

Remark. By a theorem of Weber, the class number $h(K)$ is odd for $l=2$.

The above corollary can be further refined as follows. Let J denote the automorphism of the cyclotomic field K, mapping each element in K to its complex-conjugate. Clearly J induces an automorphism of $C=C(K)$, $J: C\rightarrow C$. Let C^+ and C^- denote the kernels of the endomorphisms $1-J: C\rightarrow C$ and $1+J: C\rightarrow C$, respectively, so that we have

$$C/C^+\cong C^{1-J}\subset C^-, \qquad C/C^-\cong C^{1+J}\subset C^+.$$

It follows that the class number $h(K)$ is the product of the order $h'(K)$ of C^- and the order $h''(K)$ of C^{1+J}. $h'(K)$ is called the first factor of $h(K)$, and $h''(K)$ the second factor of $h(K)$.

Let $S_2=S_2(K)$ denote the Sylow 2-subgroup of $C=C(K)$. Then $S_2^+=S_2\cap C^+$ and $S_2^-=S_2\cap C^-$ are the Sylow 2-subgroups of C^+ and C^- respectively. We see immediately from the definition that $S_2^+\cap S_2^-$ is the group of all x in S_2^+ satisfying $x^2=1$, and that it is also the group of all y in S_2^- satisfying $y^2=1$. Hence S_2^+ and S_2^- have the same rank. It follows in particular that $S_2^+=1$ if and only if $S_2^-=1$. Suppose that $S_2^+=S_2^-=1$. Then we see from $S_2/S_2^+\cong S_2^{1-J}\subset S_2^-$ that $S_2=1$. Therefore the three conditions $S_2=1$, $S_2^+=1$, and $S_2^-=1$ are all equi-

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

valent to each other. This result was first obtained by Kummer in the form that the class number $h(K)$ is odd if and only if its first factor $h'(K)$ is odd[4].

THEOREM 6. *Let K be as in Theorem 5 and suppose that the class number $h(K)$ is even. Then the groups S_2^+ and S_2^- are both non-cyclic, and they have the same rank which is at least equal to $d(n,2)$, n being the same as in the corollary of Theorem 5.*

Proof. We have already noted that S_2^+ and S_2^- have the same rank. If $S_2^+ = S_2$, then the theorem follows immediately from the corollary of Theorem 5. Suppose that $S_2^+ \neq S_2$. Let F be the intermediate field of $\mathbf{Q}$ and K such that $[K:F] = n$, and let G denote the Galois group of K/F. Then the ideal class group $C(K)$ has a G-invariant factor group isomorphic to S_2/S_2^+. Since $h(F)$ is odd[5], it follows from the corollary of Theorem 2 that the rank of S_2/S_2^+ is at least equal to $d(n,2) \geqq 2$. Since S_2^- contains the subgroup S_2^{1-J} which is isomorphic to S_2/S_2^+, the theorem is proved also in the case $S_2^+ \neq S_2$.

EXAMPLE. Let K be the cyclotomic field of 29-th roots of unity. It is known that C^- is a group of order 8 so that $C^- = S_2^-$[6]. Since $28 = 2^2\, 7$, $d(7,2) = 3$, we see immediately from the above that C^- is an abelian group of type $(2,2,2)$.

5. Let K be the cyclotomic field of 41-st roots of unity. We know that the class number $h(K)$ is then divisible by $121 = 11^2$.[7] However, since $d(40,11) = d(5,11) = 1$, we cannot see from Theorem 5 whether the Sylow 11-subgroup of $C(K)$ is cyclic or non-cyclic. In a paper of 1853, Kummer proved an interesting theorem on cyclotomic fields by which we can settle in certain cases such as above whether or not the subgroup $C^-(K)$ of $C(K)$ is cyclic[8]. However, in his paper, Kummer worked with logarithums of ideals, not of ordinary numbers, and it seems that his proof needs some further explanation[9]. Therefore, we shall show in the following how Kummer's result can be justified from our point of view.

---

4) For a more complete result in this direction, see H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Berlin, **1952**, § 37.

5) Iwasawa, op. cit.

6) Hasse, *Klassenzahl*, p. 150.

7) Hasse, *Klassenzahl*, p. 152.

8) E. Kummer, Über die Irregularität der Determinanten, Monatsber. Akad. d. Wissensch., Berlin, **1853**, pp. 194–200.

9) Hasse, *Klassenzahl*, p. 99.

Let l be an odd prime, and let K denote as before the cyclotomic field of l^e-th roots of unity ($e \geqq 1$). The Galois group G of $K/\mathbf{Q}$ is a cyclic group of order $m = (l-1)l^{e-1}$, and it is isomorphic to the multiplicative group of integers mod l^e, a canonical isomorphism being given by $\sigma_a \to a$ mod l^e, where σ_a denotes the automorphism of K mapping each l^e-th root of unity ζ to ζ^a : $\sigma_a(\zeta) = \zeta^a$. Let $R = \mathbf{Z}[G]$ be the group ring of G over the ring of rational integers $\mathbf{Z}$. Let ω be an element of the group ring $\mathbf{Q}[G]$ defined by

$$\omega = l^{-e}\sum_a a\sigma_a^{-1}, \qquad 0 \leqq a < l^e,\ (a, l) = 1,$$

and put

$$I = \omega R \cap R.$$

Further, let R^- denote the set of all α in R such that $(1+J)\alpha = 0$, and let $I^- = I \cap R^-$. Then both R^- and I^- are ideals of R, and we have

$$h'(K) = [R^- : I^-].^{10)}$$

We shall next consider the exponent of the finite abelian group R^-/I^-.

Let F denote the cyclotomic field of m-th roots of unity. For each character χ of the multiplicative group of integers mod l^e, we define an element ε_χ of the group ring $F[G]$ by

$$\varepsilon_\chi = m^{-1}\sum_a \chi(a)\sigma_a^{-1}, \qquad 0 \leqq a < l^e,\ (a, l) = 1.$$

Then the elements ε_χ form a set of orthogonal idempotents in $F[G]$ such that

$$F[G] = \sum_\chi F\varepsilon_\chi, \qquad 1 = \sum_\chi \varepsilon_\chi,$$

$$\omega\varepsilon_\chi = h_\chi \varepsilon_\chi,$$

with

$$h_\chi = l^{-e}\sum_a a\chi(a)^{-1}, \qquad h_\chi \in F.$$

By the classical class number formula,

$$h'(K) = 2l^e \prod_\chi{}' \left(-\frac{1}{2}h_\chi\right),$$

where χ ranges over all characters mod l^e such that $\chi(-1) = -1$. Therefore $h_\chi \neq 0$ for $\chi(-1) = -1$.

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

THEOREM 7. *Let t be the exponent of the finite abelian group R^-/I^-, and let N denote the least positive rational integer such that N/h_χ is an algebraic integer for every character χ with $\chi(-1) = -1$. Then N is a factor of $2t$, and t is a factor of $\frac{1}{2}mN$.*

Proof. For each character χ with $\chi(-1) = -1$, let

$$N = g_\chi h_\chi.$$

Then g_χ is an algebraic integer in F. Since $1-J$ is an element of R^-, $t(1-J)$ is contained in I^-. Hence $t(1-J) = \omega\alpha$ with some α in R. Let $\alpha\varepsilon_\chi = a_\chi\varepsilon_\chi$ with a_χ in F. Since α is in R, a_χ is an algebraic integer in F. On the other hand, $(1-J)\varepsilon_\chi = 2\varepsilon_\chi$ for $\chi(-1) = -1$. Therefore $2t\varepsilon_\chi = t(1-J)\varepsilon_\chi = \omega\alpha\varepsilon_\chi = \omega\varepsilon_\chi\alpha\varepsilon_\chi = h_\chi\varepsilon_\chi a_\chi\varepsilon_\chi = a_\chi h_\chi\varepsilon_\chi$, and we have

$$2t = a_\chi h_\chi, \qquad \chi(-1) = -1.$$

Therefore $2t/h_\chi$ is an algebraic integer for every character χ with $\chi(-1) = -1$, and we see from the definition of N that N is a factor of $2t$.

Let

$$\xi = m\sum_\chi{}' g_\chi\varepsilon_\chi,$$

where χ ranges over all characters with $\chi(-1) = -1$. It is clear that ξ is a linear combination of the elements of G with all coefficients algebraic integers in F. We also see easily that these coefficients are invariant under the Galois automorphisms of $F/\mathbf{Q}$. Therefore ξ is contained in $R = \mathbf{Z}[G]$, and hence in R^-. Since

$$1-J = 2\sum_\chi{}'\varepsilon_\chi, \qquad \chi(-1) = -1,$$

we obtain

$$\frac{1}{2}mN(1-J) = m\sum_\chi{}' g_\chi h_\chi\varepsilon_\chi = m\sum_\chi{}' g_\chi\omega\varepsilon_\chi = \omega\xi.$$

Therefore $\frac{1}{2}mN(1-J)$ is contained in $R^-\cap\omega R = I^-$. Since $R^- = (1-J)R$, $\frac{1}{2}mNR^-$ is then contained in I^-, and we see that t is a factor of $\frac{1}{2}mN$.

We now prove the following theorem of Kummer mentioned in the above.

THEOREM 8. *The exponent of the group $C^- = C^-(K)$ is a factor of mN, and the exponent of C^{1-J} is a factor of $\frac{1}{2}mN$.*

https://doi.org/10.1017/S0027763000012046 Published online by Cambridge University Press

Proof. The group ring $R = \mathbf{Z}[G]$ may be considered as an operator domain on C in the obvious manner. It is well known that $x^{\alpha} = 1$ for any x in C and for any α in I. Since $\frac{1}{2}mN(1-J)$ is contained in I^{-} by Theorem 7, we have

$$x^{\frac{1}{2}mN(1-J)} = 1$$

for any x in C. Therefore the exponent of C^{1-J} is a factor of $\frac{1}{2}mN$.

Now, let y be any element of C^{-}. Since $y^{1+J} = 1$, we have $y^{1-J} = y^{2}$. Hence it follows from the above that $y^{mN} = 1$. Therefore the exponent of C^{-} is a factor of mN.

COROLLARY. *Suppose that $C^{-}(K)$ is a cyclic group. Then $h'(K)$ is a factor of mN.*

Proof. This is obvious, because $h'(K)$ is the order of $C^{-}(K)$.

Let p be a prime number. For any rational integer $a \geqq 1$, let $(a)_p$ denote the highest power of p dividing a. Then it follows from Theorem 7 that $(t)_p = (N)_p$ for any p with $(p, m) = 1$. We also see from Theorem 8 and from its corollary that for any prime number p, the exponent of the Sylow p-subgroup of C^{-} is a factor of $(mN)_p$, and that if the Sylow p-subgroup is cyclic, then $(h'(K))_p$ must be a factor of $(mN)_p$. By using this fact and by computing $h'(K)$ and mN, Kummer was able to see that the Sylow 11-subgroup of C^{-} for the cyclotomic field of 41-st roots of unity is non-cyclic. He also verified that the group C^{-} is cyclic for every prime $p < 100$, $p \neq 29$, 41.[11]

Massachusetts Institute of Technology

11) Kummer, op. cit.