GALOIS GROUP OF THE MAXIMAL ABELIAN EXTENSION OVER AN ALGEBRAIC NUMBER FIELD

TOMIO KUBOTA

The aim of the present work is to determine the Galois group of the maximal abelian extension Ω_A over an algebraic number field Ω of finite degree, which we fix once for all.

Let χ be a continuous character of the Galois group of Ω_A/Ω. Then, by class field theory, the character χ is also regarded as a character of the idèle group of Ω. We call such a χ a *character of* Ω. For our purpose, it suffices to determine the group X_l of the characters of Ω whose orders are powers of a prime number l.

Let L be the group of the characters χ of Ω with $\chi^l = 1$; set $L_\nu = L \cap X_l^{l^\nu}$, where $\nu = 1, 2, \ldots$. We denote by υ_ν the largest number of independent elements of the factor group $L_{\nu-1}/L_\nu$. A character $\chi \in X_l$ is said to be divisible if, for any power l^r of l, there is a character $\psi \in X_l$ such that we have $\chi = \psi^{l^r}$. We denote by $X'_{l,\infty}$ the group of all divisible characters in X_l. Let now $Z(l, \infty)$ be the group of the roots of unity whose orders are powers of l. Then $X'_{l,\infty}$ has the unique subgroup $X_{l,\infty}$ such that $X_{l,\infty}$ is the direct product of finite number of groups all isomorphic to $Z(l, \infty)$ and that $X'_{l,\infty}/X_{l,\infty}$ is a finite group. Call the number $\dim X_l$ of direct factors of $X_{l,\infty}$ the *dimension* of X_l and let there be $\upsilon_{\infty,\nu}$ cyclic factors of order l^ν in the direct decomposition of $X'_{l,\infty}/X_{l,\infty}$ into cyclic groups. Then, the structure of X_l is completely determined by υ_ν, $\upsilon_{\infty,\nu}$ and by $\dim X_l$. This conclusion, together with the above one concerning the structure of $X'_{l,\infty}$, is brought by the results of Kaplansky [3], in which υ_ν, $\upsilon_{\infty,\nu}$ are called the *Ulm invariants* of X_l. Thus the problem is reduced to the determination of υ_ν, $\upsilon_{\infty,\nu}$ and $\dim X_l$.

Let ζ_l be a primitive l-th root of unity and let ν_l be the natural number such that the field $\Omega(\zeta_l)$ contains a primitive l^{ν_l}-th root of unity but no primitive l^{ν_l+1}-th root of unity. On the other hand, let $\mathfrak{l}_1, \mathfrak{l}_2, \ldots$ be all the prime factors of l in Ω and let $\mathfrak{e}_{l,\nu}$ be the group of the units of Ω which are l^ν-th powers in every $\mathfrak{l}_i$-completion $\Omega_{\mathfrak{l}_i}$ of Ω. Then, we can prove that there is a natural number

Received May 10, 1957.

μ_l such that we have $l^{\mu_l} = (\mathrm{e}_{l,\nu} : \mathrm{e}_{l,\nu+1})$ for every sufficiently large ν. Using these constants ν_l, μ_l, the determination of υ_ν and $\dim X_l$ is done. Namely, we have $\upsilon_\nu = 0$ for $\nu < \nu_l$, $\upsilon_\nu = \infty$ for $\nu \geqq \nu_l$ and $\dim X_l = N - \mu_l$, where N is the absolute degree of Ω.

We determine also the number l^{c_ν} of the elements of $X'_{l,\infty}$ whose orders divide l^ν. It is shown that we have $\upsilon_{\infty,\nu} = 2c_\nu - c_{\nu-1} - c_{\nu+1}$. The number $\upsilon_{\infty,\nu}$ has, however, no simple expression as υ_ν or as $\dim X_l$. Assume, for example, that $l \neq 2$. Let h_ν be the number of the ideal classes of Ω whose orders divide l^ν and let $\mathfrak{w}_i$ be the group of roots of unity in $\Omega_{\mathfrak{l}_i}$. Furthermore, let $B^{(\nu)}$ be the group of $\beta \in \Omega^{\times}$[1] such that the principal ideal (β) is the l^ν-th power of an ideal of Ω, and let $B_*^{(\nu)}$ be the group of $\beta \in B^{(\nu)}$ such that β is in $\mathfrak{w}_i \Omega_{\mathfrak{l}_i}^{\times l^\nu}$ for every i. Then we have $l^{c_\nu} = h_\nu \cdot l^{N\nu} \cdot (B^{(\nu)} : B_*^{(\nu)})$ and therefore

$$l^{\upsilon_{\infty\nu}} = \frac{h_\nu^2}{h_{\nu-1} h_{\nu+1}} \cdot \frac{(B^{(\nu-1)} : B_*^{(\nu-1)})(B^{(\nu+1)} : B_*^{(\nu+1)})}{(B^{(\nu)} : B_*^{(\nu)})^2} .$$

§ 1. Preliminaries

1. In order that a homomorphism f_B, into a finite abelian group $\mathfrak{A}$, of a subgroup B of a finite abelian group A is the restriction to B of a homomorphism f of A into $\mathfrak{A}$, it is necessary and sufficient that we have $f_B(B \cap A^m) \subset \mathfrak{A}^m$ for every natural number m. In particular, if $\mathfrak{A}$ is a cyclic group $\mathfrak{Z}$ whose order is a power l^ν of a prime number l, then the above condition becomes $f_B(B \cap A^{l^\nu}) = 1$.

Let now $\mathbf{I}$, $\mathbf{U}$ be the idèle group and the unit idèle group[2] of Ω, respectively, and denote by $\Omega^\times$ the principal idèle group of Ω. Then we see at once that a character[3] $\chi_{\mathbf{U}}$ of $\mathbf{U}$ is the restriction to $\mathbf{U}$ of a character χ' with $\chi'(\Omega^\times \mathbf{I}^{l^\nu}) = 1$ of $\Omega^\times \mathbf{I}^{l^\nu} \mathbf{U}$ if and only if we have $\chi_{\mathbf{U}}(\Omega \mathbf{I}^{l^\nu} \cap \mathbf{U}) = 1$. Moreover, if the latter condition is satisfied, then $\chi_{\mathbf{U}}$ determines χ uniquely and, from what is described above, χ' is the restriction to $\Omega^\times \mathbf{I}^{l^\nu} \mathbf{U}$ of a character χ with $\chi^{l^\nu} = 1$ of Ω.

Let $\mathfrak{S}$ be a finite set of places of Ω and $\chi_{\mathbf{U}}$ be a character of $\mathbf{U}$ such that $\chi^{l^\nu} = 1$ and that the $\mathfrak{q}$-component[4] of $\chi_{\mathbf{U}}$ is trivial for every place $\mathfrak{q} \notin S$. Then

[1] Throughout the paper, we use the mark $\times$ to stand for the multiplicative group of non-zero elements of a field.

[2] In this paper, we settle no sign condition for the real infinite components of unit idèles, somewhat differently from the definition of Weil [5].

[3] This means an ordinary character of the topological abelian group.

[4] This is naturally defined by means of local components of idèles.

χ_{U} is, in a natural way, regarded as a character of the group $U_{\mathfrak{S},\nu}=\prod_{\mathfrak{p}\in\mathfrak{S}} U_{\mathfrak{p}}/U_{\mathfrak{p}}^{l^\nu}$, where $U_{\mathfrak{p}}$ is the unit group of the $\mathfrak{p}$-completion $\Omega_{\mathfrak{p}}$ of Ω. On the other hand, set $B^{(\nu)}=\Omega^\times\cap \mathbf{I}^{l^\nu}\mathrm{U}$; then $B^{(\nu)}$ consists of the numbers β of $\Omega^\times$ such that the principal ideal (β) is the l^ν-th power of an ideal of Ω, and, setting $\beta=\mathbf{a}^{l^\nu}\mathbf{u}$ $(\mathbf{a}\in\mathbf{I},\ \mathbf{u}\in\mathrm{U})$, the mapping $\beta\to\mathbf{u}$ followed by the natural mapping of $\mathbf{u}$ into $U_{\mathfrak{S},\nu}$ gives rise to a homomorphism $\iota_{\mathfrak{S},\nu}$ of $B^{(\nu)}$ into $U_{\mathfrak{S},\nu}$. Since the natural image of $\Omega^\times\mathbf{I}^{l^\nu}\cap\mathrm{U}$ into $U_{\mathfrak{S},\nu}$ coincides with $\iota_{\mathfrak{S},\nu}(B^{(\nu)})$, we have

LEMMA 1. *Let l^ν be a power of a prime number l and let $\mathfrak{S}$ be a finite set of places of Ω. Then the restriction to* U *of a character χ with $\chi^{l^\nu}=1$ of Ω unramified*[5] *at every place of Ω outside $\mathfrak{S}$ is characterized as a character χ_{U} with $\chi_{\mathrm{U}}^{l^\nu}$ of* U *which has trivial $\mathfrak{q}$-component for every place $\mathfrak{q}\notin\mathfrak{S}$ and which satisfies $\chi_{\mathrm{U}}(\iota_{\mathfrak{S},\nu}(B^{(\nu)}))=1$.*

Let $U_{\mathfrak{S},\nu}$ be as above. Lemma 1 implies

LEMMA 2. *Let V be any subgroup of $U_{\mathfrak{S},\nu}$ and let h_ν be the l^ν-class number of Ω, i.e., the index $(\mathbf{I}:\Omega^\times\mathbf{I}^{l^\nu}\mathrm{U})$. Then the number of all characters, with $\chi^{l^\nu}=1$ and with $\chi_{\mathrm{U}}(V)=1$, of Ω unramified at every $\mathfrak{q}\notin\mathfrak{S}$ is equal to $h_\nu\cdot(U_{\mathfrak{S},\nu}:\iota_{\mathfrak{S},\nu}(B^{(\nu)})\cdot V)$, where χ_{U} is the restriction to* U *of χ.*

We have also

LEMMA 3. *The kernel of $\iota_{\mathfrak{S},\nu}$ consists of the numbers $\beta\in B^{(\nu)}$ such that β is, for every $\mathfrak{p}\in\mathfrak{S}$, an l^ν-th power in the $\mathfrak{p}$-completion $\Omega_{\mathfrak{p}}$ of Ω.*

2. Let $P_{2,\infty}$ be the field obtained by adjunction to the rational number field P of all 2^m-th roots of unity, where $m=1,2,\dots$. Assume that the intersection $\Omega\cap P_{2,\infty}$ is real. Then there is an integer $T\geqq 2$ such that $\Omega\cap P_{2,\infty}$ is the largest real subfield of the field P_{2^T} obtained by adjunction to P of a primitive 2^T-th root of unity. In this case, we say that Ω is a *radical field* and, setting $\lambda_T=4\cos^2 2\pi/2^{T+1}$, we call λ_T the *radical number* of Ω.[6] The rational number field P is a radical field with radical number $\lambda_2=2$. Numbers T and λ_T are uniquely determined whenever Ω is radical.

Denote now by l^ν a power of a prime number l and by $\Omega^{(\nu)}$ the group of

5) We say that χ is ramified at $\mathfrak{p}$ if the corresponding cyclic extension of χ over Ω is ramified at $\mathfrak{p}$.

6) See Hasse [2], Einleitung.

the numbers α of $\Omega^{\times}$ such that α is an l^{ν}-th power in the field $\Omega P_{l^{\nu}}$ obtained by adjunction to Ω of a primitive l^{ν}-th root of unity. Then a result[7] of Hasse yields

LEMMA 4. *We have in general* $\Omega^{(\nu)} = \Omega^{\times l^{\nu}}$. *Only in the special case where* $l=2$, Ω *is a radical field with radical number* λ_T *and* $\nu \geqq 2$, *the factor group* $\Omega^{(\nu)}/\Omega^{\times 2^{\nu}}$ *is of order* 2 *and its only one non-trivial coset is represented by* $-\lambda_{\nu}^{2^{\nu-1}}$ *or by* $\lambda_T^{2^{\nu-1}}$ *according as* $2 \leqq \nu \leqq T$ *or* $\nu > T$.

Still assuming that Ω is a radical field with radical number λ_T, it follows from this lemma that, for every prime ideal $\mathfrak{p}$ of Ω prime to 2, $\lambda_T^{2^{\nu-1}}$ ($\nu > T$) is a 2^{ν}-th power in the $\mathfrak{p}$-completion $\Omega_{\mathfrak{p}}$ of Ω. Now, letting $\mathfrak{l}_1, \mathfrak{l}_2, \ldots$ be all the prime factors of 2 in Ω and $\Omega_{\mathfrak{l}_i}$ be the $\mathfrak{l}_i$-completion of Ω, we say that Ω is a *strongly radical field* if we have $\lambda_T = \lambda_i^2 \zeta_i$ for every i, where λ_i is an element of $\Omega_{\mathfrak{l}_i}$ and ζ_i is a root of unity in $\Omega_{\mathfrak{l}_i}$. The meaning of this definition is explained by the following

LEMMA 5. *Assume that* Ω *is radical with the radical number* λ_T. *Then* Ω *is strongly radical if and only if* $\lambda_T^{2^{\nu-1}}$ *is a* 2^{ν}*-th power in every local completion of* Ω *for every* $\nu > T$, *or equivalently for* $\nu = T+1$.

Proof. Suppose that $\lambda_T = \lambda_i^2 \zeta_i$ and $\nu > T$; then we have $\lambda_T^{2^{\nu-1}} = \lambda_i^{2^{\nu}} \zeta_i^{2^{\nu-1}}$. If $\Omega_{\mathfrak{l}_i}$ contains no primitive 2^{ν}-th root of unity, then $\zeta_i^{2^{\nu-1}} = 1$ and $\lambda_T^{2^{\nu-1}}$ is a 2^{ν}-th power in $\Omega_{\mathfrak{l}_i}$. If $\Omega_{\mathfrak{l}_i}$ contains a primitive 2^{ν}-th root of unity, then $\Omega_{\mathfrak{l}_i}$ contains $\Omega P_{2^{\nu}}$, whence, by Lemma 4, $\lambda_T^{2^{\nu-1}}$ is a 2^{ν}-th power in $\Omega P_{2^{\nu}}$ and *a fortiori* in $\Omega_{\mathfrak{l}_i}$. The converse is obvious.

§ 2. Structural constants

3. We begin by a reformulation of the main theorem of Wang [4].

Assuming that Ω is a radical field with the radical number λ_T, we say that a prime factor $\mathfrak{l}$ of 2 in Ω is *even* if λ_T is of the form $\lambda^2\zeta$, where λ is an element of the $\mathfrak{l}$-completion $\Omega_{\mathfrak{l}}$ of Ω and ζ is a root of unity in $\Omega_{\mathfrak{l}}$. Otherwise we say that $\mathfrak{l}$ is odd. In Wang [4], $\mathfrak{l}$ is said to be odd if $\Omega_{\mathfrak{l}}$ does not contain any of three numbers $\sqrt{-1}$, $\cos 2\pi/2^{T+1}$, $\sqrt{-1}\cos 2\pi/2^{T+1}$; otherwise, to be even. We now show that our definition is equivalent with Wang's one. Suppose that $\mathfrak{l}$ is

7) See Hasse [2], § 1, Satz 1 and Satz 2.

even. Then since $\lambda_T = 4\cos^2 2\pi/2^{T+1}$, $\Omega_{\mathfrak{l}}$ must contain at least one of the three numbers above. Conversely, suppose that $\Omega_{\mathfrak{l}}$ contains $\sqrt{-1}$. Then since $\Omega_{\mathfrak{l}}$ contains a primitive 2^T-th root ζ_{2^T} of unity and since $-\lambda_T^{2^{T-1}}$ is, by Lemma 4, a 2^T-th power in $\Omega(\zeta_{2^T})$, we see that $\mathfrak{l}$ is even. Furthermore, if we have either $\cos 2\pi/2^{T+1} \in \Omega_{\mathfrak{l}}$ or $\sqrt{-1}\cos 2\pi/2^{T+1} \in \Omega_{\mathfrak{l}}$, then $\mathfrak{l}$ is obviously even.

After these preliminaries, it follows from the main theorem of Wang [4] that we have

THEOREM 1. *Let χ be a character of Ω whose order $l^{\nu-r}$ $(0 \leqq r \leqq \nu)$ is a power of a prime number l and let $\mathfrak{S}$ be a finite set of places of Ω containing all ramification places of χ. Furthermore, denoting by $\chi_{\mathfrak{p}}$ the $\mathfrak{p}$-component[8] of χ and by $\Omega_{\mathfrak{p}}$ the $\mathfrak{p}$-completion of Ω, let there be given for every $\mathfrak{p} \in \mathfrak{S}$ a character $\psi_{\Omega_{\mathfrak{p}}}$ of $\Omega_{\mathfrak{p}}^{\times}$ such that $\chi_{\mathfrak{p}} = \psi_{\Omega_{\mathfrak{p}}}^{l^r}$. In the case where $l=2$, Ω is radical with the radical number λ_T, $r > T$ and all odd prime factors of 2 in Ω are in $\mathfrak{S}$, suppose that $\mathfrak{S}$ contains all prime factors of 2 in Ω and that we have $\prod_{\mathfrak{p}\in\mathfrak{S}} \psi_{\Omega_{\mathfrak{p}}}(\lambda_T^{2^{r-1}}) = 1$. Then there is a character ψ of order l^{ν} of Ω such that we have $\chi = \psi^{l^r}$ and that the $\mathfrak{p}$-component $\psi_{\mathfrak{p}}$ of ψ coincides with $\psi_{\Omega_{\mathfrak{p}}}$ for every $\mathfrak{p} \in \mathfrak{S}$.*

4. Let l be a prime number and ζ_l be a primitive l-th root of unity. Denote by ν_l a natural number such that the field $\Omega(\zeta_l)$ contains a primitive l^{ν_l}-th root of unity but no primitive l^{ν_l+1}-th root of unity. Then we have

LEMMA 6. *Let χ be a character of order $l^{\nu_l - r}$ of Ω with $0 \leqq r \leqq \nu_l$. Then there is a character ψ of order l^{ν_l} of Ω such that we have $\chi = \psi^{l^r}$.*

Proof. If $l=2$, $\nu_l = 1$, then the lemma is obvious. We may therefore assume that $\sqrt{-1} \in \Omega$ whenever we have $l=2$. Let $\mathfrak{S}$ be the set of all ramification prime ideals of χ. Since then, for every $\mathfrak{p} \in \mathfrak{S}$, we have $N\mathfrak{p} - 1 \equiv 0 \pmod{l}$, the $\mathfrak{p}$-completion $\Omega_{\mathfrak{p}}$ contains ζ_l and we have consequently $\Omega_{\mathfrak{p}} \supset \Omega(\zeta_l) = \Omega(\zeta_{l^{\nu_l}})$. From this follows $N\mathfrak{p} - 1 \equiv 0 \pmod{l^{\nu_l}}$, whence there is a character $\psi_{\Omega_{\mathfrak{p}}}$ of $\Omega_{\mathfrak{p}}^{\times}$ such that $\chi_{\mathfrak{p}} = \psi_{\Omega_{\mathfrak{p}}}^{l^r}$. Hence, Theorem 1 assures that there is a character ψ of order l^{ν_l} of Ω such that we have $\chi = \psi^{l^r}$, which completes the proof.

Another meaning of ν_l as a structural constant of the maximal abelian extension over Ω is found in the following

LEMMA 7. *Let ν be a rational integer with $\nu_l \leqq \nu$. Then there is an infinite*

[8] See foot-note 4.

set $\mathfrak{M}$ *of characters of* Ω *satisfying the following conditions*: i) *every character* $\chi \in \mathfrak{M}$ *is of order* l. ii) *for every ramification prime ideal* $\mathfrak{p}$ *of* $\chi \in \mathfrak{M}$, *we have* $N\mathfrak{p} - 1 \equiv 0 \pmod{l^{\nu}}$, $N\mathfrak{p} - 1 \not\equiv 0 \pmod{l^{\nu+1}}$. iii) *none of characters of* $\mathfrak{M}$ *is unramified and every two different characters of* $\mathfrak{M}$ *have no common ramification prime ideal.* iv) *for every* $\chi \in \mathfrak{M}$ *there is a character* ψ *of* Ω *such that we have* $\chi = \psi^{l^{\nu-1}}$.

Proof. Using notations in §1, **1**, set $B^{(\nu)} = \Omega^{\times} \cap \mathbf{I}^{l^{\nu}}\mathbf{U}$. Let $\mathfrak{S} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$ be a set of prime ideals, prime to l, of Ω such that m is larger than the rank of $B^{(\nu)}/B^{(\nu)l}$ and that we have $N\mathfrak{p}_i - 1 \equiv 0 \pmod{l^{\nu}}$, $N\mathfrak{p}_i - 1 \not\equiv 0 \pmod{l^{\nu+1}}$ for every i. Moreover, choose for every i a character ψ_i of order l^{ν} of $\mathbf{U}$ with trivial $\mathfrak{q}$-component for every place $\mathfrak{q}$ of Ω different from $\mathfrak{p}_i$. Then since the group $U_{\mathfrak{S},\nu}$ defined in §1, **1** is of type $(l^{\nu}, \ldots, l^{\nu})$ and since the rank of $\iota_{\mathfrak{S},\nu}(B^{(\nu)})$ is smaller than m, $U_{\mathfrak{S},\nu}/\iota_{\mathfrak{S},\nu}(B^{(\nu)})$ contains an element of order l^{ν}. Therefore a suitable multiplicative combination $\psi_{\mathbf{U}} = \psi_1^{a_1} \ldots \psi_m^{a_m}$ is trivial on $\iota_{\mathfrak{S},\nu}(B^{(\nu)})$, while the order of $\psi_{\mathbf{U}}$ is l^{ν}. By Lemma 1, $\psi_{\mathbf{U}}$ is the restriction to $\mathbf{U}$ of a character ψ of order l^{ν} of Ω. Therefore, a required set $\mathfrak{M}$ can be constructed as a set of characters of the form $\chi = \psi^{l^{\nu-1}}$, which completes the proof.

5. We insert here a lemma concerning the structure of local fields.[9]

LEMMA 8. *Let* $\mathfrak{l}$ *be a prime factor in* Ω *of a prime number* l *and let* $\Omega_{\mathfrak{l}}$ *be the* $\mathfrak{l}$*-completion of* Ω. *Denote by* $U_{\mathfrak{l},1}$ *the group of units* u *of* $\Omega_{\mathfrak{l}}$ *with* $u \equiv 1 \pmod{\mathfrak{l}}$ *and by* $N_{\mathfrak{l}}$ *the degree of* $\Omega_{\mathfrak{l}}$ *over the* l*-completion* P_l *of the rational number field. Then* $U_{\mathfrak{l},1}$ *is, as a topological group, the direct product of* $N_{\mathfrak{l}}$ *groups all isomorphic to the additive group of integers of* P_l *by the finite cyclic group consisting of all roots of unity in* $\Omega_{\mathfrak{l}}$ *whose orders are powers of* l.

Now, let l^{ν} be a power of a prime number l and $\mathfrak{S} = \{\mathfrak{l}_1, \mathfrak{l}_2, \ldots\}$ be the set of all prime factors of l in Ω. Denote by $\Omega_{\mathfrak{l}_i}$ the $\mathfrak{l}_i$-completion of Ω and by $B_0^{(\nu)}$ the kernel of the homomorphism $\iota_{\mathfrak{S},\nu}$ of §1, **1**. Then we have

LEMMA 9. *Let* $\mathbf{e}$ *be the unit group of* Ω. *Then the index* $(B^{(\nu)} : \mathbf{e}B_0^{(\nu)})$ *becomes constant for sufficiently large* ν.

Proof. It follows from the finiteness of the class number of Ω that, for sufficiently large ν, $B^{(\nu)}/\mathbf{e}\Omega^{\times l^{\nu}}$ is isomorphic to $B^{(\nu+1)}/\mathbf{e}\Omega^{\times l^{\nu+1}}$ and that the iso-

9) See Hasse [1], §15, p. 177.

morphism is given by $B^{(\nu)} \in \beta^{(\nu)l} \to \beta^{(\nu)l} \in B^{(\nu+1)}$. Furthermore, by Lemma 3, the image of $\mathrm{e}B_0^{(\nu)}/\mathrm{e}$ by the isomorphism is in $\mathrm{e}B_0^{(\nu+1)}/\mathrm{e}$. This means that the index $(B^{(\nu)} : \mathrm{e}B_0^{(\nu)})$ is monotonously decreasing for such a ν, from which at once follows our assertion.

Still using same notations, we now prove

LEMMA 10. *Set* $\mathrm{e}_{l,\nu} = \mathrm{e} \cap B_0^{(\nu)}$. *Then the index* $(\mathrm{e}_{l,\nu} : \mathrm{e}_{l,\nu+1})$ *becomes constant for sufficiently large* ν.

Proof. It follows from Lemma 8 that, for sufficiently large ν, a unit ε of Ω is an l^ν-th power in $\Omega_{\mathfrak{l}_i}$ if and only if ε^l is an $l^{\nu+1}$-th power in $\Omega_{\mathfrak{l}_i}$. Therefore, for such a ν, the l-th power $\varepsilon^{(\nu)l} \in \mathrm{e}_{l,\nu+1}$ of an element $\varepsilon^{(\nu)} \in \mathrm{e}_{l,\nu}$ is not in $\mathrm{e}_{l,\nu+2}$ unless we have $\varepsilon^{(\nu)} \in \mathrm{e}_{l,\nu+1}$. This means that we have $(\mathrm{e}_{l,\nu} : \mathrm{e}_{l,\nu+1}) \leqq (\mathrm{e}_{l,\nu+1} : \mathrm{e}_{l,\nu+2})$. Since from the finiteness of the dimension of e follows the boundedness of the index $(\mathrm{e}_{l,\nu} : \mathrm{e}_{l,\nu+1})$, the lemma is proved.

By this lemma, we have a new constant μ_l with $(\mathrm{e}_{l,\nu} : \mathrm{e}_{l,\nu+1}) = l^{\mu_l}$ for sufficiently large ν. The meaning of μ_l as a structural constant of the maximal abelian extension over Ω lies in the following

LEMMA 11. *Let* l^ν *be a power of a prime number* l *and* $\mathfrak{S} = \{\mathfrak{l}_1, \mathfrak{l}_2, \ldots\}$ *be the set of all prime factors of* l *in* Ω. *Denote by* $T_{l,\nu}$ *the group of the characters* χ *of* Ω *such that the order of* χ *divides* l^ν *and that every ramification place of* χ *is in* $\mathfrak{S}$. *Then we have* $(T_{l,\nu+1} : T_{l,\nu}) = l^{N-\mu_l}$ *for sufficiently large* ν, *where* N *is the absolute degree of* Ω.

Proof. Denote by N_i the degree of the $\mathfrak{l}_i$-completion $\Omega_{\mathfrak{l}_i}$ of Ω over the l-completion of the rational number field and denote by $U_{\mathfrak{l}_i}$ the unit group of $\Omega_{\mathfrak{l}_i}$. Moreover, let $w_{\nu,i}$ be the number of roots of unity in $\Omega_{\mathfrak{l}_i}$ whose orders divide l^ν and let $U_{\mathfrak{l}_i,1}$ be the group consisting of all $u \in U_{\mathfrak{l}_i}$ with $u \equiv 1 \pmod{\mathfrak{l}_i}$. Then the number of characters of $U_{\mathfrak{l}_i}$ whose orders divide l^ν is, by Lemma 8, equal to $l^{N_i\nu} w_{\nu,i}$. Therefore Lemma 2 shows that, if h_ν is the l^ν-class number of Ω, then we have

$$(T_{l,\nu} : 1) = h_\nu \cdot \prod_i (l^{N_i\nu} w_{\nu,i}) \cdot (\iota_{\mathfrak{S},\nu}(B^{(\nu)}) : 1)^{-1}.$$

Now, with notations in Lemma 9 and in Lemma 10, we have $(\iota_{\mathfrak{S},\nu}(B^{(\nu)}) : 1) = (B^{(\nu)} : B_0^{(\nu)}) = (B^{(\nu)} : \mathrm{e}B_0^{(\nu)})(\mathrm{e} : \mathrm{e}_{l,\nu})$. From this and from the relation $\sum_i N_i = N$ follows

$$(T_{l,\nu+1} : T_{l,\nu}) = \frac{h_{\nu+1}}{h_\nu} \cdot l^N \cdot \prod_i \left(\frac{w_{\nu+1,i}}{w_{\nu,i}} \right) \cdot \frac{(B^{(\nu)} : \mathrm{e}B_0^{(\nu)})}{(B^{(\nu+1)} : \mathrm{e}B_0^{(\nu+1)})} \cdot (\mathrm{e}_{l,\nu} : \mathrm{e}_{l,\nu+1})^{-1}.$$

Numbers h_ν, $w_{\nu,i}$ are constant for sufficiently large ν and, by Lemma 9, so is also $(B^{(\nu)} : \mathrm{e}B_0^{(\nu)})$. Thus, by Lemma 10, we have $\lim_{\nu\to\infty} (T_{l,\nu+1} : T_{l,\nu}) = l^{N-\mu_l}$, which completes the proof.

§ 3. Divisible characters

6. A character χ of Ω whose order is a power of a prime number l is said to be *divisible* if, for an arbitrary power l^r of l, there is a character ψ of Ω such that we have $\chi = \psi^{l^r}$. On the other hand, if $\mathfrak{p}$ is a place of Ω and if $\Omega_\mathfrak{p}$ is the $\mathfrak{p}$-completion of Ω, then χ is said to be divisible at $\mathfrak{p}$ whenever, for every l^r, there is a character $\psi_{\Omega_\mathfrak{p}}$ of $\Omega_\mathfrak{p}^\times$ such that we have $\chi_\mathfrak{p} = \psi_{\Omega_\mathfrak{p}}^{l^r}$, where $\chi_\mathfrak{p}$ is the $\mathfrak{p}$-component of χ. If χ is divisible at every place of Ω, then we say that χ is *everywhere locally divisible*. A character χ is of course everywhere locally divisible if it is divisible.

Taking a character χ of Ω whose order is a power of l, suppose that, for any place $\mathfrak{p}$ of Ω which either is a prime ideal prime to l or is infinite, χ is unramified at $\mathfrak{p}$. Moreover, letting $\mathfrak{l}$ be any prime factor of l in Ω and $\Omega_\mathfrak{l}$ be the $\mathfrak{l}$-completion of Ω, suppose that the $\mathfrak{l}$-component $\chi_\mathfrak{l}$ is trivial on the group consisting of all roots of unity in $\Omega_\mathfrak{l}$. Then it follows from Lemma 8 that χ is everywhere locally divisible. We see that the converse also is true.

Now, let l^ν be a power of a prime number l, let $\mathfrak{S} = \{\mathfrak{l}_1, \mathfrak{l}_2, \ldots\}$ be the set of all prime factors of l in Ω and let $U_{\mathfrak{l}_i}$ be the unit group of the $\mathfrak{l}_i$-completion $\Omega_{\mathfrak{l}_i}$ of Ω. Denote by $\mathfrak{w}_i$ the group of roots of unity in $\Omega_{\mathfrak{l}_i}$ and set $V_{\mathfrak{S},\nu} = \prod_i \mathfrak{w}_i U_{\mathfrak{l}_i}^{l^\nu} / U_{\mathfrak{l}_i}^{l^\nu}$. Furthermore, let N be the absolute degree of Ω and $U_{\mathfrak{S},\nu}$ be as in § 1, **1.** Then it follows from Lemma 8 that the factor group $U_{\mathfrak{S},\nu}/V_{\mathfrak{S},\nu}$ is isomorphic to the direct product of N cyclic groups of order l^ν. On the other hand, we see that, with notations in § 1, **1**, the index $(\iota_{\mathfrak{S},\nu}(B^{(\nu)}) \cdot V_{\mathfrak{S},\nu} : V_{\mathfrak{S},\nu})$ is equal to the index $(B^{(\nu)} : B_*^{(\nu)})$, where $B_*^{(\nu)}$ is the group of all $\beta \in B^{(\nu)}$ with $\beta \in \mathfrak{w}_i \Omega_{\mathfrak{l}_i}^{l^\nu}$ for every $\mathfrak{l}_i$. Furthermore, it follows from what is stated above that a character χ of Ω with order dividing l^ν and with trivial $\mathfrak{q}$-component for every place $\mathfrak{q}$ of Ω outside $\mathfrak{S}$ is everywhere locally divisible if and only if its restriction χ_U to the unit idèle group U of Ω is, as a homomorphism of $U_{\mathfrak{S},\nu}$, trivial on $V_{\mathfrak{S},\nu}$. Therefore, by Lemma 2, the number of all everywhere locally

https://doi.org/10.1017/S0027763000022042 Published online by Cambridge University Press

divisible characters of Ω whose orders divide l^ν is equal to $h_\nu \cdot l^{N_\nu} \cdot (B^{(\nu)} : B_*^{(\nu)})^{-1}$, where h_ν is the l^ν-class number of Ω.

7. We now prove two theorems which display characteristic properties of divisible characters.

THEOREM 2. *Let χ be an everywhere locally divisible character of Ω whose order is a power of a prime number l. Then, in general, the character χ is divisible. In the special case where $l=2$ and Ω is strongly radical with the radical number λ_T, the character χ is divisible if and only if the following condition is fulfilled: let $\mathfrak{S} = \{\mathfrak{l}_1, \mathfrak{l}_2, \ldots\}$ be the set of all prime factors of 2 in Ω and write, for every i, $\lambda_T = \lambda_i^2 \zeta_i$ with an element λ_i of the $\mathfrak{l}_i$-completion $\Omega_{\mathfrak{l}_i}$ of Ω and with a root of unity ζ_i in $\Omega_{\mathfrak{l}_i}$; then we have $\prod_i \chi_{\mathfrak{l}_i}(\lambda_i) = 1$, where $\chi_{\mathfrak{l}_i}$ is the $\mathfrak{l}_i$-component of χ.*

Proof. Suppose that Ω is not radical whenever $l=2$. Then, since χ is everywhere locally divisible, the ramification places of χ are, by **6**, in $\mathfrak{S}$, and we can choose for any $\mathfrak{l}_i \in \mathfrak{S}$ and for any power l^r of l a character $\psi_{\Omega_{\mathfrak{l}_i}}$ of $\Omega_{\mathfrak{l}_i}^\times$ such that we have $\chi_{\mathfrak{l}_i} = \psi_{\Omega_{\mathfrak{l}_i}}^{l^r}$. Therefore, by Theorem 1, there is a character ψ of Ω with $\chi = \psi^{l^r}$.

Suppose next that $l=2$, and that Ω is radical with the radical number λ_T but not strongly radical. Then since we have $(\prod_i \psi_{\Omega_{\mathfrak{l}_i}}(\lambda_T^{2^{r-1}}))^2 = \prod_i \chi_{\mathfrak{l}_i}(\lambda_T) = \chi(\lambda_T) = 1$, the product $\prod_i \psi_{\Omega_{\mathfrak{l}_i}}(\lambda_T^{2^{r-1}})$ is ± 1. We may, however, assume that the product is 1, provided that we have $r > T$. For, since Ω is not strongly radical, we can choose a character η, say, of $\Omega_{\mathfrak{l}_1}^\times$ such that $\eta^2 = 1$, $\eta(\lambda_T) = -1$ and that η is trivial on the group of roots of unity in $\Omega_{\mathfrak{l}_1}$, whence, choosing a character η' of $\Omega_{\mathfrak{l}_1}^\times$ with $\eta'^{2^{r-1}} = \eta$ and using $\psi'_{\Omega_{\mathfrak{l}_1}} = \psi_{\Omega_{\mathfrak{l}_1}}\eta'$ instead of $\psi_{\Omega_{\mathfrak{l}_1}}$, the above product becomes 1. Therefore, again by Theorem 1, we find a character ψ of Ω with $\chi = \psi^{2^r}$.

Lastly considering the very special case in the theorem, suppose that χ is divisible. Then, for any power 2^r of 2, there is a character ψ of Ω with $\chi = \psi^{2^r}$. Therefore, if $\psi_{\mathfrak{l}_i}$ is the $\mathfrak{l}_i$-component of ψ, then we have $\prod_i \psi_{\mathfrak{l}_i}(\lambda_T^{2^{r-1}}) = 1$, because λ_T is prime to every prime ideal of Ω outside $\mathfrak{S}$.[10] Provided that, for every i, there is no root of unity whose order is higher than 2^{r-1}, we have $\psi_{\mathfrak{l}_i}(\lambda_T^{2^{r-1}}) = \psi_{\mathfrak{l}_i}(\lambda_i^{2^r} \zeta_i^{2^{r-1}}) = \psi_{\mathfrak{l}_i}^{2^r}(\lambda_i) = \chi_{\mathfrak{l}_i}(\lambda_i)$, whence $\prod_i \chi_{\mathfrak{l}_i}(\lambda_i) = 1$. Conversely, assume this

[10] See foot-note 6

relation and take a character $\psi_{\Omega_{\mathfrak{l}_i}}$ of $\Omega_{\mathfrak{l}_i}^{\times}$ for every i such that we have $\chi_{\mathfrak{l}_i} = \psi_{\Omega_{\mathfrak{l}_i}}^{2^r}$. Then we have $\prod_i \psi_{\Omega_{\mathfrak{l}_i}}(\lambda_T^{2^{r-1}}) = \prod_i \psi_{\Omega_{\mathfrak{l}_i}}(\lambda_i^{2^r} \zeta_i^{2^{r-1}}) = \prod_i \chi_{\mathfrak{l}_i}(\lambda_i) = 1$ whenever r is so large that $\zeta_i^{2^{r-1}} = 1$. Hence, by Theorem 1, χ is divisible. The theorem is thus completely proved.

THEOREM 3. *Let Ω be a strongly radical field with the radical numer λ_T and let $\mathfrak{S} = \{\mathfrak{l}_1, \mathfrak{l}_2, \ldots\}$, λ_i and ζ_i be as in Theorem 2. Let $\mathfrak{l}$ be the idèle of Ω whose $\mathfrak{l}_i$-component is λ_i for every i and whose $\mathfrak{q}$-component is 1 for every place $\mathfrak{q} \notin \mathfrak{S}$, and let 2^ν be a power of 2. Denote by $U_{\mathfrak{l}_i}$ the unit group of the $\mathfrak{l}_i$-completion $\Omega_{\mathfrak{l}_i}$ of Ω, by $\mathfrak{w}_i$ the group of roots of unity in $\Omega_{\mathfrak{l}_i}$ and by $\mathbf{V}_{\mathfrak{S},\nu}$ the group of unit idèles $\mathbf{u}$ of Ω such that the $\mathfrak{l}_i$-component of $\mathbf{u}$ is in $\mathfrak{w}_i U_{\mathfrak{l}_i}^{2^\nu}$ for every i. Furthermore, let $\mathbf{I}$, $\Omega^\times$ be the idèle group and the principal idèle group of Ω, respectively. Then the group of the everywhere locally divisible characters of Ω whose orders divide 2^ν coincides with the group of the divisible characters of Ω whose orders divide 2^ν whenever we have $\mathfrak{l} \in \Omega^\times \mathbf{I}^{2^\nu} \mathbf{V}_{\mathfrak{S},\nu}$. Otherwise, the latter group is a subgroup of index 2 of the former one.*

Proof. In order that a character χ of Ω is everywhere locally divisible and that the order of χ divides 2^ν, it is, by **6**, necessary and sufficient that we have $\chi(\Omega^\times \mathbf{I}^{2^\nu} \mathbf{V}_{\mathfrak{S},\nu}) = 1$. On the other hand, Theorem 2 shows that such a χ is divisible if and only if we have $\chi(\mathfrak{l}) = 1$. This, together with the fact that $\mathfrak{l}^2$ is in $\Omega^\times \mathbf{I}^{2^\nu} \mathbf{V}_{\mathfrak{S},\nu}$, proves the theorem.

§ 4. Main results

8. We arrange preliminary results about infinite abelian groups which are for the most part obtained in Kaplansky [3].

An abelian group A is said to be a *torsion abelian group* if every element of A is of finite order, and A is said to be a *torsion abelian l-group* if the orders of all the elements of A are powers of a prime number l. Every torsion abelian group A has the unique largest torsion abelian l-group A_l for every prime number l and A is the direct product[11] of all the A_l. We call A_l the *l-component* of A.

Let A be a torsion abelian l-group. Then an element a of A is said to be *divisible* if, for any power l^r of l, there is an element b of A with $a = b^{l^r}$. If

[11] This means so called "weak" direct product arising most commonly in abstract algebra.

https://doi.org/10.1017/S0027763000022042 Published online by Cambridge University Press

every element of A is divisible, then we say that A is divisible. Every torsion abelian l-group A has the unique *largest divisible subgroup* A_∞ and, if $Z(l, \infty)$ is the group of roots of unity whose orders are powers of l, then A_∞ is isomorphic to the direct product of finite or infinite number of groups all isomorphic to $Z(l, \infty)$. Moreover A_∞ is contained in the group A'_∞ consisting of all divisible elements of A.

Let again A be a torsion abelian l-group and L be the subgroup of A consisting of $a \in A$ with $a^l = 1$. We call the number of finite or infinite independent elements of L the rank of A. Furthermore, setting $L_\nu = L \cap A^{l^\nu}$, we call the rank υ_ν of $L_{\nu-1}/L_\nu$ the ν-th *Ulm invariant* of A, where $\nu = 1, 2, \ldots$.

9. Let now A be a countable torsion abelian l-group such that the group A'_∞ of all divisible elements of A is of finite rank; denote by $\upsilon_{\infty,\nu}$ the ν-th Ulm invariant of A'_∞. Then, except a finite number of ν, $\upsilon_{\infty,\nu}$ is equal to 0. In this case, we call $\upsilon_{\infty,\nu}$ the ν-th *infinite Ulm invariant* of A and, accordingly, call the ν-th Ulm invariant of A itself the ν-th *finite Ulm invariant* of A. Moreover, if A_∞ is the largest divisible subgroup of A, then we call the rank of A_∞ the *dimension* of A. Under this terminology, the theorem of Ulm[12] shows that the structure of A is determined whenever the finite and the infinite Ulm invariants of A as well as the dimension of A are known. The theorem also implies that A'_∞/A_∞ is a finite group because A'_∞/A_∞ contains no non-trivial divisible subgroup and its system of Ulm invariants coincides with that of a finite group.

Let l^{c_ν} be the number of elements of A'_∞ whose orders divide l^ν. Then since A'_∞ is isomorphic to the direct product A_∞ by the finite group A'_∞/A_∞, it follows from elementary properties of finite abelian groups that we have $\upsilon_{\infty,\nu} = 2c_\nu - c_{\nu-1} - c_{\nu+1}$. On the other hand, if T is a subgroup of finite rank of A containing A_∞, then we see, as in the case of $T = A'_\infty$ above, that T is isomorphic to the direct product of A_∞ by the finite group T/A_∞. Therefore, denoting by T_ν the group of elements of T whose orders divide l^ν, we can determine the dimension $\dim A$ of A by $l^{\dim A} = \lim_{\nu\to\infty} (T_{\nu+1} : T_\nu)$.

10. We are now able to expose the structure of the group X_l which is the l-component of the countable torsion abelian group X consisting of all the characters of Ω, where l is a prime number. Denote by $X'_{l,\infty}$ the group of all

[12] See Kaplansky [3], §11.

divisible elements of X_l. Then, by **6**, $X'_{l,\infty}$ is contained in the group T of characters $\chi \in X_l$ such that χ is unramified at any place $\mathfrak{q}$ of Ω coinciding with none of the prime factors of l in Ω. Since T is of finite rank, so is also $X'_{l,\infty}$. Therefore, the results of **9** show that the structure of X_l is determined whenever the finite and the infinite Ulm invariants and the dimension of X_l are known. By Lemma 6 and Lemma 7, we have

THEOREM 4. *Let l be a prime number and ζ_l be a primitive l-th root of unity. Denote by ν_l a natural number such that the field $\Omega(\zeta_l)$ contains a primitive l^{ν_l}-th root of unity but no primitive l^{ν_l+1}-th root of unity. Then the ν-th finite Ulm invariant of X_l is* 0 *for $\nu < \nu_l$ and is* ∞ *for $\nu \geqq \nu_l$.*

The largest divisible subgroup $X_{l,\infty}$ of X_l is contained in the group T defined above. Therefore, by **9** and by Lemma 11, we have

THEOREM 5. *Let l be a prime number, $\mathfrak{S} = \{\mathfrak{l}_1, \mathfrak{l}_2, \ldots\}$ be the set of all prime factors of l in Ω and $\Omega_{\mathfrak{l}_i}$ be the $\mathfrak{l}_i$-completion of Ω. Denote by* $\mathfrak{e}$ *the unit group of Ω and by $\mathfrak{e}_{l,\nu}$ the group of $\varepsilon \in \mathfrak{e}$ such that ε is an l^ν-th power in every $\Omega_{\mathfrak{l}_i}$. Then there is a constant μ_l such that we have $l^{\mu_l} = (\mathfrak{e}_{l,\nu} : \mathfrak{e}_{l,\nu+1})$ for every sufficiently large ν and the dimension of X_l is equal to $N - \mu_l$, where N is the absolute degree of Ω.*

11. There is thus remained only the determination of infinite Ulm invariants of X_l. But this is substantially done in § 3. For we obtained there a method of finding the number l^{c_ν} of elements in X_l whose orders divide a power l^ν of l. We add here a few remarks.

Let l^ν be a power of an add prime number l and $B^{(\nu)}$ be the group of $\beta \in \Omega^\times$ such that the principal ideal (β) is the l^ν-th power of an ideal of Ω. Let $\mathfrak{S}$ and $\Omega_{\mathfrak{l}_i}$ be as in Theorem 5, let $\mathfrak{w}_i$ be the group of roots of unity in $\Omega_{\mathfrak{l}_i}$ and let $B_*^{(\nu)}$ be the group of $\beta \in B^{(\nu)}$ such that β is in $\mathfrak{w}_i \Omega_{\mathfrak{l}_i}^{l^\nu}$ for every i. Then, by **6** and by Theorem 2, we have $l^{c_\nu} = h_\nu \cdot l^{N\nu} \cdot (B^{(\nu)} : B_*^{(\nu)})^{-1}$. Therefore, by **9**, the ν-th infinite Ulm invariant $\upsilon_{\infty,\nu}$ of X_l is given by

$$l^{\upsilon_{\infty,\nu}} = \frac{h_\nu^2}{h_{\nu-1} h_{\nu+1}} \quad \frac{(B^{(\nu-1)} : B_*^{(\nu-1)})(B^{(\nu+1)} : B_*^{(\nu+1)})}{(B^{(\nu)} : B_*^{(\nu)})^2},$$

where h_ν is the l^ν-class number of Ω. Let the first factor of the right side of this formula be equal to l^{b_ν}. Then b_ν is the number of direct factors of order

https://doi.org/10.1017/S0027763000022042 Published online by Cambridge University Press

l^{ν} in the direct decomposition of the ideal class group of Ω into indecomposable cyclic groups.

References

[1] H. Hasse, Zahlentheorie, Berlin (1949).
[2] H. Hasse, Zum Existenzsatz von Grunwald in der Klassenkörpertheorie, J. Reine Angew. Math., **188** (1950), pp. 40-64.
[3] I. Kaplansky, Infinite abelian groups, Univ. of Michigan Publ. in Math., No. **2** (1954).
[4] S. Wang, On Grunwald's theorem, Ann. of Math., **51** (1950), pp. 471-484.
[5] A. Weil, Sur la théorie du corps de classes, J. Math. Soc. Japan, **3** (1951), pp. 1-35.

Mathematical Institute
Nagoya University