Conspectus materiae tomi XX, fasciculi 4

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange | Address of the Editorial Board and of the exchange | Die Adresse der Schriftleitung und des Austausches | Адрес редакции и книгообмена

ACTA ARITHMETICA

ul. Śniadeckich 8, Warszawa 1

Les volumes IV et suivants sont à obtenir chez | Volumes from IV on are available at | Die Bände IV und folgende sind zu beziehen durch | Томы IV и следующие можно получить через

Ars Polona-Ruch, Krakowskie Przedmieście 7, Warszawa 1

Prix d'un fascicule | Price of an issue | Preis für ein Heft | Цена номера

$ 4.35

Les volumes I-III sont à obtenir chez | Volumes I-III are available at | Die Bände I-III sind zu beziehen durch | Томы I-III можно получить через

Johnson Reprint Corporation, 111 Fifth Ave., New York, N. Y.

PRINTED IN POLAND

W R O C Ł A W S K A   D R U K A R N I A   N A U K O W A

On relations between units of normal algebraic number fields and their subfields

by

JOSEPH LIANG* (Tampa, Fla)

Let K be a normal algebraic number field with Galois group $G(K/Q)$, where Q is the rational number field and $\{K_1, \ldots, K_u\}$ is a class of subfields of K. How much information about the arithmetic unit group U of K can one draw from the knowledge of the arithmetic unit groups U_i of K_i, for $i = 1, \ldots, u$? Before we give answers to this question, let us make the following investigation. We shall assume first of all the following groups are known:

G_i: the automorphism groups of K over K_i which are subgroups of G.

R_i: subgroups of U_i formed by the roots of unity.

R: subgroup of U formed by the roots of unity.

k: element of G that maps any element of K onto its complex conjugate.

Since K is normal over Q, we have the following two cases:

Case 1. $k = 1$, in this case K is totally real.

Case 1. $k \neq 1$, $k^2 = 1$, in this case K is totally complex.

Let n be the order of the group G and $G = \bigcup_{j=1}^{n_i} \sigma_{ij} G_i$ be the left coset decomposition of G over G_i with $n_i = [K_i : Q]$, for $1 \leqslant i \leqslant u$. The number s_i of conjugate subgroups $\sigma_{ij} G_i \sigma_{ij}^{-1}$ containing k is equal to the number of isomorphisms of K_i into $\mathscr{R}$, the real number field. Consequently, $n_i = s_i + 2t_i$, $0 \leqslant t_i \in Z$. Let $\overline{U} = U/R$ be the factor group of U mod R. Then by Dirichlet unit theorem ([1]), $\overline{U}$ is free abelian of rank $s+t-1$, where $s = n$ in case 1 and $s = 0$ in case 2 and the non-negative integer t

* The author wishes to express his thanks to Professor Zassenhaus for his help and to California Institute of Technology for granting him a post-doctoral fellowship during 1969–70.

is defined by $t = \frac{1}{2}(n-s)$. Furthermore, the factor group is free abelian of rank s_i+t_i-1 $(1 \leqslant i \leqslant u)$. We would like to know some answers to the following two questions:

A. What can we say about the rank of the free abelian group $\overline{V}$ where $\overline{V}$ is defined as

$$\overline{V} = \Big(\prod_{i=1}^{u} U_i\Big) R/R\,?$$

B. If we define the pure embedding group $\overline{V}^*$ of $\overline{V}$ in $\overline{U}$ as

$$\overline{V}^* = \{\varepsilon |\ \varepsilon \in \overline{U} \text{ and either } \varepsilon = 1 \text{ or } \langle\varepsilon\rangle \cap \overline{V} \neq 1\}$$

what can we say in regard to the index of $\overline{V}$ in $\overline{V}^*$? Can one establish some bound for it?

We discover soon that the case that $\{K_i, \ldots, K_u\}$ is a class of conjugate subfields of K is most interesting from the practical point of view. In the following, we shall have all groups U, U_i, V, V^* written additively. Then each of the groups concerned has a finite Z-basis. For each $\sigma \in G$, $\varepsilon/R \in \overline{U}$, define $\sigma(\varepsilon/R) = \sigma(\varepsilon)/R$. According to this definition, the module $\overline{U}$ can be considered as a proper G-module and hence $Q\overline{U}$ is a proper representation space of G of finite degree over Q. In what follows, we shall discuss the first case, and the second case will be briefly discussed in the end.

Let $\Delta_Q G$ be the augmentation ideal of the group algebra $Q[G]$ of G over Q and hence $\Delta_Q G$ is defined as

$$\Delta_Q G = \Big\{a|\ a = \sum_{g\in G}\lambda(g)g \text{ and for every } g\ (g\in G \text{ implies } \lambda(g)\in Q) \text{ and } \sum_{g\in G}\lambda(g) = 0\Big\}.$$

It follows that $\Delta_Q G = \sum_{\substack{g\in G\\ g\neq 1_G}} Q(g-1_G)$.

In this case, $Q\overline{U}$ is operator isomorphic to $\Delta_Q G$ and there is a G-isomorphism θ of $\overline{U}$ into the augmentation ideal $\Delta_Z G = \{a | a \in \Delta_Q G \cap Z[G]\}$ of the integral group ring $Z[G]$ of G over Z. In other words, $\theta\overline{U}$ is a left ideal of $Z[G]$ contained in $\Delta_Z G$. Any other G-isomorphism θ' of U in $Q[G]$ is obtained by setting $\theta' V = (\theta V)\Lambda$ when Λ is a unit of $\Delta_Q G$ such that $\Lambda \equiv 1 \pmod{\Delta_Q G}$. Hence $\theta\overline{U}$ is unique up to G-equivalence from the right. It follows from integral representation theory that there are only finitely many non-equivalent left ideals of $Z(G)$ of rank $n-1$ contained in $\Delta_Z G$. Some information on it may be obtained by studying the action G on the group U_i. If $\{K_1, \ldots, K_u\}$ is normal (i. e. invariant under G), then $\overline{V}$ is a two-sided ideal of $Z[G]$. Moreover, $\overline{V}^*$ is the intersection

of a two-sided ideal A of $Q[G]$ with $\theta\overline{U}$. If $X_1, X_2, \ldots, X_v$ are the irreducible characters of G with X_1 as the principal character, then A consists of the elements a of $Q[G]$ for which $X_i(ag) = 0$ $(g\in G)$ and either $i=1$ or $1 < i \leqslant v$ and $\sum_{g\in G_j} X_i(g) = 0$, $j = i, \ldots, u$. Hence, we have the following:

THEOREM 1. *Rank* $A = \sum X_j(1)^2$, *where the sum is taken over all characters* X_j *for which* $j>1$ *and* $\sum_{g\in G_h} X_j(g) > 0$ *for some* h *satisfying the inequality* $1 \leqslant h \leqslant u$(¹).

The following is true:

THEOREM 2. *If* K *is normal (totally real) algebraic number field of degree* n *over* Q, *with the Galois group* $G(K/Q) = S_m$ *or* A_m *for* $m>3$, *then there exists a proper subfield* K_1 *of* K *such that if* $\{K_1, \ldots, K_{u(K_1)}\}$ *is a class of conjugate subfields of* K_1, *then* $[\overline{U}:\overline{V}]$ *is finite, i. e.,* $\overline{V}$ *already contains* $n-1$ *independent units of* $\overline{U}$ *where* $\overline{U}$, $\overline{V}$ *are defined as previously.*

We need the following lemma to prove Theorem 2:

LEMMA 1. *Let* Γ *be a representation of* G *which affords the character* X. *Let* H *be the kernel of* X *and* 1_G *the identity element of* G. *Then*

1. $X(h) = X(1_G)$ *if and only if* $h\in H$;
2. *If* $|X(h)| = X(1_G)$ *then* h/H *is in the center of* G/H ([3]).

Now, proceed to show Theorem 2.

Let $X_1, \ldots, X_v$ be the set of all irreducible characters of G. It follows that v is equal to the number of conjugate classes of G. We know that ([2])

$$X_1^2(1_G) + X_2^2(1_G) + \ldots + X_v^2(1_G) = [G:1] \tag{1}$$

where 1_G denotes the identity of G. Let K_1 be the subfield of K which corresponds to the subgroup of G generated by the element of order 2, say $(12)(34)$ (since our hypothesis says $m \geqslant 4$, so $(12)(34)\in G$). Let $\{K_1, \ldots, K_u\}$ be the class of conjugate subfields of K. Assert $\overline{V}$ contains independent units of $\overline{U}$. By Theorem 1, rank $\overline{V} = \sum X_j^2(1_G)$ where the sum is taken over all characters X_j for which $j>1$ and $\sum_{g\in G_h} X_j(g) > 0$ for some h. From identity (1), we see that $X_2^2(1_G) + \ldots + X_v^2(1_G) = |G|-1$ and this already gives us the correct number of independent units. So if we can show that $X_j(a) + X_j(1_G) > 0$ for every j and for any element a in the conjugate class of $(12)(34)$ then we are done. This is equivalent to show that for all j and for any a in that conjugate class, $X_j(a) \neq -X_j(1_G)$. By Lemma 1, $|X_j(a)| = X_j(1_G)$ if and only if a/H is in the center

(¹) It suffices to verify this equation for only one of each class of conjugate subgroups of G among the normal set $\{G_1, G_2, \ldots, G_u\}$.

of G/H, where H is the kernel of X_j. If $m > 4$, H can only be G, A_m or 1. If $H = G$ then $X_j(a) = 1$ and if $H = A_m$ then $X_j(a) = 1$, since $a \in A_m$. But if $H = \{1_G\}$ and $X_j(a) = -X_j(1_G)$, then we have $a \in Z(G)$, the center of G. If we let $a = (12)(34)$, $b = (123) \in G$ then $ba \neq ab$, a contradiction. Therefore, $X_j(a) \neq -X_j(1_G)$. If $m = 4$, H can be G, A_4, V_4 or 1. The same argument can be applied to G, A_4, or 1. Now, let $H = V_4$, then $X_j(a) = 1$, since $a \in V_4$. This proves Theorem 2.

Let K be a normal real algebraic number field over Q with the Galois group $G(K/Q) = S_3$ and let K_1, K_2, K_3 be the conjugate subfields of K of degree 3 over Q corresponding to the subgroups $G_1 = \{(1), (12)\}$, $G_2 = \{(1), (23)\}$, $G_3 = \{(1), (13)\}$ respectively.

For the character table for S_3, we have ([2])

	C_1	C_2	C_3	
X_1	1	1	1	$C_1 = \{(1)\}$,
X_2	1	-1	1	$C_2 = \{(12), (23), (13)\}$,
X_3	2	0	-1	$C_3 = \{(123, (132)\}$.

Rank of $\overline{V} = \sum X_j^2(1)$, where $j > 1$ and $\sum_{g \in G_i} X_j(g) > 0$. Since $X_2(C_1) + X_2(C_2) = 0$, therefore the only choice of j is 3 and hence rank of $\overline{V} = X_3^2(1) = 2^2 = 4$.

However, K should have 5 independent units, where can we find the fifth independent unit? I assert it can be found in the quadratic field K_4 which corresponds to the normal subgroup A_3. A verification of this can be found on page 340.

In case $\overline{V}$ has full rank, then there exists a natural number m such that for every $u \in \overline{U}$, we have $u^m \in \overline{V}$. A bound for m can be found by the following four lemmas.

Lemma 2. *Let H be a subgroup of G and $\{H_1, \ldots, H_t\}$ a class of conjugate subgroups of G where $H = H_1$. Let ψ_1 be the principal character of H and X_{ψ_1} the character of G induced from ψ_1. If $G = \bigcup_{i=1}^{s} g_i H$ is the left coset decomposition of G over H, then*

$$\sum_{g \in G} X_{\psi_1}(g) g = \sum_{i=1}^{s} g_i H g_i^{-1}.$$

Proof. By definition, $X_{\psi_1}(g) = \sum_{i=1}^{s} \dot{\psi}_1(g_i^{-1} g g_i)$, where $\dot{\psi}_1(g) = 1$ if $g \in H$ and $\dot{\psi}_1(g) = 0$ otherwise. Thus

$$X_{\psi_1}(g) g = \sum_{i=1}^{s} \dot{\psi}_1(g_i^{-1} g g_i) g.$$

It follows that

$$\sum_{g \in G} X_{\psi_1}(g) g = \sum_{g \in G} \sum_{i=1}^{s} \dot{\psi}_1(g_i^{-1} g g_i) g = \sum_{i=1}^{s} \sum_{g \in G} \dot{\psi}_1(g_i^{-1} g g_i) g.$$

But $\dot{\psi}_1(g_i^{-1} g g_i) = 1$ if and only if $g_i^{-1} g g_i \in H$, this implies $g \in g_i H g_i^{-1}$. Therefore,

$$\sum_{g \in G} X_{\psi_1}(g) g = \sum_{i=1}^{s} \sum_{h \in H} g_i h g_i^{-1} = \sum_{i=1}^{s} g_i H g_i^{-1}.$$

Remark. From Lemma 2, it follows that if we let $f = [N_G(H) : H]$, where $N_G(H)$ is the normalizer of H in G, then

$$\sum_{g \in G} X_{\psi_1}(g) g = f \sum_{i=1}^{t} H_i.$$

Lemma 3. *Let H be as before and let $\{X_1, \ldots, X_r\}$ be the set of irreducible characters of G, then*

$$X_{\psi_1} = c_1 X_1 + c_2 X_2 + \ldots + c_r X_r, \quad \textit{where} \quad c_i = (1/[H:1]) \sum_{h \in H} X_i(h)$$

are non-negative integers.

Proof. By Frobenius reciprocity theorem, we have

$$c_i = (1/[H:1]) \sum_{h \in H} X_i(h) \dot{\psi}_1(h^{-1}).$$

Thus

$$c_i = (1/[H:1]) \sum_{h \in H} X_i(h)$$

since

$$\dot{\psi}_1(h^{-1}) = 1 \quad \text{for every } h \in H.$$

Lemma 4. *Let $H, \overline{U}, \overline{V}, c_i$ be defined as before. If rank $\overline{U}$ = rank $\overline{V}$, then $c_i \neq 0$ for $i = 1, \ldots, r$.*

Proof. By Lemma 3, $c_i = (1/[H:1]) \sum_{h \in H} X_i(h)$ and by Theorem 1, $\overline{V}$ is full rank if and only if for every i, $\sum_{h \in H} X_i(h) > 0$. Thus, for every i, $c_i \neq 0$.

Lemma 5. *Assume rank $\overline{U}$ = rank $\overline{V}$ and let $Q[G]$ be the group algebra of G over Q and $E_1, \ldots, E_r$ be the primitive central idempotent elements of $Q[G]$ such that $1 = E_1 + \ldots + E_r$. Then*

$$\sum_{g \in G} X_{\psi_1}(g) g = \sum_{i=1}^{r} a_i E_i,$$

where $a_i \in Q$ and for every i, $a_i \neq 0$.

Proof. We know that

$$E_j = (z_j/[G:1]) \Big(\sum_{i=1}^{r} X_j(C_i)(c_i) \Big),$$

where z_j is the degree of the representation Γ_j which affords the character X_j, C_i is the sum of the elements of the ith conjugate class of G and c_i are defined previously. Let $X_{\psi_1} = c_1 X_1 + \ldots + c_r X_r$. It follows from Lemma 4 that $c_i \neq 0$ and $c_i \in Z$. We then have

$$X_{\psi_1}(g)g = c_1 X_1(g)g + \ldots + c_r X_r(g)g,$$

and for every i, $c_i \neq 0$. Therefore,

$$\begin{aligned}\sum_{g\in G} X_{\psi_1}(g)g &= \sum_{g\in G} c_1 X_1(g)g + \ldots + \sum_{g\in G} c_r X_r(g)g\\ &= ([G:1]/z_1)c_1 E_1 + \ldots + ([G:1]/z_r)c_r E_r\\ &= a_1 E_1 + \ldots + a_r E_r = \sum_{i=1}^{r} a_i E_i,\end{aligned}$$

where $a_i = ([G:1]/z_i)c_i$, for every i, $a \neq 0$, since for every i, $c_i \neq 0$. This proves Lemma 5.

Now, we are ready to give a bound for the exponent m, where m is such that for every $u \in \overline{U}$, $u^m \in \overline{V}$. Combining Lemma 2 and Lemma 5, we obtain

$$f\sum_{i=1}^{u} H_i = \sum_{i=1}^{r} a_i E_i \tag{2}$$

where $f = [N_G(H):H]$ and $a_i = ([G:1]/z_i)c_i$.

Recall that $c_i = (1/[H:1]) \sum_{h\in H} X_i(h)$. Multiplying both sides of (2) by E_j, we obtain

$$fE_j \sum_{i=1}^{u} H_i = a_j E_j.$$

Therefore

$$[G:N_G(H)][H:1]fE_j \sum_{i=1}^{u} H_i = [G:N_G H][H:1]a_j E_j,$$

this implies

$$([G:N_G H][G:1])/z_j \sum_{h\in H} X_j(h) E_j \in Z[G] \sum H_i.$$

Let $m = \text{l.c.m.}\left([G:N_G H][G:1]/z_j \sum_{h\in H} X_j(h)\right)$.

Since $1 = E_1 + \ldots + E_r$, so $m = mE_1 + \ldots + mE_r$. If $u \in \overline{\overline{U}}$, then $u^m = u^{mE_1 + \ldots + mE_r} \in \overline{V}$.

We would like to make the following remark: In case $\overline{V}$ itself does not have full rank but $\overline{\overline{V}} = \overline{V} + \ldots + \overline{X}$ does, where each $\overline{V}, \ldots, \overline{X}$ corresponds to a class of conjugate subfields, then for each of them we find a bound for the exponent, say respectively $m(\overline{V}), \ldots, m(\overline{X})$. Let $m = \text{l.c.m.}\left(m(\overline{V}), \ldots, m(\overline{X})\right)$. Then one can see that m should be a bound for $\overline{\overline{V}}$. In certain special cases, our result can be sharpened as in the following theorem:

THEOREM 3. *Let $G(K/Q) = S_n$ or A_n, $n \geq 4$ and let K_1 be the subfield of K which is corresponding to the subgroup of G generated by* (12) (34), *then the exponent m defined above is bounded by $2\binom{n}{4}$.*

Proof. Let $C_{(12)(34)}$ be the class consisting of all elements of the form (12) (34) in G. Then $c = |C_{(12)(34)}| = n(n-1)(n-2)(n-3)/2^3$. Since c is divisible by 3, so we can separate the class $C_{(12)(34)}$ into $c/3$ disjoint sets, each of which containing three such elements and together with 1 they form a subgroup G_i of order 4. Let $E_1, \ldots, E_{c/3}$ be the subfields of K corresponding to these subgroups then $[E_i:Q] = |G|/4$. Since each group contains elements of the form (12) (34), so the E's are contained in our K_j's. By suitable numbering, we have for any arbitrary unit $u \in \overline{U}$, $u^{1+g_1+g_2+g_3} \in K_1$, $u^{1+g_4+g_5+g_6} \in K_2, \ldots,$ where $g_1, g_2, g_3 \in G_1$, $g_4, g_5, g^6 \in G_2, \ldots$ This implies $u^{1+g_1+g_2+g_3+1+g_4+g_5+g_6+\cdots} \in \overline{V}$. But $u^{1+g_1+1+g_2+\cdots} \in \overline{V}$, hence $u^{c-c/3} = u^{2\binom{n}{4}} \in \overline{V}$. This proves our Theorem.

In the following, I shall give a purely constructive method to determine the rank of $\overline{V}$ and a bound for the index of $\overline{V}$ in its pure embedding. In case $\overline{V}$ is of full rank, a bound for the index of $\overline{V}$ in $\overline{U}$ can be computed. Also, $\overline{V}$ does not necessarily correspond to one class of conjugate subfields, it may be the sum of modules corresponding to several classes. A computer program has been written for this purpose and the corresponding results for the simple group A_5 are obtained from our program and will be appended.

By Galois theory, we know that we can find a unit u_1 in K such that u_1 and all its conjugates generate a subgroup M of finite index m in U. Let $u_1, u_2, \ldots, u_{n-1}$ be a basis. Again, let $\overline{M} = M/R_M$, where R_M are roots of unity contained in M and let $\overline{u}_1, \ldots, \overline{u}_{n-1}$ be a basis for $\overline{M}$. Let $\mathscr{M}$ be the module generated by $me, mg_2e, \ldots, mg_ne$ where e is the idempotent element defined by $1 - 1/n \sum_{g\in G} g$ and g_i running over all elements of the group G. Consider the mapping $\varphi\colon \overline{M} \to \mathscr{M}$ defined by $\varphi(\overline{u}_i) = mg_ie$, $i = 1, \ldots, n-1$ and $g_1 = 1$. Clearly, one can see that φ is an operator isomorphism from $\overline{M}$ onto $\mathscr{M}$. Since $u \in \overline{U}$ implies $mu \in \overline{M}$, it follows that $\varphi(\overline{U}) \subset \mathscr{M}/m = \mathscr{M}^*$. Assert $[\mathscr{M}^* : \varphi(\overline{U})] \leq m^{n-1}$. Let $\overline{\overline{u}}_1, \ldots, \overline{\overline{u}}_{n-1}$ be a basis of $\varphi(\overline{U})$, let $v_i = g_ie$, $i = 1, \ldots, n-1$. We have

$$\begin{aligned}\overline{\overline{u}}_1 &= a_{1,1}v_1 + \ldots + a_{1,n-1}v_{n-1},\\ \overline{\overline{u}}_2 &= a_{2,1}v_1 + \ldots + a_{2,n-1}v_{n-1},\\ &\cdots\cdots\cdots\cdots\cdots\\ \overline{\overline{u}}_{n-1} &= a_{n-1,1}v_1 + \ldots + a_{n-1,n-1}v_{n-1}\end{aligned} \tag{3}$$

and

$$(4)\qquad \begin{aligned} mv_1 &= b_{1,1}\bar{\bar{u}}_1 + \ldots + b_{1,n-1}\bar{\bar{u}}_{n-1},\\ &\ldots\ldots\ldots\ldots\ldots\ldots\\ mv_{n-1} &= b_{n-1,1}\bar{\bar{u}}_1 + \ldots + b_{n-1,n-1}\bar{\bar{u}}_{n-1}. \end{aligned}$$

From (3) and (4) we obtain

$$\begin{bmatrix} b_{1,1} & \ldots & b_{1,n-1}\\ \cdot & \cdots & \cdot\\ b_{n-1,1} & \ldots & b_{n-1,n-1}\end{bmatrix}\begin{bmatrix} a_{1,1} & \ldots & a_{1,n-1}\\ \cdot & \cdots & \cdot\\ a_{n-1,1} & \ldots & a_{n-1,n-1}\end{bmatrix} = \begin{bmatrix} m & & \\ & m & 0\\ 0 & & \ddots \\ & & & m\end{bmatrix}$$

Thus

$$\left|\det\begin{bmatrix} a_{1,1} & \ldots & a_{1,n-1}\\ \cdot & \cdots & \cdot\\ a_{n-1,1} & \ldots & a_{n-1,n-1}\end{bmatrix}\right| \leqslant m^{n-1}$$

This implies

$$[\mathscr{M}^*: \varphi(\bar{U})] \leqslant m^{n-1}.$$

Let H be a subgroup of G. Denote by $\tilde{H}$ the sum of all elements $h \in H$, i. e. $\tilde{H} = \sum_{h\in H} h$. Let $\mathfrak{A}_H$ be the module generated by $\tilde{H}e, \tilde{H}g_2e, \ldots, Hg_{n-1}e$. Then $\mathfrak{A}_H$ has finite index in $\varphi(\bar{V}_H)$. For, let $b \in \varphi(\bar{V}_H)$, $b = a_1e + a_2g_2e + \ldots + a_{n-1}g_{n-1}e$, $a_i \in Z$. Thus

$$\bar{h}(b) = \tilde{H}(b) = a_i\tilde{H}e + \ldots + a_{n-1}\tilde{H}g_{n-1}e \in \mathfrak{A}_H, \quad \text{where} \quad \bar{h} = [H:1].$$

Let $\{H = H_1, H_2, \ldots, H_u\}$ be a class of conjugate subgroups of G and let $\mathfrak{A}_{H_i}$ be the corresponding modules. Further, let $\mathfrak{A} = \sum_{i=1}^{u}\mathfrak{A}_{H_i}$. It follows that $\mathfrak{A}$ has finite index in $\varphi(\bar{V})$. Our computer program will give ranks of the $\mathfrak{A}$'s which can be seen immediately equal to the ranks of the $\bar{V}$'s, and we give bound on the index of $\mathfrak{A}$ in its pure embedding in $\mathscr{M}^*$ and this is also a bound of the index of $\varphi(\bar{V})$ in its pure embedding in $\varphi(\bar{U})$ as can be seen from the following theorem:

THEOREM 4. *Let $\widehat{\varphi(\bar{V})}$ be the pure embedding of $\varphi(\bar{V})$ in $\varphi(\bar{U})$ and $\overline{\varphi(\bar{V})}$ be the pure embedding of $\widehat{\varphi(\bar{V})}$ in $\mathscr{M}^*$. Further, if $\hat{\mathfrak{A}}$ is the pure embedding of $\mathfrak{A}$ in $\mathscr{M}^*$ and $\widetilde{\varphi(\bar{V})}$ pure embedding of $\varphi(\bar{V})$ in $\mathscr{M}^*$, then we have $\hat{\mathfrak{A}} = \widetilde{\varphi(\bar{V})}$ and $\widetilde{\varphi(\bar{V})} = \overline{\varphi(\bar{V})}$.*

Proof. By definition,

$$\hat{\mathfrak{A}} = \{\alpha \in \mathscr{M}^* \mid \text{either } \alpha = 0 \text{ or } r\alpha \in \mathfrak{A} \text{ for some } r > 0\}$$

and

$$\widetilde{\varphi(\bar{V})} = \{\beta \in \mathscr{M}^* \mid \text{either } \beta = 0 \text{ or } s\beta \in \varphi(\bar{V}) \text{ for some } s > 0\}.$$

Firstly, let $0 \neq \alpha \in \hat{\mathfrak{A}}$. This implies there exists $r_\alpha > 0$ such that $r_\alpha\alpha \in \mathfrak{A} \subset \varphi(\bar{V})$. Hence $\alpha \in \widetilde{\varphi(\bar{V})}$. Thus, $\hat{\mathfrak{A}} \subseteq \widetilde{\varphi(\bar{V})}$. Conversely, let $0 \neq \beta \in \widetilde{\varphi(\bar{V})}$. This implies there exists $s_\beta > 0$ such that $s_\beta\beta \in \varphi(\bar{V})$. This implies $s_\beta h\beta \in \mathfrak{A}$. Thus $\beta \in \hat{\mathfrak{A}}$. This shows $\widetilde{\varphi(\bar{V})} \subseteq \hat{\mathfrak{A}}$. Therefore, $\hat{\mathfrak{A}} = \widetilde{\varphi(\bar{V})}$. Now, we want to show $\widetilde{\varphi(\bar{V})} = \overline{\varphi(\bar{V})}$. Let $0 \neq a \in \widetilde{\varphi(\bar{V})}$. This implies $a \in \mathscr{M}^*$ and there exists $s_a > 0$ such that $s_a a \in \varphi(\bar{V}) \subset \widehat{\varphi(\bar{V})}$. Thus $a \in \overline{\varphi(V)}$. Finally, let $0 \neq b \in \overline{\varphi(V)}$. This implies $b \in \mathscr{M}^*$ and there exists $r_b > 0$ such that $r_b b \in \widehat{\varphi(\bar{V})}$. This implies there exists s such that $sr_b b \in \varphi(\bar{V})$. Hence $b \in \widetilde{\varphi(\bar{V})}$ and this proves our theorem.

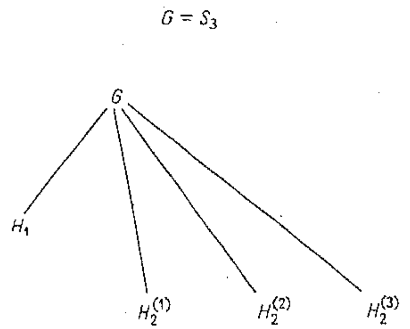
Remark. It follows from Theorem 4 that

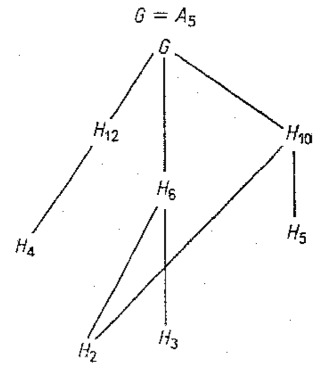
$$[\hat{\mathfrak{A}} : \mathfrak{A}] = [\overline{\varphi(\bar{V})} : \mathfrak{A}]$$

and further,

$$[\widehat{\varphi(\bar{V})} : \varphi(\bar{V})] \leqslant [\overline{\varphi(\bar{V})} : \mathfrak{A}].$$

We include here the results for the groups S_3 and A_5. The subgroup lattices of S_3 and A_5 are as follows:





We denote by H_i the class consisting of conjugate subgroups $H_i^{(1)}, H_i^{(2)}, \ldots, H_i^{(u)}$ and by $\mathfrak{A}_i^{(j)}$ the module generated by $\left(\sum_{h\in H_i^{(j)}} h\right)\mathscr{M}^*$ and $\mathfrak{A}_i = \sum_j \mathfrak{A}_i^{(j)}$, where $\mathscr{M}^*$ was defined previously. We shall give the index of $\mathfrak{A}_i$ in its pure embedding in $\mathscr{M}^*$ and the rank of $\mathfrak{A}_i$. In case $\mathfrak{A}_i$ is of full rank, the index of $\mathfrak{A}_i$ in $\mathscr{M}^*$ will be given. Finally, the rank of certain modules formed by the sum of $\mathfrak{A}_i$ and also their corresponding indices will be also considered. Again, we let the symbol $\hat{\mathfrak{A}}_i$ denote the pure embedding of $\mathfrak{A}_i$ in $\mathscr{M}^*$. Our results are as follows:

(I) $G = S_3$, $\quad H_3 = \{(1), (123), (132)\}$,

$$H_2^{(1)} = \{(1), (12)\},$$
$$H_2^{(2)} = \{(1), (13)\},$$
$$H_2^{(3)} = \{(1), (23)\},$$

$\mathfrak{A}_i$	rank	index
$\mathfrak{A}_3$	1	1
$\mathfrak{A}_2$	4	1
$\mathfrak{A}_2+\mathfrak{A}_3$	5	3

From this result, one can see that if K is a normal real algebraic number field over Q with Galois group $G(K/Q) = S_3$ and if K_1, K_2, K_3 are the conjugate subfields of K corresponding to the subgroups $H_2^{(1)}$, $H_2^{(2)}, H_2^{(3)}$ respectively, and $\overline{V}$ is the corresponding free abelian group and if u_1, u_2, u_3, u_4 are four independent units obtained from $\overline{V}$, then the fifth unit of K can be found in K_4 which is corresponding to H_3.

(II) $G = A_5$,

H_i = class of conjugate subgroups of order i, $\quad i = 12, 10, 6, 5, 4, 3, 2$

$\mathfrak{A}_i$	rank	index
$\mathfrak{A}_{12}$	16	2
$\mathfrak{A}_{10}$	25	2^{10}
$\mathfrak{A}_6$	41	$2^8\cdot 3$
$\mathfrak{A}_5$	43	2^8
$\mathfrak{A}_4$	41	2
$\mathfrak{A}_3$	59	$2^7\cdot 3$
$\mathfrak{A}_2$	59	2
$\mathfrak{A}_{12}+\mathfrak{A}_6$	41	$2^8\cdot 3$
$\mathfrak{A}_4+\mathfrak{A}_{10}$	41	1
$\mathfrak{A}_6+\mathfrak{A}_{10}$	41	2^8
$\mathfrak{A}_{12}+\mathfrak{A}_6+\mathfrak{A}_{10}$	41	2^8
$\mathfrak{A}_{12}+\mathfrak{A}_5$	59	$2^8\cdot 3^{16}\cdot 5^9$
$\mathfrak{A}_6+\mathfrak{A}_5$	59	$2^8\cdot 5^9$
$\mathfrak{A}_{12}+\mathfrak{A}_6+\mathfrak{A}_5$	59	$2^8\cdot 5^9$
$\mathfrak{A}_2+\mathfrak{A}_5$	59	1
$\mathfrak{A}_2+\mathfrak{A}_3$	59	1
$\mathfrak{A}_4+\mathfrak{A}_6$	41	1
$\mathfrak{A}_4+\mathfrak{A}_5$	59	$2^8\cdot 5^9$

It can be seen clearly from our table that the following modules are of full rank: $\mathfrak{A}_3, \mathfrak{A}_2, \mathfrak{A}_{12}+\mathfrak{A}_5, \mathfrak{A}_{12}+\mathfrak{A}_6+\mathfrak{A}_5, \mathfrak{A}_2+\mathfrak{A}_5, \mathfrak{A}_2+\mathfrak{A}_3$ and $\mathfrak{A}_4+\mathfrak{A}_5$. Among all these modules both $\mathfrak{A}_2+\mathfrak{A}_5$ and $\mathfrak{A}_2+\mathfrak{A}_3$ have index 1 in their pure embedding. This is to say that we can obtain a system of fundamental units for the field K by either adjoining the units of the subfield which correspond to $\mathfrak{A}_2$ and of the subfields which corresponds to $\mathfrak{A}_5$, or adjoining the units of the subfields which correspond to $\mathfrak{A}_2$ and $\mathfrak{A}_3$. For all other ones, the indices are non-trivial and a system of fundamental unit can be obtained by extracting roots of elements in the subfields and we assume this can be done.

Let us now compare our results obtained for A_5 with Theorem 1. Let C_1, C_2, C_3, C_4, C_5 be the conjugate sets consisting of identity, the operations of order 2, those of order 3 and the two sets of order 5 respectively in the group A_5.

For the character table of A_5, we have ([3])

	C_1	C_2	C_3	C_4	C_5
X_1	1	1	1	1	1
X_2	3	-1	0	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
X_3	3	-1	0	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$
X_4	4	0	1	-1	-1
X_5	5	1	-1	0	0

1. $\mathfrak{A}_{12}$: Each subgroup of H_{12} consists of 3 elements in C_2 and 8 elements in C_3. Hence, rank of $\mathfrak{A}_{12} = 16$ [2].
2. $\mathfrak{A}_{10}$: Each subgroup in H_{10} consists of 2 elements in C_4, 2 elements in C_5 and 5 elements in C_2. Hence, rank of $\mathfrak{A}_{10} = 25$.
3. $\mathfrak{A}_6$: Each subgroup in H_6 consists of 3 elements in C_2 and 2 elements in C_3. Hence, rank of $\mathfrak{A}_6 = 5^2+4^2 = 41$.
4. $\mathfrak{A}_5$: Each subgroup in H_5 consists of 2 elements in C_4 and 2 elements in C_5. Hence, rank of $\mathfrak{A}_5 = 3^2+3^2+5^2 = 43$.
5. $\mathfrak{A}_4$: Each subgroup in H_4 consists of 3 elements in C_2. Hence, rank of $\mathfrak{A}_4 = 4^2+5^2 = 41$.
6. $\mathfrak{A}_3$: Each subgroup in H_3 consists of 2 elements in C_3. Hence, rank of $\mathfrak{A}_3 = 3^2+3^2+4^2+5^2 = 59$.
7. $\mathfrak{A}_2$: Each subgroup in H_2 consists of 1 element in C_2. Hence, rank of $\mathfrak{A}_2 = 3^2+3^2+4^2+5^2 = 59$.

(2) In each of the seven cases, the group also contains one element from C_1. But this does not effect the rank of the corresponding $\mathfrak{A}_i$.

If we compare these results with those given in the table, we see that they agree with each other in all cases. It should be remarked here that there are groups, e. g., G_8, the quaternion group of order 8, and $T = \langle a, b\rangle$, $a^6 = 1$, $b^2 = a^3 = (ab)^2$, for which no submodule of full rank can be obtained in case K is totally real.

If K is totally complex, i. e., $k \neq 1$, the situation is slightly different. However, our results obtained from the real case can be applied here. Let G be a group of finite order n, let $G_1, \ldots, G_s$ be a set of subgroups that is closed under the inner automorphism of G. Again, let

$$\Delta_Z[G] = \Big\{\sum_{g\in G}\lambda(g)g \mid \lambda(g)\in Z \text{ for all } g \text{ of } G \text{ and } \sum_{g\in G}\lambda(g) = 0\Big\}.$$

Define

$$A = A(G_1, \ldots, G_s) = \sum_{i=1}^{s}\sum_{g\in G_i} g\,\Delta_Z[G].$$

Clearly, A is a two-sided ideal of $Z[G]$ depending only on $G_1, \ldots, G_s$. It follows that $QA = E_0Q[G]$, where E_0 is a certain central idempotent of $Q[G]$. We have determined already a bound m such that $0 < m\in Z$, $mE_0\in A$. In the case K is non-real, set $e = \big((1+k)/2\big) - (1/n)\sum_{g\in G} g$, where k is a certain element of order 2 in G and set $M = Q[G]e \cap Z[G]$. As remarked before, there exists an operator isomorphism θ from $\overline{U}$ into M. It follows that the left ideal $\theta\overline{U}$ of M is of finite index in M. Let $\overline{U}_i$ also have the same meaning as before. Then the submodules $\theta\overline{U}_i$ can be defined as follows:

$$\theta\overline{U}_i = \{x \mid x\in\theta\overline{U} \text{ and for every } g_i \ (g_i\in G \text{ implies } g_ix = 0)\}, \quad 1 \leqslant i \leqslant s.$$

Let $\overline{V} = \sum_{i=1}^{s}\theta\overline{U}_i$ and the pure embedding $\hat{V}$ of $\overline{V}$ in $\theta\overline{U}$ is defined as:

$$\hat{V} = \{x \mid x\in\theta\overline{U} \text{ and either } x = 0 \text{ or } Z\hat{V}\cap\overline{V} \neq 0\}.$$

It follows that $x = E_0x$ for $x\in\hat{V}$ and $(mE_0)x\in\overline{V}$. Hence $m\hat{V} \subseteq \overline{V}$.

Our constructive method given previously can be applied for the complex case. We only have to make some changes to the module M and the idempotent element e. We shall do this in the next paragraph.

Again, by Galois theory, the maximum real subfield Ω of K belongs to the subgroup of order 2. And we can choose a unit u_1 in Ω such that u_1 and all its conjugates generate a subgroup M of finite index m in U. Let $u_1, \ldots, u_{n/2-1}$ be a basis for M and $\overline{u}_1, \ldots, \overline{u}_{n/2-1}$ the corresponding basis for $\overline{M} = M/R_M$. Let $H = \langle k\rangle$, and let the idempotent element e of $Q[G]$ be defined as $e = 1/2\big(\sum_{h\in H} h\big) - 1/n\sum_{g\in G} g$. Let $G = \bigcup_{i=1}^{n/2} g_iH$ be the left coset decomposition of G over H and let $\mathscr{M}$ be the module generated by $(m/2)\sum he$, $(m/2)g_2\sum he, \ldots, (m/2)g_{n/2}\sum he$. Define our mapping by

$$\varphi\colon \overline{M} \to \mathscr{M} \equiv \varphi(\overline{u}_i) = (m/2)g_i\sum he = mg_ie, \quad i = 1, \ldots, n/2-1, \quad g_1 = 1.$$

Again, φ is an operator isomorphism and let $\mathscr{M}^* = \mathscr{M}/m$. It follows that $\varphi(\overline{U})$ has finite index in $\mathscr{M}^*$. Let $\mathfrak{A}_{H_i}$ be defined as in the real case and let $\mathfrak{A} = \bigcup_{i=1}^{u}\mathfrak{A}_{H_i}$. Then $\mathfrak{A}$ has finite index in $\varphi(\overline{V})$. Again, our computer program will give ranks of the $\mathfrak{A}$'s which can be seen equal to the ranks of $\overline{V}$'s. And we will give bound on the index of $\mathfrak{A}$ in its pure embedding in $\mathscr{M}^*$ and this is also a bounds of the index of $\varphi(\overline{V})$ in its pure embedding in $\varphi(\overline{U})$ by Theorem 4.

We are including here corresponding results for the group A_5 which are as follows:

$\mathfrak{A}_i$	rank	index
$\mathfrak{A}_{12}$	8	1
$\mathfrak{A}_{10}$	16	2^{10}
$\mathfrak{A}_6$	23	$2^9\cdot 3$
$\mathfrak{A}_5$	21	2^4
$\mathfrak{A}_4$	24	2^7
$\mathfrak{A}_3$	29	$2^3\cdot 3$
$\mathfrak{A}_2$	29	2
$\mathfrak{A}_{12}+\mathfrak{A}_6$	23	$2^8\cdot 3$
$\mathfrak{A}_4+\mathfrak{A}_{10}$	25	2^6
$\mathfrak{A}_6+\mathfrak{A}_{10}$	24	2^9
$\mathfrak{A}_{12}+\mathfrak{A}_6+\mathfrak{A}_{10}$	24	2^9
$\mathfrak{A}_{12}+\mathfrak{A}_5$	29	$2^4\cdot 3^3\cdot 5^3$
$\mathfrak{A}_6+\mathfrak{A}_5$	29	$2^4\cdot 5^3$
$\mathfrak{A}_{12}+\mathfrak{A}_6+\mathfrak{A}_5$	29	$2^4\cdot 5^3$
$\mathfrak{A}_2+\mathfrak{A}_5$	29	1
$\mathfrak{A}_2+\mathfrak{A}_3$	29	1
$\mathfrak{A}_4+\mathfrak{A}_6$	24	2^6
$\mathfrak{A}_4+\mathfrak{A}_5$	29	$2^4\cdot 5^2$

References

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

[2] C. W. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, New York 1962.

[3] W. Feit, *Characters of Finite Groups*, New York 1967.

[4] D. Hilbert, *Bericht über die Theorie der algebraischen Zahlkörper*, Jahresbericht der Deutschen Mathematiker — Vereinigung 4 (1894–1895), pp. 175–546.
[5] H. Nehrkorn, *Über absolute Idealklassengruppen und Einheiten in algebraischen Zahlkörpern*, Abh. Math. Sem. Uni. Hamburg 9 (1933), pp. 318–334.
[6] M. J. Weiss, *Fundamental systems of units in normal fields*, Amer. J. Math. 58 (1936), pp. 249–254.

UNIVERSITY OF SOUTH FLORIDA
Tampa, Florida

Received on 24. 12. 1970 (175)

ACTA ARITHMETICA
XX (1972)

Sur la repartition modulo 1 de la suite $n\alpha$

par

JACQUES LESCA (Talence)

§ 1. Introduction. Principaux resultats. Identifions le tore $T = \boldsymbol{R}/Z$ à un cercle orienté de longueur 1, muni d'une origine 0.

Si β est un point de T, $\{\beta\}$ désigne le représentant de β dans $\boldsymbol{R}$ caractérisé par

$$0 \leqslant \{\beta\} < 1.$$

Si β, γ sont des points distincts de T, $[\beta, \gamma[$ désigne l'*arc* défini par

$$\begin{array}{ll} \{\delta \in T:\ \{\beta\} \leqslant \{\delta\} < \{\gamma\}\}, & \text{si } \{\beta\} < \{\gamma\}, \\ \{\delta \in T:\ \{\delta\} < \{\gamma\} \text{ ou } \{\delta\} \geqslant \{\beta\}\}, & \text{si } \{\beta\} > \{\gamma\}. \end{array}$$

L'arc $]\beta, \gamma]$ est défini à partir de $[\beta, \gamma[$ par suppression de β et adjonction de γ.

Par la suite, *α est un irrationnel de T.*

On définit, pour $\beta, \gamma \in T$, $u \in \boldsymbol{N}^*$:

$$\begin{aligned} \Pi^+(\beta, \gamma; u) &= \operatorname{card}\{n:\ n\alpha \in\,]\beta, \gamma];\ 1 \leqslant n \leqslant u\}, \\ \Pi^-(\beta, \gamma; u) &= \operatorname{card}\{n:\ n\alpha \in [\beta, \gamma[;\ 0 \leqslant n \leqslant u-1\}, \\ E^+(\beta, \gamma; u) &= \Pi^+(\beta, \gamma; u) - u \operatorname{mes}(]\beta, \gamma]) \end{aligned}$$

(mes $]\beta, \gamma]$ désignant la longueur de l'arc $]\beta, \gamma]$)

$$E^-(\beta, \gamma; u) = \Pi^-(\beta, \gamma; u) - u \operatorname{mes}([\beta, \gamma[)$$

enfin, pour $\beta = 0$, on pose:

$$\begin{aligned} E^+(\gamma; u) &= E^+(0, \gamma; u), \\ E^-(\gamma; u) &= E^-(0, \gamma; u). \end{aligned}$$

Ce papier est consacré à *l'étude des fonctions E^+ et E^-.*

THÉORÈME A (Relation de réciprocité). *Pour tout $\beta \in T$, $u, v \in \boldsymbol{N}^*$*

$$E^+(\beta, \beta + u\alpha; v) = E^-(-\beta, -\beta + v\alpha; u)$$