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 \( \{ K_i \} \) 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 \( i = 1, \ldots, n \)? 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.
- \( B_i \): subgroup of \( U_i \) 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 2. \( k \neq 1 \), \( k^n = 1 \), in this case \( K \) is totally complex.

Let \( n \) be the order of the group \( G \) and \( G = \bigcup a_i G_i \) be the left coset decomposition of \( G \) over \( G_i \), with \( a_i = [K_i:Q] \), for \( 1 \leq i \leq n \). The number \( s_i \) of conjugate subgroups \( a_i G_i a_i^{-1} \) containing \( k \) is equal to the number of isomorphisms of \( K_i \) into \( \mathbb{G} \), the real number field. Consequently, \( a_i = a_i + 2a_i, 0 \leq a_i \leq Z \). Let \( \bar{U} = U/R \) be the factor group of \( U \mod R \). Then by Dirichlet unit theorem \((1)\), \( U \) is free abelian of rank \( s + 1 = 1 \), 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 \( n_i - 1 \) \((1 \leq i \leq u)\). 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

\[
\overline{V} = \left( \prod_{i=1}^{u} U_i \right) R/R^1
\]

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

\[
\overline{V}^* = \{ \epsilon \in \overline{U} \text{ and either } \epsilon = 1 \text{ or } \{ \epsilon \} \cap \overline{V} \neq 1 \}
\]

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 \( \{ K_1, \ldots, K_u \} \) 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 \( U, U_1, V, V^* \) written additively. Then each of the groups concerned has a finite \( Z \)-basis. For each \( \sigma \in G, \epsilon \in \overline{U} \), define \( \sigma \epsilon/R = \sigma(\epsilon)/R \). According to this definition, the module \( \overline{U} \) can be considered as a proper \( G \)-module and hence \( \overline{U}/V \) 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 \( \Delta_1 \) be the augmentation ideal of the group algebra \( Q[G] \) of \( G \) over \( Q \) and hence \( \Delta_1 \) is defined as

\[
\Delta_1 G = \{ a | a = \sum_{g \in G} \lambda(g) g \text{ and for every } g \in G \text{ implies } \lambda(g) \epsilon Q \text{ and } \sum_{g \in G} \lambda(g) = 0 \}.
\]

It follows that \( \Delta_1 G = \sum_{g \in G} Q(g-1) \).

In this case, \( \overline{U} \) is operator isomorphic to \( \Delta_1 G \) and there is a \( G \)-isomorphism \( \theta \) of \( \overline{U} \) into the augmentation ideal \( \Delta_1 G \) of \( \sum_{g \in G} Q(g-1) \) of the integral group ring \( Z[G] \) of \( G \) over \( Z \). In other words, \( \theta \) is a left ideal of \( Z[G] \) contained in \( \Delta_1 G \). Any other \( G \)-isomorphism \( \theta' \) of \( U \) in \( Q[G] \) obtained by setting \( \theta' \overline{V} = \theta \overline{V} \) when \( \Delta_1 G \) is a unit of \( \Delta_1 G \) such that \( \theta \theta' \theta = \theta \) (mod \( \Delta_1 G \)). 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 \( \Delta_1 G \). Some information on it may be obtained by studying the addition \( G \) on the group \( U \). 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 \( \overline{X}_1, \overline{X}_2, \ldots, \overline{X}_u \) are the irreducible characters of \( G \) with \( \overline{X}_i \) as the principal character, then \( A \) consists of the elements \( \epsilon \) of \( Q[G] \) for which \( \overline{X}_j(\epsilon) = 0 \) \((j \neq i)\) and either \( i = 1 \) or \( 1 \leq i < p \) and \( \sum_{\epsilon \in X_j} \lambda(g) = 0 \). Hence, we have the following:

**Theorem 1.** Rank \( \Lambda = \sum_{j=1}^{u} \lambda_j \) where the sum is taken over all characters \( \overline{X}_j \) for which \( j > 1 \) and \( \sum_{\epsilon \in X_j} \lambda(g) > 0 \) for some \( k \) satisfying the inequality \( 1 \leq k \leq u \).

The following is true:

**Theorem 2.** If \( K \) is normal (totally real) algebraic number field of degree \( n \) over \( Q \), with the Galois group \( G \) of \( G/K \), then there exists a proper subgroup \( K_1 \) of \( K \) such that \( K \) is contained in \( \{ K_1, \ldots, K_u \} \) is a class of conjugate subfields of \( K_1 \) then \( \overline{V}/V \) is finite, i.e., \( V \) contains \( n-1 \) independent units of \( U \) where \( \overline{U} \) is defined as previously.

We need the following lemma to prove Theorem 2:

**Lemma 1.** Let \( I \) be a representation of \( G \) which affords the character \( X \).

Let \( \Lambda \) be the kernel of \( I \) and \( \lambda_0 \) the identity element of \( G \). Then

1. \( X(1) = \lambda_1(1) \) if and only if \( h(1) \in \Lambda \);
2. If \( X(h) = \lambda_1(1) \) then \( h(1) \) is in the center of \( G/\Lambda \) (13).

Now, proceed to show Theorem 2.

Let \( X_1, \ldots, X_u \) be the set of all irreducible characters of \( G \). It follows that \( \lambda \) is equal to the number of conjugate classes of \( G \). We know that \( (12) \)

\[
X_1(1) + X_2(1) + \ldots + X_u(1) = [G : 1]
\]

where \( 1 \) denotes the identity of \( G \). Let \( K \) be the subfield of \( K \) which corresponds to the subgroup of \( G \) generated by the element of order 2, say \( (12) \) (since our hypothesis says \( m > 4 \), so \( (12) \) is in \( G \)). Let \( \{ K_1, \ldots, K_u \} \) be the class of conjugate subfields of \( K \). Assume \( \overline{V} \) contains independent units of \( G \). By Theorem 1, rank \( \overline{V} = \sum_{j=1}^{u} \lambda_j \) where the sum is taken over all characters \( X_j \) for which \( j > 1 \) and \( \sum_{\epsilon \in X_j} \lambda(g) > 0 \) for some \( k \). From identity (1), we see that \( X_1(1) \) is independent of \( \lambda_j \) for any \( j \) 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, \( \overline{X}_j(\epsilon) \neq -\overline{X}_j(\epsilon) \). By Lemma 1, \( |X_j(\epsilon)| = \overline{X}_j(1) \) if and only if \( s/H \) is in the center.

\(^{(1)}\) It suffices to verify this equation only for one 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 $a \neq A_m$. But if $H = (1_2)$ and $X_j(a) = -X_j(1_2)$, then we have $a \in Z(G)$, the center of $G$. If we let $a = (12) (34), b = (123)$, then $ba \neq ab$, a contradiction. Therefore, $X_j(a) = -X_j(1_2)$, 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 $G_i = \{(1), (12), (13), (23), (123), (132)\}$. For the character table for $S_3$, we have (2)

<table>
<thead>
<tr>
<th>Table</th>
<th>Character</th>
<th>$C_1$</th>
<th>$C_2$</th>
<th>$C_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$X_1$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>$C_1 = {(1)}$</td>
</tr>
<tr>
<td>$X_2$</td>
<td>1</td>
<td>-1</td>
<td>1</td>
<td>$C_2 = {(12), (23), (13)}$</td>
</tr>
<tr>
<td>$X_3$</td>
<td>2</td>
<td>0</td>
<td>-1</td>
<td>$C_3 = {(123), (132)}$</td>
</tr>
</tbody>
</table>

Ranks of $\overline{V} = \sum_{i=1}^{3} X_j(1_i)$, where $j > 1$ and $\sum_{i=1}^{3} X_j(1_i) = 0$, since $X_j(C_1) = +X_j(C_2) = 0$, therefore the only choice of $j$ is 3 and hence rank of $\overline{V} = X_3(1_3) = 2^3 = 8$.

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 $K_2$ 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 $u \in U$, we have $u^m \in V$. A bound for $m$ can be found by the following four lemmas.

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

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

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

$$X_{V_i}(g) = \sum_{i=1}^{s} \psi_i(g_i^{-1} g g_i) g.$$  

It follows that

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

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

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

**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

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

**Lemma 3.** Let $H$ be a subgroup of $G$ and $\{X_1, \ldots, X_s\}$ be the set of irreducible characters of $G$, then

$$X_{\psi_i} = c_1 X_1 + c_2 X_2 + \ldots + c_s X_s,$$  

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

are non-negative integers.

**Proof.** By Frobenius reciprocity theorem, we have

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

Thus

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

since

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

**Lemma 4.** Let $H, \overline{V}, \psi_i, c_i$ be defined as before. If rank $\overline{U} = \dim \overline{V}$, 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 $\overline{U} = \dim \overline{V}$ 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 $H = E_1 + \ldots + E_r$. Then

$$\sum_{g \in H} X_{\psi_i}(g) = \sum_{i=1}^{s} \sum_{g \in H} g_i H g_i^{-1} = \sum_{i=1}^{s} \sum_{g \in H} g_i H g_i^{-1} = \sum_{i=1}^{s} \sum_{g \in H} g_i H g_i^{-1} \psi_i(g_i^{-1} g g_i),$$  

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

**Proof.** We know that

$$E_j = (c_j/[G : 1]) \left( \sum_{i=1}^{r} X_i(C_i)(c_i) \right),$$  

then

$$\sum_{g \in H} X_{\psi_i}(g) = \sum_{i=1}^{s} \sum_{g \in H} g_i H g_i^{-1} = \sum_{i=1}^{s} \sum_{g \in H} g_i H g_i^{-1} \psi_i(g_i^{-1} g g_i),$$  

where $a_i \in Q$ and for every $i, a_i \neq 0$.
where $x_i$ is the degree of the representation $I_i$ which affords the character $X_i$, $c_i$ is the sum of the elements of the $i$th conjugate class of $G$ and $c_i$ are defined previously. Let $X_0 = c_0 X_0 + \ldots + c_r X_r$. It follows from Lemma 4 that $c_i \neq 0$ and $c_i \in \mathbb{Z}$. We then have

$$X_{x_i}(g) = c_i X_i(g) + \ldots + c_r X_r(g),$$

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

$$\sum_{i=0}^{r} X_{x_i}(g) = \sum_{i=0}^{r} c_i X_i(g) + \ldots + \sum_{i=0}^{r} c_r X_r(g)$$

$$= (\{G : 1\} | x_1) c_1 E_1 + \ldots + (\{G : 1\} | x_r) c_r E_r$$

$$= c_1 E_1 + \ldots + c_r E_r = \sum_{i=1}^{r} c_i E_i,$$

where $a_i = (\{G : 1\} | x_i) c_i$, for every $i$, $a_i \neq 0$, 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 $u \in U$, $uw^m \in V$. Combining Lemma 2 and Lemma 5, we obtain

$$(2) \quad f \sum_{i=1}^{r} H_i = \sum_{i=1}^{r} a_i E_i$$

where $f = \lceil N_G(H) : H \rceil$ and $a_i = (\{G : 1\} | x_i) c_i$.

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

$$f E_j \sum_{i=1}^{r} H_i = a_i E_j.$$

Therefore

$$(\{G : N_G(H)\} | H) f E_j \sum_{i=1}^{r} H_i = (\{G : N_G(H)\} | H) a_i E_j,$$

this implies

$$(\{G : N_G(H)\} | G | H) E_j \sum_{i=1}^{r} H_i = (\{G : N_G(H)\} | G | H) a_i E_j.$$
and
\[ m_{n-1} = b_{1,1}v_1 + \ldots + b_{1,n-1}v_{n-1}, \]
\[ \vdots \]
\[ m_{n-1} = b_{n-1,1}v_1 + \ldots + b_{n-1,n-1}v_{n-1}. \]
From (3) and (4) we obtain
\[ \begin{bmatrix} b_{1,1} & \cdots & b_{1,n-1} \\ \vdots & \ddots & \vdots \\ b_{n-1,1} & \cdots & b_{n-1,n-1} \end{bmatrix} \begin{bmatrix} a_{1,1} & \cdots & a_{1,n-1} \\ \vdots & \ddots & \vdots \\ a_{n-1,1} & \cdots & a_{n-1,n-1} \end{bmatrix} = \begin{bmatrix} m_1 & 0 \\ 0 & \cdots & 0 \end{bmatrix} \]
Thus
\[ \det \begin{bmatrix} a_{1,1} & \cdots & a_{1,n-1} \\ \vdots & \ddots & \vdots \\ a_{n-1,1} & \cdots & a_{n-1,n-1} \end{bmatrix} \leq m^{n-1} \]
This implies
\[ [\mathcal{M}^*: \varphi(\mathcal{U})] \leq m^{n-1}. \]

Let \( \mathcal{H} \) be a subgroup of \( G \). Denote by \( \bar{\mathcal{H}} \) the sum of all elements \( b \in \mathcal{H} \), i.e., \( \bar{\mathcal{H}} = \sum_{b \in \mathcal{H}} b \). Let \( \mathcal{M}_H \) be the module generated by \( \bar{\mathcal{H}}, \bar{\mathcal{H}}a_1, a_2, \ldots, a_{n-1}, 0 \).

Then \( \mathcal{M}_H \) has finite index in \( \varphi(\mathcal{V}_H) \). For, let \( b \in \varphi(\mathcal{V}_H) \), \( b = a_1 e + a_2 g_2 e + \ldots + a_{n-1} g_{n-1} e, a_i \in \mathcal{Z} \). Thus
\[ \bar{h}(b) = \bar{h}(b) = a_1 \bar{h}e + \ldots + a_{n-1} \bar{h}g_{n-1} e \in \mathcal{M}_H, \quad \text{where} \quad \bar{h} = [H : 1]. \]

Let \( \{ \mathcal{H}_1, \mathcal{H}_2, \ldots, \mathcal{H}_n \} \) be a class of conjugate subgroups of \( G \) and let \( \mathcal{M}_{H_i} \) be the corresponding modules. Further, let \( \mathcal{M} = \sum \mathcal{M}_{H_i} \). It follows that \( \mathcal{M} \) has finite index in \( \varphi(\mathcal{V}) \). Our computer program will give ranks of the \( \mathcal{M}_i \)'s which can be seen immediately equal to the ranks of the \( \mathcal{V}_H \)'s, and we give bound on the index of \( \mathcal{M} \) in its pure embedding in \( \mathcal{M}^* \) and this is also a bound of the index of \( \varphi(\mathcal{V}) \) in its pure embedding in \( \varphi(\mathcal{U}) \) as can be seen from the following theorem:

**Theorem 4.** Let \( \varphi(\mathcal{V}) \) be the pure embedding of \( \varphi(\mathcal{V}) \) in \( \varphi(\mathcal{U}) \) and \( \varphi(\mathcal{V}) \) be the pure embedding of \( \varphi(\mathcal{V}) \) in \( \mathcal{M}^* \). Further, if \( \hat{\mathcal{U}} \) is the pure embedding of \( \mathcal{U} \) in \( \mathcal{M}^* \) and \( \varphi(\mathcal{V}) \) pure embedding of \( \varphi(\mathcal{V}) \) in \( \mathcal{M}^* \), then we have \( \hat{\mathcal{U}} = \varphi(\mathcal{V}) \) and \( \varphi(\mathcal{V}) = \varphi(\mathcal{V}). \)

**Proof.** By definition,
\[ \hat{\mathcal{U}} = \{ \alpha \in \mathcal{M}^* \mid \text{either } \alpha = 0 \text{ or } r\alpha \in \mathcal{U} \text{ for some } r > 0 \}. \]

and
\[ \varphi(\mathcal{V}) = \{ \beta \in \mathcal{M}^* \mid \text{either } \beta = 0 \text{ or } s\beta \in \varphi(\mathcal{V}) \text{ for some } s > 0 \}. \]

Firstly, let \( 0 \notin a \in \hat{\mathcal{U}}. \) This implies there exists \( r > 0 \) such that \( r\alpha \in \mathcal{U} \subset \varphi(\mathcal{V}). \) Hence \( \mathcal{U} \subset \varphi(\mathcal{V}). \) Conversely, let \( 0 \notin \beta \in \varphi(\mathcal{V}). \) This implies there exists \( s > 0 \) such that \( s\beta \in \mathcal{V}. \) This implies \( s\beta \in \mathcal{M}^* \). Thus \( \beta \in \hat{\mathcal{U}} \). This shows \( \varphi(\mathcal{V}) \subset \mathcal{U}. \) Therefore, \( \hat{\mathcal{U}} = \varphi(\mathcal{V}). \) Now, we want to show \( \varphi(\mathcal{V}) \subset \varphi(\mathcal{V}). \) Let \( 0 \notin \alpha \in \varphi(\mathcal{V}). \) This implies \( \alpha \in \mathcal{M}^* \) and there exists \( s > 0 \) such that \( s\alpha \in \varphi(\mathcal{V}). \) Thus \( \alpha \in \varphi(\mathcal{V}). \) Finally, let \( 0 \notin \beta \in \varphi(\mathcal{V}). \) This implies \( \beta \in \mathcal{M}^* \) and there exists \( t > 0 \) such that \( t\beta \in \varphi(\mathcal{V}). \) This implies there exists \( s \) such that \( st\beta \in \varphi(\mathcal{V}). \) Hence \( \beta \in \varphi(\mathcal{V}) \) and this proves our theorem.

**Remark.** It follows from Theorem 4 that
\[ [\hat{\mathcal{U}} : \mathcal{M}] = [\varphi(\mathcal{V}) : \mathcal{M}]. \]

and further,
\[ [\varphi(\mathcal{V}) : \varphi(\mathcal{V})] \leq [\varphi(\mathcal{V}) : \mathcal{M}]. \]

We include here the results for the groups \( S_4 \) and \( A_4 \). The subgroup lattices of \( S_4 \) and \( A_4 \) are as follows:

\[ \hat{\mathcal{U}} = S_4 \]
\[ \hat{\mathcal{U}} = A_4 \]

We denote by \( H_i \) the class consisting of conjugate subgroups \( H_i^{(1)}, H_i^{(2)}, \ldots, H_i^{(r)} \) and by \( \mathcal{M}_i \) the module generated by \( \sum_{k \in H_i^{(k)}} k \mathcal{M}^* \) and \( \mathcal{M}_i = \sum_{k \in H_i^{(k)}} k \mathcal{M}^* \), where \( \mathcal{M}^* \) was defined previously. We shall give the index of \( \mathcal{M}_i \) in its pure embedding in \( \mathcal{M}^* \) and the rank of \( \mathcal{M}_i \). In case \( \mathcal{M}_i \) is of full rank, the index of \( \mathcal{M}_i \) in \( \mathcal{M}^* \) will be given. Finally, the rank of certain modules formed...
by the sum of \( \mathfrak{U}_i \) and also their corresponding indices will be also considered.

Again, we let the symbol \( \mathfrak{U}_i \) denote the pure embedding of \( \mathfrak{U}_i \) in \( \mathcal{L}^* \).

Our results are as follows:

(1) \( \mathcal{L} = \mathbb{S}_3 \), \( \quad H_3 = \{(1,6),(12,3),(132)\}, \quad H_3^{(0)} = \{(1),(13)\}, \quad H_3^{(1)} = \{(1,12)\}, \quad H_3^{(2)} = \{(1),(123)\} \),

\[
\begin{array}{c|c|c}
\mathfrak{U}_i & \text{rank} & \text{index} \\
\hline
\mathfrak{U}_3 & 1 & 1 \\
\mathfrak{U}_3 & 4 & 1 \\
\mathfrak{U}_3 + \mathfrak{U}_3 & 5 & 3 \\
\end{array}
\]

From this result, one can see that if \( \mathcal{L} \) is a normal real algebraic number field over \( \mathbb{Q} \) with Galois group \( \mathcal{G}(\mathbb{Q}/\mathcal{L}) = \mathbb{S}_3 \) and if \( \mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3 \) are the conjugate subfields of \( \mathcal{L} \) corresponding to the subgroups \( H_3^{(0)}, H_3^{(1)}, H_3^{(2)} \) respectively, \( \mathcal{V} \) is the corresponding free abelian group and \( u_1, u_2, u_3, u_4 \) are four independent units obtained from \( \mathcal{V} \) then the fifth unit of \( \mathcal{L} \) can be found in \( \mathcal{L}_4 \), which is corresponding to \( H_3 \).

(2) \( \mathcal{L} = \mathbb{A}_4 \), \( \quad H_4 = \text{class of conjugate subgroups of order } 4, \quad i = 13, 10, 6, 5, 3, 2 \)

\[
\begin{array}{c|c|c}
\mathfrak{U}_i & \text{rank} & \text{index} \\
\hline
\mathfrak{U}_{13} & 16 & 2 \\
\mathfrak{U}_{10} & 25 & 2^4 \cdot 3 \\
\mathfrak{U}_6 & 41 & 2^8 \cdot 3 \\
\mathfrak{U}_6 & 43 & 2^2 \\
\mathfrak{U}_5 & 41 & 2^7 \cdot 3 \\
\mathfrak{U}_5 & 59 & 2 \\
\mathfrak{U}_{13} + \mathfrak{U}_6 & 41 & 2^4 \cdot 3 \\
\mathfrak{U}_6 + \mathfrak{U}_5 & 41 & 2^2 \cdot 3 \\
\mathfrak{U}_{13} + \mathfrak{U}_6 + \mathfrak{U}_{10} & 41 & 2^3 \\
\mathfrak{U}_{13} + \mathfrak{U}_5 & 59 & 2^8 \cdot 3^2 \cdot 5 \\
\mathfrak{U}_6 + \mathfrak{U}_5 & 59 & 2^3 \cdot 5 \\
\mathfrak{U}_{13} + \mathfrak{U}_5 + \mathfrak{U}_6 & 59 & 2^3 \cdot 5^3 \\
\mathfrak{U}_5 + \mathfrak{U}_5 & 59 & 2^3 \\
\mathfrak{U}_6 + \mathfrak{U}_5 & 41 & 2 \ \\
\mathfrak{U}_4 + \mathfrak{U}_5 & 59 & 2^3 \cdot 5^3 \\
\end{array}
\]

1. \( \mathfrak{U}_{13} \): Each subgroup of \( \mathfrak{U}_{13} \) consists of 3 elements in \( C_1 \) and 8 elements in \( C_2 \). Hence, rank of \( \mathfrak{U}_{13} = 16 \).

2. \( \mathfrak{U}_{10} \): Each subgroup in \( \mathfrak{U}_{10} \) consists of 2 elements in \( C_4 \) and 3 elements in \( C_2 \). Hence, rank of \( \mathfrak{U}_{10} = 25 \).

3. \( \mathfrak{U}_6 \): Each subgroup in \( \mathfrak{U}_6 \) consists of 3 elements in \( C_1 \) and 2 elements in \( C_2 \). Hence, rank of \( \mathfrak{U}_6 = 2^8 \cdot 3 \).

4. \( \mathfrak{U}_5 \): Each subgroup in \( \mathfrak{U}_5 \) consists of 2 elements in \( C_4 \) and 3 elements in \( C_2 \). Hence, rank of \( \mathfrak{U}_5 = 3^2 \cdot 5^2 \).

5. \( \mathfrak{U}_4 \): Each subgroup in \( \mathfrak{U}_4 \) consists of 3 elements in \( C_1 \). Hence, rank of \( \mathfrak{U}_4 = 4^3 \).

6. \( \mathfrak{U}_3 \): Each subgroup in \( \mathfrak{U}_3 \) consists of 2 elements in \( C_4 \). Hence, rank of \( \mathfrak{U}_3 = 3^3 + 3^2 \cdot 4^2 + 5^3 = 59 \).

7. \( \mathfrak{U}_2 \): Each subgroup in \( \mathfrak{U}_2 \) consists of 1 element in \( C_4 \). Hence, rank of \( \mathfrak{U}_2 = 3^3 + 3^2 + 4^2 + 5^3 = 59 \).

(\text{In each of the seven cases, the group also contains one element from } C_1. \text{ But this does not affect the rank of the corresponding } \mathfrak{U}.\)
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 \( T = \langle a, b \rangle, a^2 = 1, b^2 = (ab)^3 \), for which no submodule of full rank can be obtained in case \( K \) is totally real.

If \( K \) is totally complex, i.e., \( \delta \neq 1 \), 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

\[
\Delta_{G} = \{ \sum_{g \in G} \lambda(g)z | \lambda(g) \in \mathbb{Z} \text{ for all } g \in G \text{ and } \sum_{g \in G} \lambda(g) = 0 \}.
\]

Define

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

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

\[
\mathcal{U}_i^\theta = \{ x \in \mathcal{U}^\theta \text{ and for every } g_i (g_i x \text{ implies } g_i x = 0) \}, \quad 1 \leq i \leq s.
\]

Let \( \mathcal{V} = \sum_{i=1}^{s} \mathcal{U}_i \), and the pure embedding \( \mathcal{V}^\theta \) of \( \mathcal{V} \) in \( \mathcal{U}^\theta \) is defined as:

\[
\mathcal{V}^\theta = \{ x \in \mathcal{U}^\theta \text{ and either } x = 0 \text{ or } Z \mathcal{V} \cap x \neq 0 \}.
\]

It follows that \( x = E_0 x \) for \( x \in \mathcal{V}^\theta \) and \( (mE_0)x \in \mathcal{V}^\theta \). Hence \( m \mathcal{V} \subseteq \mathcal{V}^\theta \).

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 \( \mathcal{D} \) of \( K \) belongs to the subgroup of order 2. And we can choose a unit \( v_1 \in \mathcal{D} \) such that \( v_1 \) and all its conjugates generate a subgroup \( M \) of finite index \( m \) in \( U \). Let \( w_1, \ldots, w_{m-1} \) be a basis for \( M \) and \( w_1, \ldots, w_{m-1} \) the corresponding basis for \( \mathcal{M} = \mathcal{M} \mathbb{R} \). Let \( H = \langle b \rangle \), and let the idempotent element \( e \) of \( Q(G) \) be defined as \( e = 1/2 (\sum_{h \in H} h - 1/n \sum_{g \in G} g) \). Let \( G = \bigoplus_{i=1}^{n} g_i H \) be the left cost decomposition of \( G \) over \( H \) and let \( \mathcal{M} \) be the module generated by \( (m/2) \sum h, (m/2) \sum g \), \( (m/2) \sum h e, \ldots, (m/2) \sum g e \). Define our mapping by

\[
\varphi: M \rightarrow \mathcal{M} \equiv (m/2) \sum h, \quad i = 1, \ldots, m/2 - 1, \quad \gamma_1 = 1.
\]

Again, \( \varphi \) is an operator isomorphism and let \( \mathcal{M}^* = \mathcal{M}/m \). It follows that \( \varphi(\mathcal{U}) \) has finite index in \( \mathcal{M}^* \). Let \( \mathcal{V}_i \) be defined as in the real case and let \( \mathcal{V} = \bigcup_{i=1}^{m/2} \mathcal{V}_i \). Then \( \mathcal{V} \) has finite index in \( \varphi(\mathcal{V}) \). Again, our computer program will give ranks of the \( \mathcal{V}_i \) which can be seen equal to the ranks of \( \mathcal{V}_i \)'s. And we will give bound on the index of \( \mathcal{V} \) in its pure embedding in \( \mathcal{M}^* \) and this is also a bound of the index of \( \varphi(\mathcal{V}) \) in its pure embedding in \( \varphi(\mathcal{U}) \) by Theorem 4.

We are including here corresponding results for the group \( A_4 \), which are as follows:

<table>
<thead>
<tr>
<th>( \mathcal{V}_i )</th>
<th>rank</th>
<th>index</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \mathcal{V}_{28} )</td>
<td>29</td>
<td>2^{4} 3^{1}</td>
</tr>
<tr>
<td>( \mathcal{V}_{24} )</td>
<td>24</td>
<td>2^{2} 3^{1}</td>
</tr>
<tr>
<td>( \mathcal{V}_{20} )</td>
<td>20</td>
<td>2^{4} 5^{5}</td>
</tr>
<tr>
<td>( \mathcal{V}_{16} )</td>
<td>16</td>
<td>2^{10}</td>
</tr>
<tr>
<td>( \mathcal{V}_{12} )</td>
<td>12</td>
<td>2^{10}</td>
</tr>
<tr>
<td>( \mathcal{V}_{8} )</td>
<td>8</td>
<td>2^{10}</td>
</tr>
<tr>
<td>( \mathcal{V}_{4} )</td>
<td>4</td>
<td>2^{10}</td>
</tr>
<tr>
<td>( \mathcal{V}_{2} )</td>
<td>2</td>
<td>2^{10}</td>
</tr>
</tbody>
</table>

References

Sur la repartition modulo 1 de la suite $na$

par

JACQUES LESCA (Talence)

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

Si $\beta$ est un point de $T$, $[\beta]$ désigne le représentant de $\beta$ dans $\mathbb{R}$ caractérisé par

$$0 \leq [\beta] < 1.$$  

Si $\beta, \gamma$ sont des points distincts de $T$, $[\beta, \gamma]$ désigne l’arc défini par

$$\{\delta \in T : (\delta, \beta, \gamma), \text{ si } (\beta, \gamma), \delta < \gamma \} \cup \{\delta \in T : (\delta, \beta, \gamma), \text{ si } (\beta, \gamma), \delta > \gamma \}.$$  

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

Par la suite, $a$ est un irrationnel de $T$. 

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

$$\Pi^+(\beta, \gamma; u) = \text{card}\{n : na \in [\beta, \gamma], 0 \leq n \leq u\},$$

$$\Pi^-(\beta, \gamma; u) = \text{card}\{n : na \in [\beta, \gamma], 0 \leq n \leq u - 1\},$$

$$E^+(\beta, \gamma; u) = \Pi^+(\beta, \gamma; u) - u \text{mes}([\beta, \gamma]).$$

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

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

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

$$E^+(\gamma; u) = E^+(0, \gamma; u),$$

$$E^-(\gamma; u) = E^-(0, \gamma; u).$$

Ce papier est consacré à l’étude des fonctions $E^+$ et $E^-$. 

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

$$E^+(\beta, \beta + va; u) = E^-(\beta, -\beta + va; u).$$