Radan Kučera
A generalization of a unit index of Greither

Acta Mathematica et Informatica Universitatis Ostraviensis, Vol. 6 (1998), No. 1, 149--154

Persistent URL: http://dml.cz/dmlcz/120527

Terms of use:
© University of Ostrava, 1998

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these Terms of use.

This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project DML-CZ: The Czech Digital Mathematics Library http://project.dml.cz
A generalization of a unit index of Greither

Radan Kučera

Abstract: For an abelian field, a subgroup of the unit group, isomorphic as a Galois module to the augmentation ideal, is explicitly constructed and its index is computed.

Key Words: abelian field, circular unit, Ramachandra's construction of independent units.

Mathematics Subject Classification: 11R27, 11R20

1. Introduction

By an abelian field $k$ we have in mind a finite abelian extension of the rational numbers $\mathbb{Q}$. It is well-known that the group $E$ of units of $k$ is difficult to compute but that it contains the explicitly described subgroup of circular units $C$. But the structure of $C$ as a $\mathbb{Z}[G]$-module (where $G$ is the Galois group $\text{Gal}(k/\mathbb{Q})$) is easy to describe only in some very special cases (like for the maximal real subfield of a prime-power cyclotomic field, when it becomes isomorphic as a $\mathbb{Z}[G]$-module to the augmentation ideal of $\mathbb{Z}[G]$). Even the known formula (see [5, Theorem 4.1]) for the index $[E : C]$, which is related to the class number, is explicit only in some easiest cases (for example for a cyclotomic field, for a cyclic field, or for a compositum of several quadratic fields, see [2, Theorem 1]).

Therefore it is natural to search for an explicit submodule of $C$ which would be isomorphic as a $\mathbb{Z}[G]$-module to the augmentation ideal. The first important construction of such a submodule is due to Ramachandra in [4], who did this job for the maximal real subfield of a cyclotomic field. This construction was generalized by Washington (see [6, §8.2]) to any real abelian field. The disadvantage of their construction is the huge obtained index which usually involves quite large and unpredictable prime factors. The first successful attempt to produce such a subgroup with a smaller index is due to Levesque (see [3]). His construction for real subfields of cyclotomic fields can produce a group of smaller index than Ramachandra’s one but still his index can have huge prime factors. Recently a dramatic improvement was obtained by Greither in [1] who constructed for real subfields of cyclotomic fields a subgroup of circular units which is again isomorphic as a $\mathbb{Z}[G]$-module to the augmentation ideal but now its index is the class number multiplied by a factor divisible only by primes dividing the degree of the field.

This research is supported by the grant 201/97/0433 of the Grant Agency of the Czech Republic.
The aim of this paper is a generalization of Greither's construction to any abelian field.

2. Notation

We shall introduce the following notation:
- \( k \) an abelian field (we suppose \( k \) to be a subfield of complex numbers \( \mathbb{C} \));
- \( G = \text{Gal}(k/\mathbb{Q}) \) its Galois group;
- \( R = \mathbb{Z}[G] \) the integral group ring;
- \( s(X) = \sum_{\sigma \in X} \sigma \in R \) for any \( X \subseteq G \);
- \( m \) the conductor of \( k \);
- \( m_0 = \prod_{p | m} p \) the maximal square-free divisor of \( m \).

For a prime \( p \) dividing \( m \):
- \( T_p \subseteq G \) the inertia group for \( p \) in \( k \);
- \( \lambda_p \in G \) a fixed Frobenius automorphism for \( p \) (well defined modulo \( T_p \));
- \( D_p \subseteq G \) the decomposition group for \( p \) in \( k \), so \( D_p = (\lambda_p)T_p \);
- \( \ell_p = |T_p| \) the ramification index of \( p \) in \( k \);
- \( f_p = \frac{|D_p|}{|T_p|} \) the residue class degree of \( p \) in \( k \);
- \( g_p = \frac{|G|}{|D_p|} \) the number of primes in \( k \) dividing \( p \);
- \( e_p = \frac{1}{f_p} s(T_p) \in \mathbb{Q}[G] \) the idempotent corresponding to \( T_p \);
- \( \nu_p = \sum_{i=1}^{\ell_p} \lambda_p^i \in R \).

For a divisor \( r \) of \( m_0 \):
- \( T_r = \prod_{p | r} T_p \subseteq G \), so \( T_1 = \{1\}, T_{m_0} = G \);
- \( D_r = \prod_{p | r} D_p \subseteq G \), so \( D_1 = \{1\}, D_{m_0} = G \);
- \( \nu_r = \prod_{p | r} \nu_p \in R \);
- \( q_r = \frac{1}{\nu_r} \prod_{p | r} T_p \) (it is easy to see that \( q_r \) is a positive integer).

3. Use of Greither's construction for Sinnott's module \( U \)

Sinnott's module \( U \) is the \( R \)-module generated in the rational group ring \( \mathbb{Q}[G] \) by

\[
\{ s(T_r) \prod_{p | m_0} \frac{1}{1 - \lambda_p^{-1} e_p}; r | m_0 \}.
\]

The module \( U \) is a free \( \mathbb{Z} \)-module of \( \mathbb{Z} \)-rank \( |G| \) (see [5, Proposition 2.3]). Using Greither's method we shall construct an \( R \)-cyclic submodule of \( U \) of the same \( \mathbb{Z} \)-rank \( |G| \).

It is easy to see that \( \nu_p s(T_p) = s(D_p) \) for any prime \( p \), so

\[
q_r \nu_r s(T_r) = \nu_r \prod_{p | r} s(T_p) = \prod_{p | r} s(D_p)
\]
A generalization of a unit index of Greither does not depend on the choice of $X_p$ for any $r|m_0$. We put

$$g = \sum_{r|m_0} q_r \nu_r \left( s(T_r) \prod_{p|m_0} (1 - \lambda_p^{-1} e_p) \right) = \sum_{r|m_0} \left( \prod_{p|m_0} s(D_p) \right) \prod_{p|m_0} (1 - \lambda_p^{-1} e_p)$$

$$= \prod_{p|m_0} (s(D_p) + 1 - \lambda_p^{-1} e_p) \in U.$$ 

If $\chi$ is a multiplicative character of $G$, we denote by $\chi$ also the associated primitive Dirichlet character. Let $X$ be the group of all Dirichlet characters associated to the characters of $G$, let $X^+$ mean the subgroup of all even characters. For any $\chi \in X$ we consider the ring homomorphism $\rho_\chi : \mathbb{Q}[G] \to \mathbb{C}$ induced by $\chi$. Then we have

$$\rho_\chi(g) = \prod_{p|m_0} \left( \rho_\chi(s(D_p)) + 1 - \chi(\lambda_p)^{-1} \rho_\chi(e_p) \right).$$

But

$$\rho_\chi(e_p) = \begin{cases} 1 & \text{if } T_p \subseteq \ker \chi, \\ 0 & \text{otherwise,} \end{cases} \quad \text{and} \quad \rho_\chi(s(D_p)) = \begin{cases} t_{fp} & \text{if } D_p \subseteq \ker \chi, \\ 0 & \text{otherwise.} \end{cases}$$

Therefore

$$\rho_\chi(g) = \left( \prod_{p|m_0} t_{fp} \right) \left( \prod_{D_p \subseteq \ker \chi} \prod_{T_p \subseteq \ker \chi} (1 - \chi(\lambda_p)^{-1}) \right) \neq 0.$$

Let $j \in G$ mean the restriction of complex conjugation, $e^+ = \frac{1+i}{2}$, $e^- = \frac{1-i}{2}$. By means of [5, Lemma 1.2(b)] we obtain

$$(R : gR) = \prod_{\chi \in X} \rho_\chi(g) = \prod_{p|m_0} t_{fp}^g f_p^{2g_p}$$

$$(e^+ R : ge^+ R) = \prod_{\chi \in X^+} \rho_\chi(g) = \prod_{p|m_0} t_{fp}^g f_p^{2g_p} \prod_{j \in D_p \setminus T_p} t_{fp}^g f_p^{2g_p - 2} \prod_{p|m_0} t_{fp}^g / f_p^{g_p}$$

$$(e^- R : ge^- R) = \prod_{\chi \in X \setminus X^+} \rho_\chi(g) = \prod_{j \in D_p \setminus T_p} 2^{g_p} \prod_{p|m_0} t_{fp}^{g_p / 2} f_p^{g_p}$$

Because $(R : U)(R : gR)$, $(e^+ R : e^+ U)(e^+ R : ge^+ R)$, and $(e^- R : e^- U)(e^- R : ge^- R)$, the previous formulae give upper bounds for the indices of Sinnott’s module.

4. Circular units

Now we can transfer the above described construction from $U$ to the group of circular units $C$. At first, let us briefly recall some definitions following Sinnott. For any positive integer $n$ we put $\zeta_n = e^{2\pi i/n}$, and let $K_n$ denote the cyclotomic
field $\mathbb{Q}(\zeta_n)$, and $k_n = k \cap K_n$. Let $D$ be the subgroup generated in $k^\times$ by $-1$ and all norms $N_{K_n/k_n}(1-\zeta_n^a)$, where an integer $a$ is not divisible by $n$. Then we define $C = D \cap E$.

The logarithmic mapping $\ell : k^\times \to \mathbb{R}[G]$ is defined by

$$\ell(\alpha) = -\frac{1}{2} \sum_{\sigma \in G} \log |\alpha^{\sigma^\prime}|$$

for any $\alpha \in k^\times$. This mapping induces the isomorphism

$$C/W \simeq \ell(C) = T \cap (1 - e_1)T$$

(see [5, Lemma 4.1, Lemma 4.2 and Proposition 4.1]), where $W$ is the group of roots of unity in $k$, $e_1 = \frac{1}{|G|} s(G)$, and $T = \ell(D)$. Due to [5, Corollary to Proposition 4.2] we have $(1 - e_1)T = \omega'U$ for a suitable $\omega' \in \mathbb{R}[G]$, which satisfies

$$(1 - e_1)\ell(N_{K_n/k_n}(1-\zeta_n)) = \omega's(G(k/k_n)) \prod_{p | n} (1 - \lambda_p^{-1}e_p)$$

for any $n|m$ (see [5, Proposition 4.2]).

For any $r|m_0$ let $r'$ be the maximal divisor of $m$ which is divisible only by primes dividing $r$, i.e. $r|r', r'|m, (r, \frac{m}{r'}) = 1, (r', \frac{m}{r}) = 1$. Then $Gal(k/k_{r'}) = T_{m_0/r'}$ and it is not difficult to find out that the previous identity implies $\omega'g = (1 - e_1)\ell(\eta)$, where

$$\eta = \prod_{1 \neq r | m_0} N_{K_{r'}/k_{r'}}(1-\zeta_{r'})^{q_{m_0/r'}^{m_0/r'}/r'}.$$ 

It is easy to see that $\eta \in D$ is not a unit, but for any $\sigma \in G$ we have $\eta^{1-\sigma} \in C$. Let $C'$ mean the subgroup of $C$ generated by $W \cup \{\eta^{1-\sigma} ; \sigma \in G\}$.

We could obtain the index $[E : C']$ using the mentioned results of Sinnott, but we shall compute it directly because this way looks easier and more explicit.

From now on we shall suppose that $k$ is a real abelian field; for an imaginary field the computations would almost be the same. Due to [6, Lemma 4.15 and Lemma 5.26] we have

$$[E : C'] = \frac{R(C')}{R} = \frac{1}{R} \cdot \prod_{1 \neq \chi \in X, \sigma \in G} \chi(\sigma) \log |\eta^{\sigma}|$$

$$= \frac{1}{R} \cdot \prod_{1 \neq \chi \in X, \sigma \in G} \chi(\sigma) \sum_{1 \neq r | m_0} q_{m_0/r} \log |N_{K_{r'}/k_{r'}}(1-\zeta_{r'})^{q_{m_0/r'}^{m_0/r'}/r'}|.$$ 

Let us fix any $r|m_0$, $r \neq 1$, and $\chi \in X, \chi \neq 1$. We put $\beta = N_{K_{r'}/k_{r'}}(1-\zeta_{r'})$ and $s = \frac{ma}{r}$ for a brevity. Since $\beta \in k_{r'}$ and $Gal(k/k_{r'}) = T_s$, we have

$$\sum_{\sigma \in G} \chi(\sigma) q_s \log |\beta^{u s}| = \begin{cases} 0 & \text{if } T_s \not\subseteq \ker \chi, \\ \sum_{\sigma \in \Gal(k_{r'}/Q)} |T_s| \chi(\sigma) q_s \log |\beta^{u s}| & \text{if } T_s \subseteq \ker \chi. \end{cases}$$
It is easy to see that

$$\beta^{q_{s}v_{s}}(T_{s}) = \beta^{q_{s}v_{s}}(T_{s})$$

and

$$q_{s}v_{s} = \prod_{p|s} s(D_{p}) = \frac{\prod_{p|s} \frac{D_{p}}{|D_{s}|}}{s(D_{s})}.$$ 

Let $L_{s}$ be the maximal subfield of $k$ where each prime $p|s$ splits completely. Then $L_{s} \subseteq k^{r}$, $\text{Gal}(k/L_{s}) = D_{s}$, and $\beta^{s}(D_{s}) = N_{k/L_{s}}(\beta) = N_{k^{r}/L_{s}}(\beta)^{[k^{r}:L_{s}]} \in L_{s}$, so

$$\sum_{\sigma \in G} \chi(\sigma)q_{s} \log|\beta^{s}| = 0$$

if $D_{s} \nsubseteq \ker \chi$. Let us suppose $D_{s} \subseteq \ker \chi$ now. Then

$$\sum_{\sigma \in G} \chi(\sigma)q_{s} \log|\beta^{s}| = \sum_{\sigma \in \text{Gal}(L_{s}/Q)} \sum_{[k_{r'} : L_{s}]} \chi(\sigma) \frac{\prod_{p|s} \frac{D_{p}}{|D_{s}|}}{[k : k_{r'}]} \log|N_{k_{r'}/L_{s}}(\beta^{s})|.$$ 

But

$$[k_{r'} : L_{s}] [k : k_{r'}] = [k : L_{s}] = |D_{s}|,$$

hence

$$\sum_{\sigma \in G} \chi(\sigma)q_{s} \log|\beta^{s}| = \left( \prod_{p|s} \frac{D_{p}}{|D_{s}|} \right) \sum_{\sigma \in \text{Gal}(L_{s}/Q)} \chi(\sigma) \log|N_{k_{r'}/L_{s}}(1 - \zeta_{r'})^{s}|$$

$$= -\tau(\chi) L(1, \bar{\chi}) \left( \prod_{p|r} (1 - \chi(p)) \right) \prod_{p|s} D_{p},$$

where $\tau(\chi)$ means the Gauss sum and $L(1, \bar{\chi})$ means the value of the Dirichlet $L$-series (see [6, proof of Theorem 8.3]). Therefore by means of the well-known formula

$$hR = \prod_{1 \neq \chi \in X} \frac{1}{2} \tau(\chi) L(1, \bar{\chi})$$

with $h$ being the class number of $k$ (for example, see [6, Corollary 4.6 and the proof of Theorem 4.17]) we obtain

$$[E : C'] = 2^{[X] - 1} h \cdot \left( \prod_{1 \neq \chi \in X} \sum_{D_{s} \subseteq \ker \chi} \left( \prod_{p|m_{0}} \frac{(1 - \chi(p))}{\prod_{p|s} D_{p}} \right) \right)$$

It is easy to see that $D_{s} \subseteq \ker \chi$ implies $\chi(p) = 1$ for each prime $p|s$. Therefore for each $\chi \in X$, $\chi \neq 1$ the previous sum contains only one non-zero term, namely for $s$ being the product of all primes $p|m_{0}$ such that $\chi(p) = 1$. Hence

$$[E : C'] = 2^{[X] - 1} h \cdot \left( \prod_{1 \neq \chi \in X} \left( \prod_{p|m} \frac{(1 - \chi(p))}{\prod_{p|m} D_{p}} \right) \right)$$

$$= 2^{[X] - 1} h \cdot \prod_{p|m} \ell_{p}^{q_{p} - 1} f_{p}^{2q_{p} - 1}.$$
For any integer \( n > 1 \) and any integer \( a \) relatively prime to \( n \) we have \( \zeta_n^{(1-a)/2} \in K_n \) and
\[
(1 - \zeta_n)^{(a-1)/2}(1 - \zeta_n^{-a})^{-1} \in K_n \cap \mathbb{R}.
\]
Hence if \( k_n \) is real then for the automorphism \( \sigma \in \text{Gal}(K_n/\mathbb{Q}) \) determined by \( \sigma(\zeta_n) = \zeta_n^a \) the unit
\[
N_{K_n/k_n}(1 - \zeta_n)^{1-\sigma} = N_{K_n/k_n}(\zeta_n^{(1-a)/2}) \cdot N_{K_n/k_n}(\zeta_n^{(a-1)/2}(1 - \zeta_n)(1 - \zeta_n^{-a})^{-1})^2
\]
is a square of a unit in \( k_n \) (up to a root of unity).

Since \( k \) is real, for any \( \sigma \in G \) there is an explicit unit \( \varepsilon_\sigma \in k \) such that \( \eta^{1-\sigma} = \pm \varepsilon_\sigma^2 \). It is easy to see that the index of the group \( C'' \) generated by \( \{-1\} \cup \{\varepsilon_\sigma; \sigma \in G\} \) is
\[
[E : C''] = [E : C'] \cdot 2^{1 - |X|} = h \cdot \prod_{\pi \mid m} \frac{e_p}{2^{2\varphi_p-1}} f_p^{2\varphi_p-1}.
\]

Of course, both \( R \)-modules \( C''/\{1,-1\} \) and \( C'''/\{1,-1\} \) are \( R \)-isomorphic to the augmentation ideal of \( R \).

**Acknowledgments**

I am grateful to Claude Levesque for many remarks which improved this paper.

**References**


**Author's address:** Department of Mathematics Faculty of Science Masaryk University Janáčkovo nám. 2a 662 95 Brno, Czech Republic

**E-mail:** kucera@math.muni.cz

**Received:** April 24, 1998