Circular units of abelian fields with four ramified primes

Vladimír Sedláček

Masaryk University

6.-9.4.2017
Jarní škola Katedry algebry, Rapotín

Overview

1. Introduction
   - Motivation
   - General definitions
   - The cases of one, two or three ramified primes
2. Finding a basis of D^+ for $|P| = 4$
   - Notation and assumptions
   - General strategy
   - A special subcase
3. Open questions

Circular units appear in many situations in algebraic number theory, because in some sense they are a good approximation of the full group of units of a given abelian field, which is very hard to describe explicitly. They are also closely related to the class group of the respective field.

The problem is that a $\mathbb{Z}$-basis of the group of circular units is known only in a few very special cases, for example when the abelian field is cyclotomic, has at most two ramified primes, or has three ramified primes and satisfies some other conditions.

Circular units appear in many situations in algebraic number theory, because in some sense they are a good approximation of the full group of units of a given abelian field, which is very hard to describe explicitly. They are also closely related to the class group of the respective field.

The problem is that a $\mathbb{Z}$-basis of the group of circular units is known only in a few very special cases, for example when the abelian field is cyclotomic, has at most two ramified primes, or has three ramified primes and satisfies some other conditions.

Let k be a real abelian field, P be the set of ramified primes of k, K be the genus field of k in the narrow sense and $G = \mathrm{Gal}(K/\mathbb{Q})$, so that $G \cong \prod_{p \in P} T_p$, where T_p is the inertia group for the prime p.

Then D^+, the non-torsion part of the group D of circular numbers of k (using Lettl's modification of Sinnott's definition), has one generator η_I for each nonempty subset $I \subseteq P$.

More explicitly, if we let K_i be the largest subfield of K in which p_i is the only ramified prime for any $i \in I$, we have

$$\eta_I = \mathrm{N}_{\mathbb{Q}(\zeta_{\mathrm{cond}(\prod_{i\in I} K_i)})/(\prod_{i\in I} K_i)\cap k}\left(1 - \zeta_{\mathrm{cond}(\prod_{i\in I} K_i)}\right).$$

It turns out that D^+ is a $\mathbb{Z}[G]$-module of $\mathbb{Z}$-rank $[k : \mathbb{Q}] + |P| - 1$.

Let k be a real abelian field, P be the set of ramified primes of k, K be the genus field of k in the narrow sense and $G = \mathrm{Gal}(K/\mathbb{Q})$, so that $G \cong \prod_{p \in P} T_p$, where T_p is the inertia group for the prime p.

Then D^+, the non-torsion part of the group D of circular numbers of k (using Lettl's modification of Sinnott's definition), has one generator η_I for each nonempty subset $I \subseteq P$.

More explicitly, if we let K_i be the largest subfield of K in which p_i is the only ramified prime for any $i \in I$, we have

$$\eta_I = \mathrm{N}_{\mathbb{Q}(\zeta_{\mathrm{cond}(\prod_{i \in I} K_i)})/(\prod_{i \in I} K_i) \cap k} \left(1 - \zeta_{\mathrm{cond}(\prod_{i \in I} K_i)} \right).$$

It turns out that D^+ is a $\mathbb{Z}[G]$-module of $\mathbb{Z}$-rank $[k : \mathbb{Q}] + |P| - 1$.

Let k be a real abelian field, P be the set of ramified primes of k, K be the genus field of k in the narrow sense and $G = \mathrm{Gal}(K/\mathbb{Q})$, so that $G \cong \prod_{p \in P} T_p$, where T_p is the inertia group for the prime p.

Then D^+, the non-torsion part of the group D of circular numbers of k (using Lettl's modification of Sinnott's definition), has one generator η_I for each nonempty subset $I \subseteq P$.

More explicitly, if we let K_i be the largest subfield of K in which p_i is the only ramified prime for any $i \in I$, we have

$$\eta_I = \mathrm{N}_{\mathbb{Q}(\zeta_{\mathrm{cond}(\prod_{i\in I} K_i)})/(\prod_{i\in I} K_i)\cap k}\left(1 - \zeta_{\mathrm{cond}(\prod_{i\in I} K_i)}\right).$$

It turns out that D^+ is a $\mathbb{Z}[G]$-module of $\mathbb{Z}$-rank $[k:\mathbb{Q}] + |P| - 1$.

The generators of D^+ are subject to norm relations (which can be obtained by computing the norm of the generators to a subfield with less ramified primes) and for $|P| \geq 3$, also to the so-called Ennola relations, which are highly nontrivial relations that are not consequences of the norm relations.

Our goal will be to find a basis of D^+ (it can then be easily modified in order to obtain a basis of the group of circular units). In general, this is very difficult, so we will need to restrict ourselves to a special family of fields. It's clear from the definition of D^+ that the complexity of the problem depends on the number of ramified primes in k.

The generators of D^+ are subject to norm relations (which can be obtained by computing the norm of the generators to a subfield with less ramified primes) and for $|P| \geq 3$, also to the so-called Ennola relations, which are highly nontrivial relations that are not consequences of the norm relations.

Our goal will be to find a basis of D^+ (it can then be easily modified in order to obtain a basis of the group of circular units). In general, this is very difficult, so we will need to restrict ourselves to a special family of fields. It's clear from the definition of D^+ that the complexity of the problem depends on the number of ramified primes in k.

If $|P| = 1$, the set of all conjugates of η already forms a basis of D^+, since the rank of D^+ is exactly $[k : \mathbb{Q}]$.

If $|P| = 2$, the situation is a little more complicated, but still quite easily managable. This is dealt with in the papers of K.Dohmae.

For $|P| = 3$, R.Kučera and A.Salami have recently constructed a basis under the assumption that the relative Galois group $\mathrm{Gal}(K/k)$ is cyclic, as well as the inertia groups for all ramified primes. However, this basis is too complicated to describe here, mainly due to the presence of Ennola relations.

If $|P| = 1$, the set of all conjugates of η already forms a basis of D^+, since the rank of D^+ is exactly $[k : \mathbb{Q}]$.

If $|P| = 2$, the situation is a little more complicated, but still quite easily managable. This is dealt with in the papers of K.Dohmae.

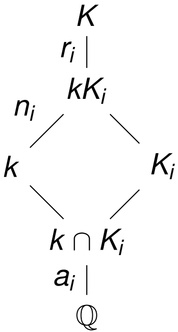
For $|P| = 3$, R.Kučera and A.Salami have recently constructed a basis under the assumption that the relative Galois group $\mathrm{Gal}(K/k)$ is cyclic, as well as the inertia groups for all ramified primes. However, this basis is too complicated to describe here, mainly due to the presence of Ennola relations.

If $|P| = 1$, the set of all conjugates of η already forms a basis of D^+, since the rank of D^+ is exactly $[k : \mathbb{Q}]$.

If $|P| = 2$, the situation is a little more complicated, but still quite easily managable. This is dealt with in the papers of K.Dohmae.

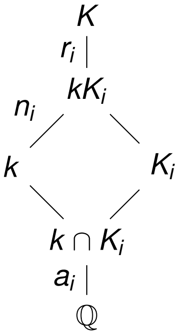
For $|P| = 3$, R.Kučera and A.Salami have recently constructed a basis under the assumption that the relative Galois group $\mathrm{Gal}(K/k)$ is cyclic, as well as the inertia groups for all ramified primes. However, this basis is too complicated to describe here, mainly due to the presence of Ennola relations.

Now let $P = \{p_1, p_2, p_3, p_4\}$, $m := [K : k]$ and for $i \in \{1, 2, 3, 4\}$, let $a_i := [k \cap K_i : \mathbb{Q}]$, $r_i := [K : kK_i]$ and $n_i := \frac{m}{r_i}$.



We will assume that $H := \mathrm{Gal}(K/k) = \langle \tau \rangle$ is cyclic, as well as the inertia subgroups $T_i = \langle \sigma_i \rangle$ (without loss of generality, we have $\tau = \sigma_1^{a_1} \sigma_2^{a_2} \sigma_3^{a_3} \sigma_4^{a_4}$).

Now let $P = \{p_1, p_2, p_3, p_4\}$, $m := [K : k]$ and for $i \in \{1, 2, 3, 4\}$, let $a_i := [k \cap K_i : \mathbb{Q}]$, $r_i := [K : kK_i]$ and $n_i := \frac{m}{r_i}$.



We will assume that $H := \mathrm{Gal}(K/k) = \langle \tau \rangle$ is cyclic, as well as the inertia subgroups $T_i = \langle \sigma_i \rangle$ (without loss of generality, we have $\tau = \sigma_1^{a_1} \sigma_2^{a_2} \sigma_3^{a_3} \sigma_4^{a_4}$).

Now let $R_i = \sum_{u=0}^{a_i-1} \sigma_i^u$ and $N_i = \sum_{u=0}^{m-1} \sigma_i^{ua_i}$. If we regard these as elements of $\mathbb{Z}[G/H]$, then $R_i N_i$ is the norm operator from k to the maximal subfield ramified at less primes.

In $\mathbb{Z}[G/H]$, we also have

$$N_4 = \sum_{u=0}^{m-1} \sigma_1^{ua_1} \sigma_2^{ua_2} \sigma_3^{ua_3}.$$

We will use these relations a lot.

Now let $R_i = \sum_{u=0}^{a_i-1} \sigma_i^u$ and $N_i = \sum_{u=0}^{m-1} \sigma_i^{ua_i}$. If we regard these as elements of $\mathbb{Z}[G/H]$, then $R_i N_i$ is the norm operator from k to the maximal subfield ramified at less primes.

In $\mathbb{Z}[G/H]$, we also have

$$N_4 \equiv \sum_{u=0}^{m-1} \sigma_1^{ua_1} \sigma_2^{ua_2} \sigma_3^{ua_3}.$$

We will use these relations a lot.

To construct the basis of D^+, we can take the union of all bases for the fields

$$k \cap K_1 K_2 K_3,\, k \cap K_1 K_2 K_4,\, k \cap K_1 K_3 K_4,\, k \cap K_2 K_3 K_4$$

(which have three ramified primes) and add in

$$a_1 a_2 a_3 a_4 \frac{m^3}{r_1 r_2 r_3 r_4} - \sum_{i,j,l} a_i a_j a_l \frac{m^2}{r_i r_j r_l} + \sum_{i,j} a_i a_j \gcd(r_i, r_j) \frac{m}{r_i r_j} - \sum_i a_i + 1$$

conjugates of the highest generator $\eta := \eta_{\{1,2,3,4\}}$.

To show that we will obtain a basis, we need to be able to generate all the missing conjugates of η. We will use the norm relations to do this.

To construct the basis of D^+, we can take the union of all bases for the fields

$$k \cap K_1 K_2 K_3,\ k \cap K_1 K_2 K_4,\ k \cap K_1 K_3 K_4,\ k \cap K_2 K_3 K_4$$

(which have three ramified primes) and add in

$$a_1 a_2 a_3 a_4 \frac{m^3}{r_1 r_2 r_3 r_4} - \sum_{i,j,l} a_i a_j a_l \frac{m^2}{r_i r_j r_l} + \sum_{i,j} a_i a_j \gcd(r_i, r_j) \frac{m}{r_i r_j} - \sum_i a_i + 1$$

conjugates of the highest generator $\eta := \eta_{\{1,2,3,4\}}$.

To show that we will obtain a basis, we need to be able to generate all the missing conjugates of η. We will use the norm relations to do this.

To construct the basis of D^+, we can take the union of all bases for the fields

$$k \cap K_1 K_2 K_3,\, k \cap K_1 K_2 K_4,\, k \cap K_1 K_3 K_4,\, k \cap K_2 K_3 K_4$$

(which have three ramified primes) and add in

$$a_1 a_2 a_3 a_4 \frac{m^3}{r_1 r_2 r_3 r_4} - \sum_{i,j,l} a_i a_j a_l \frac{m^2}{r_i r_j r_l} + \sum_{i,j} a_i a_j \gcd(r_i, r_j) \frac{m}{r_i r_j} - \sum_i a_i + 1$$

conjugates of the highest generator $\eta := \eta_{\{1,2,3,4\}}$.

To show that we will obtain a basis, we need to be able to generate all the missing conjugates of η. We will use the norm relations to do this.

Now we will focus on the subcase $a_1 = a_2 = a_3 = r_4 = 1$. Here we have

$$\mathrm{Gal}(k/\mathbb{Q}) \cong G/H \cong \{\mathrm{res}_{K/k}\left(\sigma_1^{x_1}\sigma_2^{x_2}\sigma_3^{x_3}\sigma_4^{x_4}\right); 0 \le x_1 < n_1, \\ 0 \le x_2 < n_2, 0 \le x_3 < n_3, 0 \le x_4 < a_4\},$$

where each automorphism of k determines the quadruple (x_1, x_2, x_3, x_4) uniquely.

Since the conjugates of η correspond to the elements of $\mathrm{Gal}(k/\mathbb{Q})$, we can now visualise them geometrically.

We will furthermore assume that $\gcd(r_1, r_2) = \gcd(r_1, r_3) = \gcd(r_2, r_3) = \gcd(n_1, n_2, n_3) = 1$.

Now we will focus on the subcase $a_1 = a_2 = a_3 = r_4 = 1$. Here we have

$$\mathrm{Gal}(k/\mathbb{Q}) \cong G/H \cong \{\mathrm{res}_{K/k}\left(\sigma_1^{x_1}\sigma_2^{x_2}\sigma_3^{x_3}\sigma_4^{x_4}\right); 0 \le x_1 < n_1, \\ 0 \le x_2 < n_2, 0 \le x_3 < n_3, 0 \le x_4 < a_4\},$$

where each automorphism of k determines the quadruple (x_1, x_2, x_3, x_4) uniquely.

Since the conjugates of η correspond to the elements of $\mathrm{Gal}(k/\mathbb{Q})$, we can now visualise them geometrically.

We will furthermore assume that $\gcd(r_1, r_2) = \gcd(r_1, r_3) = \gcd(r_2, r_3) = \gcd(n_1, n_2, n_3) = 1$.

Now we will focus on the subcase $a_1 = a_2 = a_3 = r_4 = 1$. Here we have

$$\mathrm{Gal}(k/\mathbb{Q}) \cong G/H \cong \{\mathrm{res}_{K/k}\left(\sigma_1^{x_1}\sigma_2^{x_2}\sigma_3^{x_3}\sigma_4^{x_4}\right); 0 \leq x_1 < n_1, 0 \leq x_2 < n_2, 0 \leq x_3 < n_3, 0 \leq x_4 < a_4\},$$

where each automorphism of k determines the quadruple (x_1, x_2, x_3, x_4) uniquely.

Since the conjugates of η correspond to the elements of $\mathrm{Gal}(k/\mathbb{Q})$, we can now visualise them geometrically.

We will furthermore assume that $\gcd(r_1, r_2) = \gcd(r_1, r_3) = \gcd(r_2, r_3) = \gcd(n_1, n_2, n_3) = 1$.

This part will be done on the board.

- What does the basis in the general case with four ramified primes look like? What about the module of relations?
- What if we remove the condition of cyclicity of the relative Galois group?
- Is it always true that new Ennola relations only show up in odd dimensions?
- What can be said about the cases of more ramified primes? Will it be possible to explore them by the same means or will we need more advanced machinery?

Thank you for your attention.

- What does the basis in the general case with four ramified primes look like? What about the module of relations?
- What if we remove the condition of cyclicity of the relative Galois group?
- Is it always true that new Ennola relations only show up in odd dimensions?
- What can be said about the cases of more ramified primes? Will it be possible to explore them by the same means or will we need more advanced machinery?

Thank you for your attention.

- What does the basis in the general case with four ramified primes look like? What about the module of relations?
- What if we remove the condition of cyclicity of the relative Galois group?
- Is it always true that new Ennola relations only show up in odd dimensions?
- What can be said about the cases of more ramified primes? Will it be possible to explore them by the same means or will we need more advanced machinery?

Thank you for your attention.

- What does the basis in the general case with four ramified primes look like? What about the module of relations?
- What if we remove the condition of cyclicity of the relative Galois group?
- Is it always true that new Ennola relations only show up in odd dimensions?
- What can be said about the cases of more ramified primes? Will it be possible to explore them by the same means or will we need more advanced machinery?

Thank you for your attention.

- What does the basis in the general case with four ramified primes look like? What about the module of relations?
- What if we remove the condition of cyclicity of the relative Galois group?
- Is it always true that new Ennola relations only show up in odd dimensions?
- What can be said about the cases of more ramified primes? Will it be possible to explore them by the same means or will we need more advanced machinery?

Thank you for your attention.