On circular units

(a series of lectures in Oujda, Morocco, May 19-21, 2015)

Radan Kučera, Masaryk University, Brno, Czech Republic

Motivation

Sometimes (e.g., trying to solve a Diophantine equation) we need to work in the ring $\mathcal{O}_K$ of algebraic integers of a number field K, a finite extension of $\mathbb{Q}$.

The ring $\mathcal{O}_K$ is not a unique factorisation domain in general, but it is a Dedekind domain, hence any non-zero ideal of $\mathcal{O}_K$ can be uniquelly written as a product of prime ideals.

So instead of decomposing an algebraic integer $a \in \mathcal{O}_K$ into the product of irreducible integers of $\mathcal{O}_K$ we can decompose the principal ideal $a\mathcal{O}_K$ into the product of prime ideals.

But at some point we need to return back from ideals to algebraic integers and this is possible only if we have a principal ideal. Then a generator of this principal ideal is well-defined up to a **unit** factor.

The obstruction for an ideal to be principal is hidden in the **class group** cl_K, which is the quotient of the group of all fractional ideals of $\mathcal{O}_K$ modulo the subgroup of the principal ideals.

So we would like to describe the following arithmetic objects of $\mathcal{O}_K$: its **class group** cl_K and its **group of units** $\mathcal{O}_K^\times$.

The group of units $\mathcal{O}_K^\times$ is a finitely generated abelian group

The torsional part W_K of $\mathcal{O}_K^\times$ is a cyclic finite group consisting of all the roots of unity belonging to K.

The rank of $\mathcal{O}_K^\times$ is given by Dirichlet unit theorem: $\mathcal{O}_K^\times \cong W_K \times \mathbb{Z}^r$, $r := \mathrm{rank}_{\mathbb{Z}}\, \mathcal{O}_K^\times = r_1 + r_2 - 1$, where r_1 is the number of real embeddings of K and r_2 is the number of pairs of complex embeddings of K. Hence the degree $[K : \mathbb{Q}] = r_1 + 2r_2$.

These embeddings can be determined also as follows: there is $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$. The minimal polynomial $f(X) \in \mathbb{Q}[X]$ of α has r_1 real roots $\alpha_1, \ldots, \alpha_{r_1}$ and r_2 pairs of complex roots $\alpha_{r_1+1}, \overline{\alpha_{r_1+1}}, \ldots, \alpha_{r_1+r_2}, \overline{\alpha_{r_1+r_2}}$.

Let σ_i be the embedding determined by $\alpha \mapsto \alpha_i$. Then σ_i is real if and only if $i \leq r_1$.

Therefore we know the rank r of $\mathcal{O}_K^\times$ but to find a system of generators of $\mathcal{O}_K^\times$ is a very difficult, often even intractable problem.

Geometry of units

Let $\ell : \mathcal{O}_K^\times \to \mathbb{R}^{r+1}$ be defined by $\ell(\varepsilon) = (\dots, \delta_i \log|\sigma_i(\varepsilon)|, \dots)$, where $\delta_i = 1$ for $i \le r_1$ and $\delta_i = 2$ otherwise.

Then $\ker \ell = W_K$ and $\operatorname{im} \ell \subset \mathcal{H} = \{(x_1, \dots, x_{r+1}) \mid \sum_{i=1}^{r+1} x_i = 0\}$.

For any r-tuple $\eta_1, \dots, \eta_r \in \mathcal{O}_K^\times$ we define the regulator

$$R(\eta_1, \dots \eta_r) = \left|\det(\delta_i \sigma_i(\eta_j))_{i,j=1,\dots,r}\right|.$$

Hence the regulator $R(\eta_1, \dots \eta_r)$ is given by the r-dimensional volume of the parallelepiped spanned by $\ell(\eta_1), \dots, \ell(\eta_r)$ in $\mathcal{H}$.

So $R(\eta_1, \dots \eta_r) = 0$ if and only if the units $\eta_1, \dots, \eta_r$ are (multiplicatively) dependent.

The regulator R_K of the field K is defined to be the regulator of any system of fundamental units, i.e., any r-tuple generating (together with W_K) the group of all units $\mathcal{O}_K^\times$.

Hence $[\mathcal{O}_K^\times : \langle W_k \cup \{\eta_1, \dots, \eta_r\}\rangle] = \frac{R(\eta_1, \dots \eta_r)}{R_K}$, if $R(\eta_1, \dots \eta_r) \neq 0$.

Dedekind ζ-function of K

Let ζ_K denote the Dedekind ζ-function of K. It is defined for any $s \in \mathbb{C}$, $\Re(s) > 1$, by the absolutely convergent series

$$\zeta_K(s) = \sum_A (N(A))^{-s},$$

where A in the sum runs over all nonzero ideals of $\mathcal{O}_K$ and $N(A) = |\mathcal{O}_K/A|$ is the absolute norm of A.

Since $\mathcal{O}_K$ is a Dedekind domain, each nonzero ideal A can be written as a product of prime ideals in a unique way.

The absolute norm is multiplicative and so $\zeta_K(s)$ can be written by the Euler product over all prime ideals of $\mathcal{O}_K$: if $\Re(s) > 1$ then

$$\zeta_K(s) = \prod_{\mathfrak{P}} (1 - N(\mathfrak{P})^{-s})^{-1}.$$

The class group cl_K is a finite abelian group

It was proven by Erich Hecke that $\zeta_K(s)$ has a meromorphic continuation to $\mathbb{C}$ having the only pole in $s = 1$. This is a simple pole with residuum

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}h_K R_K}{|W_K|\cdot\sqrt{|D_K|}},$$

where $h_K = |\,\mathrm{cl}_K\,|$ is the class number and D_K is the discriminant of K, which can be defined as follows:

The additive group $\mathcal{O}_K$ is a torsion-free abelian group whose rank is $\mathrm{rank}_{\mathbb{Z}}\,\mathcal{O}_K = [K:\mathbb{Q}] = r_1 + 2r_2$. Let $b_1,\ldots,b_{r_1+2r_2}$ be a system of independent generators of $\mathcal{O}_K$, then the discriminant D_K is the square of the determinant

$$\det\Big(\sigma_1(b_j),\ldots,\sigma_{r_1+r_2}(b_j),\overline{\sigma_{r_1+1}(b_j)},\ldots,\overline{\sigma_{r_1+r_2}(b_j)}\Big)_{j=1,\ldots,r_1+2r_2}.$$

The aim of this series of talks: Abelian fields

Let K be an abelian field, i.e., $K/\mathbb{Q}$ is a finite Galois extension having abelian Galois group $\mathrm{Gal}(K/\mathbb{Q})$.

Then K is a subfield of a cyclotomic field due to Kronecker – Weber theorem and we can be more specific:

- we have a group of circular units which is a subgroup of $\mathcal{O}_K^\times$ of finite index defined by explicit generators;
- there is a formula for this index having a factor h_{K^+}, the class number of the maximal real subfield $K^+ = K\cap\mathbb{R}$;
- if $K\subset\mathbb{R}$, we can use circular units to get annihilators of the class group cl_K.

The main aim of this series of talks consists in an explanation of these three items.

Dirichlet characters

A Dirichlet character modulo $m \in \mathbb{Z}$, $m > 0$, is a group homomorphism $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$.

If $m \mid n$ then χ induces a homomorphism $(\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$ by composition with the natural map $(\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times$.

Therefore, we can regard χ as being defined modulo m or n, since both are essentially the same map. It is convenient to choose n minimal and call it the conductor of χ, denoted by f_χ. Then χ can be given by a Dirichlet character modulo m if and only if $f_\chi \mid m$.

To emphasize that we consider χ modulo f_χ, we say that χ is a primitive character.

Often we regard a Dirichlet character χ as a map $\mathbb{Z} \to \mathbb{C}$ by letting $\chi(a) = 0$ if $(a, f_\chi) \neq 1$; and $\chi(a) = \chi(a + f_\chi\mathbb{Z})$ if $(a, f_\chi) = 1$. So χ is then periodic of period f_χ.

Example: for any odd prime p the Legendre symbol $\left(\frac{a}{p}\right)$ is a Dirichlet character of conductor p.

The group of Dirichlet characters

To define the product of Dirichlet characters χ and ψ, let $m = \operatorname{lcm}(f_\chi, f_\psi)$ and let $\gamma : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ be defined by $\gamma(a) = \chi(a)\psi(a)$ if $(a, m) = 1$; then the product $\chi\psi$ is defined to be the primitive Dirichlet character associated to γ.

The set of all primitive Dirichlet characters together with this product forms an infinite abelian group.

Example: Let the Dirichlet characters χ, ψ be given by

$$\chi(a) = \begin{cases} 1 & \text{if } a \equiv \pm 1 \pmod{12}, \\ -1 & \text{if } a \equiv \pm 5 \pmod{12}, \\ 0 & \text{otherwise,} \end{cases} \quad \psi(a) = \begin{cases} 1 & \text{if } a \equiv 1 \pmod{3}, \\ -1 & \text{if } a \equiv 2 \pmod{3}, \\ 0 & \text{otherwise.} \end{cases}$$

Then $f_\chi = 12$, $f_\psi = 3$, but $f_{\chi\psi} = 4$, since

$$(\chi\psi)(a) = \begin{cases} 1 & \text{if } a \equiv 1 \pmod{4}, \\ -1 & \text{if } a \equiv 3 \pmod{4}, \\ 0 & \text{otherwise.} \end{cases}$$

Note that $(\chi\psi)(3) = -1 \neq 0 = \chi(3) \cdot \psi(3)$.

Cyclotomic polynomials

Let m be a positive integer, $\zeta_m = e^{2\pi i/m}$. The m-th cyclotomic polynomial is defined as

$$\Phi_m(x) = \prod_{a=1,\dots,m,\,(a,m)=1} (x - \zeta_m^a).$$

The polynomial Φ_m is monic and has a root ζ_m.

Since $\prod_{d|m} \Phi_d(x) = x^m - 1$, by induction we get $\Phi_m(x) \in \mathbb{Q}[x]$.

As its roots are algebraic integers, $\Phi_m(x) \in \mathbb{Z}[x]$.

Finally, $\Phi_m(x)$ is irreducible over $\mathbb{Z}$. If m is a prime power, the irreducibility of $\Phi_m(x)$ can be obtained using Eisenstein criterion. In general the proof of its irreducibility is tricky but short and not complicated.

Hence the cyclotomic polynomial Φ_m is the minimal polynomial of ζ_m over $\mathbb{Q}$, and the m-th cyclotomic field $\mathbb{Q}_m = \mathbb{Q}(\zeta_m)$ is of degree $[\mathbb{Q}_m : \mathbb{Q}] = \varphi(m)$.

Dirichlet characters as characters on a Galois group

Therefore we have $(\mathbb{Z}/m\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}_m/\mathbb{Q})$, where the class $a + m\mathbb{Z}$ (here $(a, m) = 1$) corresponds to the automorphism σ_a of $\mathbb{Q}_m$ determined by $\sigma_a(\zeta_m) = \zeta_m^a$.

If χ is a Dirichlet character of conductor $f_\chi \mid m$ then χ can be understood as a character on $\mathrm{Gal}(\mathbb{Q}_m/\mathbb{Q})$.

Example: Let us return to the Dirichlet character χ given by

$$\chi(a) = \begin{cases} 1 & \text{if } a \equiv \pm 1 \pmod{12}, \\ -1 & \text{if } a \equiv \pm 5 \pmod{12}, \\ 0 & \text{otherwise.} \end{cases}$$

Considering χ as a character on $\mathrm{Gal}(\mathbb{Q}_{12}/\mathbb{Q}) = \{\sigma_1, \sigma_5, \sigma_{-1}, \sigma_{-5}\}$, we get $\ker \chi = \{\sigma_1, \sigma_{-1}\} = \mathrm{Gal}(\mathbb{Q}_{12}/\mathbb{Q}(\sqrt{3}))$.

Therefore the character χ gives the field $\mathbb{Q}(\sqrt{3})$.

Abelian field given by a finite group of Dirichlet characters

Let X be a **finite** subgroup of the group of all Dirichlet characters, let m be the least common multiple of conductors f_χ, $\chi \in X$.

Then all $\chi \in X$ are characters on $\mathrm{Gal}(\mathbb{Q}_m/\mathbb{Q})$ and they define a unique subfield K of $\mathbb{Q}_m$ as follows: $\mathrm{Gal}(\mathbb{Q}_m/K)$ is the intersection of the kernels of all $\chi \in X$. Moreover $\chi \in X$ give all characters on $\mathrm{Gal}(K/\mathbb{Q})$, since

$$\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}_m/\mathbb{Q})/\mathrm{Gal}(\mathbb{Q}_m/K).$$

The above procedure $X \mapsto K$ forms a natural isomorphism between the lattice of all finite subgroups of the group of all Dirichlet characters and the lattice of all abelian fields.

It allows to describe many arithmetical properties of an abelian field K in terms of properties of the corresponding subgroup X of Dirichlet characters.

Arithmetical properties of K via the corresponding X

Let K be an abelian field and X be the group of Dirichlet characters of K. There is a non-degenerate natural pairing

$$\mathrm{Gal}(K/\mathbb{Q}) \times X \to \mathbb{C}^\times,$$

so we can identify X with the group of characters on $\mathrm{Gal}(K/\mathbb{Q})$. We also have a noncanonical isomorphism $\mathrm{Gal}(K/\mathbb{Q}) \cong X$.

It is convenient to classify characters into two types: if $\chi(-1) = 1$ then χ is called even; if $\chi(-1) = -1$ then χ is called odd.

Since the complex conjugation corresponds to σ_{-1}, it is clear that K is real if and only if each $\chi \in X$ is even. Or even more precisely: the number r_2 of pairs of complex embeddings of K equals the number of odd characters in X.

A much deeper result is the following Conductor-Discriminant Formula

$$D_K = (-1)^{r_2} \prod_{\chi \in X} f_\chi = \prod_{\chi \in X} \chi(-1) f_\chi.$$

Decomposition of prime numbers in $\mathcal{O}_K$ via X

Let K be an abelian field and X be the group of Dirichlet characters of K, let $G = \mathrm{Gal}(K/\mathbb{Q})$.

For a fixed prime number p we can decompose the ideal

$$p\mathcal{O}_K = (\mathfrak{P}_1 \cdot \ldots \cdot \mathfrak{P}_g)^e$$

into prime ideals $\mathfrak{P}_i$ of the same norm $N(\mathfrak{P}_i) = p^f$.

So e, f, and g are the ramification index, the residue class degree, and the number of prime ideals of K lying above p, respectively.

Since G is abelian, all prime ideals $\mathfrak{P}_i$ have the same decomposition group $D = \{\sigma \in G \mid \sigma(\mathfrak{P}_i) = \mathfrak{P}_i\}$ and the same inertia group $I = \{\sigma \in G \mid \forall \alpha \in O_K : \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}_i}\}$.

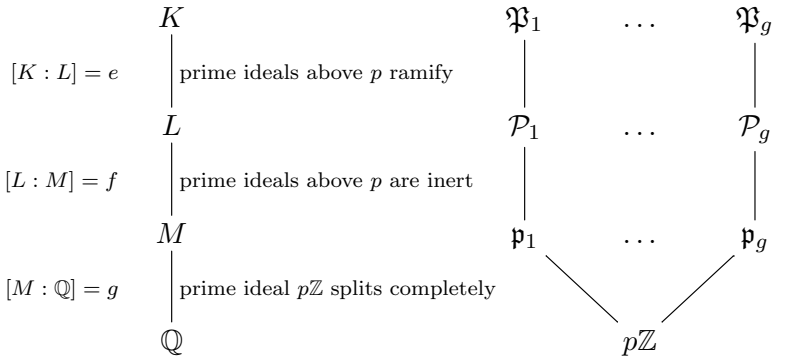
The inertia field L and the decomposition field M are determined by $\mathrm{Gal}(K/L) = I$ and $\mathrm{Gal}(K/M) = D$. Then

$Y = \{\chi \in X \mid \chi(p) \neq 0\}$ is the group of Dirichlet characters of L,

$Z = \{\chi \in X \mid \chi(p) = 1\}$ is the group of Dirichlet characters of M.

Decomposition of prime numbers graphically

X is the group of Dirichlet characters of K, p is a prime number,
$Y = \{\chi \in X \mid \chi(p) \neq 0\}$ is the group of Dirichlet characters of L,
$Z = \{\chi \in X \mid \chi(p) = 1\}$ is the group of Dirichlet characters of M,
$I = \mathrm{Gal}(K/L) \cong X/Y, \qquad D = \mathrm{Gal}(K/M) \cong X/Z.$



$p\mathcal{O}_M = \mathfrak{p}_1 \ldots \mathfrak{p}_g, \qquad \mathfrak{p}_i\mathcal{O}_L = \mathcal{P}_i, \qquad \mathcal{P}_i\mathcal{O}_K = \mathfrak{P}_i^e.$

Dedekind ζ-function ζ_K of an abelian field K

Let K be an abelian field and X be the group of Dirichlet characters of K. Recall that for $s \in \mathbb{C}$, $\Re(s) > 1$,

$$\zeta_K(s) = \prod_{\mathfrak{P}} (1 - N(\mathfrak{P})^{-s})^{-1}.$$

Since each prime ideal $\mathfrak{P}$ is a divisor of a unique prime number p, denoting f_p and g_p the residue class degree and the number of prime ideals of K lying above p, respectively, we have

$$\zeta_K(s) = \prod_{p} (1 - p^{-f_p s})^{-g_p} = \prod_{p} \prod_{\chi \in X} (1 - \chi(p) p^{-s})^{-1},$$

again if $\Re(s) > 1$. Hence $\zeta_K(s) = \prod_{\chi \in X} L(s, \chi)$, where

$$L(s, \chi) = \prod_{p} (1 - \chi(p) p^{-s})^{-1} = \sum_{n=1}^{\infty} \chi(n) n^{-s}$$

is the Dirichlet L-function corresponding to χ.

Comparing two formulas for the residuum of $\zeta_K(s)$ at $s = 1$

Let K be an abelian field and X be the group of Dirichlet characters of K. Then we have

$$\prod_{\chi \in X,\ \chi \neq 1} L(1, \chi) = \lim_{s \to 1} (s - 1) \zeta_K(s) = \frac{2^{r_1} (2\pi)^{r_2} h_K R_K}{|W_K| \cdot \sqrt{|D_K|}}.$$

An important corollary: for each $\chi \in X$, $\chi \neq 1$, we have $L(1, \chi) \neq 0$ (this allows to prove Dirichlet's theorem on primes in arithmetic progressions).

The formula above can be used to compute the product $h_K R_K$. We have

$$L(1, \chi) = \begin{cases} -\frac{\pi i}{f_\chi \tau(\overline{\chi})} \sum_{a=1}^{f_\chi - 1} \overline{\chi}(a) \cdot a & \text{if } \chi \text{ is odd,} \\ -\frac{1}{\tau(\overline{\chi})} \sum_{a=1}^{f_\chi - 1} \overline{\chi}(a) \cdot \log |1 - \zeta_{f_\chi}^a| & \text{if } \chi \text{ is even,} \end{cases}$$

where $\tau(\chi) = \sum_{a=1}^{f_\chi} \chi(a) \zeta_{f_\chi}^a$ is the Gauss sum of χ.

Analytic Class Number Formula for a real abelian field K

Let K be a real abelian field and X be the group of Dirichlet characters of K. Then we have

$$h_K R_K = \prod_{\chi\in X,\ \chi\neq 1} \left(-\frac{1}{2} \sum_{a=1}^{f_\chi - 1} \overline{\chi}(a) \cdot \log|1 - \zeta_{f_\chi}^a| \right). \tag{1}$$

The factors of (1) have the following interpretation: for even $\chi \neq 1$

$$L'(0,\chi) = -\frac{1}{2} \sum_{a=1}^{f_\chi - 1} \chi(a) \cdot \log|1 - \zeta_{f_\chi}^a|, \tag{2}$$

where we deal with the analytic continuation of $L(s,\chi)$ to $\mathbb{C}$.

Have a look at these interesting numbers that have appeared here:

$$1 - \zeta_{f_\chi}^a, \qquad a = 1, \ldots, f_\chi - 1.$$

These are so-called circular numbers, the main topic of our talks!

Basic properties of circular numbers

Recall that $\Phi_m(x)$ is the m-th cyclotomic polynomial.

Since $\prod_{d|m} \Phi_d(x) = x^m - 1$, we have $\prod_{1<d|m} \Phi_d(x) = \sum_{i=0}^{m-1} x^i$, setting $x = 1$ we obtain $\prod_{1<d|m} \Phi_d(1) = m$.

So for any $m > 1$ we obtain by induction

$$\Phi_m(1) = \begin{cases} p & \text{if } m \text{ is a power of a prime } p, \\ 1 & \text{otherwise.} \end{cases}$$

Hence if m is not a prime power, $1 - \zeta_m^a$ is a unit of $\mathcal{O}_{\mathbb{Q}_m}$ for any $a \in \mathbb{Z}$, $(a, m) = 1$.

Suppose that m is a power of a prime p. Let $a, b \in \mathbb{Z}$, $p \nmid ab$. Since there is a positive integer k satisfying $ak \equiv b \pmod{m}$, we have $1 - \zeta_m^b = (1 - \zeta_m^a) \cdot \sum_{i=0}^{k-1} \zeta_m^{ia}$. Hence, using the symmetry $a \leftrightarrow b$, we get that

$$\frac{1 - \zeta_m^b}{1 - \zeta_m^a} \qquad \text{is a unit of } \mathcal{O}_{\mathbb{Q}_m}.$$

Basic properties of circular numbers, relations

Let $0 < d \mid m$, then

$$\prod_{i=0}^{d-1}(x - \zeta_d^i) = x^d - 1,$$

put $x = \zeta_m^{-a}$ for any $a \in \mathbb{Z}$, $m \nmid a$, to get

$$\prod_{i=0}^{d-1}(\zeta_m^{-a} - \zeta_d^i) = \zeta_m^{-ad} - 1,$$

hence

$$\prod_{i=0}^{d-1}(1 - \zeta_m^{a+i\cdot(m/d)}) = 1 - \zeta_m^{ad}. \tag{3}$$

We also have

$$1 - \zeta_m^a = -\zeta_m^a(1 - \zeta_m^{-a}). \tag{4}$$

Groups of circular numbers/units of a cyclotomic field

Let $m \in \mathbb{Z}$, $m > 1$. The group D_m of **circular numbers** of m-th cyclotomic field $\mathbb{Q}_m$ is defined as the subgroup of the multiplicative group $\mathbb{Q}_m^\times$ generated by the following set:

$$D_m = \big\langle \{-1, \zeta_m\} \cup \{1 - \zeta_m^a \mid a \in \mathbb{Z},\, 1 \le a < m\} \big\rangle,$$

so D_m contains all roots of unity in $\mathbb{Q}_m$.

The group C_m of **circular units** of m-th cyclotomic field $\mathbb{Q}_m$ is defined as the intersection $C_m = D_m \cap \mathcal{O}_{\mathbb{Q}_m}^\times$.

It is clear that we do not need all generators used in the definition of D_m, for example, using (4), we get

$$D_m = \big\langle \{-1, \zeta_m\} \cup \{1 - \zeta_m^a \mid a \in \mathbb{Z},\, 1 \le a \le \tfrac{m}{2}\} \big\rangle.$$

But there are more relations in general!

The situation is easier if m is a prime power.

The prime-power case

Let us suppose $m = p^k > 2$, where p is a prime and $k \in \mathbb{Z}$. Denote $M = \{a \in \mathbb{Z},\, 1 < a \le \frac{m}{2},\, p \nmid a\}$. Relations (3) and (4) imply that

$$D_m = \big\langle \{-1, \zeta_m\} \cup \{1 - \zeta_m^a \mid a \in M \cup \{1\}\} \big\rangle,$$

hence

$$C_m = \Big\langle \{-1, \zeta_m\} \cup \Big\{ \frac{1-\zeta_m^a}{1-\zeta_m} \mid a \in M \Big\} \Big\rangle.$$

Since $\eta_a = \frac{1-\zeta_m^a}{1-\zeta_m} \zeta_m^{(1-a)/2} \in \mathbb{R}$, we can work in $\mathbb{Q}_m^+ = \mathbb{Q}_m \cap \mathbb{R}$, because

$$C_m \cap \mathbb{R} = \big\langle \{-1\} \cup \{\eta_a \mid a \in M\} \big\rangle \subseteq \mathcal{O}^\times_{\mathbb{Q}_m^+}.$$

There are exactly $\frac{\varphi(m)}{2} - 1 = \operatorname{rank}_{\mathbb{Z}} \mathcal{O}^\times_{\mathbb{Q}_m^+}$ units η_a there.

Let us compute their regulator to find out whether they are multiplicatively independent.

The regulator of η_a, $a \in M$, in $\mathbb{Q}_m^+$, for $m = p^k$

Recall: $M = \{a \in \mathbb{Z},\, 1 < a \le \frac{m}{2},\, p \nmid a\}$, $\eta_a = \frac{1-\zeta_m^a}{1-\zeta_m} \zeta_m^{(1-a)/2}$,

$$R(\eta_a;\, a \in M) = \Big| \det\Big(\log|1 - \zeta_m^{ab}| - \log|1 - \zeta_m^b| \Big)_{a,b \in M} \Big|.$$

Theorem on group determinants. Let G be a finite abelian group, $\widehat{G}$ the group of all characters of G, i.e., homomorphisms $G \to \mathbb{C}^\times$. Then for any function $f : G \to \mathbb{C}$ we have

$$\begin{aligned} \det\big(f(g \cdot h^{-1})\big)_{g,h \in G} &= \prod_{\chi \in \widehat{G}} \sum_{g \in G} \chi(g) f(g), \\ \det\big(f(g \cdot h^{-1}) - f(g)\big)_{g,h \in G - \{1\}} &= \prod_{\chi \in \widehat{G},\, \chi \ne 1} \sum_{g \in G} \chi(g) f(g). \end{aligned}$$

Let $G = (\mathbb{Z}/m\mathbb{Z})^\times / \{1, -1\}$, then $M \cup \{1\}$ is a system of representatives of G. Then $\widehat{G}$ is the group of even Dirichlet characters χ whose conductor $f_\chi \mid m$. Let $f(a) = \log|1 - \zeta_m^a|$. Using (3) we get for any such $\chi \ne 1$

$$\sum_{a \in M \cup \{1\}} \chi(a) f(a) = \tfrac{1}{2} \sum_{1 \le a < f_\chi,\, p \nmid a} \chi(a) \log|1 - \zeta_{f_\chi}^a|$$

and (1) gives $R(\eta_a;\, a \in M) = h_{\mathbb{Q}_m^+} \cdot R_{\mathbb{Q}_m^+}$, i.e.,

$$[\mathcal{O}^\times_{\mathbb{Q}_m} : C_m] = [\mathcal{O}^\times_{\mathbb{Q}_m^+} : (C_m \cap \mathbb{R})] = h_{\mathbb{Q}_m^+},$$

which has been known already to Kummer.

Generalization to $\mathbb{Q}_m^+$ for any m

For a general m we need another method. Our computation is based on the fact that there is a circular number $\varepsilon = 1 - \zeta_m$ such that

$$C_m \cap \mathbb{R} = \Big\langle \{-1\} \cup \big\{ |\varepsilon^{\sigma-1}| \mid \sigma \in \mathrm{Gal}(\mathbb{Q}_m^+/\mathbb{Q}) \big\} \Big\rangle,$$

where $\varepsilon^{\sigma-1} = \frac{\varepsilon^\sigma}{\varepsilon}$.

But such a circular number does not exist in general, i.e. for m not being a prime-power!

If m is not a prime-power, then even sometimes the units

$$(1-\zeta_m)^{\sigma-1}, \qquad \sigma \in \mathrm{Gal}(\mathbb{Q}_m^+/\mathbb{Q}) - \{1\},$$

are multiplicatively dependent.

Ramachandra's approach

Let $m > 2$, $m \not\equiv 2 \pmod 4$. Define

$$\varepsilon = \prod_{1<d|m,\,(d,\frac{m}{d})=1} (1-\zeta_d).$$

Then the regulator of $|\varepsilon^{\sigma-1}|$, where $\sigma \in \mathrm{Gal}(\mathbb{Q}_m^+/\mathbb{Q}) - \{1\}$, can be computed similarly as in the case of m being prime-power (up to some manageable technical difficulties).

This shows that, for each such m, the regulator is non-zero. In fact, it is a large multiple of $h_{\mathbb{Q}_m^+} R_{\mathbb{Q}_m^+}$.

This implies that the index $[\mathcal{O}_{\mathbb{Q}_m}^\times : C_m] = [\mathcal{O}_{\mathbb{Q}_m^+}^\times : C_m \cap \mathbb{R}]$ is finite though we are not able to compute it by this method.

Sinnott's computation of the index $[\mathcal{O}^\times_{\mathbb{Q}_m} : C_m]$

Theorem (Sinnott). *Let $m \in \mathbb{Z}$, $m > 1$, $m \not\equiv 2 \pmod 4$. Then*

$$[\mathcal{O}^\times_{\mathbb{Q}_m} : C_m] = 2^b \cdot h_{\mathbb{Q}^+_m},$$

where b is given by the number g of prime divisors of m as follows

$$b = \begin{cases} 0 & \text{if } g = 1, \\ 2^{g-2} - g + 1 & \text{if } g > 1. \end{cases}$$

A key ingredient in Sinnott's proof is a construction of his module U and some cohomology computation.

By difficult and extensive numerical computations we know that $h_{\mathbb{Q}^+_m} = 1$ if $m \le 135$. So in this case we have $C_m = \mathcal{O}^\times_{\mathbb{Q}_m}$, each unit is circular.

We also know $h_{\mathbb{Q}^+_{136}} = 2$, so $[\mathcal{O}^\times_{\mathbb{Q}_{136}} : C_{136}] = 2$.

Back to the relations

Recall that if $0 < d \mid m$, then $\prod_{i=0}^{d-1}(1 - \zeta_m^{a+i\cdot(m/d)}) = 1 - \zeta_m^{ad}$. This gives the **"distribution relations"** (they are also called the **"norm relations"**): If a prime $p \mid m$, $p < m$, and $p \nmid a \in \mathbb{Z}$, then

$$\mathrm{N}_{\mathbb{Q}_m/\mathbb{Q}_{m/p}}(1 - \zeta_m^a) = \begin{cases} 1 - \zeta_{m/p}^a & \text{if } p \mid \frac{m}{p}, \\ \frac{1-\zeta_{m/p}^b}{1-\zeta_{m/p}^{b/p}} & \text{if } p \nmid \frac{m}{p}, \end{cases}$$

where, in the latter case, $b \in \mathbb{Z}$, $b \equiv a \pmod{\frac{m}{p}}$, $b \equiv 0 \pmod p$.

If $m = p$ is a prime and $p \nmid a \in \mathbb{Z}$, then

$$\mathrm{N}_{\mathbb{Q}_p/\mathbb{Q}}(1 - \zeta_p^a) = p.$$

Of course, if $p \mid m$ and $p \mid a$ then $1 - \zeta_m^a = 1 - \zeta_{m/p}^{a/p}$, so in this case

$$\mathrm{N}_{\mathbb{Q}_m/\mathbb{Q}_{m/p}}(1 - \zeta_m^a) = (1 - \zeta_{m/p}^{a/p})^{[\mathbb{Q}_m:\mathbb{Q}_{m/p}]}.$$

There are also the **"mirror relations"**: for any $a \in \mathbb{Z}$

$$1 - \zeta_m^a = -\zeta_m^a \cdot (1 - \zeta_m^{-a}).$$

Theorem of Bass – Ennola

Theorem. *Let $m \in \mathbb{Z}$, $m > 1$, $m \not\equiv 2 \pmod 4$, and let A_m be the additive abelian group with generators*

$$\{g(a) \mid a \in \mathbb{Z}/m\mathbb{Z},\, a \neq 0\}$$

(where 0 means $m\mathbb{Z}$) and relations

$$g(a) = g(-a) \qquad \text{for each } 0 \neq a \in \mathbb{Z}/m\mathbb{Z},$$

$$\sum_{j=0}^{d-1} g(a + j\tfrac{m}{d}) = g(da) \qquad \text{for each } 0 < d \mid m,\ a \in \mathbb{Z}/m\mathbb{Z},\ da \neq 0.$$

Then there is the following exact sequence of abelian groups

$$0 \to (\mathbb{Z}/2\mathbb{Z})^{c_m} \to A_m \to D_m/\langle \pm\zeta_m \rangle \to 0$$

for an integer $c_m \geq 0$.

The nonzero elements in the image of $(\mathbb{Z}/2\mathbb{Z})^{c_m}$ are called **relations of Ennola's type**.

Let g be the number of prime divisors of m. Schmidt proved that $c_m = 0$ if $g = 1$ and $c_m = 2^{g-1} - g$ if $g > 1$.

A $\mathbb{Z}$-basis of C_m

For m being a prime-power, we have computed the index $[\mathcal{O}_{\mathbb{Q}_m}^{\times} : C_m]$. The key ingredients has been the construction of a $\mathbb{Z}$-basis of C_m and the computation of its regulator.

Sinnott was able to compute this index for any positive integer m without a construction of a $\mathbb{Z}$-basis of C_m.

So do we need a $\mathbb{Z}$-basis of C_m?

Such a basis could be useful when we need to decide whether a given unit of $\mathbb{Q}_m$ belongs to C_m or not. A construction of a $\mathbb{Z}$-basis of C_m played a crucial role in the following result of Gold and Kim:

Theorem. *The groups of circular units C_m of cyclotomic fields satisfy Galois descent, i.e., if n, m are positive integers and $n \mid m$ then*

$$C_n = C_m \cap \mathbb{Q}_n.$$

A description of this basis is very technical; we avoid giving it here.

Circular units of an abelian field – required properties

Let K be an abelian field.

What should a group $C(K)$ of circular units of K satisfy?

(1) a finite set of explicit generators;

(2) a finite index $[\mathcal{O}_K^\times : C(K)]$, which should be a small explicit multiple of h_{K^+};

(3) an understandable Galois-module structure;

(4) the Galois descent (if $L \subseteq K$ then $C(L) = C(K) \cap L$);

(5) for $K = \mathbb{Q}_m$ we should have $C(\mathbb{Q}_m) = C_m$ defined above.

Can we require all this properties?

Sorry, but *we cannot.*

Let us have a look why a definition satisfying all these required properties does not exist...

Washington's definition

Due to the mentioned theorem of Gold and Kim, (4) and (5) are not contradicting to each other.

Assuming (4) and (5), there is only one possible definition satisfying both of them:

Let m be the conductor of K (the smallest m such that $K \subseteq \mathbb{Q}_m$). The **Washington group of circular units** of K is defined as follows:

$$C_{\mathrm{W}}(K) = K \cap C_m.$$

But we have neither (1) nor (3). Concerning (2), the index is finite and relatively small. But we do not have a formula for the index.

Which fields K have the index $[\mathcal{O}_K^\times : C_{\mathrm{W}}(K)]$ known?

If $K = \mathbb{Q}_m$ then $C_W(K) = C_m$ and the index is given by Sinnott's formula.

If $K = \mathbb{Q}_m^+$ then $[C_m : C_{\mathrm{W}}(K)]$ is an explicit power of 2.

I know only the following two special cases of abelian fields for which we have a formula for the index (an explicit construction of a $\mathbb{Z}$-basis and the computation of the index is due to Werl):

- any real abelian field whose Galois group is the direct product of inertia groups;
- a cyclic field K (i.e., $\mathrm{Gal}(K/\mathbb{Q})$ is a cyclic group) satisfying: each prime which ramifies in $K/\mathbb{Q}$ is totally ramified here and the genus field of K in narrow sense is real.

Therefore in general the Washington group of circular units is too difficult to work with.

Taking norm instead of intersection

Let m be the conductor of an abelian field K. Let W_K be the group of roots of unity of K.

The **group of circular units of conductor level** of K is defined by

$$C_{\mathrm{cl}}(K) = W_K \cdot \{\mathrm{N}_{\mathbb{Q}_m/K}(\alpha) \mid \alpha \in C_m\}.$$

Explicitly

$$C_{\mathrm{cl}}(K) = \left\langle W_K \cup \left\{\mathrm{N}_{\mathbb{Q}_m/K}(1-\zeta_m^a);\, a \in \mathbb{Z},\, m \nmid a\right\}\right\rangle \cap \mathcal{O}_K^\times.$$

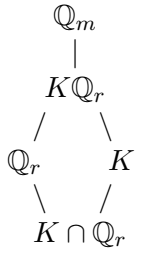
But as we shall compute, if $(a, m) > 1$ then the norm $\mathrm{N}_{\mathbb{Q}_m/K}(1-\zeta_m^a)$ is a power of an explicit number.

Due to (2) we want the index $[\mathcal{O}_K^\times : C(K)]$ to be small, so we should add these explicit numbers into the set of generators of $C(K)$!

Extracting root of $\mathrm{N}_{\mathbb{Q}_m/K}(1-\zeta_m^a)$ for $(a,m)>1$

Let m be the conductor of an abelian field K.

Let $a\in\mathbb{Z}$, $m\nmid a$, $(a,m)>1$. Put $r=\frac{m}{(a,m)}<m$, $b=\frac{a}{(a,m)}$, then $1-\zeta_m^a=1-\zeta_r^b$. We have the following diagram of fields:



Hence $\mathrm{Gal}(K\mathbb{Q}_r/K)\cong\mathrm{Gal}(\mathbb{Q}_r/(K\cap\mathbb{Q}_r)$ via restriction. So for any $\alpha\in\mathbb{Q}_r$ we have

$$\mathrm{N}_{K\mathbb{Q}_r/K}(\alpha)=\prod_{\sigma\in\mathrm{Gal}(K\mathbb{Q}_r/K)}\alpha^\sigma=\prod_{\sigma\in\mathrm{Gal}(\mathbb{Q}_r/(K\cap\mathbb{Q}_r)}\alpha^\sigma$$
$$=\mathrm{N}_{\mathbb{Q}_r/(K\cap\mathbb{Q}_r)}(\alpha).$$

Moreover $\mathrm{N}_{\mathbb{Q}_m/K\mathbb{Q}_r}(\alpha)=\alpha^{[\mathbb{Q}_m:K\mathbb{Q}_r]}$. Therefore

$$\mathrm{N}_{\mathbb{Q}_m/K}(1-\zeta_m^a)=\mathrm{N}_{\mathbb{Q}_m/K}(1-\zeta_r^b)=\mathrm{N}_{\mathbb{Q}_r/K\cap\mathbb{Q}_r}(1-\zeta_r^b)^{[\mathbb{Q}_m:K\mathbb{Q}_r]}.$$

So we can enlarge $C_{\mathrm{cl}}(K)$ replacing the generator $\mathrm{N}_{\mathbb{Q}_m/K}(1-\zeta_m^a)$ by a new generator $\mathrm{N}_{\mathbb{Q}_r/K\cap\mathbb{Q}_r}(1-\zeta_r^b)$.

Sinnott group of circular units of an abelian field

Let m be the conductor of an abelian field K. The **Sinnott group of circular units** of K is defined by

$$C_{\mathrm{S}}(K)=\langle\pm\,\mathrm{N}_{\mathbb{Q}_r/\mathbb{Q}_r\cap K}(1-\zeta_r^a);\ r\mid m,\ 1\le a<r\rangle\cap\mathcal{O}_K^\times.$$

Properties of $C_{\mathrm{S}}(K)$:

(1) a finite set of explicit generators;

(2) a finite index $[\mathcal{O}_K^\times:C(K)]=c_K\cdot h_{K^+}$, we have Sinnott's formula for c_K, where one of the factors is the index of so-called Sinnott's module U; this factor is not easy to compute in general;

(3) an understandable Galois-module structure given by Sinnott's module U;

(4) the Galois descent does **not** hold true for $C_{\mathrm{S}}(K)$;

(5) for $K=\mathbb{Q}_m$ we have $C_{\mathrm{S}}(\mathbb{Q}_m)=C_m$.

Other definitions of circular units of an abelian field

We have seen that Sinnott's definition has fulfilled almost all required properties (well, we do not have Galois descent and one factor in the formula for the index is not fully explicit).

In the literature we can find other definitions, e.g., groups obtained via Ramachandra-type construction (Ramachandra, Levesque, Greither) or via cyclic subfields (Hasse, Leopoldt, Gillard). The groups obtained by both of these approaches have much easier Galois module structure allowing to compute the index as h_{K^+} multiplied by an explicit factor, but these factors are huge.

Another good property of Sinnott's definition: for $p \neq 2$ Sinnott's group is useful in Iwasawa theory since the p-part of the factors c_K stabilizes in the $\mathbb{Z}_p$-tower of the cyclotomic $\mathbb{Z}_p$-extension of an abelian field.

Résumé

There are several different definitions giving different groups of circular units of an abelian field K.

The largest one is the Washington group of circular units $C_{\mathrm{W}}(K)$ but we do not know explicit generators.

The group of circular units of Ramachandra's type has the easiest possible Galois module structure. This allows to compute its index and it is used to prove the p-adic version of the class number formula for an abelian field.

The one being admitted to be optimal is the Sinnott group of circular units $C_{\mathrm{S}}(K)$. This group can be used to derive a result on the class number or even on the structure of the class group.

The connection of circular units to the class group consists just in the analytic class number formula, there is *no direct algebraic relation*. This formula gives just the class number, so how can we say anything more concerning *the structure of the class group?*

Group rings and $\mathbb{Z}[G]$-modules

Recall the notion of a group ring: having a finite group G then the group ring $\mathbb{Z}[G]$ consists of all mappings $G \to \mathbb{Z}$. It is customary to write them as formal sums:

$$\mathbb{Z}[G] = \Big\{ \sum_{g \in G} a_g g \mid a_g \in \mathbb{Z} \Big\},$$

where the addition is defined "componentwise" and the multiplication is given by formula $(rg) \cdot (sh) = (r \cdot s)(g \cdot h)$ for each $r, s \in \mathbb{Z}$ and $g, h \in G$ and by the distributive laws.

For example, if $K/\mathbb{Q}$ is a Galois extension and $G_K = \mathrm{Gal}(K/\mathbb{Q})$ then the group $\mathcal{I}_K$ of fractional ideals of K is a $\mathbb{Z}[G_K]$-module, the action of any $\alpha = \sum_{\sigma \in G_K} a_\sigma \sigma \in \mathbb{Z}[G_K]$ on a fractional ideal I is given by

$$I^\alpha = \prod_{\sigma \in G_K} \sigma(I)^{a_\sigma}.$$

Similarly $(K, +)$, $(K^\times, \cdot)$, $(\mathcal{O}_K, +)$, $(\mathcal{O}_K^\times, \cdot)$, $(\mathrm{cl}_K, \cdot)$ form $\mathbb{Z}[G_K]$-modules.

The class group as a $\mathbb{Z}[G_K]$-module

Let K be an abelian field, $G_K = \mathrm{Gal}(K/\mathbb{Q})$. For a prime p, let $\mathrm{cl}_{K,p}$ denote the p-Sylow subgroup of cl_K, and $(\mathcal{O}_K^\times / C_{\mathrm{S}}(K))_p$ the p-Sylow subgroup of $\mathcal{O}_K^\times / C_{\mathrm{S}}(K)$.

Sinnott's formula implies:
if $p \nmid 2[K : \mathbb{Q}]$ then $|(E(K)/C_{\mathrm{S}}(K))_p| = |\,\mathrm{cl}_{K,p}\,|$.

Example. In general $\mathrm{cl}_{K,p} \ncong (\mathcal{O}_K^\times / C_{\mathrm{S}}(K))_p$. If $K = \mathbb{Q}(\sqrt{62501})$ and $p = 3$ then $\mathrm{cl}_{K,p} \cong (\mathbb{Z}/3\mathbb{Z})^2$ while $(\mathcal{O}_K^\times / C_{\mathrm{S}}(K))_p \cong \mathbb{Z}/9\mathbb{Z}$.

What can be said about the structure of these G_K-modules?

Conjecture of G. Gras: If $p \nmid 2[K : \mathbb{Q}]$ then these $\mathbb{Z}[G_K]$-modules have the same Jordan-Hölder series.

This is not a conjecture anymore as Greenberg proved that this follows from the Main Conjecture of Iwasawa theory. And later on Mazur and Wiles proved the Main Conjecture. An easier proof via Euler system machinery is based on a work of Thaine and Kolyvagin.

What are annihilators of the class group?

Let K be an abelian field, $G_K = \mathrm{Gal}(K/\mathbb{Q})$.

If M is a $\mathbb{Z}[G_K]$-module, the annihilator ideal of M is defined to be $\mathrm{Ann}_{\mathbb{Z}[G_K]}\big(M\big) = \{\alpha \in \mathbb{Z}[G_K] \mid \alpha M = 0\}$, an annihilator of M is any $\alpha \in \mathbb{Z}[G_K]$ such that $\alpha M = 0$.

So the annihilator ideal of the class group cl_K is

$$\mathrm{Ann}_{\mathbb{Z}[G_K]}\big(\mathrm{cl}_K\big) = \{\alpha \in \mathbb{Z}[G_K] \mid \forall \text{ ideal } I \text{ of } \mathcal{O}_K\colon\ I^\alpha \text{ is principal}\}.$$

For example the class number $|\mathrm{cl}_K|$ is a nontrivial annihilator of the class group cl_K.

The classical source of annihilators of the class group of an abelian field is the Stickelberger ideal. But it gives no interesting annihilator if the field is real.

A method producing annihilators of the class group of a real abelian field via circular units has been discovered by Thaine.

Annihilators of cl_K via circular units

Theorem (Thaine). *Let K be a real abelian field, $G_K = \mathrm{Gal}(K/\mathbb{Q})$, let p be a prime, $p \nmid [K : \mathbb{Q}]$. Then*

$$2 \cdot \mathrm{Ann}_{\mathbb{Z}[G_K]}\big((E(K)/C_{\mathrm{S}}(K))_p\big) \subseteq \mathrm{Ann}_{\mathbb{Z}[G_K]}\big(\mathrm{cl}_{K,p}\big).$$

Thaine's method was generalized by Rubin. To simplify, we formulate it here only for a real abelian field K and an odd prime p which does not ramify in $K/\mathbb{Q}$.

Rubin introduces the notion of *a special number* $\varepsilon \in K^\times$ (each Sinnott's circular unit is special) and proves: if we have

- a positive $n \in \mathbb{Z}$ such that $p^n \nmid h_K$,
- a finitely generated $\mathbb{Z}[G_K]$-submodule $V \subset K^\times/(K^\times)^{p^n}$,
- a $\mathbb{Z}[G_K]$-module homomorphism $\rho\colon V \to (\mathbb{Z}/p^n\mathbb{Z})[G_K]$ such that each $\alpha \in V$ containing a rational number belongs to $\ker\rho$,
- a special number $\varepsilon \in K^\times$ whose class $\bar\varepsilon = \varepsilon(K^\times)^{p^n} \in V$,

then $\rho(\bar\varepsilon) \in \mathrm{Ann}_{\mathbb{Z}[G_K]}\big(\mathrm{cl}_{K,p}\big)$.

Which numbers are special?

Rubin introduced special numbers for abelian extensions of any number field. To simplify, let us take the base field $\mathbb{Q}$.

Let K be an abelian field.

Let $\mathcal{S}$ be the set of all primes q which splits completely in $K/\mathbb{Q}$.

For a prime $q \in \mathcal{S}$, let $K(q) = K\mathbb{Q}_q^+$, the compositum of K and of the maximal real subfield of the q-th cyclotomic field.

Let $\tilde{q}$ be the product of prime ideals of $K(q)$ dividing q.

A number $\varepsilon \in K^\times$ is called special if for all but finitely many $q \in \mathcal{S}$ there is a unit $\varepsilon_q \in \mathcal{O}_{K(q)}^\times$ having the same image in $\mathcal{O}_{K(q)}/\tilde{q}$ as ε^2 and satisfying $\mathrm{N}_{K(q)/K}(\varepsilon_q) = 1$.

We have mentioned that in a real abelian field each Sinnott's circular unit is special. But it is still an open problem whether in this situation each special number, which is a unit, belongs to $C_{\mathrm{S}}(K)$.