Dirichlet Series Associated with Cubic and Quartic Fields

Henri Cohen, Frank Thorne

Institut de Mathématiques de Bordeaux

October 23, 2012, Bordeaux

Introduction I

Number fields will always be considered up to isomorphism.
Dirichlet series associated to number fields of given degree n :

$$\Phi_n(s) = \sum_{[K:\mathbb{Q}]=n} |\operatorname{disc}(K)|^{-s} .$$

Knowing Φ_n explicitly is equivalent to knowing how many K for each discriminant. One usually imposes additional conditions : for instance $\Phi_n(G; s)$: Galois group of the Galois closure isomorphic to G, or $\Phi_n(k; s)$: quadratic resolvent field of cubic field, or cubic resolvent field of quartic field isomorphic to k.

Introduction II

Theorem (Mäki et al)

If G is an abelian group then $\Phi_n(G;s)$ is an explicitly determinable finite linear combination of (infinite) Euler products.

Examples :

$$\Phi_2(C_2;s) = -1 + \left(1 + \frac{1}{2^{2s}} + \frac{2}{2^{3s}}\right) \prod_{p \neq 2} \left(1 + \frac{1}{p^s}\right) ,$$

$$\Phi_3(C_3;s) = -\frac{1}{2} + \frac{1}{2}\left(1 + \frac{2}{3^{4s}}\right) \prod_{p \equiv 1 \pmod 6} \left(1 + \frac{2}{p^{2s}}\right) .$$

If G is not abelian, conjecturally not possible.

Introduction II

Theorem (Mäki et al)

If G is an abelian group then $\Phi_n(G;s)$ is an explicitly determinable finite linear combination of (infinite) Euler products.

Examples :

$$\Phi_2(C_2;s) = -1 + \left(1 + \frac{1}{2^{2s}} + \frac{2}{2^{3s}}\right) \prod_{p \neq 2} \left(1 + \frac{1}{p^s}\right) ,$$

$$\Phi_3(C_3;s) = -\frac{1}{2} + \frac{1}{2}\left(1 + \frac{2}{3^{4s}}\right) \prod_{p \equiv 1 \pmod 6} \left(1 + \frac{2}{p^{2s}}\right) .$$

If G is not abelian, conjecturally not possible.

Introduction III

Instead of fixing the Galois group, in small degree we can fix the resolvent field :

- If K is a noncyclic cubic field, its Galois closure contains a unique quadratic field $k = \mathbb{Q}(\sqrt{D})$, the quadratic resolvent. We may want to consider $\Phi_3(k; s)$, where k (or D) is fixed.
- If K is a quartic field with A_4 or S_4 Galois group of Galois closure, the latter contains a cubic field k, unique in the A_4 case and unique up to conjugation in the S_4 case, the cubic resolvent. We may want to consider $\Phi_4(k; s)$, where k is fixed.

Theorem

- *(Morra, C.) $\Phi_3(k; s)$ is a finite linear combination of explicit Euler products.*
- *(Diaz y Diaz, Olivier, C.) $\Phi_4(k; s)$ is a finite linear combination of explicit Euler products.*

Introduction III

Instead of fixing the Galois group, in small degree we can fix the resolvent field :

- If K is a noncyclic cubic field, its Galois closure contains a unique quadratic field $k = \mathbb{Q}(\sqrt{D})$, the quadratic resolvent. We may want to consider $\Phi_3(k; s)$, where k (or D) is fixed.
- If K is a quartic field with A_4 or S_4 Galois group of Galois closure, the latter contains a cubic field k, unique in the A_4 case and unique up to conjugation in the S_4 case, the cubic resolvent. We may want to consider $\Phi_4(k; s)$, where k is fixed.

Theorem

- *(Morra, C.)* $\Phi_3(k; s)$ *is a finite linear combination of explicit Euler products.*
- *(Diaz y Diaz, Olivier, C.)* $\Phi_4(k; s)$ *is a finite linear combination of explicit Euler products.*

Introduction IV

Unfortunately, in both theorems “explicit” is not very nice : they both involve sums over characters of certain twisted ray class groups, not easy to determine except in special cases.

In fact, case in point : our knowledge of the size of say 3-part of class groups is very poor : smaller than the whole of course, but even gaining a small exponent is hard (Ellenberg–Venkatesh). For instance, conjecturally the number of cubic fields of given discriminant d should be d^{ε} for any $\varepsilon > 0$, but the best known result due to EV is $d^{1/3+\varepsilon}$.

We do not improve on this, but give instead nice explicit formulas for $\Phi_3(k;s)$ and $\Phi_4(k;s)$. Note that in both cases we have $\mathrm{disc}(K) = \mathrm{disc}(k) f(K)^2$ for some $f(K) \in \mathbb{Z}_{\geq 1}$. Thus for $n = 3, 4$ we set :

$$\Phi_n(k;s) = 1/|\operatorname{Aut}(k)| + \sum_K f(K)^{-s},$$

$|\operatorname{Aut}(k)|$ number of Galois automorphism of k.

Introduction IV

Unfortunately, in both theorems “explicit” is not very nice : they both involve sums over characters of certain twisted ray class groups, not easy to determine except in special cases.

In fact, case in point : our knowledge of the size of say 3-part of class groups is very poor : smaller than the whole of course, but even gaining a small exponent is hard (Ellenberg–Venkatesh). For instance, conjecturally the number of cubic fields of given discriminant d should be d^{ε} for any $\varepsilon > 0$, but the best known result due to EV is $d^{1/3+\varepsilon}$.

We do not improve on this, but give instead nice explicit formulas for $\Phi_3(k;s)$ and $\Phi_4(k;s)$. Note that in both cases we have $\mathrm{disc}(K) = \mathrm{disc}(k) f(K)^2$ for some $f(K) \in \mathbb{Z}_{\geq 1}$. Thus for $n = 3, 4$ we set :

$$\Phi_n(k;s) = 1/|\operatorname{Aut}(k)| + \sum_K f(K)^{-s},$$

$|\operatorname{Aut}(k)|$ number of Galois automorphism of k.

Introduction IV

Unfortunately, in both theorems "explicit" is not very nice : they both involve sums over characters of certain twisted ray class groups, not easy to determine except in special cases.

In fact, case in point : our knowledge of the size of say 3-part of class groups is very poor : smaller than the whole of course, but even gaining a small exponent is hard (Ellenberg–Venkatesh). For instance, conjecturally the number of cubic fields of given discriminant d should be d^{ε} for any $\varepsilon > 0$, but the best known result due to EV is $d^{1/3+\varepsilon}$.

We do not improve on this, but give instead nice explicit formulas for $\Phi_3(k; s)$ and $\Phi_4(k; s)$. Note that in both cases we have $\mathrm{disc}(K) = \mathrm{disc}(k) f(K)^2$ for some $f(K) \in \mathbb{Z}_{\geq 1}$. Thus for $n = 3, 4$ we set :

$$\Phi_n(k; s) = 1/|\operatorname{Aut}(k)| + \sum_K f(K)^{-s} ,$$

$|\operatorname{Aut}(k)|$ number of Galois automorphism of k.

The Cubic Case I

Note : D always a fundamental discriminant (including 1, special case of cyclic cubic fields).
To give the result in the cubic case, need to define :

- D^* discriminant of mirror field of $k = \mathbb{Q}(\sqrt{D})$, i.e., $D^* = -3D$ if $3 \nmid D$, $D^* = -D/3$ if $3 \mid D$.
- $\mathcal{L}_N$: cubic fields of discriminant N (only used for $N = D^*$ and $N = -27D$).
- $\mathcal{L}(D) = \mathcal{L}_{D^*} \cup \mathcal{L}_{-27D}$.
- If E is a cubic field and p a prime number,

$$\omega_E(p) = \begin{cases} -1 & \text{if } p \text{ is inert in } E\ , \\ 2 & \text{if } p \text{ is totally split in } E\ , \\ 0 & \text{otherwise.} \end{cases}$$

The Cubic Case I

Note : D always a fundamental discriminant (including 1, special case of cyclic cubic fields).
To give the result in the cubic case, need to define :

- D^* discriminant of mirror field of $k = \mathbb{Q}(\sqrt{D})$, i.e., $D^* = -3D$ if $3 \nmid D$, $D^* = -D/3$ if $3 \mid D$.
- $\mathcal{L}_N$: cubic fields of discriminant N (only used for $N = D^*$ and $N = -27D$).
- $\mathcal{L}(D) = \mathcal{L}_{D^*} \cup \mathcal{L}_{-27D}$.
- If E is a cubic field and p a prime number,

$$\omega_E(p) = \begin{cases} -1 & \text{if } p \text{ is inert in } E\ , \\ 2 & \text{if } p \text{ is totally split in } E\ , \\ 0 & \text{otherwise.} \end{cases}$$

The Cubic Case II

Theorem (Thorne, C.)

We have

$$c_D \Phi_3(D;s) = \frac{1}{2} M_1(s) \prod_{\left(\frac{-3D}{p}\right)=1} \left(1+\frac{2}{p^s}\right) + \sum_{E \in \mathcal{L}(D)} M_{2,E}(s) \prod_{\left(\frac{-3D}{p}\right)=1} \left(1+\frac{\omega_E(p)}{p^s}\right)$$

where $c_D = 1$ *if* $D = 1$ *or* $D < -3$, $c_D = 3$ *if* $D = -3$ *or* $D > 1$, *and the* 3*-Euler factors* $M_1(s)$ *and* $M_{2,E}(s)$ *are given in the following table.*

Condition on D	$M_1(s)$	$M_{2,E}(s),\ E \in \mathcal{L}_{D^*}$	$M_{2,E}(s),\ E \in \mathcal{L}_{-27D}$
$3 \nmid D$	$1+2/3^{2s}$	$1+2/3^{2s}$	$1-1/3^{2s}$
$D \equiv 3 \pmod 9$	$1+2/3^{s}$	$1+2/3^{s}$	$1-1/3^{s}$
$D \equiv 6 \pmod 9$	$1+2/3^{s}+6/3^{2s}$	$1+2/3^{s}+3\omega_E(3)/3^{2s}$	$1-1/3^{s}$

The Cubic Case III

Examples :

$$\Phi_3(-4;s) = \frac{1}{2}\left(1+\frac{2}{3^{2s}}\right)\prod_{\left(\frac{12}{p}\right)=1}\left(1+\frac{2}{p^s}\right) .$$

Here $\mathcal{L}(D) = \emptyset$.

$$\Phi_3(-255;s) = \frac{1}{2}\left(1+\frac{2}{3^s}+\frac{6}{3^{2s}}\right)\prod_{\left(\frac{6885}{p}\right)=1}\left(1+\frac{2}{p^s}\right)$$
$$+\left(1-\frac{1}{3^s}\right)\prod_{p}\left(1+\frac{\omega_E(p)}{p^s}\right) ,$$

where E is the cubic field determined by $x^3 - 12x - 1 = 0$.

In words, the splitting of primes in the single cubic field E determines all cubic fields with quadratic resolvent $\mathbb{Q}(\sqrt{-255})$ ("One field to rule them all").

The Cubic Case III

Examples :

$$\Phi_3(-4;s) = \frac{1}{2}\left(1+\frac{2}{3^{2s}}\right)\prod_{\left(\frac{12}{p}\right)=1}\left(1+\frac{2}{p^s}\right) .$$

Here $\mathcal{L}(D) = \emptyset$.

$$\Phi_3(-255;s) = \frac{1}{2}\left(1+\frac{2}{3^s}+\frac{6}{3^{2s}}\right)\prod_{\left(\frac{6885}{p}\right)=1}\left(1+\frac{2}{p^s}\right) + \left(1-\frac{1}{3^s}\right)\prod_{p}\left(1+\frac{\omega_E(p)}{p^s}\right) ,$$

where E is the cubic field determined by $x^3 - 12x - 1 = 0$.

In words, the splitting of primes in the single cubic field E determines all cubic fields with quadratic resolvent $\mathbb{Q}(\sqrt{-255})$ ("One field to rule them all").

The Cubic Case III

Examples :

$$\Phi_3(-4;s) = \frac{1}{2}\left(1+\frac{2}{3^{2s}}\right)\prod_{\left(\frac{12}{p}\right)=1}\left(1+\frac{2}{p^s}\right) .$$

Here $\mathcal{L}(D) = \emptyset$.

$$\Phi_3(-255;s) = \frac{1}{2}\left(1+\frac{2}{3^s}+\frac{6}{3^{2s}}\right)\prod_{\left(\frac{6885}{p}\right)=1}\left(1+\frac{2}{p^s}\right)$$
$$+\left(1-\frac{1}{3^s}\right)\prod_{p}\left(1+\frac{\omega_E(p)}{p^s}\right) ,$$

where E is the cubic field determined by $x^3 - 12x - 1 = 0$.

In words, the splitting of primes in the single cubic field E determines all cubic fields with quadratic resolvent $\mathbb{Q}(\sqrt{-255})$ ("One field to rule them all").

The Cubic Case : Comments I

To estimate the number of cubic fields of given discriminant Dn^2, it is in particular necessary to estimate the number of auxiliary fields E which occur, i.e., the cardinality of $\mathcal{L}(D)$. This is given as follows :

Theorem (Nakagawa, Ono, Thorne)

Denote by $\mathrm{rk}_3(D)$ *the* 3*-rank of the class group of* $k = \mathbb{Q}(\sqrt{D})$*. We have*

$$|\mathcal{L}(D)| = \begin{cases} (3^{\mathrm{rk}_3(D)} - 1)/2 & \text{if } D < 0\ , \\ (3^{\mathrm{rk}_3(D)+1} - 1)/2 & \text{if } D > 0\ . \end{cases}$$

As mentioned, the problem is that we have only very weak upper bounds for $3^{\mathrm{rk}_3(D)}$ (in $O(|D|^{1/3+\varepsilon})$), although should be $O(|D|^{\varepsilon})$.

The Cubic Case : Comments II

Computing the number $N_3(k; X)$ of cubic fields having a given quadratic resolvent $k = \mathbb{Q}(\sqrt{D})$ and absolute discriminant up to X can be done very fast using the theorem and standard techniques of analytic number theory ($X = 10^{25}$ is feasible). We can also sum on D and compute the total number $N_3(X)$ of cubic fields, although this is less efficient than the method of K. Belabas.

It is tempting to try to prove the known result that $N_3(X) \sim c \cdot X$ for a known constant c (essentially $c = 1/\zeta(3)$). It is probably possible to do this, or at least to obtain $N_3(X) = O(X^{1+\varepsilon})$, but since this has been proved (rather easily in fact) by other methods, it seems to be unnecessary work.

The Cubic Case : Comments II

Computing the number $N_3(k; X)$ of cubic fields having a given quadratic resolvent $k = \mathbb{Q}(\sqrt{D})$ and absolute discriminant up to X can be done very fast using the theorem and standard techniques of analytic number theory ($X = 10^{25}$ is feasible). We can also sum on D and compute the total number $N_3(X)$ of cubic fields, although this is less efficient than the method of K. Belabas.

It is tempting to try to prove the known result that $N_3(X) \sim c \cdot X$ for a known constant c (essentially $c = 1/\zeta(3)$). It is probably possible to do this, or at least to obtain $N_3(X) = O(X^{1+\varepsilon})$, but since this has been proved (rather easily in fact) by other methods, it seems to be unnecessary work.

The Cubic Case : Indication of Proof I

This is essentially in Anna Morra's thesis. We may assume $D \neq 1, -3$, easier and known.
K cubic field with resolvent $k = \mathbb{Q}(\sqrt{D})$, i.e., discriminant Dn^2. Let N be the Galois closure of K. $L = \mathbb{Q}(\sqrt{D}, \sqrt{-3})$, τ_1, τ_2 generators of $\mathrm{Gal}(L/\mathbb{Q}) \simeq C_2 \times C_2$.

Kummer theory : $N(\sqrt{-3}) = L(\sqrt[3]{\alpha})$ for some $\alpha \in L^*$, unique modulo cubes up to changing α into its inverse, such that $\alpha\tau_i(\alpha)$ is a cube for $i = 1, 2$; we write $\alpha \in (L^*/L^{*3})[T]$ with $T = \{\tau_1 + 1, \tau_2 + 1\}$.

Writing $\alpha\mathbb{Z}_L = \mathfrak{a}_0\mathfrak{a}_1^2\mathfrak{q}^3$, immediate consequence : bijection between cubic fields K with given k and triples $(\mathfrak{a}_0, \mathfrak{a}_1, \overline{u})$, where $\mathfrak{a}_0$, $\mathfrak{a}_1$ coprime squarefree ideals, $\overline{\mathfrak{a}_0\mathfrak{a}_1^2} \in Cl(L)^3$, $\mathfrak{a}_0\mathfrak{a}_1^2 \in (I/I^3)[T]$, $\overline{u} \in (L^*/L^{*3})[T]$ such that $u\mathbb{Z}_L = \mathfrak{q}^3$, some $\mathfrak{q}$ (we write $\overline{u} \in S_3(L)[T]$, the 3-Selmer group of L).

The Cubic Case : Indication of Proof I

This is essentially in Anna Morra's thesis. We may assume $D \neq 1, -3$, easier and known.
K cubic field with resolvent $k = \mathbb{Q}(\sqrt{D})$, i.e., discriminant Dn^2. Let N be the Galois closure of K. $L = \mathbb{Q}(\sqrt{D}, \sqrt{-3})$, τ_1, τ_2 generators of $\mathrm{Gal}(L/\mathbb{Q}) \simeq C_2 \times C_2$.

Kummer theory : $N(\sqrt{-3}) = L(\sqrt[3]{\alpha})$ for some $\alpha \in L^*$, unique modulo cubes up to changing α into its inverse, such that $\alpha\tau_i(\alpha)$ is a cube for $i = 1, 2$; we write $\alpha \in (L^*/L^{*3})[T]$ with $T = \{\tau_1 + 1, \tau_2 + 1\}$.

Writing $\alpha\mathbb{Z}_L = \mathfrak{a}_0\mathfrak{a}_1^2\mathfrak{q}^3$, immediate consequence : bijection between cubic fields K with given k and triples $(\mathfrak{a}_0, \mathfrak{a}_1, \overline{u})$, where $\mathfrak{a}_0$, $\mathfrak{a}_1$ coprime squarefree ideals, $\overline{\mathfrak{a}_0\mathfrak{a}_1^2} \in Cl(L)^3$, $\mathfrak{a}_0\mathfrak{a}_1^2 \in (I/I^3)[T]$, $\overline{u} \in (L^*/L^{*3})[T]$ such that $u\mathbb{Z}_L = \mathfrak{q}^3$, some $\mathfrak{q}$ (we write $\overline{u} \in S_3(L)[T]$, the 3-Selmer group of L).

The Cubic Case : Indication of Proof I

This is essentially in Anna Morra's thesis. We may assume $D \neq 1, -3$, easier and known.
K cubic field with resolvent $k = \mathbb{Q}(\sqrt{D})$, i.e., discriminant Dn^2. Let N be the Galois closure of K. $L = \mathbb{Q}(\sqrt{D}, \sqrt{-3})$, τ_1, τ_2 generators of $\mathrm{Gal}(L/\mathbb{Q}) \simeq C_2 \times C_2$.

Kummer theory : $N(\sqrt{-3}) = L(\sqrt[3]{\alpha})$ for some $\alpha \in L^*$, unique modulo cubes up to changing α into its inverse, such that $\alpha\tau_i(\alpha)$ is a cube for $i = 1, 2$; we write $\alpha \in (L^*/L^{*3})[T]$ with $T = \{\tau_1 + 1, \tau_2 + 1\}$.

Writing $\alpha\mathbb{Z}_L = \mathfrak{a}_0\mathfrak{a}_1^2\mathfrak{q}^3$, immediate consequence : bijection between cubic fields K with given k and triples $(\mathfrak{a}_0, \mathfrak{a}_1, \overline{u})$, where $\mathfrak{a}_0$, $\mathfrak{a}_1$ coprime squarefree ideals, $\overline{\mathfrak{a}_0\mathfrak{a}_1^2} \in Cl(L)^3$, $\mathfrak{a}_0\mathfrak{a}_1^2 \in (I/I^3)[T]$, $\overline{u} \in (L^*/L^{*3})[T]$ such that $u\mathbb{Z}_L = \mathfrak{q}^3$, some $\mathfrak{q}$ (we write $\overline{u} \in S_3(L)[T]$, the 3-Selmer group of L).

The Cubic Case : Indication of Proof II

Then need to compute $\mathrm{disc}(K)$ in terms of $(\mathfrak{a}_0, \mathfrak{a}_1, \overline{u})$:

Theorem

1. *There exists an ideal* $\mathfrak{a}_\alpha$ *of* $k = \mathbb{Q}(\sqrt{D})$ *such that* $\mathfrak{a}_0\mathfrak{a}_1 = \mathfrak{a}_\alpha\mathbb{Z}_L$.
2. *We have* $\mathrm{disc}(K) = Df(K)^2$, *where* $f(K)$ *is equal to* $\mathfrak{a}_\alpha$ *times a complicated but explicit* 3*-adic factor.*

The 3-adic factor is computed thanks to an important theorem of Hecke which complements Kummer theory, which involves the solubility of the congruence $x^3 \equiv \alpha \pmod{{}^*\mathfrak{p}^k}$ for prime ideals $\mathfrak{p}$ of L above 3. This leads to the introduction of $\mathcal{B} = \{(1), (\sqrt{-3}), (3), (3\sqrt{-3})\}$.

The condition $\overline{\mathfrak{a}_0\mathfrak{a}_1^2} \in Cl(L)^3$ is detected by summing over characters χ of $Cl(L)/Cl(L)^3$, and together with the 3-adic complications, we in fact sum over characters of the 3-group $G_\mathfrak{b} = Cl_\mathfrak{b}(L)/Cl_\mathfrak{b}(L)^3$ with $\mathfrak{b} \in \mathcal{B}$.

The Cubic Case : Indication of Proof II

Then need to compute $\mathrm{disc}(K)$ in terms of $(\mathfrak{a}_0, \mathfrak{a}_1, \overline{u})$:

Theorem

1. *There exists an ideal* $\mathfrak{a}_\alpha$ *of* $k = \mathbb{Q}(\sqrt{D})$ *such that* $\mathfrak{a}_0\mathfrak{a}_1 = \mathfrak{a}_\alpha\mathbb{Z}_L$.
2. *We have* $\mathrm{disc}(K) = Df(K)^2$, *where* $f(K)$ *is equal to* $\mathfrak{a}_\alpha$ *times a complicated but explicit* 3*-adic factor.*

The 3-adic factor is computed thanks to an important theorem of Hecke which complements Kummer theory, which involves the solubility of the congruence $x^3 \equiv \alpha \pmod{{}^*\mathfrak{p}^k}$ for prime ideals $\mathfrak{p}$ of L above 3. This leads to the introduction of $\mathcal{B} = \{(1), (\sqrt{-3}), (3), (3\sqrt{-3})\}$.

The condition $\overline{\mathfrak{a}_0\mathfrak{a}_1^2} \in Cl(L)^3$ is detected by summing over characters χ of $Cl(L)/Cl(L)^3$, and together with the 3-adic complications, we in fact sum over characters of the 3-group $G_\mathfrak{b} = Cl_\mathfrak{b}(L)/Cl_\mathfrak{b}(L)^3$ with $\mathfrak{b} \in \mathcal{B}$.

The Cubic Case : Indication of Proof II

Then need to compute $\mathrm{disc}(K)$ in terms of $(\mathfrak{a}_0, \mathfrak{a}_1, \overline{u})$:

Theorem

1. *There exists an ideal* $\mathfrak{a}_\alpha$ *of* $k = \mathbb{Q}(\sqrt{D})$ *such that* $\mathfrak{a}_0\mathfrak{a}_1 = \mathfrak{a}_\alpha\mathbb{Z}_L$.
2. *We have* $\mathrm{disc}(K) = Df(K)^2$, *where* $f(K)$ *is equal to* $\mathfrak{a}_\alpha$ *times a complicated but explicit* 3*-adic factor.*

The 3-adic factor is computed thanks to an important theorem of Hecke which complements Kummer theory, which involves the solubility of the congruence $x^3 \equiv \alpha \pmod{{}^*\mathfrak{p}^k}$ for prime ideals $\mathfrak{p}$ of L above 3. This leads to the introduction of $\mathcal{B} = \{(1), (\sqrt{-3}), (3), (3\sqrt{-3})\}$.
The condition $\overline{\mathfrak{a}_0\mathfrak{a}_1^2} \in Cl(L)^3$ is detected by summing over characters χ of $Cl(L)/Cl(L)^3$, and together with the 3-adic complications, we in fact sum over characters of the 3-group $G_\mathfrak{b} = Cl_\mathfrak{b}(L)/Cl_\mathfrak{b}(L)^3$ with $\mathfrak{b} \in \mathcal{B}$.

The Cubic Case : Indication of Proof III

Using complicated but straightforward combinatorial arguments and some local and global class field theory, we are led to a formula (in C.-Morra and in Morra's thesis), which in our special case where the base field is $\mathbb{Q}$ simplifies to an expression of the type :

$$\Phi_3(D;s) = \frac{3}{2c_D} \sum_{\mathfrak{b}\in\mathcal{B}} A_{\mathfrak{b}}(s) \sum_{\chi\in\widehat{G_{\mathfrak{b}}}} \omega_\chi(3) F(\mathfrak{b},\chi,s) \ ,$$

with $A_{\mathfrak{b}}(s)$ constant multiples of a single Euler factor at 3, ω_χ depends on the character χ but takes only the values 0, ± 1, and 2, and

$$F(\mathfrak{b},\chi,s) = \prod_{\left(\frac{-3D}{p}\right)=1} \left(1 + \frac{\omega_\chi(p)}{p^s}\right) \ .$$

The Cubic Case : Explicit Formula

This proves the claim that we have an "explicit" finite linear combination of Euler products. Want to make it completely explicit (characters of $G_{\mathfrak{b}}$ not very nice). The basic result is :

Theorem (Thorne)

There exists a bijection between pairs of conjugate nontrivial characters $(\chi, \overline{\chi})$ of $G_{\mathfrak{b}}$ and the following sets of cubic fields :

- *If $\mathfrak{b} = (1)$ or $(\sqrt{-3})$, or $\mathfrak{b} = (3)$ and $3 \mid D$, the bijection is with $\mathcal{L}_{D^*}$.*
- *If $\mathfrak{b} = (3)$ and $3 \nmid D$ or $\mathfrak{b} = (3\sqrt{-3})$, the bijection is with $\mathcal{L} = \mathcal{L}_{D^*} \cup \mathcal{L}_{-27D}$.*

In addition, under this bijection, if E is the field associated to $(\chi, \overline{\chi})$ we have $\omega_\chi(p) = \omega_E(p)$.

This theorem combined with some further computations prove our main theorem in the cubic case.

The Quartic A_4 and S_4-Case : Introduction I

Let K be a quartic field, $\widetilde{K}$ its Galois closure, assume $\mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \simeq A_4$ or S_4. There exists a cubic subfield k of $\widetilde{K}$, unique up to conjugation, the resolvent cubic. In the same way, we want to compute explicitly $\Phi_4(k; s)$ (if $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ not A_4 or S_4, different and simpler). Here Kummer theory much simpler since no roots of unity to adjoin.

But S_4 more complicated group : we will need to distinguish between a great number of possible splittings of the prime 2 (more than 20). We first give the result, and then an indication of the (much more complicated) proof. Very similar to the cubic case : Need to define $\omega_E(p)$, and a set $\mathcal{L}(k)$ of quartic fields, but also $s_k(p)$ for a cubic field k.

The Quartic A_4 and S_4-Case : Introduction I

Let K be a quartic field, $\widetilde{K}$ its Galois closure, assume $\mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \simeq A_4$ or S_4. There exists a cubic subfield k of $\widetilde{K}$, unique up to conjugation, the resolvent cubic. In the same way, we want to compute explicitly $\Phi_4(k; s)$ (if $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ not A_4 or S_4, different and simpler). Here Kummer theory much simpler since no roots of unity to adjoin.

But S_4 more complicated group : we will need to distinguish between a great number of possible splittings of the prime 2 (more than 20). We first give the result, and then an indication of the (much more complicated) proof. Very similar to the cubic case : Need to define $\omega_E(p)$, and a set $\mathcal{L}(k)$ of quartic fields, but also $s_k(p)$ for a cubic field k.

The Quartic A_4 and S_4-Case : Notation

Let p be a prime number.

- If k is a cubic field, we set

$$s_k(p) = \begin{cases} 1 & \text{if } p \text{ is } (21) \text{ or } (1^2 1) \text{ in } k\ , \\ 3 & \text{if } p \text{ is } (111) \text{ in } k\ , \\ 0 & \text{otherwise.} \end{cases}$$

- If E is a quartic field, we set

$$\omega_E(p) = \begin{cases} -1 & \text{if } p \text{ is } (4),\ (22),\ (21^2) \text{ in } E \\ 1 & \text{if } p \text{ is } (211),\ (1^2 11) \text{ in } E \\ 3 & \text{if } p \text{ is } (1111) \text{ in } E \\ 0 & \text{otherwise.} \end{cases}$$

(Splitting notation self-explanatory.)

The Quartic A_4 and S_4-Case : The Theorem I

Let k be a cubic field.

- $\mathcal{L}_{k,n^2}$: quartic fields with cubic resolvent k and discriminant $n^2\,\mathrm{disc}(k)$, in addition totally real if k is totally real.
- $\mathcal{L}(k) = \mathcal{L}_{k,1} \cup \mathcal{L}_{k,4} \cup \mathcal{L}_{k,16} \cup \mathcal{L}_{k,64,tr}$, where the index tr means that 2 must be totally ramified.

Theorem (Thorne, C.)

Let k be a cubic field, $r_2(k)$ number of complex places, $a(k) = |\mathrm{Aut}(k)|$ (3 for k cyclic, 1 otherwise). We have

$$2^{r_2(k)}\Phi_4(k;s) = \frac{1}{a(k)} M_1(s) \prod_{p\neq 2}\left(1+\frac{s_k(p)}{p^s}\right) + \sum_{E\in\mathcal{L}(k)} M_{2,E}(s) \prod_{p\neq 2}\left(1+\frac{\omega_E(p)}{p^s}\right),$$

The Quartic A_4 and S_4-Case : The Theorem I

Let k be a cubic field.

- $\mathcal{L}_{k,n^2}$: quartic fields with cubic resolvent k and discriminant $n^2\,\mathrm{disc}(k)$, in addition totally real if k is totally real.
- $\mathcal{L}(k) = \mathcal{L}_{k,1} \cup \mathcal{L}_{k,4} \cup \mathcal{L}_{k,16} \cup \mathcal{L}_{k,64,tr}$, where the index tr means that 2 must be totally ramified.

Theorem (Thorne, C.)

Let k be a cubic field, $r_2(k)$ number of complex places, $a(k) = |\mathrm{Aut}(k)|$ (3 for k cyclic, 1 otherwise). We have

$$2^{r_2(k)}\Phi_4(k;s) = \frac{1}{a(k)} M_1(s) \prod_{p\neq 2}\left(1+\frac{s_k(p)}{p^s}\right) + \sum_{E\in\mathcal{L}(k)} M_{2,E}(s) \prod_{p\neq 2}\left(1+\frac{\omega_E(p)}{p^s}\right),$$

The Quartic A_4 and S_4-Case : The Theorem II

where $M_1(s)$ and $M_{2,E}(s)$ are Euler factors at 2 which are polynomials of degree less than or equal to 4 in $1/2^s$: 6 splitting types for $M_1(s)$, and 23 types for $M_{2,E}(s)$:

k-split	$M_1(s)$	$8M_1(1)$
(3)	$1+3/2^{3s}$	11
(21)	$1+1/2^{2s}+4/2^{3s}+2/2^{4s}$	15
(111)	$1+3/2^{2s}+6/2^{3s}+6/2^{4s}$	23
$(1^21)_0$	$1+1/2^{s}+2/2^{3s}+4/2^{4s}$	16
$(1^21)_4$	$1+1/2^{s}+2/2^{2s}+4/2^{4s}$	18
(1^3)	$1+1/2^{s}+2/2^{3s}$	14

(Index 0 or 4 indicates discriminant modulo 8).

The Quartic A_4 and S_4-Case : The Theorem III

k-split	E-split	n^2	$M_{2,E}(s),\ E \in \mathcal{L}_{k,n^2}$	k-split	E-split	n^2	$M_{2,E}(s),\ E \in \mathcal{L}_{k,n^2}$
(3)	(31)	1	$1+3/2^{3s}$	$(1^21)_0$	(21^2)	1	$1+1/2^s+2/2^{3s}-4/2^{4s}$
(3)	(1^4)	64	$1-1/2^{3s}$	$(1^21)_0$	(1^211)	1	$1+1/2^s+2/2^{3s}+4/2^{4s}$
(21)	(4)	1	$1+1/2^{2s}-2/2^{4s}$	$(1^21)_0$	(1^21^2)	4	$1+1/2^s-2/2^{3s}$
(21)	(211)	1	$1+1/2^{2s}+4/2^{3s}+2/2^{4s}$	$(1^21)_0$	(1^4)	64	$1-1/2^s$
(21)	(2^2)	16	$1+1/2^{2s}-4/2^{3s}+2/2^{4s}$	$(1^21)_4$	(21^2)	1	$1+1/2^s+2/2^{2s}-4/2^{4s}$
(21)	(1^21^2)	16	$1+1/2^{2s}-2/2^{4s}$	$(1^21)_4$	(1^211)	1	$1+1/2^s+2/2^{2s}+4/2^{4s}$
(21)	(1^4)	64	$1-1/2^{2s}$	$(1^21)_4$	(2^2)	4	$1+1/2^s-2/2^{2s}$
(111)	(22)	1	$1+3/2^{2s}-2/2^{3s}-2/2^{4s}$	$(1^21)_4$	(2^2)	16	$1-1/2^s$
(111)	(2^2)	16	$1-1/2^{2s}-2/2^{3s}+2/2^{4s}$	$(1^21)_4$	(1^21^2)	16	$1-1/2^s$
(111)	(1111)	1	$1+3/2^{2s}+6/2^{3s}+6/2^{4s}$	(1^3)	(1^31)	1	$1+1/2^s+2/2^{3s}$
(111)	(1^21^2)	16	$1-1/2^{2s}+2/2^{3s}-2/2^{4s}$	(1^3)	(1^4)	4	$1+1/2^s-2/2^{3s}$
				(1^3)	(1^4)	64	$1-1/2^s$

The Quartic A_4 Case : Example

We give three examples : one in the much simpler A_4 case, two in the S_4 case.
Let k be the cyclic cubic field of discriminant 49 defined by $x^3 - x^2 - 2x + 1 = 0$. We have

$$\Phi_4(k;s) = \frac{1}{3}\left(1 + \frac{3}{2^{3s}}\right) \prod_{p \equiv \pm 1 \pmod{14}} \left(1 + \frac{3}{p^s}\right)$$

Note that since we are in an abelian situation, the splitting of p is equivalent to congruences.
Thus

$$\Phi_4(k;s) = \frac{1}{3} + \frac{1}{8^s} + \frac{1}{13^s} + \frac{1}{29^s} + \frac{1}{41^s} + \frac{1}{43^s} + \frac{1}{71^s} + \frac{1}{83^s} + \frac{1}{97^s} + \frac{3}{104^s} + \cdots,$$

where a/f^s means that there are a quartic A_4-fields of discriminant $49 \cdot f^2$.

The Quartic A_4 Case : Example

We give three examples : one in the much simpler A_4 case, two in the S_4 case.
Let k be the cyclic cubic field of discriminant 49 defined by $x^3 - x^2 - 2x + 1 = 0$. We have

$$\Phi_4(k;s) = \frac{1}{3}\left(1 + \frac{3}{2^{3s}}\right) \prod_{p \equiv \pm 1 \pmod{14}} \left(1 + \frac{3}{p^s}\right)$$

Note that since we are in an abelian situation, the splitting of p is equivalent to congruences.
Thus

$$\Phi_4(k;s) = \frac{1}{3} + \frac{1}{8^s} + \frac{1}{13^s} + \frac{1}{29^s} + \frac{1}{41^s} + \frac{1}{43^s} + \frac{1}{71^s} + \frac{1}{83^s} + \frac{1}{97^s} + \frac{3}{104^s} + \cdots,$$

where a/f^s means that there are a quartic A_4-fields of discriminant $49 \cdot f^2$.

The Quartic S_4 Case : Examples

- Let k be the noncyclic totally real cubic of discriminant 148 defined by $x^3 - x^2 - 3x + 1 = 0$. Then

$$\Phi_4(k;s) = \left(1 + \frac{1}{2^s} + \frac{2}{2^{3s}}\right) \prod_{p \neq 2} \left(1 + \frac{s_k(p)}{p^s}\right) .$$

- Let k be the noncyclic totally real cubic of discriminant 229 defined by $x^3 - 4x - 1 = 0$. Then

$$\Phi_4(k;s) = \left(1 + \frac{1}{2^{2s}} + \frac{4}{2^{3s}} + \frac{2}{2^{4s}}\right) \prod_{p \neq 2} \left(1 + \frac{s_k(p)}{p^s}\right) + \left(1 - \frac{1}{2^{2s}}\right) \prod_{p} \left(1 + \frac{\omega_E(p)}{p^s}\right) ,$$

where E is the S_4-quartic field of discriminant $64 \cdot 229$ defined by $x^4 - 2x^3 - 4x^2 + 4x + 2 = 0$.

The Quartic A_4 and S_4 Cases : Comments

Comments essentially identical to the cubic case : the number of necessary auxiliary quartic fields $|\mathcal{L}(k)|$ is equal to

$$2^{\mathrm{rk}_2(Cl_4(k))} - 1 \ ,$$

where rk_2 is the 2-rank and $Cl_4(k)$ the ray class group of conductor 4. We do not know how to control this well.

In fact, it is widely conjectured that $N_4(A_4; X) \sim c \cdot X^{1/2} \log X$, but the above does not allow to obtain any nontrivial result (best known, using in fact elementary methods, is $O(X^{3/4+\varepsilon})$).

On the other hand computing the number $N_4(k; X)$ of quartic fields having a given cubic resolvent k and absolute discriminant up to X can again be done very fast using the theorem and standard techniques of analytic number theory.

The Quartic A_4 and S_4 Cases : Comments

Comments essentially identical to the cubic case : the number of necessary auxiliary quartic fields $|\mathcal{L}(k)|$ is equal to

$$2^{\mathrm{rk}_2(Cl_4(k))} - 1 \ ,$$

where rk_2 is the 2-rank and $Cl_4(k)$ the ray class group of conductor 4.
We do not know how to control this well.
In fact, it is widely conjectured that $N_4(A_4; X) \sim c \cdot X^{1/2} \log X$, but the above does not allow to obtain any nontrivial result (best known, using in fact elementary methods, is $O(X^{3/4+\varepsilon})$).
On the other hand computing the number $N_4(k; X)$ of quartic fields having a given cubic resolvent k and absolute discriminant up to X can again be done very fast using the theorem and standard techniques of analytic number theory.

The Quartic A_4 and S_4 Cases : Comments

Comments essentially identical to the cubic case : the number of necessary auxiliary quartic fields $|\mathcal{L}(k)|$ is equal to

$$2^{\mathrm{rk}_2(Cl_4(k))} - 1 \ ,$$

where rk_2 is the 2-rank and $Cl_4(k)$ the ray class group of conductor 4.
We do not know how to control this well.
In fact, it is widely conjectured that $N_4(A_4; X) \sim c \cdot X^{1/2} \log X$, but the above does not allow to obtain any nontrivial result (best known, using in fact elementary methods, is $O(X^{3/4+\varepsilon})$).
On the other hand computing the number $N_4(k; X)$ of quartic fields having a given cubic resolvent k and absolute discriminant up to X can again be done very fast using the theorem and standard techniques of analytic number theory.

The Quartic A_4 and S_4 Case : Indication of Proof I

The techniques are similar to the cubic case (without the complication of adjoining cube roots of unity), but we need to work much more for essentially two reasons.

- First, we must make a precise list of all possible splittings in an S_4-quartic extension : apparently not in the literature. Done partly in the 1970's by J. Martinet and A. Jehanne, but incomplete (they could have completed it but did not really need it).
- Second, we need to compute precisely some subtle arithmetic quantities, and this is done using techniques of global, but mainly local class field theory. This was done around 2000 by F. Diaz y Diaz, M. Olivier, and C.
- We must then study in detail the set of quartic fields $\mathcal{L}(k)$ (this was not necessary in the cubic case), and relate some twisted ray class groups to more common objects.

The Quartic A_4 and S_4 Case : Indication of Proof II

The main theorem of [CDO] is as follows :

Theorem (Diaz y Diaz, Olivier, C.)

Let k be a cubic field. We have

$$\Phi_4(k;s)=\frac{2^{2-r_2(k)}}{a(k)2^{3s}}\sum_{\mathfrak{c}|2\mathbb{Z}_k}z_k(\mathfrak{c})(\mathcal{N}\mathfrak{c})^{s-1}\prod_{\mathfrak{p}|\mathfrak{c}}\left(1-\frac{1}{\mathcal{N}\mathfrak{p}^s}\right)\sum_{\chi\in\widehat{G_{\mathfrak{c}^2}}}F_k(\chi,s)\ ,$$

$$F_k(\chi,s)=\prod_p\left(1+\frac{s_\chi(p)}{p^s}\right)\ ,\quad s_\chi(p)=\sum_{\substack{\mathfrak{a}|p\mathbb{Z}_k\ \text{squarefree}\\ \mathcal{N}\mathfrak{a}\ \text{square}}}\chi(\mathfrak{a})\ ,$$

$z_k(\mathfrak{c})=1$ or 2 depending on $\mathfrak{c}$ and the splitting of 2 in k, and $G_{\mathfrak{c}^2}$ is essentially (but not exactly) $Cl_{\mathfrak{c}^2}(k)/Cl_{\mathfrak{c}^2}(k)^2$ (recall that $a(k)=|\operatorname{Aut}(k)|$).

The Quartic A_4 and S_4 Case : Indication of Proof III

For exposition, we treat S_4. Classical result (Hasse ?) :

Theorem

There is a bijection between S_4-quartic fields K with cubic resolvent k and quadratic extensions K_6/k of trivial norm, i.e., $K_6 = k(\sqrt{\alpha})$ with $\mathcal{N}_{k/\mathbb{Q}}(\alpha)$ a square, so in particular $\mathcal{N}(\mathfrak{d}(K_6/k))$ is a square.

In fact K_6 is the unique extension of k in $\widetilde{K}$ such that $\mathrm{Gal}(\widetilde{K}/K_6) \simeq C_4$.

In addition $\zeta_K(s) = \zeta(s)\zeta_{K_6}(s)/\zeta_k(s)$ and
$\mathrm{disc}(K) = \mathrm{disc}(k)\,\mathcal{N}(\mathfrak{d}(K_6/k))$.

Finally, if $K_6 = k(\sqrt{\alpha})$ of trivial norm and $x^3 + a_2x^2 + a_1x + a_0$ is the characteristic polynomial of α, a defining polynomial for K is
$x^4 + 2a_2x^2 - 8\sqrt{-a_0}x + a_2^2 - 4a_1$.

The Quartic A_4 and S_4 Case : Indication of Proof IV

Proposition

There is a one-to-one correspondence between on the one hand quadratic extensions of k of trivial norm, together with the trivial extension k/k, and on the other hand pairs $(\mathfrak{a}, \overline{u})$, where $\mathfrak{a}$ is an integral, squarefree ideal of k of square norm whose class modulo principal ideals is a square in the class group of k, and $\overline{u} \in S[N]$, where

$$S(N) = \{\overline{u},\ u\mathbb{Z}_k = \mathfrak{q}^2,\ \mathcal{N}(u)\ \textit{square}\}\ .$$

Using the same theorem of Hecke as in the cubic case, introducing suitable twisted ray class groups and ray Selmer groups, and doing some combinatorial work, we obtain essentially the CDO theorem, where $z_k(\mathfrak{c})$ is given as the index of a twisted ray class group in another.

The Quartic A_4 and S_4 Case : Indication of Proof IV

Proposition

There is a one-to-one correspondence between on the one hand quadratic extensions of k of trivial norm, together with the trivial extension k/k, and on the other hand pairs $(\mathfrak{a}, \overline{u})$, where $\mathfrak{a}$ is an integral, squarefree ideal of k of square norm whose class modulo principal ideals is a square in the class group of k, and $\overline{u} \in S[N]$, where

$$S(N) = \{\overline{u},\ u\mathbb{Z}_k = \mathfrak{q}^2,\ \mathcal{N}(u)\ \textit{square}\}\ .$$

Using the same theorem of Hecke as in the cubic case, introducing suitable twisted ray class groups and ray Selmer groups, and doing some combinatorial work, we obtain essentially the CDO theorem, where $z_k(\mathfrak{c})$ is given as the index of a twisted ray class group in another.

The Quartic A_4 and S_4 Case : Indication of Proof V

Using a number of exact sequences, we can then show that $z_k(\mathfrak{c})$ is the index of $(\mathbb{Z}_k/\mathfrak{c}^2)^*[N]$ in $(\mathbb{Z}_k/\mathfrak{c}^2)^*$, where $[N]$ means the subgroup of elements having a lift of square norm.

This is "elementary" : no more class groups, unit groups, or Selmer groups. However difficult to compute ; we have done it only when k is a cubic field. It uses local class field theory and some rather surprising algebraic arguments.

Challenge : prove without using CFT the following

Proposition

Let k be a cubic field and $\mathfrak{p}$ an unramified prime ideal dividing 2. Then if $\mathfrak{c} = 2\mathbb{Z}_k/\mathfrak{p}$ we have $z_k(\mathfrak{c}) = 1$, in other words any element of $(\mathbb{Z}_k/\mathfrak{c}^2)^*$ has a lift of square norm.

We would be interested to know such a proof. Putting everything together proves the CDO theorem.

The Quartic A_4 and S_4 Case : Indication of Proof V

Using a number of exact sequences, we can then show that $z_k(\mathfrak{c})$ is the index of $(\mathbb{Z}_k/\mathfrak{c}^2)^*[N]$ in $(\mathbb{Z}_k/\mathfrak{c}^2)^*$, where $[N]$ means the subgroup of elements having a lift of square norm.

This is "elementary" : no more class groups, unit groups, or Selmer groups. However difficult to compute ; we have done it only when k is a cubic field. It uses local class field theory and some rather surprising algebraic arguments.

Challenge : prove without using CFT the following

Proposition

Let k be a cubic field and $\mathfrak{p}$ an unramified prime ideal dividing 2. Then if $\mathfrak{c} = 2\mathbb{Z}_k/\mathfrak{p}$ we have $z_k(\mathfrak{c}) = 1$, in other words any element of $(\mathbb{Z}_k/\mathfrak{c}^2)^*$ has a lift of square norm.

We would be interested to know such a proof. Putting everything together proves the CDO theorem.

The Quartic A_4 and S_4 Case : Indication of Proof V

Using a number of exact sequences, we can then show that $z_k(\mathfrak{c})$ is the index of $(\mathbb{Z}_k/\mathfrak{c}^2)^*[N]$ in $(\mathbb{Z}_k/\mathfrak{c}^2)^*$, where $[N]$ means the subgroup of elements having a lift of square norm.
This is "elementary" : no more class groups, unit groups, or Selmer groups. However difficult to compute ; we have done it only when k is a cubic field. It uses local class field theory and some rather surprising algebraic arguments.
Challenge : prove without using CFT the following

Proposition

Let k be a cubic field and $\mathfrak{p}$ an unramified prime ideal dividing 2. Then if $\mathfrak{c} = 2\mathbb{Z}_k/\mathfrak{p}$ we have $z_k(\mathfrak{c}) = 1$, in other words any element of $(\mathbb{Z}_k/\mathfrak{c}^2)^*$ has a lift of square norm.

We would be interested to know such a proof. Putting everything together proves the CDO theorem.

The Quartic A_4 and S_4 Case : Indication of Proof VI

We are now in the same situation as in the cubic case after A. Morra's thesis : the Dirichlet series $\Phi_4(k;s)$ is an explicit finite linear combination of Euler products. However these involve characters over rather complicated class groups, so not sufficiently explicit to allow algorithmic computation. We will do the same as for the cubic case, make it completely explicit and algorithmic.

We essentially need to do four things :

- Compute and/or interpret the twisted class groups G_{c^2} in terms of more standard types of class groups.
- Determine all possible splitting types of primes in the fields (k, K_6, K).
- Study the fields in $\mathcal{L}(k)$.
- Interpret the sums over characters of G_{c^2} as sums over quartic fields $E \in \mathcal{L}(k)$.

The Quartic A_4 and S_4 Case : Indication of Proof VI

We are now in the same situation as in the cubic case after A. Morra's thesis : the Dirichlet series $\Phi_4(k;s)$ is an explicit finite linear combination of Euler products. However these involve characters over rather complicated class groups, so not sufficiently explicit to allow algorithmic computation. We will do the same as for the cubic case, make it completely explicit and algorithmic.
We essentially need to do four things :

- Compute and/or interpret the twisted class groups $G_{\mathfrak{c}^2}$ in terms of more standard types of class groups.
- Determine all possible splitting types of primes in the fields (k, K_6, K).
- Study the fields in $\mathcal{L}(k)$.
- Interpret the sums over characters of $G_{\mathfrak{c}^2}$ as sums over quartic fields $E \in \mathcal{L}(k)$.

The Quartic A_4 and S_4 Case : Indication of Proof VII

• Twisted class groups $G_{\mathfrak{c}^2}$: needs to be studied in detail (1 page), uses global CFT but not difficult. This study has a surprising corollary :

Proposition

Let k be a cubic field. There exists $u \in k^*$ coprime to 2 such that $u\mathbb{Z}_k = \mathfrak{q}^2$, $\mathcal{N}(u)$ is a square, and $u \not\equiv 1 \pmod{4\mathbb{Z}_k}$.

I do not know how to prove this without CFT.

• Splitting of primes in (k, K_6, K). As mentioned, this was partly done by Martinet and Jehanne, but need to do it completely. Two steps : first prove that certain splittings are impossible, second for the remaining ones find examples. For fun, here is the table of impossibilities :

The Quartic A_4 and S_4 Case : Indication of Proof VII

• Twisted class groups G_{c^2} : needs to be studied in detail (1 page), uses global CFT but not difficult. This study has a surprising corollary :

Proposition

Let k be a cubic field. There exists $u \in k^*$ coprime to 2 such that $u\mathbb{Z}_k = \mathfrak{q}^2$, $\mathcal{N}(u)$ is a square, and $u \not\equiv 1 \pmod{4\mathbb{Z}_k}$.

I do not know how to prove this without CFT.

• Splitting of primes in (k, K_6, K). As mentioned, this was partly done by Martinet and Jehanne, but need to do it completely. Two steps : first prove that certain splittings are impossible, second for the remaining ones find examples. For fun, here is the table of impossibilities :

The Quartic A_4 and S_4 Case : Prime Splits I

k-split	K_6-split	K-split	Possible for $p \neq 2$?	Possible for $p = 2$?
(3)	(6)	—	ZETA	ZETA
(3)	(33)	(31)	OK	OK
(3)	(3^2)	(1^4)	SQN	OK
(21)	(42)	(4)	OK	OK
(21)	(411)	—	ZETA	ZETA
(21)	(41^2)	—	ZETA	ZETA
(21)	(222)	(22)	STICK	STICK
(21)	(2211)	(211)	OK	OK
(21)	(221^2)	(21^2)	SQN	GRP(1)
(21)	(2^22)	(2^2)	OK	OK
(21)	(2^211)	(1^31)	RAM	RAM
(21)	(2^211)	(1^21^2)	OK	OK
(21)	(2^21^2)	(1^4)	SQN	OK

The Quartic A_4 and S_4 Case : Prime Splits II

k-split	K_6-split	K-split	Possible for $p \neq 2$?	Possible for $p = 2$?
(111)	(222)	—	ZETA	ZETA
(111)	(2211)	(22)	OK	OK
(111)	(221^2)	—	ZETA	ZETA
(111)	(21111)	(211)	STICK	STICK
(111)	(2111^2)	(21^2)	SQN	GRP(2)
(111)	(21^21^2)	(2^2)	OK	OK
(111)	(111111)	(1111)	OK	OK
(111)	(1^21111)	(1^211)	SQN	GRP(3)
(111)	(1^21^211)	(1^21^2)	OK	OK
(111)	(1^21^211)	(1^31)	RAM	RAM
(111)	$(1^21^21^2)$	(1^4)	SQN	OK

The Quartic A_4 and S_4 Case : Prime Splits III

k-split	K_6-split	K-split	Possible for $p \neq 2$?	Possible for $p = 2$?
$(1^2 1)$	$(2^2 2)$	—	ZETA	ZETA
$(1^2 1)$	$(2^2 11)$	(21^2)	OK	OK
$(1^2 1)$	$(2^2 1^2)$	(2^2)	SQN	GRP(4)
$(1^2 1)$	$(1^2 1^2 2)$	(21^2)	GRP(5)	GRP(5)
$(1^2 1)$	$(1^2 1^2 11)$	$(1^2 11)$	OK	OK
$(1^2 1)$	$(1^2 1^2 1^2)$	$(1^2 1^2)$	SQN	GRP(6)
$(1^2 1)_0$	$(1^4 2)$	(2^2)	SQN	PARITY
$(1^2 1)_4$	$(1^4 2)$	(2^2)	SQN	OK
$(1^2 1)$	$(1^4 11)$	$(1^2 1^2)$	SQN	OK
$(1^2 1)$	$(1^4 1^2)$	(1^4)	OK	OK
(1^3)	(2^3)	(2^2)	GRP(7)	GRP(7)
(1^3)	$(1^3 1^3)$	$(1^2 1^2)$	GRP(8)	GRP(8)
(1^3)	$(1^3 1^3)$	$(1^3 1)$	OK	OK
(1^3)	(1^6)	(1^4)	SQN	OK

The Quartic A_4 and S_4 Case : Prime Splits IV and $\mathcal{L}(k)$ I

In these tables, anything other than OK means the splitting is impossible, for quite a number of reasons : ZETA because of the zeta relation, SQN because of the square norm condition, STICK because of Stickelberger's theorem, RAM because of ramification indices, and more generally GRP(i) because of case-by-case reasoning on decomposition and inertia groups. The whole study with proof requires 6 tedious pages.

- Study of $\mathcal{L}(k)$: recall that

$$\mathcal{L}(k) = \mathcal{L}_{k,1} \cup \mathcal{L}_{k,4} \cup \mathcal{L}_{k,16} \cup \mathcal{L}_{k,64,tr} \cdot$$

The reason for the importance of this set is :

Proposition

$E \in \mathcal{L}(k)$ if and only if the corresponding K_6 of trivial norm is of the form $K_6 = k(\sqrt{\alpha})$ with α coprime to 2, totally positive, and $\alpha\mathbb{Z}_k = \mathfrak{q}^2$ (i.e., α virtual unit).

The Quartic A_4 and S_4 Case : Prime Splits IV and $\mathcal{L}(k)$ I

In these tables, anything other than OK means the splitting is impossible, for quite a number of reasons : ZETA because of the zeta relation, SQN because of the square norm condition, STICK because of Stickelberger's theorem, RAM because of ramification indices, and more generally GRP(i) because of case-by-case reasoning on decomposition and inertia groups. The whole study with proof requires 6 tedious pages.

- Study of $\mathcal{L}(k)$: recall that

$$\mathcal{L}(k) = \mathcal{L}_{k,1} \cup \mathcal{L}_{k,4} \cup \mathcal{L}_{k,16} \cup \mathcal{L}_{k,64,tr} \ .$$

The reason for the importance of this set is :

Proposition

$E \in \mathcal{L}(k)$ if and only if the corresponding K_6 of trivial norm is of the form $K_6 = k(\sqrt{\alpha})$ with α coprime to 2, totally positive, and $\alpha\mathbb{Z}_k = \mathfrak{q}^2$ (i.e., α virtual unit).

The Quartic A_4 and S_4 Case : $\mathcal{L}(k)$ II

Proposition

- $|\mathcal{L}(k)| = 2^{\mathrm{rk}_2(Cl_4(k))} - 1$.
- $|\mathcal{L}_{k,1}| = (2^{\mathrm{rk}_2(Cl(k))} - 1)/a(k)$.
- $\mathcal{L}_{k,4} = \mathcal{L}_{k,16} = \mathcal{L}_{k,64,tr} = \emptyset$ *(equivalently* $\mathcal{L}(k) = \mathcal{L}_{k,1}$*) if and only if* k *is totally real and all totally positive units are squares.*
- *If one of* $\mathcal{L}_{k,4}$, $\mathcal{L}_{k,16}$, $\mathcal{L}_{k,64,tr}$ *is nonempty the other two are empty.*

It is then possible to give in terms of the splitting of 2 in k and the existence or nonexistence of certain virtual units, necessary and sufficient conditions for $\mathcal{L}_{k,4}$, $\mathcal{L}_{k,16}$, or $\mathcal{L}_{k,64,tr}$ to be nonempty. The complete study of these sets require in all an additional 6 pages.

The Quartic A_4 and S_4 Case : $\mathcal{L}(k)$ II

Proposition

- $|\mathcal{L}(k)| = 2^{\mathrm{rk}_2(Cl_4(k))} - 1$.
- $|\mathcal{L}_{k,1}| = (2^{\mathrm{rk}_2(Cl(k))} - 1)/a(k)$.
- $\mathcal{L}_{k,4} = \mathcal{L}_{k,16} = \mathcal{L}_{k,64,tr} = \emptyset$ *(equivalently* $\mathcal{L}(k) = \mathcal{L}_{k,1}$*) if and only if* k *is totally real and all totally positive units are squares.*
- *If one of* $\mathcal{L}_{k,4}$, $\mathcal{L}_{k,16}$, $\mathcal{L}_{k,64,tr}$ *is nonempty the other two are empty.*

It is then possible to give in terms of the splitting of 2 in k and the existence or nonexistence of certain virtual units, necessary and sufficient conditions for $\mathcal{L}_{k,4}$, $\mathcal{L}_{k,16}$, or $\mathcal{L}_{k,64,tr}$ to be nonempty. The complete study of these sets require in all an additional 6 pages.

The Quartic A_4 and S_4 Case : Sums over Characters

- The final thing that we need to do is to show that the sums over characters of G_{ζ^2} as which occur in the CDO theorem correspond to sums over quartic fields $E \in \mathcal{L}(k)$. Even though this is analogous to the cubic case, it is much more subtle, and again involves some local and global class field theory and 4 additional pages.

Once this is done, the usual combinatorics done in the cubic case lead to our main theorem.

The Quartic A_4 and S_4 Case : Sums over Characters

• The final thing that we need to do is to show that the sums over characters of G_{ζ^2} as which occur in the CDO theorem correspond to sums over quartic fields $E \in \mathcal{L}(k)$. Even though this is analogous to the cubic case, it is much more subtle, and again involves some local and global class field theory and 4 additional pages.
Once this is done, the usual combinatorics done in the cubic case lead to our main theorem.

Signatures or Local Conditions I

We may require that our fields K, in addition to having k as cubic resolvent, satisfies a finite number of local conditions (for instance splittings of certain primes, etc...). One of the most natural generalizations of our work, already mentioned in [CDO] is to add signature conditions : if k is a cubic field of signature $(1,1)$ then K has necessarily signature $(2,1)$. But if k is totally real then K is either totally real or totally complex, and we may want to compute explicitly the corresponding Dirichlet series $\Phi_4^+(k;s)$, where we restrict the sum to totally real K.

The CDO theorem is valid almost verbatim :

Signatures or Local Conditions I

We may require that our fields K, in addition to having k as cubic resolvent, satisfies a finite number of local conditions (for instance splittings of certain primes, etc...). One of the most natural generalizations of our work, already mentioned in [CDO] is to add signature conditions : if k is a cubic field of signature $(1,1)$ then K has necessarily signature $(2,1)$. But if k is totally real then K is either totally real or totally complex, and we may want to compute explicitly the corresponding Dirichlet series $\Phi_4^+(k;s)$, where we restrict the sum to totally real K.

The CDO theorem is valid almost verbatim :

Signatures II

Theorem

$$\Phi_4^+(k;s) = \frac{1}{a(k)2^{3s}} \sum_{\mathfrak{c}|2\mathbb{Z}_k} z_k(\mathfrak{c})(\mathcal{N}\mathfrak{c})^{s-1} \prod_{\mathfrak{p}|\mathfrak{c}} \left(1 - \frac{1}{\mathcal{N}\mathfrak{p}^s}\right) \sum_{\chi \in \widehat{G_{\mathfrak{c}^2}^+}} F_k(\chi, s) \ ,$$

with the same definition of $z_k(\mathfrak{c})$ and $F_k(\chi, s)$, and $G_{\mathfrak{c}^2}^+$ is a "narrow" twisted ray class group.

Thus the only difference with the CDO theorem is the replacement of $G_{\mathfrak{c}^2}$ by $G_{\mathfrak{c}^2}^+$, and the coefficient in front equal to 1 instead of $2^{2-r_2(k)} = 4$ since k is totally real.

As a consequence (already noted in CDO) it is a theorem that asymptotically the proportion of totally real K with given cubic resolvent k among all of them is $1/4$: in fact we can prove that the convergence is quite fast (at least $O(X^{-1/2})$, but in practice $O(X^{-3/4+\varepsilon})$).

Signatures II

Theorem

$$\Phi_4^+(k;s) = \frac{1}{a(k)2^{3s}} \sum_{\mathfrak{c}|2\mathbb{Z}_k} z_k(\mathfrak{c})(\mathcal{N}\mathfrak{c})^{s-1} \prod_{\mathfrak{p}|\mathfrak{c}} \left(1 - \frac{1}{\mathcal{N}\mathfrak{p}^s}\right) \sum_{\chi \in \widehat{G_{\mathfrak{c}^2}^+}} F_k(\chi, s) \ ,$$

with the same definition of $z_k(\mathfrak{c})$ and $F_k(\chi, s)$, and $G_{\mathfrak{c}^2}^+$ is a "narrow" twisted ray class group.

Thus the only difference with the CDO theorem is the replacement of $G_{\mathfrak{c}^2}$ by $G_{\mathfrak{c}^2}^+$, and the coefficient in front equal to 1 instead of $2^{2-r_2(k)} = 4$ since k is totally real.

As a consequence (already noted in CDO) it is a theorem that asymptotically the proportion of totally real K with given cubic resolvent k among all of them is $1/4$: in fact we can prove that the convergence is quite fast (at least $O(X^{-1/2})$, but in practice $O(X^{-3/4+\varepsilon})$).

Signatures II

Theorem

$$\Phi_4^+(k;s) = \frac{1}{a(k)2^{3s}} \sum_{\mathfrak{c}|2\mathbb{Z}_k} z_k(\mathfrak{c})(\mathcal{N}\mathfrak{c})^{s-1} \prod_{\mathfrak{p}|\mathfrak{c}} \left(1 - \frac{1}{\mathcal{N}\mathfrak{p}^s}\right) \sum_{\chi \in \widehat{G_{\mathfrak{c}^2}^+}} F_k(\chi, s) \ ,$$

with the same definition of $z_k(\mathfrak{c})$ and $F_k(\chi, s)$, and $G_{\mathfrak{c}^2}^+$ is a "narrow" twisted ray class group.

Thus the only difference with the CDO theorem is the replacement of $G_{\mathfrak{c}^2}$ by $G_{\mathfrak{c}^2}^+$, and the coefficient in front equal to 1 instead of $2^{2-r_2(k)} = 4$ since k is totally real.

As a consequence (already noted in CDO) it is a theorem that asymptotically the proportion of totally real K with given cubic resolvent k among all of them is $1/4$: in fact we can prove that the convergence is quite fast (at least $O(X^{-1/2})$, but in practice $O(X^{-3/4+\varepsilon})$).

Signatures III

We then transform the CDO+ theorem into a theorem of the same nature as the main theorem without signatures : the only changes are : first, an additional factor of $1/4$, and second and more importantly, the set $\mathcal{L}(k)$ is changed into a new set $\mathcal{L}^*(k)$, where we simply remove the condition that E be totally real when k is totally real. We give one example in the A_4 case and one in the S_4 case.

Example for A_4 : Let again k be the cyclic cubic field of discriminant 49. Then

$$\Phi_4^+(k;s) = \frac{1}{4}\left(\Phi_4(k;s) + \left(1 - \frac{1}{2^{3s}}\right) \prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3} \left(1 + \frac{\omega_E(p)}{p^s}\right)\right),$$

where E is the totally complex A_4-quartic field of discriminant $64 \cdot 49$ with cubic resolvent k defined by $x^4 - 2x^3 + 2x^2 + 2 = 0$.

Signatures III

We then transform the CDO+ theorem into a theorem of the same nature as the main theorem without signatures : the only changes are : first, an additional factor of $1/4$, and second and more importantly, the set $\mathcal{L}(k)$ is changed into a new set $\mathcal{L}^*(k)$, where we simply remove the condition that E be totally real when k is totally real. We give one example in the A_4 case and one in the S_4 case.

Example for A_4 : Let again k be the cyclic cubic field of discriminant 49. Then

$$\Phi_4^+(k;s) = \frac{1}{4}\left(\Phi_4(k;s) + \left(1 - \frac{1}{2^{3s}}\right) \prod_{p\mathbb{Z}_k = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3} \left(1 + \frac{\omega_E(p)}{p^s}\right)\right) ,$$

where E is the totally complex A_4-quartic field of discriminant $64 \cdot 49$ with cubic resolvent k defined by $x^4 - 2x^3 + 2x^2 + 2 = 0$.

Signatures IV

Example for S_4 : Let k be the noncyclic totally real cubic field of discriminant 229 defined by $x^3 - 4x - 1 = 0$. Then

$$\Phi_4^+(k;s) = \frac{1}{4}\left(\Phi_4(k;s) + \left(1 + \frac{1}{2^{2s}} - \frac{2}{2^{4s}}\right)\prod_{p\neq 2}\left(1 + \frac{\omega_{E_1}(p)}{p^s}\right)\right.$$
$$\left. + \left(1 - \frac{1}{2^{2s}}\right)\prod_{p\neq 2}\left(1 + \frac{\omega_{E_{64}}(p)}{p^s}\right)\right),$$

where E_1 is the unique totally complex quartic field of discriminant 229 and cubic resolvent k defined by $x^4 - x + 1 = 0$ and E_{64} is the unique totally complex quartic field of discriminant $64 \cdot 229$ and cubic resolvent k in which 2 is totally ramified, defined by $x^4 - 2x^3 + 4x^2 - 2x + 5$.