



**HAL**  
open science

## A program to test the p-rationality of any number field

Georges Gras

► **To cite this version:**

| Georges Gras. A program to test the p-rationality of any number field. 2017. hal-01590183v1

**HAL Id: hal-01590183**

**<https://hal.science/hal-01590183v1>**

Preprint submitted on 19 Sep 2017 (v1), last revised 16 Mar 2019 (v2)

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# A PROGRAM TO TEST THE $p$ -RATIONALITY OF ANY NUMBER FIELD

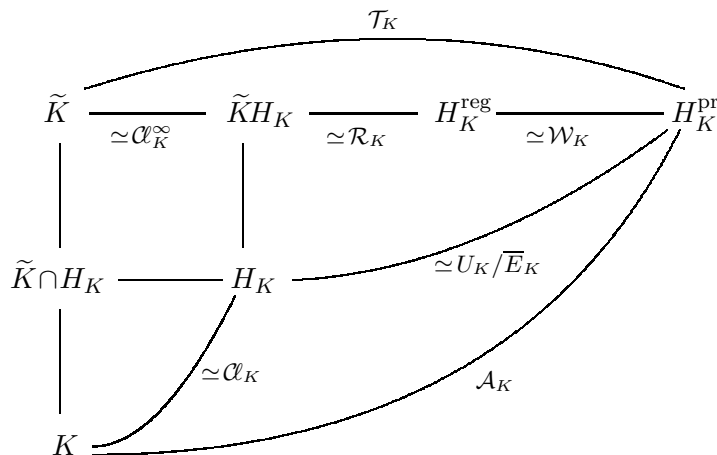
GEORGES GRAS

ABSTRACT. We give very short PARI programs (see §§ 4.1, 4.2) to test if the number field  $K$  (defined by an irreducible polynomial) is  $p$ -rational for a given prime  $p \geq 2$ . For the convenience of any user, the programs are written with “verbatim” characters, so that it is sufficient to “copy and paste” them from the pdf file to the “Terminal Session–Math–gp” of <http://pari.math.u-bordeaux.fr/> or of “Sage” <http://www.sagemath.org/fr/telecharger.html>.

## 1. DEFINITION AND PROPERTIES OF $p$ -RATIONALITY

Let  $K$  be a number field and let  $p \geq 2$  be a fixed prime number. We denote by  $\mathcal{C}_K$  the  $p$ -class group of  $K$  in the ordinary sense and by  $E_K$  the group of  $p$ -principal global units  $\varepsilon \equiv 1 \pmod{\prod_{v|p} \mathfrak{p}_v}$  of  $K$ , where  $\mathfrak{p}_v$  is the prime ideal corresponding to the place  $v \mid p$ .

We shall describe the diagram of the so called *abelian  $p$ -ramification theory* (from [5, § III.2 (c), Fig. 2.2] and [6, Section 3]), in which  $\tilde{K}$  is the compositum of the  $\mathbb{Z}_p$ -extensions of  $K$ ,  $H_K$  the  $p$ -Hilbert class field and  $H_K^{\text{pr}}$  the maximal abelian  $p$ -ramified (i.e., unramified outside  $p$ ) pro- $p$ -extension of  $K$  (see [1] and [10, Diagram 2] for a similar context with logarithmic class groups):



Since we intend to give numerical algorithms, we implicitly assume the Leopoldt conjecture for  $p$  in  $K$ .

Let  $U_K := \bigoplus_{v|p} U_v^1$  be the  $\mathbb{Z}_p$ -module of  $p$ -principal local units of  $K$  where each  $U_v^1$  is the group of  $v$ -principal units of the completion  $K_v$  of  $K$  at  $v \mid p$  (i.e.,  $U_v^1 = \{u \in K_v^\times, u \equiv 1 \pmod{\overline{\mathfrak{p}}_v}\}$ , where  $\overline{\mathfrak{p}}_v$  is the maximal ideal of the ring of integers of  $K_v$ ).

For any field  $k$ , denote by  $\mu_k$  the  $p$ -group of roots of unity of  $k$  and let  $W_K := \text{tor}_{\mathbb{Z}_p}(U_K) = \bigoplus_{v|p} \mu_{K_v}$ . Let  $\overline{E}_K$  be the closure in  $U_K$  of the diagonal image of the group  $E_K$  of  $p$ -principal global units of  $K$ . Then put:

$$\mathcal{T}_K := \text{tor}_{\mathbb{Z}_p}(\text{Gal}(H_K^{\text{pr}}/K)).$$

We have the exact sequence defining  $\mathcal{W}_K$  and  $\mathcal{R}_K$  (from [5, Lemma III.4.2.4]; see also [6, Lemma 3.1] for a proof):

$$1 \longrightarrow W_K/\mu_K =: \mathcal{W}_K \longrightarrow \text{tor}_{\mathbb{Z}_p}(U_K/\overline{E}_K) \\ \xrightarrow{\log} \text{tor}_{\mathbb{Z}_p}(\log(U_K)/\log(\overline{E}_K)) =: \mathcal{R}_K \longrightarrow 0.$$

The group  $\mathcal{R}_K$  (or its order) is called the *normalized  $p$ -adic regulator of  $K$* ; when  $K$  is totally real, one has the relation [6, Section 5, Proposition 5.2]:

$$\#\mathcal{R}_K \sim \frac{1}{2} \cdot \frac{(\mathbb{Z}_p : \log(\mathbb{N}_{K/\mathbb{Q}}(U_K)))}{\#\mathcal{W}_K \cdot \prod_{v|p} \mathbb{N}_{\mathfrak{p}_v}} \cdot \frac{R_K}{\sqrt{D_K}},$$

from a formula of Coates [2], where  $\sim$  means equality up to a  $p$ -adic unit factor,  $R_K$  is the usual  $p$ -adic regulator of  $K$  [16, § 5.5],  $D_K$  the discriminant of  $K$ , and  $\mathbb{N}$  the absolute norm for ideals.

**Definition 1.1.** The field  $K$  is said to be  *$p$ -rational* if the torsion group  $\mathcal{T}_K$  is trivial (under the Leopoldt conjecture).

See [4], [5], [10], [11], [12] for more information on  $p$ -rationality and [9] for applications to Galois representations  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \text{GL}_n(\mathbb{Z}_p)$  with open image. We have conjectured in [7] that  $K$  is  $p$ -rational for all  $p \gg 0$ .

Then  $\mathcal{T}_K = 1$  if and only if the three invariants  $\mathcal{W}_K$ , the normalized  $p$ -adic regulator  $\mathcal{R}_K$  and the subgroup  $\mathcal{C}_K^\infty$  of  $\mathcal{C}_K$ , are trivial. Thus, in some cases, it is more convenient to test each of these trivialities, depending on the knowledge of the field  $K$ ; for instance, when the  $p$ -class group is trivial and if  $p$  is unramified in  $K/\mathbb{Q}$ , the computation of the normalized  $p$ -adic regulator  $\mathcal{R}_K$  may be given in a specific program and the computation of  $\mathcal{W}_K$  is in general easy directly (e.g., quadratic or cubic fields, cyclotomic fields...). But a field given by means of a polynomial  $P$  may be more mysterious and we shall recal the PARI instructions to get all the necessary data about  $K$ .

## 2. COMPUTATION OF BASIC INVARIANTS OF $K$

The reader wishing to test only  $p$ -rationalities may go directly to Subsections 4.1, 4.2. The examples are given with the polynomial:

$$P = x^3 - 5x + 3$$

(recall that  $P$  must be in  $\mathbb{Z}[x]$ ), for which one gives the classical information (test of irreducibility, Galois group of the Galois closure of  $K$ , discriminant of  $K$ ) which are the following, with the PARI responses (from [13]):

```
polisirreducible(x^3-5*x+3)
1
polgalois(x^3-5*x+3)
[6,-1,1,"S3"]
factor(nfdisc(x^3-5*x+3))
[257 1]
```

showing that  $P$  is irreducible, that the Galois closure of  $K$  is the dihedral group of order 6, and that the discriminant of  $K$  is the prime 257.

Then  $K$  is defined by the following instructions in which we obtain the signature  $[r_1, r_2]$  of  $K$ , the structure of the whole class group and the fundamental units:

```
{P=x^3-5*x+3;p=2;K=bnfinit(P,1);
Sign=component(component(K,7),2);print("Signature of K: ",Sign);
print("Structure of the class group: ",component(component(K,8),1));
print("Fundamental system of units: ",component(component(K,8),5))}
[3,0]
[1,[]]
[x-1,x^2+2*x-2]
```

giving a totally real field, a trivial class group and the two fundamental units. The next program gives, for information, the decomposition of the primes  $p$  (up to 47):

```
{P=x^3-5*x+3;K=bnfinit(P,1);
forprime(p=2,50,print(p," ",idealfactor(K,p)))}
2 Mat([[2,[2,0,0]~,1,3,1],1])
3 [[3,[0,0,1]~,1,1,[1,1,-1]~],1];[3,[4,1,-1]~,1,2,[0,0,1]~],1]
5 [[5,[2,0,1]~,1,1,[2,1,2]~],1];[5,[2,1,-3]~,1,2,[2,0,1]~],1]
7 [[7,[1,0,1]~,1,1,[-1,1,-2]~],1];[7,[6,1,-2]~,1,2,[1,0,1]~],1]
11 Mat([[11,[11,0,0]~,1,3,1],1])
13 Mat([[13,[13,0,0]~,1,3,1],1])
```

showing that 2, 11, 13 are inert, that 3, 5, 7 split into two prime ideals with residue degrees 1 and 2, respectively. Taking  $p = 257$ , one obtains as expected:

```
257 [[257,[-101,0,1]~,1,1,[-81,1,100]~],1];
[257,[-78,0,1]~,2,1,[-86,1,77]~],2]
```

which split into  $\mathfrak{p}_1 \cdot \mathfrak{p}_2^2$ .

To obtain a polynomial from a compositum of known fields (e.g., quadratic fields) one uses by induction the instructions:

```
Q=polcompositum(P1,P2);Q=component(Q,1)
(since  $Q$  is first given as a matrix  $[Q]$ ); for instance:
{P1=x^2-2;P2=x^2+5;P3=x^2-7;
Q=polcompositum(P1,P2);Q=component(Q,1);
P=polcompositum(Q,P3);P=component(P,1);print(P)}
x^8 - 16*x^6 + 344*x^4 + 2240*x^2 + 19600
```

### 3. GENERAL THEORETICAL TEST OF $p$ -RATIONALITY

In [14] and [15, Theorem 3.11], are given methods for the general computation of the structure of  $\mathcal{T}_K$ , but here we need only to characterize the triviality (or not) of  $\mathcal{T}_K$  in the relation:

$$\mathcal{A}_K := \text{Gal}(H_K^{\text{pr}}/K) \simeq \mathbb{Z}_p^r \times \mathcal{T}_K,$$

where  $r = r_2 + 1$ ,  $2r_2$  being the number of complex embeddings of  $K$ .

As  $\mathcal{T}_K$  is a direct factor in  $\mathcal{A}_K$ , the structure of the whole Galois group  $\mathcal{A}_K$  may be analyzed at a finite step by computing the Galois group of a suitable ray class field  $K(p^n)$  of modulus  $(p^n)$ . Since PARI gives the structure of ray class groups of the form  $\mathcal{C}_K(p^n) := \text{Gal}(K(p^n)/K)$ , the test of  $p$ -rationality is obtained for  $n$  large enough as follows.

If  $\mathcal{C}_K(p^n)$  has a  $p$ -rank such that:

$$\text{rk}_p(\mathcal{C}_K(p^n)) \geq r + 1,$$

then  $K$  is not  $p$ -rational since  $\text{Gal}(\tilde{K}/K)$  has  $p$ -rank  $r$ . The minimal  $n_0$  for the test is given as a consequence of the following results (stated in the ordinary sense):

**Theoreme 3.1.** For any  $v \mid p$  and any  $j \geq 1$ , let  $U_v^j$  be the group of local units  $1 + \bar{\mathfrak{p}}_v^j$ , where  $\bar{\mathfrak{p}}_v$  is the maximal ideal of the ring of integers of  $K_v$ .

For a modulus of the form  $(p^n)$ ,  $n \geq 0$ , let  $\mathcal{C}_K(p^n)$  be the corresponding ray class group. Then for  $m \geq n \geq 0$ , we have the inequalities:

$$0 \leq \text{rk}_p(\mathcal{C}_K(p^m)) - \text{rk}_p(\mathcal{C}_K(p^n)) \leq \sum_{v \mid p} \text{rk}_p((U_v^1)^p U_v^{n e_v} / (U_v^1)^p U_v^{m e_v}),$$

where  $e_v$  is the ramification index of  $v$  in  $K/\mathbb{Q}$ .

*Proof.* From [5, Theorem I.4.5 & Corollary I.4.5.4] taking for  $T$  the set of  $p$ -places and for  $S$  the set of real infinite places (so that  $\delta_\infty = \emptyset$ ).  $\square$

**Corollary 3.2.** We have  $\text{rk}_p(\mathcal{C}_K(p^m)) = \text{rk}_p(\mathcal{C}_K(p^n)) = \text{rk}_p(\mathcal{A}_K)$  for all  $m \geq n \geq n_0$ , where  $n_0 = 3$  for  $p = 2$  and  $n_0 = 2$  for  $p > 2$ .

Thus  $K$  is  $p$ -rational if and only if  $\text{rk}_p(\mathcal{C}_K(p^{n_0})) = r$ , where  $r = r_2 + 1$ .

*Proof.* It is sufficient to get, for some fixed  $n \geq 0$ :

$$(U_v^1)^p U_v^{n e_v} = (U_v^1)^p \text{ for all } v \mid p,$$

hence  $U_v^{n e_v} \subseteq (U_v^1)^p$  for all  $v \mid p$ ; indeed, we then have:

$$\text{rk}_p(\mathcal{C}_K(p^n)) = \text{rk}_p(\mathcal{C}_K(p^m)) = r + \text{rk}_p(\mathcal{T}_K) \text{ as } m \rightarrow \infty,$$

giving  $\text{rk}_p(\mathcal{C}_K(p^n)) = r + \text{rk}_p(\mathcal{T}_K)$  for such  $n$ .

The condition  $U_v^{n e_v} \subseteq (U_v^1)^p$  is fulfilled as soon as  $n e_v > \frac{p \cdot e_v}{p-1}$ , hence  $n > \frac{p}{p-1}$  (see [3, Chap. I, §5.8, Corollary 2] or [16, Proposition 5.7]), whence the value of  $n_0$ .  $\square$

The program giving the structure of  $\mathcal{C}_K(p^{n_0})$  is the following (we compute the structure of the ray class groups with modulus  $p^n$  up to  $n = 5$  to see the stabilization of the  $p$ -ranks; this would give the invariants of  $\mathcal{T}_K$ , as in [15]):

```
{K=bnfinit(x^3-5*x+3,1);p=2;
for(n=0,5,Hpn= bnrinit(K,p^n);print(n," ",component(Hpn,5)))}
0 [1, []]
1 [1, []]
2 [2, [2]]
3 [4, [2, 2]]
4 [8, [4, 2]]
5 [16, [8, 2]]
```

then for  $p = 3$ :

```
0 [1, []]
1 [1, []]
2 [3, [3]]
3 [9, [9]]
4 [27, [27]]
5 [81, [81]]
```

for the ramified prime  $p = 257$  (where  $32896 = 2^7 \cdot 257$ ,  $8454272 = 2^7 \cdot 257^2$ ,  $2172747904 = 2^7 \cdot 257^3$ , and so on):

```
0 [1, []]
1 [128, [128]]
2 [32896, [32896]]
3 [8454272, [8454272]]
4 [2172747904, [2172747904]]
5 [558396211328, [558396211328]]
```

Thus  $K$  is  $p$ -rational for  $p = 3$  and 257, but not for  $p = 2$ .

Now we give the case of the first irregular prime  $p = 37$  for which we know that the  $p$ th cyclotomic field is not  $p$ -rational (indeed,  $\mathcal{T}_K = 1$  is equivalent to  $\mathcal{C}_K = 1$  for the  $p$ th cyclotomic fields [4]).

So we must see that the  $p$ -ranks are equal to  $19 + 1$ , at least for  $n \geq 2$ :

```
{p=37;K=bnfinit(polycyclo(p),1);
for(n=0,2,Hpn=bnrinit(K,p^n);print(n," ",component(Hpn,5)))}
0 [37,[37]]
1 [624931990990842127748277129373,[1369,37,37,37,37,37,37,37,37,37,37,
  37,37,37,37,37,37,37,37]]
2 [390539993363777986320898213181845819006713655084697379373129,
  [50653,1369,1369,1369,1369,1369,1369,1369,1369,1369,1369,1369,1369,
  1369,1369,1369,1369,1369,37,37,37]]
```

#### 4. FULL GENERAL PARI PROGRAMS

We bring together some instructions given in the previous sections and recall that, in the programs,  $n = 2$  (resp. 3) if  $p \neq 2$  (resp.  $p = 2$ ).

**4.1. General program: Main invariants – Test of  $p$ -rationality.** The reader has to introduce an *irreducible polynomial*  $P \in \mathbb{Z}[x]$  and a *prime number*  $p \geq 2$ . For  $p = 2$  the  $p$ -rationality is in the ordinary sense.

```
=====
{P=x^3-5*x+3;p=2;K=bnfinit(P,1);
Sign=component(component(K,7),2);print("Signature of K: ",Sign);
print("Galois group of the Galois closure of K: ",polgalois(P));
print("Discriminant: ",factor(component(component(K,7), 3)));
print("Structure of the class group: ",component(component(K,8),1));
print("Fundamental system of units: ",component(component(K,8),5));
r=component(Sign,2)+1;n=2;if(p==2,n=3);
print(p,"-rank of the compositum of the Z_",p,"-extensions: ",r);
Hpn=component(component(bnrinit(K,p^n),5),2);L=listcreate;
d=component(matsize(Hpn),2);R=0;for(k=1,d,c=component(Hpn,k);
if(Mod(c,p)==0,R=R+1;listinsert(L,p^valuation(c,p),1));delta=R-r;
print("Structure of the ray class group mod ",p,"^n: ",L);
if(delta>0,print("K is not ",p,"-rational"));
if(delta==0,print("K is ",p,"-rational"))}
=====
```

(i) With the above data,  $K$  is not 2-rational nor 293-rational (up to  $p \leq 10^5$ ) since the program writes, respectively:

```
Signature of K: [3,0]
Galois group of the Galois closure of K: [6,-1,1,"S3"]
Discriminant: Mat([257,1])
Structure of the class group: [1,[]]
Fundamental system of units: [x-1,x^2+2*x-2]
2-rank of the compositum of the Z_2-extensions: 1
Structure of the ray class group mod 2^n: List([2,2])
K is not 2-rational
```

```
Signature of K: [3,0]
Galois group of the Galois closure of K: [6,-1,1,"S3"]
Discriminant: Mat([257,1])
Structure of the class group: [1,[]]
Fundamental system of units: [x-1,x^2+2*x-2]
293-rank of the compositum of the Z_293-extensions: 1
Structure of the ray class group mod 293^n: List([293,293])
K is not 293-rational
```

(ii) The field  $K = \mathbb{Q}(\sqrt{-161})$  is not 2-rational (the Hilbert class field is linearly disjoint from  $\tilde{K}$  [5, Example III.6.7]):

```
Signature of K: [0,1]
Galois group of the Galois closure of K: [2,-1,1,"S2"]
Discriminant: [-1,1;2,2;7,1;23,1]
Structure of the class group: [16,[8,2]]
Fundamental system of units: []
2-rank of the compositum of the Z_2-extensions: 2
Structure of the ray class group mod 2^n: List([2,2,4,16])
K is not 2-rational
```

(iii) The field  $K = \mathbb{Q}(\sqrt{-41})$  is not 2-rational (comes from  $\mathcal{W}_K \neq 1$ ).

(iv) The field  $K = \mathbb{Q}(\sqrt{69})$  is not 3-rational (comes from  $\mathcal{R}_K \neq 1$ ).

(v) The quartic cyclic fields  $K$  defined by  $P = x^4 + 5x^2 + 5$  and by  $P = x^4 + 13x^2 + 13$  are 2-rational (see [5, Example IV.3.5.1], examples which were given first in [8, § III]).

**4.2. Simplified program – Test of  $p$ -rationality.** Since some parts of the first program are useless and some computations intricate (e.g., Galois groups), one may use the following simplified program to test only the  $p$ -rationality; we test the 3-rationality of

$$K = \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{5}, \sqrt{11}, \sqrt{97})$$

given in [9] ( $P$  is computed from the instruction *polcompositum*; then we give the  $p$ -structure of  $\mathcal{C}_K(p^{n_0})$  up to  $p \leq 100$ ):

```
=====
{P=x^16-872*x^14+313900*x^12-60356280*x^10+6720557526*x^8
-440456545944*x^6+16552772527564*x^4-327028989448904*x^2
+2685135903980209;p=3;n=2;if(p==2,n=3);
Kpn=bnrinit(bnfinit(P,1),p^n);S=component(component(Kpn,1),7);
r=component(component(S,2),2)+1;L=listcreate;
print(p,"-rank of the compositum of the Z_",p,"-extensions: ",r);
Hpn=component(component(Kpn,5),2);d=component(matsize(Hpn),2);
R=0;for(k=1,d,c=component(Hpn,k);if(Mod(c,p)==0,R=R+1;
listinsert(L,p^valuation(c,p,1)));delta=R-r;
print("Structure of the ",p,"-ray class group: ",L);
if(delta>0,print("K is not ",p,"-rational"));
if(delta==0,print("K is ",p,"-rational"))}
=====
```

If one wishes to test the  $p$ -rationality of  $K$  for  $p$  varying in an interval  $[a, b]$ , it is necessary to compute first the data  $bnfinit(P, 1)$  which is independent of  $p$  and takes lots of time. Then the tests for  $p$ -rationality are very fast.

This gives the following writing:

```
=====
{P=x^16-872*x^14+313900*x^12-60356280*x^10+6720557526*x^8
-440456545944*x^6+16552772527564*x^4-327028989448904*x^2
+2685135903980209;K=bnfinit(P,1);
r=component(component(component(K,7),2),2)+1;
print("p-rank of the compositum of the Z_p-extensions: ",r);
forprime(p=2,100,n=2;if(p==2,n=3);
Kpn=bnrinit(K,p^n);Hpn=component(component(Kpn,5),2);
d=component(matsize(Hpn),2);L=listcreate;
R=0;for(k=1,d,c=component(Hpn,k);if(Mod(c,p)==0,R=R+1;
listinsert(L,p^valuation(c,p,1)));delta=R-r;
print("Structure of the ",p,"-ray class group: ",L);
if(delta>0,print("K is not ",p,"-rational"));
if(delta==0,print("K is ",p,"-rational"))}
=====
```

$p$ -rank of the compositum of the  $\mathbb{Z}_p$ -extensions: 9

```
List([2, 2, 2, 4, 4, 4, 4, 4, 8, 8, 8, 8, 16, 64]) not 2-rational
List([3, 3, 3, 3, 3, 3, 3, 3, 9]) 3-rational
List([5, 5, 5, 5, 5, 5, 5, 5, 25]) 5-rational
List([7, 7, 7, 7, 7, 7, 7, 7, 7, 7]) not 7-rational
List([11, 11, 11, 11, 11, 11, 121, 121, 121, 121]) not 11-rational
List([13, 13, 13, 13, 13, 13, 13, 13, 13, 13]) not 13-rational
List([17, 17, 17, 17, 17, 17, 17, 17, 17, 17]) not 17-rational
List([19, 19, 19, 19, 19, 19, 19, 19, 19, 19]) 19-rational
List([23, 23, 23, 23, 23, 23, 23, 23, 23, 23]) 23-rational
List([29, 29, 29, 29, 29, 29, 29, 29, 29, 29]) 29-rational
List([31, 31, 31, 31, 31, 31, 31, 31, 31, 31]) not 31-rational
List([37, 37, 37, 37, 37, 37, 37, 37, 37, 37]) 37-rational
List([41, 41, 41, 41, 41, 41, 41, 41, 41, 41]) 41-rational
List([43, 43, 43, 43, 43, 43, 43, 43, 43, 43]) not 43-rational
List([47, 47, 47, 47, 47, 47, 47, 47, 47, 47]) 47-rational
List([53, 53, 53, 53, 53, 53, 53, 53, 53, 53]) 53-rational
List([59, 59, 59, 59, 59, 59, 59, 59, 59, 59]) 59-rational
List([61, 61, 61, 61, 61, 61, 61, 61, 61, 61]) 61-rational
List([67, 67, 67, 67, 67, 67, 67, 67, 67, 67]) 67-rational
List([71, 71, 71, 71, 71, 71, 71, 71, 71, 71]) 71-rational
List([73, 73, 73, 73, 73, 73, 73, 73, 73, 73]) not 73-rational
List([79, 79, 79, 79, 79, 79, 79, 79, 79, 79]) 79-rational
List([83, 83, 83, 83, 83, 83, 83, 83, 83, 83]) 83-rational
List([89, 89, 89, 89, 89, 89, 89, 89, 89, 89]) 89-rational
List([97, 97, 97, 97, 97, 9409, 9409, 9409, 9409]) 97-rational
```

We find that  $K$  is not  $p$ -rational (with  $p$  up to  $10^6$ ) for the primes:

$p \in \{2, 7, 11, 13, 17, 31, 43, 73, 163, 263, 409, 1049, 2671, 3331, 8941, 28477, 36899, 99149, 231901, 283979, 353711, 363719\}$  (no solutions between 363719 and  $10^6$  !).

The cases of non  $p$ -rationality are essentially due to some units of  $K$ ; for instance, for the unit  $\varepsilon = 1 + \sqrt{2} \in K$  and  $p = 31$ , we get:

$$\varepsilon^{30} = 152139002499 + 107578520350\sqrt{2} \equiv 1 \pmod{31^2},$$

which means  $\mathcal{R}_K = \frac{1}{31} \log(\varepsilon) \equiv 0 \pmod{31}$ .

## 5. CONCLUSION

As we have seen, in this paper and in [7], number fields are in general  $p$ -rational for “almost all”  $p$ , except perhaps for  $p = 2$  for which the invariant  $\mathcal{W}_K = (\bigoplus_{v|2} \mu_{K_v}) / \mu_K$ , depending on the splitting of 2 in  $K/\mathbb{Q}$ , is often non-trivial since its order is divisible by the order of  $(\bigoplus_{v|2} \mu_2) / \mu_2$ ; the case of fields  $K$  containing  $\mu_p$  also arises for the same reason. So we wonder whether another definition of  $p$ -rationality would be interesting or not (“weak  $p$ -rationality” when  $\mathcal{C}_K^\infty = \mathcal{R}_K = 1$ ) ?

However, for  $p \gg 0$ , one gets  $\mathcal{C}_K = \mathcal{W}_K = 1$  and the most deep and mysterious invariant about  $p$ -rationality is the *normalized  $p$ -adic regulator*:

$$\mathcal{R}_K = \text{tor}_{\mathbb{Z}_p}(\log(U_K) / \log(\overline{E}_K)).$$

for which we have done, for  $p \gg 0$ , extensive heuristics and conjectures in [7].



## REFERENCES

- [1] K. Belabas and J-F. Jaulent, *The logarithmic class group package in PARI/GP*, Pub. Math. Besançon (2016), 5–18.
- [2] J. Coates, *p-adic L-functions and Iwasawa's theory*, Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London (1977), 269–353.
- [3] I. B. Fesenko and S. V. Vostokov, *Local Fields and Their Extensions*, American Math Society, Translations of Math Monographs, vol. 121, Second Edition 2002. <https://www.maths.nottingham.ac.uk/personal/ibf/book/vol.pdf>
- [4] G. Gras and J-F. Jaulent, *Sur les corps de nombres réguliers*, Math. Z. **202**(3) (1989), 343–365. <https://eudml.org/doc/174095>
- [5] G. Gras, *Class Field Theory: from theory to practice*, SMM, Springer-Verlag 2003; second corrected printing 2005. <https://www.researchgate.net/publication/268005797>
- [6] G. Gras, *The p-adic Kummer-Leopoldt Constant – Normalized p-adic Regulator*, Int. Journal of Number Theory, 2018 (to appear). <https://arxiv.org/abs/1701.06857>
- [7] G. Gras, *Les  $\theta$ -régulateurs locaux d'un nombre algébrique : Conjectures p-adiques*, Canadian Journal of Mathematics **68**(3) (2016), 571–624. <http://dx.doi.org/10.4153/CJM-2015-026-3>
- [8] G. Gras, *Remarks on  $K_2$  of number fields*, Jour. Number Theory **23**(3) (1986), 322–335. <http://www.sciencedirect.com/science/article/pii/0022314X86900776>
- [9] R. Greenberg, *Galois representations with open image*, Annales de Mathématiques du Québec, special volume in honor of Glenn Stevens, **40**(1) (2016), 83–119. <https://www.math.washington.edu/~greenber/GalRep.pdf>
- [10] J-F. Jaulent, *Théorie  $\ell$ -adique globale du corps de classes*, J. Théorie des Nombres de Bordeaux **10**(2) (1998), 355–397. [http://www.numdam.org/article/JTNB\\_1998\\_\\_10\\_2\\_355\\_0.pdf](http://www.numdam.org/article/JTNB_1998__10_2_355_0.pdf)
- [11] J-F. Jaulent et T. Nguyen Quang Do, *Corps p-rationnels, corps p-réguliers et ramification restreinte*, J. Théorie des Nombres de Bordeaux **5**(2) (1993), 343–363. [http://www.numdam.org/article/JTNB\\_1993\\_\\_5\\_2\\_343\\_0.pdf](http://www.numdam.org/article/JTNB_1993__5_2_343_0.pdf)
- [12] A. Movahhedi et T. Nguyen Quang Do, *Sur l'arithmétique des corps de nombres p-rationnels*, Séminaire de Théorie des Nombres, Paris 1987–88, Progress in Mathematics, Volume 81, 1990, 155–200. [https://link.springer.com/chapter/10.1007%2F978-1-4612-3460-9\\_9](https://link.springer.com/chapter/10.1007%2F978-1-4612-3460-9_9)
- [13] THE PARI GROUP – PARI/GP, version 2.9.0, *Université de Bordeaux* (2016). <http://pari.math.u-bordeaux.fr/>.
- [14] F. Pitoun, *Calculs théoriques et explicites en théorie d'Iwasawa*, Thèse de doctorat en Mathématiques, Laboratoire de Mathématiques, Université de Franche-comté Besançon (2010). <http://indexation.univ-fcomte.fr/nuxeo/site/esupversions/4692338d-6401-40e6-8638-695d7fd1cc73>
- [15] F. Pitoun and F. Varescon, *Computing the torsion of the p-ramified module of a number field*, Math. Comp. **84**(291) (2015), 371–383. <http://www.ams.org/journals/mcom/2015-84-291/S0025-5718-2014-02838-X/S0025-5718-2014-02838-X.pdf>
- [16] L.C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Math. 83, Springer enlarged second edition 1997.

VILLA LA GARDETTE, CHEMIN CHÂTEAU GAGNIÈRE F-38520 LE BOURG D'OISANS,  
FRANCE [https://www.researchgate.net/profile/Georges\\_Gras](https://www.researchgate.net/profile/Georges_Gras)  
E-mail address: [g.mn.gras@wanadoo.fr](mailto:g.mn.gras@wanadoo.fr)