New PARI functions around abelian number fields

Takashi FUKUDA
(Nihon University)

12th Atelier PARI/GP
University of Bordeaux 2019.1.16

1. New functions in PARI/GP

`pclgpsubcyclo`	p-class group of abelian number field
`lambdasubcyclo`	Iwasawa λ^--invariant of abelian number field
`ipolsubcyclo`	Iwasawa polynomial of abelian number field
`rcnsubcyclo`	Relative class number of abelian number field
`quadlambda`	Iwasawa λ^--invariant of imaginary quadratic field
`quadstkpol`	Stickelberger element and Iwasawa polynomial of imaginary quadratic field
`ele2gen`	finds generators of $H \subset (\mathbb{Z}/f\mathbb{Z})^\times$

2. Algorithm for pclgpsubcyclo

Aoki, M. and Fukuda, T.,

An algorithm for computing p-class groups of abelian number fields,

ANTSVII 2006, pp.56–71, LNCS, vol. 4076, Springer, Berlin, 2006.

F : abelian number field

p : odd prime number not dividing $[F : \mathbb{Q}]$

A_F : p-class group of F

$A_F = \oplus_\chi \oplus_K A_{K,\chi}$

K runs all cyclic subfield of F

χ runs representatives of $\mathbb{Q}_p$-conjugacy classes of injective character $G(K/\mathbb{Q}) \longrightarrow \overline{\mathbb{Q}}_p^\times$

$A_F^+ = \oplus_{\chi:\text{even}} \oplus_K A_{K,\chi}$ is calculated using cyclotomic unit.

$A_F^- = \oplus_{\chi:\text{odd}} \oplus_K A_{K,\chi}$ is calculated using Gauss sum.

The algorithm is based on Iwasawa Main Conjecture proved by Mazur-Wiles and independent of GRH.

3. How to use

`pclgpsubcyclo(p, f, {H = [1]}, {flag=3})`

F : the subfield of $\mathbb{Q}(\zeta_f)$ corresponding to $H \subset (\mathbb{Z}/f\mathbb{Z})^\times$

p : an odd prime number not dividing $[F : \mathbb{Q}]$

The result is a 6-component vector *pclgp*.

pclgp[1] is p.

pclgp[2] contains the order and the structure of A_F^+.

pclgp[3] contains the order and the structure of A_F^-.

pclgp[4] is $G(F/\mathbb{Q})$.

pclgp[5] is the number of cyclic subfields K of F except for $\mathbb{Q}$.

pclgp[6] is the number of $\mathbb{Q}_p$-conjugacy classes of injective characters $\chi : G(K/\mathbb{Q}) \to \overline{\mathbb{Q}}_p^\times$.

The behavior of **pclgpsubcyclo** is controled by the binary digits of *flag*.

1: computes an upper bound of $|\, A_F^+ \,|$.

2: computes $|\, A_F^- \,|$.

4: ignores proper subfields of F.

8: determines the group structure of A_F and guarantees informations about A_F^+.

16: outputs K s.t. $A_K \neq 0$.

32: use an integral basis of K.

With default $flag = 3$, **pclgpsubcyclo** determines the exact value of $|\, A_F^- \,|$ and an upper bound of $|\, A_F^+ \,|$ which is expected to be equal to $|\, A_F^+ \,|$. The group structure of A_F will be determined by chance.

4. $\mathbb{Q}(\zeta_f)$

```
? pclgpsubcyclo(101, 22220)
%1 = [101, [0, []], [41, [1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1]], [100, 20, 2, 2], 479, 7999]
```

computes 101-part A_F of the ideal class group of $F = \mathbb{Q}(\zeta_{22220})$.

$A_F^+ = 0$: rigorous

$|\, A_F^- \,| = 101^{41}$, $A_F^- \cong (\mathbb{Z}/101\mathbb{Z})^{41}$: rigorous

479 cyclic subfields K of F except for $\mathbb{Q}$

7999 $\mathbb{Q}_{101}$-conjugacy classes of injective characters $\chi : G(K/\mathbb{Q}) \to \overline{\mathbb{Q}}_{101}^{\times}$

```
? pclgpsubcyclo(11, 22220)
%2 = [11, [2, [1, 1]], [16, []], [100, 20, 2, 2], 479, 1799]
```

computes 11-part A_F of the ideal class group of $F = \mathbb{Q}(\zeta_{22220})$.

$|\, A_F^+ \,| = 11^2$, $A_F^+ \cong (\mathbb{Z}/11\mathbb{Z})^2$: not rigorous

$|\, A_F^- \,| = 11^{16}$: rigorous

```
? pclgpsubcyclo(11, 22220,, 3+8)
%3 = [11, [2, [1, 1]], [16, [2, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1]], [100, 20, 2, 2], 479, 1799]
```

$|\, A_F^+ \,| = 11^2$, $A_F^+ \cong (\mathbb{Z}/11\mathbb{Z})^2$: rigorous

$|\, A_F^- \,| = 11^{16}$, $A_F^- \cong \mathbb{Z}/11^2\mathbb{Z} \oplus (\mathbb{Z}/11\mathbb{Z})^{14}$: rigorous

The outputs of **pclgpsubcyclo** without *flag* are non-rigorous for the plus part and rigorous for the minus part. Running with *flag*=11 gurantees the outputs about plus part and determines the group structure.

Schoof (Math. Comp. 2003)

$$27 \mid h(\mathbb{Q}(\zeta_{521}))^+, \quad \text{small posibility of } 81 \mid h(\mathbb{Q}(\zeta_{521}))^+$$

```
? pclgpsubcyclo(3,521,,11)
%3 = [3, [3, [1, 1, 1]], [0, []], [520], 15, 64]
```

$$A_F \cong (\mathbb{Z}/3\mathbb{Z})^3$$

Washington's book, GTM 83

$$3^8 5^4 17^4 41^2 \mid h(\mathbb{Q}(\zeta_{816}))^-$$

```
? pclgpsubcyclo([3,5,17,41],816,,11)
%4 =
[ 3 [0, []] [8, [2, 2, 1, 1, 1, 1]] [16, 4, 2, 2] 71 103]
[ 5 [0, []]       [4, [1, 1, 1, 1]] [16, 4, 2, 2] 71 127]
[17 [0, []]       [4, [1, 1, 1, 1]] [16, 4, 2, 2] 71 255]
[41 [0, []]             [2, [1, 1]] [16, 4, 2, 2] 71 191]
```

5. $F = \mathbb{Q}(\sqrt{m}\,,\,\zeta_5)$

$G(F/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

$f = \mathrm{lcm}(\mathrm{abs}(\mathrm{quaddisc}(m)),\, p)\,,\; F \leftrightarrow H \subset (Z/f\mathbb{Z})^{\times}$

```
qp(m,p,flag)=
{
my(a,d,f,H);
d=quaddisc(m);f=lcm(abs(d),p);H=vectorsmall(f);
for(a=1,f-1, if(kronecker(d,a)==1 && a%p==1, H[a]=1,));
ele2gen(H,flag);
}
? qp(36322,5)
%1 = [726440, [41, 61, 111, 131]]
```

$F = \mathbb{Q}(\sqrt{36322}\,,\,\zeta_5) \Longrightarrow f = 726440,\; H = \langle\, 41, 61, 111, 131 \,\rangle$

```
? pclgpsubcyclo(5,726440,[41,61,111,131],11)
%2 = [5, [1, [1]], [4, [3, 1]], [4, 2], 5, 7]
```

Intel Core i5 1.70GHz

m	A_F^+	A_F^-	time
1111	(5)	$(5,5)$	0.9s
7523	(5)	$(5^2,5)$	44s
36227	0	(5^3)	10s
36322	(5)	$(5^3,5)$	45s
42853	(5)	$(5^3,5,5)$	12s
-5657	(5^2)	$(5,5)$	0.5s
-14606	$(5,5)$	$(5,5)$	7s
-38602	$(5,5)$	$(5,5)$	32s
-57758	$(5,5)$	$(5,5)$	54s

6. Coates Conjecture

$$\mathbb{Q}(p^n) = \begin{cases} \mathbb{Q}(\zeta_{2^{n+2}}) \cap \mathbb{R} & p = 2 \\ \text{subfield of } \mathbb{Q}(\zeta_{p^{n+1}}) \text{ with degree } p^n & p > 2 \end{cases}$$

$G(\mathbb{Q}(p^n)/\mathbb{Q}) \cong \mathbb{Z}/p^n\mathbb{Z}$

$\mathbb{Q}(n) = \mathbb{Q}(p_1^{e_1}) \cdots \mathbb{Q}(p_r^{e_r})$ if $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$,

$G(\mathbb{Q}(n)/\mathbb{Q}) \cong \mathbb{Z}/n\mathbb{Z}$, $h(n) = h(\mathbb{Q}(n))$

Conjecture 6.1. $h(p^n) = 1$ for all p and all $n \geq 1$.

- There are no known examples $h(p^n) > 1$.

Conjecture 6.2 (Coates, 2011). $h(n)$ is bounded.

- There are 9 examples $h(n) > 1$.

$31 \mid h(2 \cdot 31)$	by theory
$73 \mid h(3 \cdot 73)$	by theory
$1546463 \mid h(2 \cdot 1546463)$	by theory
$18433 \mid h(2^8 \cdot 18433)$	by theory
$114689 \mid h(2^{10} \cdot 114689)$	by theory
$487 \mid h(3^4 \cdot 487)$	by theory
$238627 \mid h(3^4 \cdot 238627)$	by theory
$2251 \mid h(5^2 \cdot 2251)$	by theory
$107 \mid h(2 \cdot 53)$	by **pclgpsubcyclo**

In each case, the exact value of $h(n)$ is unknown.

How to get $H \subset (\mathbb{Z}/f\mathbb{Z})^\times$ corresponding to $\mathbb{Q}(n)$.

$$
\begin{aligned}
n &= p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} \\
e_i' &= \begin{cases} e_i + 2 & p = 2 \\ e_i + 1 & p > 2 \end{cases} \\
f &= p_1^{e_1'} p_2^{e_2'} \cdots p_r^{e_r'} \\
g_i &= \text{ primitive root of } p_i^2 \text{ if } p_i > 2
\end{aligned}
$$

$$
a_i = \begin{cases} -1 & p_i = 2 \\ g_i^{p_i^{e_i}} & p_i > 2 \end{cases}, \quad b_i \equiv \begin{cases} a_i & (\text{mod } p_i^{e_i'}) \\ 1 & (\text{mod } f/p_i^{e_i'}) \end{cases}
$$

Then, $H = \langle\, b_1, \cdots, b_r \,\rangle$.

```
Q(n)=
{
my(z,col,p,e,e2,a,b,f=1,H=[]);
z=factor(n);
col=matsize(z)[1];
for(i=1,col,p=z[i,1];e=z[i,2];if(p==2,e2=e+2,e2=e+1);f*=p^e2);
for(i=1,col,
p=z[i,1]; e=z[i,2];
if(p==2,e2=e+2;a=Mod(-1,p^e2),e2=e+1;a=znprimroot(p^e2)^(p^e);)
b=chinese(a,Mod(1,f/p^e2));
H=concat(H,lift(b)));
printf("n=%d: f, H = %d, %d\n",n,f,H);
}
```

```
? Q(106)
n=106: f, H = 22472, [16855,1009]
? pclgpsubcyclo(107, 8*53^2, [16855, 1009])
time = 28 ms.
%6 = [107, [1, [1]], [0, []], [106], 3, 105]
? pclgpsubcyclo(107, 8*53^2, [16855, 1009], 11)
time = 22min, 3,049 ms.
%7 = [107, [1, [1]], [0, []], [106], 3, 105]
```

Both outputs without *flag* and with *flag*=11 are the same. But *flag*=11 confirms the result.

7. Cyclotomic $\mathbb{Z}_3$-extension of $k = \mathbb{Q}(\sqrt{-239})$

$k = k_0 \subset k_1 \subset k_2 \subset \cdots \subset k_\infty$: cyclotomic $\mathbb{Z}_3$-extension

$G(k_n/k) \cong \mathbb{Z}/3^n\mathbb{Z},\ \ 3^{e_n} \mid\mid h(k_n)$

THEOREM 7.1 (Iwasawa). $e_n = \mu\, 3^n + \lambda n + \nu$ *for all* $n >> 0$.

$\mu = 0$, $\lambda = 6$. We can compute e_n $(1 \leq n \leq 7)$ explicitly.

```
quadZp(p,m,n)=
{
 my(a,d,f,pn1,H,z);
 d=quaddisc(m);pn1=p^(n+1);f=lcm(abs(d),pn1);H=vectorsmall(f);
 for(a=1,f-1,
 if(kronecker(d,a)==1 && lift(Mod(a,pn1)^(p-1))==1, H[a]=1,));
 ele2gen(H);
}
```

```
? valuation(rcnsubcyclo(239*3^2,[8]),3)
%1 = 4
? valuation(rcnsubcyclo(239*3^3,[80]),3)
%2 = 10
? valuation(rcnsubcyclo(239*3^4,[80]),3)
%3 = 16
? valuation(rcnsubcyclo(239*3^5,[242]),3)
%4 = 22
? valuation(rcnsubcyclo(239*3^6,[728]),3)
%5 = 28
? valuation(rcnsubcyclo(239*3^7,[15308]),3)
%6 = 34
? valuation(rcnsubcyclo(239*3^8,[26243]),3)
%7 = 40
```

8. Iwasawa λ^--invariant of abelian number field

$\lambda_3^-(k) = 6$ $\quad k = \mathbb{Q}(\sqrt{-239}\,)$

```
quadlambda(3,-239)
```

$\lambda_3^-(k) = 14$ $\quad k = \mathbb{Q}(\sqrt{-956238}\,)$

```
quadlambda(3,-956238)
```

$\lambda_3^-(k) = 45$ $\quad k = \mathbb{Q}(\sqrt{-2}\,, \sqrt{-5}\,, \sqrt{-11}\,, \sqrt{-17}\,, \sqrt{-23}\,, \sqrt{-29}\,)$

```
lambdasubcyclo(3,4989160,[3,49,163])
```

$\lambda_5^-(k) = 37$ $\quad k = \mathbb{Q}(\sqrt{-1}\,, \sqrt{-11}\,, \sqrt{-19}\,, \sqrt{-29}\,, \sqrt{-31}\,, \sqrt{-41}\,)$

```
lambdasubcyclo(5,30814124,[5, 49, 169])
```

$\lambda_{41}^-(k) = 217$ $\quad k = \mathbb{Q}(\zeta_{22220})$

```
lambdasubcyclo(41,22220)
```

9. Cyclotomic $\mathbb{Z}_3$-extension of $k = \mathbb{Q}(\sqrt{-956238})$

$k = k_0 \subset k_1 \subset k_2 \subset \cdots \subset k_\infty$: cyclotomic $\mathbb{Z}_3$-extension

A_n : 3-part of the ideal class group of k_n

$q_n = 4 \cdot 956238 \cdot 3^n$, $\Sigma_n = G(\mathbb{Q}_n/\mathbb{Q}) \cong \mathbb{Z}/3^n\mathbb{Z}$

$$\xi_n^\chi = \frac{1}{q_n} \sum_{\substack{a=1 \\ (a,q_n)=1}}^{q_n} a\chi(a)^{-1} \left(\frac{\mathbb{Q}_n/\mathbb{Q}}{a}\right)^{-1} \in \mathbb{Z}_3[\Sigma_n]$$

THEOREM 9.1 (Coates-Lichtenbaum, 1973).
Since $A_0 \cong \mathbb{Z}/3Z$ and $p = 3$ does not split in $k/\mathbb{Q}$, we have

$$A_n \cong \mathbb{Z}_p[\Sigma_n]/(\xi_n^\chi) \quad (n \geq 0)$$

We prepare a GP script snf to compute the structure of $\mathbb{Z}_p[\Sigma_n]/(\xi_n^\chi)$.

```
snf(p,v)=
{
my(i,j,e,col,A,B=[],M);
v=Vecrev(v);
col=matsize(v)[2];
M=matrix(col,col);M[1,]=v;
for(i=2,col,for(j=1,col,M[i,j]=M[1,1+(j-i)%col]));
A=matsnf(M);
for(i=1,col,
if(A[i]!=0 && (e=valuation(A[i],p))>0, B=concat(B,p^e),));
B;
}
```

Then we can compute A_n as in the following way.

```
? z=quadstkpol(3,-956238,1,1);snf(3,z)
? z=quadstkpol(3,-956238,2,1);snf(3,z)
? z=quadstkpol(3,-956238,3,1);snf(3,z)
? z=quadstkpol(3,-956238,4,1);snf(3,z)
? z=quadstkpol(3,-956238,5,1);snf(3,z)
```

$$A_n \cong \begin{cases} \left(\mathbb{Z}/3\mathbb{Z}\right)^3 & n=1 \quad \text{by computation} \\ \left(\mathbb{Z}/3\mathbb{Z}\right)^9 & n=2 \quad \text{by computation} \\ \left(\mathbb{Z}/3^2\mathbb{Z}\right)^9 \oplus \left(\mathbb{Z}/3\mathbb{Z}\right)^5 & n=3 \quad \text{by computation} \\ \left(\mathbb{Z}/3^3\mathbb{Z}\right)^9 \oplus \left(\mathbb{Z}/3^2\mathbb{Z}\right)^5 & n=4 \quad \text{by computation} \\ \left(\mathbb{Z}/3^{n-1}\mathbb{Z}\right)^9 \oplus \left(\mathbb{Z}/3^{n-2}\mathbb{Z}\right)^5 & n \geq 5 \quad \text{by theory} \end{cases}$$

10. Time of rcnsubcyclo(n)

n	h^-	Time(ms)
10000	1933 digits	100
10001	5787 digits	850
10002	1556 digits	470
10003	4848 digits	750
10004	2444 digits	35
10005	2317 digits	75
10006	2634 digits	5658
10007	6018 digits	76908
10008	1536 digits	23
10009	6020 digits	25203

Acknowledgment.

I would like to express my gratitude to

Karim Belabas and Bill Allombert.

Bibliography

[1] Aoki, M. and Fukuda, T., An algorithm for computing p-class groups of abelian number fields, Algorithmic Number Theory, 56–71, Lecture Notes in Computer Science, vol. 4076, Springer, Berlin, 2006.

[2] Coates, J, The enigmatic Tate-Shafarevich group, In: Fifth International Congress of Chinese Mathematicians. Part 1. 2. AMS/IP Studies in Advance Mathematics, vol. 51, Part 1. 2, pp.43–50. American Mathematical Society, Providence (2012)

[3] Coates, J. and Lichitenbaum, S., On ℓ-adic zeta functions, Ann. of Math., **98** (1973), 498–550.

[4] Gold, R., Γ-extensions of imaginary quadratic fields, Pacific J. Math., **40** (1972), 83–88.

[5] Gold, R., Examples of Iwasawa invariants, Acta Arith., **26** (1974), 21–32; part II: **26** (1975), 233–240.