PARI/GP Atelier (13/01/2022)

[Tutorial] The subcyclo package

Karim Belabas

Introduction

This is tutorial about a branch developped by Takashi Fukuda, who started working on it in 2018 during the last Atelier in Besançon, and recently merged into the `master` branch.

PARI already includes many functions and algorithms to determine and work with class groups of *general number fields*, notably `bnfinit`, `bnrinit` and `bnrclassfield`. Unconditionally in small degrees, assuming GRH in moderate degrees, and with little hope of success in huge degrees (> 150, say).

On the other hand, Iwasawa theory deals with (infinite!) towers of number fields, in particular cyclotomic $\mathbb{Z}_p$-extensions and can give partial information about class groups of number fields of very high degrees, in particular abelian fields. This tutorial centers on the `subcyclopclgp` function which deals with the p-Sylow subgroups of the ideal class group of *abelian number fields*.

Abelian number fields (1/2)

By Kronecker-Weber, these are subfields of cyclotomic fields. A good description for such a field F is by a pair (f, H), where H is the subgroup of $(\mathbb{Z}/f\mathbb{Z})^* = \mathrm{Gal}(\mathbb{Q}(\zeta_f)/\mathbb{Q})$ fixing F. If f is minimal, we call it the conductor of the extension: this is the critical parameter for all complexities involved.

In PARI terms, we will use an argument `fH` to denote either of

- an integer f, describing $\mathbb{Q}(\zeta_f)$ (implicitly $H = (1)$);
- a pair $[f, H]$, where f is an integer and H is a vector of generators as `t_INTMOD`s modulo f or `t_INT`s (implicitly mapped to $(\mathbb{Z}/f\mathbb{Z})^*$);
- a pair $[G, H]$ where G is `idealstar`$(f, 1)$ and H is a subgroup, given by the canonical HNF matrix giving the generators of H in terms of G`.gen`. This HNF matrix divides the diagonal matrix with diagonal G`.cyc` and there is a one-to-one correspondence between subgroups of a finite abelian group and such matrices; the determinant of the matrix is equal to the subgroup index.

Abelian number fields (2/2)

- a pair $[G, H]$ where G is a `bnr` structure attached to a ray class group $\mathrm{Cl}_{\mathfrak{f}}(\mathbb{Q})$ and H is a subgroup given by a canonical HNF matrix; the place at infinity must not be forgotten: after `Q = bnfinit(y)`, the structure `bnrinit(Q, [f,[1]])` for an integer f is attached to $\mathbb{Q}(\zeta_f)$ and isomorphic to $(\mathbb{Z}/f\mathbb{Z})^*$, whereas `bnrinit(Q, f)` is attached to its maximal real subfield $\mathbb{Q}(\zeta_f + \zeta_f^{-1})$ and isomorphic to $(\mathbb{Z}/f\mathbb{Z})^*/(\pm 1)$;
- an irreducible integral monic polynomial defining a primitive element for F.

The function `bnrcompositum` is particularly useful to build compositums in class field theoretic terms: given two pairs `[bnr1, H1]` and `[bnr2, H2]` attached to abelian fields as above, it returns a pair `[bnr, H]` attached to their compositum. This is much more efficient than using `polcompositum` to obtain a defining polynomial.

`subcyclopclgp(fH, p, {flag = 0})` (1/3)

This function takes two arguments: an abelian number field F (given by an `fH` argument) and an *odd* prime $p > 2$ not dividing $[F : \mathbb{Q}]$. It returns information about the p-Sylow subgroup $A = A_F$ of the ideal class group of F. An optional `flag` allows to compute only part of the structure to save time.

We write $A = A^+ \oplus A^-$ according to the eigenvalues of complex conjugation. The function returns a 6-component vector v and we shall concentrate on $v[2]$ and $v[3]$:

- $v[1]$ is p
- $v[2]$ is $[E, [e_1, \ldots, e_k]]$ with $E = \sum_i e_i$ and $e_1 \geqslant \cdots \geqslant e_k$. Meaning that A^+ has order p^E and is isomorphic to $\mathbb{Z}/p^{e_1} \times \cdots \times \mathbb{Z}/p^{e_k}$ (elementary divisors).
- $v[3]$ similarly describes A^-.
- $v[4]$ gives the structure of $\mathrm{Gal}(F/\mathbb{Q})$ (elementary divisors)
- $v[5]$ is the number of cyclic subfields $K \neq \mathbb{Q}$ contained in F

`subcyclopclgp` (2/3)

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

A vector of primes is also accepted and the result is then a vector of vectors as above, one for each prime and in the same order.

This is the behaviour if `flag` $= 1$ which is *not* the default value, since it is likely to be very costly. By default (`flag` $= 0$) the function quickly computes

- $E(A^-)$ and the structure of A^- if it is easy to determine,
- a proven sharp *upper bound* for $E(A^+)$ (which is *expected*, but not proven, to be the exact value unless it is 0)

The corresponding (e_i) vectors for non-computed structures are replaced by dummy empty vectors.

`subcyclopclgp` (3/3)

- bit 1 of `flag`: finish and certify all computations;
- bit 2 of `flag`: don't compute anything about A^+;
- bit 4 of `flag`: don't compute anything about A^-.

E.g., `flag` $= 1 + 4$ (always) computes fully A^+ but doesn't compute anything about A^-.

Examples

Simple examples for $F = \mathbb{Q}(\zeta_{22220})$, i.e., $f = 110 \times 101$ or $F = \mathbb{Q}(\zeta_{44440})$:

```
?  subcyclopclgp(22220, 101)
time = 100 ms.
%1 = [101, [0, []], [41, [1, ..., 1]], ...]
?  subcyclopclgp(44440, 101)
time = 300 ms.
%2 = [101, [1, [1]], [76, []], ...]
?  subcyclopclgp(44440, 101, 1)
time = 43,942 ms.
%3 = [101, [1, [1]], [76, [2, 1, ..., 1]], ...]
?  subcyclopclgp(22220, 11)
%4 = [11, [2, [1, 1]], [16, []], ...]
?  subcyclopclgp(22220, 11, 1)
%5 = [11, [2, [1, 1]], [16, [2, 1, ..., 1]], ...]
```

Examples

$F = \mathbb{Q}(\sqrt{36322}, \zeta_5)$

```
?  T = polcompositum(x^2-36322, polcyclo(5), 2);
?  bnfinit(T).cyc
time = 2,870 ms.
%7 = [2000, 20, 20, 2]
?  subcyclopclgp(T, 5)
time = 89 ms.
%6 = [5, [1, [1]], [4, []], ...]
?  subcyclopclgp(T, 5, 1+4)
time = 93 ms.
%7 = [5, [1, [1]], [], ...]
?  default(parisizemax, "4G")
?  subcyclopclgp(T, 5, 1)
time = 33,468 ms.
%9 = [5, [1, [1]], [4, [3, 1]], ...]
```

Examples

Still $F = \mathbb{Q}(\sqrt{36322}, \zeta_5)$, using a class-field theoretic description:

```
?  Q = bnfinit(y);
?  [,bnr1,H1] = rnfconductor(Q, x^2-36322);
?  [,bnr2,H2] = rnfconductor(Q, polcyclo(5));
?  [bnr,H] = bnrcompositum([bnr1,H1], [bnr2,H2]);
?  subcyclopclgp([bnr,H], 5)
%14 = [5, [1, [1]], [4, []], ...]
```

Examples

Compositum of $\mathbb{Q}(\sqrt{2})$ and the subfield of $\mathbb{Q}(\zeta_{53^2})$ of degree 53:

```
?  bnr1 = bnrinit(Q, 8); H1 = Mat(2);
?  bnr2 = bnrinit(Q, [53^2, [1]]); H2 = Mat(53);
?  [bnr,H] = bnrcompositum([bnr1, H1], [bnr2, H2]);
?  subcyclopclgp([bnr,H], 107)
time = 21 ms.
%18 = [107, [1, [1]], [0, []], ...]
```

The simpler direct construction is a disaster :

```
T = polcompositum(x^2-2,polsubcyclo(53^2,53), 2)
subcyclopclgp(T, 107)
```

will run for years trying to compute an $[f, H]$ description (*old efficiency* bug*, hard to fix*).

Other functions: `subcyclohminus`

`subcyclohminus(fH)` computes the relative class number $h^-(F)$ up to Hasse's unit index $Q \in \{1, 2\}$ using an analytic class number formula: more precisely it returns $[h^-, Q]$, or $[2h^-/Q, 0]$ if Q could not be determined.

`subcyclohminus(fH, p)`, with p an odd prime number, returns $v_p(h^-(F))$.

```
?  subcyclohminus(22220, 101)
time = 40 ms.
%19 = 41

?  p = 7860079; G = znstar(p, 1);
?  subcyclohminus([G, Mat(13122)], 3)
time = 1,203 ms.
%21 = 65
```

This gives the 3-part of the subfield of degree 13122 in $\mathbb{Q}(\zeta_{7860079})$.

Other functions: `subcycloiwasawa`

`subcycloiwasawa(fH, p)`; let p be a prime, F_∞ the cyclotomic $\mathbb{Z}_p$-extension of F and let F_n be its n-th layer. Computes the λ-invariant attached to F_∞

`subcycloiwasawa(fH, p, k)` compute the Iwasawa polynomial (of degree λ) modulo $p^{k-\log_p \lambda}$.

Not all cases are implemented in this function; e.g., p must be odd and not divide $[F : \mathbb{Q}]$ unless F is quadratic. For quadratic fields, more information is actually output about the behaviour of A_F along F_∞:

```
?  subcycloiwasawa(x^2 + 1501391, 3)
time = 28 ms.
%22 = [14, -16, [2, 5]]
```

This says that at $p = 3$, we have $\lambda = 14$ and that $e_0 = 2, e_1 = 5$ and $e_n = 14n - 16$ for all $n \geqslant 2$, where 3^{e_n} is the 3-part of the class number of F_n.