Finite abelian group morphisms in PARI/GP

Jared Asuncion

21 January 2020

Motivation

Let K be a CM field and let $\mathfrak{m}$ be an ideal of $\mathcal{O}_K$. That is, K is a totally imaginary quadratic extension of a totally real field K_0. We would like to compute the middle term in a short exact sequence of (finite) abelian groups:

$$1 \to A \to B \to C \to 1$$

where

$$A = \frac{\mathcal{O}_{K_0^+}^\times}{N_{K/K_0}\left(\mathcal{O}_{K,1 \bmod m}^\times\right)} \qquad C = \frac{\{\mathfrak{a} \in I_K(\mathfrak{m}) : \mathfrak{a}\bar{\mathfrak{a}} = u\mathcal{O}_K, u \gg 0\}}{P_K(\mathfrak{m})}$$

- Practical application: computing Shimura ray class groups and type norm subgroups (i.e. images of a so-called type norm map).
- The type norm subgroup is used to construct abelian extensions of CM fields.

Goal

- Implement morphisms between (finite) abelian groups in PARI/GP...
- ...in such a way that the code is somehow readable.

Groups in PARI/GP

- the additive group $\mathbb{Z}/n\mathbb{Z}$ implicitly given by `Mod(-, n)`.
- $(\mathcal{O}_K/\mathfrak{m})^\times$ given by `idealstar(K, m)`.
  `nfeltmul`, `nfeltpow`, `ideallog`
- the class group `K.clgp` of a number field K
  `idealmul`, `idealpow`, `bnfisprincipal`
- the unit group of a number field K generated by `K.fu`, `K.tu`.
  `nfeltmul`, `nfeltpow`, `bnfisunit`
- the group of rational points of an elliptic curve E
  `elladd`, `ellmul`

- Main Source:
  Advanced Topics in Computational Number Theory (Cohen)
- Code: `abgrps.gp`

Describing finite abelian groups...

Let `Gr` be the `abgrp` representation of a finite abelian group G.

gens	row matrix G	`ag_G(Gr)`
identity element	element of G	`ag_id(Gr)`
binary operation	$\times : G \times G \to G$	`ag_mul(Gr, x, y)`
repeated operation	$\hat{\cdot} : G \times \mathbb{Z} \to G$	`ag_pow(Gr, x, n)`
context	more information	`ag_context(Gr)`
reduction	simpler representation	`ag_red(Gr, x)`
orders of gens	diagonal matrix D	`ag_DG(Gr)`
discrete logarithm	$d : G \to \prod_{i=1}^{n} \mathbb{Z}/G_{i,i}\mathbb{Z}$	`ag_dlg(Gr, x)`
cardinality	det of D or $+\infty$	`ag_card(Gr)`

Example: Ideal Class Group I

```
? K = bnfinit(y^2 + 2020);
?
```

Example: Ideal Class Group I

```
? K = bnfinit(y^2 + 2020);
? ClK = ag_clgp_of( K );
?
```

Example: Ideal Class Group I

```
? K = bnfinit(y^2 + 2020);
? ClK = ag_clgp_of( K );
? K.gen
% = [[11, 10; 0, 1], [2, 1; 0, 1]]
?
```

Example: Ideal Class Group I

```
? K = bnfinit(y^2 + 2020);
? ClK = ag_clgp_of( K );
? K.gen
% = [[11, 10; 0, 1], [2, 1; 0, 1]]
? G = ag_G(ClK)
% = [[11, 10; 0, 1] [2, 1; 0, 1]]
?
```

Example: Ideal Class Group I

```
? K = bnfinit(y^2 + 2020);
? ClK = ag_clgp_of( K );
? K.gen
% = [[11, 10; 0, 1], [2, 1; 0, 1]]
? G = ag_G(ClK)
% = [[11, 10; 0, 1] [2, 1; 0, 1]]
? type(ag_G(ClK))
% = "t_MAT"
?
```

Example: Ideal Class Group I

```
? K = bnfinit(y^2 + 2020);
? ClK = ag_clgp_of( K );
? K.gen
% = [[11, 10; 0, 1], [2, 1; 0, 1]]
? G = ag_G(ClK)
% = [[11, 10; 0, 1] [2, 1; 0, 1]]
? type(ag_G(ClK))
% = "t_MAT"
? K.cyc
% = [4, 2]
?
```

Example: Ideal Class Group I

```
? K = bnfinit(y^2 + 2020);
? ClK = ag_clgp_of( K );
? K.gen
% = [[11, 10; 0, 1], [2, 1; 0, 1]]
? G = ag_G(ClK)
% = [[11, 10; 0, 1] [2, 1; 0, 1]]
? type(ag_G(ClK))
% = "t_MAT"
? K.cyc
% = [4, 2]
? ag_DG(ClK)
% =
 [4 0]
 [0 2]
```

Example: Ideal Class Group II

```
? K = bnfinit(y^2 + 2020);
? ClK = ag_clgp_of( K );
?
```

Example: Ideal Class Group II

```
? K = bnfinit(y^2 + 2020);
? ClK = ag_clgp_of( K );
? ag_id(ClK)
% = 1
?
```

Example: Ideal Class Group II

```
? K = bnfinit(y^2 + 2020);
? ClK = ag_clgp_of( K );
? ag_id(ClK)
% = 1
? ag_funmul(ClK)
% = (c,x,y)->idealmul(c[1],x,y)
?
```

Example: Ideal Class Group II

```
? K = bnfinit(y^2 + 2020);
? ClK = ag_clgp_of( K );
? ag_id(ClK)
% = 1
? ag_funmul(ClK)
% = (c,x,y)->idealmul(c[1],x,y)
? elt = ag_mul(ClK, ag_pow(ClK, G[1,1], 23),
                    ag_pow(ClK, G[1,2], -1));
?
```

Example: Ideal Class Group II

```
? K = bnfinit(y^2 + 2020);
? ClK = ag_clgp_of( K );
? ag_id(ClK)
% = 1
? ag_funmul(ClK)
% = (c,x,y)->idealmul(c[1],x,y)
? elt = ag_mul(ClK, ag_pow(ClK, G[1,1], 23),
                    ag_pow(ClK, G[1,2], -1));
? ag_dlg(ClK, elt)
% = [3, 1]~
```

Describing morphisms...

- `agmor_kernel(GrB, GrC, morBtoC)`
- `agmor_image(GrB, GrC, morBtoC)`

Describing morphisms...

- `agmor_kernel(GrB, GrC, morBtoC)`
- `agmor_image(GrB, GrC, morBtoC)`

Describing subgroups...

Subgroups are represented by a vector with two elements.

- `HNF`, the HNF matrix of a subgroup H of G
- `Gr`, the abgrp structure of G

Describing morphisms...

- `agmor_kernel(GrB, GrC, morBtoC)`
- `agmor_image(GrB, GrC, morBtoC)`

Describing subgroups...

Subgroups are represented by a vector with two elements.

- `HNF`, the HNF matrix of a subgroup H of G
- `Gr`, the abgrp structure of G

More-phisms...

- `agmor_inverseimageofsubgrp(GrB, GrC, morBtoC, HB)`
- `agmor_imageofsubgrp((GrB, GrC, morBtoC, HC)`

Example: kernel of relative norm

```
?
```

Example: kernel of relative norm

```
? K0 = bnfinit(z^2 + 584*z + 27508);
? K0plus = bnrinit(K0, [1, [1, 1]], 1);
? ClK0plus = ag_clgp_of( K0plus );
?
```

Example: kernel of relative norm

```
? K0 = bnfinit(z^2 + 584*z + 27508);
? K0plus = bnrinit(K0, [1, [1, 1]], 1);
? ClK0plus = ag_clgp_of( K0plus );
? KoverK0 = rnfinit(K0, y^2 - z);
? K = bnfinit(nfinit(KoverK0));
? Km = bnrinit(K, m = 2, 1);
? ClKm = ag_clgp_of( Km );
?
```

Example: kernel of relative norm

```
? K0 = bnfinit(z^2 + 584*z + 27508);
? K0plus = bnrinit(K0, [1, [1, 1]], 1);
? ClK0plus = ag_clgp_of( K0plus );
? KoverK0 = rnfinit(K0, y^2 - z);
? K = bnfinit(nfinit(KoverK0));
? Km = bnrinit(K, m = 2, 1);
? ClKm = ag_clgp_of( Km );
? {ker = agmor_kernel( ClKm, ClK0plus,
      ((x)->rnfidealnormrel(KoverK0, idealhnf(K, x)))}
?
```

Example: kernel of relative norm

```
? K0 = bnfinit(z^2 + 584*z + 27508);
? K0plus = bnrinit(K0, [1, [1, 1]], 1);
? ClK0plus = ag_clgp_of( K0plus );
? KoverK0 = rnfinit(K0, y^2 - z);
? K = bnfinit(nfinit(KoverK0));
? Km = bnrinit(K, m = 2, 1);
? ClKm = ag_clgp_of( Km );
? {ker = agmor_kernel( ClKm, ClK0plus,
      ((x)->rnfidealnormrel(KoverK0, idealhnf(K, x)))}
? ker[1]
% = [2, 0; 0, 2]
?
```

Example: kernel of relative norm

```
? K0 = bnfinit(z^2 + 584*z + 27508);
? K0plus = bnrinit(K0, [1, [1, 1]], 1);
? ClK0plus = ag_clgp_of( K0plus );
? KoverK0 = rnfinit(K0, y^2 - z);
? K = bnfinit(nfinit(KoverK0));
? Km = bnrinit(K, m = 2, 1);
? ClKm = ag_clgp_of( Km );
? {ker = agmor_kernel( ClKm, ClK0plus,
      ((x)->rnfidealnormrel(KoverK0, idealhnf(K, x)))}
? ker[1]
% = [2, 0; 0, 2]
? ker[2] == ClKm
% = 1
```

Use `fag_snfofsubgrp` for getting a group structure out of a subgroup.

Use `fag_snfofsubgrp` for getting a group structure out of a subgroup.

Example: SNF of subgroup

```
? K0 = bnfinit(z^2 + 584*z + 27508);
? K0plus = bnrinit(K0, [1, [1, 1]], 1);
? ClK0plus = ag_clgp_of( K0plus );
? KoverK0 = rnfinit(K0, y^2 - z);
? K = bnfinit(nfinit(KoverK0));
? Km = bnrinit(K, m = 2, 1);
? ClKm = ag_clgp_of( Km );
? {ker = agmor_kernel( ClKm, ClK0plus,
      ((x)->rnfidealnormrel(KoverK0, idealhnf(K, x)))}
?
```

Use fag_snfofsubgrp for getting a group structure out of a subgroup.

Example: SNF of subgroup

```
? K0 = bnfinit(z^2 + 584*z + 27508);
? K0plus = bnrinit(K0, [1, [1, 1]], 1);
? ClK0plus = ag_clgp_of( K0plus );
? KoverK0 = rnfinit(K0, y^2 - z);
? K = bnfinit(nfinit(KoverK0));
? Km = bnrinit(K, m = 2, 1);
? ClKm = ag_clgp_of( Km );
? {ker = agmor_kernel( ClKm, ClK0plus,
      ((x)->rnfidealnormrel(KoverK0, idealhnf(K, x))))}
? kersnf = fag_snfofsubgrp(ker);
?
```

Use `fag_snfofsubgrp` for getting a group structure out of a subgroup.

Example: SNF of subgroup

```
? K0 = bnfinit(z^2 + 584*z + 27508);
? K0plus = bnrinit(K0, [1, [1, 1]], 1);
? ClK0plus = ag_clgp_of( K0plus );
? KoverK0 = rnfinit(K0, y^2 - z);
? K = bnfinit(nfinit(KoverK0));
? Km = bnrinit(K, m = 2, 1);
? ClKm = ag_clgp_of( Km );
? {ker = agmor_kernel( ClKm, ClK0plus,
      ((x)->rnfidealnormrel(KoverK0, idealhnf(K, x))))}
? kersnf = fag_snfofsubgrp(ker);
? ag_DG(kersnf)
% = [64, 0; 0, 4]
?
```

Use `fag_snfofsubgrp` for getting a group structure out of a subgroup.

Example: SNF of subgroup

```
? K0 = bnfinit(z^2 + 584*z + 27508);
? K0plus = bnrinit(K0, [1, [1, 1]], 1);
? ClK0plus = ag_clgp_of( K0plus );
? KoverK0 = rnfinit(K0, y^2 - z);
? K = bnfinit(nfinit(KoverK0));
? Km = bnrinit(K, m = 2, 1);
? ClKm = ag_clgp_of( Km );
? {ker = agmor_kernel( ClKm, ClK0plus,
      ((x)->rnfidealnormrel(KoverK0, idealhnf(K, x)))}
? kersnf = fag_snfofsubgrp(ker);
? ag_DG(kersnf)
% = [64, 0; 0, 4]
? ag_DG(ClKm)
% = [128, 0; 0, 8]
```

Goal

Compute

$$A = \frac{\mathcal{O}_{K_0^+}^\times}{N_{K/K_0}\left(\mathcal{O}_{K,1 \bmod m}^\times\right)}$$

Define $\mathcal{O}_{K,1 \bmod \mathfrak{m}}^*$ to be the kernel of the natural map $\mathcal{O}_K^\times \to (\mathcal{O}_K/\mathfrak{m})^\times$.

$\mathcal{O}_{K,1 \bmod \mathfrak{m}}^*$

?

Goal

Compute

$$A = \frac{\mathcal{O}_{K_0^+}^\times}{N_{K/K_0}\left(\mathcal{O}_{K,1 \bmod m}^\times\right)}$$

Define $\mathcal{O}_{K,1 \bmod \mathfrak{m}}^*$ to be the kernel of the natural map $\mathcal{O}_K^\times \to (\mathcal{O}_K/\mathfrak{m})^\times$.

$\mathcal{O}_{K,1 \bmod \mathfrak{m}}^*$

```
? OKstar = ag_OKstar_of(K);
?
```

Goal

Compute

$$A = \frac{\mathcal{O}_{K_0^+}^\times}{N_{K/K_0}\left(\mathcal{O}_{K,1 \bmod m}^\times\right)}$$

Define $\mathcal{O}_{K,1 \bmod \mathfrak{m}}^*$ to be the kernel of the natural map $\mathcal{O}_K^\times \to (\mathcal{O}_K/\mathfrak{m})^\times$.

$\mathcal{O}_{K,1 \bmod \mathfrak{m}}^*$

```
? OKstar = ag_OKstar_of(K);
? OKmstar = ag_OKmstar_of(K, m = 2);
?
```

Goal

Compute

$$A = \frac{\mathcal{O}_{K_0^+}^\times}{N_{K/K_0}\left(\mathcal{O}_{K,1 \bmod m}^\times\right)}$$

Define $\mathcal{O}_{K,1 \bmod \mathfrak{m}}^*$ to be the kernel of the natural map $\mathcal{O}_K^\times \to (\mathcal{O}_K/\mathfrak{m})^\times$.

$\mathcal{O}_{K,1 \bmod \mathfrak{m}}^*$

```
? OKstar = ag_OKstar_of(K);
? OKmstar = ag_OKmstar_of(K, m = 2);
? H_OKm1star = agmor_kernel(OKstar, OKmstar, ((x)->x))[1];
```

Goal

Compute

$$A = \frac{\mathcal{O}_{K_0^+}^\times}{N_{K/K_0}\left(\mathcal{O}_{K,1 \bmod m}^\times\right)}$$

Define $\mathcal{O}_{K,1 \bmod \mathfrak{m}}^*$ to be the kernel of the natural map $\mathcal{O}_K^\times \to (\mathcal{O}_K/\mathfrak{m})^\times$.

$\mathcal{O}_{K,1 \bmod \mathfrak{m}}^*$

```
? OKstar = ag_OKstar_of(K);
? OKmstar = ag_OKmstar_of(K, m = 2);
? H_OKm1star = agmor_kernel(OKstar, OKmstar, ((x)->x))[1];
```

Exercise: Compute the HNF of $N_{K/K_0}(\mathcal{O}_{K,1 \bmod \mathfrak{m}}^*) \subseteq \mathcal{O}_{K_0}^\times$.

Goal

Compute

$$A = \frac{\mathcal{O}^{\times}_{K_0^+}}{N_{K/K_0}\left(\mathcal{O}^{\times}_{K,1 \bmod m}\right)}$$

Define $\mathcal{O}^{*}_{K,1 \bmod \mathfrak{m}}$ to be the kernel of the natural map $\mathcal{O}^{\times}_{K} \to (\mathcal{O}_K/\mathfrak{m})^{\times}$.

$\mathcal{O}^{*}_{K,1 \bmod \mathfrak{m}}$

```
? OKstar = ag_OKstar_of(K);
? OKmstar = ag_OKmstar_of(K, m = 2);
? H_OKm1star = agmor_kernel(OKstar, OKmstar, ((x)->x))[1];
```

Exercise: Compute the HNF of $N_{K/K_0}(\mathcal{O}^{*}_{K,1 \bmod \mathfrak{m}}) \subseteq \mathcal{O}^{\times}_{K_0}$.
Define $\mathcal{O}^{\times}_{K_0^+} \subseteq \mathcal{O}^{\times}_{K_0}$ to be the totally positive units of K_0.
Exercise: Compute the HNF of $\mathcal{O}^{\times}_{K_0^+} \subseteq \mathcal{O}^{\times}_{K_0}$.

To get the quotient:
use `ag_quogrp_oftwosubgroups(SubGrA, SubGrB, Gr)`.

Computing $\dfrac{\mathcal{O}^{\times}_{K_0^+}}{N_{K/K_0}(\mathcal{O}^{\times}_{K,1 \bmod m})}$

```
? K0 = bnfinit(z^2 + 292*z + 14439);
? K0plus = bnrinit(K0, [1, [1, 1]], 1);
? ClK0plus = ag_clgp_of( K0plus );
? KoverK0 = rnfinit(K0, y^2 - z);
? K = bnfinit(nfinit(KoverK0));
?
```

To get the quotient:
use `ag_quogrp_oftwosubgroups(SubGrA, SubGrB, Gr)`.

Computing $\frac{\mathcal{O}^{\times}_{K_0^+}}{N_{K/K_0}\left(\mathcal{O}^{\times}_{K,1 \bmod m}\right)}$

```
? K0 = bnfinit(z^2 + 292*z + 14439);
? K0plus = bnrinit(K0, [1, [1, 1]], 1);
? ClK0plus = ag_clgp_of( K0plus );
? KoverK0 = rnfinit(K0, y^2 - z);
? K = bnfinit(nfinit(KoverK0));
? OK0star = ag_OKstar_of(K0);
?
```

To get the quotient:
use `ag_quogrp_oftwosubgroups(SubGrA, SubGrB, Gr)`.

Computing $\frac{\mathcal{O}_{K_0^+}^\times}{N_{K/K_0}(\mathcal{O}_{K,1 \bmod m}^\times)}$

```
? K0 = bnfinit(z^2 + 292*z + 14439);
? K0plus = bnrinit(K0, [1, [1, 1]], 1);
? ClK0plus = ag_clgp_of( K0plus );
? KoverK0 = rnfinit(K0, y^2 - z);
? K = bnfinit(nfinit(KoverK0));
? OK0star = ag_OKstar_of(K0);
? H_OK0plusstar = [2, 0; 0, 2];
?
```

To get the quotient:
use `ag_quogrp_oftwosubgroups(SubGrA, SubGrB, Gr)`.

Computing $\dfrac{\mathcal{O}^{\times}_{K_0^+}}{N_{K/K_0}(\mathcal{O}^{\times}_{K,1 \bmod m})}$

```
? K0 = bnfinit(z^2 + 292*z + 14439);
? K0plus = bnrinit(K0, [1, [1, 1]], 1);
? ClK0plus = ag_clgp_of( K0plus );
? KoverK0 = rnfinit(K0, y^2 - z);
? K = bnfinit(nfinit(KoverK0));
? OK0star = ag_OKstar_of(K0);
? H_OK0plusstar = [2, 0; 0, 2];
? H_relnorm_imageof_OK1star = [2, 0; 0, 6];
?
```

To get the quotient:
use `ag_quogrp_oftwosubgroups(SubGrA, SubGrB, Gr)`.

Computing $\frac{\mathcal{O}^{\times}_{K_0^+}}{N_{K/K_0}(\mathcal{O}^{\times}_{K,1 \bmod m})}$

```
? K0 = bnfinit(z^2 + 292*z + 14439);
? K0plus = bnrinit(K0, [1, [1, 1]], 1);
? ClK0plus = ag_clgp_of( K0plus );
? KoverK0 = rnfinit(K0, y^2 - z);
? K = bnfinit(nfinit(KoverK0));
? OK0star = ag_OKstar_of(K0);
? H_OK0plusstar = [2, 0; 0, 2];
? H_relnorm_imageof_OK1star = [2, 0; 0, 6];
? coker = ag_quogrp_oftwosubgroups(
             H_relnorm_imageof_OK1star,
             H_OK0plusstar,
             OK0star);
```

List of functions so far:

- `is_ag`
- `is_subgrp`
- `ag_mulbasis(Gr, B, M)`
- `ag_almostsnfofsubgrp(SubGr)`
- `ag_intsumofsubgrps(Gr, H1, H2)`
- `ag_intofsubgrps(Gr, H1, H2)`
- `ag_sumofsubgrps(Gr, H1, H2)`
- `ag_issubgrp(Gr, H1, H2)`
- `ag_grpext(c, eff, effinv, gee, geeinv)`