Number Fields – Sage versus Magma: Status Report

William Stein
University of Washington, Seattle

Sage Days 5: Clay Math Institute

Elements of Number Fields

1. All elements represented as absolute polys over $\mathbb{Q}$, though arbitrary towers of relative number fields are supported.
2. (J Mohler) Uses NTL $\mathbb{Z}[x]$ for all arithmetic (ZZ poly and denominator). Slightly slower than Magma, though not too bad. (timings use V2.13-10 Magma on Intel Core2 Linux)
3. (R Bradshaw) Special optimized class for quadratic fields, that is off today, and will be on after a coding sprint this week.

Sage and Magma basic arithmetic...

```
sage: K.<a> = NumberField(x^5 + 17*x^3 + 2*x^2 + 3*x -15)
sage: b = (a+1/3)^10; b
-766181/243*a^4 - 12095555/729*a^3 - 2411338/729*a^2 + 193
sage: time for _ in xrange(10^5): c=b*b
CPU times: user 1.56 s, sys: 0.04 s, total: 1.60 s
Wall time: 1.61
```

```
MAGMA:
> R<x> := PolynomialRing(RationalField());
> K<a> := NumberField(x^5 + 17*x^3 + 2*x^2 + 3*x -15);
> b := (a+1/3)^10; b;
1/59049*(-186181983*a^4 - 979739955*a^3 - 195318378*a^2 + 5
> time for i in [1..10^5] do c := b*b; end for;
Time: 0.390
```

Sage and Magma basic arithmetic... (bigger degree)

```
sage: K.<a> = NumberField(x^100 + 17*x^3 + 2*x^2 + 3*x - 15
sage: b = (a+1/3)^100
sage: time for _ in xrange(10^3): c=b*b
CPU times: user 0.91 s, sys: 0.00 s, total: 0.91 s
Wall time: 0.98
```

MAGMA:

```
> R<x> := PolynomialRing(RationalField());
> K<a> := NumberField(x^100 + 17*x^3 + 2*x^2 + 3*x -15);
> b := (a+1/3)^100;
> time for i in [1..10^3] do c := b*b; end for;
Time: 0.420
```

Sage and Magma basic arithmetic... (even bigger degree)

```
sage: K.<a> = NumberField(x^500 + 17*x^3 + 2*x^2 + 3*x - 15
sage: b = (a+1/3)^500
sage: time for _ in xrange(10^2): c=b*b
CPU times: user 2.17 s, sys: 0.01 s, total: 2.18 s
Wall time: 2.18
```

MAGMA:

```
> R<x> := PolynomialRing(RationalField());
> K<a> := NumberField(x^500 + 17*x^3 + 2*x^2 + 3*x -15);
> b := (a+1/3)^500;
> time for i in [1..10^2] do c := b*b; end for;
Time: 0.450
```

FLINT

FLINT will make Sage faster for general number fields arithmetic...

1. Now in Sage, but only in a testing/development form.
2. See Bill Hart's talk tonight.

Sage and Magma Quadratic field arithmetic...

Thanks to Robert Bradshaw, quadratic field arithmetic in Sage is (about to be!) faster in Sage than in PARI and Magma:

```
sage: K.<a> = QuadraticField(7)
sage: b = (2/3)*a + 5/8
sage: time for _ in xrange(10^5): c=b*b + b*b
CPU times: user 0.31 s, sys: 0.00 s, total: 0.31 s
```

```
MAGMA:
> K<a> := QuadraticField(7);
> b := (2/3)*a + 5/8;
> time for i in [1..10^5] do c := b*b+b*b; end for;
Time: 0.610
```

```
PARI:
? b = Mod((2/3)*a + 5/8, a^2 -7); gettime;
? for(i=0,10^5,c=b*b+b*b); gettime/1000.0
%6 = 0.673000000000000000000000000000000000
```

A relative number field arithmetic example...

Magma is *vastly* better than Sage in the example below, maybe because Sage chooses a horrible absolute poly and works modulo it:

```
sage: K.<a,b,c> = NumberField([x^2 + 1, x^3 - 2, x^2 - 5])
# a^2 == -1, b^3 == 2, c^2 == 5
sage: d = (a+b+c)^5; d
(140*b^2 + (80*c + 10)*b + 40*c + 76)*a + (20*c + 2)*b^2 +
sage: time for _ in xrange(10^3): c=d*d + d*d
CPU times: user 1.42 s, sys: 0.04 s, total: 1.46 s
sage: d.polynomial()      # absolute poly rep
535290512/29215513833*x^11 + 186767562/9738504611*x^10 - .
```

```
MAGMA:
> K<a,b,c> := NumberField([x^2 + 1, x^3 - 2, x^2 - 5]);
> d := (a+b+c)^5;
(140*b^2 + (80*c + 10)*b + (40*c + 76))*a + (20*c + 2)*b^2
> time for i in [1..10^3] do c := d*d + d*d; end for;
Time: 0.060
```

Class Group Computation

1. Easy to set a global proof True and proof False flag for all number field functions (me and David Roe).
2. The default is proof True.
3. Sage uses PARI for its class group computations.
4. Class group computations in Sage are already usually faster than in Magma (Bill Hart).

Class Group Examples...

```
sage: K.<a> = NumberField(x^3 + 1838)
sage: C = K.class_group(); C
Class group of order 27 with structure C9 x C3 of Number Field i
sage: C.gens()
[Fractional ideal class (50, a - 8) of Number Field in a with de
 Fractional ideal class (26, a - 2) of Number Field in a with de
sage: I = C.0; J = C.1
sage: I
Fractional ideal class (50, a - 8) of Number Field in a with def
sage: I^9
Trivial principal fractional ideal class of Number Field in a wi
sage: J^2
Fractional ideal class (6, a^2 - 2*a - 2) of Number Field in a w
```

Class Groups: Sage versus Magma without Proof

Timings from Bill Hart (see sage-devel):
Proof = False

```
deg, bits, iter   :    Pari    Magma

2,    10,    10000 :     27s      86s
2,    20,     2000 :     25s     142s
2,    30,      300 :     25s     115s
2,    40,      100 : 50-80s     348s
```

```
                                                        Pari   Magma
x^2 - 678650306441557*x + 232491039415161   :     5.81s   243s
x^2 + 4003599118850 97*x + 1023437292772615 :     8.33s   ....
x^2 + 788021445418312*x + 62108142321374    :   136.??s   ....
x^2 + 31010400109008 1*x + 526420096868844  :     2.18s   156s
x^2 + 29148692184930*x + 697845351766239    :     1.45s    63.5s
```

Class Groups: Sage versus Magma without Proof (degree 3)

Timings from Bill Hart (see sage-devel):
Proof = False

```
deg, bits, iter   :    Pari    Magma
3,    5,    5000   :     15s      28s
3,   10,    1000   :     23s      26s
3,   15,     100   : 15-20s   14-39s
```

```
                                                        Pari      Magma
x^3 - 327878*x^2 - 1038886*x + 711300          :    1.12s      10.6s
x^3 + 244636*x^2 + 536860*x - 435475           :    0.545s      5.25s
x^3 - 840752*x^2 + 979860*x - 141846           :    2.38s      26.15s
x^3 - 994421*x^2 - 866767*x - 513979           :    3.53s      35.5s
x^3 - 649099*x^2 + 997454*x + 787504           :    0.332s      3.81s
x^3 + 33354817*x^2 - 17000985*x - 4985420      :  10.2s      109s
x^3 + 16766060*x^2 + 491009*x - 25868840       :    8.24s     111s
x^3 - 3069789*x^2 + 31777984*x - 24323311      :    7.93s     100s
x^3 + 11823123*x^2 + 20775154*x - 20239321     :  17.6s      192s
x^3 - 26450070*x^2 + 10700466*x - 27026226     :  38.7s       ....
```

Class Groups: Sage versus Magma with Proof

Timings from Bill Hart (see sage-devel):
Proof = True

```
Degree, Bits, Iterations : Pari   Magma
2,      10,   5000       : 29s    72s
2,      15,   100        : 19-38s 9-24s

x^2 + 16537*x - 774810   :  0.088s 4.89s
x^2 - 88874*x - 377973   :  1.35s  7.64s
x^2 - 807645*x + 521195  : 46.0s  64.9s
x^2 + 298895*x + 178437  : 20.9s  12.5s
x^2 - 980711*x + 369932  : 92.2s  94.2s
```

Relative Number Fields

The interface now makes sense (it really sucked before). Also, many nice convenience functions for moving between absolute and relative extensions, vector spaces, etc.

```
sage: K.<a,b,c> = NumberField([x^2 + 1, x^2 + 3, x^2 + 5])
sage: (a+b+c).matrix()
[b + c     1]
[   -1 b + c]
sage: L = K.base_field(); M = L.base_field()
sage: (a+b+c).norm(L)
2*c*b + -7
sage: (a+b+c).norm(M)
-11
sage: z = (a+b+c).norm(L); z.norm(M)
-11
sage: R.<x> = K[]
sage: f = (x^3 - (a+b)*x + c)*(x-2*a)*(x^2 - b); f
x^6 + ((-2)*a)*x^5 + ((-1)*a + (-2)*b)*x^4 + ...
sage: f.factor()
(x + (-2)*a) * (x^2 + (-1)*b) * (x^3 + ((-1)*a + (-1)*b)*x + c)
```

Embeddings

```
sage: K.<a,b,c> = NumberField([x^2 + 1, x^2 + 3, x^2 + 5])
sage: K.embeddings(L)
[Relative number field endomorphism of Number Field in a with de
  Defn: a |--> a         b |--> b          c |--> c,
...   Relative number field endomorphism of Number Field in a wi
  Defn: a |--> (-1)*a    b |--> (-1)*b     c |--> c]
sage: f = K.embeddings(L)[-1];   f(a+b+c+2/3)
(-1)*a + (-1)*b + c + 2/3

sage: K.<a> = NumberField(x^3 - 2)
sage: L = K.galois_closure()
sage: K.embeddings(L)
sage: K.<a> = NumberField(x^3 - 2)
sage: L = K.galois_closure()
sage: K.embeddings(L)   # 3 morphisms output; L can be CC, CDF,
[Ring morphism:
  From: Number Field in a with defining polynomial x^3 - 2
  To:   Number Field in a1 with defining polynomial x^6 + 40*x^3
  Defn: a |--> 1/84*a1^4 + 13/42*a1,  ...
```

Orders

```
sage: K.<a> = NumberField(x^3 - 2)
sage: O2 = K.order(2*a); O2
Order with module basis 1, 2*a, 4*a^2 in Number Field in a with
sage: O3 = K.order([12*a^2, 24]); O3
Order with module basis 1, 288*a, 12*a^2 in Number Field in a wi
sage: O3.index_in(O2)
432
sage: a in O2
False
sage: O2.intersection(O3)
Order with module basis 1, 288*a, 12*a^2 in Number Field in a wi

sage: time NumberField(x^19 + 23*x + 12, 'a').maximal_order()
CPU times: user 0.04 s, sys: 0.02 s, total: 0.05 s
Wall time: 0.06
Order with module basis 1, 1/6*a^18 + 1/6*a^17 + 1/6*a^16 + ...
```

User always see everything in terms of the number field basis, unlike in Magma.

Number Fields: Status Report

1. Doctest coverage is now better. I brought it to 100%, but then Robert and I wrote a lot of new code...
2. Aside from speed issues mentioned above, there is a still much general work to be done on number fields.
3. Over 50 messages in sage-devel recently like this:

   ```
   From: Bill Hart to sage-devel
   Subject: [sage-devel] Re: number fields
   My personal opinion is that SAGE should ...
   ```

4. Much work in this direction hasn't begun yet: $\overline{\mathbb{Q}}$, completions, embeddings, linear algebra, order pseudo-basis
5. Focus right now is in having a sane interface that has usable speed, and at least provides most of the functionality of Magma's number fields package **as soon as possible** (!), so that we can port code and worry about making things faster.

Thanks. Questions?

Now is the time to report bugs, concerns, issues, etc., with number fields!