Quaternion algebras

A GP tutorial

A. Page

Inria/Université de Bordeaux/IMB

09/01/2025

Institut Pascal, Saclay

Documentation

- refcard-nf.pdf p.3 : list of functions with a short description.
- users.pdf Section 3.14: introduction and detailed descriptions of the functions.
- in gp, `?11`: list of functions.
- in gp, `?functionname`: short description of the function.
- in gp, `??functionname`: long description of the function.

To record the commands we will type during the tutorial:

```
? \l quatalg.log
```

Hamilton quaternions

The **Hamilton quaternion algebra** $\mathbb{H}$ is

$$\mathbb{H} = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}ij$$

where $i^2 = j^2 = -1$ and $ji = -ij$.

It is a noncommutative division algebra.

Define

- $\overline{x_1 + x_2 i + x_3 j + x_4 ij} = x_1 - x_2 i - x_3 j - x_4 ij$ (involution);
- $\mathrm{trd}(w) = w + \overline{w} \in \mathbb{R}$ (reduced trace);
- $\mathrm{nrd}(w) = w\overline{w} \in \mathbb{R}_{\geq 0}$ (reduced norm).

Creation

We create an object representing $\mathbb{H}$ as follows.

```
? H = alginit(1.,1/2);
? algdim(H)
% = 4
? algisdivision(H)
% = 1
? algiscommutative(H)
% = 0
```

Elements

We represent elements of $\mathbb{H}$ by column vectors of 4 real numbers. Functions operating on algebras are of the form `algxxx(al,...)`, and we can omit the `al` to mean $\mathbb{H}$.

```
? w = [Pi,2,sqrt(3),-7]~
% = [3.1415926535, 2, 1.7320508075, -7]~
? algmul(,w,w)
% = [-46.130395, 12.566370, 10.882796, -43.982297]~
? alginv(,w)
% = [0.047694, -0.030363, -0.026295, 0.106270]~
? alginvol(,w)
% = [3.1415926535, -2, -1.7320508075, 7]~
? algtrace(,w)
% = 6.2831853071795864769252867665590057684
? algnorm(,w)
% = 65.869604401089358618834490999876151135
```

Maps to matrix algebras

The algebra has two natural embeddings into matrix algebras, accessible via `algtomatrix`:

- an embedding $\mathbb{H} \to M_2(\mathbb{C})$ (default)
- an embedding $\mathbb{H} \to M_4(\mathbb{R})$ (`flag`=1)

```
? W = algtomatrix(,w)
% =
[3.1415926535 + 2*I -1.7320508075 + 7*I]
[1.7320508075 + 7*I 3.14159265358 - 2*I]
? trace(W) - algtrace(,w)
% = 0.E-37
? matdet(W) - algnorm(,w)
% = 0.E-36 + 0.E-37*I
```

Maps to matrix algebras

The algebra has two natural embeddings into matrix algebras, accessible via `algtomatrix`:

- an embedding $\mathbb{H} \to M_2(\mathbb{C})$ (default)
- an embedding $\mathbb{H} \to M_4(\mathbb{R})$ (`flag`=1)

```
? W2 = algtomatrix(,w,1)
% =
[3.141592653 -2 -1.732050807]
[2 3.141592653 7 1.732050807]
[1.732050807 -7 3.1415926535 -2]
[-7 -1.7320508075 2 3.1415926535]
? trace(W2) - 2*algtrace(,w)
% = -4.7019774032891500032 E-38
? matdet(W2) - algnorm(,w)^2
% = 2.407412430484044816 E-35
```

$\mathrm{SU}_2(\mathbb{C})$

In particular we recover the isomorphism from the reduced norm 1 group $\mathbb{H}^1 \to \mathrm{SU}_2(\mathbb{C})$.

```
? u = w/sqrt(algnorm(,w))
% = [0.387085, 0.246426, 0.213411, -0.862492]~
? U = algtomatrix(,u)
% =
[0.387085 + 0.246426*I -0.213411 + 0.862492*I]
[0.213411 + 0.862492*I  0.387085 - 0.246426*I]
? exponent(conj(U)~ * U - matid(2))
% = -127
```

$SO_3(\mathbb{R})$

We also recover the isomorphism $\mathbb{H}^1/\{\pm 1\} \to SO_3(\mathbb{R})$

```
? C = alginvol(H);
? rot(w) = ((algtomatrix(,w,1)*C)^2)[^1,^1];
? R = rot(u)
% =
[-0.5788769485  0.7728982258 -0.2598649858]
[-0.5625370648 -0.6092399668 -0.5589085019]
[-0.5902995249 -0.1773555617  0.7874588723]
? exponent(R~*R - matid(3))
% = -126
```

Quaternion algebras

More generally, a **quaternion algebra** over a field K of characteristic not 2 is one of the form

$$(a,b)_K = K + Ki + Kj + Kij$$

with $i^2 = a$, $j^2 = b$ and $ji = -ij$, for some $a, b \in K^\times$.
It is a central simple algebra over K.

Define

- $\overline{x_1 + x_2 i + x_3 j + x_4 ij} = x_1 - x_2 i - x_3 j - x_4 ij$ (involution);
- $\mathrm{trd}(w) = w + \overline{w} \in K$ (reduced trace);
- $\mathrm{nrd}(w) = w\overline{w} \in K$ (reduced norm).
- $X^2 - \mathrm{trd}(w)X + \mathrm{nrd}(w) \in K[X]$ (reduced char. polynomial).

Creation

We create $(a, b)_K$ with `alginit`. Requirement: $a, b \in \mathbb{Z}_K$.

```
? nf = nfinit(y^4-y-1);
? al = alginit(nf,[-7,y]);
? algdim(al) \\dimension over nf
% = 4
? algdim(al,1) \\dimension over Q
% = 16
? algiscommutative(al)
% = 0
? algissimple(al)
% = 1
```

We can recover the pair (a, b) that defines the algebra.

```
? [a,b] = algisquatalg(al)
% = [-7, y]
```

Operations on elements

Elements are internally represented on a $\mathbb{Q}$-basis. We can convert from and to the $1, i, j, ij$ basis with `algquattobasis` and `algbasistoquat`.

```
? z = algquattobasis(al, [-2,y,1+y,y/2]~)
% = [-7,-1,0,-7,-4,-5,0,-7,-1,0,0,-9/2,-3,0,0,7]~
? lift(algbasistoquat(al, alginvol(al, z)))
% = [-2, -y, -y - 1, -1/2*y]~
? algtrace(al, z)
% = -4
? algpoleval(al, algcharpoly(al,z), z)
% = [0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0]~
```

Maps to matrix algebras

The algebra A/K has two natural embeddings into matrix algebras, accessible via `algtomatrix`:

- an embedding $A \to M_2(L)$ where $L = K(\sqrt{a})$ (default)
- an embedding $A \to M_4(K)$ (`flag`=1)

```
? Z = algtomatrix(al,z); liftall(Z)
% =
[             y*x - 2  1/2*y^2*x + (y^2 + y)]
[-1/2*y*x + (y + 1)               -y*x - 2]
? trace(Z) - algtrace(al,z)
% = Mod(0, x^2 + 7)
? matdet(Z) - algnorm(al,z)
% = Mod(0, x^2 + 7)
```

Maps to matrix algebras

The algebra A/K has two natural embeddings into matrix algebras, accessible via `algtomatrix`:

- an embedding $A \to M_2(L)$ where $L = K(\sqrt{a})$ (default)
- an embedding $A \to M_4(K)$ (`flag`=1)

```
? Z2 = algtomatrix(al,z,1); matsize(Z2)
% = [16, 16]
? trace(Z2) - 2*nfelttrace(nf,algtrace(al,z))
% = 0
? matdet(Z2) - nfeltnorm(nf,algnorm(al,z))^2
% = 0
```

Ramification

Let v be a place of K. Ramification at v is defined according to the behaviour of the quaternion algebra $(a, b)_K \otimes_K K_v$:

- a quaternion algebra over $\mathbb{C}$ is isomorphic to $M_2(\mathbb{C})$ (split);
- q.a. over $\mathbb{R}$ is isomorphic to $M_2(\mathbb{R})$ (split) or $\mathbb{H}$ (ramified);
- q.a. over a p-adic field E is isomorphic to $M_2(E)$ (split) or a division algebra $\mathbb{H}_E$ (ramified).

Theorem

- *The ramification set is finite of even cardinality.*
- *Quaternion algebras are isomorphic if and only if they have the same ramification set.*
- *Every finite set of noncomplex places of even cardinality is the ramification set of some quaternion algebra.*

Computing ramification

We can test for ramification at a place with `algisramified`.

```
? algisramified(al, 1) \\1st place at infinity
% = 1
? pr = idealprimedec(nf,2)[1];
? algisramified(al, pr)
% = 0
```

We can test ramification without the algebra with `nfhilbert`.

```
? nfhilbert(nf, a, b, pr) \\Hilbert symbol
% = 1                      \\1=split, -1=ramified
```

We get the ramification set with `algramifiedplaces`.

```
? algramifiedplaces(al)
% = [1, [7, ... , 1, 1, ...]]
? algisdivision(al)
% = 1
```

Construction from ramification

We can construct a quaternion algebra from its ramification set with `alginit(nf,[PR,HI])` where `PR` is a vector of prime ideals and $\mathtt{HI} \in \{0,1\}^{r_1}$ specifies the ramified real places.

```
? al2 = alginit(nf, [[pr],[0,1]]);
? #algramifiedplaces(al2)
% = 2
? algisramified(al2,pr)
% = 1
? algisquatalg(al2)
% = [-21, -294*y^3 + 127]
```

Lattices and orders

Let A be a quaternion algebra over a number field K.
A **lattice** $L \subset A$ is a $\mathbb{Z}$-submodule generated by a $\mathbb{Q}$-basis of A.
An **order** $\mathcal{O} \subset A$ is a lattice that is also a subring (with unit).

Example: $\mathcal{O} = \mathbb{Z}_K + \mathbb{Z}_K i + \mathbb{Z}_K j + \mathbb{Z}_K ij$ if $a, b \in \mathbb{Z}_K$.

Given a lattice L, its **left order** (resp. right order) is

$$\mathcal{O}_l(L) = \{x \in A \mid xL \subseteq L\}, \text{ resp. } \mathcal{O}_r(L) = \{x \in A \mid Lx \subseteq L\}.$$

A **maximal order** is an order not properly contained in an order.
Maximal orders always exist but are not unique (for instance, most conjugates are distinct).

Integral basis

In PARI/GP, the $\mathbb{Q}$-basis representation is with respect to a $\mathbb{Z}$-basis $\omega_1, \ldots, \omega_n$ of a maximal order containing the non-maximal order $\mathbb{Z}_K + \mathbb{Z}_K i + \mathbb{Z}_K j + \mathbb{Z}_K ij$.
We check that it is an order.

```
? mt = algmultable(al);
? denominator(mt)
% = 1
```

We check that it is maximal from a formula for the discriminant $\det((\mathrm{Tr}(\omega_i \omega_j))_{1 \le i,j \le n})$.

```
? algdisc(al)
% = 20597843435782144
? D = idealnorm(nf, algramifiedplaces(al)[2]);
? 2^algdim(al,1) * (nf.disc^2 * D)^2
% = 20597843435782144
```

Ramification and maximal orders

Let $\mathcal{O} \subset A$ be a maximal order, and let $\mathfrak{p}$ be a prime ideal.

- If $\mathfrak{p}$ is split, then
$$\mathcal{O}/\mathfrak{p}\mathcal{O} \cong M_2(\mathbb{F}_\mathfrak{p}).$$
- If $\mathfrak{p}$ is ramified, then there exists a surjection
$$\mathcal{O}/\mathfrak{p}\mathcal{O} \to \mathcal{O}/\mathfrak{P} \cong \mathbb{L}$$
where $\mathbb{L}/\mathbb{F}_\mathfrak{p}$ is the quadratic extension and $\mathfrak{P} \subset \mathcal{O}$ is a two-sided ideal with $\mathfrak{P}^2 = \mathfrak{p}\mathcal{O}$.

In both cases, several such maps exist.

Mod $\mathfrak{p}$ splitting

We initialise a map $\mathcal{O}/\mathfrak{p}\mathcal{O} \to M_k(\mathbb{F}_q)$ as above with `algmodprinit`.

```
? pr3 = idealprimedec(nf,3)[1];
? pr3.f
% = 4
? modP3 = algmodprinit(al, pr3);
```

This map will be $\mathcal{O}/\mathfrak{p}_3\mathcal{O} \to M_2(\mathbb{F}_{3^4})$.

```
? pr7 = algramifiedplaces(al)[2];
? pr7.f
% = 1
? modP7 = algmodprinit(al, pr7);
```

This map will be $\mathcal{O}/\mathfrak{p}_7\mathcal{O} \to M_1(\mathbb{F}_{7^2})$.

Mod $\mathfrak{p}$ splitting

We then compute the image of an element with `algmodpr`.

```
? algmodpr(al, z, modP3)
% =
[x^3 + 2*x^2 + 2 x^3 + x^2 + 2*x + 2]
[  2*x^2 + x + 2          2*x^3 + x^2]
? algmodpr(al, z, modP7)
% =
[3*x + 3]
? t = algquattobasis(al,[0,1,2,1/7*y^3+1/7*y-2/7]~)
? algmodpr(al, t, modP7)
% =
[5*x + 6]
```

Mod $\mathfrak{p}$ splitting

We find preimages with `algmodprlift`.

```
? li1 = algmodprlift(al, [1,x;0,1], modP3)
% = [2,2,2,1,2,2,1,0,2,1,1,0,2,2,1,1]~
? algmodpr(al, li1, modP3)
% =
[1 x]
[0 1]
? li2 = algmodprlift(al, Mat(x), modP7)
% = [6,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1]~
? algmodpr(al, li2, modP7)
% =
[x]
```

Real and complex splitting

Splitting at infinite places is not implemented yet but is very easy in the quaternion case.

```
? quatembed(al,x,pl) =
{
  [... cf GP code file ...]
};
```

The first real place is ramified, yielding a map $A \to \mathbb{H}$.

```
? quatembed(al,z,1)
% = [-2, -1.916825, 0.234504, -0.815773]~
```

Real and complex splitting

The second real place is split, yielding a map $A \to M_2(\mathbb{R})$.

```
? quatembed(al,z,2)
% =
[0.453639 -3.824523]
[1.895127 -4.453639]
```

The third place is complex, yielding a map $A \to M_2(\mathbb{C})$.

```
? quatembed(al,z,3)
% =
[-4.735659 - 0.656479*I -0.576890 - 0.812000*I]
[ 2.119703 + 1.362221*I  0.735659 + 0.656479*I]
```

Eichler orders

Let $\mathfrak{N}$ be an ideal coprime to the discriminant and let $\mathcal{O}$ be a maximal order. We then have an isomorphism

$$\mathcal{O}/\mathfrak{N}\mathcal{O} \to M_2(\mathbb{Z}_K/\mathfrak{N}).$$

Let $\mathcal{O}_0(\mathfrak{N})$ denote the preimage of the set of upper-triangular matrices. This is an order, and an order of this form is called an **Eichler order of level $\mathfrak{N}$.**

A maximal order is an Eichler order of level 1.

Eichler order construction

We can obtain a basis for an Eichler order of given level with `algeichlerbasis`.

```
? eich = algeichlerbasis(al, Mat([pr3,3]))
% =
[1     0   0   0   0   0   0   0   0]
   ...
[0    27   0   0   0  20   9   6  25]
[0     0  27   0   0  26   8   0   2]
[0     0   0  27   0  17   5  13   7]
[0     0   0   0  27  25  24   2  17]
[0     0   0   0   0   1   0   0   0]
[0     0   0   0   0   0   1   0   0]
[0     0   0   0   0   0   0   1   0]
[0     0   0   0   0   0   0   0   1]
```

Lattice representation

We represent a lattice $L \subset A$ by a pair $[H, t]$ where

- $H \in M_n(\mathbb{Z})$ is upper-triangular nonsingular, and
- $t \in \mathbb{Q}_{>0}$,

representing the lattice $t \cdot H \cdot \mathbb{Z}^n$.

It is recommended to use H in Hermite normal form and primitive (GCD of all coefficients is 1). In this case, the representation is unique.

The prefix for functions working with lattices in algebras is `alglat`.

Lattice creation

We obtain a representation as above from an arbitrary basis of a lattice with `alglathnf`.

```
? lat1 = alglathnf(al,z);
? lat1[2]
% = 1/2
```

We created the lattice $L_1 = z\mathcal{O}$.

```
? lat2 = alglathnf(al,eich);
? lat2[2]
% = 1
```

We created the lattice $L_2 = \mathcal{O}_0(\mathfrak{p}_3^3)$.

Lattice operations

We can perform elementary operations on lattices

- `alglatadd` for $L_1 + L_2$,
- `alglatinter` for $L_1 \cap L_2$,
- `alglatmul` for $L_1 \cdot L_2$.

The generalised index

$$[L_2 : L_1] = \frac{[L_2 : L_1 \cap L_2]}{[L_1 : L_1 \cap L_2]} \in \mathbb{Q}$$

is computed with `alglatindex`.

```
? alglatsubset(al,lat1,lat2)
% = 0
? alglatsubset(al,lat2,lat1)
% = 0
? alglatindex(al,lat2,lat1)
% = 34828517376/12115625041
```

Lattice operations

The **left transporter** from L_1 to L_2 is the lattice

$$\{x \in A \mid x \cdot L_1 \subset L_2\},$$

and is computed by `alglatlefttransporter`.
This allows us to compute $\mathcal{O}_l(L)$, and in particular to check whether a lattice is an order.

```
? alglatlefttransporter(al,lat2,lat2) == lat2
% = 1
```

We can also use it for inversion.

```
? triv = alglathnf(al,matid(16));
? lat1inv = alglatlefttransporter(al,lat1,triv);
? alglatmul(al,lat1inv,lat1) == triv
% = 1
```

More general central simple algebras

The Pari package can actually deal with arbitrary central simple algebras over number fields.

- quaternion algebras $\rightsquigarrow$ cyclic algebras
- ramification $\rightsquigarrow$ Hasse invariants
- ...

Read the documentation for more details!

Have fun with GP !