Algebraic Number Theory

(PARI-GP version 2.13.0)

Binary Quadratic Forms

create $ax^2+bxy+cy^2$ (distance d)	`Qfb(a,b,c,{d})`
reduce x ($s=\sqrt{D}$, $l=\lfloor s\rfloor$)	`qfbred(x,{flag},{D},{l},{s})`
return $[y,g]$, $g\in SL_2(\mathbf{Z})$, $y=g\cdot x$ reduced	`qfbredsl2(x)`
composition of forms	`x*y` or `qfbnucomp(x,y,l)`
n-th power of form	`x^n` or `qfbnupow(x,n)`
composition without reduction	`qfbcompraw(x,y)`
n-th power without reduction	`qfbpowraw(x,n)`
prime form of disc. x above prime p	`qfbprimeform(x,p)`
class number of disc. x	`qfbclassno(x)`
Hurwitz class number of disc. x	`qfbhclassno(x)`
solve $Q(x,y)=n$ in integers	`qfbsolve(Q,n)`

Quadratic Fields

quadratic number $\omega=\sqrt{x}$ or $(1+\sqrt{x})/2$	`quadgen(x)`
minimal polynomial of ω	`quadpoly(x)`
discriminant of $\mathbf{Q}(\sqrt{x})$	`quaddisc(x)`
regulator of real quadratic field	`quadregulator(x)`
fundamental unit in real $\mathbf{Q}(\sqrt{D})$	`quadunit(D,{'w})`
class group of $\mathbf{Q}(\sqrt{D})$	`quadclassunit(D,{flag},{t})`
Hilbert class field of $\mathbf{Q}(\sqrt{D})$	`quadhilbert(D,{flag})`
... using specific class invariant ($D<0$)	`polclass(D,{inv})`
ray class field modulo f of $\mathbf{Q}(\sqrt{D})$	`quadray(D,f,{flag})`

General Number Fields: Initializations

The number field $K=\mathbf{Q}[X]/(f)$ is given by irreducible $f\in\mathbf{Q}[X]$. We denote $\theta=\bar{X}$ the canonical root of f in K. A *nf* structure contains a maximal order and allows operations on elements and ideals. A *bnf* adds class group and units. A *bnr* is attached to ray class groups and class field theory. A *rnf* is attached to relative extensions L/K.

init number field structure *nf*	`nfinit(f,{flag})`
known integer basis B	`nfinit([f,B])`
order maximal at $vp=[p_1,\dots,p_k]$	`nfinit([f,vp])`
order maximal at all $p\le P$	`nfinit([f,P])`
certify maximal order	`nfcertify(nf)`
nf members:	
a monic $F\in\mathbf{Z}[X]$ defining K	`nf.pol`
number of real/complex places	`nf.r1/r2/sign`
discriminant of *nf*	`nf.disc`
primes ramified in *nf*	`nf.p`
T_2 matrix	`nf.t2`
complex roots of F	`nf.roots`
integral basis of $\mathbf{Z}_K$ as powers of θ	`nf.zk`
different/codifferent	`nf.diff`, `nf.codiff`
index $[\mathbf{Z}_K:\mathbf{Z}[X]/(F)]$	`nf.index`
recompute *nf* using current precision	`nfnewprec(nf)`
init relative *rnf* $L=K[Y]/(g)$	`rnfinit(nf,g)`
init *bnf* structure	`bnfinit(f,1)`
bnf members: same as *nf*, plus	
underlying *nf*	`bnf.nf`
class group, regulator	`bnf.clgp`, `bnf.reg`
fundamental/torsion units	`bnf.fu`, `bnf.tu`
add S-class group and units, yield *bnf*S	`bnfsunit(bnf,S)`
init class field structure *bnr*	`bnrinit(bnf,m,{flag})`
bnr members: same as *bnf*, plus	
underlying *bnf*	`bnr.bnf`
big ideal structure	`bnr.bid`
modulus m	`bnr.mod`
structure of $(\mathbf{Z}_K/m)^*$	`bnr.zkst`

Fields, subfields, embeddings

Defining polynomials, embeddings

smallest poly defining $f=0$ (slow)	`polredabs(f,{flag})`
small poly defining $f=0$ (fast)	`polredbest(f,{flag})`
random Tschirnhausen transform of f	`poltschirnhaus(f)`
$\mathbf{Q}[t]/(f)\subset\mathbf{Q}[t]/(g)$? Isomorphic?	`nfisincl(f,g)`, `nfisisom`
reverse polmod $a=A(t)$ mod $T(t)$	`modreverse(a)`
compositum of $\mathbf{Q}[t]/(f)$, $\mathbf{Q}[t]/(g)$	`polcompositum(f,g,{flag})`
compositum of $K[t]/(f)$, $K[t]/(g)$	`nfcompositum(nf,f,g,{flag})`
splitting field of K (degree divides d)	`nfsplitting(nf,{d})`
signs of real embeddings of x	`nfeltsign(nf,x,{pl})`
complex embeddings of x	`nfeltembed(nf,x,{pl})`
$T\in K[t]$, # of real roots of $\sigma(T)\in R[t]$	`nfpolsturm(nf,T,{pl})`

Subfields, polynomial factorization

subfields (of degree d) of *nf*	`nfsubfields(nf,{d})`
maximal subfields of *nf*	`nfsubfieldsmax(nf)`
maximal CM subfield of *nf*	`nfsubfieldscm(nf)`
d-th degree subfield of $\mathbf{Q}(\zeta_n)$	`polsubcyclo(n,d,{v})`
roots of unity in *nf*	`nfrootsof1(nf)`
roots of g belonging to *nf*	`nfroots(nf,g)`
factor g in *nf*	`nffactor(nf,g)`

Linear and algebraic relations

poly of degree $\le k$ with root $x\in\mathbf{C}$	`algdep(x,k)`
alg. dep. with pol. coeffs for series s	`seralgdep(s,x,y)`
small linear rel. on coords of vector x	`lindep(x)`

Basic Number Field Arithmetic (nf)

Number field elements are `t_INT`, `t_FRAC`, `t_POL`, `t_POLMOD`, or `t_COL` (on integral basis `nf.zk`).

Basic operations

$x+y$	`nfeltadd(nf,x,y)`
$x\times y$	`nfeltmul(nf,x,y)`
x^n, $n\in\mathbf{Z}$	`nfeltpow(nf,x,n)`
x/y	`nfeltdiv(nf,x,y)`
$q=x\backslash/y$:= `round`(x/y)	`nfeltdiveuc(nf,x,y)`
$r=x\%y := x-(x\backslash/y)y$	`nfeltmod(nf,x,y)`
... $[q,r]$ as above	`nfeltdivrem(nf,x,y)`
reduce x modulo ideal A	`nfeltreduce(nf,x,A)`
absolute trace $\mathrm{Tr}_{K/\mathbf{Q}}(x)$	`nfelttrace(nf,x)`
absolute norm $\mathrm{N}_{K/\mathbf{Q}}(x)$	`nfeltnorm(nf,x)`

Multiplicative structure of K^*; $K^*/(K^*)^n$

valuation $v_{\mathfrak{p}}(x)$	`nfeltval(nf,x,pr)`
... write $x=\pi^{v_{\mathfrak{p}}(x)}y$	`nfeltval(nf,x,pr,&y)`
quadratic Hilbert symbol (at $\mathfrak{p}$)	`nfhilbert(nf,a,b,{pr})`
b such that $xb^n=v$ is small	`idealredmodpower(nf,x,n)`

Maximal order and discriminant

integral basis of field $\mathbf{Q}[x]/(f)$	`nfbasis(f)`
field discriminant of $\mathbf{Q}[x]/(f)$	`nfdisc(f)`
... and factorization	`nfdiscfactors(f)`
express x on integer basis	`nfalgtobasis(nf,x)`
express element x as a polmod	`nfbasistoalg(nf,x)`

Dedekind Zeta Function ζ_K, Hecke L series

$R=[c,w,h]$ in initialization means we restrict $s\in\mathbf{C}$ to domain $|\Re(s)-c|<w$, $|\Im(s)|<h$; $R=[w,h]$ encodes $[1/2,w,h]$ and $[h]$ encodes $R=[1/2,0,h]$ (critical line up to height h).

ζ_K as Dirichlet series, $N(I)<b$	`dirzetak(nf,b)`
init $\zeta_K^{(k)}(s)$ for $k\le n$	`L = lfuninit(bnf,R,{n=0})`
compute $\zeta_K(s)$ (n-th derivative)	`lfun(L,s,{n=0})`
compute $\Lambda_K(s)$ (n-th derivative)	`lfunlambda(L,s,{n=0})`
init $L_K^{(k)}(s,\chi)$ for $k\le n$	`L = lfuninit([bnr,chi],R,{n=0})`
compute $L_K(s,\chi)$ (n-th derivative)	`lfun(L,s,{n})`
Artin root number of K	`bnrrootnumber(bnr,chi,{flag})`
$L(1,\chi)$, for all χ trivial on H	`bnrL1(bnr,{H},{flag})`

Class Groups & Units (bnf, bnr)

Class field theory data $a_1,\{a_2\}$ is usually *bnr* (ray class field), *bnr*, H (congruence subgroup) or *bnr*, χ (character on `bnr.clgp`). Any of these define a unique abelian extension of K.

units / S-units	`bnfunits(bnf,{S})`
remove GRH assumption from *bnf*	`bnfcertify(bnf)`
expo. of ideal x on class gp	`bnfisprincipal(bnf,x,{flag})`
expo. of ideal x on ray class gp	`bnrisprincipal(bnr,x,{flag})`
expo. of x on fund. units	`bnfisunit(bnf,x)`
... on S-units, U is `bnfunits(bnf,S)`	`bnfisunit(bnfs,x,U)`
signs of real embeddings of `bnf.fu`	`bnfsignunit(bnf)`
narrow class group	`bnfnarrow(bnf)`

Class Field Theory

ray class number for modulus m	`bnrclassno(bnf,m)`
discriminant of class field	`bnrdisc(a1,{a2})`
ray class numbers, l list of moduli	`bnrclassnolist(bnf,l)`
discriminants of class fields	`bnrdisclist(bnf,l,{arch},{flag})`
decode output from `bnrdisclist`	`bnfdecodemodule(nf,fa)`
is modulus the conductor?	`bnrisconductor(a1,{a2})`
is class field (bnr,H) Galois over K^G	`bnrisgalois(bnr,G,H)`
action of automorphism on `bnr.gen`	`bnrgaloismatrix(bnr,aut)`
apply `bnrgaloismatrix` M to H	`bnrgaloisapply(bnr,M,H)`
characters on `bnr.clgp` s.t. $\chi(g_i)=e(v_i)$	`bnrchar(bnr,g,{v})`
conductor of character χ	`bnrconductor(bnr,chi)`
conductor of extension	`bnrconductor(a1,{a2},{flag})`
conductor of extension $K[Y]/(g)$	`rnfconductor(bnf,g)`
canonical projection $\mathrm{Cl}_F\to\mathrm{Cl}_f$, $f\mid F$	`bnrmap`
Artin group of extension $K[Y]/(g)$	`rnfnormgroup(bnr,g)`
subgroups of *bnr*, index <= b	`subgrouplist(bnr,b,{flag})`
class field defined by $H<\mathrm{Cl}_f$	`bnrclassfield(bnr,H)`
... low level equivalent, prime degree	`rnfkummer(bnr,H)`
same, using Stark units (real field)	`bnrstark(bnr,sub,{flag})`
is a an n-th power in K_v ?	`nfislocalpower(nf,v,a,n)`
cyclic L/K satisf. local conditions	`nfgrunwaldwang(nf,P,D,pl)`

© 2020 Karim Belabas. Permissions on back. v2.37

Logarithmic class group

logarithmic ℓ-class group	bnflog(bnf, ℓ)
$[\tilde{e}(F_v/Q_p), \tilde{f}(F_v/Q_p)]$	bnflogef(bnf, pr)
$\exp\deg_F(A)$	bnflogdegree(bnf, A, ℓ)
is ℓ-extension L/K locally cyclotomic	rnfislocalcyclo(rnf)

Ideals: elements, primes, or matrix of generators in HNF

is id an ideal in nf ?	nfisideal(nf, id)
is x principal in bnf ?	bnfisprincipal(bnf, x)
give $[a,b]$, s.t. $a\mathbf{Z}_K + b\mathbf{Z}_K = x$	idealtwoelt($nf, x, \{a\}$)
put ideal a ($a\mathbf{Z}_K + b\mathbf{Z}_K$) in HNF form	idealhnf($nf, a, \{b\}$)
norm of ideal x	idealnorm(nf, x)
minimum of ideal x (direction v)	idealmin(nf, x, v)
LLL-reduce the ideal x (direction v)	idealred($nf, x, \{v\}$)

Ideal Operations

add ideals x and y	idealadd(nf, x, y)
multiply ideals x and y	idealmul($nf, x, y, \{flag\}$)
intersection of ideal x with Q	idealdown(nf, x)
intersection of ideals x and y	idealintersect($nf, x, y, \{flag\}$)
n-th power of ideal x	idealpow($nf, x, n, \{flag\}$)
inverse of ideal x	idealinv(nf, x)
divide ideal x by y	idealdiv($nf, x, y, \{flag\}$)
Find $(a,b) \in x \times y$, $a+b=1$	idealaddtoone($nf, x, \{y\}$)
coprime integral A, B such that $x = A/B$	idealnumden(nf, x)

Primes and Multiplicative Structure

check whether x is a maximal ideal	idealismaximal(nf, x)
factor ideal x in $\mathbf{Z}_K$	idealfactor(nf, x)
expand ideal factorization in K	idealfactorback($nf, f, \{e\}$)
is ideal A an n-th power ?	idealispower(nf, A, n)
expand elt factorization in K	nffactorback($nf, f, \{e\}$)
decomposition of prime p in $\mathbf{Z}_K$	idealprimedec(nf, p)
valuation of x at prime ideal pr	idealval(nf, x, pr)
weak approximation theorem in nf	idealchinese(nf, x, y)
$a \in K$, s.t. $v_{\mathfrak{p}}(a) = v_{\mathfrak{p}}(x)$ if $v_{\mathfrak{p}}(x) \neq 0$	idealappr(nf, x)
$a \in K$ such that $(a \cdot x, y) = 1$	idealcoprime(nf, x, y)
give bid =structure of $(\mathbf{Z}_K/id)^*$	idealstar($nf, id, \{flag\}$)
structure of $(1+\mathfrak{p})/(1+\mathfrak{p}^k)$	idealprincipalunits(nf, pr, k)
discrete log of x in $(\mathbf{Z}_K/bid)^*$	ideallog(nf, x, bid)
idealstar of all ideals of norm $\leq b$	ideallist($nf, b, \{flag\}$)
add Archimedean places	ideallistarch($nf, b, \{ar\}, \{flag\}$)
init modpr structure	nfmodprinit($nf, pr, \{v\}$)
project t to $\mathbf{Z}_K/pr$	nfmodpr($nf, t, modpr$)
lift from $\mathbf{Z}_K/pr$	nfmodprlift($nf, t, modpr$)

Galois theory over Q

conjugates of a root θ of nf	nfgaloisconj($nf, \{flag\}$)
apply Galois automorphism s to x	nfgaloisapply(nf, s, x)
Galois group of field $\mathbf{Q}[x]/(f)$	polgalois(f)
initializes a Galois group structure G	galoisinit($pol, \{den\}$)
character table of G	galoischartable(G)
conjugacy classes of G	galoisconjclasses(G)
$\det(1-\rho(g)T)$, χ character of ρ	galoischarpoly($G, \chi, \{o\}$)
$\det(\rho(g))$, χ character of ρ	galoischardet($G, \chi, \{o\}$)
action of p in nfgaloisconj form	galoispermtopol($G, \{p\}$)
identify as abstract group	galoisidentify(G)
export a group for GAP/MAGMA	galoisexport($G, \{flag\}$)
subgroups of the Galois group G	galoissubgroups(G)
is subgroup H normal?	galoisisnormal(G, H)

Algebraic Number Theory

(PARI-GP version 2.13.0)

subfields from subgroups	galoissubfields($G, \{flag\}, \{v\}$)
fixed field	galoisfixedfield($G, perm, \{flag\}, \{v\}$)
Frobenius at maximal ideal P	idealfrobenius(nf, G, P)
ramification groups at P	idealramgroups(nf, G, P)
is G abelian?	galoisisabelian($G, \{flag\}$)
abelian number fields/$\mathbf{Q}$	galoissubcyclo(N,H,{flag},{v})

The galpol package

query the package: polynomial	galoisgetpol(a,b,{s})
...: permutation group	galoisgetgroup(a,b)
...: group description	galoisgetname(a,b)

Relative Number Fields (rnf)

Extension L/K is defined by $T \in K[x]$.

absolute equation of L	rnfequation($nf, T, \{flag\}$)
is L/K abelian?	rnfisabelian(nf, T)
relative nfalgtobasis	rnfalgtobasis(rnf, x)
relative nfbasistoalg	rnfbasistoalg(rnf, x)
relative idealhnf	rnfidealhnf(rnf, x)
relative idealmul	rnfidealmul(rnf, x, y)
relative idealtwoelt	rnfidealtwoelt(rnf, x)

Lifts and Push-downs

absolute $\to$ relative representation for x	rnfeltabstorel(rnf, x)
relative $\to$ absolute representation for x	rnfeltreltoabs(rnf, x)
lift x to the relative field	rnfeltup(rnf, x)
push x down to the base field	rnfeltdown(rnf, x)

idem for x ideal: (rnfideal)reltoabs, abstorel, up, down

Norms and Trace

relative norm of element $x \in L$	rnfeltnorm(rnf, x)
relative trace of element $x \in L$	rnfelttrace(rnf, x)
absolute norm of ideal x	rnfidealnormabs(rnf, x)
relative norm of ideal x	rnfidealnormrel(rnf, x)
solutions of $N_{K/\mathbf{Q}}(y) = x \in \mathbf{Z}$	bnfisintnorm(bnf, x)
is $x \in \mathbf{Q}$ a norm from K?	bnfisnorm($bnf, x, \{flag\}$)
initialize T for norm eq. solver	rnfisnorminit($K, pol, \{flag\}$)
is $a \in K$ a norm from L?	rnfisnorm($T, a, \{flag\}$)
initialize t for Thue equation solver	thueinit(f)
solve Thue equation $f(x,y) = a$	thue($t, a, \{sol\}$)
characteristic poly. of a mod T	rnfcharpoly($nf, T, a, \{v\}$)

Factorization

factor ideal x in L	rnfidealfactor(rnf, x)
$[S,T]$: $T_{i,j} \mid S_i$; S primes of K above p	rnfidealprimedec(rnf, p)

Maximal order $\mathbf{Z}_L$ as a $\mathbf{Z}_K$-module

relative polredbest	rnfpolredbest(nf, T)
relative polredabs	rnfpolredabs(nf, T)
relative Dedekind criterion, prime pr	rnfdedekind(nf, T, pr)
discriminant of relative extension	rnfdisc(nf, T)
pseudo-basis of $\mathbf{Z}_L$	rnfpseudobasis(nf, T)

General $\mathbf{Z}_K$-modules: $M = [\text{matrix}, \text{vec. of ideals}] \subset L$

relative HNF / SNF	nfhnf(nf, M), nfsnf
multiple of det M	nfdetint(nf, M)
HNF of M where $d = nfdetint(M)$	nfhnfmod(x, d)
reduced basis for M	rnflllgram(nf, T, M)
determinant of pseudo-matrix M	rnfdet(nf, M)
Steinitz class of M	rnfsteinitz(nf, M)
$\mathbf{Z}_K$-basis of M if $\mathbf{Z}_K$-free, or 0	rnfhnfbasis(bnf, M)
n-basis of M, or $(n+1)$-generating set	rnfbasis(bnf, M)
is M a free $\mathbf{Z}_K$-module?	rnfisfree(bnf, M)

Associative Algebras

A is a general associative algebra given by a multiplication table mt (over $\mathbf{Q}$ or $\mathbf{F}_p$); represented by al from algtableinit.

create al from mt (over $\mathbf{F}_p$)	algtableinit($mt, \{p=0\}$)
group algebra $\mathbf{Q}[G]$ (or $\mathbf{F}_p[G]$)	alggroup($G, \{p=0\}$)
center of group algebra	alggroupcenter($G, \{p=0\}$)

Properties

is (mt, p) OK for algtableinit?	algisassociative($mt, \{p=0\}$)
multiplication table mt	algmultable(al)
dimension of A over prime subfield	algdim(al)
characteristic of A	algchar(al)
is A commutative?	algiscommutative(al)
is A simple?	algissimple(al)
is A semi-simple?	algissemisimple(al)
center of A	algcenter(al)
Jacobson radical of A	algradical(al)
radical J and simple factors of A/J	algsimpledec(al)

Operations on algebras

create A/I, I two-sided ideal	algquotient(al, I)
create $A_1 \otimes A_2$	algtensor($al1, al2$)
create subalgebra from basis B	algsubalg(al, B)
quotients by ortho. central idempotents e	algcentralproj(al, e)
isomorphic alg. with integral mult. table	algmakeintegral(mt)
prime subalgebra of semi-simple A over $\mathbf{F}_p$	algprimesubalg(al)
find isomorphism $A \cong M_d(\mathbf{F}_q)$	algsplit(al)

Operations on lattices in algebras

lattice generated by cols. of M	alglathnf(al, M)
...by the products xy, $x \in lat1$, $y \in lat2$	alglatmul($al, lat1, lat2$)
sum $lat1 + lat2$ of the lattices	alglatadd($al, lat1, lat2$)
intersection $lat1 \cap lat2$	alglatinter($al, lat1, lat2$)
test $lat1 \subset lat2$	alglatsubset($al, lat1, lat2$)
generalized index $(lat2 : lat1)$	alglatindex($al, lat1, lat2$)
$\{x \in al \mid x \cdot lat1 \subset lat2\}$	alglatlefttransporter($al, lat1, lat2$)
$\{x \in al \mid lat1 \cdot x \subset lat2\}$	alglatrighttransporter($al, lat1, lat2$)
test $x \in lat$ (set c = coord. of x)	alglatcontains($al, lat, x, \{\&c\}$)
element of lat with coordinates c	alglatelement(al, lat, c)

Operations on elements

$a+b$, $a-b$, $-a$	algadd(al, a, b), algsub, algneg
$a \times b$, a^2	algmul(al, a, b), algsqr
a^n, a^{-1}	algpow(al, a, n), alginv
is x invertible ? (then set $z = x^{-1}$)	algisinv($al, x, \{\&z\}$)
find z such that $x \times z = y$	algdivl(al, x, y)
find z such that $z \times x = y$	algdivr(al, x, y)
does z s.t. $x \times z = y$ exist? (set it)	algisdivl($al, x, y, \{\&z\}$)
matrix of $v \mapsto x \cdot v$	algtomatrix(al, x)
absolute norm	algnorm(al, x)
absolute trace	algtrace(al, x)
absolute char. polynomial	algcharpoly(al, x)
given $a \in A$ and polynomial T, return $T(a)$	algpoleval(al, T, a)
random element in a box	algrandom(al, b)

Based on an earlier version by Joseph H. Silverman
October 2020 v2.37. Copyright © 2020 K. Belabas
Permission is granted to make and distribute copies of this card provided the copyright and this permission notice are preserved on all copies.
Send comments and corrections to ⟨Karim.Belabas@math.u-bordeaux.fr⟩

Central Simple Algebras

A is a central simple algebra over a number field K; represented by al from `alginit`; K is given by a nf structure.

create CSA from data	`alginit`$(B, C, \{v\}, \{maxord = 1\})$
multiplication table over K	$B = K$, $C = mt$
cyclic algebra $(L/K, \sigma, b)$	$B = rnf$, $C = [sigma, b]$
quaternion algebra $(a, b)_K$	$B = K$, $C = [a, b]$
matrix algebra $M_d(K)$	$B = K$, $C = d$
local Hasse invariants over K	$B = K$, $C = [d, [PR, HF], HI]$

Properties

type of al (mt, CSA)	`algtype`(al)
dimension of A over $\mathbf{Q}$	`algdim`$(al, 1)$
dimension of al over its center K	`algdim`(al)
degree of A $(= \sqrt{\dim_K A})$	`algdegree`(al)
al a cyclic algebra $(L/K, \sigma, b)$; return σ	`algaut`(al)
... return b	`algb`(al)
... return L/K, as an rnf	`algsplittingfield`(al)
split A over an extension of K	`algsplittingdata`(al)
splitting field of A as an rnf over center	`algsplittingfield`(al)
multiplication table over center	`algrelmultable`(al)
places of K at which A ramifies	`algramifiedplaces`(al)
Hasse invariants at finite places of K	`alghassef`(al)
Hasse invariants at infinite places of K	`alghassei`(al)
Hasse invariant at place v	`alghasse`(al, v)
index of A over K (at place v)	`algindex`$(al, \{v\})$
is al a division algebra? (at place v)	`algisdivision`$(al, \{v\})$
is A ramified? (at place v)	`algisramified`$(al, \{v\})$
is A split? (at place v)	`algissplit`$(al, \{v\})$

Operations on elements

reduced norm	`algnorm`(al, x)
reduced trace	`algtrace`(al, x)
reduced char. polynomial	`algcharpoly`(al, x)
express x on integral basis	`algalgtobasis`(al, x)
convert x to algebraic form	`algbasistoalg`(al, x)
map $x \in A$ to $M_d(L)$, L split. field	`algtomatrix`(al, x)

Orders

$\mathbf{Z}$-basis of order $\mathcal{O}_0$	`algbasis`(al)
discriminant of order $\mathcal{O}_0$	`algdisc`(al)
$\mathbf{Z}$-basis of natural order in terms $\mathcal{O}_0$'s basis	`alginvbasis`(al)

Based on an earlier version by Joseph H. Silverman
October 2020 v2.37. Copyright © 2020 K. Belabas
Permission is granted to make and distribute copies of this card provided the copyright and this permission notice are preserved on all copies.

Send comments and corrections to ⟨Karim.Belabas@math.u-bordeaux.fr⟩