

Algebraic Number Theory

(PARI-GP version 2.13.4)

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 $[y, g]$, $g \in \text{SL}_2(\mathbf{Z})$, $y = g \cdot x$ reduced `qfbreds12(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 `qfbcomprow(x,y)`
 n -th power without reduction `qfbpowrow(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 $p \leq P$ `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,l)`

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 $bnfS$ `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 $a = A(t) \bmod T(t)$ `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 $\leq k$ 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)`
 $q = x \setminus y := \text{round}(x/y)$ `nfeltdivu(nf,x,y)`
 $r = x \% y := x - (x \setminus y)y$ `nfeltmod(nf,x,y)`
... $[q,r]$ as above `nfeltdivrem(nf,x,y)`
reduce x modulo ideal A `nfeltreduce(nf,x,A)`
absolute trace $\text{Tr}_{K/\mathbf{Q}}(x)$ `nfelttrace(nf,x)`
absolute norm $N_{K/\mathbf{Q}}(x)$ `nfeltnorm(nf,x)`

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

valuation $v_p(x)$ `nfeltval(nf,x,p)`
... write $x = \pi^{v_p(x)}y$ `nfeltval(nf,x,p,&y)`
quadratic Hilbert symbol (at p) `nfhilbert(nf,a,b,{p})`
 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 $k \leq n$ `L = lfunitinit(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 $k \leq n$ `L = lfunitinit([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,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 `bnrdisc1ist(bnf,l,{arch},{flag})`
decode output from `bnrdisc1ist` `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 $\text{Cl}_F \rightarrow \text{Cl}_f, f \mid F$ `bnrmmap`
Artin group of extension $K[Y]/(g)$ `rnfnormgroup(bnr,g)`
subgroups of bnr , index $\leq b$ `subgroup1ist(bnr,b,{flag})`
class field defined by $H \subset \text{Cl}_f$ `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)`

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

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

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

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

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

Extension L/K is defined by $T \in K[x]$.	
absolute equation of L	<code>rnequation(nf, T, {flag})</code>
is L/K abelian?	<code>rneisabelian(nf, T)</code>
relative <code>nfalgtobasis</code>	<code>rnfalgtobasis(rnf, x)</code>
relative <code>nfbasistoalg</code>	<code>rnfbasistoalg(rnf, x)</code>
relative <code>ideahhnf</code>	<code>rnfideahhnf(rnf, x)</code>
relative <code>idealmul</code>	<code>rnfidealmul(rnf, x, y)</code>
relative <code>idealtwoelt</code>	<code>rnfidealtwoelt(rnf, x)</code>

absolute \rightarrow relative representation for x	<code>rnfeltabstorel(rmf, x)</code>
relative \rightarrow absolute representation for x	<code>rnfeltreltoabs(rmf, x)</code>
lift x to the relative field	<code>rnfeltup(rmf, x)</code>
push x down to the base field	<code>rnfeltdown(rmf, x)</code>
idem for x ideal: (<code>rnfideal</code>) <code>reltoabs</code> , <code>abstorel</code> , <code>up</code> , <code>down</code>	

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

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

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)

\mathbf{Z}_K -basis of M if \mathbf{Z}_K -free, or 0	<code>rnfhnfbasis(bnf, M)</code>
n -basis of M , or $(n + 1)$ -generating set	<code>rnfbasis(bnf, M)</code>
is M a free \mathbf{Z}_K -module?	<code>rnfisfree(bnf, M)</code>

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?	algisissimple(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)

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

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

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

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