

Algebraic Number Theory

(PARI-GP version 2.10.0)

Binary Quadratic Forms

create $ax^2 + bxy + cy^2$ (distance d)	<code>Qfb($a, b, c, \{d\}$)</code>
reduce x ($s = \sqrt{D}$, $l = \lfloor s \rfloor$)	<code>qfbred($x, \{flag\}, \{D\}, \{l\}, \{s\}$)</code>
return $[y, g]$, $g \in \text{SL}_2(\mathbf{Z})$, $y = g \cdot x$ reduced	<code>qfbreds12(x)</code>
composition of forms	$x*y$ or <code>qfbnucomp(x, y, l)</code>
n -th power of form	x^n or <code>qfbnupow(x, n)</code>
composition without reduction	<code>qfbcomprow(x, y)</code>
n -th power without reduction	<code>qfbpowrow(x, n)</code>
prime form of disc. x above prime p	<code>qfbprimeform(x, p)</code>
class number of disc. x	<code>qfbclassno(x)</code>
Hurwitz class number of disc. x	<code>qfbhclassno(x)</code>
Solve $Q(x, y) = p$ in integers, p prime	<code>qfbsolve(Q, p)</code>

Quadratic Fields

quadratic number $\omega = \sqrt{x}$ or $(1 + \sqrt{x})/2$	<code>quadgen(x)</code>
minimal polynomial of ω	<code>quadpoly(x)</code>
discriminant of $\mathbf{Q}(\sqrt{D})$	<code>quaddisc(x)</code>
regulator of real quadratic field	<code>quadregulator(x)</code>
fundamental unit in real $\mathbf{Q}(x)$	<code>quadunit(x)</code>
class group of $\mathbf{Q}(\sqrt{D})$	<code>quadclassunit($D, \{flag\}, \{t\}$)</code>
Hilbert class field of $\mathbf{Q}(\sqrt{D})$	<code>quadhilbert($D, \{flag\}$)</code>
... using specific class invariant ($D < 0$)	<code>polclass($D, \{inv\}$)</code>
ray class field modulo f of $\mathbf{Q}(\sqrt{D})$	<code>quadray($D, f, \{flag\}$)</code>

General Number Fields: Initializations

The number field $K = \mathbf{Q}[X]/(f)$ is given by irreducible $f \in \mathbf{Q}[X]$. A nf computes 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	<code>nfinit($f, \{flag\}$)</code>
known integer basis B	<code>nfinit($[f, B]$)</code>
order maximal at $vp = [p_1, \dots, p_k]$	<code>nfinit($[f, vp]$)</code>
order maximal at all $p \leq P$	<code>nfinit($[f, P]$)</code>
certify maximal order	<code>nfcertify(nf)</code>

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	$nf.disc$
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	$nf.newprec(nf)$
init relative rnf $L = K[Y]/(g)$	$rnfinit(nf, g)$
init bnf structure	$bnfinit(f, \{flag\})$

bnf members: same as nf , plus

underlying nf	$bnf.nf$
classgroup	$bnf.clgp$
regulator	$bnf.reg$
fundamental/torsion units	$bnf.fu, bnf.tu$
compress a bnf for storage	$bnf.compress(bnf)$
recover a bnf from compressed $bnfz$	$bnfinit(bnfz)$
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	$bnr.mod$
structure of $(\mathbf{Z}_K/m)^*$	$bnr.zkst$

Basic Number Field Arithmetic (nf)

Elements are `t_INT`, `t_FRAC`, `t_POL`, `t_POLMOD`, or `t_COL` (on integral basis $nf.zk$). Basic operations (prefix `nfelt`): (`nfelt`)`add`, `mul`, `pow`, `div`, `diveuc`, `mod`, `divrem`, `val`, `trace`, `norm`
express x on integer basis `nfalgtobasis(nf, x)`
express element x as a polmod `nfbasistoalg(nf, x)`
complex embeddings of `t_POLMOD` x `conjvec(x)`
reverse polmod $a = A(X) \bmod T(X)$ `modreverse(a)`
integral basis of field def. by $f = 0$ `nfbasis(f)`
field discriminant of field $f = 0$ `nfdisc(f)`
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)`
 $\mathbf{Q}[x]/(f) \subset \mathbf{Q}[x]/(g)$? Isomorphic? `nfisincl(f, g)`, `nfisisom`
compositum of $\mathbf{Q}[X]/(f)$, $\mathbf{Q}[X]/(g)$ `polcompositum($f, g, \{flag\}$)`
compositum of $K[X]/(f)$, $K[X]/(g)$ `nfcompositum($nf, f, g, \{flag\}$)`
splitting field of K (degree divides d) `nfsplitting($nf, \{d\}$)`
subfields (of degree d) of nf `nfsubfields($nf, \{d\}$)`
 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 `nfactor(nf, g)`
factor $g \bmod$ prime pr in nf `nfactormod(nf, g, pr)`
conjugates of a root θ of nf `nfgaloisconj($nf, \{flag\}$)`
apply Galois automorphism s to x `nfgaloisapply(nf, s, x)`
quadratic Hilbert symbol (at p) `nfhilbert($nf, a, b, \{p\}$)`

Linear and algebraic relations

poly of degree $\leq k$ with root $x \in \mathbf{C}$	<code>algdep(x, k)</code>
alg. dep. with pol. coeffs for series s	<code>seralgdep(s, x, y)</code>
small linear rel. on coords of vector x	<code>linddep(x)</code>

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, $N(I) < b$	<code>dirzetak(nf, b)</code>
init $\zeta_K^{(k)}(s)$ for $k \leq n$	<code>L = lfuninit($bnf, R, \{n = 0\}$)</code>
compute $\zeta_K(s)$ (n -th derivative)	<code>lfun($L, s, \{n = 0\}$)</code>
compute $\Lambda_K(s)$ (n -th derivative)	<code>lfunlambda($L, s, \{n = 0\}$)</code>

init $L_K^{(k)}(s, \chi)$ for $k \leq n$	<code>L = lfuninit($[bnr, chi], R, \{n = 0\}$)</code>
compute $L_K(s, \chi)$ (n -th derivative)	<code>lfun($L, s, \{n\}$)</code>
Artin root number of K	<code>bnrrootnumber($bnr, chi, \{flag\}$)</code>
$L(1, \chi)$, for all χ trivial on H	<code>bnrL1($bnr, \{H\}, \{flag\}$)</code>

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 .
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)`
as above for S -units `bnfissunit($bnfs, x$)`

signs of real embeddings of $bnf.fu$	<code>bnfsignunit(bnf)</code>
narrow class group	<code>bnfnarrow(bnf)</code>
Class Field Theory	
ray class number for modulus m	<code>bnrclassno(bnf, m)</code>
discriminant of class field	<code>bnrdisc($a_1, \{a_2\}$)</code>
ray class numbers, l list of moduli	<code>bnrclassolist(bnf, l)</code>
discriminants of class fields	<code>bnrdisclist($bnf, l, \{arch\}, \{flag\}$)</code>
decode output from <code>bnrdisclist</code>	<code>bnfdecodemodule(nf, fa)</code>
is modulus the conductor?	<code>bnrisconductor($a_1, \{a_2\}$)</code>
is class field (bnr, H) Galois over K^G	<code>bnrisgalois(bnr, G, H)</code>
action of automorphism on <code>bnr.gen</code>	<code>bnrgaloismatrix(bnr, aut)</code>
apply <code>bnrgaloismatrix</code> M to H	<code>bnrgaloisapply(bnr, M, H)</code>
characters on <code>bnr.clgp</code> s.t. $\chi(g_i) = e(v_i)$	<code>bnrchar($bnr, g, \{v\}$)</code>
conductor of character χ	<code>bnrconductor(bnr, chi)</code>
conductor of extension	<code>bnrconductor($a_1, \{a_2\}, \{flag\}$)</code>
conductor of extension $K[Y]/(g)$	<code>rnfconductor(bnf, g)</code>
Artin group of extension $K[Y]/(g)$	<code>rnfnormgroup(bnr, g)</code>
subgroups of bnr , index $\leq b$	<code>subgrouplist($bnr, b, \{flag\}$)</code>
rel. eq. for class field def'd by sub	<code>rnfkummer($bnr, sub, \{d\}$)</code>
same, using Stark units (real field)	<code>bnrstark($bnr, sub, \{flag\}$)</code>
is a an n -th power in K_v ?	<code>nfislocalpower(nf, v, a, n)</code>
cyclic L/K satisf. local conditions	<code>nfgrunwaldwang(nf, P, D, pl)</code>

Logarithmic class group

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(rmf)</code>

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

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

Primes and Multiplicative Structure

factor ideal x in \mathbf{Z}_K	<code>idealfactor(nf, x)</code>
expand ideal factorization in K	<code>idealfactorback($nf, f, \{e\}$)</code>
expand elt factorisation 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. $v_p(a) = v_p(x)$ if $v_p(x) \neq 0$	<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 $(1 + \mathfrak{p})/(1 + \mathfrak{p}^k)$	<code>idealprincipalunits(nf, pr, k)</code>
discrete log of x in $(\mathbf{Z}_K/bid)^*$	<code>ideallog(nf, x, bid)</code>

Algebraic Number Theory

(PARI-GP version 2.10.0)

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)
 project t to \mathbf{Z}_K/pr **nfmodpr**($nf, t, modpr$)
 lift from \mathbf{Z}_K/pr **nfmodprlift**($nf, t, modpr$)

Galois theory over \mathbf{Q}

Galois group of field $\mathbf{Q}[x]/(f)$ **polgalois**(f)
 initializes a Galois group structure G **galoisinit**($pol, \{den\}$)
 action of p in **nfgaloisconj** form **galoispermopol**($G, \{p\}$)
 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)
 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**($\mathbf{N}, \mathbf{H}, \{flag\}, \{v\}$)
 query the **galpol** package **galoisgetpol**($a, b, \{s\}$)

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 **nfalttobasis** **rnfalttobasis**(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 \rightarrow relative repres. for x **rnfeltabstorel**(rnf, x)
 relative \rightarrow absolute repres. 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 **rnfidealnrmabs**(rnf, x)
 relative norm of ideal x **rnfidealnrmrel**(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 Dedekind criterion, prime pr **rnfdedekind**(nf, T, pr)
 discriminant of relative extension **rnfdisc**(nf, T)
 pseudo-basis of \mathbf{Z}_L **rnfpsedobasis**(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 mult. table mt (over \mathbf{Q} or \mathbf{F}_p); represented by al from **algtbleinit**.
 create al from mt (over \mathbf{F}_p) **algtbleinit**($mt, \{p=0\}$)
 group algebra $\mathbf{Q}[G]$ (or $\mathbf{F}_p[G]$) **alggroup**($G, \{p=0\}$)

Properties

is (mt, p) OK for **algtbleinit**? **algisassociative**($mt, \{p=0\}$)
 multiplication table mt **algmtable**(al)
 multiplication table over center **algrelmtable**(al)
 dimension of A over prime subfield **algabsdim**(al)
 characteristic of A **algchar**(al)
 is A commutative? **algiscommutative**(al)
 is A simple? **algissimple**(al)
 is A semi-simple? **algissemisimple**(al)
 is A ramified? (at place v) **algisramified**($al, \{v\}$)
 is A split? (at place v) **algissplit**($al, \{v\}$)
 center of A **algcenter**(al)
 Jacobson radical of A **algradical**(al)
 radical J and simple factors of A/J **algdecomposition**(al)
 simple factors of semi-simple A **algsimpledec**(al)

Operations on algebras

create A/I , I two-sided ideal **algquotient**($al, I, \{flag=0\}$)
 create $A_1 \otimes A_2$ **algtensor**($al1, al2$)
 create subalgebra from basis B **algsubalg**(al, B)
 \dots from orthogonal central idempotents e **algcentralproj**(al, e)
 prime subalgebra of semi-simple A over \mathbf{F}_p **algprimesubalg**(al)
 lattice generated by cols. of M **alglathnf**(al, M)

Operations on elements

$a+b, a-b, -a$ **algadd**(al, a, b), **algsub**, **algneg**
 $a \times b, a \times a$ **algmul**(al, a, a), **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 $v \mapsto x \cdot v$ **algleftmtable**(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)

Central Simple Algebras

A is a central simple algebra over a number field K ; represented by al from **alginitt**; K is given by a nf structure.
 create CSA from data **alginitt**($B, C, \{v\}, \{flag=0\}$)
 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)
 is al a division algebra? (at place v) **algisdivision**($al, \{v\}$)
 dimension of al over its center **algdim**(al)
 degree of A ($= \sqrt{\dim}$) **algdegree**(al)
 index of A over K (index at v) **algindex**($al, \{v\}$)
 al a cyclic algebra $(L/K, \sigma, b)$; return σ **algaut**(al)
 \dots return b **algb**(al)
 \dots 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)
 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)

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 **algsplittingmatrix**(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
 January 2017 v2.30. Copyright © 2017 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)