

# Algebraic Number Theory

(PARI-GP version 2.17.1)

## Binary Quadratic Forms

create  $ax^2 + bxy + cy^2$  **Qfb**( $a, b, c$ ) or **Qfb**( $[a, b, c]$ )  
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 **qfbcomp**( $x, y$ )  
... without reduction **qfbcomppraw**( $x, y$ )  
 $n$ -th power **qfbpow**( $x, n$ )  
... 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**( $Q, n$ )  
solve  $x^2 + Dy^2 = p$ ,  $p$  prime **qfbcornacchia**( $D, p$ )  
...  $x^2 + Dy^2 = 4p$ ,  $p$  prime **qfbcornacchia**( $D, 4 * p$ )

## Quadratic Fields

quadratic number  $\omega = \sqrt{x}$  or  $(1 + \sqrt{x})/2$  **quadgen**( $x$ )  
minimal polynomial of  $\omega$  **quadpoly**( $x$ )  
discriminant of  $\mathbf{Q}(\sqrt{x})$  **quaddisc**( $x$ )  
regulator of real quadratic field **quadregulator**( $x$ )  
fundamental unit in  $O_D$ ,  $D > 0$  **quadunit**( $D, \{w\}$ )  
norm of fundamental unit in  $O_D$  **quadunitnorm**( $D$ )  
index of  $O_{Df^2}^\times$  in  $O_D^\times$  **quadunitindex**( $D, f$ )  
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**( $D, \{inv\}$ )  
test if  $T$  is **polclass**( $D$ ); if so return  $D$  **polisclass**( $T$ )  
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  $rmf$  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  $\theta$  **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  $rmf$   $L = K[Y]/(g)$  **rnfininit**( $nf, g$ )  
init  $bnf$  structure **bnfininit**( $f, l$ )

**bnf members:** same as  $nf$ , plus  
underlying  $nf$   
class group, regulator  
fundamental/torsion units  
add  $S$ -class group and units, yield  $bnfS$   
init class field structure  $bnr$

**bnr members:** same as  $bnf$ , plus

underlying  $bnf$   
big ideal structure  
modulus  $m$   
structure of  $(\mathbf{Z}_K/m)^*$

## Fields, subfields, embeddings

### Defining polynomials, embeddings

(some) number fields with Galois group  $G$  **nflist**( $G$ )  
... and  $|\text{disc}(K)| = N$  and  $s$  complex places **nflist**( $G, N, \{s\}$ )  
... and  $a \leq |\text{disc}(K)| \leq b$  **nflist**( $G, [a, b], \{s\}$ )  
smallest poly defining  $f = 0$  (slow) **polredabs**( $f, \{flag\}$ )  
small poly defining  $f = 0$  (fast) **polredbest**( $f, \{flag\}$ )  
monic integral  $g = Cf(x/L)$  **polmonic**( $f, \{\&L\}$ )  
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**( $nf, T, \{pl\}$ )  
absolute Weil height **nfweilheight**( $nf, v$ )

### Subfields, polynomial factorization

subfields (of degree  $d$ ) of  $nf$  **nfsubfields**( $nf, \{d\}$ )  
maximal subfields of  $nf$  **nfsubfieldsmax**( $nf$ )  
maximal CM subfield of  $nf$  **nfsubfieldscm**( $nf$ )  
 $K_d \subset \mathbf{Q}(\zeta_n)$ , using Gaussian periods **polsubcyclo**( $n, d, \{v\}$ )  
... using class field theory **polsubcyclofast**( $n, d$ )  
roots of unity in  $nf$  **nfrootsof1**( $nf$ )  
roots of  $g$  belonging to  $nf$  **nfroots**( $nf, g$ )  
factor  $g$  in  $nf$  **nfactor**( $nf, g$ )

### Linear and algebraic relations

poly of degree  $\leq k$  with root  $x \in \mathbf{C}$  or  $\mathbf{Q}_p$  **algdep**( $x, k$ )  
alg. dep. with pol. coeffs for series  $s$  **seralgdep**( $s, x, y$ )  
diff. dep. with pol. coeffs for series  $s$  **serdiffdep**( $s, x, y$ )  
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**( $nf, x, y$ )  
 $q = x \backslash y := \text{round}(x/y)$  **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  $\text{Tr}_{K/\mathbf{Q}}(x)$  **nfelttrace**( $nf, x$ )  
absolute norm  $N_{K/\mathbf{Q}}(x)$  **nfeltnorm**( $nf, x$ )

**bnf.nf**  
**bnf.clgp**, **bnf.reg**  
**bnf.fu**, **bnf.tu**  
**bnfsunit**( $bnf, S$ )  
**bnrinit**( $bnf, m, \{flag\}$ )

**bnr.bnf**  
**bnr.bid**  
**bnr.mod**  
**bnr.zkst**

**nflist**( $G$ )  
**nflist**( $G, N, \{s\}$ )  
**nflist**( $G, [a, b], \{s\}$ )  
**polredabs**( $f, \{flag\}$ )  
**polredbest**( $f, \{flag\}$ )  
**polmonic**( $f, \{\&L\}$ )  
**poltschirnhaus**( $f$ )

**nfisincl**( $f, g$ ), **nfisisom**  
**modreverse**( $a$ )  
**polcompositum**( $f, g, \{flag\}$ )  
**nfcompositum**( $nf, f, g, \{flag\}$ )  
**nfsplitting**( $nf, \{d\}$ )  
**nfeltsign**( $nf, x, \{pl\}$ )  
**nfeltembed**( $nf, x, \{pl\}$ )  
**nfpolsturm**( $nf, T, \{pl\}$ )  
**nfweilheight**( $nf, v$ )

**nfsubfields**( $nf, \{d\}$ )  
**nfsubfieldsmax**( $nf$ )  
**nfsubfieldscm**( $nf$ )  
**polsubcyclo**( $n, d, \{v\}$ )  
**polsubcyclofast**( $n, d$ )  
**nfrootsof1**( $nf$ )  
**nfroots**( $nf, g$ )  
**nfactor**( $nf, g$ )

**algdep**( $x, k$ )  
**seralgdep**( $s, x, y$ )  
**serdiffdep**( $s, x, y$ )  
**lindep**( $x$ )

**nfeltadd**( $nf, x, y$ )  
**nfeltmul**( $nf, x, y$ )  
**nfeltpow**( $nf, x, n$ )  
**nfeltdiv**( $nf, x, y$ )  
**nfeltdiveuc**( $nf, x, y$ )  
**nfeltmod**( $nf, x, y$ )  
**nfeltdivrem**( $nf, x, y$ )  
**nfeltreduce**( $nf, x, A$ )  
**nfelttrace**( $nf, x$ )  
**nfeltnorm**( $nf, x$ )

is  $x$  a square? **nfeltissquare**( $nf, x, \{\&y\}$ )  
... an  $n$ -th power? **nfeltispower**( $nf, x, n, \{\&y\}$ )

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

valuation  $v_{\mathfrak{p}}(x)$  **nfeltval**( $nf, x, \mathfrak{p}$ )  
... write  $x = \pi^{v_{\mathfrak{p}}(x)} y$  **nfeltval**( $nf, x, \mathfrak{p}, \&y$ )  
quadratic Hilbert symbol (at  $\mathfrak{p}$ ) **nfhilbert**( $nf, a, b, \{\mathfrak{p}\}$ )  
 $b$  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**( $nf, x$ )

### Hecke Grossencharacters

Let  $K$  be a number field and  $m$  a modulus. A **gchar** structure  
describes the group of Hecke Grossencharacters of  $K$  of modulus  $m$   
and allows computations with these characters. A character  $\chi$  is  
described by its components modulo  $gc.cyc$ .

init **gchar** structure  $gc$  for modulus  $m$  **gcharinit**( $bnf, m, \{cm\}$ )

### gc members:

underlying  $bnf$  **gc.bnf**  
modulus **gc.mod**  
elementary divisors (including 0s) **gc.cyc**  
recompute  $gc$  using current precision **gcharnewprec**( $gc$ )  
evaluate Hecke character  $chi$  at ideal  $id$  **gchareval**( $gc, chi, id$ )  
exponent column of  $id$  in  $\mathbf{R}^n$  **gcharideallog**( $gc, id$ )  
log representation of ideal  $id$  **gcharlog**( $gc, id$ )  
... of character  $\chi$  **gcharduallog**( $gc, chi$ )  
exponent vector of  $\chi$  in  $\mathbf{R}^n$  **gcharparameters**( $gc, chi$ )  
conductor of  $\chi$  **gcharconductor**( $gc, chi$ )  
L-function of  $\chi$  **lfuncreate**( $[gc, chi]$ )  
local component  $\chi_v$  of  $\chi$  **gcharlocal**( $gc, chi, v$ )  
 $\chi$  s.t.  $\chi_v \approx Lchiv[i]$  for  $v = Lv[i]$  **gcharidentify**( $gc, Lv, Lchiv$ )  
basis of group of algebraic characters **gcharalgebraic**( $gc$ )  
algebraic character of given infinity type **gcharalgebraic**( $gc, type$ )  
is  $\chi$  algebraic? **gcharisalgebraic**( $gc, chi$ )

### Dedekind Zeta Function $\zeta_K$ , 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  $h$ ).

$\zeta_K$  as Dirichlet series,  $N(I) \leq b$  **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  $\chi$  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  $bnr, \chi$  (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	<code>bnfisprincipal(<i>bnf</i>, <math>x</math>, {<i>flag</i>})</code>
... on ray class gp	<code>bnrisprincipal(<i>bnr</i>, <math>x</math>, {<i>flag</i>})</code>
expo. of $x$ on fund. units	<code>bnfisunit(<i>bnf</i>, <math>x</math>)</code>
... on $S$ -units, $U$ is <code>bnfunits(<i>bnf</i>, <math>S</math>)</code>	<code>bnfisunit(<i>bnfs</i>, <math>x</math>, <math>U</math>)</code>
signs of real embeddings of <i>bnf</i> .fu	<code>bnfsignunit(<i>bnf</i>)</code>
narrow class group	<code>bnfnarrow(<i>bnf</i>)</code>

### Class Field Theory

ray class number for modulus $m$	<code>bnrclassno(<i>bnf</i>, <math>m</math>)</code>
discriminant of class field	<code>bnrdisc(<math>a_1</math>, {<math>a_2</math>})</code>
ray class numbers, $l$ list of moduli	<code>bnrclassnolist(<i>bnf</i>, <math>l</math>)</code>
discriminants of class fields	<code>bnrdisclist(<i>bnf</i>, <math>l</math>, {<i>arch</i>}, {<i>flag</i>})</code>
decode output from <code>bnrdisclist</code>	<code>bnfdecodemodule(<i>nf</i>, <math>f</math>, <math>a</math>)</code>
is modulus the conductor?	<code>bnrisconductor(<math>a_1</math>, {<math>a_2</math>})</code>
is class field ( <i>bnr</i> , $H$ ) Galois over $K^G$	<code>bnrisgalois(<i>bnr</i>, <math>G</math>, <math>H</math>)</code>
action of automorphism on <code>bnr.gen</code>	<code>bnrgaloismatrix(<i>bnr</i>, <math>aut</math>)</code>
apply <code>bnrgaloismatrix</code> $M$ to $H$	<code>bnrgaloisapply(<i>bnr</i>, <math>M</math>, <math>H</math>)</code>
characters on <code>bnr.clgp</code> s.t. $\chi(g_i) = e(v_i)$	<code>bnrchar(<i>bnr</i>, <math>g</math>, {<math>v</math>})</code>
conductor of character $\chi$	<code>bnrconductor(<i>bnr</i>, <math>chi</math>)</code>
conductor of extension	<code>bnrconductor(<math>a_1</math>, {<math>a_2</math>}, {<i>flag</i>})</code>
conductor of extension $K[Y]/(g)$	<code>rnfconductor(<i>bnf</i>, <math>g</math>)</code>
canonical projection $Cl_F \rightarrow Cl_f$ , $f \mid F$	<code>bnrmap</code>
Artin group of extension $K[Y]/(g)$	<code>rnfnormgroup(<i>bnr</i>, <math>g</math>)</code>
subgroups of <i>bnr</i> , index $\leq b$	<code>subgrouplist(<i>bnr</i>, <math>b</math>, {<i>flag</i>})</code>
compositum as <code>[bnr,H]</code>	<code>bnrcompositum([<i>bnr</i>1, <math>H</math>1], [<i>bnr</i>2, <math>H</math>2])</code>
class field defined by $H \subset Cl_f$	<code>bnrclassfield(<i>bnr</i>, <math>H</math>)</code>
... low level equivalent, prime degree	<code>rnfkummer(<i>bnr</i>, <math>H</math>)</code>
same, using Stark units (real field)	<code>bnrstark(<i>bnr</i>, {<i>sub</i>}, {<i>flag</i>})</code>
Stark unit	<code>bnrstarkunit(<i>bnr</i>, {<i>sub</i>})</code>
is $a$ an $n$ -th power in $K_v$ ?	<code>nfislocalpower(<i>nf</i>, <math>v</math>, <math>a</math>, <math>n</math>)</code>
cyclic $L/K$ satisf. local conditions	<code>nfgrunwaldwang(<i>nf</i>, <math>P</math>, <math>D</math>, <math>p</math>)</code>

### Cyclotomic and Abelian fields theory

An Abelian field  $F$  given by a subgroup  $H \subset (Z/fZ)^*$  is described by an argument  $F$ , e.g.  $f$  (for  $H = 1$ , i.e.  $Q(\zeta_f)$ ) or  $[G, H]$ , where  $G$  is `idealstar( $f$ , 1)`, or a minimal polynomial.

minus class number $h^-(F)$	<code>subcyclohminus(<math>F</math>)</code>
... $p$ -part	<code>subcyclohminus(<math>F</math>, <math>p</math>)</code>
minus part of Iwasawa polynomials	<code>subcycloiwasawa(<math>F</math>, <math>p</math>)</code>
$p$ -Sylow of $Cl(F)$	<code>subcyclopclgp(<math>F</math>, <math>p</math>)</code>

### Logarithmic class group

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

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

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

### Ideal Operations

add ideals $x$ and $y$	<code>idealadd(<i>nf</i>, <math>x</math>, <math>y</math>)</code>
multiply ideals $x$ and $y$	<code>idealmul(<i>nf</i>, <math>x</math>, <math>y</math>, {<i>flag</i>})</code>
intersection of ideal $x$ with $Q$	<code>idealdown(<i>nf</i>, <math>x</math>)</code>
intersection of ideals $x$ and $y$	<code>idealintersect(<i>nf</i>, <math>x</math>, <math>y</math>, {<i>flag</i>})</code>
$n$ -th power of ideal $x$	<code>idealpow(<i>nf</i>, <math>x</math>, <math>n</math>, {<i>flag</i>})</code>
inverse of ideal $x$	<code>idealinv(<i>nf</i>, <math>x</math>)</code>

# Algebraic Number Theory

(PARI-GP version 2.17.1)

divide ideal $x$ by $y$	<code>idealdiv(<i>nf</i>, <math>x</math>, <math>y</math>, {<i>flag</i>})</code>
Find $(a, b) \in x \times y$ , $a + b = 1$	<code>idealaddtoone(<i>nf</i>, <math>x</math>, {<math>y</math>})</code>
coprime integral $A, B$ such that $x = A/B$	<code>idealnumden(<i>nf</i>, <math>x</math>)</code>

### Primes and Multiplicative Structure

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

### Galois theory over Q

conjugates of a root $\theta$ of <i>nf</i>	<code>nfgaloisconj(<i>nf</i>, {<i>flag</i>})</code>
apply Galois automorphism $s$ to $x$	<code>nfgaloisapply(<i>nf</i>, <math>s</math>, <math>x</math>)</code>
Galois group of field $Q[x]/(f)$	<code>polgalois(<math>f</math>)</code>
resolvent field of $Q[x]/(f)$	<code>nfresolvent(<math>f</math>)</code>
initializes a Galois group structure $G$	<code>galoisinit(<i>pol</i>, {<i>den</i>})</code>
... for the splitting field of <i>pol</i>	<code>galoissplittinginit(<i>pol</i>, {<math>d</math>})</code>
character table of $G$	<code>galoischartable(<math>G</math>)</code>
conjugacy classes of $G$	<code>galoisconjclasses(<math>G</math>)</code>
det( $1 - \rho(g)T$ ), $\chi$ character of $\rho$	<code>galoischarpoly(<math>G</math>, <math>\chi</math>, {<math>o</math>})</code>
det( $\rho(g)$ ), $\chi$ character of $\rho$	<code>galoischarpoly(<math>G</math>, <math>\chi</math>, {<math>o</math>})</code>
action of $p$ in <code>nfgaloisconj</code> form	<code>galoispermtopol(<math>G</math>, {<math>p</math>})</code>
identify as abstract group	<code>galoisidentify(<math>G</math>)</code>
export a group for GAP/MAGMA	<code>galoisexport(<math>G</math>, {<i>flag</i>})</code>
subgroups of the Galois group $G$	<code>galoissubgroups(<math>G</math>)</code>
is subgroup $H$ normal?	<code>galoisisnormal(<math>G</math>, <math>H</math>)</code>
subfields from subgroups	<code>galoissubfields(<math>G</math>, {<i>flag</i>}, {<math>v</math>})</code>
fixed field	<code>galoisfixedfield(<math>G</math>, <i>perm</i>, {<i>flag</i>}, {<math>v</math>})</code>
Frobenius at maximal ideal $P$	<code>idealfrobenius(<i>nf</i>, <math>G</math>, <math>P</math>)</code>
ramification groups at $P$	<code>idealramgroups(<i>nf</i>, <math>G</math>, <math>P</math>)</code>
is $G$ abelian?	<code>galoisisabelian(<math>G</math>, {<i>flag</i>})</code>
abelian number fields/ $Q$	<code>galoissubcyclo(N,H,{<i>flag</i>},{<math>v</math>})</code>

### The galpol package

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

### Relative Number Fields (rnf)

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

absolute equation of $L$	<code>rnfequation(<i>nf</i>, <math>T</math>, {<i>flag</i>})</code>
is $L/K$ abelian?	<code>rnfisabelian(<i>nf</i>, <math>T</math>)</code>
relative <code>nfalgtobasis</code>	<code>rnfalgtobasis(<i>rnf</i>, <math>x</math>)</code>
relative <code>nfbasistoalg</code>	<code>rnfbasistoalg(<i>rnf</i>, <math>x</math>)</code>
relative <code>idealhnf</code>	<code>rnfidealhnf(<i>rnf</i>, <math>x</math>)</code>

relative <code>idealmul</code>	<code>rnfidealmul(<i>rnf</i>, <math>x</math>, <math>y</math>)</code>
relative <code>idealtwoelt</code>	<code>rnfidealtwoelt(<i>rnf</i>, <math>x</math>)</code>

### Lifts and Push-downs

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

### Norms and Trace

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

### Factorization

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

### Maximal order $Z_L$ as a $Z_K$ -module

relative <code>polredbest</code>	<code>rnfpolredbest(<i>nf</i>, <math>T</math>)</code>
relative <code>polredabs</code>	<code>rnfpolredabs(<i>nf</i>, <math>T</math>)</code>
relative Dedekind criterion, prime $pr$	<code>rnfdedekind(<i>nf</i>, <math>T</math>, <math>pr</math>)</code>
discriminant of relative extension	<code>rnfdisc(<i>nf</i>, <math>T</math>)</code>
pseudo-basis of $Z_L$	<code>rnfpseudobasis(<i>nf</i>, <math>T</math>)</code>

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

relative HNF / SNF	<code>nfhnf(<i>nf</i>, <math>M</math>), nfsnf</code>
multiple of det $M$	<code>nfdetint(<i>nf</i>, <math>M</math>)</code>
HNF of $M$ where $d = nfdetint(M)$	<code>nfhnfmod(<math>x</math>, <math>d</math>)</code>
reduced basis for $M$	<code>rnfilllgram(<i>nf</i>, <math>T</math>, <math>M</math>)</code>
determinant of pseudo-matrix $M$	<code>rnfdet(<i>nf</i>, <math>M</math>)</code>
Steinitz class of $M$	<code>rnfsteeinitz(<i>nf</i>, <math>M</math>)</code>
$Z_K$ -basis of $M$ if $Z_K$ -free, or 0	<code>rnfhnfbasis(<i>bnf</i>, <math>M</math>)</code>
$n$ -basis of $M$ , or $(n + 1)$ -generating set	<code>rnfbasis(<i>bnf</i>, <math>M</math>)</code>
is $M$ a free $Z_K$ -module?	<code>rnfisfree(<i>bnf</i>, <math>M</math>)</code>

Based on an earlier version by Joseph H. Silverman  
 September 2024 v2.39. Copyright © 2024 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)

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                    `alggrouppcenter(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)                    `algsdivl(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)`

Central Simple Algebras

$A$  is a central simple algebra over a number field  $K$ ; represented by  $al$  from `algininit`;  $K$  is given by a  $nf$  structure.  
create CSA from data                    `algininit(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  $\sigma$                     `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  $v$ )                    `algsdivision(al, {v})`  
is  $A$  ramified? (at place  $v$ )                    `algsramified(al, {v})`  
is  $A$  split? (at place  $v$ )                    `algsisplit(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)`