SOME PARI COMMANDS IN ALGEBRAIC NUMBER THEORY

KEITH CONRAD

The free computer algebra package PARI is designed for computations in number theory. A copy can be downloaded by searching on the internet for "PARI download".

The following list provides some commands in PARI that are useful in algebraic number theory, and after listing command we will work through some examples.

Primes and Factoring

`factor(n)` factors the integer n into primes. (This works on rational numbers also and will give prime factorizations with negative exponents.)

`gcd(a,b)` is the greatest common divisor of a and b.

`isprime(n)` returns `1` if n is prime and `0` otherwise.

`prime(n)` returns the nth prime.

`primes(n)` is a vector whose components are the first n primes.

Polynomials

`factor(f(x))` factors $f(x)$ into (monic) irreducibles in $\mathbf{Q}[x]$. (This is the same command as for integers. PARI treats it as a polynomial when there is a variable appearing. If any coefficient has a decimal point then the factorization is done in $\mathbf{C}[x]$.)

`factormod(f(x),p)` factors $f(x)$ mod p.

`poldisc(f(x))` gives the discriminant of the polynomial $f(x)$.

`polgalois(f(x))` gives the Galois group of the splitting field of $f(x)$ over $\mathbf{Q}$. The output is a vector whose first component is the size of the Galois group and other components describe the group structure.

`polisirreducible(f(x))` returns `1` if $f(x)$ is irreducible in $\mathbf{Q}[x]$ and `0` otherwise.

`polroots(f(x))` is a vector whose components are the roots of $f(x)$ in $\mathbf{C}$.

`subst(F,x,a)` returns the value of F when the variable x in F is replaced by a. Here F can be any algebraic object involving the variable x: a polynomial (in several variables), matrix, vector, and so on.

Linear Algebra

`A = [1,2;4,9]` defines A to be the 2×2 matrix $\left(\begin{smallmatrix} 1 & 2 \\ 4 & 9 \end{smallmatrix}\right)$. Larger matrices can be defined in the same way, using a semicolon to end each row.

`charpoly(A)` is the characteristic polynomial $\det(xI - A)$.

`matdet(A)` is the determinant of the matrix A.

`trace(A)` is the trace of the matrix A.

`v = [1,2,3,6]` defines `v` as a row vector with components 1, 2, 3, and 6.

`v = [1,2,3,6]~` defines `v` as a column vector with components 1, 2, 3, and 6. This is important if you want to multiply a matrix and vector in the usual way, where vectors are written in column form.

`v[n]` is the nth component of a vector `v`. For example, `polroots(f(x))` is the vector whose components are the roots of $f(x)$ and `polroots(f(x))[1]` is the first component of the vector of roots of $f(x)$.

Number Fields

Now $f(x)$ is an irreducible polynomial in $\mathbf{Q}[x]$ and K_f below will denote the number field $\mathbf{Q}(\alpha)$ where α is a root of $f(x)$. Algebraically, this is $\mathbf{Q}[x]/(f(x))$. (If you use a reducible polynomial for $f(x)$, some of the commands will give answers, so make sure your polynomial is irreducible.)

`abs(z)`, `real(z)`, `imag(z)` are the absolute value, real part, and imaginary part of the complex number z.

`algdep(z,n)` is the polynomial in $\mathbf{Z}[x]$ of degree at most n which is most likely to have the complex number z as a root. (If z is not of degree at most n over $\mathbf{Q}$ the answer will be useless, so use of this command requires judgment.)

`bnfclgp(f(x))` gives the ideal class group of K_f. The output is a vector whose first component is the class number and the second component is the cyclic decomposition of the class group.

`bnfinit(f(x))` is a long vector containing information about K_f which is used in unit and class group computations. It is best to assign this a name right away, *e.g.*, `B = bnfinit(f(x));`. The semicolon stops PARI from outputting the data on the screen all at once.

`bnfinit(f(x)).fu` gives the fundamental units of K_f, expressed as polynomials in x mod $f(x)$.

`bnfreg(f(x))` gives the regulator of K_f.

`dirzetak(nfinit(f(x)),N)` gives the coefficients of the first N terms in the Dirichlet series for K_f when it is written as a sum over positive integers. That is, if $\zeta_K(s) = \sum_{n\geq 1} a_n/n^s$ then this command returns $[a_1, a_2, \ldots, a_N]$.

`idealfactor(nfinit(f(x)),p)` gives the prime ideal factorization of p in K_f. (If you have already given the vector `nfinit(f(x))` a name, you can use that label in the first component, and you can use `bnfinit(f(x))` there too.) The answer is an array where each row is associated to a different prime ideal. A row has the form `[[p, v, e, f, w] e]`, where e and f are the ramification index and residue field degree for that prime ideal. The vector `v` is related to a second generator γ such that the prime ideal being described is (p, γ) and `w` is related to the inverse of the prime ideal.

`nfbasis(f(x))` gives a $\mathbf{Z}$-basis of K_f.

`nfdisc(f(x))` gives the discriminant of the number field K_f.

`nfinit(f(x))` is a long vector containing information about the number field K_f. It starts off as `[f(x),[r1,r2],d, I,...]` where `r1` and `r2` are the number of real embeddings and half the number of complex (no real) embeddings. `d` is $\mathrm{disc}(K)$, and `I` is the index $[\mathcal{O}_K : \mathbf{Z}[\alpha]]$ for α a root of $f(x)$. As with `bnfinit`, it is best to use this command as a definition, say `v = nfinit(f(x));` with the semi-colon at the end.

`nfisincl(f(x),g(x))` is a vector whose components describe the roots of $f(x)$ as polynomials in a root of $g(x)$ if this possible (that is, if the number field defined by a root of $f(x)$ has an embedding into the number field defined by a root of $g(x)$). When $g(x) = f(x)$ and a root of $f(x)$ generates a Galois extension of $\mathbf{Q}$, the output provides formulas for the Galois group acting on a root of $f(x)$.

`nfrootsof1(nfinit(f(x)))` is the number of roots of unity in K_f.

`zetak(zetakinit(f(x)),s)` is $\zeta_{K_f}(s)$, where s is a complex number. (The output may not be accurate if s is unreasonably chosen.)

There are many further commands (*e.g.*, , to add and multiply ideals or test if an ideal is principal), but the above is a basic list to get started.

Note: PARI does arithmetic with fractions exactly. If you want PARI to treat a rational number as a decimal approximation, multiply it by 1.0, *e.g.*, `3/7*1.0`. The numbers π and i are entered in PARI as `Pi` and `I`, and e^z is `exp(z)`. Make sure to include multiplication operations explicitly: $2x$ and $2i$ are entered into PARI as `2*x` and `2*I`, *not* as `2x` and `2I`.

The meaning of any PARI command can be found by typing `?` followed by the command, *e.g.*, `?nfbasis` tells you what `nfbasis` does. Of course this only helps if you know the name of the command. To get a complete list of all PARI commands, type `?`, and a list of the number field commands is `?6`.

For the most part, the PARI commands above receive exact input (*e.g.*, `nfbasis` expects an integral polynomial). The only command where the input is an approximation and the output is expected to be exact, rather than another approximation, is the minimal polynomial command `algdep`. This command produces good answers under reasonable conditions, but when the correct minimal polynomial has very large coefficients there can be errors.

Example 1. In PARI, set `f(x) = x^3 + 453603*x^2 + 51438694443*x - 51247953119` and then type `v = polroots(f(x))`. The answer is a vector of length three whose first coordinate is `0.99628311790670270346685176802 + 0.E-28*I`. This is (approximately) the unique real root of $f(x)$. If you now type `algdep(v[1],3)` to find the minimal polynomial over $\mathbf{Q}$ of the first coordinate of v, knowing it should have degree at most 3, the answer is not $f(x)$. Instead it is `287542*x^3 + 101724*x^2 - 365673*x - 21003` (which is very small at that number, roughly 10^{-19}). If you type `algdep(v[1],10)` the answer turns out to be $(x-1)^9(x+1)$, which is wrong in an even worse way.

As practice with these commands, let's run through PARI computations on the quartic field $K = \mathbf{Q}(\sqrt[4]{65})$. (This will be much more meaningful if you download PARI and follow the steps yourself.)

(1) What is a $\mathbf{Z}$-basis of $\mathcal{O}_K$?
Type `nfbasis(x^4-65)` and we get the answer
`[1, x, 1/2*x^2 + 1/2, 1/4*x^3 + 1/4*x^2 + 1/4*x + 1/4]`.
which means $\{1, \sqrt[4]{65}, \frac{\sqrt{65}+1}{2}, \frac{\sqrt[4]{65}^3+\sqrt{65}+\sqrt[4]{65}+1}{4}\}$ is a $\mathbf{Z}$-basis.

(2) What is a polynomial over $\mathbf{Q}$ for the fourth term in the $\mathbf{Z}$-basis?
Set `r = polroots(x^4-65)[1]`, which is
`-2.8394115144336774440822629 39 + 0.E-28*I`.
(This is $-\sqrt[4]{65}$, so setting `r = real(polroots(x^4-65)[1])` will remove the imaginary part.) The command `algdep(r^3/4 + r^2/4 + r/4 + 1/4,4)` returns
`x^4 - x^3 - 24*x^2 - 256*x - 1024`.
(It would have been more efficient to set `b = nfbasis(x^4-65);` in the first question and then compute `algdep(subst(b[4],x,r))` to avoiding having to type the polynomial expression in `r` inside `algdep`.)

(3) What is the discriminant of K?
Type `d = nfdisc(x^4 - 65)` and we get

`-1098500`.

Its factorization is found with `factor(d)`:

```
[-1 1]
[2 2]
[5 3]
[13 3]
```

which means $\mathrm{disc}(K) = -2^2 \cdot 5^3 \cdot 13^3$. The ramified primes in K are 2, 5, and 13.

(4) What is $[\mathcal{O}_K : \mathbf{Z}[\sqrt[4]{65}]]$?

This can be found in two ways. First, the discriminant of $x^4 - 65$ is found with `poldisc(x^4-65)` and it is

`-70304000`

whose factorization is $-2^8 \cdot 5^3 \cdot 13^3$. This discriminant divided by $\mathrm{disc}(K)$ is $2^6 = 8^2$, so $[\mathcal{O}_K : \mathbf{Z}[\sqrt[4]{65}]] = 8$. As an alternate solution, the fourth component of `nfinit(x^4-65)` is this index, so we can find it by computing `nfinit(x^4-65)`, which is

```
[x^4 - 65, [2, 1], -10985000, 8, ...]
```

and looking at the fourth component, or type `nfinit(x^4-65)[4]` directly.

(5) What is the shape of the prime ideal factorizations of 2, 3, 5, and 7 in K?

Set `K = nfinit(x^4-65);` and type `idealfactor(K,2)`. We get

```
[[2, [-1, 0, 0, 1] , 1, 1, [0, 0, 0, 1] ] 1]
[[2, [0, 1, -1, 0] , 2, 1, [1, 1, 0, 0] ] 2]
[[2, [2, 0, 1, 1] , 1, 1, [1, 0, 1, 1] ] 1]
```

so $2\mathcal{O}_K = \mathfrak{p}_2\mathfrak{p}_2'^2\mathfrak{p}_2''$. Similarly, `idealfactor(K,3)` returns

```
[[3, [0, -1, 2, 0] , 1, 2, [0, 1, -1, 0] ] 1]
[[3, [0, 1, 2, 0] , 1, 2, [0, -1, -1, 0] ] 1]
```

so $3\mathcal{O}_K = \mathfrak{p}_9\mathfrak{p}_9'$. Typing `idealfactor(K,5)` and `idealfactor(K,7)` returns

```
[[5, [0, 1, 0, 0] , 4, 1, [2, -1, 2, -1] ] 4]
```

and

```
[[7, [5, 1, 0, 0] , 1, 1, [-2, 3, -1, -3] ] 1]
[[7, [9, 1, 0, 0] , 1, 1, [-1, 3, -2, -3] ] 1]
[[7, [-2, 0, 2, 0] , 1, 2, [-3, 0, 2, 0] ] 1]
```

so $5\mathcal{O}_K = \mathfrak{p}_5^4$ and $7\mathcal{O}_K = \mathfrak{p}_7\mathfrak{p}_7'\mathfrak{p}_{49}$.

For the primes 3 and 7, which don't divide $\mathrm{disc}(x^4 - 65)$, we can also obtain the shape of their factorization in K from the degree types of factorizations of $x^4 - 65$ mod 3 and 5: `factormod(x^4-65,3)` and `factormod(x^4-65,5)` return

```
[Mod(1, 3)*x^2 + Mod(1, 3)*x + Mod(2, 3) 1]
[Mod(1, 3)*x^2 + Mod(2, 3)*x + Mod(2, 3) 1]
```

and

```
[Mod(1, 7)*x + Mod(2, 7) 1]
[Mod(1, 7)*x + Mod(5, 7) 1]
[Mod(1, 7)*x^2 + Mod(4, 7) 1].
```

(6) What is the class group of K?

Type `bnfclgp(x^4 - 65)` and we get

```
[4, [2, 2], ...]
```

where only the first two components of the answer are given here. This tells us $h(K) = 4$ and $\mathrm{Cl}(K)$ is a product of two cyclic groups of order 2.

(7) What is a system of fundamental units of K?

Since $r_1 = 2$ and $r_2 = 1$, the unit group has rank 2 by the unit theorem and `bnfinit(x^4 - 65).fu` returns the answer

```
[Mod(x^2 + 8, x^4 - 65),
Mod(1096*x^3 - 3112*x^2 + 8836*x - 25089, x^4 - 65]
```

which is giving us numbers in $\mathbf{Q}(\sqrt[4]{65})$ as elements of $\mathbf{Q}[x]/(x^4 - 65)$. The unit group (modulo ± 1) is generated by $\sqrt{65}+8$ and $1096\sqrt[4]{65}^3 - 3112\sqrt{65} + 8836\sqrt[4]{65} - 25089$.

(8) What is the regulator of K?

The command `R = bnfreg(x^4-65)` returns `63.950452792426709750086292 69`.

(9) How does $\zeta_K(s)$ begin?

Recalling that `K = nfinit(x^4-65)`, typing `dirzetak(K,10)` returns `[1, 3, 0, 6, 1, 0, 2, 10, 2, 3]` so

$$\zeta_K(s) = 1 + \frac{3}{2^s} + \frac{6}{4^s} + \frac{1}{5^s} + \frac{2}{7^s} + \frac{10}{8^s} + \frac{2}{9^s} + \frac{3}{10^s} + \cdots.$$

(10) What is $\zeta_K(2)$?

Set `Z = zetakinit(x^4-65);` and then `zetak(Z,2)` has value `2.6789530905706088229936116 23.`

(11) Let's numerically check the leading term formulas

$$\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} hR}{w\sqrt{|\mathrm{disc}(K)|}} \frac{1}{s-1} + \cdots \text{ for } s \text{ near } 1$$

and

$$\zeta_K(s) = -\frac{hR}{w} s^{r_1+r_2-1} + \cdots \text{ for } s \text{ near } 0.$$

Since $r_1 > 0$, $w = 2$ and `2^2*(2*Pi)*4*R/(2*sqrt(abs(d)))` is `3.0669976873807157299912283 80.`

This is supposed to be the limit of $\zeta_K(s)(s-1)$ as $s \to 1$. Set `g(x) = zetak(Z,x)*(x-1)` and evaluate this for `x` close to 1: `g(1.000001)` is `3.0669965409258450512531022 76`

which matches the previous computation to 5 digits after the decimal point.

Turning to behavior at $s = 0$, `-4*R/2` has value `-127.90090558485341950017258 54.`

This is the limit of $\zeta_K(s)/s^2$ as $s \to 0$. Set `G(x) = zetak(Z,x)/x^2` and evaluate it at a small value of `x`: `G(1/10^10)` is `-127.90090553528822020881917 97,`

which matches the computation of $-hR/w$ to 7 digits after the decimal point.