Examples: Number Fields

Using the program pari-gp the calcullator gives us 50-decimal places of roots of polynomial $f(x) = x^3 + 10x - 12$.

Ex if we solve $f(x) = 0$ accurate two 2 or 5 decimal places?

So here's the answer accurate to 50 decimal places. The answer runs off the page.

```
? F = nfinit(x^3 +10*x - 12)
%1 = [x^3 + 10*x - 12, [1, 1], -1972, 2,
[[1, 1.0755719270367992295362348940064398938, 3.5784274851148268827250
 [1, 1.0755719270367992295362348940064398938, 3.5784274851148268827250
 [16, 17, 57; 16, 44, -65; 16, -61, -8],
 [3, 0, -1; 0, -20, 18; -1, 18, 17],
 [986, 588, 950; 0, 2, 1; 0, 0, 1],
 [332, 9, 10; 9, -25, 27; 10, 27, 30],
 [986, [329, -2070, 2082; 346, 327, -689; 1, 692, 330]], [2, 17, 29]],
 [1.0755719270367992295362348940064398938, -0.537785963518399614768117
]
```

The number field database page returns the "integral basis" (basis as a $\mathbb{Z}$-module) of the ring of integers $\mathcal{O}_F \simeq 1 \cdot \mathbb{Z} + a \cdot \mathbb{Z} + \frac{1}{2}a^2 \cdot \mathbb{Z}$ (e.g. this is an **integral domain**) (`https://www.lmfdb.org/NumberField/3.1.1972.1`) The ideal class group quotient of the **fractional ideals** modulo the **principal fractional ideals**.

The unit group is $\mathcal{O}_K^\times = \langle a - 1 \rangle \simeq \mathbb{Z}$.

Let's try to get more answers from the computer. Notice the positive result on the first try:

```
? idealfactor(F,5)
%2 =
[[5, [2, 1, 0]~, 1, 1, [-2, 24, 0; -2, -6, 10; 2, -4, 0]] 1]

[   [5, [-2, -2, 2]~, 1, 2, [2, -6, 6; 1, 2, -2; 0, 2, 2]] 1]
```

and keep looking. The ideal $\mathfrak{p} = 7$ is "prime" in F ...

```
? idealfactor(F,7)
%3 =
[[7, [7, 0, 0]~, 1, 3, 1] 1]
```

The next result $\mathfrak{p} = 11$ factors:

```
? idealfactor(F,11)
%4 =
[[11, [5, 1, 0]~, 1, 1, [-4, 42, -18; -5, -8, 16; 2, -10, -2]] 1]

[      [11, [-4, -5, 2]~, 1, 2, [5, -6, 6; 1, 5, -2; 0, 2, 5]] 1]
```

and we continue to get more answers:

```
? idealfactor(F,13)
%5 =
[[13, [13, 0, 0]~, 1, 3, 1] 1]

? idealfactor(F,17)
%6 =
[[17, [5, 1, 0]~, 2, 1, [-5, 42, -18; -5, -9, 16; 2, -10, -3]] 2]

[  [17, [7, 1, 0]~, 1, 1, [2, 54, -30; -7, -2, 20; 2, -14, 4]] 1]
```

Our result of the “splitting of the primes” is successful, once we type up our result or $\mathfrak{p} = 19, 23, 29$.

```
? idealfactor(F,19)
%7 =
[[19, [19, 0, 0]~, 1, 3, 1] 1]

? idealfactor(F,23)
%8 =
[  [23, [-4, 1, 0]~, 1, 1, [-3, -12, 36; 4, -7, -2; 2, 8, -1]] 1]

[       [23, [1, 1, 0]~, 1, 1, [5, 18, 6; -1, 1, 8; 2, -2, 7]] 1]

[[23, [3, 1, 0]~, 1, 1, [-10, 30, -6; -3, -14, 12; 2, -6, -8]] 1]

? idealfactor(F,29)
%9 =
[ [29, [-8, 1, 0]~, 1, 1, [10, -36, 60; 8, 6, -10; 2, 16, 12]] 1]

[[29, [4, 1, 0]~, 2, 1, [-9, 36, -12; -4, -13, 14; 2, -8, -7]] 2]
```

The Galois group is S_3 so the equation is “solvable”. Litrally solvable has to do with the permutations of the variables in solving the cubic equation. We would also like to see the “box” implied by the Dirichlet unit theorem.

Here's a more straightforward example:

```
parisize = 8000000, primelimit = 500000
? F = nfinit(x^3 + 5)
%1 = [x^3 + 5, [1, 1], -675, 1,
[[ 1, -1.7099759466766969893531088725438601099, 2.924017738212866065500
 [ 1, -1.7099759466766969893531088725438601099, 2.924017738212866065500
 [-1.7099759466766969893531088725438601099, 0.854987973338348494676554
```

Let's try any prime $\mathfrak{p}$ with $N(\mathfrak{p}) < 5 \times 10^4$:

The prime $\mathfrak{p} = 7$ remains prime. $7\mathcal{O}_F$ is "prime".

```
? idealfactor(F,7)
%3 =
[[7, [7, 0, 0]~, 1, 3, 1] 1]
```

The prime $p = 11$ "splits":

$$11\mathcal{O}_F = \big(11\mathcal{O}_F + (3 + \sqrt[3]{-5})\mathcal{O}_F\big)\big(11\mathcal{O}_F + (-1) \times (2 + 3\sqrt[3]{-5})\mathcal{O}_F\big)$$

```
? idealfactor(F,11)
%4 =
[[11, [3, 1, 0]~,   1, 1, [-2, -5, 15; -3, -2, -5; 1, -3, -2]] 1]

[[11, [-2, -3, 1]~, 1, 2, [3, 0, -5; 1, 3, 0; 0, 1, 3]]         1]

? idealfactor(F,13)
%5 =
[[13, [-6, 1, 0]~, 1, 1, [-3, -5, -30; 6, -3, -5; 1, 6, -3]] 1]

[[13, [-5, 1, 0]~, 1, 1, [-1, -5, -25; 5, -1, -5; 1, 5, -1]] 1]

[[13, [-2, 1, 0]~, 1, 1, [4, -5, -10 ; 2,  4, -5; 1, 2,  4]] 1]
```

The "splitting of the primes" looks somewhat controversial to me. In a number field extension, Spec($\mathbb{Z}$) $\to$ Spec($\mathbb{Z}[\sqrt[3]{-5}]$). These are specific number systems. We could find "rings" or even "schemes" with nice factorization properties if we "commit" to certain arithmetic rules.

Here are some definitions from Ring Theory. Here "rings" were just collections of numbers or collections of formulas that behaved nicely together:

- $A + B = \{a + b : a \in A$ and $b \in\}$
- $A \times B = \{a \times b : a \in A$ and $b \in\}$

These formulas work as numbers or as "formulas":

- $2\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z}$ (written somewhat tersely as

  o $(2) + (3) = (1)$ or

  o $(3) + (5) = (1)$ or

  o $(5) + (7) = (1)$

  o too-good-to-be-true.

The last formula $\mathfrak{p} = 13$ is a product of ideals:

$$\begin{aligned} 13\mathcal{O}_F &= \big(13\mathcal{O}_F + (-6 + \sqrt[3]{-5})\mathcal{O}_F\big) \\ &\times \big(13\mathcal{O}_F + (-5 + \sqrt[3]{-5})\mathcal{O}_F\big) \\ &\times \big(13\mathcal{O}_F + (-2 + \sqrt[3]{-5})\mathcal{O}_F\big) \end{aligned}$$

The factorization differs is we consider $\mathcal{O}_F$ as a $\mathbb{Z}$-module or as a $\mathbb{Q}$-vector space.

$$\mathcal{O}_F = \mathbb{Z}[\sqrt[3]{-5}] \simeq \mathbb{Z}[x]/(x^3 + 5)$$

The encyclopedic entry (`https://www.lmfdb.org/NumberField/3.1.675.1`) has that:

$$\big(\mathbb{Z}[x]/(x^3 + 5)\big)^\times \simeq \langle 2x^2 - 4x + 1\rangle$$

There is also "trivial" class group, so there is still unique factorization here.

References

[1]