# Algebraic Number Theory

First, we create a number field.

```
K.<a> = NumberField(x^3 - 15*x^2 - 94*x - 3674); K
```

```
Number Field in a with defining polynomial x^3 - 15*x^2 - 94*x -
3674
```

```
Oa = K.order(a); Oa
```

```
Order in Number Field in a with defining polynomial x^3 - 15*x^2 -
94*x - 3674
```

```
OK = K.ring_of_integers(); OK
```

```
Maximal Order in Number Field in a with defining polynomial x^3 -
15*x^2 - 94*x - 3674
```

```
Oa.index_in(OK)
```

```
2197
```

```
OK.basis()
```

```
[25/169*a^2 + 10/169*a + 1/169, 5/13*a^2 + 1/13*a, a^2]
```

```
K.complex_embeddings(); K.signature()
```

```
[
Ring morphism:
  From: Number Field in a with defining polynomial x^3 - 15*x^2 -
94*x - 3674
  To:   Complex Field with 53 bits of precision
  Defn: a |--> -4.88896809422969 - 11.1523571457373*I,
Ring morphism:
  From: Number Field in a with defining polynomial x^3 - 15*x^2 -
94*x - 3674
  To:   Complex Field with 53 bits of precision
  Defn: a |--> -4.88896809422969 + 11.1523571457373*I,
Ring morphism:
  From: Number Field in a with defining polynomial x^3 - 15*x^2 -
94*x - 3674
  To:   Complex Field with 53 bits of precision
  Defn: a |--> 24.7779361884594
]
(1, 1)
```

```
U = K.unit_group(); U; K.units()[0]==U.1
```

```
Unit group with structure C2 x Z of Number Field in a with definir
polynomial x^3 - 15*x^2 - 94*x - 3674
True
```

```
K.<g>=NumberField(x^2-15); K.class_number()
```

```
2
```

```
L.<n>=QQ[15^(1/2)]; L.class_number()
```

```
2
```

```
eqn =  x^3 + 2^(1/3)*x + 5 == 0
```

```
solve(eqn, x)
```

```
[x == -1/2*(I*sqrt(3) + 1)*(1/18*sqrt(3)*sqrt(683) - 5/2)^(1/3) +
1/6*(-I*sqrt(3) + 1)*2^(1/3)/(1/18*sqrt(3)*sqrt(683) - 5/2)^(1/3),
== -1/2*(-I*sqrt(3) + 1)*(1/18*sqrt(3)*sqrt(683) - 5/2)^(1/3) +
1/6*(I*sqrt(3) + 1)*2^(1/3)/(1/18*sqrt(3)*sqrt(683) - 5/2)^(1/3),
== (1/18*sqrt(3)*sqrt(683) - 5/2)^(1/3) -
1/3*2^(1/3)/(1/18*sqrt(3)*sqrt(683) - 5/2)^(1/3)]
```

```
a = solve(eqn, x)[0].rhs()
```

```
show(a)
```

$$-\frac{1}{2}\left(i\sqrt{3}+1\right)\left(\frac{1}{18}\sqrt{3}\sqrt{683}-\frac{5}{2}\right)^{\left(\frac{1}{3}\right)}+\frac{\left(-i\sqrt{3}+1\right)2^{\left(\frac{1}{3}\right)}}{6\left(\frac{1}{18}\sqrt{3}\sqrt{683}-\frac{5}{2}\right)^{\left(\frac{1}{3}\right)}}$$

```
K.<b>=QQ[a]; K
```

```
Number Field in a with defining polynomial x^9 + 15*x^6 + 77*x^3 +
125
```

```
K.degree()
```

```
9
```

```
K.discriminant()
```

```
401359343367744
```

```
K.is_galois()
```

```
False
```

```
G=K.galois_group(names='prim')
G.order(); G
```

```
36
Galois group of Galois closure in prim of Number Field in a with
defining polynomial x^9 + 15*x^6 + 77*x^3 + 125
```

```
K.class_number()
```

```
2
```

```
O=K.ring_of_integers(); O.basis()
```

```
[1, 3/5*a^7 + 1/5*a, 13/25*a^8 + 4/5*a^5 + 1/25*a^2, a^3, a^4, a^5
a^6, a^7, a^8]
```

```
K.primes_above(3); P=K.primes_above(3)[0];
P.residue_class_degree(); P.ramification_index()
```

```
[Fractional ideal (3, a^3 - a + 5)]
3
3
```

```
y = PolynomialRing(GF(3), 'y').gen()
```

```
f=y^9 + 15*y^6 + 77*y^3 + 125; f.factor()
```

```
(y^3 + 2*y + 2)^3
```

```
List=K.primes_above(5); len(List); List
```

```
5
[Fractional ideal (5, 1/25*a^8 - 2/5*a^7 - a^6 + 3/5*a^5 - 6*a^4 -
10*a^3 + 77/25*a^2 - 104/5*a - 26), Fractional ideal (5, -1/25*a^8
2/5*a^7 - 2*a^6 - 3/5*a^5 + 6*a^4 - 20*a^3 - 77/25*a^2 + 104/5*a -
53), Fractional ideal (5, a^2 - 2*a - 2), Fractional ideal (5, a^2
2*a - 2), Fractional ideal (5, a^2 - 2)]
```

```
P=K.primes_above(5)[0]; P.residue_class_degree();
P.ramification_index()
```

```
1
1
```

```
z = PolynomialRing(GF(5), 'z').gen()
```

```
g=z^9 + 15*z^6 + 77*z^3 + 125; g.factor()
```

```
z^3 * (z^2 + 3) * (z^2 + 2*z + 3) * (z^2 + 3*z + 3)
```

```
L.<c>=QQ[3^(1/3)+2^(1/2)]; L
```

```
Number Field in a with defining polynomial x^6 - 6*x^4 - 6*x^3 +
12*x^2 - 36*x + 1
```

```
L.is_galois()
```

```
False
```

```
G=L.galois_group(names='d'); G.order()
```

```
12
```

```
C=L.class_group(); C
```

```
Class group of order 2 with structure C2 of Number Field in sqrt15
with defining polynomial x^2 - 15
```

```
L.unit_group()
```

```
Unit group with structure C2 x Z of Number Field in sqrt15 with
defining polynomial x^2 - 15
```

```
L.units()
```

```
[sqrt15 - 4]
```

```
M.<j>=QQ[sqrt(3)];M.units()[0].trace()
```

```
-4
```

```
M.minkowski_bound()
```

```
sqrt(3)
```

```
M.Minkowski_embedding()
```

```
[ 1.00000000000000000000000000000
-1.73205080756887729352744634151]
[ 1.00000000000000000000000000000
1.73205080756887729352744634151]
```

```
O=M.ring_of_integers(); O
```

```
Maximal Order in Number Field in sqrt3 with defining polynomial x^
- 3
```

```
O.basis()
```

```
[1, sqrt3]
```

```
P=M.prime_above(2); P; P.decomposition_group()
```

```
Fractional ideal (sqrt3 + 1)
Galois group of Number Field in sqrt3 with defining polynomial x^2
3
```

```
Q=M.prime_above(11); Q; Q.decomposition_group()
```

```
Fractional ideal (-2*sqrt3 + 1)
Subgroup [()] of Galois group of Number Field in sqrt3 with defini
polynomial x^2 - 3
```

```
for p in primes(100):
    print p, len(M.primes_above(p)), Mod(p,12), Mod(p,6)
```

```
2 1 2 2
3 1 3 3
5 1 5 5
7 1 7 1
11 2 11 5
13 2 1 1
17 1 5 5
19 1 7 1
23 2 11 5
29 1 5 5
31 1 7 1
37 2 1 1
41 1 5 5
43 1 7 1
47 2 11 5
53 1 5 5
59 2 11 5
61 2 1 1
67 1 7 1
71 2 11 5
73 2 1 1
79 1 7 1
83 2 11 5
89 1 5 5
97 2 1 1
```