In [1]:
```
print("Suppose that we have a solution in integers to the Mordell equation\n\n"
    "\t\t  x^3 = y^2-2.\n\n"
    "By descent, one can show that y+sqrt(2) = (1+sqrt(2))^c * (a+b*sqrt(2))^3,\n"
    "where the power c is 0, 1 or -1. The case c=0 is easy to deal with, and does not lead to any solutions.\n"
    "The cases c=1 and c=-1 are equivalent.\n\n")

print("We focus on the case c=1, which leads to the following equation:")

var('a b')
rt2=sqrt(2)
pretty_print("y +", rt2," = ", expand( (1+rt2) * (a+b*rt2)^3 ))
```

```
Suppose that we have a solution in integers to the Mordell equation

                  x^3 = y^2-2.

By descent, one can show that y+sqrt(2) = (1+sqrt(2))^c * (a+b*sqrt(2))^3,
where the power c is 0, 1 or -1. The case c=0 is easy to deal with, and does not lead to any solutions.
The cases c=1 and c=-1 are equivalent.


We focus on the case c=1, which leads to the following equation:
```

$y + \sqrt{2} = \sqrt{2}a^3 + 3\sqrt{2}a^2b + 6\sqrt{2}ab^2 + 2\sqrt{2}b^3 + a^3 + 6a^2b + 6ab^2 + 4b^3$

In [2]:
```
print("Equating coefficients of sqrt(2), we obtain the Thue equation:\n")
print("\t\t  a^3 + 3*a^2*b + 6*a*b^2+ 2*b^3 = 1.\n")
print("This implies that if we let alpha be a root of the polynomial\n")
f(x) = x^3 + 3*x^2 + 6*x + 2
print("\t\t  f(x)=", f(x),",\n")
print("then a+b*alpha is a unit in the ring Z[alpha].")
```

```
Equating coefficients of sqrt(2), we obtain the Thue equation:

                  a^3 + 3*a^2*b + 6*a*b^2+ 2*b^3 = 1.

This implies that if we let alpha be a root of the polynomial

                  f(x)= x^3 + 3*x^2 + 6*x + 2 ,

then a+b*alpha is a unit in the ring Z[alpha].
```

In [3]:
```
print("Define k to be the field generated by alpha.")

k.<alpha> = NumberField(f)

print("There are three homomorphisms tau, tau2, sigma from k2 to the complex numbers.\n"
      "The third of these is a homomorphism to the real numbers. tau2 is the complex conjugate of tau.\n")

tau, tau2, sigma = k.embeddings(CC)
print( tau, tau2, sigma)
```

```
Define k to be the field generated by alpha.
There are three homomorphisms tau, tau2, sigma from k2 to the complex numbers.
The third of these is a homomorphism to the real numbers. tau2 is the complex conjugate of tau.

Ring morphism:
  From: Number Field in alpha with defining polynomial x^3 + 3*x^2 + 6*x + 2
  To:   Complex Field with 53 bits of precision
  Defn: alpha |--> -1.29803581899166 - 1.80733949445202*I Ring morphism:
  From: Number Field in alpha with defining polynomial x^3 + 3*x^2 + 6*x + 2
  To:   Complex Field with 53 bits of precision
  Defn: alpha |--> -1.29803581899166 + 1.80733949445202*I Ring morphism:
  From: Number Field in alpha with defining polynomial x^3 + 3*x^2 + 6*x + 2
  To:   Complex Field with 53 bits of precision
  Defn: alpha |--> -0.403928362016678
```

In [4]:
```
print("Sage finds the following unit u and claims that it is the fundamental unit.\n"
      "This means that every other unit in ZZ[alpha] has the form u^n or -u^n for some integer n")

u = (k.units()[0])^-1
pretty_print("u=",u)

print("sigma(u) is approximately", sigma(u))
```

```
Sage finds the following unit u and claims that it is the fundamental unit.
This means that every other unit in ZZ[alpha] has the form u^n or -u^n for some integer n
```

$u = 5\alpha^2 + 13\alpha + 25$

```
sigma(u) is approximately 20.5647219019906
```

In [5]:
```
print("To prove in lean that `u` is a fundamental unit, it is enough to\n"
    "check that there are no units w satisfying  1 < sigma(w) <= sqrt(sigma(u)).\n"
    "Any such w would have norm 1, so would also satisfy the (equivalent) bounds |tau(w)|, |tau2(w)| < 1.\n")

print("We shall make a list containing all the elements of `ZZ[beta]` satisfying these bounds.")

sigma_bound = sqrt(sigma(u))
tau_bound = 1
```

```
To prove in lean that `u` is a fundamental unit, it is enough to
check that there are no units w satisfying  1 < sigma(w) <= sqrt(sigma(u)).
Any such w would have norm 1, so would also satisfy the (equivalent) bounds |tau(w)|, |tau2(w)| < 1.

We shall make a list containing all the elements of `ZZ[beta]` satisfying these bounds.
```

In [6]:
```
print("Give an element A = x + y *alpha + z*alpha^2, the vector (sigma(a), tau(A), tau2(A))^t\n"
     "is equal to M*(x,y,z)^t, where M is the following Vardermonde matrix:")

M = Matrix([[1, sigma(alpha), sigma(alpha^2)],[1, tau(alpha), tau(alpha^2)],[1, tau(alpha).conjugate(), tau(alpha^2).conjugate()]])
pretty_print(M)
```

```
Give an element A = x + y *alpha + z*alpha^2, the vector (sigma(a), tau(A), tau2(A))^t
is equal to M*(x,y,z)^t, where M is the following Vardermonde matrix:
```

$$\begin{pmatrix} 1.00000000000000 & -0.403928362016678 & 0.163158121641477 \\ 1.00000000000000 & -1.29803581899166 - 1.80733949445202i & -1.58157906082074 + 4.69198280175401i \\ 1.00000000000000 & -1.29803581899166 + 1.80733949445202i & -1.58157906082074 - 4.69198280175401i \end{pmatrix}$$

In [7]:
```
print("Given an element A = x + y*alpha + z*alpha^2, we have\n\n"
    "\t\t(sigma A, tau A, tau2 A)^t = M * (x, y, z)^t.\n\n"
    "We have bounds on sigma A, tau A, tau2 A, and we would like to obtain bounds on x,y,z.\n"
    "We can find such bounds by inverting the matrix M.")
M_inv = M^-1
pretty_print("M^-1=", M_inv)
```

```
Given an element A = x + y*alpha + z*alpha^2, we have

                (sigma A, tau A, tau2 A)^t = M * (x, y, z)^t.

We have bounds on sigma A, tau A, tau2 A, and we would like to obtain bounds on x,y,z.
We can find such bounds by inverting the matrix M.
```

$$\text{M\^{}-1=}\begin{pmatrix} 1.21777907219993 - 2.77555756156289 \times 10^{-17}i & -0.108889536099963 + 0.0578780218746513i & -0.108889536099963 - 0.0578780218746513i \\ 0.638497985900640 - 5.55111512312578 \times 10^{-17}i & -0.319248992950320 + 0.118714328674823i & -0.319248992950320 - 0.118714328674823i \\ 0.245947752965953 - 4.16333634234434 \times 10^{-17}i & -0.122973876482977 - 0.0608363068001714i & -0.122973876482977 + 0.0608363068001714i \end{pmatrix}$$

In [8]:
```
M_inv_bound = Matrix( [[abs(r) for r in row] for row in M_inv])
print("Here is the matrix of absolute values of entries of M^-1:")
pretty_print(M_inv_bound)


print("This gives the following bounds on x, y and z:")
x_bound, y_bound, z_bound = (M_inv_bound * column_matrix([sigma_bound,tau_bound,tau_bound])).list()

print("|x| <", x_bound)
print("|y| <", y_bound)
print("|z| <", z_bound)
```

```
Here is the matrix of absolute values of entries of M^-1:
```

$$\begin{pmatrix} 1.21777907219993 & 0.123315840378225 & 0.123315840378225 \\ 0.638497985900640 & 0.340606828076754 & 0.340606828076754 \\ 0.245947752965953 & 0.137199236595307 & 0.137199236595307 \end{pmatrix}$$

```
This gives the following bounds on x, y and z:
|x| < 5.76905795678341
|y| < 3.57669620715361
|z| < 1.38973077320733
```

In [9]:
```
print("If A = x+y*alpha+z*alpha^2 is a unit and 1 < sigma(A) <= sqrt(sigma(u)) then we must have\n\n"
      "\t\t|x| <=5, |y| <= 3 and |z| <= 1\n\n"
    "Since we are free to replace A by -A, we may also assume without loss of generality that\n\n"
      "\t\tx >= 0.\n\n"
    "The number of elements of Z[alpha] satisfying these bounds is 6 * 7 * 3 = 126. This is the number of cases which lean must check
    "Here is the list of all ring elements satisying these bounds, which are units.")

pretty_print([x + y*alpha +z * alpha^2 for x in range(6) for y in range(-3, 4) for z in range(-1, 2)
       if (x+y*alpha +z * alpha^2).norm().abs() == 1])

print("These units are u^0 and -u^-1 respectively:")

pretty_print("u^-1 = ", -u^-1)

print("Hence u is a fundamental unit.")
```

```
If A = x+y*alpha+z*alpha^2 is a unit and 1 < sigma(A) <= sqrt(sigma(u)) then we must have

                |x| <=5, |y| <= 3 and |z| <= 1

Since we are free to replace A by -A, we may also assume without loss of generality that

                x >= 0.

The number of elements of Z[alpha] satisfying these bounds is 6 * 7 * 3 = 126. This is the number of cases which lean must check.

Here is the list of all ring elements satisying these bounds, which are units.
```

$$\left[1, \alpha^2 + 3\alpha + 1\right]$$

```
These units are u^0 and -u^-1 respectively:
```

u^-1 $= \alpha^2 + 3\alpha + 1$

```
Hence u is a fundamental unit.
```

In [ ]: