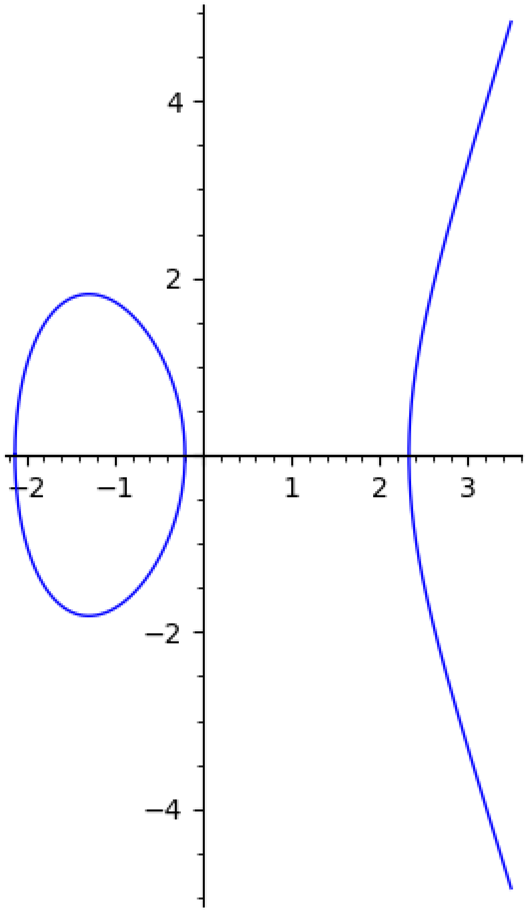
In [51]:
```
E = EllipticCurve([-5, -1])
```

In [52]:
```
E
```

Out[52]:
```
Elliptic Curve defined by y^2 = x^3 - 5*x - 1 over Rational Field
```

In [53]:
```
E.plot(aspect_ratio=True)
```

Out[53]:



In [57]:
```
P = E.an_element()
P
```

Out[57]:
```
(-2 : 1 : 1)
```

In [58]:
```
Q = E(-2, -1)
Q
```

Out[58]:
```
(-2 : -1 : 1)
```

In [60]:
```
P + Q
```

Out[60]:
```
(0 : 1 : 0)
```

In [61]:
```
2*P
```

Out[61]:
```
(65/4 : -519/8 : 1)
```

In [62]:
```
R = 2*P
R
```

Out[62]: (65/4 : -519/8 : 1)

In [63]:
```
Zp = IntegerModRing(31)
Zp
```

Out[63]: Ring of integers modulo 31

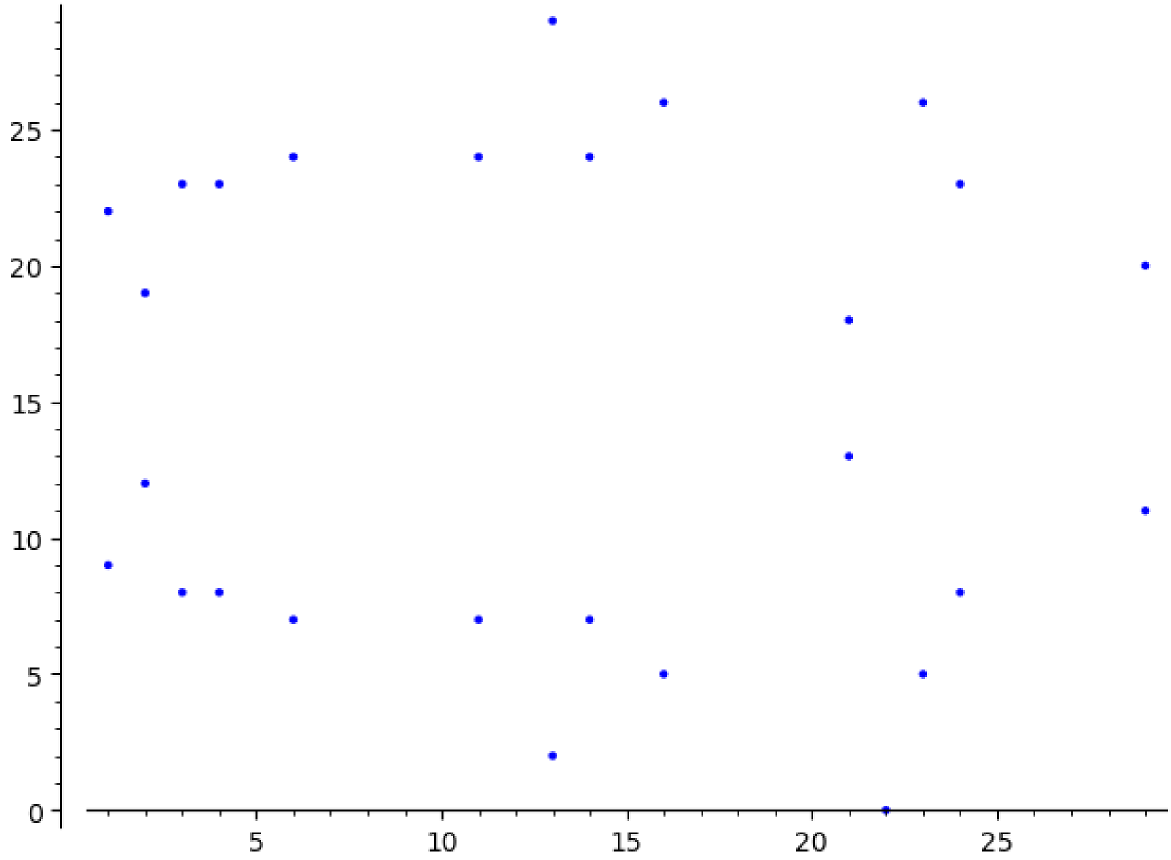
In [64]:
```
a = Zp.random_element()
b = Zp.random_element()
```

In [65]:
```
E = EllipticCurve(Zp, [a, b])
E
```

Out[65]: Elliptic Curve defined by y^2 = x^3 + 25*x + 24 over Ring of integers modulo 31

In [66]:
```
E.plot()
```

Out[66]:



In [67]:
```
E.cardinality()
```

Out[67]: 28

In [70]:
```
P = E.random_point()
Q = E.random_point()
P, Q
```

Out[70]: ((4 : 8 : 1), (21 : 18 : 1))

In [71]:
```
P+Q
```

Out[71]: (16 : 5 : 1)

In [72]:
```
28*P
```
Out[72]:
```
(0 : 1 : 0)
```
In [74]:
```
for k in divisors(28):
    print(k*P, k)
```
```
(4 : 8 : 1) 1
(11 : 24 : 1) 2
(16 : 26 : 1) 4
(3 : 23 : 1) 7
(22 : 0 : 1) 14
(0 : 1 : 0) 28
```
In [75]:
```
a = 5
Q = 5*P
ChPub = E, P, Q
ChPub
```
Out[75]:
```
(Elliptic Curve defined by y^2 = x^3 + 25*x + 24 over Ring of integers modulo 31,
 (4 : 8 : 1),
 (21 : 13 : 1))
```
In [76]:
```
Mens = E.random_point()
Mens
```
Out[76]:
```
(3 : 23 : 1)
```
In [79]:
```
k = randint(2, 28)
gama = k*P
delta = Mens + k*Q
gama, delta
```
Out[79]:
```
((6 : 24 : 1), (24 : 8 : 1))
```
In [80]:
```
-a*gama+delta
```
Out[80]:
```
(3 : 23 : 1)
```
In [ ]:
```

```