Sage - Grundlagen für algebraische Zahlentheorie

Christian Steck

23. Dezember 2013

In diesem Dokument geben wir eine kurze Einführung in das Computer-Algebra-System Sage und bearbeiten damit einige der in der Vorlesung gestellten Übungsaufgaben. Die verwendete Version ist Sage 5.13.

1 Grundlagen

Um in dem Polynomring mit rationalen Koeffizienten zu rechnen, muss man diesen in Sage zunächst erstellen.

```
sage: R.<x> = QQ[]; R
Univariate Polynomial Ring in x over Rational Field
```

Man kann sich nun vergewissern, dass die Variable x tatsächlich in R liegt:

```
sage: x in R
True
sage: 1/x in R
False
```

Um ein Polynom, etwa $f = x^6 - x^5 - x^2 - 1$ zu erstellen, verwendet man einfach:

```
sage: f = x^6 - x^5 - x^2 - 1; f
x^6 - x^5 - x^2 - 1
sage: f.parent()
Univariate Polynomial Ring in x over Rational Field
```

Der Befehl `.parent()` zeigt dabei an, in welchem Ring das Polynom definiert ist.
Sage kann auch überprüfen, ob es sich bei f um ein irreduzibles Polynom handelt:

```
sage: f.factor()
(x - 1) * (x^5 - x - 1)
```

Das Polynom zerfällt also zu $f = (x-1) \cdot (x^5 - x - 1)$.
Will man f über einem anderen Körper faktorisieren, etwa über $\mathbb{F}_3$, so muss man Sage zunächst mitteilen, dass wir nun in $\mathbb{F}_3$ rechnen wollen:

```
sage: F3 = FiniteField(3); F3
Finite Field of size 3
sage: R3.<x> = F3[]; R3
Univariate Polynomial Ring in x over Finite Field of size 3
sage: fbar = R3(f); fbar
x^6 + 2*x^5 + 2*x^2 + 2
sage: fbar.parent()
Univariate Polynomial Ring in x over Finite Field of size 3
sage: fbar.factor()
(x + 1)^4 * (x^2 + x + 2)
```

2 Idealklassengruppe von $\mathbb{Q}[\sqrt{-14}]$

Wir erstellen zunächst den Körper $K = \mathbb{Q}[\sqrt{-14}]$ in Sage:

```
sage: R.<x> = QQ[]; R
Univariate Polynomial Ring in x over Rational Field
sage: K.<a> = NumberField(x^2 + 14);K
Number Field in a with defining polynomial x^2 + 14
sage: a^2
-14
```

Im Falle von quadratischen Zahlkörpern geht dies auch einfacher:

```
sage: K.<a> = QuadraticField(-14); K
Number Field in a with defining polynomial x^2 + 14
sage: a^2
-14
```

Um die Idealklassengruppe zu berechnen verwendet man die Befehle:

```
sage: Cl = K.class_group(); Cl
Class group of order 4 with structure C4 of Number Field in a with defining polynomial x^2 +
    14
sage: Cl.gens()
(Fractional ideal class (3, a + 2),)
```

In der Vorlesung hatten wir bereits gesehen, dass die Idealklassengruppe von einem Primideal $\mathfrak{p}_3$ über $3\mathbb{Z}$ erzeugt wird. Nun wissen wir, dass es sich dabei um $\mathfrak{p}_3 = (3, \sqrt{-14} + 2)$ handelt.

3 Beispiel von Dirichlet

Dirichlet betrachtete den Zahlkörper $K = \mathbb{Q}[\theta]$ mit θ einer Nullstelle des Polynoms $f = x^3 + x^2 - 2x + 8$. Wir wollen zunächst f definieren, auf Irreduzibilität prüfen und dann K erstellen.

```
sage: f = x^3 + x^2 - 2*x + 8; f
x^3 + x^2 - 2*x + 8
sage: f.is_irreducible()
True
sage: K.<theta> = NumberField(f); K
Number Field in theta with defining polynomial x^3 + x^2 - 2*x + 8
```

Wir können uns auch die Diskriminanten von f und K ausgeben lassen:

```
sage: f.discriminant()
-2012
sage: K.discriminant()
-503
```

Es ist also $\mathcal{O}_K \neq \mathbb{Z}[\theta]$, wie uns auch Sage bestätigt:

```
sage: OK = K.ring_of_integers()
sage: OK.gens()
[1, 1/2*theta^2 + 1/2*theta, theta^2]
sage: OK == ZZ[theta]
False
sage: alpha = 1/2*(theta^2 + theta);
sage: alpha in OK
True
sage: alpha in ZZ[theta]
False
```

In der Vorlesung wurde das Ideal (503) in $\mathcal{O}_K$ in Primideale faktorisiert, indem das Polynom f in $\mathbb{F}_{503}$ faktorisiert wurde. Sage beherrscht das Faktorisieren in endlichen Körpern:

```
sage: F = FiniteField(503); F
Finite Field of size 503
sage: R503.<x> = F[]; R503
Univariate Polynomial Ring in x over Finite Field of size 503
sage: fbar = R503(f); fbar
x^3 + x^2 + 501*x + 8
sage: fbar.parent()
Univariate Polynomial Ring in x over Finite Field of size 503
sage: fbar.factor()
(x + 299) * (x + 354)^2
```

Und auch das direkte Faktorisieren in Primideale:

```
sage: I = OK.ideal(503); I
Fractional ideal (503)
sage: I.factor()
(Fractional ideal (3*theta^2 - 3*theta + 5)) * (Fractional ideal (-8*theta^2 + 14*theta - 25))
    ^2
```

Wir können abschließend noch das Ideal (2) faktorisieren:

```
sage: I = OK.ideal(2); I
Fractional ideal (2)
sage: I.factor()
(Fractional ideal (-1/2*theta^2 + 1/2*theta - 1)) * (Fractional ideal (-theta^2 + 2*theta - 3)
    ) * (Fractional ideal (3/2*theta^2 - 5/2*theta + 4))
```

Es lässt sich auch leicht die Idealklassengruppe berechnen:

```
sage: K.class_number()
1
sage: K.class_group()
Class group of order 1 of Number Field in theta with defining polynomial x^3 + x^2 - 2*x + 8
```

Es handelt sich bei $\mathcal{O}_K$ also um einen faktoriellen Ring, was sich mit Sage jedoch nicht direkt überprüfen lässt.