## CONTENTS

1 Univariate Ore polynomial rings 1
  1.1 Univariate Ore Polynomial Rings ....................................................... 1
  1.2 Univariate Ore Polynomials .............................................................. 12
  1.3 Skew Univariate Polynomial Rings ...................................................... 38
  1.4 Univariate Skew Polynomials ............................................................ 43
  1.5 Univariate Dense Skew Polynomials over a field equipped with a finite order automorphism 47
  1.6 Univariate Dense Skew Polynomials over Finite Fields .......................... 51

2 Fraction field of Ore polynomial rings 59
  2.1 Fraction fields of Ore polynomial rings. ............................................ 59
  2.2 An element in the fraction field of a Ore polynomial ring. ...................... 68

3 Noncommutative Multivariate Polynomials 75
  3.1 Noncommutative Polynomials via libSINGULAR/Plural ............................ 75

4 Indices and Tables 95

Python Module Index 97

Index 99
1.1 Univariate Ore Polynomial Rings

This module provides the `OrePolynomialRing`, which constructs a general dense univariate Ore polynomial ring over a commutative base with equipped with an endomorphism and/or a derivation.

AUTHOR:

• Xavier Caruso (2020-04)

class sage.rings.polynomial.ore_polynomial_ring.OrePolynomialRing(base_ring, twisting_map, names, sparse, category=None)

Bases: sage.structure.unique_representation.UniqueRepresentation, sage.rings.ring.Algebra

Construct and return the globally unique Ore polynomial ring with the given properties and variable names.

Given a ring $R$ and a ring automorphism $\sigma$ of $R$ and a $\sigma$-derivation $\partial$, the ring of Ore polynomials $R[X; \sigma, \partial]$ is the usual abelian group polynomial $R[X]$ equipped with the modification multiplication deduced from the rule $Xa = \sigma(a)X + \partial(a)$. We refer to [Ore1933] for more material on Ore polynomials.

INPUT:

• `base_ring` – a commutative ring
• `twisting_map` – either an endomorphism of the base ring, or a (twisted) derivation of it
• `names` – a string or a list of strings
• `sparse` – a boolean (default: False); currently not supported

EXAMPLES:
The case of a twisting endomorphism

We create the Ore ring $F_{5^3}[x, \text{Frob}]$ where Frob is the Frobenius endomorphism:

```sage
definitions:
sage: k.<a> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S = OrePolynomialRing(k, Frob, 'x')
sage: S
Ore Polynomial Ring in x over Finite Field in a of size 5^3 twisted by a |--> a^5
```

In particular, observe that it is not needed to create and pass in the twisting derivation (which is 0 in our example). As a shortcut, we can use the square brackets notation as follow:

```sage
definitions:
sage: T.<x> = k['x', Frob]
sage: T
Ore Polynomial Ring in x over Finite Field in a of size 5^3 twisted by a |--> a^5
sage: T is S
True
```

We emphasize that it is necessary to repeat the name of the variable in the right hand side. Indeed, the following fails (it is interpreted by Sage as a classical polynomial ring with variable name Frob):  

```sage
definitions:
sage: T.<x> = k[Frob]
Traceback (most recent call last):
  ...
ValueError: variable name 'Frobenius endomorphism a |--> a^5 on Finite Field in a → of size 5^3' is not alphanumeric
```

Note moreover that, similarly to the classical case, using the brackets notation also sets the variable:

```sage
definitions:
sage: x.parent() is S
True
```

We are now ready to carry on computations in the Ore ring:

```sage
definitions:
sage: x*a
(2*a^2 + 4*a + 4)*x
sage: Frob(a)*x
(2*a^2 + 4*a + 4)*x
```

The case of a twisting derivation

We can similarly create the Ore ring of differential operators over $\mathbb{Q}[t]$, namely $\mathbb{Q}[t][d, \frac{d}{dt}]$:

```sage
definitions:
sage: R.<t> = QQ[]
sage: der = R.derivation(); der
sage: A = OrePolynomialRing(R, der, 'd')
sage: A
Ore Polynomial Ring in d over Univariate Polynomial Ring in t over Rational Field twisted by d/dt
```

Again, the brackets notation is available:
and computations can be carried out:

```sage
d*t
1 + d*t
```

### The combined case

Ore polynomial rings involving at the same time a twisting morphism \( \sigma \) and a twisting \( \sigma \)-derivation can be created as well as follows:

```sage
F.<u> = Qq(3^2)
sigma = F.frobenius_endomorphism(); sigma
Frobenius endomorphism on 3-adic Unramified Extension Field in u
defined by \( x^2 + 2x + 2 \) lifting \( u \) \( \mapsto \) \( u^3 \) on the residue field
der = F.derivation(3, twist=sigma); der
(3 + O(3^21))*([Frob] - id)
M.<X> = F['X', der]
Ore Polynomial Ring in X over 3-adic Unramified Extension Field in u
defined by \( x^2 + 2x + 2 \) twisted by Frob and \( (3 + O(3^21))*([Frob] - id) \)

We emphasize that we only need to pass in the twisted derivation as it already contains in it the datum of the twisting endomorphism. Actually, passing in both twisting maps results in an error:

```sage
F['X', sigma, der]
Traceback (most recent call last):
... ValueError: variable name 'Frobenius endomorphism ...' is not alphanumeric
```

### Examples of variable name context

Consider the following:

```sage
R.<t> = ZZ[]
sigma = R.hom([t+1])
S.<x> = SkewPolynomialRing(R, sigma); S
Ore Polynomial Ring in x over Univariate Polynomial Ring in t over Integer Ring
twisted by t \( \mapsto \) t + 1
```

The names of the variables defined above cannot be arbitrarily modified because each Ore polynomial ring is unique in Sage and other objects in Sage could have pointers to that Ore polynomial ring.

However, the variable can be changed within the scope of a `with` block using the `localvars` context:

```sage
R.<t> = ZZ[]
sigma = R.hom([t+1])
S.<x> = SkewPolynomialRing(R, sigma); S
Ore Polynomial Ring in x over Univariate Polynomial Ring in t over Integer Ring
twisted by t \( \mapsto \) t + 1
```

(continues on next page)
Uniqueness and immutability

In Sage, there is exactly one Ore polynomial ring for each quadruple (base ring, twisting morphism, twisting derivation, name of the variable):

```
sage: k.<a> = GF(7^3)
sage: Frob = k.frobenius_endomorphism()
sage: S = k['x', Frob]
sage: T = k['x', Frob]
sage: S is T
True
```

Rings with different variables names are different:

```
sage: S is k['y', Frob]
False
```

Similarly, varying the twisting morphisms yields to different Ore rings (expect when the morphism coincide):

```
sage: S is k['x', Frob^2]
False
sage: S is k['x', Frob^3]
False
sage: S is k['x', Frob^4]
True
```

Todo:

- Sparse Ore Polynomial Ring
- Multivariate Ore Polynomial Ring

`change_var(var)`

Return the Ore polynomial ring in variable `var` with the same base ring, twisting morphism and twisting derivation as `self`.

INPUT:

- `var` – a string representing the name of the new variable

EXAMPLES:

```
sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: R.<x> = OrePolynomialRing(k,Frob); R
Ore Polynomial Ring in x over Finite Field in t of size 5^3 twisted by t |--> t^5
sage: Ry = R.change_var('y'); Ry
Ore Polynomial Ring in y over Finite Field in t of size 5^3 twisted by t |--> t^5
```
characteristic()

Return the characteristic of the base ring of self.

EXAMPLES:

```python
sage: R.<t> = QQ[]
sage: sigma = R.hom([t+1])
sage: R['x', sigma].characteristic()
0
sage: k.<u> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: k['y', Frob].characteristic()
5
```

fraction_field()

Return the fraction field of this skew ring.

EXAMPLES:

```python
sage: k.<a> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x', Frob]
sage: K = S.fraction_field(); K
Ore Function Field in x over Finite Field in a of size 5^3 twisted by a |--> a^5
sage: f = 1/(x + a); f
(x + a)^(-1)
sage: f.parent() is K
True
```

Below is another example with differentiel operators:

```python
sage: R.<t> = QQ[]
sage: der = R.derivation()
sage: A.<d> = R['d', der]
sage: A.fraction_field()
Ore Function Field in d over Fraction Field of Univariate Polynomial Ring in t over Rational Field twisted by d/dt
sage: f = t/d; f
(d - 1/t)^(-1) * t
sage: f*d
t
```

See also:

`sage.rings.polynomial.ore_function_field`

gen(n=0)

Return the indeterminate generator of this Ore polynomial ring.

INPUT:

- `n` – index of generator to return (default: 0); exists for compatibility with other polynomial rings
EXAMPLES:

```python
sage: R.<t> = QQ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x',sigma]; S
Ore Polynomial Ring in x over Univariate Polynomial Ring in t over Rational Field twisted by t |--> t + 1
sage: y = S.gen(); y
x
sage: y == x
True
sage: y is x
True
sage: S.gen(0)
x
```

This is also known as the parameter:

```python
sage: S.parameter() is S.gen()
True
```

gens_dict()

Return a {name: variable} dictionary of the generators of this Ore polynomial ring.

EXAMPLES:

```python
sage: R.<t> = ZZ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = SkewPolynomialRing(R,sigma)
sage: S.gens_dict()
{'x': x}
```

is_commutative()

Return True if this Ore polynomial ring is commutative, i.e. if the twisting morphism is the identity and the twisting derivation vanishes.

EXAMPLES:

```python
sage: k.<a> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x', Frob]
sage: S.is_commutative()
False
sage: T.<y> = k['y', Frob^3]
sage: T.is_commutative()
True
sage: R.<t> = GF(5)[]
sage: der = R.derivation()
sage: A.<d> = R['d', der]
sage: A.is_commutative()
False
sage: B.<b> = R['b', 5*der]
sage: B.is_commutative()
True
```

is_exact()
Return True if elements of this Ore polynomial ring are exact. This happens if and only if elements of the base ring are exact.

**EXAMPLES:**

```sage
k.<t> = GF(5^3)
k.<a> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x', Frob]
sage: S.is_exact()
True
sage: S.is_exact()
True
sage: R.<u> = k[]
sage: sigma = R.hom([u+u^2])
sage: T.<y> = R['y', sigma]
sage: T.is_exact()
False
sage: T.is_exact()
False
```

**is_field()**

Return always False since Ore polynomial rings are never fields.

**EXAMPLES:**

```sage
k.<a> = GF(5^3)
k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x', Frob]
sage: S.is_field()
False
```

**is_finite()**

Return False since Ore polynomial rings are not finite (unless the base ring is 0).

**EXAMPLES:**

```sage
k.<t> = GF(5^3)
True
sage: Frob = k.frobenius_endomorphism()
True
sage: S.<x> = k['x', Frob]
False
sage: S.is_finite()
False
```

**is_sparse()**

Return True if the elements of this Ore polynomial ring are sparsely represented.

**Warning:** Since sparse Ore polynomials are not yet implemented, this function always returns False.

**EXAMPLES:**

```sage
R.<t> = RR[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x', sigma]
(continues on next page)
```
sage: S.is_sparse()
False

ngens()

Return the number of generators of this Ore polynomial ring, which is 1.

EXAMPLES:

sage: R.<t> = RR[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x',sigma]
sage: S.ngens()
1

parameter(n=0)

Return the indeterminate generator of this Ore polynomial ring.

INPUT:

• n – index of generator to return (default: 0); exists for compatibility with other polynomial rings

EXAMPLES:

sage: R.<t> = QQ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x',sigma]; S
Ore Polynomial Ring in x over Univariate Polynomial Ring in t over Rational Field twisted by t |--> t + 1
sage: y = S.gen(); y
x
sage: y == x
True
sage: y is x
True
sage: S.gen(0)
x

This is also known as the parameter:

sage: S.parameter() is S.gen()
True

random_element(degree=2, monic=False, *args, **kwds)

Return a random Ore polynomial in this ring.

INPUT:

• degree – (default: 2) integer with degree or a tuple of integers with minimum and maximum degrees
• monic – (default: False) if True, return a monic Ore polynomial
• *args, **kwds – passed on to the random_element method for the base ring

OUTPUT:

Ore polynomial such that the coefficients of $x^i$, for $i$ up to degree, are random elements from the base ring, randomized subject to the arguments *args and **kwds.

EXAMPLES:
Use degree to obtain polynomials of higher degree:

```
sage: p = S.random_element(degree=5)  # random
(t^2 + 3*t)*x^4 + (4*t + 4)*x^3 + (4*t^2 + 4*t)*x^2 + (2*t^2 + 1)*x + 3
sage: p.degree() <= 5
True
```

When monic is False, the returned Ore polynomial may have a degree less than degree (it happens when the random leading coefficient is zero). However, if monic is True, this cannot happen:

```
sage: p = S.random_element(degree=4, monic=True)
sage: p.leading_coefficient() == S.base_ring().one()
True
sage: p.degree() == 4
True
```

If a tuple of two integers is given for the degree argument, a random integer will be chosen between the first and second element of the tuple as the degree, both inclusive:

```
sage: S.random_element(degree=(2,7))  # random
(3*t^2 + 1)*x^4 + (4*t + 2)*x^3 + (4*t^2 + 2*t + 3)*x + 3*t^2 + 2*t + 2
```

If the first tuple element is greater than the second, a ValueError is raised:

```
sage: S.random_element(degree=(5,4))
Traceback (most recent call last):
  ...
ValueError: first degree argument must be less or equal to the second
```

**random_irreducible**(degree=2, monic=True, *args, **kwds)

Return a random irreducible Ore polynomial.

**Warning:** Elements of this Ore polynomial ring need to have a method `is_irreducible()`. Currently, this method is implemented only when the base ring is a finite field.

**INPUT:**

- degree - Integer with degree (default: 2) or a tuple of integers with minimum and maximum degrees
- monic - if True, returns a monic Ore polynomial (default: True)
- *args, **kwds - passed in to the random_element method for the base ring

**EXAMPLES:**

```
sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
```

(continues on next page)
sage: S.<x> = k['x', Frob]
sage: A = S.random_irreducible(); A
x^2 + (4*t^2 + 3*t + 4)*x + 4*t^2 + t
sage: A.is_irreducible()
True
sage: B = S.random_irreducible(degree=3, monic=False); B
# random
(4*t + 1)*x^3 + (t^2 + 3*t + 3)*x^2 + (3*t^2 + 2*t + 2)*x + 3*t^2 + 3*t + 1
sage: B.is_irreducible()
True

\textbf{\texttt{twist_map}} (n=1)

Return the twisting endomorphism defining this Ore polynomial ring iterated \(n\) times or \texttt{None} if this Ore polynomial ring is not twisted by an endomorphism.

This method is deprecated. Use \texttt{twisting_morphism()} instead.

\textbf{INPUT:}

\begin{itemize}
  \item \texttt{n} - an integer (default: 1)
\end{itemize}

\textbf{EXAMPLES:}

\begin{Verbatim}
sage: R.<t> = QQ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x', sigma]
sage: S.twist_map()
...
DeprecationWarning: The method \texttt{twist_map} is deprecated; use \texttt{twisting_morphism()} (same semantic) instead
See https://trac.sagemath.org/29629 for details.
Ring endomorphism of Univariate Polynomial Ring in \(t\) over Rational Field
Defn: \(t \mapsto t + 1\)
\end{Verbatim}

\textbf{\texttt{twisting_derivation}()}

Return the twisting derivation defining this Ore polynomial ring or \texttt{None} if this Ore polynomial ring is not twisted by a derivation.

\textbf{EXAMPLES:}

\begin{Verbatim}
sage: R.<t> = QQ[]
sage: der = R.derivation(); der
d/dt
sage: A.<d> = R['d', der]
sage: A.twisting_derivation()
d/dt
sage: k.<a> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x', Frob]
sage: S.twisting_derivation()
\end{Verbatim}

\textbf{See also:}

\texttt{twisting_morphism()}

\textbf{\texttt{twisting_morphism}} (n=1)

Return the twisting endomorphism defining this Ore polynomial ring iterated \(n\) times or \texttt{None} if this Ore polynomial ring is not twisted by an endomorphism.

\textbf{INPUT:}
• \( n \) - an integer (default: 1)

**EXAMPLES:**

```
sage: R.<t> = QQ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x', sigma]
sage: S.twisting_morphism()
Ring endomorphism of Univariate Polynomial Ring in t over Rational Field
  Defn: t |--> t + 1
sage: S.twisting_morphism() == sigma
True
sage: S.twisting_morphism(10)
Ring endomorphism of Univariate Polynomial Ring in t over Rational Field
  Defn: t |--> t + 10
```

If \( n \) in negative, Sage tries to compute the inverse of the twisting morphism:

```
sage: k.<a> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: T.<y> = k['y',Frob]
sage: T.twisting_morphism(-1)
Frobenius endomorphism a |--> a^(5^2) on Finite Field in a of size 5^3
```

Sometimes it fails, even if the twisting morphism is actually invertible:

```
sage: K = R.fraction_field()
sage: phi = K.hom([(t+1)/(t-1)])
sage: T.<y> = K['y', phi]
sage: T.twisting_morphism(-1)
Traceback (most recent call last):
  ... NotImplementedError: inverse not implemented for morphisms of Fraction Field...
```

When the Ore polynomial ring is only twisted by a derivation, this method returns nothing:

```
sage: der = R.derivation()
sage: A.<d> = R['x', der]
sage: A
Ore Polynomial Ring in x over Univariate Polynomial Ring in t over Rational Field twisted by d/dt
sage: A.twisting_morphism()
```

Here is an example where the twisting morphism is automatically inferred from the derivation:

```
sage: k.<a> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: der = k.derivation(1, twist=Frob)
sage: der
[a |--> a^5] - id
sage: S.<x> = k['x', der]
sage: S.twisting_morphism()
Frobenius endomorphism a |--> a^5 on Finite Field in a of size 5^3
```

See also:

```
twisting_derivation()
```
1.2 Univariate Ore Polynomials

This module provides the OrePolynomial, which constructs a single univariate Ore polynomial over a commutative base equipped with an endomorphism and/or a derivation. It provides generic implementation of standard arithmetical operations on Ore polynomials as addition, multiplication, gcd, lcm, etc.

The generic implementation of dense Ore polynomials is OrePolynomial_generic_dense. The classes ConstantOrePolynomialSection and OrePolynomialBaseringInjection handle conversion from a Ore polynomial ring to its base ring and vice versa.

AUTHORS:

• Xavier Caruso (2020-05)

class sage.rings.polynomial.ore_polynomial_element.ConstantOrePolynomialSection
Bases: sage.categories.map.Map

Representation of the canonical homomorphism from the constants of a Ore polynomial ring to the base ring.

This class is necessary for automatic coercion from zero-degree Ore polynomial ring into the base ring.

EXAMPLES:

```
sage: from sage.rings.polynomial.ore_polynomial_element import ConstantOrePolynomialSection
sage: R.<t> = QQ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x',sigma]
sage: m = ConstantOrePolynomialSection(S, R); m
Generic map:
   From: Ore Polynomial Ring in x over Univariate Polynomial Ring in t over Rational Field twisted by t |--> t + 1
   To:   Univariate Polynomial Ring in t over Rational Field
```

class sage.rings.polynomial.ore_polynomial_element.OrePolynomial
Bases: sage.structure.element.AlgebraElement

Abstract base class for Ore polynomials.

This class must be inherited from and have key methods overridden.

Definition

Let $R$ be a commutative ring equipped with an automorphism $\sigma$ and a $\sigma$-derivation $\partial$.

A Ore polynomial is given by the equation:

$$F(X) = a_n X^n + \cdots + a_0,$$

where the coefficients $a_i \in R$ and $X$ is a formal variable.

Addition between two Ore polynomials is defined by the usual addition operation and the modified multiplication is defined by the rule $Xa = \sigma(a)X + \partial(a)$ for all $a$ in $R$. Ore polynomials are thus non-commutative and the degree of a product is equal to the sum of the degrees of the factors.

Let $a$ and $b$ be two Ore polynomials in the same ring $S$. The left (resp. right) euclidean division of $a$ by $b$ is a couple $(q, r)$ of elements in $S$ such that

• $a = qb + r$ (resp. $a = bq + r$)
• the degree of $r$ is less than the degree of $b$
q (resp. r) is called the quotient (resp. the remainder) of this euclidean division.

**Properties**

Keeping the previous notation, if the leading coefficient of b is a unit (e.g. if b is monic) then the quotient and the remainder in the right euclidean division exist and are unique.

The same result holds for the left euclidean division if in addition the twisting morphism defining the Ore polynomial ring is invertible.

**EXAMPLES:**

We illustrate some functionalities implemented in this class.

We create the Ore polynomial ring (here the derivation is zero):

```sage
sage: R.<t> = ZZ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x',sigma]; S
Ore Polynomial Ring in x over Univariate Polynomial Ring in t over Integer Ring
  twisted by t |--> t + 1
```

and some elements in it:

```sage
sage: a = t + x + 1; a
x + t + 1
sage: b = S([t^2,t+1,1]); b
x^2 + (t + 1)*x + t^2
sage: c = S.random_element(degree=3,monic=True); c
x^3 + (2*t - 1)*x
```

Ring operations are supported:

```sage
sage: a + b
x^2 + (t + 2)*x + t^2 + t + 1
sage: a - b
-x^2 - t*x - t^2 + t + 1
sage: a * b
x^3 + (2*t + 3)*x^2 + (2*t^2 + 4*t + 2)*x + t^3 + t^2
sage: b * a
x^3 + (2*t + 4)*x^2 + (2*t^2 + 3*t + 2)*x + t^3 + t^2
sage: a * b == b * a
False
sage: b^2
x^4 + (2*t + 4)*x^3 + (3*t^2 + 7*t + 6)*x^2
  + (2*t^3 + 4*t^2 + 3*t + 1)*x + t^4
sage: b^2 == b*b
True
```

Sage also implements arithmetic over Ore polynomial rings. You will find below a short panorama:

```sage
sage: q, r = c.right_quo_rem(b)
sage: q
x - t - 2
sage: r
3*t*x + t^3 + 2*t^2
```
The operators \(/\) and \(\%\) give respectively the quotient and the remainder of the *right* euclidean division:

```plaintext
sage: q == c // b
True
sage: r == c % b
True
```

Here we can see the effect of the operator evaluation compared to the usual polynomial evaluation:

```plaintext
sage: a = x^2
doctest:...: FutureWarning: This class/method/function is marked as experimental. It, its functionality or its interface might change without a formal deprecation. See http://trac.sagemath.org/13215 for details.
sage: a(t)
t + 2
```

Here is another example over a finite field:

```plaintext
sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x',Frob]
sage: a = x^4 + (4*t + 1)*x^3 + (3*t^2 + 2*t + 2)*x + (3*t^3 + 3*t + 1)
sage: b = (2*t^2 + 3)*x^2 + (3*t^2 + 1)*x + 4*t + 2
sage: q, r = a.left_quo_rem(b)
sage: q
(4*t^2 + t + 1)*x^2 + (2*t^2 + 2*t + 2)*x + 2*t^2 + 4*t + 3
sage: r
(t + 2)*x + 3*t^2 + 2*t + 4
sage: a == b*q + r
True
```

Once we have euclidean divisions, we have for free \(\gcd\) and \(\text{lcm}\) (at least if the base ring is a field):

```plaintext
sage: a = (x + t) * (x + t^2)^2
sage: b = (x + t) * (t*x + t + 1) * (x + t^2)
sage: a.right_gcd(b)
x + t^2
sage: a.left_gcd(b)
x + t
```

The left \(\text{lcm}\) has the following meaning: given Ore polynomials \(a\) and \(b\), their left \(\text{lcm}\) is the least degree polynomial \(c = ua = vb\) for some Ore polynomials \(u, v\). Such a \(c\) always exist if the base ring is a field:

```plaintext
sage: c = a.left_lcm(b); c
x^5 + (4*t^2 + t + 3)*x^4 + (3*t^2 + 4*t)*x^3 + 2*t^2*x^2 + (2*t^2 + t)*x + 4*t^2 + 4
sage: c.is_right_divisible_by(a)
True
sage: c.is_right_divisible_by(b)
True
```

The right \(\text{lcm}\) is defined similarly as the least degree polynomial \(c = au = bv\) for some \(u, v\):
sage: d = a.right_lcm(b); d
x^5 + (t^2 + 1)*x^4 + (3*t^2 + 3*t + 3)*x^3 + (3*t^2 + t + 2)*x^2 + (4*t^2 +
→3*t)*x + 4*t + 4
sage: d.is_left_divisible_by(a)
True
sage: d.is_left_divisible_by(b)
True

See also:

• sage.rings.polynomial.ore_polynomial_ring

**base_ring()**

Return the base ring of self.

**EXAMPLES:**

```
sage: R.<t> = ZZ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x', sigma]
sage: a = S.random_element()
sage: a.base_ring()
Univariate Polynomial Ring in t over Integer Ring
sage: a.base_ring() is R
True
```

**change_variable_name**(var)

Change the name of the variable of self.

This will create the Ore polynomial ring with the new name but same base ring, twisting morphism and twisting derivation. The returned Ore polynomial will be an element of that Ore polynomial ring.

**INPUT:**

• var – the name of the new variable

**EXAMPLES:**

```
sage: R.<t> = ZZ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x', sigma]
sage: a = x^3 + (2*t + 1)*x + t^2 + 3*t + 5
sage: b = a.change_variable_name('y'); b
y^3 + (2*t + 1)*y + t^2 + 3*t + 5
```

Note that a new parent is created at the same time:

```
sage: b.parent()
Ore Polynomial Ring in y over Univariate Polynomial Ring in t over Integer
→Ring twisted by t |--> t + 1
```

**coefficients**(sparse=True)

Return the coefficients of the monomials appearing in self.

If sparse=True (the default), return only the non-zero coefficients. Otherwise, return the same value as self.list().
Note: This should be overridden in subclasses.

EXAMPLES:

```python
sage: R.<t> = QQ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x', sigma]
sage: a = 1 + x^4 + (t+1)*x^2 + t^2
sage: a.coefficients()
[t^2 + 1, t + 1, 1]
sage: a.coefficients(sparse=False)
[t^2 + 1, 0, t + 1, 0, 1]
```

**constant_coefficient()**

Return the constant coefficient (i.e. the coefficient of term of degree 0) of `self`.

EXAMPLES:

```python
sage: R.<t> = ZZ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x', sigma]
sage: a = x + t^2 + 2
sage: a.constant_coefficient()
t^2 + 2
```

**degree()**

Return the degree of `self`.

By convention, the zero Ore polynomial has degree $-1$.

EXAMPLES:

```python
sage: R.<t> = ZZ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x', sigma]
sage: a = x^2 + t*x^3 + t^2*x + 1
sage: a.degree()
3
sage: S.zero().degree()
-1
sage: S(5).degree()
0
```

**exponents()**

Return the exponents of the monomials appearing in `self`.

EXAMPLES:

```python
sage: R.<t> = QQ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x', sigma]
sage: a = 1 + x^4 + (t+1)*x^2 + t^2
sage: a.exponents()
[0, 2, 4]
```

**hamming_weight()**

Return the number of non-zero coefficients of `self`.

16 Chapter 1. Univariate Ore polynomial rings
This is also known as the weight, hamming weight or sparsity.

**EXAMPLES:**

```python
sage: R.<t> = QQ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x',sigma]
sage: a = 1 + x^4 + (t+1)*x^2 + t^2
sage: a.number_of_terms()
3
```

This is also an alias for `hamming_weight`:

```python
sage: a.hamming_weight()
3
```

**is_constant()**

Return whether `self` is a constant polynomial.

**EXAMPLES:**

```python
sage: R.<t> = QQ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x',sigma]
sage: R(2).is_constant()
True
sage: (x + 1).is_constant()
False
```

**is_left_divisible_by(other)**

Check if `self` is divisible by `other` on the left.

**INPUT:**

- `other` – a Ore polynomial in the same ring as `self`

**OUTPUT:**

Return `True` or `False`.

**EXAMPLES:**

```python
sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x',Frob]
sage: a = x^2 + t*x + t^2 + 3
sage: b = x^3 + (t + 1)*x^2 + 1
sage: c = a*b
sage: c.is_left_divisible_by(a)
True
sage: c.is_left_divisible_by(b)
False
```

Divisibility by 0 does not make sense:

```python
sage: c.is_left_divisible_by(S(0))
Traceback (most recent call last):
...
ZeroDivisionError: division by zero is not valid
```
**is_monic()**

Return `True` if this Ore polynomial is monic.

The zero polynomial is by definition not monic.

**EXAMPLES:**

```python
sage: R.<t> = ZZ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x',sigma]
sage: a = x + t
sage: a.is_monic()  # Returns True
True
sage: a = 0*x
sage: a.is_monic()  # Returns False
False
sage: a = t*x^3 + x^4 + (t+1)*x^2
sage: a.is_monic()  # Returns True
True
sage: a = (t^2 + 2*t)*x^2 + x^3 + t^10*x^5
sage: a.is_monic()  # Returns False
False
```

**is_monomial()**

Return `True` if `self` is a monomial, i.e., a power of the generator.

**EXAMPLES:**

```python
sage: R.<t> = ZZ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x',sigma]
sage: x.is_monomial()  # Returns True
True
sage: (x+1).is_monomial()  # Returns False
False
sage: (x^2).is_monomial()  # Returns True
True
sage: S(1).is_monomial()  # Returns True
True
```

The coefficient must be 1:

```python
sage: (2*x^5).is_monomial()  # Returns False
False
sage: S(t).is_monomial()  # Returns False
False
```

To allow a non-1 leading coefficient, use `is_term()`:

```python
sage: (2*x^5).is_term()  # Returns True
True
sage: S(t).is_term()  # Returns True
True
```

**is_nilpotent()**

Check if `self` is nilpotent.

**Note:** The paper “Nilpotents and units in skew polynomial rings over commutative rings” by M. Rimmer and K.R. Pearson describes a method to check whether a given skew polynomial is nilpotent. That method
However, requires one to know the order of the automorphism which is not available in Sage. This method is thus not yet implemented.

**EXAMPLES:**

```python
sage: R.<t> = ZZ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x',sigma]
sage: x.is_nilpotent()
Traceback (most recent call last):  
...  
NotImplementedError
```

**is_one()**

Test whether this polynomial is 1.

**EXAMPLES:**

```python
sage: R.<t> = QQ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x',sigma]
sage: R(1).is_one()  
True
sage: (x + 3).is_one()  
False
```

**is_right_divisible_by**(other)

Check if self is divisible by other on the right.

**INPUT:**
- other -- a Ore polynomial in the same ring as self

**OUTPUT:**

Return True or False.

**EXAMPLES:**

```python
sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x',Frob]
sage: a = x^2 + t*x + t^2 + 3
sage: b = x^3 + (t + 1)*x^2 + 1
sage: c = a*b
sage: c.is_right_divisible_by(a)  
False
sage: c.is_right_divisible_by(b)  
True
```

Divisibility by 0 does not make sense:

```python
sage: c.is_right_divisible_by(S(0))
Traceback (most recent call last):  
...  
ZeroDivisionError: division by zero is not valid
```

This function does not work if the leading coefficient of the divisor is not a unit:

1.2. Univariate Ore Polynomials
```python
sage: R.<t> = QQ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x',sigma]
sage: a = x^2 + 2*x + t
sage: b = (t+1)*x + t^2
sage: c = a*b
sage: c.is_right_divisible_by(b)
Traceback (most recent call last):
  ...  
NotImplementedError: the leading coefficient of the divisor is not invertible
```

### is_term()
Return True if `self` is an element of the base ring times a power of the generator.

**EXAMPLES:**
```python
sage: R.<t> = ZZ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x',sigma]
sage: x.is_term()  # True
sage: R(1).is_term()  # True
sage: (3*x^5).is_term()  # True
sage: (1+3*x^5).is_term()  # False
```

If you want to test that `self` also has leading coefficient 1, use `is_monomial()` instead:

```python
sage: (3*x^5).is_monomial()  # False
```

### is_unit()
Return True if this Ore polynomial is a unit.

When the base ring $R$ is an integral domain, then a Ore polynomial $f$ is a unit if and only if degree of $f$ is 0 and $f$ is then a unit in $R$.

**Note:** The case when $R$ is not an integral domain is not yet implemented.

**EXAMPLES:**
```python
sage: R.<t> = ZZ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x',sigma]
sage: a = x + (t+1)*x^5 + t^2*x^3 - x^5
sage: a.is_unit()  # False
```

### is_zero()
Return True if `self` is the zero polynomial.

**EXAMPLES:**
```python
sage: R.<t> = ZZ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x',sigma]
sage: a = x + 1
sage: a.is_zero()
False
sage: b = S.zero()
Sage: b.is_zero()
True
```

**leading_coefficient()**

Return the coefficient of the highest-degree monomial of `self`.

**EXAMPLES:**

```python
sage: R.<t> = ZZ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x',sigma]
sage: a = (t+1)*x^5 + t^2*x^3 + x
sage: a.leading_coefficient()
t + 1
```

By convention, the leading coefficient to the zero polynomial is zero:

```python
sage: S(0).leading_coefficient()
0
```

**left_divides(other)**

Check if `self` divides `other` on the left.

**INPUT:**

- `other` – a Ore polynomial in the same ring as `self`

**OUTPUT:**

Return True or False.

**EXAMPLES:**

```python
sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x',Frob]
sage: a = x^2 + t*x + t^2 + 3
sage: b = x^3 + (t + 1)*x^2 + 1
sage: c = a*b
sage: a.left_divides(c)
True
sage: b.left_divides(c)
False
```

Divisibility by 0 does not make sense:

```python
sage: S(0).left_divides(c)
Traceback (most recent call last):
  ... ZeroDivisionError: division by zero is not valid
```

**left_gcd(other, monic=True)**

Return the left gcd of `self` and `other`.

*1.2. Univariate Ore Polynomials 21*
INPUT:

- other – a Ore polynomial in the same ring as self
- monic – boolean (default: True); return whether the left gcd should be normalized to be monic

OUTPUT:

The left gcd of self and other, that is a Ore polynomial \( g \) with the following property: any Ore polynomial is divisible on the left by \( g \) iff it is divisible on the left by both self and other. If monic is True, \( g \) is in addition monic. (With this extra condition, it is uniquely determined.)

Note: Works only if following two conditions are fulfilled (otherwise left gcd do not exist in general): 1) the base ring is a field and 2) the twisting morphism is bijective.

EXAMPLES:

```
sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x',Frob]
sage: a = (x + t) * (x^2 + t*x + 1)
sage: b = 2 * (x + t) * (x^3 + (t+1)*x^2 + t^2)
sage: a.left_gcd(b)
x + t
```

Specifying monic=False, we can get a nonmonic gcd:

```
sage: a.left_gcd(b,monic=False)
2*t*x + 4*t + 2
```

The base ring needs to be a field:

```
sage: R.<t> = QQ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x',sigma]
sage: a = (x + t) * (x^2 + t*x + 1)
sage: b = 2 * (x + t) * (x^3 + (t+1)*x^2 + t^2)
sage: a.left_gcd(b)
```

Traceback (most recent call last):
...
TypeError: the base ring must be a field

And the twisting morphism needs to be bijective:

```
sage: FR = R.fraction_field()
sage: f = FR.hom([FR(t)^2])
sage: S.<x> = FR['x',f]
sage: a = (x + t) * (x^2 + t*x + 1)
sage: b = 2 * (x + t) * (x^3 + (t+1)*x^2 + t^2)
sage: a.left_gcd(b)
```

Traceback (most recent call last):
...
NotImplementedError: inversion of the twisting morphism

```
left_lcm (other, monic=True)
```

Return the left lcm of self and other.
INPUT:

- `other` – a Ore polynomial in the same ring as `self`
- `monic` – boolean (default: `True`); return whether the left lcm should be normalized to be monic

OUTPUT:

The left lcm of `self` and `other`, that is a Ore polynomial `g` with the following property: any Ore polynomial divides `g` on the right iff it divides both `self` and `other` on the right. If `monic` is `True`, `g` is in addition monic. (With this extra condition, it is uniquely determined.)

**Note:** Works only if the base ring is a field (otherwise left lcm do not exist in general).

**EXAMPLES:**

```python
sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x',Frob]
sage: a = (x + t^2) * (x + t)
sage: b = 2 * (x^2 + t + 1) * (x + t)
sage: c = a.left_lcm(b); c
x^5 + (2*t^2 + t + 4)*x^4 + (3*t^2 + 4)*x^3 + (3*t^2 + 3*t + 2)*x^2 + (t^2 + t + 2)*x
sage: c.is_right_divisible_by(a)
True
sage: c.is_right_divisible_by(b)
True
sage: a.degree() + b.degree() == c.degree() + a.right_gcd(b).degree()
True

Specifying `monic=False`, we can get a nonmonic gcd:

```python
sage: a.left_lcm(b,monic=False)
(t^2 + t)*x^5 + (4*t^2 + 4*t + 1)*x^4 + (t + 1)*x^3 + (t^2 + 2)*x^2 + (3*t + 4)*x
```

The base ring needs to be a field:

```python
sage: R.<t> = QQ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x',sigma]
sage: a = (x + t^2) * (x + t)
sage: b = 2 * (x^2 + t + 1) * (x + t)
sage: a.left_lcm(b)
Traceback (most recent call last):
  ... AttributeError: the base ring must be a field
```

**left_mod**(other)

Return the remainder of left division of `self` by `other`.

**EXAMPLES:**

```python
sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x',Frob]
sage: a = 1 + t*x^2
```
Return the unique monic Ore polynomial \( m \) which divides this polynomial on the left and has the same degree.

Given a Ore polynomial \( P \) of degree \( n \), its left monic is given by \( P \cdot \sigma^{-n}(1/k) \), where \( k \) is the leading coefficient of \( P \) and \( \sigma \) is the twisting morphism.

**EXAMPLES:**

```python
sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x',Frob]
sage: a = (3*t^2 + 3*t + 2)*x^3 + (2*t^2 + 3)*x^2 + (4*t^2 + t + 4)*x + 2*t^2
    ...+ 2
sage: b = a.left_monic(); b
x^3 + (4*t^2 + 3*t)*x^2 + (4*t + 2)*x + 2*t^2 + 4*t + 3
```

Check list:

```python
sage: b.degree() == a.degree()
True
sage: b.is_left_divisible_by(a)
True
sage: twist = S.twisting_morphism(-a.degree())
sage: a == b * twist(a.leading_coefficient())
True
```

Note that \( b \) does not divide \( a \) on the right:

```python
sage: a.is_right_divisible_by(b)
False
```

This function does not work if the leading coefficient is not a unit:

```python
sage: R.<t> = QQ[]
sage: der = R.derivation()
sage: S.<x> = R['x', der]
sage: a = t*x
sage: a.left_monic()
Traceback (most recent call last):
  ...
NotImplementedError: the leading coefficient is not a unit
```

Return the quotient and remainder of the left euclidean division of \( \text{self} \) by \( \text{other} \).

**INPUT:**

- \( \text{other} \) – a Ore polynomial in the same ring as \( \text{self} \)

**OUTPUT:**

- the quotient and the remainder of the left euclidean division of this Ore polynomial by \( \text{other} \)
Note: This will fail if the leading coefficient of \texttt{other} is not a unit or if Sage can’t invert the twisting morphism.

EXAMPLES:

```python
sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x',Frob]
sage: a = (3*t^2 + 3*t + 2)*x^3 + (2*t^2 + t + 4)*x + 2*t^2
sage: a == b*q + r
True
```

In the following example, Sage does not know the inverse of the twisting morphism:

```python
sage: R.<t> = QQ[]
sage: K = R.fraction_field()
sage: sigma = K.hom([(t+1)/(t-1)])
sage: S.<x> = K['x',sigma]
sage: a = (-2*t^2 - t + 1)*x^3 + (-t^2 + t)*x^2 + (-12*t - 2)*x - t^2 - 95*t
sage: b = x^2 + (5*t - 6)*x - 4*t^2 + 4*t - 1
sage: a.left_quo_rem(b)
Traceback (most recent call last):
  ... NotImplementedError: inversion of the twisting morphism
```

```

1.2. Univariate Ore Polynomials

\texttt{left\_xgcd}\ (\texttt{other}, \texttt{monic=\textit{True}})

Return the left gcd of \texttt{self} and \texttt{other} along with the coefficients for the linear combination.

If \(a\) is \texttt{self} and \(b\) is \texttt{other}, then there are Ore polynomials \(u\) and \(v\) such that \(g = au + bv\), where \(g\) is the left gcd of \(a\) and \(b\). This method returns \((g, u, v)\).

**INPUT:**

- \texttt{other} — a Ore polynomial in the same ring as \texttt{self}
- \texttt{monic} — boolean (default: \texttt{True}); return whether the left gcd should be normalized to be monic

**OUTPUT:**

- The left gcd of \texttt{self} and \texttt{other}, that is a Ore polynomial \(g\) with the following property: any Ore polynomial is divisible on the left by \(g\) iff it is divisible on the left by both \texttt{self} and \texttt{other}. If \texttt{monic} is \texttt{True}, \(g\) is in addition monic. (With this extra condition, it is uniquely determined.)
- Two Ore polynomials \(u\) and \(v\) such that:

\[
g = a\cdot u + b\cdot v,
\]

where \(s\) is \texttt{self} and \(b\) is \texttt{other}.

**Note:** Works only if following two conditions are fulfilled (otherwise left gcd do not exist in general): 1) the base ring is a field and 2) the twisting morphism is bijective.

25
EXAMPLES:

```sage
sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x', Frob]
sage: a = (x + t) * (x^2 + t*x + 1)
sage: b = 2 * (x + t) * (x^3 + (t+1)*x^2 + t^2)
sage: g, u, v = a.left_xgcd(b); g
x + t
```

```
True
```

Specifying `monic=False`, we can get a nonmonic gcd:

```sage
sage: g, u, v = a.left_xgcd(b, monic=False); g
2*t*x + 4*t + 2
```

```
True
```

The base ring must be a field:

```sage
sage: R.<t> = QQ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x', sigma]
sage: a = (x + t) * (x^2 + t*x + 1)
sage: b = 2 * (x + t) * (x^3 + (t+1)*x^2 + t^2)
sage: a.left_xgcd(b)
Traceback (most recent call last):
...  TypeError: the base ring must be a field
```

And the twisting morphism must be bijective:

```sage
sage: FR = R.fraction_field()
sage: f = FR.hom([FR(t)^2])
sage: S.<x> = FR['x', f]
sage: a = (x + t) * (x^2 + t*x + 1)
sage: b = 2 * (x + t) * (x^3 + (t+1)*x^2 + t^2)
sage: a.left_xgcd(b)
Traceback (most recent call last):
...  Not ImplementedError: inversion of the twisting morphism
```

`left_xlcm(other, monic=True)`

Return the left lcm \( L \) of `self` and `other` together with two Ore polynomials \( U \) and \( V \) such that

\[
U \cdot self = V \cdot other = L.
\]

EXAMPLES:

```sage
sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x', Frob]
sage: P = (x + t^2) * (x + t)
sage: Q = 2 * (x^2 + t + 1) * (x * t)
sage: L, U, V = P.left_xlcm(Q)
```
number_of_terms()  
Return the number of non-zero coefficients of self.

This is also known as the weight, hamming weight or sparsity.

EXAMPLES:

```
sage: R.<t> = QQ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x',sigma]
sage: a = 1 + t*x^3 + t^2*x^5
sage: a.number_of_terms()
3
```

This is also an alias for hamming_weight:

```
sage: a.hamming_weight()
3
```

padded_list(n=None)  
Return list of coefficients of self up to (but not including) degree n.

Includes 0.

INPUT:

- n – (default: None); if given, an integer that is at least 0

EXAMPLES:

```
sage: R.<t> = QQ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x',sigma]
sage: a = 1 + t*x^3 + t^2*x^5
sage: a.padded_list()
[1, 0, 0, t, 0, t^2]
sage: a.padded_list(10)
[1, 0, 0, t, 0, t^2, 0, 0, 0, 0]
sage: len(a.padded_list(10))
10
sage: a.padded_list(3)
[1, 0, 0]
sage: a.padded_list(0)
[]
sage: a.padded_list(-1)
Traceback (most recent call last):
...
ValueError: n must be at least 0
```
prec()
Return the precision of self.
This is always infinity, since polynomials are of infinite precision by definition (there is no big-oh).

EXAMPLES:

```sage
sage: R.<t> = QQ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x',sigma]
sage: x.prec()
+Infinity
```

right_divides(other)
Check if self divides other on the right.

INPUT:
- • other – a Ore polynomial in the same ring as self

OUTPUT:
Return True or False.

EXAMPLES:

```sage
sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x',Frob]
sage: a = x^2 + t*x + t^2 + 3
sage: b = x^3 + (t + 1)*x^2 + 1
sage: c = a*b
sage: a.right_divides(c)
False
sage: b.right_divides(c)
True
```

Divisibility by 0 does not make sense:

```sage
sage: S(0).right_divides(c)
Traceback (most recent call last):
... 
ZeroDivisionError: division by zero is not valid
```

This function does not work if the leading coefficient of the divisor is not a unit:

```sage
sage: R.<t> = QQ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x',sigma]
sage: a = x^2 + 2*x + t
sage: b = (t+1)*x + t^2
sage: c = a*b
sage: b.right_divides(c)
Traceback (most recent call last):
... 
NotImplementedError: the leading coefficient of the divisor is not invertible
```

right_gcd(other, monic=True)
Return the right gcd of self and other.

INPUT:
• other – a Ore polynomial in the same ring as self
• monic – boolean (default: True); return whether the right gcd should be normalized to be monic

OUTPUT:
The right gcd of self and other, that is a Ore polynomial \( g \) with the following property: any Ore polynomial is divisible on the right by \( g \) iff it is divisible on the right by both self and other. If monic is True, \( g \) is in addition monic. (With this extra condition, it is uniquely determined.)

Note: Works only if the base ring is a field (otherwise right gcd do not exist in general).

EXAMPLES:

```sage
def gcd_example():
    k.<t> = GF(5^3)
    Frob = k.frobenius_endomorphism()
    S.<x> = k['x',Frob]
    a = (x^2 + t*x + 1) * (x + t)
    b = 2 * (x^3 + (t+1)*x^2 + t^2) * (x + t)
    g = a.right_gcd(b)
    return g

def main():
    gcd_value = gcd_example()
    print(gcd_value)

if __name__ == '__main__':
    main()
```

Specifying monic=False, we can get a nonmonic gcd:

```sage
def nonmonic_gcd_example():
    a = (x^2 + t*x + 1) * (x + t)
    b = 2 * (x^3 + (t+1)*x^2 + t^2) * (x + t)
    g = a.right_gcd(b,monic=False)
    return g

def main():
    nonmonic_value = nonmonic_gcd_example()
    print(nonmonic_value)

if __name__ == '__main__':
    main()
```

The base ring need to be a field:

```sage
def field_example():
    R.<t> = QQ[]
    sigma = R.hom([t+1])
    S.<x> = R['x',sigma]
    a = (x^2 + t*x + 1) * (x + t)
    b = 2 * (x^3 + (t+1)*x^2 + t^2) * (x + t)
    g = a.right_gcd(b)
    g

def main():
    field_value = field_example()
    print(field_value)

if __name__ == '__main__':
    main()
```

right_lcm (other, monic=True)

Return the right lcm of self and other.

INPUT:
• other – a Ore polynomial in the same ring as self
• monic – boolean (default: True); return whether the right lcm should be normalized to be monic

OUTPUT:
The right lcm of self and other, that is a Ore polynomial \( g \) with the following property: any Ore polynomial divides \( g \) on the left iff it divides both self and other on the left. If monic is True, \( g \) is in addition monic. (With this extra condition, it is uniquely determined.)

Note: Works only if two following conditions are fulfilled (otherwise right lcm do not exist in general): 1) the base ring is a field and 2) the twisting morphism on this field is bijective.

EXAMPLES:
```python
sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x', Frob]
sage: a = (x + t) * (x + t^2)
sage: b = 2 * (x + t) * (x^2 + t + 1)
sage: c = a.right_lcm(b);
c
x^4 + (2*t^2 + t + 2)*x^3 + (3*t^2 + 4*t + 1)*x^2 + (3*t^2 + 4*t + 1)*x + t^2
˓→ 4
sage: c.is_left_divisible_by(a)
True
sage: c.is_left_divisible_by(b)
True
sage: a.degree() + b.degree() == c.degree() + a.left_gcd(b).degree()
True

Specifying monic=False, we can get a nonmonic gcd:

```python
sage: a.right_lcm(b, monic=False)
2*t*x^4 + (3*t + 1)*x^3 + (4*t^2 + 4*t + 3)*x^2
+ (3*t^2 + 4*t + 2)*x + 3*t^2 + 2*t + 3
```

The base ring needs to be a field:

```python
sage: R.<t> = QQ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x', sigma]
sage: a = (x + t) * (x + t^2)
sage: b = 2 * (x + t) * (x^2 + t + 1)
sage: a.right_lcm(b)
Traceback (most recent call last):
...
TypeError: the base ring must be a field
```

And the twisting morphism needs to be bijective:

```python
sage: FR = R.fraction_field()
sage: f = FR.hom([FR(t)^2])
sage: S.<x> = FR['x', f]
sage: a = (x + t) * (x + t^2)
sage: b = 2 * (x + t) * (x^2 + t + 1)
sage: a.right_lcm(b)
Traceback (most recent call last):
...
NotImplementedError: inversion of the twisting morphism
```

`right_mod(other)`

Return the remainder of right division of self by other.

**EXAMPLES:**

```python
sage: R.<t> = QQ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x', sigma]
sage: a = 1 + t*x^2
sage: b = x + 1
```
right_monic()

Return the unique monic Ore polynomial which divides this polynomial on the right and has the same degree.

Given a Ore polynomial \( P \) of degree \( n \), its left monic is given by \((1/k)\cdot P\), where \( k \) is the leading coefficient of \( p \).

EXAMPLES:

```python
sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x', Frob]
sage: a = (3*t^2 + 3*t + 2)*x^3 + (2*t^2 + 3)*x^2 + (4*t^2 + t + 4)*x + 2*t^2 + 2
sage: b = a.right_monlic(); b
x^3 + (2*t^2 + 3*t + 4)*x^2 + (3*t^2 + 4*t + 1)*x + 2*t^2 + 4*t + 3
```

Check list:

```python
sage: b.degree() == a.degree()
True
sage: b.is_right_divisible_by(a)
True
sage: a == a.leading_coefficient() * b
True
```

Note that \( b \) does not divide \( a \) on the right:

```python
sage: a.is_left_divisible_by(b)
False
```

This function does not work if the leading coefficient is not a unit:

```python
sage: R.<t> = QQ[]
sage: der = R.derivation()
sage: S.<x> = R['x', der]
sage: a = t*x
sage: a.right_monlic()
Traceback (most recent call last):
  ...
NotImplementedError: the leading coefficient is not a unit
```

right_quo_rem(other)

Return the quotient and remainder of the right euclidean division of self by other.

INPUT:

- other – a Ore polynomial in the same ring as self

OUTPUT:

- the quotient and the remainder of the left euclidean division of this Ore polynomial by other
Note: This will fail if the leading coefficient of the divisor is not a unit.

EXAMPLES:

```
sage: R.<t> = ZZ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x',sigma]
sage: a = S.random_element(degree=4); a
(-t - 95)*x^4 + x^3 + (2*t - 1)*x
sage: b = S.random_element(monic=True); b
x^2 + (-12*t - 2)*x
sage: q,r = a.right_quo_rem(b)
sage: a == q*b + r
True
```

The leading coefficient of the divisor need to be invertible:

```
sage: c = S.random_element(); c
(t - 1)*x^2 + t^2*x
sage: a.right_quo_rem(c)
Traceback (most recent call last):
... NotImplementedError: the leading coefficient of the divisor is not invertible
```

**right_xgcd**(other, monic=True)

Return the right gcd of self and other along with the coefficients for the linear combination.

If a is self and b is other, then there are Ore polynomials u and v such that g = ua + vb, where g is the right gcd of a and b. This method returns (g, u, v).

**INPUT:**

- other – a Ore polynomial in the same ring as self
- monic – boolean (default: True); return whether the right gcd should be normalized to be monic

**OUTPUT:**

- The right gcd of self and other, that is a Ore polynomial g with the following property: any Ore polynomial is divisible on the right by g iff it is divisible on the right by both self and other. If monic is True, g is in addition monic. (With this extra condition, it is uniquely determined.)
- Two Ore polynomials u and v such that:

  \[ g = u \ast a + v \ast b \]

  where \( a \) is self and \( b \) is other.

**Note:** Works only if the base ring is a field (otherwise right gcd do not exist in general).

EXAMPLES:

```
sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x',Frob]
sage: a = (x^2 + t*x + 1) * (x + t)
sage: b = 2 * (x^3 + (t+1)*x^2 + t^2) * (x + t)
```
Specifying `monic=False`, we can get a nonmonic gcd:

```python
sage: g,u,v = a.right_xgcd(b,monic=False); g
(4*t^2 + 4*t + 1)*x + 4*t^2 + 4*t + 3
sage: u*a + v*b == g
True
```

The base ring must be a field:

```python
sage: R.<t> = QQ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x',sigma]
sage: a = (x^2 + t*x + 1) * (x + t)
sage: b = 2 * (x^3 + (t+1)*x^2 + t^2) * (x + t)
sage: a.right_xgcd(b)
Traceback (most recent call last):
 ... 
TypeError: the base ring must be a field
```

**right_lcm(other, monic=True)**

Return the right lcm \( L \) of \( self \) and \( other \) together with two Ore polynomials \( U \) and \( V \) such that

\[
self \cdot U = other \cdot V = L.
\]

**INPUT:**

- `other` – a Ore polynomial in the same ring as `self`
- `monic` – a boolean (default: True); whether the right lcm should be normalized to be monic

**EXAMPLES:**

```python
sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x',Frob]
sage: P = (x + t) * (x + t^2)
sage: Q = 2 * (x + t) * (x^2 + t + 1)
sage: L, U, V = P.right_lcm(Q)
sage: L
x^4 + (2*t^2 + t + 2)*x^3 + (3*t^2 + 4*t + 1)*x^2 + (3*t^2 + 4*t + 1)*x + t^2
˓→ 4
sage: P*U == L
True
sage: Q*V == L
True
```

**shift**(n)

Return `self` multiplied on the right by the power \( x^n \).

If \( n \) is negative, terms below \( x^n \) will be discarded.

**EXAMPLES:**
sage: R.<t> = QQ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x', sigma]
sage: a = x^5 + t^4*x^4 + t^2*x^2 + t^10
sage: a.shift(0)
x^5 + t^4*x^4 + t^2*x^2 + t^10
sage: a.shift(-1)
x^4 + t^4*x^3 + t^2*x
sage: a.shift(-5)
1
sage: a.shift(2)
x^7 + t^4*x^6 + t^2*x^4 + t^10*x^2

One can also use the infix shift operator:

sage: a >> 2
x^3 + t^4*x^2 + t^2
sage: a << 2
x^7 + t^4*x^6 + t^2*x^4 + t^10*x^2

**square()**

Return the square of self.

**EXAMPLES:**

sage: R.<t> = QQ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x', sigma]
sage: a = x + t; a
x + t
sage: a.square()
x^2 + (2*t + 1)*x + t^2
sage: a.square() == a*a
True
sage: der = R.derivation()
sage: A.<d> = R['d', der]
sage: (d + t).square()
d^2 + 2*t*d + t^2 + 1

**variable_name()**

Return the string name of the variable used in self.

**EXAMPLES:**

sage: R.<t> = QQ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x', sigma]
sage: a = x + t
sage: a
x + t
sage: a.variable_name()
'x'

**class** sage.rings.polynomial.ore_polynomial_element.OrePolynomialBaseringInjection

Bases: sage.categories.morphism.Morphism

Representation of the canonical homomorphism from a ring $R$ into a Ore polynomial ring over $R$.

This class is necessary for automatic coercion from the base ring to the Ore polynomial ring.

See also:
PolynomialBaseringInjection

**EXAMPLES:**

```python
sage: R.<t> = QQ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x', sigma]
sage: S.coerce_map_from(S.base_ring()) # indirect doctest
Ore Polynomial base injection morphism:
  From: Univariate Polynomial Ring in t over Rational Field
  To:   Ore Polynomial Ring in x over Univariate Polynomial Ring in t over Rational Field twisted by t |→ t + 1
```

`an_element()`

Return an element of the codomain of the ring homomorphism.

**EXAMPLES:**

```python
sage: from sage.rings.polynomial.ore_polynomial_element import OrePolynomialBaseringInjection
sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x', Frob]
sage: m = OrePolynomialBaseringInjection(k, k['x', Frob])
sage: m.an_element()
x
```

`section()`

Return the canonical homomorphism from the constants of a Ore polynomial ring to the base ring according to `self`.

**class** sage.rings.polynomial.ore_polynomial_element.OrePolynomial_generic_dense

Bases: sage.rings.polynomial.ore_polynomial_element.OrePolynomial

Generic implementation of dense Ore polynomial supporting any valid base ring, twisting morphism and twisting derivation.

`coefficients(sparse=True)`

Return the coefficients of the monomials appearing in `self`.

If `sparse=True` (the default), return only the non-zero coefficients. Otherwise, return the same value as `self.list()`.

**EXAMPLES:**

```python
sage: R.<t> = QQ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x', sigma]
sage: a = 1 + x^4 + (t+1)*x^2 + t^2
sage: a.coefficients()  # sparse=True
[t^2 + 1, t + 1, 1]
sage: a.coefficients(sparse=False)
[t^2 + 1, 0, t + 1, 0, 1]
```

`degree()`

Return the degree of `self`.

By convention, the zero Ore polynomial has degree $-1$.

**EXAMPLES:**

```python
```
sage: R.<t> = ZZ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x',sigma]
sage: a = x^2 + t*x^3 + t^2*x + 1
sage: a.degree()
3

By convention, the degree of 0 is −1:

sage: S(0).degree()
-1

dict()

Return a dictionary representation of self.

EXAMPLES:

sage: R.<t> = ZZ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x',sigma]
sage: a = x^2012 + t*x^1006 + t^3 + 2*t
sage: a.dict()
{0: t^3 + 2*t, 1006: t, 2012: 1}

hilbert_shift(s, var=None)

Return this Ore polynomial with variable shifted by \( s \), i.e. if this Ore polynomial is \( P(x) \), return \( P(x+s) \).

INPUT:

- \( s \) – an element in the base ring
- \( var \) – a string; the variable name

EXAMPLES:

sage: R.<t> = GF(7)[]
sage: der = R.derivation()
sage: A.<d> = R['d', der]
sage: L = d^3 + t*d^2
sage: L.hilbert_shift(t)
d^3 + 4*t*d^2 + (5*t^2 + 3)*d + 2*t^3 + 4*t
sage: (d+t)^3 + t*(d+t)^2

One can specify another variable name:

sage: L.hilbert_shift(t, var='x')
x^3 + 4*t*x^2 + (5*t^2 + 3)*x + 2*t^3 + 4*t

When the twisting morphism is not trivial, the output lies in a different Ore polynomial ring:

sage: k.<a> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x', Frob]
sage: P = x^2 + a*x + a^2
sage: Q = P.hilbert_shift(a); Q
x^2 + (2*a^2 + a + 4)*x + a^2 + 3*a + 4

(continues on next page)
This behavior ensures that the Hilbert shift by a fixed element defines an homomorphism of rings:

\[
\begin{align*}
\text{sage: } & U = S.random_element(degree=5) \\
\text{sage: } & V = S.random_element(degree=5) \\
\text{sage: } & s = k.random_element() \\
\text{sage: } & (U+V).hilbert_shift(s) == U.hilbert_shift(s) + V.hilbert_shift(s) \\
\text{True} \\
\text{sage: } & (U*V).hilbert_shift(s) == U.hilbert_shift(s) * V.hilbert_shift(s) \\
\text{True}
\end{align*}
\]

We check that shifting by an element and then by its opposite gives back the initial Ore polynomial:

\[
\begin{align*}
\text{sage: } & P = S.random_element(degree=10) \\
\text{sage: } & s = k.random_element() \\
\text{sage: } & P.hilbert_shift(s).hilbert_shift(-s) == P \\
\text{True}
\end{align*}
\]

\textbf{list (copy=True)}

Return a list of the coefficients of self.

\textbf{EXAMPLES:}

\[
\begin{align*}
\text{sage: } & R.<t> = QQ[] \\
\text{sage: } & sigma = R.hom([t+1]) \\
\text{sage: } & S.<x> = R['x',sigma] \\
\text{sage: } & a = 1 + x^4 + (t+1)*x^2 + t^2 \\
\text{sage: } & l = a.list(); l \\
\text{[t^2 + 1, 0, t + 1, 0, 1]}
\end{align*}
\]

Note that \(l\) is a list, it is mutable, and each call to the list method returns a new list:

\[
\begin{align*}
\text{sage: } & \text{type(l)} \\
\langle... 'list'> \\
\text{sage: } & l[0] = 5 \\
\text{sage: } & a.list() \\
\text{[t^2 + 1, 0, t + 1, 0, 1]}
\end{align*}
\]

\textbf{truncate (n)}

Return the polynomial resulting from discarding all monomials of degree at least \(n\).

\textbf{EXAMPLES:}

\[
\begin{align*}
\text{sage: } & R.<t> = ZZ[] \\
\text{sage: } & sigma = R.hom([t+1]) \\
\text{sage: } & S.<x> = R['x',sigma] \\
\text{sage: } & a = t*x^3 + x^4 + (t+1)*x^2 + t^2 \\
\text{sage: } & a.truncate(4) \\
t*x^3 + (t + 1)*x^2 \\
\text{sage: } & a.truncate(3) \\
(t + 1)*x^2
\end{align*}
\]
valuation()

Return the minimal degree of a non-zero monomial of self.

By convention, the zero Ore polynomial has valuation +\infty.

EXAMPLES:

```
sage: R.<t> = ZZ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x',sigma]
sage: a = x^2 + t*x^3 + t^2*x
sage: a.valuation()
1
```

By convention, the valuation of 0 is +\infty:

```
sage: S(0).valuation()
+Infinity
```

1.3 Skew Univariate Polynomial Rings

This module provides the \texttt{SkewPolynomialRing}. In the class hierarchy in Sage, the locution \textit{Skew Polynomial} is used for a Ore polynomial without twisting derivation.

This module also provides:

- the class \texttt{SkewPolynomialRing\_finite\_order}, which is a specialized class for skew polynomial rings over fields equipped with an automorphism of finite order. It inherits from \texttt{SkewPolynomialRing} but contains more methods and provides better algorithms.

- the class \texttt{SkewPolynomialRing\_finite\_field}, which is a specialized class for skew polynomial rings over finite fields.

See also:

\texttt{OrePolynomialRing}

AUTHOR:

- Xavier Caruso (2012-06-29): initial version
- Arpit Merchant (2016-08-04): improved docstrings, fixed doctests and refactored classes and methods
- Johan Rosenkilde (2016-08-03): changes for bug fixes, docstring and doctest errors

```
class sage.rings.polynomial.skew_polynomial_ring.SectionSkewPolynomialCenterInjection
Bases: sage.categories.map.Section

Section of the canonical injection of the center of a skew polynomial ring into this ring.
```

```
class sage.rings.polynomial.skew_polynomial_ring.SkewPolynomialCenterInjection
    (domain, codomain, order)
Bases: sage.rings.morphism.RingHomomorphism

Canonical injection of the center of a skew polynomial ring into this ring.
```
section()

Return a section of this morphism.

EXAMPLES:

```
sage: k.<a> = GF(5^3)
sage: S.<x> = SkewPolynomialRing(k, k.frobenius_endomorphism())
sage: Z = S.center()
sage: iota = S.convert_map_from(Z)
sage: sigma = iota.section()
sage: sigma(x^3)
z
```

class SageRingPolynomialSkewPolynomialRing(SkewPolynomialRing(base_ring, twisting_morphism, derivation, name, sparse, category=None))

Bases: SageRingPolynomialOrePolynomialRing

Initialize self.

INPUT:

- `base_ring` – a commutative ring
- `twisting_morphism` – an automorphism of the base ring
- `name` – string or list of strings representing the name of the variables of ring
- `sparse` – boolean (default: False)
- `category` – a category

EXAMPLES:

```
sage: R.<t> = ZZ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = SkewPolynomialRing(R, sigma)
sage: S.category()
Category of algebras over Univariate Polynomial Ring in t over Integer Ring
sage: S([-1]) + S([1])
0
sage: TestSuite(S).run()
```

lagrange_polynomial(points)

Return the minimal-degree polynomial which interpolates the given points.

More precisely, given \( n \) pairs \((x_1, y_1), \ldots, (x_n, y_n)\) \( \in R^2 \), where \( R \) is `self.base_ring()`, compute a skew polynomial \( p(x) \) such that \( p(x_i) = y_i \) for each \( i \), under the condition that the \( x_i \) are linearly independent over the fixed field of `self.twisting_morphism()`.

If the \( x_i \) are linearly independent over the fixed field of `self.twisting_morphism()` then such a polynomial is guaranteed to exist. Otherwise, it might exist depending on the \( y_i \), but the algorithm used in this implementation does not support that, and so an error is always raised.

INPUT:
• **points** — a list of pairs \((x_1, y_1), \ldots, (x_n, y_n)\) of elements of the base ring of `self`; the \(x_i\) should be linearly independent over the fixed field of `self.twisting_morphism()`

**OUTPUT:**

The Lagrange polynomial.

**EXAMPLES:**

```python
sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x',Frob]
sage: points = [(t, 3*t^2 + 4*t + 4), (t^2, 4*t)]
sage: d = S.lagrange_polynomial(points); d
x + t
sage: R.<t> = ZZ[]
sage: sigma = R.hom([t+1])
sage: T.<x> = R['x', sigma]
sage: points = [ (1, t^2 + 3*t + 4), (t, 2*t^2 + 3*t + 1), (t^2, t^2 + 3*t + 4) ]
sage: p = T.lagrange_polynomial(points); p
((-t^4 - 2*t - 3)/(-2))*x^2 + (-t^4 - t^3 - t^2 - 3*t - 2)*x + (-t^4 - 2*t^3 -
\rightarrow 4*t^2 - 10*t - 9)/(-2)
sage: p.multi_point_evaluation([1, t, t^2]) == [ t^2 + 3*t + 4, 2*t^2 + 3*t + 1,
\rightarrow t^2 + 3*t + 4 ]
True
```

If the \(x_i\) are linearly dependent over the fixed field of `self.twisting_morphism()`, then an error is raised:

```python
sage: T.lagrange_polynomial([(t, 1), (2*t, 3)])
Traceback (most recent call last):
  ...
ValueError: the given evaluation points are linearly dependent over the fixed
\rightarrow field of the twisting morphism, so a Lagrange polynomial could not be determined (and might not exist)
```

minimal_vanishing_polynomial (eval_pts)

Return the minimal-degree, monic skew polynomial which vanishes at all the given evaluation points.

The degree of the vanishing polynomial is at most the length of `eval_pts`. Equality holds if and only if the elements of `eval_pts` are linearly independent over the fixed field of `self.twisting_morphism()`.

• **eval_pts** — list of evaluation points which are linearly independent over the fixed field of the twisting morphism of the associated skew polynomial ring

**OUTPUT:**

The minimal vanishing polynomial.

**EXAMPLES:**

```python
sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x',Frob]
sage: eval_pts = [1, t, t^2]
sage: b = S.minimal_vanishing_polynomial(eval_pts); b
x^3 + 4
```
The minimal vanishing polynomial evaluates to 0 at each of the evaluation points:

```
sage: eval = b.multi_point_evaluation(eval_pts); eval
[0, 0, 0]
```

If the evaluation points are linearly dependent over the fixed field of the twisting morphism, then the returned polynomial has lower degree than the number of evaluation points:

```
sage: S.minimal_vanishing_polynomial([t])
x + 3*t^2 + 3*t
sage: S.minimal_vanishing_polynomial([t, 3*t])
x + 3*t^2 + 3*t
```

**class** `sage.rings.polynomial.skew_polynomial_ring.SkewPolynomialRing_finite_field`

A specialized class for skew polynomial rings over finite fields.

See also:

- `sage.rings.polynomial.skew_polynomial_ring.SkewPolynomialRing`
- `sage.rings.polynomial.skew_polynomial_finite_field`

**Todo:** Add methods related to center of skew polynomial ring, irreducibility, karatsuba multiplication and factorization.

```
```
center \(\text{name=\text{None}, \text{names=\text{None}, \text{default=\text{False}}}\)}\)

Return the center of this skew polynomial ring.

Note: If \(F\) denotes the subring of \(R\) fixed by \(\sigma\) and \(\sigma\) has order \(r\), the center of \(K[x, \sigma]\) is \(F[x^r]\), that is a univariate polynomial ring over \(F\).

INPUT:

- \text{name} – a string or \text{None} (default: \text{None}); the name for the central variable (namely \(x^r\))
- \text{default} – a boolean (default: \text{False}); if True, set the default variable name for the center to \text{name}

EXAMPLES:

```
sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x',Frob]; S
Ore Polynomial Ring in x over Finite Field in t of size 5^3 twisted by t |--> t^5
sage: Z = S.center(); Z
Univariate Polynomial Ring in z over Finite Field of size 5
sage: Z.gen()
z
```

We can pass in another variable name:

```
sage: S.center(name='y')
Univariate Polynomial Ring in y over Finite Field of size 5
```

or use the bracket notation:

```
sage: Zy.<y> = S.center(); Zy
Univariate Polynomial Ring in y over Finite Field of size 5
sage: y.parent() is Zy
True
```

A coercion map from the center to the skew polynomial ring is set:

```
sage: S.has_coerce_map_from(Zy)
True
sage: P = y + x; P
x^3 + x
sage: P.parent()
Ore Polynomial Ring in x over Finite Field in t of size 5^3 twisted by t |--> t^5
sage: P.parent() is S
True
```

together with a conversion map in the reverse direction:

```
sage: Zy(x^6 + 2*x^3 + 3)
y^2 + 2*y + 3
sage: Zy(x^2)
```

(continues on next page)
Two different skew polynomial rings can share the same center:

```python
sage: S1.<x1> = k['x1', Frob]
sage: S2.<x2> = k['x2', Frob]
sage: S1.center() is S2.center()
```

```
True
```

### About the default name of the central variable

A priori, the default is $z$.

However, a variable name is given the first time this method is called, the given name become the default for the next calls:

```python
sage: K.<t> = GF(11^3)
sage: phi = K.frobenius_endomorphism()
sage: A.<X> = K['X', phi]
sage: C.<u> = A.center()  # first call
sage: C
Univariate Polynomial Ring in u over Finite Field of size 11
sage: A.center()  # second call: the variable name is still u
Univariate Polynomial Ring in u over Finite Field of size 11
sage: A.center() is C
```

```
True
```

We can update the default variable name by passing in the argument `default=True`:

```python
sage: D.<v> = A.center(default=True)
sage: D
Univariate Polynomial Ring in v over Finite Field of size 11
sage: A.center()
Univariate Polynomial Ring in v over Finite Field of size 11
sage: A.center() is D
```

```
True
```

### 1.4 Univariate Skew Polynomials

This module provides the `SkewPolynomial`. In the class hierarchy in Sage, the locution `Skew Polynomial` is used for a Ore polynomial without twisting derivation.

**Warning:** The current semantics of `__call__()` are experimental, so a warning is thrown when a skew polynomial is evaluated for the first time in a session. See the method documentation for details.

**AUTHORS:**

- Xavier Caruso (2012-06-29): initial version
• Arpit Merchant (2016-08-04): improved docstrings, fixed doctests and refactored classes and methods
• Johan Rosenkilde (2016-08-03): changes for bug fixes, docstring and doctest errors

class sage.rings.polynomial.skew_polynomial_element.SkewPolynomial_generic_dense
    Bases: sage.rings.polynomial.ore_polynomial_element.OrePolynomial_generic_dense

    Generic implementation of dense skew polynomial supporting any valid base ring and twisting morphism.

    conjugate (n)
    Return self conjugated by \( x^n \), where \( x \) is the variable of self.
    The conjugate is obtained from self by applying the \( n \)-th iterate of the twisting morphism to each of its coefficients.
    INPUT:
    • \( n \) – an integer, the power of conjugation

    EXAMPLES:
    
    sage: R.<t> = QQ[
    sage: K = R.fraction_field()
    sage: sigma = K.hom([1 + 1/t])
    sage: S.<x> = K['x',sigma]
    sage: a = t*x^3 + (t^2 + 1)*x^2 + 2*t
    sage: b = a.conjugate(2); b
    ((2*t + 1)/(t + 1))*x^3 + ((5*t^2 + 6*t + 2)/(t^2 + 2*t + 1))*x^2 + (4*t + 2)/
    →(t + 1)
    sage: x^2*a == b*x^2
    True

    In principle, negative values for \( n \) are allowed, but Sage needs to be able to invert the twisting morphism:

    sage: b = a.conjugate(-1)
    Traceback (most recent call last):
    ... 
    NotImplementedError: inverse not implemented for morphisms of Fraction Field
    →of Univariate Polynomial Ring in t over Rational Field

    Here is a working example:

    sage: k.<t> = GF(5^3)
    sage: Frob = k.frobenius_endomorphism()
    sage: T.<y> = k['y',Frob]
    sage: u = T.random_element(); u
    (2*t^2 + 3)*y^2 + (4*t^2 + t + 4)*y + 2*t^2 + 2
    sage: v = u.conjugate(-1); v
    (3*t^2 + t)*y^2 + (4*t^2 + 2*t + 4)*y + 3*t^2 + t + 4
    sage: u*y == y*v
    True

    left_power_mod (exp, modulus)
    Return the remainder of self**exp in the left euclidean division by modulus.
    INPUT:
    • exp – an Integer
    • modulus – a skew polynomial in the same ring as self
    OUTPUT:
Remainder of \texttt{self}^{\ast}\exp \text{ in the left euclidean division} by \texttt{modulus}.

\textbf{REMARK:}

The quotient of the underlying skew polynomial ring by the principal ideal generated by \texttt{modulus} is in general \textit{not} a ring.

As a consequence, Sage first computes exactly \texttt{self}^{\ast}\exp and then reduce it modulo \texttt{modulus}.

\textbf{EXAMPLES:}

\begin{verbatim}
sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x',Frob]
sage: a = x + t
sage: modulus = x^3 + t*x^2 + (t+3)*x - 2
sage: a.left_power_mod(100,modulus)
(4*t^2 + t + 1)*x^2 + (t^2 + 4*t + 1)*x + 3*t^2 + 3*t
\end{verbatim}

\textbf{multi_point_evaluation (eval\_pts)}

Evaluate \texttt{self} at list of evaluation points.

\begin{itemize}
  \item \texttt{eval\_pts} – list of points at which \texttt{self} is to be evaluated
\end{itemize}

\textbf{INPUT:}

\begin{itemize}
  \item \texttt{eval\_pts} – list of points at which \texttt{self} is to be evaluated
\end{itemize}

\textbf{OUTPUT:}

List of values of \texttt{self} at the \texttt{eval\_pts}.

\textbf{Todo:} This method currently trivially calls the evaluation function repeatedly. If fast skew polynomial multiplication is available, an asymptotically faster method is possible using standard divide and conquer techniques and \texttt{minimal_vanishing_polynomial()}.

\textbf{EXAMPLES:}

\begin{verbatim}
sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x',Frob]
sage: a = x + t
sage: eval_pts = [1, t, t^2]
sage: c = a.multi_point_evaluation(eval_pts); c
[t + 1, 3*t^2 + 4*t + 4, 4*t]
sage: c == [ a(e) for e in eval_pts ]
True
\end{verbatim}

\textbf{operator_eval (eval\_pt)}

Evaluate \texttt{self} at \texttt{eval\_pt} by the operator evaluation method.

\begin{itemize}
  \item \texttt{eval\_pt} – element of the base ring of \texttt{self}
\end{itemize}

\textbf{INPUT:}

\begin{itemize}
  \item \texttt{eval\_pt} – element of the base ring of \texttt{self}
\end{itemize}

\textbf{OUTPUT:}

The value of the polynomial at the point specified by the argument.

\textbf{EXAMPLES:}
sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: T.<x> = k['x',Frob]
sage: a = 3*t^2*x^2 + (t + 1)*x + 2
sage: a(t)  # indirect test
2*t^2 + 2*t + 3
sage: a.operator_eval(t)
2*t^2 + 2*t + 3

Evaluation points outside the base ring is usually not possible due to the twisting morphism:

sage: R.<t> = QQ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x',sigma]
sage: a = t*x + 1
sage: a.operator_eval(1/t)
Traceback (most recent call last):...
TypeError: 1/t fails to convert into the map's domain
Univariate Polynomial Ring in t over Rational Field, but a 'pushforward' method is not properly implemented

right_power_mod(exp, modulus)

Return the remainder of self**exp in the right euclidean division by modulus.

INPUT:

- exp – an integer
- modulus – a skew polynomial in the same ring as self

OUTPUT:

Remainder of self**exp in the right euclidean division by modulus.

REMARK:

The quotient of the underlying skew polynomial ring by the principal ideal generated by modulus is in general not a ring.

As a consequence, Sage first computes exactly self**exp and then reduce it modulo modulus.

EXAMPLES:

sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x',Frob]
sage: a = x + t
sage: b = a^5  # indirect doctest
sage: b
x^5 + (2*t^2 + 4)*x^4 + (t^2 + 2)*x^3 + 2*x^2 + (4*t^2 + 2)*x + 2*t^2 + 4*t + 2
sage: b == a * a * a * a * a
True

sage: modulus = x^3 + t*x^2 + (t+3)*x - 2
sage: br = a.right_power_mod(5, modulus); br
(t + 1)*x^2 + (2*t^2 + t + 1)*x + 2*t^2 + 4*t + 2
sage: br == b % modulus
True

(continues on next page)
Negative exponents are supported:

```plaintext
sage: a^(-5)
(x^5 + (2*t^2 + 4)*x^4 + (t^2 + 2)*x^3 + 2*x^2 + (4*t^2 + 2)*x + 2*t^2 + 4*t + 4)^(-1)
sage: b * a^(-5)
1
```

However, they cannot be combined with modulus:

```plaintext
tsage: a.right_power_mod(-10, modulus)
Traceback (most recent call last):
...
ValueError: modulus cannot be combined with negative exponent
```

### 1.5 Univariate Dense Skew Polynomials over a field equipped with a finite order automorphism

**AUTHOR:**
- Xavier Caruso (2012-06-29): initial version

- Arpit Merchant (2016-08-04): improved docstrings, fixed doctests and refactored classes and methods

```python
class sage.rings.polynomial.skew_polynomial_finite_order.SkewPolynomial_finite_order_dense
    Bases: sage.rings.polynomial.skew_polynomial_element.SkewPolynomial_generic_dense

This method constructs a generic dense skew polynomial over a field equipped with an automorphism of finite order.

**INPUT:**

- `parent` – parent of `self`
- `x` – list of coefficients from which `self` can be constructed
- `check` – flag variable to normalize the polynomial
- `construct` – boolean (default: False)

**bound()**

Return a bound of this skew polynomial (i.e. a multiple of this skew polynomial lying in the center).

**Note:** Since `b` is central, it divides a skew polynomial on the left iff it divides it on the right

**ALGORITHM:**

1. Sage first checks whether `self` is itself in the center. It if is, it returns `self`
2. If an optimal bound was previously computed and cached, Sage returns it
3. Otherwise, Sage returns the reduced norm of `self`
As a consequence, the output of this function may depend on previous computations (an example is given below).

**EXAMPLES:**

```sage
k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x', Frob]
sage: Z = S.center(); Z
Univariate Polynomial Ring in z over Finite Field of size 5
sage: a = x^2 + (4*t + 2)*x + 4*t^2 + 3
sage: b = a.bound(); b
z^2 + z + 4
```

We observe that the bound is explicitly given as an element of the center (which is a univariate polynomial ring in the variable \(z\)). We can use conversion to send it in the skew polynomial ring:

```sage
S(b)
x^6 + x^3 + 4
```

We check that \(b\) is divisible by \(a\):

```sage
S(b).is_right_divisible_by(a)
True
S(b).is_left_divisible_by(a)
True
```

Actually, \(b\) is the reduced norm of \(a\):

```sage
b == a.reduced_norm()
True
```

Now, we compute the optimal bound of \(a\) and see that it affects the behavior of `bound()`:

```sage
a.optimal_bound()
z + 3
a.bound()
z + 3
```

**is_central()**

Return `True` if this skew polynomial lies in the center.

**EXAMPLES:**

```sage
k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x', Frob]
sage: x.is_central()
False
sage: (t*x^3).is_central()
False
sage: (x^6 + x^3).is_central()
True
```

**optimal_bound()**

Return the optimal bound of this skew polynomial (i.e. the monic multiple of this skew polynomial of minimal degree lying in the center).
Note: The result is cached.

EXAMPLES:

```
sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x', Frob]
sage: Z = S.center(); Z
Univariate Polynomial Ring in z over Finite Field of size 5
sage: a = x^2 + (4*t + 2)*x + 4*t^2 + 3
sage: b = a.optimal_bound(); b
z + 3
```

We observe that the bound is explicitly given as an element of the center (which is a univariate polynomial ring in the variable \( z \)). We can use conversion to send it in the skew polynomial ring:

```
sage: S(b)
x^3 + 3
```

We check that \( b \) is divisible by \( a \):

```
sage: S(b).is_right_divisible_by(a)
True
sage: S(b).is_left_divisible_by(a)
True
```

__reduced_norm__(\( var=None \))

Return the reduced norm of this skew polynomial.

INPUT:

- \( \text{var} \) – a string or False or None (default: None); the variable name; if False, return the list of coefficients

Note: The result is cached.

EXAMPLES:

```
sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x', Frob]
sage: a = x^3 + (2*t^2 + 3)*x^2 + (4*t^2 + t + 4)*x + 2*t^2 + 2
sage: N = a.reduced_norm(); N
z^3 + 4*z^2 + 4
```

The reduced norm lies in the center of \( S \), which is a univariate polynomial ring in the variable \( z = x^3 \) over \( \mathbb{F}_5 \):

```
sage: N.parent()
Univariate Polynomial Ring in z over Finite Field of size 5
sage: N.parent() is S.center()
True
```

We can use explicit conversion to view \( N \) as a skew polynomial:
By default, the name of the central variable is usually \( z \) (see \texttt{center()} for more details about this). However, the user can specify a different variable name if desired:

```
sage: a.reduced_trace(var='u')
3*u + 4
```

When passing in \texttt{var=False}, a tuple of coefficients (instead of an actual polynomial) is returned:

```
sage: a.reduced_trace(var=False)
(4, 0, 4, 1)
```

\textbf{ALGORITHM:}

If \( r \) (= the order of the twist map) is small compared to \( d \) (= the degree of this skew polynomial), the reduced norm is computed as the determinant of the multiplication by \( P \) (= this skew polynomial) acting on \( K[X, \sigma] \) (= the underlying skew ring) viewed as a free module of rank \( r \) over \( K[X^r] \).

Otherwise, the reduced norm is computed as the characteristic polynomial of the left multiplication by \( X \) on the quotient \( K[X, \sigma]/K[X, \sigma]P \) (which is a \( K \)-vector space of dimension \( d \)).

\textbf{reduced_trace} (\texttt{var=None})

Return the reduced trace of this skew polynomial.

\textbf{INPUT:}

- \texttt{var} – a string or \texttt{False} or \texttt{None} (default: \texttt{None}); the variable name; if \texttt{False}, return the list of coefficients

\textbf{EXAMPLES:}

```
sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x', Frob]
sage: a = x^3 + (2*t^2 + 3)*x^2 + (4*t^2 + t + 4)*x + 2*t^2 + 2
sage: tr = a.reduced_trace(); tr
3*z + 4
```

The reduced trace lies in the center of \( S \), which is a univariate polynomial ring in the variable \( z = x^3 \) over \( F_5 \):

```
sage: tr.parent()
Univariate Polynomial Ring in z over Finite Field of size 5
sage: tr.parent() is S.center()
True
```

We can use explicit conversion to view \( tr \) as a skew polynomial:

```
sage: S(tr)
3*x^3 + 4
```

By default, the name of the central variable is usually \( z \) (see \texttt{center()} for more details about this). However, the user can specify a different variable name if desired:

```
sage: a.reduced_trace(var='u')
3*u + 4
```
When passing in `var=False`, a tuple of coefficients (instead of an actual polynomial) is returned:

```
sage: a.reduced_trace(var=False)
(4, 3)
```

1.6 Univariate Dense Skew Polynomials over Finite Fields

This module provides the class: `sage.rings.polynomial.skew_polynomial_finite_field.SkewPolynomial_finite_field_dense`, which constructs a single univariate skew polynomial over a finite field equipped with the Frobenius endomorphism. Among other things, it implements the fast factorization algorithm designed in [CL2017].

**AUTHOR:**

- Xavier Caruso (2012-06-29): initial version

- Arpit Merchant (2016-08-04): improved docstrings, fixed doctests and refactored classes and methods

```python
class sage.rings.polynomial.skew_polynomial_finite_field.SkewPolynomial_finite_field_dense:
    # Bases...

count_factorizations()
    Return the number of factorizations (as a product of a unit and a product of irreducible monic factors) of this skew polynomial.

    EXAMPLES:
    sage: k.<t> = GF(5^3)
    sage: Frob = k.frobenius_endomorphism()
    sage: S.<x> = k['x',Frob]
    sage: a = x^4 + (4*t + 3)*x^3 + t^2*x^2 + (4*t^2 + 3*t)*x + 3*t
    sage: a.count_factorizations()
    216

We illustrate that an irreducible polynomial in the center have in general a lot of distinct factorizations in the skew polynomial ring:
```
sage: Z.<x3> = S.center()
```
```
sage: N = x3^5 + 4*x3^4 + 4*x3^2 + 4*x3 + 3
```
```
sage: N.is_irreducible()
True
```
```
sage: S(N).count_factorizations()
30537115626
```

```
count_irreducible_divisors()
    Return the number of irreducible monic divisors of this skew polynomial.

    Note: One can prove that there are always as many left irreducible monic divisors as right irreducible monic divisors.

    EXAMPLES:
    sage: k.<t> = GF(5^3)
    sage: Frob = k.frobenius_endomorphism()
    sage: S.<x> = k['x',Frob]
```
We illustrate that a skew polynomial may have a number of irreducible divisors greater than its degree:

```sage
a = x^4 + (4*t + 3)*x^3 + t^2*x^2 + (4*t^2 + 3*t)*x + 3*t
a.count_irreducible_divisors()
12
```

We illustrate that an irreducible polynomial in the center have in general a lot of irreducible divisors in the skew polynomial ring:

```sage
Z.<x3> = S.center()
N = x3^5 + 4*x3^4 + 4*x3 + 4*x3^2 + 4*x3 + 3; N
N.is_irreducible()
True
N.count_irreducible_divisors()
9768751
```

**factor** *(uniform=False)*

Return a factorization of this skew polynomial.

**INPUT:**

- `uniform` - a boolean (default: False); whether the output irreducible divisor should be uniformly distributed among all possibilities

**EXAMPLES:**

```sage
k.<t> = GF(5^3)
Frob = k.frobenius_endomorphism()
S.<x> = k['x',Frob]
a = x^3 + (t^2 + 4*t + 2)*x^2 + (3*t + 3)*x + t^2 + 1
F = a.factor(); F  # random
(x + t^2 + 4) * (x + t + 3) * (x + t)
F.value() == a
True
```

The result of the factorization is cached. Hence, if we try again to factor `a`, we will get the same answer:

```sage
a.factor()  # random
(x + t^2 + 4) * (x + t + 3) * (x + t)
```

However, the algorithm is probabilistic. Hence if we first reinitialize `a`, we may get a different answer:

```sage
a = x^3 + (t^2 + 4*t + 2)*x^2 + (3*t + 3)*x + t^2 + 1
F = a.factor(); F  # random
(x + t^2 + t + 2) * (x + 2*t^2 + t + 4) * (x + t)
F.value() == a
True
```

There is a priori no guarantee on the distribution of the factorizations we get. Passing in the keyword `uniform=True` ensures the output is uniformly distributed among all factorizations:

```sage
a.factor(uniform=True)  # random
(x + t^2 + 4) * (x + t) * (x + t + 3)
a.factor(uniform=True)  # random
(x + 2*t^2) * (x + t^2 + t + 1) * (x + t^2 + t + 2)
a.factor(uniform=True)  # random
(x + 2*t^2 + 3*t) * (x + 4*t + 2) * (x + 2*t + 2)
```
By convention, the zero skew polynomial has no factorization:

```
sage: S(0).factor()
Traceback (most recent call last):
...
ValueError: factorization of 0 not defined
```

`factorizations()`  
Return an iterator over all factorizations (as a product of a unit and a product of irreducible monic factors) of this skew polynomial.

**EXAMPLES:**

```sage
k.<t> = GF(5^3)
k.<t> = GF(5^3)
k.<t> = GF(5^3)
k.<t> = GF(5^3)
k.<t> = GF(5^3)
k.<t> = GF(5^3)
k.<t> = GF(5^3)
k.<t> = GF(5^3)
Frob = k.frobenius_endomorphism()
S.<x> = k['x',Frob]
S.<x> = k['x',Frob]
S.<x> = k['x',Frob]
S.<x> = k['x',Frob]
a = x^3 + (t^2 + 1)*x^2 + (2*t + 3)*x + t^2 + t + 2
a = x^3 + (t^2 + 1)*x^2 + (2*t + 3)*x + t^2 + t + 2
a = x^3 + (t^2 + 1)*x^2 + (2*t + 3)*x + t^2 + t + 2
a = x^3 + (t^2 + 1)*x^2 + (2*t + 3)*x + t^2 + t + 2
iter = a.factorizations(); iter
iter = a.factorizations(); iter
iter = a.factorizations(); iter
iter = a.factorizations(); iter
next(iter) # random
next(iter) # random
next(iter) # random
next(iter) # random
(x + 3*t^2 + 4*t) * (x + 2*t^2) * (x + 4*t^2 + 4*t + 2)
(x + 3*t^2 + 4*t) * (x + 2*t^2) * (x + 4*t^2 + 4*t + 2)
(x + 3*t^2 + 4*t) * (x + 3*t^2 + 2*t + 2) * (x + 4*t^2 + t + 2)
(x + 3*t^2 + 4*t) * (x + 3*t^2 + 2*t + 2) * (x + 4*t^2 + t + 2)
```

We can use this function to build the list of factorizations of \(a\):

```
sage: factorizations = [ F for F in a.factorizations() ]
```

We do some checks:

```
sage: len(factorizations) == a.count_factorizations()
True
sage: len(factorizations) == Set(factorizations).cardinality()  # check no duplicates
True
sage: for F in factorizations:
.....:     assert F.value() == a, "factorization has a different value"
.....:     for d, _ in F:
.....:         assert d.is_irreducible(), "a factor is not irreducible"
```

Note that the algorithm used in this method is probabilistic. As a consequence, if we call it two times with the same input, we can get different orderings:

```
sage: factorizations2 = [ F for F in a.factorizations() ]
sage: factorizations == factorizations2
False
sage: sorted(factorizations) == sorted(factorizations2)
True
```

`is_irreducible()`  
Return True if this skew polynomial is irreducible.

**EXAMPLES:**

```
sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x',Frob]
```

(continues on next page)
Skew polynomials of degree 1 are of course irreducible:

```sage
sage: a = x + t
sage: a.is_irreducible()
True
```

A random irreducible skew polynomial is irreducible:

```sage
sage: S = S.random_irreducible(degree=4,monic=True); a
# random
x^4 + (t + 1)*x^3 + (3*t^2 + 2*t + 3)*x^2 + 3*t*x + 3*t
sage: a.is_irreducible()
True
```

By convention, constant skew polynomials are not irreducible:

```sage
sage: S(1).is_irreducible()
False
sage: S(0).is_irreducible()
False
```

**left_irreducible_divisor** *(uniform=False)*

Return a left irreducible divisor of this skew polynomial.

**INPUT:**

- `uniform` — a boolean (default: `False`); whether the output irreducible divisor should be uniformly distributed among all possibilities

**EXAMPLES:**

```sage
sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x',Frob]
sage: a = x^6 + 3*t*x^5 + (3*t + 1)*x^3 + (4*t^2 + 3*t + 4)*x^2 + (t^2 + 2)*x + 4*t^2 + 3*t
sage: dl = a.left_irreducible_divisor(); dl
# random
x^3 + (t^2 + t + 2)*x^2 + (t + 2)*x + 3*t^2 + t + 4
sage: a.is_left_divisible_by(dl)
True
```

The algorithm is probabilistic. Hence, if we ask again for a left irreducible divisor of `a`, we may get a different answer:

```sage
sage: a.left_irreducible_divisor()  # random
x^3 + (4*t + 3)*x^2 + (2*t^2 + 3*t + 4)*x + 4*t^2 + 2*t
```
We can also generate uniformly distributed irreducible monic divisors as follows:

```python
sage: a.left_irreducible_divisor(uniform=True)  # random
x^3 + (4*t^2 + 3*t + 4)*x^2 + (t^2 + t + 3)*x + 2*t^2 + 3
sage: a.left_irreducible_divisor(uniform=True)  # random
x^3 + (2*t^2 + t + 4)*x^2 + (2*t^2 + 4*t + 4)*x + 2*t + 3
sage: a.left_irreducible_divisor(uniform=True)  # random
x^3 + (t^2 + t + 2)*x^2 + (3*t^2 + t)*x + 2*t + 1
```

By convention, the zero skew polynomial has no irreducible divisor:

```python
sage: S(0).left_irreducible_divisor()
Traceback (most recent call last):
... ValueError: 0 has no irreducible divisor
```

`left_irreducible_divisors()`

Return an iterator over all irreducible monic left divisors of this skew polynomial.

**EXAMPLES:**

```python
sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x',Frob]
sage: a = x^6 + 3*t*x^5 + (3*t + 1)*x^3 + (4*t^2 + 3*t + 4)*x^2 + (t^2 + t + 1)*x + 4*t^2 + 3
t→+ 4*t^2 + 3*t + 3

```

We can use this function to build the list of all monic irreducible divisors of `a`:

```python
sage: leftdiv = [ d for d in a.left_irreducible_divisors() ]
```

Note that the algorithm is probabilistic. As a consequence, if we build again the list of left monic irreducible divisors of `a`, we may get a different ordering:

```python
sage: leftdiv2 = [ d for d in a.left_irreducible_divisors() ]
sage: leftdiv == leftdiv2
False
sage: Set(leftdiv) == Set(leftdiv2)
True
```

`right_irreducible_divisor(uniform=False)`

Return a right irreducible divisor of this skew polynomial.

**INPUT:**

- `uniform` — a boolean (default: `False`); whether the output irreducible divisor should be uniformly distributed among all possibilities

**EXAMPLES:**

```python
sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x',Frob]
sage: a = x^6 + 3*t*x^5 + (3*t + 1)*x^3 + (4*t^2 + 3*t + 4)*x^2 + (t^2 + t + 1)*x + 4*t^2 + 3
결과: `x^3 + (4*t^2 + 3*t + 4)*x^2 + (t^2 + t + 3)*x + 2*t^2 + 3`
sage: dr = a.right_irreducible_divisor(); dr  # random
x^3 + (2*t^2 + t + 4)*x^2 + (4*t + 1)*x + 4*t^2 + t + 1
sage: a.is_right_divisible_by(dr)
True

Right divisors are cached. Hence, if we ask again for a right divisor, we will get the same answer:

sage: a.right_irreducible_divisor()  # random
x^3 + (2*t^2 + t + 4)*x^2 + (4*t + 1)*x + 4*t^2 + t + 1

However the algorithm is probabilistic. Hence, if we first reinitialize $a$, we may get a different answer:

sage: a = x^6 + 3*t*x^5 + (3*t + 1)*x^3 + (4*t^2 + 3*t + 4)*x^2 + (t^2 + 2)*x + 4*t^2 + 3*t + 3
sage: a.right_irreducible_divisor()  # random
x^3 + (t^2 + 3*t + 4)*x^2 + (t + 2)*x + 4*t^2 + t + 1
sage: a.right_irreducible_divisor(uniform=True)  # random
x^3 + (4*t + 2)*x^2 + (2*t^2 + 2*t + 2)*x + 2*t^2 + 2
sage: a.right_irreducible_divisor(uniform=True)  # random
x^3 + (t^2 + 2)*x^2 + (3*t^2 + 1)*x + 4*t^2 + 2*t
sage: a.right_irreducible_divisor(uniform=True)  # random
x^3 + x^2 + (4*t^2 + 2*t + 4)*x + t^2 + 3

By convention, the zero skew polynomial has no irreducible divisor:

sage: S(0).right_irreducible_divisor()
Traceback (most recent call last):
... ValueError: 0 has no irreducible divisor

**right_irreducible_divisors()**

Return an iterator over all irreducible monic right divisors of this skew polynomial.

**EXAMPLES:**

sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x',Frob]
sage: a = x^4 + 2*t*x^3 + 3*t^2*x^2 + (t^2 + t + 1)*x + 4*t + 3
sage: iter = a.right_irreducible_divisors(); iter
<generator object at 0x...>
sage: next(iter)  # random
x + 2*t^2 + 4*t + 4
sage: next(iter)  # random
x + 3*t^2 + 4*t + 1

We can use this function to build the list of all monic irreducible divisors of $a$:

sage: rightdiv = [ d for d in a.right_irreducible_divisors() ]

Note that the algorithm is probabilistic. As a consequence, if we build again the list of right monic irreducible divisors of $a$, we may get a different ordering:
\texttt{sage}: rightdiv2 = [ d \textbf{for} d \textbf{in} a.right_irreducible_divisors() ]
\texttt{sage}: rightdiv == rightdiv2
False
\texttt{sage}: Set(rightdiv) == Set(rightdiv2)
True

\textbf{type} \((N)\)

Return the \(N\)-type of this skew polynomial (see definition below).

\textbf{INPUT:}

\begin{itemize}
  \item \(N\) – an irreducible polynomial in the center of the underlying skew polynomial ring
\end{itemize}

\textbf{Note:} The result is cached.

\textbf{DEFINITION:}

The \(N\)-type of a skew polynomial \(a\) is the Partition \((t_0, t_1, t_2, \ldots)\) defined by

\[ t_0 + \cdots + t_i = \frac{\deg \gcd(a, N^i)}{\deg N}, \]

where \(\deg N\) is the degree of \(N\) considered as an element in the center.

This notion has an important mathematical interest because it corresponds to the Jordan type of the \(N\)-typical part of the associated Galois representation.

\textbf{EXAMPLES:}

\begin{verbatim}
\texttt{sage}: k.<t> = GF(5^3)
\texttt{sage}: Frob = k.frobenius_endomorphism()
\texttt{sage}: S.<x> = k['x',Frob]
\texttt{sage}: Z = S.center(); x3 = Z.gen()
\texttt{sage}: a = x^4 + x^3 + (4*t^2 + 4)*x^2 + (t^2 + 2)*x + 4*t^2
\texttt{sage}: N = x3^2 + x3 + 1
\texttt{sage}: a.type(N)
[1]
\texttt{sage}: N = x3 + 1
\texttt{sage}: a.type(N)
[2]
\texttt{sage}: a = x^3 + (3*t^2 + 1)*x^2 + (3*t^2 + t + 1)*x + t + 1
\texttt{sage}: N = x3 + 1
\texttt{sage}: a.type(N)
[2, 1]
\end{verbatim}

If \(N\) does not divide the reduced map of \(a\), the type is empty:

\begin{verbatim}
\texttt{sage}: N = x3 + 2
\texttt{sage}: a.type(N)
[1]
\end{verbatim}

If \(a = N\), the type is just \([r]\) where \(r\) is the order of the twisting morphism \texttt{Frob}:

\begin{verbatim}
\texttt{sage}: N = x3^2 + x3 + 1
\texttt{sage}: S(N).type(N)
[3]
\end{verbatim}
$N$ must be irreducible:

```python
sage: N = (x3 + 1) * (x3 + 2)
sage: a.type(N)
Traceback (most recent call last):
... ValueError: N is not irreducible
```
2.1 Fraction fields of Ore polynomial rings.

Sage provides support for building the fraction field of any Ore polynomial ring and performing basic operations in it. The fraction field is constructed by the method `sage.rings.polynomial.ore_polynomial_ring.OrePolynomialRing.fraction_field()` as demonstrated below:

```python
sage: R.<t> = QQ[]
sage: der = R.derivation()
sage: A.<d> = R['d', der]
sage: K = A.fraction_field()
sage: K
Ore Function Field in d over Fraction Field of Univariate Polynomial Ring in t over Rational Field twisted by d/dt
```

The simplest way to build elements in $K$ is to use the division operator over Ore polynomial rings:

```python
sage: f = 1/d
sage: f
d^(-1)
sage: f.parent() is K
True
```

**REPRESENTATION OF ELEMENTS:**

Elements in $K$ are internally represented by fractions of the form $s^{-1}t$ with the denominator on the left. Notice that, because of noncommutativity, this is not the same that fractions with denominator on the right. For example, a fraction created by the division operator is usually displayed with a different numerator and/or a different denominator:

```python
sage: g = t / d
sage: g
(d - 1/t)^(-1) * t
sage: g.left_numerator() t
sage: g.right_denominator() d
```

The left numerator and right denominator are accessible as follows:

```python
sage: g.left_numerator() t sage: g.right_denominator() d
```

Similarly the methods `OrePolynomial.left_denominator()` and `OrePolynomial.right_numerator()` give access to the Ore polynomials $s$ and $t$ in the representation $s^{-1}t$:

```python
sage: g.left_denominator()
d - 1/t
sage: g.right_numerator()
t
```
We favored the writing \( s^{-1}t \) because it always exists. On the contrary, the writing \( st^{-1} \) is only guaranteed when the twisting morphism defining the Ore polynomial ring is bijective. As a consequence, when the latter assumption is not fulfilled (or actually if Sage cannot invert the twisting morphism), computing the left numerator and the right denominator fails:

```
sage: sigma = R.hom([t^2])
sage: S.<x> = R['x', sigma]
sage: f = S.random_element()
sage: f.left_numerator()
Traceback (most recent call last):
  ... 
NotImplementedError: inversion of the twisting morphism
```

On a related note, fractions are systematically simplified when the twisting morphism is bijective but they are not otherwise. As an example, compare the two following computations:

```
sage: P = d^2 + t*d + 1
sage: Q = d + t^2
sage: D = d^3 + t^2 + 1
sage: f = P^(-1) * Q
sage: g = (D*P)^(-1) * (D*Q)
sage: f == g
True
sage: P = x^2 + t*x + 1
sage: Q = x + t^2
sage: D = x^3 + t^2 + 1
sage: f = P^(-1) * Q
sage: g = (D*P)^(-1) * (D*Q)
sage: f == g
True
```

OPERATIONS:

Basic arithmetical operations are available:

```
sage: f = 1 / d
sage: g = 1 / (d + t)
sage: u = f + g; u
(d^2 + ((t^2 - 1)/t)*d)^(-1) * (2*d + (t^2 - 2)/t)
sage: v = f - g; v
(d^2 + ((t^2 - 1)/t)*d)^(-1) * t
sage: u + v
d^(-1) * 2
sage: f * g
(d^2 + t*d)^(-1)
sage: f / g
(continues on next page)
```
Of course, multiplication remains noncommutative:

```
sage: g * f
(d^2 + t*d + 1)^(-1)
sage: g^(-1) * f
(d - 1/t)^(-1) * (d + (t^2 - 1)/t)
```

AUTHOR:

• Xavier Caruso (2020-05)

```python
class sage.rings.polynomial.ore_function_field.OreFunctionCenterInjection(domain, codomain, ringembedding)

Bases: sage.rings.morphism.RingHomomorphism

Canonical injection of the center of a Ore function field into this field.

section()

Return a section of this morphism.

EXAMPLES:
```
sage: k.<a> = GF(5^3)
sage: S.<x> = SkewPolynomialRing(k, k.frobenius_endomorphism())
sage: K = S.fraction_field()
sage: Z = K.center()
sage: iota = K.coerce_map_from(Z)
sage: sigma = iota.section()
sage: sigma(x^3 / (x^6 + 1))
z/(z^2 + 1)
```
```
class sage.rings.polynomial.ore_function_field.OreFunctionField(ring, category=None)

Bases: sage.rings.ring.Algebra, sage.structure.unique_representation.UniqueRepresentation

A class for fraction fields of Ore polynomial rings.

change_var(var)

Return the Ore function field in variable var with the same base ring, twisting morphism and twisting derivation as self.

INPUT:

• var – a string representing the name of the new variable.

EXAMPLES:
```
sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: R.<x> = OrePolynomialRing(k,Frob)
sage: K = R.fraction_field()
sage: K
Ore Field in x over Finite Field in t of size 5^3 twisted by t |---> t^5
```
```

(continued from previous page)

```python
sage: Ky = K.change_var('y'); Ky
Ore Function Field in y over Finite Field in t of size 5^3 twisted by t |--> t^5
sage: Ky is K.change_var('y')
True
```

**characteristic()**

Return the characteristic of this Ore function field.

**EXAMPLES:**

```python
sage: R.<t> = QQ[]
sage: sigma = R.hom([t+1])
sage: S = R['x',sigma]
sage: S.fraction_field().characteristic()
0
sage: k.<u> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S = k['y',Frob]
sage: S.fraction_field().characteristic()
5
```

**fraction_field()**

Return the fraction field of this Ore function field, i.e. this Ore function field itself.

**EXAMPLES:**

```python
sage: R.<t> = QQ[]
sage: der = R.derivation()
sage: A.<d> = R['d', der]
sage: K = A.fraction_field()
sage: K
Ore Function Field in d over Fraction Field of Univariate Polynomial Ring in t over Rational Field twisted by d/dt
sage: K.fraction_field()
Ore Function Field in d over Fraction Field of Univariate Polynomial Ring in t over Rational Field twisted by d/dt
sage: K.fraction_field() is K
True
```

**gen (n=0)**

Return the indeterminate generator of this Ore function field.

**INPUT:**

- `n` – index of generator to return (default: 0). Exists for compatibility with other polynomial rings.

**EXAMPLES:**

```python
sage: k.<a> = GF(5^4)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x', Frob]
sage: K = S.fraction_field()
sage: K.gen()
```

Chapter 2. Fraction field of Ore polynomial rings
gens_dict()
Return a \{name: variable\} dictionary of the generators of this Ore function field.

EXAMPLES:

```
sage: R.<t> = ZZ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = OrePolynomialRing(R, sigma)
sage: K = S.fraction_field()
sage: K.gens_dict()
{'x': x}
```

is_commutative()
Return True if this Ore function field is commutative, i.e. if the twisting morphism is the identity and the twisting derivation vanishes.

EXAMPLES:

```
sage: k.<a> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x', Frob]
sage: K = S.fraction_field()
sage: K.is_commutative()
False
```

is_exact()
Return True if elements of this Ore function field are exact. This happens if and only if elements of the base ring are exact.

EXAMPLES:

```
sage: k.<a> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x', Frob]
sage: K = S.fraction_field()
sage: K.is_exact()
True
```

is_field()
Return always True since Ore function field are (skew) fields.

EXAMPLES:

```
sage: k.<a> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x', Frob]
sage: K = S.fraction_field()
sage: K.is_exact()
False
```

(continues on next page)
sage: K = S.fraction_field()
sage: S.is_field()
False
sage: K.is_field()
True

**is_finite()**
Return False since Ore function field are not finite.

**EXAMPLES:**

```python
sage: k.<t> = GF(5^3)
sage: k.is_finite()
True
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x', Frob]
sage: K = S.fraction_field()
sage: K.is_finite()
False
```

**is_sparse()**
Return True if the elements of this Ore function field are sparsely represented.

**Warning:** Since sparse Ore polynomials are not yet implemented, this function always returns False.

**EXAMPLES:**

```python
sage: R.<t> = RR[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x', sigma]
sage: K = S.fraction_field()
sage: K.is_sparse()
False
```

**ngens()**
Return the number of generators of this Ore function field, which is 1.

**EXAMPLES:**

```python
sage: R.<t> = RR[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x', sigma]
sage: K = S.fraction_field()
sage: K.ngens()
1
```

**parameter**(n=0)
Return the indeterminate generator of this Ore function field.

**INPUT:**
- n – index of generator to return (default: 0). Exists for compatibility with other polynomial rings.

**EXAMPLES:**
sage: k.<a> = GF(5^4)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x', Frob]
sage: K = S.fraction_field()
sage: K.gen()
x

\textbf{random_element} \texttt{(degree=2, monic=False, *args, **kwds)}

Return a random Ore function in this field.

**INPUT:**

- \texttt{degree} – (default: 2) an integer or a list of two integers; the degrees of the denominator and numerator
- \texttt{monic} – (default: False) if True, return a monic Ore function with monic numerator and denominator

- *\texttt{args}, **\texttt{kwds} – passed in to the \texttt{random_element} method for the base ring

**EXAMPLES:**

sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x', Frob]
sage: K = S.fraction_field()
sage: K.random_element()
# random
(x^2 + (2*t^2 + t + 1)*x + 2*t^2 + 2*t + 3)^(-1) * (2*t^2 + 3)*x^2 + (4*t^2 + t + 4)*x + 2*t^2 + 2)
sage: K.random_element(monic=True)
# random
(x^2 + (4*t^2 + 3*t + 4)*x + 4*t^2 + t)^(-1) * (x^2 + (2*t^2 + t + 3)*x + 3*t^2 + t + 2)
sage: K.random_element(degree=3)
# random
(x^3 + (2*t^2 + 3)*x^2 + (2*t^2 + 4)*x + t + 3)^(-1) * (x^2 + (t + 4)*x^3 + (4*t^2 + t + 2)*x^2 + (2*t^2 + 3*t + 3)*x + 3*t^2 + 3*t + 1)
sage: K.random_element(degree=[2,5])
# random
(x^2 + (4*t^2 + 2*t + 2)*x + 4*t^2 + t + 2)^(-1) * ((3*t^2 + t + 1)*x^5 + (2*t^2 + 3*t + 3)*x + 3*t^2 + 2*t + 1)
        (4)*x)

\textbf{twisting_derivation}()

Return the twisting derivation defining this Ore function field or \texttt{None} if this Ore function field is not twisted by a derivation.

**EXAMPLES:**

sage: R.<t> = QQ[]
sage: der = R.derivation(); der
d/dt
sage: A.<d> = R['d', der]
sage: F = A.fraction_field()
sage: F.twisting_derivation()
d/dt
sage: k.<a> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x', Frob]

(continues on next page)
sage: K = S.fraction_field()
sage: K.twisting_derivation()

See also:
sage.rings.polynomial.ore_polynomial_element.OrePolynomial.twisting_derivation(), twisting_morphism()

twisting_morphism(n=1)
Return the twisting endomorphism defining this Ore function field iterated \( n \) times or \( \text{None} \) if this Ore function field is not twisted by an endomorphism.

INPUT:

- \( n \) - an integer (default: 1)

EXAMPLES:

sage: R.<t> = QQ[]
sage: sigma = R.hom([t+1])
sage: S.<x> = R['x', sigma]
sage: K = S.fraction_field()
sage: K.twisting_morphism()
Ring endomorphism of Fraction Field of Univariate Polynomial Ring in t over Rational Field
Defn: t |--> t + 1

When the Ore polynomial ring is only twisted by a derivation, this method returns nothing:

sage: der = R.derivation()
sage: A.<d> = R['x', der]
sage: F = A.fraction_field()
sage: F.twisting_morphism()

See also:
sage.rings.polynomial.ore_polynomial_element.OrePolynomial.twisting_morphism(), twisting_derivation()

class sage.rings.polynomial.ore_function_field.OreFunctionField_with_large_center(ring, category=None)

Bases: sage.rings.polynomial.ore_function_field.OreFunctionField

A specialized class for Ore polynomial fields whose center has finite index.

center (name=\text{None}, names=\text{None}, default=\text{False})
Return the center of this Ore function field.

Note: One can prove that the center is a field of rational functions over a subfield of the base ring of this Ore function field.

INPUT:

- \text{name} – a string or \text{None} (default: \text{None}); the name for the central variable
- \text{default} – a boolean (default: \text{False}); if True, set the default variable name for the center to \text{name}
EXAMPLES:

```sage
sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x',Frob]
sage: K = S.fraction_field()
sage: Z = K.center(); Z
Fraction Field of Univariate Polynomial Ring in z over Finite Field of size 5
```

We can pass in another variable name:

```sage
sage: K.center(name='y')
Fraction Field of Univariate Polynomial Ring in y over Finite Field of size 5
```

or use the bracket notation:

```sage
sage: Zy.<y> = K.center(); Zy
Fraction Field of Univariate Polynomial Ring in y over Finite Field of size 5
```

A coercion map from the center to the Ore function field is set:

```sage
sage: K.has_coerce_map_from(Zy)
True
```

and pushout works:

```sage
sage: x.parent()
Ore Polynomial Ring in x over Finite Field in t of size 5^3 twisted by t |---> t^5
sage: y.parent()
Fraction Field of Univariate Polynomial Ring in y over Finite Field of size 5
sage: P = x + y; P
x^3 + x
sage: P.parent()
Ore Function Field in x over Finite Field in t of size 5^3 twisted by t |---> t^5
```

A conversion map in the reverse direction is also set:

```sage
sage: Zy(x^(-6) + 2)
(2*y^2 + 1)/y^2
sage: Zy(1/x^2)
Traceback (most recent call last):
...
ValueError: x^(-2) is not in the center
```

ABOUT THE DEFAULT NAME OF THE CENTRAL VARIABLE:

A priori, the default is \( z \).

However, a variable name is given the first time this method is called, the given name become the default for the next calls:

```sage
sage: k.<t> = GF(11^3)
sage: phi = k.frobenius_endomorphism()
sage: S.<X> = k['X', phi]
```
sage: K = S.fraction_field()
sage: C.<u> = K.center()  # first call
sage: C
Fraction Field of Univariate Polynomial Ring in u over Finite Field of size 11
sage: K.center()  # second call: the variable name is still u
Fraction Field of Univariate Polynomial Ring in u over Finite Field of size 11

We can update the default variable name by passing in the argument `default=True`:

sage: D.<v> = K.center(default=True)
sage: D
Fraction Field of Univariate Polynomial Ring in v over Finite Field of size 11
sage: K.center()
Fraction Field of Univariate Polynomial Ring in v over Finite Field of size 11

```
class sage.rings.polynomial.ore_function_field.SectionOreFunctionCenterInjection(embed)
    Bases: sage.categories.map.Section

    Section of the canonical injection of the center of a Ore function field into this field
```

### 2.2 An element in the fraction field of a Ore polynomial ring.

**AUTHOR:**

- Xavier Caruso (2020-05)

```
class sage.rings.polynomial.ore_function_element.ConstantOreFunctionSection
    Bases: sage.categories.map.Map

    Representation of the canonical homomorphism from the constants of a Ore function field to the base field.

    This class is needed by the coercion system.

    EXAMPLES:

    sage: from sage.rings.polynomial.ore_polynomial_element import _constantOrePolynomialSection
    sage: k.<a> = GF(5^3)
    sage: Frob = k.frobenius_endomorphism()
    sage: S.<x> = k['x', Frob]
    sage: K = S.fraction_field()
    sage: iota = K.coerce_map_from(k)
    sage: sigma = iota.section()
    sage: sigma
    Generic map:
    From: Ore Function Field in x over Finite Field in a of size 5^3 twisted by a |-> a^5
    To:   Finite Field in a of size 5^3
```

```
class sage.rings.polynomial.ore_function_element.OreFunction(parent, numerator, denominator=One, simplify=True)
    Bases: sage.structure.element.AlgebraElement
```

---

Chapter 2. Fraction field of Ore polynomial rings
An element in a Ore function field.

**hilbert_shift** \((s, \text{var=none})\)

Return this Ore function with variable shifted by \(s\), i.e. if this Ore function is \(f(x)\), return \(f(x + s)\).

**INPUT:**

- \(s\) – an element in the base ring
- \(\text{var}\) – a string; the variable name

**EXAMPLES:**

```sage
R.<t> = GF(7)[]
sage: f = 1 / (t-t)
sage: f.hilbert_shift(t)
```

```console
d^(-1)
```

One can specify another variable name:

```sage
f.hilbert_shift(t, var='x')
x^(-1)
```

When the twisting morphism is not trivial, the output lies in a different Ore polynomial ring:

```sage
k.<a> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x', Frob]
sage: f = (x-a)^(-2)
sage: g = f.hilbert_shift(a)
sage: g.parent()
```

```console
Ore Function Field in x over Finite Field in a of size 5^3 twisted by a |--> a^5 and a*([a |--> a^5] - id)
```

This behavior ensures that the Hilbert shift by a fixed element defines an homomorphism of fields:

```sage
U = K.random_element(degree=5)
sage: V = K.random_element(degree=5)
sage: s = k.random_element()
sage: (U+V).hilbert_shift(s) == U.hilbert_shift(s) + V.hilbert_shift(s)
```

```console
True
```

```sage
(U+V).hilbert_shift(s) == U.hilbert_shift(s) + V.hilbert_shift(s)
```

```console
True
```

**is_zero**()

Return `True` if this element is equal to zero.

**EXAMPLES:**

2.2. An element in the fraction field of a Ore polynomial ring.
```python
sage: R.<t> = GF(3)[]
sage: der = R.derivation()
sage: A.<d> = R['x', der]
sage: f = t/d
sage: f.is_zero()
False
sage: (f-f).is_zero()
True
```

**left_denominator()**

Return $s$ if this element reads $s^{-1}t$.

**WARNING:**

When the twisting morphism is bijective, there is a unique irreducible fraction of the form $s^{-1}t$ representing this element. Here irreducible means that $s$ and $t$ have no nontrivial common left divisor. Under this additional assumption, this method always returns this distinguished denominator $s$.

On the contrary, when the twisting morphism is not bijective, this method returns the denominator of some fraction representing the input element. However, the software guarantees that the method `right_numerator()` outputs the numerator of the same fraction.

**EXAMPLES:**

```python
sage: k.<a> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x', Frob]
sage: s = x + a
sage: t = x^2 + a*x + a^2
sage: f = s^(-1) * t
sage: f.left_denominator()
x + a
```  

In the example below, a simplification occurs:

```python
sage: u = S.random_element()
sage: g = (u*s)^(-1) * (u*t)
sage: g.left_denominator()
x + a
```  

When the twisting morphism is not invertible, simplifications do not occur in general:

```python
sage: R.<z> = GF(11)[]
sage: sigma = R.hom([z^2])
sage: S.<x> = R['x', sigma]
sage: s = (x + z)^2
sage: t = (x + z) * (x^2 + z^2)
sage: f = s^(-1) * t
sage: f.left_denominator()
x^2 + (z^2 + z)*x + z^2
```  

However, the following always holds true:

```python
sage: f == f.left_denominator()^(-1) * f.right_numerator()
True
```

**See also:**
left_numerator()

Return $t$ if this element reads $ts^{-1}$.

WARNING:

When the twisting morphism is bijective, there is a unique irreducible fraction of the form $ts^{-1}$ representing this element. Here irreducible means that $s$ and $t$ have no nontrivial common right divisor. Under this additional assumption, this method always returns this distinguished numerator $t$.

On the contrary, when the twisting morphism is not bijective, the existence of the writing $ts^{-1}$ is not guaranteed in general. In this case, this method raises an error.

EXAMPLES:

```
sage: k.<a> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x', Frob]
sage: s = x + a
sage: t = x^2 + a*x + a^2
sage: f = t/s
sage: f.left_numerator()
x^2 + a*x + a^2
```

In the example below, a simplification occurs:

```
sage: u = S.random_element()
sage: g = (t*u) / (s*u)
sage: g.left_numerator()
x^2 + a*x + a^2
```

right_denominator()

Return $s$ if this element reads $ts^{-1}$.

WARNING:

When the twisting morphism is bijective, there is a unique irreducible fraction of the form $ts^{-1}$ representing this element. Here irreducible means that $s$ and $t$ have no nontrivial common right divisor. Under this additional assumption, this method always returns this distinguished denominator $s$.

On the contrary, when the twisting morphism is not bijective, the existence of the writing $ts^{-1}$ is not guaranteed in general. In this case, this method raises an error.

EXAMPLES:

```
sage: k.<a> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x', Frob]
sage: s = x + a
sage: t = x^2 + a*x + a^2
sage: f = t/s
sage: f.right_denominator()
x + a
```

In the example below, a simplification occurs:
sage: u = S.random_element()
sage: g = (t*u) / (s*u)
sage: g.right_denominator()
x + a

See also:
left_numerator(), left_denominator(), right_numerator()

right_numerator()
Return $t$ if this element reads $s^{-1}t$.

WARNING:
When the twisting morphism is bijective, there is a unique irreducible fraction of the form $s^{-1}t$ representing this element. Here irreducible means that $s$ and $t$ have no nontrivial common left divisor. Under this additional assumption, this method always returns this distinguished numerator $t$.

On the contrary, when the twisting morphism is not bijective, this method returns the numerator of some fraction representing the input element. However, the software guarantees that the method left_denominator() outputs the numerator of the same fraction.

EXAMPLES:

\begin{verbatim}
sage: k.<a> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x', Frob]
sage: s = x + a
ts = x^2 + a*x + a^2
sage: f = s^(-1) * t
sage: f.right_numerator()
x^2 + a*x + a^2
\end{verbatim}

In the example below, a simplification occurs:

\begin{verbatim}
sage: u = S.random_element()
sage: g = (u*s)^(-1) * (u*t)
sage: g.right_numerator()
x^2 + a*x + a^2
\end{verbatim}

See also:
left_denominator(), left_numerator(), right_denominator()

class sage.rings.polynomial.ore_function_element.OreFunctionBaseringInjection
Bases: sage.categories.morphism.Morphism

Representation of the canonical homomorphism from a field $k$ into a Ore function field over $k$.
This class is needed by the coercion system.

an_element()
Return an element of the codomain of the ring homomorphism.

EXAMPLES:

\begin{verbatim}
sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x', Frob]
\end{verbatim}
sage: K = S.fraction_field()
sage: m = K.coerce_map_from(k)
sage: m.an_element()
x

section()  
Return the canonical homomorphism from the constants of a Ore function filed to its base field.

class sage.rings.polynomial.ore_function_element.OreFunction_with_large_center (parent,  
numerator,  
denominator=None,  
simplify=True)

Bases: sage.rings.polynomial.ore_function_element.OreFunction

A special class for elements of Ore function fields whose center has finite index.

reduced_norm (var=None)
Return the reduced norm of this Ore function.

INPUT:

• var – a string or None (default: None); the name of the central variable

EXAMPLES:

sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x', Frob]
sage: K = S.fraction_field()
sage: a = (x + t) / (x^2 + t^2)
sage: N = a.reduced_norm(); N
(z + 2)/(z^2 + 4)

The reduced norm lies in the center of S, which is the fraction field of a univariate polynomial ring in the variable z = x^3 over GF(5).

sage: N.parent() Fraction Field of Univariate Polynomial Ring in z over Finite Field of size 5
sage: N.parent() is K.center()
True

We can use explicit conversion to view N as a skew polynomial:

sage: K(N)
(x^6 + 4)^(-1) * (x^3 + 2)

By default, the name of the central variable is usually z (see sage.rings.polynomial.skew_polynomial_ring.SkewPolynomialRing_finite_order.center() for more details about this). However, the user can specify a different variable name if desired:

2.2. An element in the fraction field of a Ore polynomial ring.
reduced_trace (var=None)
Return the reduced trace of this element.

INPUT:

• var – a string or None (default: None); the name of the central variable

EXAMPLES:

sage: k.<t> = GF(5^3)
sage: Frob = k.frobenius_endomorphism()
sage: S.<x> = k['x', Frob]
sage: K = S.fraction_field()
sage: a = 1 / (x^2 + t)
sage: tr = a.reduced_trace(); tr
3/(z^2 + 2)

The reduced trace lies in the center of $S$, which is the fraction field of a univariate polynomial ring in the variable $z = x^3$ over $GF(5)$.

sage: tr.parent() Fraction Field of Univariate Polynomial Ring in z over Finite Field of size 5
sage: tr.parent() is K.center() True

We can use explicit conversion to view $tr$ as a Ore function:

sage: K(tr)
(x^6 + 2)^(-1) * 3

By default, the name of the central variable is usually $z$ (see sage.rings.polynomial.skew_polynomial_ring.OreFunctionField_with_large_center.center() for more details about this). However, the user can specify a different variable name if desired:

sage: a.reduced_trace(var='u')
3/(u^2 + 2)
3.1 Noncommutative Polynomials via libSINGULAR/Plural

This module provides specialized and optimized implementations for noncommutative multivariate polynomials over many coefficient rings, via the shared library interface to SINGULAR. In particular, the following coefficient rings are supported by this implementation:

- the rational numbers $\mathbb{Q}$, and
- finite fields $\mathbb{F}_p$ for $p$ prime

**AUTHORS:**

The PLURAL wrapper is due to:

- Burcin Erocal (2008-11 and 2010-07): initial implementation and concept
- Michael Brickenstein (2008-11 and 2010-07): initial implementation and concept
- Oleksandr Motsak (2010-07): complete overall noncommutative functionality and first release
- Alexander Dreyer (2010-07): noncommutative ring functionality and documentation
- Simon King (2011-09): left and two-sided ideals; normal forms; pickling; documentation

The underlying libSINGULAR interface was implemented by:

- Martin Albrecht (2007-01): initial implementation
- Joel Mohler (2008-01): misc improvements, polishing
- Martin Albrecht (2008-08): added $\mathbb{Q}(a)$ and $\mathbb{Z}$ support
- Simon King (2009-04): improved coercion
- Martin Albrecht (2009-05): added $\mathbb{Z}/n\mathbb{Z}$ support, refactoring
- Martin Albrecht (2009-06): refactored the code to allow better re-use

**Todo:** extend functionality towards those of libSINGULARs commutative part

**EXAMPLES:**

We show how to construct various noncommutative polynomial rings:

```
sage: A.<x,y,z> = FreeAlgebra(QQ, 3)
sage: P.<x,y,z> = A.g_algebra(relations=(y*x:-x*y), order = 'lex')
```

(continues on next page)
sage: P
Noncommutative Multivariate Polynomial Ring in x, y, z over Rational Field, nc-
relations: {y*x: -x*y}

sage: y*x + 1/2
-x*y + 1/2

sage: A.<x,y,z> = FreeAlgebra(GF(17), 3)
sage: P.<x,y,z> = A.g_algebra(relations={y*x:-x*y}, order = 'lex')
sage: P
Noncommutative Multivariate Polynomial Ring in x, y, z over Finite Field of size 17,
nc-relations: {y*x: -x*y}

sage: y*x + 7
-x*y + 7

Raw use of this class; this is not the intended use!

sage: from sage.matrix.constructor import Matrix
sage: c = Matrix(3)
sage: c[0,1] = -2
sage: c[0,2] = 1
sage: c[1,2] = 1
sage: d = Matrix(3)
sage: d[0, 1] = 17
sage: P = QQ['x','y','z']
sage: c = c.change_ring(P)
sage: d = d.change_ring(P)

sage: from sage.rings.polynomial.plural import NCPolynomialRing_plural
sage: R.<x,y,z> = NCPolynomialRing_plural(QQ, c = c, d = d, order=TermOrder('lex',3),
category=Algebras(QQ))
sage: R
Noncommutative Multivariate Polynomial Ring in x, y, z over Rational Field, nc-
relations: {y*x: -2*x*y + 17}

sage: R.term_order()
Lexicographic term order

sage: a,b,c = R.gens()
sage: f = 57 * a^2*b + 43 * c + 1; f
57*x^2*y + 43*z + 1

sage.rings.polynomial.plural.ExteriorAlgebra(base_ring, names, order='degrevlex')

Return the exterior algebra on some generators

This is also known as a Grassmann algebra. This is a finite dimensional algebra, where all generators anti-
commute.

See Wikipedia article Exterior algebra

INPUT:

• base_ring – the ground ring

• names – a list of variable names

EXAMPLES:
sage: from sage.rings.polynomial.plural import ExteriorAlgebra
sage: E = ExteriorAlgebra(QQ, ['x', 'y', 'z']); E
Quotient of Noncommutative Multivariate Polynomial Ring in x, y, z over Rational Field, nc-relations: (z*x: -x*z, z*y: -y*z, y*x: -x*y) by the ideal (z^2, y^2, x^2)

sage: sorted(E.cover().domain().relations().items(), key=str)
[(y*x, -x*y), (z*x, -x*z), (z*y, -y*z)]

sage: sorted(E.cover().kernel().gens(), key=str)
[x^2, y^2, z^2]

sage: E.inject_variables()
Defining xbar, ybar, zbar
sage: x,y,z = (xbar,ybar,zbar)
sage: y*x
-x*y

sage: all(v^2==0 for v in E.gens())
True

sage: E.one()
1

class sage.rings.polynomial.plural.ExteriorAlgebra_plural
Bases: sage.rings.polynomial.plural.NCPolynomialRing_plural

class sage.rings.polynomial.plural.G_AlgFactory
Bases: sage.structure.factory.UniqueFactory

A factory for the creation of g-algebras as unique parents.

create_key_and_extra_args(base_ring, c, d, names=None, order=None, category=None, check=None)

Create a unique key for g-algebras.

INPUT:

- base_ring - a ring
- c, d - two matrices
- names - a tuple or list of names
- order - (optional) term order
- category - (optional) category
- check - optional bool

create_object(version, key, **extra_args)

Create a g-algebra to a given unique key.

INPUT:

- key - a 6-tuple, formed by a base ring, a tuple of names, two matrices over a polynomial ring over the base ring with the given variable names, a term order, and a category
- extra_args - a dictionary, whose only relevant key is ‘check’.

class sage.rings.polynomial.plural.NCPolynomialRing_plural
Bases: sage.rings.ring.Ring

A non-commutative polynomial ring.

EXAMPLES:
```
sage: A.<x,y,z> = FreeAlgebra(QQ, 3)
sage: H = A.g_algebra({y*x:x*y-z, z*x:x*z+2*x, z*y:y*z-2*y})
sage: H._is_category_initialized()
True
sage: H.category()
Category of algebras over Rational Field
sage: TestSuite(H).run()
```

Note that two variables commute if they are not part of the given relations:

```
sage: H.<x,y,z> = A.g_algebra({z*x:x*z+2*x, z*y:y*z-2*y})
sage: x*y == y*x
True
```

### free_algebra()

The free algebra of which this is the quotient.

**EXAMPLES:**

```
sage: A.<x,y,z> = FreeAlgebra(QQ, 3)
sage: P = A.g_algebra(relations={y*x:-x*y}, order = 'lex')
sage: B = P.free_algebra()
sage: A == B
True
```

### gen (n=0)

Returns the n-th generator of this noncommutative polynomial ring.

**INPUT:**

- n – an integer >= 0

**EXAMPLES:**

```
sage: A.<x,y,z> = FreeAlgebra(QQ, 3)
sage: P = A.g_algebra(relations={y*x:-x*y}, order = 'lex')
sage: P.gen(),P.gen(1)
(x, y)
```

Note that the generators are not cached:

```
sage: P.gen(1) is P.gen(1)
False
```

### ideal (*gens, **kwds)

Create an ideal in this polynomial ring.

**INPUT:**

- *gens - list or tuple of generators (or several input arguments)
- coerce - bool (default: True); this must be a keyword argument. Only set it to False if you are certain that each generator is already in the ring.
- side - string (either “left”, which is the default, or “twosided”) Must be a keyword argument. Defines whether the ideal is a left ideal or a two-sided ideal. Right ideals are not implemented.

**EXAMPLES:**
is_commutative()
Return False.

Todo: Provide a mathematically correct answer.

EXAMPLES:

```
sage: A.<x,y,z> = FreeAlgebra(QQ, 3)
sage: P = A.g_algebra(relations={y*x:-x*y}, order = 'lex')
sage: P.is_commutative()  # This should return False.
False
```

is_field(*args, **kwargs)
Return False.

EXAMPLES:

```
sage: A.<x,y,z> = FreeAlgebra(QQ, 3)
sage: P = A.g_algebra(relations={y*x:-x*y}, order = 'lex')
sage: P.is_field()  # This should return False.
False
```

monomial_all_divisors(t)
Return a list of all monomials that divide t.
Coefficients are ignored.

INPUT:
• t - a monomial

OUTPUT:
a list of monomials

EXAMPLES:

```
sage: A.<x,y,z> = FreeAlgebra(QQ, 3)
sage: P = A.g_algebra(relations={y*x:-x*y}, order = 'lex')
sage: P.inject_variables()  # Defining x, y, z
Defining x, y, z
sage: P.monomial_all_divisors(x^2*z^3)
[x, x^2, z, x*z, x^2*z, z^2, x*z^2, x^2*z^2, z^3, x*z^3, x^2*z^3]
```

ALGORITHM: addwithcarry idea by Toon Segers
**monomial_divides** \((a, b)\)

Return `False` if \(a\) does not divide \(b\) and `True` otherwise.

Coefficients are ignored.

**INPUT:**

- \(a\) – monomial
- \(b\) – monomial

**EXAMPLES:**

```
sage: A.<x,y,z> = FreeAlgebra(QQ, 3)
sage: P = A.g_algebra(relations={y*x:-x*y}, order='lex')
sage: P.inject_variables()
Defining x, y, z

sage: P.monomial_divides(x*y*z, x^3*y^2*z^4)
True

sage: P.monomial_divides(x^3*y^2*z^4, x*y*z)
False
```

**monomial_lcm** \((f, g)\)

LCM for monomials. Coefficients are ignored.

**INPUT:**

- \(f\) – monomial
- \(g\) – monomial

**EXAMPLES:**

```
sage: A.<x,y,z> = FreeAlgebra(QQ, 3)
sage: P = A.g_algebra(relations={y*x:-x*y}, order='lex')
sage: P.inject_variables()
Defining x, y, z

sage: P.monomial_lcm(3/2*x*y,x)
x*y
```

**monomial_pairwise_prime** \((g, h)\)

Return `True` if \(h\) and \(g\) are pairwise prime.

Both \(h\) and \(g\) are treated as monomials.

Coefficients are ignored.

**INPUT:**

- \(h\) – monomial
- \(g\) – monomial

**EXAMPLES:**

```
sage: A.<x,y,z> = FreeAlgebra(QQ, 3)
sage: P = A.g_algebra(relations={y*x:-x*y}, order='lex')
sage: P.inject_variables()
Defining x, y, z

sage: P.monomial_pairwise_prime(x^2*z^3, y^4)
(continues on next page)```
monomial_pairwise_prime (f, g)  
Return True if f and g are pairwise prime, False otherwise.

```
sage: P.monomial_pairwise_prime(1/2*x^3*y^2, 3/4*y^3)
False
```

monomial_quotient (f, g, coeff=False)  
Return \( f/g \), where both \( f \) and \( g \) are treated as monomials.  
Coefficients are ignored by default.

**INPUT:**  
- \( f \) - monomial  
- \( g \) - monomial  
- coeff - divide coefficients as well (default: False)

**EXAMPLES:**
```
sage: A.<x,y,z> = FreeAlgebra(QQ, 3)
sage: P = A.g_algebra(relations={y*x:-x*y}, order='lex')
sage: P.inject_variables()
Defining x, y, z
sage: P.monomial_quotient(3/2*x*y,x,coeff=True)
3/2*y
```

Note that \( Z \) behaves differently if coeff=True:
```
sage: P.monomial_quotient(2*x,3*x)
1
sage: P.monomial_quotient(2*x,3*x,coeff=True)
2/3
```

**Warning:** Assumes that the head term of \( f \) is a multiple of the head term of \( g \) and return the multiplicant \( m \). If this rule is violated, funny things may happen.

monomial_reduce (f, G)  
Try to find a \( g \) in \( G \) where \( g.lm() \) divides \( f \). If found \((flt,g)\) is returned, \((0,0)\) otherwise, where \( flt = f/g.lm() \).

It is assumed that \( G \) is iterable and contains only elements in this polynomial ring.  
Coefficients are ignored.

**INPUT:**  
- \( f \) - monomial  
- \( G \) - list/set of mpolynomials

**EXAMPLES:**
```
sage: A.<x,y,z> = FreeAlgebra(QQ, 3)
sage: P = A.g_algebra(relations={y*x:-x*y}, order='lex')
sage: P.inject_variables()
Defining x, y, z
```

(continues on next page)
\begin{verbatim}
sage: f = x*y^2
sage: G = [ 3/2*x^3 + y^2 + 1/2, 1/4*x*y + 2/7, 1/2 ]
sage: P.monomial_reduce(f,G)
(y, 1/4*x*y + 2/7)
\end{verbatim}

\section*{ngens()}
Returns the number of variables in this noncommutative polynomial ring.

\begin{verbatim}
sage: A.<x,y,z> = FreeAlgebra(QQ, 3)
sage: P.<x,y,z> = A.g_algebra(relations={y*x:-x*y}, order = 'lex')
sage: P.ngens()
3
\end{verbatim}

\section*{relations (add_commutative=False)}
Return the relations of this g-algebra.

\begin{verbatim}
INPUT:
add_commutative (optional bool, default False)

OUTPUT:
The defining relations. There are some implicit relations: Two generators commute if they are not part of any given relation. The implicit relations are not provided, unless add_commutative==True.

\begin{verbatim}
sage: A.<x,y,z> = FreeAlgebra(QQ, 3)
sage: H.<x,y,z> = A.g_algebra({z*x:x*z+2*x, z*y:y*z-2*y})
sage: x*y == y*x
True
sage: H.relations()
{z*x: x*z + 2*x, z*y: y*z - 2*y}
sage: H.relations(add_commutative=True)
{y*x: x*y, z*x: x*z + 2*x, z*y: y*z - 2*y}
\end{verbatim}
\end{verbatim}

\section*{term_order()}
Return the term ordering of the noncommutative ring.

\begin{verbatim}
EXAMPLES:

\begin{verbatim}
sage: A.<x,y,z> = FreeAlgebra(QQ, 3)
sage: P = A.g_algebra(relations={y*x:-x*y}, order = 'lex')
sage: P.term_order()
Lexicographic term order
sage: P = A.g_algebra(relations={y*x:-x*y})
sage: P.term_order()
Degree reverse lexicographic term order
\end{verbatim}
\end{verbatim}
\end{verbatim}

\section*{class sage.rings.polynomial.plural.NCPolynomial_plural}
\begin{verbatim}
Bases: sage.structure.element.RingElement

A noncommutative multivariate polynomial implemented using libSINGULAR.

\section*{coefficient (degrees)}
Return the coefficient of the variables with the degrees specified in the python dictionary degrees.
\end{verbatim}
Mathematically, this is the coefficient in the base ring adjoined by the variables of this ring not listed in degrees. However, the result has the same parent as this polynomial.

This function contrasts with the function `monomial_coefficient()` which returns the coefficient in the base ring of a monomial.

**INPUT:**

- **degrees** - Can be any of:
  - a dictionary of degree restrictions
  - a list of degree restrictions (with None in the unrestricted variables)
  - a monomial (very fast, but not as flexible)

**OUTPUT:**

element of the parent of this element.

**Note:** For coefficients of specific monomials, look at `monomial_coefficient()`.

**EXAMPLES:**

```sage
sage: A.<x,z,y> = FreeAlgebra(QQ, 3)
sage: R = A.g_algebra(relations={y*x:-x*y + z}, order='lex')
sage: R.inject_variables()
Defining x, z, y
sage: f=x*y+y+5
sage: f.coefficient({x:0,y:1})
1
sage: f.coefficient({x:0})
y + 5
sage: f=(1+y+y^2)*(1+x+x^2)
\[
\begin{align*}
  &z + y^2 + y + 1 \\
  &y^2 - y + 1
\end{align*}
\]
```

Be aware that this may not be what you think! The physical appearance of the variable x is deceiving – particularly if the exponent would be a variable.

```sage
sage: f.coefficient(x^0) # outputs the full polynomial
\[
\begin{align*}
  &x^2*y^2 + x^2*y + x^2 + x*y^2 - x*y + x + z + y^2 + y + 1
\end{align*}
\]
```

```sage
sage: A.<x,z,y> = FreeAlgebra(GF(389), 3)
sage: R = A.g_algebra(relations={y*x:-x*y + z}, order='lex')
sage: R.inject_variables()
Defining x, z, y
sage: f=x*y+5
sage: c=f.coefficient({x:0,y:0}); c
5
sage: parent(c)
```

Noncommutative Multivariate Polynomial Ring in x, z, y over Finite Field of size 389, nc-relations: (y*x: -x*y + z)

3.1. Noncommutative Polynomials via libSINGULAR/Plural
AUTHOR:

- Joel B. Mohler (2007-10-31)

**constant_coefficient()**

Return the constant coefficient of this multivariate polynomial.

**EXAMPLES:**

```python
sage: A.<x,z,y> = FreeAlgebra(GF(389), 3)
sage: P = A.g_algebra(relations={y*x:-x*y + z}, order='lex')
sage: P.inject_variables()
Defining x, z, y
sage: f = 3*x^2 - 2*y + 7*x^2*y^2 + 5
sage: f.constant_coefficient()
5
sage: f = 3*x^2
sage: f.constant_coefficient()
0
```

**degree**(x=None)

Return the maximal degree of this polynomial in \( x \), where \( x \) must be one of the generators for the parent of this polynomial.

**INPUT:**

- \( x \) - multivariate polynomial (a generator of the parent of self) If \( x \) is not specified (or is None), return the total degree, which is the maximum degree of any monomial.

**OUTPUT:**

integer

**EXAMPLES:**

```python
sage: A.<x,z,y> = FreeAlgebra(QQ, 3)
sage: R = A.g_algebra(relations={y*x:-x*y + z}, order='lex')
sage: R.inject_variables()
Defining x, z, y
sage: f = y^2 - x^9 - x
sage: f.degree(x)
9
sage: f.degree(y)
2
sage: (y^10*x - 7*x^2*y^5 + 5*x^3).degree(x)
3
sage: (y^10*x - 7*x^2*y^5 + 5*x^3).degree(y)
10
```

**degrees()**

Returns a tuple with the maximal degree of each variable in this polynomial. The list of degrees is ordered by the order of the generators.

**EXAMPLES:**

```python
sage: A.<y0,y1,y2> = FreeAlgebra(QQ, 3)
sage: R = A.g_algebra(relations={y1*y0:-y0*y1 + y2}, order='lex')
sage: R.inject_variables()
Defining y0, y1, y2
sage: q = 3*y0*y1*y2; q
3*y0*y1^2*y2
```

(continues on next page)
dict()  
Return a dictionary representing self. This dictionary is in the same format as the generic MPolynomial:  
The dictionary consists of ETuple:coefficient pairs.  

EXAMPLES:

```python  
sage: A.<x,z,y> = FreeAlgebra(GF(389), 3)  
sage: R = A.g_algebra(relations={y*x:-x*y + z}, order='lex')  
sage: R.inject_variables()  
Defining x, z, y  
sage: f = (2*x+y)^3 + (7)*x^2 + (3)  
sage: f.dict()  
{(0, 0, 0): 3, (1, 2, 3): 2, (2, 0, 0): 7}  
```

exponents (as_ETuples=True)  
Return the exponents of the monomials appearing in this polynomial.  

INPUT:  
• as_ETuples - (default: True) if True returns the result as an list of ETuples otherwise returns a list of tuples  

EXAMPLES:

```python  
sage: A.<x,z,y> = FreeAlgebra(GF(389), 3)  
sage: R = A.g_algebra(relations={y*x:-x*y + z}, order='lex')  
sage: R.inject_variables()  
Defining x, z, y  
sage: f = x^3 + y + 2*z^2  
sage: f.exponents()  
[(3, 0, 0), (0, 2, 0), (0, 0, 1)]  
sage: f.exponents(as_ETuples=False)  
[(3, 0, 0), (0, 2, 0), (0, 0, 1)]  
```

is_constant ()  
Return True if this polynomial is constant.  

EXAMPLES:

```python  
sage: A.<x,z,y> = FreeAlgebra(GF(389), 3)  
sage: P = A.g_algebra(relations={y*x:-x*y + z}, order='lex')  
sage: P.inject_variables()  
Defining x, z, y  
sage: x.is_constant()  
False  
sage: P(1).is_constant()  
True  
```

is_homogeneous ()  
Return True if this polynomial is homogeneous.  

EXAMPLES:
sage: A.<x,z,y> = FreeAlgebra(GF(389), 3)
sage: P = A.g_algebra(relations={y*x:-x*y + z}, order='lex')
sage: P.inject_variables()
Defining x, z, y
sage: (x+y+z).is_homogeneous()
True
sage: (x.parent()(0)).is_homogeneous()
True
sage: (x+y^2+z^3).is_homogeneous()
False
sage: (x^2 + y^2).is_homogeneous()
True
sage: (x^2 + y^2*x).is_homogeneous()
False
sage: (x^2*y + y^2*x).is_homogeneous()
True

is_monomial()

Return True if this polynomial is a monomial.

A monomial is defined to be a product of generators with coefficient 1.

EXAMPLES:

sage: A.<x,z,y> = FreeAlgebra(GF(389), 3)
sage: P = A.g_algebra(relations={y*x:-x*y + z}, order='lex')
sage: P.inject_variables()
Defining x, z, y
sage: x.is_monomial()
True
sage: (2*x).is_monomial()
False
sage: (x*y).is_monomial()
True
sage: (x*y + x).is_monomial()
False

is_zero()

Return True if this polynomial is zero.

EXAMPLES:

sage: A.<x,z,y> = FreeAlgebra(QQ, 3)
sage: R = A.g_algebra(relations={y*x:-x*y + z}, order='lex')
sage: R.inject_variables()
Defining x, z, y
sage: x.is_zero()
False
sage: (x-x).is_zero()
True

lc()

Leading coefficient of this polynomial with respect to the term order of self.parent().

EXAMPLES:
sage: A.<x,y,z> = FreeAlgebra(GF(7), 3)
sage: R = A.g_algebra(relations={y*x:-x*y + z}, order='lex')
sage: R.inject_variables()
Defining x, y, z
sage: f = 3*x^1*y^2 + 2*y^3*z^4
sage: f.lc()
3
sage: f = 5*x^3*y^2*z^4 + 4*x^3*y^2*z^1
sage: f.lc()
5

lm()
Returns the lead monomial of self with respect to the term order of self.parent().

In Sage a monomial is a product of variables in some power without a coefficient.

EXAMPLES:

```
sage: A.<x,y,z> = FreeAlgebra(GF(7), 3)
sage: R = A.g_algebra(relations={y*x:-x*y + z}, order='lex')
sage: R.inject_variables()
Defining x, y, z
sage: f = x^1*y^2 + y^3*z^4
sage: f.lm()
x*y^2
sage: f = x^3*y^2*z^4 + x^3*y^2*z^1
sage: f.lm()
x^3*y^2*z^4
sage: A.<x,y,z> = FreeAlgebra(QQ, 3)
sage: R = A.g_algebra(relations={y*x:-x*y + z}, order='deglex')
sage: R.inject_variables()
Defining x, y, z
sage: f = x^1*y^2*z^3 + x^3*y^2*z^0
sage: f.lm()
x*y^2*z^3
sage: f = x^1*y^2*z^4 + x^1*y^1*z^5
sage: f.lm()
x*y^2*z^4
sage: A.<x,y,z> = FreeAlgebra(GF(127), 3)
sage: R = A.g_algebra(relations={y*x:-x*y + z}, order='degrevlex')
sage: R.inject_variables()
Defining x, y, z
sage: f = x^1*y^5*z^2 + x^4*y^1*z^3
sage: f.lm()
x*y^5*z^2
sage: f = x^4*y^7*z^1 + x^4*y^2*z^3
sage: f.lm()
x^4*y^7*z
```

lt()
Leading term of this polynomial.

In Sage a term is a product of variables in some power and a coefficient.

EXAMPLES:
sage: A.<x,y,z> = FreeAlgebra(GF(7), 3)
sage: R = A.g_algebra(relations={y*x:-x*y + z}, order='lex')
sage: R.inject_variables()
Defining x, y, z
sage: f = 3*x^1*y^2 + 2*y^3*z^4
sage: f.lt()
3*x*y^2
sage: f = 5*x^3*y^2*z^4 + 4*x^3*y^2*z^1
sage: f.lt()
-2*x^3*y^2*z^4

monomial_coefficient (mon)
Return the coefficient in the base ring of the monomial mon in self, where mon must have the same parent as self.

This function contrasts with the function coefficient () which returns the coefficient of a monomial viewing this polynomial in a polynomial ring over a base ring having fewer variables.

INPUT:

• mon - a monomial

OUTPUT:

coefficient in base ring

See also:

For coefficients in a base ring of fewer variables, look at coefficient ()

EXAMPLES:

sage: A.<x,z,y> = FreeAlgebra(GF(389), 3)
sage: P = A.g_algebra(relations={y*x:-x*y + z}, order='lex')
sage: P.inject_variables()
Defining x, z, y
The parent of the return is a member of the base ring.
sage: f = 2 * x * y
sage: c = f.monomial_coefficient(x*y); c
2
sage: c.parent()
Finite Field of size 389
sage: f = y^2 + y^2*x - x^9 - 7*x + 5*x*y
sage: f.monomial_coefficient(y^2)
1
sage: f.monomial_coefficient(x*y)
5
sage: f.monomial_coefficient(x^9)
388
sage: f.monomial_coefficient(x^10)
0

monomials ()
Return the list of monomials in self

The returned list is decreasingly ordered by the term ordering of self.parent ().

88 Chapter 3. Noncommutative Multivariate Polynomials
EXAMPLES:

```python
sage: A.<x,z,y> = FreeAlgebra(GF(389), 3)
sage: P = A.g_algebra(relations={y*x:-x*y + z}, order='lex')
sage: P.inject_variables()
Defining x, z, y
sage: f = x + (3*2)*y*z^2 + (2+3)
sage: f.monomials()
[x, z^2*y, 1]
sage: f = P(3^2)
sage: f.monomials()
[1]
```

reduce(I)

EXAMPLES:

```python
sage: A.<x,y,z> = FreeAlgebra(QQ, 3)
sage: H.<x,y,z> = A.g_algebra({y*x:x*y-z, z*x:x*z+2*x, z*y:y*z-2*y})
sage: I = H.ideal([y^2, x^2, z^2-H.one()],coerce=False)
The result of reduction is not the normal form, if one reduces by a list of polynomials:

```python
sage: (x*z).reduce(I.gens())
x*z
```

However, if the argument is an ideal, then a normal form (reduction with respect to a two-sided Groebner basis) is returned:

```python
sage: (x*z).reduce(I)
-x
```

The Groebner basis shows that the result is correct:

```python
sage: I.std() #random
Left Ideal (z^2 - 1, y*z - y, x*z + x, y^2, 2*x*y - z - 1, x^2) of
Noncommutative Multivariate Polynomial Ring in x, y, z over Rational
Field, nc-relations: {z*x: x*z + 2*x, z*y: y*z - 2*y, y*x: x*y - z}
sage: sorted(I.std().gens(),key=str)
[2*x*y - z - 1, x*z + x, x^2, y*z - y, y^2, z^2 - 1]
```

total_degree()

Return the total degree of self, which is the maximum degree of all monomials in self.

EXAMPLES:

```python
sage: A.<x,z,y> = FreeAlgebra(QQ, 3)
sage: R = A.g_algebra(relations={y*x:-x*y + z}, order='lex')
sage: R.inject_variables()
Defining x, z, y
sage: f=2*x*y^3*z^2
sage: f.total_degree()
6
sage: f=4*x^2*y^2*z^3
sage: f.total_degree()
7
sage: f=99*x^6*y^3*z^9
sage: f.total_degree()
18
```
sage: f=x*y^3*z^6+3*x^2
sage: f.total_degree()
10
sage: f=z^3+8*x^4*y^5*z
sage: f.total_degree()
10
sage: f=z^9+10*x^4+y^8*x^2
sage: f.total_degree()
10

sage.rings.polynomial.plural.SCA(base_ring, names, alt_vars, order='degrevlex')
Return a free graded-commutative algebra
This is also known as a free super-commutative algebra.

INPUT:
- base_ring – the ground field
- names – a list of variable names
- alt_vars – a list of indices of to be anti-commutative variables (odd variables)
- order – ordering to be used for the constructed algebra

EXAMPLES:

sage: from sage.rings.polynomial.plural import SCA
sage: E = SCA(QQ, ['x', 'y', 'z'], [0, 1], order = 'degrevlex')
sage: E
Quotient of Noncommutative Multivariate Polynomial Ring in x, y, z over Rational Field, nc-relations: {y*x: -x*y} by the ideal (y^2, x^2)
sage: E.inject_variables()
Defining xbar, ybar, zbar
sage: x,y,z = (xbar,ybar,zbar)
sage: y*x
-x*y
sage: z*x
x*z
sage: x^2
0
sage: y^2
0
sage: z^2
z^2
sage: E.one()
1

sage.rings.polynomial.plural.new_CRing(rw, base_ring)
Construct MPolynomialRing_libsingular from ringWrap, assuming the ground field to be base_ring

EXAMPLES:

sage: H.<x,y,z> = PolynomialRing(QQ, 3)
sage: from sage.libs.singular.function import singular_function
sage: ringlist = singular_function('ringlist')
sage: ring = singular_function("ring")
sage: L = ringlist(H, ring=H); L
[0, ['x', 'y', 'z'], [['dp', (1, 1, 1)], ['C', (0,)]], [0]]
sage: len(L)
4
sage: W = ring(L, ring=H); W
<RingWrap>
sage: from sage.rings.polynomial.plural import new_CRing
sage: R = new_CRing(W, H.base_ring())
# indirect doctest
Multivariate Polynomial Ring in x, y, z over Rational Field

Check that trac ticket #13145 has been resolved:

sage: h = hash(R.gen() + 1) # sets currRing
sage: from sage.libs.singular.ring import ring_refcount_dict, currRing_wrapper
sage: currnt = ring_refcount_dict[currRing_wrapper()]
sage: newR = new_CRing(W, H.base_ring())
sage: ring_refcount_dict[currRing_wrapper()] - currnt
2

Check that trac ticket #29311 is fixed:

sage: R.<x,y,z> = QQ[]
sage: from sage.libs.singular.function_factory import ff
sage: W = ff.ring(ff.ringlist(R), ring=R)
sage: C = sage.rings.polynomial.plural.new_CRing(W, R.base_ring())
sage: C.one()
1

sage.rings.polynomial.plural.new_NRing(rw, base_ring)
Construct NCPolynomialRing_plural from ringWrap, assuming the ground field to be base_ring

EXAMPLES:

sage: A.<x,y,z> = FreeAlgebra(QQ, 3)
sage: H = A.g_algebra({y*x:x*y-1})
sage: H.inject_variables()
Defining x, y, z
sage: z*x
x*z
sage: z*y
y*z
sage: y*x
x*y - 1
sage: I = H.ideal([y^2, x^2, z^2-1])
sage: I._groebner_basis_libsingular()
[1]
sage: from sage.libs.singular.function import singular_function
sage: ringlist = singular_function('ringlist')
sage: ring = singular_function("ring")
sage: L = ringlist(H, ring=H); L
[0 1 1]
[0 0 1]
0, ['x', 'y', 'z'], [['dp', (1, 1, 1)], ['C', (0,)]], [0], [0 0 0],
[ 0 -1 0]
[ 0 0 0]
[ 0 0 0]
]
sage: len(L)
6

sage: W = ring(L, ring=H); W
<noncommutative RingWrap>
sage: from sage.rings.polynomial.plural import new_NRing
sage: R = new_NRing(W, H.base_ring())
sage: R
# indirect doctest
Noncommutative Multivariate Polynomial Ring in x, y, z over Rational Field, nc-relations: {y*x: x*y - 1}

sage.rings.polynomial.plural.new_Ring(rw, base_ring)
Constructs a Sage ring out of low level RingWrap, which wraps a pointer to a Singular ring.

The constructed ring is either commutative or noncommutative depending on the Singular ring.

EXAMPLES:

sage: A.<x,y,z> = FreeAlgebra(QQ, 3)
sage: H = A.g_algebra({y*x:x*y-1})
sage: H.inject_variables()
Defining x, y, z
sage: z*x
x*z
sage: z*y
y*z
sage: y*x
x*y - 1
sage: I = H.ideal([y^2, x^2, z^2-1])
sage: I._groebner_basis_libsingular()
[1]
sage: from sage.libs.singular.function import singular_function
sage: ringlist = singular_function('ringlist')
sage: ring = singular_function("ring")
sage: L = ringlist(H, ring=H); L
[
[0 1 1]
[0 0 1]
0, ['x', 'y', 'z'], [['dp', (1, 1, 1)], ['C', (0,)]], [0], [0 0 0],
[ 0 -1 0]
[ 0 0 0]
[ 0 0 0]
]
sage: len(L)
6

sage: W = ring(L, ring=H); W
<noncommutative RingWrap>

sage: from sage.rings.polynomial.plural import new_Ring
sage: R = new_Ring(W, H.base_ring()); R
Noncommutative Multivariate Polynomial Ring in x, y, z over Rational Field, nc-
relations: {y*x: x*y - 1}

sage.rings.polynomial.plural.unpickle_NCPolynomial_plural(R, d)
Auxiliary function to unpickle a non-commutative polynomial.
INDICES AND TABLES

- Index
- Module Index
- Search Page
sage.rings.polynomial.ore_function_element, 68
sage.rings.polynomial.ore_function_field, 59
sage.rings.polynomial.ore_polynomial_element, 12
sage.rings.polynomial.ore_polynomial_ring, 1
sage.rings.polynomial.plural, 75
sage.rings.polynomial.skew_polynomial_element, 43
sage.rings.polynomial.skew_polynomial_finite_field, 51
sage.rings.polynomial.skew_polynomial_finite_order, 47
sage.rings.polynomial.skew_polynomial_ring, 38
INDEX

A
an_element() (sage.rings.polynomial.ore_function_element.OreFunctionBaseringInjection method), 72
an_element() (sage.rings.polynomial.ore_polynomial_element.OrePolynomialBaseringInjection method), 35

B
base_ring() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial method), 15
bound() (sage.rings.polynomial.skew_polynomial_finite_order.SkewPolynomial_finite_order_dense method), 47

C
center() (sage.rings.polynomial.ore_function_field.OreFunctionField_with_large_center method), 66
center() (sage.rings.polynomial.skew_polynomial_ring.SkewPolynomialRing_finite_order method), 41
change_var() (sage.rings.polynomial.ore_function_field.OreFunctionField method), 61
change_var() (sage.rings.polynomial.ore_polynomial_ring.OrePolynomialRing method), 4
change_variable_name() (sage.rings.polynomial.ore_function_field.OreFunctionField method), 4
class in sage.rings.polynomial.ore_function_element, 68
class in sage.rings.polynomial.ore_polynomial_element, 12
count_factorizations() (sage.rings.polynomial.skew_polynomial_finite_field.SkewPolynomial_finite_field_dense method), 51
count_irreducible_divisors() (sage.rings.polynomial.skew_polynomial_finite_field.SkewPolynomial_finite_field_dense method), 51
create_key_and_extra_args() (sage.rings.polynomial.plural.G_AlgFactory method), 77
create_object() (sage.rings.polynomial.plural.G_AlgFactory method), 77

degree() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial method), 16
degree() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial_generic_dense method), 35
degree() (sage.rings.polynomial.plural.NCPolynomial_plural method), 84
degrees() (sage.rings.polynomial.plural.NCPolynomial_plural method), 84
dict() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial_generic_dense method), 36
dict() (sage.rings.polynomial.plural.NCPolynomial_plural method), 85

E
exponents() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial method), 16
exponents() (sage.rings.polynomial.plural.NCPolynomial_plural method), 85
ExteriorAlgebra() (in module sage.rings.polynomial.plural), 76
ExteriorAlgebra_plural (class in sage.rings.polynomial.plural), 77

F
factor() (sage.rings.polynomial.skew_polynomial_finite_field.SkewPolynomial_finite_field_dense method), 52
factorizations() (sage.rings.polynomial.skew_polynomial_finite_field.SkewPolynomial_finite_field_dense method), 53
fraction_field() (sage.rings.polynomial.ore_function_field.OreFunctionField method), 62
fraction_field() (sage.rings.polynomial.ore_polynomial_ring.OrePolynomialRing method), 5
free_algebra() (sage.rings.polynomial.plural.NCPolynomialRing_plural method), 78

G
G_AlgFactory (class in sage.rings.polynomial.plural), 77
gen() (sage.rings.polynomial.ore_function_field.OreFunctionField method), 62
gen() (sage.rings.polynomial.ore_polynomial_ring.OrePolynomialRing method), 5
gen() (sage.rings.polynomial.plural.NCPolynomialRing_plural method), 78
gens_dict() (sage.rings.polynomial.ore_function_field.OreFunctionField method), 62
gens_dict() (sage.rings.polynomial.ore_polynomial_ring.OrePolynomialRing method), 6

H
hamming_weight() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial method), 16
hilbert_shift() (sage.rings.polynomial.ore_function_element.OreFunction method), 69
hilbert_shift() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial_generic_dense method), 36

I
ideal() (sage.rings.polynomial.plural.NCPolynomialRing_plural method), 78
is_central() (sage.rings.polynomial.skew_polynomial_finite_order.SkewPolynomial_finite_order_dense method), 48
is_commutative() (sage.rings.polynomial.ore_function_field.OreFunctionField method), 63
is_commutative() (sage.rings.polynomial.ore_polynomial_ring.OrePolynomialRing method), 6
is_commutative() (sage.rings.polynomial.plural.NCPolynomialRing_plural method), 79
is_constant() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial method), 17
is_constant() (sage.rings.polynomial.plural.NCPolynomial_plural method), 85
is_exact() (sage.rings.polynomial.ore_function_field.OreFunctionField method), 63
is_exact() (sage.rings.polynomial.ore_polynomial_ring.OrePolynomialRing method), 6
is_field() (sage.rings.polynomial.ore_function_field.OreFunctionField method), 63
is_field() (sage.rings.polynomial.ore_polynomial_ring.OrePolynomialRing method), 7
is_field() (sage.rings.polynomial.plural.NCPolynomialRing_plural method), 79
is_finite() (sage.rings.polynomial.ore_function_field.OreFunctionField method), 64
is_finite() (sage.rings.polynomial.ore_polynomial_ring.OrePolynomialRing method), 7
is_homogeneous() (sage.rings.polynomial.plural.NCPolynomial_plural method), 85
is_irreducible() (sage.rings.polynomial.skew_polynomial_finite_field.SkewPolynomial_finite_field_dense method), 53
is_left_divisible_by() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial method), 17
is_monic() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial method), 17
is_monomial() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial method), 18
is_monomial() (sage.rings.polynomial.plural.NCPolynomial_plural method), 86
is_nilpotent() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial method), 18
is_one() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial method), 19
is_right_divisible_by() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial method), 19
is_sparse() (sage.rings.polynomial.ore_function_field.OreFunctionField method), 64
is_sparse() (sage.rings.polynomial.ore_polynomial_ring.OrePolynomialRing method), 7
is_term() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial method), 20
is_unit() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial method), 20
is_zero() (sage.rings.polynomial.ore_function_element.OreFunction method), 69
is_zero() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial method), 20
is_zero() (sage.rings.polynomial.plural.NCPolynomial_plural method), 86

L
lagrange_polynomial() (sage.rings.polynomial.skew_polynomial_ring.SkewPolynomialRing method), 39
lc() (sage.rings.polynomial.plural.NCPolynomial_plural method), 86
leading_coefficient() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial method), 21
left_denominator() (sage.rings.polynomial.ore_function_element.OreFunction method), 70
left_divides() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial method), 21
left_gcd() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial method), 21
left_irreducible_divisor() (sage.rings.polynomial.skew_polynomial_finite_field.SkewPolynomial_finite_field_dense method), 54
left_irreducible_divisors() (sage.rings.polynomial.skew_polynomial_finite_field.SkewPolynomial_finite_field_dense method), 55
left_lcm() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial method), 22
left_mod() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial method), 23
left_monic() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial method), 24
left_numerator() (sage.rings.polynomial.ore_function_element.OreFunction method), 71
left_power_mod() (sage.rings.polynomial.skew_polynomial_element.SkewPolynomial_generic_dense method), 44
left_quo_rem() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial method), 24
left_xgcd() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial method), 25
left_xlcm() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial method), 26
list() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial method), 37
lm() (sage.rings.polynomial.plural.NCPolynomial_plural method), 87
lt() (sage.rings.polynomial.plural.NCPolynomial_plural method), 87

M
minimal_vanishing_polynomial() (sage.rings.polynomial.skew_polynomial_ring.SkewPolynomialRing method), 40
module
    sage.rings.polynomial.ore_function_element, 68
    sage.rings.polynomial.ore_function_field, 59
    sage.rings.polynomial.ore_polynomial_element, 12
    sage.rings.polynomial.ore_polynomial_ring, 1
    sage.rings.polynomial.plural, 75
    sage.rings.polynomial.skew_polynomial_element, 43
    sage.rings.polynomial.skew_polynomial_finite_field, 51
    sage.rings.polynomial.skew_polynomial_finite_order, 47
    sage.rings.polynomial.skew_polynomial_ring, 38
monomial_all_divisors() (sage.rings.polynomial.plural.NCPolynomialRing_plural method), 79
monomial_coefficient() (sage.rings.polynomial.plural.NCPolynomial_plural method), 88
monomial_divides() (sage.rings.polynomial.plural.NCPolynomialRing_plural method), 80
monomial_lcm() (sage.rings.polynomial.plural.NCPolynomialRing_plural method), 80
monomial_pairwise_prime() (sage.rings.polynomial.plural.NCPolynomialRing_plural method), 80
monomial_quotient() (sage.rings.polynomial.plural.NCPolynomialRing_plural method), 81
monomial_reduce() (sage.rings.polynomial.plural.NCPolynomialRing_plural method), 81
monomials() (sage.rings.polynomial.plural.NCPolynomial_plural method), 88
multi_point_evaluation() (sage.rings.polynomial.skew_polynomial_element.SkewPolynomial_generic_dense method), 45

N
NCPolynomial_plural (class in sage.rings.polynomial.plural), 82
NCPolynomialRing_plural (class in sage.rings.polynomial.plural), 77
new_CRing() (in module sage.rings.polynomial.plural), 90
new_NRing() (in module sage.rings.polynomial.plural), 91
new_Ring() (in module sage.rings.polynomial.plural), 92
ngens() (sage.rings.polynomial.ore_function_field.OreFunctionField method), 64
ngens() (sage.rings.polynomial.ore_polynomial_ring.OrePolynomialRing method), 8
ngens() (sage.rings.polynomial.plural.NCPolynomialRing_plural method), 82
number_of_terms() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial method), 27

O
operator_eval() (sage.rings.polynomial.skew_polynomial_element.SkewPolynomial_generic_dense method), 45
optimal_bound() (sage.rings.polynomial.skew_polynomial_element.SkewPolynomial_generic_dense method), 48
OreFunction (class in sage.rings.polynomial.ore_function_element), 68
OreFunction_with_large_center (class in sage.rings.polynomial.ore_function_element), 73
OreFunctionBaseringInjection (class in sage.rings.polynomial.ore_function_element), 72
OreFunctionCenterInjection (class in sage.rings.polynomial.ore_function_field), 61
OreFunctionField (class in sage.rings.polynomial.ore_function_field), 61
OreFunctionField_with_large_center (class in sage.rings.polynomial.ore_function_field), 66
OrePolynomial (class in sage.rings.polynomial.ore_polynomial_element), 12
OrePolynomial_generic_dense (class in sage.rings.polynomial.ore_polynomial_element), 35
OrePolynomialBaseringInjection (class in sage.rings.polynomial.ore_polynomial_element), 34
OrePolynomialRing (class in sage.rings.polynomial.ore_polynomial_ring), 1

P
padded_list() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial method), 27
parameter() (sage.rings.polynomial.ore_function_field.OreFunctionField method), 64
parameter() (sage.rings.polynomial.ore_polynomial_ring.OrePolynomialRing method), 8
prec() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial method), 27

R
random_element() (sage.rings.polynomial.ore_function_field.OreFunctionField method), 65
random_element() (sage.rings.polynomial.ore_polynomial_ring.OrePolynomialRing method), 8
random_irreducible() (sage.rings.polynomial.ore_polynomial_ring.OrePolynomialRing method), 9
reduce() (sage.rings.polynomial.plural.NCPolynomial_plural method), 89
reduced_norm() (sage.rings.polynomial.ore_function_element.OreFunction_with_large_center method), 73
reduced_norm() (sage.rings.polynomial.skew_polynomial_finite_order.SkewPolynomial_finite_order_dense method), 49
reduced_trace() (sage.rings.polynomial.ore_function_element.OreFunction_with_large_center method), 74
reduced_trace() (sage.rings.polynomial.skew_polynomial_finite_order.SkewPolynomial_finite_order_dense method), 50
relations() (sage.rings.polynomial.plural.NCPolynomialRing_plural method), 82
right_denominator() (sage.rings.polynomial.ore_function_element.OreFunction method), 71
right_divides() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial method), 28
right_gcd() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial method), 28
right_irreducible_divisor() (sage.rings.polynomial.skew_polynomial_finite_field.SkewPolynomial_finite_field_dense method), 55
right_irreducible_divisors() (sage.rings.polynomial.skew_polynomial_finite_field.SkewPolynomial_finite_field_dense method), 56
right_lcm() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial method), 29
right_monic() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial method), 30
right_numerator() (sage.rings.polynomial.ore_function_element.OreFunction method), 72
right_power_mod() (sage.rings.polynomial.skew_polynomial_element.SkewPolynomial_generic_dense method), 46
right_quo_rem() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial method), 31
right_xgcd() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial method), 32
right_xlcm() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial method), 33

S
sage.rings.polynomial.ore_function_element module, 68
sage.rings.polynomial.ore_function_field module, 59
sage.rings.polynomial.ore_polynomial_element module, 12
sage.rings.polynomial.ore_polynomial_ring module, 1
sage.rings.polynomial.plural module, 75
sage.rings.polynomial.skew_polynomial_element module, 43
sage.rings.polynomial.skew_polynomial_finite_field module, 51
sage.rings.polynomial.skew_polynomial_finite_order module, 47
sage.rings.polynomial.skew_polynomial_ring module, 38
SCA() (in module sage.rings.polynomial.plural), 90
section() (sage.rings.polynomial.ore_function_element.OreFunctionBaseringInjection method), 73
section() (sage.rings.polynomial.ore_function_field.OreFunctionCenterInjection method), 61
section() (sage.rings.polynomial.ore_polynomial_element.OrePolynomialBaseringInjection method), 35
section() (sage.rings.polynomial.skew_polynomial_ring.SkewPolynomialCenterInjection method), 38
SectionOreFunctionCenterInjection (class in sage.rings.polynomial.ore_function_field), 68
SectionSkewPolynomialCenterInjection (class in sage.rings.polynomial.skew_polynomial_ring), 38
shift() (sage.rings.polynomial.ore_polynomial_element.OrePolynomial method), 33
SkewPolynomial_finite_field_dense (class in sage.rings.polynomial.skew_polynomial_finite_field), 51
SkewPolynomial_finite_order_dense (class in sage.rings.polynomial.skew_polynomial_finite_order), 47
SkewPolynomial_generic_dense (class in sage.rings.polynomial.skew_polynomial_element), 44
SkewPolynomialCenterInjection (class in sage.rings.polynomial.skew_polynomial_ring), 38
SkewPolynomialRing (class in sage.rings.polynomial.skew_polynomial_ring), 39
SkewPolynomialRing_finite_field (class in sage.rings.polynomial.skew_polynomial_ring), 41
SkewPolynomialRing_finite_order (class in sage.rings.polynomial.skew_polynomial_ring), 41
square () (sage.rings.polynomial.ore_polynomial_element.OrePolynomial method), 34

T
term_order () (sage.rings.polynomial.plural.NCPolynomialRing_plural method), 82
total_degree () (sage.rings.polynomial.plural.NCPolynomial_plural method), 89
truncate () (sage.rings.polynomial.ore_polynomial_element.OrePolynomial_generic_dense method), 37
twist_map () (sage.rings.polynomial.ore_polynomial_element.OrePolynomial_ring.OrePolynomialRing method), 10
twisting_derivation () (sage.rings.polynomial.ore_function_field.OreFunctionField method), 65
twisting_derivation () (sage.rings.polynomial.ore_polynomial_ring.OrePolynomialRing method), 10
twisting_morphism () (sage.rings.polynomial.ore_function_field.OreFunctionField method), 66
twisting_morphism () (sage.rings.polynomial.ore_polynomial_ring.OrePolynomialRing method), 10
type () (sage.rings.polynomial.skew_polynomial_finite_field.SkewPolynomial_finite_field_dense method), 57

U
unpickle_NCPolynomial_plural () (in module sage.rings.polynomial.plural), 93

V
valuation () (sage.rings.polynomial.ore_polynomial_element.OrePolynomial_generic_dense method), 37
variable_name () (sage.rings.polynomial.ore_polynomial_element.OrePolynomial method), 34