Остаток от деления в кольцах многочленов с
переменных

Лит.: Кокс Д., Литтл Дж., О'Ши Д. Идеалы, многообразия и алгоритмы. Введение в вычисл
алгебраической геометрии и коммутативной алгебры. Гл. 2, п. 3.

Вычисление остатка

Пусть $J = (g_1, \dots g_s)$ --- список многочленов, тогда любой многочлен можно представить

$$f = \sum u_i g_i + r,$$

где мономы r не делится ни на однин из мономов $lm(g_1), \dots lm(g_s)$. При этом r называю
на J.

1) Что можно подать на вход след. функции?

На вход функции подается f - символьное выражение, J - список символьных выражений
которому принадлежат эти выражения

В [9]:

```
def rem_step(f,J,K):
    ans=0
    while ans==0:
        ans=1
        if K(f) != 0:
            for g in J:
                a = K(f).lt()/K(g).lt()
                if a in K:
                    ans=0
                    f=K(f)-a*K(g)
                    break
    return SR(f)
```

В [10]:

```
var("x0,x1,x2")
```

Out[10]:

```
(x0, x1, x2)
```

В [13]:

```
K=QQ[x0,x1,x2]
rem_step(x0*x2, [x1+x2-1,x2+5,x0^2+x1+x2+3], K)
```

Out[13]:

```
-5*x0
```

В [12]:

```
K=PolynomialRing(QQ,[x2,x1,x0],order='lex')
rem_step(x0*x2, [x1+x2-1,x2+5,x0^2+x1+x2+3], K)
```

Out[12]:

```
-x0*x1 + x0
```

2) Что происходит в цикле for? При выполнении условия a in K старший член f становитс

3) Чему равно f в тот момент, когда заканчивается цикл while? Что возвращает эта функ

В цикле for мы замняем многочлен f на новый могчлен f, который отличается от старого один из многочленов g. При этом старший член становится меньше, либо мы не можем з старший член в f не делится ни на один из старших членов в g

Когда while закнчивается f такова, что ее старший моном не делится ни на один из моном функция воврващает такой многочлен f, старший моном которого не делится ни на один и

Замечание. Эта функция возвращает такой многочлен h, что

$$f = \sum u_i g_i + h$$

и $lm(h)$ не делится ни на однин из мономов $lm(g_1), \ldots lm(g_s)$. Это еще не остаток!

4) Зависит ли результат от порядка переменных? От выбора мономиального порядка?

Результат зависит от порядка переменных и мономиального порядка

В [17]:

```
K=PolynomialRing(QQ,[x0,x1,x2],order='lex')
rem_step(x0^2, [x1^2+x2^3-1,x2^2+5,x0+x1^2+x2^2+3], K)
```

Out[17]:

```
-10*x2 - 124
```

В [18]:

```
K=PolynomialRing(QQ,[x0,x1,x2],order='deglex')
rem_step(x0^2, [x1^2+x2^3-1,x2^2+5,x0+x1^2+x2^2+3], K)
```

Out[18]:

```
x0^2
```

В [19]:

```
K=PolynomialRing(QQ,[x2,x1,x0],order='lex')
rem_step(x0^2, [x1^2+x2^3-1,x2^2+5,x0+x1^2+x2^2+3], K)
```

Out[19]:

```
x0^2
```

5) Проверить, что след. функция возвращает остаток.

В [31]:

```
def rem(f,J,K):
    p=rem_step(f,J,K)
    r=0
    while K(p)!=0:
        [f,r]=[K(p)-K(p).lt(),K(r)+K(p).lt()]
        p=rem_step(f,J,K)
    return SR(r)
```

В [30]:

```
rem(x0^5, [x1*x2-6,x0*x2-3,x0+x1+x2+2], QQ[x0,x1,x2])
```

Out[30]:

```
-x1^5 - 10*x1^4 - 61*x1^3 - 236*x1^2 - 623*x1 - 169*x2 - 902
```

Проверка

В [29]:

```
f=x0^5
J=[x1*x2-6,x0*x2-3,x0+x1+x2+2]
r=rem(f, J, QQ[x0,x1,x2])
print(r)
f-r in QQ[x0,x1,x2]*J
```

```
-x1^5 - 10*x1^4 - 61*x1^3 - 236*x1^2 - 623*x1 - 169*x2 - 902
```

Out[29]:

```
True
```

Мономы остатка

В [32]:

```
QQ[x0,x1,x2](r).monomials()
```

Out[32]:

```
[x1^5, x1^4, x1^3, x1^2, x1, x2, 1]
```

не делятся на старшие мономы в J. Поэтому r --- остаток от деления f на J.

В [33]:

```
[QQ[x0,x1,x2](g).lm() for g in J]
```

Out[33]:

```
[x1*x2, x0*x2, x0]
```

6) Что происходит в 5 и 6 строчках?

7) Что получится, если применить эту функцию к многочлену из $\mathbb{Q}[x]$?

В этих строчках переопределяются p, f, r. Новые p, f, r определяются по этим формулам:

$$f' = p - lt(p), \quad r' = r + lt(p), \quad p' = f' + \sum u_i' g_i$$

При этом $f' + r' = p + r$, но старший член из p переезжает в r. Дальше p заменяется н
отличается от f' на лин. комб. g_i и старший моном которого не делится на $lm(g_1), \dots, l$

Если применить функцию к Q[x] то остаток будет вычисляться правильно.

В [34]:

```
var("x")
f=x^3+x+1
J=[x^2+x-2]
rem(f,J,QQ[x])
```

Out[34]:

```
4*x - 1
```

В [35]:

```
QQ[x](f).quo_rem(QQ[x](J[0]))
```

Out[35]:

```
(x - 1, 4*x - 1)
```

В [36]:

```
QQ[x](f)(2)
```

Out[36]:

```
11
```

Идеалы

Условие

$$f \in J = (g_1, \dots, g_s)$$

означает, что существуют такие $u_1, \dots, u_s$, что

$$f = \sum_{i=1}^{s} u_i g_i.$$

Задача. Даны многочлен f и идеал J, выяснить, верно ли $f \in J$.

8) Является ли условие обращения в нуль остатка от деления f на J достаточным для f

Это условие является достаточным

В [37]:

```
var("x,y,z")
J=[y-x^2, z-x^3]
K=PolynomialRing(QQ,[z,y,x],order='lex')
rem(y^3-z^2, J, K)
```

Out[37]:

```
0
```

9) Является ли условие обращения в нуль остатка от деления f на J необходимым для

В [19]:

```
var("x,y,z")
J=[y-x^2, z-x^3]
K=PolynomialRing(QQ,[x,y,z],order='lex')
rem(y^3-z^2, J, K)
```

Out[19]:

```
y^3 - z^2
```

Но не является необходимым