Endliche Koerper (mit Sage)

```
# %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
# RECHNEN IN ENDLICHEN KOERPER MIT SAGE
# %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```

```
R.<X> = PolynomialRing(Integers(7))
print R
```

```
Univariate Polynomial Ring in X over Ring of integers modulo 7
```

```
# R ist also der Polynomring F_7[X] mit der Unbestimmten X
# in R koennen wir rechnen:
```

```
print (X^2+X+1)^20
print (X^2+2)*(X+1)^7
```

```
X^40 + 6*X^39 + X^37 + 6*X^36 + X^34 + 2*X^33 + 4*X^32 + X^31 +
2*X^30 + 4*X^29 + X^28 + 2*X^27 + 3*X^26 + 2*X^25 + 2*X^24 + 3*X^23
+ 2*X^22 + 2*X^21 + 3*X^20 + 2*X^19 + 2*X^18 + 3*X^17 + 2*X^16 +
2*X^15 + 3*X^14 + 2*X^13 + X^12 + 4*X^11 + 2*X^10 + X^9 + 4*X^8 +
2*X^7 + X^6 + 6*X^4 + X^3 + 6*X + 1
X^9 + 2*X^7 + X^2 + 2
```

```
# ein Polynom in R[X] kann faktorisiert werden:
```

```
factor(X^3 + 3*X^2 + 5*X + 1)
```

```
(X + 4) * (X + 3)^2
```

```
# wenn f ueber F_7 irreduzibel ist, so ist F_7[X]/(f) ein Koerper
```

```
factor(X^3 + X + 1)
```

```
X^3 + X + 1
```

```
F.<X>=R.quotient([X^3 + X + 1]) # hier wird F_{7^3} definiert
```

```
1/(X^2 + 1)
```

```
6*X
```

```
6*X*(X^2 + 1)
```

```
1
```

```
g=2*X^2+3
1/g^7777
```

```
X^2 + 5*X + 1
```

```
# Wir suchen nun ein irreduzibles Polynom vom ueber F_2 vom Grad
1000:
```

```
R.<X> = PolynomialRing(Integers(2))
print R
```

```
Univariate Polynomial Ring in X over Ring of integers modulo 2
(using GF2X)
```

```
for i in range(2,6):
    for j in range(1,i):
        for k in range(j):
            f=X^1000+X^i+X^j+X^k+1
            if len(factor(f))==1:
                print factor(f)
```

```
X^1000 + X^5 + X^4 + X^3 + 1
```

```
Ordnung=2^1000 # Anzahl Elemente in F_{2^1000}
list=Ordnung.digits()
print Ordnung
print
print "Die Zahl hat",len(list),"Stellen"
```

```
107150860718626732094842504906000181056140481170553360744375038837035105112493612249319837881569585812759467291755314682518714528569231404359845775746985748039345677748242309854210746050623711418779541821530464749835819412673987675591655439460770629145711964776865421676604298316526243868372056680693 76

Die Zahl hat 302 Stellen
```

```
F.<X>=R.quotient([X^1000 + X^5 + X^4 + X^3 + 1]) # hier wird
F_{2^1000} definiert
```

```
(X^300+X+1)^7/(X^777+X^3333) # Beispiel einer Rechnung
```

```
X^999 + X^998 + X^997 + X^996 + X^993 + X^991 + X^990 + X^988 +
X^985 + X^984 + X^982 + X^978 + X^977 + X^975 + X^972 + X^971 +
X^968 + X^967 + X^966 + X^964 + X^961 + X^958 + X^956 + X^952 +
X^949 + X^947 + X^943 + X^942 + X^941 + X^937 + X^935 + X^933 +
X^932 + X^931 + X^928 + X^922 + X^921 + X^918 + X^917 + X^916 +
X^914 + X^913 + X^911 + X^909 + X^906 + X^903 + X^900 + X^899 +
X^898 + X^897 + X^893 + X^891 + X^889 + X^888 + X^887 + X^885 +
X^880 + X^879 + X^876 + X^875 + X^873 + X^872 + X^871 + X^870 +
X^867 + X^863 + X^861 + X^860 + X^859 + X^858 + X^855 + X^852 +
X^851 + X^848 + X^844 + X^843 + X^841 + X^840 + X^836 + X^835 +
X^834 + X^833 + X^829 + X^828 + X^824 + X^823 + X^822 + X^821 +
X^820 + X^819 + X^815 + X^814 + X^812 + X^810 + X^805 + X^803 +
X^802 + X^799 + X^798 + X^796 + X^795 + X^794 + X^792 + X^790 +
X^789 + X^788 + X^787 + X^786 + X^780 + X^777 + X^775 + X^773 +
X^772 + X^768 + X^767 + X^764 + X^762 + X^761 + X^760 + X^758 +
X^757 + X^756 + X^752 + X^749 + X^746 + X^743 + X^742 + X^739 +
X^738 + X^736 + X^732 + X^731 + X^730 + X^729 + X^728 + X^724 +
X^722 + X^717 + X^713 + X^711 + X^710 + X^706 + X^705 + X^704 +
```

```
    X^702 + X^700 + X^699 + X^696 + X^689 + X^687 + X^685 + X^684 +
    X^683 + X^682 + X^681 + X^680 + X^678 + X^676 + X^675 + X^674 +
    X^672 + X^668 + X^667 + X^665 + X^662 + X^658 + X^657 + X^654 +
    X^652 + X^651 + X^650 + X^647 + X^646 + X^645 + X^644 + X^643 +
    X^641 + X^640 + X^638 + X^635 + X^634 + X^633 + X^630 + X^629 +
    X^626 + X^623 + X^621 + X^620 + X^618 + X^616 + X^615 + X^613 +
    X^612 + X^611 + X^610 + X^609 + X^601 + X^600 + X^598 + X^596 +
    X^595 + X^592 + X^589 + X^587 + X^586 + X^584 + X^582 + X^581 +
    X^577 + X^576 + X^575 + X^574 + X^573 + X^572 + X^571 + X^569 +
    X^565 + X^563 + X^562 + X^560 + X^559 + X^556 + X^555 + X^554 +
    X^552 + X^551 + X^549 + X^544 + X^540 + X^539 + X^538 + X^537 +
    X^536 + X^535 + X^534 + X^533 + X^528 + X^527 + X^526 + X^525 +
    X^523 + X^521 + X^517 + X^516 + X^514 + X^512 + X^510 + X^508 +
    X^507 + X^505 + X^502 + X^501 + X^499 + X^494 + X^493 + X^489 +
    X^488 + X^487 + X^486 + X^485 + X^484 + X^483 + X^482 + X^481 +
    X^477 + X^475 + X^474 + X^471 + X^469 + X^468 + X^462 + X^460 +
    X^458 + X^457 + X^456 + X^453 + X^451 + X^448 + X^447 + X^446 +
    X^444 + X^443 + X^442 + X^440 + X^439 + X^438 + X^436 + X^435 +
    X^433 + X^430 + X^428 + X^427 + X^426 + X^423 + X^420 + X^414 +
    X^413 + X^411 + X^410 + X^408 + X^406 + X^405 + X^403 + X^402 +
    X^399 + X^398 + X^396 + X^392 + X^390 + X^380 + X^379 + X^378 +
    X^375 + X^373 + X^372 + X^371 + X^369 + X^368 + X^364 + X^363 +
    X^361 + X^359 + X^356 + X^355 + X^354 + X^353 + X^352 + X^351 +
    X^350 + X^349 + X^346 + X^345 + X^344 + X^343 + X^342 + X^340 +
    X^339 + X^337 + X^335 + X^334 + X^333 + X^331 + X^330 + X^329 +
    X^328 + X^327 + X^326 + X^325 + X^324 + X^323 + X^322 + X^318 +
    X^317 + X^316 + X^312 + X^311 + X^309 + X^306 + X^305 + X^304 +
    X^303 + X^300 + X^299 + X^297 + X^295 + X^288 + X^287 + X^282 +
    X^281 + X^280 + X^279 + X^278 + X^277 + X^276 + X^275 + X^271 +
    X^270 + X^268 + X^266 + X^265 + X^264 + X^263 + X^261 + X^260 +
    X^258 + X^256 + X^254 + X^250 + X^248 + X^247 + X^245 + X^243 +
    X^242 + X^240 + X^238 + X^237 + X^235 + X^234 + X^233 + X^232 +
    X^230 + X^229 + X^228 + X^224 + X^223 + X^221 + X^220 + X^217 +
    X^214 + X^208 + X^207 + X^203 + X^201 + X^200 + X^192 + X^191 +
    X^190 + X^189 + X^188 + X^187 + X^182 + X^177 + X^176 + X^175 +
    X^171 + X^169 + X^166 + X^161 + X^160 + X^158 + X^156 + X^153 +
    X^150 + X^147 + X^146 + X^145 + X^144 + X^143 + X^142 + X^139 +
    X^138 + X^137 + X^136 + X^133 + X^132 + X^130 + X^127 + X^124 +
    X^119 + X^114 + X^111 + X^110 + X^103 + X^101 + X^99 + X^97 + X^95 +
    X^92 + X^91 + X^89 + X^88 + X^87 + X^86 + X^84 + X^81 + X^77 + X^75
    + X^74 + X^72 + X^68 + X^67 + X^66 + X^65 + X^63 + X^62 + X^61 +
    X^60 + X^57 + X^53 + X^51 + X^49 + X^48 + X^47 + X^46 + X^45 + X^42
    + X^41 + X^39 + X^36 + X^35 + X^34 + X^32 + X^28 + X^27 + X^25 +
    X^22 + X^20 + X^19 + X^18 + X^15 + X^14 + X^12 + X^11 + X^8 + X^6 +
    X^5 + X^4 + X + 1
```

```
# Zurueck zu Polynome ueber F_7:
#
# es gibt 7 irreduzible Polynome in F_7[X] vom Grad 1, und
# es gibt 112 irreduzible Polynome in F_7[X] vom Grad 3, denn
```

```
# r_3 = 1/3 (p^3 - p)
#
# Das Produkt aller irreduziblen Polynome vom Grad 1 und 3 ist
X^(7^3)-X
```

```
R.<X> = PolynomialRing(Integers(7))
print R
```

```
Univariate Polynomial Ring in X over Ring of integers modulo 7
```

```
Prod=1
for i in range(7):
    Prod=Prod*(X-i)
print factor(Prod)
print
u=0;
for i in range(7):
    for j in range(7):
        for k in range(7):
            f=X^3+i*X^2+j*X+k
            if gcd(f,Prod)==1:
                print u,": ",factor(f)
                Prod=Prod*f
                u=u+1
print
print "Das Produkt aller irred. Polynome vom Grad 1 und 3 ist",Prod
```

```
X * (X + 1) * (X + 2) * (X + 3) * (X + 4) * (X + 5) * (X + 6)

0 :  X^3 + 2
1 :  X^3 + 3
2 :  X^3 + 4
3 :  X^3 + 5
4 :  X^3 + X + 1
5 :  X^3 + X + 6
6 :  X^3 + 2*X + 1
7 :  X^3 + 2*X + 6
8 :  X^3 + 3*X + 2
9 :  X^3 + 3*X + 5
10 :  X^3 + 4*X + 1
11 :  X^3 + 4*X + 6
12 :  X^3 + 5*X + 2
13 :  X^3 + 5*X + 5
14 :  X^3 + 6*X + 2
15 :  X^3 + 6*X + 5
16 :  X^3 + X^2 + 1
17 :  X^3 + X^2 + 3
18 :  X^3 + X^2 + X + 2
19 :  X^3 + X^2 + X + 5
20 :  X^3 + X^2 + 2*X + 4
21 :  X^3 + X^2 + 2*X + 6
```

```
22 :  X^3 + X^2 + 3*X + 1
23 :  X^3 + X^2 + 3*X + 5
24 :  X^3 + X^2 + 4*X + 3
25 :  X^3 + X^2 + 4*X + 6
26 :  X^3 + X^2 + 5*X + 1
27 :  X^3 + X^2 + 5*X + 2
28 :  X^3 + X^2 + 5*X + 3
29 :  X^3 + X^2 + 5*X + 4
30 :  X^3 + X^2 + 6*X + 3
31 :  X^3 + X^2 + 6*X + 5
32 :  X^3 + 2*X^2 + 1
33 :  X^3 + 2*X^2 + 3
34 :  X^3 + 2*X^2 + X + 4
35 :  X^3 + 2*X^2 + X + 6
36 :  X^3 + 2*X^2 + 2*X + 3
37 :  X^3 + 2*X^2 + 2*X + 6
38 :  X^3 + 2*X^2 + 3*X + 3
39 :  X^3 + 2*X^2 + 3*X + 5
40 :  X^3 + 2*X^2 + 4*X + 2
41 :  X^3 + 2*X^2 + 4*X + 5
42 :  X^3 + 2*X^2 + 5*X + 1
43 :  X^3 + 2*X^2 + 5*X + 5
44 :  X^3 + 2*X^2 + 6*X + 1
45 :  X^3 + 2*X^2 + 6*X + 2
46 :  X^3 + 2*X^2 + 6*X + 3
47 :  X^3 + 2*X^2 + 6*X + 4
48 :  X^3 + 3*X^2 + 4
49 :  X^3 + 3*X^2 + 6
50 :  X^3 + 3*X^2 + X + 1
51 :  X^3 + 3*X^2 + X + 4
52 :  X^3 + 3*X^2 + 2*X + 2
53 :  X^3 + 3*X^2 + 2*X + 5
54 :  X^3 + 3*X^2 + 3*X + 3
55 :  X^3 + 3*X^2 + 3*X + 4
56 :  X^3 + 3*X^2 + 3*X + 5
57 :  X^3 + 3*X^2 + 3*X + 6
58 :  X^3 + 3*X^2 + 4*X + 1
59 :  X^3 + 3*X^2 + 4*X + 3
60 :  X^3 + 3*X^2 + 5*X + 2
61 :  X^3 + 3*X^2 + 5*X + 4
62 :  X^3 + 3*X^2 + 6*X + 2
63 :  X^3 + 3*X^2 + 6*X + 6
64 :  X^3 + 4*X^2 + 1
65 :  X^3 + 4*X^2 + 3
66 :  X^3 + 4*X^2 + X + 3
67 :  X^3 + 4*X^2 + X + 6
68 :  X^3 + 4*X^2 + 2*X + 2
69 :  X^3 + 4*X^2 + 2*X + 5
70 :  X^3 + 4*X^2 + 3*X + 1
```

```
71 :  X^3 + 4*X^2 + 3*X + 2
72 :  X^3 + 4*X^2 + 3*X + 3
73 :  X^3 + 4*X^2 + 3*X + 4
74 :  X^3 + 4*X^2 + 4*X + 4
75 :  X^3 + 4*X^2 + 4*X + 6
76 :  X^3 + 4*X^2 + 5*X + 3
77 :  X^3 + 4*X^2 + 5*X + 5
78 :  X^3 + 4*X^2 + 6*X + 1
79 :  X^3 + 4*X^2 + 6*X + 5
80 :  X^3 + 5*X^2 + 4
81 :  X^3 + 5*X^2 + 6
82 :  X^3 + 5*X^2 + X + 1
83 :  X^3 + 5*X^2 + X + 3
84 :  X^3 + 5*X^2 + 2*X + 1
85 :  X^3 + 5*X^2 + 2*X + 4
86 :  X^3 + 5*X^2 + 3*X + 2
87 :  X^3 + 5*X^2 + 3*X + 4
88 :  X^3 + 5*X^2 + 4*X + 2
89 :  X^3 + 5*X^2 + 4*X + 5
90 :  X^3 + 5*X^2 + 5*X + 2
91 :  X^3 + 5*X^2 + 5*X + 6
92 :  X^3 + 5*X^2 + 6*X + 3
93 :  X^3 + 5*X^2 + 6*X + 4
94 :  X^3 + 5*X^2 + 6*X + 5
95 :  X^3 + 5*X^2 + 6*X + 6
96 :  X^3 + 6*X^2 + 4
97 :  X^3 + 6*X^2 + 6
98 :  X^3 + 6*X^2 + X + 2
99 :  X^3 + 6*X^2 + X + 5
100 :  X^3 + 6*X^2 + 2*X + 1
101 :  X^3 + 6*X^2 + 2*X + 3
102 :  X^3 + 6*X^2 + 3*X + 2
103 :  X^3 + 6*X^2 + 3*X + 6
104 :  X^3 + 6*X^2 + 4*X + 1
105 :  X^3 + 6*X^2 + 4*X + 4
106 :  X^3 + 6*X^2 + 5*X + 3
107 :  X^3 + 6*X^2 + 5*X + 4
108 :  X^3 + 6*X^2 + 5*X + 5
109 :  X^3 + 6*X^2 + 5*X + 6
110 :  X^3 + 6*X^2 + 6*X + 2
111 :  X^3 + 6*X^2 + 6*X + 4
```

Das Produkt aller irred. Polynome vom Grad 1 und 3 ist X^343 + 6*X

```
F.<X>=R.quotient([X^3 + 2]) # hier wird F_343 definiert mit Polynom 0
```

```
# wir suchen eine Nullstelle vom Polynom 111
```

```
for i in range(7):
```

```
    for j in range(7):
        Y=X^2+i*X+j
        if Y^3 + 6*Y^2 + 6*Y + 4==0:
            print Y
```

```
    X^2 + 6*X + 5
```

```
Y=X^2 + 6*X + 5 # Y ist Nullstelle von X^3 + 6*X^2 + 6*X + 4
print Y^3 + 6*Y^2 + 6*Y + 4
```

```
    0
```

```
# die anderen Nullstellen von X^3 + 6*X^2 + 6*X + 4 sind von der Form
Y^(7^i):
for i in range(3):
    Z=Y^(7^i)
    print i,": ",Z,"; ",Y^3 + 6*Y^2 + 6*Y + 4
```

```
    0 :  X^2 + 6*X + 5 ;  0
    1 :  2*X^2 + 3*X + 5 ;  0
    2 :  4*X^2 + 5*X + 5 ;  0
```

```
# Beispiel mit p=2 und n=5:
```

```
R.<X> = PolynomialRing(Integers(2))
```

```
for i in range(1,5):
    f=X^5+X^i+1
    if len(factor(f))==1:
        print factor(f)
```

```
    X^5 + X^2 + 1
    X^5 + X^3 + 1
```

```
F.<X>=R.quotient([X^5 + X^3 + 1]) # hier wird F_{2^5} definiert
```

```
# wir suchen die Nullstellen von X^5 + X^3 + 1:
#
for i in range(2):
    for j in range(2):
        for k in range(2):
            for l in range(2):
                for m in range(2):
                    Y=i*X^4+j*X^3+k*X^2+l*X+m
                    # wir suchen Nullstelle von X^5 + X^3 + 1
                    if Y^5 + Y^3 + 1==0:
                        print Y
```

```
    X
    X^2
    X^3 + X^2
    X^4
    X^4 + X^3 + X
```

```
# zyklisches Vertauschen der Nullstellen:
```

```
for i in range(5):
    print i,": ",X^(2^i)
```

```
0 :  X
1 :  X^2
2 :  X^4
3 :  X^4 + X^3 + X
4 :  X^3 + X^2
```

```
for i in range(5):
    print i,": ",(X^3 + X^2)^(2^i)
```

```
0 :  X^3 + X^2
1 :  X
2 :  X^2
3 :  X^4
4 :  X^4 + X^3 + X
```

```

```