**Aufgabe 1:** Bestimmen Sie experimentell den Prozentsatz der Polynome in $\mathbb{Z}/2\mathbb{Z}$, die irreduzibel sind.

```
N= 2000
MaxDeg=200

R= IntegerModRing(2)
P.<x> = PolynomialRing( R, 'x')

percentage=0
D= {}
for i in range(N):
    # randint ist wichtig, ansonsten wird degree==2 benutzt
    p= P.random_element(degree=randint(1,MaxDeg))
    if D.has_key(p):
        print "Double"
    else:
        if ( not p.is_zero() ) and ( not p.is_unit() ) \
          and  p.is_irreducible():
            percentage+=1
            D[p] = True
        else:
            D[p] = False

print "Es sind cirka", round(n(percentage / N) *100, 3) , "%

#N=2000, grad zwischen 1 und 100:  ca 3.5%
#N=2000, grad zwischen 1 und 200:  ca 2%
```

**Aufgabe 2:** Beweisen Sie, dass $f(x) := x^4 + 5x^3 + 10x^2 + 25x + 5$ in $\mathbb{Q}[x]$ irreduzibel ist. (Hinweis: betrachten Sie die Reduktion von $f$ modulo 5 und schliessen sie auf die Gestalt der potentiellen Faktoren von $f$.)

Wir sehen mit SAGE leicht ein, dass $f$ irreduzibel ist:

```
sage: P.<x>=PolynomialRing(QQ, 'x')
sage: f=x^4+5*x^3+10*x^2+25*x +5; f
x^4 + 5*x^3 + 10*x^2 + 25*x + 5
sage: (IntegerModRing(2)['x'])(f)
x^4 + x^3 + x + 1
sage: _.is_irreducible()
False
sage: (IntegerModRing(3)['x'])(f)
x^4 + 2*x^3 + x^2 + x + 2
```

```
sage: _.is_irreducible()
True
```

Die Reduktion $f \pmod 3$ ist irreduzibel und nach Proposition 4.2 in Kapitel 11 ist $f$ irredzuzibel über $\mathbb{Q}$.

Die Aufgabenstellung verlangt aber eine andere Vorgehensweise. Es ist $f \pmod 5 \equiv x^4$.

Wenn $f$ reduzibel wäre, so gäbe es Polynome $g$ und $h$ mit $f = g \cdot h$ und $1 \leq \deg g \leq 3$. Desweiteren muss $g \equiv x^{\deg g} \pmod 5$ sein. Wir machen eine Fallunterscheidung nach dem Grad von $g$ und zeigen in jedem Fall einen Widerspruch.

Grad 1: Es ist $g_1 := x + a$ und weil das Absolutglied von $g_1$ ein Teiler des Absolutgliedes von $f$ sein muss, ist $a := 5$. ($a = 1$ geht nicht, da dann $g_1 \equiv x + 1 \not\equiv x \pmod 5$ wäre.) Es ist aber $x = 5$ keine Nullstelle von $f$, deswegen ist $g_1$ kein Faktor von $f$.

Grad 2: Es ist $g_2 = x^2 + bx + c$. Dann ist $h_2 := x^2 + h_{21}x + h_{22}$ und

$$f = g_2 \cdot h_2 = x^4 + (h_{21} + b)x^3 + (h_{22} + b \cdot h_{21} + c)x^2 + (b \cdot h_{22} + c \cdot h_{21})x + c \cdot h_{22}.$$

Es ist $c \cdot h_{22} = 5$, also $c = \pm 1$ und $h_{22} = \pm 5$ (oder umgekehrt). Auf jeden Fall ist das Polynom mit dem Absolutglied $\pm 1$ nicht kongruent $x^2 \pmod 5$ und das Produkt nicht kongruent $x^4 \pmod 5$.

Grad 3: Wie im Fall Grad 1 nur vertauschen $g$ und $h$ die Rollen.

**Aufgabe 3:** Zeigen Sie, dass $\det \begin{pmatrix} x & y \\ z & w \end{pmatrix}$ in $\mathbb{C}[x, y, z, w]$ irreduzibel ist.

Es sei $f := xw - yz$. Der Grad von $f$ ist 2. Falls $f$ reduzibel ist, so gibt es Polynome $g, h$ vom Grad 1, mit $f = g \cdot h$ und $g = g_0 + g_1x + g_2y + g_3z + g_4w$ und $h = h_0 + h_1x + h_2y + h_3z + h_4w$.

Wir betrachten das Produkt $gh$ und zeigen durch Koeffizientenvergleich, dass das Produkt nicht $f$ sein kann.

Das Absolutglied von $f$ ist 0. Das Absolutglied von $gh$ ist $g_0h_0$. Nehmen wir an es ist $\underline{g_0 = 0}$ und $\underline{h_0 \neq 0}$.

Weil in $f$ die Faktoren $x, y, z$ und $w$ nicht auftauchen, die den Koeffizienten $h_0g_1x, h_0g_2y, h_0g_3z$ und $h_0g_4w$ entsprechen, sind die Koeffizienten $g_1, g_2, g_3$ und $g_4$ ebenfalls 0. Damit ist $g = 0$.

Hätten wir im ersten Schritt $h_0 = 0$ und $g_0 \neq 0$ gewählt, so hätten wir $h = 0$ erhalten.

Nehmen wir nun an, es ist $\underline{h_0 = g_0 = 0}$: Dann ist $g = g_1x + g_2y + g_3z + g_4w$ und $h = h_1x + h_2y + h_3z + h_4w$. Da $xw$ im Produkt $gh$ auftaucht ist $g_1 \neq 0$ und $h_4 \neq 0$ (oder umgekehrt). Da $xy$ und $xz$ nicht im Produkt vorkommt, ist $h_2 = h_3 = 0$, das macht es aber unmöglich, dass $yz$ mit den Koeffizienten $h_2g_3$ oder $h_3g_2$ im Produkt auftaucht.

In jedem Fall lässt sich $f$ nicht als Produkt der obigen Form schreiben und damit ist $f$ irreduzibel.

**Aufgabe 4:** Sei $I$ das von 2 und $x^2 + x + 1$ in $\mathbb{Z}[x]$ erzeugte Ideal. Zeigen Sie, dass die Polynome $ax + b$ $(0 \leq a, b \leq 1)$ ein vollständiges Repräsentantensystem für $\mathbb{Z}[x]/I$ bilden. Zeigen Sie damit, dass $\mathbb{Z}[x]/I$ ein Körper ist.

Wir untersuchen $\mathbb{Z}[X]/I$ in ähnlicher Art und Weise, wie im Anschluss an den Beweis von Proposition 10.4.3 im Artin. Wir führen die Relationen sukzessive ein.

Es ist $\mathbb{Z}[X]/I = (\mathbb{Z}[X]/2)/(X^2 + X + 1) = \mathbb{F}_2[X]/(X^2 + X + 1)$ (nach Proposition 10.4.3 b). Wir gehen also zuerst zu dem Polynomring über $\mathbb{F}_2$ über und führen in diesem Polynomring die Relation $0 = X^2 + X + 1$ bzw. $X^2 = -X - 1 \equiv X + 1 \pmod 2$ ein.

Deswegen müssen wir nur Polynome vom Grad kleiner 2 mit Koeffizienten in $\mathbb{F}_2$ untersuchen, das sind aber nur die vier Elemente $p_0 := 0$, $p_1 := 1$, $p_2 := x$ und $p_3 := x+1$ von $\mathbb{F}_2[X]/(X^2+X+1)$ bzw. von $\mathbb{Z}[X]/I$. Damit ist gezeigt, dass die Polynome $ax+b$ mit $a, b \in \{0, 1\}$ ein vollständiges Repräsentantensystem bilden.

Wir wenden Proposition 11.2.14 (a) aus dem Artin an: $\mathbb{F}_2/(X^2 + X + 1)$ ist ein Körper, da $\mathbb{F}_2[X]$ ein Hauptidealring ist (nach Proposition 10.3.21) und $X^2 + X + 1$ in $\mathbb{F}_2$ irreduzibel ($0, 1 \pmod 2$ sind keine Nullstellen) ist.

Alternativ: Wir wissen, dass der Quotientenring $\mathbb{F}_2[X]/(X^2+X+1)$ ein Ring ist, $p_0$ und $p_1$ sind die neutralen Elemente von Addition bzw. Multiplikation. Wir können leicht überprüfen, dass gilt:

$$(X+1)^{-1} = X, \qquad \text{wegen } (X+1)X = X^2+X \equiv 1 \pmod{X^2+X+1}$$
$$X^{-1} = (X+1), \text{ dto.}$$

Damit sind die Elemente $\neq p_0$ invertierbar. Körper!

**Aufgabe 5:** Finden Sie mittels SAGE zehn paarweise nicht assoziierte irreduzible Polynome in $\mathbb{Q}[x]$ vom Grad 5.

```
P.<x> = QQ['x']

L= []
while len( L ) < 10:
    p = P.random_element( degree= 5)
    if (not p.is_zero() ) and (not p.is_unit() ) \
       and p.is_irreducible() :
          ok= True
          for l in L:
              # p und l sind assoz. falls p|l und l|p:
              if p.divides(l) and l.divides(p):
                  # wir merken uns, dass p nicht ok ist
                  # und verlassen die innere Schleife
                  ok = False
                  print "assoziiert:", p, l
                  break

          # falls p ok ist, wird es angehängt
          if ok:
              L.append(p)
              print p

# -19*x^5 - x^4 - x^3 - 1/4*x^2 + 1
# 2*x^5 + 1/261*x^4 - 1/2*x^3 - 6*x^2 + 1/3*x + 1
# -2*x^5 - 1/2*x^4 - x^2 + 2/3*x - 1/3
# x^5 + 1/12*x^3 - 1
# -1/3*x^5 - 3*x^4 + 2*x^2 - 17
# -2/3*x^5 - 1/6*x^4 - x^3 + 2*x + 2/3
# 1/2*x^5 + 1/4*x^4 + x^3 - 1/4*x^2 - 1
# 1/3*x^5 + 2*x^4 + x^3 + 2*x^2 + 3/11*x + 3
# -x^5 - 1/2*x^4 - 4/3*x^3 + 53/2*x^2 + 1
# 20*x^5 + 4*x^4 + 2*x^3 + x^2 + 3/10*x + 2/3
```