Aufgabe 1: Zeigen Sie: Aus der klassischen Form des Hilbertschen Nullstellensatzes (Artin, Kapitel 10, Hauptsatz 8.7) folgt die Form des Nullstellensatzes aus Artin Kapitel 10, Hauptsatz 7.6.

Klassische Form: Es seien $g, f_1, \ldots, f_r \in \mathbb{C}[x_1, \ldots, x_n]$ und es sei $\mathcal{I} := (f_1, \ldots, f_r)$ und $V(\mathcal{I}) := \{\vec{a} \in \mathbb{C}^n \mid h(\vec{a}) = 0 \text{ für alle } h \in \mathcal{I}\}$. Gilt $g|_{V(\mathcal{I})} \equiv 0$, dann gibt es $m \in \mathbb{N}$ mit $g^m \in \mathcal{I}$.

HNS nach Artin: Es ist $\vec{a}$ der Vektor $(a_1, \ldots, a_n)$. Die maximalen Ideale in $\mathbb{C}[x_1, \ldots, x_n]$ sind von der Form $\mathcal{I}_{\vec{a}} := (x - a_1, \ldots, x - a_n)$.

1. $\mathcal{I}_{\vec{a}}$ ist maximales Ideal: (Genau, wie im Artin im Beweis von Theorem 10.7.6:) $\mathcal{I}_{\vec{a}}$ ist der Kern der Einsetzungsabbildung $s_{\vec{a}} : \mathbb{C}[\vec{x}] \to \mathbb{C}$, die $f(\vec{x})$ auf $f(\vec{a})$ abbildet. Die Abbildung ist surjektiv und $\mathbb{C}$ ist ein Körper. Deswegen ist $\mathcal{I}_{\vec{a}}$ ein maximales Ideal. ($\mathbb{C}[\vec{x}]/\mathcal{I}_{\vec{a}} \cong \mathbb{C}$ und Korollar 10.7.3.)
2. Sei nun $\mathcal{I}$ ein maximales Ideal und $\vec{a} \in V(\mathcal{I})$. Desweiteren sei $g \in \mathcal{I}$. Deswegen ist $g|_{V(\mathcal{I})} \equiv 0$, insbesondere ist $g(\vec{a}) = 0$.

   Wir können g als Taylorentwicklung um $\vec{a}$ schreiben:

$$g(\vec{x}) = g(\vec{a}) + \sum_{k=1}^{\deg g} \sum_{\substack{j_1,\ldots,j_n \\ \sum j_i = k}} \frac{D^{j_1,\ldots,j_n} g(a)}{\prod_{i=1}^n j_i} \prod_{i=1}^n (x_i - a_i)^{j_i}$$

   Hieran erkennen wir, dass $g|_{V(\mathcal{I}_{\vec{a}})} \equiv 0$ ist, da Summanden aus $\mathcal{I}_{\vec{a}}$ sind. Nach der klassischen Form des Hilbertschen Nullstellensatzes gibt es ein m mit $g^m \in \mathcal{I}_{\vec{a}}$.

   Es ist zum einen $g^m(\vec{x}) = g(\vec{a})^m + R(\vec{x})$, wobei $R(\vec{x})$ eine Summe ist, in der jeder Summand mindestens einen der Linearfaktoren $x_i - a_i$ enthält. Zum anderen ist $g^m \in \mathcal{I}_{\vec{a}}$, deswegen ist das Absolutglied $g(\vec{a})^m = 0$, deswegen auch $g(\vec{a}) = 0$ (aber das wussten wir bereits, wegen $g \in \mathcal{I}$ und $\vec{a} \in V(\mathcal{I})$).

   Wir sehen nun an der Taylorentwicklung von g, dass g bereits eine Summe ist, deren Summanden mindestens einen der Linearfaktoren $(x_i - a_i)$ enthalten. Damit ist $g \in \mathcal{I}_{\vec{a}}$. Wir haben gezeigt: $\mathcal{I} \subset \mathcal{I}_{\vec{a}}$. Wegen der Maximalität von $\mathcal{I}$ haben wir $\mathcal{I} = \mathcal{I}_{\vec{a}}$ gezeigt.

Aufgabe 2: Finden Sie mit SAGE alle irreduziblen Polynome vom Grad ≤ 5 in $\mathbb{F}_2[X]$.

```
P.<x> = PolynomialRing( GF(2), 'x')

c=0
for p in P.polynomials(max_degree=5):
    if (not p.is_zero()) and ( not p.is_unit() ) and p.is_irre
        print p
        c+=1
print "Es wurden",c,"irreduzible Polynome in F_2[X]"\
      "gefunden mit Grad <= 5."
# 14 Stueck

# p.is_irreducible?? zeigt, dass SAGE Konstanten als
#  irreduzibel betrachtet
# Im Artin ist "Keine Einheit" neben "ungleich 0" gefordert
```

Aufgabe 3: Es seien $f = x^2 + y^2 - 1$ und $g = y^2 - x^3 - x + 3$ gegeben.

1. Zeigen Sie, dass f und g keine gemeinsamen Nullstellen haben.
2. Finden Sie Polynome u und v, so dass $1 = fu + gv$ gilt.

Es gibt gemeinsame Nullstellen :

```
sage: f
y^2 + x^2 - 1
sage: g
y^2 - x^3 - x + 3
sage: solve([f,g], x,y)
[ [x == 1.150911161731207, y == -0.569733555311020*I], ... ]
```

Deswegen lässt sich der Satz "f und g haben über $\mathbb{C}$ keine gemeinsamen Nullstelle, dann gibt es $u, v \in \mathbb{C}[\vec{x}]$ mit $1 = fu + gv$"nicht anwenden. Die Aufgabe ist falsch gestellt.

Aufgabe 4: Zeigen Sie, dass $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ in $R = \mathbb{Z}[\sqrt{-5}]$ irreduzibel sind.
Hinweis: Beweisen Sie, dass die Abbildung N: $\mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}$, mit $\mathrm{N}(\alpha) = \alpha\bar{\alpha}$ multiplikativ ist.

Wir zeigen zunächst, dass $\mathrm{N}(\cdot)$ multipikativ ist. Es sei $\alpha = a + a'\sqrt{-5}$, dann ist $\mathrm{N}(\alpha) = (a + a'\sqrt{-5})(a - a'\sqrt{-5}) = a^2 + 5a'^2$.

Es sei $\beta = b + b'\sqrt{-5}$, dann ist $\mathrm{N}(\beta) = (b + b'\sqrt{-5})(b - b'\sqrt{-5}) = b^2 + 5b'^2$.

$$\begin{aligned}\mathrm{N}(\alpha\beta) &= (a + a'\sqrt{-5})(a - a'\sqrt{-5})(b + b'\sqrt{-5})(b - b'\sqrt{-5}) \\ &= (a^2 + 5a'^2)(b^2 + 5b'^2) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta)\end{aligned}$$

Es ist $\mathrm{N}(1) = 1$. Für eine Einheit γ gilt nun

$$1 = \mathrm{N}(1) = \mathrm{N}\left(\gamma\gamma^{-1}\right) = \mathrm{N}(\gamma)\,\mathrm{N}\left(\gamma^{-1}\right)$$

Dabei ist $\mathrm{N}(\gamma), \mathrm{N}\left(\gamma^{-1}\right) \in \mathbb{Z}$. Somit ist $\mathrm{N}(\gamma) = \pm 1$.

Um zu zeigen, dass die Zahl δ irreduzibel sind, müssen wir zeigen, dass es keine Darstellung $\delta = uv$ gibt, wobei u, v keine Einheiten sind. Wir zeigen jeweils, dass die Bedingung $\mathrm{N}(\delta) = \mathrm{N}(u)\,\mathrm{N}(v)$ nicht zu erfüllen ist für Nichteinheiten.

Es ist $\mathrm{N}(2) = 4$. Für zwei Nichteinheiten u, v bleibt jeweils nur $\mathrm{N}(u) = u_1^2 + 5u_2^2 = 2$ bzw. $\mathrm{N}(v) = v_1^2 + 5v_2^2 = 2$.

Es ist $\mathrm{N}(u) = u_1^2 + 5u_2^2 = 2$ in $\mathbb{Z}$ nicht lösbar. Damit ist 2 irreduzibel.

Wir zeigen genauso, dass 3 irreduzibel ist: Es ist $\mathrm{N}(3) = 9$. Für zwei Nichteinheiten u, v bleibt jeweils nur $\mathrm{N}(u) = u_1^2 + 5u_2^2 = 3$ bzw. $\mathrm{N}(v) = v_1^2 + 5v_2^2 = 3$. Auch diese Gleichung ist in $\mathbb{Z}$ nicht lösbar.

Wir zeigen genauso, dass $1 + \sqrt{-5}$ irreduzibel ist: Es ist $\mathrm{N}\left(1 + \sqrt{-5}\right) = 6$, das führt auf $\mathrm{N}(u) = 2$ und $\mathrm{N}(v) = 3$, was wiederum nicht lösbar ist, wie wir bereits gesehen haben.

Auch $1 - \sqrt{-5}$ ist irreduzibel, da die Norm ebenfalls 6 ist.

Aufgabe 5:

1. Für welche Primzahlen p ist das Polynom $f = x^2 + x - 1$ in $\mathbb{F}_p[X]$ zerlegbar. Bestimmen Sie die Eigenschaften von p theoretisch.

   Ist f zerlegbar: $f = (x - x_1)(x - x_2)$, so gilt nach der Lösungsformel: $x_i = -1/2 \pm \sqrt{\frac{1}{4} + 1}$, dh. es ist die Wurzel aus $\frac{1}{4} + 1 = \frac{5}{4}$ zu ziehen. Anders ausgedrückt: ist f zerlegbar, so ist 5 ein Quadrat in $\mathbb{F}_p$. Es gibt ein $w \in \mathbb{F}_p$ mit $w^2 \equiv 5 \pmod{p}$.

2. Bestimmen Sie nun mittels Sage, für welche konkreten Primzahlen $p < 100$ f zerlegbar ist.

```
def checkePZ( p):
    R= GF(p)
    P.<x>= PolynomialRing(R, 'x')

    f= x^2+x-1
    F= f.factor()

    if len(F) > 1 or F[0][1] > 1:
        print p
        if not (R(5).is_square() ):
            print "Ausnahme bei",p

for p in prime_range(1,100):
    checkePZ(p)
# keine Ausnahmen
```