Aufgabe 1: Sei R ein Ring, und sei I ein Ideal.

Beweisen Sie die folgenden Aussagen :

1. I ist ein Primideal, g.d.w R/I ein Integritätsring ist.
2. I ist ein maximales Ideal, g.d.w R/I ein Körper ist.
3. Sei R ein Integritätsring. Beweisen Sie, dass der Polynomring $R[x]$ ein Integritätsring ist.

1. Ist $I \neq R$ ein Primideal, so gilt für $a, b \in R$: $ab \in I \Rightarrow (a \in I$ oder $b \in I)$.

   Wir zeigen zunächst, dass R/I ein Integritätsring ist: Dazu müssen wir zeigen, dass es in R/I keine Nullteiler gibt, dass also aus $(a+I)(b+I) = I$ folgt, dass $(a + I)$ oder $(b + I)$ Null sind. In R/I spielt $I = 0 + I$ die Rolle des neutralen Elements der Addition.

   Es ist $(a+I)(b+I) = ab+aI+bI+II = ab+I$. Weil I ein Primideal ist, ist ab nur dann aus I, falls a oder b aus I waren, also kongruent 0 (mod I) in R/I waren. Damit ist R/I nullteilerfrei.

   Wir zeigen nun die anderen Richtung: Es sei R/I ein Integritätsring, also insbesondere nullteilerfrei und $R/I \neq 0$, d.h. $R \neq I$.

   Es folgt aus $(a + I)(b + I) = ab + aI + bI + II = 0 + I$ stets $a \in I$ oder $b \in I$. D.h. aus $ab \in I$ folgt stets $a \in I$ oder $b \in I$. Damit ist I ein Primideal.

2. Wir zeigen zunächst: I ist maximales Ideal $\Rightarrow$ R/I ist ein Körper. (Im Artin haben die Ringe nach Definition bereits eine 1. Und sie sind kommutativ, solange nichts anderes erwähnt wird.) Sei also R ein kommutativer Ring mit 1. (Ohne Kommutativität kommt am Ende ein Schiefkörper raus.)

   Sei I ungleich dem Nullideal $(0)R$ und ungleich R ein maximales Ideal. Wir müssen zeigen, dass alle $a \in R/I, a \neq 0$ invertierbar sind in R/I. $a \neq 0$ bedeutet in R/I, dass $a \neq 0 + I$, also $a \neq I$ ist.

   Sei also $a \in R \setminus I$ beliebig gewählt. Wir betrachten die Menge $M_a := \{i + ar \mid i \in I, r \in R\}$. Wegen $a \in M_a$ ist $M_a \neq I$. Es ist aber $x = i + a0 \in I$ und $\in M_a$ ist. Deswegen gilt $I \subsetneq M_a$.

Wir zeigen nun, dass M_a ein Ideal ist, wegen der Maximalität von I ist dann bereits $M_a = R$. Seien $m_1 := i_1 + ar_1$ und $m_2 := i_2 + ar_2$ Elemente von M_a und $r \in R$. Dann haben wir, weil I ein Ideal ist:

$$\begin{aligned} m_1 + m_2 &= i_1 + ar_1 + i_2 + ar_2 = (i_1 + i_2) + a(r_1 + r_2) \in M_a \\ rm_1 &= r(i_1 + ar_1) = ri_1 + arr_1 \in M_a. \end{aligned}$$

Deswegen ist M_a ein Ideal und wegen der Maximalität von I ist $M_a = R$.

Alle Elemente von R sind aus M_a insbesondere hat $1 \in R$ eine Darstellung der Form $1 = i + ab$ mit $i \in I$ und $b \in R$. Deswegen haben wir

$$\begin{aligned} 1 + I &= (a + I)(b + I) \\ &(= ab + (a + b + I)I) \\ &= ab + I. \end{aligned}$$

Der letzte Summand in der Mitte ist das i von oben.

Damit haben wir gezeigt, dass ein beliebiges $a+I \neq 0$ in R/I invertierbar ist. R/I ist ein Körper.

Nun zeigen wir die umgekehrte Richtung: R/I Körper $\Rightarrow$ I ist ein maximales Ideal von R.

Wir führen die Annahme, dass es ein Ideal J mit $I \subsetneq J \subsetneq R$ zum Widerspruch.

Sei also J ein Ideal mit $I \subsetneq J \subsetneq R$ und $a \in R$ beliebig gewählt. Desweiteren sei $x \in J \setminus I$, dann sei $(y + I) := (x + I)^{-1}(a + I)$.

Dann gilt $(a+I) = (x+I)(y+I)$, woraus $a - xy \in I$ folgt. Wir hatten $I \subset J$ angenommen, deswegen ist auch $a - xy \in J$. Wegen $x \in J$ folgt $a \in J$. Da wir $a \in R$ beliebig gewählt hatten folgt $J = R$. Wir hatten aber $J \subsetneq R$ angenommen. Das ist der gesuchte Widerspruch. Es folgt I ist maximales Ideal.

3. Wir müssen zeigen, dass es keine Nullteiler gibt. Es seien f und g zwei Polynome aus $R[X]$.

   Annahme es seien beide Polynome ungleich dem Nullpolynom. Dann sei m der Grad von f und n der Grad von g. Deswegen sind f_m und g_n die höchsten von Null verschiedenen Koeffizienten von f bzw. g. Das Produkt fg hat als höchsten Summanden den Wert $f_m g_n X^{m+n}$. Ist $fg \equiv 0$,

so müssen alle Koeffizienten Produktes 0 sein. Angefangen beim höchsten. Aus $f_m g_n = 0$ folgt $f_m = 0$ oder $g_n = 0$, da R ein Integritätsbereich ist. Widerspruch zur Annahmen, dass f und g ungleich dem Nullpolynom sind.

Aufgabe 2: Beweisen Sie den folgenden Isomorphismus:

$$\mathbb{Z}[i]/(i+4) \cong \mathbb{Z}/17\mathbb{Z}.$$

(Hinweis : Finden Sie einen Homomorphismus $\varphi : \mathbb{Z}[i] \to \mathbb{Z}/17\mathbb{Z}$, sodass $\varphi(i+4) = \overline{0}$ gilt.)

In $G := \mathbb{Z}[i]$ gilt $i^2 = -1$. In $R := G/(i+4)$ gilt desweiteren $0 = i + 4 \Rightarrow i = -4$. Zusammen ergibt das: in R ist $-1 = (i)^2 = (-4)^2 = 16$, bzw. $17 = 0$.

Wenn wir einen surjektiven Homomorphismus $\varphi : \mathbb{Z} \to R$ finden, dessen Kern $17\mathbb{Z}$ ist, haben wir die Isomorphie gezeigt, da dann $\mathbb{Z}/(17\mathbb{Z})$ isomorph zu R ist.

Um Surjektivität der Abbildung zu zeigen, müssen wir zeigen, dass ein beliebiges $r \in R$, das eine Restklasse von einem $a + bi \in G$ ist auch in dem Bild von φ erscheint. Weil in R stets $-4 = i$ gilt, ist die ganze Zahl $a - 4b = \varphi(a - 4b)$ in derselben Restklassen r.

D.h. Die Restklassen jedes beliebigen Elementes $g = g_1 + g_2 i \in G$ erhalten wir auch als Restklasse der ganzen Zahl $g_1 - 4g_2$. Deswegen ist die Abbildung $\varphi : \mathbb{Z} \to R$ surjektiv, die durch $\varphi(1) = 1_R$ bzw. $\varphi(n \cdot 1) = n \cdot 1_R$ festgelegt ist.

Es folgt eine Wertetabelle für φ:

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$\varphi(n)$	0	1	2	3	-i	1-i	2-i	3-i	-2i	1-2i	2 -2i	3-2i	-3i	1-3i	2-3i	3-3i	-4i	0

Wir bestimmen nun den Kern von φ: ein $n \in \mathbb{Z}$ ist im Kern, falls es ein $\mathbb{Z}[i]$-Vielfaches von $(i+4)$ ist: $n = (a+bi)(i+4) = 4a - b + i(a+4b)$.

Weil $n \in \mathbb{Z}$ ist muss der Imaginärteil 0 sein, also $a = -4b$. Setzt man das ein, so erhalten wir $n = -17b$, also $n \in (17)\mathbb{Z}$. Es folgt, dass $\ker\varphi \subset (17)\mathbb{Z}$. Außerdem sehen wir an der Tabelle, dass ($\varphi(16) = -4i$ ist, wegen $i + 4 = 0 \Leftrightarrow 4 = -i$, folgt, dass $\varphi(16) = -1$, also $\varphi(17) = 0$ ist. Es ist $17 \in \ker\varphi$, deswegen ist $\ker\varphi = (17)\mathbb{Z}$.

Damit haben wir die Isomorphie $R \cong \mathbb{Z}/(\ker\varphi) = \mathbb{Z}/(17\mathbb{Z})$ gezeigt.

Aufgabe 3: Sei R ein Ring, und seien I, J Ideale von R. Es sei $I \cdot J := \{\sum_t a_t b_t \,|\, a_t \in I, b_t \in J\}$, und es sei $I + J := \{a + b \,|\, a \in I, b \in J\}$.

1. Beweisen Sie, dass $I \cdot J$, $I + J$ und $I \cap J$ Ideale von R sind.
2. Für $R = \mathbb{Z}$, $I = 6\mathbb{Z}$, $J = 15\mathbb{Z}$ bestimmen Sie $a, b, c \in \mathbb{Z}$, sodass $I \cdot J = a\mathbb{Z}$, $I + J = b\mathbb{Z}$ und $I \cap J = c\mathbb{Z}$ ist.

1. Wir zeigen zunächst, dass die verschiedenen Mengen Ideale sind.

   a. $I \cdot J$: Es seien $x := \sum a_t b_t$ und $y := \sum a'_t b'_t$ aus $I \cdot J$. Wir zeigen, dass auch $x + y$ aus $I \cdot J$ ist. Es ist $x + y = \sum a_t b_t + \sum a'_t b'_t = \sum a_k b_k$ mit $a_k \in I, b_k \in J$ von der richtigen Form. Desweiteren ist $rx = r \sum a_t b_t = \sum (r a_t) b_t$ aus $I \cdot J$, da I abgeschlossen ist unter Multiplikation, deswegen ist $r a_t \in I$ und rx ist eine Summe von der richtigen Form.

   b. $I + J$: Es seien $x := i_1 + j_1, y := i_2 + j_2 \in I + J$ mit $i_k \in I, j_k \in J$. Dann ist $x + y = (i_1 + i_2) + (j_1 + j_2) \in I + J$. Ebenso ist $rx = r(i_1 + j_1) = r i_1 + r j_1 \in I + J$.

   c. $I \cap J$: Es seien $x, y \in I \cap J$, also $x \in I$ und $x \in J$ und $y \in I$ und $y \in J$. Dann ist zum einen $x + y \in I$ und $\in J$, da sowohl I als auch J unter Addition abgeschlossen sind. Also ist $x + y \in I \cap J$. Ebenso ist rx sowohl in I als auch in J und damit in $I \cap J$.

2. Es sei $R = \mathbb{Z}$, $I = 6\mathbb{Z}$, $J = 15\mathbb{Z}$.

   a. $I \cdot J = (90)\mathbb{Z}$, $a = 90$

   b. $I + J = (3)\mathbb{Z}$, $b = 3$

   c. $I \cap J = (30)\mathbb{Z}$, $c = 30$

Aufgabe 4: Sei $R := \mathbb{F}_2[x]/(g(x))$ ein Restklassenring, wobei $g(x) := x^4 + x^3 + x^2 + 1$ ist. Einen Repräsentanten der Elemente in $\mathbb{F}_2[x]/(g(x))$ kann man als ein Polynom $\sum_{i=0}^{3} a_i x^i$ ($a_i \in \mathbb{F}_2$) schreiben. Implementieren Sie in Sage:

```
def ElementeDesHauptIdeals(f, g):
    r""" Elemente im Hauptdeal (f(x)) (F_2[x] /g)
      INPUT :
          f -- ein Polynom in F_2[x]
5     OUTPUT:
```

```
            Liste der Elemente im Hauptideal (f)R
        EXAMPLE:
            sage: Bits= FiniteField(2)
            sage: P.<x>= PolynomialRing( Bits )
            sage: g = x^4+x^3+x^2+1
            sage: # das R von oben ist hier (P / g)
            sage: ElementeDesHauptIdeals(x^3+1, g)
            sage: # alle Elemente in (x^3 +1 ) (P / g)
            [0, x + 1, x^2 + 1, x^2 + x, x^3 + 1, x^3 + x,
            x^3 + x^2, x^3 + x^2 + x + 1]  """
    R= g.parent()
    elems = []
    # R ist F_2, wir suchen ein Ideal in F_2, das f und g
    # enthaelt, das ist ein Ideal von R/g, das f enthaelt.
    Id=R.ideal( [f, g] )
    for p in R.polynomials( max_degree = g.degree()-1 ):
        if p in Id:
            elems.append( p )
    return elems

Bits= FiniteField(2)
P.<x>= PolynomialRing( Bits )
g = x^4+x^3+x^2+1
# das R von oben ist hier (P / g)
# alle Elemente in (x^3 +1 ) (P / g)
t=ElementeDesHauptIdeals(x^3+1, g)
print t, len(t)
# [ 0, x + 1, x^2 + 1, x^2 + x, x^3 + 1,
#   x^3 + x, x^3 + x^2, x^3 + x^2 + x + 1] 8
```