Aufgabe 1 (Frühjahr 2007)**.** Zeigen Sie:

(a) Ist R ein Hauptidealring, so ist jedes vom Nullideal verschiedene Primideal in R ein maximales Ideal.

(b) Ist R ein Integritätsring und der Polynomring $R[X]$ ein Hauptidealring, so ist R ein Körper.

Lösung. **Zu (a):** Wir zeigen daß jedes „Überideal" eines Primideals schon der ganze Ring sein muß. Also nehmen wir an, daß $P \neq \{0\}$ ein nichttriviales Primideal ist enthalten in einem echt größeren Ideal

$$P \subsetneq I.$$

Da R Hauptidealring ist, gibt es $a, p \in R$ mit

$$I = (a) \quad \text{und} \quad P = (p).$$

Insbesondere ist

$$a \notin (p) = P.$$

Da $(p) \subsetneq (a)$ gibt es $b \in R$ mit

$$p = ab.$$

Da P Primideal ist, und $a \notin P$, ist aber $b \in P = (p)$, das heißt $b = cp$ für ein $c \in R$. Dann ist aber

$$p = ab = acp,$$

nach der Kürzungsregel in Integritätsringen also $1 = ac$. Also ist a eine Einheit, und $I = (a) = R$.

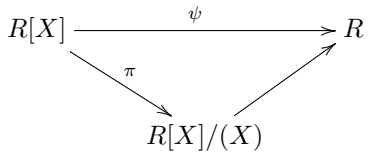
Zu (b): Betrachte den Ringhomomorphismus gegeben durch

$$\psi : R[X] \to R, X \mapsto 0.$$

Es ist $X \in \ker \psi$, also das von X erzeugte Ideal in $\ker \psi$ enthalten,

$$(X) \subset \ker \psi.$$

Nach der universellen Eigenschaft von Faktorringen gibt es also einen eindeutigen Ringhomomorphismus $R[X]/(X) \to R$ so daß das Diagramm



kommutiert. Dieser ist invers zur Abbildung $R \hookrightarrow R[X] \xrightarrow{\psi} R[X]/(X)$ und damit

$$R \cong R[X]/(X).$$

Nun ist nach Voraussetzung $R[X]$ ein Hauptidealring, also nach (a) das Ideal $0 \neq (X)$ maximal. Damit ist $R \cong R[X]/(X)$ ein Körper.

Aufgabe 2 (Herbst 2013)**.** Es sei p eine Primzahl. Man zeige, daß außer 3 jeder Primteiler von $2^p + 1$ gößer als p ist.
Hinweis: Betrachten Sie die multiplikative Ordnung von 2 modulo eines Primteilers von $2^p + 1$.

Lösung. Da $2^p + 1 \equiv 1 \mod 2$ ist, gilt dies auch für alle Teiler. Insbesondere ist 2 kein Primteiler von $2^p + 1$. Für einen Primteiler $q \mid 2^p + 1$ gilt

$$2^p \equiv -1 \mod q$$

und nach Quadrieren erhalten wir

$$2^{2p} \equiv 1 \mod q.$$

Das heißt 2 ist invertierbar in $\mathbb{Z}/q\mathbb{Z}$, $\overline{2} \in \mathbb{Z}/q\mathbb{Z}^\times$, und die Ordnung von 2 in der multiplikativen Gruppe $\mathbb{Z}/q\mathbb{Z}^\times$ teilt $2p$, $\operatorname{ord}(\overline{2}) \mid 2p$. Da $\mathbb{Z}$ faktorieller Ring ist also $\operatorname{ord}(\overline{2}) \in \{1, 2, p, 2p\}$.

- Wäre $\operatorname{ord}(\overline{2}) = 1$, dann wäre
$$2 \equiv 1 \mod q.$$
Dies ist unmöglich, da $q \geqslant 3$.

- Ist $\operatorname{ord}(\overline{2}) = 2$, dann ist
$$2^2 = 4 \equiv 1 \mod q,$$
also $3 \equiv 0 \mod q$. Dies ist nur möglich, wenn $q = 3$.

- Wäre $\operatorname{ord}(\overline{2}) = p$, dann wäre
$$2^p \equiv 1 \mod q.$$
Aber wir haben bereits festgestellt, daß $2^p \equiv -1 \mod q$. Zusammen $1 \equiv -1 \mod q$, was nur möglich ist, wenn $q = 2$, und dies ist ausgeschlossen.

- Damit bleibt $\operatorname{ord}(\overline{2}) = 2p$. Nach dem Satz von Lagrange teil die Ordnung eines Elements die Gruppenordnung, hier also
$$2p = \operatorname{ord}(\overline{2}) \,\big|\, |\,\mathbb{Z}/q\,\mathbb{Z}^\times\,| = q - 1.$$
Wir erhalten die Ungleichung
$$p < 2p \leqslant q - 1 < q.$$

Aufgabe 3 (Frühjahr 2014)**.** Es seien K ein Körper, $K[X]$ der Polynomring über K und m, n nichtnegative ganze Zahlen. Zeigen Sie:
Sei $g = \operatorname{ggT}(m, n)$ in $\mathbb{Z}$, dann ist $X^g - 1$ ein größter gemeinsamer Teiler von $X^m - 1$ und $X^n - 1$ in $K[X]$.

Lösung. Wir zeigen zuerst, daß $h = X^g - 1$ Teiler von $X^m - 1$ und $X^n - 1$ ist. Da g Teiler von m und Teiler von n ist, gibt es $k, l \in \mathbb{Z}$ mit $m = kg$ und $n = lg$. Wir rechnen im Faktorring $K[X]/(h)$. Hier gilt $X^g \equiv 1 \mod (h)$, also

$$\begin{aligned} X^m + (h) &= (X + (h))^m = (X + (h))^{kg} = ((X + (h))^g)^k = (1 + (h))^k = 1 + (h) \\ X^n + (h) &= (X + (h))^n = (X + (h))^{lg} = ((X + (h))^g)^l = (1 + (h))^l = 1 + (h) \end{aligned}$$

Also $X^m \equiv 1 \mod (h)$, dh. $X^m - 1 \equiv 0 \mod (h)$ und $X^n \equiv 1 \mod (h)$, dh. $X^n - 1 \equiv 0 \mod (h)$. In anderen Worten, $X^g - 1 = h \big| X^m - 1$ und $X^g - 1 = h \big| X^n - 1$.
Um zu zeigen, daß $X^g - 1$ ein größter Teiler ist, nehmen wir an, $f \in K[X]$ sei ein weiterer gemeinsamer Teiler von $X^m - 1$ und $X^n - 1$. Wir müssen zeigen, daß dann $f \big| X^g - 1$. Wir rechnen nun im Faktorring $K[X]/(f)$. Da $f \big| X^m - 1$ folgt wie oben $X^m + (f) = 1 + (f)$. Ebenso, da $f \big| X^n - 1$ folgt $X^n + (f) = 1 + (f)$. Nach dem Lemma von Bézout angewandt auf den Ring $\mathbb{Z}$, gibt es $k, l \in \mathbb{Z}$ mit $mk + nl = g$. Es folgt

$$\begin{aligned} X^g + (f) &= (X + (f))^g \\ &= (X + (f))^{mk+nl} \\ &= (X + (f))^{mk}(X + (f))^{nl} \\ &= (1 + (f))^k (1 + (f))^l = 1 + (f) \end{aligned}$$

Also $X^g \equiv 1 \mod (f)$, dh. $X^g - 1 \equiv 0 \mod (f)$, in anderen Worten $f \big| X^g - 1$.

Aufgabe 4 (Frühjahr 2002)**.** Sei $R = \mathbb{Z}[\![T]\!]$ der Ring der formalen Potenzreihen mit Koeffizienten in $\mathbb{Z}$.

(a) Sei $\mathfrak{m} \subset R$ ein maximales Ideal in R. Zeigen Sie: $\mathfrak{m} \cap \mathbb{Z}$ ist ein maximales Ideal in $\mathbb{Z}$.

(b) Bestimmen Sie die Gruppe der Einheiten R^*.

(c) Bestimmen Sie alle maximalen Ideale in R.

Lösung. Wir bearbeiten zuerst (b), da wir das Resultat für die (a) verwenden werden.
Zu (b): Seien $f = \sum_{i \geqslant 0} a_i T^i$ und $g = \sum_{j \geqslant 0} b_j T^j$ Elemente in R. Dann ist

$$fg = \sum_{i \geqslant 0} \sum_{j=0}^{i} a_j b_{i-j} T^i = a_0 b_0 + \sum_{i \geqslant 1} \sum_{j=0}^{i} a_j b_{i-j} T^i.$$

Das Element f ist genau dann invertierbar, wenn es g gibt mit $fg = 1$, also genau dann, wenn

$$a_0 b_0 = 1,$$
$$a_i b_j = 0 \text{ sonst.}$$

Dies ist genau dann der Fall, wenn a_0 (und damit b_0) invertierbar in $\mathbb{Z}$ ist, also $a_0 = \pm 1$, denn die restlichen Gleichungen können dann rekursiv Gelöst werden
Es folgt, daß die Einheiten in R genau die Reihen $f = \sum_{i \geqslant 0} a_i T^i$ sind, mit $a_0 \in \mathbb{Z}^*$, also $a_0 = \pm 1$.

Zu (a): Betrachte den Einsetzungshomomorphismus

$$\sigma_0 : R \to \mathbb{Z}, f \mapsto f(0).$$

Dieser ist offensichtlich surjektiv, also sind Bilder von Idealen wieder Ideale. Insbesondere ist $\sigma_0(\mathfrak{m})$, ein Ideal von $\mathbb{Z}$ also von der Form $\sigma_0(\mathfrak{m}) = d\,\mathbb{Z}$, mit $d \in \mathbb{N}_0$. Das Ideal $\sigma_0(\mathfrak{m})$ sind genau die konstanten Terme der Elemente in $\mathfrak{m}$. Weiterhin gilt, daß $d > 1$:

- Wäre $d = 0$, enthielte $\mathfrak{m}$ nur Potenzreihen ohne konstanten Term $f = \sum_{i \geqslant 1} a_i T^i$, also $\mathfrak{m} = (T)_R$, und dann wäre für ein beliebiges $n \in \mathbb{N}$ das von n und T erzeugte Ideal $\mathfrak{m} \subsetneq (n, T)_R$, und $\mathfrak{m}$ nicht maximal.
- Wäre $d = 1$, also $d\,\mathbb{Z} = \mathbb{Z}$, so gäbe es $f = \sum_{i \geqslant 0} a_i T^i \in \mathbb{Z}[\![T]\!]$ mit $a_0 = \pm 1$. Dann wäre aber f invertierbar, und somit $\mathfrak{m} = R$, Widerspruch.

Das heißt $\{0\} \subsetneq d\,\mathbb{Z} \subsetneq \mathbb{Z}$.
Andererseits ist der Schnitt $\mathfrak{m} \cap \mathbb{Z}$ nach dem ersten Isomorphiesatz ebenfalls ein Ideal von $\mathbb{Z}$. Damit gibt es $\widetilde{d} \in \mathbb{N}_0$ mit $\mathfrak{m} \cap \mathbb{Z} = \widetilde{d}\,\mathbb{Z}$. Es ist klar, daß

$$\widetilde{d}\,\mathbb{Z} = \mathfrak{m} \cap \mathbb{Z} \subset \sigma_0(\mathfrak{m}) = d\,\mathbb{Z}\,.$$

Wir zeigen durch einen Widerspruchsbeweis, daß sogar Gleichheit gilt:
Angenommen

$$\widetilde{d}\,\mathbb{Z} = \mathfrak{m} \cap \mathbb{Z} \subsetneq \sigma_0(\mathfrak{m}) = d\,\mathbb{Z}\,.$$

Dann $d \mid \widetilde{d}$ also $\widetilde{d} = rd$ für ein $r \in \mathbb{Z}$. Für das Ideal in R, das von d und $\mathfrak{m}$ erzeugt wird, würde gelten $\mathfrak{m} \subsetneq (d, \mathfrak{m})_R$, denn

$$\mathfrak{m} \cap \mathbb{Z} = \widetilde{d}\,\mathbb{Z} \subsetneq d\,\mathbb{Z} = (d, \mathfrak{m})_R \cap \mathbb{Z}\,.$$

Andererseits würde auch $(d, \mathfrak{m}) \subsetneq R$ gelten, denn

$$(d, \mathfrak{m})_R \cap \mathbb{Z} = d\,\mathbb{Z} \subsetneq \mathbb{Z} = R \cap \mathbb{Z}\,.$$

Also zusammen

$$\mathfrak{m} \subsetneq (d, \mathfrak{m})_R \subsetneq R$$

in R und damit wäre $\mathfrak{m}$ kein maximales Ideal von R, Widerspruch zur Voraussetzung.
Also gilt

$$\mathfrak{m} \cap \mathbb{Z} = \sigma_0(\mathfrak{m}).$$

Wir zeigen nun, daß d eine Primzahl sein muß: Angenommen d is nicht prim, und p ein Primteiler, also $d = pr$ für $r \in \mathbb{Z}$ keine Einheit. Wie oben zeigt man daß dann

$$\mathfrak{m} \subsetneq (p, \mathfrak{m})_R \subsetneq R$$

wäre, also $\mathfrak{m}$ nicht maximal in R, ein Widerspruch.
Es folgt, daß

$$\mathfrak{m} \cap \mathbb{Z} = p\,\mathbb{Z}$$

für eine Primzahl p. Insbesondere ist dies ein Primideal ungleich (0), und da $\mathbb{Z}$ ein Hauptidealring ist, ist es dann schon maximal.

Zu (c): Aus (a) wissen wir bereits, daß für jedes maximale Ideal $\mathfrak{m}$ in R gelten muß $\mathfrak{m} \cap \mathbb{Z} = p\,\mathbb{Z}$, für eine Primzahl p. Wir haben auch bereits gesehen, daß der konstante Term a_0 jedes Elements $f = \sum_{i \geqslant 0} a_i T^i \in \mathfrak{m}$ ein Vielfaches von p sein muß. f kann also geschrieben werden als $f = pr_0 + T(\sum_{i \geqslant 1} a_i T^{i-1})$. Es folgt $f \in (p,T)_R$, also $\mathfrak{m} \subset (p,T)_R \subsetneq R$. Da $\mathfrak{m}$ aber maximal ist, muß gelten $\mathfrak{m} = (p,T)_R$.

Bemerkung:
In der Tat ist $(p,T)_R$ maximal in R, denn

$$\mathbb{Z}[\![T]\!]/(p,T) \cong (\mathbb{Z}/p\,\mathbb{Z})[\![T]\!]/(T) \cong \mathbb{Z}/p\,\mathbb{Z}\,.$$

Dies ist ein Körper, also ist $(p,T)_R$ maximal.

Aufgabe 5 (??)**.** Für $R = \mathbb{Z}$ und $R = \mathbb{Z}[X]$ untersuche man das durch die Primzahl $2 \in \mathbb{Z}$ erzeugte Hauptideal (2) in R und beweise oder widerlege die folgenden Aussagen:

(a) (2) ist ein Primideal in R.

(b) (2) ist ein maximales Ideal in R.

Lösung. Ist $R = \mathbb{Z}$, so sind die Primideale genau die von Primelementen und der 0 erzeugten Ideale. Also ist insbesondere (2) Primideal. Explizit sieht man dies wie folgt: Es ist $(2) = 2\,\mathbb{Z} \subsetneq \mathbb{Z}$ eine echte Teilmenge. Sei desweiteren $x, y \in \mathbb{Z}$ mit $xy \in (2)$. Also gibt es $m \in \mathbb{Z}$ mit $xy = 2m$. Da $\mathbb{Z}$ faktorieller Ring ist und 2 Primelement in $\mathbb{Z}$ gilt $2 \big| x$ oder $2 \big| y$. Also ist $x \in (2)$ oder $y \in (2)$. Außerdem ist, da $\mathbb{Z}$ ein Hauptidealring ist, jedes Primideal maximal. Speziell ist (2) ein maximales Ideal.
Betrachten wir nun den Fall $R = \mathbb{Z}[X]$. Zu beachten ist, daß dies zwar ein faktorieller Ring aber kein Hauptidealring ist. Das Element 2 ist hier irreduzibel, also prim. Wie oben sieht man dann, daß das davon erzeugte Ideal (2) Primideal ist. Allerdings ist es nicht maximal, denn es ist zum Beispiel in dem Ideal $A = (2, X)$ enthalten.

Aufgabe 6 (??)**.** Sei R ein (unitärer) kommutativer Ring, $\mathfrak{m} \subset R$ ein maximales Ideal. Sei $1+a$ invertierbar für jedes Element $a \in \mathfrak{m}$. Zeigen Sie, daß $\mathfrak{m}$ das einzige maximale Ideal von R ist.

Lösung. Wir zeigen zunächst, daß jedes Element $b \in R \backslash \mathfrak{m}$ invertierbar in R ist. Sei $0 \neq \overline{b} \in R/\mathfrak{m}$ die Klasse von b modulo $\mathfrak{m}$. Da $R/\mathfrak{m}$ ein Körper ist, gibt es $c \in R$ mit $\overline{b}\overline{c} = \overline{1}$. Es folgt, daß es $a \in \mathfrak{m}$ gibt mit $bc = 1 + a$. Da $1 + a$ nach Voraussetzung invertierbar ist, ist $b \cdot (c \cdot (1+a)^{-1}) = 1$, also ist b invertierbar. Angenommen $\mathfrak{n} \subset R$ ist ein weiteres maximales Ideal. Dann gibt es $b \in \mathfrak{n} \backslash (\mathfrak{n} \cap \mathfrak{m})$. Wir haben gesehen, daß b in R invertierbar ist. Also ist $1 = b^{-1} \cdot b \in \mathfrak{n}$, also $\mathfrak{n} = R$, Widerspruch.

Aufgabe 7 (??)**.** Sei R ein Integritätsbereich und $I \subset R$ ein Primideal, so daß der Index $[R : I]$ der additiven Gruppen $(R, +)$ und $(I, +)$ endlich ist. Zeigen Sie, daß I ein maximales Ideal von R ist.

Lösung. Da I ein Primideal ist der Faktorring R/I ein Integritätsbereich. Dieser Faktorring ist die Faktorgruppe R/I der additiven Gruppen mit üblichen Multiplikation. Also ist R/I ein endlicher Integritätsbereich und damit ein Körper. Dies ist äquivalent dazu, daß I ein maximales Ideal ist.