1 Ideale und Unterringe

Sei $R = (R, +, \cdot)$ ein Ring. Um nun nachzuweisen, dass A eine Untergruppe von R ist (bzgl. der Addition) muss man zeigen, dass A nicht leer ist (hier zu weist man am leichtesten nach, dass A die Null 0 enthält), man muss zeigen, dass A unter Addition abgeschlossen ist (also $A + A \subset A$) und dass A unter Inversenbildung abgeschlossen ist.
Achtung: Hiermit ist die Inversebildung bzgl. + gemeint, also $-a$ und nicht a^{-1}.
Alternativ kann man die letzten beiden Bedingungen (also $A + A \subset A$ und $-A \subset A$) auch ersetzen durch die Bedingung: Sind $a, b \in A$, so auch $a - b \in A$. dennoch muss man (immer noch) nachweisen, dass A nicht leer ist.

Um von einer Teilmenge $I \subset R$ nachzuweisen, dass sie ein Ideal ist, muss man nicht zeigen, dass I eine Untergruppe von R ist (wieder bzgl. der Addition), auch wenn I in der Definition als Untergruppe gefordert wird.
es reicht zu zeigen: I ist nicht leer, $I + I \subset I$, $R \cdot I \subset I$ und $I \cdot R \subset I$ (für kommutative Ringe reicht es eine der letzten beiden Eigenschaften nachzuweisen).
Warum genügt es nun nur dies nachzuweisen? Dass I eine Untergruppe ist folgt ganz einfach daraus, das wegen $R \cdot I \subset I$ mit $a \in I$ auch $(-1) \cdot a = -a \in I$ ist, also I unter Inversenbildung abgeschlossen ist.

2 Ringe mit Charakteristik $p > 0$

In einem Ring R mit $\operatorname{char} R = p > 0$ gilt **nicht** notwendig $m^p = m$ für jedes $m \in R$:
Ist K zum Beispiel ein Körper mit 4 Elementen (einen solchen gibt es, typische Aufgabe in einer der Anfängervorlesungen), so ist $K^\times$ eine 3-elementige Gruppe, also zyklisch. Dann kann aber für $a \in K^\times \setminus \{1\}$ nicht $a^2 = a$ gelten.
Es gilt allgemeiner (dies kann man mit Hilfe von Zerfällungskörpern zeigen): Es gibt zu jedem primen p und jedem $n \in \mathbb{N}$ einen Körper K mit p^n Elementen, dieser hat Charakteristik p. Die multiplikative Gruppe eines endlichen Körpers ist zyklisch und somit kann nicht für alle $a \in K$ gelten $a^p = a$.

3 Lösungen

3.1 Aufgabe 1

Seien $I, J \subset R$ zwei Ideale. Wir zeigen, dass auch $I \cap J$ ein Ideal ist: $0 \in I$ und $0 \in J$, weil I und J Ideale sind, also ist der Schnitt nicht leer.
Sind $a, b \in I \cap J$, so sind sie auch in I und J enthalten. Da I und J Ideale sind, ist auch $a + b$ in I und J, also $a + b \in I \cap J$.
Seien $r \in R$ und $a \in I \cap J$, dann ist a in I und $a \in J$. Weil diese Ideale

sind, ist auch $ra \in I$ und ra in J, also $ra \in I \cap J$. Ebenso schließt man, dass $ar \in I \cap J$ gilt. Damit ist $I \cap J$ ein Ideal.

Die Ideale $2\mathbb{Z}$ und $3\mathbb{Z}$ in $\mathbb{Z}$ sind Primideale, der Schnitt $6\mathbb{Z}$ aber nicht.

Die Ideale $2\mathbb{Z}$ und $3\mathbb{Z}$ in $\mathbb{Z}$ sind Primideale, die Summe $\mathbb{Z}$ aber nicht (der ganze Ring ist als Primideal ausgeschlossen). Dass $2\mathbb{Z}+3\mathbb{Z} = \mathbb{Z}$ gilt folgt, weil $1 = 3 - 2 \in 2\mathbb{Z}+3\mathbb{Z}$ also $\mathbb{Z} = (1) \subset 2\mathbb{Z}+3\mathbb{Z}$ (die andere Inklusion ist trivial).

3.2 Aufgabe 2

Sei R ein Integritätsbereich mit $\operatorname{char} R = p > 0$, dann ist p prim. Da p prim ist teilt p aber nicht $k!$ für $k < p$. Nun ist

$$\binom{p}{k} \cdot k! = p \cdot (p-1) \cdots (p-k+1).$$

p teilt aber die rechte Seite. Da p nicht $k!$ teilt muss es $\binom{p}{k}$ teilen, da p prim ist.
Nun gilt für $\varphi : R \to R, a \mapsto a^p$ (weil R insbesondere kommutativ ist):
$\varphi(1) = 1^p = 1$ und $\varphi(ab) = (ab)^p = a^p b^p = \varphi(a)\varphi(b)$ und weil $p \cdot a = 0$ für $a \in R$

$$(a+b)^p = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k} + b^p = a^p + b^p$$

also $\varphi(a+b) = (a+b)^p = a^p + b^p = \varphi(a) + \varphi(b)$.

Die Aussage über $\mathbb{Z}/p\mathbb{Z}$ folgt nun direkt aus dem obigen, denn $m^p = (1 + 1 + \ldots + 1)^p = 1^p + 1^p + \ldots + 1^p = 1 + 1 + \ldots + 1 = m$. (Bemerkung: Hier ist mit 1 die Eins im Ring $\mathbb{Z}/p\mathbb{Z}$ gemeint, nicht die ganze Zahl 1)
Alternativ: Für $m = 0$ gilt offenbar $m^p = 0 = m$. Sei nun $m \neq 0$. $\mathbb{Z}/p\mathbb{Z}$ ist en Körper, also ist $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ eine Gruppe der Ordnung $p-1$. Nun gilt wegen Lagrange (die Ordnung von m teilt $p-1$) die Gleichheit $m^{p-1} = 1$. Multiplikation mit m liefert die Behauptung.

3.3 Aufgabe 3

Sei R ein Hauptidealring. Dann gilt für $a_1, a_2 \ldots, a_n \in R$:
$(a_1, a_2, \ldots, a_n) = R$ genau dann, wenn $T := \{t \in R \mid t \mid a_i, i = 1, 2, \ldots, n\} \subset R^\times$.

Sei $(a_1, a_2, \ldots, a_n) = R$. Sei $t \in T$, also $a_i = tc_i$ für gewisse $c_i \in R$. Es gibt $r_1, \ldots, r_n \in R$ mit $1 = \sum_{i=1}^n r_i a_i = t \cdot \sum_{i=1}^n r_i c_i$, also ist t eine Einheit.

Sei $T \subset R^\times$. Da R ein Hauptidealring ist, gibt es ein $t \in R$ mit $(t) = (a_1, a_2, \ldots, a_n)$. Insbesondere ist $a_i \in (t)$ für alle $i = 1, 2, \ldots, n$, also ist $t \in T \subset R^\times$. Das von einer Einheit erzeugte Ideal ist der Ring selbst, also $(a_1, a_2, \ldots, a_n) = R$.

3.4 Aufgabe 4

Die Menge $M = \{p \in \mathbb{C}[x] : p(0) = p'(0) = 0\} \subset \mathbb{C}[x]$ ist kein Primideal, denn $x \cdot x = x^2 \in M$, aber $x \notin M$.

Der Ring $\mathbb{C}[x, y]$ ist faktoriell, daher ist jedes unzerlegbare Element auch prim. Die von Primelementenerzeugten Ideale sind prim.
Das Polynom $x + y$ ist offenbar unzerlegbar, denn es hat Grad 1. Das Ideal $(x + y)$ ist also ein Primideal.