P.L.Ü) 1 (20,05,22 (6.10.22

Aufgabe 1)

Für ein Ideal $\mathfrak{a} \subset R$ zeige man, dass die Menge aller Elemente $a \in R$, zu denen es ein $n \in \mathbb{N}$ mit $a^n \in \mathfrak{a}$ gibt, ebenfalls wieder ein Ideal in R bildet. Dieses wird mit $\mathrm{rad}(\mathfrak{a})$ bezeichnet und heißt das Nilradikal von $\mathfrak{a}$.

Lösung:

Beachte $\mathfrak{a} \subset \mathrm{rad}(\mathfrak{a})$ & $\mathrm{rad}(\mathfrak{a}) \neq \emptyset$.

Sei nun $a \in \mathrm{rad}(\mathfrak{a})$, d.h. $a^n \in \mathfrak{a}$. Für $r \in R$ gilt dann

$$(ra)^n = r^n \cdot a^n \in \mathfrak{a} \Rightarrow ra \in \mathfrak{a}$$

$$r = -1 \Rightarrow -a \in \mathrm{rad}(\mathfrak{a})$$

Z.z.: $a, b \in \mathrm{rad}(\mathfrak{a}) \Rightarrow a+b \in \mathrm{rad}(\mathfrak{a})$

Bsp.:

$a^2, b^2 \in \mathfrak{a}$

$$(a+b)^2 = a^2 + 2ab + b^2$$
$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

$\Rightarrow (a+b)^3 \in \mathfrak{a}$ aber wegen des Termes $2ab$ lässt sich $(a+b)^2 \in \mathfrak{a}$ noch nicht schließen.

Der Allgemeinfall:

Seien $a, b \in \operatorname{rad} \square$, etwa $a^r, b^s \in \square$. Dann liefert die binomische Formel

$$(a-b)^n = \sum_{i=0}^{n} (-1)^i a^{n-i} \cdot b^i$$

Offenbar $(a-b) \in \operatorname{rad} \square$, sofern für $i = 0, \dots, n$ stets $n-i \geq r$ oder $i \geq s$

$\Rightarrow a^{n-i} \in \square$ oder $b^i \in \square$.

Setzen wir nun $t = \max\{r, s\}$ und wählen $n \geq 2t$, so ergibt sich $n-i \geq r$ & $i \geq s$ für $i \geq t$, und es folgt $a-b \in \operatorname{rad} \square$. $\square$

Aufgabe 2) Man bestimme alle Unterringe von $\mathbb{Q}$.

Lösung:

Jeder Unterring von $\mathbb{Q}$ enthält das Einselement 1 und damit auch sämtliche natürliche Zahlen, wie auch die negativen Zahlen hierzu.

d.h.

$\Longrightarrow$ Jeder Unterring von $\mathbb{Q}$ enthält den Ring der ganzen Zahlen $\mathbb{Z}$.

$\leadsto$ Dies ist der kleinste Unterring von $\mathbb{Q}$.

Sei nun $R \subset \mathbb{Q}$ ein Unterring, der eine rationale Zahl $x \in \mathbb{Q} - \mathbb{Z}$ enthält.

$\Rightarrow x = \frac{a}{b}$ mit $a, b \in \mathbb{Z}$. (den wir als gekürzt annehmen.)

$\Rightarrow ggT(a,b) = 1$

Satz:

Es seien a, b zwei von Null verschiedene Elemente eines Hauptidealrings R. Für den größten gemeinsamen Teiler $d = ggT(a,b)$ gilt dann

$$Ra + Rb = Rd.$$

Insbesondere gibt es eine Gleichung $ra + bs = d$ mit Elementen $r, s \in R$, die notwendig teilerfremd sind, d.h. $ggT(r,s) = 1$ erfüllen

$\Rightarrow ra + sb = 1$ mit $r, s \in \mathbb{Z}$.

$\Rightarrow r \cdot \frac{a}{b} + s = \frac{1}{b}$ und damit $\frac{1}{b} \in R$

! Nun ist offenbar $\mathbb{Z}[\frac{1}{b}]$, definiert als Bild des Einsetzungshomomorphismus

$$\mathbb{Z}[T] \longrightarrow \mathbb{Q}$$
$$T \longmapsto \frac{1}{b}$$

ein Unterring von $\mathbb{Q}$.

! Dieser enthält den Bruch $\frac{a}{b}$ und ist offenbar der kleinste Unterring von $\mathbb{Q}$ mit dieser Eigenschaft

$\Rightarrow \mathbb{Z}[\frac{1}{b}] \subset R$ gilt.

! Ist $d \in \mathbb{Z}$ ein Teiler von $b \Rightarrow 1/d$ ist ein ganzzahliges Vielfaches von $1/b$

$$\Rightarrow \mathbb{Z}[\tfrac{1}{d}] \subset \mathbb{Z}[\tfrac{1}{b}].$$

Hat man sogar $b = d^n$ mit einem Exponenten $n > 0$,

$$\Rightarrow \frac{1}{b} = \left(\frac{1}{d}\right)^n \in \mathbb{Z}[\tfrac{1}{d}] \Rightarrow \mathbb{Z}[\tfrac{1}{d}] = \mathbb{Z}[\tfrac{1}{b}].$$

$\rightsquigarrow$ $b = p_1^{n_1} \cdots p_t^{n_t}$ eine Primfaktorzerlegung von b mit exponenten $n_i > 0$, so gilt

$$\mathbb{Z}[1/b] = \mathbb{Z}\left[\frac{1}{p_1 \cdot \ldots \cdot p_t}\right]$$

! Beachte

- $p_1 \cdots p_t \mid b$ impliziert die Inklusion "$\supset$"

& - $b \mid (p_1 \cdot \ldots \cdot p_t)^e$ für eine geeignete Potenz e die Inklusion "$\subset$".

! Eine unendliche Folge verschiedener Primzahlen $p_1, p_2, \ldots$ führt zu einer aufsteigenden Kette von Unterringen

$$\mathbb{Z}\left[\frac{1}{p_1}\right] \subset \mathbb{Z}\left[\frac{1}{p_1 p_2}\right] \subset \cdots \subset \mathbb{Q},$$

und die Vereinigung aller dieser Ringe ergibt einen Unterring von $\mathbb{Q}$, der offenbar nicht von der Form $\mathbb{Z}[1/b]$ mit $b \in \mathbb{Z}$ ist.

! Z.Z: Es gibt außer den erwähnten Beispielen keine weiteren Unterringe von $\mathbb{Q}$.

! Sei $P \subset \mathbb{N}$ eine Menge von Primzahlen

$$R_P = \left\{ \frac{a}{b} \in \mathbb{Q} ;\ a, b \in \mathbb{Z},\ b \text{ ist Produkt von Primzahlen } p \in P \right\}.$$

$\rightsquigarrow$ ~~R~~ R_p ein Unterring von $\mathbb{Q}$

Behauptung:

R_p ~~&~~ von $R_{p'}$ verschieden ist, wenn die Primzahlmengen P & P' verschieden sind.

Beweis:

Sei p ein Primzahl & $a/b \in \mathbb{Q}$ mit $a, b \in \mathbb{Z}$.

Gibt es eine Gleichung $\frac{1}{p} = a/b$, also $pa = b$, so folgt $p \mid b$ und damit $1/p \notin$ ~~R~~ R_p. Für alle Mengen ~~der~~ von Primzahlen P, die p nicht enthalten.

$\rightsquigarrow P \neq P' \Rightarrow R_p \neq R_{p'}$.

~~Nun~~ Nun ist es z.z., dass es außer den Ringen des Typs R_p keine weiteren Unterringe von $\mathbb{Q}$ gibt.

Sei also R eine Unterring von $\mathbb{Q}$ & sei P die Menge aller Primzahlen p mit $\frac{1}{p} \in R$.

$\Rightarrow R_p \subset R$ ⊛

Behauptung:

⊛ bereits eine Gleichheit ist. Sei $x \in R$ und $x = a/b$ mit $a, b \in \mathbb{Z}$ eine Darstellung als gekürzter Bruch.

$\Rightarrow \frac{1}{b} \in R \Rightarrow \frac{1}{p} \in R$ für alle Primzahlen p, die b teilen.

$\Rightarrow x = \frac{a}{b} \in R_P$ & wir sehen dass $R = R_P$.

$\rightsquigarrow$ Es werden also die Unterringe von $\mathbb{Q}$ in bij. Weise durch die Ringe des Typs R_P parametrisiert, wobei $P \subset \mathbb{N}$ alle Teilmengen durchläuft, die lediglich aus Primzahlen bestehen.

$\rightsquigarrow$ $R_P = \mathbb{Z}$ für $P = \emptyset$ & $R_P = \mathbb{Q}$ für P die Menge aller Primzahlen.

Aufgabe 3)

Man zeige, dass der Polynomring $\mathbb{Z}[T]$ kein Hauptideal-
-ring ist.

Lösung:

Sei p eine Primzahl.
Betrachte

$$\mathfrak{a} = \mathbb{Z}[T]\cdot p + \mathbb{Z}[T]\cdot T = \left\{ \sum_{n\in\mathbb{N}} a_n T^n ;\ a_n \in \mathbb{Z},\ p \mid a_0 \right\}$$

Z.Z.: $\mathfrak{a}$ ist kein Hauptideal.

IA: Wäre $f = \sum_{n\in\mathbb{N}} a_n T^n \in \mathfrak{a}$ ein erzeugendes Element, so würde wegen $p \in \mathfrak{a}$ aus Gradgründen $a_0 \mid p$ & $a_n = 0$ für $n > 0$ folgen. Da $\mathfrak{a}$ nicht das Einheitsideal ist, müsste a_0 zu p assoziiert sein.

Andererseits gibt es aber in $\mathbb{Z}$ keine Gleichung der Form $T = h \cdot p$, so dass $\mathfrak{a}$ kein Hauptideal sein kann.

Frage: Warum besitzt der Körper $\mathbb{Q}$ keinen echten Unterkörper?

Lösung:

Sei $\mathcal{U} \subset \mathbb{Q}$ ein Unterkörper von $\mathbb{Q}$.

$\Rightarrow 1 \in \mathcal{U} \Rightarrow \mathbb{Z} \in \mathcal{U} \Rightarrow \frac{1}{m} \in \mathcal{U}$ für $m \in \mathbb{Z}^*$

$\Rightarrow n/m \in \mathcal{U}$ für $n \in \mathbb{Z}$ & $m \in \mathbb{Z}^* \Rightarrow \mathcal{U} = \mathbb{Q}$

Frage:

Z.Z: R ist ein ~~Integration~~ Integritätionsring

$\Rightarrow R[X]$ ist auch ein Integritätionsring

Lösung:

$f, g \in R[X]$ & nicht-trivial

$\Rightarrow \deg(f \cdot g) = \deg(f) + \deg(g) \geq 0$, also $f \cdot g \neq 0$

$\Rightarrow R[X]$ ist ein Integritätionsring.

Frage:

Wiso ist jeder euklidisch Ring ein Hauptidealring?