Erinnerung:

2.4.4 Proposition: Für jeden Unterring $R' \subset R$ und jede Teilmenge $A \subset R$ existiert ein eindeutiger kleinster Unterring von R, welcher R' und A enthält. Dieser besteht aus den Elementen der Form

$$\sum_{i_1,\ldots,i_n \geqslant 0}{}' \; x_{i_1,\ldots,i_n} a_1^{i_1} \cdots a_n^{i_n}$$

für alle $n \geqslant 0$ und $a_1, \ldots, a_n \in A$ und $x_{i_1,\ldots,i_n} \in R'$, fast alle gleich 0.

2.4.5 Definition: Dieser Unterring heisst *der von A über R' erzeugte Unterring* und wird bezeichnet mit $R'[A]$. Für endlich viele Elemente $a_1, \ldots, a_n \in R$ schreiben wir auch $R'[a_1, \ldots, a_n] := R'[\{a_1, \ldots, a_n\}]$.

2.4.6 Beispiel: Der Unterring $\mathbb{Z}[i] \overset{!}{=} \{a + bi \mid a, b \in \mathbb{Z}\}$ von $\mathbb{C}$.

Es gilt "$\supset$" und die rechte Seite ist ein Unterring. $\Rightarrow$ Gleichheit.

2.4.7 Beispiel: Es ist $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

Bew.: $(a+bi)(c+di) = 1 \Rightarrow |a+bi| \cdot |c+di| = 1. \Rightarrow |a+bi| = 1$

$$|a+bi| = \sqrt{a^2+b^2} = \begin{cases} 0 & \text{falls } a = b = 0 \\ 1 & \text{falls } a+bi \in \{\pm 1, \pm i\} \\ > 1 & \text{sonst.} \end{cases}$$

2.4.8 Beispiel: Der Unterring $\mathbb{Z}[\sqrt{7}\,] = \{a + b\sqrt{7} \mid a, b \in \mathbb{Z}\}$ von $\mathbb{R}$.

2.4.9 Beispiel: Es ist $\mathbb{Z}[\sqrt{7}\,]^\times = \{\pm(8 + 3\sqrt{7})^n \mid n \in \mathbb{Z}\}$.

Bew.: $\forall a,b \in \mathbb{Z}: \quad (a+b\sqrt{7})\cdot(a-b\cdot\sqrt{7}) = a^2-7b^2$

Ist $a+b\sqrt{7}$ eine Einheit, d.h. $\exists c,d\in\mathbb{Z}: (a+b\sqrt{7})\cdot(c+d\sqrt{7}) = 1$

$(a+b\sqrt{7})\cdot(c+d\sqrt{7}) = (ac+bd7) + \underbrace{(ad+bc)}_{=0}\cdot\sqrt{7}$

Dann ist auch $(a-b\sqrt{7})\cdot(c-d\sqrt{7}) = 1$

Also ist auch $a-b\sqrt{7}$ eine Einheit.

Somit auch $(a+b\sqrt{7})\cdot(a-b\sqrt{7}) = a^2-7b^2$ ist Einheit in $\mathbb{Z}[\sqrt{7}]$, d.h. $\exists c,d\in\mathbb{Z}: (a^2-7b^2)(c+d\sqrt{7}) = 1$

$\Rightarrow d=0$ und $(a^2-7b^2)c = 1$

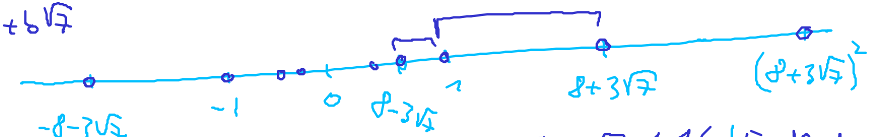
$\Rightarrow a^2-7b^2 \in \mathbb{Z}^\times = \{\pm 1\}$.

$\Rightarrow \quad |a+b\sqrt{7}|\cdot|a-b\sqrt{7}| = 1.$

$(8+3\cdot\sqrt{7})\cdot(8-3\cdot\sqrt{7}) = 64 - 9\cdot 7 = 1. \Rightarrow 8+3\sqrt{7}$ Einheit. $\Rightarrow$ "$\supseteq$".

$|8+3\sqrt{7}| = 8+3\sqrt{7} > 1 \Rightarrow \mathbb{Z}[\sqrt{7}]^\times$ unendlich!

Sei $w \in \mathbb{Z}[\sqrt{7}]^\times$ beliebig, $w = a+b\sqrt{7}$



Ersetze durch $\pm w^{\pm 1} \Rightarrow w \geq 1$

Ersetze durch $w/(8+3\sqrt{7})^k \rightsquigarrow$ OBdA: $1 \leq w < 8+3\sqrt{7} \Rightarrow$

$w = a+b\sqrt{7}, \quad w^{-1} = \pm(a-b\sqrt{7}) \in \,]8-3\sqrt{7}, 1].$

$|a+b\sqrt{7}| \leq 8+3\sqrt{7} < 16$

$|a-b\sqrt{7}| \leq 1$

$\Rightarrow 2a < 17, \quad 2b\sqrt{7} < 17 \Rightarrow a < 8, \quad b < 5$

Endliche Rechnung $\Rightarrow w = 1.$

2.4.10 Beispiel: Der Unterring $\mathbb{Z}[\frac{1}{2}] = \{\frac{a}{2^n} \mid a \in \mathbb{Z},\ n \in \mathbb{Z}^{\geqslant 0}\}$ von $\mathbb{Q}$.

2.4.11 Beispiel: Es ist $\mathbb{Z}[\frac{1}{2}]^\times = \{\pm 2^n \mid n \in \mathbb{Z}\}$.

$$\frac{a}{2^n} \cdot \frac{b}{2^m} = 1 \Leftrightarrow a \cdot b = 2^{n+m} \Rightarrow a \mid 2^{nm} \Rightarrow a = \pm 2^k \text{ für ein } k \in \mathbb{Z}^{\geq 0}.$$

$$\Rightarrow \frac{a}{2^n} = \pm 2^{k-n} \Rightarrow \text{„}\subset\text{"}.$$

„$\supset$" direkt.

2.4.12 Proposition-Definition: Das *kartesische Produkt* von Ringen $R_1 \times \ldots \times R_n$ mit komponentenweiser Addition und Multiplikation sowie dem Nullelement $(0, \ldots, 0)$ und dem Einselement $(1, \ldots, 1)$ ist ein Ring. Für diesen gilt weiter $(R_1 \times \ldots \times R_n)^\times = R_1^\times \times \ldots \times R_n^\times$ und darin $(x_1, \ldots, x_n)^{-1} = (x_1^{-1}, \ldots, x_n^{-1})$.

$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (1, \ldots, 1)$

$\Leftrightarrow a_1 b_1 = 1 \wedge \ldots \wedge a_n b_n = 1.$

2.4.13 Proposition-Definition: Für jeden Ring R und jede Menge X ist die Menge R^X aller Funktionen $f \colon X \to R$ mit punktweiser Addition $(f+g)(x) = f(x) + g(x)$ und Multiplikation $(f \cdot g)(x) = f(x) \cdot g(x)$ sowie den konstanten Funktionen 0 als Nullelement und 1 als Einselement ein Ring.

2.4.14 Bemerkung: Für $R^n = R \times \ldots \times R = R^{\{1,\ldots,n\}}$ stimmen beide Konstruktionen überein.

2.4.15 Bemerkung: Viele interessante Ringe sind Unterringe von Funktionenringen, zum Beispiel die Ringe aller stetigen oder differenzierbaren oder holomorphen Funktionen auf Teilmengen von $\mathbb{R}$ oder $\mathbb{R}^d$ oder $\mathbb{C}$.

2.5 Polynomringe

Erinnerung: Polynome in einer Variablen X

K Körper $\quad K[X] = \left\{ \sum_{i=0}^{\infty}{}' a_i X^i \;\middle|\; \begin{array}{l} \text{alle } a_i \in K \\ \text{fast alle } a_i = 0 \end{array} \right\}.$

$a_0 + a_1 X + \ldots + a_n X^n$

$(a_0, a_1, \ldots) \in K^{(\mathbb{Z}^{\geq 0})}$

2.5.1 Konstruktion: Seien R ein Ring und n eine natürliche Zahl. Sei I_n die Menge aller Tupel $\underline{i} = (i_1, \ldots, i_n)$ in $\mathbb{Z}^{\geqslant 0}$. Betrachte die Menge

$$R_n \;:=\; \big\{(a_{\underline{i}})_{\underline{i}\in I_n} \;\big|\; \text{alle } a_{\underline{i}} \in R \text{ und fast alle } a_{\underline{i}} = 0\big\}.$$

Für zwei Elemente von R_n definieren wir neue Elemente von R_n durch

$$\begin{aligned} (a_{\underline{i}})_{\underline{i}} + (b_{\underline{i}})_{\underline{i}} &:= (a_{\underline{i}} + b_{\underline{i}})_{\underline{i}} \\ (a_{\underline{i}})_{\underline{i}} \cdot (b_{\underline{i}})_{\underline{i}} &:= \Big(\sum\nolimits_{\underline{i}+\underline{j}=\underline{k}} a_{\underline{i}} \cdot b_{\underline{j}}\Big)_{\underline{k}} \end{aligned}$$

kommutativ.

Betrachte weiter die Abbildung

$$\iota\colon\; R \to R_n,\; a \mapsto \left(\begin{cases} a & \text{falls } \underline{i} = (0, \ldots, 0), \\ 0 & \text{sonst,} \end{cases} \right)_{\underline{i}}$$

und bezeichne $0 := \iota(0)$ und $1 := \iota(1)$. Für jedes $1 \leqslant \nu \leqslant n$ sei

$$X_\nu \;:=\; \left(\begin{cases} 1 & \text{falls } \underline{i} = (0, \ldots, 0, \underset{\substack{\uparrow \\ \nu}}{1}, 0, \ldots, 0), \\ 0 & \text{sonst,} \end{cases} \right)_{\underline{i}} \in R_n.$$

Für jedes $\underline{i} \in I_n$ kürzen wir ab

$$\underline{X}^{\underline{i}} \;:=\; \prod_{\nu=1}^{n} X_\nu^{i_\nu}.$$

Für alle $\underline{i}, \underline{j} \in I_n$ gilt dann

$$\underline{X}^{\underline{i}} \cdot \underline{X}^{\underline{j}} \;=\; \underline{X}^{\underline{i}+\underline{j}}.$$

2.5.2 Proposition: (a) $(R_n, +, \cdot, 0, 1)$ ist ein Ring.

(b) ι ist ein injektiver Ringhomomorphismus. Wir identifizieren R mit seinem Bild.

(c) Für jedes Element von R_n gilt

$$(a_{\underline{i}})_{\underline{i}} \;=\; {\sum_{\underline{i}\in I_n}}' a_{\underline{i}} \underline{X}^{\underline{i}}.$$

(d) Jedes Element von R_n hat eine eindeutige Darstellung der Form ${\sum}'_{\underline{i}\in I_n} a_{\underline{i}} \underline{X}^{\underline{i}}$.

Bew (a) $(R_n, +, 0)$ abelsche Gruppe ✓.

Assoziativität: $[(a_{\underline{i}})_{\underline{i}} \cdot (b_{\underline{j}})_{\underline{j}}] \cdot (c_{\underline{k}})_{\underline{k}} = \left(\sum_{\underline{i}+\underline{j}=\underline{l}} a_{\underline{i}} b_{\underline{j}}\right)_{\underline{l}} \cdot (c_{\underline{k}})_{\underline{k}} = \left(\sum_{\underline{l}+\underline{k}=\underline{m}} \left(\sum_{\underline{i}+\underline{j}=\underline{l}} a_{\underline{i}} \cdot b_{\underline{j}}\right) c_{\underline{k}}\right)_{\underline{m}}$

$$\|$$

$(a_{\underline{i}})_{\underline{i}} \cdot [(b_{\underline{j}})_{\underline{j}} \cdot (c_{\underline{k}})_{\underline{k}}]$. $\;\ldots\; = \left(\sum_{\underline{i}+\underline{j}+\underline{k}=\underline{m}} a_{\underline{i}} b_{\underline{j}} \cdot c_{\underline{k}}\right)_{\underline{m}}$

Komm., Distributivität.

Daher können wir die Elemente von R_n mit allen „formalen Ausdrücken" der Form ${\sum}'_{\underline{i}\in I_n} a_{\underline{i}} \underline{X}^{\underline{i}}$ identifizieren, und zwei solche Elemente sind genau dann gleich, wenn ihre Koeffizienten $a_{\underline{i}}$ übereinstimmen. Diese Ausdrücke gehorchen den üblichen Rechenregeln in einem Ring. Einen solchen Ausdruck nennen wir ein *Polynom über R*. Ein Polynom der speziellen Form $a\underline{X}^{\underline{i}}$ mit $a \in R$ heisst ein *Monom*. Je nach Zusammenhang wählt man andere Symbole anstatt X_ν; die aber noch nicht belegt sein dürfen. Das System dieser „neuen Variablen" kürzt man oft mit $\underline{X} = (X_1, \ldots, X_n)$ ab und schreibt den *Polynomring in den Variablen $X_1, \ldots, X_n$ über R* als

$$\boxed{R[\underline{X}] \;:=\; R[X_1, \ldots, X_n] \;:=\; R_n.}$$

$$1 \cdot (a_{\underline{i}})_{\underline{i}} = \left(\begin{cases}1 & \text{falls } \underline{j}=\underline{0}\\ 0 & \text{sonst.}\end{cases}\right)_{\underline{j}} \cdot (a_{\underline{i}})_{\underline{i}} = \left(\sum_{\underline{j}+\underline{i}=\underline{k}} \delta_{\underline{j},\underline{0}} \cdot a_{\underline{i}}\right)_{\underline{k}} = (a_{\underline{k}})_{\underline{k}}$$

(b) ✓

<u>Lemma</u>: $\forall\, \underline{i} \in I_n$: $\underline{X}^{\underline{i}} = \left(\begin{cases}1 & \underline{j}=\underline{i}\\ 0 & \underline{j}\neq\underline{i}\end{cases}\right)_{\underline{j}} = (\delta_{\underline{j},\underline{i}})_{\underline{j}}$.

<u>Beweis</u>: Wenn dies für $\underline{i}$ und $\underline{j}$ gilt, dann ist

$$\underline{X}^{\underline{i}+\underline{j}} = (\delta_{\underline{k},\underline{i}})_{\underline{k}} \cdot (\delta_{\underline{l},\underline{j}})_{\underline{l}} = \Bigg(\underbrace{\sum_{\underline{k}+\underline{l}=\underline{m}} \delta_{\underline{k},\underline{i}} \cdot \delta_{\underline{l},\underline{j}}}_{=\begin{cases}1 & \text{falls } \underline{i}+\underline{j}=\underline{m}\\ 0 & \text{sonst.}\end{cases}}\Bigg)_{\underline{m}} = (\delta_{\underline{m},\underline{i}+\underline{j}})_{\underline{m}}$$

$\Rightarrow$ gilt auch für $\underline{i}+\underline{j}$.

Sie gilt auch für $\underline{i}=(0,\dots,0)$,

und für $\underline{i}=(0,\dots,0,1,0,\dots,0)$. Rest Induktion. qed.

(c)
$$\sum_{\underline{i}\in I_n}{}' a_{\underline{i}}\, \underline{X}^{\underline{i}} = \sum_{\underline{i}} (a_{\underline{i}} \cdot \delta_{\underline{j},\underline{0}})_{\underline{j}} \cdot (\delta_{\underline{k},\underline{i}})_{\underline{k}} = \sum_{\underline{i}} \left(\sum_{\underline{j}+\underline{k}=\underline{l}} a_{\underline{i}} \cdot \delta_{\underline{j},\underline{0}} \cdot \delta_{\underline{k},\underline{i}}\right)_{\underline{l}}$$

$$(a_{\underline{l}})_{\underline{l}} = \left(\sum_{\underline{i}} a_{\underline{i}} \cdot \delta_{\underline{l},\underline{i}}\right)_{\underline{l}} = \sum_{\underline{i}} (a_{\underline{i}} \cdot \delta_{\underline{l},\underline{i}})_{\underline{l}}$$

qed.