UE 320 ► **Übungsaufgabe 5.1.3.2.** (B) Sei D eine ganze Zahl und $R := \mathbb{Z}[\sqrt{D}]$ der von $\mathbb{Z}$ und $\sqrt{D}$ erzeugte Unterring von $\mathbb{C}$. ◄ UE 320

1. Man zeige, dass R mit der gewöhnlichen Addition und Multiplikation von $\mathbb{C}$ einen Integritätsbereich bildet.
2. Man bestimme für $D < 0$ die Einheiten in $\mathcal{R}$.
3. Man zeige, dass für $D = 2$ unendlich viele Einheiten in $\mathbb{Z}[\sqrt{D}] \subseteq \mathbb{R}$ existieren.

1) a) „$(\mathbb{Z}[\sqrt{D}], +, 0, -, \cdot, 1)$ kommutativer Ring mit 1"

a.a) „$(\mathbb{Z}[\sqrt{D}], +, 0, \cdot)$ kommutativer Halbring"

a.a.a) „$(\mathbb{Z}[\sqrt{D}], +, 0)$ kommutativer Monoid"

•) „assoziativ": $(a+b\sqrt{D} + x+y\sqrt{D}) + k+n\sqrt{D} = a+b\sqrt{D} + (x+y\sqrt{D} + k + n\sqrt{D})$

•) „neutr. El." $a+b\sqrt{D}+0 = a+b\sqrt{D} = 0+a+b\sqrt{D}$

•) „kommutativ": $a+b\sqrt{D} + x+y\sqrt{D} = x+y\sqrt{D} + a+b\sqrt{D}$

a.a.b) „$(\mathbb{Z}[\sqrt{D}], \cdot)$ Halbgruppe"

•) „assoz." $((a+b\sqrt{D})(x+y\sqrt{D}))(k+n\sqrt{D}) = (ax+ay\sqrt{D}+bx\sqrt{D}+byD)(k+n\sqrt{D}) =$

$= kax + kay\sqrt{D} + kbx\sqrt{D} + kbyD + anx\sqrt{D} + anyD + bnxD + bnyD\sqrt{D} =$

$= (a+b\sqrt{D})(kx + xn\sqrt{D} + yk\sqrt{D} + nyD) = (a+b\sqrt{D})((x+y\sqrt{D})(k+n\sqrt{D}))$

a.a.c) „Distributivität"

•) $(a+b\sqrt{D})(x+y\sqrt{D} + n + k\sqrt{D}) = (a+b\sqrt{D})((x+n) + (k+y)\sqrt{D}) =$

$= ax + an + ak\sqrt{D} + ay\sqrt{D} + xb\sqrt{D} + nb\sqrt{D} + bkD + byD) =$

$= (ax + ay\sqrt{D} + bx\sqrt{D} + byD) + (an + ak\sqrt{D} + bn\sqrt{D} + bkD) =$

$= (a+b\sqrt{D})(x+y\sqrt{D}) + (a+b\sqrt{D})(n+k\sqrt{D})$ und mit der Kommutativität von $\cdot$ auch Rechtsdistr.

a.a.d) „Kommutativität $\cdot$"

•) $(a+b\sqrt{D})(x+y\sqrt{D}) = ax + ay\sqrt{D} + bx\sqrt{D} + byD = (x+y\sqrt{D})(a+b\sqrt{D})$

a.b) „$(\mathbb{Z}[\sqrt{D}], +, 0, -)$ abelsche Gruppe"

a.b.a) „$(\mathbb{Z}[\sqrt{D}], +, 0)$ kommutatives Monoid" bereits bekannt (von oben)

a.b.a) „ $a+b\sqrt{D} - a - b\sqrt{D} = 0$

a.c) „Einselement"

•) $(a+b\sqrt{D})1 = a+b\sqrt{D}$

b) „$1 \neq 0$" ✓

c) „Nullteilerfreiheit"

ganz allg. gilt in $\mathbb{C}$: $(a+b\sqrt{D})(x+y\sqrt{D}) = 0 \Leftrightarrow (a+b\sqrt{D}) = 0 \vee (x+y\sqrt{D}) = 0$

2) Sei $D<0$

$E(R) := [1]_\sim$, wobei $u \sim v :\Leftrightarrow u \mid v$ und $v \mid u$

$1 \mid a+b\sqrt{D}$ gilt stets

Fall 1: „$a \neq 0 \wedge b \neq 0$"

$(a+b\sqrt{D})(x+y\sqrt{D}) = 1 \Leftrightarrow ax + ay\sqrt{D} + bx\sqrt{D} + byD = 1 \Leftrightarrow$

$\Leftrightarrow ax+byD = 1 \wedge ay\sqrt{D}+bx\sqrt{D}=0 \Leftrightarrow ax+byD=1 \wedge ay+bx=0 \Leftrightarrow ax+byD=1 \wedge y = -\frac{bx}{a}$

also $ax - \frac{b^2x}{a}D = 1 \Leftrightarrow (a-\frac{b^2}{a}D)x = 1 \Leftrightarrow x = (a-\frac{b^2}{a}D)^{-1}$

da $x \in \mathbb{Z}$ gelten muss, verlangen wir $(a-\frac{b^2}{a}D) = \frac{a^2-b^2D}{a} \in \mathbb{Z}\setminus\{0\}^{-1}$, also $a^2-b^2D=1 \Leftrightarrow b^2D = a^2-1 \Leftrightarrow$

$\Leftrightarrow D = \frac{a^2-1}{b^2}$ $\qquad 0 \leq \frac{a^2-1}{b^2} = D < 0$ ↯ also, falls $a\neq 0 \wedge b\neq 0 \Rightarrow a+b\sqrt{D} \not\sim 1$

Fall 2: „$a=0 \wedge b=0$" $\quad 0(x+y\sqrt{D}) = 0 \overset{!}{=} 1$ ↯

Fall 3: „$a\neq 0 \wedge b=0$" $\quad a(x+y\sqrt{D}) = 1 \Leftrightarrow ax + ay\sqrt{D} = 1 \Leftrightarrow ax=1 \wedge ay=0 \Leftrightarrow x=a^{-1} \wedge y=0$

und es muss $x = a^{-1} \in \mathbb{Z}$ gelten, also $a=1 \vee a=-1$

Fall 4: „$a=0 \wedge b\neq 0$"

$b\sqrt{D}(x+y\sqrt{D}) = bx\sqrt{D} + byD \overset{!}{=} 1 \Leftrightarrow bx=0 \wedge byD=1 \Leftrightarrow x=0 \wedge y=\frac{1}{Db}$

und $\frac{1}{Db} \in \mathbb{Z} \Leftrightarrow \exists k\in\mathbb{Z}: Db = \frac{1}{k} \Leftrightarrow kb = \frac{1}{D} \Leftrightarrow b \mid \frac{1}{D}$

Also: $[1]_\sim = \{a+b\sqrt{D} \in \mathbb{Z}[\sqrt{D}] \mid ((a=1 \vee a=-1) \wedge b=0) \vee (a=0 \wedge (b \mid \frac{1}{D}))\}$

3) $(a+b\sqrt{2})(a-b\sqrt{2}) = a^2 - 2b^2 \overset{!}{=} 1 \Leftrightarrow a^2 = 1+b^2 2$

für $a=3$ und $b=2$ ist diese Gleichung erfüllt, also ist

$3+2\sqrt{2}$ eine Einheit und daher auch $\forall n \in \mathbb{N}\setminus\{0\}: (3+2\sqrt{2})^n(3-2\sqrt{2})^n = 1^n = 1$

1. Zeigen Sie, dass die Elemente 2 und 3 in R irreduzibel aber nicht prim sind.

2. Finden Sie eine Primzahl $p \in \mathbb{Z}$, die im Ring $\mathbb{Z}[\sqrt{-5}]$ nicht irreduzibel ist.

Hinweis: Verwenden Sie die Normfunktion N aus 5.1.3 und zeigen Sie, dass genau jene $x \in R$ Einheiten sind, die $N(x) = 1$ erfüllen.

Als Konsequenz dieser Übungsaufgabe werden wir den Ring $\mathbb{Z}[\sqrt{-5}]$ später auch als Beispiel eines nicht faktoriellen Ringes bemühen.

$N: \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}: a+b\sqrt{-5} \mapsto a^2+5b^2$

$N(a+b\sqrt{5}) = 1 \Leftrightarrow a^2+5b^2=1 \Leftrightarrow (b=0 \wedge (a=1 \vee a=-1)) \vee (b \neq 0 \wedge a^2+5b^2=1)$

sei also $b \neq 0$: $a^2+5b^2=1 \Leftrightarrow 5b^2 = 1-a^2 \Leftrightarrow 5 = \frac{1-a^2}{b^2} \leq \frac{1}{b^2} \leq 1$ ↯

also $N(a+b\sqrt{5}) = 1 \Leftrightarrow (b=0 \wedge (a=1 \vee a=-1)) \overset{UE320}{\Leftrightarrow} a+b\sqrt{5} \in E(\mathbb{Z}[\sqrt{-5}])$, denn $\nexists b \in \mathbb{Z}: b \mid -\frac{1}{5}$

1) $2, 3 \in \mathbb{Z}[\sqrt{-5}]$ sind keine Einheiten, sei $x+y\sqrt{-5} \notin E(\mathbb{Z}[\sqrt{-5}])$

Sei $k = (a+b\sqrt{-5})(x+y\sqrt{-5}) \Leftrightarrow a+b\sqrt{-5} = \frac{k}{x+iy\sqrt{5}} = \frac{k(x-iy\sqrt{5})}{x^2+5y^2} = \frac{kx}{x^2+5y^2} + \frac{-y}{x^2+5y^2}\sqrt{-5}$

also $N(a+b\sqrt{-5}) = \frac{k^2x^2}{(x^2+5y^2)^2} + \frac{y^2 5}{(x^2+5y^2)^2} \overset{!}{=} 1 \Leftrightarrow k^2x^2+5y^2 = (x^2+5y^2)^2 \Leftrightarrow$

$\Leftrightarrow k^2x^2+5y^2 = x^4+10x^2y^2+25y^4$

Fall 1: „$x \in \{-1, 1\}$" dann ist $y \neq 0$, da $x+y\sqrt{-5} \notin E(\mathbb{Z}[\sqrt{-5}])$

$k^2+5y^2 = 1+10y^2+25y^4 \Leftrightarrow k^2 = 1+5y^2+25y^4 \geq 31$ ↯ für $k=2$, $k=3$

Fall 2: „$x \notin \{-1, 1\}$" $k^2x^2+5y^2 = x^4+10x^2y^2+25y^4$

also $k^2x^2 - x^4 = 10x^2y^2+25y^4-5y^2 \geq 0 \Rightarrow k^2x^2 \geq x^4 \Leftrightarrow k^2 \geq x^2$

Fall 2.1: „$x=0$": $5y^2 = 25y^4 \Rightarrow y=0 \Rightarrow x+y\sqrt{-5}=0 \Rightarrow k=0$ ↯

Fall 2.2: „$x=2$": $4k^2+5y^2 = 16+40y^2+25y^4$, erfüllt für $k=2 \wedge y=0$

Fall 2.3: „$x=3$" $k^2 9+5y^2 = 81+90y^2+25y^4$, erfüllt für $k=3 \wedge x=0$

Es sind also $2, 3$ irreduzibel

nicht prim: $(a+b\sqrt{-5})(x+y\sqrt{-5}) = ax-5by+(ay+bx)\sqrt{5}$

$a=1, b=1 \leadsto x-5y+(y+x)\sqrt{-5}$

$x=7, y=1 \leadsto 2+8\sqrt{-5} = 2(1+4\sqrt{-5})$ also $2 \mid (1+\sqrt{-5})(7+\sqrt{-5})$

aber $2 \nmid (1+\sqrt{-5})$ und $2 \nmid (7+\sqrt{-5})$

$x=8, y=1 \leadsto 3+9\sqrt{-5} = 3(1+3\sqrt{-5})$ also $3 \mid (1+\sqrt{-5})(8+\sqrt{-5})$,

aber $3 \nmid (1+\sqrt{5})$ und $3 \nmid (8+\sqrt{-5})$

2) $5 = -\sqrt{-5}\sqrt{-5}$, aber $\sqrt{-5}$ ist keine Einheit.

Proposition 5.2.1.2 (Eindeutigkeit der Primelementzerlegung)**.** *Sei $\mathcal{R}$ ein Integritätsbereich, $a \in \mathcal{R} \setminus E(\mathcal{R})$, $a \neq 0$, $a = p_1 \cdots p_r = q_1 \cdots q_s$ mit Primelementen $p_1, \ldots, p_r$ und $q_1, \ldots, q_s$. Dann ist $r = s$, und es gibt eine Permutation π von $\{1, \ldots, r\}$ mit $p_i \sim q_{\pi(i)}$, $i = 1, \ldots, r$. Folglich bedeutet für einen Integritätsbereich Zerlegbarkeit in Primelemente bereits die eindeutige Zerlegbarkeit in Primelemente.*

Beweis. Wegen $p_1 | q_1 \cdot \ldots \cdot q_s$ und weil p_1 prim ist, muss $p_1 | q_j$ für ein geeignetes $j =: \pi(1)$ gelten. Als Primelement ist q_j auch irreduzibel (siehe Proposition 5.1.4.7), folglich muss auch $q_j | p_1$, also $p_1 \sim q_j$ gelten, also $p_1 = q_j e_1$ mit einer geeigneten Einheit e_1. Nach Kürzen von q_j liefert das $e_1 p_2 \cdot \cdots \cdot p_r = q_1 \cdot \ldots \cdot q_{j-1} \cdot q_{j+1} \cdots q_s = q_1 \cdot \ldots \cdot q_{\pi(1)-1} \cdot q_{\pi(1)+1} \cdots q_s$. Durch wiederholte Anwendung dieser Überlegung erhält man schließlich die Behauptung. □

Für irreduzible Elemente gilt, wie man leicht aus Aufgabe 5.1.4.8 ersehen kann, die entsprechende Aussage nicht.

UE 325 ▶ **Übungsaufgabe 5.2.1.3.** (W) Führen Sie das aus. ◀ **UE 325**

•) Betrachte $\mathbb{Z}[\sqrt{-5}]$: $(1-\sqrt{-5})(1+\sqrt{-5}) = 1+5 = 6 = 2 \cdot 3$

$1 \pm \sqrt{-5} = (a + b\sqrt{-5})\underbrace{(x + y\sqrt{-5})}_{\text{Sa} \neq 0} \overset{!}{} \Leftrightarrow \frac{x \pm 5y + (-y \pm x)\sqrt{-5}}{x^2+5y^2} = \frac{(1 \pm \sqrt{-5})(x - y\sqrt{-5})}{x^2+5y^2} = \frac{1 \pm \sqrt{-5}}{x + y\sqrt{-5}} = a + b\sqrt{-5}$

$N(a + b\sqrt{-5}) = \frac{(x \pm 5y)^2 + 5(\pm x - y)^2}{(x^2+5y^2)^2} \overset{!}{=} 1 \Leftrightarrow (x \pm 5y)^2 + 5(\pm x - y)^2 = (x^2+5y^2)^2 \Leftrightarrow$

$\Leftrightarrow x^2 \pm 10xy + 25y^2 + 5(x^2 \mp 2xy + y^2) = x^4 + 10x^2y^2 + 25y^4 \Leftrightarrow$

$\Leftrightarrow 6x^2 + 30y^2 = x^4 + 10x^2y^2 + 25y^4$ für $x=1, y=1$ erfüllt, sonst

$6x^2 + -x^4 = 10x^2y^2 + 25y^4 - 30y^2 \geq 40x^2 + 400 - 120 = 40x^2 + 280$

also $0 \geq x^4 + 36x^2 + 280 > 0$ ↯

es sind daher $1 \pm \sqrt{5}$ tatsächlich irreduzibel (unter Verwendung von UE 324) und

2, 3 sind es nach UE 324 auch.

•) Wir wollen noch zeigen, dass in $\mathbb{Z}[\sqrt{-5}]$ Zerlegbarkeit in irreduzible Elemente gilt.

Sei dazu $(a_n + b_n\sqrt{-5})_{n \in \mathbb{N}}$ eine Folge aus $\mathbb{Z}[\sqrt{-5}]$ mit $\forall n \in \mathbb{N}$: $a_{n+1} + b_{n+1}\sqrt{-5} \mid a_n + b_n\sqrt{-5}$

Also $|(a_{n+1} + b_{n+1}\sqrt{-5})(x_n + y_n\sqrt{-5})| = |a_n + b_n\sqrt{-5}| \Leftrightarrow$

$\Leftrightarrow (a_{n+1}^2 + b_{n+1}^2 5)(x_n^2 + 5y_n^2) = a_n^2 + 5b_n^2 \neq 0$ o.B.d.A.

also $a_{n+1}^2 + 5b_{n+1}^2 \leq \frac{a_n^2+5b_n^2}{x_n^2+5y_n^2} \leq a_n^2 + 5b_n^2$ und falls < gilt, dann $a_{n+1}^2 + 5b_{n+1}^2 < \frac{a_n^2+5b_n^2}{4}$

Wenn also die Teilerkette echt absteigend ist, dann ist $1 < a_n^2 + 5b_n^2 < \frac{a_0^2+5b_0^2}{4^n} \to 0$ ↯

Mit Prop. 5.2.1.6 folgt daraus bereits Zerlegbarkeit in irreduzible Elemente

Algebra TU Wien, SS 2020, Übungsaufgabe 325A

Für $n \in \mathbb{N}$ sei $E_n := \{\frac{k}{2^n} : k \in \mathbb{N}\}$, und $E := \bigcup_n E_n$. Mit der üblichen Addition sind diese Mengen Monoide.

Sei K ein Körper. In 4.2.4 haben wir den Monoidring $K(E)$ definiert, als die Menge aller formalen Summen $\sum_{e\in E} r_e e$, wobei die r_e Elemente von K sind, aber $\{e \in E \mid r_e \neq 0\}$ endlich ist.

Um die Notation an die von den Polynomen bekannte Notation anzugleichen, führen wir eine formale Variable (oder „Unbestimmte") x ein und ersetzen (wie in 4.2.4.4) die Menge E durch die Menge aller formalen Potenzen x^e, $e \in M$. Die Menge $\{x^e \mid e \in E\}$ trägt nun eine multiplikative Struktur: $x^e \cdot x^{e'} := x^{e+e'}$, und die Elemente des Monoidrings $K(E)$ schreiben wir nun als endliche Summen $\sum_{e\in E} r_e x^e$, die wie Polynome aussehen, in denen aber als Exponenten nicht nur natürliche Zahlen erlaubt sind sondern beliebige Elemente von E. Addition und Multiplikation sind wie bei gewöhnlichen Polynomen definiert (siehe 4.2.4.1).

Analog definieren wir $K(E_n)$.

Es gilt der folgende Satz.

1. Für alle $n \in \mathbb{N}$ ist $K(E_n)$ ein Unterring von $K(E_{n+1})$, und von $K(E)$, und $K(E) = \bigcup_{n\in\mathbb{N}} K(E_n)$.
2. Für alle $n \in \mathbb{N}$ gibt es einen Isomorphismus $\varphi_n : K[x] \to K(E_n)$.
   (Hinweis: Wähle φ_{n+1} so, dass $\varphi_{n+1}(x^e) = \varphi_n(x^{2e})$ für alle $e \in E_n$ gilt.)
3. Für alle n und alle $p, q \in K(E_n)$ gilt:[1] $K(E_n) \models p|q$ genau dann, wenn $K(E) \models p|q$.
   Achtung! Das klingt trivial, und ist jedenfalls für Monome auch trivial. Bemühen Sie sich trotzdem, diesen Punkt exakt zu beweisen.
4. Die Einheiten von $K(E_n)$ und von $K(E)$ sind genau die konstanten Polynome. (D.h., die Bilder von konstanten Polynomen unter φ_0.)
5. Für alle $p \in K(E_n)$ gilt:[2]
   $$K(E) \models \ p \text{ ist prim} \quad \Leftrightarrow \ \forall k \geq n: \ K(E_k) \models \ p \text{ ist prim}$$
6. Analog für „irreduzibel" statt „prim".

UE-Aufgabe 325A: Zeigen Sie den gerade formulierten Satz. Schließen Sie daraus, dass in $K(E)$ die irreduziblen Elemente genau die primen Elemente sind. Finden Sie ein echt absteigende Teilerkette in $K(E)$ und folgern Sie, dass $K(E)$ kein faktorieller Ring ist.

(Wenn Ihnen das zu leicht ist: Finden Sie eine echt absteigende Teilerkette, in der alle Elemente einen nichtverschwindenden konstanten Term haben.)

---

[1] Für einen beliebigen Ring R und Elemente $p, q \in R$ schreiben wir $R \models p|q$ für die Aussage „p teilt q in R", das heißt: es gibt ein $r \in R$ mit $p \cdot r = q$. Das Symbol $R \models \ldots$ lesen wir als „In R gilt ..." oder „R glaubt ...".

Analog schreiben wir für $p \in R$ „$R \models p$ prim", wenn weder $p = 0$ noch $R \models p|1$ gilt (also wenn p weder 0 noch Einheit in R ist), und wenn für alle a, b in R die Implikation

$$R \models p|ab \ \Rightarrow \ R \models p|a \ \vee \ R \models p|b$$

gilt, und Analoges vereinbaren wir für andere Begriffe wie Irreduzibilität.
Zum Beispiel gilt zwar $\mathbb{Z} \models (2 \text{ ist prim}) \wedge \neg(2|3)$, aber $\mathbb{Q} \models \neg(2 \text{ ist prim}) \wedge (2|3)$.

[2] Achtung: Im Allgemeinen kann man aus „$K(E_n) \models \ p$ ist prim " nicht schließen, dass p auch in $K(E)$ prim ist.

$E_n := \{\frac{k}{2^n} \mid n \in \mathbb{N}\}$ und $E := \bigcup_{n\in\mathbb{N}} E_n$ sind Monoide und sei K ein Körper

$$K(E) = \{\sum_{e\in E} r_e x^e \mid r_e \in K, \forall^\infty r_e : r_e = 0\}$$

1) „$K(E_n)$ Unterring von $K(E_{n+1})$ und $K(E)$"

•) $\sum_{e\in E_n} r_e x^e + \sum_{e\in E_n} s_e x^e = \sum_{e\in E_n} (r_e + s_e) x^e \in K(E_n)$

•) $\left(\sum_{e_1\in E_n} r_{e_1} x^{e_1}\right)\left(\sum_{e_2\in E_n} s_{e_2} x^{e_2}\right) = \sum_{e\in E_n}\left(\sum_{(e_1,e_2)\in E_n^2 : e_1+e_2=e} r_{e_1} s_{e_1}\right) x^e \in K(E_n)$

außerdem: $K(E_n) \subseteq K(E_{n+1}) \subseteq K(E)$

„$K(E) = \bigcup_{n\in\mathbb{N}} K(E_n)$"

„$\subseteq$" $\sum_{e\in E} r_e x^e \in K(E)$ bel., da nur endl. viele $r_e \neq 0$ sind gilt: $\exists\, l \in \mathbb{N}: \sum_{e\in E} r_e x^e \in K(E_l)$

„$\supseteq$" $\sum_{e\in E_l} r_e x^e \in \bigcup_{n\in\mathbb{N}} K(E_n)$ bel., dann sieht man $\sum_{e\in E_l} r_e x^e \in K(E)$

2) „$\forall n \in \mathbb{N} : \exists \varphi_n : K(E_n) \to K[x] : \varphi_n$ Isomorphismus"

„$n=0$": $E_0 = \mathbb{N}$, also den einfachen Isomorphismus: $\sum_{n\in\mathbb{N}} r_n x^n \mapsto \sum_{n\in\mathbb{N}} r_n x^n$

„$n \to n+1$": Haben wir nun schon einen Isomorphismus $\varphi_n : K(E_n) \to K[x]$

$\forall e \in E_{n+1} : 2e \in E_n$ und $\varphi_{n+1}(x^e) = \varphi_n(x^{2e})$

Die Isomorphie überträgt sich schlicht von φ_n auf φ_{n+1}

exemplarisch: $\varphi_{n+1}(x^{e_1} x^{e_2}) = \varphi_{n+1}(x^{e_1+e_2}) = \varphi_n(x^{2e_1+2e_2}) = \varphi_n(x^{2e_1})\varphi_n(x^{2e_2}) =$
$= \varphi_{n+1}(x^{e_1})\varphi_{n+1}(x^{e_2})$

3) Seien $p, q \in K(E_n)$; z.z.: $K(E_n) \models p \mid q \Leftrightarrow K(E) \models p \mid q$

„$\Rightarrow$" $\exists\, r \in K(E_n) : pr = q$ und $K(E_n) \subseteq K(E)$ also $r \in K(E)$ also $K(E) \models p \mid q$

„$\Leftarrow$" $p = \sum_{e_p\in E_n} p_e x^{e_p}$; $q = \sum_{e_q\in E_n} q_e x^{e_q}$; $\exists\, r = \sum_{e_r\in E} r_e x^{e_r} : pr = q$

$\forall e \in E : q_e = \sum_{(e_p,e_r)\in E_n\times E : e_p+e_r=e} p_e r_e$ wobei wir $q_e = 0$ für $e \notin E_n$ haben

Wir haben also $\frac{k}{2^n} = \frac{l}{2^n} + \frac{j}{2^m} \Leftrightarrow \frac{k-l}{2^n} = \frac{j}{2^m}$ also jedenfalls $\frac{j}{2^m} \in E_n$ wenn wir also $e = \frac{k}{2^n}$ darstellen

und für $e = \frac{k}{2^m} \in E \setminus E_n$ mit $\frac{k}{2^m} = \frac{l}{2^n} + \frac{j}{2^i}$ und $k, j \in 2\mathbb{N}+1$ und $m > n$. Nun muss

sicher auch $i \geq m > n$ gelten, weil $\frac{k}{2^i} \in E_i \setminus E_{i-1}$ und sonst wäre $\frac{k}{2^n} + \frac{j}{2^i} \in E_{\max\{i,n\}}$ ↯

Also können wir $\forall e \in E_n : s_e := r_e$ und $\forall e \in E \setminus E_n : s_e := 0$ und erhalten $ps = q$

4) „Einheiten in $K(E_n)$" Wir suchen also Elemente $p \in K(E_n)$ mit $p \mid 1$ mit

$\exists r \in K(E_n): pr = 1$, also jene p, die eine Inverse besitzen, da $K(E_n) \cong K[x]$ können wir diese Frage in $K[x]$ stellen und aus Prop. 3.3.6.5 Punkt 7 wissen wir bereits, dass es die konstanten Polynome, außer das Nullpolynom sind.

„Einheiten in $K(E)$" Sei $p \in K(E)$ bel. $\exists n \in \mathbb{N}: p \in K(E_n)$ und $p \mid 1$ in $K(E_n) \Leftrightarrow p$ ist konstantes Polynom und aus 3 wissen wir das ist äquivalent zu $p \mid 1$ in $K(E)$

5) z.z.: $\forall p \in K(E_n): K(E) \models p$ ist prim $\Leftrightarrow \forall k \geq n: K(E_k) \models p$ ist prim

„$\Rightarrow$" Es gilt $\forall a,b \in K(E): p \mid ab \Rightarrow p \mid a \vee p \mid b$

Seien nun $a,b \in K(E_n)$ bel. $\Rightarrow a,b \in K(E)$ ✓

„$\Leftarrow$" Gelte nun $\forall k \geq n\ \forall a,b \in K(E_k): p \mid ab \Rightarrow p \mid a \vee p \mid b$

Seien nun $a,b \in K(E)$ mit $p \mid ab$ in $K(E)$

dann gibt es $l \in \mathbb{N}: a,b,p \in K(E_l)$ und mit (3) gilt $p \mid ab$ in $K(E_l)$

dann gilt o.B.d.A $p \mid a$ in $K(E_l)$ und wieder mit (3) $p \mid a$ in $K(E)$

6) „wie (5) mit irreduzibel"

„$\Rightarrow$" Sei also $p \in K(E_n)$ und p irreduzibel in $K(E)$, also

$\forall a,b \in K(E): p = ab \Rightarrow a$ oder b ist eine Einheit, also mit (4) und $K(E_n) \subseteq K(E)$ sind wir fertig

„$\Leftarrow$" Sei nun $\forall k \geq n: \forall a,b \in K(E_k): p = ab \Rightarrow a$ oder b ist Einheit in $K(E_k)$ und mit (4) auch in $K(E)$. Sind nun $a,b \in K(E)$ mit $p = ab$, dann gibt es ein $l \in \mathbb{N}: a,b,p \in K(E_l)$

7) „$p \in K(E)$: prim $\Leftrightarrow$ irreduzibel"

$K[x]$ ist nach Prop. 5.2.3.3 euklidischer Ring und damit auch faktorieller Ring, wegen $K(E_n) \cong K[x]$ ist auch $K(E_n)$ faktorieller Ring und Integritätsbereich

Nach Prop. 5.2.1.8 ist damit p prim $\Leftrightarrow$ p irreduzibel in $K(E_n)$

also p prim in $K(E) \Leftrightarrow \forall n \in \mathbb{N}: p$ prim in $K(E_n) \Leftrightarrow \forall n \in \mathbb{N}\ p$ irreduzibel in $K(E_n) \Leftrightarrow$

$\Leftrightarrow$ p irreduzibel in $K(E)$

8) $x = x^{\frac{1}{2}} x^{\frac{1}{2}} = x^{\frac{1}{4}} x^{\frac{3}{4}} \dots$

also $x^{\frac{1}{2^{n+1}}} \mid x^{\frac{1}{2^n}}$

$x^{\frac{1}{2^n} + \frac{k}{2^m}} = x^{\frac{1}{2^{n+1}}}$, also $\frac{1}{2^n} + \frac{k}{2^m} = \frac{1}{2^{n+1}} \Leftrightarrow k = 2^m \left(\frac{1}{2^{n+1}} - \frac{1}{2^n} \right) < 0$, aber $k \in \mathbb{N}$ ↯

also $x^{\frac{1}{2^n}} \nmid x^{\frac{1}{2^{n+1}}}$, es ist also $(x^{\frac{1}{2^n}})_{n \in \mathbb{N}}$ eine absteigende Teilerkette und

wegen Satz 5.2.1.7 $K(E)$ kein faktorieller Ring

Proposition 5.2.2.4. *Sei R ein Integritätsbereich. Der Polynomring $R[x]$ ist genau dann ein Hauptidealring, wenn R ein Körper ist.*

UE 328 ▶ Übungsaufgabe 5.2.2.5. (W) Beweisen Sie Proposition 5.2.2.4. Hinweis: Betrachten Sie das von a und x erzeugte Ideal, wo $a \neq 0$ eine Nichteinheit von R ist. ◀ **UE 328**

„$\Leftarrow$" Ist R ein Körper so ist nach 5.2.3.3. $R[x]$ ein euklidischer Ring und nach Satz 5.2.3.4 auch ein Hauptidealring.

„$\Rightarrow$" $R[x]$ sei also ein Hauptidealring, wobei R ein Integritätsbereich ist

Ang. R ist kein Körper, also $\exists a \in R: \forall b \in R: ab \neq 1$ dann ist a eine Nichteinheit von R

und wir betrachten $(a, x) = \{pa + qx \mid p, q \in R[x]\}$

Da jedes Ideal ein Hauptideal ist gibt es also $p, q \in R[x]$

$(pa+qx) = (a,x)$ und $\exists\, r \in R[x]: r(pa+qx) = x$, mit

$p = \sum_{i=0}^{n} p_i x^i$ und $r = \sum_{j=0}^{m} r_j x^j$ also $p_0 r_0 a = 0$ also $r_0 = 0$ oder $p_0 = 0$

Fall 1: „$r_0 = 0$" dann gilt $\forall s \in R[x]: s(pa+qx) \neq a$ ↯

Fall 2: „$p_0 = 0$" dann muss bereits $p_1 r_0 a x = x$, also $p_1 r_0 a = 1$ gelten ↯ zu a ist Nichteinheit

UE 331 ▶ Übungsaufgabe 5.2.3.7. (F+) Zeigen Sie, dass sich in euklidischen Ringen der ggT nicht nur von zwei Elementen als deren Linearkombination schreiben lässt, sondern für eine beliebige endliche Anzahl. Beschreiben Sie, wie man diese Darstellung algorithmisch erhalten kann. Wie verhält es sich mit dem ggT unendlich vieler Elemente? **◀ UE 331**

„$n=2$" Hier wissen wir bereits aus Anmerkung 5.3.2.5, dass $\exists x_1, x_2 \in R: ggT(a_1,a_2) = a_1x_1 + a_2x_2$

„$n \rightsquigarrow n+1$" Sei also $n \geq 2$ und sei $b := ggT(a_1,\dots,a_n) = \sum_{i=1}^{n} a_i x_i$ mit $\forall i \in \{1,\dots,n\}: x_i \in R$

Nun können wir $y, y_{n+1} \in R$ finden: $ggT(b, a_{n+1}) = yb + y_{n+1}a_{n+1}$ und erhalten

mit der Definition $\forall i \in \{1,\dots,n\}: y_i := yx_i$ gilt $c := ggT(b, a_{n+1}) = \sum_{i=1}^{n+1} y_i a_i$

Es ist sicher c ein Teiler aller a_i, denn $c \mid a_{n+1}$ und $c \mid b \mid a_i$

Um zu zeigen, dass $c = ggT(a_1,\dots,a_{n+1})$ gilt betrachten wir einen weiteren Teiler t von

$a_1,\dots,a_{n+1}$. Da $t \mid a_1, t \mid a_2, \dots, t \mid a_n$ gilt und $b = ggT(a_1,\dots,a_n)$ gilt auch $t \mid b$

und $t \mid a_{n+1}$ und da $c = ggT(b, a_{n+1})$ gilt $t \mid c$

Algorithmus: $H: R\setminus\{0\} \to \mathbb{N}$ mit $\forall a \in R\setminus\{0\}\ \forall b \in R: \exists q, r \in R: b = aq + r \wedge (r = 0 \vee H(r) < H(a))$

o.B.d.A. $\exists k \in \{1,\dots,n\}: a_k \neq 0$ und o.B.d.A. $\forall i \in \{2,\dots,n\}: a_i \neq 0$, denn $ggT(0,\dots,0)=0$

$$a_1 = a_2 q_{1,1} + r_{1,1} \quad , \quad r_{1,1} = 0 \vee H(r_{1,1}) < H(a_2)$$

falls $r_i \neq 0$: $\quad r_{1,i-1} = r_{1,i}\, q_{1,i+1} + r_{1,i+1}$ mit $r_{1,i+1} = 0 \vee H(r_{1,i+1}) < H(r_{1,i})$

wenn $r_{1,k_1} \neq 0$ und $r_{1,k_1+1} = 0$ dann ist $t_1 := r_{1,k_1} = ggT(a_1, a_2)$

$r_{1,k_1} = r_{1,k_1-2} - r_{1,k_1-1}\, q_{1,k_1} = r_{1,k_1-2} - (r_{1,k_1-3} - r_{1,k_1-2}\, q_{1,k_1-1})\, q_{1,k_1} =$

$= -r_{1,k_1-3}\, q_{1,k_1} + r_{1,k_1-2}\,(1 + q_{1,k_1} q_{1,k_1-1}) = -r_{1,k_1-3}\, q_{1,k_1} + (r_{1,k_1-4} - r_{1,k_1-3}\, q_{1,k_1-2})(1 + q_{1,k_1} q_{1,k_1-1}) =$

$= r_{1,k_1-4}\,(1 + q_{1,k_1} q_{1,k_1-1}) + r_{1,k_1-3}\,(-q_{1,k_1}(1 + q_{1,k_1-1}) - q_{1,k_1-2}) = \dots = a_1x_1 + a_2x_2$ reicht das?

analog: $y(a_1x_1 + a_2x_2) + a_3y_3 = t_2 = a_1x_1y + a_2x_2y + a_3y_3 = a_1y_1 + a_2y_2 + a_3y_3$ u.s.w.

Auch von einer unendlichen Menge $A \subseteq R$ kann nach Prop. 5.2.2.6 der ggT bestimmt werden

Ist A eine abzählbar unendliche Menge, so funktioniert das wegen der Teilerkettenbed. sicher

algorithmisch denn setzt man $t_n := ggT(a_1,\dots,a_n)$ so ist wegen $t_{n+1} \mid t_n$ die Folge

$(t_n)_{n\in\mathbb{N}}$ eine Teilerkette mit $\exists N \in \mathbb{N}.\ \forall k \geq N: t_k \sim t_N$

überabzählbar unendl. Mengen?