Proposition 5.2.3.10. *Der von $\mathbb{Z}$ und der imaginären Einheit i erzeugte Ring $\mathbb{Z}[i] = \{a + ib : \ a, b \in \mathbb{Z}\}$ (genannt der* Ring der ganzen Gauß'schen Zahlen*) ist euklidisch vermittels der euklidischen Bewertung $H(z) := |z|^2$, folglich also auch ein Hauptidealring und faktoriell.*

UE 334 ▶ Übungsaufgabe 5.2.3.11. (B) Beweisen Sie Proposition $\boxed{5.2.3.10}$.

•) Wir wissen bereits von Übungsaufgabe 5.1.3.2, dass $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$ ein Integritätsbereich

mit den Einheiten $\pm i, \pm 1$

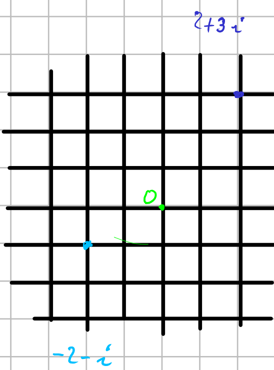
•) Sei $a+ib \in \mathbb{Z}[i]\setminus\{0\}$ bel. und $x+iy \in \mathbb{Z}[i]$ bel.

ges.: $k+il,\ p+iq \in \mathbb{Z}[i]$: $\quad x+iy = (a+ib)(k+il) + p+iq \wedge (p+iq = 0 \vee H(p+iq) < H(a+ib))$

$u+iv := \frac{x+iy}{a+ib} \in \mathbb{C}$

Beh. ein $k+il \in \mathbb{Z}[i]$ mit minimalem $|(u+iv)-(k+il)|^2$, man

muss hier nur $\lceil u \rceil, \lceil v \rceil, \lfloor u \rfloor, \lfloor v \rfloor$ in bel. Kombination betrachten



$|x+iy-(a+ib)(k+il)| \le \underbrace{|x+iy-(a+ib)(u+iv)|}_{=0} + |(a+ib)(u+iv)-(a+ib)(k+il)| =$

$= |a+ib|\underbrace{|(u+iv)-(k+il)|}_{\le \frac{1}{\sqrt{2}}} \le |a+ib|\frac{1}{\sqrt{2}} < |a+ib|$

mit $p+iq := x+iy-(a+ib)(k+il)$ also $|p+iq|^2 < |a+ib|^2$

UE 335 ▶ Übungsaufgabe 5.2.3.12. (B) Begründen Sie folgende Aussagen über den (nach Proposition 5.2.3.10) euklidischen Ring $\mathbb{Z}[i]$. **◀ UE 335**

(1) Für die Einheitengruppe von $\mathbb{Z}[i]$ gilt $E(\mathbb{Z}[i]) = \{1, -1, i, -i\}$.

(2) Ist p prim in $\mathbb{Z}[i]$ und eine natürliche Zahl, so auch eine Primzahl.

(3) Die Umkehrung gilt nicht: Es gibt Primzahlen, die nicht prim in $\mathbb{Z}[i]$ sind.

(4) Lässt sich $p = a^2 + b^2 = (a + ib)(a - ib) \in \mathbb{P}$ als Summe zweier Quadrate positiver ganzer Zahlen a, b darstellen, so sind die Faktoren $a + ib$ und $a - ib$ prim in $\mathbb{Z}[i]$.

(5) Man bestimme alle primen Elemente $z \in \mathbb{Z}[i]$ mit $|z|^2 \leq 10$

(6) Man bestimme in $\mathbb{Z}[i]$ die Primfaktorzerlegungen von $27 + 6i$ und $-3 + 4i$.

(7) Man bestimme in $\mathbb{Z}[i]$ einen ggT der Elemente $a = 7 + i$ und $b = 5$ und stelle ihn in der Form $ax + by$ mit $x, y \in \mathbb{Z}[i]$ dar.

1) Das wissen wir schon aus UE 320 (5.1.3.2)

2) Sei $p \in \mathbb{N} \cap \mathbb{Z}[i]$ und p prim in $\mathbb{Z}[i]$, nach Definition eines Primelementes ist $p \notin \{0, \pm 1, \pm i\}$ Nach dem Fundamentalsatz der Arithmetik können wir p darstellen als $p = \prod_{i=1}^{n} p_i$ mit $p_i \in \mathbb{P}$

Da p in $\mathbb{Z}[i]$ prim ist folgt $p \mid p_1 \vee p \mid \prod_{i=2}^{n} p_i \Rightarrow p \mid p_1 \vee p \mid p_2 \vee p \mid \prod_{i=3}^{n} p_i \Rightarrow \dots$

$\Rightarrow \exists k \in \{1, \dots, n\}: p \mid p_k$ und da p_k Primzahl ist und $p \neq 1$ folgt $p = p_k$ also p Primzahl

3) $(1+i)(1-i) = 2$, also $2 \in \mathbb{P}$ und $2 \mid (1+i)(1-i)$, aber $2 \nmid (1+i) \wedge 2 \nmid (1-i)$

4) Seien $(x+iy), (k+il) \in \mathbb{Z}[i]$, $p \in \mathbb{P}$ mit $a, b \in \mathbb{Z}^+$ und $p = a^2 + b^2 = (a+ib)(a-ib)$ und $(a \pm ib) = (x+iy)(k+il) \Rightarrow p = (x^2+y^2)(k^2+l^2)$

Da p Primzahl ist gilt o.B.d.A. $x^2 + y^2 = p$ und $k^2 + l^2 = 1$

also $k + il \in \{\pm 1, \pm i\} = E(\mathbb{Z}[i])$ nach Definition (5.1.4.4.) ist daher $(a \pm ib)$ irreduzibel, nach UE 334 (5.2.3.11) ist $\mathbb{Z}[i]$ euklidischer Ring, nach Satz 5.2.3.4 ist $\mathbb{Z}[i]$ faktorieller Ring und schließlich ist nach Satz 5.2.1.7 Punkt 3(i) das Element $(a \pm ib)$ als irreduzibles Element schon ein Primelement $a, b \in \mathbb{Z}^+$ nicht benötigt ?

5) Rest auf später verschoben

UE 336 ▸ Übungsaufgabe 5.2.3.13. (W) Zeigen Sie, dass der Ring $K[[x]]$ der formalen Potenzreihen über einem Körper K euklidisch, folglich auch ein Hauptidealring und faktoriell ist. Bestimmen Sie alle irreduziblen Elemente modulo Assoziiertheit und geben Sie sämtliche Ideale durch Erzeugende an, jedes genau einmal. **◂ UE 336**

•) Nach Prop. 3.3.6.5 ist $K[[x]]$ Integritätsbereich

•) $H: K[[x]]\setminus\{0\} \longrightarrow \mathbb{N}: p \mapsto \operatorname{ord}(p)$

•) Sei $a \in K[[x]]\setminus\{0\}$, $b \in K[[x]]$

$k := \operatorname{ord}(b)$ und $l := \operatorname{ord}(a)$, $e_n = (\delta_{in})_{i\in\mathbb{N}}$, $\exists \tilde{b}, \tilde{c} \in K[[x]]: b = e_k \tilde{b}$ und $c = e_l \tilde{a}$

wobei dann $\operatorname{ord}(\tilde{b}) = \operatorname{ord}(\tilde{a}) = 0$ $\qquad \left(\sum_{i=k}^{\infty} b_i x^i = x^k \sum_{i=k}^{\infty} b_i x^{i-k} = x^k \sum_{i=0}^{\infty} b_{k+i} x^i\right)$

Nach Prop. 3.3.6.5 wissen wir nun schon $\tilde{b}, \tilde{a} \in K[[x]]^*$, also $\exists \tilde{b}^{-1}, \tilde{a}^{-1}: \tilde{b}\tilde{b}^{-1} = \tilde{a}\tilde{a}^{-1} = 1$

Fall 1: „$l \leq k$" $\quad q := e_{k-l}\tilde{b}\tilde{a}^{-1} \Rightarrow aq = b$, also $r := 0$ und $b = aq + r$

Fall 2: „$l > k$" $\quad b^{(j)} := (b_0, \dots, b_j, 0, \dots)$, $c := b - b^{(l-1)}$ und $\tilde{c}$ mit $c = e_l \tilde{c}$

$q := \tilde{c}\tilde{a}^{-1} \Rightarrow c = e_l \tilde{a} q = aq$ und $r := c - b = b^{(l-1)}$

also $aq + r = aq + b^{(l-1)} = c + b^{(l-1)} = b$ und $H(r) = \operatorname{ord}(r) = \operatorname{ord}(b^{(l-1)}) \leq l - 1 < l = \operatorname{ord}(a)$

Irreduzible und Ideale fehlen noch!

Proposition 5.3.2.7 (Eisensteinsches Kriterium). *Sei R ein faktorieller Ring. Ist $f = \sum_{i=0}^{n} a_i x^i \in R[x]$ mit Grad ≥ 1 ein primitives Polynom und $p \in R$ irreduzibel mit*

$$p \nmid a_n,\ p \mid a_i \text{ für } i = 0, \dots, n-1, \text{ und } p^2 \nmid a_0,$$

dann ist f irreduzibel in $R[x]$.

UE 342 ▶ **Übungsaufgabe 5.3.2.8.** (W) Beweisen Sie Proposition 5.3.2.7. ◀ UE 342

•) Seien $g = \sum_{i=0}^{m} b_i x^i$, $h = \sum_{i=0}^{\ell} c_i x^i \in R[x]$ mit $\sum_{i=0}^{n} a_i x^i = f = g\,h = \left(\sum_{i=0}^{m} b_i x^i\right)\left(\sum_{i=0}^{\ell} c_i x^i\right)$

$a_0 = b_0 c_0$ und $p \mid a_0 \wedge p$ irreduzibel $\overset{\text{Satz 5.2.1.7 (3)a}}{\Rightarrow} p \mid b_0 c_0 \wedge p$ prim $\Rightarrow p \mid b_0 \vee p \mid c_0$, o.B.d.A: $p \mid b_0$ mit $b_0 = p\tilde{b}_0$

das impliziert $p \nmid c_0$, denn würde $p \mid c_0$, dann gälte auch $p^2 \mid a_0$ ↯ zur Voraussetzung

Als faktorieller Ring ist R definitionsgemäß ein Integritätsbereich und es gilt mit Prop. 3.3.6.5

$1 \leq n = \text{grad } f = \text{grad}(g\,h) = \text{grad}(g) + \text{grad}(h) = \ell + m$

Falls $\ell < m$ ist wollen wir $c_{\ell+1}, \dots, c_m := 0$ setzen und $h = \sum_{i=0}^{m} c_i x^i$ schreiben

Ang. es wäre $m < n$. Gilt nun für ein $0 \leq k \leq m$ bereits für alle $0 \leq i \leq k$, dass $p \mid b_i$, mit $p\tilde{b}_i = b_i$ so unterscheiden wir

Fall 1: „$k = m$", also $p \mid b_m$ und $a_n = b_m c_\ell \Rightarrow p \mid a_n$ ↯ zur Voraussetzung

Fall 2: „$k < m$", dann ist $k+1 \leq m < n$ also $p \mid a_{k+1}$ mit $p\tilde{a}_{k+1} = a_{k+1}$ und $a_{k+1} = \sum_{j=0}^{k+1} b_j c_{k+1-j} \Leftrightarrow$

$\Leftrightarrow a_{k+1} - \sum_{j=0}^{k} b_j c_{k+1-j} = b_{k+1} c_0 \Leftrightarrow p\tilde{a}_{k+1} - \sum_{j=0}^{k} p\tilde{b}_j c_{k+1-j} = b_{k+1} c_0 \Leftrightarrow p\left(\tilde{a}_{k+1} - \sum_{j=0}^{k} \tilde{b}_j c_{k+1-j}\right) = b_{k+1} c_0$

also $p \mid b_{k+1} c_0$ und wir haben bereits $p \nmid c_0$ gesehen also $p \mid b_{k+1}$

Wiederholt man das, so kommt man zu $p \mid b_m$ und Fall 1 also zu einem Widerspruch

In jedem Fall also ein Widerspruch, also muss $m = n$ gelten und damit $n = m + \ell = n + \ell \Leftrightarrow \ell = 0$

also $\sum_{i=0}^{n} a_i x^i = f = h\,g = c_0 \sum_{i=0}^{n} b_i x^i$, also $a_i = c_0 b_i$ und da f primitiv ist,

also die a_i teilerfremd, und $n \geq 1$ gilt $c_0 \in E(R)$ und daher auch $h = c_0 \in E(R[x])$

Proposition 5.3.2.11. *Seien R ein faktorieller Ring, $f \in R[x]$ mit führendem Koeffizienten a_n und konstantem Koeffizienten a_0 und $p, q \in R$ teilerfremd und das Element $\frac{p}{q}$ des Quotientenkörpers Q von R eine Nullstelle von f. Dann gilt $p|a_0$ und $q|a_n$.*

UE 344 ▶ Übungsaufgabe 5.3.2.12. (W) Beweisen Sie Proposition $\boxed{5.3.2.11}$. **◀ UE 344**

•) $f = \sum_{i=0}^{n} a_i x^i$ und $f(\frac{p}{q}) = \sum_{i=0}^{n} a_i \frac{p^i}{q^i} = 0 \iff a_0 = -\sum_{i=1}^{n} a_i \frac{p^i}{q^i} \iff q^n a_0 = -\sum_{i=1}^{n} a_i q^{n-i} p^i =$

$= p \underbrace{\left(-\sum_{i=1}^{n} a_i q^{n-i} p^{i-1}\right)}_{\in R}$ also $p | q^n a_0$. Sei nun $\prod_{i=1}^{n} p_i = p$ eine Zerlegung von p in Primelemente

Dann gilt auch $\forall j \in \{1, \dots, n\}$: $p_j | q^n a_0$ und da p_j prim ist gilt $p_j | q^n \vee p_j | a_0$ und da p und q teilerfremd sind gilt $p_j \nmid q$ also $p_j \nmid q^n$ und daher $p_j | a_0$, also kommt p_j in der eindeutigen Zerlegung in irreduzible Elemente von a_0 vor, da j bel. war gilt also $p | a_0$

•) $f(\frac{p}{q}) = \sum_{i=0}^{n} a_i p^i q^{n-i+n} = 0 \iff \sum_{i=0}^{n} a_i p^i q^{n-i} = 0 \iff p^n a_n = -\sum_{i=0}^{n-1} a_i p^i q^{n-i} = q\left(-\sum_{i=0}^{n-1} a_i p^i q^{n-i-1}\right)$

also $q | p^n a_n$. Analog wie im vorigen Punkt folgt $q | a_n$

Proposition 5.3.3.7. *Ein Polynom f über einem Körper K vom Grad 2 oder 3 ist genau dann irreduzibel, wenn f in K keine Nullstelle hat.*

UE 346 ► Übungsaufgabe 5.3.3.8. (F) Beweisen Sie Proposition 5.3.3.7 ◄ **UE 346**

Sei $f = \sum_{i=0}^{3} a_i x^i$.

„$\Rightarrow$" Kontraposition: hat f eine Nullstelle β, also $f(\beta) = \sum_{i=0}^{3} a_i \beta^i = 0$, dann gibt es nach Prop. 5.3.3.2 ein Polynom $q \in K[x]$ mit $f(x) = q(x)(x-\beta)$ und $\mathrm{grad}(q) = 2$, $\mathrm{grad}(x-\beta) = 1$ und da sicher $x - \beta \neq 1$ und $q \neq 1$, weil der Grad nicht übereinstimmen kann, sind $x-\beta, q \notin E(K[x])$ also ist f nicht irreduzibel

„$\Leftarrow$" Kontraposition: Ist f nicht irreduzibel so gibt es eine Zerlegung $f = pq$ mit p, q keine Einheiten, wäre $\mathrm{grad}\, p = 0$ so wäre $p = a_0 \in K$ also $a_0 a_0^{-1} = 1$ und daher p eine Einheit ↯ also $\mathrm{grad}(p), \mathrm{grad}(q) > 0$ und $\mathrm{grad}\, p + \mathrm{grad}\, q = \mathrm{grad}\, f$ und da $\mathrm{grad}\, f = 2$ oder $\mathrm{grad}\, f = 3$ gilt ist o.B.d.A. $\mathrm{grad}(p) = 1$ also $p(x) = x - \beta$ Nach Prop. 5.3.3.1. gilt daher $f(\beta) = 0$ also hat f eine Nullstelle