Folgerung aus Definition A.113: Teilbarkeit in $\mathcal{R}[x]$

(i) Offenbar folgt aus der Zerlegung $a(x) = q(x) * b(x) + r(x)$ dass

$$b(x)|a(x) \iff r(x) = 0$$

so dass wir in $\mathcal{R}[x]$ einen konstruktiven Teilbarkeitstest haben.

(ii) Wie im Ring der ganzen Zahlen folgt die Existenz des grössten gemeinsamen Teilers $c(x) = GGT(a(x), b(x))$, welcher allerdings nur bis auf die Multiplikation mit einer Konstanten eindeutig ist. O.B.d.A. können wir verlangen, dass der höchste Koeffizient $c_{deg(c(x))}$ von $c(x)$ zu $1\mathcal{R}$ normalisiert wird.

(iii) Die Berechnung des $GGT(a(x), b(x))$ erfolgt wiederum durch den Euklidischen Algorithmus.

(iv) Falls $deg(GGT(a(x), b(x))) = 1$ und somit nach Normalisierung $GGT(a(x), b(x)) = 1$, so heissen $a(x)$ und $b(x)$ **relativ prim zueinander** bzw **teilerfremd**.

A - 13 Faktorisierung und Nullstellen

Korollar A.117

(i) *Ein Körperelement $x_0 \in \mathcal{R}$ ist genau dann eine* **Wurzel** *eines Polynoms $a(x) \in \mathcal{R}[x]$ mit $n = deg(a(x)) > 0$, wenn es ein $q(x) \in \mathcal{R}[x]$ gibt, so dass gilt*

$$a(x) = (x - x_0) * q(x)\,.$$

(ii) *Man nennt $(x - x_0)$ einen* **Linearfaktor** *von $a(x)$ und es muss gelten*

$$deg(q(x)) = n - 1$$

(iii) *Die Koeffizienten q_i des Polynomes $q(x)$ ergeben sich aus $q_{n-1} = a_n$ gemäss dem Hornerschema als*

$$q_{i-1} = a_i + q_i * x_0 \quad \textit{für} \quad i = n - 1 \ldots 1$$

Folgerung

Durch wiederholtes Abspalten von Linearfaktoren erhält man eine Darstellung der Form

$$a(x) = (x - x_1)(x - x_2) \cdots (x - x_k)q(x)\,,$$

wobei $q(x)$ keine weiteren Nullstellen besitzt oder identisch gleich null ist. Im letzteren Fall ist auch $a(x)$ identisch gleich null.

Es kann durchaus vorkommen, dass derselbe Linearfaktor wiederholt abgespalten wird, man spricht dann von einer **mehrfachen Nullstelle**.

Folgerung

Da immer

$$n = deg(a(x)) = k + deg(q(x)) \geq k\,,$$

kann ein Polynom vom Grad n also höchstens n Nullstellen haben oder es verschwindet identisch. Damit ist auch Satz A.105(iii) bewiesen, da dort durch die Interpolationsbedingung $n + 1$ unterschiedliche Nullstellen verlangt werden.

Folgerung

Ein Polynom $a(x)$ kann also nur irreduzibel sein, wenn $deg(a(x)) = 1$ gilt. Damit ist $a(x)$ also selbst ein Linearfaktor oder besitzt keine Nullstellen im Koeffizientenkörper.

Falls ein Polynom vom Grad $deg(a(x)) = n > 0$ auch n Nullstellen

$$x_i \in \mathcal{R} \quad \text{für} \quad i = 1 \dots n$$

besitzt, so gibt es für $a(x)$ eine eindeutige Faktorisierung

$$a(x) = c_n(x - x_1)(x - x_2) \cdots (x - x_n)$$

Auch in dieser Form kann es mit einem Aufwand von n Multiplikatonen ausgewertet werden.

Beispiel A.118

$x^3 - 1$ hat genau eine Nullstelle $x_o = 1$ in $\mathcal{R} = \mathbb{R}$, da nach Abspaltung des Linearfaktors $(x - 1)$ das Polynom

$$x^2 + x + 1 = (x + \tfrac{1}{2})^2 + \tfrac{3}{4} \geq \tfrac{3}{4}$$

übrig bleibt. Wäre es reduzibel, müsste es das Produkt von zwei linearen Faktoren der Form $(x - x_1)$ und $(x - x_2)$ mit $x_1, x_2 \in \mathbb{R}$ sein und damit für $x \in \{x_1, x_2\} \subset \mathbb{R}$ verschwinden, was der obigen Ungleichung widerspricht.

Bemerkung:

Es lässt sich zeigen, dass ein nichtkonstantens Polynom $q(x) \in \mathbb{R}[x]$, das keine Nullstellen besitzt, sich immer als Produkt quadratischer Polynome $q_j(x)$ mit $deg(q_j(x)) = 2$ darstellen lässt.

Mit anderen Worten:

> *$p(x)$ ist genau dann irreduzibel in $\mathbb{R}[x]$, wenn es ein quadratisches Polynom ohne reelle Nullstelle ist.*

Bemerkung:

Erweitert man $\mathbb{R}$ zu den komplexen Zahlen $\mathbb{C}$, so haben auch diese quadratische Polynome und man erhält immer eine vollständige Zerlegung

$$a(x) = a_n(x - x_1)(x - x_2) \cdots (x - x_n),$$

wobei $n = deg(a(x))$ ist. Dabei müssen die Nullstellen $x_j \in \mathbb{C}$ nicht alle verschieden sein.

Diese Aussage nennt man **Fundamentalsatz der Algebra**.

Komplexe Wurzeln spielen eine wesentliche Rolle als Eigenwerte von nicht symmetrischen Matrizen. Diese treten bei der Analyse dynamischer (d.h. zeitabhängiger) Systeme auf.

A - 14 Die komplexen Zahlen

Definition A.119 (Komplexe Zahlen)

(i) Die beiden Wurzeln des Polynoms

$$P(x) = x^2 + 1$$

(und damit die Lösungen der Gleichung $x^2 + 1 = 0$) werden mit $\mathbf{i}$ und $-\mathbf{i}$ bezeichnet, es gilt also

$$\mathbf{i}^2 = -\mathbf{1}.$$

(ii) Ausdrücke der Form $z = x + iy$ mit $(x, y) \in \mathbb{R}^2$ nennt man **komplexe Zahlen** mit

$Re(z) = x$ **Realteil**
$Im(z) = y$ **Imaginärteil**

(iii) Die Menge der komplexen Zahlen wird mit $\mathbb{C}$ bezeichnet.

Definition A.120 (Addition und Multiplikation in $\mathbb{C}$)

Für Addition und Multiplikation zweier komplexer Zahlen $z_1 = x_1 + iy_1$ und $z_2 = x_2 + iy_2$ gilt

$$\begin{aligned} z_1 + z_2 &= (x_1 + x_2) + i(y_1 + y_2) \\ z_1 * z_2 &= (x_1 * x_2 - y_1 * y_2) + i(x_1 * y_2 + x_2 * y_1) \end{aligned}$$

Lemma A.121 (Körpereigenschaft von $\mathbb{C}$)

Bezüglich der oben definierten Verknüpfungen + und $*$ bildet $\mathbb{C}$ einen kommutativen Körper mit folgenden Eigenschaften:

(i) $0 = 0 + i * 0$ **Nullelement**
(ii) $1 = 1 + i * 0$ **Einselement**
(iii) $-(x + iy) = -x + i(-y)$ **Inverses bzgl. +**
(iv) $(x + iy)^{-1} = (x - iy)/(x^2 + y^2)$, **Inverses bzgl. $*$**
wobei z^{-1} nur für $z \neq 0$ existiert.

Lemma A.122 (Lösung einer quadratischen Gleichung)

Das Polynom

$$P(x) = \alpha x^2 + \beta x + \gamma \qquad \textit{mit} \quad \alpha, \beta, \gamma \in \mathbb{R}$$

hat im Falle $\gamma\alpha > \frac{1}{4}\beta^2$ die komplexen Wurzeln

$$x_{0,1} = -\frac{1}{2}\frac{\beta}{\alpha}\left[1 \pm i\sqrt{4\alpha\gamma/\beta^2 - 1}\right]$$