Euklidischer Algorithmus

31.5.2021

Sei $R = K[x]$ oder $\mathbb{Z}$.

Gegeben $f, g \in R$, finde $d = \operatorname{ggT}(f, g) \in R$ und Bézout-Koeffizienten $\alpha, \beta \in R$: $d = \alpha f + \beta g$.

<u>Algorithmus</u>: Ohne Einschränkung $\deg f \geq \deg g$
($|f| \geq |g|$ für $R = \mathbb{Z}$)

Schreibe $f_0 = f$, $f_1 = g$.

Für $n \in \mathbb{N}_0$, schreibe
$$f_n = \overset{\text{Quotient}}{a_n} f_{n+1} + \overset{\text{Rest}}{f_{n+2}} \qquad (*)$$
(Division mit Rest "$f_n : f_{n+1}$", Polynomdivision.)

Falls $f_{n+2} = 0$ (d.h. kein Rest), Abbruch des Verfahrens.

Dann: $f_{n+1} \mid f_n \implies f_{n+1} \mid (a_{n-1} f_n + f_{n+1}) = f_{n-1}$
$\implies \dots$
$\implies f_{n+1} \mid f_1 \implies f_{n+1} \mid f_0$.

Es gilt sogar: $\operatorname{ggT}(f, g) = f_{n+1}$. Die Bézout-Koeffizienten findet man durch Rücksubstitution von f_{n+1} in die Gleichungen $(*)$.

Beispiel: $d = \operatorname{ggT}(\underbrace{x^3 + x^2 + x + 1}_{f_0}, \underbrace{x^2 - x + 1}_{f_1})$ über $\mathbb{F}_3[x]$.

$$\begin{array}{l}
x^3 + x^2 + x + 1 \\
-(x^3 - x^2 + x) \\
\hline
\phantom{-(x^3 -{}} 2x^2 + 1 \\
-(2x^2 - 2x + 2) \\
\hline
\phantom{-(2x^2 -{}} 2x - 1
\end{array}
\qquad = (x^2 - x + 1)(x + 2) + \underbrace{2x - 1}_{f_2}$$

$$
\begin{array}{r}
x^2 - x + 1 \\
-(x^2 - 2x) \\
\hline
x + 1 \\
-(x - 2) \\
\hline
0
\end{array}
\qquad \overset{3=0}{=} \quad \underbrace{(2x - 1)}_{r_2}(2x + 2) \quad + \quad \underbrace{0}
$$

$\Rightarrow$ Abbruch des Verfahrens.

$2x - 1 = d.$

Bézout-Koeffizienten: $\quad 2x - 1 = -(x+2)(x^2 - x + 1) + 1 \cdot (x^3 + x^2 + x + 1)$