Wiederholung:

Satz 3.2: Seien $A, B, C \in \mathbb{C}[X]$ teilerfremd mit $A + B = C$
und $\mathrm{Grad}(C) = \max(\mathrm{Grad}(A), \mathrm{Grad}(B)) \geq 1$

Dann gilt $\mathrm{Grad}(C) < \mathrm{Grad}\left(\prod_{\substack{P \in I \\ P \mid ABC}} P\right)$

Lemma 3.3: Ein Polynom $f \in \mathbb{C}[X]$ hat eine Nullstelle α mit Vielfachheit $k \geq 1$ $\Leftrightarrow$ α ist eine Nullstelle von f' mit Vielfachheit $k-1$

Lemma 3.4: Sei $f \in \mathbb{C}[X]$. Dann ist
$\mathrm{Grad}(\mathrm{ggT}(f, f')) = \mathrm{Grad}(f) - N_0(f)$

Beweis von Lemma 3.3:

Eine Nullstelle α von f hat Vielfachheit $k \geq 1$

$\Leftrightarrow$ $f(X) = (X-\alpha)^k g(X)$ mit $g(X) \in \mathbb{C}[X]$ und $g(\alpha) \neq 0$

$\Leftrightarrow$ $f'(X) = k(X-\alpha)^{k-1} g(X) + (X-\alpha)^k g'(X)$
$= (X-\alpha)^{k-1}\left(k g(X) + (X-\alpha) g'(X)\right)$
$= (X-\alpha)^{k-1} h(X)$

Es gilt $h(\alpha) = k g(\alpha) + 0 \neq 0$

also ist α eine Nullstelle von f' mit Vielfachheit $k-1$. □

Bemerkung: Hier verstehen wir „Nullstelle mit Vielfachheit 0" als „keine Nullstelle".

Beweis von Lemma 3.4: Sei $m := N_0(f)$

und $f(X) = c\,(X-\alpha_1)^{k_1}(X-\alpha_2)^{k_2}\cdots(X-\alpha_m)^{k_m}$ $\quad (c \in \mathbb{C})$

Nach Lemma 3.3 ist

$$ggT(f,f') = (X-\alpha_1)^{k_1-1}(X-\alpha_2)^{k_2-1}\cdots(X-\alpha_m)^{k_m-1}$$

und so gilt

$$\begin{aligned}\mathrm{Grad}\left(ggT(f,f')\right) &= (k_1-1)+(k_2-1)+\cdots+(k_m-1)\\ &= (k_1+k_2+\cdots+k_m)-m\\ &= \mathrm{Grad}(f) - N_0(f)\end{aligned}$$

□

Satz 3.2 folgt direkt aus dem folgenden Satz.

Satz 3.5: Seien $A, B, C \in \mathbb{C}[X]$ teilerfremd, nicht alle konstant und mit $A+B=C$

Dann gilt

$$\max\left(\mathrm{Grad}(A), \mathrm{Grad}(B), \mathrm{Grad}(C)\right) \leq N_0(ABC) - 1.$$

Beweis: $A+B=C$

$$\Rightarrow A'+B'=C'$$

$$\begin{aligned}\Rightarrow A'B - AB' &= A'(C-A) - A(C'-A')\\ &= A'C - AC' \qquad (1)\end{aligned}$$

Wären A und B beide konstant, so wäre C auch konstant ↯

also o.B.d.A. ist B nicht konstant.

wäre $A'B - AB' = 0$, dann wäre $A'B = AB'$, und wegen der Teilerfremdheit von A, B, auch $B \mid B'$ ↯

Also ist $A'B - AB' = A'C - AC' \neq 0$

Es gilt $ggT(A, A') \mid A'B - AB'$

$ggT(B, B') \mid A'B - AB'$

$ggT(C, C') \mid A'C - AC' = A'B - AB'$

Da A, B, C teilerfremd sind, gilt auch

$$ggT(A, A') \cdot ggT(B, B') \cdot ggT(C, C') \mid A'B - AB'$$

Daraus folgt

$$\begin{aligned} Grad(ggT(A, A')) + Grad(ggT(B, B')) + Grad(ggT(C, C')) \\ \leq Grad(A'B - AB') \\ \leq Grad(A) + Grad(B) - 1 \end{aligned}$$

Mit Lemma 3.4 erhalten wir

$$\begin{aligned} Grad(ggT(A, A')) &= Grad(A) - N_0(A) \\ Grad(ggT(B, B')) &= Grad(B) - N_0(B) \\ Grad(ggT(C, C')) &= Grad(C) - N_0(C) \end{aligned}$$

also

$$\begin{aligned} &\big(Grad(A) - N_0(A)\big) + \big(Grad(B) - N_0(B)\big) + \big(Grad(C) - N_0(C)\big) \\ &\leq Grad(A) + Grad(B) - 1 \end{aligned}$$

$$\begin{aligned} \Rightarrow \quad Grad(C) &\leq N_0(A) + N_0(B) + N_0(C) - 1 \\ &= N_0(ABC) - 1 \end{aligned}$$

: Wegen $(-B)+C=A$ und $(-A)+C=B$

können wir ähnlich beweisen, dass

$$\text{Grad}(A) \leq N_0(ABC)-1$$

und $$\text{Grad}(B) \leq N_0(ABC)-1$$

und die Behauptung folgt. □

Bemerkung: Warum funktioniert der gleiche Beweis nicht für Zahlen?

Polynome können wir ableiten, Zahlen nicht.

Ideale und Restklassenringe

Def: Sei $(R,+,\cdot)$ ein Ring mit Eins.

Ein Ideal in R ist eine Untermenge $I \subseteq R$ sodass

(1) $(I,+)$ ist eine abelsche Gruppe $\begin{cases} 0 \in I \\ i_1+i_2 \in I \\ -i \in I \end{cases}$

(2) $R \cdot I \subseteq I \quad \forall x \in R$

Beispiele: $6\mathbb{Z} \subset \mathbb{Z}$

$\{f(x) \in \mathbb{Z}[X] : f(1)=0\} \subset \mathbb{Z}[X]$

$\{0\} \subset R$

$R \subset R$

Bemerkung: $(I,+,\cdot)$ ist automatisch ein Ring

$I \cdot I = \{i_1 \cdot i_2 : i_1, i_2 \in I\} = I$

Def: Sei $(R,+,\cdot)$ ein Ring mit Eins, $I \subseteq R$ ein Ideal und $x, y \in R$

Wir sagen x und y sind kongruent modulo I, bezeichnet $x \equiv y \bmod I$

$\Leftrightarrow x - y \in I$

$(\Leftrightarrow x \in y + I)$

Lemma 3.6: Kongruenz modulo I ist eine Äquivalenzrelation

Beweis: Aufgabe

Def: Die Äquivalenzklasse von $x \in R$ bezüglich dieser Relation bezeichnen wir mit $[x]_I = \{y \in R : x \equiv y \bmod I\}$

diese Äquivalenzklassen nennen wir Restklassen modulo I

Die Menge der Restklassen bezeichnen wir mit R/I

Auf R/I definieren wir Addition und Multiplikation durch

$$[x]_I + [y]_I := [x+y]_I$$
$$[x]_I \cdot [y]_I := [x \cdot y]_I$$

Satz 3.7: Addition und Multiplikation sind auf R/I wohldefiniert, und $(R/I, +, \cdot)$ ist ein Ring mit $0_{R/I} = [0]_I$ und $1_{R/I} = [1]_I$

$(R/I, +, \cdot)$ heisst der Restklassenring

Beweis: Wir beweisen ~~nur~~ beispielshalber nur einige Aussagen

„+ ist wohldefiniert": Sei $x, y, z \in R$ mit $[y]_I = [z]_I$

Dann ist $y \equiv z \mod I$

also $y - z \in I$

$$[x]_I + [y]_I = [x+y]_I$$
$$= \{r \in R : x+y \equiv r \mod I\}$$

aber $x+y \equiv r \mod I \iff x+z+(y-z) \equiv r \mod I$

$\iff x+z-r \in (z-y)+I = I$

da $y-z \in I \Rightarrow z-y \in I$
und $(I,+)$ eine Gruppe ist.

$\iff x+z \equiv r \mod I$

Also $\{r \in R : x+y \equiv r \mod I\} = \{r \in R : x+z \equiv r \mod I\}$
$$= [x+z]_I$$
$$= [x]_I + [z]_I$$

„$0_{R/I} = [0]_I$": Sei $[x]_I \in R/I$

Dann ist $[x]_I + [0]_I = [x+0]_I$
$$= [x]_I$$

~~[illegible]~~

„$1_{R/I} = [1]_I$": Sei $[x]_I \in R/I$

Dann ist $[x]_I \cdot [1]_I = [x \cdot 1]_I$
$$= [x]_I$$

□

Beispiel: Sei $m \in \mathbb{N}^+$. Dann ist $m\mathbb{Z}$ ein Ideal in $\mathbb{Z}$ und $\mathbb{Z}/m\mathbb{Z}$ der Restklassenring der ganzen Zahlen modulo m.

Die Elemente von $\mathbb{Z}/m\mathbb{Z}$ sind $[0]_{m\mathbb{Z}}, [1]_{m\mathbb{Z}}, \ldots, [m-1]_{m\mathbb{Z}}$
die bezeichnen wir oft einfach mit $0, 1, 2, \ldots, m-1$

Satz 3.8: Sei $(R, +, \cdot)$ ein endlicher Ring mit Eins, $R \neq \{0\}$

R ist ein Körper $\Leftrightarrow$ R hat keine Nullteiler

Korollar 3.9: $\mathbb{Z}/m\mathbb{Z}$ ist ein Körper $\Leftrightarrow m \in \mathbb{P}$

Beweis von Korollar 3.9: Aufgabe

Beweis von Satz 3.8: Nächstes Mal.