Lemma 3.4 *Siano $a(x), b(x) \in K[x]$ l'anello di polinomi su un campo K, allora*

(i) $\deg(a(x) + b(x)) \leq \max(\deg(a(x)), \deg(b(x)))$.

(ii) $\deg(a(x)b(x)) = \deg(a(x)) + \deg(b(x))$.

Rimane da considerare se sia sensato attribuire un grado anche al polinomio nullo. Nel caso in cui K è un dominio sarebbe interessante preservare la proprietà $\deg(a(x)b(x)) = \deg(a(x)) + \deg(b(x))$ (Principio di Hankel-Peacock). Questo obbliga a definire

$$\deg(0) = -\infty,$$

dove il segno meno sottintende che tale valore vada considerato come inferiore a qualsiasi altro grado.

Una conseguenza del lemma 3.4 è che $ab = 0$ sse uno dei due fattori è 0. Quindi sia $\mathbb{Z}$ che $K[x]$ sono dei **domini** ossia degli anelli commutativi in cui vale la **la legge di annullamento** del prodotto.

3.1 Algoritmo di divisione sugli Interi

Riprendiamo ed estendiamo a $\mathbb{Z}$ il classico algoritmo di divisione.

Proposizione 3.5 (Algoritmo di divisione) *Siano $a, b \in \mathbb{Z}$, $b \neq 0$. Allora esistono e sono unici $q, r \in \mathbb{Z}$ tali che:*

1. $a = bq + r$.
2. $0 \leq r < |b|$.

Dim. Sostituendo b con $-b$ e q con $-q$, possiamo supporre che $b \in \mathbb{N}$. Iniziamo ad analizzare il caso $a \in \mathbb{N}$.

Sia $R = \{a - bq : q \in \mathbb{Z}\} \cap \mathbb{N}$. Siccome $a \in R$, $R \neq \emptyset$. Pertanto, per il principio di induzione, esiste $r = \min(R)$. Il principio di induzione equivale al principio di buon ordinamento in $\mathbb{N}$, ossia ogni sottoinsieme non vuoto di $\mathbb{N}$ ammette minimo (si veda [Chi09, Chapter 2, Theorem 8]).

Se fosse $r = a - bq \geq b$, potrei scrivere $0 \leq r - b = a - (q + 1)b < r$, contro la minimalità di r. Quindi $0 \leq r < b$.

Sia $a < 0$, allora, per il caso precedente, esistono $q', r' \in \mathbb{Z}$ tali che $-a = bq' + r'$, $0 \leq r' < b$. Se $r' = 0$, allora $a = bq$ con $q = -q'$. Altrimenti $r' > 0$ e $a = -b(q' + 1) + (b - r')$ e l'asserto è verificato con $q = -(q' + 1)$ e $r = b - r'$.

Sia ora $a = bq + r = bq' + r'$ con $r \geq r'$. Allora $b|(r - r')$. Ma $r - r' < b$, quindi $r = r'$ e, di conseguenza $q' = q$. □

Questa dimostrazione si potrebbe tradurre in un algoritmo - non molto efficiente. Si parte da a e si sottrae ($q > 0$) o aggiunge ($q < 0$) b fino ad ottenere un valore in $[0, |b|)$. Il costo computazionale di questo approccio è $|q|$. L'usuale algoritmo che credo insegnino ancora in corsi pre-universitari (Scuola Primaria, Secondaria, ecc...) richiede invece $\log_{10} |q|$ passi. Puntualizzo solo il fatto che questo algoritmo lavora per approssimazioni successive individuando per eccesso

le cifre decimali di q troncando dividendo e divisore, controllando che il prodotto del valore ottenuto per il divisore non superi il dividendo e, nel caso lo superi, diminuendo di 1 il valore precedentemente ottenuto.

Esercizio 3.6 *Scrivete un codice in* MAGMA *che implementi la divisione che vi hanno insegnato e/o formalizzi la precedente descrizione vaga.*

Tutto chiaro? Forse. Credo invece che non venga più insegnato l'algoritmo per l'estrazione della radice quadrata di un numero reale. Per semplicità sia tale numero un quadrato perfetto con tre o quattro cifre n. L'obiettivo consiste nel calcolare due cifre a, b tali che

$$n = (10a + b)^2 = 100a^2 + 20ab + b^2.$$

Allora $n/100 \geq a^2$. Trovo la massima cifra a che soddisfa la precedente diseguaglianza. Si ha $(n - 100a^2)/20a \geq b$. Come prima determino la massima cifra $\tilde{b}$ che soddisfa la precedente diseguaglianza. Abbiamo finito? No, potrebbe succedere che $(10a + \tilde{b})^2 > n$. Allora riduco $\tilde{b}$ di 1.

Esercizio 3.7 *Scrivete un codice in* MAGMA *che implementi l'estrazione di radice quadrata.*

Esercizio 3.8 *Determinare con l'ausilio di* MAGMA *le terne* $[n, a, \tilde{b}]$ *con* $100 \leq n < 10000$, $a = \lfloor \sqrt{n}/10 \rfloor$ *dove* $\tilde{b} = \lfloor (n - 100a^2)/20a \rfloor$ *soddisfa* $(10a + \tilde{b})^2 > n$. *Siete in grado di enunciare una congettura che descriva queste terne? Quando* $\tilde{b} \geq 10$*?*

Esiste un algoritmo di divisione anche per polinomi a coefficienti su un campo e paradossalmente è più semplice che nel caso degli interi. Il motivo è che ogni passo fornisce una risposta univoca che non è necessario modificare.

3.2 Divisione (Lunga) di polinomi

Mostriamo che su un campo K è possibile implementare in $A = K[x]$ un **algoritmo di divisione** (noto con l'aggettivo lunga per distinguerla dall'omologo sugli interi) la cui esistenza consente di ottenere l'analogo dell'**algoritmo Euclideo**.

Introduco alcuni termini.

Definizione 3.9 *Dato un polinomio* $a(x) = \sum_{i=0}^{n} a_i x^i \in A$, *con* $a_n \neq 0$, *pongo* $\mathrm{LT}(a) := a_n x^n$ *e* $\mathrm{LC}(a) := a_n$ *e li chiamo* ***termine direttivo*** *e* ***coefficiente direttivo*** *di* a

Teorema 3.10 *Siano* K *un campo e* $a, b \in A$, *con* $b \neq 0$. *Allora esistono e sono univocamente determinati* $q, r \in A$ *tali che*

(i) $\deg(r) < \deg(b)$ *(include il caso* $r = 0_A$*).*

(ii) $a = bq + r$.

Dim. Sia $n = \deg(a)$ e $m = \deg(b)$. Se $n < m$ basta porre $q = 0$ e $r = a$. Sia quindi $n \geq m$. Siano $a_n = \mathrm{LC}(a)$ e $b_m = \mathrm{LC}(b)$ i coefficienti direttivi di a e b. Sia $\widetilde{a} := a - a_n b_m^{-1} x^{n-m} b$, allora $\deg(\widetilde{a}) < n$. Per induzione su n esistono $\widetilde{q}$ e $\widetilde{r}$ tali che $\widetilde{a} = b\widetilde{q} + \widetilde{r}$ e $\deg(\widetilde{r}) < m$. Basta porre $q = a_n b_m^{-1} x^{n-m} + \widetilde{q}$ e $r = \widetilde{r}$.

Proviamo ora l'unicità. Supponiamo che $a = bq + r = bq_1 + r_1$ con r e r_1 di grado inferiore a m. Segue quindi che $b(q - q_1) = r_1 - r$. Se per assurdo $q \neq q_1$ allora $b(q - q_1)$ avrebbe grado almeno m. Allora $\deg(r_1 - r) \geq \deg(b)$ il che è assurdo in quanto sia r che r_1 hanno grado minore di m. Allora deve essere necessariamente $q = q_1$ e $r = r_1$. □

L'unicità di quoziente e resto caratterizza univocamente gli anelli di polinomi a coefficienti su un campo (si veda [Jod67]).

Osservazione 3.11 *Nella dimostrazione precedente l'ipotesi che K sia un campo entra in gioco solo quando si afferma l'esistenza dell'inverso del coefficiente direttivo del polinomio divisore.*

Esercizio 3.12 *Imitare l'algoritmo di divisione lunga per spiegare la tecnica che avete appreso da piccoli per dividere due interi.*

Osservazione 3.13 *La procedura usata nella dimostrazione precedente fornisce il cosiddetto algoritmo di divisione lunga tra polinomi.*

Esempio 3.14 *Si vuole calcolare in $\mathbb{Q}[x]$ quoziente e resto tra i polinomi*

$$a(x) = 2x^3 + x^2 - 3x + 5 \qquad b(x) = 3x^2 - 2$$

Procedendo come descritto sopra si ottiene:

$+2x^3$	$+x^2$	$-3x$	$+5$	$3x^2 - 2$
$-2x^3$		$+(4/3)x$		$(2/3)x + 1/3$
	x^2	$-(5/3)x$	$+5$	
	x^2		$+2/3$	
		$-(5/3)x$	$+17/3$	

Quindi si ha $q(x) = (2/3)x + 1/3$ e $r(x) = (-5/3)x + 17/3$.

Esercizio 3.15 *Implementare un codice in* Magma *per il calcolo della divisione lunga tra polinomi.*

3.3 Congruenze tout court

Tra le varie relazioni di equivalenza che si possono definire su una struttura algebrica quelle che rivestono maggior interesse sono quelle compatibili con le operazioni, nel senso che verrà precisato fra breve. Tali relazioni vengono anche dette congruenze.