

L'ANELLO QUOZIENTE $K[x]/I$

Sia K un campo. Ogni ideale di $K[x]$ è principale, cioè generato da un elemento. Qui vogliamo elencare alcune proprietà dell'anello quoziente $K[x]/I$ fatto rispetto ad un ideale $I = (f)$ non banale di $K[x]$ (quindi con $\deg(f) \geq 1$).

Ricordare che:

- In $K[x]$ si possono dividere gli elementi, cioè, dati $f, g \in K[x]$, $f \neq 0$ esistono unici $q, r \in K[x]$ tali che $g = qf + r$ dove $\deg(r) < \deg(f)$.
- In $K[x]$ un elemento f è primo se e solo se è irriducibile. Si dimostra facilmente che $K[x]/(f)$ è campo se e solo se f è irriducibile (= primo).
- In $K[x]$ gli ideali primi coincidono con gli ideali massimali.

Gli elementi del quoziente $K[x]/(f)$ sono classi. Una classe $[g]$, rappresentata da un elemento g , è l'insieme

$$g + (f) = \{g + \alpha f \mid \alpha \in K[x]\}$$

Due polinomi g e g' danno la stessa classe se e solo se f divide $g - g'$. Una classe $[g]$ è rappresentata in modo unico dal polinomio r , dove r è il resto della divisione di g per f . Infatti, se abbiamo che $[g] = [g']$ e se il resto della divisione di g per f è r , mentre il resto della divisione di g' per f è r' , allora $g - g'$ è multiplo di f . Quindi, essendo $g = qf + r$ e $g' = q'f + r'$, risulta che $r - r'$ è multiplo di f , ma poiché è di grado minore del grado di f , deve essere $r - r' = 0$. Pertanto (le classi dei) polinomi di grado minore del grado di f possono essere usati come rappresentanti canonici degli elementi di $K[x]/(f)$. Si ripete quindi quanto si fa per l'anello $\mathbb{Z}_m = \mathbb{Z}/(m)$ nel quale gli elementi sono rappresentati da $[0], [1], \dots, [m-1]$, che sono i possibili resti della divisione dei numeri interi per m .

L'anello quoziente $K[x]/(f)$ contiene una copia isomorfa di K , infatti le classi $[a]$, con $a \in K$ sono univocamente determinate da a (se $[a] = [b]$, con $a, b \in K$, allora $a - b$ è multiplo di f , ma essendo f di grado almeno 1, deve essere $a - b = 0$, cioè $a = b$).

Si vede allora che $K[x]/(f)$ è uno spazio vettoriale su K (la somma è data dalla somma definita nell'anello quoziente $K[x]/(f)$, mentre il prodotto $a \cdot [g]$ è definito da $[ag]$). Se inoltre f è un polinomio di grado n , allora tutti i possibili resti della divisione di un polinomio per f sono della forma: $a_0 + a_1x + \dots + a_{n-1}x^{n-1}$ e quindi in $K[x]/(f)$ gli elementi sono della forma $a_0 + a_1[x] + \dots + a_{n-1}[x^{n-1}]$, quindi sono combinazioni lineari, con coefficienti in K , di $[1], [x], \dots, [x^{n-1}]$. Inoltre questi n elementi sono linearmente indipendenti su K (se una loro combinazione lineare $a_0 + a_1x + \dots + a_{n-1}x^{n-1}$ vale 0, significa che (f) contiene un polinomio di grado minore di n e questo accade se e solo se $a_0 = a_1 = \dots = a_{n-1} = 0$).

Pertanto $K[x]/(f)$ è uno spazio vettoriale di dimensione $n = \deg(f)$ con base $[1], [x], \dots, [x^{n-1}]$.

Infine, se $[g] = [g']$, si usa anche scrivere $g \equiv g' \pmod{(f)}$.

Esercizi proposti:

1. Trovare tutti gli elementi invertibili e i divisori dello zero di $\mathbb{Q}[x]/(x^2 - 1)$.

2. Sia $f \in \mathbb{Q}[x]$ dato da $f = x^2 + 2$. Dopo aver provato che f è irriducibile, dare una formula per calcolare l'inverso di ogni elemento (non nullo) $a_0 + a_1x$ di $\mathbb{Q}[x]/(f)$. Dare la tabella di moltiplicazione di $\mathbb{Q}[x]/(f)$ espressa rispetto alla base $[1], [x]$.
3. Sia $f = x^2 - 4 \in \mathbb{Q}[x]$. Trovare tutti gli ideali massimali di $\mathbb{Q}[x]$ che contengono $I = (f)$.
4. Trovare un anello (non campo) della forma $\mathbb{Q}[x]/(f)$ (con f opportuno) che contenga un solo ideale massimale.
5. Sia $K = \mathbb{Z}_3[x]/(x^2 + x + 2)$. Dopo aver provato che K è un campo, dire quanti elementi ha e provare che $K^* = K \setminus \{0\}$ è, rispetto al prodotto, un gruppo ciclico.
6. Sia $K = \mathbb{Z}_3[x]/(x^2 + 1)$. Provare che K è un campo perfetto. Trovare la radice cubica di $x + 2$.