Anello dei polinomi. Alcune proprietà

Ricordiamo brevemente come è stato introdotto l'anello dei polinomi su un anello A, commutativo, unitario (riferimento: lezione 7). Si costruisce l'insieme B delle sequenze di elementi di A del tipo $(a_0, a_1, \ldots)$ dove gli a_i sono quasi tutti nulli (cioè sono diversi da zero solo per un numero finito di indici). Sull'insieme B si definisce una somma componente per componente. In questo modo B diventa un gruppo abeliano. Date due successioni di B, si definisce il prodotto di Cauchy. In questo modo B diventa un anello commutativo unitario che contiene (una copia isomorfa di) A. In B si mette in evidenza un elemento x che è dato dalla sequenza $(0, 1, 0, 0, \ldots)$ e si vede che ogni elemento di B, cioè ogni sequenza $(a_0, a_1, \ldots, a_n, 0, 0, \ldots)$ si può scrivere nella forma $a_0 + a_1x + \cdots + a_nx_n$, che si chiama *polinomio* nella variabile x. L'anello B si indica con $A[x]$ e si dice *anello di polinomi* nella variabile x.

Ci occupiamo ora di alcune proprietà dell'anello dei polinomi $K[x]$ dove K è un campo. La condizione di prendere i coefficienti dei polinomi in un campo permette di ottenere molti risultati specifici che in generale non sono veri nel caso di coefficienti presi in anelli qualunque (e neppure in domini). Ad esempio la divisione di un polinomio f con un polinomio $g \neq 0$ può essere sempre eseguita in quanto il coefficiente direttivo di g è necessariamente invertibile.

Vediamo una prima prorietà:

Teorema 1 *Sia K un campo, sia $f \in K[x]$ e sia $a \in K$ un elemento fissato. Allora il resto della divisione di f per il polinomio $x - a$ vale $f(a)$ (cioè il valore del polinomio f valutato in a).*

Dim. Dividiamo f per $x - a$ e otteniamo: $f = q(x - a) + r$ dove il grado di r è minore di 1 (che è il grado di $x - a$), quindi r è una costante. Se applichiamo l'omomorfismo di valutazione (con valutazione in a) ad f, otteniamo $f(a)$. Se lo applichiamo a $q(x - a) + r$ otteniamo $q(a)(a - a) + r(a) = r(a)$. Ma essendo r una costante, $r(a) = r$ e quindi otteniamo $f(a) = r$. c.v.d.

In particolare abbiamo:

Corollario 1 *(Teorema di Ruffini) Sia K un campo. Un polinomio $f \in K[x]$ è divisibile per $x - a$ se e solo se $f(a) = 0$.*

Dim. Immediata conseguenza del risultato precedente. c.v.d.

Il seguente risultato limita il numero di radici di un polinomio:

Teorema 2 *(D'Alambert) Sia K un campo e sia $f \in K[x]$ un polinomio non nullo di grado $n \geq 1$. Allora f ha al massimo n radici.*

Dim. Si usa induzione sul grado n di f. Se $n = 0$ o $n = 1$ il risultato è banale. Vediamo allora il passo induttivo. Supponiamo che f sia un polinomio di grado n. Se non ha radici, non c'è nulla da provare. Supponiamo allora che abbia una radice a. Allora, per il precedente risultato, $f = f_1(x - a)$ dove f_1 è un polinomio di grado $n - 1$ e quindi, per ipotesi induttiva, ha al massimo $n - 1$ radici. Pertanto f ha al massimo n radici. c.v.d.

Infine, vediamo cosa si può dire riguardo al fatto che i polinomi in $K[x]$ si possono considerare anche come applicazioni $K \longrightarrow K$. Si è già accennato al fatto che ci sono situazioni in cui due polinomi diversi danno luogo alla stessa applicazione (si pensi ai polinomi $x + 1, x^2 + 1 \in \mathbb{Z}_2[x]$ che, come funzioni da

$\mathbb{Z}_2$ in sè stesso danno la stessa funzione (che manda 0 in 1 e 1 in 0)). Però se il campo K è infinito, questo non può succedere:

Teorema 3 *Sia K un campo con infiniti elementi e siano $f, g \in K[x]$ due polinomi tali che $f(a) = g(a)$ per ogni $a \in K$. Allora $f = g$.*

Dim. Consideriamo il polinomio $h = f - g$. Esso ha infiniti zeri (tutti gli elementi di K) ma allora, per il teorema precedente, non può che essere il polinomio nullo. c.v.d.

Nell'anello degli interi si è dimostrato che ogni ideale è principale. Vediamo che in $K[x]$ vale la stessa proprietà (e la dimostrazione è del tutto simile).

Teorema 4 *Nell'anello dei polinomi $K[x]$ (dove K è un campo) ogni ideale è principale (cioè è generato da un unico elemento).*

Dim. Sia I un ideale di $K[x]$. Se $I = (0)$ è certamente principale, quindi supponiamo $I \neq (0)$. Sia $g \in I$ un polinomio non nullo e scegliamolo di grado minimo possibile. Proviamo che I conicide con l'ideale (g), generato da g. Certamente $(g) \subseteq I$, in quanto $g \in I$ e (g) è il più piccolo ideale che contiene g. Sia ora $f \in I$ e dividiamolo per g: $f = qg + r$ dove il grado di r è minore del grado di g. Ma da $r = f - qg$ si ottiene che $r \in I$ e quindi r è un polinomio che sta in I di grado minore del grado di g. L'unica possibilità è che r sia il polinomio nullo. c.v.d.

La possibilità di poter fare le divisioni in $K[x]$ comporta anche il fatto che si può costruire (esattamente come in $\mathbb{Z}$) il massimo comun divisore tra due suoi elementi f, g. Più precisamente, si può costruire un algoritmo basato sulla seguente osservazione: l'insieme dei divisori di f e g coincide con l'insieme dei divisori tra f e r, dove r è il resto della divisione di f per g. In particolare $\mathrm{mcd}(f, g) = \mathrm{mcd}(r, g)$. Il procedimento può essere iterato, dividendo g per r e così via fino ad ottenere il massimo comun divisore tra 0 e un polinomio h che è h. Inoltre, proprio come si è fatto in $\mathbb{Z}$ ripercorrendo a ritroso l'algoritmo per il calcolo del massimo comun divisore d tra f e g si possono trovare due polinomi $a, b \in K[x]$ tali che valga: $d = af + bg$. Quindi anche nell'anello dei polinomi vale l'identità di Bezout.

Sia ora A un dominio d'integrità e sia $a \in A$. Si dice che $b \in A$ *divide* a se esiste un elemento $d \in A$ tale che $a = bd$ (si scrive $b|a$). Dato $a \in A$ ci sono sempre dei divisori di a. Ad esempio $1, -1, a, -a$ sono tra questi. Più in generale, si vede che anche un qualunque elemento unitario è sempre un divisore di a e infine anche un qualunque elemento associato ad a (cioè che è della forma ua, con u unitario) è divisore di a. Un elemento a, diverso da 0 e non unitario, che ha solo questi elementi per divisori, si dice *irriducibile*. Una definizione equivalente, più operativa, è la seguente:

Definizione. Un elemento a in un dominio d'integrità A si dice *irriducibile* se vale la seguente condizione:

$$\text{se } a = fg \text{ allora } f \text{ è unitario o } g \text{ è unitario}$$

Possiamo poi mettere in evidenza un'altra proprietà che può essere soddisfatta da alcuni elementi di A:

Definizione. Un elemento p in un dominio d'integrità A si dice *primo* se vale la seguente condizione:

$$\text{se } p|fg \text{ allora } p|f \text{ o } p|g$$

Vi è un legame tra primo e irriducibile:

Teorema 5 *Ogni elemento primo in un dominio d'integrità è anche irriducibile.*

Dim. Sia p primo e supponiamo che sia $p = fg$. Allora p certamente divide il prodotto fg e quindi, per ipotesi, divide ad sempio f, cioè vale $f = dp$. In conseguenza, $p = (dp)g$. Essendo in un dominio, otteniamo che $dg = 1$ e quindi g è invertibile. c.v.d.

In generale, non è vero il viceversa, cioè che irriducibile implica primo. Torneremo in seguito su tale argomento.

Definizione. Un dominio d'integrità A si dice un *dominio a fattorizzazione unica* (in sigla: UFD) se valgono le seguenti condizioni:

- Ogni elemento diverso da zero e non unitario è prodotto di (uno o più) elementi irriducibili.
- Se $a = f_1 \cdots f_r$ e anche $a = g_1 \cdots g_s$ con f_i e g_j irriducibili, allora $r = s$ ed esiste una permutazione σ degli indici $\{1, 2, \ldots, r\}$ tale che f_i e $g_{\sigma(i)}$ sono associati.