Algebra n. 3 - NOTE ALLA LEZIONE 19

Teorema 19.9

$B[\alpha]$ indica il sottoanello di A generato da $B \cup \{\alpha\}$. È il seguente insieme:

$$\{f(\alpha) | f(x) \in B[x]\}.$$

Esso ammette B come sottoanello unitario (è il sottoinsieme formato dalle valutazioni in α dei polinomi costanti di $B[x]$). Quindi ha una naturale struttura di B-modulo (v. Esempio 17.4 b)).

Naturalmente, per ogni intero positivo n, si ha $B[\alpha] \supset \sum_{i=0}^{n-1} B\alpha^i$. D'altra parte, per ogni $g(x) = \sum_{i=0}^{N} c_i x^i \in B[x]$, si ha $g(\alpha) = \sum_{i=0}^{n-1} c_i \alpha^i + \sum_{i=n}^{N} c_i \alpha^i \in \sum_{i=0}^{n-1} B\alpha^i$, in quanto a questo modulo appartengono entrambi gli addendi: il primo per definizione, il secondo in virtù della dimostrazione appena effettuata. Ciò prova l'inclusione $B[\alpha] \subset \sum_{i=0}^{n-1} B\alpha^i$.

Considerata la matrice $M = (b_{ij})$, si ha

$$xI_r - M = \begin{pmatrix} x - b_{11} & -b_{12} & \cdots & -b_{1r} \\ -b_{21} & x - b_{22} & \cdots & -b_{2r} \\ \vdots & & \ddots & \\ -b_{r1} & -b_{r2} & \cdots & x - b_{rr} \end{pmatrix}$$

Il suo determinante è un polinomio monico di grado r a coefficienti in B.

Corollario 19.11

Per la dimostrazione, basta osservare che la condizione c) del Teorema 19.9 è soddisfatta da $C = A$, e quindi la condizione a) è soddisfatta da ogni elemento α di A.

Esempio 19.12

b) Consideriamo l'anello quoziente

$$\mathbb{Z}[x]/(f(x)) = \{r(x) + (f(x)) | r(x) \in \mathbb{Z}[x], r(x) = 0 \text{ oppure } r(x) \neq 0 \text{ e } \deg(r) < \deg(f) = n\}.$$

Tramite il monomorfismo di anelli $\mathbb{Z} \to \mathbb{Z}[x]/(f(x))$ definito da $a \mapsto a + (f(x))$, l'anello $\mathbb{Z}$ può essere identificato con un sottoanello unitario di $\mathbb{Z}[x]/(f(x))$, che dunque possiede una naturale struttura di $\mathbb{Z}-$modulo, secondo la quale, per ogni $r(x) = \sum_{i=0}^{n-1} a_i x^i \in \mathbb{Z}[x]$, risulta

$$r(x)+(f(x))=\sum_{i=0}^{n-1}a_i(x^i+f(x)).$$

L'insieme $\left\{x^i+(f(x))\middle| i=0,...,n-1\right\}$ costituisce dunque un sistema (finito) di generatori di $\mathbb{Z}[x]\big/(f(x))$ come $\mathbb{Z}-$modulo.

Proposizione 19.13

Dimostrazione: Sia A intero su B. Sia $\alpha\in A$. Sia $f(x)=\sum_{i=0}^{n}a_ix^i\in B[x]$ (con $a_n=1$) un'equazione di dipendenza intera per α su B. Allora α è intero su $C[a_0,...,a_{n-1}]$, e quindi $C[a_0,...,a_{n-1}][\alpha]$ è finitamente generato su $C[a_0,...,a_{n-1}]$. Ma, essendo B intero su C, $C[a_0]$ è finitamente generato su C, e, in generale, per ogni indice $i=1,...,n-1$, $C[a_0,...,a_{i-1}][a_i]$ è finitamente generato su $C[a_0,...,a_{i-1}]$ (in quanto a_i è, in particolare, intero su $C[a_0,...,a_{i-1}]$.) Segue, in virtù della transitività delle estensioni finite di anelli (analoga a quella valida per i campi, vedi, più avanti, il Lemma 19.22), che $C[a_0,...,a_{n-1}][\alpha]$ è finitamente generato su C. Ne consegue che α è intero su C, in quanto risulta verificata, dal sottoanello $C[a_0,...,a_{n-1}][\alpha]$, intermedio fra C ed A, la condizione c) del Teorema 19.9.

Teorema 19.14

Si osservi che, senza l'ipotesi sull'estensione intera, due domini di integrità A e B , ove il secondo è sottoanello del primo, possono essere o non essere campi in maniera del tutto indipendente l'uno dall'altro, secondo ogni possibile combinazione:

A	B
$\mathbb{R}$ campo	$\mathbb{Q}$ campo
$\mathbb{R}$ campo	$\mathbb{Z}$ non campo
$\mathbb{R}[x]$ non campo	$\mathbb{R}$ campo
$\mathbb{Z}[x]$ non campo	$\mathbb{Z}$ non campo

Supponiamo che nella (1) si abbia $b_0=0$. Allora

$$(\alpha^{n-1}+b_{n-1}\alpha^{n-2}+\cdots+b_1)\alpha=0,$$

ove, essendo $\alpha\neq 0$, a causa dell'integrità di A, si ha necessariamente $\alpha^{n-1}+b_{n-1}\alpha^{n-2}+\cdots+b_1=0$, il che non può accadere se n è il più piccolo possibile.

Proposizione 19.27

Nella dimostrazione, l'ipotesi di fattorizzazione unica è stata utilizzata nel momento in cui u, v sono stati supposti relativamente primi. Ciò presuppone la possibilità di ridurre una frazione ai minimi termini, operazione sempre garantita in un dominio a fattorizzazione unica (tramite la cancellazione dei fattori primi comuni a numeratore e denominatore).