Algebra n. 3 - NOTE ALLA LEZIONE 23

Dimostrazione della **Proposizione 23.8**:

Teorema di Cayley-Hamilton

Sia M una matrice quadrata a coefficienti in un campo, e sia $p(x)$ il suo polinomio caratteristico. Allora $p(M) = 0$.

Sia dunque μ_α l'applicazione F-lineare da K a K definita dalla moltiplicazione per α. Detta M_α la matrice ad essa associata rispetto ad una base fissata, sia $\mathrm{char}_{K/F}(\alpha) = \sum_{i=0}^{n} a_i x^i$. Allora, per il precedente teorema, $\sum_{i=0}^{n} a_i {M_\alpha}^i$ è la matrice nulla. Tale matrice è associata all'applicazione lineare $\sum_{i=0}^{n} a_i {\mu_\alpha}^i$, che è dunque l'omomorfismo nullo. Ma questa applicazione è definita dalla moltiplicazione per $\sum_{i=0}^{n} a_i \alpha^i$. Ne consegue che $\sum_{i=0}^{n} a_i \alpha^i = 0_K$.

Le componenti, rispetto alla base prescelta, delle immagini, secondo la moltiplicazione per α, degli elementi del blocco j-esimo

$$\beta_1\gamma_j, \dots, \beta_p\gamma_j$$

sono nulle al di fuori dello stesso blocco, e, all'interno di questo, sono, nell'ordine, le stesse che quelle relative alla moltiplicazione per α su $\beta_1, .., \beta_p$. Precisamente, esse formano una matrice quadrata $p \times p$:

$$B = \begin{pmatrix} b_{11} & \cdots & b_{1p} \\ \vdots & \ddots & \vdots \\ b_{p1} & \cdots & b_{pp} \end{pmatrix}$$

Questa matrice, all'interno di M_α, forma il j-esimo blocco diagonale, corrispondente al blocco di vettori $\beta_1\gamma_j, \dots, \beta_p\gamma_j$ in "partenza" e in "arrivo".

Corollario 23.14

Siano $\alpha, \beta \in D_K$. Allora

$$N((\alpha)(\beta)) = N((\alpha\beta)) = |N(\alpha\beta)| = |N(\alpha)N(\beta)| = |N(\alpha)||N(\beta)| = N((\alpha))N((\beta)).$$

Corollario 23.18

Sia I un ideale proprio non primo (e dunque non nullo). Siano P e Q due fattori primi della sua decomposizione. Allora, per la moltiplicatività della norma di ideali, il prodotto $N(P)N(Q)$, di due interi maggiori di 1, divide $N(I)$. Ne consegue che $N(I)$ è un numero composto.

Esempio 23.25

Se $I=(p)$, allora p è un numero primo in D_K, e dunque, in base alla Proposizione 22.8, la congruenza quadratica $x^2 \equiv m \pmod p$ non ha soluzione. Viceversa, se ciò avviene, allora l'ideale (p) è primo (non nullo), e dunque l'inclusione $(p) \subset I$, tra ideali massimali, è necessariamente un'uguaglianza.