Algebra n. 3 - NOTE ALLA LEZIONE 20

Lemma 20.8

$$T(1,\alpha,\dots,\alpha^{n-1})=\begin{pmatrix}\sigma_1(1) & \sigma_1(\alpha) & \cdots & \sigma_1(\alpha^{n-1})\\ \sigma_2(1) & \sigma_2(\alpha) & \cdots & \sigma_2(\alpha^{n-1})\\ \vdots & \vdots & \vdots & \\ \sigma_n(1) & \sigma_n(\alpha) & \cdots & \sigma_n(\alpha^{n-1})\end{pmatrix}$$

$$=\begin{pmatrix}1 & \alpha_1 & \cdots & \alpha_1^{\,n-1}\\ 1 & \alpha_2 & \cdots & \alpha_2^{\,n-1}\\ \vdots & \vdots & \vdots & \\ 1 & \alpha_n & \cdots & \alpha_n^{\,n-1}\end{pmatrix}$$

<u>Dimostrazione</u> del **Lemma 20.9**:

Si considera la matrice:

$$T(\vartheta_1,\vartheta_2,\dots,\vartheta_n)=\begin{pmatrix}\sigma_1(\vartheta_1) & \sigma_1(\vartheta_2) & \cdots & \sigma_1(\vartheta_n)\\ \sigma_2(\vartheta_1) & \sigma_2(\vartheta_2) & & \sigma_2(\vartheta_n)\\ \vdots & \vdots & & \vdots\\ \sigma_n(\vartheta_1) & \sigma_n(\vartheta_2) & & \sigma_n(\vartheta_n)\end{pmatrix}$$

Supposta la lineare dipendenza di $\vartheta_1,\dots,\vartheta_n$, esisterà una loro combinazione lineare nulla, a coefficienti in F non tutti nulli. Da questa se ne deriverà, per la F-linearità delle applicazioni $\sigma_1,\dots,\sigma_n$, una analoga su ciascuna riga della matrice T. Tali combinazioni lineari daranno origine, a loro volta, ad una combinazione lineare nulla delle colonne:

$$\lambda_1\vartheta_1+\lambda_2\vartheta_2+\cdots+\lambda_n\vartheta_n=0$$

$$\begin{pmatrix}
\lambda_1\sigma_1(\vartheta_1)+ & \lambda_2\sigma_1(\vartheta_2)+ & \cdots & +\lambda_n\sigma_1(\vartheta_n)=0 \\
\lambda_1\sigma_2(\vartheta_1)+ & \lambda_2\sigma_2(\vartheta_2)+ & & +\lambda_n\sigma_2(\vartheta_n)=0 \\
\vdots & \vdots & & \vdots \\
\lambda_1\sigma_n(\vartheta_1)+ & \lambda_2\sigma_n(\vartheta_2)+ & & +\lambda_n\sigma_n(\vartheta_n)=0
\end{pmatrix}$$

Nella seconda parte della dimostrazione, si suppone per assurdo la lineare dipendenza delle righe di T, che darebbe luogo ad una combinazione lineare nulla non banale delle righe della matrice:

$$\begin{array}{c}
\begin{pmatrix}
\lambda_1\sigma_1(\vartheta_1) & \lambda_1\sigma_1(\vartheta_2) & \cdots & \lambda_1\sigma_1(\vartheta_n) \\
+\lambda_2\sigma_2(\vartheta_1) & +\lambda_2\sigma_2(\vartheta_2) & & +\lambda_2\sigma_2(\vartheta_n) \\
\vdots & \vdots & & \vdots \\
+\lambda_n\sigma_n(\vartheta_1)+ & \lambda_n\sigma_n(\vartheta_2) & & +\lambda_n\sigma_n(\vartheta_n)
\end{pmatrix} \\
\begin{matrix} \quad 0 \quad & \quad\quad 0 \quad\quad & & \quad\quad 0 \quad \end{matrix}
\end{array}$$

Questa identità, letta lungo ciascuna delle colonne, comporta l'annullamento dell'applicazione $\lambda_1\sigma_1+\cdots+\lambda_n\sigma_n$ in ogni elemento della base $\vartheta_1,\ldots,\vartheta_n$. Per linearità, segue che $\lambda_1\sigma_1+\cdots+\lambda_n\sigma_n=0$.

<u>Dimostrazione</u> del **Lemma 20.10**:

Si applica il Lemma 20.8 con $F=\mathbb{Q}$. In particolare $K=\mathbb{Q}(\alpha)$, ove α è un elemento algebrico su F, avente come polinomio minimo $f(x)\in\mathbb{Q}[x]$, di grado n. In particolare $\Delta(f)\in\mathbb{Q}$, inoltre gli elementi $1,\alpha,\ldots,\alpha^{n-1}$ formano una base di K su $\mathbb{Q}$. Esiste pertanto, per ognuno degli elementi $\vartheta_1,\ldots,\vartheta_n$, una rappresentazione come combinazione lineare razionale di $1,\alpha,\ldots,\alpha^{n-1}$:

$$\vartheta_j = \sum_{k=1}^{n} \alpha^{k-1} c_{kj},$$

e quindi, per ogni $i, j = 1, ..., n,$ si ha

$$\sigma_i(\vartheta_j) = \sum_{k=1}^{n} \sigma_i(\alpha^{k-1}) c_{kj}.$$

Esiste dunque una matrice quadrata di dimensione *n*, a coefficienti razionali, $C = (c_{ij}),$ tale che

$$T(\vartheta_1, ..., \vartheta_n) = T(1, \alpha, ..., \alpha^{n-1})C.$$

Passando ai determinanti:

$$\det T = \det T(1, \alpha, ..., \alpha^{n-1}) \det C.$$

Formando i quadrati:

$$d = \det T(1, \alpha, ..., \alpha^{n-1})^2 (\det C)^2.$$

Ma, per il Lemma 20.8, $\det T(1, \alpha, ..., \alpha^{n-1})^2 = \Delta(f).$ Ciò prova che *d* e $\Delta(f)$ differiscono per un fattore razionale.

Teorema 20.12

Dall'Osservazione 20.11 segue che D_K è isomorfo ad un sottomodulo di $\mathbb{Z}^n$, $\mathbb{Z}-$modulo libero di rango *n* (e quindi è libero di rango al più *n*) e contemporaneamente, contiene, a meno di isomorfismo, il sottomodulo $(d\mathbb{Z})^n$, a sua volta libero di rango *n* (avente come base $de_1, ..., de_n$). Quindi il rango di D_K è almeno *n*, e pertanto è esattamente *n*.

<u>Dimostrazione</u> del **Teorema 20.17**:

Per ogni *i*, $(a) \subset (a_i),$ da cui segue che a_i divide *a*. Ora, in un UFD, ogni elemento non invertibile e non nullo *a* possiede una fattorizzazione $up_1^{\alpha_1} \cdots p_s^{\alpha_s}$ (ove *u* è un elemento invertibile, e i p_i sono fattori primi a due a due non associati). Per l'unicità della fattorizzazione, i suoi divisori sono (a meno di fattori invertibili) tutti e soli i prodotti parziali che è possibile estrarre da $p_1^{\alpha_1} \cdots p_s^{\alpha_s}$. Tali prodotti, a due a due non associati, sono in corrispondenza biunivoca con gli ideali principali contenenti (a). E costituiscono, evidentemente, un insieme finito.

Per definizione, $bL \subset I.$ D'altra parte, $I \subset (b),$ e dunque, per ogni $x \in I,$ esiste $y \in A$ tale che $x = by.$ Ma, evidentemente, si ha allora che $y \in L.$ Ciò prova che $I \subset bL.$

Esempio 20.21

L'anello $\mathbb{Z}[\alpha]$ è formato da tutti e soli gli elementi del tipo $g(\alpha)$, con $g(x) \in \mathbb{Z}[x]$. Essendo α un intero algebrico, lo sono anche tutti questi elementi. Inoltre, per ogni $g(x) \in \mathbb{Z}[x]$, essendo $f(x) \in \mathbb{Z}[x]$ (per la Proposizione 19.8) e monico, è possibile determinare $q(x), r(x) \in \mathbb{Z}[x]$, quoziente e resto della divisione di $g(x)$ per $f(x)$, così che, in particolare, $g(\alpha) = f(\alpha)q(\alpha) + r(\alpha) = r(\alpha)$. Poiché il polinomio $r(x)$ è nullo oppure è non nullo di grado minore di *n*, ne consegue che $\mathbb{Z}[\alpha]$ è generato su $\mathbb{Z}$ dagli elementi $1, \alpha, \ldots, \alpha^{n-1}$. Questi, d'altra parte, costituiscono una base di $\mathbb{Q}(\alpha)$ su $\mathbb{Q}$, e quindi sono linearmente indipendenti su $\mathbb{Z}$. Essi costituiscono dunque, in definitiva, una base di $\mathbb{Z}[\alpha]$ su $\mathbb{Z}$. Pertanto $\mathbb{Z}[\alpha]$ è libero di rango *n*. Lo stesso vale, evidentemente, per $\frac{1}{d}\mathbb{Z}[\alpha]$.