(1) $C = (g(\bar{x}))$

(2) π suriezione naturale preserva il prodotto (è un omomorfismo)

Nota 1 : se abbiamo G, possiamo costruire $g(x)$

A/I sono le immagini tramite l'omomorfismo canonico $A \to A/I$ degli ideali J di A che contengono I. Applicando tale fatto generale al caso $A = \mathbb{F}_q[x]/(x^n - 1)$ ed $I = (x^n - 1)$, troviamo che un ideale $C \subset \mathbb{F}_q[x]/(x^n - 1)$ é immagine di un ideale $J \subset \mathbb{F}_q[x]$ che contiene $(x^n - 1)$. Qualsiasi ideale J di $\mathbb{F}_q[x]$ é principale, ossia $J = (g(x))$, ed esso contiene $(x^n - 1)$ se e solo se $x^n - 1 \in (g(x))$, ossia se $x^n - 1 = g(x)h(x)$, il che conclude la dimostrazione. □

Corollario 4.1. *Sia C un codice ciclico, generato da $g(\bar{x})$ con $g(x)|x^n - 1$, e sia $c(\bar{x}) \in \mathbb{F}_q[x]/(x^n-1)$ un elemento non nullo. Allora $c(\bar{x}) \in C$ se e solo $c(\bar{x})$ é rappresentato da un polinomio $c(x) = g(x)p(x)$ multiplo di $g(x)$ e di grado $< n$. Consequentemente C é identificato in modo naturale con il sottospazio vettoriale $\{g(x)p(x) \mid p(x) \in \mathbb{F}_q[x]$ e $p(x) = 0$ oppure $\deg p(x) < n - \deg g(x)\}$.* $\leq \mathbb{F}_q[x]_{n-1}$ = spazio vett. polinomi di grado $\leq n-1$

Dimostrazione. Un elemento $c(\bar{x}) \in \mathbb{F}_q[x]/(x^n - 1)$ é rappresentato da un unico polinomio $c(x)$ della forma $c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$. Si ha $c(\bar{x}) \in C \overset{(1)}{\iff} g(\bar{x})|c(\bar{x}) \overset{(2)}{\iff} g(x)|c(x)$, da cui la tesi. Scegliendo per ogni $c(\bar{x}) \in C$ l'unico rappresentante $c(x)$ di grado $< n$, si ha l'identificazione di C con lo spazio vettoriale come nell' enunciato. □

Proposizione 4.3. *Sia C lineare ciclico associato a $g(x)|x^n - 1$ come sopra, e scriviamo $g(x) = g_0 + g_1x + \cdots + g_{n-k}x^{n-k}$. Allora $\dim C = k$ ed una base di C é data da $g(\bar{x}), \bar{x}g(\bar{x}), \ldots, \bar{x}^{k-1}g(\bar{x})$. Rispetto alla base canonica $1, \bar{x}, \ldots, \bar{x}^{n-1}$ di $\mathbb{F}_q[x]/(x^n - 1)$ tale base di C ha per coefficienti le colonne della matrice*

$g_{n-k} \neq 0$, $\dim C > 0$

$$G = \begin{pmatrix} g_0 & 0 & \cdots & 0 \\ g_1 & g_0 & \cdots & 0 \\ & g_1 & \ddots & \vdots \\ \vdots & & \ddots & g_0 \\ & & & g_1 \\ g_{n-k} & & & \\ 0 & g_{n-k} & & \vdots \\ & & \ddots & \\ 0 & 0 & & g_{n-k} \end{pmatrix} \in n \times k$$

G^t *la quale pertanto è una matrice generatrice di C.* Nota 1

Dimostrazione. Per il corollario precedente, un elemento $c(\bar{x}) \in C$ si scrive in modo unico come $g(\bar{x})p(\bar{x})$ con $p(x)$ della forma $p(x) = p_0 + p_1x + \cdots + p_{k-1}x^{k-1}$. ~~Segue immediatamente che $c(\bar{x})$ é combinazione lineare unica dei polinomi $\bar{x}^i g(\bar{x})$ per $i = 0, 1, \ldots, k-1$,~~

Cor 4.1 $\Rightarrow \deg p(x) < n - \deg g(x) = n - (n-k) = k$ (3) $\Rightarrow$ il massimo grado di $p(x)$ è $k-1$ (3')

$c(\bar{x}) = g(\bar{x})p(\bar{x}) = p_0 g(\bar{x}) + p_1 g(\bar{x})x + \cdots + p_{k-1} g(\bar{x}) x^{k-1}$, $\deg g(\bar{x})x^{k-1} = n - k + k - 1 = n-1$ (4)

$p_i \in \mathbb{F}_q$ (potrebbe essere nullo)

(3') (4) $\Rightarrow$ Al variare dei p_i (nulli o meno) otteniamo tutti gli $c(x) \Rightarrow g(\bar{x}), g(\bar{x})x, \ldots, g(\bar{x})x^{k-1}$ genera C

e d'altronde sono l.i. : $\lambda_1 g(x) + \lambda_2 g(x)x + \cdots + \lambda_{k-1} g(x)x^{k-1} = 0 \Rightarrow \lambda_1 + \lambda_2 x + \cdots + \lambda_{k-1}x^{k-1} = 0 \Rightarrow$

$\Rightarrow \lambda_1 = \lambda_2 = \cdots = \lambda_{k-1} = 0$ (x^i l.i.) ; $C \neq 0 \Rightarrow g(\bar{x}) \neq 0$

Quindi $\{g(x)x^i\}$ è una base di C (5)