Algebra n. 3 - NOTE ALLA LEZIONE 9

Radici dell'unità:

Sia n un intero positivo. L'insieme R_n delle radici n-esime dell'unità è un sottogruppo del gruppo moltiplicativo del campo complesso, ed è un gruppo ciclico di ordine n. Precisamente,

$$R_n = \left\langle e^{\frac{2\pi i}{n}} \right\rangle = \left\{ e^{\frac{2k\pi i}{n}} \,\middle|\, k = 0, \ldots, n-1 \right\}.$$

Posto $\omega = e^{\frac{2\pi i}{n}}$, i generatori di R_n sono tutti e soli gli elementi ω^k con $0 \le k \le n-1$, e k coprimo con n. Questi sono tutte e sole le radici n-esime di 1 che hanno periodo n, dette *radici primitive n-esime* dell'unità. In generale, ogni elemento di R_n ha periodo pari ad un divisore d di n, e, per ogni d siffatto vi sono, in R_n, esattamente $\phi(d)$ (funzione di Eulero) elementi aventi periodo d. Questi sono le radici primitive d-esime dell'unità. Chiamiamo P_d il loro insieme. Allora, da un lato, abbiamo la seguente unione disgiunta

$$R_n = \bigcup_{d|n} P_d,$$

dall'altra si ha, per ogni siffatto d,

$$\Phi_d(x) = \prod_{\eta \in P_d} (x - \eta).$$

Inoltre, poiché gli elementi di R_n sono le n radici complesse del polinomio $x^n - 1$, per il Teorema di Ruffini si ha

$$x^n - 1 = \prod_{\eta \in R_n} (x - \eta).$$

Le ultime tre uguaglianze implicano l'enunciato della **Proposizione 9.2**. In particolare si ha anche:

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n, d \ne n} \Phi_d(x)}.$$

<u>Dimostrazione</u> della **Proposizione 9.6**:

Sia i un intero tale che $1 \le i \le p-1$. Consideriamo

$$\binom{p}{i} = \frac{p!}{i!(p-i)!}$$

Allora, poiché tutti i fattori dei fattoriali a denominatore sono interi positivi minori di p, il denominatore non ha p fra i suoi fattori primi. Questo è invece presente a numeratore. Ne consegue che il coefficiente binomiale è divisibile per p.