Algebra n. 3 - NOTE ALLA LEZIONE 5

<u>Dimostrazione</u> del **Corollario 5.5**

La condizione char $F = p$ significa che p è il periodo di 1_F nel gruppo additivo di F. Ora, per per ogni $a \in F$, ed ogni $n \in \mathbb{Z}$, si ha

$$na = (n1_F)a,$$

e questo è nullo se e solo se

- $a = 0,$ oppure
- $a \neq 0$ e $p|n$.

Sia $f(x) = \sum_{i=0}^{n} a_i x^i \in F[x]$. Allora $f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$ è il polinomio nullo se e solo se sono nulli tutti i suoi coefficienti, ossia, se e solo se, per ogni $i = 1, \ldots, n$ tale che $a_i \neq 0$, si ha $p|i$. Ciò avviene se e solo se i termini con coefficiente non nullo sono potenze di x^p, ossia se e solo se $f(x)$ è un polinomio in x^p a coefficienti in F.

Osservazione 5.8

a) Si ha $F \subset L \subset K$, ove K è un'estensione separabile di F. Poiché ogni elemento di L appartiene a K, segue banalmente che L è separabile su F. Sia ora $\alpha \in K$. Siano $p(x)$ e $q(x)$ i polinomi minimi di α su F e su L rispettivamente. Poiché $p(x)$ è, in particolare, un polinomio di $L[x]$ che si annulla in α, segue che allora $q(x)$ è un suo divisore in $L[x]$. Ora, per ipotesi, $p(x)$ è separabile su F, quindi non ha radici multiple nel suo campo di spezzamento. Ciò vale di conseguenza per i suoi fattori irriducibili in $L[x]$. Ma $q(x)$ è il prodotto di alcuni di questi ultimi fattori irriducibili, e quindi è separabile su L. Ciò prova che K è separabile su L.

Esempio 5.15

Supponiamo per assurdo che il polinomio $f(x) = x^2 - t \in \mathbb{Z}_2(t)[x]$ abbia una radice in $\mathbb{Z}_2(t)$. Sia questa $\frac{h(t)}{g(t)}$, per opportuni $h(t), g(t) \in \mathbb{Z}_2[t]$. Allora $\left(\frac{h(t)}{g(t)}\right)^2 = t,$ da cui $h(t)^2 = tg(t)^2$. Ciò è impossibile, in quanto il fattore irriducibile t, nella fattorizzazione del primo membro, compare un numero pari di volte, e un numero dispari di volte nella fattorizzazione del secondo membro.