Lezione 5

Prerequisiti: Caratteristica di un campo. Radici e proprietà di divisibilità per i polinomi a coefficienti in un campo.

Estensioni separabili. Campi perfetti.

Richiamo: Dati un polinomio $f(x) \in F[x]$ (con F campo) ed una sua radice α in un'estensione K di F, α si dice una radice di molteplicità m se, in $K[x]$, $(x-\alpha)^m$ divide $f(x)$, mentre $(x-\alpha)^{m+1}$ non divide $f(x)$. Una radice di molteplicità 1 si dice *semplice*, una radice di molteplicità maggiore di 1 si dice *multipla*.

Definizione 5.1 Sia F un campo, e sia $f(x) \in F[x]$. Il polinomio $f(x)$ si dice *separabile* su F se ogni suo fattore irriducibile è privo di radici multiple in ogni suo campo di spezzamento su F.

Osservazione 5.2 Naturalmente, un polinomio $f(x) \in F[x]$ è separabile se e solo se sono separabili tutti i suoi fattori irriducibili in $F[x]$. Il prodotto di polinomi separabili è separabile. Ogni divisore di un polinomio separabile è separabile.

Diamo ora un criterio necessario e sufficiente di separabilità. Esso è fondato sulla cosiddetta *derivata (formale)* di un polinomio, definita come segue: dato il polinomio

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

si considera

$$f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}.$$

Chiaramente, alle derivate formali si estendono le usuali regole di derivazione. Per la dimostrazione del prossimo risultato, sarà utile il seguente

Lemma 5.3 Dati $f(x), g(x) \in F[x]$, se K è un'estensione di F, si ha

$$\mathrm{MCD}(f(x), g(x)) = 1 \text{ in } F[x] \quad \Leftrightarrow \quad \mathrm{MCD}(f(x), g(x)) = 1 \text{ in } K[x].$$

Dimostrazione: L'implicazione $\Leftarrow$ è ovvia. Per provare l'altra, ricordiamo che, se è vera la prima affermazione, allora, per il Lemma di Bézout, esistono $a(x), b(x) \in F[x]$ tali che $a(x)f(x) + b(x)g(x) = 1$. Poiché i tutti i polinomi considerati appartengono a $K[x]$, segue che il $\mathrm{MCD}(f(x), g(x))$ in $K[x]$ è un divisore di 1, e quindi è 1.

Proposizione 5.4 Sia F un campo, e sia $f(x) \in F[x]$. Allora $f(x)$ ha solo radici semplici in ogni suo campo di spezzamento su F se e solo se $\mathrm{MCD}(f(x), f'(x)) = 1$.

Dimostrazione: Sia K un campo di spezzamento di $f(x)$ su F. Supponiamo dapprima che $f(x)$ abbia un radice α di molteplicità $m>1$ in K. Allora, per definizione, esiste $q(x) \in K[x]$ tale che $f(x) = (x-\alpha)^m q(x)$. Pertanto, derivando, si ottiene

$$f'(x) = m(x-\alpha)^{m-1}q(x) + (x-\alpha)^m q'(x).$$

Segue che $(x-\alpha)^{m-1}$ è un fattore non banale comune a $f(x)$ e $f'(x)$ in $K[x]$. Dunque $\mathrm{MCD}(f(x), f'(x)) \neq 1$ in $K[x]$, e pertanto, in virtù del Lemma 5.3, $\mathrm{MCD}(f(x), f'(x)) \neq 1$ anche in $F[x]$.
Supponiamo ora, invece, che $f(x)$ non abbia radici multiple in K. Sia α una radice di $f(x)$ in K. Allora, come sopra con m=1, si ha $f(x) = (x-\alpha)q(x)$, ove $(x-\alpha)$ non divide $q(x)$, e

$$f'(x) = q(x) + (x-\alpha)q'(x),$$

da cui

$$f'(\alpha) = q(\alpha) \neq 0.$$

Segue che $f(x)$ e $f'(x)$ non hanno radici comuni in K. Ora, se in $K[x]$ avessero in comune un fattore non banale, avrebbero in comune anche le sue radici. Se ne conclude che $f(x)$ e $f'(x)$ sono coprimi in $K[x]$ e quindi in $F[x]$.

Corollario 5.5 Sia $f(x) \in F[x]$ irriducibile. Allora

- se F è di caratteristica 0, $f(x)$ è separabile;
- se F è di caratteristica p>0, $f(x)$ è separabile se e solo se non è della forma $g(x^p)$, per alcun $g(x) \in F[x]$.

Dimostrazione: In base alla Proposizione 5.4, $f(x)$ ha radici multiple nel suo campo di spezzamento su F se e solo se $f(x)$ e $f'(x)$ hanno in comune un fattore non banale. Essendo $f(x)$ irriducibile, questo fattore può essere solo (a meno di costanti moltiplicative non nulle) $f(x)$. Ciò è possibile solo se $f'(x)$=0, perché altrimenti il grado di $f'(x)$ è minore del grado di $f(x)$. In caratteristica 0, ciò avviene se e solo se $f(x)$ è costante, contro l'ipotesi che sia irriducibile. In caratteristica p>0, ciò avviene se e solo se tutti gli esponenti delle potenze di x che compaiono in $f(x)$ con coefficiente non nullo sono multipli di p. □

Esempi 5.6

a) In virtù dell'Osservazione 5.2 e del Corollario 5.5. sono separabili tutti i polinomi non costanti di $\mathbf{Q}[x]$, $\mathbf{R}[x]$, $\mathbf{C}[x]$.

b) In base alla Proposizione 5.4, se F è un campo di caratteristica p>0, il polinomio $f(x) = x^{p^n} - x \in F[x]$ è separabile. Lo avevamo già dimostrato, in maniera diretta, per $F = \mathbf{Z}_p$, al momento di costruire un campo finito di ordine p^n. (vedi Algebra 2, Proposizione 24.5).

Definizione 5.7 Sia F un campo, e sia K una sua estensione. Un elemento $\alpha \in K$ algebrico su F si dice *separabile* su F se il suo polinomio minimo su F è separabile. Se K è un'estensione algebrica di F, K si dice *separabile* se ogni suo elemento è separabile su F.

Osservazione 5.8

a) Se K è un'estensione separabile su F, e L è un campo intermedio tra F e K, allora L è separabile su F e K è separabile su L.
b) Ogni estensione algebrica di un campo di caratteristica 0 è separabile.

c) Ogni campo F di ordine p^n è un'estensione separabile del proprio sottocampo fondamentale, isomorfo a $\mathbf{Z}_p$. Basta ricordare che F è formato dalle radici del polinomio $x^{p^n} - x$, che è separabile.

Definizione 5.9 Un campo si dice *perfetto* se ogni sua estensione algebrica è separabile.

Osservazione 5.10 Un campo F è perfetto se e solo se ogni polinomio $f(x) \in F[x]$ è separabile.

Dall'Osservazione 5.10 e dal Corollario 5.5 segue:

Proposizione 5.11 Ogni campo di caratteristica 0 è perfetto.

Il criterio per i campi di caratteristica positiva è il seguente:

Proposizione 5.12 Un campo F di caratteristica $p>0$ è perfetto se e solo se $F = F^p$ (in altri termini: se e solo se l'omomorfismo di Frobenius è suriettivo).

Dimostrazione: Supponiamo che F sia un campo perfetto. Sia $a \in F$. Proviamo che a ha una radice p-esima in F. Sia K un campo di spezzamento di $f(x) = x^p - a$ su F. Sia $\alpha \in K$ una radice di $f(x)$. Allora in $K[x]$ si ha la decomposizione $f(x) = (x - \alpha)^p$. Il polinomio minimo di α su F è un divisore di $f(x)$ in $F[x]$, quindi, non avendo radici multiple, è necessariamente $x - \alpha$. Segue che $\alpha \in F$, come volevasi.
Viceversa, sia $F = F^p$. Sia K un'estensione algebrica di F, sia $f(x) \in F[x]$ un polinomio minimo su F di un elemento di K. Supponiamo per assurdo che $f(x)$ non sia separabile su F, per il Corollario 5.5 esiste allora $g(x) \in F[x]$ tale che $f(x) = g(x^p)$. Sia $g(x) = \sum_{i=0}^{n} a_i x^i$. Per ipotesi esiste, per ogni $i = 0, \ldots, n$, un elemento $b_i \in F$ tale che $b_i{}^p = a_i$. Allora $f(x) = \sum_{i=0}^{n} a_i x^{pi} = \sum_{i=0}^{n} b_i{}^p x^{pi} = \left(\sum_{i=0}^{n} b_i x^i \right)^p$.
Ma ciò nega l'irriducibilità di $f(x)$. □

Corollario 5.13 Ogni campo finito è perfetto.

Dimostrazione: Basta applicare la Proposizione 5.12, dopo aver ricordato che l'omomorfismo di Frobenius è suriettivo su un campo finito (infatti è sempre iniettivo). □

Poiché un campo algebricamente chiuso non ha estensioni algebriche proprie, dalla Definizione 5.9 segue banalmente:

Corollario 5.14 Ogni campo algebricamente chiuso è perfetto.

Esempio 5.15 Il campo delle funzioni razionali su $\mathbf{Z}_2$, $F = \mathbf{Z}_2(t)$, in base alla Proposizione 5.12, non è un campo perfetto: infatti è un campo di caratteristica 2, e in esso l'elemento t è privo di radici quadrate (provare per esercizio). Verifichiamo che, in effetti, esiste un polinomio $f(x) \in \mathbf{Z}_2(t)[x]$ non separabile.
Sia

$$f(x) = x^2 - t.$$

Osserviamo che il polinomio $f(x)$ è irriducibile su *F*. In base al Corollario 5.5, questo polinomio non è separabile. Effettuiamo anche una verifica diretta, in base alla Definizione 5.1. Sia α una radice di $f(x)$ nel campo di spezzamento *K* di *f* su *F*. Allora, in *K*[*x*],

$$f(x) = (x - \alpha)^2,$$

e quindi $f(x)$ non è separabile su *F*.

Invece il polinomio irriducibile $g(x) = x^3 - t$ è separabile su *F*.

Aggiungiamo, in vista di future applicazioni, il seguente risultato:

Proposizione 5.16 Un'estensione finita generata da elementi separabili è separabile.

Dimostrazione: [Mi2], Corollary 3.12.