

# Corso: Algebra IV

## I1/ Appendici/ Separabilità e inseparabilità

### 1 Campi perfetti

Sia  $F$  un campo di caratteristica  $p$ , con  $p > 0$  primo. Allora esiste l'omomorfismo di Frobenius  $\phi : F \rightarrow F$  tale che  $\phi(a) = a^p$ . Vale che

$$\begin{aligned}\phi(a + b) &= (a + b)^p = a^p + b^p = \phi(a) + \phi(b) \\ \phi(ab) &= (ab)^p = a^p * b^p = \phi(a) * \phi(b)\end{aligned}$$

Inoltre  $\phi(1) = 1$  e in particolare  $\phi$  è iniettivo.

L'immagine di  $\phi$ , indicata con  $F^p$ , è l'insieme  $\{a^p, a \in F\}$  ed è un sottocampo di  $F$ .

#### Definizione 6.1

$F$  si dice *perfetto* se  $F^p = F$ , cioè se  $\phi$  è suriettivo: in altre parole,  $F$  è perfetto se comunque prendo  $a \in F$ , esiste  $b \in F$  tale che  $a = b^p$ .

#### Esempio 6.1

Ogni campo  $F$  finito di caratteristica prima è tale che  $|F| = |F^p|$ , e quindi è perfetto.

#### Esempio 6.2 (esempio di campo non perfetto infinito)

Considero  $F = F_p(t)$  campo delle funzioni razionali a coefficienti in  $F_p$  nell'indeterminata  $t$ . Allora  $t \notin F^p$ . Infatti, se  $t \in F^p$ , esisterebbe  $f(t)/g(t) \in F$  con  $f(t), g(t) \in F[t]$ , tale che  $t = (f(t)/g(t))^p = \frac{f(t)^p}{g(t)^p}$ , cioè  $t * (g(t))^p = (f(t))^p$ , ma questo non può avvenire perché se così fosse si avrebbe  $p \operatorname{gr}(f(t)) = 1 + p * \operatorname{gr}(g(t))$ .

#### Teorema 6.3

Sia  $f(x) \in F(x)$  un polinomio irriducibile e non separabile. Allora  $\operatorname{car} F = p$  primo, e  $F$  non è perfetto (e quindi in particolare non è finito).

*Dimostrazione*



Dire  $f$  irriducibile e non separabile significa che  $f'(x) = 0$ , e quindi necessariamente  $\text{car}F = p$  primo, e  $f(x) = g(x^p)$  per un certo  $g(x) \in F[x]$ . Ora  $g(x)$  è un polinomio della forma  $\sum_i a_i x^i$ ,  $a_i \in F$ . Se  $F$  fosse perfetto, si avrebbe che  $a_i = b_i^p$  per un certo  $b_i \in F$ , e quindi

$$\begin{aligned} f(x) &= \sum_i a_i x^{ip} = \sum_i b_i^p (x^i)^p \\ &= \sum_i (b_i x^i)^p = \left( \sum_i b_i x^i \right)^p = (h(x))^p \end{aligned}$$

dove ho posto  $h(x) = \sum_i b_i x^i$ . Quindi  $f(x) = (h(x))^p$  ma  $f$  è irriducibile quindi questo non può avvenire.

### Corollario 6.1

Sia  $F$  un campo con  $\text{car}F = 0$  o  $\text{car}F = p$  primo e  $F$  perfetto. Allora ogni estensione algebrica di  $F$  è separabile.

*Dimostrazione*

Sia  $E \supseteq F$  un'estensione algebrica di  $F$ , allora ogni  $\alpha \in E$  è algebrico su  $F$ . Il polinomio minimo di  $\alpha$  che è irriducibile in  $F[x]$  dev'essere separabile, altrimenti per il lemma precedente  $F$  non sarebbe perfetto.

### Corollario 6.2

Sia  $F$  un campo con caratteristica prima, e  $f(x) \in F[x]$  un polinomio irriducibile allora  $f(x) = g(x^{p^n})$  per  $n \geq 0$ , e per un certo polinomio  $g(x)$  irriducibile e separabile.

*Dimostrazione*

CASO 1: Se  $f'(x) \neq 0$ ,  $f(x)$  è separabile, allora il risultato è vero se prendo  $n = 0$ , e  $g(x) = f(x)$ .

CASO 2: Se invece  $f'(x) = 0$ ,  $f(x) = h(x^p)$  per un certo  $h(x) \in F[x]$ . Ora  $h(x)$  dev'essere irriducibile, perché se  $h$  ammettesse una fattorizzazione propria, si avrebbe  $h(x) = s(x) * t(x)$ , e  $f(x) = h(x^p) = s(x^p) * t(x^p)$ , ma  $f$  è irriducibile e quindi questo non può avvenire. In particolare  $\text{gr}(h(x)) < \text{gr}(f(x))$ .

Per induzione sul grado, il risultato è vero per  $h(x)$ , cioè posso scrivere  $h(x) = g(x^{p^n})$ , con  $n \geq 0$  e  $g(x)$  separabile e irriducibile. Allora  $f(x) = h(x^p) = g(x^{p^{n+1}})$  e quindi vale l'asserto anche per  $f$ .

## 2 Estensione puramente inseparabile

### Definizione 6.2



Data  $E \supseteq F$  un'estensione algebrica,  $E \supseteq F$  si dice *separabile* (su  $F$ ) se ogni elemento di  $E$  è separabile su  $F$ , ovvero se per ogni  $\alpha \in E$ , il polinomio minimo di  $\alpha$  in  $F[x]$  è un polinomio separabile (su  $F$ ).

### Definizione 6.3

Data  $E \supseteq F$  un'estensione algebrica, dico che  $E \supseteq F$  è *puramente inseparabile* se gli unici elementi di  $E$  separabili su  $F$  sono gli elementi di  $F$  (un'estensione puramente inseparabile ha il minor numero possibile di elementi separabili).

### Esempio 6.3

$F$  come estensione di se stesso è puramente inseparabile.

### Osservazione 6.1

Se  $E \supset F$  è un'estensione algebrica e puramente inseparabile, allora  $\text{car} F = p$  e  $F$  non può essere perfetto per il primo teorema dimostrato.

### Teorema 6.4

Sia  $E \supseteq F$  un'estensione algebrica, con  $F$  campo di caratteristica  $p$  prima. Allora sono equivalenti queste tre affermazioni:

1.  $E$  è puramente inseparabile su  $F$  ;
2. comunque prendo  $\alpha \in E$ ,  $\alpha^{p^n} \in F$  per  $n \geq 0$  ;
3. ogni elemento di  $E$  ha polinomio minimo su  $F$  della forma  $x^{p^n} - a$ , con  $a \in F$  e  $n \geq 0$ .

### Corollario 6.3

Sia  $E = F(\alpha)$  un'estensione semplice, con  $F$  di caratteristica  $p$  primo, e  $\alpha^{p^n} \in F$  per un certo  $n \geq 0$ . Allora  $E$  è puramente inseparabile su  $F$ .

*Dimostrazione*

Sia  $\beta \in E = F(\alpha)$ , **devo mostrare che**  $\beta^{p^n} \in F$ . Infatti, se questo avviene,  $E$  è puramente inseparabile su  $F$  per il teorema appena enunciato.

$\beta \in F(\alpha)$ , allora  $\beta = a_m \alpha^m + a_{m-1} \alpha^{m-1} + \dots + a_1 \alpha + a_0$  con  $a_i \in F$ . Quindi, siccome siamo in caratteristica  $p$

$$\beta^{p^n} = a_m^{p^n} * \alpha^{p^n * m} + a_{m-1}^{p^n} * \alpha^{p^n * (m-1)} + \dots + a_1^{p^n} \alpha^{p^n} + a_0^{p^n} \in F$$

perché per ipotesi  $\alpha^{p^n} \in F$ .

### Esempio 6.4

Per avere un esempio non banale di estensione puramente inseparabile prendo  $F$  un campo di caratteristica  $p$  primo, non perfetto. Allora esiste un elemento



$a \in F \setminus F^p$ . Pongo  $f(x) = x^p - a \in F[x]$ , sia  $M$  il campo di spezzamento per  $f(x)$  su  $F$ , e  $\alpha$  una radice di  $f(x)$ . Considero  $E = F(\alpha)$ . Siccome  $f(\alpha) = 0$ ,  $\alpha^p = a \in F$ , quindi  $E$  è un'estensione di  $F$  puramente inseparabile.

Osservo che  $E \neq F$ , perché  $a \notin F^p$ . Inoltre  $E = F(\alpha)$  è campo di spezzamento per  $f(x)$  su  $F$ , perché  $f(x) = x^p - a$  con  $a = \alpha^p$ , cioè  $f(x) = x^p - \alpha^p = (x - \alpha)^p$ .

Conclusione: se  $F$  è un campo con  $\text{car}F = p$  primo e  $F$  non perfetto, allora  $F$  ammette un'estensione puramente inseparabile non banale.

### 3 Condizioni equivalenti ad essere puramente inseparabile

#### Teorema 6.5

Data un'estensione algebrica  $E \supseteq F$  con  $\text{car}F = p$  primo, allora sono equivalenti

1.  $E \supseteq F$  è puramente inseparabile.
2. per ogni  $\alpha \in E$ , esiste  $n \geq 0$  con  $\alpha^{p^n} \in F$ ;
3. il polinomio minimo su  $F$  di ogni elemento di  $E$  è della forma  $x^{p^n} - a$ ,  $n \geq 0$ ,  $a \in F$

#### Dimostrazione

1  $\longrightarrow$  2 : sia  $\alpha \in E$  e  $f(x)$  il polinomio minimo di  $\alpha$  su  $F$ . Allora per il corollario precedente posso scrivere  $f(x) = g(x^{p^n})$  con  $g(x) \in F[x]$  polinomio irriducibile e separabile. Allora  $g(x)$  è polinomio minimo di  $\alpha^{p^n}$  essendo  $g(x)$  irriducibile e monico, e quindi  $\alpha^{p^n}$  è separabile su  $F$ . Ma per l'ipotesi l'estensione è puramente inseparabile quindi tutti gli elementi separabili su  $F$  stanno in  $F$ , allora  $\alpha^{p^n} \in F$ .

2  $\longrightarrow$  3 : per ipotesi,  $\alpha^{p^n} \in F$ , cioè  $\alpha$  è radice del polinomio  $x^{p^n} - \alpha^{p^n} \in F[x]$ . Ma essendo in caratteristica  $p$ ,  $g(x) = x^{p^n} - \alpha^{p^n} = (x - \alpha)^{p^n}$ , quindi un fattore irriducibile di  $g(x)$  in  $F[x]$  sarà della forma  $f(x) = (x - \alpha)^r$ . Siccome  $f(\alpha) = 0$ , segue che  $f(x)$  è il polinomio minimo di  $\alpha$  su  $F$  e quindi  $f(x)$  è univocamente determinato. Dunque  $f(x)$  è l'unico fattore irriducibile di  $g(x)$  in  $F[x]$  e pertanto  $g(x)$  è una potenza di  $f(x)$ , quindi  $r \mid p^n$  e  $r = p^m$ ,  $m \in \mathbb{N}$ . Segue che  $f(x) = x^{p^m} - a$  con  $a = \alpha^{p^m} \in F$ .

3  $\longrightarrow$  1 : sia  $\alpha \in E$  e supponiamo che  $\alpha$  sia separabile su  $F$ . **Vogliamo mostrare che**  $\alpha \in F$ . Per ipotesi il polinomio minimo di  $\alpha$  su  $F$  è della forma  $f(x) = x^{p^n} - a$ ,  $a \in F$ ,  $n \geq 0$ .

$f(\alpha) = 0$  implica che  $a = \alpha^{p^n}$ . Allora  $f(x) = x^{p^n} - \alpha^{p^n} = (x - \alpha)^{p^n}$ . Se  $n \geq 1$  (e quindi  $p^n > 1$ ),  $(x - \alpha)^2 \mid f(x)$  ma  $f(x)$  dev'essere separabile, allora non può avere radici multiple, rimane provato che  $n = 0$  e  $\alpha \in F$ .

#### Corollario 6.4



Sia  $F$  un campo di caratteristica  $p$ , con  $p$  primo, e  $E$  un'estensione di  $F$  puramente inseparabile. Allora

1. Se  $E \supseteq L \supseteq F$ , allora  $E \supseteq L$  e  $L \supseteq F$  sono puramente inseparabili.
2. se  $|E : F|$  è finito, allora  $|E : F| = p^*$ .

*Dimostrazione*

1.  $E \supseteq F$  è puramente inseparabile, quindi per il teorema appena dimostrato, dato  $\alpha \in E$ , si ha che  $\alpha^{p^n} \in F$  per  $n \geq 0$ . Allora  $\alpha^{p^n} \in L$ , quindi  $E \supseteq L$  è puramente inseparabile. Inoltre se  $\beta \in L$ , si ha  $\beta \in E$ , e siccome  $E \supseteq F$  è puramente inseparabile,  $\beta^{p^m} \in F$  per un certo  $m \geq 0$ , quindi  $L \supseteq F$  è puramente inseparabile.
2. Procediamo per induzione su  $|E : F|$ . Se  $|E : F| = 1$ , allora  $1 = p^0$  e quindi il passo base vale. Altrimenti, prendo  $\alpha \in E \setminus F$ , allora per la condizione 3 del teorema precedente, il polinomio minimo di  $\alpha$  su  $F$  è della forma  $x^{p^n} - a$ . Quindi  $|F(\alpha) : F| = p^n$ . Considero la catena di estensioni  $E \supseteq F(\alpha) \supseteq F$ . Per la prima parte di questo corollario,  $E \supseteq F(\alpha)$  è puramente inseparabile, e ha grado  $< |E : F|$  perché ho scelto  $\alpha \in E \setminus F$ , allora per induzione  $|E : F(\alpha)| = p^m$  e il resto segue dal teorema della torre, cioè  $|E : F| = p^{n+m}$ .

**Corollario 6.5** (transitività delle estensioni puramente inseparabili)

Data la catena di estensioni  $E \supseteq L \supseteq F$ , con  $E \supseteq L$  e  $L \supseteq F$  estensioni puramente inseparabili, allora  $E \supseteq F$  è puramente inseparabile.

*Dimostrazione*

Sia  $E \supseteq F$ , e  $E \neq F$ , allora  $L \supset F$  oppure  $E \supset L$ , da cui segue che  $\text{car} F = p$  (voglio escludere il caso di caratteristica 0). Data  $\alpha \in E$ ,  $\alpha^{p^n} \in L$ , ma  $E \supseteq L$  è puramente inseparabile quindi posso applicare questa proprietà ad  $\alpha^{p^n}$ , cioè  $(\alpha^{p^n})^{p^m} = \alpha^{p^{n+m}} \in F$ , e quindi  $E \supseteq F$  è puramente inseparabile.

## 4 Proprietà del campo degli elementi separabili su $F$

Sia  $E \supseteq F$  un'estensione algebrica, e considero l'insieme

$$S = \{\alpha \in E \text{ t.c. } \alpha \text{ separabile su } F\}$$

Allora  $S$  è un campo, ed è l'unico campo con  $E \supseteq S \supseteq F$ ,  $E \supseteq S$  puramente inseparabile e  $S \supseteq F$  separabile.

Per dimostrare questo fatto è necessario il seguente lemma:

**Lemma 6.1**



Sia  $E = F(\alpha, \beta)$  con  $\alpha, \beta$  separabili su  $F$ , allora  $E \supseteq F$  è separabile.

*Dimostrazione*

Siano  $f(x), g(x)$  i polinomi minimi di  $\alpha$  e  $\beta$  rispettivamente su  $F$ , e sia  $h(x) = f(x) * g(x) \in F[x]$ .

Sia  $L$  campo di spezzamento per  $h(x)$  su  $F$ . Ora  $h(x)$  è un polinomio i cui fattori irriducibili,  $f, g$ , sono separabili su  $F$ , allora  $L \supseteq F$  è normale di grado finito.

Se considero la catena di estensioni  $L \supseteq E \supseteq F$ , con  $L \supseteq F$  separabile, segue che anche  $E \supseteq F$  è separabile.

### **Teorema 6.6**

Sia  $E \supseteq F$  un'estensione algebrica, e sia

$$S = \{\alpha \in E \text{ t.c. } \alpha \text{ separabile su } F\}$$

Allora  $S$  è un campo, ed è l'unico campo intermedio  $E \supseteq S \supseteq F$  tale che  $E \supseteq S$  è puramente inseparabile e  $S \supseteq F$  è separabile.

*Dimostrazione*

1. Per dimostrare che  $S$  è **un campo**, basta mostrare che, dati  $\alpha, \beta \in S$ ,  $\alpha - \beta \in S$  e  $\alpha\beta^{-1} \in S$  per  $\beta \neq 0$ . Considero  $F(\alpha, \beta)$ , che è un'estensione separabile di  $F$  per il lemma precedente.  $F(\alpha, \beta)$  contiene  $\alpha - \beta$  e  $\alpha\beta^{-1}$ , e quindi sono separabili su  $F$ . In particolare stanno in  $S$ .
2. ovviamente  $S \supseteq F$  è **separabile** per come  $S$  è definito.
3. Rimane da provare che  $E \supseteq S$  è **puramente inseparabile**. Possiamo assumere che  $\text{Car}F = p$ , perché in caratteristica 0,  $S$  esaurisce tutti gli elementi di  $E$ . Sia  $\alpha \in E$ , e considero  $f(x)$  polinomio minimo di  $\alpha$  su  $F$ . Si avrà  $f(x) = g(x^{p^n})$  con  $g(x)$  monico, irriducibile e separabile. Inoltre  $0 = f(\alpha) = g(\alpha^{p^n})$ , allora  $g$  è il polinomio minimo di  $\alpha^{p^n}$  ed è separabile, quindi  $\alpha^{p^n}$  è separabile su  $F$ , cioè per definizione  $\alpha^{p^n} \in S$ , quindi  $E \supseteq S$  è puramente inseparabile perché vale la condizione 3 del teorema.
4. **Mostriamo l'unicità di  $S$** . Sia  $T$  un campo con  $E \supseteq T \supseteq F$ , con  $T \supseteq F$  separabile e  $E \supseteq T$  puramente inseparabile. Mostriamo che  $T = S$ . Dal fatto che  $T \supseteq F$  è separabile, segue che tutti gli elementi di  $T$  sono separabili su  $F$ , quindi  $T \subseteq S$ . Allora considero la catena di estensioni  $E \supseteq S \supseteq T$ : siccome  $E \supseteq T$  è puramente inseparabile, anche  $S \supseteq T$  lo è. Considero ora la catena di estensioni  $S \supseteq T \supseteq F$ , siccome  $S \supseteq F$  è separabile, anche  $S \supseteq T$  è separabile. Allora  $S = T$  perché  $S$  è contemporaneamente separabile e puramente inseparabile su  $T$ .

### **Corollario 6.6**

Sia  $E \supseteq F$  un'estensione di grado finito e non separabile, allora  $\text{car}F \mid |E : F|$ .



*Dimostrazione*

Siccome per ipotesi l'estensione è non separabile, si ha che  $\text{Car}F = p$  primo. Sia  $S$  l'insieme degli elementi di  $E$  separabili su  $S$ , allora  $E \neq S$ ,  $E \supseteq S$  è puramente inseparabile e  $|E : S| = p^*$ . Dal teorema della torre segue che  $\text{car}F = p \mid |E : S| \mid |E : F| = |E : S| * |S : F|$ .

### Proposizione 6.2

Sia  $E \supseteq L \supseteq F$  una catena di estensioni con  $E \supseteq L$  separabile e  $L \supseteq F$  separabile, allora  $E \supseteq F$  è separabile.

*Dimostrazione*

Sia  $S$  l'insieme degli elementi di  $E$  separabili su  $F$ . Siccome  $L \supseteq F$  è separabile, segue che  $L \subseteq S$ , allora posso considerare la catena di estensioni  $E \supseteq S \supseteq L$ . Siccome  $E \supseteq L$  è separabile segue che  $E \supseteq S$  è separabile per un argomento già visto. Inoltre  $E \supseteq S$  è puramente inseparabile e unendo le due condizioni si ha  $E = S$ , e quindi  $E \supseteq F$  è separabile.

## 5 Grado di separabilità

### Definizione 6.4

Sia  $E \supseteq F$  un'estensione di grado finito, e sia  $S$  l'insieme degli elementi di  $E$  separabili su  $F$ . Si dice *grado di separabilità* di  $E$  su  $F$  il grado di  $S$  su  $F$ , cioè  $|E : F|_s = |S : F|$ .

L'estensione  $E \supseteq F$  è separabile se e solo se  $|E : F| = |E : F|_s$ . In generale  $|E : F|_s \mid |E : F|$ , e il quoziente  $\frac{|E:F|}{|E:F|_s}$  è una potenza di  $p$ .

### Lemma 6.2

Sia  $E \supseteq F$  un'estensione puramente inseparabile, e sia  $f(x) \in F[x]$  monico, irriducibile e separabile. Allora  $f(x)$  è irriducibile in  $E[x]$ .

*Dimostrazione*

Sia  $g(x)$  un fattore monico e irriducibile di  $f(x)$  in  $E[x]$ , e **mostriamo che**  $g = f$ , provando così che  $f$  rimane irriducibile in  $E[x]$ . Sia  $M$  il campo di spezzamento per  $f(x)$  su  $E$ , quindi  $M \supseteq E \supseteq F$ . Allora in  $M$ , posso scrivere  $g(x) = \prod_i (x - \alpha_i)$  dove gli  $\alpha_i$  sono radici di  $g(x)$  e quindi anche di  $f(x)$ .

Sia

$$S = \{\beta \in M \text{ t.c. } \beta \text{ separabile su } F\}$$

e voglio mostrare che  $g(x) \in S[x]$ . Gli  $\alpha_i$ , radici di  $g$ , sono anche radici di  $f$ . Ora  $f$  è polinomio minimo di ciascuna sua radice in particolare di ciascun  $\alpha_i$ .



Per ipotesi  $f(x)$  è separabile su  $F$ , allora gli  $\alpha_i$  stanno in  $S$ ,  $x - \alpha_i \in S[x]$  allora  $g(x) \in S[x]$ . Inoltre  $g(x) \in E[x]$  quindi i coefficienti di  $g$  stanno in  $S \cap E$ .

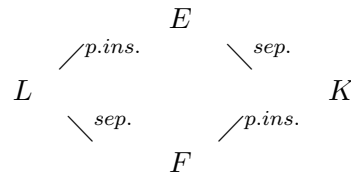
Concludo che  $E \cap S = F$  infatti valgono questi fatti:

1.  $E \supseteq E \cap S \supseteq F$  e  $E \supseteq F$  è puramente inseparabile, allora  $E \cap S \supseteq F$  è puramente inseparabile.
2. per costruzione  $S \supseteq F$  è separabile, e quindi anche  $E \cap S \supseteq F$  è separabile.

Allora  $E \cap S = F$ , cioè  $g(x) \in F[x]$ , allora  $g = f$ .

### Teorema 6.7

Sia  $E \supseteq F$  un'estensione di grado finito, e siano  $K, L$  campi intermedi tra  $E$  ed  $F$  con  $E \supseteq L$  puramente inseparabile,  $L \supseteq F$  separabile,  $E \supseteq K$  separabile,  $K \supseteq F$  puramente inseparabile, come mostra lo schema seguente:



Allora  $|L : F| = |E : K|$ .

*Dimostrazione*

Mostro le due disuguaglianze:

**DISUGUAGLIANZA 1:**  $|L : F| \leq |E : K|$ : Sia  $\alpha \in L$ , e sia  $f(x) \in F[x]$  il suo polinomio minimo. Siccome  $K \supseteq F$  è puramente inseparabile,  $f(x)$  rimane irriducibile come polinomio in  $K[x]$ . Allora  $|F(\alpha) : F| = |K(\alpha) : K|$ . Per il teorema dell'elemento primitivo, siccome  $L \supseteq F$  è separabile, posso scrivere  $L = F(\alpha)$  (con abuso di notazione). Allora  $|L : F| = |F(\alpha) : F| = |K(\alpha) : K| \leq |E : K|$ . **DISUGUAGLIANZA 2:**  $|E : K| \leq |L : F|$ :  $E \supseteq K$  e per il teorema dell'elemento primitivo posso scrivere  $E = K(\beta)$  per un certo  $\beta$ .  $E \supseteq L$  è puramente inseparabile, allora  $\beta^{p^n} \in L$  per un certo  $n \geq 0$ ,  $p = \text{car}F$  (se  $\text{car}F = 0$ ,  $L = E$  e  $K = F$ ). Considero  $E = K(\beta) \supseteq K(\beta^{p^n})$ . Da un lato, siccome  $\beta^{p^n} \in K(\beta^{p^n})$ ,  $E \supseteq K(\beta^{p^n})$  è puramente inseparabile; d'altra parte  $E \supseteq K(\beta^{p^n}) \supseteq K$ , e siccome  $E \supseteq K$  è separabile, lo è anche  $E \supseteq K(\beta^{p^n})$ . Deduco che  $E = K(\beta^{p^n})$ .

Quindi

$$|E : K| = |K(\beta^{p^n}) : K| = |F(\beta^{p^n}) : F| \leq |L : F|$$

perché  $\beta^{p^n} \in L$ . Noto anche che la seconda uguaglianza segue dallo stesso argomento usato all'inizio di questa dimostrazione.

**Teorema 6.8** (moltiplicatività del grado di separabilità)

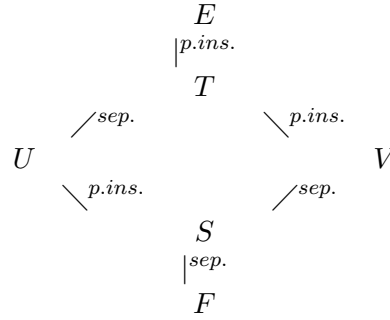




Siano  $E \supseteq U \supseteq F$  campi con  $|E : F|$  finito. Allora  $|E : F|_s = |E : U|_s * |U : F|_s$ .

*Dimostrazione*

Considero lo schema seguente:



Considero  $E \supseteq U$ , e chiamo

$$T = \{\beta \in E \text{ t.c. } \beta \text{ separabile su } U\}$$

allora segue che  $E \supseteq T$  è puramente inseparabile,  $T \supseteq U$  è separabile.

Considero poi  $U \supseteq F$ , e pongo

$$S = \{\alpha \in U \text{ t.c. } \alpha \text{ separabile su } F\}$$

allora segue che  $U \supseteq S$  è puramente inseparabile e  $S \supseteq F$  è separabile.

Considero la catena di estensioni

$$E \supseteq T \supseteq U \supseteq S \supseteq F$$

e pongo

$$V = \{\gamma \in T \text{ t.c. } \gamma \text{ separabile su } S\}$$

allora  $T \supseteq V$  è puramente inseparabile, mentre  $V \supseteq S$  è separabile.

Ogni pezzo della catena di estensioni  $V \supseteq S \supseteq F$  è separabile. Allora  $V \supseteq F$  è **separabile** per transitività.

Se considero  $E \supseteq T \supseteq V$ ,  $E \supseteq T$  è puramente inseparabile e  $T \supseteq V$  è puramente inseparabile, allora  $E \supseteq V$  è **puramente inseparabile**. Per l'unicità del campo intermedio  $V$  che soddisfa queste due condizioni segue che

$$V = \{\gamma \in E \text{ t.c. } \gamma \text{ separabile su } F\}$$

Segue che  $|E : F|_s = |V : F|$ , inoltre per il teorema della torre

$$|V : F| = |V : S| * |S : F| = |V : S| * |U : F|_s,$$



---

ma  $|V : S| = |T : U|$  per il teorema precedente, e  $|T : U| = |E : U|_s$  cioè, unendo queste formule,  $|E : F|_s = |E : U|_s * |U : F|_s$ .



---

## 6 Fonti per testo e immagini; autori; licenze

### 6.1 Testo

- **Corso:Algebra IV I1/Appendici/Separabilità e inseparabilità** *Fonte:* [https://it.wikitolearn.org/Corso%3AAlgebra\\_IV\\_I1/Appendici/Separabilit%C3%A0\\_e\\_inseparabilit%C3%A0?oldid=48536](https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Appendici/Separabilit%C3%A0_e_inseparabilit%C3%A0?oldid=48536) *Contributori:* Toma.luca95, ScimmiaSpaziale e Mmontrasio

### 6.2 Immagini

### 6.3 Licenza dell'opera

- [Project:Copyright Creative Commons Attribution Share Alike 3.0 & GNU FDL]
- Creative Commons Attribution-Share Alike 3.0

