ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

FACOLTÀ DI SCIENZE
Corso di Laurea in Matematica

Estensioni trascendenti di campi

Tesi in Algebra

Relatore:
Prof.ssa MARTA MORIGI

Candidato:
Alessandro Frassineti

Anno Accademico 2020-2021

Alla mia famiglia

Indice

Introduzione

Supponiamo di avere un campo K e un polinomio $f \in K[x]$ irriducibile, è noto che il quoziente $K[x]/(f)$ è un campo che contiene una copia isomorfa $K + (f)$ di K e un elemento $\alpha = [x]$ che è radice di f. D'altra parte, se abbiamo un'estensione di campi $K \subseteq F$ con F che contiene una radice α di f, allora il "più piccolo" sottocampo di F contenente α e K, che denotiamo con $K[\alpha]$, si dimostra essere isomorfo a $K[x]/(f)$. Questa si dice *estensione semplice* di K, ed inoltre risulta essere uno spazio vettoriale su K di dimensione pari al grado di f. Il ragionamento si può iterare fino a considerare estensioni di K con una quantità numerabile di elementi *algebrici* su K, costruendo ancora spazi vettoriali su K, talvolta di dimensione infinita.
Se però consideriamo l'anello dei polinomi $K[x]$, essendo un dominio d'integrità possiamo costruire il cosiddetto *campo dei quozienti*, che è anch'esso un'estensione di K. Questo tipo di estensione è profondamente diverso dai precedenti in quanto x non è radice di polinomi in K. Un elemento con questa proprietà si dice *trascendente* su K e le estensioni che contengono elementi di questo tipo si dicono *estensioni trascendenti*.
Dopo aver dato nel primo capitolo alcune definizioni e nozioni di base, nel secondo capitolo studieremo le principali proprietà delle estensioni trascendenti. In particolare il fatto che ogni estensione di campi si possa spezzare in un'estensione *puramente trascendente* e in una algebrica. Verrà poi intro-

dotto il *grado di trascendenza* di un'estensione, che non dipende dalla scelta di suddivisione sopra descritta.

Nel terzo capitolo ci poniamo invece l'obiettivo di estendere la definizione di *estensione separabile*, riservata alle sole estensioni algebriche, ad un'estensione qualsiasi. Per fare ciò introdurremo la nozione di campi *linearmente disgiunti*. Lavoreremo prevalentemente con campi di caratteristica $p \neq 0$, in quanto nei campi di caratteristica 0 si dimostra che l'estensione della definizione è una condizione sempre verificata, così come avveniva nel caso di estensioni algebriche di campi di caratteristica 0. Vedremo che anche altre proprietà della separabilità si conservano, come la transitività e la stretta relazione con i campi perfetti.

L'intero elaborato è ispirato all'esposizione di Thomas W. Hungerford nel Capitolo VI del suo *Algebra*, mentre alcuni degli ultimi risultati esposti sono attribuiti al matematico Saunders Mac Lane.

Capitolo 1

Nozioni preliminari

1.1 Definizioni e risultati di base

Definizione 1.1.1. Dato un insieme non vuoto X, una relazione d'ordine $\leq$ su X si dice essere un **buon ordinamento** se ogni sottoinsieme non vuoto di X ha un minimo secondo questa relazione.

Teorema 1.1.2. *Le seguenti affermazioni sono equivalenti:*

i) **(Assioma della scelta)** *Data una famiglia non vuota di insiemi non vuoti esiste una funzione che ad ogni insieme fa corrispondere un suo elemento;*

ii) **(Lemma di Zorn)** *Se $(X, \leq)$ è un insieme parzialmente ordinato e non vuoto tale che ogni catena possiede un maggiorante in X, allora X ha un elemento massimale;*

iii) **(Teorema del buon ordinamento)** *Su ogni insieme non vuoto è possibile definire un buon ordinamento.*

Dimostrazione. Si vedano i paragrafi 8.2 e 8.3 di [1]. □

Per i risultati qui esposti assumeremo valide queste tre affermazioni.

Definizione 1.1.3. Siano K e L sottocampi di F, definiamo **campo composito** di K e L in F come il sottocampo di F generato da $K \cup L$. Lo denotiamo con KL.

Osservazione 1.1.4. Immediata conseguenza della definizione è la sua simmetria, ossia $KL = LK$. Inoltre abbiamo che $KL = K(L) = L(K)$.

Da qui in avanti i simboli x, y, x_i, y_i con $i = 0, 1, 2, ...$ indicheranno delle indeterminate.

Osservazione 1.1.5. Fissato un anello commutativo R, l'anello dei polinomi in n indeterminate $(R[x_1, ..., x_n], +, \cdot)$ è una R-algebra.

Proposizione 1.1.6 (Proprietà universale)**.** *Dati due anelli commutativi con unità R e S, un morfismo di anelli $\varphi : R \to S$ e una n-upla $(a_1, ..., a_n)$ di elementi di S esiste un unico morfismo di anelli $\overline{\varphi} : R[x_1, ..., x_n] \to S$ che estende φ e tale che l'immagine di x_i sia a_i.*

Dimostrazione. Si veda il Teorema 5.5 del Capitolo III di [2]. □

Teorema 1.1.7 (Lemma di Gauss)**.** *Sia A un dominio a fattorizzazione unica e sia K il suo campo dei quozienti, se $f \in A[x]$ è un polinomio primitivo, ossia tale che il massimo comune divisore tra i suoi coefficienti è 1, allora f è irriducibile su A se e solo se lo è su K.*

Dimostrazione. Si veda il Lemma 6.13 del Capitolo III di [2]. □

1.2 Estensioni di campi

Definizione 1.2.1. Un campo C si dice **algebricamente chiuso** se ogni polinomio di grado positivo a coefficienti in C ha tutte le radici in C.

Sia F un'estensione algebrica di K, F si dice **chiusura algebrica** di K se è algebricamente chiuso.

Teorema 1.2.2. *Sia F un'estensione di K, le seguenti condizioni sono equivalenti:*

i) F è algebrico su K e F è algebricamente chiuso;

ii) F è il campo di spezzamento su K dell'insieme di tutti i polinomi in $K[x]$.

Dimostrazione. $(i) \Rightarrow (ii)$ Se F è algebricamente chiuso in particolare contiene tutte le radici dei polinomi in $K[x]$. Poiché è inoltre un'estensione algebrica di K lo si ottiene estendendo K con tutti e soli gli elementi di F algebrici su K.
$(ii) \Rightarrow (i)$ Dato che F è un campo di spezzamento di un insieme di polinomi in $K[x]$ è un'estensione algebrica di K. Sia $f \in F[x]$ e sia α una sua radice in una qualche estensione di F, allora $F[\alpha]$ è un'estensione algebrica di F e quindi di K. Questo implica che α è radice di un polinomio a coefficienti in K e quindi deve appartenere a F, ossia F è algebricamente chiuso. □

Proposizione 1.2.3. *Dato un campo K esiste (ed è unico a meno di isomorfismo) un campo C algebricamente chiuso estensione algebrica di K.*

Dimostrazione. Si veda il Teorema 3.6 del Capitolo V di [2]. □

Teorema 1.2.4 (Lemma di Estensione)**.** *Dato un isomorfismo di campi $\varphi : K_1 \to K_2$ con $K_i \subseteq C_i$, consideriamo un polinomio irriducibile $f \in K_1[x]$ con una radice $\alpha \in C_1$. Sia $\beta \in C_2$ una radice di $\varphi(f) \in K_2[x]$, allora esiste un unico isomorfismo di campi $\overline{\varphi} : K_1[\alpha] \to K_2[\beta]$ che estende φ e tale che $\overline{\varphi}(\alpha) = \beta$.*

Dimostrazione. Si veda il Teorema 1.8 del Capitolo V di [2]. □

Corollario 1.2.5. *Se in aggiunta alle ipotesi del Teorema 1.2.4 supponiamo che C_i sia chiusura algebrica di K_i, allora φ si estende ad un isomorfismo tra C_1 e C_2.*

Dimostrazione. Supponiamo dapprima che C_1 sia il campo di spezzamento di una famiglia di polinomi $S_1 \subseteq K_1[x]$ e che C_2 sia il campo di spezzamento su K_2 di $S_2 = \{\varphi(f) \mid f \in S_1\}$, e dimostriamo che φ si estende ad un isomorfismo tra C_1 e C_2. Se S_1 consiste di un solo polinomio allora il risultato è vero per il Teorema 1.2.4. Se S_1 è un sottoinsieme qualsiasi di $K_1[x]$, sia X la famiglia delle terne (E_1, E_2, τ) dove E_i è un campo intermedio tra K_i e C_i e $\tau : E_1 \to E_2$ è un isomorfismo che estende φ. Su X definiamo la relazione d'ordine $(E_1, E_2, \tau) \leq (E_1', E_2', \tau')$ se e solo se $E_1 \subseteq E_2'$, $E_1 \subseteq E_2'$ e $\tau'_{|E_1} = \tau$. Consideriamo una catena in X e consideriamo la terna che ha come primo elemento l'unione U_1 di tutti i primi elementi delle terne che compongono la catena, come secondo elemento l'unione U_2 di tutti i secondi elementi delle terne che compongono la catena, e come terzo elemento l'applicazione $\rho : U_1 \to U_2$ tale che, per ogni $u \in U_1$, $\rho(u) = \tau(u)$, con τ un isomorfismo relativo a un campo intermedio contenente u. Osserviamo che la terna così costruita appartiene ancora a X ed è un maggiorante della catena. Perciò per il Lemma di Zorn esiste un elemento massimale $(F, G, \sigma) \in X$. Ora, se $F \neq C_1$, esiste un polinomio $f \in S_1$ che non si spezza su F, e quindi C_1 contiene un campo di spezzamento F' di f su F. Poiché anche $\sigma(f)$ non si spezza su G, C_2 contiene un campo di spezzamento G' di $\sigma(f)$ su G. Per quanto visto ad inizio dimostrazione possiamo allora estendere σ a $\overline{\sigma} : F' \to G'$, ma questo contraddice la massimalità di (F, G, σ). Perciò abbiamo che $F = C_1$ e allo stesso modo otteniamo che $G = C_2$. Scegliendo come S_1 la famiglia di tutti i polinomi in $K_1[x]$ otteniamo la tesi. □

Lemma 1.2.6. *Sia K un campo di caratteristica $p \neq 0$ e sia F una sua estensione. Sia $a \in F$ tale che $a^{p^s} \in K$, se k è il minimo intero con questa proprietà allora $p_K = x^{p^k} - a^{p^k}$ è irriducibile su K.*

Dimostrazione. Visto in $F[x]$, $p_K = (x-a)^{p^k}$ quindi ogni suo fattore proprio è della forma $(x-a)^{p^r m}$ con m e p coprimi e $r < k$. Poiché $(x-a)^{p^r m} = \left(x^{p^r} - a^{p^r}\right)^m$, se questo fattore appartenesse a $K[x]$ si avrebbe $a^{p^r m} \in K$. Per l'identità di Bézout esistono due interi s e t tali che $1 = ms + pt$, da cui si ha

$$a^{p^{k-1}} = a^{p^{k-1}(ms+pt)} = \left(a^{p^{k-1}m}\right)^s \left(a^{p^k}\right)^t = \left(a^{p^r m}\right)^{p^{k-1-r}s} \left(a^{p^k}\right)^t.$$

Poiché $a^{p^r m}, a^{p^k} \in K$, abbiamo che anche $a^{p^{k-1}} \in K$, che è assurdo per la scelta di k. □

Definizione 1.2.7. Dato un campo K, un polinomio irriducibile $f \in K[x]$ si dice **separabile** se in un qualche campo di spezzamento di f su K ogni sua radice è semplice.
Data un'estensione di campi $K \subseteq F$, un elemento di F algebrico su K si dice **separabile** se il suo K-polinomio minimo è separabile. Se inoltre F è un'estensione algebrica di K e ogni suo elemento è separabile su K allora F si dice **separabile** su K.

Definizione 1.2.8. Un campo K si dice **perfetto** se ogni polinomio in $K[x]$ irriducibile è separabile.

Osservazione 1.2.9. Se K ha caratteristica 0 allora è un campo perfetto.

Proposizione 1.2.10. *Un campo di caratteristica $p \neq 0$ è perfetto se e solo se l'endomorfismo di Frobenius $\mathcal{F} : K \to K$, $\mathcal{F}(a) = a^p$ è suriettivo, ossia se e solo se $K = K^p$.*

Dimostrazione. Osserviamo innanzitutto che $\mathcal{F}$ è un morfismo di campi iniettivo, infatti si ha che $(ab)^p = a^p b^p$ e $(a+b)^p = a^p + b^p$ per ogni $a, b \in K$. Inoltre se $a^p = b^p$ allora $(a-b)^p = 0$ e quindi $a = b$.

Se $\mathcal{F}$ non è suriettivo allora esiste $a \in K \setminus K^p$ e, per il Lemma 1.2.6, $x^p - a$ è irriducibile su K. In un campo di spezzamento esiste b tale che $b^p = a$ e $x^p - a = (x-b)^p$ che quindi non è separabile.

Supponiamo ora di avere un polinomio $g \in K[x]$ con radici multiple, allora $g \in K[x^p]$, $g = a_n x^{np} + ... + a_1 x^p + a_0$. Se $\mathcal{F}$ è suriettivo esistono opportuni $b_i \in K$ tali che $g = a_n x^{np} + ... + a_1 x^p + a_0 = b_n^p x^{np} + ... + b_1^p x^p + b_0^p = (b_n x^n + ... + b_1 x + b_0)^p$. Perciò ogni polinomio con radici multiple è riducibile e quindi K è perfetto. □

Capitolo 2

Basi di trascendenza

2.1 Definizioni e primi risultati

Definizione 2.1.1. Sia F un'estensione di K, diciamo che un sottoinsieme S di F è **algebricamente dipendente** su K se esistono $s_1, ..., s_n \in S$ ed esiste un polinomio non nullo $f \in K[x_1, ..., x_n]$ tali che $f(s_1, ..., s_n) = 0$.
Diciamo che S è **algebricamente indipendente** su K se non è algebricamente dipendente.

Osservazione 2.1.2. S è algebricamente indipendente su K se e solo se per ogni $\{s_1, ..., s_n\} \subseteq S$ e per ogni $f \in K[x_1, ..., x_n]$, se $f(s_1, ..., s_n) = 0$ si ha $f = 0$.

Osservazione 2.1.3. Il singoletto $\{u\} \subseteq F$ è algebricamente dipendente su K se e solo se u è algebrico su K.
Ogni elemento di un insieme algebricamente indipendente su K è trascendente su K.

Teorema 2.1.4. *Se* $\{s_1, ..., s_n\}$ *è algebricamente indipendente su* K *allora* $K(x_1, ..., x_n)$ *e* $K(s_1, ..., s_n)$ *sono isomorfi tramite un isomorfismo che fissa gli elementi di* K*.*

Dimostrazione. Per la Proposizione 1.1.6, la mappa $x_i \longmapsto s_i$ si estende a un morfismo di anelli $\varphi : K[x_1, ..., x_n] \longrightarrow K[s_1, ..., s_n]$ che fissa ogni elemento di K. Un generico elemento di $K[s_1, ..., s_n]$ è $f(s_1, ..., s_n)$ con $f \in K[x_1, ..., x_n]$, perciò $f(s_1, ..., s_n) = \varphi(f)$, ossia φ è suriettiva.
Siano $f, g \in K[x_1, ..., x_n]$, se $f(s_1, ..., s_n) - g(s_1, ..., s_n) = 0$ allora $f - g \in K[x_1, ..., x_n]$ e $(f - g)(s_1, ..., s_n) = 0$. Questo, per l'ipotesi di indipendenza algebrica, implica $f = g$, perciò φ è iniettiva. Estendiamo ora φ a $\overline{\varphi} : K(x_1, ..., x_n) \longrightarrow K(s_1, ..., s_n)$ definendo $\overline{\varphi}(fg^{-1}) = \varphi(f)\varphi(g)^{-1}$. Otteniamo che $\overline{\varphi}$ è un isomorfismo di campi che fissa K. □

Corollario 2.1.5. *Per i=1,2 sia* F_i *un'estensione di* K_i *e sia* S_i *algebricamente indipendente su* K_i*. Se* $\eta : S_1 \longrightarrow S_2$ *è una mappa iniettiva e* $\sigma : K_1 \longrightarrow K_2$ *è un morfismo iniettivo di campi, allora* σ *si estende ad un morfismo iniettivo di campi* $\overline{\sigma} : K_1(S_1) \longrightarrow K_2(S_2)$ *tale che* $\overline{\sigma}(s) = \eta(s)$ *per ogni* $s \in S_1$*. Inoltre se* η *è biettiva e* σ *è un isomorfismo, allora* $\overline{\sigma}$ *è un isomorfismo.*

Dimostrazione. Per ogni intero $n \geq 1$, σ induce un morfismo iniettivo da $K_1(x_1, ..., x_n)$ a $K_2(x_1, ..., x_n)$, che chiamiamo ancora σ. Un generico elemento di $K_1(S_1)$ è $f(s_1, ..., s_n)(g(s_1, ..., s_n))^{-1}$ con $s_1, ..., s_n \in S_1$. Perciò definiamo $\overline{\sigma} : K_1(S_1) \longrightarrow K_2(S_2)$ come:

$$f(s_1, ..., s_n)(g(s_1, ..., s_n))^{-1} \longmapsto (\sigma f)(\eta s_1, ..., \eta s_n)((\sigma g)(\eta s_1, ..., \eta s_n))^{-1}.$$

Osserviamo che $\overline{\sigma}(s) = \eta(s)$ per ogni $s \in S_1$.

Consideriamo i due morfismi di valutazione $\varphi_1 : K_1(x_1, ..., x_n) \longrightarrow K_1(s_1, ..., s_n)$ e $\varphi_2 : K_2(x_1, ..., x_n) \longrightarrow K_2(\eta s_1, ..., \eta s_n)$, per il Teorema 2.1.4 sono entrambi isomorfismi. L'applicazione $\varphi_2 \circ \sigma \circ \varphi_1^{-1} : K_1(s_1, ..., s_n) \longrightarrow K_2(\eta s_1, ..., \eta s_n)$ è quindi ben definita e coincide con $\overline{\sigma}$ ristretta a $K_1(s_1, ..., s_n)$ per ogni $\{s_1, ..., s_n\} \subseteq S_1$. Per l'iniettività di η, φ_2 è univocamente determinata una volta fissato $f(s_1, ..., s_n)(g(s_1, ..., s_n))^{-1} \in K_1(S_1)$, e anche φ_1 e σ, perciò $\overline{\sigma}$ è un morfismo iniettivo. Se inoltre σ è un isomorfismo, allora $\varphi_2 \circ \sigma \circ \varphi_1^{-1}$ è un isomorfismo. Infine, supponendo che η sia biettiva, possiamo costruire allo stesso modo di prima l'inversa di $\overline{\sigma}$, che diventa quindi un isomorfismo. □

Definizione 2.1.6. Sia F un'estensione di K, un sottoinsieme S di F si dice **base di trascendenza** di F su K se è algebricamente indipendente su K ed è massimale rispetto all'inclusione nella famiglia di tutti i sottoinsiemi di F algebricamente indipendenti su K.

Osservazione 2.1.7. Poiché il passaggio a sottoinsiemi conserva l'indipendenza algebrica, l'insieme vuoto è algebricamente indipendente su ogni campo. In particolare, F è un'estensione algebrica di K se e solo se l'insieme vuoto è una base di trascendenza, e in tal caso è anche l'unica.

Proposizione 2.1.8. *Sia F un'estensione di K, allora:*

i) esiste una base di trascendenza di F su K.

ii) ogni sottoinsieme di F algebricamente indipendente su K può essere completato ad una base di trascendenza di F su K.

Dimostrazione. La famiglia di tutti i sottoinsiemi di F algebricamente indipendenti su K è un insieme non vuoto parzialmente ordinato con la relazione d'ordine data dall'inclusione. Consideriamo ora una catena di sottoinsiemi

e l'unione S di tutti gli elementi della catena. Questo è ancora un sottoinsieme di F e se dimostriamo che è algebricamente indipendente su K allora per il Lemma di Zorn abbiamo l'esistenza di una base di trascendenza. Sia $\{s_1, ..., s_n\} \subseteq S$ e sia $f \in K[x_1, ..., x_n]$ tale che $f(s_1, ..., s_n) = 0$. Per ogni $j = 1, ..., n$ esiste un insieme S_{i_j} nella catena tale che $s_j \in S_{i_j}$. Sia S_m l'elemento di $\{S_{i_1}, ..., S_{i_n}\}$ tale che $S_{i_j} \subseteq S_m$ per ogni $j = 1, ..., n$, allora $\{s_1, ..., s_n\} \subseteq S_m$ che è algebricamente indipendente su K, perciò si ha $f = 0$. Per il secondo punto basta considerare la famiglia di tutti i sottoinsiemi di F contenenti il sottoinsieme di partenza e procedere come sopra. □

Esempio 2.1.9. Sia K un campo e $F = K(x)$, allora $\{x\}$ è una base di trascendenza di F su K. Per definizione, $\{x\}$ è algebricamente indipendente su K; se aggiungiamo un qualsiasi elemento di $K(x)$, ad esempio $f(x)(g(x))^{-1}$, con $g \neq 0$, abbiamo che il polinomio $g(y_1)y_2 - f(y_1) \in K[y_1, y_2]$ è non nullo e ha $\left(x, f(x)(g(x))^{-1}\right)$ come radice.

2.2 Un'utile caratterizzazione

Teorema 2.2.1. *Sia F un'estensione di K, sia S un sottoinsieme di F algebricamente indipendente su K e sia $u \in F \setminus K(S)$, allora $S \cup \{u\}$ è algebricamente indipendente su K se e solo se u è trascendente su $K(S)$.*

Dimostrazione. Supponiamo dapprima che u sia trascendente su $K(S)$. Siano $s_1, ..., s_{n-1} \in S$ e $f \in K[x_1, ..., x_n]$ tali che $f(s_1, ..., s_{n-1}, u) = 0$, allora u è radice di $f(s_1, ..., s_{n-1}, x_n) \in K(S)[x_n]$ che implica $f(s_1, ..., s_{n-1}, x_n) = 0$. Possiamo pensare $f = h_r x_n^r + ... + h_1 x_n + h_0$ con $h_i \in K[x_1, ..., x_{n-1}]$, perciò abbiamo che $h_i(s_1, ..., s_{n-1}) = 0$ per ogni $i = 0, ..., r$. Poiché S è algebricamente indipendente su K, $h_i = 0$ per ogni $i = 0, ..., r$, ossia $f = 0$ e $S \cup \{u\}$ è algebricamente indipendente su K.

Supponiamo ora che $S \cup \{u\}$ sia algebricamente indipendente su K.
Sia $f \in K(S)[x]$ tale che $f(u) = 0$, $f = \sum_{i=0}^{r} a_i x^i$ con $a_i \in K(S)$. Poiché gli a_i sono in numero finito, esiste $\{s_1, ..., s_{n-1}\} \subseteq S$ tale che $a_i \in K(s_1, ..., s_{n-1})$ per ogni $i = 0, ..., r$, ossia $a_i = f_i(s_1, ..., s_{n-1})(g_i(s_1, ..., s_{n-1}))^{-1}$ con $g_i \neq 0$. Poniamo $g = g_0 g_1 \cdots g_r$ e $\overline{f_i} = f_i \prod_{j \neq i} g_j$, allora

$$f(x) = (g(s_1, ..., s_{n-1}))^{-1} \left(\sum_{i=0}^{r} \overline{f_i}(s_1, ..., s_{n-1}) x^i \right)$$

perciò il polinomio $h = \sum_{i=0}^{r} \overline{f_i}(y_1, ..., y_{n-1}) y_n^i$ si annulla in $(s_1, ..., s_{n-1}, u)$. Per l'indipendenza algebrica si ha $h = 0$, ossia $\overline{f_i}(s_1, ..., s_{n-1}) = 0$ per ogni i e quindi $a_i = \overline{f_i}(s_1, ..., s_{n-1})(g(s_1, ..., s_{n-1}))^{-1} = 0$ per ogni $i = 0, ..., r$. Perciò u è trascendente su $K(S)$. □

Corollario 2.2.2. *Sia F un'estensione di K e sia S un sottoinsieme di F algebricamente indipendente su K, S è una base di trascendenza se e solo se F è algebrico su $K(S)$.*

Dimostrazione. Sia $u \in F \setminus K(S)$, se S è una base di trascendenza allora $S \cup \{u\}$ è algebricamente dipendente su K e per il Teorema 2.2.1 u è algebrico su $K(S)$.
Viceversa se per ogni $u \in F \setminus K(S)$ si ha che u è algebrico su $K(S)$ allora per il Teorema 2.2.1 S è massimale tra i sottoinsiemi di F algebricamente indipendenti su K con la relazione di inclusione, ossia S è una base di trascendenza su K. □

Definizione 2.2.3. Un'estensione di campi $K \subseteq F$ si dice **puramente trascendente** se $F = K(S)$, con S un sottoinsieme di F algebricamente indipendente su K.

Osservazione 2.2.4. In questo caso S è banalmente una base di trascendenza di F su K. Più in generale se F è un'estensione qualsiasi di K e S è una sua base di trascendenza, se $E = K(S)$ per il Corollario 2.2.2 si ha che F è un'estensione algebrica di E e E è puramente trascendente su K.

Esempio 2.2.5. Sia K un campo e sia $F = K(x_1, ..., x_n)$, allora $\{x_1, ..., x_n\}$ è una base di trascendenza di F su K, infatti è per definizione un insieme algebricamente indipendente su K.

Corollario 2.2.6. *Sia F un'estensione di K, sia $X \subseteq F$ tale che F è algebrico su $K(X)$ allora esiste una base di trascendenza di F su K contenuta in X.*

Dimostrazione. La famiglia di tutti i sottoinsiemi di X algebricamente indipendenti su K è un insieme non vuoto parzialmente ordinato con la relazione d'ordine data dall'inclusione. Consideriamo ora una catena di sottoinsiemi e l'unione S di tutti gli elementi della catena. Come abbiamo visto nella dimostrazione del Teorema 2.1.8, S è ancora un sottoinsieme di X algebricamente indipendente su K, ed è un maggiorante della catena. Perciò per il Lemma di Zorn esiste un sottoinsieme T di X massimale tra i sottoinsiemi di X algebricamente indipendenti su K. Per il Teorema 2.2.1, per ogni $u \in X \setminus T$ abbiamo che u è algebrico su $K(T)$, quindi $K(X)$ è algebrico su $K(T)$. Poiché per ipotesi F è algebrico su $K(X)$, F è algebrico su $K(T)$ e, per il Corollario 2.2.2, T è una base di trascendenza di F su K. □

2.3 Il teorema di scambio

Teorema 2.3.1. *Sia F un'estensione di K con base di trascendenza S, se S ha cardinalità finita allora ogni base di trascendenza di F su K ha la stessa cardinalità di S.*

Dimostrazione. Sia $S = \{s_1, ..., s_n\}$ e sia T un'altra base di trascendenza di F su K. Vogliamo mostrare che esiste $t_1 \in T$ trascendente su $K(s_2, ..., s_n)$. Se così non fosse avremmo che $K(s_2, ..., s_n)(T)$ è un'estensione algebrica di $K(s_2, ..., s_n)$. Poiché F è un'estensione algebrica di $K(T)$, è anche un'estensione algebrica di $K(T)(s_2, ..., s_n) = K(s_2, ..., s_n)(T)$. Ciò implica che F è algebrico su $K(s_2, ..., s_n)$ contraddicendo l'ipotesi. Perciò esiste $t_1 \in T$ trascendente su $K(s_2, ..., s_n)$ e $\{t_1, s_2, ..., s_n\}$ è algebricamente indipendente su K per il Teorema 2.2.1. Poiché S è una base di trascendenza, s_1 è algebrico su $K(t_1, s_2, ..., s_n)$ e quindi $K(S)(t_1) = K(t_1, s_2, ..., s_n)(s_1)$ è algebrico su $K(t_1, s_2, ..., s_n)$, da cui F è algebrico su $K(t_1, s_2, ..., s_n)$. Per il Corollario 2.2.2, $\{t_1, s_2, ..., s_n\}$ è una base di trascendenza di F su K. Continuando a scambiare s_i con $t_i \in T$ otteniamo che $\{t_1, ..., t_n\}$ è una base di trascendenza di F su K, da cui $T = \{t_1, ..., t_n\}$ e $|S| = |T|$. □

Teorema 2.3.2. *Sia F un'estensione di K con base di trascendenza S, se S ha cardinalità infinita allora ogni base di trascendenza di F su K ha la stessa cardinalità di S.*

Dimostrazione. Sia T un'altra base di trascendenza, allora per il Teorema 2.3.1 T ha cardinalità infinita. Per ogni $s \in S$, s è algebrico su $K(T)$ quindi esiste il polinomio minimo f di s in $K(T)$. Poiché l'i-esimo coefficiente di f è del tipo $h_i\left(t_{i_1}, ..., t_{i_{n_i}}\right)$ e sono in numero finito, $f \in K(T_s)[x]$ con T_s un sottoinsieme finito di T. Perciò per ogni $s \in S$, s è algebrico su $K(T_s)$. L'insieme $\bigcup_{s\in S} T_s$ è algebricamente indipendente su K poiché è un sottoinsieme di T, inoltre F è algebrico su $K(S)$ e per costruzione $K\left(\bigcup_{s\in S} T_s\right)(S)$ è algebrico su $K\left(\bigcup_{s\in S} T_s\right)$. Ne segue che F è algebrico su $K\left(\bigcup_{s\in S} T_s\right)$, ossia $\bigcup_{s\in S} T_s$ è una base di trascendenza di F su K, quindi $\bigcup_{s\in S} T_s = T$.
Poiché S è un insieme non vuoto, esiste un buon ordinamento $(S, <)$, indichiamo con 1 il primo elemento. Sia $T_1' = T_1$ e per ogni $1 < s \in S$ sia

$T'_s = T_s \setminus \left(\bigcup_{r<s} T_r\right)$, allora gli insiemi T'_i sono di cardinalità finita e a due a due disgiunti. Inoltre vale che $\bigcup_{s\in S} T'_s = \bigcup_{s\in S} T_s$. Per ogni $s \in S$ scegliamo di elencare gli elementi di T'_s come $t_1, ..., t_{n_s}$, perciò la mappa da $\bigcup_{s\in S} T'_s$ in $S \times \mathbb{N}$ definita da $t_i \longmapsto (s, i)$ è iniettiva. Quindi

$$|T| = |\bigcup_{s\in S} T_s| = |\bigcup_{s\in S} T'_s| \leq |S \times \mathbb{N}| = |S|\aleph_0 = |S|.$$

Invertendo S con T abbiamo $|S| \leq |T|$, che implica $|T| = |S|$. □

Definizione 2.3.3. Sia F un'estensione di K, si dice **grado di trascendenza** di F su K (denotato con $[F : K]_t$) la cardinalità di una qualunque base di trascendenza di F su K.

Osservazione 2.3.4. Se consideriamo F come spazio vettoriale su K, la sua dimensione è $[F : K]$. Poiché ogni insieme di elementi algebricamente indipendenti su K è anche un insieme di elementi linearmente indipendenti su K, si ha che $[F : K]_t \leq [F : K]$.
Inoltre $[F : K]_t = 0$ se e solo se F è un'estensione algebrica di K.

Osservazione 2.3.5. Se F ha grado di trascendenza finito su K, allora questo rappresenta il numero massimo di elementi di F algebricamente indipendenti su K.

Teorema 2.3.6. *Se F è un'estensione di E e E è un'estensione di K, allora*

$$[F : K]_t = [F : E]_t + [E : K]_t .$$

Dimostrazione. Sia S una base di trascendenza di E su K e sia T una base di trascendenza di F su E. Poiché $S \subseteq E$, ogni elemento di S è algebrico su E, quindi $S \cap T = \emptyset$. Vogliamo mostrare che $S \cup T$ è una base di trascendenza

di F su K. Poiché ogni elemento di E è algebrico su $K(S)$ lo è anche su $K(S \cup T)$, e quindi $K(S \cup T)(E)$ è algebrico su $K(S \cup T)$. Essendo

$$K(S \cup T) = K(S)(T) \subseteq E(T) \subseteq K(S \cup T)(E),$$

si ha che $E(T)$ è algebrico su $K(S \cup T)$. Inoltre poiché F è algebrico su $E(T)$, abbiamo che F è algebrico su $K(S \cup T)$.
Rimane da mostrare che $S \cup T$ è algebricamente indipendente su K. Siano $s_1, ..., s_n \in S$, $t_1, ..., t_m \in T$ distinti tra loro e sia f un polinomio in $K[x_1, ..., x_n, y_1, ..., y_m]$ tale che $f(s_1, ..., s_n, t_1, ..., t_m) = 0$. Consideriamo $g = f(s_1, ..., s_n, y_1, ..., y_m)$, $g \in K(S)[y_1, ..., y_m] \subseteq E[y_1, ..., y_m]$. Per costruzione $g(t_1, ..., t_m) = 0$ e per l'indipendenza algebrica di T su E abbiamo che $0 = g = f(s_1, ..., s_n, y_1, ..., y_m)$. Possiamo scrivere

$$f = f(x_1, ..., x_n, y_1, ..., y_m) = \sum_{i=1}^{r} h_i(x_1, ..., x_n) k_i(y_1, ..., y_m)$$

con $h_i \in K[x_1, ..., x_n]$ e $k_i \in K[y_1, ..., y_m]$, k_i monomi distinti tra loro, da cui $h_i(s_1, ..., s_n) = 0$ per ogni i. Per l'indipendenza algebrica di S su K abbiamo che $h_i = 0$ per ogni i, che implica $f = 0$. Ora che $S \cup T$ è una base di trascendenza di F su K, abbiamo

$$[F : K]_t = |S \cup T| = |T| + |S| = [F : E]_t + [E : K]_t.$$

□

Proposizione 2.3.7. *Sia F un'estensione di K e siano E_1, E_2 campi intermedi, allora*

$$[E_i : K]_t \leq [E_1 E_2 : K]_t \leq [E_1 : K]_t + [E_2 : K]_t \qquad \text{per } i = 1, 2.$$

Dimostrazione. Poiché $E_1E_2 = E_1(E_2) = E_2(E_1)$, per il Teorema 2.3.6

$$[E_1E_2 : K]_t = [E_1E_2 : E_1]_t + [E_1 : K]_t = [E_1E_2 : E_2]_t + [E_2 : K]_t .$$

Essendo $[E_1E_2 : E_i]_t \geq 0$ per $i = 1, 2$, abbiamo la prima disuguaglianza.
Per il Corollario 2.2.6 esiste una base di trascendenza di $E_1(E_2)$ su E_1 contenuta in E_2. Questa è un sottoinsieme di E_2 di elementi algebricamente indipendenti su E_1 e quindi su K, perciò è contenuta in una base di trascendenza di E_2 su K per il secondo punto della Proposizione 2.1.8. Per questo si ha $[E_1E_2 : E_1]_t \leq [E_2 : K]_t$, da cui

$$[E_1E_2 : K]_t = [E_1E_2 : E_1]_t + [E_1 : K]_t \leq [E_2 : K]_t + [E_1 : K]_t ,$$

ossia la seconda disuguaglianza. □

Teorema 2.3.8. *Sia C_i un campo algebricamente chiuso estensione di K_i, per $i = 1, 2$. Se $[C_1 : K_1]_t = [C_2 : K_2]_t$, allora ogni isomorfismo $K_1 \cong K_2$ si estende a $C_1 \cong C_2$.*

Dimostrazione. Sia S_i una base di trascendenza di C_i su K_i per $i = 1, 2$, allora $|S_1| = |S_2|$. Per il Corollario 2.1.5 un isomorfismo $\sigma : K_1 \longrightarrow K_2$ si estende ad un isomorfismo $\overline{\sigma} : K_1(S_1) \longrightarrow K_2(S_2)$. C_i è algebrico su $K_i(S_i)$ quindi è una sua chiusura algebrica. Per il Lemma di Estensione (Corollario 1.2.5) $\overline{\sigma}$ si estende ad un isomorfismo tra C_1 e C_2. □

2.4 Applicazione al campo complesso

Lemma 2.4.1. *Sia F un'estensione algebrica di K, allora $|F| \leq \aleph_0|K|$.*

Dimostrazione. Si veda il Lemma 3.5 del Capitolo V di [2]. □

Proposizione 2.4.2. *Sia S una base di trascendenza del campo complesso $\mathbb{C}$ sul campo $\mathbb{Q}$ dei razionali, allora S è infinito.*

Dimostrazione. Supponiamo per assurdo che S sia finito, $S = \{s_1, ..., s_n\}$. Per il Teorema 2.1.4, $|\mathbb{Q}(S)| = |\mathbb{Q}(x_1, ..., x_n)|$. Mostriamo per induzione che $|\mathbb{Q}[x_1, ..., x_n]| = \aleph_0$. Osserviamo innanzitutto che $|\mathbb{Q}[x]| = |\mathbb{Q}|$, infatti $\mathbb{Q}[x] = \bigcup_{r\geq 0} \{ f \in \mathbb{Q}[x] \mid \deg_f \leq r \}$ che è unione numerabile di insiemi di cardinalità $(\aleph_0)^{r+1} = \aleph_0$ e quindi ha cardinalità $\aleph_0 = |\mathbb{Q}|$. Essendo $\mathbb{Q}[x_1, ..., x_n] = \mathbb{Q}[x_1, ..., x_{n-1}][x_n]$, per quanto appena detto e per l'ipotesi induttiva otteniamo che $|\mathbb{Q}[x_1, ..., x_n]| = |\mathbb{Q}[x_1, ..., x_{n-1}]| = \aleph_0$.
Infine, usando l'Assioma della scelta, consideriamo la funzione che per ogni classe $[fg^{-1}] \in \mathbb{Q}(x_1, ..., x_n)$ sceglie un rappresentante fg^{-1} e gli associa la coppia $(f, g) \in \mathbb{Q}[x_1, ..., x_n] \times \mathbb{Q}[x_1, ..., x_n]$. Questa mappa è iniettiva, perciò

$$|\mathbb{Q}(x_1, ..., x_n)| \leq |\mathbb{Q}[x_1, ..., x_n] \times \mathbb{Q}[x_1, ..., x_n]| = |\mathbb{Q}[x_1, ..., x_n]| = \aleph_0.$$

Viceversa, la mappa iniettiva che associa a $f \in \mathbb{Q}[x_1, ..., x_n]$ l'elemento $f \in \mathbb{Q}(x_1, ..., x_n)$ dimostra che $|\mathbb{Q}[x_1, ..., x_n]| \leq |\mathbb{Q}(x_1, ..., x_n)|$. Abbiamo quindi provato che $|\mathbb{Q}(S)| = \aleph_0 < |\mathbb{C}|$. Poiché $\mathbb{C}$ è un'estensione algebrica di $\mathbb{Q}(S)$, per il Lemma 2.4.1, si ha $|\mathbb{C}| \leq \aleph_0 |\mathbb{Q}(S)| = \aleph_0$, che è un assurdo. Perciò necessariamente S deve essere infinito. □

Proposizione 2.4.3. *Esistono infiniti automorfismi del campo complesso.*

Dimostrazione. Per il Corollario 2.1.5 con $K_1 = K_2 = \mathbb{Q}$, $F_1 = F_2 = \mathbb{C}$ e $\sigma = \mathrm{id}_{\mathbb{Q}}$, se come η consideriamo una qualsiasi permutazione di una base di trascendenza S di $\mathbb{C}$ su $\mathbb{Q}$, abbiamo un automorfismo di $\mathbb{Q}(S)$. Per il Teorema 2.3.8 questo automorfismo di estende ad un automorfismo di $\mathbb{C}$. Per la Proposizione 2.4.2 abbiamo infinite permutazioni di S, e ognuna dà luogo ad un automorfismo distinto. □

Osservazione 2.4.4. La dimostrazione della Proposizione 2.4.3 prova che esistono infiniti automorfismi che fissano $\mathbb{Q}$. Inoltre notiamo che ogni isomorfismo di sottocampi di $\mathbb{C}$ estende $\mathrm{id}_{\mathbb{Q}}$, poiché ogni sottocampo di $\mathbb{C}$ contiene $\mathbb{Q}$ e per definizione fissa l'unità, quindi ogni intero e ogni suo inverso. Conseguenza di questo fatto è che il gruppo di Galois di $\mathbb{C}$ su $\mathbb{Q}$ è infinito.

Capitolo 3

Disgiunzione lineare

3.1 Definizioni e primi risultati

Per l'intera sezione assumiamo l'ipotesi che tutti i campi considerati siano contenuti in un campo algebricamente chiuso C.

Definizione 3.1.1. Siano K, E, F campi tali che $K \subseteq E, F$. Diciamo che E è **linearmente disgiunto** da F su K se ogni sottoinsieme di E linearmente indipendente su K è linearmente indipendente su F.

Osservazione 3.1.2. Per definizione di lineare indipendenza, un sottoinsieme X di E è linearmente indipendente su K se e solo se ogni suo sottoinsieme finito lo è.

Teorema 3.1.3. *Siano K, E, F campi tali che $K \subseteq E, F$. Allora E è linearmente disgiunto da F su K se e solo se F è linearmente disgiunto da E su K, ossia la definizione è simmetrica e possiamo quindi dire "E e F sono linearmente disgiunti su K".*

Dimostrazione. Chiaramente basta dimostrare una sola delle due implicazioni, supponiamo allora che E sia linearmente disgiunto da F su K. Sia $X \subseteq F$

linearmente indipendente su K ma non su E. Perciò esistono alcuni $u_i \in X$, $e_i \in E$ non tutti nulli tali che $u_1e_1 + ... + u_ne_n = 0$. Consideriamo un sottoinsieme di $\{e_1, ..., e_n\}$ linearmente indipendente su K massimale (rispetto all'inclusione tra i sottoinsiemi di $\{e_1, ..., e_n\}$ linearmente indipendenti su K) e lo reindicizziamo come $\{e_1, ..., e_t\}$ con $1 \leq t \leq n$. Se $t = n$ allora $e_1, ..., e_n$ sono linearmente indipendenti su K e quindi su F, ossia $u_i = 0$ per ogni $i = 1, ..., n$. Questo è assurdo per la lineare indipendenza su K; supponiamo allora $t < n$. Gli elementi omessi sono quindi combinazione K-lineare di $e_1, ..., e_t$, ossia $e_j = \sum_{i=1}^{t} a_{ij}e_i$ per $t < j \leq n$. Si ha che

$$0 = \sum_{j=1}^{n} e_j u_j = \sum_{j=1}^{t} e_j u_j + \sum_{j=t+1}^{n} \left(\sum_{i=1}^{t} a_{ij} e_i \right) u_j = \sum_{k=1}^{t} \left(u_k + \sum_{j=t+1}^{n} a_{kj} u_j \right) e_k.$$

Poiché E è linearmente disgiunto da F su K, $\{e_1, ..., e_t\}$ è linearmente indipendente su F, da cui $u_k + \sum_{j=t+1}^{n} a_{kj}u_j = 0$ per ogni $k = 1, ..., t$. Dato che $t \geq 1$ abbiamo trovato un sottoinsieme di X linearmente dipendente su K, che è assurdo. Perciò X deve essere linearmente indipendente su E. □

Proposizione 3.1.4. *Siano K, E, F campi tali che $K \subseteq E, F$. Sia R un sottoanello di E contenente K tale che $K(R) = E$. Le seguenti affermazioni sono equivalenti:*

i) E e F sono linearmente disgiunti su K;

ii) ogni sottoinsieme di R linearmente indipendente su K lo è anche su F;

iii) esiste una base di R su K (come spazio vettoriale) composta da elementi linearmente indipendenti su F.

Dimostrazione. Osserviamo che $(i) \Rightarrow (ii)$ e $(i) \Rightarrow (iii)$ sono vere per definizione di disgiunzione lineare.

$(ii) \Rightarrow (i)$ Sia $X = \{u_1, ..., u_n\}$ un sottoinsieme di E linearmente indipendente su K. Poiché $u_i \in E = K(R)$, $u_i = c_i d_i^{-1}$ dove $c_i = f_i(r_1, ..., r_{t_i})$ e $0 \neq d_i = g_i(r_1, ..., r_{t_i})$, con $f_i,\ g_i \in K[x_1, ..., x_{t_i}]$ e $r_j \in R$. Definiamo $d = d_1 \cdots d_n \neq 0$ e $v_i = d_1 \cdots d_{i-1} c_i d_{i+1} \cdots d_n \in R$ per ogni $i = 1, ..., n$. Allora $u_i = v_i d^{-1}$ e il sottoinsieme $X' = \{v_1, ..., v_n\}$ di R è linearmente indipendente su un sottocampo di C se e solo se X lo è. Per costruzione X è linearmente indipendente su K, quindi X' lo è. Per ipotesi abbiamo che X' è linearmente indipendente su F e quindi X è linearmente indipendente su F.
$(iii) \Rightarrow (ii)$ Sia U una base di R su K composta da elementi linearmente indipendenti su F e sia X un sottoinsieme finito di R linearmente indipendente su K. Notiamo che X è contenuto in $V = \mathrm{Span}_K(U_1)$ con $U_1 \subseteq U$ finito. Definiamo $V_1 = \mathrm{Span}_F(U_1)$. Poiché per ipotesi U_1 è linearmente indipendente su F abbiamo che U_1 è una base di V_1 e quindi $\dim_K V = \dim_F V_1 = |U_1|$. Dato che X è un sottoinsieme di V di vettori linearmente indipendenti su K, possiamo completarlo ad una base W di V su K. Poiché $V = \mathrm{Span}_K(W) = \mathrm{Span}_K(U_1)$, abbiamo che $V_1 = \mathrm{Span}_F(U_1) = \mathrm{Span}_F(W)$. Quindi W contiene una base W_1 di V_1 su F e perciò

$$|W_1| \leq |W| = \dim_K V = \dim_F V_1 = |W_1|,$$

ossia $W = W_1$. Poiché $X \subseteq W$ abbiamo che X è linearmente indipendente su F. □

Teorema 3.1.5. *Siano K, E, L, F campi tali che $K \subseteq E$ e $K \subseteq L \subseteq F$. E e F sono linearmente disgiunti su K se e solo se valgono le seguenti condizioni:*

(a) E e L sono linearmente disgiunti su K;

(b) EL e F sono linearmente disgiunti su L.

Dimostrazione. ($\Leftarrow$) Sia X un sottoinsieme di E linearmente indipendente su K, allora per (a) è linearmente indipendente su L. Poiché $X \subseteq E \subseteq EL$, (b) implica che X è linearmente indipendente su F.
($\Rightarrow$) Poiché $L \subseteq F$, se ogni sottoinsieme di E linearmente indipendente su K è linearmente indipendente su F, lo è anche su L. Sia $R = L[E]$ il sottoanello di C generato da E e L, abbiamo che $K(R) = EL$. Sia U una base di E su K, allora $R = \mathrm{Span}_L(U)$, ma U è linearmente indipendente su L per (a), quindi U è una base di R su L. Per ipotesi E e F sono linearmente disgiunti su K, perciò U è linearmente indipendente su F. Per la Proposizione 3.1.4 EL e F sono linearmente disgiunti su L. □

Definizione 3.1.6. Sia K un campo di caratteristica $p \neq 0$; per ogni intero $n \geq 0$ definiamo

$$K^{\frac{1}{p^n}} = \{\, u \in C \mid u^{p^n} \in K \,\}.$$
$$K^{\frac{1}{p^\infty}} = \bigcup_{n \geq 0} K^{\frac{1}{p^n}} = \{\, u \in C \mid u^{p^n} \in K \text{ per qualche } n \geq 0 \,\}.$$

Osservazione 3.1.7. Poiché in un campo di caratteristica $p \neq 0$ per ogni intero $n \geq 0$ vale che $(u - v)^{p^n} = u^{p^n} - v^{p^n}$, $K^{\frac{1}{p^n}}$ è un sottocampo di C per ogni $n \geq 0$. Inoltre, se $n \leq m$, si ha

$$K = K^{\frac{1}{p^0}} \subseteq K^{\frac{1}{p^n}} \subseteq K^{\frac{1}{p^m}} \subseteq K^{\frac{1}{p^\infty}}$$

da cui otteniamo che $K^{\frac{1}{p^\infty}}$ è anch'esso un campo.

Proposizione 3.1.8. *Per ogni $n \geq 0$, $K^{\frac{1}{p^n}}$ è il campo di spezzamento su K di $\{\, x^{p^n} - k \mid k \in K \,\}$.*

Dimostrazione. Per ogni $k \in K$ sia $u \in C$ tale che $u^{p^n} = k$ (esiste poiché C è algebricamente chiuso), allora $u \in K^{\frac{1}{p^n}}$ per definizione. Perciò $K^{\frac{1}{p^n}}$ contiene

K e tutte le radici dei polinomi in $\{ x^{p^n} - k \mid k \in K \}$. Viceversa ogni elemento di $K^{\frac{1}{p^n}}$ è per costruzione una radice di un polinomio in $\{ x^{p^n} - k \mid k \in K \}$, da cui la tesi. □

Proposizione 3.1.9. *Sia K un campo di caratteristica $p \neq 0$, allora per ogni $n \geq 0$ un sottoinsieme X di C è linearmente indipendente su $K^{\frac{1}{p^n}}$ se e solo se $X^{p^n} = \{ u^{p^n} \mid u \in X \}$ è linearmente indipendente su K.*
Inoltre X è linearmente indipendente su $K^{\frac{1}{p^\infty}}$ se e solo se X è linearmente indipendente su $K^{\frac{1}{p^n}}$ per ogni $n \geq 0$.

Dimostrazione. Come abbiamo notato nella dimostrazione della Proposizione 3.1.8, ogni elemento $a \in K$ è della forma v^{p^n} con $v \in K^{\frac{1}{p^n}}$. Fissiamo $X \subseteq C$ e consideriamo una combinazione K-lineare di $\left\{ u_1^{p^n}, ..., u_r^{p^n} \right\} \subseteq X^{p^n}$, allora

$$0 = \sum_{i=1}^{r} a_i u_i^{p^n} = \sum_{i=1}^{r} v_i^{p^n} u_i^{p^n} = \left(\sum_{i=1}^{r} v_i u_i \right)^{p^n} \iff \sum_{i=1}^{r} v_i u_i = 0.$$

Per la seconda affermazione basta notare che per ogni combinazione lineare di elementi di $K^{\frac{1}{p^\infty}}$ esiste $n \geq 0$ tale che $K^{\frac{1}{p^n}}$ contenga tutti gli elementi della combinazione. □

Teorema 3.1.10. *Sia K un campo di caratteristica $p \neq 0$, se F è un'estensione puramente trascendente di K allora F e $K^{\frac{1}{p^n}}$ sono linearmente disgiunti su K per ogni $0 \leq n \leq \infty$.*

Dimostrazione. Sia S una base di trascendenza di F su K, allora $F = K(S)$. Il risultato è vero per definizione se $S = \emptyset$, ossia se $F = K$. Consideriamo allora S non vuoto, sia M l'insieme dei prodotti finiti di elementi di S. Poiché S è algebricamente indipendente su K abbiamo che M è linearmente indipendente su K. Inoltre $\mathrm{Span}_K(M) = K[S]$, ossia M è una base di $K[S]$ su K. Sempre per l'indipendenza algebrica di S su K otteniamo che

$M^{p^n} = \{ m^{p^n} \mid m \in M \}$ è linearmente indipendente su K per ogni $n \geq 0$, quindi per la Proposizione 3.1.9 abbiamo che M è linearmente indipendente su $K^{\frac{1}{p^n}}$ e su $K^{\frac{1}{p^\infty}}$. Per la Proposizione 3.1.4 (con $K[S]$, F, $K^{\frac{1}{p^n}}$ al posto di R, E, F rispettivamente), F e $K^{\frac{1}{p^n}}$ sono linearmente disgiunti su K per ogni $0 \leq n \leq \infty$. □

3.2 Legame con la separabilità

Definizione 3.2.1. Sia F un'estensione di K e sia u un elemento di F algebrico su K. Diciamo che u è **puramente inseparabile** su K se il suo K-polinomio minimo si fattorizza in $F[x]$ come $(x-u)^m$.
Diciamo che F è un'**estensione puramente inseparabile** di K se ogni suo elemento è puramente inseparabile su K.

Osservazione 3.2.2. Un elemento $u \in F$ è sia separabile che puramente inseparabile su K se e solo se $u \in K$.

Osservazione 3.2.3. Se K ha caratteristica 0 ogni elemento algebrico su K è separabile su K, perciò gli unici elementi puramente inseparabili di F sono gli elementi di K.

Lemma 3.2.4. *Sia K un campo di caratteristica $p \neq 0$ e sia F una sua estensione con $u \in F$, allora esiste $n \geq 0$ tale che $u^{p^n} \in K$ se e solo se u è puramente inseparabile su K. In particolare se F è un'estensione algebrica allora questo accade per ogni $u \in F$ se e solo se F è puramente inseparabile su K.*

Dimostrazione. ($\Rightarrow$) Per ipotesi $x^{p^n} - u^{p^n} \in K[x]$ per un certo $n \geq 0$. Poiché $x^{p^n} - u^{p^n} = (x-u)^{p^n}$, il polinomio minimo di u su K è del tipo $(x-u)^m$, ossia u è puramente inseparabile su K.

($\Leftarrow$) Sia $(x-u)^m$ il polinomio minimo di $u \in F$ e sia $m = np^r$ con p che non divide n. Allora $(x-u)^m = \left(x^{p^r} - u^{p^r}\right)^n \in K[x]$ quindi il suo coefficiente di grado $p^r(n-1)$, $-nu^{p^r}$, deve appartenere a K. Poiché p non divide n, abbiamo che $u^{p^r} \in K$. □

Teorema 3.2.5. *Sia K un campo di caratteristica $p \neq 0$ e sia F una sua estensione algebrica, se F è separabile su K allora F e $K^{\frac{1}{p}}$ sono linearmente disgiunti su K.*

Dimostrazione. Sia $X = \{u_1, ..., u_n\}$ un sottoinsieme finito di F linearmente indipendente su K, consideriamo $E = K(u_1, ..., u_n)$, che ha dimensione finita su K. Possiamo completare X ad una base di E su K, ad esempio con $\{u_{n+1}, ..., u_r\}$. Siano $v \in E$ e $k \in \mathbb{N}$, $v^k = \sum_{i=1}^r a_i u_i$ con $a_i \in K$ e quindi $v^{kp} = \sum_{i=1}^r a_i^p u_i^p$. Poiché per ogni elemento $w \in K(v)$ si ha $w^p \in K(v^p)$, per il Lemma 3.2.4 $K(v)$ è puramente inseparabile su $K(v^p)$. Poiché v è separabile su K, lo è su $K(v^p)$ e quindi $K(v)$ è separabile su $K(v^p)$. Per l'Osservazione 3.2.2 abbiamo che $K(v) = K(v^p)$. Perciò v è combinazione K-lineare degli elementi del tipo v^{kp} e quindi degli u_i^p, da cui $E = \mathrm{Span}_K(u_1^p, ..., u_r^p)$. Essendo $[E : K] = r$, $\{u_1^p, ..., u_r^p\}$ è una base di E su K. Perciò X^p è linearmente indipendente su K e, per la Proposizione 3.1.9, X è linearmente indipendente su $K^{\frac{1}{p}}$. □

Definizione 3.2.6. Sia F un'estensione di K, una base di trascendenza S di F su K si dice **base di trascendenza separabile** se F è un'estensione algebrica e separabile di $K(S)$. Se una tale base di trascendenza esiste F si dice essere **generato in modo separabile** su K.

Osservazione 3.2.7. Se un'estensione di campi $K \subseteq F$ è puramente trascendente con $F = K(S)$ allora S è una base di trascendenza separabile di F su K, quindi F è generato in modo separabile su K.

Osservazione 3.2.8. Se F è un'estensione di K finitamente generata, ossia $F = K(u_1, ..., u_n)$, allora esiste una base di trascendenza S di F su K contenuta in $\{u_1, ..., u_n\}$ per il Corollario 2.2.6. Perciò F è algebrico su $K(S)$. A meno di reindicizzare gli u_i, possiamo supporre $S = \{u_1, ..., u_r\}$. Abbiamo che $F = K(S)(u_{r+1}, ..., u_n)$, ossia è un'estensione finita di $K(S)$. Se aggiungiamo l'ipotesi che K sia di caratteristica 0, allora otteniamo che F è un'estensione separabile di $K(S)$ e quindi F è generato in modo separabile su K.

3.3 Nuova definizione di separabilità

Osservazione 3.3.1. Se K è un campo di caratteristica 0 definiamo

$$K^{\frac{1}{0}} = K^{\frac{1}{0^n}} = K^{\frac{1}{0^\infty}} = K.$$

Definizione 3.3.2. Un'estensione F di K con K di caratteristica $p \geq 0$ si dice **separabile** se F e $K^{\frac{1}{p}}$ sono linearmente disgiunti su K.

Teorema 3.3.3. *Sia F un'estensione di K di caratteristica $p \geq 0$, le seguenti affermazioni sono equivalenti:*

i) F e $K^{\frac{1}{p}}$ sono linearmente disgiunti su K;

ii) F e $K^{\frac{1}{p^n}}$ sono linearmente disgiunti su K per un qualche $n \geq 1$;

iii) F e $K^{\frac{1}{p^\infty}}$ sono linearmente disgiunti su K;

iv) ogni campo intermedio E finitamente generato è generato in modo separabile su K;

v) F e $C^{\mathrm{Aut}_K C}$ sono linearmente disgiunti su K.

Dimostrazione. $(iii) \iff (v)$ Denotiamo con $\widetilde{K}$ il campo fisso di $\mathrm{Aut}_K C$, ci basta provare che $\widetilde{K} = K^{\frac{1}{p^\infty}}$. Sia $u \in \widetilde{K}$, se u è trascendente su K allora anche $v = u^2$ lo è. Abbiamo $K(u) \cong K(x) \cong K(v)$, ossia esiste un isomorfismo σ che fissa K e manda u in v. Inoltre $1 = [K(x) : K]_t = [K(u) : K]_t = [K(v) : K]_t$, quindi per il Teorema 2.3.6 $[C : K(u)]_t = [C : K(v)]_t$. Per il Teorema 2.3.8, σ si estende ad un automorfismo di C, ma $\sigma(u) = v \neq u$, contraddicendo $u \in \widetilde{K}$. Perciò u deve essere algebrico su K, sia f il suo polinomio minimo. Se w è un'altra radice di f, per il Lemma di Estensione (Teorema 1.2.4) esiste un isomorfismo $\tau : K(u) \to K(w)$ che fissa K e manda u in w. Per il Teorema 2.3.8 possiamo estendere τ ad un isomorfismo di C, da cui $\tau(u) = u = w$, ossia f ha una sola radice e quindi u è puramente inseparabile su K. Se K ha caratteristica 0 allora f è separabile e quindi ha grado 1; perciò $u \in K = K^{\frac{1}{0^\infty}}$. Se K ha caratteristica $p \neq 0$ allora per il Lemma 3.2.4 esiste $n \geq 0$ tale che $u^{p^n} \in K$, da cui $u \in K^{\frac{1}{p^n}} \subseteq K^{\frac{1}{p^\infty}}$.
Il viceversa in caratteristica 0 è banale. Se K ha caratteristica $p \neq 0$, sia $u \in K^{\frac{1}{p^\infty}}$, allora esiste $n \geq 1$ tale che $u \in K^{\frac{1}{p^n}}$. Per ogni $\sigma \in \mathrm{Aut}_K C$ si ha $\sigma(u)^{p^n} = \sigma\left(u^{p^n}\right) = u^{p^n}$, da cui $(\sigma(u) - u)^{p^n} = \sigma(u)^{p^n} - u^{p^n} = 0$ e $\sigma(u) = u$.

Notiamo che le prime tre condizioni sono sempre vere nel caso di $p = 0$, e che la quarta lo è per l'Osservazione 3.2.8. Consideriamo d'ora in poi $p \neq 0$.

$(iii) \Rightarrow (ii) \Rightarrow (i)$ sono ovvie per l'Osservazione 3.1.7.

$(i) \Rightarrow (iv)$ Sia $E = K(s_1, ..., s_n)$ e sia $r = [E : K]_t$, allora $r \leq n$. A meno di reindicizzazione possiamo dire che $\{s_1, ..., s_r\}$ è una base di trascendenza di E su K per il Corollario 2.2.6. Se $r = n$ allora la tesi è ovvia. Se $r < n$, allora s_{r+1} è algebrico su $K(s_1, ..., s_r)$, sia f il suo polinomio minimo. Possiamo riscrivere f raccogliendo il denominatore comune:

$$f = \sum_{i=0}^{m} a_i x^i = d^{-1} \left(\sum_{i=0}^{m} h_i(s_1, ..., s_r) x^i \right)$$

con $0 \neq d \in K[s_1, ..., s_r]$, $h_i \in K[x_1, ..., x_r]$. Sia $f_1 = \sum_{i=0}^{m} h_i(x_1, ..., x_r) x_{r+1}^i$ allora $f_1 \in K[x_1, ..., x_{r+1}]$ e $f_1(s_1, ..., s_{r+1}) = 0$.

Consideriamo un polinomio $g \in K[x_1, ..., x_{r+1}]$ che abbia grado minimo tra i polinomi che si annullano in $(s_1, ..., s_{r+1})$. Se g fosse riducibile allora tra i suoi fattori ci sarebbe un polinomio di grado strettamente minore che si annulla in $(s_1, ..., s_{r+1})$, e ciò è assurdo per la scelta di g. Dimostriamo ora che qualche x_i compare in g con un esponente non divisibile per p. Se così non fosse, $g = c_0 + c_1 m_1(x_1, ..., x_{r+1})^p + ... + c_k m_k(x_1, ..., x_{r+1})^p$, con $c_j \in K$ e dove $m_j(x_1, ..., x_{r+1})$ è un monomio in $x_1, ..., x_{r+1}$. Se definiamo $m_0 = 1$ e per ogni $j = 0, ..., k$ scegliamo $d_j \in K^{\frac{1}{p}}$ tale che $d_j^p = c_j$, allora

$$0 = g(s_1, ..., s_{r+1}) = \left(\sum_{j=0}^{k} d_j m_j(s_1, ..., s_{r+1}) \right)^p$$

ossia $\sum_{j=0}^{k} d_j m_j(s_1, ..., s_{r+1}) = 0$ e quindi $\{ m_j(s_1, ..., s_{r+1}) \mid j = 0, ..., k \}$ è un sottoinsieme di F è linearmente dipendente su $K^{\frac{1}{p}}$. Osserviamo che $\{ m_j(s_1, ..., s_{r+1}) \mid j = 0, ..., k \}$ è linearmente indipendente su K poiché una qualsiasi combinazione lineare non banale che si annulla negli $m_j(s_1, ..., s_{r+1})$ rappresenterebbe un polinomio in $K[x_1, ..., x_{r+1}]$ di grado strettamente minore del grado di g con $(s_1, ..., s_{r+1})$ come radice. Ciò porta ad una contraddizione con l'ipotesi e quindi qualche x_i, ad esempio x_1, compare in g con esponente non divisibile per p.

Consideriamo il polinomio $g(x, s_2, ..., s_{r+1}) \in K(s_2, ..., s_{r+1})[x]$. Se fosse il polinomio nullo allora potremmo costruire un polinomio di grado strettamente minore di quello di g che si annulla in $(s_1, ..., s_{r+1})$. Poiché $g(x, s_2, ..., s_{r+1})$ è un polinomio non nullo che si annulla in s_1, s_1 è algebrico su $K(s_2, ..., s_{r+1})$. Perciò E è algebrico su $K(s_2, ..., s_{r+1})$ e, dato che $r = [E : K]_t$, per il Corollario 2.2.6 $\{s_2, ..., s_{r+1}\}$ è una base di trascendenza di E su K.

La prova del Teorema 2.1.4 mostra che la mappa che manda x_i in s_i si estende ad un K-isomorfismo $\phi : K[x_2, ..., x_{r+1}] \to K[s_2, ..., s_{r+1}]$ che possiamo estendere ad un isomorfismo tra $K[x_1, x_2, ..., x_{r+1}]$ e $K[s_2, ..., s_{r+1}][x]$ che manda x_1 in x e $g(x_1, ..., x_{r+1})$ in $g(x, s_2, ..., s_{r+1})$. Perciò abbiamo che $g(x, s_2, ..., s_{r+1})$ è irriducibile su $K[s_2, ..., s_{r+1}]$, quindi primitivo e, per il Lemma di Gauss (Teorema 1.1.7), irriducibile su $K(s_2, ..., s_{r+1})$. Inoltre x deve comparire in $g(x, s_2, ..., s_{r+1})$ con esponente non divisibile per p. Di conseguenza $g(x, s_2, ..., s_{r+1})$ ha tutte le radici distinte, ossia è separabile. Abbiamo allora che s_1 è separabile su $K(s_2, ..., s_{r+1})$ e quindi su $K(s_2, ..., s_n)$, ossia E è un'estensione algebrica e separabile di $K(s_2, ..., s_n)$.
Ora, se $\{s_2, ..., s_n\}$ è una base di trascendenza di E su K abbiamo finito. Altrimenti, per il Corollario 2.2.6, $\{s_2, ..., s_n\}$ contiene una base di trascendenza di E su K che, a meno di reindicizzazione, è $\{s_2, ..., s_{r+1}\}$. Possiamo ripetere quanto visto prima con questa nuova base, e ottenere che E è un'estensione algebrica e separabile di $K(s_3, ..., s_n)$. Perciò dopo un numero finito di passi troviamo $s_1, ..., s_{n-r}$ tali che $\{s_{n-r+1}, ..., s_n\}$ è una base di trascendenza separabile di E su K.

$(iv) \Rightarrow (iii)$ Sia W un sottoinsieme finito di F linearmente indipendente su K e sia $E = K(W)$. Se mostriamo che E e $K^{\frac{1}{p^\infty}}$ sono linearmente disgiunti su K allora abbiamo che W è linearmente indipendente su $K^{\frac{1}{p^\infty}}$. Per ipotesi E ha una base di trascendenza separabile su K, denotiamola con S. Per il Teorema 3.1.10, $K(S)$ e $K^{\frac{1}{p^\infty}}$ sono linearmente disgiunti su K.
Sia X un sottoinsieme di E linearmente indipendente su $K(S)$, poiché E è un'estensione algebrica e separabile di $K(S)$, il Teorema 3.2.5 implica che X è linearmente indipendente su $K(S)^{\frac{1}{p}}$. Per la Proposizione 3.1.9, X^p è linearmente indipendente su $K(S)$. Se supponiamo X^{p^r} linearmente indipendente su $K(S)$, per il Teorema 3.2.5 X^{p^r} è linearmente indipendente su

$K(S)^{\frac{1}{p}}$ e per la Proposizione 3.1.9 abbiamo che $\left(X^{p^r}\right)^p = X^{p^{r+1}}$ è linearmente indipendente su $K(S)$. Questo permette di dimostrare per induzione che X^{p^m} è linearmente indipendente su $K(S)$ per ogni $m \geq 0$. Per la Proposizione 3.1.9, X è linearmente indipendente su $K(S)^{\frac{1}{p^m}}$ per ogni $m \geq 0$, ossia è linearmente indipendente su $K(S)^{\frac{1}{p^\infty}}$. Notiamo che $K^{\frac{1}{p^\infty}}(S)$ è un sottocampo di $K(S)^{\frac{1}{p^\infty}}$, quindi X è linearmente indipendente su $K^{\frac{1}{p^\infty}}K(S)$. Abbiamo quindi dimostrato che E e $K^{\frac{1}{p^\infty}}K(S)$ sono linearmente disgiunti su $K(S)$. Per il Teorema 3.1.5 (con $K^{\frac{1}{p^\infty}}$, $K(S)$ e E al posto di E, L e F rispettivamente) $K^{\frac{1}{p^\infty}}$ e E sono linearmente disgiunti su K. □

Teorema 3.3.4. *Sia K un campo di caratteristica $p \neq 0$ e sia F una sua estensione algebrica, F e $K^{\frac{1}{p}}$ sono linearmente disgiunti su K se e solo se F è separabile su K.*

Dimostrazione. ($\Leftarrow$) Corrisponde al risultato del Teorema 3.2.5.
($\Rightarrow$) Per ogni $u \in F$, $K(u)$ è un campo intermedio finitamente generato su K, quindi per l'implicazione $(i) \Rightarrow (iv)$ del Teorema 3.3.3 $K(u)$ è generato in modo separabile su K. Poiché $K(u)$ è algebrico su K l'unica sua base di trascendenza è l'insieme vuoto e quindi $K(u)$ è separabile su $K(\emptyset) = K$, ossia u è separabile su K. □

Osservazione 3.3.5. Il teorema 3.3.4 mostra che in caratteristica $p \neq 0$ la nuova definizione di separabilità estende quella precedente.
In caratteristica 0 abbiamo notato che le condizioni del Teorema 3.3.3 sono sempre vere, quindi possiamo dire che ogni estensione di un campo di caratteristica 0 è separabile.

Corollario 3.3.6 (Criterio di Mac Lane)**.** *Se F è un'estensione di K generata in modo separabile allora F è separabile su K. Viceversa se F è separabile e finitamente generato su K, ad esempio $F = K(u_1, ..., u_n)$, allora esiste un sottoinsieme di $\{u_1, ..., u_n\}$ che è una base di trascendenza separabile di F su K, in particolare F è generato in modo separabile su K.*

Dimostrazione. Per ipotesi F ha una base di trascendenza separabile su K, denotiamola con S. Come nell'implicazione $(iv) \Rightarrow (iii)$ del Teorema 3.3.3, con F al posto di E, si dimostra che F e $K^{\frac{1}{p^\infty}}$ sono linearmente disgiunti su K. Quindi F è separabile su K.
Se F è separabile su K allora per il Teorema 3.3.3 ogni campo intermedio finitamente generato è generato in modo separabile su K. In particolare se F è finitamente generato su K, $F = K(u_1, ..., u_n)$, allora come nell'implicazione $(i) \Rightarrow (iv)$ possiamo estrarre un sottoinsieme di $\{u_1, ..., u_n\}$ che sia una base di trascendenza separabile di F su K. □

Esempio 3.3.7. Mostriamo un controesempio al Corollario 3.3.6 nel caso in cui non valga l'ipotesi che F sia finitamente generato su K.
Sia K un campo di caratteristica $p \neq 0$ e sia u trascendente su K. Sia $F = K(u, v_1, v_2, ...)$, dove v_i è una radice di $x^{p^i} - u \in K(u)[x]$ per ogni $i = 1, 2, ...$ Per prima cosa dimostriamo che F è separabile su K mediante la Proposizione 3.1.9. Siano $f_1, ..., f_n \in F$ linearmente indipendenti su K, vogliamo mostrare che $f_1^p, ..., f_n^p$ sono linearmente indipendenti su K. Per costruzione esiste un intero s tale che $f_i \in K(v_s)$ per ogni $i = 1, ..., n$. Inoltre, poiché in generale vale che $\frac{c_1}{d_1}, ..., \frac{c_n}{d_n}$ sono linearmente indipendenti su K se e solo se $c_1\frac{d}{d_1}, ..., c_n\frac{d}{d_n}$ (con $c_i, d_i \in K[v_s]$, $d = d_1...d_n$) lo sono, possiamo supporre che $f_i \in K_{\leq m}[v_s]$ per ogni $i = 1, ..., n$. Scriviamo $f_i = (a_{i,0}, a_{i,1}, ..., a_{i,m})$, identificando il vettore di K^{m+1} col polinomio $a_{i,0} + a_{i,1}x + ... + a_{i,m}x^m$ valutato in v_s. Per ipotesi la matrice

$$A = \begin{pmatrix} a_{1,0} & a_{1,1} & \cdots & a_{1,m} \\ a_{2,0} & a_{2,1} & \cdots & a_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,0} & a_{n,1} & \cdots & a_{n,m} \end{pmatrix}$$

ha rango n su K; consideriamo una sua sottomatrice quadrata A' di ordine n invertibile. Poiché $f_i^p = \left(a_{i,0}^p, a_{i,1}^p, ..., a_{i,m}^p\right)$, ci basta dimostrare che la matrice

$$B = \begin{pmatrix} a_{1,0}^p & a_{1,1}^p & \cdots & a_{1,m}^p \\ a_{2,0}^p & a_{2,1}^p & \cdots & a_{2,m}^p \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,0}^p & a_{n,1}^p & \cdots & a_{n,m}^p \end{pmatrix}$$

ha rango n su K. Sia B' la sua sottomatrice con la stessa indicizzazione di A'. Dato che il determinante di una matrice è un polinomio negli elementi della matrice, vale che $\det(B') = \det(A')^p \neq 0$. Perciò $f_1^p, ..., f_n^p$ sono linearmente indipendenti su K.

Mostriamo ora che F non è generato in modo separabile su K. Sia $w \in F$ un elemento trascendente su K, allora esiste un intero s tale che $w \in K(v_s)$. Per alleggerire la notazione poniamo $L = K(w)$, $E = K(u, w)$, $T = K(u)$ e $z = v_{s+1}$. Notiamo che F è un'estensione algebrica dei tre campi T, L, E.

Il polinomio minimo di z su T è $p_T = x^{p^{s+1}} - u$ che, visto in $F[x]$, può essere scritto come $(x - z)^{p^{s+1}}$. Il polinomio minimo di z su E deve dividere p_T e perciò è della forma $p_E = x^{p^r} - z^{p^r}$ con $z^{p^r} \in E$ (queste ultime affermazioni seguono dal Lemma 1.2.6). Allo stesso modo p_E divide il polinomio minimo di z su L. Se $r = 0$ allora $p_E = x - z$ e $z = v_{s+1} \in E \subseteq K(v_s)$, che è un assurdo. Se $r > 0$ allora p_L non è separabile, ossia $\{w\}$ non è una base di trascendenza separabile di F su K.

Corollario 3.3.8. *Sia F un'estensione di K con campo intermedio E, valgono le seguenti:*

i) Se F è separabile su K allora E è separabile su K;

ii) Se F è separabile su E e E è separabile su K allora F è separabile su K;

iii) Se F è separabile su K e E è algebrico su K allora F è separabile su E.

Dimostrazione. Possiamo supporre K di caratteristica $p \neq 0$, altrimenti la tesi è ovvia. (i) Se F e $K^{\frac{1}{p}}$ sono linearmente disgiunti su K allora anche E e $K^{\frac{1}{p}}$ sono linearmente disgiunti su K.
(ii) Per ipotesi F e $E^{\frac{1}{p}}$ sono linearmente disgiunti su E, E e $K^{\frac{1}{p}}$ sono linearmente disgiunti su K. Consideriamo ora il Teorema 3.1.5 con $K^{\frac{1}{p}}$ e E al posto di E e L rispettivamente. Per dimostrare che F e $K^{\frac{1}{p}}$ sono linearmente disgiunti su K ci basta verificare le due condizioni:

(a) $K^{\frac{1}{p}}$ e E sono linearmente disgiunti su K;

(b) $K^{\frac{1}{p}}E$ e F sono linearmente disgiunti su E.

La (a) vale per ipotesi. Notiamo che $K^{\frac{1}{p}}E$ è un sottocampo di $E^{\frac{1}{p}}$, che è linearmente disgiunto con F su E. Perciò $K^{\frac{1}{p}}E$ e F sono linearmente disgiunti su E.
(iii) Sia X un sottoinsieme di F linearmente indipendente su E, possiamo estenderlo ad una base U di F su E. Sia V una base di E su K, consideriamo $a_1u_1v_1 + ... + a_su_sv_s = 0$ con $a_i \in K$, $u_i \in U$ e $v_i \in V$. Per la lineare indipendenza di U su E si ha $a_iv_i = 0$ e per la lineare indipendenza di V su K si ha $a_i = 0$. Perciò $UV = \{\, uv \mid u \in U, v \in V \,\}$ è linearmente indipendente su K e quindi su $K^{\frac{1}{p}}$. Per la proposizione 3.1.9 abbiamo che $(UV)^p$ è linearmente indipendente su K. Per il punto (i), E è separabile su K, quindi V

è linearmente indipendente su $K^{\frac{1}{p}}$ e, sempre per la proposizione 3.1.9, V^p è linearmente indipendente su K. Sappiamo che E è un'estensione algebrica e separabile di K, allora E è separabile su KE^p. Inoltre, poiché per ogni $e \in E$ si ha $e^p \in KE^p$, per il Lemma 3.2.4 E è puramente inseparabile su KE^p. Perciò, per l'Osservazione 3.2.2, $E = KE^p$. Abbiamo quindi dimostrato che V^p è una base di E su K. Mostriamo ora che X è linearmente indipendente su $E^{\frac{1}{p}}$. Consideriamo $r_1u_1 + ... + r_su_s = 0$ con $r_i \in E^{\frac{1}{p}}$ e $u_i \in X$, allora $r_1^p u_1^p + ... + r_s^p u_s^p = 0$. Per ogni i, $r_i^p = \sum_j c_{ij} v_j^p$ con $v_j \in V$ e $c_{ij} \in K$, quindi $0 = \sum_{i,j} c_{ij} u_i^p v_j^p$. Poiché $(UV)^p$ è linearmente indipendente su K, $c_{ij} = 0$ e quindi $r_i = 0$ per ogni $i = 1, ..., s$. □

Esempio 3.3.9. Mostriamo con un esempio che se esiste una base di trascendenza separabile di F su K non è sempre vero che ogni base di trascendenza di F su K sia separabile. Questa costruzione mostra anche che il punto (iii) del Corollario 3.3.8 non vale senza l'ipotesi che E sia algebrico su K.
Sia p un primo, consideriamo $K = \mathbb{Z}_p$, $F = \mathbb{Z}_p(x)$ e $E = \mathbb{Z}_p(x^p)$. Poiché F è un'estensione puramente trascendente di K, per l'Osservazione 3.2.7 abbiamo che F è generato in modo separabile su K con base di trascendenza separabile data da $\{x\}$. In particolare per il Teorema 3.3.6 F è separabile su K. Osserviamo che $E \subsetneq F$, infatti $x \notin E$ e $x \in F$. Notiamo invece che x è algebrico su E essendo radice di $y^p - x^p \in E[y]$, da cui

$$F = K(x) = K(x, x^p) = K(x^p)(x) = E(x) = E[x].$$

Poiché ogni elemento di F è un polinomio in x a coefficienti in E, se lo eleviamo alla p otteniamo un polinomio in x^p a coefficienti in E, ossia un elemento di E. Per il Lemma 3.2.4 abbiamo che F è un'estensione puramente inseparabile di E. Infine, per il Corollario 2.2.2, $\{x^p\}$ è una base di trascendenza di F

su K ma per quanto appena detto non è una base di trascendenza separabile.

Proposizione 3.3.10. *Un campo K è perfetto se e solo se ogni sua estensione è separabile.*

Dimostrazione. Se K ha caratteristica 0 allora la Proposizione è ovvia; supponiamo quindi K di caratteristica $p \neq 0$.
($\Leftarrow$) Se K non è perfetto allora esiste un polinomio $f \in K[x]$ irriducibile su K ma non separabile. L'estensione di K data da $K[x]/(f)$ è perciò un'estensione (algebrica) non separabile di K.
($\Rightarrow$) Sia $u \in K^{\frac{1}{p}}$, allora $u^p = a \in K$. Poiché K è perfetto esiste $b \in K$ tale che $b^p = a$, quindi $0 = b^p - u^p = (b-u)^p$ e $u = b \in K$. Ciò dimostra che se K è perfetto allora $K = K^{\frac{1}{p}}$, per cui per ogni estensione di K la condizione di separabilità è banalmente verificata. □

Corollario 3.3.11. *Sia K un campo perfetto e sia F una sua estensione tale che $[F:K]_t = 1$. Se F non è perfetto allora F è generato in modo separabile su K.*

Dimostrazione. Sia $v \in F$ un elemento trascendente su K, quindi $\{v\}$ è una base di trascendenza di F su K. Se per ogni $n \geq 0$ si ha $v^{\frac{1}{p^n}} \in F$ allora F è algebrico su $E = K\left(v, v^{\frac{1}{p}}, v^{\frac{1}{p^2}}, ...\right)$. Poiché K è perfetto, possiamo chiaramente scrivere ogni elemento di E come potenza p-esima di un altro elemento E, perciò anche E è perfetto. Sia ora L una qualunque estensione di F, per la Proposizione 3.3.10 L è separabile su E e per il Corollario 3.3.8 L è separabile su F. Sempre per la Proposizione 3.3.10 questo implica che F è un campo perfetto, contraddicendo l'ipotesi. Perciò deve esistere un intero m tale che $u = v^{\frac{1}{p^m}} \in F$ ma $u^{\frac{1}{p}} = v^{\frac{1}{p^{m+1}}} \notin F$. Ovviamente u è ancora trascendente su K quindi costituisce una base di trascendenza di F su K.
Sia ora $D = K(u)$, supponiamo per assurdo che esista $a \in F$ inseparabile su

D, allora il suo polinomio minimo appartiene a $D[x^p]$. Sia esso $\sum_{i=0}^{r} \frac{f_i(u)}{g_i(u)} x^{p^i}$, perciò

$$0 = \sum_{i=0}^{r} \frac{f_i(u)}{g_i(u)} a^{p^i} = \left(\frac{\tilde{f}_0\left(u^{\frac{1}{p}}\right)}{\tilde{g}_0\left(u^{\frac{1}{p}}\right)} + \sum_{i=1}^{r} \frac{\tilde{f}_i\left(u^{\frac{1}{p}}\right)}{\tilde{g}_i\left(u^{\frac{1}{p}}\right)} a^{p^{i-1}} \right)^p$$

dove $\tilde{f}_i, \tilde{g}_i$ hanno come coefficienti gli elementi di K che elevati alla p danno i coefficienti dei polinomi f_i, g_i rispettivamente. Questo mostra che in $K\left(u^{\frac{1}{p}}\right)$ il polinomio minimo di a ha grado al più p^{r-1}. Poiché $u \notin D^p$, per il Lemma 1.2.6 abbiamo che $x^p - u$ è irriducibile su D, quindi $\left[D\left[u^{\frac{1}{p}}\right] : D\right] = p$. Per quanto detto prima $[D[a] : D] = p^r$ e $\left[D\left[u^{\frac{1}{p}}, a\right] : D\left[u^{\frac{1}{p}}\right]\right] \leq p^{r-1}$. Abbiamo quindi che $D[a]$ ha dimensione p^r come spazio vettoriale su D mentre $D\left[u^{\frac{1}{p}}, a\right]$ ha dimensione al più p^r come spazio vettoriale su D. Essendo che $D[a] \subseteq D\left[u^{\frac{1}{p}}, a\right]$, otteniamo che $D[a] = D\left[u^{\frac{1}{p}}, a\right]$, ossia che $u^{\frac{1}{p}} \in D[a] \subseteq F$, assurdo. □

Bibliografia

[1] Marco Manetti, *Topologia*. Unitext, 91. La Matematica per il 3+2. Springer-Verlag Italia, Roma (2014).

[2] Thomas W. Hungerford, *Algebra*. Graduate Texts in Mathematics, 73. Springer-Verlag, New York-Berlin, (1980).

[3] David Jacobson, *On perfect subfields over which a field is separably generated*. Proc. Amer. Math. Soc. 33 (1972), 292–296.

[4] Saunders Mac Lane, *Modular fields. I. Separating transcendence bases*. Duke Math. J. 5 (1939), no. 2, 372–393.