**49.** ***Il numero degli automorfismi relativi di un corpo $K$ algebrico e 0-dimensionale sopra $k$ non supera il grado $\frac{K_0}{k}$ del massimo corpo intermedio $K_0$ separabile sopra $k$. Esso uguaglia questo grado nel caso di $K$ galoisiano sopra $k$ e soltanto allora.***

DIMOSTRAZIONE. - Sia $K_0 = (k, x)$ definito sopra $k$ da $f(x) = x^n + \ldots = 0$.

I. Secondo **46** ogni automorfismo $\sigma$ di $K$ sopra $k$ è individuato dal suo effetto su $K_0$ che a sua volta è determinato da $x^\sigma$. Ora. $f(x) = 0$ comporta $f(x^\sigma) = 0$ e perciò l'esistenza di un divisore $X - x^\sigma$ di $f(X)$ in $K[X]$. Quindi, il numero degli automorfismi relativi di $K$ non può essere maggiore del grado $n$ di $f(X)$.

II. Se ci sono precisamente $n$ automorfismi $\sigma_1, \sigma_2, \ldots, \sigma_n$ di $K$ sopra $k$, si conoscono $n$ divisori diversi $X - x^{\sigma_i}$ di $f(X)$ cosicché

$$f(X) = \prod_{i=1}^{n} (X - x^{\sigma_i}).$$

Sia $(K, K^\tau)$ la composizione di $K$ con sè stesso sopra $k$. Da $f(x^\tau) = 0$ segue $\Pi (x^\tau - x^{\sigma_i}) = 0$ nel corpo $(K, K^\tau)$ e quindi $x^\tau = x^{\sigma_i}$, cioè $\tau = \sigma_i$, $K^\tau = K^{\sigma_i} = K$, e ciò mostra che $K$ è galoisiano sopra $k$.

III. Supponendo, viceversa, $K$ galoisiano sopra $k$, da $f(x) = 0$ in $K$ segue (ved. **48**) la riducibilità completa $f(X) = \prod_i (X - x_i)$ in $K[X]$, da $f_x(x) \neq 0$ (ved. **23**) segue poi $f_x(x_i) \neq 0$ e quindi $x_i \neq x_j$ per $i \neq j$. Gli isomorfismi $\sigma_i$ di $K_0$ sopra $k$ definiti da

$$(\sum_m a_m \cdot x^m)^{\sigma_i} = \sum_m a_m \cdot x_i^m \qquad (a_m \in k)$$

sono dunque distinti. Ora, essendo (ved. **22**) il corpo $(K_0, K_0^{\sigma_i}) \subset K$ separabile sopra $k$ come $K_0$ e $K_0^{\sigma_i}$, si ha $(K_0, K_0^{\sigma_i}) = K_0$. Quegli isomorfismi $\sigma_i$ sono pertanto automorfismi di $K_0$. Estendendoli (ved. **41**) a $K$ e componendo $K$ sopra $K_0 = K_0^{\sigma_i}$ con $K^{\sigma_i}$, si ottiene un corpo $(K, K^{\sigma_i\tau})$ che in quanto è composizione di $K$ sopra $k$ con $K$ coincide con $K$. Ciò dimostra che $\sigma_i\tau$ sono automorfismi di $K$ sopra $k$, i quali sono distinti, avendo essi in $K_0$ lo stesso effetto degli automorfismi $\sigma_i$ ivi distinti.

## § 5. La teoria di Galois.

**50.** Conveniamo d'intendere, qualunque siano i corpi $K \supset k$, con

$$\frac{K}{k}$$

l'insieme, evidentemente *gruppo*, degli automorfismi di $K$ sopra $k$.

Si verificano allora subito le relazioni

$$\frac{K}{k_1} \subset \frac{K}{k_2} \quad \text{per } k_1 \supset k_2,$$

$$\frac{K}{k^\sigma} = \sigma^{-1}\frac{K}{k}\sigma, \quad \text{se } \sigma \text{ è automorfismo di } K.$$

Analogamente intendiamo, se $G$ designa un gruppo di automorfismi di un corpo $K$, con

$$\frac{K}{G}$$

l'insieme, evidentemente *corpo*, degli elementi di $K$ invarianti di fronte a tutti gli automorfismi appartenenti a $G$.

Alle relazioni suddette corrispondono allora le formule

$$\frac{K}{G_1} \subset \frac{K}{G_2} \quad \text{per } G_1 \supset G_2,$$

$$\frac{K}{\sigma^{-1}G\sigma} = \left(\frac{K}{G}\right)^\sigma, \quad \text{se } \sigma \text{ è automorfismo di } K.$$

**51.** Ogni elemento di $G$ lasciando fissi gli elementi di $\frac{K}{G}$, si ha

$$\frac{K}{\left(\frac{K}{G}\right)} \supset G.$$

Ogni elemento di $k$ essendo invariante di fronte a tutti gli elementi di $\frac{K}{k}$, si ha

$$\frac{K}{\left(\frac{K}{k}\right)} \supset k.$$

**52.** *Se $K$ è galoisiano e separabile sopra $k$, esso è galoisiano e separabile sopra ogni $K_0$ intermedio fra $K$ e $k$, e l'ordine del gruppo $\frac{K}{K_0}$ coincide col grado di $K$ su $K_0$.*

DIMOSTRAZIONE. - Ogni composizione $(K, K^\sigma)$ di $K$ con $K$ sopra $K_0$ è anche composizione di $K$ con $K$ sopra $k$ e pertanto uguale a $K$, cioè $K$ è galoisiano sopra $K_0$.

La separabilità di $K$ sopra $k$ permette di supporre che $K = (k, x)$ sia definito da $f(x) = 0$ con $f_x(x) \neq 0$, allora $K = (K_0, x)$ sarà definito sopra $K_0$

da un equazione $g(x) = 0$ il cui membro sinistro corrisponde a un divisore $g(X) \in K_0[X]$ di $f(X) = g(X) \cdot h(X)$. Da $f_x(x) = g_x(x) \cdot h(x)$ segue $g_x(x) \neq 0$ cioè la separabilità di $K$ sopra $K_0$.

Essendo dunque $K$ stesso il massimo corpo intermedio fra $K$ e $K_0$ separabile sopra $K_0$, il teorema **49** ci permette di concludere che il numero degli automorfismi di $K$ sopra $K_0$ uguaglia il grado di $K$ sopra $K_0$.

**53.** *Per ogni corpo $K_0$ intermedio di un corpo $K$ galoisiano e separabile sopra $k$ vale*

$$\frac{K}{\left(\frac{K}{K_0}\right)} = K_0.$$

Di fatto, secondo **51** si ha

$$K_1 = \frac{K}{\left(\frac{K}{K_0}\right)} \supset K_0, \text{ e quindi } \text{grado}\,\frac{K}{K_1} \leq \text{grado}\,\frac{K}{K_0};$$

si ha altresì, ponendo $\frac{K}{K_0} = G$,

$$\frac{K}{K_1} = \frac{K}{\left(\frac{K}{G}\right)} \supset G, \text{ e quindi, tenuto conto del teorema } \mathbf{52},$$

$$\text{grado}\,\frac{K}{K_1} = \text{ordine}\,\frac{K}{K_1} \geq \text{ordine}\ G = \text{grado}\,\frac{K}{K_0};$$

il che mostra $K_1 = K_0$, c. d. d.

**54.** *Se $K$ è galoisiano e separabile sopra $k$, vale per ogni sottogruppo $G$ di $\frac{K}{k}$*

(*)
$$\frac{K}{\left(\frac{K}{G}\right)} = G,$$

*e il polinomio $g(X) = \prod_{\sigma \in G} (X - x^\sigma)$ è irriducibile in $\frac{K}{G}[X]$.*

DIMOSTRAZIONE. - L'equazione $g(x) = 0$ mostra che il grado di $K$ relativo al corpo $\frac{K}{G}$ non supera l'ordine del gruppo $G$. D'altro canto si ricava dalla ipotesi $G \subset \frac{K}{k}$ che il corpo $\frac{K}{G}$ è intermedio fra $k$ e $K$ cosicchè quel grado re-

lativo coincide (ved. **52**) con l'ordine del gruppo

$$\frac{K}{\left(\frac{K}{G}\right)} \supset G \qquad \text{(ved. 51).}$$

Avendo dimostrato

$$\text{ordine } G \geq \text{grado } \frac{K}{\left(\frac{K}{G}\right)} = \text{ordine } \frac{K}{\left(\frac{K}{G}\right)} \geq \text{ordine } G$$

risulta verificata tanto l'eguaglianza (*) quanto la irriducibilità dell'equazione $g(x) = 0$ sopra $\frac{K}{G}$.

**55.** Introduciamo in analogia ai simboli $[M]$, $(M)$ definiti in **1** il simbolo

$$\{M\}$$

intendendo con ciò, qualora $M$ designi un sottoinsieme di un gruppo $G$, il gruppo generato da $M$ in $G$, cioè il minimo sottogruppo di $G$ contenente l'insieme $M$.

**56.** *Se $K$ è galoisiano e separabile sopra $k$, e $K_1$, $K_2$ sono corpi intermedi fra $K$ e $k$, si hanno le relazioni*

$$\frac{K}{K_1 \cap K_2} = \left\{\frac{K}{K_1}, \frac{K}{K_2}\right\}, \qquad \frac{K}{(K_1, K_2)} = \frac{K}{K_1} \cap \frac{K}{K_2}.$$

DIMOSTRAZIONE. - I. Da $K_1 \cap K_2 \subset K_i$ segue (ved. **50**)

$$\frac{K}{K_1 \cap K_2} \supset \frac{K}{K_i} \ (i = 1, 2) \text{ e quindi } \frac{K}{K_1 \cap K_2} \supset \left\{\frac{K}{K_1}, \frac{K}{K_2}\right\}$$

mentre da $\left\{\frac{K}{K_1}, \frac{K}{K_2}\right\} \supset \frac{K}{K_i}$ si conclude, tenuto conto di **53**,

$$\frac{K}{\left\{\frac{K}{K_1}, \frac{K}{K_2}\right\}} \subset \frac{K}{\left(\frac{K}{K_i}\right)} = K_i, \text{ cioè } \frac{K}{\left\{\frac{K}{K_1}, \frac{K}{K_2}\right\}} \subset K_1 \cap K_2,$$

donde si trae con **54** e **50**

$$\left\{\frac{K}{K_1}, \frac{K}{K_2}\right\} \supset \frac{K}{K_1 \cap K_2}$$

che, insieme con l'affermazione poc'anzi ottenuta, dimostra la prima delle relazioni asserite.

II. - Da $(K_1, K_2) \supset K_i$ segue

$$\frac{K}{(K_1, K_2)} \subset \frac{K}{K_1} \cap \frac{K}{K_2}.$$

Ogni elemento di $\frac{K}{K_1} \cap \frac{K}{K_2}$ lascia fisso ogni elemento di $(K_1, K_2)$, cioè

$$\frac{K}{K_1} \cap \frac{K}{K_2} \subset \frac{K}{(K_1, K_2)}.$$

Con ciò è chiara la seconda relazione del teorema.

**57.** *Ogni corpo $(K_1, K)$ generato da un corpo $K_1$ galoisiano e separabile sopra $k$ con un corpo qualunque $K \supset k$ è galoisiano e separabile sopra $K$. Si ottiene ogni automorfismo di $(K_1, K)$ sopra $K$ dall'estensione di un automorfismo di $K_1$ sopra $K_1 \cap K$. Identificando un automorfismo di $K_1$ ogni volta con la sua estensione si stabilisce l'identità*

$$\frac{(K_1, K)}{K} = \frac{K}{K_1 \cap K}$$

DIMOSTRAZIONE. - I. Se $K_1$ è galoisiano sopra $k$, tutte le composizioni $((K_1, K), (K_1, K)^\tau) = (K_1, K_1^\tau, K)$ di $(K_1, K)$ con sè stesso sopra $K$ coincidono con $(K_1, K)$ perché $(K_1, K_1^\tau) = K_1$. Dunque $(K_1, K)$ è galoisiano sopra $K$.

II. Supposto $K_1$ separabile sopra $k$, sia $K_1 = (k, x)$ definito da $f(x) = 0$ con $f_x(x) \neq 0$. Allora $(K_1, K) = (K, x)$ è definito sopra $K$ da un'equazione $g(x) = 0$ con $g_x(x) \neq 0$ perché $g(X)$ è divisore di $f(X)$. Ne risulta che $(K_1, K)$ è separabile sopra $K$.

III. Ogni automorfismo $\sigma \in \frac{(K_1, K)}{K}$ è isomorfismo di $K_1$ sopra $k$ e pertanto $(K_1, K_1^\sigma) = K_1$, essendo $K_1$ galoisiano sopra $k$. Ponendo, come in II, $K_1 = (k, x)$, si ricava da

$$(\sum_m a_m \cdot x^m)^\sigma = \sum_m a_m \cdot (x^\sigma)^m \qquad (a_m \in K)$$

che $\sigma$ è individuato dal suo effetto quale automorfismo di $K_1$ e costituisce pertanto l'unica estensione di tale automorfismo al corpo $(K_1, K)$. In questo senso possiamo dire

(*) $$\frac{(K_1, K)}{K} \subset \frac{K_1}{K_1 \cap K}.$$

Se si applica il teorema **54** al caso $G = \frac{(K_1, K)}{K}$, cioè (ved. **53**) $\frac{(K_1, K)}{G} = K$, si riconosce che il polinomio

$$\prod_{\sigma \in \frac{(K_1, K)}{K}} (X - x^\sigma) = g(X)$$

è irriducibile in $K[X]$ e tanto più in $(K_1 \frown K)[X]$, anello cui esso appartiene essendo $x^\sigma \in K_1$. L'equazione $g(x) = 0$ definente $(K_1, K)$ sopra $K$ definisce dunque altresì il corpo $K_1 = (k, x)$ sopra $K_1 \frown K$, il che mostra la coincidenza dei due gradi relativi corrispondenti. Ma essendo questi anche (ved. **52**) gli ordini dei gruppi (*), si ha l'uguaglianza fra i due membri della (*). C. d. d.

**58.** *Un corpo $K_0$, intermedio fra un corpo $K$ galoisiano e separabile sopra $k$ ed il corpo $k$, è galoisiano sopra $k$ allora e soltanto allora che il gruppo $\frac{K}{K_0}$ sia invariante in $\frac{K}{k}$. Associando a ogni automorfismo di $K_0$ sopra $k$ l'insieme delle sue estensioni a $K$, si stabilisce un isomorfismo fra $\frac{K_0}{k}$* e il *gruppo fattoriale $\frac{K}{k} / \frac{K}{K_0}$.*

DIMOSTRAZIONE. - I. Se $K_0$ è galoisiano sopra $k$, vale $(K_0, K_0^\sigma) = K_0$ oppure $K_0^\sigma = K_0$ per ogni $\sigma \in \frac{K}{k}$. Applicando la relazione

$$\sigma^{-1} \frac{K}{K_0} \sigma = \frac{K}{K_0^\sigma} \qquad \text{(ved. 50)} \tag{*}$$

si trova $\sigma^{-1} \frac{K}{K_0} \sigma = \frac{K}{K_0}$ per ogni $\sigma \in \frac{K}{k}$.

II. Supponendo, viceversa, che $\frac{K}{K_0}$ sia invariante nel gruppo $\frac{K}{k}$, cioè che valga $\sigma^{-1} \frac{K}{K_0} \sigma = \frac{K}{K_0}$ per ogni $\sigma \in \frac{K}{k}$, si conclude, tenuto conto della relazione (*) che $K_0^\sigma = K_0$, cioè $\sigma$ induce un automorfismo di $K_0$ sopra $k$. Ora l'ipotesi, che due elementi $\sigma$, $\tau$ di $\frac{K}{k}$ abbiano lo stesso effetto su tutti gli elementi di $K_0$, equivale evidentemente a $\tau \in \frac{K}{K_0} \sigma$. Dunque, il numero degli automorfismi di $K_0$ sopra $k$, determinati dagli elementi del gruppo $\frac{K}{k}$, è uguale all'ordine del gruppo fattoriale $\frac{K}{k} / \frac{K}{K_0}$. Essendo questo numero il massimo possibile, cioè uguale al grado di $K_0$ sopra $k$ (ved. **52**), si riconosce non soltanto che $K_0$ è galoisiano sopra $k$ (ved. **49**), ma altresì che t u t t i gli automorfismi di $K_0$ sopra $k$ sono forniti dagli automorfismi di $K$ sopra $k$.

III. Gli elementi di $\frac{K}{k}$ appartenenti ad un medesimo elemento $\frac{K}{K_0} \sigma$ del gruppo fattoriale $\frac{K}{k} / \frac{K}{K_0}$ sono proprio quelli che estendono l'elemento $\sigma$, considerato come automorfismo di $K_0$, al corpo totale $K$.