§ 4. Corpi galoisiani.

38. DEFINIZIONE. – *Comporre un corpo $K \supset k$ con un corpo $K_1 \supset k$ sopra k* significa generare un corpo (K, K_1') da K e da un corpo K_1', il quale sia isomorfo a K_1 mediante un *isomorfismo sopra k*, cioè un isomorfismo σ tale che sia $a^\sigma = a$ per ogni $a \in k$.

39. *Ogni sopracorpo K di k può essere composto sopra k con un qualsiasi corpo K_1 algebrico rispetto a k.*

DIMOSTRAZIONE. – I. Sia $K_1 = (k, x_1, x_2, \ldots, x_m)$. Formiamo gli anelli $A_0 = k[X_1, X_2, \ldots, X_m]$ e $A = K[X_1, X_2, \ldots, X_m]$ dei polinomi in m variabili $X_1, X_2, \ldots, X_m$ con coefficienti appartenenti a k, risp. a K e chiamiamo $\mathfrak{f}$ l'ideale primo di tutti i polinomi $f(X_1, X_2, \ldots, X_m) \in A_0$ con la proprietà $f(x_1, x_2, \ldots, x_m) = 0$.

L'ideale $\mathfrak{f} \cdot A = \mathfrak{f} \cdot K$ generato da $\mathfrak{f}$ in A è costituito da tutte le somme $\sum_i C_i \cdot f_i$ (con $C_i \in K$, $f_i \in \mathfrak{f}$).

Sia $g(X_1, X_2, \ldots, X_m) = \sum_i C_i \cdot f_i$ un qualsiasi elemento dell'intersezione $\mathfrak{f} \cdot A \cap A_0$ dell'ideale $\mathfrak{f} \cdot A$ con l'anello A_0. Designando con $P_1, P_2, \ldots, P_N$ i diversi prodotti delle potenze delle $X_1, X_2, \ldots, X_m$ che entrano in almeno uno dei polinomi f_i, g e ponendo $g = \sum_j b_j \cdot P_j$, $f_i = \sum_j a_{ij} \cdot P_j$ si ottengono le relazioni $b_j = \sum_i C_i \cdot a_{ij}$ $(j = 1, 2, \ldots, N)$. Ora è noto che un sistema $b_j = \sum_i \xi_i \cdot a_{ij}$ $(j = 1, 2, \ldots, N)$ di equazioni lineari con coefficienti in k che ammetta una soluzione $\xi_i = C_i$ in un sopracorpo K di k ammette necessariamente anche una soluzione $\xi_i = c_i$ in k. Avremo allora $b_j = \sum_i c_i \cdot a_{ij}$ e quindi $g(X_1, X_2, \ldots, X_m) = \sum_i c_i \cdot f_i$. Ne risulta

$$(*) \qquad \mathfrak{f} \cdot A \cap A_0 = \mathfrak{f}.$$

II. Sia $\mathfrak{f} \cdot A = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \ldots \cap \mathfrak{q}_h$ la decomposizione dell'ideale $\mathfrak{f} \cdot A$ in ideali primari appartenenti agli ideali primi $\mathfrak{F}_i \supset \mathfrak{f}$. Allora $\mathfrak{F}_i \cap A_0 \supset \mathfrak{f}$. Se fosse $\mathfrak{F}_i \cap A_0 \neq \mathfrak{f}$ per tutti gli indici i si potrebbero scegliere $f_i \in \mathfrak{F}_i \cap A_0$ tali che $f_i \subset\!\!\!\!- \mathfrak{f}$ cosicché per L abbastanza grande varrebbero le due affermazioni contradittorie $(f_1 \cdot f_2 \ldots f_h)^L \subset \mathfrak{f} \cdot A \cap A_0 = \mathfrak{f}$ (ved. (*)) e $(f_1 \cdot f_2 \ldots \cdot f_h)^L \subset\!\!\!\!- \mathfrak{f}$, essendo $\mathfrak{f}$ ideale primo.

Supponiamo dunque per esempio

$$(**) \qquad \mathfrak{F}_1 \cap A_0 = \mathfrak{f}.$$

L'ideale primo $\mathfrak{F}_1$ definisce allora un sopracorpo $(K, y_1, y_2, \ldots, y_m)$ di K caratterizzato dalle equazioni

$$F(y_1, y_2, \ldots, y_m) = 0 \text{ (allora e soltanto allora che sia } F(X) \in \mathfrak{F}_1)$$

e questo corpo contiene $(k, y_1, y_2, \ldots, y_m)$ isomorfo a K_1 mediante l'isomorfismo σ definito da $a^\sigma = a$ $(a \in k)$, $x_i{}^\sigma = y_i$ $(i = 1, 2, \ldots, m)$. Infatti l'ipotesi (**) garantisce che le equazioni definenti questo sottocorpo $(k, y_1, y_2, \ldots, y_m)$ di $(K, y_1, y_2, \ldots, y_m)$ sopra k coincidono formalmente con le equazioni che definiscono K_1 sopra k.

Il corpo $(K, y_1, y_2, \ldots, y_m) = (K, K_1{}^\sigma)$ è una delle possibili composizioni di K con K_1 sopra k. C. d. d.

40. Come risultato accessorio del ragionamento precedente notiamo per applicazioni ulteriori il lemma seguente:

Supponendo K sopracorpo di k. $A_0 =$ anello $k[X_1, X_2, \ldots, X_m]$ dei polinomi in $X_1, X_2, \ldots, X_m$ sopra k, $A =$ anello $K[X_1, X_2, \ldots, X_m]$ dei polinomi in $X_1, X_2, \ldots, X_m$ sopra K e designando per ogni ideale $\mathfrak{f}$ in A_0 con $\mathfrak{f} \cdot A$ l'ideale generato da $\mathfrak{f}$ in A, si ha

$$\mathfrak{f} \cdot A \cap A_0 = \mathfrak{f}.$$

41. *Ogni isomorfismo σ di un corpo k può estendersi in modo che esso diventi isomorfismo di un dato corpo $(k, x_1, x_2, \ldots, x_m)$ algebrico sopra k.*

DIMOSTRAZIONE. - Riprendiamo le notazioni della dimostrazione **39**.

Ponendo

$$(\Sigma\, a_{i_1 i_2 \ldots i_m} \cdot X_1{}^{i_1} \cdot X_2{}^{i_2} \ldots X_m{}^{i_m})^\sigma = \Sigma\, a^\sigma_{i_1 i_2 \ldots i_m} \cdot X_1{}^{i_1} \cdot X_2{}^{i_2} \ldots X_m{}^{i_m}$$

$$(a_{i_1 i_2 \ldots i_m} \text{ elementi qualunque di } k)$$

si definisce un isomorfismo σ di $A_0 = k[X_1, X_2, \ldots, X_m]$ sull'anello $A_0{}^\sigma = k^\sigma[X_1, X_2, \ldots, X_m]$ dei polinomi di X con coefficienti in k^σ.

All'ideale primo $\mathfrak{f} \neq A_0$ corrisponde allora un ideale primo $\mathfrak{f}^\sigma \neq A_0{}^\sigma$ cosicché le equazioni

$$f^\sigma(y_1, y_2, \ldots, y_m) = 0 \quad \text{(allora e soltanto allora che sia } f^\sigma(X) \in \mathfrak{f}^\sigma)$$

definiscono un corpo $(k^\sigma, y_1, y_2, \ldots, y_m)$ isomorfo a $(k, x_1, x_2, \ldots, x_m)$ mediante l'associazione

$$\left(\frac{\Sigma\, a_{i_1 i_2 \ldots i_m} \cdot x_1{}^{i_1} \cdot x_2{}^{i_2} \ldots x_m{}^{i_m}}{\Sigma\, b_{i_1 i_2 \ldots i_m} \cdot x_1{}^{i_1} \cdot x_2{}^{i_2} \ldots x_m{}^{i_m}}\right)^\sigma = \frac{\Sigma\, a^\sigma_{i_1 i_2 \ldots i_m} \cdot y_1{}^{i_1} \cdot y_2{}^{i_2} \ldots y_m{}^{i_m}}{\Sigma\, b^\sigma_{i_1 i_2 \ldots i_m} \cdot y_1{}^{i_1} \cdot y_2{}^{i_2} \ldots y_m{}^{i_m}}.$$

Che tale associazione stabilisca un isomorfismo si verifica subito tenendo conto delle relazioni $f^\sigma(y_1, y_2, \ldots, y_m) = 0$ e dell'isomorfismo $A_0 \to A_0{}^\sigma$.

42. *Fra le composizioni sopra k di un corpo $K \supset k$ con un corpo K_1 algebrico e n-dimensionale sopra k ce n'è una che è n-dimensionale sopra K.*

DIMOSTRAZIONE. - I. Nel caso particolare $K_1 = (k, x_1, x_2, \ldots, x_n)$, dall'ipotesi $\dim \frac{K_1}{k} = n$, col ragionamento **39** si conclude che l'ideale ivi designato con $\mathfrak{f}$ è 0, cosicché si può prendere $\mathfrak{F}_1 = 0$ ottenendo con questo un corpo $(K, K_1^\sigma) = (K, y_1, y_2, \ldots, y_n)$ n-dimensionale sopra K.

II. Nel caso generale $K_1 = (k, x_1, x_2, \ldots, x_m)$ possiamo supporre che $K_0 = (k, x_1, x_2, \ldots, x_n)$ sia n-dimensionale sopra k. Secondo I esiste allora una composizione (K, K_0^σ) di K con K_0 sopra k con $\dim \frac{(K, K_0^\sigma)}{K} = n$.

Estendendo, come descrive **41**, l'isomorfismo $K_0 \to K_0^\sigma$ al corpo $K_1 = (K_0, x_{n+1}, \ldots, x_m)$ si ottiene un sopracorpo $K_1^\sigma = (K_0^\sigma, y_{n+1}, \ldots, y_m)$ di K_0^σ con cui può essere composto (K, K_0^σ) sopra K_0^σ. Siccome in tale composizione $((K, K_0^\sigma), (K_1^\sigma)^\tau) = (K, K_1^{\sigma\tau})$ il prodotto $\sigma\tau$ è isomorfismo sopra k come i suoi fattori σ, τ, si tratta di una composizione sopra k. Quale sopracorpo di (K, K_0^σ) essa è almeno n-dimensionale sopra K mentre è chiaro d'altra parte, che non esistono composizioni sopra k di K con K_1 la cui dimensione sopra K superi quella di K_1 sopra k.

43. DEFINIZIONE. - Un corpo K è detto *galoisiano sopra* k allora e soltanto allora che esso sia algebrico su k e che la composizione di K con K sopra k dia sempre K.

Ne segue subito, che *un corpo galoisiano sopra* k *è necessariamente* 0*-dimensionale sopra* k. Infatti, il teorema precedente comporta l'esistenza di una composizione di K con K sopra k avente la dimensione relativa $2 \cdot \dim \frac{K}{k}$.

44. *La composizione sopra* k *di un corpo* K *galoisiano sopra* k *con un corpo intermedio fra* k *e* K *dà sempre* K.

DIMOSTRAZIONE. - Sia $k \subset K_0 \subset K$ e (K, K_0^σ) composizione di K con K_0 sopra k. K essendo algebrico su K_0, l'isomorfismo $K_0 \to K_0^\sigma$ può essere esteso (ved. **41**) al corpo totale K, dando così un corpo $K^\sigma \supset K_0^\sigma$. Esiste allora una composizione $((K, K_0^\sigma), (K^\sigma)^\tau) = (K, K^{\sigma\tau})$ di (K, K_0^σ) con K^σ sopra K_0^σ che è altresì composizione di K con K sopra k, perché $\sigma\tau$ lascia fissi gli elementi di k. Dall'ipotesi che K sia galoisiano sopra k segue $(K, K^{\sigma\tau}) = K$ e tanto più $(K, K_0^\sigma) = K$, c. d. d.

45. *La composizione sopra* k *di un corpo* K_1 *galoisiano sopra* k *con un corpo* K_2 *galoisiano sopra* k *è galoisiano sopra* k *e determinata univocamente a meno di isomorfismi sopra* K_1.

DIMOSTRAZIONE. - Siano $K = (K_1, K_2^\sigma)$, $K' = (K_1, K_2^\tau)$ composizioni di K_1 con K_2 sopra k e (K', K'^ρ) una composizione qualunque di K' con K sopra

K_1. Vale allora $(K', K^\rho) = ((K_1, K_2^\tau), (K_1, K_2^{\sigma\rho})) = (K_1, (K_2^\tau, K_2^{\sigma\rho}))$. L'isomorfismo τ^{-1} di K_2^τ su K_2 può estendersi (ved. **41**) al corpo $(K_2^\tau, K_2^{\sigma\rho})$ dando $(K_2^\tau, K_2^{\sigma\rho})^{\tau^{-1}} = (K_2, K_2^{\sigma\rho\tau^{-1}}) = K_2$ giacché K_2 è galoisiano sopra k mentre $\sigma\rho\tau^{-1}$ è isomorfismo sopra k. Abbiamo dunque $(K_2^\tau, K_2^{\sigma\rho}) = K_2^\tau$ e pertanto $(K', K^\rho) = (K_1, K_2^\tau)$ ovvero $(K', K^\rho) = K'$.

Prendendo $K' = K$ si trova $(K, K^\rho) = K$, il che significa, data l'arbitrarietà nella scelta di ρ, che K è galoisiano sopra k.

Per K' qualunqe da $(K', K^\rho) = K'$ segue subito

$$(*) \qquad K' \supset K^\rho$$

cosicché grado $\frac{K'}{k} \geq$ grado $\frac{K^\rho}{k} =$ grado $\frac{K}{k}$. Per la simmetria del ragionamento si ha anche grado $\frac{K}{k} \geq$ grado $\frac{K'}{k}$ e quindi nella (*) vale il segno di uguale. Ma $K' = K^\rho$ dice appunto, che K' è isomorfo a K sopra K_1.

C. d. d.

46. *Se gli isomorfismi σ, τ di un corpo K agiscono entro a un medesimo corpo K', (cioè K^σ, $K^\tau \subset K'$), e hanno lo stesso effetto dentro un sottocorpo K_0 di K su cui K è puramente inseparabile, essi coincidono.*

DIMOSTRAZIONE. - Sia p la caratteristica di K e z un elemento qualunque di K. Esiste una potenza $p^m = q$ tale che z^q appartiene al sottocorpo K_0, cosicché vale

$$(z^q)^\sigma = (z^q)^\tau \quad \text{e pertanto} \quad 0 = (z^\sigma)^q - (z^\tau)^q = (z^\sigma - z^\tau)^q$$

cioè $z^\sigma - z^\tau = 0$, c. d. d.

47. *Da ogni corpo K algebrico e 0-dimensionale sopra k, per mezzo di successive composizioni sopra k con K, si ottiene alla fine un corpo galoisiano sopra k determinato univocamente da K e k a meno di isomorfismi sopra K. Ogni sopracorpo di K galoisiano sopra k contiene un tale corpo galoisiano determinato da K sopra k.*

DIMOSTRAZIONE. - I. Sia $K^* = (k, x)$, definito da $f(x) = 0$, il massimo corpo intermedio fra K e k separabile sopra k (ved. **26**), e sia n il grado di K^* sopra k.

Partendo da $K = K_0$ e componendo successivamente con K sopra k, si costruiscano i corpi $K_0, K_1, K_2, \ldots$ di modo che sia $K_{i+1} = (K_i, K^{\sigma_{i+1}}) \neq K_i$.

Dall'ipotesi $x^{\sigma_i} = x^{\sigma_j}$ segue $z^{\sigma_i} = z^{\sigma_j}$ per z qualunque di K^* e quindi (ved. **46**), essendo K puramente inseparabile sopra K^*, $z^{\sigma_i} = z^{\sigma_j}$ per z qualunque di K, cioè $i = j$. L'equazione $f(x^{\sigma_i}) = 0$ di grado n mostra allora che quella costruzione finisce al massimo dopo $n - 1$ passi.

Sia K_m $(m \geq 0)$ l'ultimo corpo in questa serie cosicché sappiamo:

$$(*) \qquad (K_m, K^\tau) = K_m$$

comunque sia scelta la composizione di K_m con K sopra k. Ne risulta subito K_m essere galoisiano sopra k. Infatti ogni composizione

$$(K_m, K_m^\rho) = (K_m, K^\rho, K^{\sigma_1\rho}, \ldots, K^{\sigma_m\rho})$$

di K_m con sè stesso sopra k coincide per la (*) con K_m.

II. Siano $K_I = (K, K^{\sigma_1}, \ldots, K^{\sigma_p})$, $K_{II} = (K, K^{\tau_1}, \ldots, K^{\tau_q})$ corpi galoisiani ottenuti da K per mezzo di composizioni successive con K sopra k. Componendoli sopra K si ottiene un corpo $(K_I, K_{II}^\rho) = (K_I, K^\rho, K^{\tau_1\rho}, \ldots, K^{\tau_q\rho})$ in cui $(K_I, K^\rho) = K_I$, $(K_I, K^{\tau_i\rho}) = K_I$, essendo K_I galoisiano sopra k e K intermedio fra k e K_I (ved. **44**). Vale dunque $(K_I, K_{II}^\rho) = K_I$ cioè

$$K_{II}^\rho \subset K_I, \qquad \text{grado } \frac{K_{II}}{k} = \text{grado } \frac{K_{II}^\rho}{k} \leq \text{grado } \frac{K_I}{k}$$

e per la simmetria del ragionamento

$$\text{grado } \frac{K_I}{k} \leq \text{grado } \frac{K_{II}}{k}$$

cosicché $K_{II}^\rho = K_I$ come afferma il teorema.

III. Supponendo in II che K_I sia un sopracorpo qualunque di K, galoisiano sopra k, e K_{II} stia a indicare lo stesso corpo detto prima, si ritrova $K_{II}^\rho \subset K_I$, il che costituisce l'ultima affermazione del teorema.

48. *Un corpo K algebrico e 0-dimensionale sopra k è galoisiano sopra k allora e soltanto allora che ogni polinomio $f(X)$ irriducibile in $k[X]$ e annullantesi in K sia prodotto di fattori lineari in $K[X]$.*

DIMOSTRAZIONE. - I. Sia $f(x) = 0$ con $x \in K$, e designi $g(X)$ un fattore irriducibile nella decomposizione di $f(X)$ in $K[X]$. Il corpo (K, y) definito sopra K da $g(y) = 0$ è composizione $(K, (k, y)) = (K, (k, x)^\sigma)$ sopra k di K con (k, x) perché (k, y), definito sopra k da $f(y) = 0$, è isomorfo a (k, x) sopra k. Se dunque K è galoisiano sopra k, per il teorema **44** $(K, y) = K$, cioè $g(X)$ è lineare.

II. Viceversa, supponiamo che ogni polinomio irriducibile in $k[X]$ avente uno zero in K si spezzi dentro all'anello $K[X]$ in fattori lineari. Sotto l'ipotesi che $K = (k, x_1, x_2, \ldots, x_m)$ sia 0-dimensionale sopra k si hanno equazioni $f_i(x_i) = 0$ con $f_i(X)$ irriducibili in $k[X]$. Per ogni composizione $(K, K^\sigma) = (K, x_1^\sigma, x_2^\sigma, \ldots, x_m^\sigma)$ di K con K sopra k vale allora $f_i(x_i^\sigma) = 0$ donde si conclude $x_i^\sigma \in K$ perché $f_i(x_i) = 0$ induce la riducibilità completa di $f_i(X)$ in $K[X]$. Valendo dunque $(K, K^\sigma) = K$, il corpo K è galoisiano sopra k.

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 σ di K sopra k è individuato dal suo effetto su K_0 che a sua volta è determinato da x^σ. 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^τ) 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^τ) 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 σ_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 σ_i sono pertanto automorfismi di K_0. Estendendoli (ved. **41**) a K e componendo K sopra $K_0 = K_0^{\sigma_i}$ con K^{σ_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 σ_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.