Cenni sulla Teoria di Galois

Alcuni cenni tratti dalla teoria di Galois

Considero un'equazione di n-esimo grado a coefficienti $a_1 - a_n \in \mathbb{Q}$ insieme dei numeri razionali.

Def $\mathbb{Q}$ = campo dei numeri razionali

Def $a_1 X + a_2 X^2 + a_3 X^3 + \dots + a_n X^n = 0$

equazione di n-esimo grado a coefficienti $a_1 - a_n \in \mathbb{Q}$

Def $\mathbb{Q}(x_1, x_2)$ = ampliamento del campo dei numeri razionali $\mathbb{Q}$ ottenuto aggiungendo radici dell'equazione di partenza in questo caso $x_1 e x_2 \notin \mathbb{Q}$ se l'equazione di partenza è irriducibile.

Processo

$Q(x_1 \dots x_n)$ = processo iterativo che completa il campo dei numeri razionali $\mathbb{Q}$ aggiungendo tutte le radici dell'equazione date.

Teorema funzioni simmetriche

I coefficienti $a_1 \dots a_n$ dell'equazione possono essere espresse come funzioni simmetriche delle radici $x_1 \dots x_n$.

Basti considerare l'insieme delle funzioni simmetriche così definite:

$$\begin{cases} a_1 = \sum_i x_i \\ a_2 = \sum_{i<j} x_i x_j \\ a_3 = \sum_{i<j<k} x_i x_j x_k \\ \vdots \\ a_n = x_1 \cdot x_2 \cdot x_3 \cdots x_n \end{cases}$$

La dimostrazione è semplice basta scrivere l'equazione

$$a_1 X + a_2 X^2 + \dots + a_n X^n = (X - X_1)(X - X_2) \dots (X - X_n)$$

sviluppare e raccogliere i termini comuni.

Esempio per $n = 3$

$$a_1 = X_1 + X_2 + X_3$$

$$a_2 = X_1 X_2 + X_1 X_3 + X_2 X_3$$

$$a_3 = X_1 X_2 X_3$$

Def.

$S(X_1 \dots X_n)$: gruppo delle permutazioni delle radici $X_1 \dots X_n$ della equazione di partenza

Dim $S(X_1 \dots X_n) = n!$

(Dim per esempio)

Ipotesi

Equazione risolubile per radicali

Procedimento iterativo

Posso partire da $\mathbb{Q}$ e aggiungere la soluzione y_1 di un'equazione ad esempio $(y^p = q)$ con q razionale e p primo. Vale la equazione $y_1 = \sqrt[p]{q}$

Ottengo un campo T' con

$$T' = \mathbb{Q} + \left\{ \sqrt[p]{q} \; ; \; \sqrt[p]{q^2} \; ; \; \dots \; \sqrt[p]{q^{p-1}} \right\} \quad q \in \mathbb{Q}$$

p = primo

processo iterativo

Posso poi individuare un nuovo campo a partire da T' che chiamo T'' ad esempio aggiungendo la radice $y_2 = \sqrt[m]{q' + \sqrt[p]{q}}$ $\quad m; p =$ primi $\quad q', q = \in \mathbb{Q}$

Individuazione di una catena

Posso così avere una serie di ~~campi~~ campi

$$\mathbb{Q} \subset T' \subset T'' \subset T''' \ldots \subset \mathbb{Q}(x_1 - x_n)$$

fino ad avere il campo definitivo

$\mathbb{Q}(x_1 - x_n)$ ~~impossibile~~ ottenuto aggiungendo a $\mathbb{Q}$ le radici dell'equazione data ed invertendo le permutazioni $n!$ delle n radici.

Nel campo T' individuo f permutazioni che lasciano inviariato $T' \subset T''$.

Nel campo T'' individuo p gruppi ognuno composto da f permutazioni (con p primo) per cui il primo gruppo lascia inviariato T' gli altri permettono di scomporre T'' in un gruppo quoziente

$$\frac{G(T'')}{G(T')} = p$$

cioè di suddividere T'' in sotto p gruppi (p=primo) inviariati ciascuno per i p gruppi di permutazioni individuati.

*

~~Se un'equazione è risolubile~~

Tesi

Se un'equazione è risolubile per radicali è possibile individuare una catena di gruppi quozienti

$$\frac{G(Q(x_1,\dots,x_n))}{G(T''''')} \; ; \; \frac{G(T''''')}{G(T''')} \; ; \; \frac{G(T''')}{G(T'')} \; ; \; \frac{G(T'')}{G(T')}$$

~~con tutti~~ aventi rapporto di composizione primo per ognuno di essi.

Negazione della tesi

Un'equazione di ordine $n=5$ non è sempre risolubile per radicali perché non è sempre possibile trovare sottogruppi tra le 5! permutazioni delle radici dell'equazione date tale da individuare una catena tra i rapporti di composizione

$$\frac{G(Q(x_1-x_4))}{G(T''')} \; ; \; \frac{G(T''')}{G(T'')} \; ; \; \frac{G(T'')}{G(T')}$$

aventi rapporto di composizione primo per ogni i.