Università degli Studi di Torino
Facoltà di Scienze Matematiche, Fisiche e Naturali
Corso di Laurea in Matematica

Tesi di Laurea Triennale

NON RISOLUBILITÀ DELL'EQUAZIONE DI 5° GRADO

Relatore:
Prof.ssa Margherita Roggero

Candidato:
Nando Davide Pellicano

Anno Accademico 2004-2005

Indice

Introduzione

Questa tesina si propone di presentare una dimostrazione della non risolubilità per radicali dell'equazione quintica che sia il più possibile semplice e completa. Spesso questo fondamentale risultato, dovuto ai grandi matematici Ruffini(1765-1822) e Abel(1802-1829) viene presentato come applicazione, sia pur importante, di fatti generali della Teoria dei gruppi e della Teoria delle estensioni di campi. La sollecitazione a questo lavoro ci è giunta da un gruppo di insegnanti di matematica delle scuole medie superiori. Alcuni di loro, laureati in fisica, non avevano mai seguito corsi sulla Teoria di Galois; altri, laureati in matematica da alcuni anni, la ricordavano come una teoria estremamente affascinante ma anche difficile da cogliere nelle sue vie essenziali per la mole non indifferente di risultati preliminari richiesti. Abbiamo così deciso di raccogliere in poche pagine questo pilastro della matematica moderna, sforzandoci il più possibile di ridurre allo stretto necessario la tecnica, la generalità e i prerequisiti, affinchè ne possano emergere la struttura e le idee guida. Abbiamo per questo cercato di mettere in luce i fatti essenziali, evitando di sommergerli in dettagli tecnici o procedure puramente formali, per evidenziare invece i significati e le idee portanti. Per non interrompere e non appesantire la linea del ragionamento abbiamo evitato di inserire di volta in volta richiami a definizioni di nozioni di base (quale quella di gruppo, di campo, ecc...) e alle loro proprietà elementari che abbiamo ritenuto essere ben note. Per completezza abbiamo però inserito tali prerequisiti di base in alcuni appendici, in modo che la trattazione risulti completamente self-included e non richieda la consultazione di testi di algebra superiore, non sempre a portata di mano e non sempre di agevole lettura.
Per la dimostrazione ci servono fondamentalmente due concetti: la struttura del gruppo simmetrico trattata nel primo capitolo e il gruppo di Galois trattato nel secondo e terzo capitoli.

Capitolo 1

Il gruppo simmetrico S_n

Sia X un insieme qualsiasi. Si dice PERMUTAZIONE una biezione di X in sè. L'insieme di tutte le permutazioni di X è un gruppo rispetto alla composizione di funzioni. In caso $X = I_n = \{1, 2, \ldots, n\}$, il gruppo delle permutazioni è detto GRUPPO SIMMETRICO DI ORDINE n e si indica con S_n.
L'ordine di tale gruppo è $n!$.
Per rappresentare una permutazione σ di S_n spesso si usa una matrice $2 \times n$: dove nella prima riga si scrivono tutti i numeri da 1 a n (ad esempio nel loro ordine naturale) mentre nella seconda si scrivono ordinatamente le immagini di ciascun numero della prima riga:

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$$

Si noti che i numeri in ciascuna riga sono scritti una e una sola volta, poichè la permutazione è una biezione. Osserviamo inoltre che σ è data dalle colonne di questa matrice, mentre l'ordine con cui si si scrivono le colonne una dopo l'altra è un fatto non essenziale.

Esempio 1.1. Una permutazione di S_6 è :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 6 & 1 & 5 \end{pmatrix}$$

L'elemento neutro del gruppo S_n è la permutazione identica

$$Id = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix}$$

L'inverso di una permutazione σ è la permutazione che si ottiene scambiando tra loro le righe di σ (e volendo si possono riordinare le colonne in modo che i numeri della prima riga siano in ordine crescente).

Esempio 1.2. L'inverso della permutazione σ di prima è:

$$\sigma^{-1} = \begin{pmatrix} 2 & 4 & 3 & 6 & 1 & 5 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 3 & 2 & 6 & 4 \end{pmatrix}$$

Il prodotto tra due permutazioni, avviene da destra a sinistra secondo l'abitudine della composizione di funzioni. Inoltre come per la composizione di funzioni dipende dall'ordine dei fattori.

Esempio 1.3. In S_3:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

e

$$\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Il loro prodotto

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Avendo applicato prima la τ e dopo la σ. Così $(\sigma\tau)(1) = \sigma(\tau(1)) = \sigma(2) = 1$.

Vi è un altro modo per indicare alcune permutazioni. Dati $a_1, \ldots, a_k \in I$, distinti, si indica con $(a_1\ a_2\ \ldots\ a_k)$ la permutazione che manda a_i in a_{i+1} e a_k in a_1 e lascia invariati gli altri elementi. Tale permutazione è detta CICLO di lunghezza k. Un ciclo di lunghezza 2 viene detto TRASPOSIZIONE o scambio.

Esempio 1.4. La permutazione di prima è un 5-ciclo in S_6:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 6 & 1 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 & 6 & 5 \end{pmatrix}$$

Definizione 1.1. Due cicli sono disgiunti se lo sono gli insiemi degli elementi da loro permutati.

I cicli permettono di scrivere tutte le permutazioni; ci sono anzi due modi equalmenti importanti in cui questo può avvenire.

Teorema 1.1. *Sia σ una permutazione di S_n. Allora:*

1. *(**Decomposizione in cicli disgiunti**) $\sigma = \gamma_1 \cdots \gamma_s$ con γ_i cicli due a due disgiunti. Tale scrittura è unica a meno dell'ordine dei fattori.*

2. *(**Decomposizione in scambi**) $\sigma = \tau_1 \cdots \tau_s$ dove le τ_i sono trasposizioni. Tale scrittura non è unica, ma la parità di s dipende solo da σ. È inoltre possibile scegliere tutte le trasposizioni τ_i del tipo $(1\ h)$.*

Dimostrazione. Prima di tutto osserviamo che il prodotto di cicli disgiunti non dipende dall'ordine e quindi l'ordine delle γ_i non conta, mentre conta l'ordine degli scambi τ_i.

1. Diamo una dimostrazione algoritmica. Prendiamo il più piccolo i che viene spostato da σ e consideriamo il ciclo $(i\ \sigma(i)\ \sigma(\sigma(i))\ \cdots)$ che si chiude con un numero di passaggi minore o uguale di n. Se abbiamo elencato tutti gli elementi che in σ si spostano, ci fermiamo; altrimenti prendiamo il minimo j che viene spostato da σ e che non compare nel ciclo precedente e facciamo la stessa cosa.

2. Un modo concreto di convincersi è provare a riordinare n carte poste una accanto all'altra su un tavolo, eseguendo solo degli scambi. Usare un scambio $(1\ h)$ vuol dire scambiare tra loro la carta al 1° posto e la carta all'h-esimo posto. È facile convincersi che è sempre possibile e magari costruire in modo esplicito una procedura generale.
   Volendo una dimostrazione formale si inizi con l'osservare che $(a_1\ ...\ a_k) = (a_1\ a_k)(a_1\ a_{k-1})...(a_1\ a_2)$. In tal modo possiamo scrivere ogni ciclo come prodotto di scambi e quindi, grazie alla decomposizione in cicli ottenta al punto precedente, possiamo scrivere ogni permutazione come prodotti di scambi.
   Per far vedere che possibile scegliere le trasposizioni del tipo $(1\ h)$ notiamo che se $h \neq k$ allora $(h\ k) = (1\ k)(1\ h)(1\ k)$.
   Per la parità di s bisogna fare un ragionamento un pò più lungo. Sia $I_n = \{1, 2, \ldots, n\}$ e sia m il numero naturale non nullo valore del seguente prodotto:

$$P = \prod_{1 \leq i < j \leq n} (i - j) = (1-2)(1-3)\cdots(n-1-n)$$

   Operando su I_n con una permutazione σ il prodotto P o si muta in se stesso mantenendo il valore P, o si muta in un prodotto analogo il cui valore è $-P$, in quanto le differenze sopra scritte si scambiano eventualmente tra loro e possono mutare di segno. Esaminiamo l'effetto che ha su P una trasposizione (hk) con $h < k$. Consideriamo i vari fattori di P, esaminando separatamente l'effetto che ha su di essi lo scambio su indicato.

(a) I fattori che non contengono né h né k non cambiano.

(b) Il fattore $(h-k)$ diventa $(k-h)$(il segno del prodoto cambia).

(c) Se $j<h$ il fattore $(j-h)$ si cambia in $(j-k)$ e viceversa(vi è solo uno scambio di posto, quindi il segno del prodotto non cambia).

(d) Se $h<j<k$ il fattore $(h-j)$ diventa $(k-j)=-(j-k)$ e $(j-k)$ si muta in $(j-h)=-(h-j)$ (il segno del prodotto non cambia).

(e) Se $k<j$ il fattore $(h-j)$ diventa $(k-j)$ e $(k-j)$ si muta in $(h-j)$, ovvero si ha solo lo scambio dei due termini fra loro lasciando immutato il segno.

Quindi una trasposizione muta il prodotto P in un prodotto di valore $-P$. Così se σ è tale da lasciare inalterato il valore di P, essa può essere decomposta solo in un numero pari di trasposizioni, se invece muta il valore del prodotto P in uno analogo di valore $-P$ essa può essere decomposta solo in un numero dispari di trasposizioni.

■

Definizione 1.2. Una permutazione è detta PARI se il numero di trasposizioni in cui si decompone è pari. Altrimenti è DISPARI.

Definizione 1.3. L'insieme delle permutazioni pari è un gruppo e prende il nome di GRUPPO ALTERNO e si indica con A_n.

È evidente che tale insieme è un gruppo in quanto è stabile per il prodotto. La cardinalità di tale gruppo è $\frac{n!}{2}$.

Proposizione 1.2. *Il gruppo alterno A_n è normale in S_n.*

Dimostrazione. Ci sono solo 2 laterali destri: A_n e $S_n - A_n$.
In modo analogo ci sono soltanto 2 laterali sinistri coicidenti con con quelli destri. ■

Proposizione 1.3. *Il gruppo alterno A_n è generato dai 3-cicli.*

Dimostrazione. Basta provare che ogni elemento di A_n è prodotto di 3-cicli. Ogni $\sigma \in A_n$ è, per definizione, prodotto di un numero pari di trasposizioni. Il risultato sarà provato se mostreremo che il prodotto di due trasposizioni è sempre un 3-ciclo o prodotto di due 3-cicli. Se le due trasposizioni coincidono, si ottiene la permutazione identica ($Id \in A_n$), se le due trasposizioni sono disgiunte $\sigma = (a\ b)$ e $\tau = (c\ d)$ allora $\sigma\tau = (a\ b\ c)(b\ c\ d)$. Se le due trasposizioni hanno un simbolo in comune $\sigma = (a\ b)\ \tau = (b\ c)$ si ha $\sigma\tau = (a\ b\ c)$.
■

I risultati seguenti saranno punti chiave per provare la non risulubilità dell'equzione di quinto grado.

Proposizione 1.4. *Se H è un sottogruppo di S_5 che contiene un 5-ciclo e un 2-ciclo, allora $H = S_5$.*

Dimostrazione. A meno di un cambio di nomi, si può supporre che lo scambio sia $\tau = (1\ 2)$. Componendo con se stesso il 5-ciclo un numero opportuno di volte(al massimo 4 volte) si trova un 5-ciclo σ in cui $\sigma(1) = 2$. Cambiando se necessario i nomi agli altri indici si può supporre che σ sia $(1\ 2\ 3\ 4\ 5)$. Proviamo che con questi si ottengono tutte le permutazioni.
Si ha:

$$\sigma = (1\ 2)$$
$$\tau\sigma\tau\sigma^{-1}\tau = (1\ 3)$$
$$\sigma^{-1}\tau\sigma^{-1}\tau\sigma\tau\sigma = (1\ 4)$$
$$\sigma^{-1}\tau\sigma = (1\ 5)$$

Poichè si possono ottenere tutti gli scambi $(1\ k)$ il teorema 1.1 ci permette di concludere. ∎

Definizione 1.4. Un gruppo G si dice RISOLUBILE se è possibile trovare una catena finita di sottogruppi G_i

$$G = G_0 \supset G_1 \supset G_2 \supset ... \supset G_s = \{1_G\}$$

tale che ciascuno degli G_i sia normale nel precedente G_{i-1} e ogni quoziente G_{i-1}/G_i sia abeliano.

Proposizione 1.5. *A_5 non è risolubile.*

Dimostrazione. Sia N un sottogruppo di A_5 tale che A_5/N sia abeliano. Allora per ogni coppia di elementi σ e τ di A_5 si deve avere $\sigma N\tau N = \tau N\sigma N$ e quindi $\sigma\tau\sigma^{-1}\tau^{-1} \in N$.
Presi ad esempio i 3-cicli $\sigma = (1\ 4\ 3)$ e $\tau = (3\ 2\ 5)$ si ottiene $\sigma\tau\sigma^{-1}\tau^{-1} = (1\ 2\ 3)$. In generale $(i_1\ i_2\ i_3)$ si otterrà con $\sigma = (i_1\ i_4\ i_3)$ e $\tau = (i_3\ i_2\ i_5)$ dove $\{1, 2, 3, 4, 5\} = \{i_1, i_2, i_3, i_4, i_5\}$. Quindi N contiene tutti i 3-cicli.
Grazie alla proposizione 1.3 N coincideA_5 e quindi la catena si interrompe senza raggiungere il sottogruppo banale $\{Id\}$. ∎

Osservazione 1.6. È opportuno notare che S_n/A_n è isomorfo a $\mathbb{Z}/2\mathbb{Z}$ (basta vedere che la cardinalità di S_n/A_n è 2 e ogni gruppo d'ordine 2 è isomorfo a $\mathbb{Z}/2\mathbb{Z}$).

Esempi di gruppi risolubili:

- Il gruppo simmetrico S_3 è risolubile, infatti basta prendere la catena

$$S_3 \supset A_3 \supset \{I_d\}$$

  visto che A_3 è abeliano.

- Il gruppo simmetrico S_4 è risolubile; infatti, basta prendere la catena

$$S_4 \supset A_4 \supset V \supset \{I_d\}$$

  con $V = \{I_d, (1\ 2\ )(3\ 4\ ), (1\ 3\ )(2\ 4\ ), (1\ 4\ )(2\ 3\ )\}$, che è abeliano così come A_4/V.

Proposizione 1.7. *Il gruppo simmetrico S_5 non è risolubile.*

Dimostrazione. Abbiamo già visto che A_5 per non è risolubile. Se S_5 avesse un sottogruppo normale H t.c. S_5/H fosse abeliano, allora $A_5 \cap H$ sarebbe un sottogruppo normale di A_5 ossia sarebe A_5 stesso oppure $\{Id\}$ Nel primo caso avremmo la catena

$$S_5 \supset A_5$$

non ulteriormente prolungabile (perchè A_5 non è risolubile). Nel secondo caso H coterebbe solo Id e una permutazione σ dispari t.c. $\sigma^2 = Id$. In S_5 permutazioni dispari si fatte sono solo gli scambi e quindi H è del tipo $\{Id, (1\ 2)\}$ che non è però normale in S_5 poichè ad esempio $(1\ 3)(1\ 2)(1\ 3) \notin H$

■

Capitolo 2

Equazioni algebriche

Consideriamo ora le equazioni algebriche. Salvo altre indicazioni l'ambiente in cui ci muoviamo sono i campi. Alcuni risultati fondamentali sui campi e sugli spazi vettoriali sono trattati nell'appendice 3.

Definizione 2.1. Si dice equazione algebrica o POLINOMIALE in una incognita, di grado n a coefficienti in un campo F, un'equazione della forma

$$a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \ldots + a_1 x + a_0 = 0$$

dove $a_0, a_1, \ldots, a_n$ sono coefficienti assegnati in F: scriveremo in breve $p(x) = 0$.
Si dice GRADO di tale equazione l'intero n, se $a_n \neq 0$. Indicheremo il grado con $\partial p(x)$.
Inoltre indicheremo con $F[x]$ l'anello dei polinomi e i coefficienti nel campo F.
Con abuso di terminologia diremo RADICE o SOLUZIONE di un polinomio $p(x)$ ogni valore α per cui $p(\alpha) = 0$.

Definizione 2.2. Si dice che un polinomio $p(x)$ di grado n è RIDUCIBILE se si può spezzare in un prodotto di polinomi con grado inferiore a n ma > 1. Se ciò non è possibile il polinomio si dice IRRIDUCIBILE.

Teorema 2.1 (FONDAMENTALE DELL'ALGEBRA). *Ogni polinomio con coefficienti complessi di grado n ($n > 0$) ha almeno una radice nel campo dei numeri complessi.*

Teorema 2.2 (RUFFINI). *Sia $\alpha \in F$ una radice di $p(x) \in F[x]$; allora $(x - \alpha)$ divide $p(x)$.*

Dimostrazione. Eseguiamo la divisione $p(x)$ con $(x-\alpha)$:
$p(x) = (x-a)q(x)+r(x)$ con $\partial r(x) < \partial(x-a) = 1$, quindi $r(x) = r \in F$ Valutiamo quest'espressione in α: $p(\alpha) = 0 = (\alpha-\alpha)q(\alpha)+r \Rightarrow r = 0$, cioè $p(x)$ è divisibile per $(x-\alpha)$. ∎

Questi teoremi ci permettono di concludere che ogni polinomio di grado n ha esatteamete n radici complesse (eventualmente coicidenti) e di fattorizzare un polinomio in fattori lineari. Ma essendo il teorema fondamentale dell'algebra di sola esistenza, non ci permette di trovare le radici e poter fattorizzare esplicitamente il polinomio. Nel caso i polinomi a cui siamo interessati abbiano coefficienti reali, per trovare tutte le soluzioni, ossia un numero di soluzioni pari al grado, dobbiamo comunque ammettere anche soluzioni complesse non reali. Così se $p(x) \in F[x]$, sarà utile ammettere anche soluzioni di $p(x) = 0$ in campi K che sono estensioni di F, in particolare nella chiusura algebrica $\overline{F}$ di F che (come $\mathbb{C}$, se $F = \mathbb{R}$) contiene tutte le soluzioni dei polinomi a coefficienti in F.

Definizione 2.3. Sia $p(x) \in F[x]$ e siano $\alpha_1, \alpha_2, \ldots, \alpha_n$ tutte le radici di $p(x)$. Il campo minimo che contiene sia $p(x)$ che $\alpha_1, \alpha_2, \ldots, \alpha_n$ si chiama CAMPO DI SPEZZAMENTO di $p(x)$ e si indica con $F(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, \alpha_n)$ oppure con $= F(\alpha_1)(\alpha_2)\ldots(\alpha_{n-1})(\alpha_n)$. Nel proprio campo di spezzamento ogni polinomio si spezza quindi in fattori lineari.

Esempio 2.1. Prendiamo $F = \mathbb{Q}$ e $p(x) = x^4 - 5x^2 + 6$. In $\mathbb{Q}$ il polinomio si spezza $p(x) = (x^2-2)(x^2-3)$, ma non si può spezzare in fattori lineari. Consideriamo allora $F_1 = \mathbb{Q}(\sqrt{2})$ in questo campo si ha $p(x) = (x-\sqrt{2})(x+\sqrt{2})(x^2-3)$. Per poterlo linearizzare dobbiamo passare ad un'altra estensione $F_2 = F_1(\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$ dove finalmente $p(x)$ si spezza in fattori lineari: $p(x) = (x-\sqrt{2})(x+\sqrt{2})(x-\sqrt{3})(x+\sqrt{3})$. Abbiamo così ottenuto il campo di spezzamento $\mathbb{Q}(\sqrt{2},\sqrt{3})$ di $p(x)$.

Proposizione 2.3. *Sia $p(x) \in F[x]$ irriducibile; allora l'ideale $(p(x))$ è massimale.*

Dimostrazione. Bisogna far vedere che $F[x]/(p(x))$ è un campo, cioè che un elemento non nullo di $F[x]/(p(x))$ ha inverso rispetto al prodotto. Sia $g(x) + (p(x)) \in F[x]/(p(x))$ invertibile, cioè $\exists h(x) \in F[x]$ t.c. $(h(x)+(p(x)))(g(x)+(p(x))) = h(x)g(x)+(p(x)) = 1+(p(x))$ ossia $h(x) \in F[x]$ t.c. $h(x)g(x)+p(x)q(x) = 1$ per qualche $q(x) \in F[x]$. Visto che $p(x)$ è irriducibile
$MCD(p(x),\ g(x)) = \begin{cases} 1 \\ p(x) \end{cases}$. Se vale il secondo caso $\Rightarrow g(x) = k(x)p(x)$ per qualche $k(x) \in F[x] \Rightarrow g(x) \in (p(x)) \Rightarrow g(x)+(p(x)) = 0+(p(x))$

che è una contraddizione col fatto di essere non nullo. Per l'identità di Bezout $\exists h(x), q(x) \in F[x]$ t.c. $h(x)g(x) + p(x)q(x) = MCD(p(x), g(x)) = 1$.
■

Proposizione 2.4. *Se $p(x) \in F[x]$ è irriducibile allora $F[x]/(p(x))$ è un campo che contiene almeno una radice di $p(x)$.*

Dimostrazione. Scriviamo $E = F[x]/(p(x))$
$E[x] = \{$polinomi a coefficienti in $E\}$ e si ha che $F[x] \subseteq E[x]$. Sia $p'(x) = \sum_{i=0}^{n} a_i x^i$ con gli $a_i \in E$. Sostituiamo $\theta = x + (p(x)) \in E$
$p'(\theta) = \sum_{i=0}^{n} a_i \theta^i = \sum_{i=0}^{n} a_i (x + (p(x)))^i = \sum_{i=0}^{n} a_i (x^i + (p(x))) = \sum_{i=0}^{n} (a_i x^i + (p(x))) = \sum_{i=0}^{n} a_i x^i + (p(x)) = p(x) + (p(x)) = 0 + (p(x)) \in E$ che è elemento neutro rispetto alla somma in E quindi $p'(\theta)$ è nullo in $E \Rightarrow \theta$ è una radice di $p'(x)$. Ma $p'(x)$ è uguale a $p(x)$ che quindi ha almeno una radice in E.
■

Proposizione 2.5. *Sia $p(x) \in F[x]$ irriducibile e α una sua radice in un'estensione E di F allora $F(\alpha) \cong F[x]/(p(x))$.*

Dimostrazione. Consideriamo l'applicazione

$$\phi : F[x] \to F(\alpha)$$

$$f(x) \mapsto f(\alpha)$$

f è un omomorfismo di anelli, infatti: $\phi(f(x)+g(x)) = f(\alpha)+g(\alpha) = \phi(f(x))+\phi(g(x))$ e $\phi(f(x)g(x)) = f(\alpha)g(\alpha) = \phi(f(x))\phi(g(x))$
Il nucleo $Ker\phi$ di ϕ (osia l'insieme degli elementi la cui immagine è 0) contiene i polinomi $f(x)$t.c.$f(\alpha) = 0$. Per il teorema di Ruffini si tratta dei multipli di $(x - \alpha)$ in $E[x]$. Se dividiamo $f(x)$ per $p(x)$ anche il resto della divisione si annulla in α poichè $f(x) = p(x)q(x) + r(x)$ e quindi $r(\alpha) = 0$. D'altra parte $p(x)$ e $r(x)$ non possono avere fattori in comune a parte 1 e $p(x)$ stesso, perchè abbiamo supposto $p(x)$ irriducibile. Allora $r(x)$ è multiplo di $p(x)$ pur avendo grado inferiore: non può essere altro che $r(x) = 0$ e quindi $f(x)$ è multiplo di $p(x)$. Per il teorema fondamentale degli anelli(che si ottiene da quello dei gruppi con qualche piccola osservazione) $F[x]/Ker\phi \cong Im\phi$.

Dimostriamo che $Im\phi = F(\alpha)$. Basta verificare che $1/g(\alpha)$ ha controimmagine in $F[x]$ perché se $\phi(f(x)/g(x)) = \phi(f(x))\phi(1/g(x))$
ϕ è suriettiva $\Leftrightarrow$ $f(\alpha)/g(\alpha)$ ha controimmagine $\Leftrightarrow$ sia $f(\alpha)$ che $1/g(\alpha)$ hanno controimmagine in $F[x]$. Per $f(\alpha)$ si ha per come è stata definita la funzione. Se $h(x) \in F[x]$ t.c. $\phi(f(x)) = 1/g(\alpha)$, poichè $g(\alpha) \neq 0$ e $p(x)$ irriducibile

$\Rightarrow$ MCD$(g(x), p(x)) = \begin{cases} 1 \\ p(x) \end{cases}$, ma non può essere $p(x)$ perché α è radice di $p(x)$ ma non lo è di $g(x)$. Per l'identità di Bezout $\exists h(x), k(x) \in F[x]$ t.c. $1 = MCD(g(x), p(x)) = h(x)g(x) + k(x)p(x) = h(\alpha)g(\alpha) + k(\alpha)p(\alpha)$ ma α è radice di $p(x)$ quindi $k(\alpha)p(\alpha) = 0 \Rightarrow h(\alpha)g(\alpha) = 1 \Rightarrow h(\alpha) = 1/g(\alpha) \Rightarrow h(x)$ è controimmagine di $1/g(\alpha) \Rightarrow \phi$ è suriettiva
ϕ iniettiva e suriettiva allora ϕ è un isomorfismo. ∎

Definizione 2.4. Sia $E \supset F$ un'estensione di F, un elemento $\alpha \in E$ si dice ALGEBRICO su F se $\exists$ un polinomio $p(x) \in F[x]$ t.c. $p(\alpha) = 0$.

Proposizione 2.6. *Sia $E \supset F$ un estensione di F, allora E è uno spazio vettoriale su F e la sua dimensione come spazio vettoriale è così indicata*

$$Dim_F E = grado\ di\ E\ su\ F = [E : F]$$

Proposizione 2.7. *Sia α algebrico su F e $p(x)$ il polinomio minimo di α allora $[F(\alpha) : F] = dim_F F(\alpha) = \partial p(x)$.*

Dimostrazione. $F(\alpha) = \{a_0 + a_1\alpha + ... + a_{m-1}\alpha^{m-1} / a_i \in F\}$ dove $m = \partial p(x)$. Affermiamo che $\{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}\}$ è una base dello spazio vettoriale di $F(\alpha)$ su F; per essere base deve:

1. sistema di generatori
2. linearmente indipendenti

la prima condizione è immediatamente verificata in quanto è evidente che forma effettivamente $F(\alpha)$. Per la seconda se $\{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}\}$ fossero linearmente dipendenti $\Rightarrow \exists a_0, a_1, \ldots, a_{m-1}$ t.c. $a_0 + a_1\alpha + ... + a_{m-1}\alpha^{m-1} = 0$ il polinomio $p'(x) = a_0 + a_1x + ... + a_{m-1}x^{m-1} \in F[x]$ ha α come radice, ma $\partial p'(x) < \partial p(x)$ mentre $p(x)$ deve essere di grado minimo di α, contraddizione. ∎

Proposizione 2.8. *Date estensioni $E \supset K \supset F$ con $[E : F] < +\infty \Rightarrow [E : F] = [E : K][K : F]$.*

Corollario 2.9. *Se $[E : F]$ è un primo $\Rightarrow$ non esiste alcun sottocampo intermedio tra E e F.*

Proposizione 2.10. *Dato un campo F, α è un elemento algebrico su $F \Leftrightarrow [F(a) : F] < +\infty$.*

Dimostrazione. $''\Rightarrow''$ Sia α algebrico su F allora $[F(\alpha):F]$ =grado del polinomio minimo di α su F, sia $p(x)$ il polinomio di α t.c. $p(x)=n$ allora $\{1,\alpha,\alpha^2,...,\alpha^{m-1}\}$ è base di $F(\alpha)$ su F.
$''\Leftarrow''$Se $[F(a):F]<+\infty=n=dim_F F(\alpha)$. Siano $1,\alpha,\alpha^2,...,\alpha^{n-1},\alpha^n\in F(\alpha)n+1$ vettori linearmente dipendenti $\Rightarrow\exists a_0,a_1,..,a_n\in F$ t.c. $a_0+a_1\alpha+\ldots+a_{n-1}\alpha^{n-1}+a_n\alpha^n=0$. Posto $p(x)=a_0+a_1x+...+a-n-1x^{n-1}+a_nx^n$ allora α è una radice di $p(x)$ e quindi α è algebrico su F. ∎

Proposizione 2.11. *Dato un campo F se α e β sono algebrici su F allora $\alpha\pm\beta,\alpha\beta,\alpha^{-1},\beta^{-1}$ sono algebrici su F.*

Definizione 2.5. Un'estensione $E\supset F$ ALGEBRICA su F se ogni elemento di E è algebrico su F.

Proposizione 2.12. *Se E è un'estensione algebrica su F e K su E, allora K è un'estensione algebrica su F.*

Definizione 2.6. Sia α una radice di $p(x)\in F[x]$, α si dice radice MULTIPLA se $(x-\alpha)^2$ divide $p(x)$.

Definizione 2.7. $p(x)=a_0+a_1x+...+a_nx^n$ la DERIVATA di $p(x)$ è $p'(x)=a_1+2a_2x+...+na_nx^{n-1}$.

Proposizione 2.13. *$p(x)\in F[x]$ non ha alcuna radice multipla $\Leftrightarrow$ $MCD(p(x),p'(x))=1$.*

Definizione 2.8. Dato un isomorfismo di campi $\sigma:F\to F'$ allora definiamo

$$\sigma^*:F[x]\to F'[x]$$

$$f(x)=\sum_{i=1}^{n}a_ix^i\mapsto\sum_{i=1}^{n}\sigma(a_i)x^i=f^*(x)$$

Proposizione 2.14. *σ^* è un isomorfismo di anelli.*

Dimostrazione. $\sigma^*(f(x)+g(x))=\sigma^*(f(x))+\sigma^*(g(x))$
$\sigma^*(f(x)g(x))=\sigma^*(f(x))\sigma^*(g(x))$
Ker$\sigma^*=\{f(x)\in F[x]$ t.c.$\sigma^*(f(x))=0\}=\{f(x)\in F[x]$ t.c.$f^*(x)=0\}=\{f(x)=0\}$
Quindi σ^* è iniettiva.
σ^* è suriettiva dalla suriettività di σ. ∎

Proposizione 2.15. *Sia $p(x)\in F[x]$ un polinomio irriducibile. Sia α una radice di $p(x)$ e α^* una radice di $p^*(x)=\sigma^*(f(x))\in F'[x]$. Allora $\exists!$ Isomorfismo $\sigma':F[\alpha]\to F'[\alpha^*]$ con σ' ristretta su $F=\sigma$ e $\sigma'(\alpha)=\alpha^*$.*

Dimostrazione. Definiamo

$$\sigma' : F(\alpha) \to F'(\alpha^*)$$

$$\sum_{i=1}^{n} a_i \alpha^i \mapsto \sum_{i=1}^{n} \sigma(a_i) \alpha^{*^i} = f^*(x)$$

σ' è un morfismo di anelli suriettivo e iniettivo.
$p(x)$ irriducibile in $F[x] \Leftrightarrow p^*(x)$ è irriducibile in $F'[x]$ e si ha $F(\alpha) \cong F[x]/(p(x))$ e $F'(\alpha^*) \cong F'[x]/(p^*(x))$ con $\sigma^*(p(x)) = (p^*(x)) \subset F'[x]$.
Per la proprietà di anelli che dati A e A' anelli t.c. $\sigma' : A \cong A'$ e per un ideale $H \subset A \Rightarrow A/H \cong A'/\sigma^*(H)$ t.c. $\forall a \in A a + H \mapsto \sigma^*(a) + \sigma^*(H)$ si ha così che $F[x]/(p(x)) \cong F'[x]/(p * (x))$.
Quindi

$$F(\alpha) \cong F[x]/(p(x)) \cong F'[x]/(p * (x) \cong F'(\alpha^*)$$

$$\alpha \mapsto \alpha + p(x) \mapsto \alpha^* + p(x) \mapsto \alpha^*$$

$$a \mapsto a + p(x) \mapsto \sigma(a) + p(x) \mapsto \sigma(a)$$

questa composizione è σ' e σ' su F dà $\sigma \forall a \in F \sigma'(a) = \sigma(a)$. Per dimostrare l'unicità si prende un'altra funzione $\tau : F(\alpha) \to F'(\alpha^*)$ t.c. $\tau(a) = \sigma(a) \forall a \in F$. Poiché sia τ che σ' sono isomorfismi e ristretti su F danno σ basta dimostrare che $\tau(\alpha) = \sigma(\alpha) = \alpha^*$.
$p^*(\tau(\alpha)) = \sum_{i=1}^{n} \sigma(a_i) \tau(\alpha)^i = \sum_{i=1}^{n} \tau(a_i \alpha^i) = \tau(\sum_{i=1}^{n} (a_i \alpha^i)) = \tau(p(\alpha)) = \tau(0) = 0$. Ma $t(\alpha) \in F'(\alpha^*)$ è anche radice di $p^*(x)$ e α^* radice di $p^*(x)$, contraddizione con $\tau(\alpha) = \sigma^*$ perché questa è generatore e non radice.

Teorema 2.16. *Sia $\sigma : F \to F'$ un isomorfismo di campi. Sia $E \supset F$ un campo di spezamento di $f(x) \in F[x]$ e $E' \supset F'$ anche campo di spezzamento di $f(x)^* \in F'[x]$. Allora:*

1. *$\exists$ un isomorfismo $\widetilde{\sigma} : E \to E'$ che estende σ*
2. *$\exists$ esattamente un numero $[E : F]$ di estensioni $\widetilde{\sigma} : E \to E'$ di σ*

Dimostrazione. Dimostriamo 1)
Si usa l'induzione su $[E : F]$
Se $[E : F] = 1 \Rightarrow E = F$ in modo banale
Per $[E : F] \geq 2$ sia $p(x)$ un fattore irriducibile di $f(x)$ in $F[x]$ con $\partial p(x) \geq 2$.
Sia $\alpha \in E$ una radice di $p(x) \Rightarrow \exists \widetilde{\sigma} : F(\alpha) \to F'(\alpha^*)$ isomorfismo con $\widetilde{\sigma}|_F = \sigma$ dove α^* è una radice di $p^*(x) \in F'[x]$
Poichè E è un campo di spezzamento di $f(x)$ su $F(\alpha)$ e $[E : F(\alpha)] < [E : F]$ e

E' è un campo di spezzamento di $f^*(x)$ su $F'(\alpha)$ allora per l'ipotesi induttiva $\exists$ un isomorfismo $\widehat{\sigma} : E \to E'$ che estende $\widetilde{\sigma} \Rightarrow$ estensione di σ
Dimostriamo 2)
Si usa l'induzione su $[E : F]$
Se $[E : F] = 1 \Rightarrow$ ovvio
Per $[E : F] \geq 2$ sia $f(x) = p_1(x)p_2(x)\dots p_r(x)$ con $p_i(x) \in F[x]$ irriducibili $\exists$ almeno un $p_j(x)$ con $\partial p_j(x) > 1$. Sia $\partial p_1(x) = d \geq 2$ allora $p_1(x)$ ha d radici distinte in E. Sia α una radice di $p_1(x)$, siano $\alpha_1^*, \dots, \alpha_d^*$ radici di $p_1^*(x)$ esistono d isomorfismi estensioni di σ

$$\widehat{\sigma} : F(\alpha) \to F(\alpha_i^*)$$

$$\sum_j a_j \alpha^j \mapsto \sum_j \sigma(a_j)\alpha^{*j}$$

$\forall \widehat{\sigma}_i \ \exists [E : F(\alpha)]$ estensioni $\widetilde{\sigma} : E \to E' \ \widetilde{\sigma}|_{F(\alpha)} = \widehat{\sigma}_i$. Ma $[E : F(\alpha)] = \frac{[E:F]}{d}$ perchè $[F(\alpha) : F] = d \Rightarrow \exists$ un numero $d[E : F(\alpha)] = [E : F]$ estensioni di σ $\widetilde{\sigma} : E \to E'$ ∎

Proposizione 2.17. *Dato $K \supset F$, $f(x) \in F[x]$, K contiene un unico campo di spezzamento di $f(x)$ se K contiene tutte le radici di $f(x)$*

Proposizione 2.18. *Per ogni monomorfismo $\sigma : F(\alpha_1, \dots, \alpha_n) \to E$ con $\sigma|_F = Id$ si ha $\sigma(F(\alpha_1, \dots, \alpha_n)) = F(\alpha_1, \dots, \alpha_n)$ campo di spezzamento di $f(x)$ dove E è un'estensione di F che contiene tutte le radici $\{\alpha_1, \dots, \alpha_n\}$ di un polinomio $f(x) \in F[x]$.*

Dimostrazione. $\sigma(\alpha_i)$ radice di $f^*(x) = f(x) \Rightarrow \sigma(\alpha_i) = \alpha_j$ per qualche $1 \leq j \leq n \Rightarrow \sigma(F(\alpha_1, \dots, \alpha_n)) \subseteq F(\alpha_1, \dots, \alpha_n)$
Vediamo l'altra inclusione
Visto che σ è un monomorfismo $\Rightarrow \sigma : F(\alpha_1, \dots, \alpha_n) \to \sigma(F(\alpha_1, \dots, \alpha_n)) \subseteq F(\alpha_1, \dots, \alpha_n)$ è un isomorfismo, infatti $\forall \beta \in F(\alpha_1, \dots, \alpha_n)$ si trova un controimmagine in $F(\alpha_1, \dots, \alpha_n)$. Se $\beta = g(\alpha_1, \dots, \alpha_n) \in F(\alpha_1, \dots, \alpha_n)$ allora $\sigma(g(\sigma^{-1}(\alpha_1), \dots, \sigma^{-1}(\alpha_n))) = g(\alpha_1, \dots, \alpha_n)$ controimmagine di $g(\alpha_1, \dots, \alpha_n)$ e quindi σ è suriettiva. Visto che un campo non può essere isomorfo a un suo sottocampo $\Rightarrow \sigma(F(\alpha_1, \dots, \alpha_n)) = F(\alpha_1, \dots, \alpha_n)$. ∎

Capitolo 3

Teorema di Abel-Ruffini

Definizione 3.1. $E \supset F$ un'estensione $Aut|_F E = \{\sigma \in Aut\ E\ t.c.\ \sigma(a) = a\ \forall a \in F\}$.

Osservazione 3.1. Si nota immediatamente che dati $\sigma_1, \sigma_2 \in Aut|_F E$ si ha che $\sigma_1^{-1} \in Aut|_F E$ e la composizione $\sigma_1\sigma_2 \in Aut|_F E \Rightarrow Aut|_F E$ è un gruppo.

Teorema 3.2. *Sia E un'estensione di un campo F e siano $\alpha_1, \ldots, \alpha_n \in E$. Allora il numero di morfismi*

$F(\alpha_1, \ldots, \alpha_n) \to E =$ *coincide con il grado dell'estensione* $[F(\alpha_1, \ldots, \alpha_n) : F]$

Definizione 3.2. Se E è un campo di spezzamento di $f(x) \in F[x]$, $Gal(E/F) = Aut|_F E$ si chiama GRUPPO DI GALOIS di $f(x)$.

Esempio 3.1. Consideriamo il polinomio $f(x) = x^4 - 2$ tale polinomio è irriducbile in $\mathbb{Q}$, perchè le sue radici sono $\alpha_1 = \sqrt[4]{2}, \alpha_2 = -\sqrt[4]{2}, \alpha_3 = i\sqrt[4]{2}, \alpha_4 = -i\sqrt[4]{2}$ dove la i è l'unità immmaginaria ($i^2 = -1$).
Consideriamo un omomorfismo $\varphi : \mathbb{Q}(\sqrt[4]{2}, i) \to \mathbb{C}$. Tale funzione fissa tutto il campo $\mathbb{Q}$, ma non può agire liberamente sulle soluzioni del polinomio, perchè non è ammissibile che

$$\alpha_1 \mapsto \alpha_3$$

$$\alpha_2 \mapsto \alpha_2$$

$$\alpha_3 \mapsto \alpha_1$$

$$\alpha_4 \mapsto \alpha_4$$

perchè $\alpha_1 + \alpha_2 = 0$ mentre $\varphi(\alpha_1 + \alpha_2) = \varphi(\alpha_1) + \varphi(\alpha_2) = \alpha_3 + \alpha_2 \neq 0$
Si può invece costituire tale permutazione ammissibile:

$$\alpha_1 \mapsto \alpha_3$$

$$\alpha_2 \mapsto \alpha_4$$

$$\alpha_3 \mapsto \alpha_1$$

$$\alpha_4 \mapsto \alpha_2$$

Tutte le permutazioni ammissibili dunque sono 8 e sono, oltre l'I_d:

$$\sigma_{\mathbf{1}} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_3 & \alpha_4 & \alpha_2 & \alpha_1 \end{pmatrix}$$

$$\sigma_{\mathbf{2}} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_2 & \alpha_1 & \alpha_4 & \alpha_3 \end{pmatrix}$$

$$\sigma_{\mathbf{3}} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_4 & \alpha_3 & \alpha_1 & \alpha_2 \end{pmatrix}$$

$$\sigma_{\mathbf{4}} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_1 & \alpha_2 & \alpha_4 & \alpha_3 \end{pmatrix}$$

$$\sigma_{\mathbf{5}} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_4 & \alpha_3 & \alpha_2 & \alpha_1 \end{pmatrix}$$

$$\sigma_{\mathbf{6}} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_2 & \alpha_1 & \alpha_3 & \alpha_4 \end{pmatrix}$$

$$\sigma_{\mathbf{7}} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_3 & \alpha_4 & \alpha_1 & \alpha_2 \end{pmatrix}$$

Queste permutazioni costituiscono il gruppo di Galois del polinomio.

Teorema 3.3. *Sia $f(x) \in F[x]$ e E il suo campo di spezzamento. Se $f(x)$ ha n radici distinte allora $Gal(E/F) \cong$ sottogruppo di S_n.*

Dimostrazione. $X = \{\alpha_1, \ldots, \alpha_n\}$ radici distinte di $f(x)$ sia ha che per $\sigma \in Gal(E/F)$ $\sigma(X) = X$.

$$\varphi : Gal(E/F) \to S_X = S_n$$

$$\sigma \mapsto \sigma|_X$$

È un omomorfismo in quanto $\varphi(\sigma\tau) = (\sigma\tau)|_X = \sigma\tau = \varphi(\sigma)\varphi(\tau)$
Ker$\varphi = \{\sigma \in Gal(E/F)/\varphi(\sigma) = Id\} = \{Id\}$ quindi φ è iniettiva.
E è campo di spezzaento di $f(x) \in F[x] \Rightarrow [E : F] = n = \partial p(x)$. Le $\sigma \in Gal(E/F)$ fissano F in $E \Rightarrow |Gal(E/F)| = |S_X|$ quindi φ è anche suriettiva $\Rightarrow \varphi$ è isomorfismo. ∎

Definizione 3.3. Un ampliamento K di un campo F si dice FINITO se il grado $[K : F]$ è finito. Si dice INFINITO in caso contrario.

Definizione 3.4. Sia K un'estensione di un campo F. Due elementi α e β di K, algebrici sopra F, si dicono CONIUGATI su F se hanno lo stesso polinomio minimo su F.

Definizione 3.5. Un'estensione K di F si dice estensione NORMALE di F se K è chiuso rispetto ai coniugati.

Definizione 3.6. Un'estensione K di F finita e normale si dice ESTENSIONE GALOISIANA.

Definizione 3.7. Un'estensione L di un campo F si dice RADICALE se

$$L = F(\alpha_1, \alpha_2, \ldots, \alpha_m)$$

con $\alpha_1^{n_1} \in F, \alpha_i^{n_i} \in F(\alpha_1, \ldots, \alpha_i)(i = 1, \ldots, m)$ per interi positivi $n_1, n_2, \ldots, n_m$.

Definizione 3.8. Sia $f(x) \in F[x]$. Si dice che $f(x)$ è RISOLUBILE PER RADICALI se il suo campo di spezzamento K è contenuto in un'estensione radicale L su F.

Teorema 3.4 (della CORRISPONDENZA di GALOIS). *Sia $f(x)$ un polinomio a coefficienti in un campo F. Detto K il suo campo di spezzamento, sia $G(K, F)$ il suo gruppo di Galois. Indicato con* F *l'insieme di tutti i sottocampi T di K che contengono F e con* G *l'insieme di tutti i sottogruppi di $G(K, F)$, la*

$$\Psi : \mathrm{F} \to \mathrm{G}$$

$$T \mapsto G(K, T)$$

è una corrispodenza biunivoca tra F *e* G*, la cui inversa è la*

$$\Phi : \mathrm{G} \to \mathrm{F}$$

$$H \mapsto K_H$$

dove con K_H indichiamo il campo K fissato da H.

Lemma 3.5. *Sia F un campo che contiene tutte le radici n-esime dell'unità, allora il gruppo di Galois di $x^n - a$ è abeliano.*

Dimostrazione. Sia α una radice di $x^n - a$ e ω radice n-esima primitiva dell'unità. Tutte le radici di $x^n - a$ sono $\alpha, \alpha\omega, \alpha\omega^2, \ldots, \alpha\omega^{n-1}$. Quindi il campo $K = F(\alpha)$ è il campo di spezzamento di $x^n - a$. Detti σ e τ due elementi di $G(K, F)$ per provare che $\sigma\tau = \tau\varsigma$ basta provare che $\sigma(\tau(\alpha)) = \tau(\sigma(\alpha))$. Ora, dato che un elemento di $G(K, F)$ manda una radice di $x^n - a$ in un'altra radice dello stesso polinomio, si avrà

$$\sigma(\alpha) = \alpha\omega^h, \tau(\alpha) = \alpha\omega^k$$

Quindi

$$\sigma(\tau(\alpha)) = \sigma(\alpha\omega^h) = \alpha\omega^k\omega^h = \alpha\omega^h\omega^k = \tau\sigma(\alpha)$$

dato che $\sigma(\omega^i) = \omega^i$ perchè $\omega \in F$. ∎

Lemma 3.6. *Sia L un'estensione radicale su F. Allora L è contenuta in un'estensione radicale M di F tale che M sia un'estensione galoisiana su F.*

Dimostrazione. Sia $L = F(\alpha_1, \alpha_2, \ldots, \alpha_m)$ con $\alpha_1^{n_1} \in F$ e $\alpha_i^{n_i} \in F(\alpha_1, \alpha_2, \ldots, \alpha_{i-1})$. Se $p_i(x)$ è il polinomio minimo di α_i, sia M il campo di spezzamento del polinomio $f(x) = p_1(x)p_2(x)\cdots p_m(x)$. M è un'estensione galoisiana di F contenente L e radicale: infatti $F(\alpha_i)$ è isomorfo a $F(\beta_{ij})$, dove β_{ij} è una qualunque radice di $p_i(x)$, e tale isomorfismo si può estendere ad un automorfismo che fissa F in M. Dato che α_i appartiene ad un'estensione radicale di F, anche ogni β_{ij} appartiene ad un'estensione radicale di F. ∎

Teorema 3.7. *Sia L un'estensione galoisiana radicale di un campo F. Allora il suo gruppo di Galois $G(L, F)$ è risolubile.*

Dimostrazione. Sia $L = F(\alpha_1, \alpha_2, \ldots, \alpha_m)$ con $\alpha_1^{n_1} \in F$ e $\alpha_i^{n_i} \in F(\alpha_1, \alpha_2, \ldots, \alpha_{i-1})$. Se indichiamo con n il mcm$(n_1, n_2, \ldots, n_m)$, ogni α_i è tale che $\alpha_1^n \in F$ e $\alpha_i^n \in F(\alpha_1, \alpha_2, \ldots, \alpha_{i-1})$, quindi nella definizione di estensione radicale si può, senza perdere di generalità, supporre tutti gli n_i siano uguali ad un intero n. Sia ς una radice n-esima primitiva dell'unità, e sia $L' = L(\varsigma)$. L' è anch'essa un'estensione galoisiana di F. Sia $H = G(L', F)$ il gruppo di Galois di L' su F. Poniamo

$$L_0 = F,\ L_1 = F(\varsigma),\ L_i = F(\varsigma, \alpha_1, \alpha_2, \ldots, \alpha_{i-1})$$

per $i = 2, \ldots, m+1$. Ovviamente $L_{m+1} = L'$ e

$$F = L_0 \subseteq L_1 \subseteq \ldots \subseteq L_{m+1} = L'$$

In base al teorema di corrispodenza di Galois, a tale catena di estensioni corrisponde la seguente catena di sottogruppi di $G(L', F)$

$$G(L', F) \supseteq G(L', L_1) \supseteq G(L', L_2) \supseteq \ldots \supseteq G(L', L') = Id.$$

Asseriamo che ciascuno dei sottogruppi della catena è normale nel precedente e che i quozienti sono abeliani. L_1 è campo di spezzamento del polinomio $x^n - 1$ e in quanto tale è un'estensione galoisiana, quindi, per il teorema di corrispodenza di Galois, $G(L', L_1) \trianglelefteq G(L', F)$; inoltre il suo gruppo di Galois $G(L_1, F)$ è abeliano; ma $G(L_1, F) \cong G(L', F)/G(L', L_1)$, quindi il primo quoziente della catena è abeliano. Esaminiamo ora le altre estensioni, L_{i+1} su L_i, della catena 3: ciascuna di queste estensioni contiene le radici n-esime dell'unità, ed è tale da che $L_{i+1} = L_i(\alpha_i), \alpha_i$ essendo una radice di $x^n - \alpha_i, \alpha_i = \alpha_i^n \in L_i$. Ma allora ogni L_{i+1} è un'estensione galoisiana di L_i, e quindi per il teorema di corrispondenza di Galois si ha $G(L', L_{i+1}) \trianglelefteq G(L', L_i)$; inoltre per il lemma 83 ha gruppo di Galois $G(L_{i+1}, L_i) \cong G(L', L_i)/G(L', L_{i+1})$ abeliano. Abbiamo così provato che il gruppo $G(L', F)$ è risolubile. Resta da provare che $G(L, F)$ è risolubile. La situazione è la seguente:

$$F \subseteq L \subseteq L'.$$

Posto $H_1 = G(L', F), H_2 = G(L', L)$ si ha $H_2 \trianglelefteq H_1$ essendo L su F galoisiana e $G(L, F) \cong H_1/H_2$. Essendo $G(L, F)$ quoziente di un gruppo risolubile è anch'esso risolubile. ∎

Teorema 3.8. *Un polnomio $f(x) \in F[x]$ è risulubile per radicali se il suo gruppo di Galois è risolubile.*

Dimostrazione. Per definizione di polinomio risolubile, esisterà un'estensione radicale, che possiamo supporre galoisiana senza perdita di generalità, L tale che $F \subseteq K \subseteq L$. Dobbiamo provare che $G(K, F)$ è risolubile. Essendo K estensione galoisiana di F, $G(L, K) \trianglelefteq G(K, F)$, e $G(K, F) \cong G(L, F)/G(L, K)$. Ma $G(L, F)$, per il teorema 3.7, è risolubile, e quindi lo è anche $G(K, F)$ in quanto immagine omomorfa di un gruppo risolubile. ∎

Teorema 3.9 (Abel-Ruffini). *Il polinomio generale di grado ≥ 5 non è risolubile per radicali.*

Dimostrazione. Dimostreremo il teorema sul polinomio $p(x) = 2x^5 - 5x^4 + 5 \in \mathbb{Q}[x]$. Basta provare che il suo gruppo di Galois non è risolubile. Proveremo esattamente che è S_5. Per il teorema fondamentale dell'algebra tale polinomio

ha 5 radici nel campo dei numeri complessi. Facendo lo studio di funzione di tale polinomio si nota che ha 3 radici reali e 2 complesse coniugate. Indichiamo con $\alpha_1, \alpha_2, \alpha_3$ le tre radici reali e α_4, α_5 le due radici complesse. Le due radici complesse sono coniugate, cioè con stessa parte reale ma parte immaginaria opposta, questo fatto indica che le due radici sono interscambiabili tra di loro, infatti la permutazione che scambia tra loro le soluzioni complesse coniugate (e quindi lascia ferme quelle reali) è sempre accettabile, perchè non modifica i numeri interi (che sono particolari numeri reali) e va d'accordo con le operazioni. Quindi il gruppo di Galois contiene il $2-ciclo$ $(\alpha_4\ \alpha_5)$.
Visto che il polinomio è irriducibile, α_1 ha ordine 5 in quanto $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = 5$. Fissando α_1 ho un sottogruppo con quoziente fatto da 5 elementi, quindi l'ordine del gruppo è un multiplo di 5. Da ciò si evince che contiene un $5-ciclo$. Quindi il gruppo di Galois contiene un $2-ciclo$ e un $5-ciclo$ e come abbiamo visto nella proposizione 1.4 un gruppo così formato è S_5, che sappiamo dalla proposizione 1.7 non essere risolubile. ∎

Capitolo 4

Appendice 1: I Gruppi

Definizione 4.1. Si dice GRUPPO un insieme non vuoto G dotato di un'operazione binaria $* : G \times G \to G$ tali che valgono le seguenti proprietà:

1. Associativa: $\forall a, b, c \in G a * (b * c) = (a * b) * c = a * b * c$
2. elemento neutro: $\exists 1_G \ \forall a \in G$ t. c. $a * 1_G = 1_G * a = a$
3. inverso: $\forall a \in G \ \exists a^{-1}$ t. c. $a * a^{-1} = a^{-1} * a = 1_G$

Definizione 4.2. In un gruppo valgono le seguenti proprietà:
- l'elemento neutro è unico
- l'inverso di ogni elemento è unico
- l'inverso del prodotto di due elementi è il prodotto degli inversi in ordine opposto, cioè

$$\forall a, b \in G \ \ (a * b)^{-1} = b^{-1} * a^{-1}$$

In modo naturale è ora data la definizione di sottogruppo.

Definizione 4.3. Un sottoinsieme non vuoto S di un gruppo G è un SOTTOGRUPPO se è un gruppo per la stessa operazione di G.

Con $S \leq G$ indicheremo che S è sottogruppo di G.
Dalla definizione si deduce subito che l'elemento neutro deve appartenere al sottogruppo e che per ogni elemento del sottogruppo deve appartenere al sottogruppo anche il suo inverso. Vi è un importante criterio per determinare se un sottoinsieme S di G sia un sottogruppo.

Criterio 4.1. *Un sottoinsieme non vuoto S di un gruppo G è un SOTTOGRUPPO se e solo se $\forall a, b \in S \ a * b^{-1} \in S$.*

Diciamo infine che un gruppo per cui vale la proprietà commutativa, si chiama GRUPPO COMMUTATIVO o ABELIANO.
L'ordine di un gruppo finito G è il numero dei suoi elementi ed è denotato $|G|$.

Definizione 4.4. Si dice ORDINE o PERIODO di un elemento $a \in G$ il più piccolo intero $r > 0$ t. c. $a^r = 1_G$.

Presi un gruppo $(G, *)$ e un suo sottogruppo S definiamo su G la relazione σ nel modo seguente:

$$a\sigma b \Leftrightarrow b * a^{-1} \in S \text{ ovvero se } \exists s \in S \; t. \; c. \; b = s * a$$

Si verifica facilmente che questa relazione σ è una equivalenza: ossia che soddisfa le seguenti proprietà:

- Riflessiva: $\forall a \in G$ si ha $a\sigma a$ (infatti $1_G \in S$ e $a = 1_G * a$)
- Simmetrica: $a\sigma b \Rightarrow b\sigma a$ (infatti se $a\sigma b$, ossia $\exists s \in S$ t. c. $b = s * a$ allora $a = s^{-1} * b$, visto che S è un sottogruppo e quindi $s^{-1} \in S$)
- Transitiva: $a\sigma b$ e $b\sigma c \Rightarrow a\sigma c$ (infatti $\exists s_1 \in S$ t. c. $b = s_1 * a$ ed $\exists s_2 \in S$ t. c. $c = s_2 * b$ allora $c = (s_2 * s1) * a$ con $s_2 * s_1 \in S$ essendo S un sottogruppo).

Si può ora dare la seguente definizione.

Definizione 4.5. Le classi di equivalenza della relazione σ sono dette LATERALI DESTRI di S e si denotano così:

$$Sa = \{s * a \text{ t. c. } s \in S\}$$

Si può definire in modo analogo la relazione di equivalenza σ':

$$a \; \sigma' b \Leftrightarrow a^{-1} * b \in S \Leftrightarrow \exists s \in S \text{ t. c. } b = a * s$$

Le classi di equivalenza sono dette LATERALI SINISTRI di S e si denotano con

$$aS = \{a * s \text{ t. c. } s \in S\}$$

Ora possiamo dare una definizione molto importante.

Definizione 4.6. Un sottogruppo N di G si dice NORMALE se i suoi laterali destri coincidono con quelli sinistri, cioè se valgono le seguenti condizioni equivalenti:

1. $\forall a \in G$ si ha $aN = Na$
2. $\forall a \in G\ \forall n \in N\ \exists n' \in N$ t.c. $n' * a = a * n$
3. $\forall a \in G\ \forall n \in N$ si ha $a * n * a^{-1} \in N$

Con $N \triangleleft G$ indicheremo che N è sottogruppo normale di G.

Definizione 4.7. Un gruppo G si dice SEMPLICE se non ha sottogruppi normali non banali.

Il seguente teorema fornisce la motivazione dell'importanza data alla nozione di sottogruppo normale.

Teorema 4.2. *Sia $(G, *)$ un gruppo e N un suo sottogruppo normale. L'insieme quoziente G/N è un gruppo.*

Dimostrazione. Iniziamo col definire l'operazione. Presi due laterali Na eNb si ha il prodotto $(Na) * (Nb) = N(a * b)$.
Innanzi tutto la definizione non dipende dai rappresentati. Infatti presi $a' \in Na$ *e* $b' \in Nb$ $\exists m, n \in N$ t. c. $a' = n * a$ e $b' = m * b$ poichè N è normale, $\exists m' \in N$ t.c. $a * m = m' * a$. Si ha allora $a' * b' = (n * a) * (m * b) = n * (a * m) * b = n * m' * a * b \in Nab$.
Vediamo che G/N è un gruppo rispetto tale prodotto
-proprietà associativa $(Na)(NbNc) = (Na)(N(a*b)) = N(a*(b*c)) = N((a*b)*c) = N(a*b)Nc = (NaNb)Nc$
- elemento neutro: è $N1$, ossia è N stesso. Infatti $N1Na = N(1 * a) = Na = NaN1 = N(a * 1) = Na$
- inverso: l'inverso di N_a è Na^{-1} infatti $NaNa^{-1} = N(a * a^{-1}) = N1 = N$ e $Na^{-1}Na = N(a^{-1} * a) = 1N = N$. ∎

Omomorfismi di gruppi

Definizione 4.8. Siano G, G' due gruppi. Una funzione $f : G \to G'$ è detta OMOMORFISMO se $\forall x, y \in G\ f(xy) = f(x)f(y)$.
Un omomorfismo è INIETTIVO se $\forall x, y \in G$ con $x \neq y \Rightarrow f(x) \neq f(y)$ e tale omomorfismo si chiama MONOMORFISMO.
Un omomorfismo è SURIETTIVO se $Im(f) = G'$ ossia se $\forall z \in G'\ \exists x \in G$ t. c. $f(x) = z$ tale omomrfismo è detto EPIMORFISMO.
Un omomorfismo che è sia iniettivo che iniettivo è detto ISOMORFISMO.

Proposizione 4.3. *Sia $f : G \to G'$ un omomorfismo di gruppi. L'immagine di un sottogruppo di G è un sottogruppo di G'.*

Dimostrazione. Sia $H < G$; usiamo il criterio per dimostrare che $f(H) < G'$. Presi $x', y' \in f(H)$ $\exists x, y \in H$ t.c. $f(x) = x'$ e $f(y) = y'$ poichè H è un sottogruppo, si ha $xy^{-1} \in H$ e quindi $f(xy^{-1}) = f(x)f(y^{-1}) = f(x)(f(y))^{-1} = x'(y')^{-1} \in f(H)$. ∎

Definizione 4.9. Dato un omomorfismo $f : G \to G'$ si dice NUCLEO di f e lo si indica con $Ker(f)$ l'insieme delle controimmagini dell'elemento neutro $1'_G \in G'$

$$Ker(f) = \{x \in G \text{ t. c. } f(x) = 1_{G'}\}$$

Tale insieme è un sottogruppo di G in quanto controimmagine del sottogruppo improprio $1_{G'}$. Diamo un criterio per capire quando un omomorfismo è un monomorfismo.

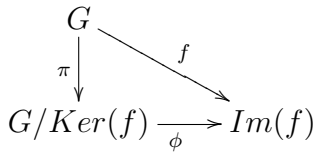
Criterio 4.4. *f è un monomorfismo se e solo se $Ker(f) = 1_G$*

Dimostrazione. $''\Rightarrow''$ Se f è iniettiva $1'_G$ ha una sola controimmagine che è necessariamente 1_G
$''\Leftarrow''$ Sia $Ker(f) = 1_G$ e $x, y \in G$ t. c. $f(x) = f(y)$;allora $f(x)(f(y))^{-1} = 1_{G'}$. D'altra parte $f(x)f(y^{-1}) = 1_{G'} \Rightarrow f(xy^{-1}) = 1_{G'}$ e quindi $xy^{-1} \in Ker(f)$, conseguentemente $xy^{-1} = 1_G$ ossia $x = y$. ∎

Teorema 4.5. *Se $f : G \to G'$ è un omomorfismo di gruppi, allora $Ker(f)$ è un sottogruppo normale di G.*

Dimostrazione. Sia $x \in G$ e $k \in Ker(f)$. Allora $f(xkx^{-1}) = f(x)f(k)f(x^{-1}) = f(x)1_{G'}(f(x))^{-1} = f(x)(f(x))^{-1} = 1_{G'}$ quindi $xkx^{-1} \in Ker(f)$ ossia $Ker(f)$ è normale. ∎

Teorema 4.6 (Teorema fondamentale degli omomorfismi di gruppi). *Sia $f : G \to G'$ un omomorfismo di gruppi. Esiste un isomorfismo $\phi : G/Ker(f) \to Im(f)$tale da rendere commutativo il seguente diagramma:*



Dimostrazione. Posto $K = Ker(f)$. $\forall k \in Ke \forall a \in G$ si ha $f(Ka) = f(k)f(a) = 1'_G f(a) = f(a)$ quindi tutti gli elementi del laterale Ka hanno la stessa immagine mediante f, perciò è corretto definire la funzione $f : G/K \to Im(f) \subseteq G'$ avendo posto $f(Ka) = f(a)$. Per definizione si ha $\phi \circ \pi = f$

ϕ è un omomorfismo infatti $\phi(KaKb) = \phi(Kab) = f(ab) = f(a)f(b) = \phi(Ka)\phi(Kb)$
ϕ è suriettiva:un elemento $f(a) \in Im(f)$ ha come controimmagine Ka.
ϕ è iniettiva:$Ker(\phi) = \{Ka/\phi(Ka) = 1'_G\} = \{Ka/f(a) = 1_{G'}\} = \{Ka/a \in K\} = \{K\} = \{1_{G/K}\}$ Quindi ϕ è un isomorfismo. ∎

Capitolo 5

Appendice 2: Semplicità di A_n con $n \geq 5$

Riportiamo qui due risultati visti per $n = 5$, ma che si possono generalizzare.

Proposizione 5.1. *Il gruppo alterno A_n è semplice per $n \geq 5$.*

Dimostrazione. Per iniziare dobbiamo provare che le permutazioni di N, dato $N \triangleleft A_n$, che lasciano fissi il maggior numero di elementi di I_n sono dei 3-cicli. Sia $\rho \in N$ una permutazione che lascia fissi almeno tanti elementi quanti ogni altra permutazione di N. Supponiamo che ρ non sia un 3-ciclo e consideriamo la decomposizione di ρ in cicli a due a due disgiunti. Sia hanno 2 casi:

1. se tutti i cicli di questa decomposizione sono scambi si ha:
   $\rho = (a\ b)(c\ d)\cdots$
2. uo dei cicli è d'ordine ≥ 3 e si ha:
   $\rho = (a\ b\ c\ \ldots)\cdots$

In quest'ultimo caso esistono almeno 2 elementi di $I_n - \{a, b, c\}$ che non sono lasciati fissi da da ρ. Indichiamoli con e e f. Siccome $n \geq 5$, possiamo considerare, in ognuno dei casi, il 3-ciclo $\upsilon = (c\ e\ f)$ (gli elementi a, b, c, e, f sono sempre supposti distinti 2 a 2). Trasformiamo ρ mediante υ. Se vale la (1) si ha:

$$\rho_1 = \upsilon\rho\upsilon^{-1} = (c\ e\ f)(a\ b)(c\ d)\cdots(c\ e\ f)^{-1} = (a\ b)(d\ e)\cdots$$

Se invce vale (2) si ha:

$$\rho_1 = \upsilon\rho\upsilon^{-1} = (c\ e\ f)(a\ b\ c\ \ldots)\cdots(c\ e\ f)^{-1} = (a\ b\ e\ \ldots)\cdots$$

Siccome N è un sottogruppo normale, si ha $\rho_1 \in N$ e $\rho_1^{-1}\rho \in N$. Tutti gli elementi di $I_n - \{a, b, c, e, f\}$ lasciati fissi dalla permutazione ρ sono lasciarti fissi anche da $\rho_1^{-1}\rho$.
Nel primo caso, nessuno degli elementi a, b, c, d è lasciato fisso da ρ. Ora

$$(\rho_1^{-1}\rho)(a) = a \quad e \quad (\rho_1^{-1}\rho)(b) = b$$

e ciò prova che $\rho_1^{-1}\rho$ lascia fissi più elementi di ρ, contrariamente all'ipotesi.
Nel secondo caso, nessuno degli elementi a, b, c, e, f è lasciato fisso da ρ. Ora, $(\rho_1^{-1}\rho)(a) = a$, il che mostra di nuovo che $\rho_1^{-1}\rho$ lascia fissi più elementi di ρ.
Avendo trovato una contraddizione risulta che ρ è un 3-ciclo.
Sia N un sottogruppo normale in A_n diverso da $\{I_d\}$, supponiamo che$N$ contenga il ciclo (1 2 3), allora $\forall i \geq 4$ conterrà, essendo $N \triangleleft A_n$ ed essendo ogni 3-ciclo una permutazione pari, il 3-ciclo (3 2 i)(1 2 3)(3 2 i)$^{-1}$ = (1 i 2). Ma allora N conterrà (1 i 2)$^{-1}$ = (1 2 i) $\forall i \geq 4$. Questi 3-cicli generano tutto A_n e così $N = A_n$. ∎

Proposizione 5.2. *Il gruppo simmetrico S_n non è risolubile per $n \geq 5$.*

Dimostrazione. Il ragionamento è uguale a quello fatto per $n = 5$. ∎

Capitolo 6

Appendice 3

6.1 I Campi

Definizione 6.1. Si dice ANELLO COMMUTATIVO CON UNITÀ un insieme non vuoto A dotato di due operazioni binarie

$$+ : A \times A \to A$$

e

$$* : A \times A \to A$$

tale che valgono i seguenti assiomi:

1. A è un gruppo abeliano rispetto alla prima operazione
2. A la seconda operazione è abeliana
3. $\forall a,\ b,\ c \in A\ \ a * (b * c) = (a * b) * c = a * b * c$
4. $\forall a,\ b \in A\ \ a * b = b * a$
5. $\exists 1_A \forall a \in A\ \ 1_A a = a 1_A = a$
6. Distributiva: $\forall a, b, c \in A a * (b + c) = a * b + a * c$

Se in A (meno lo 0_A) tutti gli elementi hanno l'inverso, allora A è un CAMPO. Da ora in poi ometteremo il simbolo $*$, cioè $a * b = ab$.

Definizione 6.2. Un sottoinsieme non vuoto N di un anello A è un SOTTOANELLO se è un anello per le stesse operazioni di A e $1_N = 1_A$, ossia:

1. $\forall a, b \in N$ si ha $a - b \in N$
2. $\forall a, b \in N$ si ha $ab \in N$
3. $1_N = 1_A$

Definizione 6.3. Si dice IDEALE di un anello A un sottoanello I per cui valgono:

1. $\forall r_1, r_2 \in I$ si ha $r_1 - r_2 \in I$
2. $\forall a \in A \ \forall r \in I$ si ha $ar \in I$.

Definizione 6.4. Sia I un ideale di A. Si definisce ANELLO QUOZIENTE $A/I = \{a + I / \forall a \in A\}$. Inoltre, poichè ogni ideale è un sottogruppo di $(A, +)$ si può considerare il quoziente A/I. Tra i sottogruppi di A, gli ideali sono esattamente tutti e soli quelli per cui A/I è un anello con il prodotto $(a + I)(b + I) = ab + I$

Il teorema fondamentale degli omomorfismi di gruppi vale anche per gli anelli e quindi per i campi.

Definizione 6.5. Si dice che I è un ideale MASSIMALE di un anello A se non esiste un ideale maggiore di lui, a parte A stesso.

Ricordiamo un'importante caratterizzazione.

Proposizione 6.1. *I ideale massimale di $A \Leftrightarrow A/I$ è un campo.*

Definizione 6.6. Siano $F \subseteq K$ campi e $a \in K$ ma $a \notin F$. Allora $F(a)$ è un campo contenente sia F che a e viene detto ESTENSIONE di F.

Definizione 6.7. Gli isorfismi di campi da K in se stesso vengono detti AUTOMORFISMI. Se un automorfismo fissa, cioè lascia invariato, un sottocampo F di K, si indica con $Aut|_F K$

6.2 Spazi vettoriali

Definizione 6.8. Dato un insieme E dotato di una legge di composizione interna

$$+ : A \times A \to A$$

e di una legge di composizione esterna su K

$$\cdot : A \times A \to A$$

Si dice che E è SPAZIO VETTORIALE su un campo K se:

1. $(E, +)$ è un gruppo abeliano
2. $\forall \lambda \in K \ \forall v_1,\ v_2 \in E \ \ \lambda \cdot (v_1 + v_2) = \lambda \cdot v_1 + \lambda \cdot v_2$
3. $\forall \lambda,\ \mu \in K \ \ \forall v \in E \ \ (\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$
4. $\forall \lambda,\ \mu \in K \ \ \forall v \in E \ \ (\lambda \cdot \mu) \cdot v = \lambda \cdot (\mu \cdot v)$
5. $\exists 1_K \ \forall v \in E \ \ 1_K v = v$

Gli elementi di K sono detti SCALARI, mentre gli elementi di E sono detti VETTORI.

Definizione 6.9. Sia E uno spazio vettoriale su KŮn sistema di vettori $\{v_1, \ldots, v_p\}$ dello spazio E è detto LINEARMENTE INDIPEDENTE se $\exists$ un sistema di scalari tutti nulli $\{\alpha_1, \ldots, \alpha_p\}$ t.c.

$$\alpha_1 v_1 + \ldots + \alpha_p v_1 = 0$$

In questo caso i vettori $v_1, \ldots, v_p$ sono detti LINEARMENTE INDIPEDENTI. Se ciò non succede i vettori sono detti LINEARMENTE DIPEDENTI.

Definizione 6.10. Sia E uno spazio vettoriale su KĎiciamo che i vettori $v_1, \ldots, v_p$ dello spazio E costituiscono un sistema di generatori di E se qualsiasi vettore $v \in E$ è combinazione lineare dei vettori $v_1, \ldots, v_p$, cioè se

$$v = a_1 v_1 + \ldots + a_p v_p$$

dove $a_1, \ldots, a_p$ sono scalari.

Definizione 6.11. Si dice BASE dello spazio vettoriale E un sistema di generatori linearmente indipedenti di E.

Definizione 6.12. Sia E uno spazio vettoriale su KṠe $\{e_1, \ldots, e_n\}$ è una base dello spazio E, l'espressione

$$v = a_1 e_1 + \ldots + a_n e_n$$

è detta decomposizione del vettore $v \in E$ rispetto la base $\{e_1, \ldots, e_n\}$. Gli scalari $a_1, \ldots, a_p$ completamente determinati dal vettore v, si chiamono le componenti di v rispetto alla base $\{e_1, \ldots, e_n\}$.

Definizione 6.13. Se esiste un intero positivo n t.c. lo spazio vettoriale E ha una base composta da n vettori, questo intero è unico ed è detto la DIMENSIONE dello spazio vettoriale E.

Dato uno spazio vettoriale E su un campo K, la dimensione sarà indicata $dim_K E = [E : K]$.

Bibliografia

[1] G.M. Piacentini Cattaneo, *ALGEBRA un approccio algoritmico*, Decibel-Zanichelli (1996)

[2] J.B. Fraleigh, *A first course in Abstract Algebra*, Addison-Wesley (1967)

[3] G. Papy, *I gruppi*, Feltrinelli (1961)

[4] M. Stoka, *Lezioni di algebra lineare*, CELUP (1980)

[5] I. Stwart, *Galois Theory*, London Chapman and Hall (1973)

[6] M.A. Lavrentev, *Le Matematiche: analisi, algebra, geometria analitica*, Boringhieri (1974)