POLINOMI SIMMETRICI

Queste note unite ai primi due capitoli della II parte del libro di Lang, Algebra, dovrebbero coprire gli argomenti svolti nella prima parte del corso (fino alla settimana di pausa per gli esoneri). Più precisamente le parti del libro di Lang in questione sono: tutto il capito "algebraic extensions" tranne la parte sulle estensioni puramente inseparabili, e i paragrafi 1, 2, 4, 6 e 7 del capitolo "Galois theory" (prossimamente faremo però anche il materiale coperto dalle sezioni 3, 5 e forse anche 8, 10 e 12). Le dimostrazioni di Lang non sono sempre identiche a quelle che abbiamo dato a lezione ma l'impostazione generale è abbastanza simile.

L'obiettivo di questa parte del corso è quella di mostrare come sia effettivamente possibile calcolare il gruppo di Galois e le radici di un polinomio. Invece di esporre una teoria generale ho preferito sviluppare qualche esempio che mi sembrava potesse illustrare abbastanza bene qualcuno dei metodi e dei temi tipici. Infine i polinomi simmetrici sono un oggetto importante in matematica e che forse avrete occasione di riincontrare ancora.

Rispetto alle lezioni fatte in classe queste note dovrebbero[1] contenere poche differenze e qualche ulteriore esempio.

1. Alcuni richiami e alcune notazioni

In questa sezione A è un anello[2].

1.1. **Proprietà universale dell'anello dei polinomi.** Se $f = \sum a_n x^n$ è un polinomio a coefficienti in A nella variabile x e a un elemento di A possiamo valutare il polinomio in A ovvero possiamo considerare l'elemento $f(a) := \sum a_n a^n$. Analogamente, se f è un polinomio in n variabili e $a_1, \dots, a_n \in A$ possiamo definire $f(a_1, \dots, a_n)$. È facile verificare che l'applicazione da $A[x_1, \dots, x_n]$ in A che manda f in $f(a_1, \dots, a_n)$ è un morfismo di anelli.

Se $\varphi : A \longrightarrow B$ è un morfismo di anelli e $f = \sum a_n x^n$ è un polinomio a coefficienti in A nella variabile x possiamo considerare il polinomio $\varphi(f) := \sum \varphi(a_n) x^n$. Analogamente possiamo procedere nel caso di un polinomio con n variabili e osserviamo che l'applicazione da $A[x_1, \dots, x_n]$ in $B[x_1, \dots, x_n]$ che manda f in $\varphi(f)$ è un morfismo di anelli.

Combinando queste due costruzioni possiamo dimostrare la "proprietà universale dell'anello dei polinomi":

Proposizione 1. *Sia $\varphi : A \longrightarrow B$ un morfismo di anelli e siano $b_1, \dots, b_n \in B$. Allora esiste ed è unica una applicazione $\tilde{\varphi} : A[x_1, \dots, x_n] \longrightarrow B$ tale che $\tilde{\varphi}(a) = \varphi(a)$ per ogni $a \in A$ e $\tilde{\varphi}(x_i) = b_i$ per $i = 1, \dots, n$.*

Dimostrazione. Definiamo $\tilde{\varphi}(f) = \varphi(f)(b_1, \dots, b_n)$ e osserviamo che ha tutte le proprietà richieste. L'unicità di $\tilde{\varphi}$ è lasciata come esercizio. □

Molto spesso la mappa $\tilde{\varphi}$ della proposizione viene a sua volta indicata con φ.

1.2. **Anello generato.** Se C è un anello e $B_i \subset C$ sono dei sottoanelli di C la loro intersezione $\bigcap B_i$ è ancora un sottoanello di C.

In particolare se X è un sottoinsieme di un anello C possiamo considerare l'intersezione di tutti i sottoanelli di C che contengono X. Per ciò che abbiamo appena osservato questa intersezione è a sua volta un sottoanello di C ed è quindi il minimo sottoanello di C contenente X. Possiamo quindi dare le seguente definizione.

Definizione 1. Sia $A \subset C$ una estensione di anelli e S un sottoinsieme di C allora indichiamo con $A[S]$ il minimo anello contente A e S. $A[S]$ viene chiamato anche l'anello generato da A unione S o da S su A.

Se $S = \{s_1, \dots, s_n\}$ invece di scrivere $A[\{s_1, \dots, s_n\}]$ si usa scrivere $A[s_1, \dots, s_n]$.

Attenzione. Osserviamo che $A[s_1, \dots, s_n]$ ha un significato diverso dal considerare l'anello dei polinomi $A[x_1, \dots, x_n]$ nelle variabili $x_1, \dots, x_n$ infatti questo anello non è costruito come sottoanello di un anello dato. Tuttavia la notazione è abbastanza coerente infatti il minimo sottoanello di $A[x_1, \dots, x_n]$ contenente A e gli elementi x_i come sarà chiaro tra poco è l'anello dei polinomi stesso.

Poichè $A[S]$ è chiuso rispetto al prodotto in particolare conterrà tutti gli elementi della forma $a s_1 \cdots s_n$ con $a \in A$ e $s_1, \dots, s_n \in S$ e piché è chiuso rispetto alla somma conterrà anche gli elementi della forma

$$\sum_{j=1}^{m} a_j \, s_{j,1} \cdots s_{j,n_j}$$

con $m, n_j \in \mathbb{N}$, $a_j \in A$ e $s_{j,\ell} \in S$.[3] Se indichiamo con B il sottoinsieme degli elementi di C che si possono scrivere in questa forma avremo quindi che $A[S]$ contiene B. Viceversa è facile verificare che B è un sottoanello di C che contiene A e S e quindi contiene $A[S]$. Quindi $A[S] = B$.

[1] Quando e se saranno completate

[2] Per noi anello significherà sempre anello commutativo unitario e morfismo di anelli significherà, a meno che non sia esplicitamente menzionato il contrario, un morfismo di anelli che manda 1 in 1

[3] per queste note $\mathbb{N}$ conterrà anche 0. Inoltre (non solo per queste note) un prodotto $x_1 \cdots x_n$ con $n = 0$ si pone essere uguale a 1

Esercizio 1. Siano A un sottoanello di C siano $s_1, \dots, s_n \in C$ allora

$$A[s_1, \dots, s_n] = \big\{ f(s_1, \dots, s_n) \ : \ \text{con } f \text{ polinomio in } n \text{ variabili a coefficienti in } A \big\}.$$

Possibile svolgimento. Sia $P = A[x_1, \dots, x_n]$ l'anello dei polinomi nelle variabili $x_1, \dots, x_n$ a coefficienti in A e infine sia $s = (s_1, \dots, s_n)$. Sia φ l'applicazione che manda $f \in P$ in $f(s) \in A[s_1, \dots, s_n]$ è un morfismo e la sua immagine coincide con l'insieme che indichiamo con B a destra dell'uguale. In particolare B è un sottoanello di C che contiene A e gli elementi s_i e quindi è uguale a $A[s_1, \dots, s_n]$. □

Definizioni analoghe a quelle di questo paragrafo le abbiamo date nel caso di estensioni di campi (vedi l'esercizio 67 e la definizione che lo precede nei fogli degli esercizi).

2. Azioni di gruppi su anelli

Sia G un gruppo con unità e_G e S un anello. Una azione (di anelli) di G su S è una applicazione $\sigma : G \times S \longrightarrow S$ tale che

1) $\sigma(g, \sigma(h, a)) = \sigma(gh, a)$ per ogni $g, h \in G$ e per ogni $a \in S$;
2) $\sigma(e_G, a) = a$ per ogni $a \in S$;
3) per ogni $g \in G$ l'applicazione $a \mapsto \sigma(g, a)$ è un morfismo di anelli di S.

Molto spesso invece di scrivere $\sigma(g, a)$ si scrive $g \cdot a$ oppure $g(a)$ o anche $g\,a$. Osserviamo anche che se un gruppo G agisce su un anello A allora possiamo estendere questa azione in modo canonico all'anello dei polinomi $A[t]$ ponendo $g \cdot t = t$ per ogni $g \in G$.

2.1. **Invarianti.** Se un gruppo G agisce su un anello S indichiamo con S^G l'insieme degli elementi di S invarianti per l'azione di G, ovvero

$$S^G = \{a \in S \ : \ g \cdot a = a \text{ per ogni } g \in G\}.$$

Osserviamo che 1 è sempre fissato da G e inoltre che se $a, b \in S^G$ allora anche $a + b$ e $a\,b$ appartengono ad S^G. Inoltre se S è un campo e $a \neq 0$ anche l'inverso è fissato da G infatti $1 = g \cdot 1 = g \cdot (a\,a^{-1}) = (g \cdot a)(g \cdot a^{-1})$ e quindi $(g \cdot a^{-1}) = (g \cdot a)^{-1}$. In particolare S^G è un sottoanello di S e se S è un campo è un sottocampo.

2.2. **Traccia, norma e costruzione di alcuni elementi invarianti nel caso di un gruppo finito.** Se G è un gruppo finito alcuni elementi invarianti sono facili da costruire. Per esempio, per ogni $a \in S$, l'elemento $\sum_{g \in G} g \cdot a$ che si chiama la traccia di a e viene indicato con $\mathrm{Tr}_G(a)$ e l'elemento $\prod_{g \in G} g \cdot a$ che si chiama norma e che viene indicato con $\mathrm{N}_G(a)$ sono invarianti.

Possiamo generalizzare e unificare la costruzione degli invarianti norma e traccia considerando l'azione di G sull'anello $S[t]$ definita nel paragrafo precedente. Osserviamo innanzitutto che un polinomio è invariante per l'azione di G se e solo se i suoi coefficienti sono invarianti, ovvero $S[t]^G = S^G[t]$. Se $a \in S$ allora la norma del polinomio $t - a$,

$$\prod_{g \in G} g \cdot (t - a) = \prod_{g \in G} (t - g \cdot a)$$

è un polinomio invariante, detto polinomio caratteristico di a, che indicheremo con $c_{G,a}(t)$. Per quanto abbiamo osservato i coefficienti di questo polinomio sono elementi invarianti di S. In particolare si osservi che se $card\, G = n$ il coefficiente del termine di grado $n - 1$ è l'opposto della traccia di a e il termine noto è $(-1)^n$ per la norma di a.

2.3. **Risolventi.** È spesso utile considerare una leggera variante della costruzione precedente. Se $a \in S$ indichiamo con $G \cdot a$ o con $G(a)$ l'orbita di a ovvero l'insieme degli elementi $g \cdot a$ con $g \in G$. Poiché G agisce su $G \cdot a$ permutandone gli elementi l'elemento $\mathrm{Trrid}_G(a) := \sum_{b \in G \cdot a} b$, che chiameremo traccia ridotta, e l'elemento $\mathrm{Nrid}_G(a) := \prod_{b \in G \cdot a} b$, che chiameremo norma ridotta, sono invarianti.

Come nel caso della traccia e della norma possiamo generalizzare queste costruzioni considerando l'azione di G sull'anello dei polinomi $S[t]$. Definiamo quindi il risolvente rispetto a G di un elemento a, che indicheremo con $R_G(a)$ come la norma ridotta di $t - a$. Abbiamo quindi

$$R_G(a) = \prod_{f \in G \cdot (t-a)} f = \prod_{b \in G \cdot a} (t - b).$$

Il seguente esercizio chiarisce la differenza tra risolvente e polinomio caratteristico.

Esercizio 2. Sia $a \in S$ e sia n la cardinalità dello stabilizzatore di a. Allora $c_{G,a} = R_G(a)^n$.

Svolgimento. Sia H lo stabilizzatore di a e osserviamo che $g \cdot a = g' \cdot a$ se e solo se $g' \in gH$. Quindi per ogni $b \in G \cdot a$ esistono esattamente n elementi di G tali che $g \cdot a = b$. Spezziamo ora la produttoria che definisce il polinomio caratteristico raggruppando insieme gli elementi di G che hanno la stessa immagine se applicati ad a. In questo modo otteniamo:

$$c_{G,a} = \prod_{g \in G} (t - g \cdot a) = \prod_{b \in G \cdot a} \ \prod_{\substack{g \in G : \\ g \cdot a = b}} (t - g \cdot a) = \prod_{b \in G \cdot a} (t - b)^n = R_G(a)^n.$$

□

Nel caso in cui G sia un gruppo di Galois il risolvente non è nient'altro che il polinomio minimo, abbiamo infatti il seguente lemma.

Lemma 2. *Se $S = F$ è un campo, $E \subset F$ è una estensione finita [4] di Galois, $G = \mathrm{Gal}(F, E)$ e $a \in S$ allora $R_G(a)$ è il polinomio minimo di a su E.*

Dimostrazione. Infatti sappiamo che G agisce transitivamente sulle radici del polinomio minimo, quindi $G(a) = \{\text{radici del polinomio minimo di } a\}$. □

2.4. **Azione sul campo dei quozienti di un dominio.** Sia D un dominio e sia K il suo campo dei quozienti. Sia G un gruppo che agisce su D. L'azione di G su D si estende a tutto K ponendo

$$g \cdot \frac{a}{b} := \frac{g \cdot a}{g \cdot b}$$

per ogni $a, b \in S$ con $b \neq 0$. La definizione è ben posta infatti $g^{-1} \cdot (g \cdot b) = b \neq 0$ quindi in particolare $g \cdot b \neq 0$ e se $\frac{a}{b} = \frac{c}{d}$ ovvero se $ad = bc$ allora $(g \cdot a)(g \cdot d) = (g \cdot b)(g \cdot c)$ e quindi $\frac{g \cdot a}{g \cdot b} = \frac{g \cdot c}{g \cdot d}$. È facile verificare che questa azione di G su K ha le proprietà 1), 2), 3) elencae sopra.

Esercizio 3. Sia D un dominio e sia K il suo campo dei quozienti. Sia G un gruppo finito che agisce su D e estendiamo questa azione a K come descritto sopra. Dimostrare che K^G è il campo dei quozienti di D^G.

Svolgimento. Osserviamo che se $a, b \in D^G$ e $b \neq 0$ allora $\frac{a}{b} \in K^G$. Quindi sicuramente il campo dei quozienti di D^G è contenuto in K^G.

Sia ora $\varphi \in K^G$ e sia $\varphi = \frac{a}{b}$ con $a, b \in D$ e $b \neq 0$. Moltiplicando sopra e sotto per $c = \prod_{g \neq e_G} g \cdot b$ (che sicuramente è diverso da zero) otteniamo

$$\frac{a}{b} = \frac{a\, c}{\prod_{g \in G} g \cdot b}.$$

In particolare l'elemento al denominatore è invariante per G. Quindi $\varphi = \frac{d}{N}$ con $d \in D$ e $N \in D^G$. In particolare $d = \varphi N$ e, poichè N e φ sono invarianti, ne ricaviamo che anche d è invariante. Quindi abbiamo scritto φ come quoziente di due elementi di D^G. □

3. L'azione di permutazione sui polinomi in n variabili

Sia ora A un anello e $S = A[x_1, \dots, x_n]$ l'anello dei polinomi in n variabili a coefficienti in A. Su S è definita una azione naturale del gruppo di permutatione S_n data nel seguente modo:

$$\sigma \cdot a = a \quad \text{per ogni } a \in A \qquad \text{e} \qquad \sigma(x_i) = x_{\sigma(i)} \quad \text{per } i = 1, \dots, n.$$

Gli elementi di S invarianti per questa azione si dicono polinomi simmetrici. Introduciamo ora alcuni particolari polinomi simmetrici.

3.1. **Polinomi simmetrici elementari.** Per $h = 1, \dots, n$ definiamo l'h-simo polinomio simmetrico elementare e_h come la traccia ridotta di $x_1 x_2 \cdots x_h$, abbiamo quindi

$$e_h(x) = \sum_{1 \leqslant i_1 < i_2 < \cdots < i_h \leqslant n} x_{i_1} x_{i_2} \cdots x_{i_h}.$$

In particolare abbiamo $e_1 = x_1 + \cdots + x_n$ e $e_n = x_1 \cdots x_n$.

La seguente relazione sarà per noi fondamentale e renderà i polinomi simmetrici elementari uno dei principali oggetti del corso:

$$(t - x_1) \cdots (t - x_n) = t^n - e_1\, t^{n-1} + e_2\, t^{n-2} \cdots + (-1)^n e_n. \tag{RF}$$

3.2. **Polinomi di Newton.** Per $h \in \mathbb{N}$ l'h-esimo polinomio di Newton nelle variabili è definito come la traccia ridotta di x^h, abbiamo quindi

$$p_h(x) = x_1^h + \cdots + x_n^h.$$

In particolare $p_0 = n$ e $p_1 = e_1$. I polinomi di Newton non saranno durante questo corso al centro della nostra attenzione ma costituiranno più che altro un modo per creare esercizi e saltuariamente uno strumento ausiliario, in particolare i due esercizi e le osservazioni che seguono si possono sicuramente saltare ad una prima lettura.

A lezione abbiamo dimostrato la seguente relazione tra polinmi simmetrici e polinomi di Newton.

Esercizio 4. Sia $A = \Bbbk$ un campo di caratteristica 0. Dimostrare che

$$1 - e_1\, t + e_2\, t^2 \cdots \pm e_n t^n = \prod_{i=1}^{n} (1 - t x_i) = e^{-\sum_{h \geqslant 1} \frac{p_h}{h} t^h}$$

[4] in realtà in questo caso questa ipotesi non è necessaria

Svolgimento. La prima uguaglianza si ricava dalla relazione fondamentale (RF) sostituendo t con t^{-1} e moltiplicando per t^n. Per dimostrare la seconda uguaglianza sviluppiamo il termine sulla destra:

$$e^{-\sum_{h\geqslant 1}\frac{p_h}{h}t^h} = e^{-\sum_{h\geqslant 1}(\frac{x_1^h}{h}+\cdots+\frac{x_n^h}{h})t^h} = e^{-\sum_{h\geqslant 1}\frac{x_1^h}{h}t^h\cdots-\sum_{h\geqslant 1}\frac{x_n^h}{h}t^h} = e^{-\sum_{h\geqslant 1}\frac{x_1^h t^h}{h}}\cdots e^{-\sum_{h\geqslant 1}\frac{x_n^h t^h}{h}}$$

Ora osserviamo che $-\sum_{h\geqslant 1}\frac{y^h t^h}{h}t^h = \log(1-ty)$ e quindi il prodotto sulla destra è uguale a $(1-tx_1)\cdots(1-tx_n)$. □

L'esercizio in particolare mostra che i polinomi simmetrici elementari si possono esprimere per mezzo dei polinomi di Newton. Una applicazione di questo fatto è il seguente esercizio (l'esercizio 52) che in classe non abbiamo mai corretto.

Esercizio 5. Sia A una matrice $n\times n$ a coefficienti razionali (va bene qualsiasi campo di caratteristica 0) e supponiamo che $\operatorname{Tr}(\mathsf{A}) = \operatorname{Tr}(\mathsf{A}^2) = \cdots = \operatorname{Tr}(\mathsf{A}^n) = 0$. Allora $\mathsf{A}^n = 0$.

Svolgimento. Sia f il polinomio caratteristico di A e siano $\lambda_1,\dots,\lambda_n$ le radici di f contate con la loro molteplicità e $\lambda = (\lambda_1,\dots,\lambda_n)$. Osserviamo intanto che $\operatorname{Tr}\mathsf{A}^i = p_i(\lambda)$. Infatti possiamo scegliere una base in $\mathbb{C}^n$ che triangolarizza la matrice (per esempio la mettiamo in forma di Jordan) allora è chiaro che gli autovalori di A sono gli elementi sulla diagonale e che gli autovalori di A^i sono $\lambda_1^i,\dots,\lambda_n^i$ da cui $\operatorname{Tr}(\mathsf{A}^i) = p_i(\lambda)$. [5]

Quindi le nostre ipotesi implicano che $p_1(\lambda) = \cdots = p_n(\lambda) = 0$. La relazione dimostrata nell'esercizio precedente ci dice allora che $1 - e_1(\lambda)\,t + \cdots \pm e_n(\lambda)t^n = e^{t^{n+1}h(t)}$ con h una serie nelle t. Ma sviluppando il termine sulla destra compaiono potenze di t solo di grado maggiore di n quindi $e_i = 0$ per $i = 1,\dots,n$ da cui $f = t^n$ e $\mathsf{A}^n = 0$ perché il polinomio caratteristico annulla la matrice. □

Volendo possiamo rendere più esplicita la relazione tra le e_i e le p_i che abbiamo trovato nell'esercizio 4. Non è che questa cosa ci interessi più di tanto e la potete sicuramente saltare in una prima lettura ma può essere un buon esercizio per impratichirsi con alcune notazioni tipo $\alpha!$ con α una successione di interi. Sviluppando infatti il termine sulla destra otteniamo

$$\sum_{k=0}^{\infty}\frac{(-\sum_{h\geqslant 1}\frac{p_h}{h}t^h)^k}{k!} = \sum_{k=0}^{\infty}\frac{(-1)^k}{k!}\Big(\sum_{\alpha\,:\,[\alpha]=k}\frac{[\alpha]!}{\alpha!}\frac{p^\alpha t^{\{\alpha\}}}{ex(\alpha)}\Big) = \sum_{h=0}^{\infty}\Big(\sum_{\alpha\,:\,\{\alpha\}=h}\frac{(-1)^{[\alpha]}p^\alpha}{\alpha!\,ex(\alpha)}\Big)t^h.$$

dove $\alpha = (\alpha_1,\alpha_2,\dots)$ è una succesione di interi definitivamente nulla, $[\alpha] = \sum\alpha_i$, $\{\alpha\} = \sum i\,\alpha_i$, $p^\alpha = p_1^{\alpha_1}p_2^{\alpha_2}\cdots$, $ex(\alpha) = 1^{\alpha_1}2^{\alpha_2}\cdots$ e $\alpha! = \alpha_1!\alpha_2!\cdots$. Per $h = 1,\dots,n$ abbiamo quindi

$$e_h = (-1)^h\sum_{\alpha\,:\,\{\alpha\}=h}\frac{(-1)^{[\alpha]}p^\alpha}{\alpha!\,ex(\alpha)}.$$

3.3. **Il discriminante.** Il discriminante è il seguente particolare polinomio

$$\Delta(x) = \prod_{i>j}(x_i - x_j)^2.$$

Definiamo anche il polinomio δ come

$$\delta(x) = \prod_{i>j}(x_i - x_j).$$

Lemma 3. *Per ogni $\sigma\in\mathsf{S}_n$ abbiamo $\sigma\cdot\delta = \varepsilon(\sigma)\delta$ dove $\varepsilon(\sigma)$ è il segno della permutazione σ. In particolare δ è invariante per il sottogruppo delle permutazioni pari A_n e Δ è un polinomio simmetrico.*

Dimostrazione. Basta dimostrare questa relazione per σ uguale ad una trasposizione della forma $(h,h+1)$. In questo caso i fattori $(x_i - x_j)$ per $i,j\notin\{h,h+1\}$, i fattori $(x_i - x_h)(x_i - x_{h+1})$ per $i > h+1$ e i fattori $(x_h - x_j)(x_{h+1} - x_j)$ per $j < h$ rimangono invariati. Rimane fuori da questa lista solo il fattore $(x_{h+1} - x_h)$ che cambia segno. □

[5] La forma di Jordan qui non è strettamente necessaria. Diamo un cenno di una dimostrazione alternativa che usa un ragionamento che si può utilizzare in molte situazioni. Per quello che abbiamo detto la relazione è vera per matrici diagonalizzabili. Consideriamo le due funzioni $\varphi : A\mapsto\operatorname{Tr}(A^i)$ e $\psi : A\mapsto p_i(\lambda)$ definite sullo spazio vettoriale delle matrici. Poiché le p_i si possono esprimere per mezzo delle e_i (questo lo vedremo nella prossima sezione) queste sono entrambe funzioni polinomiali nelle A (se questo non vi è troppo chiaro cosa significhi per i nostri scopi basta osservare che sono funzioni continue). Inoltre φ e ψ coincidono sull'insieme delle matrici diagonalizzabili. Quindi basta verificare che questo è un insieme denso nell'insieme delle matrici. Sia A una matrice non diagonalizzabile e B una matrice con tutti autovalori distinti. Consideriamo il discriminante di $f(t) = \det(t\mathsf{I} - tB - (1-t)A)$ questa è una funzione polinomiale nella variabile t e non identicamente nulla perché per $t = 1$ è il discriminante del polinomio caratteristico di B che ha tutti autovalori distinti. Quindi $tB + (1-t)A$ ha tutti gli autovalori distinti per tutti i t tranne un numero finito di valori quindi A può essere approssimata a piacere con matrici diagonalizzabili.

3.4. **Risolventi di polinomi sotto l'azione del gruppo di permutazione.** Sia $P \in S$ un polinomio nelle variabili $x_1, \dots, x_n$. Se applichiamo la definizione data nella sezione precedente nel caso di un sottogruppo G di S_n e di $a = P$ otteniamo un polinomio nella variabile t a coefficienti in S^G che sarà indicato con $R_G(P, x)$ (invece che con $R_G(P)$ come nel caso generale) per evidenziare il ruolo della variabile x.

Particolarmente interessante per noi sarà il caso di $G = \mathsf{S}_n$. In questo caso indichiamo il risolvente di P rispetto a S_n semplicemente con $R(P, x)$ e ricordiamo in questo caso la definizione:

$$R(P, x)(t) = \prod_{Q \in \mathsf{S}_n(P)} (t - Q(x)).$$

Evidenziamo ancora una volta che $R(P, x)$ è un polinomio nella variabile t a coefficienti nei polinomi simmetrici.

4. Il teorema fondamentale per i polinomi simmetrici

In questa sezione manteniamo le notazioni della sezione precedente. Per tutta la sezione inoltre $\alpha = (\alpha_1, \dots, \alpha_n)$, $\beta = (\beta_1, \dots, \beta_n)$, $\gamma = (\gamma_1, \dots, \gamma_n)$ saranno n-uple di numeri naturali.

Possiamo dare un ordine totale (detto ordine lessicografico) alle n-uple di naturali nel seguente modo: poniamo $\alpha > \beta$ se esiste $i \in \{1, \dots, n\}$ tale che $\alpha_j = \beta_j$ per $j < i$ e $\alpha_i > \beta_i$.

Possiamo utilizzare questo ordine per costruire un ordine sui monomi (e su zero). Per comodità poniamo $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. Allora diciamo che $a\,x^\alpha > b\,x^\beta$ se $\alpha > \beta$ e $a, b \neq 0$. Poniamo inoltre per comodità $a\,x^\alpha > 0$ per ogni $a \neq 0$.

Osserviamo che ogni polinomio $F \in S$ si scrive nella forma $\sum_\alpha a_\alpha\, x^\alpha$ con gli $a_\alpha \in A$ e tutti nulli tranne in un numero finito. Se $F \neq 0$ poniamo allora $\mathcal{L}(F) = a_\alpha x^\alpha$ se $a_\alpha\, x^\alpha$ è il monomio più grande tra quelli che compaiono nella espressione di F. Poniamo inoltre $\mathcal{L}(0) = 0$. Abbiamo così definito una funzione $\mathcal{L} : S \longrightarrow S$. Se $\mathcal{L}(F) = a\,x^\alpha$ definiamo inoltre $\mathcal{M}(F) = a$, $\mathcal{N}(F) = \alpha$ se $a \neq 0$ e $\mathcal{N}(0) = -1$ e considero questo elemento un elemento minore di tutte le n-uple di numeri naturali.

$\mathcal{L}$ non è un morfismo di anelli (infatti non conserva la somma) ma ha alcune proprietà la cui verifica lasciamo al lettore (che saresti te che stai leggendo e che ti serve per capire cosa è questa funzione $\mathcal{L}$ e perché poi queste cose te le chiedo all'esame!):

1) se $\mathcal{M}(F) = 1$ allora $\mathcal{L}(F\,G) = \mathcal{L}(F)\mathcal{L}(G)$ per ogni $G \in S$;
2) se $\mathcal{L}(F) = \mathcal{L}(G) \neq 0$ allora $\mathcal{L}(F - G) < \mathcal{L}(F)$;
3) se $\mathcal{L}(F) > \mathcal{L}(G)$ allora $\mathcal{L}(F + G) = \mathcal{L}(F)$;
4) $\mathcal{L}(e_i) = x_1 \cdots x_i$.

Utilizzeremo queste proprietà per dimostrare il teorema fondamentale dei polinomi simmetrici. Introduciamo anche la notazione $e^\alpha = e_1^{\alpha_1} \cdots e_n^{\alpha_n}$.

Ricordiamo che una A-base di S è un sottoinsieme $\mathcal{B}$ di S tale che ogni elemento di S si può scrivere in modo unico come combinazione lineare a coefficienti in A di un numero finito di elementi di B. (La definzione è la stessa che avete dato per A un campo ma nel caso di un anello qualsiasi non è detto che esista sempre una A-base).

Lemma 4. *Se $F \neq 0$ è un polinomio simmetrico allora e $\mathcal{L}(F) = a\,x^\beta$ allora $\beta_1 \geqslant \beta_2 \cdots \geqslant \beta_n$.*

Dimostrazione. Sia $F = \sum a_\alpha x^\alpha$. Poiché F è simmetrico abbiamo che $a_\alpha = a_{\alpha'}$ per ogni riordinamento α' di α.

Osserviamo inoltre che se prendiamo una n-upla di interi γ e la riordiniamo in ordine decrescente ottenendo così una n-upla γ' avremo sicuramente $\gamma' \geqslant \gamma$ (come mai? il lettore, lo stesso di prima, farebbe bene a verificarlo).

Sia ora $c_\beta x^\beta = \mathcal{L}(F)$ e β' è un riordinamento decrescente di β allora, essendo F simmetrico, $c_{\beta'} = c_\beta \neq 0$ e quindi $c_{\beta'} x^{\beta'} \geqslant c_\beta x^\beta$ e per massimalità di β otteniamo $\beta = \beta'$. □

Teorema 5. *L'insieme dei polinomi e^α con α n-upla di naturali è una A-base dell'anello S^{S_n} dei polinomi simmetrici. In particolare $S^{\mathsf{S}_n} = A[e_1, \dots, e_n]$.*

Dimostrazione. Dalle proprietà 1) e 4) ricaviamo che

$$\mathcal{L}(e^\alpha) = x^\beta \quad \text{con } \beta_1 = \alpha_1 + \cdots + \alpha_n,\ \dots,\ \beta_{n-1} = \alpha_{n-1} + \alpha_n,\ \beta_n = \alpha_n.$$

Indichiamo β con $\ell(\alpha)$. Osserviamo che $\beta_1 \geqslant \beta_2 \cdots \geqslant \beta_n$. Viceversa se β è una n-upla di naturali con questa proprietà e poniamo $\alpha_i = \beta_i - \beta_{i+1}$ per $i < n$ e $\alpha_n = \beta_n$ abbiamo $\ell(\alpha) = \beta$. In particolare ℓ è una bigezione tra l'insieme di tutte le n-uple di numeri naturali e l'insieme delle n-uple di numeri naturali decrescenti.

Gli e^α sono linearmente indipendenti. Sia $F = \sum c_\alpha e^\alpha = 0$. Osserviamo che per la proprietà 3) $\mathcal{L}(F) = max\{\mathcal{L}(c_\alpha e^\alpha)\}$. Quindi, essendo $F = 0$, dobbiamo avere $\mathcal{L}(c_\alpha e^\alpha) = 0$ per ogni α ovvero $c_\alpha = 0$ per ogni α.

Gli e^α generano i polinomi simmetrici. Procediamo per induzione su $\mathcal{N}(F)$. Se $\mathcal{N}(F) = -1$ allora $F = 0$ e non c'è nulla da dimostrare. Sia ora $F \neq 0$ e sia $\mathcal{L}(F) = ax^\beta$. Allora per il lemma abbiamo che $\beta_1 \geqslant \ldots \geqslant \beta_n$ e quindi per quanto osservato all'inizio di questa dimostrazione esiste α tale che $\mathcal{L}(e^\alpha) = x^\beta$. Quindi per la propietà 2) se poniamo $H = F - ae^\alpha$ abbiamo $\mathcal{L}(H) < \mathcal{L}(F)$. Quindi $\mathcal{N}(H) < \mathcal{N}(F)$ e per ipotesi induttiva H si può scrivere come combinazione lineare a coefficienti in A degli e^α. Infine $F = H + a\,e^\alpha$. □

Corollario 6. *L'anello dei polinomi simmetrici è isomorfo ad un anello di polinomi in n variabili a coefficienti in A.*

Dimostrazione. Sia $T = A[y_1, \cdots, y_n]$ l'anello dei polinomi nelle variabili y_i e sia $\varphi : T \longrightarrow S^{\mathsf{S}_n}$ definito dal $\varphi(a) = a$ per ogni $a \in A$ e da $\varphi(y_i) = e_i$. Per il teorema φ è un isomorfismo. □

Corollario 7. *Sia $A = \Bbbk$ un campo e sia $K = \Bbbk(x_1, \ldots, x_n)$ il campo delle funzioni razionali in n variabili con la stessa azione di S_n che abbiamo definito su S. Allora K^{S_n} è il campo dei quozienti di S^{S_n} e quindi è uguale a $\Bbbk(e_1, \ldots, e_n)$.*

Dimostrazione. K è il campo dei quozienti di S e il corollario segue dal teorema precedente e dall'esercizio 3. □

4.1. **Polinomi semisimmetrici.** Nella rimanente parte di questa sezione assumiamo che $A = \Bbbk$ sia un campo di caratteristica diversa da due e risolviamo gli esercizi 48 e 49. Diciamo che un polinomio $F \in S$ è semisimmetrico se è invariante per il gruppo delle trasformazioni pari. Ovviamente ogni polinomio simmetrico è semisimmetrico e abbiamo già osservato nel lemma 2 che δ è un polinomio semisimmetrico. Il lemma seguente è un inverso di quel risultato.

Lemma 8. *Sia $F \in S$ tale che $\sigma F = \varepsilon(\sigma)F$ per ogni $\sigma \in \mathsf{S}_n$. Allora δ divide F.*

Dimostrazione. Basta dimostrare che $x_i - x_j$ divide F per $i \neq j$. Per semplicità di scrittura facciamo il caso $i = 2$ e $j = 1$. Sia $T = \Bbbk[x_2 \ldots, x_n]$ e consideriamo F come un polinomio $\tilde{F}(x_1)$ a coefficienti in T nella variabile x_1. Per il criterio di Ruffini basta dimostrare che $\tilde{F}(x_2) = 0$ ovvero che $F(x_2, x_2, x_3, \ldots, x_n) = 0$. Ma per ipotesi $F(x_1, x_2, x_3, \ldots, x_n) = -F(x_2, x_1, x_3, \ldots, x_n)$ quindi $F(x_2, x_2, x_3, \ldots, x_n) = -F(x_2, x_2, x_3, \ldots, x_n)$ ovvero $2\,F(x_2, x_2, x_3, \ldots, x_n) = 0$. Infine essendo la caratteristica diversa da 2 ricaviamo $\tilde{F}(x_2) = 0$. □

Proposizione 9. *Ogni polinomio semisimmetrico si scrive in modo unico nella forma $F + G\delta$ con F, G simmetrici. In particolare $S^{\mathsf{A}_n} = \Bbbk[e_1, \ldots, e_n, \delta]$.*

Dimostrazione. Unicità. Sia $F + G\delta = 0$. Se applichiamo $\tau = (12)$ otteniamo $F - G\delta = 0$ da cui sommando e dividendo per 2 otteniamo $F = 0$ e di conseguenza $G = 0$. Se ora $F+G\delta = F'+G'\delta$ otteniamo $(F-F')+(G-G')\delta = 0$ da cui $F = F'$ e $G = G'$.

Esistenza. Sia H un polinomio semisimmetrico, sia $\tau = (12)$ e definiamo

$$F = \frac{H + \tau H}{2} \quad \text{e} \quad H' = \frac{H - \tau H}{2}.$$

$H = F + H'$ e osserviamo che l'invarianza di H per A_n implica quella di F e H'. Infatti se $\sigma \in \mathsf{A}_n$ allora $\sigma(\tau H) = \tau(\tau^{-1}\sigma\tau)H = \tau H$ poiché $\tau^{-1}\sigma\tau \in \mathsf{A}_n$. Inoltre $\tau F = F$ e $\tau H' = -H'$. Quindi poiché ogni elemento non pari di S_n si può scrivere nella forma $\tau\rho$ con $\rho \in \mathsf{A}_n$ otteniamo che $\sigma F = F$ e che $\sigma H' = \varepsilon(\sigma)H'$ per ogni permutazione σ. Quindi per il lemma $H' = G'\delta$ e $(\sigma G)\,\delta = G\delta$ per ogni σ da cui $\sigma G = G$ per ogni σ poiché S è un dominio. □

Esercizio 6. La proposizione precedente rimane vera se al posto di un campo $\Bbbk$ si mette $\mathbb{Z}$?

5. Applicazione al calcolo del gruppo di Galois del polinomio generico

Nella discussione della sezione precedente supponiamo che $A = \Bbbk$ sia un campo. Poniamo inoltre $K = \Bbbk(x_1, \ldots, x_n)$ il campo dei quozienti di S e $L = K^{\mathsf{S}_n}$ il sottocampo fissato da S_n e in particolare $\mathrm{Gal}(K : L) = \mathsf{S}_n$. Osserviamo inoltre che il polinomio $f = t^n - e_1 t^{n-1} + \cdots \pm e_n$ è un polinomio a coefficienti in L e che K è il campo di spezzamento di f su L.

Applichiamo questa discussione al calcolo del gruppo di Galois del polinomio generico. Il polinomio generico di grado n su $\Bbbk$ non è un polinomio a coefficienti in $\Bbbk$ ma è il polinomio i cui coefficienti sono delle variabili:

$$g = t^n - y_1 t^{n-1} + \cdots \pm y_n$$

con y_i delle variabili. In particolare se fossimo capaci di risolvere il polinomio generico su $\Bbbk$ saremmo capaci di risolvere qualsiasi polinomio a coefficienti in $\Bbbk$.

Sia quindi $T = \Bbbk[y_1, \ldots, y_n]$, $E = \Bbbk(y_1, \ldots, y_n)$ il suo campo dei quozienti e F il campo di spezzamento di f su K. Vogliamo calcolare $G = \mathrm{Gal}(F; E)$.

Come abbiamo già osservato nel corollario 6 il teorema fondamentale sui polinomi simmetrici implica che il morfismo di anelli da T in S^{S_n} definito da $\varphi(a) = a$ per $a \in \Bbbk$ e $\varphi(y_i) = e_i$ è un isomorfismo e quindi induce un isomorfismo, che continueremo ad indicare con φ tra il campo dei quozienti E di T e il campo dei quozienti di S^{S_n}. Ma per il corollario 7 il campo dei quozienti di S^{S_n} è uguale a $L = K^{\mathsf{S}_n}$. In questo isomorfismo abbiamo inoltre che $\varphi(g) = f$, quindi tramite φ, K è un campo di spezzamento di g su E. In particolare abbiamo dimostrato la seguente proposizione.

Proposizione 10. *Il gruppo di Galois del polinomio generico di grado n è isomorfo a S_n.*

6. Calcolo di alcuni polinomi simmetrici e di alcuni risolventi

Sia $A = \Bbbk$ un campo, $f = t^n - a_1\, t^{n-1} + \cdots \pm a_n$ un polinomio a coefficienti in $\Bbbk$ e $F \in S$ un polinomio in n variabili. Siano inoltre $\lambda_1, \dots, \lambda_n$ le radici di f contate con le loro molteplicità e $\lambda = (\lambda_1, \dots, \lambda_n)$. Osserviamo che se $F(x)$ è un polinomio simmetrico $F(\lambda)$ è un elemento di $\Bbbk$ che possiamo calcolare. Infatti possiamo esprimere $F(x)$ come un polinomio $\tilde{F}(e_1(x), \dots, e_n(x))$ nelle funzioni simmetriche elementari e abbiamo quindi

$$F(\lambda) = \tilde{F}(e_1(\lambda), \dots, e_n(\lambda)) = \tilde{F}(a_1, \dots, a_n).$$

Spesso utilizzeremo la seguente convenzione: se F è un polinomio simmetrico e f è come sopra definiamo $F(f)$ come $F(\lambda)$. In particolare definiamo in questo modo il discriminante $\Delta(f)$ di un polinomio, e se $P \in S$ è qualsiasi, il risolvente $R(P, f)$ di f rispetto a f. Facciamo un esempio equivalente all'esercizio 37.

Esercizio 7. Sia $f = t^3 - 2\, t^2 + t + 4$ e $P = x_1^2$. Calcolare il risolvente $R(P, f)$.

Svolgimento. Esprimiamo intanto il risolvente $R(P, x)$ per mezzo delle funzioni simmetriche elememtari. L'orbita di x_1^2 rispetto al gruppo delle permutazioni è l'insieme $\{x_1^2, x_2^2, x_3^2\}$. Quindi

$$R(P, x) = (t - x_1^2)(t - x_2^2)(t - x_3^2) = t^3 - (x_1^2 + x_2^2 + x_3^2)t^2 + (x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2)t - x_1^2x_2^2x_3^2$$

I coefficienti di $R(P, x)$ sono polinomi simmetrici nelle x e quindi si possono esprimere nelle funzioni simmetriche elementari. Infatti abbiamo $x_1^2 + x_2^2 + x_3^2 = e_1^2 - 2e_2$, $x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2 = e_2^2 - 2\, e_1e_3$ e $x_1^2x_2^2x_3^2 = e_3^2$. Quindi

$$R(P, f) = t^3 - (2^2 - 2 \cdot 1)t^2 + (1^2 - 2 \cdot 2 \cdot (-4))t - (-4)^2 = t^3 - 2\, t^2 + 17\, t - 16.$$

□

In linea di principio la dimostrazione del teorema 5 che abbiamo dato fornisce un algoritmo per esprimere un polinomio simmetrico come polinomio nelle funzioni simmetriche elementari e_i. Tuttavia questo algoritmo è molto inefficiente e spesso è impraticabile e è molto più utile soprattutto se si volgiono dare anche delle applicazioni teoriche procedere con qualche trucco.

6.1. Discriminante.

In questa sezione risolviamo gli esercizi 41 e 134 in cui si chiede di calcolare alcuni discriminanti. Il primo esercizio è solo un caso particolare del secondo. Mi sembra comunque utile illustrarlo apparte per mettere in evidenza il metodo che vogliamo seguire.

Esercizio 8. Sia $f = x^3 + px + q$. Esprimere $\Delta(f)$ in funzione di p e q.

Svolgimento. $\Delta(x)$ è un polinomio omogeneo nelle x di grado 6. Inoltre sappiamo che possiamo esprimere Δ in un unico modo come polinomio nelle e_i. Poiché il grado nelle x è 6 avremo che Δ è una combinazione lineare di e_1^6, $e_1^4e_2$, $e_1^3e_3$, $e_1^2e_2^2$, $e_1e_2e_3$, e_2^3 e e_3^2. Quando andiamo a calcolare $\Delta(f)$ nel nostro caso abbiamo $e_1 = 0$, $e_2 = p$ e $e_3 = -q$. Quindi $\Delta(f) = \lambda p^3 + \mu q^2$.

Per calcolare λ e μ scegliamo dei particolari polinomi.

Se prendiamo $f = x^3 - x$ (ovvero $p = -1$ e $q = 0$) allora le radici sono $1, 0, -1$ e quindi $\Delta = 4$. In particolare otteniamo $\lambda = -4$.

Se prendiamo $f = x^3 - 1$ (ovvero $p = 0$ e $q = -1$) allora le radici sono $1, \omega, \omega^2$ con ω radici primitiva terza di 1. Quindi $\Delta = ((1 - \omega)(1 - \omega^2))^2(\omega - \omega^2)^2 = 9(-3) = -27$. In particolare otteniamo $\mu = -27$.

Quindi $\Delta(f) = -4\, p^3 - 27\, q^2$. □

Esercizio 9. Si calcoli il discriminante del polinomio $x^n + ax + b$.

Svolgimento. Ragionando come prima osserviamo che Δ si potrà esprimere come polinomio in a e b della forma $\Delta = \lambda a^n + \mu b^{n-1}$.

Se poniamo $a = 0$ e $b = -1$ otteniamo $f = x^n - 1$ e le radici di f sono gli elementi ζ_n^i con $i = 0, \dots, n-1$ e ζ_n radice primitiva n-sima di 1. Quindi

$$\Delta = \prod_{n-1 \geqslant i > j \geqslant 0} (\zeta_n^i - \zeta_n^j)^2 = (-1)^{\binom{n}{2}} \prod_{i,j \in \mathbb{Z}/n \text{ e } i \neq j} (\zeta_n^i - \zeta_n^j) = (-1)^{\binom{n}{2}} \prod_{i \in \mathbb{Z}/n} \prod_{j \in \mathbb{Z}/n \smallsetminus \{i\}} \zeta_n^i (1 - \zeta_n^{j-i})$$

Sia h il polinomio $x^{n-1} + \cdots + 1 = \frac{x^n - 1}{x - 1} = \prod_{i \in \mathbb{Z}/n \smallsetminus \{0\}} (x - \zeta_n^i)$. Nell'ultima produttoria $j - i$ varia tra tutti gli elementi di $\mathbb{Z}/n$ diversi da zero quindi abbiamo

$$\Delta = (-1)^{\binom{n}{2}} \prod_{i \in \mathbb{Z}/n} \zeta_n^{i(n-1)} h(1) = (-1)^{\binom{n}{2}} \zeta_n^{-\frac{n(n-1)}{2}} n^n.$$

Ora $\zeta_n^{-\frac{n(n-1)}{2}} = (-1)^{n-1}$ infatti sia ω una radice primitiva $2n$-sima[6] con $\omega^2 = \zeta_n$ allora $\zeta_n^{-\frac{n(n-1)}{2}} = \omega^{-n(n-1)} = (-1)^{n-1}$. Quindi $\Delta = (-1)^{\binom{n}{2} + n - 1} n^n$ da cui $\mu = (-1)^{\binom{n}{2}} n^n$.

[6] questa dimostrazione di questo fatto mi è stata suggerita da Valerio Capraro

Poniamo ora $a = -1$ e $b = n-1$. Allora $f = xg(x)$ con $g = x^{n-1} - 1$. Quindi le radici di f sono 0 e le radici di g che chiamiamo α_i.Quindi

$$\Delta(f) = \prod_i (0 - \alpha_i)^2 \cdot \prod_{i>j} (\alpha_i - \alpha_j)^2 = g(0)^2 \Delta(g) = \Delta(g).$$

Ma g è un polinomio come quello che abbiamo analizzato nel precedente caso con $n-1$ al posto di n, quindi $\Delta(f) = \Delta(g) = (-1)^{\binom{n-1}{2}+n}(n-1)^{n-1}$ e $\lambda = (-1)^{\binom{n-1}{2}}(n-1)^{n-1}$.

Quindi $\Delta = (-1)^{\binom{n-1}{2}}(n-1)^{n-1}a^n + (-1)^{\binom{n}{2}} n^n b^{n-1}$. □

6.2. **Qualche risolvente.** In modo simile a quanto fatto per i discriminanti negli esercizi precedenti è possibile calcolare alcuni risultanti limitando i conti necessari. Negli esercizi seguenti sono elencati qualcuno di questi risolventi alcuni dei quali avremo occasione di utilizzare a lezione (non è neessario farseli tutti basta avere capito e essere in grado di farne uno).

Esercizio 10. Sia $f = t^3 + pt + q$ e $P = x_1 + x_2$, allora $R(P, f) = t^3 + pt - q$.

Esercizio 11. Sia $f = t^4 + pt + q$ e $P = (x_1 + x_3)(x_2 + x_4)$, allora $R(P, f) = t^3 - 4qt + p^2$.

Un ulteriore modo per calcolare risolventi e discriminanti è legato ai risultanti di cui trovate un cenno tra gli appunti degli esercizi dati in classe che trovate in rete. Per il corso non avremo mai bisogno di ricorrere a questi altri risultati, tranne per creare qualche esercizio.

6.3. **Risolventi per sottogruppi.** Può essere utile a volte calcolare un risolvente non rispetto a tutto il gruppo simmetrico ma solo rispetto ad un suo sottogruppo. Se $P \in S$ e $G \subset \mathsf{S}_n$ nel paragrafo 3.4 abbiamo definito $R_G(P, x)$.

Procediamo come abbiamo fatto all'inizio di questa sezione e definiamo $R_G(P, f)$ sostituendo in $R_G(P, f)$ alle x le radici di f. La notazione qui è leggermente fuorviante, infatti mentre nel caso di $G = \mathsf{S}_n$ il risolvente $R_G(P, f)$ dipende solo da f nel caso generale dipende anche dall'ordinamento $(\lambda_1, \dots, \lambda_n)$ che abbiamo dato alle radici: (per rendersi conto di questo basta pensare all'esempio $G = \{id\}$ e $F = x_1$). Inoltre per calcolare $R_G(P, f)$ non possiamo procedere come abbiamo fatto nel caso di S_n riesprimendo tutto per mezzo delle funzioni simmetriche elementari e quindi sostituendo i coefficienti del polinomio f. Possiamo però di calcolarci un sistema di generatori dell'anelli S^G, esprimere $R_G(P, x)$ per mezzo di questo sistema di generatori e quindi valutare questi generatori.

Nel caso di $G = \mathsf{A}_n$, per esempio per quanto abbiamo dimostrato nel paragrafo 4.1, sappiamo che ogni polinomio semisimmetrico si esprime per mezzo delle funzioni simmetriche elementari e di δ.

Esercizio 12. Sia $f = t^3 + 2t + 1$ e sia $P = x_1 - x_2$ allora $R_{\mathsf{A}_3}(P, f) = t^3 + 4t + \sqrt{-59}$.

Dimostrazione. Osserviamo che $\mathsf{A}_3(P) = \{x_1 - x_2, x_2 - x_3, x_3 - x_1\}$ quindi

$$R_{\mathsf{A}_3}(P, x) = (t - x_1 + x_2)(t - x_2 + x_3)(t - x_3 + x_1) = t^3 - (x_1^2 + x_2^2 + x_3^2)t + \delta(x) = t^3 - (e_1^2(x) - 2\,e_2(x))t + \delta(x).$$

Inoltre, grazie all'esercizio 8 abbiamo $\Delta(f) = -4(2)^3 - 27 = -59$. Quindi $\delta(f) = \sqrt{-59}$ e $R_{\mathsf{A}_3}(P, f) = t^3 + 4t + 9$ □

Nota bene: le radici quadrate di -59 sono due: r e $-r$, la radice che appare nella espressione del risolvente nell'esercizio sopra dipende dall'ordinamento che abbiamo dato alle radici di f. Per esempio per se con l'ordinamento $(\lambda_1, \lambda_2, \lambda_3)$ otteniamo r con l'ordinamento $(\lambda_2, \lambda_1, \lambda_3)$ otteniamo $-r$.

7. Risolventi e calcolo del gruppo di Galois

Siano f, n, $A = \Bbbk$, λ, S e K come nelle sezioni precedenti. Supponiamo inoltre che f sia separabile e irriducibile e sia F il campo di spezzamento di F su $\Bbbk$ e Gal il gruppo di Galois di F su $\Bbbk$. Il gruppo di Galois permuta le radici e quindi una volta fissato l'ordinamento delle radici possiamo associare ad ogni elemento $\sigma \in \mathrm{Gal}$ la permutazione, che indicheremo a sua volta con σ, tale che $\sigma(\lambda_i) = \lambda_{\sigma(i)}$. In questo modo identifichiamo Gal con un sottogruppo di S_n.

In generale sappiamo che Gal non è uguale a tutto il gruppo delle permutazioni. Possono infatti sussistere relazioni tra le radici che non sono conservate dal gruppo simmetrico. Le prossime proposizioni spiegano questo fatto. Il primo lemma confronta l'azione di Gal sui polinomi indotta dal fatto che stiamo vedendo Gal come un sottogruppo si S_n e l'azione di Gal su F[7] .

[7] Potremmo considerare una terza azione naturale di Gal sugli oggetti in questione. Per evitare possibili confusioni e perché ritengo possa essere istruttivo rendiamo esplicita anche questa terza azione anche se di fatto non ne avremo bisogno in seguito.

Se B è un insieme allora abbiamo una azione naturale di S_n su B^n. Se $\sigma \in \mathsf{S}_n$ e $b = (b_1, \dots, b_n)$ definiamo

$$\sigma \cdot (b_1, \dots, b_n) := (b_{\sigma^{-1}(1)}, \dots, b_{\sigma^{-1}(n)}).$$

La presenza di σ^{-1} è dovuta al fatto che se ci si mette σ non è più una azione (non verifica $\sigma \cdot (\tau \cdot b) = (\sigma\tau) \cdot b$); se questo vi sembra poco naturale considerate il caso di B un campo e osservate che l'azione così definita corrisponde all'azione che manda l'i-esimo vettore della base canonica nel $\sigma(i)$-esimo. Il seguente lemma chiarisce la relazione tra questa azione e quella sui polinomi. Sia ora B una estensione di $A = \Bbbk$.

Lemma. *Sia $\sigma \in \mathsf{S}_n$, $b = (b_1, \dots, b_n) \in B^n$ e $P \in S$, allora $(\sigma P)(b) = P(\sigma^{-1} \cdot b)$.*

Dimostrazione. Basta verificare la tesi per $P = x_i$. $(\sigma\, x_i)(b) = x_{\sigma(i)}(b) = b_{\sigma(i)} = x_i(\sigma^{-1} \cdot b)$. □

Lemma 11. *Sia $P \in S$ e $\sigma \in \mathrm{Gal} \subset \mathsf{S}_n$ allora $\sigma(P(\lambda)) = (\sigma P)(\lambda)$.*

Dimostrazione. Basta verificar ela tesi per $P = x_i$. In questo caso abbiamo $\sigma(x_i(\lambda)) = \lambda_{\sigma(i)} = x_{\sigma(i)}(\lambda)$. □

Proposizione 12. *Sia $P \in S$ un polinomio invariante per* Gal *allora $P(\lambda) \in \Bbbk$.*

Dimostrazione. Infatti dal lemma 11 abbiamo $\sigma(P(\lambda)) = (\sigma P)(\lambda) = P(\lambda)$. Quindi $P(\lambda)$ è invariante per il gruppo di Galois ovvero è un elemento di $\Bbbk$. □

Questa proposizione non è sempre invertibile cioè non è detto che se $P(\lambda) \in \Bbbk$ allora P è invariante per Gal. Per esempio se $n = 2$ e $f = t^2 - 2$ e $P = x_1^2 - x_2^2$ allora $P(\lambda) = 0$ ma P non è invariante per $\mathbb{Z}/2$. In alcuni casi però vale anche l'inverso.

Supponiamo che *car.* $\Bbbk \neq 2$, consideriamo $\delta = \prod_{i>j}(\lambda_i - \lambda_j)$ e osserviamo che essendo il polinomio separabile $\delta \neq 0$. Quindi poiché $\sigma\delta = \varepsilon(\sigma)\,\delta$ abbiamo che $\delta \in \Bbbk$ se e solo se $\mathrm{Gal} \subset \mathsf{A}_n$. In particolare abbiamo dimostrato la seguente proposizione.

Proposizione 13. *Sia car.*$\Bbbk \neq 2$ *e f separabile, allora $\Delta(f)$ è un quadrato in $\Bbbk$ se e solo se* $\mathrm{Gal} \subset \mathsf{A}_n$.

Dimostrazione. Infatti Δ è un quadrato in $\Bbbk$ se e solo $\delta(f) = \prod_{i>j}(\lambda_i - \lambda_j) \in \Bbbk$ e la tesi segue dalla discussione che precede la proposizione. □

In generale dato f e un sottogruppo G di S_n è sempre possibile trovare un polinomio P che abbia le stesse proprietà che ha il discriminante nel caso di $G = \mathsf{A}_n$. Prima di far vedere alcune applicazioni di questo modo di procedere vogliamo però sottolineare come la conoscenza di tutti gli invarianti non determini solo il gruppo di Galois ma l'estensione stessa. Sia infatti $I = \{P \in S \,:\, P(\lambda) = 0\}$ e consideriamo l'applicazione da S a F che manda P in $P(\lambda)$. Per quanto osservato nella sezione 1 questa mappa è surgettiva e il suo nucleo è evidentemente I. Quindi $F \simeq S/I$.

7.1. **Un esempio con i polinomi di quarto grado.** In questa sezione vogliamo mostrare come si possa stabilire se il gruppo di Galois sia un sottogruppo di un gruppo isomorfo a D_4. Fissiamo quindi $n = 4$ nella discussione precedente. Essendo f irriducibile Gal agirà transitivamente sulle radici. I sottogruppi, a meno di coniugio, di S_4 che agiscono transitivamente su $\{1, 2, 3, 4\}$ sono elencati nella seguente tabella

sottogruppo	descrizione	cardinalità	numero di sottogruppi a lui coniugati
S_4		24	1
A_4	permutazioni pari	12	1
D_4	isometrie di un quadrato	8	3
V	$\{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$	4	1
C_4	gruppo generato da un 4 ciclo	4	3

Nella discussione che segue fissiamo D_4 come il sottogruppo delle isometrie del quadrato le cui coppie di vertici opposti sono $\{1, 3\}$ e $\{2, 4\}$ e C_4 come il sottogruppo generato dal 4-ciclo $(1\,2\,3\,4)$. Osserviamo che C_4 e V sono due sottogruppi normali di D_4.

Sia $P = (x_1 + x_3)(x_2 + x_4)$ e osserviamo che è invariante per D_4.

Lemma 14. *Sia car.*$\Bbbk \neq 2, 3$ *e supponiamo f separabile e irriducibile. Allora $P(\lambda) \in \Bbbk$ se e solo se* $\mathrm{Gal} \subset \mathsf{D}_4$.

Dimostrazione. Se $\mathrm{Gal} = \mathsf{D}_4$ allora per la proposizione 12 $P(\lambda) \in \Bbbk$.

Supponiamo ora che $P(\lambda) \in \Bbbk$ e dimostriamo che $\mathrm{Gal} \subset \mathsf{D}_4$. Quindi se $\mathrm{Gal} \not\subset \mathsf{D}_4$ allora Gal contiene (1243) o (1324) (ho semplicemente scelto due elementi nei coniugati di C_4 e osservato che un coniugato di D_4 contiene sicuramente un coniugato di C_4 e che V è normale). Per fissare le idee supponiamo che Gal contenga $\tau = (1324)$ (l'altro caso è del tutto analogo). Allora poiché $P(\lambda) \in \Bbbk$ abbiamo

$$(\lambda_1 + \lambda_3)(\lambda_2 + \lambda_4) = P(\lambda) = \tau(P(\lambda)) = (\tau P)(\lambda) = (\lambda_3 + \lambda_2)(\lambda_4 + \lambda_1)$$

da cui semplificando $(\lambda_1 - \lambda_2)(\lambda_3 - \lambda_4) = 0$ ovvero due radici coincidono in contraddizione con la separabilità del polinomio. [8] □

Proposizione 15. *Sia car.*$\Bbbk \neq 2, 3$ *e supponiamo f separabile e irriducibile. Sia $R = R(P, f)$ allora R ha una radice in $\Bbbk$ se e solo se* Gal *è contenuto in un coniugato di* D_4.

Dimostrazione. Le radici di R sono gli elementi $(\sigma P)(\lambda)$. Supponiamo quindi che $(\sigma P)(\lambda) \in \Bbbk$. Se $\sigma = \mathrm{id}$ allora il lemma precedente dimostra che $\mathrm{Gal} = \mathsf{D}_4$. Nel caso generale bisogna solo tenere conto che bisogna riodinare le radici. Infatti $(\sigma P)(\lambda) \in \Bbbk$ vuol dire che $(\lambda_{\sigma(1)} + \lambda_{\sigma(3)})(\lambda_{\sigma(2)} + \lambda_{\sigma(4)})$ e applicando il lemma precedente alle radiciriodinate da σ otteniamo che $\mathrm{Gal} = \sigma\mathsf{D}_4\sigma^{-1}$. □

Nell'esercizio 14 generalizzeremo questa proposizione.

Nel caso in cui $B = F$ e $\sigma \in \mathrm{Gal}$ allora abbiamo due azioni di Gal su F^n, una componente per componente che indichiamo con $\sigma(b)$, e l'altra, indotta dall'azione di permutazione di S_n, che indichiamo con $\sigma \cdot b$. In generale queste due azioni sono completamente diverse ma per $b = \lambda$ sono strettamente collegate infatti $\sigma(\lambda) = \sigma^{-1} \cdot \lambda$. Quindi se $P \in S$ e $\sigma \in \mathrm{Gal}$ abbiamo $\sigma(P(\lambda)) = P(\sigma(\lambda)) = P(\sigma^{-1} \cdot \lambda) = (\sigma P)(\lambda)$.

[8] Questa dimostrazione è più veloce di quella che ho fatto in classe. Quella fatta in classe metteva però in evidenza che una volta calcolato $P(\lambda)$ si potevano ricavare le radici. Vedremo questo fatto nella prossima sezione.

7.2. **Un risultato generale e un esempio con i polinomi di quinto grado.** Iniziamo con un lemma semplice ma che utilizzeremo spesso.

Lemma 16. *Sia $P \in S$, sia $H = Stab_{\mathsf{S}_n} P$ e sia $R = R(P, f)$. Supponiamo che R sia separabili e sia $R = R_1 \cdots R_\ell$ con $R_i \in \Bbbk[t]$ irriducibile e di grado d_i. Allora*

1) Gal *ha esattamente ℓ orbite in $\mathsf{S}_n(P)$ e queste hanno cardinalità $d_1, \dots, d_\ell$;*

2) R ha una radice in $\Bbbk$ se e solo se Gal *è coniugato (in S_n) ad un sottogruppo di H.*

Dimostrazione. Consideriamo il morfismo di anelli $\phi : S[t] \longrightarrow F[t]$ definito da $\phi(t) = t$ e $\phi(P) = P(\lambda)$ se $P \in S$ e osserviamo che $\phi(R(P, x)) = R(P, f)$.

Sia $\mathcal{P} = \mathsf{S}_n P$ e sia $\mathcal{P}' = \phi(\mathcal{P})$. Se R ha tutte le radici distinte vuol dire che per ogni $Q, Q' \in \mathcal{P}$ se $Q(\lambda) = Q'(\lambda)$ allora $Q = Q'$. Quindi ϕ ristretta a $\mathcal{P}$ è una bigezione tra $\mathcal{P}$ e $\mathcal{P}'$. Inoltre abbiamo visto per il lemma 11 ϕ preserva l'azione di Gal ovvero $\phi(\sigma\, Q) = \sigma(\phi(Q))$. Quindi le orbite di Gal in $\mathcal{P}$ sono in corrispondenza con le orbite di Gal in $\mathcal{P}'$ e $R = \prod_{\beta \in \mathcal{P}'}(t - \beta)$. Siano ora $\mathcal{P}'_1, \dots, \mathcal{P}'_m$ le orbite di Gal in $\mathcal{P}'$ e per $i = 1, \dots, m$ poniamo $R'_i = \prod_{\beta \in \mathcal{P}'}(t - \beta)$. Quindi poichè $\mathcal{P}$ è l'unione disgiunta delle sue orbite abbiamo $R = R'_1 \cdots R'_m$. Infine osserviamo che per il lemma 2 i polinomi R'_i sono irriducibili. Quindi poiché $E[t]$ è un anello fattoriale $\ell = m$ e gli R_i (a meno di invertibili) sono una permutazione degli R'_i. Infine osserviamo che il grado degli R'_i è uguale alla cardinalità dell'orbita $\mathcal{P}'_i$.

Supponiamo ora che R abbia una radice in E allora uno dei fattori R_i ha grado 1 quindi Gal ha un'orbita in $\mathsf{S}_n(P)$ costituita da un solo elemento, sia $Q = \sigma\, P$ questo elemento. Allora per ogni $\varphi \in$ Gal abbiamo $\varphi(Q) = Q$ ovvero $\sigma^{-1}\varphi\,\sigma \in Stab_{\mathsf{S}_n} P = H$. Quindi Gal $\subset \sigma H \sigma^{-1}$. □

I seguenti due esercizi mostrano come si possa applicare questa proposizione allo studio dei polinomi di quarto grado generalizzando la proposizione 15.

Esercizio 13. Sia f un polinomio irriducibile e separabile di quarto grado, allora $R((x_1 + x_3)(x_2 + x_4), f)$ ha tutte le radici distinte.

Esercizio 14. Sia *car.*$\Bbbk \neq 2, 3$. Sia f un polinomio irriducibile di quarto grado, Gal il suo gruppo di Galois, Δ il suo discriminante e sia $R = R((x_1 + x_3)(x_2 + x_4), f)$. Allora

1) se Δ non è un quadrato e R è irriducibile allora Gal $\simeq \mathsf{S}_4$;
2) se Δ non è un quadrato e R è riducibile allora Gal $\simeq \mathsf{D}_4$ o Gal $\simeq \mathbb{Z}/4$;
3) se Δ è un quadrato e R è irriducibile allora Gal $\simeq \mathsf{A}_4$;
4) se Δ è un quadrato e R è riducibile allora Gal $\simeq \mathbb{Z}/2 \times \mathbb{Z}/2/$

Per distinguere tra C_4 e D_4 si può procedere in vari modi: calcolare il grado dell'estensione, calcolare la cardinalità del gruppo di Galois (vedi per esempio il prossimo paragrafo), oppure, quando ha radici distinte utilizzare il risolvente $R(x_1 - x_2, f)$ o altri possibili risolventi.

Nello stesso modo possiamo affrontare lo studio dei polinomi di quinto grado. Nel seguito fissiamo quindi $n = 5$ e f un polinomio irriducibile su un campo di caratteristica diversa da $2, 3$ e 5 (queste ipotesi possono essere indebolite per alcune delle affermazioni che faremo). In particolare f è separabile. Supponiamo inoltre che il campo base $\Bbbk$ contenga una radici primitiva terza di 1 che indichiamo con ω, una radice primitiva quarta che indichiamo con i e una radice primitiva quinta che indichiamo con ζ (questo in realtà ci sarà utile solo nella prossima sezione).

I sottogruppi di S_5 che agiscono transitivamente su $\{1, 2, 3, 4, 5\}$ sono coniugati a uno dei sottogruppi listati nella seguente tabella.

sottogruppo	descrizione	cardinalità	numero di sottogruppi a lui coniugati
S_5		120	1
A_5	permutazioni pari	60	1
M_5	gruppo generato da (1 2 3 4 5) e da (1 2 4 3)	20	6
D_5	isometrie del pentagono	10	6
$\mathbb{Z}/5$	gruppo generato da un 5 ciclo	5	6

Nel seguito indicheremo con D_5 le simmetrie del pentagono i cui vertici sono numerati in successione 1, 2, 3, 4 e 5 ovvero il sottogruppo di S_5 generato da (1 2 3 4 5) e da (1 4)(2 3). Indicheremo inoltre con $\mathbb{Z}/5$ il gruppo generato da (1 2 3 4 5).

Con queste notazioni bbiamo inoltre le seguenti relazioni di inclusione e normalità: $\mathbb{Z}/5 \lhd \mathsf{D}_5 \lhd \mathsf{M}_5 < \mathsf{S}_5$ e $\mathsf{D}_5 < \mathsf{A}_5 \lhd \mathsf{S}_5$. In particolare $\mathbb{Z}/5, \mathsf{D}_5, \mathsf{M}_5$ sono gruppi risolubili mentre A_5 e S_5 non lo sono.

Deduciamo da questa breve discussione che f è risolubile per radicali se e solo se il suo gruppo di Galois è contenuto in un coniugato di M_5. Vogliamo quindi presentare un risolvente che riesca a discriminare questo fatto.

Scegliamo intanto alcuni polinomi invarianti. Poniamo

$$\psi = x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1, \qquad \psi' = e_2(x) - \psi, \qquad \chi = \psi - \psi', \quad \text{e} \quad \varphi = \frac{\chi^2}{4}.$$

Calcoliamone gli stabilizzatori:

$$Stab_{\mathsf{S}_5}\psi = \mathsf{D}_5, \qquad Stab_{\mathsf{S}_5}\psi' = \mathsf{D}_5, \qquad Stab_{\mathsf{S}_5}\chi = \mathsf{D}_5, \qquad Stab_{\mathsf{S}_5}\psi = \mathsf{M}_5,$$

inoltre per ogni $\sigma \in \mathsf{M}_5$ abbiamo $\sigma\,\chi = \varepsilon(\sigma)\,\chi$.