Alcuni risultati di Teoria dei Gruppi e di Teoria di Galois

Francesco Parisio

In queste pagine ho intenzione di presentare alcuni risultati interessanti di teoria dei gruppi e di esporre una soluzione ad uno studio del gruppo di Galois di due polinomi. Sono rivolte a un lettore che, come me, ha qualche conoscenza "di base" di algebra astratta. Alcune volte, preferirò omettere alcuni dettagli sulle dimostrazioni o su risultati di base, per dare spazio allo svolgimento di esercizi e a qualche osservazione personale.

Qualora siano presenti errori o imprecisioni, vi invito a segnalarmele, inviando una e-mail alla mia casella personale:

`7frapar@gmail.com`

Grazie, e buona lettura.

Il gruppo dei quaternioni

I quaternioni sono una struttura complessa che emerge naturalmente, nelle applicazioni, parlando di rotazioni nello spazio tridimensionale. Dal solo punto di vista intuitivo, possiamo pensare ad un quaternione ad un numero insieme a una componente vettoriale tridimensionale:

$$\mathbb{H} = \{a + b\mathtt{i} + c\mathtt{j} + d\mathtt{k} \mid a, b, c, d \in \mathbb{R}\}.$$

$\mathbb{H}$ forma un corpo (cioè un campo il cui gruppo moltiplicativo non risulta abeliano). Il gruppo di cui ci occuperemo adesso è il gruppo dei *versori unitari* di tale gruppo moltiplicativo. Una costruzione formale e precisa passa dalle matrici invertibili nel campo complesso. Osserviamo che questa costruzione è simile, in qualche modo, a quello del campo complesso. Ricordiamo, infatti, che

$$\mathbb{C} = \mathrm{Span}_{\mathbb{R}}\left\{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}0 & -1\\ -1 & 0\end{pmatrix}\right\}.$$

Procediamo allora con la costruzione dei quaternioni. Per iniziare, consideriamo il gruppo delle matrici invertibili nel campo complesso $\mathrm{GL}(2, \mathbb{C})$. Siano, ivi,

$$\eta = \begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix} \quad \zeta = \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$$

quindi sia $G = \langle \eta, \zeta \rangle$. Per calcolo diretto, si può verificare che η e ζ hanno ordine 4, e sono tali che $\eta^2 = \zeta^2$. Inoltre,

$$\eta^\zeta = \eta^{-1} = \eta^3 = \zeta^3 \eta \zeta$$

dunque il gruppo non risulta commutativo. Poiché $\eta^\zeta \in \langle \eta \rangle$, $\langle \eta \rangle$ è normale in G, dunque

$$\langle \eta, \zeta \rangle = \langle \eta \rangle \langle \zeta \rangle.$$

L'ordine del prodotto è esattamente

$$\frac{\mathrm{ord}\ \eta \times \mathrm{ord}\ \zeta}{\mathrm{ord}\ \eta^2} = 8$$

essendo $\langle \eta^2 = \zeta^2 \rangle = \langle \eta \rangle \cap \langle \zeta \rangle$. Possiamo quindi elencare gli elementi di G nel modo seguente.

$$G = \{1, \eta, \eta^2 = \zeta^2, \eta^3, \zeta, \zeta^3, \eta\zeta, \eta^3\zeta\}$$

A dimostrazione di ciò, è sufficiente notare che gli elementi $\eta\zeta$ e $\eta^3\zeta$ sono distinti.

Studiamo allora i sottogruppi di G. Tanto per cominciare, vediamo subito che $\langle\eta\rangle$ e $\langle\zeta\rangle$ sono normali perché hanno indice 2. Inoltre, il sottogruppo generato da $\eta^2 = \zeta^2$ è pure normale.

Se un sottogruppo $H < G$ contiene un generatore tra η e ζ e contiene un qualsiasi altro elemento di ordine > 2, allora H coincide con G per questioni di ordine. Quindi, se esiste un altro sottogruppo di G, non si ha speranza di trovarlo combinando gli elementi η e ζ. In effetti, vi è un altro sottogruppo di G distinto da quelli già elencati: si tratta di $\langle\eta\zeta\rangle$.

Si può osservare che gli elementi $\eta\zeta$ e $\eta^3\zeta$ sono entrambi di ordine 4, e generano lo stesso gruppo, essendo

$$\langle\eta\zeta\rangle = \{1, \eta\zeta, (\eta\zeta)^2, (\eta\zeta)^{-1}\} = \{1, \eta\zeta, \eta^2, \eta^3\zeta\} = \langle\eta^{-1}\zeta\rangle$$

Allora, sia H un sottogruppo di G che contiene $\langle\eta\zeta\rangle$ e un altro elemento non contenuto in H (ad esempio η oppure ζ). Se H contiene anche η, allora contiene anche $\eta \cdot \eta^3\zeta = \zeta$, quindi H contiene $\langle\eta, \zeta\rangle$ quindi $H = G$. Se contiene ζ, contiene ζ^3, quindi anche $\eta\zeta \cdot \zeta^3 = \eta$. Un argomento del tutto equivalente vale per gli altri elementi di ordine > 2. Possiamo allora affermare che gli unici sottogruppi di G sono

$$1 \quad \langle\eta^2\rangle \quad \langle\eta\rangle \quad \langle\zeta\rangle \quad \langle\eta\zeta\rangle \quad G$$

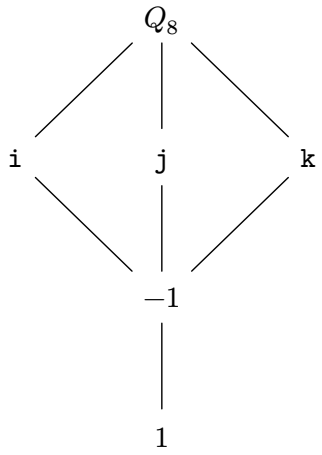
rispettivamente di ordine 1, 2, 4 e 8. Poiché l'indice di $\langle\eta\zeta\rangle$ in G è 2, tutti i sottogruppi di ordine 4 sono normali. Anche $\langle\eta^2\rangle$ è normale, poiché è intersezione di sottogruppi normali.

Come osservato inizialmente, il gruppo G non risulta abeliano. Questo è un esempio di gruppo non abeliano con tutti i sottogruppi normali: si tratta di un gruppo *hamiltoniano*.

Poniamo allora $\eta^2 = -\mathtt{1}$, $\eta = \mathtt{i}$, $\zeta = \mathtt{j}$, $\eta\zeta = \mathtt{k}$. È immediato mostrare che, con questa scelta, valgono le relazioni $\mathtt{i}^2 = \mathtt{j}^2 = \mathtt{k}^2 = -\mathtt{1}$. Inoltre, valgono le formule

$$\begin{array}{lll} \mathtt{i} \cdot \mathtt{j} = \mathtt{k} & \mathtt{j} \cdot \mathtt{k} = \mathtt{i} & \mathtt{k} \cdot \mathtt{i} = \mathtt{j} \\ \mathtt{j} \cdot \mathtt{i} = -\mathtt{k} & \mathtt{k} \cdot \mathtt{j} = -\mathtt{i} & \mathtt{i} \cdot \mathtt{k} = -\mathtt{j}. \end{array}$$

Il gruppo G appena definito si chiama gruppo dei quaternioni, e si indica spesso con Q_8. Di seguito, il reticolo dei sottogruppi di Q_8.



Poiché Q_8 ha ordine 8, è in particolare un 2-gruppo: il suo centro non è mai banale. Dalle proprietà sugli elementi $\mathtt{i}$, $\mathtt{j}$ e $\mathtt{k}$, possiamo concludere che $Z(Q_8) = \langle -1\rangle$.

Il prodotto semidiretto e il gruppo diedrale

Lo studio dei gruppi non sarebbe così interessante senza le azioni di gruppi. In modo del tuto informale, un gruppo rappresenta un insieme di operazioni che possiamo usare per muovere gli oggetti di un certo insieme. Una struttura che probabilmente abbiamo avuto modo di toccare con mano almeno qualche volta è lo spazio vettoriale. In un corso introduttivo all'algebra lineare, un insieme V è uno spazio vettoriale su un campo K se V è un gruppo abeliano rispetto alla somma $+$, e se vale, oltre alla distributività, la condizione seguente

$$\lambda(\mu \boldsymbol{v}) = (\lambda\mu)\boldsymbol{v} \quad 1\boldsymbol{v} = \boldsymbol{v} \quad \forall \lambda, \mu \in K \quad \forall \boldsymbol{v} \in V.$$

In termini più complessi, il gruppo moltiplicativo di K deve agire per moltiplicazione a sinistra su V. Questo vuol dire sia ben definito un morfismo di gruppi

$$\rho : K^\times \to \mathrm{Aut}(V)$$

definito come $\rho(\lambda) = (\boldsymbol{x} \mapsto \lambda \boldsymbol{v} \ \forall \boldsymbol{v} \in V)$. La moltiplicazione a sinistra di un elemento è ovviamente un automorfismo su V, quindi ρ è ben definito, e la condizione che caratterizza i morfismi

$$\rho(\lambda)\rho(\mu) = \rho(\lambda\mu)$$

si traduce, immediatamente, nella proprietà che richiediamo nei campi vettoriali.

Il tipo di azione che ho cercato di spiegare nel paragrafo precedente è un azione agli automorfismi, cioè è tale che rispetta l'operazione $+$ del gruppo V. In generale, le azioni sono definite sul gruppo simmetrico $\mathrm{Sym}(\Omega)$ di un certo insieme Ω, cioè l'insieme di tutte le bigezioni di Ω (che hanno diversi nomi, in base al contesto: le si chiamano permutazioni, simmetrie, etc).

Il prodotto semidiretto tra due gruppi consente di produrre nuovi gruppi usando le azioni agli automorfismi. Procuriamoci due gruppi A e B, e supponiamo che sia definita un'azione

$$\rho : A \to \mathrm{Aut}(B)$$

Consideriamo il prodotto cartesiano tra i due gruppi. L'insieme $A \times B$ è un gruppo con l'operazione

$$(a, b)(\alpha, \beta) = (a\alpha, b\rho(a^-1)(\beta)) \quad \forall (a, b), (\alpha, \beta) \in A \times B$$

detto prodotto semidiretto tra A e B, denotato con la scrittura $B \rtimes_\rho A$ (la dimostrazione che questa operazione sia ben posta e che la struttura che definisce sia a tutti gli effetti un gruppo, è omessa).

Osserviamo che, se decidiamo di individuare con b^a l'immagine $\rho(a)(b)$ e con ab il prodotto $(a, 1)(1, b)$, il coniugio di b tramite a è proprio

$$b^a = a^{-1}ba = (1, \varphi(a)(b)).$$

È chiaro che questa notazione porti notevoli vantaggi in termini di scrittura: converrà allora utilizzarla!

Una struttura di prodotto semidiretto emerge naturalmente qualora G sia un gruppo e N sia un suo sottogruppo normale. Se esiste un sottogruppo $K < G$, non necessariamente normale, tale che $N \cap K = 1$ e $HK = G$, allora

$$G \simeq N \rtimes_{\mathrm{conj}} K$$

dove conj è esattamente l'azione di coniugio di K su N, definita dal morfismo

$$\mathrm{conj} : k \mapsto \bigcirc^k \ \big(= h \mapsto h^k \ \forall h \in H\big).$$

Questo è ancora un prodotto semidiretto, ed è quello più immediato che possiamo costruire. Solitamente, il pedice ρ viene rimosso per alleggerire la notazione, ma va specificato qualora generi ambiguità: la struttura di prodotto semidiretto dipende essenzialmente dalla scelta di tale morfismo!

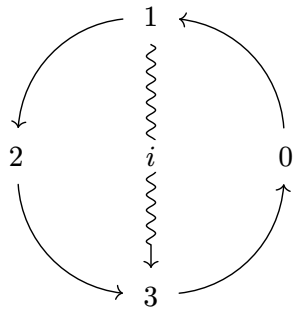
Il gruppo delle simmetrie di un poligono regolare di n vertici si chiama gruppo *diedrale*, ed è rappresentato da $n-1$ operazioni di rotazioni non banali intorno all'origine, più una riflessione attorno ad un asse. La loro combinazione per composizione genera un gruppo di $2n$ elementi, descritto formalmente dal prodotto semidiretto

$$D_{2n} \stackrel{\text{def}}{\cong} C_n \rtimes_i C_2 \lesssim S_n$$

dove l'azione i è definita come

$$\begin{aligned} i : C_2 &\to \mathrm{Aut}(C_n) \\ 1 &\mapsto 1 \\ -1 &\mapsto \bigcirc^{-1} \end{aligned}$$

cioè l'azione di inversione sugli elementi di C_n. Possiamo pensare a i come alla riflessione del poligono attorno all'asse orizzontale, qualora i punti del poligono si facciano coincidere con le radici n-esime dell'unità. Ad esempio, se decidiamo di costruire D_8 con i gruppi ciclici in notazione additiva, otteniamo



$$1^i = 3 \quad 1 + 3 = 0.$$

In questo modo, il numero 0 tiene fisso il quadrato, i lo riflette, 1 muove i suoi veritici in senso orario di $2\frac{\pi}{4}$ radianti, etc. La relazione $1^i = 3$ ci dice che riflettere, ruotare di 90 gradi e riflettere di nuovo ha lo stesso effetto di ruotare tre volte il quadrato in senso orario di 90 gradi.

Studio delle radici del polinomio $x^4 - 2$

Consideriamo il polinomio $p = x^4 - 2 \in \mathbb{Q}[x]$. Per procedere con lo studio delle radici del polinomio p, è necessario calcolare la classe di isomorfia del gruppo di Galois associata all'estensione $E \mid \mathbb{Q}$, dove E è il campo di spezzamento del polinomio, ovvero $\mathbb{Q}(p)$.

Il polinomio si scompone come $p = x^4 - 2 = \big(x^2 - \sqrt{2}\big)\big(x^2 + \sqrt{2}\big)$, dunque le sue radici sono

$$\Omega = \big\{\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}\big\}.$$

Il campo di spezzamento del polinomio è dunque $E = \mathbb{Q}\big(\sqrt[4]{2}, i\big)$. Calcoliamone anzitutto il grado su $\mathbb{Q}$. Per utilizzare la regola della torre, consideriamo il sottocampo $L = \mathbb{Q}\big(\sqrt[4]{2}\big)$. Osserviamo che $E = L(i)$: poiché E è complessa ed estende un campo reale, il grado $[E : L] \neq 1$. Inoltre, $\min_L(i) = x^2 + 1$. Infatti, $x^2 + 1$ è monico, ha come radice i, ed è irriducibile in L. Dimostrare

che un polinomio di secondo grado è irriducibile in un certo campo è semplice: in questo caso un polinomio $q \in L[x]$ con $\partial q = 2$ è riducibile se e solo se

$$q = (x - \alpha)(x - \beta) \quad \alpha, \beta \in L.$$

Questo ovviamente non è vero per $x^2 + 1$ in L. Quindi, per il teorema dell'elemento algebrico,

$$[E : L] = \partial \min_{L}(i) = 2.$$

Vogliamo allora calcolare il grado dell'estensione $L \mid \mathbb{Q}$. Per il criterio di Eisenstein (applicato con $p = 2$), il polinomio $x^4 - 2$ risulta irriducibile in $\mathbb{Q}$. Poiché è monico e una sua radice è $\sqrt[4]{2}$, p coincide con il polinomio minimo di $\sqrt[4]{2}$ su $\mathbb{Q}$. Ancora, come conseguenza del teorema dell'elemento algebrico,

$$[L : \mathbb{Q}] = \partial \min_{\mathbb{Q}}\left(\sqrt[4]{2}\right) = 4.$$

Concludiamo allora che $[E : \mathbb{Q}] = 8$. Poiché E è un campo di spezzamento e estende un campo con caratteristica zero, risulta, rispettivamente, normale e separabile, quindi di Galois. Come conseguenza, il gruppo di Galois $G = \mathrm{Gal}(E \mid \mathbb{Q})$ ha ordine 8.

Il gruppo G agisce transitivamente sull'insieme delle radici Ω, quindi G è isomorfo a un sottogruppo di S_4. Per la caratterizzazione dei gruppi di ordine 8, G è isomorfo a D_8 oppure a Q_8. Possiamo distinguere i due gruppi studiandone i sottogruppi normali: siccome Q_8 è Hamiltoniano, per dimostrare che $G \simeq D_8$, sarà sufficiente trovare un sottogruppo di G non normale.

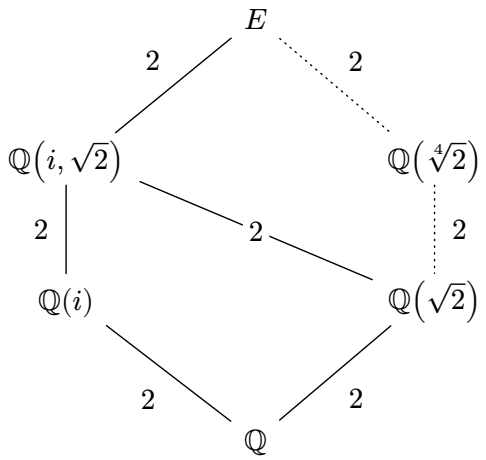
Consideriamo la sottoestensione $\mathbb{Q}\left(\sqrt[4]{2}\right) \mid \mathbb{Q}$: p contiene due radici in $\mathbb{Q}\left(\sqrt[4]{2}\right)$, ma non si spezza in $\mathbb{Q}\left(\sqrt[4]{2}\right)$. Per il primo criterio di normalità, tale estensione non risulta normale. Per il teorema di corrispondenza di Galois, G contiene un sottogruppo di ordine 4 non normale. Questo esclude la possibilità che G sia abeliano e che G sia hamiltoniano. L'unica possibilità è che $G \simeq D_8$.

Per procedere con lo studio degli elementi del gruppo G, osserviamo che esiste un sottocampo intermedio tra E e $\mathbb{Q}(i)$, cioè $\mathbb{Q}\left(i, \sqrt{2}\right)$.

Dalla formula dei gradi, si ha

$$4 = [E : \mathbb{Q}(i)] = \left[E : \mathbb{Q}\left(i, \sqrt{2}\right)\right]\left[\mathbb{Q}\left(\sqrt{2}, i\right) : \mathbb{Q}(i)\right].$$

Osserviamo che $Q\left(i, \sqrt{2}\right)$ è un sottocampo proprio. Infatti, $\sqrt{2} \notin \mathbb{Q}(i)$, e $\sqrt[4]{2} \in E \setminus \mathbb{Q}\left(\sqrt{2}, i\right)$. Disegnamo allora il seguente diagramma.



Solleviamo gli automorfismi seguendo il percorso disegnato a linea solida.

Cominciamo considerando la sottoestensione $\mathbb{Q}(i) \mid \mathbb{Q}$. Il gruppo di Galois associato ha ordine 2. Chiamiamo r il suo generatore. r è la restrizione dell'automorfismo di coniugio $a + ib \mapsto a - ib$ del piano complesso, ed è l'unico automorfismo non banale del simmetrico di $\{i, -i\}$.

Analogamente, consideriamo l'estensione di $\mathbb{Q}\left(\sqrt{2}\right) \mid \mathbb{Q}$. Anche questa estensione è di Galois, il suo gruppo ha ordine due, e contiene i due automorfismi della retta reale: l'identità e $\sqrt{2} \mapsto -\sqrt{2}$. Gli automorfismi dei gruppi $\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{2}\right) \mid \mathbb{Q}\right)$ e $\mathrm{Gal}(\mathbb{Q}(i) \mid \mathbb{Q})$ si sollevano entrambi a 4 automorfismi del gruppo $\mathrm{Gal}\left(\mathbb{Q}\left(i, \sqrt{2}\right) \mid \mathbb{Q}\right)$.

Gli automorfismi che otteniamo sono determinati dalle immagini di $\sqrt{2}$ e i.

	i	$\sqrt{2}$
τ_1	i	$\sqrt{2}$
τ_2	i	$-\sqrt{2}$
τ_3	$-i$	$\sqrt{2}$
τ_4	$-i$	$-\sqrt{2}$

Osserviamo che τ_1 e τ_2 estendono l'automorfismo identico dell'estensione complessa, mentre τ_1, τ_3 estendono l'automorfismo identico dell'estensione reale. Il gruppo di automorfismi che ne risulta è il gruppo di Klein V_4 su 4 elementi, siccome ogni elemento ha ordine 2.

Ogni morfismo del gruppo $\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{2}, i\right) \mid \mathbb{Q}\right)$ si estende in esattamente due automorfismi di E che fissano $\mathbb{Q}$, e ciascuno di essi è determinato dalle immagini di i e $\sqrt[4]{2}$. Per dedurre una descrizione esaustiva degli elementi di G, calcoliamo i campi fissati dai sottogruppi di G.

Scriviamo $G = H \rtimes K$, dove $H = \langle h \rangle$ e $K = \langle k \rangle$. Ovviamente $\operatorname{ord} h = 4$ e $\operatorname{ord} k = 2$.

Il campo fissato da K in E ha grado $2 = [E : E^K]$, quindi per la formula della torre otteniamo $[E^K : \mathbb{Q}] = 4$. Il campo fissato da K quindi può essere $\mathbb{Q}\left(i, \sqrt{2}\right)$ oppure $\mathbb{Q}\left(\sqrt[4]{2}\right)$, siccome entrambi hanno grado due e entrambi hanno grado 4 su $\mathbb{Q}$. Per il teorema di corrispondenza di Galois, il campo fissato da K è normale su $\mathbb{Q}$ se e solo se K lo è in G: l'unica possibilità è che $E^K = \mathbb{Q}\left(\sqrt[4]{2}\right)$. Infatti, $\mathbb{Q}\left(\sqrt[4]{2}\right) \mid \mathbb{Q}$ *non* è normale per il primo criterio di normalità, e il sottogruppo C_2 non è mai normale in $C_n \rtimes C_2$. Come conseguenza, il sottogruppo K agisce sulle radici di p nel modo seguente.

$$i \mapsto -i \quad \sqrt[4]{2} \mapsto \sqrt[4]{2}$$

Consideriamo ora il sottogruppo H. Il sottocampo fissato da H è tale che

$$[E : E^H] = 4 \quad \text{quindi } [E^H : \mathbb{Q}] = 2.$$

Il sottogruppo H è normale in G, quindi il suo campo fissato è normale su $\mathbb{Q}$. I candidati per E^H sono i campi intermedi $\mathbb{Q}(i)$ e $\mathbb{Q}\left(\sqrt{2}\right)$.

Poiché H è normale, $E \mid E^H$ è normale e risulta ancora di Galois: come conseguenza $\mathrm{Gal}(E \mid E^H) = H$. Il teorema di corrispondenza di Galois applicato a questa estensione ci dice che i sottogruppi di H sono in biezione con i campi intermedi $E^H \subset L \subset E$. Poiché H è ciclico, H contiene un unico sottogruppo di ordine 2. Come conseguenza, il campo fissato da H non è $\mathbb{Q}\left(\sqrt{2}\right)$, perché è contenuto in due campi intermedi (nella fattispecie, $\mathbb{Q}\left(\sqrt[4]{2}\right)$ e $\mathbb{Q}\left(i, \sqrt{2}\right)$). L'unica possibilità è che $E^H = \mathbb{Q}(i)$.

Questo aiuta a concludere che una possibile descrizione degli elementi di G è la seguente.

	i	$\sqrt[4]{2}$	sollevamento di
1	i	$\sqrt[4]{2}$	τ_1
h	i	$i\sqrt[4]{2}$	τ_2
h^2	i	$-\sqrt[4]{2}$	τ_1
h^3	i	$-i\sqrt[4]{2}$	τ_2
k	$-i$	$\sqrt[4]{2}$	τ_3
hk	$-i$	$i\sqrt[4]{2}$	τ_4
h^2k	$-i$	$-\sqrt[4]{2}$	τ_3
h^3k	$-i$	$-i\sqrt[4]{2}$	τ_4

Nello stesso spirito, si può studiare l'estensione $\mathbb{Q}\big(\sqrt[8]{5}, i\big) \mid \mathbb{Q}\big(\sqrt{5}\big)$: risulta normale, e la sua classe di isomorfia è ancora D_8. In realtà, non è facile trovare estensioni di campi che abbiano gruppo di Galois quaternionico. Il primo esempio è l'estensione semplice del numero

$$\alpha = \sqrt{\big(2+\sqrt{2}\big)\big(3+\sqrt{3}\big)}$$

su $\mathbb{Q}$, che però non tratterò in questa sede.