Estensioni finite di campi

Le considerazioni che seguono riguardano i *campi di numeri* e cioè i sottocampi del campo $\mathbb{C}$ dei numeri complessi.

Definizione 1. *Dati due campi di numeri E e K, si dice che E è una estensione di K se $E \supseteq K$.*

Definizione 2. *Una estensione $E \supseteq K$ si dice finita se E, visto come spazio vettoriale su K, ha dimensione finita:*

$$\dim_K E < \infty .$$

In questo caso si scrive:

$$\dim_K E = [E : K] ,$$

e si dice che $[E : K]$ è il grado dell'estensione $E \supseteq K$.

Naturalmente $[E : K] = 1$ se e solo se $E = K$.

Definizione 3. *Sia K un campo di numeri. Un numero complesso α si dice algebrico su K se esiste un polinomio $p(t) \in K[t]$ tale che $p(\alpha) = 0$.*

Lemma 1. *Sia α algebrico su K. Allora esiste un unico polinomio $p_\alpha(t) \in K[t]$ monico e di grado minimo tra quelli che si annullano in α. Tale polinomio prende il nome di polinomio minimo di α su K. Il grado di α su K è, per definizione, il grado del suo polinomio minimo $p_\alpha(t)$.*

Dim. Sia $p_\alpha(t) \in K[t]$ un polinomio, monico e quindi non nullo, di grado minimo tra quelli che si annullano in α. Se $q(t) \in K[t]$ gode delle stesse proprietà di $p_\alpha(t)$, usando l'algoritmo euclideo, si può scrivere

$$q(t) = f(t)p_\alpha(t) + r(t) , \qquad r(t) \in K[t] , \ \deg r(t) < \deg p_\alpha(t) .$$

Poiché $q(\alpha) = p_\alpha(\alpha) = 0$, si ha anche $r(\alpha) = 0$ e quindi, per la minimalità del grado di $p_\alpha(t)$, si deve avere $r(t) = 0$. Sempre per la minimalità dei gradi di $p_\alpha(t)$ e di $q(t)$, si ha che il grado di $p_\alpha(t)$ coincide con quello di $q(t)$. Dunque $f(t)$ è un polinomio costante, che deve necessariamente essere eguale a 1, essendo sia $p_\alpha(t)$ che $q(t)$ polinomi monici. Q.E.D.

Osservazione 1. *Si osservi che un polinomio monico e irriducibile $q(t) \in K[t]$ che si annulli in α è necesssariamente il polinomio minimo di α su K, perchè, se non lo fosse, $p_\alpha(t)$ ne sarebbe un fattore.*

Teorema 1. *Sia α algebrico su K. Sia $K[\alpha]$ l'insieme delle espressioni polinomiali in α a coefficienti in K:*

$$K[\alpha] = \{q(\alpha) \mid q(t) \in K[t]\} .$$

Allora $K[\alpha]$ è un campo di numeri che si denota anche con il simbolo $K(\alpha)$. Inoltre, il campo $K(\alpha)$ è estensione finita di K e si ha:

$$[K(\alpha):K] = \deg p_\alpha(t)\,.$$

Dim. Dati $p(t)$ e $q(t)$ in $K[t]$, si ha che $p(\alpha) \pm q(\alpha) \in K[\alpha]$. Per verificare che $K[\alpha]$ è un campo di numeri basta quindi verificare che, se $q(\alpha) \neq 0$, allora anche $1/q(\alpha) \in K[\alpha]$. Supponiamo che $\deg q(t) \geq \deg p_\alpha(t)$. Scriviamo

$$q(t) = f(t)p_\alpha(t) + r(t) \qquad r(t) \in K[t]\,, \;\; \deg r(t) < \deg p_\alpha(t)\,.$$

Se ne deduce che $q(\alpha) = r(\alpha)$. A meno di sostituire $q(t)$ con $r(t)$, possiamo dunque assumere che $\deg q(t) < \deg p_\alpha(t)$. Scriviamo allora:

$$p_\alpha(t) = h(t)q(t) + s(t) \qquad s(t) \in K[t]\,, \;\; \deg s(t) < \deg q(t) < \deg p_\alpha(t)\,.$$

Per la minimalità del grado di $p_\alpha(t)$ deve quindi risultare $s(\alpha) \neq 0$. Poniamo $s(\alpha) = c$ e $k(t) = -h(t)/c$. Si ottiene

$$0 = \frac{p_\alpha(t)}{c} = -k(\alpha)q(\alpha) + 1\,.$$

Dunque $k(\alpha) = 1/q(\alpha)$. Ciò dimostra che $K[\alpha]$ è un campo, che d'ora in poi denotiamo con il simbolo $K(\alpha)$. Posto $n = \deg p_\alpha(t)$, dimostriamo infine che $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ è una base di $K(\alpha)$ su K. Dalla dimostrazione precedente deduciamo che ognoi elemento $q(\alpha) \in K(\alpha)$ può scriversi nella forma $r(\alpha)$ per un opportuno polinomio $r(t) \in K[t]$ di grado minore o uguale a $n-1$. Ciò mostra che $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ è un sistema di generatori di $K(\alpha)$ su K. La indipendenza lineare, su K, degli elementi di $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$, segue immediatamente dalla minimalità di $p_\alpha(t)$. Q.E.D.

Teorema 2. *Sia $E \supseteq F \supseteq K$ una catena di estensioni finite. Allora*

$$[E:K] = [E:F][F:K]$$

Dim. Sia $\{e_1, \ldots, e_n\}$ una base di E su F e $\{f_1, \ldots, f_m\}$ una base di F su K. Dimostriamo che $\{e_i f_j\}_{i=1,\ldots,n\,,j=1,\ldots,m}$ è una base di E su K. Sia $a \in E$. Allora $a = \sum_{i=1}^n c_i e_i$, con $c_i \in F$. D'altro canto $e_i = \sum_{j=1}^m d_{ij} f_j$, con $d_{ij} \in K$, e quindi

$$a = \sum_{i=1}^n \sum_{j=1}^m c_i d_{ij} e_i f_j\,.$$

Dunque $\{e_i f_j\}_{i=1,\ldots,n\,,j=1,\ldots,m}$ è un sistema di generatori di E su K. Per verificarne la lineare indipendenza, supponiamo che

$$\sum_{i=1}^n \sum_{j=1}^m a_{ij} e_i f_j = 0\,, \qquad a_{ij} \in K\,.$$

Scriviamo

$$\sum_{i=1}^n \sum_{j=1}^m a_{ij} e_i f_j = \sum_{i=1}^n \left(\sum_{j=1}^m a_{ij} f_j \right) e_i\,, \quad \sum_{j=1}^m a_{ij} f_j \in F\,, \quad i = 1, \ldots, n\,.$$

Per la lineare indipendenza degli e_i su F, si ha

$$\sum_{j=1}^{m} a_{ij} f_j = 0\,, \quad i = 1, \dots, n\,.$$

Per la lineare indipendenza degli f_j su K, si ha $a_{ij} = 0$.

Q.E.D.

Nel nostro contesto, le estensioni di grado 2 svolgono il ruolo principale.

Corollario 1. *Sia $E \supseteq K$ una estensione. Allora $[E : K] \leq 2$, se e solo se esiste $D \in K$ tale che $E = K(\sqrt{D})$.*

Dim. Che sia: $[K(\sqrt{D}) : K] \leq 2$, è ovvio. Infatti, o $\sqrt{D} \in K$, nel qual caso, $K(\sqrt{D}) = K$, oppure no, nel qual caso $\{1, \sqrt{D}\}$ è una base di $K(\sqrt{D})$ su K. Viceversa, supponiamo $[E : K] \leq 2$. Se $E = K$, non vi è nulla da dimostrare: basta prendere $D = c^2 \in K$. Supponiamo dunque che $[E : K] = 2$. Sia $\{1, \alpha\}$ una base di E su K. I numeri $\{1, \alpha, \alpha^2\}$ sono linearmente dipendenti su K e quindi esistono numeri b e c in K tali che

$$\alpha^2 + b\alpha + c = 0\,.$$

Sia

$$D = b^2 - 4c\,.$$

Allora $\alpha \in K(\sqrt{D})$. Si ha dunque $E \subset K(\sqrt{D})$. Poichè $\alpha \notin K$ si ha che $\sqrt{D} \notin K$ e dunque $[K(\sqrt{D}) : K] = 2$. Per il teorema precedente si ha

$$2 = [E : K] = [E : K(\sqrt{D})][K(\sqrt{D}) : K] = [E : K(\sqrt{D})] \cdot 2$$

e quindi $E = K(\sqrt{D})$. Q.E.D.

Esercizio 1. *Sia K un campo di numeri. Sia α algebrico su K e sia n il grado del suo polinomio minimo. Si ponga $E = K(\alpha)$. Sia $F_\alpha : E \to E$ l'applicazione definita da $F_\alpha(v) = \alpha v$, per ogni $v \in E$. Dimostrare che F_α è K-lineare, che il polinomio caratteristico di F_α su K coincide con il polinomio minimo di F_α su K e che entrambe coincidono con il polinomio minimo di α su K.*

Costruzioni con riga e compasso

Si fissino, una volta per tutte, due punti distinti O e U nel piano euclideo.

Definizione 4. *Una costruzione euclidea è una successione finita $\{A_1, \dots, A_n\}$ dove, per ogni $i_0 \in \{1, \dots n\}$, vi sono, per l'elemento A_{i_0}, solo le seguenti possibilità*

$$A_{i_0} = \begin{cases} O \\ U \\ \textit{una retta} \\ \textit{un cerchio} \\ \textit{un punto} \end{cases}$$

soggette alle seguenti condizioni. Se A_{i_0} è una retta, allora deve essere una retta per due punti A_i e A_j, con $i < i_0$ e $j < i_0$. Se A_{i_0} è un cerchio, allora deve essere un cerchio di centro un punto A_k, con $k < i_0$ e raggio d, dove d è la distanza tra due punti A_i e A_j, con $i < i_0$ e $j < i_0$. Se A_{i_0} è un punto, allora $A_{i_0} \in A_i \cap A_j$, dove A_i e A_j sono, o due rette, o una retta e un cerchio, o due cerchi, con $i < i_0$ e $j < i_0$.

Definizione 5. *Un punto, una retta o un cerchio del piano euclideo si dice costruibile se appare in una costruzione euclidea. Un numero complesso $\alpha = a + ib$ si dice costruibile se il punto $P = (a, b)$ è costruibile.*

Esercizio 2. *i) Dimostrare che gli assi coordinati sono costruibili.*
ii) Dimostare che dati un punto p e una retta r, entrambi costruibili, lo è anche la retta per P parallela a r.
iii) Dimostrare che se a e b sono costruibili lo sono anche $a + b$, ab e a/b.
iv) Dimostrare che tutti i punti con coordinate razionali sono costruibili.

La costruzione fondamentale è la seguente.

Lemma 2. *Se il numero reale γ è costrubile, lo è anche $\sqrt{\gamma}$.*

Dim. La costruzione è illustrata dalla seguente figura in cui il centro del cerchio è nel punto $(0, (\gamma - 1)/2)$:

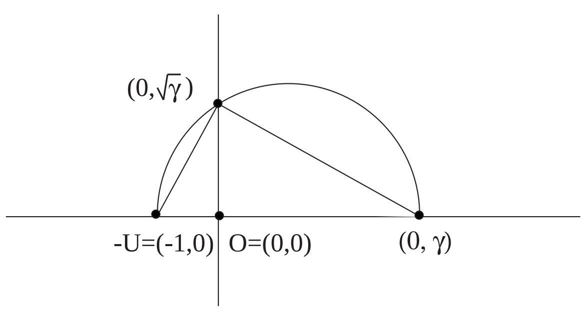

Fig. 1

Q.E.D.

Teorema 3. *Un numero complesso $\alpha = a + ib$ è costruibile se e solo se esiste una catena di estensioni*

$$\mathbb{Q} = E_0 \subseteq E_1 \subseteq E_2 \subseteq \cdots \subseteq E_n \subseteq E_{n+1}\,,$$

tale che
a) $[E_i : E_{i-1}] \leq 2$, per $i = 1, \ldots, n + 1$.
b) $\alpha \in E_{n+1}$.

Dim. Supponiamo che α sia costruibile. Sia $\{A_1, \ldots, A_n\}$ la costruzione del punto $P = (a, b)$. Definiamo induttivamente i campi $E_0, \ldots, E_{n+1}$. Si pone, come richiesto

$E_0 = \mathbb{Q}$. Supponiamo di avere costruito E_j. Se A_{j+1} è una retta o un cerchio si pone $E_{j+1} = E_j$. Se A_{j+1} è un punto di cooordinate (σ, τ), si pone $E_{j+1} = E_j(\sigma, \tau)$. In particolare, si pone $E_n = E_{n-1}(a, b)$. Infine si pone $E_{n+1} = E_n(i)$. Si osservi che, con queste definizioni, se A_j è una retta o un cerchio, si può asssumere che i coefficienti dell'equazione cartesiana di A_j siano in E_j. Infatti questi coefficienti sono espressioni razionali nelle coordinate di punti A_s, con $s < j$, e queste coordinate, per costruzione, appartengono a $E_s \subseteq E_j$. Verifichiamo ora che le condizioni a) e b) sono soddisfatte dalla catena di estensioni appena costruita. Che $\alpha = a+ib \in E_{n+1}$ è evidente. Dimostriamo dunque la a). Consideriamo l'estensione $E_{j+1} \supseteq E_j$. Se A_{j+1} è una retta o un cerchio si ha $E_{j+1} = E_j$ e non vi è quindi nulla da dimostrare. Se A_{j+1} è un punto P di coordinate (σ, τ), si ha

$$E_{j+1} = E_j(\sigma, \tau)$$

e vi sono tre casi da esaminare. Se il punto P è ottenuto come intersezione di due rette A_h e A_k con $h < j+1$ e $k < j+1$, le coordinate di P possono esprimersi razionalmente nei coefficienti delle equazioni cartesiane di A_h e A_k. Questi coefficienti, come abbiamo osservato, appartengono certamente a E_j. Dunque sia σ che τ apppartengono a E_j e quindi $E_{j+1} = E_j$. Nel secondo caso, supponiamo che P appartenga all'intersezione di una retta A_h:

$$a_1x + b_1y + c_1 = 0\,,$$

con $h < j+1$ e di un cerchio A_k:

$$x^2 + y^2 + a_2x + b_2y + c_2 = 0$$

con $k < j+1$. Supponiamo che $a_1 \neq 0$, il caso in cui $b_1 \neq 0$ si tratta in modo simile. Eliminando la x nelle due precedenti equazioni, si ottiene una equazione quadratica:

$$y^2 + ry + s = 0\,,$$

dove r e s sono espressioni razionali in a_1, b_1, c_1, a_2, b_2 e c_2. Dunque le coordinate σ e τ di un punto di intersezione tra A_h e A_k sono espressioni razionali in a_1, b_1, c_1, a_2, b_2, c_2 e $\sqrt{D}$, dove

$$D = r^2 - 4s\,.$$

Essendo $E_{j+1} = E_j(\sigma, \tau)$, si ha dunque che $E_{j+1} = E_j(\sqrt{D})$ e dal Corollario 1, segue che $[E_{j+1} : E_j] \leq 2$. Nel terzo e ultimo caso, supponiamo che P appartenga all'intersezione di un cerchio A_h:

$$x^2 + y^2 + a_1x + b_1y + c_1 = 0\,,$$

con $h < j+1$ e di un cerchio A_k:

$$x^2 + y^2 + a_2x + b_2y + c_2 = 0$$

con $k < j+1$. Il sistema delle due equazioni appena scritte è equivalente al seguente:

$$(a_1 - a_2)x + (b_1 - b_2)y + (c_1 - c_2) = 0$$
$$x^2 + y^2 + a_2x + b_2y + c_2 = 0$$

Supponiamo che $a_1 - a_2 \neq 0$, il caso in cui $b_1 - b_2 \neq 0$ si tratta in modo simile. Eliminando la x nelle equazioni del precedente sistema, si ottiene una equazione quadratica:

$$y^2 + uy + v = 0\,,$$

dove u e v sono espressioni razionali in a_1, b_1, c_1, a_2, b_2 e c_2. Dunque le coordinate σ e τ di un punto di intersezione tra A_h e A_k sono espressioni razionali in a_1, b_1, c_1, a_2, b_2, c_2 e $\sqrt{D'}$, dove

$$D' = u^2 - 4v \,.$$

Essendo $E_{j+1} = E_j(\sigma, \tau)$, si ha che $E_{j+1} = E_j(\sqrt{D'})$ e, come prima, si conclude che $[E_{j+1} : E_j] \leq 2$. Il punto a) è ora completamente dimostrato. Non ci resta ora che dimostrare la implicazione opposta. Supponiamo quindi che vi sia una catena di estensioni

$$\mathbb{Q} = E_0 \subseteq E_1 \subseteq E_2 \subseteq \cdots \subseteq E_n \subseteq E_{n+1} \,,$$

che soddisfi le condizioni a) e b) e dimostriamo che il numero α è costruibile. Per la condizione b) è sufficiente mostrare che il punto $P = (a, b)$ è costruibile. Dimostreremo di più e cioè che tutti i numeri in E_n sono costruibili. Faremo ciò per induzione, partendo dal primo caso, ovvio, in cui $E_0 = \mathbb{Q}$. Supponiamo dunque la nostra asserzione vera per il campo E_j. Per E_{j+1} vi sono solo due possibilità. La prima è che $E_{j+1} = E_j$. In questo caso l'asserzione è banalmente verificata. Nel secondo caso si ha $[E_{j+1} : E_j] = 2$. Per il Corollario 1, si ha che $E_{j+1} = E_j(\sqrt{D})$, con $D \in E_j$. Ma, per il Lemma 2, la radice quadrata di D è costruibile e dunque tutti i numeri in E_{j+1} lo sono. Q.E.D.

Corollario 2. *Sia α un numero costruibile. Allora $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^n$, per un qualche intero, non negativo, n.*

Esercizio 3. *i) Dimostrare che non è possibile duplicare il cubo con la riga e il compasso. Con ciò si intende che non è possibile costruire, con la riga e il compasso, il lato di un cubo avente volume doppio di un cubo di lato costruibile, per esempio di un cubo di lato uguale a 1.*
ii) Dimostrare che non è possibile trisecare un angolo con la riga e il compasso.

Costruibilità e non costruibilità dei poligoni regolari

La costrubilità, o meno, di un poligono regolare con n lati è ovviamente equivalente alla costruibilità, o meno, di una radice primitiva n-esima dell'unità. Denotiamo con ε_n una tale radice. Si ha:

$$\varepsilon_n = \cos(\tfrac{2\pi}{n}) + i \sin(\tfrac{2\pi}{n}) \,.$$

Decomponiamo l'intero n in fattori primi:

$$n = 2^k p_1^{\nu_1} \cdots p_s^{\nu_s}$$

dove $p_1, \ldots, p_s$ sono primi distinti e dispari.

Lemma 3. *Siano h e k due numeri naturali primi tra loro. Allora ε_{hk} è costruibile se e solo se lo sono ε_h e ε_k .*

Dim. Chiaramente, dal momento che $\varepsilon_h = \varepsilon_{hk}^k$ e $\varepsilon_k = \varepsilon_{hk}^h$, una delle due implicazioni è ovvia. Supponiamo dunque che ε_h e ε_k siano costruibili. Dal momento che h e k sono primi fra loro, esistono interi ν e μ tali che

$$\nu h + \mu k = 1 .$$

Verifichiamo che, allora,

$$\varepsilon_{hk} = \varepsilon_h^\mu \varepsilon_k^\nu .$$

Infatti:

$$\varepsilon_h^\mu \varepsilon_k^\nu = \cos(\tfrac{2\mu\pi}{h} + \tfrac{2\nu\pi}{k}) + i\sin(\tfrac{2\mu\pi}{h} + \tfrac{2\nu\pi}{k}) = \cos(\tfrac{2\pi}{hk}) + i\sin(\tfrac{2\pi}{hk}) = \varepsilon_{hk} .$$

Q.E.D.

Ne consegue che, per avere un criterio di costruibilità per ε_n, basta averne uno per tutti i numeri della forma p^ν, dove p è un primo. Dal Teorema 1 segue che, per trovare il grado dell'estensione $\mathbb{Q}(\varepsilon_{p^\nu}) \supset \mathbb{Q}$, bisogna determinare il grado del polinomio minimo di ε_{p^ν}. In virtù dell'Osservazione 1, basta trovare un polinomio monico e irriducibile

$$\varphi_{p^\nu}(t) \in \mathbb{Q}[t] ,$$

che si annulli in ε_{p^ν}. Scriviamo

$$t^{p^\nu} - 1 = \left(t^{p^{\nu-1}} - 1\right)\left(\left(t^{p^{\nu-1}}\right)^{p-1} + \left(t^{p^{\nu-1}}\right)^{p-2} + \cdots + \left(t^{p^{\nu-1}}\right) + 1\right) .$$

Poniamo

$$\varphi_{p^\nu}(t) = \left(\left(t^{p^{\nu-1}}\right)^{p-1} + \left(t^{p^{\nu-1}}\right)^{p-2} + \cdots + \left(t^{p^{\nu-1}}\right) + 1\right) .$$

Poiché $\varepsilon_{p^\nu}^{p^\nu} = 1$, mentre $\varepsilon_{p^\nu}^{p^{\nu-1}} \neq 1$, il polinomio $\varphi_{p^\nu}(t)$ si annulla in ε_{p^ν}. A questo punto, usando opportunamente il criterio di irriducibilità di Eisenstein (che qui non vogliamo trattare), si può dimostrare, in modo elementare, il seguente:

Lemma 4. *Il polinomio $\varphi_{p^\nu}(t)$ è irriducibile in $\mathbb{Q}[t]$.*

Corollario 3. $[\mathbb{Q}(\varepsilon_{p^\nu}) : \mathbb{Q}] = p^{\nu-1}(p-1)$.

Corollario 4. *Se ε_{p^ν} è costruibile, allora o $p = 2$, oppure $p = 2^{2^n} + 1$.*

Dim. Dal Teorema 3 segue che, per qualche k deve risultare $p^{\nu-1}(p-1) = 2^k$ Ne segue che se $p \neq 2$, deve necessariamente risultare $\nu = 1$ e dunque $p = 2^k + 1$. Scriviamo $k = 2^\mu q$, con q dispari. Si ha: $p = 2^{2^\mu q} + 1$. Poniamo $m = 2^{2^\mu}$, cosicché

$$p = m^q + 1 = (m+1)\left(m^{q-1} - m^{q-2} + \cdots + 1\right) .$$

Essendo p un numero primo deve necessariamente esssere $q = 1$. Q.E.D.

I numeri della forma $2^{2^\mu} + 1$ si chiamano *numeri di Fermat.* Tenendo conto del Corollario 4 e del Lemma 3 abbiamo dimostrato il seguente:

Teorema 4. *Se un poligono regolare di n lati è costruibile con la riga e il compasso, allora*

$$n = 2^k p_1 \cdots p_s \,,$$

dove i p_i sono primi di Fermat distinti:

$$p_i = 2^{2^{\mu_i}} + 1 \,, \qquad i = 1, \ldots, s \,.$$

Dopo aver sviluppato un minimo di teoria di Galois, è possibile dimostrare che la condizione enunciata nel teorema precedente è anche condizione sufficiente per la costruibilità di un poligono regolare di n lati.

Esercizio 4. *i) Trovare un numero di Fermat che non sia primo.*
ii) Costruire, con la riga e il compasso, poligoni regolari con 3, 4, 5, 6 e 15 lati
iii) Dimostrare l'impossibilità di costruire, con la riga e il compasso, poligoni regolari con 7, 9, 11 e 13 lati.
iv) Discutere la costruibilità, o meno, del lato di un tetraedro di volume unitario.