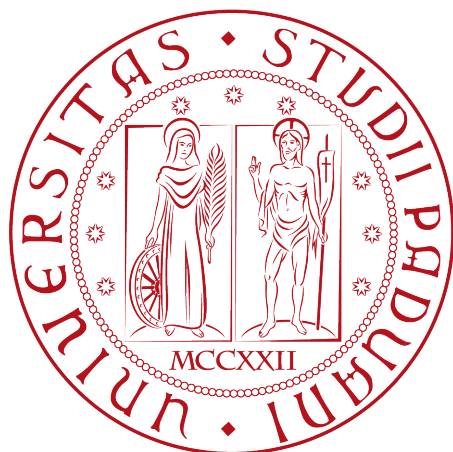


UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"

Corso di Laurea Magistrale in Matematica



DIPARTIMENTO
MATEMATICA

LA GEOMETRIA DEGLI ORIGAMI

ESTENSIONE DELL'APPROCCIO EUCLIDEO ALLA
CICLOTOMIA

Relatore:

Prof. Francesco Ciraulo

Laureando:

Stefano Pietrogrande

Matricola:

2063544

anno accademico 2022/2023

15 Dicembre

INDICE

ELENCO DELLE FIGURE	i
INTRODUZIONE	iii
1 GLI ELEMENTI, E POCO PIÙ IN LÀ	1
1.1 Alcune Costruzioni Importanti	1
1.2 I Poligoni Classici	4
1.3 Qualche Generalizzazione	6
2 LE DISQUISITIONES ARITHMETICAE	11
2.1 I risultati in Breve	11
2.2 La Teoria dei Residui	13
2.3 Determinare i Periodi Gaussiani	20
2.4 Un Esempio Celebre: L'Eptadecagono	21
3 WANTZEL E GALOIS	25
3.1 La Condizione Sufficiente	25
3.2 Il Campo dei Numeri Costruibili	27
3.3 L'Argomento di Wantzel	30
3.4 Il Teorema di Gauss-Wantzel	34
4 LA GEOMETRIA DEGLI ORIGAMI	37
4.1 Gli Assiomi di Huzita-Hatori-Justin	37
4.2 Breve Discussione su alcuni Assiomi	41
4.3 Il Campo dei Numeri Origami	44
4.4 Completezza degli Assiomi HHJ	50
4.5 I Poligoni Origami	52
4.6 Un Esempio: L'Eptagono	54
5 ORIGAMI A PIEGHE SIMULTANEE	59
5.1 Origami a Doppia Piegna	60
5.2 Il Metodo di Lill	63
5.3 I Poligoni Multi-Fold	72
5.4 Un Esempio: L'Endecagono	74
CONCLUSIONE	78
BIBLIOGRAFIA	81

ELENCO DELLE FIGURE

1.1	Bisettrice di un Angolo	2
1.2	Asse di un Segmento	2
1.3	Proporzionalità sui Lati	2
1.4	Segmento Medio Proporzionale	2
1.5	Parallela per un Punto	3
1.6	Costruzione di AH , Sezione Aurea di AB	3
1.7	Costruzione del Triangolo Equilatero	4
1.8	Costruzione del Quadrato	5
1.9	Il Triangolo Aureo	5
1.10	Pentagono Regolare e Triangolo Aureo	6
1.11	Costruzione del Pentadecagono Regolare	8
2.1	Una Costruzione dell'Eptadecagono	24
3.1	Somma di due Lunghezze	28
3.2	Prodotto di due Lunghezze	28
3.3	Suddivisione del Segmento Unitario per $n = 7$	29
3.4	Due Circonferenze e il loro Asse Radicale	32
4.1	Assioma O1	38
4.2	Assioma O2	38
4.3	Assioma O3, Rette Parallele	39
4.4	Assioma O3, Rette Incidenti	39
4.5	Assioma O4	39
4.6	Assioma O5	40
4.7	Assioma O6	40
4.8	Assioma O7	40
4.9	Pieghe Possibili per O5 e Parabola Associata	42
4.10	Una piega descritta da O6 come tangente simultanea a due parabole	43
4.11	Assioma O7 nel Caso di Rette Parallele	43
4.12	Trasporto di una Lunghezza su una Retta	45
4.13	Quattro possibili posizioni di P' e cubica associata a O6	47

4.14	La Piegia per $2c_7$	56
4.15	Una Costruzione dell'Eptagono con gli Origami	58
5.1	AL6ab8 nel caso in cui $L_1 = L_2 := L$	62
5.2	Il Metodo di Lill applicato a $2x^4 - 7x^3 + 5x^2 + x + 2$	64
5.3	La Rappresentazione di Horner realizzata attraverso il Metodo di Lill	65
5.4	Un Esempio con $3x^2 + 5x - 2$	66
5.5	Di nuovo $3x^2 + 5x - 2$, con gli Origami a Piegia Singola	67
5.6	$3x^3 + 3x^2 + 4x - 1$ evidenziando il Quadrato di Beloch.	68
5.7	$2x^5 + 5x^4 + 3x^3 + x^2 + 2x - 2$ attraverso l'uso di tre pieghe simultanee	71
5.8	La Doppia Piegia per $2c_{11}$	76
5.9	Una Costruzione dell'Endecagono con gli Origami a Doppia Piegia Simultanea	77

INTRODUZIONE

L'argomento di questa tesi è il problema della *ciclotomia*, cioè quello della suddivisione (*temno*, tagliare) della circonferenza (*kyklos*, cerchio) in archi di uguale lunghezza. È facile immaginare come questo sia equivalente ad inscrivere in quella circonferenza i vari poligoni regolari.

Questo problema ha, al giorno d'oggi e in termini algebrici, una soluzione elementare: i punti che suddividono la circonferenza unitaria in n parti uguali sono quelli, nel piano dei numeri complessi \mathbb{C} , corrispondenti alle radici del polinomio $x^n - 1$, vale a dire le *radici dell'unità*, che hanno la forma

$$e^{2i\frac{k}{n}\pi} = \cos\left(\frac{2k\pi}{n}\right) + i \sin\left(\frac{2k\pi}{n}\right) \quad k = 1, \dots, n$$

Se però si intende determinare questi punti, che dei poligoni regolari costituiscono i vertici, attraverso una costruzione geometrica, delle difficoltà tecniche rendono immediatamente la soluzione ben più complessa dell'applicazione di una formula. La maggiore di queste difficoltà è la scelta di quali strumenti utilizzare nella costruzione o, in altre parole, decidere cosa "sia permesso" disegnare e cosa no.

Nella prima parte della tesi mi concentrerò sul ripercorrere da un punto di vista storico l'evoluzione dell'approccio alla ciclotomia attraverso gli strumenti classici della *riga* e del *compasso*. Disegnare con riga e compasso significa, a partire da (almeno) una coppia di punti assegnati, costruire nuovi enti geometrici attraverso unicamente le azioni di:

- tracciare quelle linee rette che passano per almeno due punti già individuati oppure
- tracciare quegli archi di circonferenze che sono centrati e passano per punti già individuati oppure
- marcare come nuovi punti le intersezioni di linee già individuate.

Il compasso euclideo è *collassante*, cioè "si chiude se staccato dal foglio". A priori si possono dunque tracciare circonferenze unicamente se centrate e passanti per punti già individuati. Si può però dimostrare che è possibile usare altri segmenti come raggio, dunque confonderemo i due tipi di operazione riferendoci semplicemente al "compasso". La riga invece è non graduata.

Ci si accorge subito che, a meno di confondere quegli enti geometrici che *esistono* con quelli che sono *costruibili*, queste azioni sono equivalenti all'assunzione dei primi tre dei cinque postulati classici della Geometria Euclidea, che qui liberamente sono riformulati:

1. ogni coppia di punti è congiunta da un segmento;
2. ogni segmento è contenuto in una linea retta;
3. ogni punto e ogni segmento costituiscono il centro e il raggio di una circonferenza.

La natura degli altri due assiomi invece, utilizzando la riga e il compasso, risulta *nascosta*. Ad esempio

4. tutti gli angoli retti sono equivalenti

è frutto di un principio di carattere più generale, che Euclide chiamerebbe una *nozione comune*. Se infatti gli unici oggetti geometrici che esistono sono quelli che costruiamo diventa intuitivo che, una volta costruito un angolo che chiamiamo "retto", tutti gli altri angoli similmente costruiti risultano a esso congruenti, cioè sottendono su qualsiasi circonferenza archi della stessa lunghezza. Stiamo dunque sottintendendo che diverse iterazioni della stessa costruzione diano risultati congruenti. Invece

5. due rette che, tagliate da una trasversale, formano in un semipiano angoli coniugati interni la cui somma è inferiore a due angoli retti sono in quel semipiano incidenti

rimane una proposizione indipendente dagli altri assiomi, che classicamente assumiamo.

Vedremo che, in questa teoria, la costruzione di alcuni poligoni regolari risulta impossibile. Dimosteremo una condizione, nota come *Teorema di Gauss-Wantzel*, che distingue in modo esatto quali poligoni regolari siano costruibili e quali no, a seconda del numero dei loro lati. Fra il primo approccio al problema nel 300 aC e questa dimostrazione, che è del 1837, passano più di due millenni, rendendo quella della ciclotomia una delle questioni più longeve della storia della matematica.

Nella seconda parte della tesi mi dedicherò a una teoria geometrica alternativa. Questa nuova geometria è ottenuta sostituendo agli strumenti di riga e compasso le *pieghe della carta* e viene chiamata descrittivamente *Geometria degli Origami*.

Questa teoria pone un focus speciale sulla costruzione delle linee rette, identificate come le tracce lasciate sul foglio da, appunto, pieghe della carta. I possibili modi di operare una piega sulla carta costituiscono in effetti gli assiomi della teoria o, come nel caso della Geometria Euclidea, le costruzioni elementari. Le rette *costruibili*, che chiameremo "tracciabili", sono quelle che coincidono con pieghe che, se

effettuate, portano oggetti precedentemente individuati in disposizioni particolari. I punti costruibili saranno quelli che giacciono sull'intersezione di rette costruibili.

Dopo aver introdotto la Geometria degli Origami in modo assiomatico vedremo come non solo questa sia in grado di superare alcune difficoltà proprie della Geometria Classica ma in effetti propriamente la estenda, cioè sia in grado di costruire tutti quegli oggetti che erano costruibili con riga e compasso. Questo fatto deve sembrare in qualche modo stupefacente poiché, ad esempio, non pare affatto ovvio come le pieghe della carta possano supplire all'assenza di un compasso.

Ci concentreremo infine sull'identificare una nuova condizione equivalente alla costruibilità dei poligoni regolari constatando una notevole simmetria rispetto alla forma della caratterizzazione precedente.

Nella parte finale troverà spazio una generalizzazione ulteriore della teoria delle pieghe della carta, quella che consente le così dette *pieghe simultanee*, cioè che permette di segnare quelle righe che costituiscono la traccia di gruppi di pieghe la cui posizione sul foglio viene scelta ciascuna in funzione delle altre. Saremo in grado una terza volta di individuare una soluzione al problema della ciclotomia, ma la teoria delle pieghe simultanee è ancora "giovane": la condizione che troveremo è solo sufficiente. Ciò nonostante la generalità a questo punto raggiunta sarà notevole e in un certo senso *completa*, poiché in effetti qualsiasi poligono regolare risulterà costruibile, a condizione che un numero sufficiente di pieghe simultanee sia consentito.

Capitolo 1

GLI ELEMENTI, E POCO PIÙ IN LÀ

1.1 Alcune Costruzioni Importanti

Prima di concentrarci sulle costruzioni dei poligoni è più importante soffermarsi su sei costruzioni fondamentali la cui importanza diventerà chiara proseguendo e che in effetti costituiscono la base su cui caratterizzeremo i punti costruibili nel modo più preciso. I teoremi che seguono, tratti direttamente dal corpo degli *Elementi*, sono contrassegnati con una dicitura del tipo "LaPb", che significa che nell'opera di Euclide, consultabile per intero in [Joy98], questi teoremi costituiscono la proposizione numero b dell' a -esimo libro¹. Questa notazione permette di seguire in maniera ordinata il pensiero di Euclide, poiché ogni proposizione poggia sugli assiomi o su proposizioni precedenti, nonostante in questa tesi i risultati siano riordinati per il ruolo che ricoprono rispetto al problema della ciclotomia.

Teorema 1.1 (L1P9).

Assegnato un angolo è costruibile la sua bisettrice.

Teorema 1.2 (L1P10).

Assegnato un segmento è costruibile il suo asse.

Teorema 1.3 (L1P31).

Assegnati una retta ed un punto ad essa non appartenente è costruibile una retta parallela a quella data e passante per il punto fissato.

Teorema 1.4 (L2P11).

Assegnato un segmento è costruibile un punto al suo interno che ne realizza la sezione aurea, cioè tale da dividere il segmento in media ed estrema ragione².

¹Le traduzioni in italiano, però, sono mie. Le parole sono scelte in modo da rispettare il contesto delle costruzioni con riga e compasso.

²Significa trovare un punto P interno al segmento AB tale che $AB : AP = AP : PB$

Teorema 1.5 (L6P2).

Se una retta è tracciata parallelamente a un lato di un triangolo in modo da intercettare gli altri due lati allora i segmenti individuati su questi sono proporzionali. Viceversa se due punti sono scelti ciascuno su un diverso lato di uno stesso triangolo in modo da dividerli in parti proporzionali allora il segmento che congiunge quei due punti è parallelo al terzo lato.

Teorema 1.6 (L6P13).

Assegnati due segmenti ne è costruibile un terzo la cui lunghezza risulti media proporzionale fra le lunghezze dei primi due.

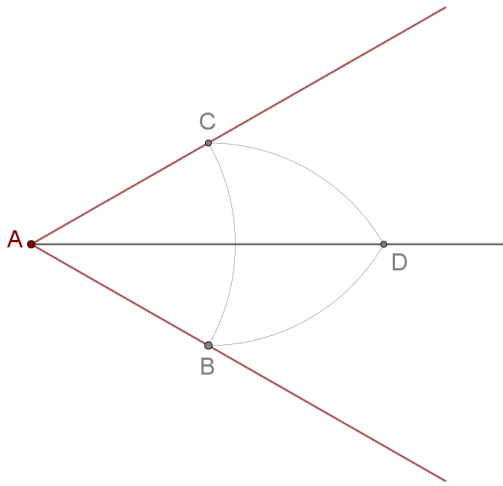


Figura 1.1: Bisettrice di un Angolo

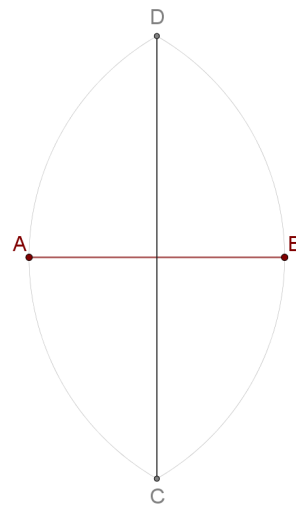


Figura 1.2: Asse di un Segmento

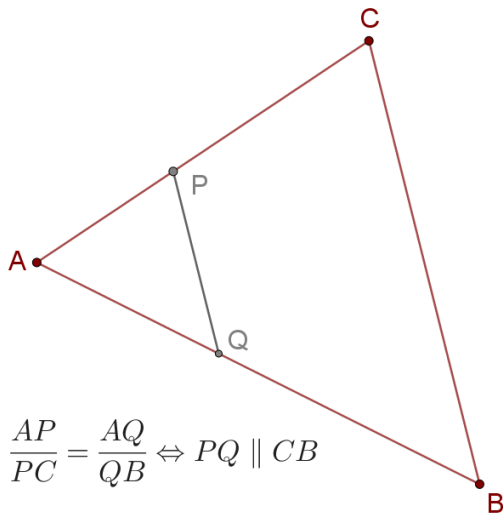


Figura 1.3: Proporzionalità sui Lati

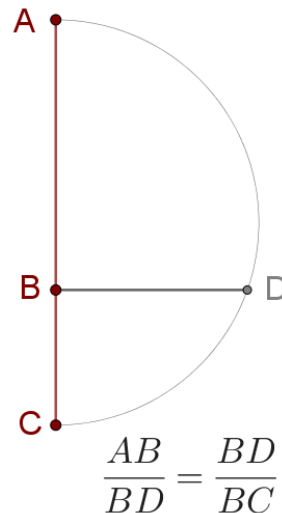


Figura 1.4: Segmento Medio Proporzionale

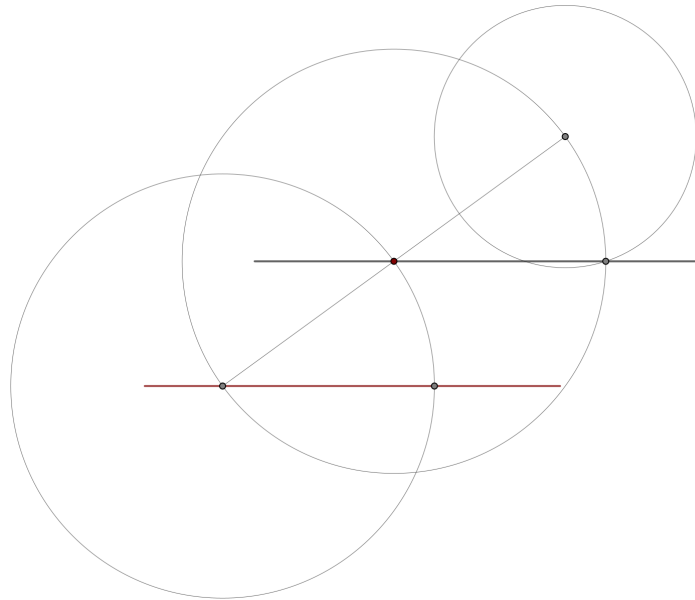


Figura 1.5: Parallela per un Punto

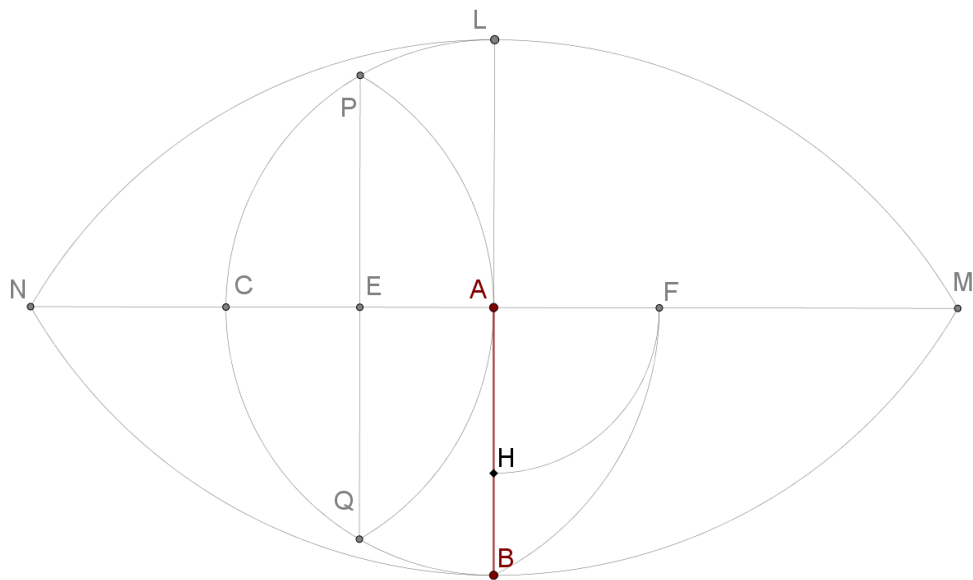


Figura 1.6: Costruzione di AH , Sezione Aurea di AB .

1.2 I Poligoni Classici

Fin proprio dagli *Elementi* di Euclide, che risalgono circa al 300 aC, la costruibilità di particolari poligoni regolari è nota in modo esplicito, cioè ne è noto l'algoritmo di costruzione. Addirittura la costruzione del Triangolo Equilatero, per noi anche 3-gono, è in assoluto la prima proposizione dell'opera.

Teorema 1.7 (L1P1).

Assegnato un segmento è costruibile il triangolo equilatero che ha per lato quel segmento.

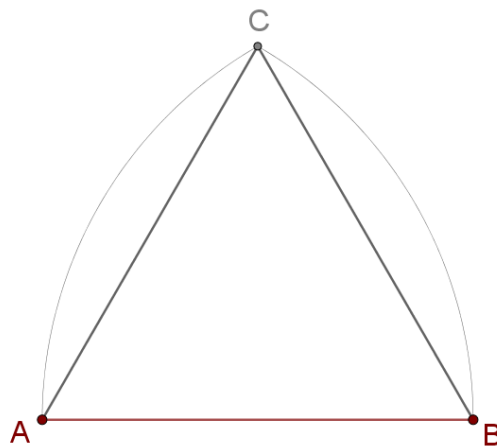


Figura 1.7: Costruzione del Triangolo Equilatero

È bene fare una distinzione: Euclide effettua una costruzione *dato il lato*. A noi, in realtà, interessano costruzioni *dato il raggio*. Non è un problema e anzi confonderemo le cose, infatti se il n -gono è costruibile dato il lato allora è costruibile anche la circonferenza circoscritta a questo poligono e con essa il suo centro. Di conseguenza è costruibile l'angolo al centro, che è riportabile al centro di qualsiasi altra circonferenza, costruendo così il n -gono dato il raggio. Viceversa se il n -gono è costruibile dato il raggio allora è costruibile l'angolo compreso fra due lati adiacenti e di conseguenza, riportando questo angolo e la misura del lato col compasso, il n -gono è costruibile anche dato il lato.

La costruibilità dell'asse di un segmento implica la costruibilità di angoli retti. Questo permette, riportando la lunghezza di un segmento assegnato col compasso, di costruire un quadrato. Come nel caso del triangolo, anche se la costruzione è effettuata a partire dal lato, questo equivale alla suddivisione della circonferenza in quattro parti.

Teorema 1.8 (L1P46).

Assegnato un segmento è costruibile il quadrato che ha per lato quel segmento.

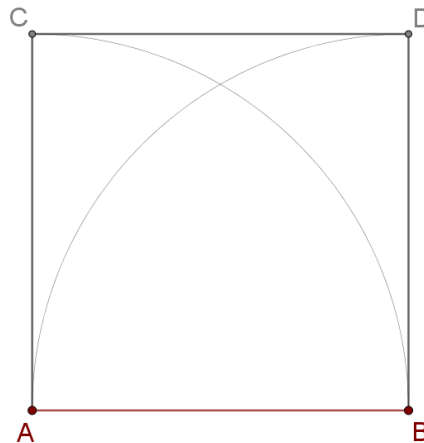


Figura 1.8: Costruzione del Quadrato

Il pentagono, che come vedremo con ordine nei Teoremi 1.12, 1.13 e 2.1 è l'unico altro poligono la cui costruzione gioca un ruolo importante, non arriva per via "diretta".

Euclide ottiene in realtà la costruzione di un particolare triangolo isoscele, che risulta poi essere quello formato da un lato e dalle due diagonali del pentagono che dagli estremi di quel lato concorrono nel vertice opposto. È il *Triangolo Aureo*, cioè quello la cui base è la sezione aurea del lato. Questo triangolo isoscele ha per angolo alla base esattamente $\frac{2\pi}{5}$, che è l'angolo al centro del 5-gono.

Teorema 1.9 (L4P10).

È costruibile un triangolo isoscele il cui angolo alla base è doppio di quello al vertice.

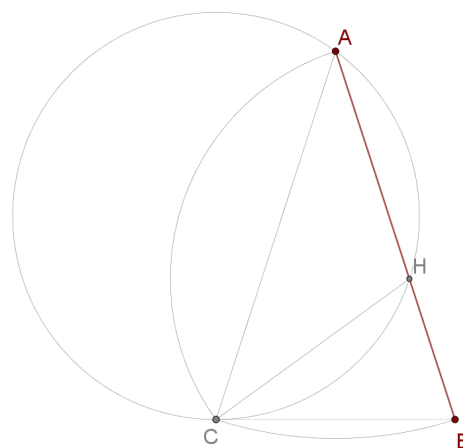


Figura 1.9: Il Triangolo Aureo

La tesi di Euclide è quella sul rapporto fra gli angoli, ma la dimostrazione procede basandosi sulla *sezione aurea* (L2P11 e Figura 1.6).

Il punto che la realizza nella Figura 1.9 per il segmento AB è H , così che $AH^2 = AB \cdot BH$. In questa costruzione BC è preso congruente a AH intersecando l'arco di centro A e raggio AB con quello di centro B e raggio AH , dunque $AB \cdot BH = BC^2$, che è una condizione equivalente alla tangenza del segmento BC alla circonferenza AHC .

Vale di conseguenza $\angle BCA = 2\angle BAC$ e la condizione sulla somma degli angoli interni dà immediatamente $\angle BCA = \frac{2\pi}{5}$.

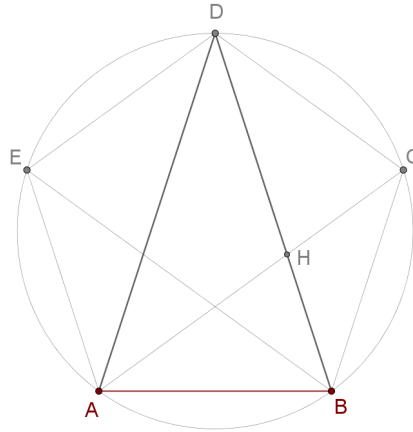


Figura 1.10: Pentagono Regolare e Triangolo Aureo

La costruzione del Pentagono viene completata inscrivendo nella circonferenza il triangolo aureo³ e tracciando le bisettrici (L1P9 e Figura 1.1) dei suoi angoli alla base, le cui intersezioni con la circonferenza individuano i due vertici mancanti.

1.3 Qualche Generalizzazione

È curioso notare come, in figura 1.10, essendo l'angolo in D esattamente $\frac{2\pi}{10}$, si sia provata anche la costruibilità del Decagono. Questa costruzione non compare esplicitamente negli *Elementi*, ma vi è presente ad esempio quella dell'Esagono. In entrambi i casi l'esistenza di queste costruzioni, e altre con esse, è prevista dal seguente

Teorema 1.10.

Se il n -gono è costruibile allora anche il $2^k n$ -gono è costruibile, per qualsiasi $k \in \mathbb{N}$.

Dimostrazione.

Si costruisca il n -gono. Bisecandone un qualunque angolo al centro si trova l'angolo al centro del $2n$ -gono. L'algoritmo è iterabile. \square

³Con riga e compasso è possibile inscrivere in una circonferenza un triangolo simile a uno fissato. Si veda L4P2 in [Joy98].

Questo risultato non è fra quelli di Euclide, tuttavia glielo si può serenamente attribuire, comprendendo in un'unica soluzione la costruibilità del 6-gono e del 10-gono.

Similmente vi sono altri due Teoremi, non propriamente attribuibili ad Euclide ma in un certo senso "alla sua portata", che garantiscono la costruibilità di alcuni poligoni a partire da quella di altri.

Teorema 1.11.

Se $d \mid n$ e il n -gono è costruibile allora anche il d -gono è costruibile.

Dimostrazione.

Di nuovo semplicemente si costruisca il n -gono. Siano Q_0, \dots, Q_{n-1} i suoi vertici. I vertici del d -gono sono $Q_{\frac{kn}{d}}$ per $k = 0, \dots, d - 1$. In altre parole è sufficiente congiungere i vertici del n -gono uno ogni $\frac{n}{d}$. \square

Prima di enunciare e dimostrare il secondo teorema vale la pena osservare che combinazioni lineari intere di angoli costruibili sono a loro volta costruibili. In simboli:

$$\alpha, \beta \text{ costruibili} \implies \forall h, k \in \mathbb{Z} (h\alpha + k\beta \text{ costruibile})$$

Questo è vero perché attraverso l'uso del compasso è possibile costruire multipli interi di angoli ed effettuare la loro somma o sottrazione misurando gli archi che questi angoli sottendono su circonferenze di pari raggio.

È inoltre equivalente, come già abbiamo sottointeso riferendoci al Decagono, la costruibilità del n -gono a quella dell'angolo $\frac{2\pi}{n}$. Ammesso infatti che il poligono sia costruibile tale risulta anche, in quanto intersezione di due qualsiasi assi dei suoi lati, il centro della circonferenza circoscritta. Viceversa se l'angolo è costruibile allora su qualsiasi circonferenza di centro il vertice di quell'angolo è possibile riportare n volte la misura dell'arco sotteso, individuando i vertici del poligono.

Teorema 1.12.

Siano n, m coprimi e assumiamo che il n -gono e il m -gono siano entrambi costruibili. Allora anche il nm -gono è costruibile.

Dimostrazione.

Se il n -gono e il m -gono sono costruibili allora sono costruibili i due angoli $\frac{2\pi}{n}$ e $\frac{2\pi}{m}$. Vogliamo costruire l'angolo $\frac{2\pi}{nm}$ e per fare ciò è sufficiente che esistano $h, k \in \mathbb{Z}$ tali che

$$\frac{2\pi}{nm} = h\frac{2\pi}{n} + k\frac{2\pi}{m}$$

che è una richiesta equivalente a

$$1 = hm + kn$$

L'esistenza di tali coefficienti h e k è garantita dal *Lemma di Bezout*, essendo n, m coprimi. \square

Il *Lemma di Bezout*⁴ è uno strumento matematico di gran lunga successivo a Euclide, facendo la sua comparsa per la prima volta nel 1624 negli scritti del matematico francese Claude Gaspard Bachet de Méziriac. Ciò nonostante la costruzione del Pentadecagono, il 15-gono, presente negli *Elementi* si basa esattamente sul riconoscere che il doppio dell'angolo al centro del pentagono, meno quello del triangolo equilatero, corrisponde all'angolo al centro del 15-gono, cioè essenzialmente sulla determinazione dei coefficienti $h = 2$ e $k = -1$ per la coppia $n = 3$, $m = 5$ nel teorema precedente, come si vede in Figura 1.11.

Questo teorema costituisce dunque la naturale generalizzazione di un ragionamento "originale" di Euclide.

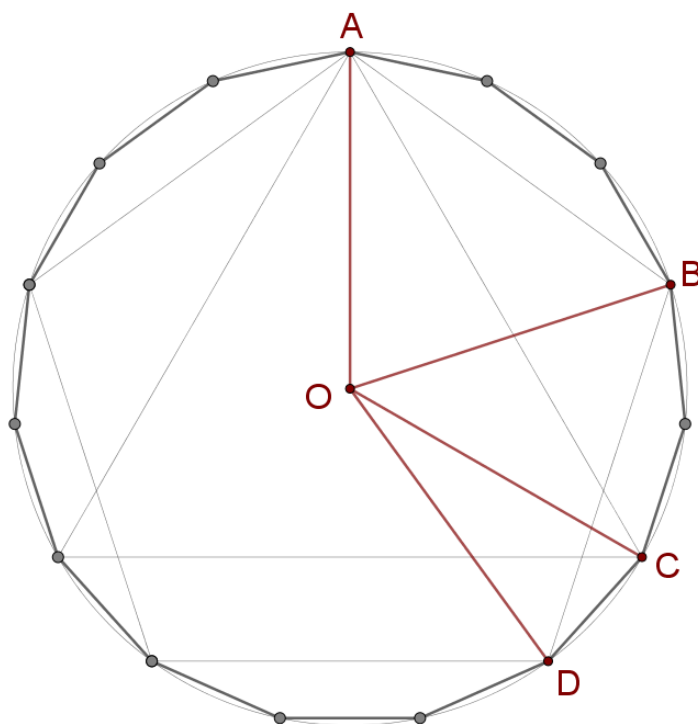


Figura 1.11: Costruzione del Pentadecagono Regolare

Il Teorema 1.11 fornisce informazioni principalmente sulla non costruibilità di determinati poligoni, nel senso che se non è costruibile il poligono con n lati allora non lo è nemmeno quello il cui numero di lati è un qualsiasi multiplo di n . I Teoremi 1.10 e 1.12 messi insieme invece danno:

Teorema 1.13.

Se in fattori primi $n = 2^k 3^\alpha 5^\beta$, con $k \in \mathbb{N}$ e $\alpha, \beta \in \{0, 1\}$, allora il n -gono è costruibile.

⁴Questo risultato è intitolato a Etienne Bezout, matematico francese del secolo XVIII, che lo dimostrò per i polinomi.

E con ciò ci prepariamo a un balzo in avanti di due millenni poiché, salvo gli interventi che anacronisticamente abbiamo anticipato, il problema è rimasto per moltissimo tempo congelato a questa risposta che è solo parziale. È infatti ora noto che se un poligono ha un certo numero di lati allora è costruibile, ma non c'è alcun modo per determinare se un poligono *non* sia costruibile, né se tutti i poligoni costruibili soddisfino questa proprietà.

Capitolo 2

LE DISQUISITIONES ARITHMETICAE

2.1 I risultati in Breve

Conviene cominciare togliendo tutta la sorpresa enunciando il risultato che chiude il capitolo.

Teorema 2.1 (Gauss-Wantzel).

Il n -gono è costruibile con riga e compasso se, e solo se:

$$n = 2^k p_1 \dots p_h$$

con $k, h \in \mathbb{N}$ e p_1, \dots, p_h primi di Fermat distinti.

Ricordiamo che i *Primi di Fermat* sono quei numeri primi della forma $2^s + 1$ per qualche $s \in \mathbb{N}$. Con un semplice argomento algebrico ci si può convincere che, se p è un primo di Fermat, l'esponente s deve essere a sua volta una potenza di 2. Infatti:

$$b \text{ dispari} \Rightarrow x^b + y^b = (x + y)(x^{b-1} - x^{b-2}y + \dots + y^{b-1})$$

Dunque se $s = ab, b \neq 1$ e b dispari allora:

$$q = 2^{ab} + 1 = (2^a)^b + 1^b = (2^a + 1)(2^{a(b-1)} - 2^{a(b-2)} + \dots + 1)$$

Che è assurdo sotto l'ipotesi che q sia un numero primo.

La somiglianza della condizione nel Teorema 1.13 con quella nel Teorema 2.1 è sorprendente, soprattutto alla luce del fatto che la via per estendere la prima alla seconda è fin da subito chiara grazie al Teorema 1.12 e al fatto che 3 e 5 sono, in effetti, *Primi di Fermat*. Se si dimostrasse che il p -gono è costruibile quando p è un primo di Fermat automaticamente si dedurrebbe la validità del Teorema 2.1, anche se solo nella direzione della sufficienza.

Questa è esattamente la conclusione raggiunta da Gauss nella settima e ultima sezione dell'opera *Disquisitiones Arithmeticae* del 1801, la cui edizione di riferimento è [Gau66], come conseguenza di

Teorema 2.2.

Sia p primo dispari e tale che $p - 1 = q_1^{\alpha_1} \dots q_h^{\alpha_h}$ in fattori primi. Allora risolvere l'equazione $x^p - 1 = 0$ è equivalente a risolvere α_1 equazioni di grado q_1 , α_2 equazioni di grado q_2 e così via fino a α_h equazioni di grado q_h .

Le equazioni predette dal Teorema 2.2 costituiscono un sistema ordinato secondo l'ordine *decrecente* dei fattori q_i in modo che i coefficienti di ciascun gruppo di α_i equazioni siano una *funzione razionale* delle soluzioni delle equazioni del gruppo precedente. Gauss non trae questa conclusione in modo esplicito. Essa piuttosto è resa evidente dallo sviluppo della teoria. Un esempio della determinazione dei polinomi associati a queste equazioni si trova in Sezione 2.4.

Poiché i numeri razionali sono tutti costruibili, così come lo sono combinazioni razionali di e le soluzioni di un'equazione di grado 2 a coefficienti costruibili sono ancora costruibili (vedremo la dimostrazione, che a Gauss era nota, nel prossimo capitolo) segue che

Teorema 2.3.

Se p è un primo di Fermat allora le soluzioni di $x^p - 1 = 0$ sono costruibili.

Costruire le soluzioni dell'equazione ciclotomica significa esattamente trovare i vertici del p -gono, quindi infine

Corollario 2.3.1.

Se p è un primo di Fermat il p -gono è costruibile.

Ci concentreremo dunque sulla dimostrazione del Teorema 2.2, che si articola in molteplici risultati intermedi il cui oggetto sono, in termini attuali, i *Periodi Gaussiani* e la *Teoria dei Residui*.

È degno di nota che i risultati di Gauss riportati nelle prossime pagine siano tutti modernamente parte della *Teoria di Galois*, nel contesto della quale la loro forma è più semplice, soprattutto nel formalismo, e il loro denominatore comune diventa, invece che un complesso approccio alla risoluzione di una classe di equazioni, la struttura delle estensioni di \mathbb{Q} note come *Campi Ciclotomici*.

La *Teoria di Galois*, le cui nozioni sono esposte postume per la prima volta da Liouville nel 1846, è successiva alle *Disquisitiones* e molto distante dal loro linguaggio. A Gauss va il merito, si potrebbe dire incredibile, di essersi sostanzialmente ricavato "a mano" risultati che ora sono ritenuti conseguenza di una Teoria molto più vasta e complessa.

2.2 La Teoria dei Residui

Nel lavoro di Gauss viene usata una notazione particolare, che introdurremo in parte più avanti, quando naturalmente si renderà necessaria. Questa notazione è qui riadattata, rispettando l'uso che se ne fa nelle *Disquisitiones*, per assecondare il contesto più generale di questa tesi e per inglobare altre notazioni comuni ma successive. Fin da subito:

- $r_k := e^{2i\frac{k}{p}\pi}$ è la k -esima soluzione all'equazione $x^p - 1 = 0$;
- Ω è l'insieme di quelle soluzioni, escluso il numero 1;
- $[\lambda] := r^\lambda$ con r una soluzione qualsiasi in Ω e $\lambda \in \mathbb{Z}$.

Il simbolo $[\lambda]$ non è definito del tutto fino alla scelta della radice r su cui si basa. Quando $\lambda < p$ ci riferiamo a $[\lambda]$ col termine *residuo*, poiché λ è il minimo rappresentante della classe di equivalenza $\{\lambda + kp \mid k \in \mathbb{Z}\}$.

Definizione 2.1 (Numero Primitivo).

Un numero g è detto Primitivo per il modulo p se:

$$\Omega = \{[1], [g], \dots, [g^{p-2}]\}$$

cioè se alle potenze di g corrispondono, eventualmente a meno dell'ordine, tutte le classi resto modulo p .

Esempio 2.1.

Per $p = 7$ il numero $h = 2$ non è primitivo, invece $g = 3$ sì.

esponente	0	1	2	3	4	5
residui per $h = 2$	1	2	4	1	2	4
residui per $g = 3$	1	3	2	6	4	5

Da questo esempio si intuisce come, modulo p , la successione delle potenze di qualsiasi residuo sia una successione periodica. L'*esponente* di un residuo h è il minimo $e \in \mathbb{N}$ tale che $h^e \equiv_p 1$ e in effetti $h^{n+e} \equiv_p h^n$ per qualsiasi $n \in \mathbb{N}$, cioè la successione è periodica. Un numero primitivo è dunque un residuo il cui esponente è $p - 1$.

Teorema 2.4.

Siano p primo e $\lambda \in \mathbb{Z}$. Si ha:

$$\sum_{n=0}^{p-1} [\lambda n] = \begin{cases} p & \text{se } p \mid \lambda \\ 0 & \text{se } p \nmid \lambda \end{cases}$$

Inoltre se $p \nmid \lambda$ si ha

$$\{[\lambda], [2\lambda], \dots, [(p-1)\lambda]\} = \Omega$$

Dimostrazione.

Se $p \mid \lambda$ allora $[\lambda] = 1$, mentre se $p \nmid \lambda$ si ha

$$\sum_{n=0}^{p-1} [n\lambda] = \sum_{n=0}^{p-1} [n]^\lambda = \left(\sum_{n=0}^{p-1} [n] \right)^\lambda = 0$$

Questo è vero perché, in termini di numeri complessi:

$$\sum_{n=0}^{p-1} e^{2ni\frac{\pi}{p}} = 0$$

Sempre se $p \nmid \lambda$ la funzione $[n] \mapsto [\lambda n]$ è ben definita, cioè mappa $\Omega \mapsto \Omega$, perché $k \equiv_p n \Rightarrow \lambda k \equiv_p \lambda n$. Basta provare che è iniettiva, poiché allora è anche suriettiva.

$$\begin{aligned} [\lambda n] = [\lambda m] &\Rightarrow p \mid \lambda(n - m) \\ &\Rightarrow p \mid (n - m) \\ &\Rightarrow [n] = [m] \end{aligned}$$

□

Corollario 2.4.1.

Se g è primitivo e $p \nmid \lambda$ allora

$$\Omega = \left\{ [\lambda], [\lambda g], \dots, [\lambda g^{p-2}] \right\}$$

Questo, a posteriori, significa che anche la successione (λg^n) deve essere periodica di periodo $p - 1$, ovvero $[\lambda g^n] = [\lambda g^m] \Leftrightarrow n \equiv_{p-1} m$. Inoltre, se $p - 1 = ef$ allora posto $h = g^e$ la sequenza

$$[1], [h], \dots, [h^{f-1}], [h^f], \dots$$

ha periodo f . Lo stesso deve valere per la successione (λh^n) i cui termini in ciascun periodo coincidono, a meno dell'ordine, con quelli della successione delle potenze del residuo h .

Questo fa giustamente sospettare che l'insieme degli elementi in un periodo di questa successione in realtà *non* dipenda dalla scelta del residuo primitivo g . In effetti vale

Teorema 2.5.

Se g, G sono due residui primitivi, $p - 1 = ef$ e $h = g^e$, $H = G^e$ allora

$$\left\{ [1], [h], \dots, [h^{f-1}] \right\} = \left\{ [1], [H], \dots, [H^{f-1}] \right\}$$

Dimostrazione.

sia $\mu < f$ qualsiasi. Proviamo $\exists \nu (h^\nu \equiv_p H^\mu)$.

Poiché g è primitivo deve essere $G = g^\omega$ per qualche ω opportuno. Prendiamo ν il residuo tale che $\nu \equiv_f \mu\omega$. In questo caso

$$h^\nu \equiv_p g^{e\nu} \equiv_p g^{e\mu\omega} \equiv_p G^{e\mu} \equiv_p H^\mu$$

□

Corollario 2.5.1.

Se $p \nmid \lambda$ allora

$$\{[\lambda], [\lambda h], \dots, [\lambda h^{f-1}]\} = \{[\lambda], [\lambda H], \dots, [\lambda H^{f-1}]\}$$

Esempio 2.2.

$p = 7, g = 3, G = 5, 7 - 1 = 3 \cdot 2, e = 2, f = 3.$

$$\begin{array}{c|cccccc|cccc} g^n & 1 & 3 & 2 & 6 & 4 & 5 & 1 & 3 & \dots \\ \hline G^n & 1 & 5 & 4 & 6 & 2 & 3 & 1 & 5 & \dots \end{array}$$

e si vede che il periodo è costituito dagli stessi elementi salvo l'ordine. Posto poi $h = 9 \equiv_7 2, H = 25 \equiv_7 4$ si osserva che di nuovo i periodi, a meno dell'ordine, sono gli stessi.

$$\begin{array}{c|ccc|ccc} h^n & 1 & 2 & 4 & 1 & 2 & \dots \\ \hline H^n & 1 & 4 & 2 & 1 & 4 & \dots \end{array}$$

Se infine si sceglie $\lambda = 3$ (cioè g^{e-1} , come vedremo non è un caso) si ottengono i residui rimanenti:

$$\begin{array}{c|ccc|ccc} \lambda h^n & 3 & 6 & 5 & 3 & 6 & \dots \\ \hline \lambda H^n & 5 & 6 & 3 & 5 & 6 & \dots \end{array}$$

Abbiamo così suddiviso l'insieme dei residui modulo p in due sottoinsiemi complementari e disgiunti. Questa suddivisione è operata seguendo le potenze periodiche di un residuo primitivo, ma **indipendentemente** dalla scelta di questo residuo. In effetti la suddivisione dipende unicamente dalla scelta di e e nella fattorizzazione di $p - 1$.

Nel suo lavoro Gauss si riferisce alla somma degli elementi di questi sottoinsiemi di radici dell'unità col nome di *periodum*. Nelle traduzioni e nei riferimenti successivi tali insiemi (e le somme dei loro elementi) sono ricordati come *periodi Gaussiani*. In tutto ciò il primo p è sottinteso.

Definizione 2.2 (Periodo Gaussiano).

Il simbolo (f, λ) denota allo stesso tempo, a seconda del contesto:

- la somma $[\lambda] + [\lambda h] + \dots + [\lambda h^{f-1}]$
- l'insieme $\{[\lambda], [\lambda h], \dots, [\lambda h^{f-1}]\}$

Facciamo alcune osservazioni:

1. $\lambda h^f \equiv_p \lambda$ dunque per qualsiasi $n < f$ si ha $(f, \lambda h^n) = (f, \lambda)$;
2. se μ è uno dei residui in (f, λ) allora $(f, \mu) = (f, \lambda)$;
3. di conseguenza, se due periodi hanno un residuo in comune allora coincidono;
4. se $\mu_1, \mu_2 \in (f, \lambda)$ allora $\frac{\mu_1}{\mu_2} = h^\nu$ per qualche $\nu < f$;
5. $\Omega = (p - 1, 1)$.

Teorema 2.6.

Con le notazioni precedenti se p è primo, $p - 1 = ef$ e g è primitivo per il modulo p allora:

$$\Omega = \bigcup_{n=0}^{e-1} (f, g^n)$$

Alla luce dell'osservazione 5 questo teorema, oltre che dare informazioni sulla struttura delle soluzioni all'equazione ciclotomica, significa anche che, rispetto ai suoi sottoperiodi, possiamo scomporre un periodo come segue:

$$(ef, \lambda) = \begin{bmatrix} (f, \lambda) \\ (f, \lambda g) \\ \vdots \\ (f, \lambda g^{e-1}) \end{bmatrix}$$

e questo algoritmo è iterabile.

Esempio 2.3.

$p = 19$, $p - 1 = 2 \cdot 3 \cdot 3$, usando $g = 2$.

$$\Omega = (18, 1) = \begin{bmatrix} (9, 1) = \begin{bmatrix} (3, 1) \\ (3, 4) \\ (3, 16) \end{bmatrix} \\ (9, 2) = \begin{bmatrix} (3, 2) \\ (3, 8) \\ (3, 13) \end{bmatrix} \end{bmatrix}$$

che esplicitamente, dove ovunque si intende che il numero rappresenta il residuo della sua classe, corrisponde a:

$$\Omega = \begin{bmatrix} 1, 4, 16, 7, 9, 17, 11, 6, 5 \\ 2, 8, 13, 14, 18, 15, 3, 12, 10 \end{bmatrix} = \begin{bmatrix} 1, 7, 11 \\ 4, 9, 6 \\ 16, 17, 5 \\ 2, 14, 3 \\ 8, 18, 12 \\ 13, 15, 10 \end{bmatrix}$$

Teorema 2.7.

Sia $(f, \lambda_1) = [\lambda_1] + \cdots + [\lambda_{f-1}]$. Allora

$$(f, \lambda_1)(f, \mu) = (f, \lambda_1 + \mu) + \cdots + (f, \lambda_{f-1} + \mu)$$

Dimostrazione.

Fattorizziamo $p - 1 = ef$, prendiamo g primitivo e $h = g^e$. Scegliamo $\lambda = \lambda_i$ per un i qualsiasi.

$$\begin{aligned} (f, \lambda)(f, \mu) &= (f, \lambda)([\mu] + \cdots + [\mu h^{f-1}]) \\ &= \begin{array}{ccccccc} [\lambda + \mu] & + & [\lambda h + \mu] & + & \cdots & + & [\lambda h^{f-1} + \mu] \\ + & & [\lambda h + \mu h] & + & [\lambda h^2 + \mu h] & + & \cdots & + & [\lambda + \mu h] \\ & & \vdots & & \vdots & & \vdots & & \\ + & & [\lambda h^{f-1} + \mu h^{f-1}] & + & [\lambda + \mu h^{f-1}] & + & \cdots & + & [\lambda h^{f-2} + \mu h^{f-1}] \\ & & \downarrow & & \downarrow & & \downarrow & & \\ = & & (f, \lambda + \mu) & + & (f, \lambda h + \mu) & + & \cdots & + & (f, \lambda h^{f-1} + \mu) \end{array} \end{aligned}$$

che è la tesi, a meno dell'ordine degli addendi. \square

Ciò che è importante capire è che questo teorema essenzialmente rappresenta il prodotto di periodi simili (f, λ) , (f, μ) come una combinazione lineare dei periodi $(f, 0)$, (f, g^i) , poiché in effetti ciascun periodo della forma $(f, \lambda + \mu)$ corrisponde a:

- $(f, 0) = \underbrace{[0] + \cdots + [0]}_{f \text{ volte}} = f$ perché $[0] = r^0 = 1$ a prescindere dalla scelta di r oppure
- (f, g^i) per qualche $i \in \{0, \dots, e-1\}$, che sono tutti ottenuti da $(f, 1)$ moltiplicando ciascun addendo per g^i , come nel Teorema 2.5 e l'osservazione che ne segue.

Vedremo tra poco come questo implichi che qualsiasi periodo di lunghezza f , ossia della forma (f, λ) , si possa esprimere come polinomio a coefficienti *razionali* nel periodo $(f, 1)$.

Quanto osservato si riassume formalmente in

Corollario 2.7.1.

Esistono coefficienti $\beta, \alpha_0, \dots, \alpha_{e-1} \in \mathbb{Z}$ tali che:

$$(f, \lambda)(f, \mu) = \beta f + \alpha_0(f, 1) + \alpha_1(f, g) + \cdots + \alpha_{e-1}(f, g^{e-1})$$

Inoltre $\forall k \in \mathbb{Z}$:

$$(f, k\lambda)(f, k\mu) = \beta f + \alpha_0(f, k) + \alpha_1(f, kg) + \cdots + \alpha_{e-1}(f, kg^{e-1})$$

Infine questo risultato si può estendere a prodotti arbitrari finiti di periodi simili.

Ancora più in generale in tale forma di combinazione lineare si possono esprimere *funzioni razionali algebriche intere* di periodi simili. Una tale funzione è

$$\Phi(\underline{x}) = \sum_{k \in \mathbb{N}^h} \alpha_k \underline{x}^k$$

dove k è un *multi-indice*, $\underline{x} = \{x_1, \dots, x_h\}$ e $\alpha_k \in \mathbb{Z}$.

Corollario 2.7.2.

Se alle variabili di una funzione Φ come sopra sostituiamo periodi simili il risultato è ancora una funzione nella forma del Corollario 2.7.1.

A questo punto siamo in grado di mettere in relazione questa teoria dei *periodi di gaussiani* con quella dei polinomi e tornare al problema della ciclotomia. Come promesso infatti

Teorema 2.8.

Supponiamo $p \nmid \lambda$ e chiamiamo $z = (f, \lambda)$. Qualsiasi periodo (f, μ) simile a z si può scrivere come:

$$(f, \mu) = \beta + \alpha_1 z + \alpha_2 z^2 + \dots + \alpha_{e-1} z^{e-1}$$

per opportuni coefficienti $\beta, \alpha_1, \dots, \alpha_{e-1} \in \mathbb{Q}$.

Si noti che in particolare $p \nmid 1$ dunque si può assumere $z = (f, 1)$, ma questo non è rilevante per le conseguenze sulla risolubilità dell'equazione ciclotomica.

Dimostrazione. (parziale)

Chiamiamo $z_i := (f, \lambda g^i)$ per $i = 1, \dots, e-1$. Sappiamo dal Teorema 2.6 che Ω si ripartisce nei periodi z, z_1, \dots, z_{e-1} . Si ha, indipendentemente da λ grazie al Teorema 2.4:

$$1 + z + z_1 + z_2 + \dots + z_{e-1} = \sum_{n=1}^{p-1} [n] \equiv_p 0 \quad (2.1)$$

Senza perdere di generalità possiamo assumere $(f, \mu) = z_1$ e, siccome le potenze di z si esprimono come combinazione lineare affine (può esserci un termine "noto", il coefficiente di $(f, 0)$) dei periodi z, z_1, \dots, z_{e-1} , è possibile eliminare in (2.1) le dipendenze da z_2, \dots, z_{e-1} in favore delle potenze di z . Questo porta a

$$B + \sum_{i=1}^{e-1} A_i z^i + C(f, \mu) = 0$$

A questo punto la tesi è immediata se $C \neq 0$. L'ipotesi che C sia nullo è assurda poichè in questo caso si sarebbe trovato che per una scelta di coefficienti razionali opportuna il polinomio

$$\sum_{n=0}^{e-1} a_n x^n$$

sarebbe un divisore di $1 + x + x^2 + \dots + x^{p-1}$. Questo è inconsistente, poichè i polinomi ciclotomici sono irriducibili e non hanno pertanto divisori di questo tipo. Omettiamo i dettagli. \square

Facciamo un'ulteriore osservazione chiave necessaria a proseguire il ragionamento di Gauss. Se in un *polinomio simmetrico elementare* di f variabili sostituiamo gli f residui che compongono il periodo (f, λ) questo si riduce ad un'espressione della forma

$$\alpha + \alpha_1[1] + \alpha_2[2] + \dots + \alpha_{p-1}[p-1] \quad (2.2)$$

Teorema 2.9.

In (2.2) residui appartenenti allo stesso periodo gaussiano (f, λ) hanno lo stesso coefficiente.

Questo significa che anche (2.2) è riducibile alla forma di combinazione presente nel Corollario 2.7.1.

Dimostrazione.

Siano $[s], [q] \in (f, \lambda)$ e ν minimo tale che $q = sh^\nu$. Supponiamo

$$(f, \lambda) = [\lambda_1] + [\lambda_2] + \dots + [\lambda_{f-1}]$$

Chiamiamo μ_i il residuo di $\lambda_i h^\nu$ modulo p , così che

$$(f, \lambda) = [\mu_1] + [\mu_2] + \dots + [\mu_{f-1}]$$

anche se non necessariamente nello stesso ordine. Se φ è un polinomio simmetrico elementare di f variabili e

$$\varphi([\lambda_1], \dots, [\lambda_{f-1}]) = (2.2)$$

grazie al Corollario 2.7.1 si ha

$$\varphi([\lambda_1 h^\nu], \dots, [\lambda_{f-1} h^\nu]) = \alpha + \alpha_1[h^\nu] + \alpha_2[2h^\nu] \dots + \alpha_{p-1}[(p-1)h^\nu]$$

allora evidentemente α_s è il coefficiente:

- di $[q]$ nell'ultima equazione;
- di $[s]$ in (2.2);

ma siccome φ è simmetrica

$$\varphi([\lambda_1 h^\nu], \dots, [\lambda_{f-1} h^\nu]) = \varphi([\mu_1], \dots, [\mu_{f-1}]) = \varphi([\lambda_1], \dots, [\lambda_{f-1}])$$

\square

Ricordando infine che i coefficienti di un polinomio sono ordinatamente i polinomi simmetrici elementari calcolati nelle sue radici si deduce che

Corollario 2.9.1.

I coefficienti del polinomio (di grado f) le cui radici sono i residui in (f, λ) sono tutti riducibili ad un'espressione polinomiale nelle potenze del periodo (f, λ) , come indicato dal Teorema 2.8.

Poiché l'insieme delle radici dell'unità Ω è ripartito in e periodi di lunghezza f , questo significa che tali radici sono ricavabili come soluzioni di e equazioni di grado f , non appena una delle somme (f, λ) , e di conseguenza tutte quelle di periodi simili, è nota. Per semplicità, come già osservato, si può assumere che questo sia vero non appena è nota la somma $(f, 1)$.

2.3 Determinare i Periodi Gaussiani

Il percorso logico di Gauss trova conclusione estendendo agli interi periodi (f, λ) l'argomento del Teorema 2.9 passando attraverso il Corollario 2.7.2.

Contrariamente alle singole radici, tuttavia, alcuni valori di particolari periodi sono facilmente determinabili algebricamente. Per esempio $(p-1, 1) = -1$ per il Teorema 2.4, oppure ancora i periodi di lunghezza 2 si ha $(2, \lambda) = 2 \cos(\theta)$, dove θ è l'argomento della radice dell'unità associata a $[\lambda]$. Questo è vero perché i periodi di lunghezza 2 devono essere costituiti da una radice e dalla sua coniugata¹.

Supponiamo che $p-1 = abc$. Grazie al Teorema 2.6 sappiamo che (bc, λ) si scompone in b sottoperiodi di lunghezza c , i residui di ciascuno di questi differendo dai componenti degli altri per un fattore g^a .

Prendiamo nuovamente un polinomio simmetrico elementare, stavolta di b variabili, e chiamiamolo φ . Per il Corollario 2.7.2 sostituendo i sottoperiodi $(c, \lambda), (c, \lambda g^a), \dots, (c, \lambda g^{a(b-1)})$ in φ si ottiene una combinazione lineare del tipo:

$$A + \alpha_0(c, \lambda) + \alpha_1(c, \lambda g) + \dots + \alpha_{a(b-1)}(c, \lambda g^{a(b-1)}) + \dots + \alpha_{ab-1}(c, \lambda g^{ab-1}) \quad (\star)$$

¹Questo è evidente nell'esempio di Sezione 2.4 guardando all'albero dei sottoperiodi di Ω . È un fatto di natura generale la cui validità non è fondamentale per la teoria, dunque non vale la pena soffermarvisi

Teorema 2.10.

Sotto le ipotesi appena assunte, in (\star) i sottoperiodi che compongono lo stesso periodo (bc, λ) hanno lo stesso coefficiente.

Dimostrazione.

Sappiamo che $(bc, \lambda) = (bc, \lambda g^a)$ dunque i sottoperiodi di $(c, \lambda g^a)$ coincidono con quelli di (c, λ) a meno dell'ordine e di conseguenza la sostituzione dei primi o dei secondi in φ deve rendere lo stesso risultato, ovvero (\star) . Nel primo caso, tuttavia, quello che si ottiene è:

$$A + \alpha_0(c, \lambda g^a) + \alpha_1(c, \lambda g^{a+1}) + \cdots + \alpha_{a(b-1)}(c, \lambda) + \cdots + \alpha_{ab-1}(c, \lambda g^{a(b+1)-1}) \quad (\star\star)$$

e questo perché $(c, \lambda g^{ab}) = (c, \lambda)$.

Si vede allora, dal confronto di (\star) e $(\star\star)$, che tutti i sottoperiodi della forma $(c, \mu g^{ka})$, al variare di $k = 0, \dots, b-1$, devono avere lo stesso coefficiente. Questi sottoperiodi, di nuovo dal Teorema 2.6, sono esattamente quelli che compongono il periodo (bc, λ) . \square

Corollario 2.10.1.

Se $p-1 = ef$ tutti i sottoperiodi (f, λ) si riferiscono allo stesso periodo $(p-1, 1)$ e hanno di conseguenza tutti lo stesso coefficiente in (\star) . Si ha dunque

$$(\star) = A + \alpha(p-1, 1) = A - \alpha$$

I periodi (f, λ) sono quindi le radici di un polinomio di grado e i cui coefficienti sono determinabili numeri *reali*. Si noti che i coefficienti delle combinazioni di periodi erano con sicurezza *razionali* fino al Teorema 2.8. Le somme dei singoli periodi, tuttavia, non sono vincolate ad appartenere a \mathbb{Q} .

2.4 Un Esempio Celebre: L'Eptadecagono

Poiché, come spesso accade, la teoria è incredibilmente più nebulosa degli esempi in cui viene applicata, ci facciamo accompagnare da Gauss nel caso $p = 17$. La costruzione del 17-gono, o Eptadecagono, venne individuata dal diciannovenne Gauss nel 1796, 5 anni prima della pubblicazione delle *Disquisitiones Arithmeticae*. La leggenda vuole che il desiderio di Gauss fosse di avere questa costruzione incisa sulla sua pietra tombale nel cimitero di Göttingen, ma che lo scultore a cui il compito fu assegnato si sia rifiutato ritenendolo "uno sforzo eccessivo per tracciare un cerchio".

Cominciamo con lo scomporre l'insieme di radici $\Omega = (16, 1)$ nei suoi sottoperiodi.

$$(16, 1) = \begin{cases} (8, 1) = \begin{cases} (4, 1) = \begin{cases} (2, 1) = [1] + [16] \\ (2, 13) = [4] + [13] \end{cases} \\ (4, 9) = \begin{cases} (2, 9) = [8] + [9] \\ (2, 15) = [2] + [15] \end{cases} \end{cases} \\ (8, 3) = \begin{cases} (4, 3) = \begin{cases} (2, 3) = [3] + [14] \\ (2, 5) = [5] + [12] \end{cases} \\ (4, 10) = \begin{cases} (2, 10) = [7] + [10] \\ (2, 11) = [6] + [11] \end{cases} \end{cases} \end{cases}$$

Procediamo ora a determinare i coefficienti delle equazioni polinomiali le cui soluzioni sono i periodi in ciascuna parentesi quadra. Vogliamo determinare la misura, nel senso proprio di lunghezza di un segmento, $\cos(\frac{2\pi}{17})$. Se questa misura è costruibile anche l'angolo $\frac{2\pi}{17}$ risulta costruibile e con esso il 17-gono. Nel 1801 Gauss fece questi conti a mano, d'altra parte lui era il *Principe dei Matematici*, dunque non vale la pena entrarci in competizione.

Il Teorema 2.2 ci prospetta la necessità di risolvere 4 equazioni di grado 2. Vedremo tra un attimo come i coefficienti di ciascuna di queste equazioni dipendano dalle soluzioni delle precedenti. Il valore $\cos(\frac{2\pi}{17})$, che come si è già osservato coincide con $\frac{(2,1)}{2}$ se si sceglie $r = e^{i\frac{2\pi}{17}}$ (si veda la definizione del simbolo $[\lambda]$ all'inizio di Sezione 2.2), sarà dunque una combinazione razionale di radici quadrate ragionevolmente complessa, che tuttavia vogliamo visualizzare in forma esatta e non in approssimazione numerica. Facciamo quindi uso di un software CAS², presentando i risultati ma omettendo alcuni dettagli che riempirebbero la pagina di conti il cui unico senso è semplificare tali espressioni.

L'equazione le cui radici sono i periodi (8, 1) e (8, 3) ha per coefficienti:

$$\begin{aligned} (8, 1) + (8, 3) &= -1 \\ (8, 1)(8, 3) &= -4 \end{aligned} \implies x^2 + x - 4 = 0 \quad (\heartsuit)$$

Similmente per i periodi di lunghezza 4 si ottiene:

$$\begin{aligned} (4, 1) + (4, 9) &= (8, 1) \\ (4, 1)(4, 9) &= -1 \end{aligned} \implies x^2 - (8, 1)x - 1 = 0 \quad (\diamondsuit)$$

$$\begin{aligned} (4, 3) + (4, 10) &= (8, 3) \\ (4, 3)(4, 10) &= -1 \end{aligned} \implies x^2 - (8, 3)x - 1 = 0 \quad (\clubsuit)$$

²Computer Algebra System, un tipo di software che esegue operazioni algebriche in maniera simbolica.

Per i periodi di lunghezza 2 è sufficiente un'unica equazione, cioè quella fra le cui soluzioni si trova $(2, 1)$:

$$\begin{aligned} (2, 1) + (2, 13) = (4, 1) & \implies x^2 - (4, 1) + (4, 3) = 0 & (\spadesuit) \\ (2, 1)(2, 13) = (4, 3) & \end{aligned}$$

Risolviamo le equazioni nell'ordine in cui sono state ricavate :

$$(\heartsuit) \quad \begin{cases} (8, 1) = \frac{1}{2}(\sqrt{17} - 1) \\ (8, 3) = -\frac{1}{2}(\sqrt{17} + 1) \end{cases}$$

$$(\diamondsuit) \quad (4, 1) = \frac{1}{4}(\sqrt{17} - 1 + \sqrt{34 - 2\sqrt{17}})$$

$$(\clubsuit) \quad (4, 3) = \frac{1}{4}(-\sqrt{17} - 1 + \sqrt{34 + 2\sqrt{17}})$$

Possiamo infine usare l'ultima equazione per determinare $\cos(\frac{2\pi}{17})$:

$$\begin{aligned} (\spadesuit) \quad \frac{(2, 1)}{2} &= \frac{1}{16}(\sqrt{17} - 1 + \sqrt{34 - 2\sqrt{17}}) + \\ &+ \frac{1}{8}(\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}) \end{aligned}$$

Siccome anche l'occhio vuole la sua parte proponiamo nella prossima pagina una possibile costruzione dell'Eptadecagono, tralasciando le linee di costruzione necessarie a determinare oggetti comuni come assi e bisettrici e tracciando di ciascuna linea solo la porzione necessaria.

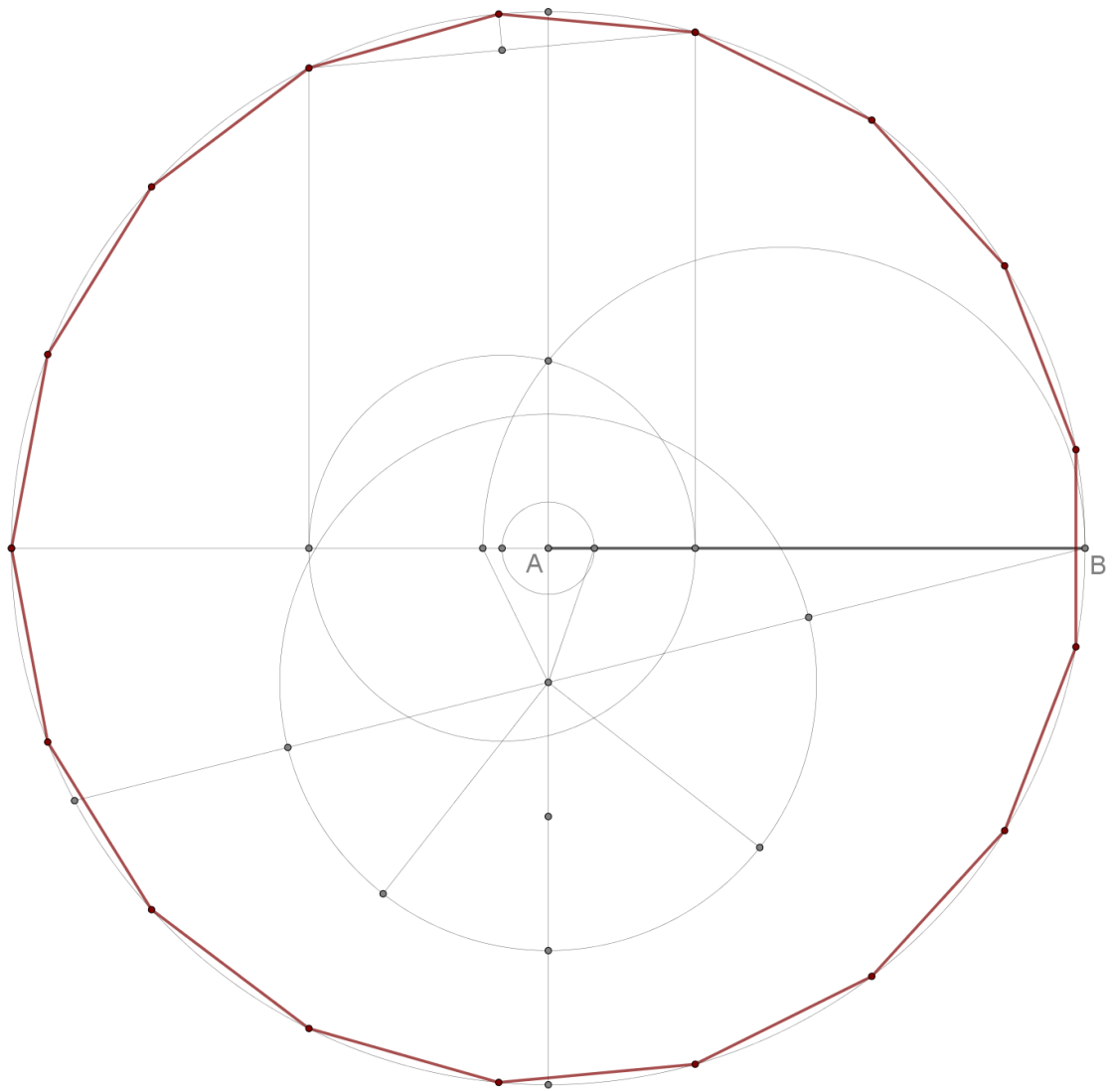


Figura 2.1: Una Costruzione dell'Eptadecagono

Capitolo 3

WANTZEL E GALOIS

3.1 La Condizione Sufficiente

Riassumiamo in breve il punto della situazione. Solo una parte del Teorema 2.1 è stata dimostrata, cioè l'implicazione della sufficienza. L'argomento di Gauss si è sviluppato sostanzialmente come segue:

- I. è possibile raddoppiare il numero di lati di qualsiasi poligono costruibile (Teorema 1.10);
- II. è possibile costruire il poligono che ha per numero di lati il prodotto del numero dei lati di altri due poligoni costruibili, purché queste due quantità siano coprime (Teorema 1.12);
- III. le soluzioni di equazioni di grado 2 a coefficienti costruibili sono ancora costruibili;
- IV. i numeri razionali sono costruibili e risolvere la p -esima equazione ciclotomica è equivalente a risolvere una serie di equazioni i cui gradi corrispondono ai fattori primi di $p - 1$ (Teorema 2.2);
- V. se $p - 1$ è una potenza di 2, cioè se p è un *Primo di Fermat*, le soluzioni dell'equazione $x^p - 1 = 0$ sono costruibili e dunque è costruibile il p -gono;
- VI. il n -gono è costruibile se n si fattorizza in potenze di 2 e primi di Fermat distinti.

Viceversa non è ancora chiaro se la costruibilità del n -gono implichi che n si fattorizzi come nel Teorema 2.1, cioè non è chiaro se esistano *altri* poligoni regolari costruibili *diversi* da quelli previsti dal ragionamento di Gauss.

In questo capitolo vedremo esplicitamente la dimostrazione del punto III e della costruibilità dell'intero campo \mathbb{Q} , che a Gauss erano entrambe note. Studieremo

queste dimostrazioni usando un formalismo che è successivo al lavoro di Gauss, cioè quello della teoria delle *estensioni di campi*, in particolare di \mathbb{Q} , e della Teoria di Galois.

Vedremo anche la dimostrazione del fatto che, in effetti, i poligoni costruibili sono *esclusivamente* quelli il cui numero di lati si fattorizza come nel punto VI. Questo argomento è dovuto al lavoro del matematico francese Pierre Wantzel. Non analizzeremo in modo preciso questo contributo poiché il suo contenuto è parafrasabile con sorprendente aderenza nel linguaggio moderno che abbiamo deciso di adottare, la cui potenza si rivelerà tale da permetterci di ridurre l'argomento di Wantzel al calcolo di una funzione.

Riassumiamo comunque, di nuovo per punti, il modo in cui Wantzel dimostrò che la condizione individuata da Gauss è *necessaria*, in modo da constatarne la simmetria con la dimostrazione che costruiremo nel resto del capitolo:

- I. qualsiasi algoritmo di costruzione di un segmento o di un angolo è riducibile ad una ricorsione di intersezioni di rette e cerchi;
- II. da un punto di vista algebrico intersecare rette e cerchi significa risolvere equazioni di grado 2 i cui coefficienti dipendono dai punti di passaggio di queste linee;
- III. se una quantità è costruibile allora è soluzione di un sistema *ordinato* di equazioni di grado 2, i coefficienti di ciascuna dipendendo dalle soluzioni delle precedenti;
- IV. un tale sistema di equazioni di grado 2 corrisponde ad una singola equazione di ordine una potenza di 2;
- V. le radici p -esime dell'unità, con p primo, sono soluzioni di equazioni di grado $p - 1$ e il ragionamento si può limitare senza perdere di generalità all'ipotesi di costruibilità dei poligoni il cui numero di lati è un numero primo (Teorema 1.11);
- VI. se il p -gono è costruibile allora lo sono le radici p -esime dell'unità e di conseguenza $p - 1$ è una potenza di 2, cioè un primo di Fermat.

3.2 Il Campo dei Numeri Costruibili

Definizione 3.1 (Numero Costruibile).

Un numero $\alpha \in \mathbb{R}$ è detto costruibile se è la lunghezza di un segmento costruibile con riga e compasso.

Indichiamo con \mathbb{E} l'insieme dei numeri costruibili in onore di Eulero. Ci diamo l'obiettivo di dimostrare il seguente

Teorema 3.1.

\mathbb{E} è un'estensione intermedia tra i campi \mathbb{Q} e \mathbb{R} chiusa per radici quadrate, cioè:

$$\alpha \in \mathbb{E} \wedge \alpha > 0 \Rightarrow \sqrt{\alpha} \in \mathbb{E}$$

La dimostrazione è articolata e risulta più ordinata se suddivisa in sezioni. Occorre dimostrare che \mathbb{E} :

- è chiuso per somme e per differenze;
- è chiuso per prodotti;
- ha inversi moltiplicativi per ogni suo elemento (e dunque è chiuso per rapporti);
- contiene \mathbb{Q} ;
- è chiuso per radici quadrate.

La commutatività delle operazioni risulterà evidente dagli algoritmi di costruzione così come l'esistenza di inversi additivi arbitrari, una volta identificato il numero 0, che è neutro per l'addizione, con il segmento di lunghezza nulla.

Dal momento che ogni costruzione prende il via dalla presenza postulata di una coppia di punti possiamo assumere, chiamati questi O e U (per *zero* e *uno*), che la loro distanza reciproca corrisponda alla lunghezza 1.

Chiusura per Addizioni e Sottrazioni

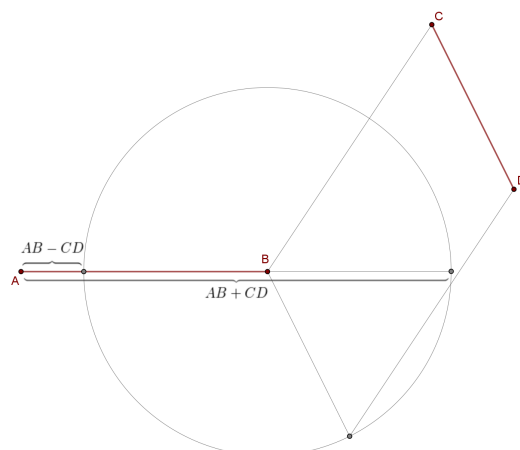


Figura 3.1: Somma di due Lunghezze

Supponiamo costruiti due segmenti AB e CD , in posizione relativa arbitraria nel piano. Assumiamo che CD sia il segmento più corto, cosa che possiamo controllare usando il compasso. Prolunghiamo AB dal lato di B e descriviamo con centro in B la circonferenza di raggio CD . Questa incontra AB e il suo prolungamento in due punti, uno interno al segmento, uno esterno: i segmenti i cui estremi sono questi e A corrispondono rispettivamente alla somma e alla differenza dei segmenti AB e CD .

Chiusura per Prodotti

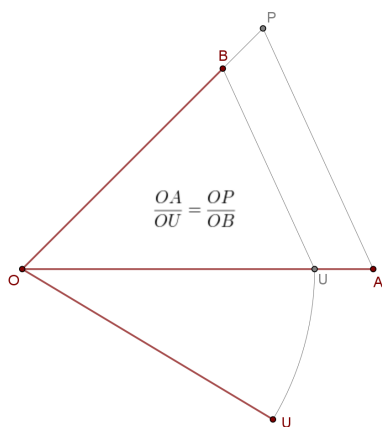


Figura 3.2: Prodotto di due Lunghezze

Assegnati due segmenti ne riportiamo le lunghezze, usando [L1P31](#), in modo che i nuovi segmenti abbiano un estremo comune in O . Chiamiamo i due segmenti OA e OB . Riportiamo col compasso la misura OU unitaria su OA e congiungiamo U con B , dopodiché individuamo in P l'intersezione della parallela a UB per il punto A

e del prolungamento di OB dal lato di B . Si sono costruiti così due triangoli simili OUB e OAP che realizzano la proporzione:

$$\frac{OA}{OU} = \frac{OP}{OB} \Rightarrow OA \cdot OB = OP \cdot OU = OP^2$$

Il punto P individua dunque il segmento OP la cui lunghezza è il prodotto delle lunghezze di OA e OB . Si noti che nel caso di $OB = OU$ questa costruzione prova che OU è elemento neutro per il prodotto.

Inversi Moltiplicativi e Chiusura per Rapporti

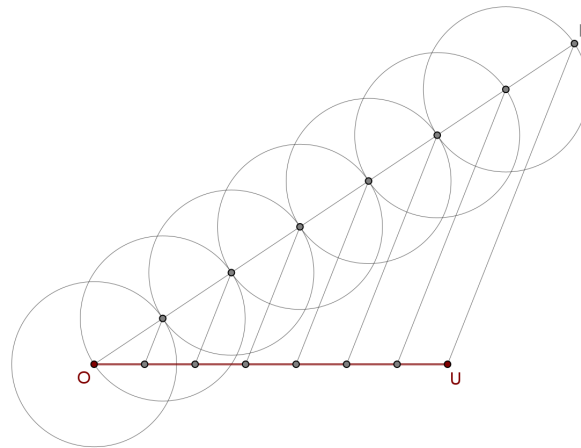


Figura 3.3: Suddivisione del Segmento Unitario per $n = 7$

Vogliamo costruire la lunghezza $\frac{1}{n}$, $n \in \mathbb{N}$. Tracciamo da O una semiretta arbitraria, cioè nella direzione di qualsiasi altro punto costruibile distinto da U . Con un'apertura fissata, e indipendentemente da questa, iterativamente individuiamo su quella semiretta n punti, ciascuno equidistante dal precedente. Congiungiamo il n -esimo punto, diciamo N , con U e tracciamo per ciascun punto della successione le parallele a NU . I punti di intersezione individuati su OU dividono il segmento unitario in n parti uguali per **L6P2** e ciascuna di queste parti misura $\frac{1}{n}$.

Poiché \mathbb{E} è chiuso per prodotti e contiene tutti gli inversi moltiplicativi dei numeri interi¹ contiene anche tutti i numeri razionali \mathbb{Q} .

Abbiamo così dimostrato che l'insieme \mathbb{E} è un campo intermedio tra \mathbb{Q} e \mathbb{R} .

¹I numeri negativi sono interpretati ancora come lunghezze di segmenti, ma con gli estremi invertiti. Equivalentemente sono il risultato della costruzione di una differenza fra lunghezze in cui il secondo segmento ha lunghezza maggiore.

Chiusura per Radici Quadrate

Supponiamo di aver costruito un segmento AO . Basandoci su L6P13 ripetiamo la costruzione in Figura 1.4 con $BC = OU$. In questo caso il punto D , individuato come intersezione della perpendicolare per O e la semicirconferenza di diametro AU (in figura rispettivamente la perpendicolare per B alla semicirconferenza di diametro AC), soddisfa:

$$OD^2 = AO \cdot OU = AO \Rightarrow OD = \sqrt{AO}$$

A questo punto la dimostrazione del Teorema 3.1 è conclusa.

Chiudiamo questa sezione con una considerazione molto importante che, come abbiamo anticipato, era nota anche a Gauss nel suo lavoro.

Corollario 3.1.1.

Se $a, b, c \in \mathbb{E}$ allora le soluzioni di $ax^2 + bx + c = 0$ sono anch'esse numeri costruibili.

Dimostrazione.

Le soluzioni sono date da

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \quad (3.1)$$

dunque $x_1, x_2 \in \mathbb{E}$ perché \mathbb{E} è un campo chiuso per radici quadrate. \square

Esiste un metodo grafico molto elegante, di cui un esempio si trova in Figura 5.4, per risolvere con riga e compasso qualsiasi equazione quadratica a coefficienti costruibili che ammetta almeno una radice reale, senza dover passare per la costruzione di tutte le quantità che figurano nella formula (3.1).

3.3 L'Argomento di Wantzel

All'inizio del capitolo abbiamo accennato all'intuizione di Wantzel che ogni numero costruibile fosse, in un qualche senso che dipende dalla struttura della sua costruzione con riga e compasso, la soluzione di un sistema ordinato di equazioni di grado 2.

Il linguaggio della *Teoria di Galois* permette di esprimere questo fatto in un modo conciso utilizzando la nozione di *estensione* di un campo. Ricordiamo alcuni risultati senza riportarne la dimostrazione.

Pochi Richiami

Se un campo K è contenuto in un secondo campo L si dice che L *estende* K . In questo caso L è uno spazio vettoriale a coefficienti in K la cui dimensione è detta *grado* dell'estensione. Il simbolo per il grado di un'estensione è:

$$[K(\alpha) : K] := \deg_K K(\alpha)$$

L'estensione di K generata di un elemento α , indicata con $K(\alpha)$, è il minimo campo contenente sia K che l'elemento α . In questo caso il grado dell'estensione coincide col grado del *polinomio minimo* di α rispetto al campo K , vale a dire il minimo polinomio, rispetto al grado, a coefficienti in K e che abbia α come radice. Questo polinomio è essenzialmente unico.

Poiché $[K(\alpha) : K] = 1$ succede se e solo se $\alpha \in K$, il grado minimo di un'estensione propria di K è 2. Questo accade appena $\alpha \notin K$ ed esiste un polinomio di grado 2 qualsiasi a coefficienti in K ad avere α come radice, perché allora quel polinomio è minimo per α . Se $[K(\alpha) : K] = n$ una base dello spazio vettoriale su $K(\alpha)$ su K è:

$$\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$$

Ricordiamo infine che se $K \leq M \leq L$, cioè M è un campo intermedio tra K e L , allora:

$$[M : K] \mid [L : K]$$

Dalla Costruzione alla Struttura Algebrica

Traduciamo in operazioni algebriche le costruzioni di rette e cerchi. Abbiamo già identificato la coppia di punti iniziali O, U come gli estremi del segmento unitario. Possiamo pertanto assumere che O e U corrispondano ai punti $O = (0, 0)$ e $U = (0, 1)$ del piano cartesiano, che possiamo identificare all'occorrenza con \mathbb{R}^2 o con \mathbb{C} . Un numero $\zeta \in \mathbb{C}$ è costruibile se lo è come punto geometrico nel piano di Gauss.

Teorema 3.2.

Un punto $P \in \mathbb{R}^2$ è costruibile se, e solo se, le sue coordinate sono due numeri costruibili. Equivalentemente un numero $\zeta \in \mathbb{C}$ è costruibile se e solo se sono costruibili le sue parti reale e immaginaria.

Dimostrazione.

Possiamo restringerci al caso di \mathbb{R}^2 , quello di \mathbb{C} è analogo. Identifichiamo gli assi cartesiani con la retta $O \vee U$ e con la perpendicolare a questa nel punto O . Se P è costruibile allora sono costruibili i piedi P_x e P_y delle perpendicolari da P agli assi cartesiani. Sono dunque costruibili i segmenti OP_x e OP_y , le cui lunghezze sono le coordinate del punto P .

Viceversa se sono costruibili le lunghezze che corrispondono alle coordinate di P queste possono essere riportate sugli assi cartesiani centrando il compasso in O e individuando così i punti P_x e P_y in modo che OP_x corrisponda all'ascissa di P e OP_y alla sua ordinata. Le perpendicolari agli assi cartesiani nei punti P_x e P_y sono incidenti in P . \square

Supponiamo che A, B siano punti costruibili, mantenendo la convenzione degli indici x, y per le loro coordinate. L'equazione della retta $A \vee B$ che passa per questi

due punti si può scrivere come:

$$y - A_y = \frac{A_y - B_y}{A_x - B_x}(x - A_x)$$

Questa è un'equazione i cui coefficienti sono funzioni razionali delle coordinate dei punti di passaggio, che sono numeri costruibili.

Similmente se sono costruibili il punto C e un qualsiasi segmento di lunghezza R allora la circonferenza di centro C e raggio R ha equazione:

$$(x - C_x)^2 + (y - C_y)^2 = R^2$$

che di nuovo ha coefficienti che sono una funzione razionale di quantità costruibili. Questi coefficienti sono dunque a loro volta numeri costruibili, poiché come abbiamo visto nel Teorema 3.1 \mathbb{E} è un campo.

Vi sono tre possibili configurazioni con cui si identifica un punto costruibile P , cioè l'incidenza di:

1. due rette oppure
2. una retta e un cerchio oppure
3. due cerchi.

Nei primi due casi è evidente che la coordinata P_x si possa ricavare come soluzione di un'equazione di grado al più 2 a coefficienti costruibili. Nel terzo caso invece il sistema composto dalle equazioni di due circonferenze è di ordine 4. Si può aggirare questa difficoltà osservando che l'intersezione fra due circonferenze è equivalente all'intersezione fra una di queste e il loro *asse radicale*, cioè la retta passante per le loro intersezioni. Da un punto di vista algebrico l'asse radicale è la *differenza* termine a termine delle equazioni delle due circonferenze e ovviamente è l'equazione di una retta.

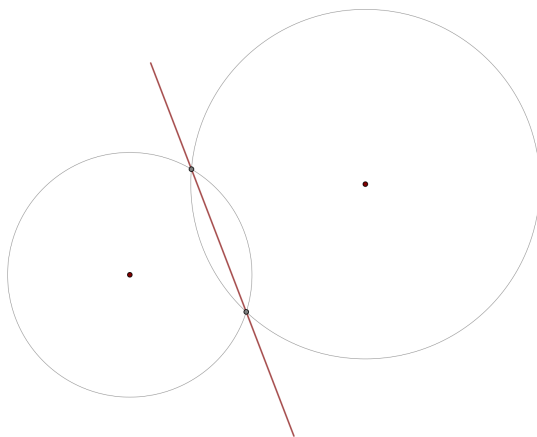


Figura 3.4: Due Circonferenze e il loro Asse Radicale

Possiamo dunque dedurre che in tutte e tre le configurazioni possibili le coordinate di un punto costruibile siano esprimibili in funzione di quelle di punti precedentemente costruiti (quelli che determinano i coefficienti delle equazioni delle linee coinvolte) attraverso la formula (3.1).

Per esprimere le equazioni coinvolte in una qualsiasi delle tre configurazioni elencate sono sufficienti 5 coefficienti, diciamo $\alpha_1, \dots, \alpha_5$. Questi coefficienti potrebbero non essere numeri razionali, ma sicuramente si trovano in un'estensione della forma $\mathbb{Q}(\alpha_1, \dots, \alpha_5)$ e quanto detto si traduce in:

$$[Q(\alpha_1, \dots, \alpha_5)(P_x) : Q(\alpha_1, \dots, \alpha_5)] \in \{1, 2\} \quad (3.2)$$

Questo stesso ragionamento è però applicabile a quegli stessi punti che determinavano i coefficienti delle linee usate per segnare il punto P , e iterativamente a ritroso a tutti i punti individuati durante la costruzione del punto P . Questo ci porta a dedurre il seguente

Teorema 3.3.

Un numero $\alpha \in \mathbb{C}$ è costruibile se e solo se si trova in un'estensione del tipo

$$\mathbb{Q}(\sqrt{\alpha_1}, \dots, \sqrt{\alpha_n})$$

dove $\forall i = 1, \dots, n$ ($\alpha_i \in \mathbb{Q}(\sqrt{\alpha_1}, \dots, \sqrt{\alpha_{i-1}})$)

Dimostrazione.

I paragrafi precedenti provano che se α è costruibile allora si trova in un'estensione di \mathbb{Q} come quella della tesi, che solitamente viene detta *torre di radici quadrate*, poiché ogni nuovo elemento è raggiunto aggiungendo la radice quadrata di un elemento dell'estensione precedente.

Viceversa se un numero α si trova in cima a una torre del genere questo risulta costruibile direttamente per il Teorema 3.1. Per esempio, infatti, se

$$\alpha \in \mathbb{Q}(\sqrt{a}, \sqrt{b}) \quad \text{con } b \in \mathbb{Q}(\sqrt{a}), a \in \mathbb{Q}$$

allora per la natura vettoriale di $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ α si scrive:

$$\alpha = q + r\sqrt{b} \quad \text{con } q, r \in \mathbb{Q}(\sqrt{a})$$

Per gli stessi motivi più esplicitamente:

$$\begin{aligned} \alpha &= \underbrace{(s + t\sqrt{a})}_q + \underbrace{(u + v\sqrt{a})}_r \underbrace{\sqrt{c + d\sqrt{a}}}_{\sqrt{b}} \quad \text{con } s, t, u, v, c, d \in \mathbb{Q} \\ &= s + t\sqrt{a} + u\sqrt{c + d\sqrt{b}} + v\sqrt{ac + ad\sqrt{b}} \end{aligned}$$

che per la struttura di \mathbb{E} implica $\alpha \in \mathbb{E}$. Questo argomento è ripetibile ad ogni estensione successiva della torre. \square

Si noti che l'espressione trovata in Sezione 2.4 attraverso l'equazione (♠) per il coseno di $\frac{2\pi}{17}$ è, coerentemente, della forma prevista da questo Teorema.

Corollario 3.3.1.

Se $\alpha \in \mathbb{E}$ allora $[Q(\alpha) : Q] = 2^n$ per qualche $n \in \mathbb{N}$.

Dimostrazione.

Abbiamo appena provato che $\alpha \in \mathbb{Q}(\sqrt{\alpha_1}, \dots, \sqrt{\alpha_n})$ e sicuramente per qualche $k \in \mathbb{N}$:

$$[\mathbb{Q}(\sqrt{\alpha_1}, \dots, \sqrt{\alpha_n}) : \mathbb{Q}] = 2^k$$

Ma $[Q(\alpha) : Q] \mid [\mathbb{Q}(\sqrt{\alpha_1}, \dots, \sqrt{\alpha_n}) : \mathbb{Q}]$, dunque $[Q(\alpha) : Q]$ è a sua volta una potenza di 2. \square

Questo ultimo Corollario è equivalente alla dimostrazione fatta da Wantzel del fatto che ogni numero costruibile sia soluzione di un particolare sistema di equazioni di ordine 2 riducibile ad un unico problema di ordine potenza di 2.

3.4 Il Teorema di Gauss-Wantzel

Ci discostiamo ora dal ragionamento originale di Wantzel. La teoria algebrica che abbiamo usato nelle sezioni precedenti di questo capitolo permette, semplicemente con un calcolo, di ricavare l'implicazione mancante nel Teorema 2.1.

Definizione 3.2 (Funzione Toziente di Eulero).

Sia $n \in \mathbb{N}$. La funzione $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ associa ad n la cardinalità dell'insieme:

$$\{k < n \mid MCD(k, n) = 1\}$$

ossia la quantità di predecessori di n che siano con questo coprimi.

Ricordiamo che esiste un'espressione esplicita per la funzione φ con riferimento alla fattorizzazione unica $n = 2^m p_1^{\alpha_1} \dots p_h^{\alpha_h}$:

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) = 2^{m-1} \prod_{i=1}^h p_i^{\alpha_i-1} (p_i - 1) \quad (3.3)$$

Supponiamo ora che il n -gono sia costruibile. Equivalentemente è costruibile il punto $(\cos(\frac{2\pi}{n}), \sin(\frac{2\pi}{n}))$ nel piano o il numero complesso $\zeta_n := e^{i\frac{2\pi}{n}}$.

Il numero ζ_n , grazie al Corollario 3.3.1, è costruibile solo se $[Q(\zeta_n) : Q] = 2^s$ per qualche $s \in \mathbb{N}$. D'altra parte è noto che il polinomio minimo di ζ_n è l' n -esimo polinomio ciclotomico

$$\Phi_n(x) = \prod_{k: MCD(k, n)=1} (x - e^{i\frac{2k}{n}\pi})$$

il cui grado è evidentemente $\varphi(n)$. Questo comporta che:

$$\text{il } n\text{-gono è costruibile} \implies \exists s \in \mathbb{N} (\varphi(n) = 2^s)$$

Imponendo nell'Equazione (3.3) la condizione $\varphi(n) = 2^s$ si ottiene:

$$\text{il } n\text{-gono è costruibile} \implies \forall i = 1, \dots, h (\alpha_i = 1 \wedge \exists t \in \mathbb{N} (p_i - 1 = 2^t))$$

Questo significa esattamente che eventuali fattori primi dispari in n , se presenti, sono primi di Fermat distinti. Il Teorema 2.1 è dimostrato.

Capitolo 4

LA GEOMETRIA DEGLI ORIGAMI

Da questo momento in poi ci occupiamo di una teoria della geometria piana basata su un'assiomatizzazione diversa da quella della riga e del compasso. In un certo senso riduciamo gli strumenti a nostra disposizione, rinunciando al compasso e con esso alla possibilità di tracciare cerchi, ma d'altra parte sostituendo la riga con uno strumento più versatile: le pieghe della carta.

Con la riga e il compasso le uniche rette costruibili erano quelle congiungenti due punti costruibili. Con le pieghe della carta invece le rette che possiamo individuare sul piano, il "foglio", sono tutte quelle che corrispondono alla traccia di una possibile piega della carta¹.

Non si può piegare la carta in modo totalmente arbitrario. Le pieghe permesse, che corrispondono all'individuare sul foglio le rette che chiameremo *tracciabili*, poiché corrispondono alle tracce che le pieghe lasciano sul foglio, sono quelle che portano gli oggetti già individuati in particolari configurazioni. I possibili modi in cui è consentito piegare la carta per allineare punti e rette già tracciate costituisce l'insieme degli assiomi di questa teoria. Ciascuna di queste pieghe deve essere effettuata *individualmente*, nel senso che fra una piega e la successiva il foglio deve essere ridisteso.

Come nel caso della riga e del compasso un nuovo punto può essere segnato ovunque due tracce di pieghe si intersechino.

4.1 Gli Assiomi di Huzita-Hatori-Justin

Gli assiomi che ora esponiamo vennero formulati per la prima volta in un articolo del 1986 dal matematico francese Pierre Justin. In questo articolo questa assiomatizzazione della geometria veniva proposta per permettere la risoluzione di equazioni

¹Dunque a priori una retta potrebbe essere costruibile senza che su di essa vi sia alcun punto costruibile.

di terzo grado. Nel 1995 i primi sei assiomi vennero riscoperti dal matematico italo-giapponese Humiaki Huzita, mentre il settimo assioma non ricomparve prima del 2001, in un articolo del matematico giapponese Koshiro Hatori. Ci riferiremo al loro complesso come *Assiomi HHJ*, dai nomi Huzita-Hatori-Justin.

Come nel caso classico si postula sempre la presenza di una coppia di punti. Li indichiamo con O e U e assumiamo che la loro distanza sia unitaria.

O1. Dati due punti è possibile tracciare la piega che li fissa entrambi.

Notiamo subito che una piega della carta *fixa* un punto, cioè lo fa coincidere con la sua traccia dopo la piega, se e solo se il punto si trova sulla traccia della piega. Questo assioma dunque permette di tracciare le rette che congiungono coppie di punti ed è pertanto equivalente all'uso della riga euclidea.

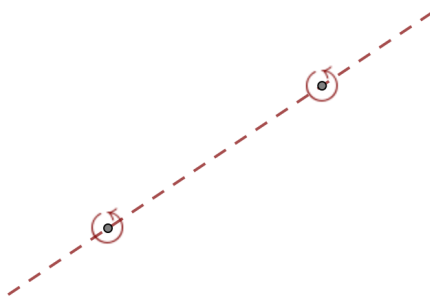


Figura 4.1: Assioma O1

O2. Dati due punti distinti è possibile tracciare la piega che porta il primo sul secondo.

La piega che porta un punto su un altro è quella la cui traccia corrisponde con l'asse di simmetria per il quale il primo punto è riflesso sul secondo: è l'asse del segmento. Lo postuliamo tracciabile perché, nello stato attuale della teoria, non siamo in grado di tracciare i cerchi che sono coinvolti nella costruzione euclidea dell'asse.

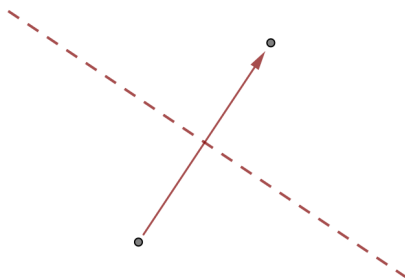


Figura 4.2: Assioma O2

O3. Date due rette distinte è possibile tracciare la piega che porta la prima sulla seconda.

Questa costruzione permette di tracciare le bisettrici degli angoli se la coppia di rette a cui si fa riferimento è una coppia di rette *incidenti*, individuanti dunque quattro angoli, a due a due bisecabili. L'assioma è utilizzabile anche su coppie di rette parallele e in questo caso la retta tracciabile è il luogo dei punti medi dei segmenti i cui estremi si trovano ciascuno su una parallela o, in altre parole, quella terza retta parallela alle precedenti e da esse equidistante.



Figura 4.3: Assioma O3, Rette Parallele

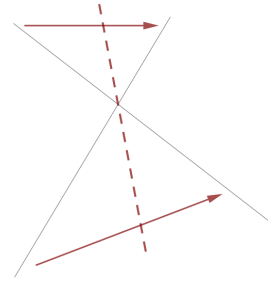


Figura 4.4: Assioma O3, Rette Incidenti

O4. Dati un punto e una retta è possibile tracciare l'unica piega che fissa il punto e porta la retta su sé stessa.

Come abbiamo già osservato una piega fissa un punto se e solo se la sua traccia passa per quel punto. Allo stesso tempo una piega porta una retta su sé stessa se e solo se è perpendicolare a quella retta, dunque questo assioma permette di tracciare le perpendicolari ad una retta per un punto, a prescindere dalla posizione del punto.

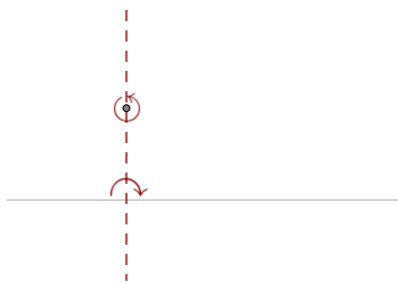


Figura 4.5: Assioma O4

Questi primi quattro assiomi garantiscono la tracciabilità di rette che erano già costruibili con riga e compasso. Torneremo a breve su questo aspetto quando confronteremo le due teorie. I prossimi tre assiomi li raggruppiamo rimandando la discussione sulla natura della piega individuata, da una parte perché questa potrebbe *non esistere* e dall'altra perché, qualora esistesse, potrebbe non essere unica.

- O5.** Dati due punti e una retta è possibile tracciare, *se esiste*, la piega che fissa uno dei due punti e porta l'altro sulla retta.

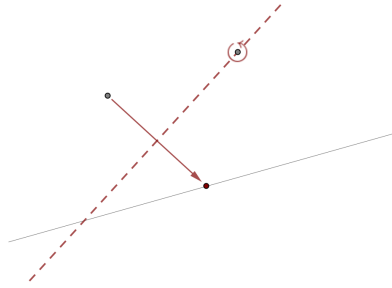


Figura 4.6: Assioma O5

- O6.** Dati due punti e due rette è possibile tracciare, *se esiste*, la piega che porta il primo punto sulla prima retta e il secondo punto sulla seconda retta.

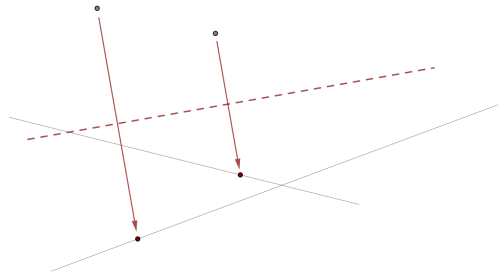


Figura 4.7: Assioma O6

- O7.** Dati un punto e due rette è possibile tracciare, *se esiste*, la piega che porta una retta su sé stessa e il punto sull'altra retta.

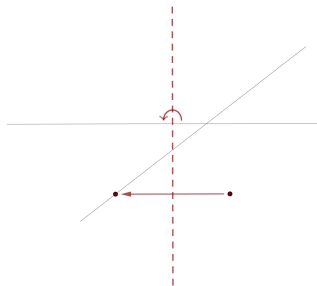


Figura 4.8: Assioma O7

4.2 Breve Discussione su alcuni Assiomi

Gli ultimi tre assiomi giocano un ruolo importante, in particolare il sesto, nel determinare "l'ampiezza" della geometria ottenuta dalle pieghe della carta. Le rette descritte dai primi quattro assiomi sono tutte costruibili con riga e compasso, pertanto l'assunzione degli assiomi O1-O4 determina una teoria che è più debole, almeno in senso lato, di quella euclidea. È anche chiaro quale sia il pezzo mancante: la carta può essere piegata solo con tracce rettilinee, dunque non c'è modo di simulare a pieno e in modo diretto l'uso del compasso, nel senso che apparentemente non è possibile, in un algoritmo di costruzione con riga e compasso, sostituire ogni uso del compasso con l'utilizzo di un assioma degli origami.

A dire il vero una simulazione "parziale" del compasso è possibile. Abbiamo osservato nel Capitolo 3 che i punti costruibili con riga e compasso sono individuati attraverso tre tipi di incidenza: retta-retta, retta-arco oppure arco-arco.

Il caso retta-retta non presenta alcun ostacolo in quanto se una retta è costruibile allora vi sono almeno due punti costruibili su essa e in questo caso quella retta è anche tracciabile con l'assioma O1.

Supponiamo invece individuati una retta r e un segmento CR . Si può marcare con le pieghe della carta un punto P che si trova sull'intersezione di r con la circonferenza di centro C e raggio CR usando l'assioma O5 per individuare la piega che passa per C e porta R su r ². Questo risolve il caso retta-arco, tuttavia nessuno degli assiomi HHJ rappresenta una scorciatoia per l'incidenza arco-arco. Vedremo che ciò nonostante questo tipo di punti è tracciabile con le pieghe della carta.

Vediamo ora in quali casi è *possibile* tracciare le pieghe previste dagli assiomi O5-O7 soffermandoci sulla natura geometrica di queste operazioni.

O5: Tangenti ad una Parabola

Fissiamo un punto F e una retta d , con l'intenzione che F sia il punto che la piega individuata da O5 porti su d . Tale piega r varia, anche nella sua esistenza o meno, a seconda della scelta del secondo punto P per il quale essa deve passare.

Se r esiste e chiamiamo F' il punto in cui F viene portato su d è chiaro che r costituisce l'asse del segmento FF' , pertanto l'insieme delle pieghe che possono essere descritte usando O5 è l'insieme dei possibili assi di segmenti che hanno un estremo in F e l'altro sulla retta d . I punti P per i quali tale piega esiste sono di conseguenza quelli che si trovano nella regione di piano descritta dal variare di queste rette.

²Si noti che non è detto che questa piega esista, come non è detto che la circonferenza intersechi la retta, inoltre non è al momento chiaro se queste situazioni si corrispondano.

Tale regione di piano è delimitata dalla parabola di fuoco F e direttrice d , alla quale r è allora tangente. I possibili punti P sono dunque quelli *esterni* alla parabola rispetto al suo fuoco. Si ricordi che le tangenti ad una parabola per un punto ad essa esterno sono due.

Teorema 4.1.

Assegnati due punti P, F e una retta d , una piega che porta F su d fissando P esiste se e solo se esistono le tangenti da P alla parabola di fuoco F e direttrice d . In questo caso quelle tangenti sono le tracce delle due possibili pieghe che soddisfano l'assioma O5.

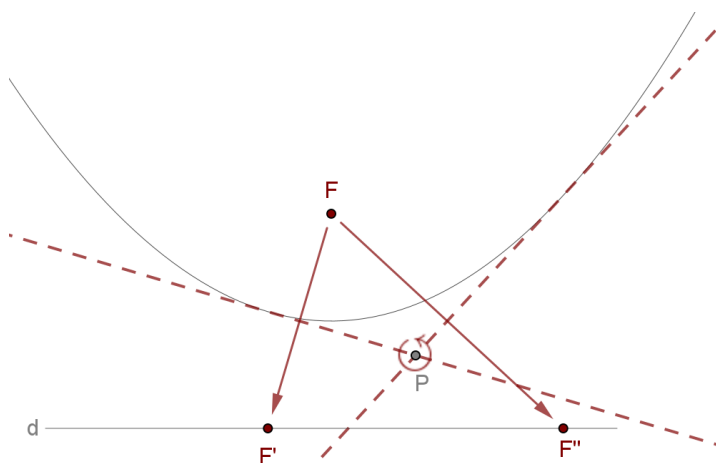


Figura 4.9: Pieghe Possibili per O5 e Parabola Associata

Questo risolve anche la questione in nota 2: la parabola è il luogo dei punti di uguale distanza tra F e d , dunque la regione di piano per i cui punti esistono le tangenti coincide con quella i cui punti sono centro di circonferenze che, passando per F , intersecano d .

Prima di proseguire ci accorgiamo che la presenza del punto P è in un certo senso geometricamente superflua: la richiesta di individuare le pieghe che portino F su d avrebbe ugualmente identificato le tangenti alla medesima parabola, in modo tuttavia eccessivamente sovradeterminato. In effetti *ogni* tangente alla parabola avrebbe soddisfatto la richiesta. La condizione che queste pieghe fissino P ha dunque il ruolo di dare al problema un numero *finito* di soluzioni.

O6: Tangenti Comuni a due Parabole

Fissiamo due punti F_1, F_2 e due rette d_1, d_2 , come prima con l'intenzione di individuare, secondo O6 e dove possibile, quelle pieghe che portano simultaneamente F_1 su d_1 e F_2 su d_2 . Abbiamo di nuovo a disposizione due punti, ma stavolta il secondo punto anziché dover essere fissato deve a sua volta essere portato su una retta. Riprendendo il ragionamento della sezione precedente la piega che cerchiamo, se esiste,

deve innanzitutto lasciare una traccia tangente alla parabola di fuoco F_1 e direttrice d_1 . La stessa traccia deve però essere tangente anche alla parabola di fuoco F_2 e direttrice d_2 .

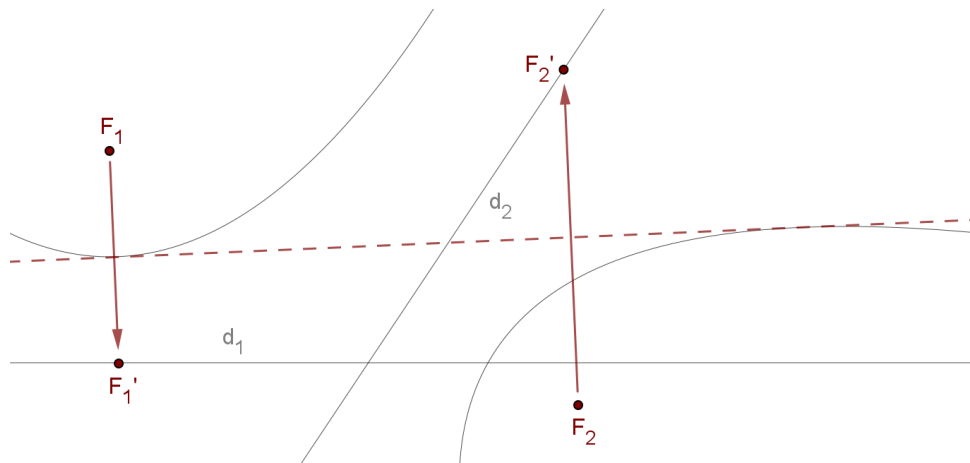


Figura 4.10: Una piega descritta da O6 come tangente simultanea a due parabole

Il problema di determinare le tangenti comuni a due parabole ha in generale tre soluzioni, pertanto ci sono al massimo tre pieghe della carta che rispettano la richiesta dell'assioma O6. Definire quali configurazioni permettano quante soluzioni non è semplice, tuttavia vale la pena spenderci del tempo, poiché questo assioma si rivelerà quello che in effetti rende la teoria delle pieghe della carta più forte di quella classica. Ci penseremo nella prossima sezione.

O7: Traslazione in Parallelo

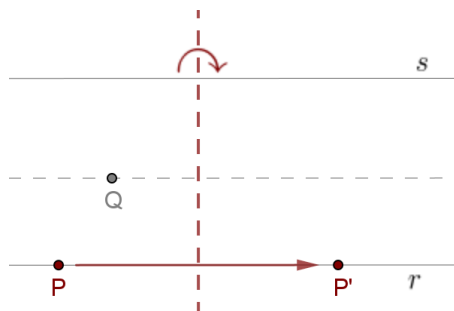


Figura 4.11: Assioma O7 nel Caso di Rette Parallele

Fissiamo un punto P e due rette r e s . La piega prescritta dall'assioma O7 è perpendicolare a s e porta P su r . Una piega del genere, se esiste, è l'asse del segmento PP' , dove P' è il punto di intersezione fra r e la retta per P parallela ad s . Da questo punto di vista è evidente che una piega di questo tipo esiste sempre solo nel caso in cui r, s sono incidenti. Se invece $r \parallel s$ questa si trova unicamente nel caso in cui $P \in r$, poiché il luogo descritto da P' al variare della piega è ancora una retta

parallela a s . In effetti se $P \in r$ qualsiasi piega la cui traccia sia ortogonale a s va bene.

In Figura 4.11 si vede come per $P \in r$ esista un piega mentre per $Q \notin r$ no.

4.3 Il Campo dei Numeri Origami

Definizione 4.1 (Punto Tracciabile). *Un punto del piano³ è detto tracciabile se si trova sull'intersezione di una coppia di rette tracciabili.*

Definizione 4.2 (Numeri Origami). *Un numero $\alpha \in \mathbb{R}$ è un numero origami⁴ se corrisponde alla lunghezza di un segmento i cui estremi sono tracciabili.*

Ci piacerebbe poter confondere queste due nozioni deducendo un risultato analogo al Teorema 3.2. Perché ciò sia possibile è innanzitutto necessario poter tracciare, con le pieghe della carta, un riferimento cartesiano.

Possiamo ottenere il nostro sistema di assi coordinati partendo dalla coppia di punti O, U , con le proprietà usuali, tracciando $O \vee U$ con l'assioma O1 e la perpendicolare a questa retta nel punto O con l'assioma O4.

Il prossimo passo è la capacità di individuare su questi assi le *coordinate* di un punto P . Il modo più semplice per fare ciò consiste nel tracciare per P le parallele agli assi coordinati. Poiché gli assi sono fra loro ortogonali possiamo semplicemente applicare di nuovo O4, con riferimento a P e rispettivamente a ciascun asse. In realtà vale più in generale che

Teorema 4.2.

Assegnati un punto P e una retta r è tracciabile la retta passante per P e parallela a r .

Dimostrazione.

Si applichi O4 a P e r individuando la retta $s \perp r$ e tale che $P \in s$. Si applichi di nuovo O4 a P e s , individuando una terza retta che passa per P e stavolta parallela a r . □

Sappiamo già dalla discussione sull'assioma O5 che questo permette di simulare l'uso del compasso per marcare l'intersezione fra una retta e "un cerchio". Per essere precisi O5 permette di intersecare una retta con un arco di circonferenza il cui centro è un estremo dello stesso segmento che ne individua il raggio (si veda la Sezione 4.2). Per poter davvero simulare l'uso del compasso, anche solo limitatamente all'intersezione retta-arco, avremmo bisogno però di poter intersecare rette con archi

³Come già abbiamo fatto identificheremo il "piano" con \mathbb{R}^2 oppure con \mathbb{C} quando è opportuno.

⁴Nella letteratura ci si riferisce a questi numeri coi termini "crease-numbers" o "foldable numbers" o ancora "origami numbers".

il cui raggio è un segmento arbitrario o , in altre parole, dovremmo essere in grado di riportare segmenti individuati su rette che non li contengono.

Corollario 4.2.1. *Assegnati una retta r , un punto $P \in r$ e un segmento AB è possibile individuare su r un punto Q tale che $PQ = AB$.*

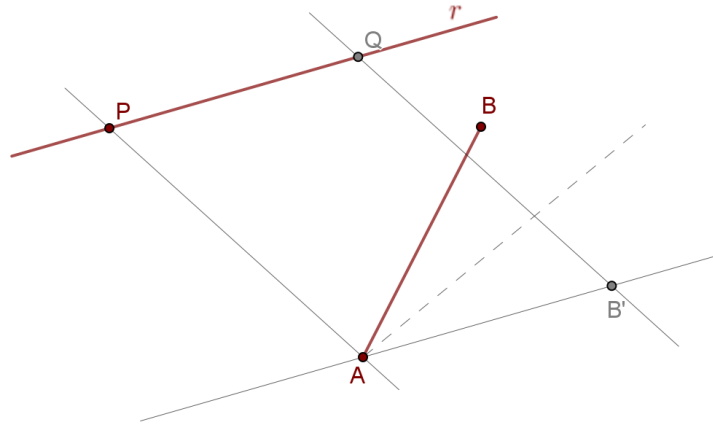


Figura 4.12: Trasporto di una Lunghezza su una Retta

Dimostrazione. Si faccia riferimento a Figura 4.12. Grazie al Teorema 4.2 è possibile tracciare la parallela per A a r . Usando O5 si individui B' su questa in modo che $AB = AB'$. Si congiunga poi A con P e si tracci la parallela per B' a AP , individuando così il punto Q tale che $PQ = AB' = AB$. \square

Ripetendo esattamente la dimostrazione del Teorema 3.2 si ottiene allora

Teorema 4.3.

Un punto $P \in \mathbb{R}^2$ è tracciabile se, e solo se, le sue coordinate sono due numeri origami. Equivalentemente un numero $\zeta \in \mathbb{C}$ è origami se e solo se sono origami le sue parti reale e immaginaria.

Vogliamo a questo punto dare una struttura algebrica all'insieme dei *Numeri Origami*, che denotiamo con \mathbb{O} . Ci accorgeremo subito che \mathbb{O} contiene \mathbb{E} . Questo ci darà la conferma definitiva che ogni costruzione possibile con riga e compasso è possibile anche con le pieghe della carta. Riusciremo a provare più di questo, cioè che in effetti la Geometria degli Origami permette di costruire più oggetti rispetto a quella Classica. Il risultato che fissiamo all'orizzonte è il seguente

Teorema 4.4.

\mathbb{O} è un'estensione intermedia tra i campi \mathbb{Q} e \mathbb{R} , chiusa per radici quadrate e per radici cubiche, cioè:

$$\alpha \in \mathbb{O} \wedge \alpha > 0 \Rightarrow \sqrt{\alpha} \in \mathbb{O}$$

$$\alpha \in \mathbb{O} \Rightarrow \sqrt[3]{\alpha} \in \mathbb{O}$$

Anziché strutturare questa dimostrazione da capo possiamo ereditare gran parte del ragionamento dalla dimostrazione del Teorema 3.1 con pochi aggiustamenti, poiché siamo in grado di sostituire con pieghe della carta ogni costruzione di intersezioni retta-retta e retta-arco.

In particolare si possono ripetere con gli stessi passaggi, a meno di questa sostituzione, le costruzioni per tracciare:

- la somma e la differenza di due numeri origami, Figura 3.1;
- il prodotto di due numeri origami, Figura 3.2;
- l'inverso moltiplicativo di un numero origami, Figura 3.3.

Queste costruzioni, come nel caso euclideo, nascondono al loro interno anche la prova dell'esistenza degli elementi neutri (il segmento nullo e il segmento OU) e la commutatività delle operazioni di somma e prodotto. Lo stesso si può dire della costruzione per la radice quadrata, dunque l'insieme \mathbb{O} risulta un campo chiuso per radici quadrate e contenente \mathbb{Q} . Questo dimostra $\mathbb{E} \leq \mathbb{O}$. L'unica parte delicata, a prova del fatto che l'inclusione è stretta, è la chiusura per radici cubiche.

Chiusura per Radici Cubiche

Torniamo a discutere dell'assioma O6 e cerchiamo di convincerci del motivo per cui le pieghe prescritte sono in generale tre.

Fissiamo due punti F, P e una sola retta d . Senza perdere di generalità possiamo assumere che d sia l'asse orizzontale $y = -1$ nel riferimento cartesiano e che $F = (0, 1)$, in questo modo la parabola le cui tangenti individuano le pieghe che portano F su d ha equazione $y = x^2$. Parametizziamo il punto P attraverso le sue coordinate $P = (a, b)$ e ci domandiamo, a seconda della posizione della seconda retta r , se e quante tangenti alla parabola individuata identifichino anche pieghe che portano P su r . Per fare questo cerchiamo di identificare il luogo del riflesso P' al variare delle pieghe che portano F su d , cioè delle tangenti alla parabola.

Al variare della tangente scelta F' ha coordinate $(t, -1)$ e la tangente stessa, che può essere pensata come asse del segmento FF' , passa per il suo punto medio $(\frac{t}{2}, 0)$ e ha pendenza $\frac{t}{2}$. Si può dunque parametrizzare l'insieme delle tangenti come:

$$t \mapsto Y = \frac{t}{2} \left(X - \frac{t}{2} \right) = \frac{t}{2} X - \frac{t^2}{4} \quad (4.1)$$

Poiché vogliamo derivare un'equazione per il luogo dei punti P' denotiamo $P' = (x, y)$. La tangente che scegliamo come traccia della piega deve essere l'asse anche del segmento PP' , cioè passare per il punto medio $(\frac{x+a}{2}, \frac{y+b}{2})$ con pendenza $-\frac{x-a}{y-b}$. Inserendo queste informazioni in (4.1) otteniamo:

$$\frac{y+b}{2} = -\frac{(x+a)(x-a)}{2(y-b)} - \left(\frac{x-a}{y-b} \right)^2$$

Riarrangiando i termini

$$(y - b)^2(y + b) = (x + a)(x - a)(y - b) - 2(x - a)^2$$

e usando infine il cambio di variabile $x \mapsto x + a$, $y \mapsto y + b$ si arriva all'equazione

$$y^3 + 2by^2 - (x^2 + 2ax)y + 2x^2 = 0 \quad (4.2)$$

che è l'equazione di una *curva cubica*. Poiché questa curva descrive il luogo delle immagini P' portate da una piega presa tangente alla parabola di fuoco F e direttrice d tale piega soddisfa l'assioma O6 se e solo se la seconda retta r incide questa curva cubica⁵. In tal caso ciascuna intersezione, che come è noto sono al massimo tre, individua una possibile posizione per il punto P' .

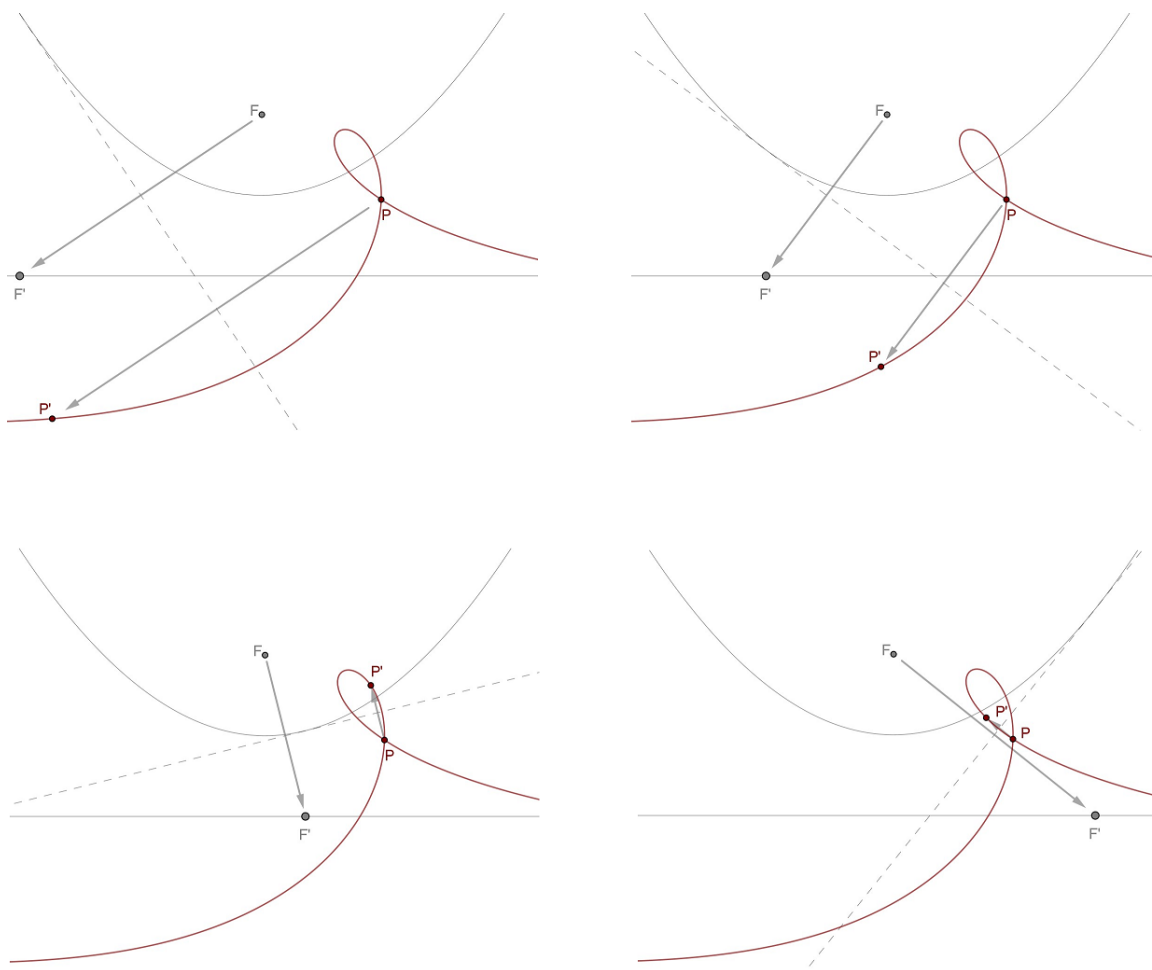


Figura 4.13: Quattro possibili posizioni di P' e cubica associata a O6

⁵In realtà esiste una caratterizzazione geometrica precisa, dovuta al professor Jorge C. Lucero dell'Università di Brasilia, di quando O6 è applicabile o meno. Vi faremo accenno nel prossimo capitolo e l'articolo in cui tale condizione è dimostrata è [Luc19b] in bibliografia.

Questa cubica contiene un nodo se, e solo se, P e F sono da parti opposte della parabola. Questo è vero perché il nodo della cubica è associato alla presenza di due tangenti alla parabola che fissano P (il nodo si verifica quando $P' = P$), cioè è presente se e solo se da P esistono le tangenti alla parabola.

La struttura algebrica che abbiamo dato al problema è chiaramente simmetrica nei punti F, P e nelle rette d, r , che possono essere, in una coppia o entrambe, scambiati di ruolo.

Assumiamo ora che la seconda retta sia fissata, diciamo nella forma

$$r : \alpha x + \beta y + \gamma = 0$$

e usiamo questa relazione per eliminare una delle variabili in (4.2), che diventa così un'equazione di terzo grado. I coefficienti di questa equazione sono numeri origami, infatti tali coefficienti sono funzioni razionali:

- delle coordinate (a, b) di P ;
- dei coefficienti della retta r , che come abbiamo già visto si posso esprimere attraverso le coordinate di una coppia di punti di passaggio della piega.

Ricordiamo che l'equazione generica di terzo grado

$$ax^3 + bx^2 + cx + d = 0$$

si può sempre ricondurre attraverso il cambio di variabile $x \mapsto x - \frac{b}{3a}$ alla forma

$$x^3 + px + q = 0$$

dove p, q sono ancora numeri origami.

Utilizzare l'assioma O6 significa quindi risolvere una cubica a coefficienti in \mathbb{O} . Viceversa una qualsiasi cubica a coefficienti in \mathbb{O} può essere risolta usando O6.

Supponiamo $p, q \in \mathbb{O}$. Allora sono tracciabili i punti $F_1 = (\frac{q}{2}, \frac{p}{2})$ e $F_2 = (0, \frac{1}{2})$ e le rette $d_1 : x = -\frac{q}{2}$ e $d_2 : y = -\frac{1}{2}$. Se usati ordinatamente come coppie di fuoco e direttrice questi individuano le parabole:

$$\gamma_1 : \left(y - \frac{p}{2}\right)^2 = 2qx \qquad \gamma_2 : y = \frac{x^2}{2}$$

O6 permette di tracciare una piega che porta F_1 e F_2 rispettivamente su d_1 e d_2 individuando una retta tangente a entrambe le parabole. Sia m la sua pendenza⁶.

Derivando l'equazione di γ_1 si ottiene:

$$2 \left(y - \frac{p}{2}\right) \frac{dy}{dx} = 2q \Rightarrow \frac{dy}{dx} = \frac{q}{y - \frac{p}{2}}$$

⁶Dal momento che γ_2 ha asse verticale e r è tangente a γ_2 non è possibile che r sia verticale.

Siano (x_1, y_1) e (x_2, y_2) i punti di tangenza di r con $\gamma_{1,2}$. Deve valere:

$$m = \frac{q}{y_1 - \frac{p}{2}} \Rightarrow y_1 = \frac{q}{m} + \frac{p}{2}$$

Sostituendo nell'equazione di γ_1 deduciamo:

$$x_1 = \frac{q}{2m^2}$$

Ripetendo gli stessi passaggi sull'equazione per γ_2 si vede che:

$$x_2 = m \quad y_2 = \frac{m^2}{2}$$

D'altra parte deve valere $m = \frac{y_2 - y_1}{x_2 - x_1}$, così

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

e si può semplificare questa espressione deducendo:

$$m^3 + pm + q = 0$$

che significa che m è soluzione dell'equazione cubica. m è anche un numero origami, poiché r è una retta tracciabile, dunque su di essa si può individuare almeno un punto. Da questo punto si può tracciare una parallela all'asse delle ascisse e riportarvi il segmento unitario. Il terzo cateto del triangolo retto così formato è notoriamente lungo m . Abbiamo così dimostrato

Teorema 4.5.

L'assioma O6 è equivalente alla chiusura di \mathbb{O} per soluzioni di equazioni cubiche, cioè al fatto che qualunque equazione cubica a coefficienti in \mathbb{O} abbia soluzione in \mathbb{O} .

Corollario 4.5.1.

$$\alpha \in \mathbb{O} \implies \sqrt[3]{\alpha} \in \mathbb{O}$$

Dimostrazione.

Seguendo i passi del ragionamento appena concluso è sufficiente scegliere $p = 0$, $q = -\alpha$. □

Questo conclude la dimostrazione del Teorema 4.4.

4.4 Completezza degli Assiomi HHJ

Il fatto che O7 sia passato inosservato per anni non è un caso. Questo assioma predica la tracciabilità di una piega che non è ottenibile *direttamente* attraverso gli assiomi precedenti e che pertanto amplia l'insieme degli oggetti geometrici costruibili. Abbiamo però appena visto che, nella determinazione delle proprietà del campo dei *numeri origami*, O7 non gioca alcun ruolo. In effetti la costruzione postulata da O7 è possibile anche con riga e compasso. In altre parole O7 permette di tracciare rette che, a priori, sfuggono agli altri assiomi, ma non punti⁷ in più su queste rette.

L'aver "riscoperto" l'assioma O7 ha fatto sorgere dubbi sulla "completezza" degli assiomi HHJ, o meglio la domanda riguardo al se questi assiomi rappresentino tutti gli allineamenti possibili usando pieghe della carta oppure no.

Una risposta in questo senso, fortunatamente, si può dare per enumerazione. Ogni assioma degli HHJ corrisponde ad una possibile configurazione di oggetti precedentemente costruiti dopo che una parte di questi (quelli indifferentemente da un lato o dall'altro della piega) viene riflesso sulla traccia di questa piega. Anziché domandarci se gli HHJ rappresentino tutti i modi possibili di tracciare una piega possiamo individuare una famiglia di *allineamenti elementari* e scoprire se gli assiomi permettano di produrne tutte le combinazioni.

Poiché le pieghe della carta consentono di tracciare unicamente punti e rette una nuova piega non può che essere individuata attraverso l'allineamento:

- di due punti;
- di un punto e una retta;
- di due rette;

o da combinazioni di questi allineamenti.

Un punto P è individuato attraverso le sue coordinate (P_x, P_y) mentre per quanto riguarda le rette scegliamo di parametrizzarle attraverso coppie (α, d) in modo che la retta r con queste coordinate sia quella con direzione ortogonale al versore $(\cos(\alpha), \sin(\alpha)) := u_\alpha$ e la cui distanza da O sia d . Sono le *coordinate polari* della retta.

I punti su r sono, al variare di un parametro $t \in \mathbb{R}$:

$$t \longmapsto du_\alpha + tu_\alpha^\perp \quad (4.3)$$

dove $u_\alpha^\perp := (\sin(\alpha), -\cos(\alpha))$. La retta r in sé è invece il luogo delle soluzioni a:

$$P \cdot u - d = 0 \quad (4.4)$$

⁷e dunque non nuovi segmenti, le cui lunghezze sono i numeri origami.

La condizione di allineamento di due punti distinti è pertanto quella della coincidenza delle loro coordinate: sono due equazioni.

La condizione di allineamento di un punto con una retta invece è la richiesta $P_x \cos(\alpha) + P_y \sin(\alpha) - d = 0$: una sola equazione. Ciò è vero anche nel caso dell'allineamento di un punto con sé stesso, poiché questo equivale all'appartenenza di quel punto alla retta che è traccia della piega, cioè ad un allineamento punto-retta.

Per quanto riguarda l'allineamento di due rette, diciamo (α, d) e (β, q) , occorre che ogni punto di una retta appartenga all'altra, e qui torna comoda la parametrizzazione in (4.3). Sostituendola in (4.4) si ottiene:

$$(du_\alpha + tu_\alpha^\perp) \cdot u_\beta - q = 0$$

Riarrangiando i termini in modo da esporre il parametro t abbiamo

$$(du_\alpha \cdot u_\beta - q) + t(u_\alpha^\perp \cdot u_\beta) = 0$$

e poiché questo deve essere vero per tutti i punti sulla prima retta, cioè per ogni $t \in \mathbb{R}$, devono valere di nuovo due equazioni⁸:

$$\begin{cases} du_\alpha \cdot u_\beta = q \\ u_\alpha^\perp \cdot u_\beta = 0 \end{cases}$$

Di nuovo il caso dell'allineamento di una retta con sé stessa è un'eccezione e corrisponde ad una sola equazione, quella per cui i due versori devono essere ortogonali.

Denotiamo con $r(A)$ la posizione dell'oggetto A dopo aver effettuato la piega di traccia r e col simbolo $A \leftrightarrow B$ la coincidenza degli oggetti A e B . I tre tipi di allineamento fondamentale possono essere combinati in 5 modi differenti rispetto a una coppia di punti P_1, P_2 e di rette L_1, L_2 :

$$\begin{array}{l|l} r(P_1) \leftrightarrow P_1 & \text{allineamento di un punto con sé stesso} \\ r(P_1) \leftrightarrow P_2 & \text{allineamento di due punti distinti} \\ r(L_1) \leftrightarrow L_1 & \text{allineamento di una retta con sé stessa} \\ r(L_1) \leftrightarrow L_2 & \text{allineamento di due rette distinte} \\ r(P_1) \leftrightarrow L_1 & \text{allineamento di un punto con una retta} \end{array}$$

Per individuare una piega della carta occorrono due parametri, angolo e distanza dall'origine, dunque gli allineamenti di due punti o rette distinti individuano da soli una piega, poiché impongono due equazioni ciascuno. Sono rispettivamente O2 e O3.

Gli altri tre tipi di allineamento impongono una condizione ciascuno sui parametri della piega e possono essere accoppiati complessivamente nei nove modi riassunti di seguito nella Tabella 4.1.

⁸Si noti il significato geometrico del sistema. La seconda equazione equivale a chiedere che le rette siano parallele e di conseguenza che $u_\alpha \cdot u_\beta = \pm 1$. In entrambi i casi sostituendo nella prima equazione si legge la coincidenza delle rette.

	$r(P_2) \leftrightarrow P_2$	$r(L_2) \leftrightarrow L_2$	$r(P_2) \leftrightarrow L_2$
$r(P_1) \leftrightarrow P_1$	O1	O4	O5
$r(L_1) \leftrightarrow L_1$	O4	??	O7
$r(P_1) \leftrightarrow L_1$	O5	O7	O6

Tabella 4.1: Coppie di allineamenti possibili

La combinazione centrale non porta ad una piega ben determinata: se L_1 e L_2 sono parallele il sistema delle condizioni imposte ha infinite soluzioni (qualsiasi retta perpendicolare a entrambe), mentre se sono incidenti è privo di soluzione. Questa tabella non solo conferma in modo definitivo che O7 ha una natura geometrica distinta dai precedenti assiomi, ma anche che non ci sono altre possibili configurazioni di allineamenti se non quelle prescritte dagli assiomi HHJ.

4.5 I Poligoni Origami

Abbiamo visto che utilizzare l'assioma O6 è equivalente alla risoluzione di un'equazione cubica. Un caso particolare di costruzione di questo tipo permette di individuare le radici cubiche di ogni numero origami, tuttavia non ogni applicazione di O6 è riconducibile unicamente al calcolo di una radice cubica.

La formula risolutiva per le equazioni di terzo grado nella forma $x^3 + px + q = 0$ è:

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \quad (4.5)$$

È dunque evidente che, ammesso che $p, q \in \mathbb{O}$, x non si esprime come una combinazione razionale *unicamente* di radici cubiche, infatti (4.5) contiene anche radici quadrate. Per questo quando α è ottenuto da punti di coordinate in $\mathbb{Q}(p, q)$ applicando O6 non è possibile concludere che $\alpha \in \mathbb{Q}(p, q, \sqrt[3]{\beta})$ per qualche $\beta \in \mathbb{Q}(p, q)$, come invece abbiamo fatto guardando al Corollario 3.1.1 per dimostrare il Teorema 3.3. Possiamo comunque ricavare una formula analoga a (3.2) nel senso che se α si ottiene attraverso O6 allora:

$$[\mathbb{Q}(p, q, \alpha) : \mathbb{Q}(p, q)] \in \{1, 2, 3\} \quad (4.6)$$

Teorema 4.6.

$\alpha \in \mathbb{O}$ se e solo se esiste una catena ascendente di campi

$$\mathbb{Q} = F_0 < F_1 < \dots < F_n < \mathbb{R}$$

tale per cui $\alpha \in F_n$ e:

$$\forall i = 1, \dots, n \left([F_i : F_{i-1}] \in \{2, 3\} \right)$$

Dimostrazione.

Quanto detto nella sezione precedente prova che se $\alpha \in \mathbb{O}$ allora α si trova in un'estensione di \mathbb{Q} della forma richiesta, infatti ad ogni passo della sua costruzione viene applicato O6, che determina un'estensione di grado 3, oppure uno degli altri sei assiomi, che rappresentando costruzioni possibili con riga e compasso determinano estensioni di grado 2.

Viceversa se α si trova in una torre della forma descritta allora ogni estensione successiva è contenuta in \mathbb{O} per il Teorema 4.4, cioè per la chiusura di \mathbb{O} su radici quadrate e cubiche.

Se infatti $[F_i : F_{i-1}] = 2$ la chiusura per radici quadrate implica immediatamente la risolubilità di un'equazione di grado 2. Se invece $[F_i : F_{i-1}] = 3$ sappiamo che attraverso O6 qualunque equazione di grado 3 è risolubile grazie ad una *combinazione* di radici quadrate e cubiche. \square

Corollario 4.6.1.

Se $\alpha \in \mathbb{O}$ allora $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^a 3^b$ per qualche coppia $a, b \in \mathbb{N}$.

Dimostrazione.

Se $\alpha \in \mathbb{O}$ allora esiste una catena di estensioni

$$\mathbb{Q} = F_0 < F_1 < \dots < F_n < \mathbb{R}$$

come prescritto dal Teorema 4.6. Sappiamo che in questo caso il grado dell'ultima estensione rispetto alla base della torre è calcolato come segue:

$$[F_n : \mathbb{Q}] = \prod_{i=1}^n [F_i : F_{i-1}] = 2^a 3^b \quad \text{con } a + b = n$$

Siccome $\alpha \in \mathbb{O}$ allora necessariamente

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] \mid [F_n : \mathbb{Q}]$$

e la tesi immediatamente segue. \square

A questo punto possiamo ripetere passo-passo la dimostrazione della Sezione 3.4 e confrontare la condizione sulla costruibilità del n -gono, che è la costruibilità della radice primitiva ζ_n , con il Corollario 4.6.1. Questo ci porta a dedurre che:

$$\text{il } n\text{-gono è tracciabile con le pieghe della carta} \implies \exists a, b \in \mathbb{N} (\varphi(n) = 2^a 3^b)$$

Teorema 4.7.

Il n -gono è tracciabile con le pieghe della carta se, e solo se:

$$n = 2^a 3^b p_1 \dots p_h$$

con $a, b \in \mathbb{N}$ e p_1, \dots, p_h primi della forma⁹ $2^l 3^k + 1$.

Dimostrazione.

Assumiamo dapprima che il poligono sia costruibile.

È sufficiente ripetere il calcolo usato per dimostrare il Teorema 2.1. Supponiamo che la fattorizzazione di n sia $n = 2^a 3^b p_1^{\alpha_1} \dots p_h^{\alpha_h}$. Allora con riferimento alla formula (3.3):

$$\varphi(n) = 2^a 3^{b-1} \prod_{i=1}^h p_i^{\alpha_i-1} (p_i - 1)$$

D'altra parte per il Corollario 4.6.1 $\varphi(n) = 2^s 3^t$ e questo è vero se, e solo se:

$$\forall i = 1, \dots, h \ (\alpha_i = 1 \wedge \exists l, k \in \mathbb{N} (p_i - 1 = 2^l 3^k))$$

Viceversa se n si fattorizza come nell'enunciato allora $\varphi(n) = 2^s 3^t$ per qualche $s, t \in \mathbb{N}$. Sia ζ_n una radice primitiva n -esima dell'unità. L'estensione ciclotomica $\mathbb{Q}(\zeta_n)$ ha gruppo di Galois ciclico. Questo implica¹⁰ l'esistenza di una catena di estensioni intermedie come nel Teorema 4.6 e di conseguenza la costruibilità del poligono. \square

4.6 Un Esempio: L'Eptagono

L'Eptagono regolare, il 7-gono, è il poligono regolare col minor numero di lati a non poter essere costruito con riga e compasso. Il numero 7 è in effetti il più piccolo primo di Pierpont che non è un primo di Fermat (3 è di Pierpont, ma anche di Fermat), o una potenza di 2 (4 è di Pierpont, ma è potenza di due). La prima costruzione con gli origami, addirittura precedente alla formulazione degli HHJ, è di Benedetto Scimemi in [Sci89], del 1989, a cui si fa riferimento più di recente in [Hul09] del 2009.

Siccome $7 - 1 = 3 \cdot 2$ il Teorema 2.2 ci assicura che per identificare il punto $\zeta_7 = e^{2i\frac{\pi}{7}}$ occorre risolvere un'equazione cubica e una quadratica. Sappiamo che O6

⁹Questi primi sono noti come *Primi di Pierpont*. Curiosamente il matematico americano James Pierpont nel 1895 studiò questi primi proprio in relazione alla costruibilità dei poligoni regolari. Il suo studio riguardava l'estensione della Geometria Euclidea con la possibilità di tracciare sezioni coniche. In effetti si può dimostrare che la teoria sviluppata da Pierpont e quella degli Origami sono equivalenti.

¹⁰Il motivo è che i gruppi ciclici di ordine d possiedono sottogruppi di ordine arbitrario fra i divisori di d . Per la corrispondenza di Galois esiste la catena cercata.

permette di risolvere qualsiasi equazione cubica a coefficienti costruibili. Cerchiamo di capire dunque quali siano le equazioni che dobbiamo risolvere.

Cominciamo ricordando innanzitutto che il polinomio minimo di ζ_7 è

$$\Phi_7(x) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6$$

cioè il settimo *polinomio ciclotomico*. Il Teorema 2.2 garantisce che le radici di Φ_7 si possano trovare come soluzione di un'equazione di grado 3, in cui coefficienti sono funzione razionale delle soluzioni di un'equazione di grado 2. In termini algebrici moderni questo fatto corrisponde esattamente alla previsione del Teorema 4.6.1 dell'esistenza di una torre

$$\mathbb{Q} < F < \mathbb{Q}(\zeta) \tag{4.7}$$

tale per cui le estensioni siano, in quest'ordine, di grado 3 e grado 2.

Facciamo subito un'osservazione importante: $p - 1$ è sempre pari, qualsiasi sia il p -gono che intendiamo costruire. Perché è importante? Perché allora nella costruzione del p -gono, secondo il Teorema 2.2, è *sempre* richiesta la soluzione di almeno un'equazione quadratica. Questa equazione è della stessa forma a prescindere da p e corrisponde al polinomio minimo di $\zeta_p := e^{2i\frac{\pi}{p}}$ sul campo $\mathbb{Q}(c_p)$ dove $c_p := \cos\left(\frac{2\pi}{p}\right)$. Questo polinomio è sempre:

$$(x - \zeta_p)(x - \overline{\zeta_p}) = x^2 - 2c_p + 1$$

Ciò significa che, a prescindere da p :

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}(c_p)] = 2$$

Questo ci fa sospettare che, tornando al caso $p = 7$ e con riferimento all'equazione (4.7), si abbia $F = \mathbb{Q}(c_7)$ e di conseguenza

$$[\mathbb{Q}(c_7) : \mathbb{Q}] = 3$$

Questo è un ottimo suggerimento per identificare la cubica che occorre risolvere: quella che costituisce il polinomio minimo¹¹ su \mathbb{Q} di c_7 . Tale polinomio minimo si può identificare sfruttando il fatto che:

- $c_7 = \zeta_7 + \overline{\zeta_7}$;
- $\overline{\zeta_7} = \zeta_7^{-1}$;
- $\Phi_7(\zeta_7) = 0$.

¹¹Questo polinomio ha necessariamente grado almeno 3, altrimenti il 7-gono sarebbe stato costruibile con riga e compasso, dunque per (4.7) il suo grado è esattamente 3.

Procedendo con ordine, detto $\zeta := \zeta_7$ si ha:

$$\begin{aligned} & 1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6 = 0 \\ \Leftrightarrow & 1 + \zeta + \zeta^2 + \zeta^3 + \frac{1}{\zeta^3} + \frac{1}{\zeta^2} + \frac{1}{\zeta} = 0 \\ \Leftrightarrow & \left(\zeta + \frac{1}{\zeta}\right)^3 + \left(\zeta + \frac{1}{\zeta}\right)^2 - 2\left(\zeta + \frac{1}{\zeta}\right) - 1 = 0 \end{aligned}$$

Da cui si deduce che il polinomio minimo di $2c_7$ è:

$$x^3 + x^2 - 2x - 1$$

Cerchiamo ora di costruire il punto $C = (2c_7, 0)$, così completando il triangolo, rettangolo in C e che ha per cateto OC , con un'ipotenusa unitaria avremo individuato l'angolo $\frac{2\pi}{7}$.

Consideriamo, sempre in un riferimento cartesiano di centro O , i punti $P = (0, 1)$ e $Q = (-1, -\frac{1}{2})$. Costruiamo con O6 la piega che porta P sull'asse delle ascisse e Q sull'asse delle ordinate, come in Figura 4.14. Chiamiamo P' e Q' le immagini portate da questa piega sui rispettivi assi e indichiamo con t e s le loro coordinate x e y .

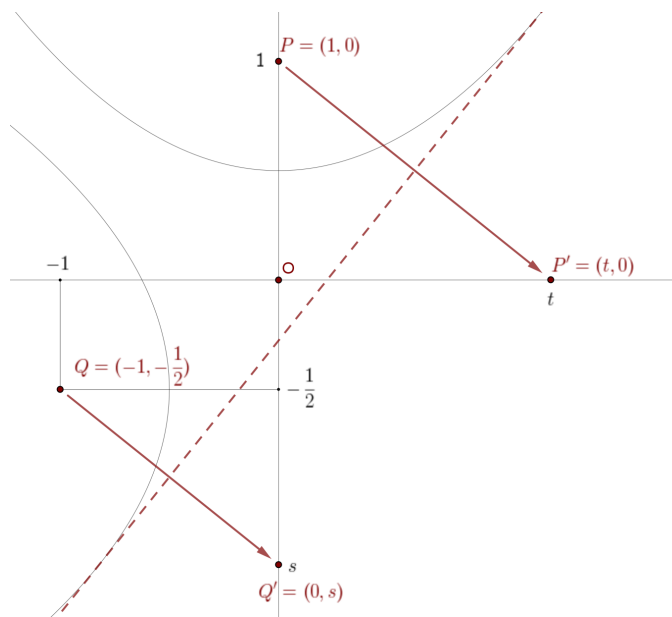


Figura 4.14: La Piega per $2c_7$

La piega individuata, r , è asse del segmento PP' , dunque ha equazione

$$y = tx - \frac{t^2}{2} + \frac{1}{2}$$

d'altra parte r è anche asse di QQ' , dunque:

$$y = \frac{-2}{2s+1}x - \frac{1}{2s+1} + \frac{2s-1}{4}$$

Confrontando queste equazioni, che identificano la stessa retta, si deduce che:

$$\begin{cases} s = -\frac{t+2}{2t} \\ \frac{1}{2} - \frac{t^2}{2} = \frac{2s-1}{4} - \frac{1}{2s+1} \end{cases}$$

Sostituendo la prima equazione nella seconda al posto della variabile s otteniamo:

$$\frac{1}{2} - \frac{t^2}{2} = -\frac{t+1}{2t} + \frac{t}{2}$$

moltiplicando ovunque per $2t$ e riordinando si ha

$$t^3 + t^2 - 2t - 1 = 0$$

dunque t , positiva per costruzione, è l'unica radice positiva¹² della cubica che ci interessa, cioè $t = 2c_7$.

In Figura 4.15 riportiamo la costruzione del 7-gono nella circonferenza di raggio 2, in modo da poter sfruttare la costruzione fatta in figura 4.14, che è evidenziata con un grigio più scuro.

¹²Che le altre due radici siano negative si può vedere per via analitica, ad esempio considerando che per $x = 0$ la cubica è negativa con derivata negativa, dunque entrambi gli zeri sono precedenti a $x = 0$.

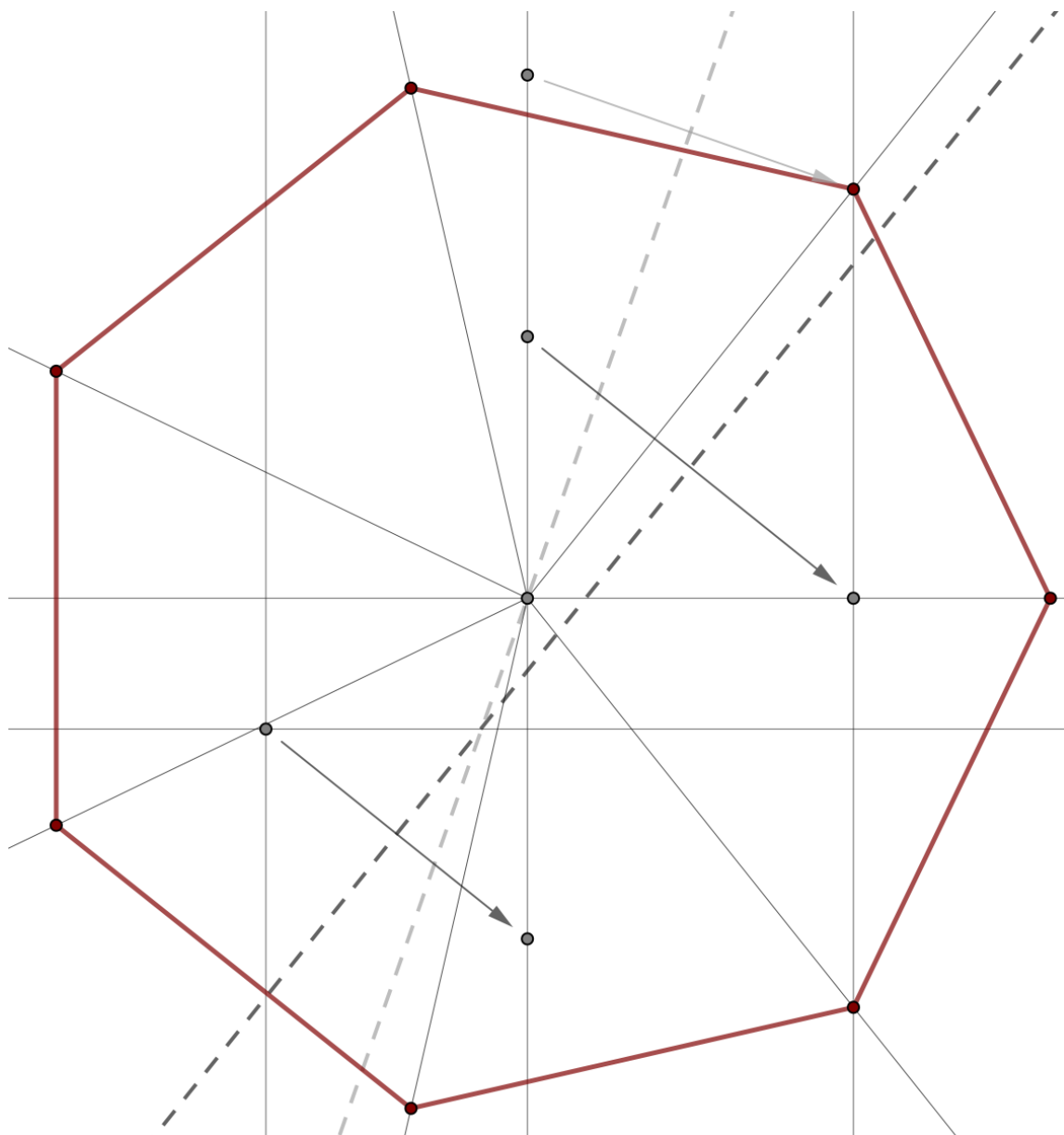


Figura 4.15: Una Costruzione dell'Eptagono con gli Origami

Capitolo 5

ORIGAMI A PIEGHE SIMULTANEE

Permettere di effettuare sul foglio più pieghe simultanee significa concedere di scegliere la posizione di una o più pieghe in funzione della posizione "provvisoria" di altre pieghe, ovvero prima che queste vengano effettuate, per poi tracciare ogni piega del gruppo contemporaneamente. Facciamo un esempio con due pieghe simultanee, che è il caso più semplice e quello di cui ci occuperemo con maggior dettaglio, nonostante alla fine i risultati più importanti riguarderanno un numero di pieghe arbitrario.

Fissiamo quattro punti P_1, P_2, Q_1, Q_2 e due rette L_1, L_2 . Vogliamo costruire due pieghe del tipo O5 *svincolate* dalla scelta del punto di passaggio, cioè due pieghe r_1, r_2 tali da portare P_1 su L_1 e P_2 su L_2 . Sappiamo che ci sono infinite soluzioni a questo problema, poiché ciascuna delle due rette è una fra infinite tangenti a una parabola. Aggiungiamo la richiesta che Q_1 e Q_2 vengano portati, ciascuno da una piega, nello stesso punto. Con la notazione introdotta nella Sezione 4.4 possiamo riassumere lo schema di allineamento, che nel seguito e al di fuori di questo esempio chiameremo *AL6ab8*, così:

$$\begin{array}{l|l} r_1(P_1) \leftrightarrow L_1 & \text{Allineamento di un punto e una retta} \\ r_2(P_2) \leftrightarrow L_2 & \text{Allineamento di un punto e una retta} \\ r_1(Q_1) \leftrightarrow r_2(Q_2) & \text{Allineamento di due punti} \end{array}$$

Coerentemente con quanto detto in Sezione 4.4 due pieghe sono individuate da quattro parametri e gli allineamenti richiesti consumano rispettivamente un grado di libertà (punto-retta) e due gradi di libertà (punto-punto), per un totale di quattro vincoli imposti.

Grazie alla discussione nella Sezione 4.3 sappiamo che, se r_1 e r_2 vengono scelte in modo da soddisfare le prime due richieste, i luoghi descritti da $r_1(Q_1)$ e $r_2(Q_2)$ sono due curve cubiche. Ciascuna intersezione di queste due curve cubiche individua una "buona posizione" per la coincidenza $r_1(Q_1) \leftrightarrow r_2(Q_2)$ e di conseguenza fissa una possibile scelta per la coppia r_1, r_2 . Com'è noto¹ tali intersezioni sono al più nove.

Le due pieghe trovate in questo modo, se esistono, *non* possono essere tracciate individualmente rispettando gli stessi vincoli. Il motivo principale è che ciascuno dei due allineamenti punto-retta è, di per sé, sovradeterminato. Per poter utilizzare O5 occorre specificare due punti di passaggio S_1 e S_2 per le pieghe e questi non possono certo essere ovunque nel piano (devono essere punti di \mathbb{O}^2), di conseguenza non tutte le tangenti alle parabole sono tracciabili.

Per convincerci di questo immaginiamo una parabola la cui direttrice passi per l'origine O . Per qualsiasi punto della direttrice esistono due tangenti alla parabola e se tutte queste tangenti fossero tracciabili allora tutti i punti della direttrice sarebbero tracciabili in quanto intersezione di rette tracciabili. Questo implicherebbe $\mathbb{R} \leq \mathbb{O}$, che sappiamo essere falso perché tutti i numeri origami sono algebrici. Il punto in cui la coincidenza di $r_1(Q_1)$ e $r_2(Q_2)$ ha luogo nel caso di due pieghe individuali consecutive, se esiste, è quindi ovviamente ancora un punto di \mathbb{O} .

Nel caso delle pieghe simultanee invece la scelta delle tracce varia *con continuità* fra tutte le tangenti possibili alle rispettive parabole e il punto di coincidenza di $r_1(O_1)$ e $r_2(O_2)$, se esiste, potrebbe non essere affatto in \mathbb{O} .

5.1 Origami a Doppia Piegia

Ci concentriamo ora su una assiomatizzazione della geometria ottenuta dall'uso di due pieghe simultanee. Il metodo che useremo per individuarne una lista di assiomi è facilmente generalizzabile a numeri arbitrariamente maggiori di pieghe e segue lo stesso filo logico con cui abbiamo enumerato le possibili combinazioni di allineamenti elementari in Sezione 4.4.

Come già abbiamo fatto ci proponiamo di individuare le possibili combinazioni di allineamenti elementari, che sono sempre tre (punto-punto, punto-retta e retta-retta), di oggetti precedentemente individuati e delle tracce delle pieghe. Il numero di vincoli da soddisfare deve stavolta essere 4, mentre nel caso di n pieghe simultanee è $2n$. Poiché il numero di combinazioni di questo tipo cresce con n in maniera esplosiva è conveniente, seguendo l'approccio di [AL09], adottare delle regole per ignorare determinate combinazioni e ridurre così il numero di assiomi.

Definizione 5.1.

Una combinazione di allineamenti è detta separabile se è partizionabile in due combinazioni, ciascuna delle quali corrisponde a un assioma HHJ.

Le combinazioni separabili sono quindi quelle che corrispondono all'applicazione *consecutiva* di due pieghe singole, in particolare quelle in cui la scelta di una piega non dipende dalla posizione dell'altra.

¹Il *Teorema di Bezout*, da non confondere con l'omonimo Lemma citato nel Teorema 1.12, afferma che due curve algebriche piane di grado rispettivamente n e m si intersecano in un piano affine in al più mn punti ed esattamente mn punti in un piano proiettivo su un campo algebricamente chiuso.

Definizione 5.2.

Due combinazioni sono equivalenti se i loro allineamenti coincidono a meno di una permutazione degli oggetti geometrici in gioco.

Le combinazioni equivalenti sono quelle che coinvolgono le stesse operazioni su oggetti che, essenzialmente, differiscono tra loro solo per il loro "nome".

Definizione 5.3.

Due combinazioni sono simmetriche se applicare la stessa piega della carta ad entrambi i lati di uno o più dei loro allineamenti le rende equivalenti.

Le combinazioni simmetriche sono essenzialmente quelle che differiscono per la scelta di quale porzione di foglio sia statica e quale si muova attraverso la piega. Due allineamenti simmetrici sono ad esempio $r(P_1) \leftrightarrow L_2$ e $r(L_1) \leftrightarrow P_2$, infatti l'applicazione ad uno dei due della piega su r in entrambi i membri li rende equivalenti a meno dello scambio degli indici 1, 2.

Definizione 5.4.

Due combinazioni sono distinte se non sono simmetriche né equivalenti.

Le combinazioni che costituiscono gli assiomi degli origami a doppia piega sono quelle *distinte e non separabili*. Si trovano dieci allineamenti con queste caratteristiche, di cui tre interessano in modo simmetrico entrambe le linee di piegatura. Questo porta il totale degli allineamenti possibili a diciassette: i dieci essenzialmente differenti più le sette varianti di quelli suscettibili all'inversione di ruolo delle pieghe. I dieci allineamenti sono riportati in Tabella 5.1, dove a e b sono le linee di piegatura e P e L rappresentano punti e rette già individuati, ciascuno eventualmente coi suoi indici.

$AL1$, $AL8$ e $AL9$ non sono interessati dallo scambio delle pieghe, gli altri sono denotati con un suffisso a o b a seconda che la loro applicazione sia riferita a una o all'altra linea di piegatura.

Dal momento che ciascuno di questi allineamenti impone uno o due vincoli sui gradi di libertà delle pieghe ogni assioma dev'essere costituito da combinazioni di due, tre o quattro di queste combinazioni. Alperin e Lang in [AL09] individuano, assistiti dal software *Mathematica*, 489 distinti assiomi per gli origami a doppia piega. Questi assiomi sono denotati $ALxyzw$, dove ciascuna variabile viene sostituita con un numero da 1 a 10 ed eventualmente una lettera a o b a seconda delle combinazioni usate, senza ripetere il numero quando due varianti della stessa combinazione sono usate in successione.

La doppia piega che costituisce l'esempio all'inizio del capitolo è $AL6ab8$, consistendo cioè di due combinazioni $AL6$ (punto-retta), ciascuna su una piega diversa, e poi di $AL8$ (punto-punto).

AL1	$a(b) \leftrightarrow b$	allineamento simultaneo delle due pieghe
AL2a	$a(L) \leftrightarrow L$	allineamento di una retta con sé stessa
AL3a	$a(P) \leftrightarrow P$	allineamento di un punto con sé stesso
AL4a	$a(L) \leftrightarrow b$	allineamento di una retta con l'altra piega
AL5a	$a(P) \leftrightarrow b$	allineamento di un punto con l'altra piega
AL6a	$a(P) \leftrightarrow L$	allineamento di un punto e una retta
AL7a	$a(P) \leftrightarrow b(L)$	portare un punto e una retta ad allinearsi
AL8	$a(P_1) \leftrightarrow b(P_2)$	portare due punti ad allinearsi
AL9	$a(L_1) \leftrightarrow b(L_2)$	portare due rette ad allinearsi
AL10a	$a(b \wedge L_1) \leftrightarrow L_2$	portare su una retta un'intersezione con l'altra piega

Tabella 5.1: Le 10 combinazioni di due pieghe simultanee

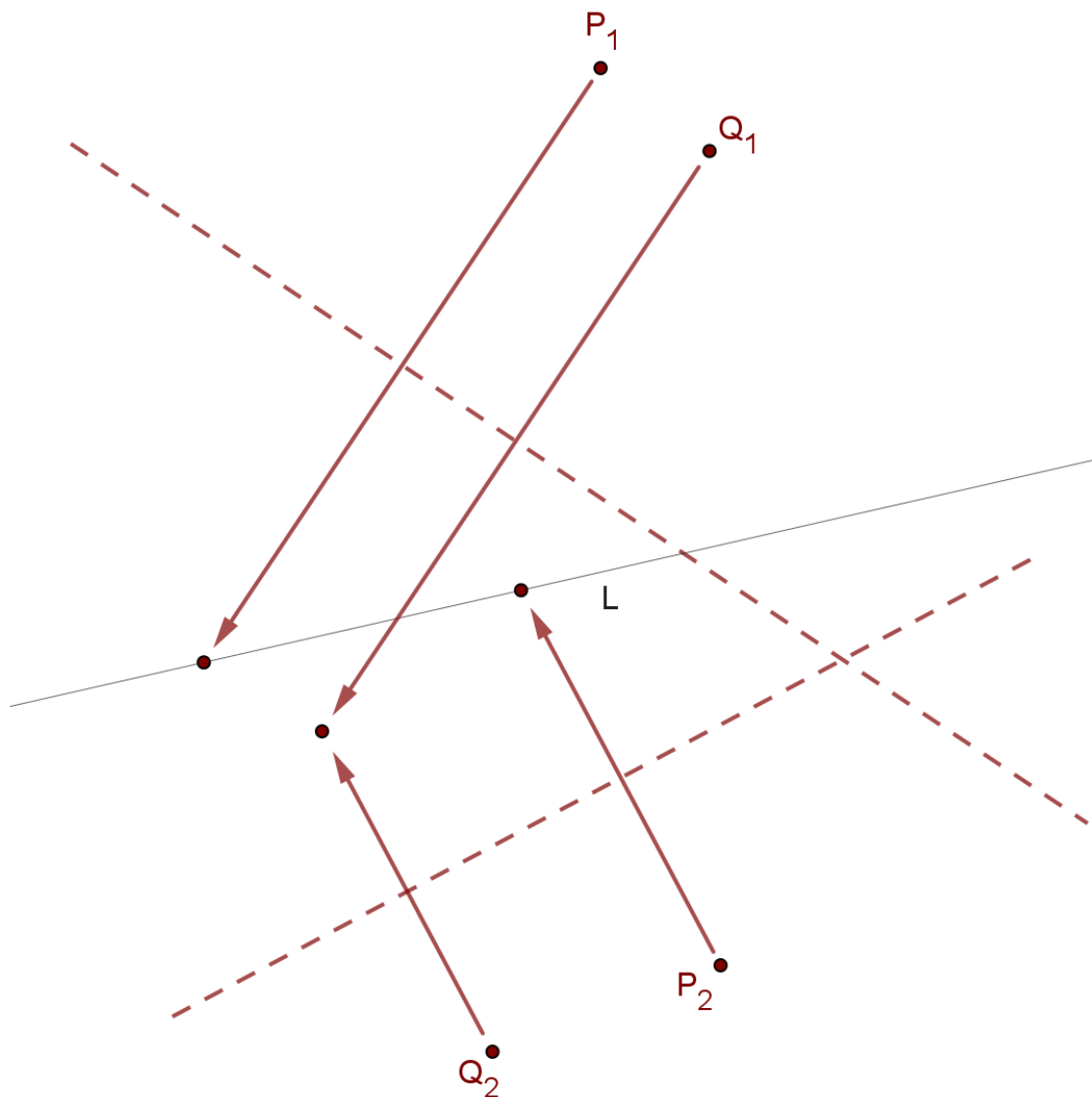


Figura 5.1: AL6ab8 nel caso in cui $L_1 = L_2 := L$

5.2 Il Metodo di Lill

La nostra intenzione rimane sempre quella di generalizzare la soluzione al problema della ciclotomia, che al momento è data dal Teorema 4.7. L'argomento che abbiamo usato per provare sia il Teorema 2.1 che il Teorema 4.7 si basa sulla struttura a torre delle estensioni contenenti i numeri costruibili o i numeri origami, provata rispettivamente nei Corollari 3.3.1 e 4.6.1. Questa struttura a torre deriva essenzialmente dalla chiusura dei campi per soluzioni di equazioni di grado 2 (in entrambi i casi) e di grado 3 (per gli origami a piega singola).

L'insieme dei numeri costruibili tramite n pieghe simultanee è un campo che estende \mathbb{O} . La dimostrazione segue semplicemente dallo scegliere tutte pieghe in modo che le loro tracce coincidano con la stessa retta e che di conseguenza esse "non abbiano effetto" oltre la prima piega. In questo modo ogni costruzione nella dimostrazione del Teorema 4.4 è ripetibile di pari passo. Basterebbe quindi provare che attraverso l'uso di pieghe simultanee è possibile risolvere equazioni di grado superiore al terzo per poterne dedurre i gradi possibili delle estensioni che compongono la torre.

Nel 1867 l'ingegnere austriaco Eduard Lill pubblicò un articolo, qui [Lil67], in cui si proponeva un metodo grafico per trovare le radici reali di equazioni polinomiali di una variabile e qualsiasi grado. Con riferimento ad un polinomio

$$p(x) = \sum_{n=0}^d a_n x^n$$

per risolvere $p(x) = 0$ si procede come segue:

1. si fissa un verso a partire dall'origine O degli assi cartesiani, ad ogni passo il verso ruota di $\frac{\pi}{2}$ in senso antiorario;
2. al passo n -esimo si traccia un segmento di lunghezza a_{d-n} nel verso opportuno se questo coefficiente è positivo, in quello opposto altrimenti, raggiungendo il punto A_n ;
3. dopo $d+1$ passi è stata tracciata una linea spezzata ad angoli retti, il cui punto finale è detto $T := A_d$;
4. si cerca una seconda linea spezzata ad angoli retti tale che il punto d'origine sia O , il punto finale sia T e i suoi vertici giacciono ordinatamente sugli spigoli o sui prolungamenti degli spigoli della spezzata originale, inoltre
5. ad ogni vertice si prosegue nello stesso semipiano se il punto di contatto è su uno spigolo, nel semipiano opposto se il contatto è sul prolungamento di uno spigolo.

Una volta che tale linea spezzata è stata individuata il coefficiente angolare² m del primo spigolo, quello uscente da O , è tale che $p(-m) = 0$.

Facciamo un esempio, riportato in Figura 5.2, col polinomio

$$p(x) = 2x^4 - 7x^3 + 5x^2 + x + 2$$

L'ordine delle direzioni in cui tracciare i segmenti della spezzata per coefficienti positivi è: destra, su, sinistra, giù. Partendo dal coefficiente direttore tracciamo dunque un segmento verso destra di lunghezza 2 fino al vertice A_0 , poi uno verso l'alto di lunghezza -7 (dunque verso il basso) individuando A_1 , poi verso sinistra di 5 per A_2 , verso il basso di 1 fino a A_3 e infine verso destra di 2, individuando il punto $T = A_4$. Cerchiamo ora una seconda linea spezzata ad angoli retti che origini da O e i cui vertici siano nell'ordine sulle rette contenenti: $OA_0, A_0A_1, A_1A_2, A_2A_3, A_3T$. L'ultimo vertice di questa spezzata deve essere T . Una tale traiettoria può essere pensata come quella di un raggio di luce che si riflette ad angolo retto sul corpo dei segmenti e rifrange ad angolo retto sui loro prolungamenti. Un esempio di questo raggio di luce è quello il cui coefficiente angolare in O è $m = -2$. In effetti $p(-2) = 0$.

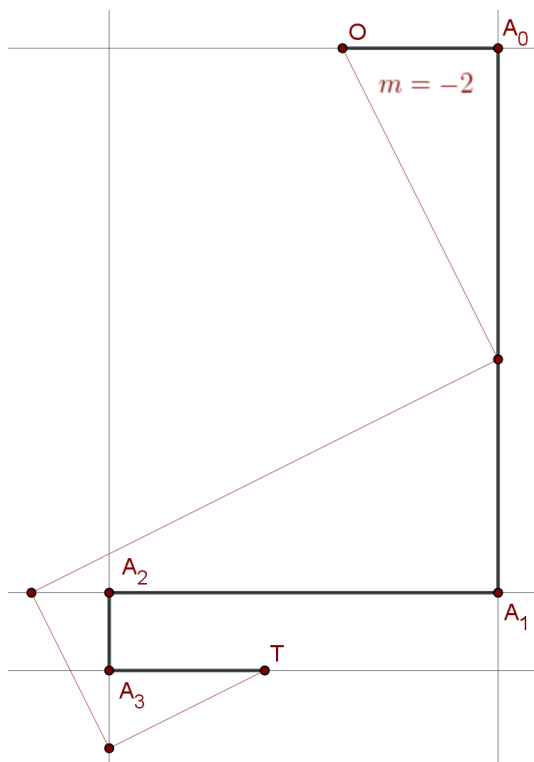


Figura 5.2: Il Metodo di Lill applicato a $2x^4 - 7x^3 + 5x^2 + x + 2$

²Il coefficiente angolare dello spigolo è determinato identificando con la direzione del primo spigolo della spezzata originale l'asse positivo delle ascisse.

Il motivo per cui questo metodo grafico funziona è da ricondursi alla *rappresentazione di Horner*³:

$$p(x) = a_0 + x (a_1 + x (a_2 + x (\dots (a_{d-1} + a_d x) \dots)))$$

La costruzione proposta da Lill efficacemente valuta il polinomio $p(x)$ in $-m$, dove m è il coefficiente angolare scelto per il "raggio di luce" uscente da O nel semipiano contenente A_0 . Facciamo riferimento a Figura 5.3.

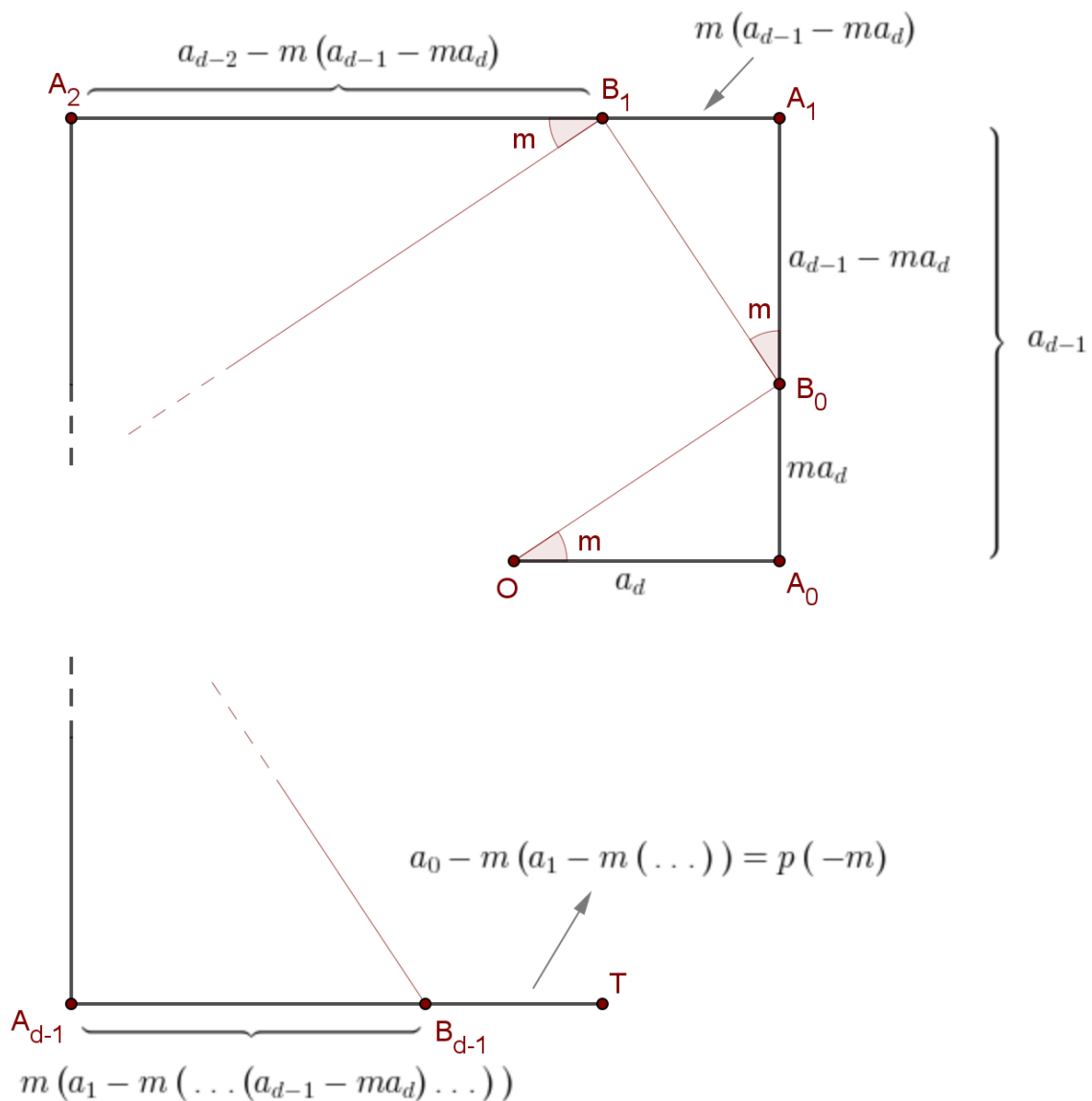


Figura 5.3: La Rappresentazione di Horner realizzata attraverso il Metodo di Lill

³William G. Horner, matematico britannico vissuto a cavallo tra i secoli XVIII e XIX. Egli stesso attribuisce questo metodo di valutazione di un polinomio, che prende il suo nome e che si basa sulla rappresentazione annidata, a Lagrange.

Se chiamiamo B_0, B_1, \dots, B_{d-1} i punti di riflessione o rifrazione del raggio di luce è chiaro che la distanza $B_{d-1}T$ corrisponde a $p(-m)$ e dunque che

$$p(-m) = 0 \iff T = B_{d-1}$$

cioè $-m$ è una radice di p se e solo se il raggio di luce lanciato con pendenza m colpisce T .

Questo metodo grafico è quindi estremamente efficace e in effetti individua tutte e sole le radici del polinomio, ma come facciamo a stabilire, a priori, le angolazioni giuste con cui lanciare il raggio?

Equazioni Quadratiche

Nel caso delle equazioni quadratiche determinare il percorso del "raggio di luce" è semplice e si può fare con riga e compasso congiungendo OT e tracciando la circonferenza che ha questo segmento per diametro. Tale circonferenza interseca la retta $A_0 \vee A_1$ in un massimo, a seconda dell'esistenza di radici reali all'equazione, di due punti. Per un noto risultato della Geometria Euclidea quei due punti di intersezione sono vertici di angoli retti i cui spigoli passano per O e T e individuano dunque il tracciato di Lill. Come si è già discusso nella Sezione 4.3, il coefficiente angolare di una retta costruibile è un numero costruibile.

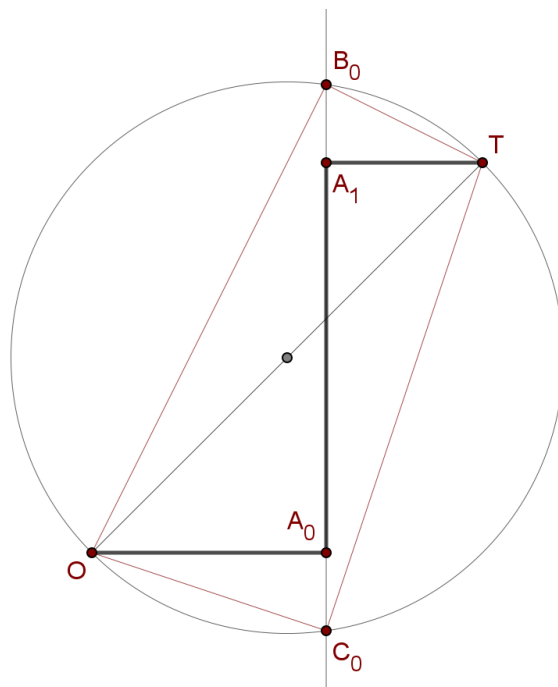


Figura 5.4: Un Esempio con $3x^2 + 5x - 2$

Un risultato analogo si può ottenere con gli origami classici portando con la piega di traccia $A_0 \vee A_1$ i punti O e T nei loro riflessi O' e T' . Per questi tracciamo, grazie al Teorema 4.2, le parallele a $A_0 \vee A_1$. Chiamiamo queste rette rispettivamente L_O e L_T .

Usando ora O5 individuuiamo, se esistono, quelle pieghe che portano O su $O'' \in L_O$, r , e T su $T'' \in L_T$, s .

r e s intersecano $A_0 \vee A_1$ rispettivamente in C_0 e B_0 . Gli angoli $\angle OB_0T$ e $\angle OC_0T$ sono retti perché i loro vertici sono rispettivamente i punti medi di OO'' e TT'' e le pieghe ne sono gli assi.

r e s , insieme ai segmenti B_0T e OC_0 , individuano gli stessi tracciati per il raggio di luce che avevamo individuato con riga e compasso nell'Immagine 5.4. Questa costruzione si trova in Immagine 5.5.

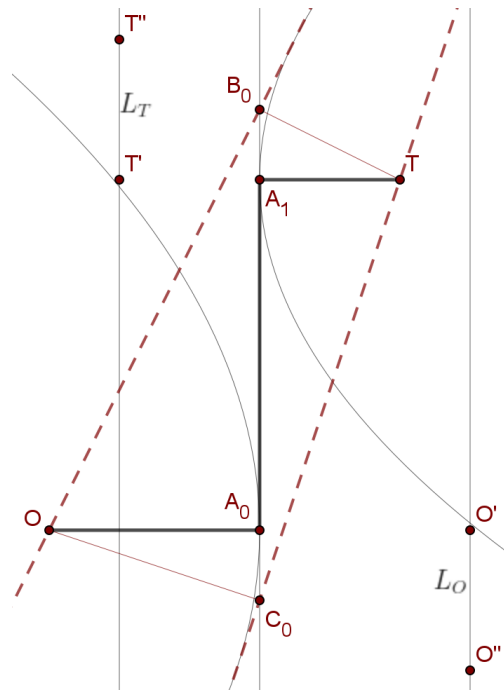


Figura 5.5: Di nuovo $3x^2 + 5x - 2$, con gli Origami a Piega Singola

Equazioni Cubiche: Il Quadrato di Beloch

Nel 1936, come riportato da Hull in [Hul11], la matematica italiana Margherita Piazzolla Beloch provò di poter utilizzare l'assioma O6 per costruire un particolare quadrato che da allora prende il nome di *Quadrato di Beloch*.

Teorema 5.1 (Quadrato di Beloch).

Assegnati due punti O e T distinti e due rette incidenti r e s è tracciabile un quadrato che abbia un vertice su r e uno su s , e i cui spigoli siano contenuti in rette passanti per O e T .

Dimostrazione.

Si traccino L_O e L_T , rette parallele a r e s passanti rispettivamente per i riflessi O' di O su r e T' di T su s .

Come dimostrato da Lucero in [Luc19b] esiste una piega che soddisfa O6 se e solo se

la distanza tra i punti da muovere è maggiore di quella fra le rette bersaglio. Questo in particolare è vero se i punti sono distinti e le rette incidenti. Usiamo dunque O6 per portare O su L_O e T su L_T , individuando rispettivamente O'' e T'' . Come più volte si è osservato la piega individuata è l'asse di entrambi i segmenti OO'' e TT'' , di cui chiamiamo B_0 e B_1 i punti medi. Il segmento B_0B_1 è il lato del *Quadrato di Beloch*, che può essere completato riportandone la misura sulle rette $O \vee O''$ e $T \vee T''$. \square

Si osservi che questa costruzione individua di fatto una spezzata a tre spigoli e ad angoli retti dal punto O al punto T e che per il Teorema 1.5 i punti $B_0 B_1$ non possono che trovarsi sulle rette che nell'ipotesi sono chiamate r e s .

Se dunque per r e s prendiamo le rette contenenti i segmenti A_0A_1 e A_1A_2 nella costruzione di Lill per un polinomio cubico la costruzione di Beloch⁴ produce esattamente il tracciato di un raggio di luce da O a T .

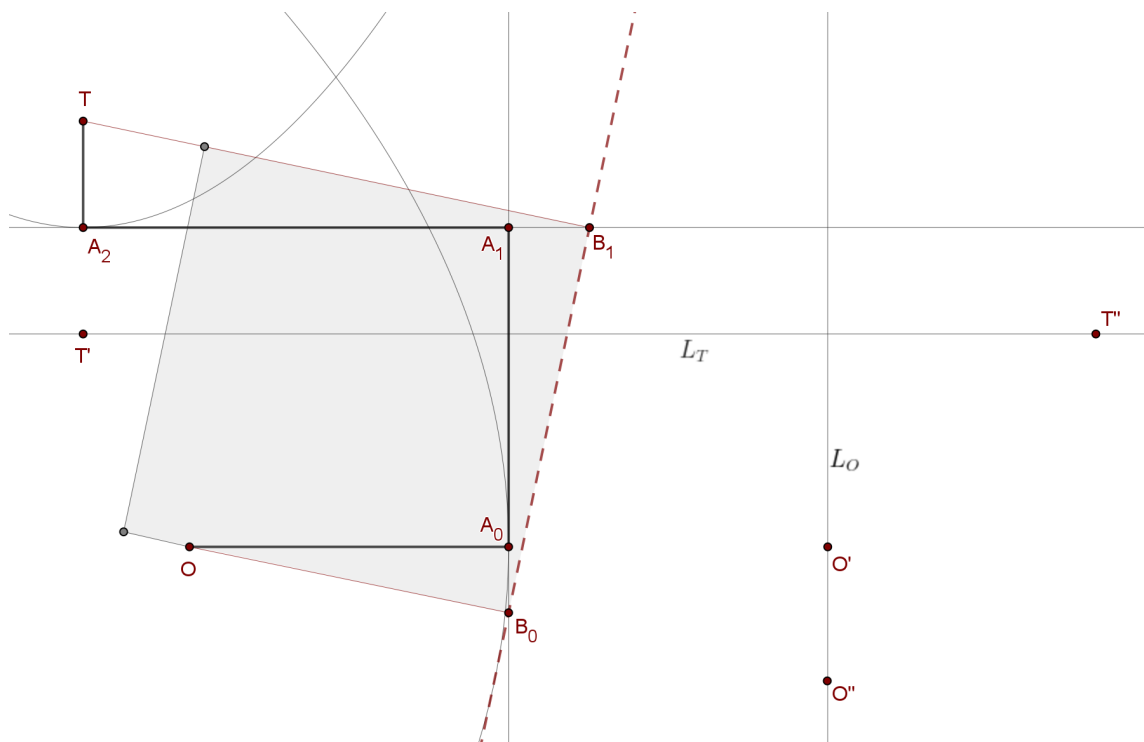


Figura 5.6: $3x^3 + 3x^2 + 4x - 1$ evidenziando il Quadrato di Beloch.

La costruzione per questo tracciato ad angoli retti procede esattamente come nella dimostrazione del Teorema 5.1:

1. si costruisce la spezzata di base secondo l'algoritmo di Lill;
2. si piegano O e T rispettivamente su $A_0 \vee A_1$ e $A_1 \vee A_2$, individuando O' e T' ;

⁴Si osservi che nel caso della spezzata di Lill le due rette bersaglio L_O, L_T sono *necessariamente* incidenti. Questo fatto è equivalente all'esistenza di almeno una radice reale a qualsiasi equazione cubica a coefficienti reali.

3. si tracciano le parallele L_O e L_T per O' e T' rispettivamente alle rette $A_0 \vee A_1$ e $A_1 \vee A_2$;
4. si applica O6 portando O su L_O e T su L_T , individuando la piega che interseca $A_0 \vee A_1$ in B_0 e $A_1 \vee A_2$ in B_1 ;
5. si aggiungono i segmenti OB_0 e B_1T completando il tracciato di Lill.

Equazioni Quartiche e Gradi Superiori

Beloch ha dimostrato l'esistenza di una piega⁵ che individua il tracciato di Lill per le equazioni cubiche sfruttando essenzialmente una singola idea geometrica. Fissiamo la parabola di fuoco O e direttrice d e tracciamo per il vertice della parabola la retta parallela a d , diciamo r . Scegliamo una tangente alla parabola e supponiamo che O' sia il riflesso di O su questa tangente, e chiamiamo B il punto di intersezione $r \wedge OO'$. In questo caso l'angolo formato da OB e da r in B è sempre retto. Ciò è vero, come abbiamo già notato, semplicemente perché la piega è l'asse di OO' , il cui punto medio appartiene a r .

Torniamo brevemente alle pieghe elementari elencate in Tabella 5.1. Nel caso di origami con più di due pieghe simultanee quella tabella non è esaustiva, ma resta valida. Esistono allineamenti che non vi sono descritti, ma tutti gli allineamenti descritti sono elementari anche per più di due pieghe simultanee, semplicemente non ponendo condizioni sulle restanti pieghe. La differenza essenziale è che una combinazione di allineamenti elementari, per costituire un valido *assioma* per la teoria delle n pieghe simultanee, deve consumare $2n$ gradi di libertà. Si noti, osservando Tabella 4.1, che lo stesso assioma O6 nasce come combinazione di due allineamenti del tipo AL6 su punti distinti.

Nel caso di un'equazione quartica la spezzata individuata dal metodo di Lill è $OA_0A_1A_2A_3T$. Un valido esempio di questa situazione è già in Figura 5.2, dove il raggio di luce è la spezzata $OB_0B_1B_2T$, ammesso di nominare B_i il punto di riflessione o rifrazione sulla retta $A_i \vee A_{i+1}$.

Basandoci sul ragionamento appena concluso sappiamo di poter individuare simultaneamente due pieghe della carta, $B_0 \vee B_1$ e $B_1 \vee B_2$, in modo che $\angle OB_0B_1$ e $\angle TB_2B_1$ siano retti, combinando due allineamenti AL6. Queste due richieste corrispondono a due vincoli, uno ciascuna, sui quattro gradi di libertà delle equazioni delle due pieghe.

Sono sufficienti i due gradi rimanenti per imporre che l'intersezione B_1 descriva un angolo retto e si trovi sulla retta $A_1 \vee A_2$? La risposta è Sì.

⁵Questa piega è quella individuata da O6. Ci si riferisce a questo assioma, per questo motivo, anche col nome di *Beloch Fold*.

Come più volte abbiamo fatto chiamiamo O', T' i riflessi di O, T rispettivamente sul secondo e penultimo segmento del tracciato e L_O, L_T le parallele per O', T' a questi segmenti. Indichiamo per semplicità con r la retta $A_1 \vee A_2$ e consideriamo il seguente schema di allineamenti per le pieghe a, b :

AL6a	$a(O) \leftrightarrow L_O$
AL6b	$b(T) \leftrightarrow L_T$
AL1	$a(b) \leftrightarrow b$
AL10b	$b(a \wedge r) \leftrightarrow r$

Tabella 5.2: Allineamento AL16ab10b

I primi due allineamenti determinano la traiettoria del raggio in uscita da O e in entrata in T , e con queste il primo e l'ultimo angolo retto. AL1 impone $a \perp b$. AL10b, il più complicato fra gli allineamenti, forza l'incidenza fra a e r a rimanere, portato da b , sulla retta r . Avendo impiegato AL1 però b porta quell'intersezione necessariamente in un punto della retta a , e dunque questa combinazione non può che fissare l'intersezione $a \wedge r$ rendendola punto di passaggio di entrambe le pieghe, che vi si incontrano ad angolo retto. Questa combinazione, che con le regole descritte chiamiamo AL16ab10b, consiste di tre allineamenti punto-retta e di un allineamento di una retta con sé stessa. Ciascuno di questi consuma precisamente un grado di libertà portando il totale delle condizioni imposte a quattro, individuando così a e b in modo esatto⁶.

Proviamo ad estendere questo ragionamento ad un'equazione quintica⁷. Facciamo riferimento all'esempio di $2x^5 + 5x^4 + 3x^3 + x^2 + 2x - 2$ in Figura 5.7.

Usiamo AL6 per imporre che il secondo e il penultimo tratto del raggio di luce formino rispettivamente con OB_0 e B_4T angoli retti. Dobbiamo poi individuare, insieme a queste due pieghe, una terza piega che sia perpendicolare ad entrambe ed intersechi la prima su $A_1 \vee A_2 := r$ e la seconda su $A_1 \vee A_3 := s$. Questo risultato è ottenibile, in generale in modo non unico, attraverso la combinazione di allineamenti in Tabella 5.3.

⁶Ammesso che esista almeno una soluzione reale alla quartica in esame.

⁷Analogamente alla cubica se i coefficienti sono reali esiste sempre almeno una radice reale e questo garantisce l'applicabilità di ogni allineamento in almeno un modo.

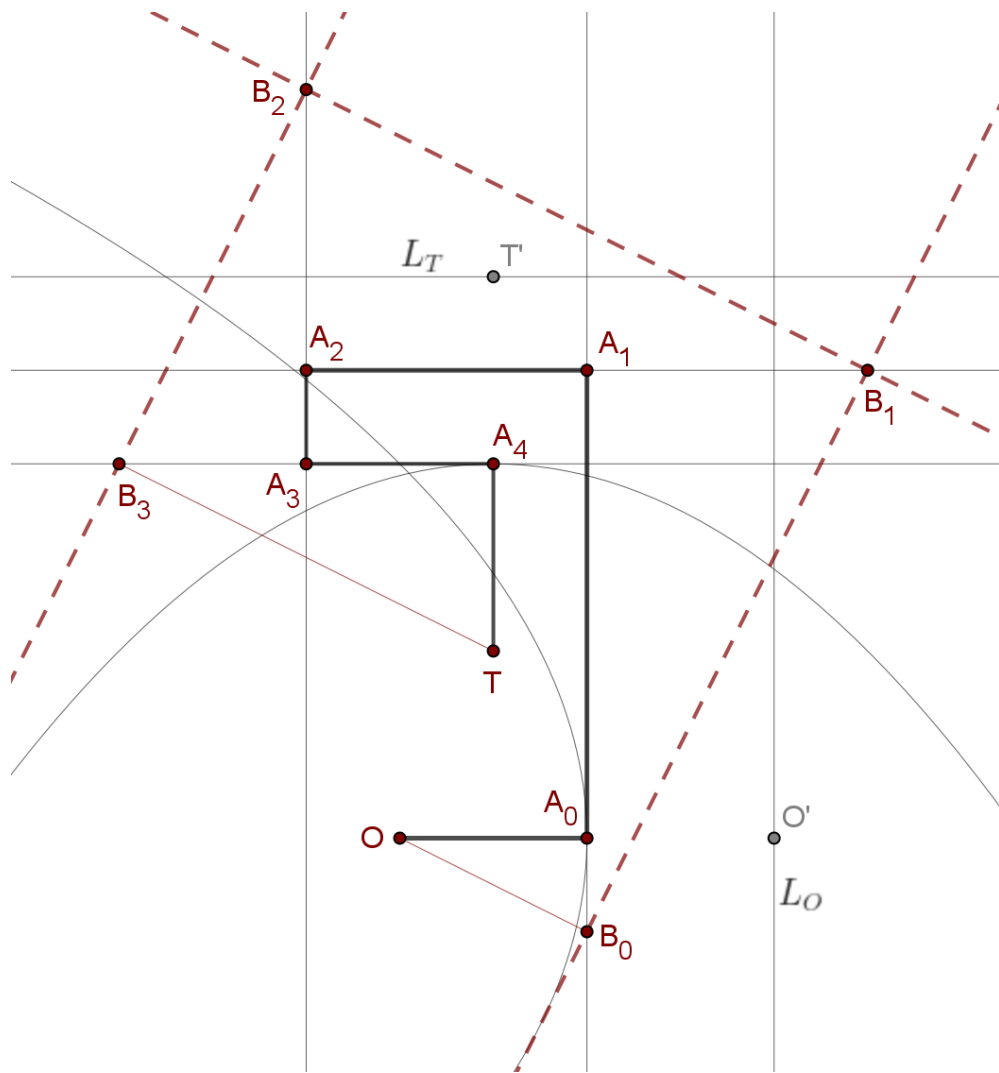


Figura 5.7: $2x^5 + 5x^4 + 3x^3 + x^2 + 2x - 2$ attraverso l'uso di tre pieghe simultanee

AL6a	$a(O) \leftrightarrow L_O$
AL6c	$c(T) \leftrightarrow L_T$
AL1a,b	$a(b) \leftrightarrow b$
AL10a,b	$b(a \wedge r) \leftrightarrow r$
AL1b,c	$b(c) \leftrightarrow c$
AL10b,c	$c(b \wedge s) \leftrightarrow s$

Tabella 5.3: La combinazione di allineamenti per la soluzione di una quintica

In generale seguendo lo stesso schema possiamo usare $n - 2$ pieghe simultanee per risolvere un'equazione polinomiale di grado n con almeno una radice reale. Queste $n - 2$ pieghe sono individuate da due utilizzi di AL6 per il primo e l'ultimo tratto di raggio coi relativi angoli retti, insieme a $n - 4$ applicazioni in coppia di AL1 e AL10 per garantire che le pieghe intermedie siano consecutivamente incidenti sulle rette opportune e perpendicolari.

Per induzione si dimostra dunque che

Teorema 5.2.

Il campo dei numeri costruibili con $n - 2$ pieghe simultanee della carta è chiuso sulle radici reali di polinomi di grado al più n e in particolare è chiuso per radici n -esime.

Identificando, come abbiamo già fatto, i punti del piano con gli elementi di \mathbb{C} e le loro coordinate con le parti reale e immaginaria, ed estendendo di conseguenza il concetto di *numero costruibile*, dal Teorema 5.2 si può rimuovere l'ipotesi che le radici siano reali.

5.3 I Poligoni Multi-Fold

Siamo pronti a riprendere in mano la struttura a torre del campo dei numeri origami e dedurne una nuova condizione di costruibilità per i poligoni regolari. Questa volta possiamo andare in una sola direzione, perché al contrario dei casi precedenti non possiamo trarre conclusioni sui gradi delle estensioni come nei Corollari 3.3.1 e 4.6.1.

Il motivo per cui non siamo in grado di ragionare in entrambe le direzioni è che stavolta non abbiamo garanzie sul fatto che applicare un assioma per le pieghe simultanee corrisponda a risolvere un'equazione di un grado specifico, e in particolare che l'applicazione di *qualunque* assioma delle n -pieghe simultanee corrisponda alla soluzione di un'equazione di grado *al più* $n + 2$. Di conseguenza non siamo in grado di ricostruire la struttura a torre osservando l'algoritmo di costruzione.

Teorema 5.3.

Sia $\zeta \in \mathbb{C}$. Supponiamo che esista una torre di estensioni

$$\mathbb{Q} = F_0 < F_1 < \dots < F_h < \mathbb{C}$$

tale per cui $\zeta \in F_h$ e

$$\forall i = 1, \dots, h \left([F_i : F_{i-1}] \in \{2, 3, \dots, k\} \right)$$

Allora ζ è costruibile usando $k - 2$ pieghe simultanee della carta.

Dimostrazione.

Come abbiamo già visto \mathbb{Q} è costruibile con qualsiasi numero di pieghe della carta. I numeri contenuti in ogni estensione sono radici di polinomi a coefficienti nell'estensione precedente e di grado al più k , cioè sono soluzioni di equazioni che, grazie al Teorema 5.2, sono risolubili rimanendo all'interno del campo dei costruibili. Ne segue che ζ è costruibile con gli origami a $k - 2$ pieghe simultanee. \square

Il Teorema 5.3 prova che se un numero complesso è *algebrico* su \mathbb{Q} allora esiste un opportuno numero di pieghe simultanee per il quale quel numero è costruibile. Viceversa al momento non si è ancora trovata prova che se un numero è costruibile con un certo numero di pieghe simultanee allora è algebrico.

Nel caso della riga e del compasso, ad esempio, non solo sapevamo che ogni equazione di grado 2 è risolubile, ma viceversa anche che eseguire una qualsiasi dei tre tipi di intersezione implica risolvere un'equazione di grado 2. Nel caso degli origami a piega singola sappiamo che tutte le equazioni quadratiche e cubiche sono costruibili, che l'applicazione di O6 è *equivalente* alla soluzione di una cubica e che tutti gli altri assiomi individuano estensioni raggiungibili con riga e compasso, cioè di ordine 2.

Nel caso delle pieghe simultanee questo tipo di equivalenze, se c'è, non è ancora stato provato. In termini algebrici ciò che non sappiamo è se sia vero che, se $\zeta \in \mathbb{C}$ è costruibile con n pieghe simultanee a partire dall'estensione $\frac{K}{\mathbb{Q}}$, allora si trova in un'estensione $\frac{M}{K}$ con il grado $[M : K] \leq n + 2$.

Definizione 5.5 (Numero Liscio).

$n \in \mathbb{N}$ è detto numero k -liscio se tutti i suoi fattori primi sono minori o uguali a k .

Teorema 5.4.

Se $\varphi(n)$ è un numero k -liscio allora il n -gono è costruibile con $k - 2$ pieghe simultanee della carta.

Dimostrazione.

La dimostrazione è del tutto analoga a quella del Teorema 4.7. Se la condizione sul toziente di n è vera allora la n -esima estensione ciclotomica di \mathbb{Q} ha una catena di estensioni intermedie che rispetta la forma del Teorema 5.3 e di conseguenza la radice primitiva dell'unità è costruibile, e con essa il n -gono. \square

La condizione sulla fattorizzazione di n in realtà è strettamente legata a quella sul suo toziente e continua a valere, ma è difficilmente esplicitabile poiché non esiste una formula per esprimere il k -esimo numero primo. Ad ogni modo, per esempio quando $k = 5$, rimane vero che se

$$n = 2^a 3^b 5^c p_1 \dots p_h$$

allora il n -gono è costruibile con 3 pieghe simultanee della carta, dove i primi p_i , distinti, hanno la forma $2^s 3^t 5^u + 1$. Tali primi sono detti *primi di Pierpont generalizzati*.

5.4 Un Esempio: L'Endecagono

Per concludere questa tesi vediamo un ultimo esempio. Questo esempio, la costruzione del 11-gono o Endecagono, ha un valore doppio. Da un lato la costruzione mostrerà esplicitamente l'utilizzo di pieghe simultanee, dall'altro lo farà in numero minore di quanto ci aspettiamo, andando a sottolineare la *non-necessità* della condizione nel Teorema 5.4.

Nel caso di $p = 11$ si ha $p - 1 = 2 \cdot 5$ dunque, grazie alle conclusioni di carattere generale che abbiamo tratto nella Sezione 4.6 studiando L'Eptagono, il polinomio minimo di $c_{11} := \cos\left(\frac{2\pi}{11}\right)$ ha grado 5. Ricaviamo questo polinomio seguendo esattamente gli stessi passaggi svolti per il 7-gono⁸. Con la notazione della Sezione 4.6 sia $\zeta := \zeta_{11}$. Si ha

$$x^{-5} \Phi_{11}(x) = x^{-5} \sum_{n=0}^{10} x^n = 1 + \sum_{n=1}^5 \left(x^n + \frac{1}{x^n}\right) \quad (5.1)$$

e sappiamo già che i primi termini dell'ultimo membro di questa uguaglianza corrispondono a:

$$1 + \sum_{n=1}^3 \left(x^n + \frac{1}{x^n}\right) = \left(x + \frac{1}{x}\right)^3 + \left(x + \frac{1}{x}\right)^2 - 2\left(x + \frac{1}{x}\right) - 1$$

Per il termine di ordine cinque si ha invece:

$$\begin{aligned} \left(x + \frac{1}{x}\right)^5 &= x^5 + \frac{1}{x^5} + 5\left(x^3 + \frac{1}{x^3}\right) + 10\left(x + \frac{1}{x}\right) \\ \Leftrightarrow x^5 + \frac{1}{x^5} &= \left(x + \frac{1}{x}\right)^5 - 5\left[\left(x + \frac{1}{x}\right)^3 - 3\left(x + \frac{1}{x}\right)\right] - 10\left(x + \frac{1}{x}\right) \\ &= \left(x + \frac{1}{x}\right)^5 - 5\left(x + \frac{1}{x}\right)^3 + 5\left(x + \frac{1}{x}\right) \end{aligned}$$

In modo simile il termine di grado quattro diventa:

$$\begin{aligned} \left(x + \frac{1}{x}\right)^4 &= x^4 + \frac{1}{x^4} + 4\left(x^2 + \frac{1}{x^2}\right) + 6 \\ \Leftrightarrow x^4 + \frac{1}{x^4} &= \left(x + \frac{1}{x}\right)^4 - 4\left[\left(x + \frac{1}{x}\right)^2 - 2\right] - 6 \\ &= \left(x + \frac{1}{x}\right)^4 - 4\left(x + \frac{1}{x}\right)^2 + 2 \end{aligned}$$

Sostituendo queste informazioni in (5.1) deduciamo che:

$$\left(x + \frac{1}{x}\right)^5 + \left(x + \frac{1}{x}\right)^4 - 4\left(x + \frac{1}{x}\right)^3 - 3\left(x + \frac{1}{x}\right)^3 + 3\left(x + \frac{1}{x}\right) + 1 = 0$$

⁸Si noti che questo algoritmo per ricavare il polinomio minimo di c_p è valido per qualsiasi primo p tale che $p - 1 = 2q$, con q a sua volta primo. 7 e 11 sono di questa forma. Questo è vero perché, tolto il fatto di grado 2 legato all'estensione $\mathbb{Q}(\zeta_p)/\mathbb{Q}(c_p)$, il fattore rimanente ha grado q ed è dunque irriducibile.

Il polinomio minimo di $2c_{11}$, che corrisponde all'equazione quintica che è necessario risolvere, è quindi:

$$z^5 + z^4 - 4z^3 - 3z^2 + 3z + 1 \quad (5.2)$$

La teoria che abbiamo esaminato prevede che sia sufficiente usare tre pieghe simultanee per risolvere questa equazione. Tale conclusione si basa sull'uso del Metodo di Lill ma non ci sono risultati generali circa la soluzione di equazioni polinomiali con costruzioni differenti. In questo caso specifico tuttavia è stato di recente dimostrato da Nishimura in [Nis15] e Lucero in [Luc18b] che la quintica generale possa essere risolta usando solo due pieghe simultanee.

In un modo molto simile a quello con cui O_6 risolve le equazioni cubiche, in [Luc18b] si mostra che l'assioma delle due pieghe simultanee $AL4a6ab$ si può utilizzare per risolvere le equazioni quintiche. Si torni per riferimento alla Tabella 5.1.

Consideriamo due punti $P = (-\frac{5}{2}, -3)$, $Q = (0, 1)$ e tre rette $l : x = 0$, $s : m = -\frac{3}{2}$ e $n : y = -1$. Usiamo $AL4a6ab$ per trovare quelle pieghe a, b che realizzano il seguente schema di allineamenti:

$$\begin{array}{l|l} AL4a & a(l) \leftrightarrow b \\ AL6a & a(Q) \leftrightarrow n \\ Al6b & b(P) \leftrightarrow m \end{array}$$

Tabella 5.4: Allineamento $AL4a6ab$

Si osservi che in questo caso specifico $Q \in l$ e di conseguenza $Q' := a(Q) = n \wedge b$ come si può vedere in Figura 5.8. Questo implica che a e b sono incidenti in un punto che chiamiamo S .

Parametizziamo $Q' = (2t, -1)$ e $P' = (-\frac{3}{2}, 2s)$. Il punto $R = (t, 0)$ è medio per il segmento QQ' . Verifichiamo che t è radice di (5.2) e di conseguenza⁹ $t = 2c_{11}$. La piega a , in quanto asse di QQ' , ha equazione:

$$a : y = t(x - t)$$

Analogamente b , asse di PP' , ha invece equazione:

$$b : y - s + \frac{3}{2} = -\frac{1}{2s+3}(x+2) \Leftrightarrow y = -\frac{x}{2s+3} + \frac{2s^2 - \frac{13}{2}}{2s+3}$$

Sappiamo già che a deve essere la bisettrice dell'angolo formato in S da b e l , pertanto $S \in l$ e possiamo determinarne l'ordinata imponendo $x = 0$ nell'equazione di a . Si ottiene $S = (0, -t^2)$. Possiamo dunque trovare una seconda equazione per la retta b esprimendola come $S \vee Q'$. Una tale equazione dipende solo da t .

$$b : y = \frac{t^2 - 1}{2t}x - t^2$$

⁹Di nuovo come per il caso del 7-gono si verifica per via analitica che t è la radice a (5.2) di modulo maggiore.

Confrontando le due equazioni per b si ricava il sistema:

$$\begin{cases} \frac{t^2-1}{2t} = -\frac{1}{2s+3} \\ -t^2 = \frac{2s^2-\frac{13}{2}}{2s+3} \end{cases}$$

Dalla prima equazione

$$s = \frac{-t}{t^2-1} - \frac{3}{2} \quad s^2 = \frac{t^2 + 3t(t^2-1) + \frac{9}{4}(t^2-1)^2}{(t^2-1)^2}$$

e sostituendo nella seconda si ricava:

$$-t^2 = 2 \left(\frac{t^2 + 3t(t^2-1) - (t^2-1)^2}{(t^2-1)^2} \right) \left(\frac{1-t^2}{2t} \right)$$

$$t^2 (t^2-1)t = t^2 + 3t(t^2-1) - (t^2-1)^2$$

Pazientemente riordinando i termini deduciamo infine quello che volevamo:

$$t^5 + t^4 - 4t^3 - 3t^2 + 3t + 1 = 0$$

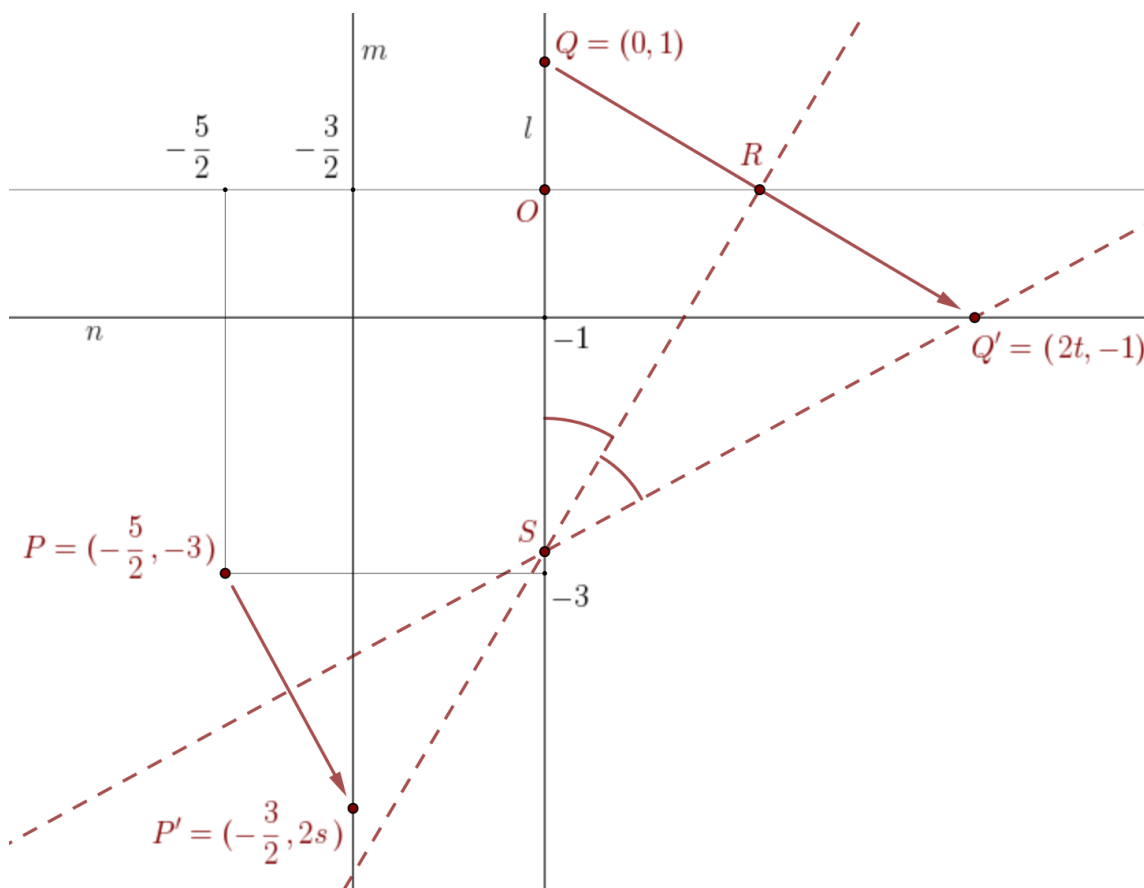


Figura 5.8: La Doppia Piegata per $2c_{11}$

Con le pieghe degli Origami classici, usando O5, possiamo a questo punto completare il triangolo rettangolo in R la cui ipotenusa misura 2 e che ha per cateto OR . Avremo così costruito l'angolo $\frac{2\pi}{11}$ in O e con esso l'Endecagono. Omettiamo le pieghe necessarie a riportare la misura del lato. Con un grigio più scuro è evidenziata la piega in Figura 5.8.

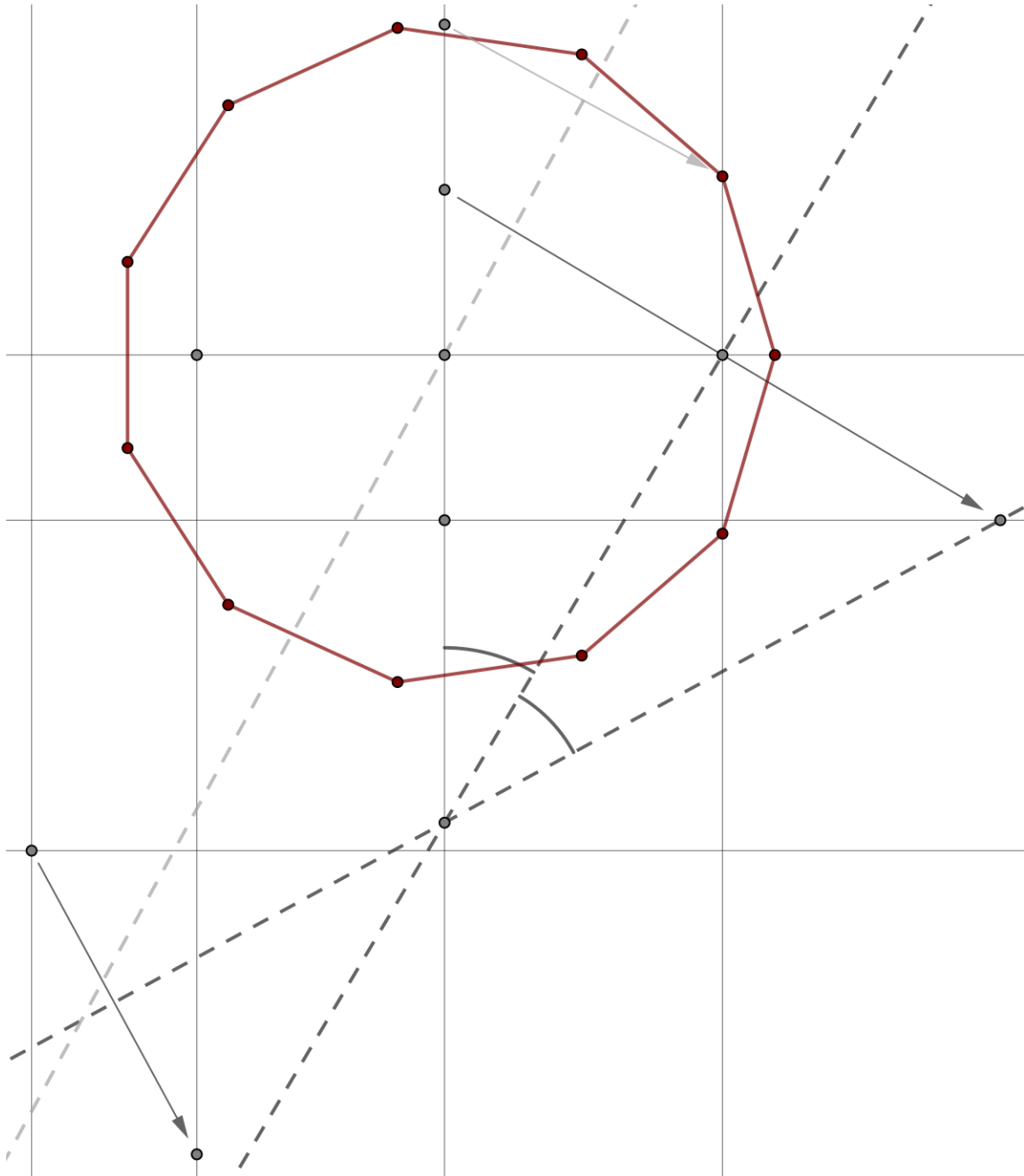


Figura 5.9: Una Costruzione dell'Endecagono con gli Origami a Doppia Piega Simultanea

CONCLUSIONE

Partendo dal contesto familiare della Geometria Euclidea abbiamo determinato una condizione sufficiente di costruibilità per i poligoni regolari basandoci unicamente sulle costruzioni classiche dagli *Elementi*. Questa condizione è il Teorema 1.13.

Ripercorrendo l'opera del *principe dei matematici* Carl Friedrich Gauss, le *Disquisitiones Arithmeticae* del 1801, abbiamo visto questa prima condizione estendersi al Teorema 2.1, la cui dimostrazione è stata portata a termine nel 1837 dal matematico francese Pierre Wantzel. Abbiamo poi parafrasato l'argomento di Wantzel usando un linguaggio matematico più moderno, quello della *Teoria di Galois*. Questa scelta ci ha permesso di cogliere un aspetto della struttura algebrica del problema della ciclotomia che si presta, attraverso una via chiara ma non semplice, ad una generalizzazione.

Abbiamo dunque introdotto un'estensione della Teoria classica della geometria, sviluppatasi alla fine del secolo XX, la Geometria degli Origami, che sostituisce gli strumenti della riga e del compasso con le pieghe della carta. Abbiamo dimostrato che in questa nuova e più estesa teoria lo stesso problema che abbiamo studiato in precedenza ammette una classe di soluzioni più ampia. Questo risultato generalizzato costituisce il Teorema 4.7.

Con l'intenzione di determinare una condizione di costruibilità per il poligono regolare arbitrario e di conseguenza dare una risposta definitiva al problema della ciclotomia, almeno in termini di classificazione, ci siamo spinti in una generalizzazione ulteriore della Teoria degli Origami inserendovi la possibilità di tracciare pieghe *simultanee*. Le conseguenze di questa aggiunta sono correntemente in molti loro aspetti oggetto di studio. Alcuni dei nostri riferimenti risalgono a non prima del biennio 2018-2019, grazie agli articoli del professor Jorge C. Lucero.

Siamo stati in grado di provare una correlazione fra il numero di pieghe simultanee permesse e la risolubilità di equazioni polinomiali di grado crescente e di conseguenza abbiamo raggiunto, anche se solo in una direzione, una caratterizzazione definitiva nel Teorema 5.4. Questo Teorema determina un numero sufficiente di pieghe simultanee per la costruzione di ciascun poligono regolare.

In [AL09], datato 2009, Alperin e Lang ipotizzano che $n - 2$, il numero di pieghe sufficiente a risolvere equazioni polinomiali di grado n , sia anche in tutta generalità minimo, ossia necessario. Questo renderebbe invertibile il Teorema 5.3 e con esso anche il Teorema 5.4. Al momento questa rimane una congettura, alla quale l'unico controesempio trovato finora è quello per il caso $n = 5$.

BIBLIOGRAFIA

- [AL09] Roger C. Alperin e Robert J. Lang. «One-, two-, and multi-fold origami axioms». In: *Origami*⁴. A K Peters, Natick, MA, 2009, pp. 371–393. DOI: [10.1201/b10653-37](https://doi.org/10.1201/b10653-37). URL: <https://doi.org/10.1201/b10653-37>.
- [Gau66] Carl Friedrich Gauss. *Disquisitiones Arithmeticae*. Translated into English by Arthur A. Clarke, S. J. Yale University Press, New Haven, Conn.-London, 1966.
- [Hul09] Thomas Hull. «Folding Regular Heptagons». In: feb. 2009, pp. 181–191. ISBN: 978-1-56881-315-8. DOI: [10.1201/b10580-22](https://doi.org/10.1201/b10580-22).
- [Hul11] Thomas C. Hull. «Solving cubics with creases: the work of Beloch and Lill». In: *Amer. Math. Monthly* 118.4 (2011), pp. 307–315. ISSN: 0002-9890. DOI: [10.4169/amer.math.monthly.118.04.307](https://doi.org/10.4169/amer.math.monthly.118.04.307). URL: <https://doi.org/10.4169/amer.math.monthly.118.04.307>.
- [Joy98] David E. Joyce. *Euclid's Elements*. Department of Mathematics and Computer Science, Clark University. 1998. URL: <http://aleph0.clarku.edu/~djoyce/java/elements/elements.html>.
- [Lan15] Robert J. Lang. *Origami and Geometric Constructions*. Pubblicato sul sito personale dell'autore. 2015. URL: https://langorigami.com/wp-content/uploads/2015/09/origami_constructions.pdf.
- [Lil67] Eduard Lill. «Résolution graphique des équations numériques de tous degrés à une seule inconnue, et description d'un instrument inventé dans ce but». In: *Nouvelles Annales de Mathématique* 6 (1867), pp. 359–362.
- [Luc18a] Jorge C. Lucero. «Construction of a regular hendecagon by two-fold origami». In: *Cruce Mathematicorum* 44 (2018), pp. 207–213. URL: <https://doi.org/10.48550/arXiv.1807.09557>.
- [Luc18b] Jorge C. Lucero. «Geometric solution of a quintic equation by two-fold origami». In: *Int. J. Geom.* 7.1 (2018), pp. 61–68. ISSN: 2247-9880.
- [Luc19a] Jorge C. Lucero. «Division of an angle into equal parts and construction of regular polygons by multi-fold origami». In: *Forum Geom.* 19 (2019), pp. 45–52. DOI: [10.2478/cait-2019-0025](https://doi.org/10.2478/cait-2019-0025). URL: <https://doi.org/10.2478/cait-2019-0025>.

- [Luc19b] Jorge C. Lucero. «Existence of a solution for Beloch's fold». In: *Math. Mag.* 92.1 (2019), pp. 24–31. ISSN: 0025-570X. DOI: [10.1080/0025570X.2019.1526591](https://doi.org/10.1080/0025570X.2019.1526591). URL: <https://doi.org/10.1080/0025570X.2019.1526591>.
- [Nis15] Yasuzo Nishimura. «Solving quintic equations by two-fold origami». In: *Forum Math.* 27.3 (2015), pp. 1379–1387. ISSN: 0933-7741,1435-5337. DOI: [10.1515/forum-2012-0123](https://doi.org/10.1515/forum-2012-0123). URL: <https://doi.org/10.1515/forum-2012-0123>.
- [Sci89] Benedetto Scimemi. «Draw of a regular heptagon by the folding». In: *Proceedings of the First International Meeting of Origami Science and Technology* (1989), pp. 71–77.
- [Suz08] Jeff Suzuki. «A brief history of impossibility». In: *Math. Mag.* 81.1 (2008), pp. 27–38. ISSN: 0025-570X. DOI: [10.1080/0025570x.2008.11953524](https://doi.org/10.1080/0025570x.2008.11953524). URL: <https://doi.org/10.1080/0025570x.2008.11953524>.