Comitato per la Edizione Nazionale delle Opere di

FEDERIGO ENRIQUES

Questioni riguardanti le Matematiche elementari

(III ed.) Zanichelli, Bologna, 1926. (Di Enriques: art. XVII, Sulle equazioni algebriche risolubili per radicali quadratici e sulla costruibilità dei poligoni regolari, pp. 263-305; art. XXIII, Alcune osservazioni generali sui problemi geometrici, pp. 575-596)

L'utilizzo di questo documento digitale è consentito liberamente per motivi di ricerca e studio. Non è consentito l'utilizzo dello stesso per motivi commerciali.

Il presente testo è stato digitalizzato nell'ambito del progetto "Edizione nazionale delle opere di Federigo Enriques"
promosso dal
Ministero per i Beni e le attività Culturali
Area 4 – Area Archivi e Biblioteche
Direzione Generale per i Beni Librari e gli Istituti Culturali

ARTICOLO DICIASSETTESIMO

Sulle equazioni algebriche risolubili per radicali quadratici e sulla costruibilità dei poligoni regolari, di FEDERIGO ENRIQUES a Roma.

La questione di decidere se un problema geometrico costruttivo sia risolubile elementarmente, cioè operando sui dati, colla riga e col compasso, viene ricondotta dalla geometria analitica ad una questione algebrica.

Del modo come tale riduzione si effettua e delle osservazioni ad essa inerenti, discorre il signor CASTELNUOVO nell' articolo XVI. A noi basta qui ricordare la conclusione fondamentale:

Sia proposto un problema geometrico determinato, ricondotto alla ricerca dei punti di un piano che hanno relazioni prestabilite con certi punti dati nel piano stesso; affinchè la costruzione dei punti cercati si possa effettuare operando sui dati (e, se si vuole, anche sopra punti, rette e circoli arbitrari) cogli istrumenti riga e compasso, è condizione necessaria e sufficiente che le coordinate cartesiane dei punti incogniti si possano ottenere effettuando, sopra le coordinate dei dati, operazioni razionali e successive estrazioni di radicali quadratici (in numero finito).

Designeremo brevemente col nome di « *espressioni* (irrazionali) *quadratiche* » le espressioni formate operando sopra quantità date con operazioni razionali ed estrazioni di radicali quadratici; perciò, potremo enunciare l' anzidetta condizione di risolubilità d' un problema dicendo che: le coordinate dei punti incogniti debbono essere delle espressioni quadratiche formate colle coordinate dei dati.

Dimostreremo tra poco che ogni espressione quadratica soddisfa ad un' equazione algebrica i cui coefficienti si espri-

mono razionalmente per le quantità date, cioè sono razionali nel dato campo di razionalità. Con ciò la questione di decidere se un problema proposto sia risolubile elementarmente, verrà ricondotta alle due questioni seguenti:

1) decidere se il problema stesso (posto previamente sotto la forma innanzi accennata) sia *algebrico*, cioè venga a dipendere da un' equazione algebrica a coefficienti razionali nel campo dato;

2) decidere se una data equazione algebrica sia risolubile con operazioni razionali ed estrazioni di radicali quadratici, in un dato campo di razionalità a cui appartengono i coefficienti dell' equazione.

Riguardo alla prima questione notiamo che la geometria analitica insegna a tradurre le relazioni geometriche in relazioni analitiche; se queste ultime si presentano sotto forma algebrica, la questione anzidetta è subito risoluta affermativamente. Essa si presenta invece molto più difficile quando si pervenga a relazioni analitiche che non si presentino sotto forma algebrica, giacchè si tratta allora di riconoscere se queste relazioni analitiche (per quanto riguarda la determinazione delle incognite in un caso determinato) possano essere rimpiazzate con relazioni algebriche; tale ricerca conduce invero ai più alti problemi dell'Analisi (cfr. art. XXII).

Noi vogliamo qui occuparci della seconda questione, dando un teorema generale sul grado delle equazioni algebriche risolubili con radicali quadratici. La questione non viene così esaurita (e per esaurirla si richiedono maggiori sviluppi); ma il risultato ottenuto basta alle applicazioni nel campo della Geometria elementare, che abbiamo in vista.

Fra queste applicazioni compariscono prima di tutto quelle relative alla costruzione dei poligoni regolari, che in questo stesso scritto trattiamo, e quelle relative ai problemi della duplicazione del cubo e della trisezione dell' angolo trattate nell' art. XIX.

Gli antichi ci hanno tramandato le costruzioni elementari del poligono regolare di 2^n lati, del triangolo equilatero e del pentagono regolare, nonchè quelle dei poligoni regolari di $2^n \cdot 3$ lati, $2^n \cdot 5$ lati, $3 \cdot 5$ lati, $2^n \cdot 3 \cdot 5$ lati, che dalle precedenti dipendono.

Ora si potrebbero cercare p. es. le costruzioni elementari dell' ettagono o del nonagono regolare, e mal ci si renderebbe ragione delle difficoltà a cui si andrebbe incontro quando non venisse fatto di porre in dubbio la risolubilità di tali problemi. Si accumulerebbero quindi inutili sforzi, senza trarre neppure dall' insuccesso un insegnamento qualsiasi intorno alla natura delle questioni proposte.

Ma chi avesse acquistato la persuasione che si tratta di questioni irresolubili, come oserebbe tentare la prova pei casi successivi nei quali le difficoltà vanno apparentemente crescendo? Dopo avere constatato, o supposto, che non sono costruibili elementarmente i poligoni regolari di 7, 9, 11, 13, 14 lati, come potrebbe venir in mente di cercare la costruzione di quello di 17 lati? Eppure accade in fatto che la costruzione dell' ettadecagono è possibile, mentre sono impossibili (colla riga e col compasso) le costruzioni dei poligoni regolari di 7, 9, 11, 13, 14 lati.

Di ciò rende ragione la bellissima teoria di GAUSS delle equazioni binomie.

La costruzione del poligono regolare di n lati viene a dipendere dalla risoluzione dell' equazione binomia

$$z^n = 1,$$

la quale, tolta la radice $z = 1$, si riduce alla

$$z^{n-1} + z^{n-2} + \ldots + 1 = 0.$$

Perchè lo $n$gono sia elementarmente costruibile occorre che la precedente equazione sia risolubile per radicali quadratici (nel campo di razionalità assoluto [1]). Ora tale risolubilità dipende dalla forma del numero n; precisamente l' equazione è risolubile se n, decomposto in fattori primi, è della forma

$$n = 2^{\nu}\left(2^{2^{\nu_1}} + 1\right)\left(2^{2^{\nu_2}} + 1\right)\ldots\left(2^{2^{\nu_s}} + 1\right)$$

ove $\nu_1\ \nu_2 \ldots\ \nu_s$ sono tutti differenti fra loro.

In questa formula sono dunque racchiusi tutti i poligoni regolari costruibili elementarmente (1).

Diamo qualche notizia particolareggiata su tali poligoni nel § 9 di questo articolo; e terminiamo con un cenno relativo al problema dell'ettagono. Rimandiamo all'art. XVIII per le svariate costruzioni dell'ettadecagono, di cui qui ci limitiamo a rilevare la possibilità teorica come conseguenza del teorema generale accennato.

Citeremo infine i principali lavori, ove si trovano svolte le teorie che formano oggetto del presente scritto, di cui ci siamo valsi nella compilazione di esso:

1° Intorno alle equazioni algebriche risolubili per radicali quadratici:

J. PETERSEN: *Teoria delle equazioni algebriche*, trad. it. ROZZOLINO e SFORZA. Napoli, Pellerano, 1891-92. — F. KLEIN: *Conferenze sopra alcune questioni di geometria elementare*, trad. it. GIUDICE. Torino, Rosenberg e Sellier, 1896. — CAPELLI: *Lezioni di Algebra complementare*. Pellerano, Napoli, 1895.

2° Per la teoria delle equazioni binomie in relazione al problema dei poligoni regolari:

C. F. GAUSS: *Disquisitiones arithmeticae* sectio VII, Werke Bd I. (1801). — P. BACHMANN: *Die Lehre von der Kreistheilung*.... Leipzig, Teubner, 1872. — F. KLEIN: *l. c.* — L. BIANCHI: *Lezioni sulla teoria delle sostituzioni e delle equazioni algebriche secondo Galois*. Pisa, Nistri, 1896.

I.

§ 1. **Riduzione delle espressioni irrazionali quadratiche a forma normale.** — Consideriamo un'espressione (*quadratica*) x, formata con operazioni razionali e successive estrazioni di radicali quadratici a partire da certe quantità date $1, \alpha, \beta, \ldots$ che definiscono il nostro campo di razionalità $[1, \alpha, \beta, \ldots]$.

Per ottenere x occorre ampliare il campo $R = [1, \alpha, \beta \ldots]$, aggiungendovi successivamente dei radicali quadratici, fino a che x appaia razionale nel campo ampliato.

(1) Relativamente agli istrumenti da adoperarsi per le costruzioni il signor HILBERT ha osservato che l'uso del compasso può qui essere rimpiazzato dall'uso del *trasportatore di segmenti* (Cfr. art. XVI).

Se si sono aggiunti m radicali (ognuno dei quali si suppone allargare effettivamente il campo cui si aggiunge) possiamo dire che l'espressione quadratica x è d'*ordine* o di *grado* m.

Un' espressione del 1° ordine apparirà razionale dopo l'aggiunta ad R d'un radicale quadratico

$$\sqrt{X},$$

dove X dipende razionalmente da α, β... Pertanto una tale espressione potrà presentarsi, in generale, come una frazione, in cui numeratore e denominatore sono polinomi ordinati per le potenze di $\sqrt{X}$, con coefficienti $a_0, a_1 \ldots; b_0, b_1 \ldots$ razionali in R:

$$x = \frac{a_0 + a_1\sqrt{X} + a_1(\sqrt{X})^2 + \ldots\ a_n(\sqrt{X})^n}{b_0 + b_1\sqrt{X} + b_2(\sqrt{X})^2 + \ldots\ b_m(\sqrt{X})^m}.$$

Ma poichè $(\sqrt{X})^2 = X$, $(\sqrt{X})^3 = X\sqrt{X}$, $(\sqrt{X})^4 = X^2 \ldots$, si avrà

$$x = \frac{l + p\sqrt{X}}{r + s\sqrt{X}},$$

con l, p, r, s razionali (in R).

Ora, moltiplicando e dividendo per $r - s\sqrt{X}$, si otterrà

$$x = \frac{lr - psX}{r^2 - s^2X} + \left(\frac{pr - lsX}{r^2 - s^2X}\right)\sqrt{X} = A + B\sqrt{X},$$

dove A e B sono razionali.

In conclusione le *espressioni quadratiche del 1° ordine* si riducono alla *forma normale*

$$x = A + B\sqrt{X},$$

dove A, B e X sono razionali nel dato campo R.

Passiamo ora alle espressioni quadratiche del 2° *ordine.*

Sono tali le espressioni che si ottengono aggiungendo al nostro campo di razionalità R, *due* radicali, che possono essere sovrapposti (come nell' espressione

$$\sqrt{a + \sqrt{b}}),$$

ovvero non sovrapposti (come in

$$\sqrt{a}+\sqrt{b}, \quad \frac{\sqrt{a}}{1+\sqrt{b}} \quad \text{ecc.}).$$

Ora, l'ipotesi che l'aggiunta successiva ad R dei due radicali porti un effettivo allargamento del campo, significa che i detti radicali sono *indipendenti*, cioè che non è possibile sostituire uno di essi con un'espressione razionale dell'altro: altrimenti l'espressione — apparentemente del 2° ordine — si riduce senz'altro al 1°; come avviene p. es. per la

$$x=\sqrt{1+a+2\sqrt{a}}=\pm(1+\sqrt{a}).$$

Le espressioni quadratiche del 2° ordine, a somiglianza di quelle del 1° ordine, si lasciano ridurre a una forma normale

$$x_1=A_1+B_1\sqrt{X_1},$$

dove A_1, B_1, X_1 sono in generale espressioni quadratiche del 1° ordine (cioè razionali in un campo R_1, ottenuto da R per l'aggiunta d'*un* radicale $\sqrt{X}$), a ciascuna delle quali si può dare a sua volta la forma normale trovata innanzi.

Questa riduzione si estende dunque — per induzione completa — a tutte le espressioni quadratiche. Ogni espressione quadratica d'ordine m si ridurrà ad una *forma normale*

$$x_m=A_{m-1}+B_{m-1}\sqrt{X_{m-1}},$$

dove A_{m-1}, B_{m-1}, X_{m-1} sono espressioni d'ordine $\leq m-1$, ciascuna delle quali potrà essere assunta a sua volta sotto forma normale ecc. Ed è lecito supporre che nella forma normale di x_m compaiano m *radicali indipendenti*; poichè ogniqualvolta uno dei radicali che figurano in x possa esprimersi razionalmente per mezzo di altri che non lo contengono (e che si presumono aggiunti precedentemente ad R), è lecito mettere al suo posto questa espressione, e abbassare così l'ordine della x_m. Per es. se il radicale $\sqrt{X_{m-1}}$ potesse esprimersi razionalmente per mezzo dei radicali che entrano in A_{m-1}, B_{m-1}, X_{m-1}, la x_m data innanzi si ridurrebbe tosto ad un'espressione d'ordine $m-1$ al più.

Illustreremo la riduzione a forma normale delle espressioni irrazionali quadratiche, indicando alcuni esempi che offriranno materia d'esercizio al lettore.

Designamo con a, b, c... espressioni razionali nel nostro campo fondamentale R. L'espressione del 2° ordine

$$x_2 = \sqrt{b} + \frac{1}{\sqrt{a + \frac{1}{1+\sqrt{b}}}}$$

si riduce anzitutto alla forma

$$x_2 = \sqrt{b} + \frac{\sqrt{a + \frac{1}{1+\sqrt{b}}}}{a + \frac{1}{1+\sqrt{b}}} = A_1 + B_1\sqrt{X_1}.$$

Poi si scriverà

$$\frac{1}{1+\sqrt{b}} = \frac{1-\sqrt{b}}{1-b^2},$$

$$x_2 = \sqrt{b} + \frac{(1-b^2)}{1-\sqrt{b}}\sqrt{a + \frac{1}{1-b^2} - \frac{\sqrt{b}}{1-b^2}},$$

$$\frac{1-b^2}{1-\sqrt{b}} = 1+\sqrt{b},$$

$$x_2 = \sqrt{b} + (1+\sqrt{b})\sqrt{a + \frac{1}{1-b^2} - \frac{\sqrt{b}}{1-b^2}},$$

che è la forma normale

$$\left(A_1 = \sqrt{b},\ B_1 = 1+\sqrt{b},\ X_1 = a + \frac{1}{1-b^2} - \frac{\sqrt{b}}{1-b^2}\right).$$

Indichiamo ancora un secondo esempio.

L'espressione

$$x = \frac{\sqrt{a}+\sqrt{b}+\sqrt{ab}}{\sqrt{b}+\sqrt{c}+\sqrt{\frac{c}{b}}},$$

appare, a prima vista, d'ordine 5, ma si riduce di 3° ordine, ponendo

$$\sqrt{ab} = \sqrt{a} \cdot \sqrt{b}, \quad \sqrt{\frac{c}{b}} = \frac{\sqrt{c}}{\sqrt{b}}.$$

Si ottiene così l'espressione

$$x = \frac{\sqrt{a} + \sqrt{b} + \sqrt{a} \cdot \sqrt{b}}{\sqrt{b} + \sqrt{c} + \dfrac{\sqrt{c}}{\sqrt{b}}},$$

in cui tutti i radicali sono indipendenti (salvo che si pongano particolari relazioni fra a, b, c).

Ora, per ridurre questa espressione a forma normale, potremo ritenere aggiunti ad R i radicali $\sqrt{a}$, $\sqrt{b}$, $\sqrt{c}$ nell'ordine che più ci piace (circostanza che tiene al non aversi qui dei radicali sovrapposti). Poniamo p. es. che si sia aggiunto: prima $\sqrt{c}$, poi $\sqrt{b}$, poi $\sqrt{a}$. Rispetto a $\sqrt{a}$ si ha senz'altro la forma normale

$$(1) \qquad x = A_2 + B_2 \sqrt{X_2} = \frac{\sqrt{b}}{\sqrt{b} + \sqrt{c} + \dfrac{\sqrt{c}}{\sqrt{b}}} + \frac{(1 + \sqrt{b})}{\sqrt{b} + \sqrt{c} + \dfrac{\sqrt{c}}{\sqrt{b}}} \cdot \sqrt{a}$$

e si tratta di ridurre i termini di 2° ordine A_2, B_2, che in questa figurano, avendosi già $X_2 = a$.

Ora, per ridurre il primo termine rispetto a $\sqrt{b}$, scriveremo

$$A_2 = \frac{\sqrt{b}}{\sqrt{b} + \sqrt{c} + \dfrac{\sqrt{c}}{\sqrt{b}}} = \frac{b}{b + \sqrt{c} + \sqrt{c} \cdot \sqrt{b}} =$$

$$= \frac{b(b + \sqrt{c} - \sqrt{c} \cdot \sqrt{b})}{(b + \sqrt{c})^2 - cb} =$$

$$= \frac{b^2 + b\sqrt{c}}{(b + \sqrt{c})^2 - cb} - \frac{b\sqrt{c}}{(b + \sqrt{c})^2 - cb} \sqrt{b};$$

e si avranno quindi da ridurre a forma normale (rispetto

a $\sqrt{c}$) le espressioni del 1° ordine:

$$A_1 = \frac{b^2 + b\sqrt{c}}{(b+\sqrt{c})^2 - cb} = \frac{b^2 + b\sqrt{c}}{b^2 + c - cb + 2b\sqrt{c}} =$$

$$= \frac{(b^2 + b\sqrt{c})(b^2 + c - cb - 2b\sqrt{c})}{(b^2 + c - cb)^2 - 4b^2c} =$$

$$= \frac{b^2(b^2 + c - cb) - 4b^2c}{(b^2 + c - cb)^2 - 4b^2c} + \frac{\{b(b^2 + c - cb) - 2b^3\}}{(b^2 + c - cb)^2 - 4b^2c} \cdot \sqrt{c},$$

e

$$B_1 = \frac{b\sqrt{c}}{(b+\sqrt{c})^2 - cb} = \frac{b\sqrt{c}}{b^2 + c - cb + 2b\sqrt{c}} =$$

$$= \frac{b\sqrt{c}\cdot(b^2 + c - cb - 2b\sqrt{c})}{(b^2 + c - cb)^2 - 4b^2c} =$$

$$= \frac{2b^2c}{(b^2 + c - cb)^2 - 4b^2c} + \frac{b(b^2 + c - cb)}{(b^2 + c - cb)^2 - 4b^2c} \cdot \sqrt{c}.$$

Analogamente si tratterà il secondo termine coefficiente di $\sqrt{a}$ nella (1), cioè:

$$\frac{1 + \sqrt{b}}{\sqrt{b} + \sqrt{c} + \frac{\sqrt{c}}{\sqrt{b}}}.$$

NOTIZIA. — La riduzione a forma normale delle espressioni irrazionali quadratiche, rientra in una riduzione più generale per le espressioni contenenti radicali d'ordine qualunque, che è stata assegnata da ABEL: *Opere*. Cristiania, 1881, t. I, pag. 66-75; Giornale di Crelle I, pag. 66. (Cfr. art. XXI).

§ 2. **Formazione di un' equazione algebrica a cui soddisfa un' espressione quadratica.** — I ragionamenti che istituiremo sulle espressioni irrazionali quadratiche si basano sull' ipotesi che esse siano preliminarmente ricondotte a contenere *radicali indipendenti sotto forma normale*: avremo dunque m radicali indipendenti (sovrapposti o no) per le espressioni quadratiche di grado m.

Un' espressione quadratica, x, *di grado* n, *soddisfa ad una equazione algebrica di grado* 2^n, *a coefficienti razionali* (nel dato campo di razionalità).

Immaginiamo di dare agli n radicali che entrano nell'espressione x tutti i valori (positivi e negativi) che essi possono ricevere; otteniamo così 2^n valori di x: $x_1, x_2, \ldots x_i, \ldots x_{2^n}$, alcuni dei quali (come mostreremo fra poco) potranno essere uguali fra loro.

Costruiamo l'equazione

$$f(x) = (x - x_1)(x - x_2) \ldots (x - x_{2^n}) = x^{2^n} + p_1 x^{2^n - 1} + \ldots + p_{2^n} = 0$$

che ha per radici le x_i.

I coefficienti di tale equazione si esprimono colle funzioni simmetriche elementari delle x_i, per mezzo delle formule

$$\begin{aligned} p_1 &= -\Sigma x_i \\ p_2 &= \Sigma x_i x_k \\ &\ldots\ldots\ldots \\ p_{2^n} &= x_1 x_2 \ldots x_n . \end{aligned}$$

Si tratta di provare che questi coefficienti sono razionali.

Questa proprietà risulta dal fatto fondamentale che le p_r sono funzioni *simmetriche* delle x_i, cioè che esse rimangono inalterate quando si permuti in un modo qualsiasi l'ordine delle x_i (p. es.

$$p_1 = -(x_1 + x_2 + \ldots + x_{2^n}) = -(x_2 + x_1 + x_3 \ldots + x_{2^n}) \ldots).$$

Anzitutto, essendo le p_r funzioni simmetriche delle x_i, esse non dovranno alterarsi allorchè in un modo comunque determinato si cambiano i segni dei radicali che entrano nelle x_i, giacchè un tale cambiamento produce soltanto una permutazione nell'ordine delle x_i stesse. Se p. es.

$$x = \sqrt{a + \sqrt{b}},$$

possiamo indicare i valori dell'espressione x con

$$\begin{aligned} x_1 &= +\sqrt{a + \sqrt{b}} \\ x_2 &= -\sqrt{a + \sqrt{b}} \\ x_3 &= +\sqrt{a + \sqrt{b}} \\ x_4 &= -\sqrt{a - \sqrt{b}}, \end{aligned}$$

ed allora si vede che cambiando il segno di $\sqrt{b}$, si permutano i valori di x_1, x_3 e di x_2, x_4; invece cambiando i segni di ambedue i radicali si permutano i valori di x_1, x_4 e di x_2, x_3; infine cambiando il segno del radicale esterno $\sqrt{a+\sqrt{b}}$, si permutano x_1, x_2 e x_3, x_4.

Ciò posto consideriamo p_r come un' espressione quadratica formata coi radicali che entrano nella x e supponiamo tale espressione posta sotto forma normale. Supposto che essa contenga termini d' ordine m, $\sqrt{X}$, $\sqrt{Y}$, $\sqrt{Z}$... poniamo in evidenza il termine $\sqrt{X}$, scrivendo

$$p_r = P + Q\sqrt{X}.$$

Poichè p_r non cambia mutando il segno di $\sqrt{X}$, avremo allora

$$P + Q\sqrt{X} = P - Q\sqrt{X},$$

ossia

$$Q\sqrt{X} = 0,$$

e quindi

$$Q = 0.$$

Dunque p_r non dipende dal radicale $\sqrt{X}$. In modo analogo essa non dipende neppure da $\sqrt{Y}$, $\sqrt{X}$..., e perciò in essa figurano termini contenenti radicali, d' ordine $m-1$ al più.

Ma ripetendo il ragionamento precedente in relazione ai termini d' ordine $m-1$, si vede che p_r non può dipendere neppure da questi. Così proseguendo successivamente si prova che p_r non dipende da nessun radicale, ossia che p_r è un'espressione razionale (nel campo dato). Resta dunque stabilito che la $f(x)=0$ è un' equazione a coefficienti razionali. *c. d. d.*

Abbiamo avvertito che fra i valori $x_1 x_2 \ldots$ di x possono trovarsene alcuni uguali fra loro; se p. es.:

$$x = \sqrt{a+\sqrt{b}} + \sqrt{a-\sqrt{b}},$$

risultano uguali i valori di x ottenuti cambiando il segno di $\sqrt{b}$.

Poniamo di scegliere, fra i 2^n valori della x, tutti i valori *differenti*; sieno p. es. $x_1 x_2 \ldots x_r$. Allora, l' equazione, di grado r,

$$\varphi(x) = (x - x_1)(x - x_2)\ldots(x - x_r) = 0,$$

ha anch' essa i coefficienti razionali; la cosa si dimostra come per la $f(x) = 0$.

Paragonando le due equazioni

$$f(x) = 0, \quad \varphi(x) = 0,$$

si vede che la prima ammette tutte le radici della seconda, e però essa è riducibile, se $r < 2^n$, avendosi

$$f(x) = \varphi(x)\psi(x),$$

ove $\psi(x)$ è un polinomio a coefficienti razionali.

§ 3. **Sul grado delle equazioni irriducibili risolubili per radicali quadratici.** — Dimostriamo anzitutto il teorema: *Se un'equazione algebrica a coefficienti razionali* (in un dato campo) *è soddisfatta da un valore dell' espressione quadratica* x, *essa è soddisfatta da tutti i valori della* x *ottenuti cambiando i segni dei radicali.*

Sia

$$F(x) = 0,$$

l' equazione data.

Prendiamo x ridotta a contenere radicali indipendenti, e sotto forma normale, ponendo in evidenza un termine dell' ordine più alto m, $\sqrt{X}$:

$$x = A + B\sqrt{X}.$$

Sostituiamo questa espressione in F e riduciamo F a forma normale relativamente a $\sqrt{X}$, scrivendo

$$F(x) = L + M\sqrt{X};$$

L ed M dipendono razionalmente dagli altri termini di ordine m, $\sqrt{Y}$, $\sqrt{Z}$... e dai termini d' ordine inferiore che figurano in x.

Ora si ha (per ipotesi)

$$F(x) = L + M\sqrt{X} = 0;$$

onde

$$L = M = 0,$$

oppure

$$\sqrt{X} = -\frac{L}{M};$$

ma quest' ultima relazione contraddice all' ipotesi che tutti i radicali contenenti in x sieno indipendenti; resta dunque provato che

$$L = M = 0,$$

e perciò

$$L - M\sqrt{X} = 0,$$

onde l' equazione

$$F(x) = 0,$$

è soddisfatta non soltanto da

$$x = A + B\sqrt{X},$$

ma anche da

$$x = A - B\sqrt{X}.$$

In modo analogo si prova che la $F(x) = 0$ è soddisfatta dai valori ottenuti mutando comunque nell' espressione di x, il segno dei termini d' ordine m, $\sqrt{Y}$, $\sqrt{Z}$...

Supponiamo, per semplicità di ragionamento, che in x entrino soltanto due termini dell' ordine m,

$$\sqrt{X} \quad \text{e} \quad \sqrt{Y},$$

avremo

$$F(x) = L + M\sqrt{X}$$

con

$$L = L_1 + L_2\sqrt{Y}$$
$$M = M_1 + M_2\sqrt{Y},$$

e, dall' essere $F(x) = 0$, concluderemo

$$L_1 = L_2 = M_1 = M_2 = 0.$$

Ora L_1, L_2, M_1, M_2 sono espressioni contenenti soltanto termini in cui figurano radicali, d' ordine $m - 1$ al più; col ragionamento precedente si prova che queste espressioni si annullano cambiando comunque in x il segno dei radicali

dei termini d'ordine $m-1$; se ne deduce che la $F(x)=0$ è soddisfatta quando si cambino nell'espressione di x i segni dei radicali costituenti i termini dell'ordine $m-1$.

È chiaro come il ragionamento si possa proseguire, pervenendo così alla conclusione che se l'equazione

$$F(x)=0$$

è soddisfatta da un valore dell'espressione quadratica x, essa è pure soddisfatta da tutti quei valori che si ottengono dal dato cambiando segno in modo arbitrario ai radicali costituenti i termini degli ordini

$$m,\quad m-1,\quad m-2,\ldots 1.$$

Resta da far vedere che la $F(x)=0$ è ancora soddisfatta se si cambiano i segni dei radicali che entrano sotto un altro radicale, p. es. i radicali costituenti i termini dell'espressione X che figura in $\sqrt{X}$. Ma ciò è stato già implicitamente dimostrato, perchè avendosi

$$F(x)=L+M\sqrt{X}$$

ove

$$L=M=0,$$

sarà sempre

$$F(x)=0,$$

comunque si cambi il segno dei radicali che figurano in X.

Dunque il teorema è completamente stabilito.

Esso conduce immediatamente al corollario:

Se un' equazione algebrica

$$F(x)=0,$$

a coefficienti razionali, è soddisfatta da un valore di una espressione quadratica x, *e se si designa con*

$$\varphi(x)=0,$$

l' equazione (a coefficienti razionali) del medesimo grado r, *a cui soddisfano tutti i valori differenti che la* x *può ricevere*

cambiando il segno dei radicali in essa contenuti, si ha

$$F(x) = \varphi(x)\theta(x),$$

e $\theta(x)$ *è un polinomio a coefficienti razionali.*

Se la $F(x) = 0$ è un' equazione *irriducibile*, il polinomio θ si potrà dunque ridurre ad un fattore costante.

Riprendiamo ora l' equazione $f(x) = 0$ innanzi considerata, cioè l' equazione, del grado 2^n, che ha per radici i 2^n valori dell' espressione quadratica x.

Abbiamo già avvertito che, se $r < 2^n$, si ha

$$f(x) = \varphi(x)\psi(x)$$

ove ψ è un polinomio a coefficienti razionali. Ora l' equazione $\psi(x) = 0$ ha per radici alcuni valori dell' espressione quadratica x, e quindi tutti i valori di essa; perciò si ha ancora

$$\psi(x) = \varphi(x)\psi_1(x) \quad \text{e} \quad f(x) = \varphi^2(x)\psi_1(x),$$

ove ψ_1 è un nuovo polinomio a coefficienti razionali, oppure una costante. Applichiamo a ψ_1 (supposto che non sia una costante) il ragionamento svolto relativamente a ψ, e così di seguito; in definitiva dovremo trovare un quoziente che si riduca ad una costante c, avendosi dunque

$$f(x) = c\varphi^s(x);$$

poichè la divisione non può procedere indefinitamente, avendo f un grado finito.

Ora avendosi, come si è detto,

$$f(x) = c\varphi^s(x),$$

ed essendo r il grado di φ, e 2^n il grado di f, sarà

$$rs = 2^n,$$

sicchè tanto r che s non contengono alcun fattore primo diverso da 2; in conclusione il grado dell' equazione

$$\varphi(x) = 0$$

sarà

$$r = 2^\nu.$$

Da ciò, ricordando i precedenti risultati, si deduce il teorema fondamentale:

Se un' equazione algebrica irriducibile è risolubile con soli radicali quadratici (in un dato campo di razionalità cui appartengono i suoi coefficienti), il suo grado è una potenza di 2.

Questa condizione necessaria non è però sufficiente; così p. es. un' equazione generale del 4° grado non è risolubile per radicali quadratici (cfr. art. XX).

NOTIZIA. — Il teorema sul grado delle equazioni irriducibili risolubili per radicali quadratici appartiene a JULIUS PETERSEN, che — nella citata « Teoria delle equazioni algebriche » — lo dimostra, come anche qui è fatto, basandosi sulla riduzione delle espressioni contenenti radicali, data in generale da ABEL (cfr. Notizia a pag. 271).

Un' altra dimostrazione, assai elegante, dello stesso teorema trovasi nella recente Nota di FRANCESCO GIUDICE « Sulle equazioni risolubili per radicali quadratici » (Rendic. Istituto lombardo, 1925). Il GIUDICE non fa uso della riduzione delle espressioni irrazionali quadratiche a forma normale, ed invece si basa sul seguente lemma: « Se un' equazione $f=0$ di grado m possiede coefficienti non razionali (in un dato campo R) ma esprimibili razionalmente per le radici d' un' equazione (risolvente) di 2° grado a coefficienti razionali, l' equazione irriducibile a coefficienti razionali che ammette le m radici di $f=0$ è di grado $2m$ ».

Le condizioni a cui deve soddisfare un' equazione di grado 2^r, affinchè sia risolubile per radicali quadratici, e i procedimenti da adoperare in generale per la risoluzione effettiva, sono ampiamente studiati da PETERSEN in varii lavori, e p. es. nell' opera citata.

II.

§ 4. Riduzione del problema dei poligoni regolari alle equazioni binomie. — Noi vogliamo applicare i risultati precedenti, relativi alle equazioni risolubili per radicali quadratici, al problema della costruzione dei poligoni regolari.

Dobbiamo anzitutto tradurre il problema sotto forma analitica. E perciò cominciamo a ricondurlo a tal forma, che

sieno dati dei punti, e si cerchino punti aventi con essi relazioni prestabilite.

Bastano a tal fine le seguenti osservazioni semplicissime:

a) Tutti gli *n*goni regolari sono simili fra loro, quindi il problema di costruire lo *n*gono regolare che ha un lato assegnato si riconduce subito al problema di costruire un qualsiasi *n*gono regolare. L' incognita è l' angolo del poligono, o, se si vuole, l' angolo al centro che proietta un lato; il lato compare nella questione come un parametro arbitrario.

b) Quando si sappia costruire un *n*gono regolare, si può anche costruire lo *n*gono regolare iscritto in un dato circolo e avente un dato vertice, cioè si può *dividere il circolo in* n *archi uguali,* partendo da un punto di divisione assegnato, o viceversa.

Dunque il problema dei poligoni regolari è perfettamente equivalente a quello della divisione del circolo in n parti uguali, ove si può supporre che sieno dati il centro O del circolo ed un punto di divisione A. È lecito assumere la distanza dei due punti dati, cioè il raggio del circolo, come unità.

Sotto questa forma il problema, in cui i dati sono punti, è ricondotto alla ricerca di $n-1$ punti (di divisione) che, insieme ad A, costituiscono i vertici di un *n*gono regolare.

Ciascuno di questi punti determina con A (in uno qualunque dei due sensi) un arco che moltiplicato per n dà un multiplo dell' intero circolo, cioè un arco

$$\frac{2\pi r}{n}$$

(ove si può prendere $r < n$).

Riferiamoci a due assi coordinati ortogonali, prendendo O come origine ed OA come asse delle x. Il punto A avrà come coordinate 1, 0; i punti incogniti avranno certe coordinate

$$x_1 y_1, \quad x_2 y_2 \ldots x_{n-1} y_{n-1},$$

(soddisfacenti all' equazione

$$x^2 + y^2 = 1$$

del circolo), coordinate che appunto si tratta di determinare,

partendo dalle sole quantità date 0, 1, le quali definiscono il campo di razionalità assoluto [1].

Immaginiamo rappresentati nel piano i valori della variabile complessa

$$z = x + iy$$

(rappresentazione di ARGAND-GAUSS). A ciascun valore z, corrispondono (come è noto) un *modulo*

$$\rho = \sqrt{x^2 + y^2}$$

e un *argomento*

$$\theta = \operatorname{arctg} \frac{y}{x},$$

coordinate polari del punto (xy) indice di z, sicchè si ha

$$z = \rho(\cos\theta + i \operatorname{sen}\theta).$$

Il modulo è la distanza assoluta del punto (xy) dall' origine (*raggio vettore*): l' argomento è l' angolo (*anomalia*) che la congiungente il punto stesso coll' origine forma coll' asse x.

Ora la moltiplicazione di due numeri complessi

$$z = x + iy, \quad z' = x' + iy'$$

si può effettuare: algebricamente, secondo le ordinarie regole del calcolo, ponendo

$$Z = zz' = (xx' - yy') + i(xy' + x'y);$$

oppure geometricamente, determinando il punto che ha come coordinate polari

$$P = \rho\rho' = \sqrt{x^2 + y^2} \cdot \sqrt{x'^2 + y'^2}$$

$$\Theta = \theta + \theta' = \operatorname{arctg} \frac{y}{x} + \operatorname{arc}\, tg \frac{y'}{x'},$$

cioè facendo il prodotto dei moduli e la somma degli argomenti.

Applicando questa regola geometrica, formiamo le successive potenze dei numeri complessi

$$z_s = x_s + iy_s,$$

aventi come indici i nostri punti incogniti

$$(x_1 y_1), \ldots (x_{n-1} y_{n-1}).$$

Il modulo

$$\sqrt{x_s^2 + y_s^2} = 1,$$

e l'argomento è

$$\frac{2\pi r}{n}$$

$$\left(\text{onde } z_s = \cos\frac{2\pi r}{n} + i \operatorname{sen}\frac{2\pi r}{n}\right),$$

quindi il modulo di z_s^n sarà sempre $= 1$, mentre il suo argomento sarà

$$\frac{2\pi r h}{n}.$$

In particolare per $h = n$, il punto z_s^n si troverà sulla parte positiva dell'asse delle x, e quindi coinciderà con

$$A \equiv (1,0);$$

per conseguenza

$$z_s^n = 1.$$

Viceversa si abbia un punto (xy), diverso dal punto A, tale che

$$z^n = (x + iy)^n = 1;$$

questo punto deve avere un modulo ρ tale che $\rho^n = 1$, e quindi un modulo $= 1$; inoltre esso deve avere un argomento θ che moltiplicato per n differisca da 0 per multipli di 2π, onde

$$\theta = \frac{2\pi r}{n};$$

dunque il detto punto è uno dei punti

$$(x_1 y_1) \ldots . (x_{n-1} y_{n-1})$$

che soddisfano al nostro problema.

In conclusione:

Il problema della costruzione di un ngono regolare, viene a dipendere dalla risoluzione dell' equazione binomia

$$z^n = 1,$$

e precisamente dalla ricerca delle radici di essa diverse da $z=1$, *cioè dalla risoluzione dell' equazione*

$$\frac{z^n-1}{z-1}=z^{n-1}+z^{n-2}+\ldots+1=0.$$

Questa equazione si può scindere in due altre relative ad x e y; ma ciò non è necessario, nè utile. Se l' equazione indicata in z può essere risoluta per radicali quadratici (nel campo di razionalità [1] dato dai coefficienti), anche le coordinate x, y dei punti incogniti verranno espresse per radicali quadratici, giacchè si ha

$$\sqrt{a+ib}=\sqrt{\frac{a}{2}+\sqrt{a+b^2}}+i\sqrt{\frac{a}{2}+\sqrt{a+b^2}},$$

e quindi lo $n$gono sarà costruibile colla riga e col compasso. Viceversa se lo $n$gono è costruibile, le x, y sono espressioni quadratiche e quindi anche le radici

$$z=x+iy$$

dell' equazione binomia, risulteranno pure esprimibili per radicali quadrati.

Il problema della costruzione elementare dei poligoni regolari è così ricondotto alla questione di risolvere (quando sia possibile), per radicali quadratici, l' equazione binomia

$$z^n=1.$$

§ 5. **Irriducibilità dell' equazione** $\frac{z^p-1}{z-1}=0$, **quando** p **è un numero primo.** — Consideriamo l' equazione

$$z^p-1=0$$

nell' ipotesi in cui p sia un numero primo. Togliendo il fattore lineare $z-1$, essa si riduce alla forma

$$F(z)=\frac{z^p-1}{z-1}=z^{p-1}+z^{p-2}+\ldots+z+1=0.$$

Noi vogliamo dimostrare che questa equazione è irriducibile, nel campo assoluto di razionalità [1], cioè che $F(z)$ non può spezzarsi nel prodotto di due polinomi a coefficienti (numerici) razionali.

A tale scopo occorre premettere un lemma sopra la decomponibilità dei polinomi, lemma dovuto a GAUSS.

Si abbia un polinomio

$$f(z) = a_0 z^n + a_1 z^{n-1} + \dots + a_n,$$

i cui coefficienti sieno numeri interi; diremo che questo polinomio è *primitivo* allorchè i numeri $a_0, a_1, \dots a_n$ non ammettono alcun divisore comune, diverso dall' unità.

Ora sieno

$$f(z) = a_0 z^n + a_1 z^{n-1} + \dots + a_n,$$

e

$$\varphi(z) = b_0 z^m + b_1 z^{m-1} + \dots + b_m$$

due polinomi a coefficienti interi, primitivi. Formiamo il prodotto

$$F(z) = f(z)\varphi(z) = c_0 z^{m+n} + c_1 z^{m+n-1} + \dots c_{m+n},$$

dove

$$c_0 = a_0 b_0$$

$$c_1 = a_0 b_1 + a_1 b_0,$$

e in generale

$$c_h = a_0 b_h + a_1 b_{h-1} + \dots + a_h b_0,$$

coll' avvertenza che

$$a_r = 0 \quad \text{per} \quad r > n,$$

$$b_s = 0 \quad \text{per} \quad s > m.$$

Mostriamo che il polinomio $F(z)$ è primitivo, cioè che non esiste alcun numero primo p (> 1), il quale divida tutti i numeri $c_0, c_1 \dots c_{m+n}$.

Dato un numero primo p (> 1), questo non può dividere tutti i coefficienti a di f, nè i coefficienti b di φ; si troverà dunque un primo coefficiente a_r

$$(\text{con } r \leq n)$$

e così un primo coefficiente b_s

$$(\text{con } s \leq m)$$

i quali non saranno divisibili per p. Allora consideriamo il coefficiente

$$c_{r+s} = a_0 b_{r+s} + \ldots + a_{r-1} b_{s+1} + a_r b_s + a_{r+1} b_{s-1} + \ldots + a_{r+s} b_0 .$$

Tutti i termini della somma sono divisibili per p, tranne $a_r b_s$; dunque c_{r+s} non è divisibile per p.

L'osservazione precedente ci permette di dimostrare il

LEMMA DI GAUSS. — *Se un polinomio a coefficienti interi* F(z) *è riducibile, esso può decomporsi nel prodotto di due polinomi a coefficienti interi.*

Possiamo supporre, senza restrizione, che F sia un polinomio primitivo, altrimenti esso potrebbe porsi sotto la forma $\mu F'$ ove F' è primitivo e μ è un numero intero (divisore comune dei coefficienti di F), sicchè basterebbe evidentemente dimostrare il teorema per F'.

Ammettiamo dunque che $F(z)$ si decomponga nel prodotto di due polinomi $f(z)$ e $\varphi(z)$ a coefficienti razionali, e vogliamo provare che F riesce allora anche il prodotto di polinomi a coefficienti interi.

Riduciamo tutti i coefficienti di f ad avere il minimo comun denominatore a; i numeratori avranno allora un massimo comun divisore α primo con a. Operiamo nello stesso modo sui coefficienti di φ, riducendoli ad avere un minimo comun denominatore b; sia β il massimo comun divisore dei numeratori dei coefficienti così ridotti. Allora i polinomi $\frac{af}{\alpha}$ e $\frac{b\varphi}{\beta}$ avranno i coefficienti interi e saranno primitivi; il loro prodotto

$$\frac{ab}{\alpha\beta} f\varphi = \frac{ab}{\alpha\beta} F$$

sarà dunque un polinomio a coefficienti interi e primitivo.

Per la prima condizione, poichè i coefficienti di F non ammettono alcun divisore comune, ogni fattore primo contenuto in $\alpha\beta$ dovrà dividere ab, e perciò $\alpha\beta$ dividerà ab; per la seconda il quoziente $\frac{ab}{\alpha\beta} = c$ (che come si è detto è un numero intero) dovrà essere uguale ad 1, altrimenti tutti i coefficienti di cF sarebbero divisibili per $c > 1$.

In conclusione $F(z)$ è il prodotto di due polinomi a coefficienti interi e primitivi $\frac{a}{\alpha}f$ e $\frac{b}{\beta}\varphi$. c. d. d.

In base al lemma di GAUSS, si può facilmente dimostrare, usando del ragionamento di ESENSTEIN [1], che:

L' equazione $\frac{z^p - 1}{z - 1} = 0$, *dove* p *è un numero primo, è irriducibile.*

Ponendo

$$z = x + 1$$

l' equazione predetta diventa

$$F(x) = x^{p-1} + px^{p-2} + \frac{p(p-1)}{2}x^{p-3} + \ldots +$$

$$+ \left(\frac{p}{r}\right)x^{p-r-1} + \ldots + p = 0.$$

Basta evidentemente dimostrare la irriducibilità della $F(x) = 0$, perchè dall' essere

$$\frac{z^p - 1}{z - 1} = \varphi_1(z)f_1(z),$$

ove φ_1 e f_1 sono due polinomi, segue

$$F(x) = \varphi_1(x + 1)f_1(x + 1) = \varphi(x)f(x),$$

ove φ e f sono due polinomi in x.

Supponiamo che la $F(x) = 0$ sia riducibile, allora si avrà

$$F(x) = \varphi(x)f(x)$$

ove φ e f sono due polinomi in x, a coefficienti interi:

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$$
$$\varphi(x) = b_0x^m + b_1x^{m-1} + \ldots + b_m.$$

[1] Crelle 's Journal, Bd. 39, pag. 167. Due diverse dimostrazioni dello stesso teorema sono state date da KRONECKER, Crelle 's J., Bd. 29, e Journal de Liouville 12, vol. 1. Cfr. BACHMANN, *l. c.*

Eseguendo il prodotto φf si troverà un polinomio identicamente uguale ad F:

$$c_0 x^{n+m} + c_1 x^{n+m-1} + \ldots + c_{n+m},$$

il cui grado $n + m = p$.

Si avranno le formule:

$$\begin{aligned}
c_0 &= a_0 b_0 = 1 \\
c_1 &= a_0 b_1 + a_1 b_0 = p \\
c_2 &= a_0 b_2 + a_1 b_1 + a_2 b_0 = \frac{p(p-1)}{2} \\
&\ldots\ldots\ldots\ldots\ldots\ldots \\
c_{n+m-1} &= a_{n-1} b_m + a_n b_{m-1} = \frac{p(p-1)}{2} \\
c_{n+m} &= a_n b_m = p,
\end{aligned}$$

e perciò tutti i coefficienti c, eccetto c_0, saranno divisibili per il numero primo p.

Ora l'ultima relazione scritta, appunto perchè p è un numero primo, porta che uno dei due numeri a_n, b_m sia uguale a $a \pm 1$, e l'altro a $b \pm p$; sia p. es.

$$a_n = 1, \quad b_n = p.$$

Sostituendo questi valori nella penultima relazione si trova

$$c_{n+m-1} = a_{n-1} p + b_{m-1},$$

e poichè p divide c_{n+m-1}, b_{m-1} è divisibile per p, ossia:

$$b_{m-1} = p b'_{m-1}.$$

Proseguendo analogamente a considerare l'espressione di c_{n+m-2}, si trova

$$c_{n+m-2} = a_{n-2} p + a_{n-1} b'_{m-1} p + b_{m-2},$$

e quindi b_{m-2} è divisibile per p, ossia:

$$b_{m-2} = p b'_{m-2}.$$

Successivamente dalle espressioni di $c_{n+m-3} \dots c_n$ si ricava che sono divisibili per p tutti i coefficienti $b_{m-3} \dots b_0$, ma la conclusione che si riferisce a b_0 si rivela subito assurda perchè l'uguaglianza

$$c_0 = a_0 b_0 = 1$$

dà

$$a_0 = \pm 1, \quad b_0 = \pm 1.$$

L'assurdo a cui si è condotti dall'ipotesi della decomponibilità di F, prova che l'equazione $F = 0$, e quindi la

$$\frac{z^p - 1}{z - 1} = 0$$

è irriducibile. c. d. d.

§ 6. **Impossibilità di costruire elementarmente i poligoni regolari di un numero primo p di lati, quando p non ha la forma $2^n + 1$.** — Ora ricordando il risultato fondamentale del § 3, concludiamo:

Se l'equazione $\frac{z^p - 1}{z - 1} = 0$, *ove* p *è un numero primo è risolubile per radicali quadratici, deve essere* $p - 1$ *una potenza del 2 e perciò:*

$$p = 2^n + 1.$$

E per conseguenza:

Non è possibile costruire colla riga e col compasso il poligono regolare avente un numero primo p *di lati, quando* p *non sia della forma* $2^n + 1$.

Così ad es. *non sono costruibili*, nel modo anzidetto, i poligoni regolari di 7, 11, 13, 19... lati.

§ 7. **Costruibilità dei poligoni regolari di un numero primo p di lati, quando p ha la forma $2^n + 1$.** — A questo risultato negativo fa riscontro il seguente risultato positivo:

Il poligono regolare di p *lati ove* p *è un numero primo della forma* $2^n + 1$, *è costruibile colla riga e col compasso.*

Per dimostrare questo teorema, occorre far vedere che l'equazione (irriducibile)

$$\frac{z^p - 1}{z - 1} = z^{p-1} + z^{p-2} + \dots + z + 1 = 0,$$

è risolubile con successive estrazioni di radici quadrate, quando p è un numero primo della forma $2^n + 1$.

Le radici della nostra equazione, cioè le radici p^{me} dell'unità, diverse da 1, sono

$$\varepsilon_1 = \cos\frac{2\pi}{p} + i\,\mathrm{sen}\,\frac{2\pi}{p},$$

. . . . . .

$$\varepsilon_r = \cos\frac{2\pi r}{p} + i\,\mathrm{sen}\,\frac{2\pi r}{p},$$

. . . . . .

$$\varepsilon^{p-1} = \cos\frac{2\pi(p-1)}{p} + i\,\mathrm{sen}\,\frac{2\pi(p-1)}{p}.$$

Esse possono ottenersi tutte formando le successive potenze di una qualunque radice ε. Partendo p. es. dalla radice $\varepsilon = \varepsilon_1$, avremo infatti $\varepsilon_r = \varepsilon^r$.

Partendo dalla radice $\varepsilon = \varepsilon_2$, avremo

$$\varepsilon_2 = \varepsilon \quad \varepsilon_4 = \varepsilon^2 \quad \varepsilon_6 = \varepsilon^3 \ldots \varepsilon_{p-1} = \varepsilon^{\frac{p-1}{2}},$$

$$\varepsilon_1 = \varepsilon^{\frac{p-1}{2}+1} \qquad \varepsilon_3 = \varepsilon^{\frac{p-1}{2}+2} \qquad \varepsilon_7 = \varepsilon^{\frac{p-1}{2}+3}$$

$$\ldots \varepsilon_{p-2} = \varepsilon^{p-1}.$$

In modo analogo le potenze successive di una qualunque $\varepsilon = \varepsilon_r$, cogli esponenti 1, 2... $p-1$, sono tutte diverse fra loro, e quindi riproducono (in altro ordine) le radici $\varepsilon_1 \varepsilon_2 \ldots \varepsilon_{p-1}$. Invero non può aversi per $h < p$, $k < p$.

$$\varepsilon_r^{\,h} = \varepsilon_r^{\,k},$$

senza che si abbia

$$\varepsilon_r^{\,h-k} = 1$$

cioè

$$\cos\frac{2\pi r(h-k)}{p} + i\,\mathrm{sen}\,\frac{2\pi r(h-k)}{p} = 1,$$

onde

$$2\pi\frac{r(h-k)}{p} = 2\pi s$$

con s intero; e questa uguaglianza è assurda perchè, essendo p un numero primo ed $r < p$, p non può dividere $r(h-k)$ senza dividere $h-k$.

Si noti ancora che sussiste sempre l'uguaglianza

$$\varepsilon^{l+mp} = \varepsilon^{l},$$

essendo

$$\varepsilon^{mp} = 1.$$

Volendo ora approfondire lo studio delle radici della nostra equazione, ci occorre prendere dalla teoria dei numeri il seguente teorema (1):

Dato un numero primo p, *esiste sempre fra i numeri* 1, 2... p − 1, *qualche numero* g, *tale che le potenze*

$$g,\quad g^2,\ldots\quad g^{p-1},$$

divise per p, *dieno per resti i numeri*

$$1,\ 2\ldots p-1$$

presi in altro ordine.

Un tal numero g si dice una *radice primitiva* del *modulo* p.

Se ad esempio $p = 5$, prendendo a considerare il numero 2 si ha

$$2^1 = 2,\quad 2^2 = 4,\quad 2^3 = 8,\quad 2^4 = 16$$

e questi numeri divisi per 5 danno rispettivamente come resti

$$2,\quad 4,\quad 3,\quad 1,$$

onde 2 è una radice primitiva del modulo 5.

Nel caso di $p = 7$, formando le potenze successive del 2 si ottengono i numeri

$$2^1 = 2,\quad 2^2 = 4,\quad 2^3 = 8,\quad 2^4 = 16,\quad 2^5 = 32,\quad 2^6 = 64.$$

che divisi per 7 danno come resti

$$2,\quad 4,\quad 1,\quad 2,\quad 4,\quad 1,$$

(1) Cfr. p. es. U. SCARPIS: *Primi elementi della teoria dei numeri*, Hoepli 1897, ed art. XXIV, cap. III (nel vol. IV).

e quindi 2 non è una radice primitiva del modulo 7. Invece le successive potenze del 3,

$$3^1 = 3, \quad 3^2 = 9, \quad 3^3 = 27, \quad 3^4 = 81, \quad 3^5 = 243, \quad 3^6 = 729$$

divise per 7 danno come resti

$$3, \quad 2, \quad 6, \quad 4, \quad 5, \quad 1,$$

onde il numero 3 è una radice primitiva del modulo 7.

Riferendoci al caso generale di un qualsivoglia numero p, supponiamo di aver determinato una radice primitiva g del modulo p, e consideriamo nuovamente una radice ε dell'equazione

$$\frac{z^p - 1}{z - 1} = 0.$$

Formando le successive potenze

$$\varepsilon^g \quad \varepsilon^{g^2}, \quad \varepsilon^{g^3} \ldots \varepsilon^{g^{p-1}},$$

vediamo che queste riproducono in altro ordine le radici

$$\varepsilon \quad \varepsilon_2 \ldots \varepsilon^{p-1}.$$

Infatti, indicando con s_r il resto della divisione di g^r per p, avremo

$$(g^r = ph + s_r)$$

$$\varepsilon^{g^r} = \varepsilon^{s_r} \quad (\varepsilon^p = 1),$$

dove s_r prende (in altro ordine) tutti i valori $1, 2 \ldots p-1$, mentre r riceve successivamente i valori $1, 2 \ldots p-1$.

Ora dividiamo le radici

$$\varepsilon^g \quad \varepsilon^{g^2} \ldots \varepsilon^{g^{p-1}}$$

in due gruppi

$$\varepsilon^g \quad \varepsilon^{g^3} \ldots \varepsilon^{g^{p-2}}$$

$$\varepsilon^{g^2} \quad \varepsilon^{g^4} \ldots \varepsilon^{g^{p-1}}$$

e poniamo

$$\eta_1 = \varepsilon^g + \varepsilon^{g^3} + \ldots + \varepsilon^{g^{p-2}}$$
$$\eta_2 = \varepsilon^{g^2} + \varepsilon^{g^3} + \ldots + \varepsilon^{g^{p-1}}$$

Dividiamo successivamente ciascuno dei gruppi formati innanzi, in altri due, ponendo

$$\left.\begin{aligned}\eta_{11} &= \varepsilon^g + \varepsilon^{g^5} + \ldots + \varepsilon^{g^{p-4}} \\ \eta_{12} &= \varepsilon^{g^3} + \varepsilon^{g^7} + \ldots + \varepsilon^{g^{p-2}}\end{aligned}\right\} \quad \eta_{11} + \eta_{12} = \eta_1$$

$$\left.\begin{aligned}\eta_{21} &= \varepsilon^{g^2} + \varepsilon^{g^6} + \ldots + \varepsilon^{g^{p-3}} \\ \eta_{22} &= \varepsilon^{g^4} + \varepsilon^{g^8} + \ldots + \varepsilon^{g^{p-1}}\end{aligned}\right\} \quad \eta_{21} + \eta_{12} = \eta_2.$$

In questo modo si può seguitare formando successivamente delle somme di

$$\frac{p-1}{4}, \quad \frac{p-1}{8} \ldots$$

termini, arrivando infine (*poichè* $p-1$ *è una potenza del* 2) a somme di un solo termine, cioè alle radici della nostra equazione. Le somme sopra indicate prendono il nome di *periodi di Gauss.* Noi mostreremo come questi periodi si possono calcolare con successive estrazioni di radici quadrate.

Osserviamo anzitutto che la somma

$$\eta_1 + \eta_2 = \eta = \varepsilon^g + \varepsilon^{g^2} + \ldots + \varepsilon^{g^{p-1}} = -1,$$

giacchè η è, a parte il segno, il coefficiente di z^{p-2} nella equazione

$$z^{p-1} + z^{p-2} + \ldots + 1 = 0$$

di cui le ε sono radici.

Consideriamo il prodotto $\eta_1\eta_2$.

Eseguendo la moltiplicazione delle due somme costituenti η_1 e η_2, si ottiene una somma di termini del tipo

$$\varepsilon^{g^r} \varepsilon^{g^s} = \varepsilon^{g^r + g^s} = \varepsilon^{g^h} = \varepsilon^{g^t},$$

cioè una somma di termini ciascuno dei quali si trova in uno dei due gruppi costituenti η_1 o η_2.

Ora l'espressione

$$\eta_1\eta_2 = \Sigma\varepsilon^t$$

non cambia quando in essa si sostituisca ε con ε^g, perchè una tale sostituzione produce soltanto (come è facile verificare) lo scambio di

$$\eta_1 \text{ con } \eta_2 \text{ e di } \eta_2 \text{ con } \eta_1.$$

Questo fatto fondamentale porta di conseguenza che la somma $\Sigma\varepsilon^{g^t}$ contiene uno stesso numero ρ di volte ogni radice dell'equazione

$$\frac{z^p - 1}{z - 1} = 0,$$

e quindi si ha

$$\eta_1\eta_2 = \Sigma\varepsilon^{g^t} = \rho\eta = -\rho.$$

Per vedere chiaramente come si arrivi a tale conseguenza, cominciamo a raggruppare nella somma i termini simili, scrivendo

$$\eta_1\eta_2 = k\varepsilon^{g^r} + \lambda\varepsilon^{g^s} + \ldots,$$

e mostriamo che i coefficienti interi k, λ... sono tutti uguali fra loro, al quale scopo basta mostrare che nessuno di essi può essere inferiore ad un altro arbitrariamente scelto.

Se ad es. nella anzidetta somma entra il termine $\rho\varepsilon^g$, sostituendo in esso ε con ε^g, si troverà il termine $\rho\varepsilon^{g^2}$ e da questo si dedurranno successivamente i termini $\rho\varepsilon^{g^3}$, $\rho\varepsilon^{g^4}$..., che dovranno tutti comparire nella somma stessa. Se nella somma compare il termine $\rho\varepsilon^{g^2}$, sostituendo in esso ε con ε^g ed operando successivamente la medesima sostituzione nei termini via via ottenuti, troveremo i termini

$$\rho\varepsilon^{g^3}, \quad \rho\varepsilon^{g^4} \ldots \rho\varepsilon^{g^{p-1}}, \quad \left(\rho\varepsilon^{g^p} = \rho\varepsilon^g\right)$$

i quali tutti dovranno comparire similmente nella somma stessa.

E così in generale dall' esistenza del termine $\rho\varepsilon^{g^t}$ si deduce che la somma deve contenere tutti i termini

$$\rho\varepsilon^{g^{t+1}} \quad \rho\varepsilon^{g^{t+2}} \ldots \rho\varepsilon^{g^{t+p-1}},$$

i quali riproducono in altro ordine

$$\rho\varepsilon^{g} \quad \rho\varepsilon^{g^2} \ldots \rho\varepsilon^{g^{p-1}}.$$

Dunque abbiamo che $\eta_1 + \eta_2$ ed $\eta_1\eta_2$ sono numeri interi, e perciò η_1, η_2 soddisfano ad un' equazione di 2° grado:

$$x^2 + x - \rho = 0$$

a coefficienti interi.

Tale equazione si risolve coll' estrazione del radicale $\sqrt{1+4\rho}$, per mezzo del quale η_1 e η_2 vengono espressi.

Procediamo ora al calcolo dei periodi di $\frac{p-1}{4}$ termini

$$\eta_{11}, \quad \eta_{12}, \quad \eta_{21}, \quad \eta_{22}.$$

Si ha anzitutto

$$\eta_{11} + \eta_{12} = \eta_1, \quad \eta_{21} + \eta_{22} = \eta_2.$$

Ora formiamo i prodotti

$$\eta_{11}\,\eta_{12}, \quad \eta_{21}\,\eta_{22}.$$

Considerando ad es. il primo di questi prodotti, vediamo che esso può ridursi ad una somma di termini del tipo ε^{g^t}, e precisamente ad una somma che non cambia quando si sostituisca in ogni termine ε con ε^{g^2}; infatti per tale sostituzione i periodi η_{11} e η_{12} vengono soltanto scambiati l'uno coll'altro. Da ciò si desume (come innanzi) che se l'espressione di $\eta_{11}\,\eta_{21}$ contiene un certo numero ρ_1 di volte un termine di η_1, essa contiene altrettante volte gli altri termini della stessa somma (se ad es. $\eta_{11}\,\eta_{12}$ contiene il termine $\rho_1\varepsilon^g$, contiene pure $\rho_1\varepsilon^{g^3}$, $\rho_1\varepsilon^{g^5}$...); analogamente se l' espressione suddetta con-

tiene ρ_2 volte un termine di η_2, essa contiene ρ_2 volte tutti gli altri termini, sicchè

$$\eta_{11}\,\eta_{12} = \rho_1\,\eta_1 + \rho_2\,\eta_2$$

ove ρ_1 e ρ_2 sono numeri interi.

Quindi η_{11}, η_{12} sono radici dell'equazione di 2° grado

$$x^2 - \eta_1\,x + (\rho_1\,\eta_1 + \rho_2\,\eta_2) = 0.$$

Così $\eta_{11}\,\eta_{12}$ si possono calcolare coll'estrazione d'una radice quadrata, partendo da η_1, η_2. Analogamente si ottengono η_{21}, η_{22}.

È chiaro ormai come si possa procedere successivamente al calcolo dei periodi di $\frac{p-1}{8}$ termini.

Considerando ad es. η_{11}, η_{12}, la loro somma è

$$\eta_{111} + \eta_{112} = \eta_{11},$$

ed il loro prodotto si esprime con una combinazione lineare a coefficienti interi di η_{11}, η_{12}, η_{21}, η_{22}; così $\eta_{111}\,\eta_{112}$ si ottengono coll'estrazione d'un nuovo radicale quadratico che porta sopra i periodi ottenuti innanzi.

Proseguendo nello stesso modo si possono costruire i periodi di

$$\frac{p-1}{16}, \quad \frac{p-1}{32} \cdots$$

termini, e finalmente i periodi di un termine

$$\left(\frac{p-1}{2^n} = 1\right),$$

cioè le radici ε dell'equazione proposta.

Possiamo dunque concludere: *Quando* p *è un numero primo della forma* $2^n + 1$, *l'equazione*

$$\frac{z^p - 1}{z - 1} = 0$$

si può risolvere con successive estrazioni di radici quadrate,

quindi il poligono regolare di p *lati è costruibile colla riga e col compasso.*

OSSERVAZIONE. — Nel ragionamento precedente non abbiamo tenuto conto dell'ambiguità che si presenta nella scelta dei segni da attribuirsi ai radicali quadratici successivamente introdotti. E di tale ambiguità non occorre invero preoccuparsi, quando si ha in vista di mostrare soltanto come i periodi η possono esprimersi mediante radicali quadratici, e quindi la stessa equazione data $\frac{z^p - 1}{z - 1} = 0$ sia risolubile mediante i radicali suddetti. Procedendo alla risoluzione effettiva, ove si lasci sussistere l'indeterminatezza dei segni dei nominati radicali, si troveranno tutte le radici ε dell'equazione proposta. Ma se venisse assegnata *a priori* una particolare radice ε per la costruzione dei periodi η, volendo giungere al calcolo di essa, si dovrebbe via via determinare i segni suindicati in modo conveniente. Le particolari regole di determinazione che qui occorrono, si troveranno spiegate, pel caso $p = 17$, nell'art. XVIII, ove hanno un'interesse per la costruzione effettiva dell'ettadecagono.

§ 8. **Sui numeri primi della forma $2^n + 1$.** — I risultati ottenuti diventano più espressivi in forza della seguente osservazione:

Ogni numero primo della forma $2^n + 1$ *è un numero della forma* $2^{2^\nu} + 1$, vale a dire se $2^n + 1$ è un numero primo, n deve essere, alla sua volta, una potenza del 2.

Per giustificare questa proposizione, basta notare che se n ammette qualche divisore dispari

$$2k + 1 \quad [n = h(2k + 1)],$$

il numero

$$2^n + 1 = 2^{h(2k+1)} + 1$$

non può essere primo.

Ora si riconosce subito che il numero $2^{h(2k+1)}$ non può esser primo, essendo divisibile per $2^h + 1$. Infatti il binomio

$$x^{2k+1} + 1$$

si annulla per $x = -1$ e perciò è divisibile per $x + 1$:

$$x^{2k+1} + 1 = (x + 1)[x^{2k} - x^{2k-1} + \ldots + (-1)^r x^{2k-2} + \ldots + 1];$$

facendo

$$x = 2^h$$

si ha appunto che $2^{h(2k+1)} + 1$ è divisibile per $2^h + 1$.

Ora i risultati dei numeri precedenti si possono enunciare dicendo:

I poligoni regolari di un numero primo p *di lati, costruibili colla riga e col compasso, sono quelli per cui* p *è della forma*

$$p = 2^{2^\nu} + 1.$$

Per vedere la portata di questo enunciato, diamo a ν i valori

$$\nu = 0, \quad 1, \quad 2, \quad 3, \quad 4;$$

otteniamo dalla formula

$$p = 2^{2^\nu} + 1$$

i numeri primi

$$3, \quad 5, \quad 17, \quad 257, \quad 65537.$$

I valori 1, 3 e 5 di p corrispondono ai casi notissimi del triangolo equilatero e del pentagono regolare; mentre i valori successivi danno luogo a tre nuovi poligoni regolari costruibili, fra i quali è particolarmente notevole il caso $p = 17$. La risoluzione dell' equazione binomia $z^{17} = 1$ fu data dal GAUSS, ed alle costruzioni geometriche dell'ettadecagono si volsero successivi lavori (LEGENDRE, GRUNERT, STAUDT, SERRET, SCHRÖTER, GÉRARD) dei quali è dato un resoconto nell' art. XVIII.

Il caso $p = 257$ fu studiato da RICHELOT [1], i risultati di lui furono interpretati geometricamente dal sig. AFFOLTER e dal sig. PASCAL [2].

(1) Crelle's Journal, Bd. 9.

(2) Rendic. della R. Accademia di Napoli, 1887.

Il caso $p = 65537$ è stato oggetto di un accuratissimo studio del sig. HERMES (1).

Ora che cosa accade per $\nu > 4$? Si otterranno ancora dei numeri primi

$$p = 2^{2^\nu} + 1,$$

e quindi dei nuovi poligoni regolari costruibili?

I casi finora studiati si riferiscono ai numeri corrispondenti a

$$\nu = 5, \quad 6, \quad 7,$$

cioè ai numeri

$$2^{2^5} + 1, \quad 2^{2^6} + 1, \quad 2^{2^7} + 1,$$

i quali sono composti.

Pertanto resta dubbio se la serie dei numeri

$$2^{2^\nu} + 1$$

comprenda altri numeri primi, all'infuori di quelli corrispondenti ai valori

$$\nu = 0, \quad 1, \quad 2, \quad 3, \quad 4.$$

§ 9. **Applicazione del metodo di Gauss al caso del pentagono regolare.** — Daremo infine, come esempio, l'applicazione del metodo esposto alla risoluzione dell'equazione

$$z^5 = 1,$$

da cui dipende la costruzione del pentagono regolare.

Le radici della equazione predetta sono

$$1, \quad \varepsilon, \quad \varepsilon^2, \quad \varepsilon^3, \quad \varepsilon^4,$$

ove

$$\varepsilon = \cos\frac{2\pi}{5} + i \operatorname{sen}\frac{2\pi}{5}.$$

Scegliamo una radice primitiva del modulo 5, e sia $g = 2$; allora le ε verranno ordinate nel modo seguente:

$$\varepsilon^2, \quad \varepsilon^4, \quad \varepsilon^8, \quad \varepsilon^3, \quad \varepsilon^{16} = \varepsilon.$$

(1) Cfr. *Göttinger Nachrichten*, 1894.

I periodi binari sono dati da

$$\eta_1 = \varepsilon^2 + \varepsilon^3, \quad \eta_2 = \varepsilon^4 + \varepsilon;$$

e si ha

$$\eta_1 + \eta_2 = \eta = -1$$

$$\eta_1\eta_2 = (\varepsilon^2 + \varepsilon^3)(\varepsilon^4 + \varepsilon) = \varepsilon^6 + \varepsilon^3 + \varepsilon^7 + \varepsilon^4 =$$

$$= \varepsilon + \varepsilon^3 + \varepsilon^2 + \varepsilon^4 = \eta = -1,$$

onde η_1 e η_2 sono le radici dell'equazione

$$x^2 + x - 1 = 0,$$

cioè

$$\eta_1 = -\frac{1}{2} \pm \frac{1}{2}\sqrt{5}$$

$$\eta_2 = -\frac{1}{2} \pm \frac{1}{2}\sqrt{5}.$$

Consideriamo i periodi di un termine

$$\eta_{21} = \varepsilon^4, \quad \eta_{22} = \varepsilon,$$

dove

$$\eta_{21} + \eta_{22} = \eta_2$$

$$\eta_{21}\eta_{22} = \varepsilon^5 = 1,$$

costruiremo l'equazione di 2° grado

$$x^2 - \eta x_2 + 1 = 0,$$

e risolvendola otterremo

$$\varepsilon = \frac{1}{4}\left\{-1 \mp \sqrt{5} \pm \sqrt{-10 \pm 2\sqrt{5}}\right\}$$

ossia

$$\varepsilon = \frac{1}{4}\left\{-1 \mp \sqrt{5} \pm i\sqrt{10 \mp 2\sqrt{5}}\right\}.$$

Le 4 radici ε dell'equazione binomia sono date da questa formula ove si attribuiscano ai radicali i segni + e −. Si può riconoscere geometricamente (in modo molto facile) che la radice

$$\varepsilon = \cos\frac{2\pi}{5} + i\,\mathrm{sen}\,\frac{2\pi}{5}$$

viene data assumendo tutti i radicali positivamente, cioè ponendo

$$\varepsilon = \frac{1}{4}\left\{-1+\sqrt{5}+i\sqrt{10+2\sqrt{5}}\right\}.$$

La formula

$$r_{12} = 2\cos\frac{2\pi}{5} = -\left(\frac{1}{2}+\sqrt{5}\right)$$

dà una semplicissima costruzione del pentagono regolare, che giova confrontare con la costruzione di EUCLIDE (IV, 11) e colle altre costruzioni elementari che vi si riattaccano.

§ 10. **Poligoni regolari con un numero di lati composto.** — Diciamo ora qualche cosa intorno alla costruibilità dei poligoni regolari di n lati, dove n è un numero composto. Anzitutto osserviamo che se n si decompone nel prodotto di due numeri interi p, q:

$$n = pq,$$

dato lo $n$gono regolare si costruiranno subito il $p$gono e il $q$gono. Infatti dato l'arco di cerchio $\frac{2\pi}{n}$ (la cui corda è il lato dello $n$gono), o, se si vuole, dato il relativo angolo al centro, basterà moltiplicarlo per q per ottenere l'arco o angolo

$$\frac{2\pi q}{n} = \frac{2\pi}{p},$$

da cui dipende la costruzione del $p$gono.

Pongasi ora che n sia scomposto nei suoi fattori primi $p_1, p_2, \ldots p_r$:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}.$$

Affinchè la costruzione dello $n$gono sia possibile, dovrà esser possibile la costruzione dei poligoni regolari di $p_1^{\alpha_1}$, $p_2^{\alpha_2}, \ldots p_r^{\alpha_r}$ lati.

La costruzione del poligono regolare di p^α lati, $(\alpha > 1)$, dipende dalla risoluzione dell'equazione binomia

$$z^{p^\alpha} = 1,$$

la quale (come è chiaro anche geometricamente) ammette tutte le radici dell'equazione

$$z^{p^{\alpha-1}} = 1.$$

L'equazione

$$\frac{z^{p^{\alpha}} - 1}{z^{p^{\alpha-1}} - 1}$$

è irriducibile.

Questo teorema si dimostra collo stesso ragionamento di EISENSTEIN che ha servito pel caso $\alpha = 1$ (§ 5).

Da esso discende la conseguenza che l'equazione anzidetta sarà risolubile per radicali quadratici, solo quando il suo grado $p^{\alpha} - p^{\alpha-1} = p^{\alpha-1}(p-1)$ sia una potenza del 2. Ma il numero $p^{\alpha-1}$ ove $\alpha > 1$, non può essere una potenza del 2 se non è $p = 2$.

Di qui si deduce che non vi è alcun poligono regolare costruibile di p^{α} lati, ove

$$\alpha > 1, \quad p > 2.$$

Dunque se lo *n*gono regolare è costruibile, il numero

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r},$$

deve contenere, all'infuori di una certa potenza del 2, tutti fattori primi differenti (elevati alla potenza 1), e questi fattori p debbono essere ciascuno della forma $2^{2^{\nu}} + 1$, giacchè il poligono regolare di p lati deve risultare costruibile (§ 8); insomma il numero n deve essere della forma

$$n = 2^{\nu}\left(2^{2^{\nu_1}} + 1\right) \dots \left(2^{2^{\nu_s}} + 1\right),$$

ove $\nu_1, \nu_2 \dots \nu_s$ sono tutti differenti fra loro, e

$$p_1 = 2^{2^{\nu_1}} + 1, \quad p_2 = 2^{2^{\nu_2}} + 1 \dots$$

sono numeri primi.

Dimostriamo infine che quando n è un numero della forma indicata, la costruzione dello *n*gono regolare è effettuabile.

A tal fine basta far vedere come « dati i poligoni regolari di r, s lati ove r, s sono numeri primi fra loro, si possa costruire il poligono regolare di $n = rs$ lati ».

Supponendo dati i poligoni regolari di r, s lati, sono dati gli angoli al centro corrispondenti

$$a = \frac{2\pi}{r}, \quad b = \frac{2\pi}{s}.$$

Ora, essendo r e s primi fra loro, si può risolvere l'equazione d'analisi indeterminata

$$sx - ry = 1,$$

determinando due numeri interi x, y che vi soddisfino; allora si avrà

$$ax - by = 2\pi\left(\frac{x}{r} - \frac{y}{s}\right) = \frac{2\pi}{rs} = \frac{2\pi}{n}.$$

e perciò si otterrà la costruzione dell'angolo al centro dello $n$gono (e quindi la costruzione dello $n$gono stesso) facendo la differenza tra gli angoli ax e by.

Come esempio consideriamo il caso del pentadecagono regolare ($n = 15$), la cui costruzione si può dedurre da quelle del triangolo equilatero e del pentagono regolare. Risolviamo l'equazione d'analisi indeterminata

$$3x - 5y = 1,$$

ponendo

$$x = 2, \quad y = 1.$$

L'angolo al centro del pentadecagono si costruisce quindi facendo la differenza fra il doppio dell'angolo al centro del pentagono e l'angolo al centro del triangolo equilatero:

$$\frac{2\pi}{15} = 2 \cdot \frac{2\pi}{5} - \frac{2\pi}{3}.$$

Questa costruzione non differisce sostanzialmente da quella di EUCLIDE (IV, 16) ove si biseca l'angolo

$$\frac{2\pi}{3} - \frac{2\pi}{5} = \frac{4\pi}{15}.$$

Riassumendo infine i risultati ottenuti, possiamo enunciare il teorema:

Gli n*goni regolari costruibili colla riga e col compasso sono, tutti e soli, quelli per i quali il numero* n *decomposto in fattori primi, è della forma*

$$n = 2^{\nu} \cdot (2^{2^{\nu_1}} + 1) \cdot (2^{2^{\nu_2}} + 1) \dots (2^{2^{\nu_s}} + 1),$$

ove $\nu_1, \nu_2 \dots \nu_s$ *sono differenti fra loro.*

§ 11. **Osservazioni sulla determinazione dei poligoni regolari che non sono costruibili elementarmente.** — Termineremo questo articolo con alcune osservazioni relative alla determinazione dei poligoni regolari che non sono costruibili colla riga e col compasso. E riferendoci al più semplice caso di un poligono regolare di p lati, ove p è un numero primo, spiegheremo sopra un esempio che cosa c' insegni a tale proposito il metodo di GAUSS per la risoluzione dell' equazione binomia:

$$z^p = 1.$$

Prendiamo dunque $p = 7$, e consideriamo le radici dell' equazione $z^7 = 1$ (tolta la $z = 1$):

$$\varepsilon, \quad \varepsilon^2, \quad \varepsilon^3, \quad \varepsilon^4, \quad \varepsilon^5, \quad \varepsilon^6,$$

ove

$$\varepsilon = \cos\frac{2\pi r}{7} + i \operatorname{sen}\frac{2\pi r}{7}.$$

Scegliamo una radice primitiva del modulo 7, e sia $g = 3$; essa ci permette di ordinare le ε nel modo seguente:

$$\varepsilon^3, \quad \varepsilon^{3^2} = \varepsilon^2, \quad \varepsilon^{3^3} = \varepsilon^6, \quad \varepsilon^{3^4} = \varepsilon^4, \quad \varepsilon^{3^5} = \varepsilon^5, \quad \varepsilon^{3^6} = \varepsilon.$$

Formiamo i periodi di tre termini

$$\eta_1 = \varepsilon^3 + \varepsilon^{3^3} + \varepsilon^{3^5} = \varepsilon^3 + \varepsilon^6 + \varepsilon^5$$
$$\eta_2 = \varepsilon^{3^2} + \varepsilon^{3^4} + \varepsilon^{3^6} = \varepsilon^3 + \varepsilon^4 + \varepsilon;$$

abbiamo

$$\eta_1 + \eta_2 = -1 \quad (\eta = \Sigma\varepsilon)$$

$$\eta_1 \eta_2 = (\varepsilon^3 + \varepsilon^6 + \varepsilon^5)(\varepsilon^2 + \varepsilon^4 + \varepsilon) = \varepsilon^5 + \varepsilon^7 + \varepsilon^4 + \varepsilon^8 + \\ + \varepsilon^{10} + \varepsilon^7 + \varepsilon^7 + \varepsilon^9 + \varepsilon^6 = \eta + 3 = 2,$$

e quindi η_1, η_2 soddisfano all'equazione di 2° grado

$$x^2 + x + 2 = 0.$$

Una volta calcolati η_1, η_2, la determinazione delle radici ε viene a dipendere da un'equazione di 3° grado; infatti si ha per es.

$$\varepsilon^2 + \varepsilon^4 + \varepsilon = \eta_2$$
$$\varepsilon^2 \cdot \varepsilon^4 + \varepsilon^2 \cdot \varepsilon + \varepsilon^4 \cdot \varepsilon = \eta_1$$
$$\varepsilon^2 \cdot \varepsilon^4 \cdot \varepsilon = 1,$$

e quindi ε^2, ε^4, ε sono radici dell'equazione

$$x^3 - \eta_2 x^2 + \eta_1 x - 1 = 0.$$

Dalla effettuata riduzione dipende la *possibilità di ricondurre la costruzione dell' ettagono regolare alla trisezione d'un angolo* (cfr. art. XIX).

Il problema generale dell'equazione binomia $z^p = 1$, ove p è un numero primo qualunque, ammette sempre una riduzione (come per $p = 7$), potendosi ricondurre alla risoluzione di una serie di equazioni di grado inferiore: se $p - 1$, decomposto in fattori primi, è della forma

$$p - 1 = 2^{\alpha_1} \cdot 3^{\alpha_2} \cdot 5^{\alpha_3} \ldots,$$

si dovranno risolvere precisamente

α_1 equazioni successive di 2° grado,
α_2 equazioni del 3°,
α_3 equazioni del 5°, ecc.

Una tale riduzione è portata dal metodo di GAUSS che conduce a formare successivamente periodi di

$$\frac{p-1}{2}, \quad \frac{p-1}{4}, \ldots \quad \frac{p-1}{2^{\alpha_1}}$$

termini, quindi periodi di

$$\frac{p-1}{2^{\alpha}\cdot 3}\cdots\frac{p-1}{2^{\alpha_1}3^{\alpha_2}}$$

termini, periodi di

$$\frac{p-1}{2^{\alpha_1}3^{\alpha_2}\cdot 5}\cdots\frac{p-1}{2^{\alpha_1}3^{\alpha_2}5^{\alpha_3}}$$

termini ecc. (1).

NOTA. — I problemi concernenti la costruzione dei poligoni regolari di $p=9$ e di $p=7$ lati hanno un interesse storico particolare per la loro antichità, offrendoci una catena di risultati che collegano il libro IV dell' EUCLIDE alla teoria generale di GAUSS.

La costruzione del 9gono trovasi ricondotta ad un problema di 3° grado già dagli Arabi, e prima del 1000 della nostra èra; un' analoga riduzione s' incontra poi nell' Algebra di RAFFAELE BOMBELLI.

La costruzione dell' ettagono (similmente ridotta a equazioni di 3° grado) viene brillantemente trattata da PACIOLI, FERRARI, CARDANO e KEPLERO. Sviluppi interessanti su tali costruzioni sono dati da AMEDEO AGOSTINI nel libro IV de « Gli Elementi d' Euclide e la critica antica e moderna » editi da FEDERIGO ENRIQUES (Roma, Stock, 1925).

Aggiungeremo che le equazioni binomie, prima di GAUSS, furono oggetto di studio dei matematici del secolo 18°; in particolare VANDERMONDE (1776) ha ricondotto l' equazione $z^{11}=1$ all' estrazione d' una $\sqrt[5]{\ }$.

In tal guisa appunto il pensiero matematico si avvia sulla strada che Gauss ha percorsa; ma occorreva, non solo spingere più avanti le indagini accennate, sì anche comprendere il legame fra le equazioni binomie e il problema dei poligoni regolari: che è un frutto della rappresentazione geometrica dei numeri complessi.

Infine daremo l' indicazione di altri lavori più recenti che — al lume della teoria di Gauss — illustrano alcuni

(1) Cfr. BACHMANN *l. c.*, BIANCHI *l. c.*, ove sono pure date le formule per la risoluzione effettiva.

casi semplici relativi a poligoni regolari di p lati, in cui $p-1$ ha soltanto fattori primi uguali a 2 e 3. Questi casi c' interessano dal punto di vista geometrico, perchè conducono a costruzioni effettuabili con un *trisettore degli angoli* o con una *parabola fissa* (cfr. art. XIX).

Per $p=7$, 13, 97, si può vedere E. PASCAL « Giornale di Matematiche di Napoli » vol. XXV. Per $p=19$, 37, I. AMALDI, *ibidem*, vol. XXX.

ARTICOLO VENTITREESIMO

Alcune osservazioni generali sui problemi geometrici di Federigo Enriques a Roma.

Allo studio particolare delle varie questioni trattate nei precedenti articoli, facciamo seguire alcune osservazioni sintetiche intorno ai problemi geometrici, accennando in qualche punto a considerazioni di un ordine superiore. Ma anche dove le nostre osservazioni poco aggiungano a ciò che fu detto in occasione di questo o di quel gruppo di problemi, stimiamo non inutile di averle sott'occhio nel loro insieme, a fine di istituire più facilmente un giudizio comparativo delle accennate ricerche.

§ 1. **Scopo pratico delle ricerche geometriche.** — La risoluzione grafica dei problemi costruttivi costituisce un primo e fondamentale scopo della Geometria. Anche dove codesto scopo sembri quasi dimenticato nel procedere della ricerca teorica, è facile rintracciare la sua influenza direttrice su questa.

In primo luogo, ogni teorema geometrico, facendoci conoscere alcuni rapporti fra gli elementi di una figura, si può considerare come una *condizione* imposta alla costruzione di essa. Così per es. l'inverso del teorema di Pitagora, ci apprende che se il quadrato del segmento a, deve equivalere alla somma dei quadrati di b, c, il triangolo avente per lati a, b, c deve essere rettangolo, essendo retto l'angolo contenuto da b, c; questo insegnamento esprime una condizione a cui deve soddisfare chi voglia sommare o sottrarre due quadrati, la quale contiene anzi la risoluzione dello stesso problema costruttivo, trattandosi di condizione *sufficiente*.

In generale l'analisi delle proprietà di una figura geometrica, riuscendo analogamente a stabilire delle condizioni costruttive di essa, potrà ritenersi esaurita solo quando le relazioni scoperte fra i suoi elementi permettano di vedere come la figura stessa riesca determinata dall'assumere alcuni di questi in modo arbitrario.

Si tratti per es. di un poliedro regolare a dodici facce (dodecaedro). Anzitutto si riconoscerà che le sue facce sono pentagoni e i suoi angoli solidi sono triedri; ma la costruzione effettiva del poliedro potrà dirsi determinata solamente quando sia messo in luce che, nella proiezione ortogonale di esso sul piano di una faccia, le immagini dei vertici costituiscono due decagoni regolari concentrici, tali che il raggio del cerchio circoscritto al maggiore supera l'altro di un segmento uguale alla sezione aurea di questo (1).

§ 2. **Problemi indeterminati.** — I problemi della Geometria possono concernere figure *piane* o *solide*; ma, in questo secondo caso, il metodo semplice e generale delle proiezioni ortogonali dovuto a MONGE, permette di ridurci sempre a costruzioni nel piano, ed una tale riduzione può anche raggiungersi facilmente con apposite considerazioni dirette, nei varî casi particolari, come ad es. per la duplicazione del cubo si è visto nell'art. XIX.

Pertanto ci riferiremo sempre nel seguito a questioni di Geometria in un piano.

I problemi geometrici possono essere *determinati* o *indeterminati*.

Si considerano come determinati quei problemi in cui si tratta di costruire una figura, per mezzo di elementi e di relazioni date, quando la figura che risolve il problema non è suscettibile di movimento o di *variazione continua*; all'opposto si chiamano indeterminati quei problemi che ammettono infinite soluzioni, capaci di variare con continuità, per modo che sia possibile ancora di assegnare, entro certi limiti, qualche elemento o qualche relazione ulteriore, a cui la figura proposta debba soddisfare.

(1) Cfr. per es. ENRIQUES, *Lezioni di Geometria descrittiva*. Bologna, Zanichelli, 2ª ed. 1908, pag. 95

Appartengono in particolare alla prima categoria dei problemi determinati, tutti i problemi che ammettono uno od un numero finito di soluzioni; ma è anche determinato per es. il problema di costruire sopra una retta, a partire da un'origine assegnata, un segmento avente la lunghezza di arco di raggio 1 di cui è data la tangente trigonometrica, giacchè le soluzioni che qui si ottengono, costituiscono una serie discreta (se y è uno dei segmenti che risolve il problema $\text{arc tg}\, x = y \pm n\pi$).

Sono invece, secondo la definizione, problemi indeterminati, quelli in cui è questione soltanto della grandezza degli elementi (segmenti, angoli,...,) di una figura, poichè insieme ad una soluzione si hanno allora tutte quelle ottenute col movimento di essa. Si conviene però di ridurre sistematicamente questo genere di problemi, prescindendo da quella indeterminazione che tiene soltanto alla posizione della figura; ciò equivale ad aggiungere alle condizioni assegnate la posizione di un qualche elemento della figura stessa (per es. di un segmento di essa), in modo da rendere impossibile il suo movimento nel piano.

Con questa avvertenza i problemi geometrici possono generalmente trasformarsi in modo che i dati siano dei punti del piano, e gli elementi incogniti sieno ancora dei punti che hanno con quelli certe relazioni prestabilite (cfr. art. XVI, § 7). Se allora i punti incogniti sono suscettibili di variare con continuità sopra linee o entro superficie, il problema sarà indeterminato; determinato nel caso opposto.

Il tipo più elementare dei problemi indeterminati è quello in cui si tratta di descrivere una *linea*, i cui punti soddisfino (rispetto a certi dati) ad una relazione prestabilita. Un tale problema è da riguardarsi praticamente come risoluto quando è dato un *istrumento* (costituito da un sistema meccanico dotato di un certo grado di libertà) atto a tracciare la linea proposta, e quando inoltre si riesca, mediante l'istrumento o mediante altri istrumenti dati, a determinare gli elementi da cui la linea dipende.

Trattasi per es. di costruire il luogo dei punti da cui vedesi un dato segmento AB, secondo un angolo dato α: questo luogo è un arco di circolo, che può essere tracciato col *compasso*, dopo avere determinato il centro e il raggio,

ciò che può farsi (come è noto) col compasso stesso (o col compasso e la riga).

Pertanto il problema della costruzione di una linea richiede generalmente:

1) una trasformazione delle proprietà geometriche a cui debbono soddisfare i punti della linea, che permetta di riconoscere una *generazione meccanica* di essa;

2) un *istrumento* capace di realizzarla;

3) la determinazione degli elementi della linea cui si collega la generazione suddetta.

In questo senso il problema della costruzione di una linea può riguardarsi sempre come *risolubile*, restando al ricercatore ampia facoltà d'immaginare istrumenti adatti allo scopo. Così per es. varie generazioni meccaniche dell'ellisse rendono possibile, in diversi modi, la costruzione di un istrumento descrittore (*compasso ellittico* di LEONARDO DA VINCI, cfr. art. XIX); così ancora la proprietà della parabola algebrica d'ordine n di essere curva integrale di una parabola d'ordine $n-1$, permette di tracciare la curva (a partire dalla retta), con $n-1$ applicazioni successive dell'*integrafo* (art. XXII) ecc.

La cosa si presenta sotto un aspetto diverso se si tratti di costruire una linea con *istrumenti assegnati*. Allora è subito facile di riconoscere se la linea proposta appartenga o no alla classe di quelle generabili cogli istrumenti dati; e, se non vi appartiene, il problema appare, nel senso anzidetto, *irrisolubile*. Così è per es. se si domandi di costruire colla riga e col compasso il luogo dei punti equidistanti da un centro e da una retta data; questo luogo è una *parabola*, e non appartiene quindi alla classe delle linee (rette e circoli) costruibili cogl'istrumenti dati.

In simili casi in luogo di una *costruzione immediata* della linea, può esserne richiesta una *costruzione per punti* assai vicini, la quale è da riguardarsi come una *risoluzione approssimata* del problema proposto.

Nell'esempio citato, la parabola si costruisce per punti intersecando un cerchio variabile che abbia il centro nel punto dato (fuoco) colla parallela alla retta (direttrice) distante da essa del raggio del cerchio, e giacente nella banda del punto suddetto. In un modo analogo si può costruire per punti, colla squadra, il circolo che ha un dato diametro AB;

ed anzi lo stesso circolo può costruirsi per punti, colla sola riga, se è dato anche il diametro di esso perpendicolare ad AB (cfr. art. XV).

La costruzione di una linea per punti riconduce in sostanza il problema indeterminato proposto ad una successione (teoricamente grande quanto si vuole) di problemi determinati dipendenti da elementi in parte arbitrarii. Analiticamente si tratta della *rappresentazione parametrica* di una linea $f(xy)=0$, per mezzo di funzioni di un parametro t:

$$x=\varphi(t), \quad y=\psi(t);$$

per ogni valore arbitrariamente dato a t devonsi costruire i segmenti x ed y (1).

§ 3. **Problemi determinati.** — Abbiamo visto che il tipico problema indeterminato della costruzione di una linea, dove non si tratti dell'invenzione meccanica di apposito istrumento, viene subordinato alla risoluzione di una serie di problemi determinati (costruzione delle linee per punti).

Viceversa « i punti che risolvono un problema determinato si ottengono generalmente (mercè il metodo dei luoghi) come *intersezioni di linee*, che i nostri istrumenti ci permettono di tracciare ». In questo senso si adoperano di continuo,

(1) Appare di qui che non sempre può essere domandata la costruzione per punti di una linea per mezzo di costruzioni assegnate. Per es. la costruzione *lineare* per punti esige (art. XVI) che le funzioni φ e ψ sieno razionali, e quindi che la curva $f(xy)=0$ sia algebrica *di genere* 0 (Clebsch).

Tuttavia queste osservazioni si riferiscono al caso in cui si voglia far dipendere la determinazione del punto generico della linea da una costruzione assegnata, sempre la stessa, che operi sopra un elemento arbitrario. Ben più ardua è la questione di decidere se una curva contenga una serie infinita di punti, vicini tra loro quanto si vuole, ciascuno dei quali sia costruibile con una costruzione propria, effettuabile con dati mezzi. Per es. la curva di 3° ordine, senza punti doppi, è di genere 1 e non può essere costruita linearmente per punti nel senso detto prima, perchè è impossibile esprimere le sue coordinate con funzioni razionali di un parametro; tuttavia essa può contenere infiniti punti di coordinate razionali, ed è stato dimostrato da B. Levi che — ove ciò accada — vicino a ciascun punto razionale ne cadono infiniti. Cfr. Enriques-Chisini, *Lezioni sulla teoria geometrica delle equazioni e delle funzioni algebriche*, Vol. III, pagina 348. Bologna, Zanichelli, 1924.

nella risoluzione dei problemi determinati, gl'*istrumenti descrittori di linee*, per es. la riga, il compasso ecc.

Accanto a questo genere d'istrumenti, trovano anche impiego istrumenti di una natura diversa (costituiti da sistemi che realizzano una relazione geometrica data) i quali porgono in un modo più immediato certe costruzioni determinate. Tali sono per es. il *trasportatore di segmenti* costituito da un'asticella o da una striscia di carta di lunghezza fissa, la *squadra* e la *falsa squadra*, la *riga a due orli paralleli* (art. XV, XVI): istrumenti suscettibili di essere adoprati in vario modo, ad ottenere la costruzione immediata di punti o rette, che trovinsi in certe semplici relazioni con punti o rette dati.

Ma in un primo sguardo ai problemi è permesso di attribuire a questo genere d'istrumenti un'importanza secondaria; perciò nel seguito, riferendoci espressamente ai problemi determinati, riterremo il punto di vista dominante nella risoluzione di essi, che è la « ricerca dei punti incogniti come *intersezioni di linee* ». D'altronde alcune distinzioni e classificazioni che saremo condotti a sviluppare, riesciranno indipendenti dalla restrizione così introdotta.

§ 4. **Principio di economia.** — Ogni problema *possibile* (che ammetta soluzioni) può essere *risoluto* coll'impiego di istrumenti adatti allo scopo; e la fantasia può moltiplicare all'infinito l'invenzione dei mezzi meccanici atti a fornire la risoluzione anzidetta. Ma (secondo le vedute generali del MACH) la scienza non chiede soltanto la risoluzione dei problemi proposti, bensì anche la risoluzione *più economica*. E qui si tratta non soltanto di *economia del pensiero*, ma anche di *risparmio di complicate fabbricazioni meccaniche*, o di *economia di lavoro* per ogni istrumento dato ecc.

Vediamo dunque quale influenza direttrice il criterio della economia abbia esercitato nel campo dei problemi geometrici costruttivi.

§ 5. **Classificazione dei problemi.** — La fantasia non disciplinata cerca per *ogni* costruzione particolare il mezzo *più semplice* di effettuarla. La scienza tende a *classificare e ordinare i problemi per gruppi*, in guisa che per ciascun gruppo occorra l'impiego dei medesimi istrumenti.

Questa è una prima esigenza economica relativa ad una veduta dei problemi nel loro insieme.

§ 6. **Criterii di classificazione.** — Si presentano tre aspetti principali sotto cui i problemi si lasciano naturalmente classificare.

Questi criterii di classificazione scaturiscono dalla ricerca sistematica (che abbiam detto dominante in quest'ordine di questioni) di ottenere la risoluzione dei problemi determinati per mezzo della intersezione di linee.

Pertanto i problemi stessi si lasciano classificare, in base

1) alla *semplicità meccanica* degli istrumenti atti a descrivere le linee risolutrici;

2) oppure alla *semplicità geometrica* di queste linee;

3) o infine alla *semplicità analitica* delle equazioni da cui il problema viene a dipendere, secondo il metodo cartesiano.

Secondo il primo criterio (tenuto in vista dal NEWTON) si potranno porre ad es., subito dopo i problemi risolubili col cerchio (compasso), quelli che vengono risolti dalla concoide di NICOMEDE (cfr. art. XIX); mentre in ordine al secondo criterio appare più semplice la risoluzione dei problemi mediante coniche.

Il criterio geometrico, che si riferisce alla semplicità delle linee da cui può farsi dipendere la risoluzione di un problema, trova riscontro, almeno fino ad un certo punto, nel criterio analitico (di DESCARTES) che guarda alla natura delle equazioni da cui dipende la determinazione delle incognite.

In ordine a questo criterio i problemi si distinguono in *algebrici* e *trascendenti*, ed i problemi algebrici si lasciano classificare secondo il loro *grado*.

È da notarsi che i gruppi di problemi occupanti i primi posti nella classificazione analitico-geometrica (problemi di 1° e 2° grado) si trovano in pari tempo i più elementari anche sotto l'aspetto meccanico della costruzione risolutrice.

Quanto al valore comparativo dei citati punti di vista, sono da fare le osservazioni seguenti.

Il criterio meccanico risponde meglio allo scopo, quando (imponendoci una condizione teorica di esattezza) si vogliano adoprare soltanto linee che sappiansi meccanicamente trac-

ciare; se invece si ammetta di usare linee costruite per punti, la facilità della costruzione sarà generalmente in rapporto alla semplicità geometrica delle linee stesse, e quindi, ove si scelga un'adatta rappresentazione, alla semplicità analitica delle equazioni rappresentative.

È anche da avvertire che la questione di classificare i problemi costruttivi si presenta diversamente, secondo si tratta di *ordinare i problemi già risoluti*, oppure di misurare anticipatamente la difficoltà che possono presentare certe classi di *problemi da risolvere*. Se, al primo scopo, risponde meglio il criterio meccanico, appare invece più confacente al secondo, il criterio geometrico e soprattutto quello analitico; infatti, quando un problema sia soltanto enunciato, riesce in generale difficile di giudicare subito quali mezzi meccanici esso potrà richiedere, mentre si riconosceranno più facilmente certi caratteri geometrici delle linee che si presentano come atte a risolverlo secondo il metodo dei luoghi, e soprattutto riuscirà facile di formarne le equazioni colla Geometria analitica. D'altronde è opportuno che diversi aspetti dominino la classificazione dei problemi, poichè diverse possono essere le esigenze ad essi relative.

§ 7. **Come si misura la semplicità della risoluzione di un problema.** — Il principio generale della *risoluzione più economica* si può intendere:

1) in un *senso qualitativo*, ove si domandi di effettuare una certa costruzione con dati istrumenti piuttosto che con altri;

2) in un *senso quantitativo* ove si chieda la costruzione *più rapida*, per la quale occorra un *minimo numero di operazioni* effettuate coi medesimi istrumenti.

Naturalmente il criterio quantitativo è subordinato al criterio qualitativo. A priori non si può ritenere indifferente di tirare una retta oppure un cerchio, di usare la riga o il compasso o la squadra. Bisogna dunque *numerare separatamente le operazioni che si fanno con ciascun istrumento*; come appunto insegna la Geometrografia di LÉMOINE. Ma è permesso di stabilire un certo *rapporto di equivalenza* fra il numero delle operazioni effettuate con un dato istrumento e il numero delle operazioni effettuate con un altro, fissando

per es. questo rapporto in base al tempo richiesto per effettuare serie di operazioni equivalenti.

La possibilità di misurare — in base a criterii diversi — il suddetto rapporto d'equivalenza, riconduce anche, nell'ambito di queste considerazioni quantitative, il caso (nettamente qualitativo) in cui l'operazione che esige un certo istrumento si considera rimpiazzata utilmente da un numero — comunque grande — di operazioni effettuate con un altro. Se infatti questo istrumento non è a nostra disposizione o lo diviene soltanto a costo di gravi sacrifici, si può dire che l'anzidetto *rapporto d'equivalenza* fra operazioni eseguite col secondo istrumento e operazioni eseguite col primo, diventa grandissimo o addirittura *infinito*.

In tal caso nasce la ricerca sistematica di risolvere tutti i problemi col primo istrumento a preferenza del secondo; e — per quei problemi che non sieno risolubili in tal modo — sorge la domanda se *una sola operazione* fatta col secondo istrumento (o magari una costruzione per punti) possa fornirci una *linea* o *figura fondamentale, data la quale* i problemi di cui si tratta si risolvano facendo uso soltanto del primo istrumento.

Così appunto accade nella ricerca sistematica di STEINER di risolvere i problemi di 2° grado coll'uso della sola riga, quando sia *dato un cerchio fisso* (cfr. art. XV, XVI). Un secondo esempio è offerto dalla risoluzione dei problemi di 3° grado con *riga* e *compasso, data una parabola fissa* (articolo XIX).

§ 8. **Valore relativo degli istrumenti.** — La conclusione più importante che scaturisce dalle varie classificazioni dei problemi in ordine ad istrumenti diversi, è un giudizio comparativo sul valore degli istrumenti stessi.

Poichè ad ogni istrumento (di cui sia fissato il modo d'impiego) corrisponde un *corpo di problemi* con esso *risolubili*, il valore dell'istrumento può venire apprezzato in rapporto all'estensione di questo corpo.

Se due istrumenti, o gruppi d'istrumenti, corrispondono al medesime corpo, essi sono da riguardarsi come *equivalenti*; così è per es., relativamente alle costruzioni determinate, del compasso e della riga a due orli ecc. (art. XIV, XV, XVI).

Allorchè invece il corpo dei problemi risolubili mediante un certo istrumento A, contiene quello dei problemi risolubili mediante un altro istrumento B, l'istrumento A ha un *valore maggiore* di B. Così per es. il compasso ha un valore maggiore della riga graduata presa come trasportatore dei segmenti (art. XVI), e questa ha alla sua volta un valore maggiore della squadra adoprata soltanto come mezzo di trasporto di un angolo retto (cfr. art. XV).

Così ancora l'integrafo (art. XXII) — aggiunto alla riga — permette di risolvere tutti i problemi risolubili col compasso, coi compassi conici, col trisettore degli angoli, cogl'istrumenti generatori della cissoide ecc. Infatti i problemi di grado n potendosi far dipendere dalle intersezioni di rette e parabole d'ordine n, la loro risoluzione richiede di applicare successivamente $n-1$ volte l'istrumento integratore.

Ma due istrumenti possono anche avere un *valore diverso* e *non comparabile*; questo avviene se i corpi di problemi corrispondenti non sono contenuti l'uno nell'altro, sia che essi abbiano comune un sotto-corpo, sia che non esista alcun problema comune ai due corpi. Un esempio in proposito si avrebbe confrontando (in base ai criterii dell'art. XVI) ciò che dà il compasso, e ciò che permette di ottenere un trisettore d'angoli preso unitamente alla riga.

§ 9. **Esattezza delle costruzioni.** — La semplicità delle costruzioni, e l'ampiezza del corpo dei problemi risolubili con un dato istrumento, non sono i soli criterii che debbano tenersi in vista nel giudicare della *utilità* di esso. Devesi tener conto per ciò anche dell'*esattezza* delle costruzioni medesime.

Sotto questo riguardo è ad es. pregevole la Geometria del compasso di MASCHERONI (art. XIV).

La questione dell'esattezza suggerisce alcune riflessioni: *Teoricamente si parla di costruzioni esatte e di costruzioni approssimate; praticamente tutte le costruzioni hanno soltanto un valore approssimato.*

Come si può valutare il *grado di esattezza* o l'approssimazione raggiunta da una costruzione teoricamente precisa?

È questo un problema che entra nell'ordine di vedute svolte dal KLEIN nella sua Vorlesung « Anwendung der Differential und Integralrechnung auf der Geometrie » (Lipsia, 1902).

Si può dargli una risposta matematica, quando si trasformino sistematicamente gli enunciati delle proposizioni goometriche, che si traducono analiticamente con *uguaglianze*, sostituendo a queste uguaglianze delle *disuguaglianze*. Così per es. il teorema « gli angoli alla base d'un triangolo isoscele sono uguali » si tradurrà in un teorema della forma seguente « se due lati a, b di un triangolo differiscono per meno di ε, gli angoli opposti α, β differiscono per meno di τ, ove τ è una funzione di ε (facilmente assegnabile) che diviene infinitesima con ε » (1). Allora quando in una costruzione si applichi un toorema, come quello enunciato innanzi, si dovrà anzitutto assumere che i dati teoricamente uguali, sieno uguali solo sensibilmente, e differiscono fra loro per una quantità ε dipendeute immediatamente dall'istrumento adoperato, e poi valutare in conseguenza il grado d'esattezza, τ, con cui gli elementi costruiti soddisfano alle condizioni proposte. Quando τ è dello stesso ordine di ε, non apprezzabile rispetto ai nostri istrumenti ed ai sensi, la risoluzione del problema è praticamente esatta.

Pertanto lo stesso grado pratico di esattezza può venire raggiunto anche dalla risoluzione di un problema più semplice di quello proposto, che sia *prossimo* ad esso. Appare quindi conforme al criterio di economia di preferire in questi casi la soluzione teoricamente approssimata del problema a quella esatta.

Però non bisogna disconoscere il vantaggio delle soluzioni teoricamente esatte, poichè in esse, a differenza che nelle approssimate, non s'introduce alcuna causa d'*errore sistematico*, la cui ripetizione tenda a rendersi sempre più sensibile in un gran numero di casi.

Nonostante questo si può ben dire che nella maggior parte dei casi dobbiamo o ci conviene di contentarci della ricerca di soluzioni approssimate. Ma a proposito di queste il KLEIN distingue opportunamente l'approssimazione che trascura un errore dato a priori e l'*approssimazione sistematica* nella quale, pur di compiere un numero d'operazioni sufficientemente grande, si ottiene un grado di precisione grande quanto occorre.

(1) Precisamente è in valore assoluto $\operatorname{sen}\beta - \operatorname{sen}\alpha = \dfrac{\varepsilon \operatorname{sen}\alpha}{a}$.

Tutto il procedimento della misura, in base al quale si risolvono i problemi per via analitica, è in sostanza un metodo di approssimazione sistematica applicato su larga scala; con espedienti particolari si ottengono poi vantaggiose costruzioni dei segmenti (o di altri elementi) di cui sia data la misura (cfr. per es. art. XVIII). Di costruzioni approssimate a meno di un errore dato si sono visti notevoli esempii negli art. XIV, XVIII, XIX.

§ 10. **Metodi di risoluzione.** — A proposito della classificazione dei problemi abbiamo già accennato al diverso aspetto sotto cui si presentano i problemi risoluti e i problemi da risolvere. Ora quando si considerano più da vicino i problemi, come domanda a cui non sia ancor data una risposta, assume fondamentale importanza la veduta del *metodo di risoluzione.*

Il principio d'economia interviene qui come criterio comparativo dei metodi, in quanto essi ci permettono di raggiungere più *facilmente* (cioè col minimo sforzo di pensiero) la risoluzione dei problemi proposti.

Ora quali metodi dovranno ritenersi più economici?

Se si guarda alla *preparazione scientifica* richiesta nel ricercatore, un metodo dovrebbe dirsi tanto più economico quanto più *elementare.* Ma i metodi più elementari, largamente accessibili a chi possegga uno scarso numero di cognizioni, non porgono nei varii casi criterii direttivi d'ordine generale, onde l'applicazione loro esige ogni volta un piccolo sforzo di genio.

La risoluzione per vie elementari riesce dunque la più economica soltanto per riguardo al caso singolo; *rispetto all'insieme* vale la pena di affrontare la fatica di una maggiore preparazione scientifica per ottenere qualche guida d'ordine generale e non incontrare ad ogni passo una nuova difficoltà.

Il progresso della scienza rappresenta appunto un perfezionamento dei metodi nel senso economico, quando si guardi ai problemi da risolvere nel loro insieme; così come la macchina da tessere rappresenta un'economia per l'industria che deve fabbricare una grande quantità di stoffe.

§ 11. **Evoluzione dei metodi.** — È interessante di notare come i metodi più elevati che la Geometria moderna usa nella trattazione dei problemi, sieno sorti dallo sviluppo degli elementari, sotto la spinta dell'esigenza economica.

Consideriamo il metodo dei luoghi che si presenta primo a risolvere numerosi problemi. La Geometria elementare lo usa entro i limiti ristretti segnati dalla conoscenza di poche linee particolari. Se ci s'impone di non uscire dalla considerazione della retta e del circolo, si è arrestati nell'applicazione del metodo, appenachè una delle condizioni del problema porti come luogo una conica.

La necessità di allargare questi confini si presentò già agli antichi; ma l'estensione veramente generale fu compiuta da DESCARTES, allorchè la rappresentazione analitica delle curve permise di riguardare, in un certo senso, come trattabile, ogni curva di cui sia scritta l'equazione. Il metodo analitico, sorto per questa via, offre un punto di vista sistematico per la risoluzione dei problemi e realizza quindi la *maggior economia nell' insieme.*

Vero è che esso non riesce altrettanto luminoso in ogni singolo caso, e non conduce sempre alla risoluzione più rapida e semplice. Vero è ancora che esso non scioglie pienamente la difficoltà quando si oltrepassino quei tipi di equazioni, la cui risoluzione si effettua con istrumenti dei quali si è bene analizzato l'uso. Ma questo difetto è compensato (come già accennammo) dalla circostanza che le radici di un'equazione possono almeno costruirsi in modo approssimato, avvicinandosi ad esse quanto si vuole; ed i teoremi dell'analisi sugli sviluppi in serie di potenze, o in frazioni continue, servono meravigliosamente allo scopo.

Il secondo metodo generale per la risoluzione dei problemi si appoggia al concetto della trasformazione. E nell'art. XIII si è già mostrato come questo concetto sia suscettibile di utili applicazioni anche nel campo più ristretto della Geometria elementare.

Ma proseguendo la ricerca dei vantaggi per cui le trasformazioni sono poste in opera, si viene naturalmente ad allargarne il campo: ad ogni gruppo di proprietà delle figure corrisponde un gruppo di trasformazioni che le lascia invariate e viceversa. Così le proiettività, le trasformazioni per

raggi vettori reciproci, le trasformazioni cremoniane ecc. divengono successivamente oggetto di studio, e danno origine allo sviluppo sistematico della Geometria sotto un particolare punto di vista (1).

L'apprezzamento di questi sviluppi ci condurrebbe troppo lontano dallo scopo segnato a questo articolo. Ci limiteremo pertanto a poche considerazioni intorno al valore delle trasformazioni rispetto alla risoluzione dei problemi costruttivi, tenendoci generalmente vicini agli oggetti di studio della Geometria elementare.

§ 12. **Metodi di trasformazione: vantaggi di posizione.** — Come si vede nell'art. XIII, il primo uso della trasformazione risponde allo scopo di *portare la figura* su cui si opera, o alcune parti di essa, *in una posizione più opportuna*. Un tale scopo può venire raggiunto sia con un movimento del piano, sia con una trasformazione la quale alteri qualcuno degli elementi della figura, ma lasci invariato ciò che è essenziale per la costruzione.

Notiamo in modo speciale due applicazioni di questo principio:

1) *La riduzione delle costruzioni entro i limiti di un foglio assegnato,* la quale si può effettuare vantaggiosamente secondo i casi, coll'omotetia, coll'omologia, ed anche coll'inversione rispetto ad un circolo.

L'omotetia presenta il vantaggio di conservare gli angoli e i rapporti segmentarii, ed in particolare quindi di sostituire un cerchio ad un cerchio; ma essa non ci porta a distanza finita gli elementi all'infinito e non riesce quindi a ridurre nei limiti prefissati tutte le costruzioni lineari, segnatamente quelle ove si tratta di parallele. Si ricorre per ciò utilmente ad un'omologia generale. La riduzione delle costruzioni lineari entro i limiti del foglio, ottenuta nell'art. XV, si fonda in sostanza sopra una trasformazione omologica.

2) *La sostituzione di una linea ad un'altra nel problema d'intersezione,* è ancora una brillante applicazione delle trasformazioni, riguardate sotto l'aspetto che stiamo considerando.

(1) Cfr. il *Programma di Erlangen* di F. KLEIN, trad it. di G. FANO, *Annali di Matematica*, serie II, vol. XVII, 1889.

Un semplice esempio si è visto nell'art. XV, dove si è adoperata l'omotetia per trasformare un cerchio qualsiasi (individuato ma non descritto) in un cerchio fondamentale tracciato, deducendone la possibilità di sostituire in generale l'uso del compasso con quello di un cerchio fisso (si suppone data la riga).

Più in generale un'omografia ci permette di ridurre la ricerca delle intersezioni di una conica con una retta a quella delle intersezioni di un'altra conica arbitrariamente fissata, ciò che costituisce anche più di un semplice vantaggio di posizione, potendosi trasformare la conica data in una conica particolare, per es. in un cerchio. E basta a tale scopo una trasformazione omologica; mediante la quale si apprende dunque a risolvere col compasso il problema d'intersecare una conica qualsiasi, individuata ma non tracciata, con una retta [1] (cfr. n. 13).

Un altro esempio notevole concerne la possibilità di *determinare linearmente le intersezioni di una conica o di un cerchio* k *con una retta, quando di* k *sia tracciato un arco, comunque piccolo.*

Basta per ciò assegnare una trasformazione omografica di k in sè stessa, per modo che un suo arco contenente i punti incogniti (arco determinabile linearmente) si muti nell'arco dato [2].

§ 13. **Riduzione a casi particolari.** — Dalle considerazioni che precedono scaturisce già un uso ulteriore delle trasformazioni.

Oltre ai vantaggi di posizione, esse ci permettono anche di raggiungerne altri, particolarizzando e semplificando le figure in modi diversi. Sebbene applicazioni siffatte si presentino fino nei casi più elementari (art. XIII), un'enorme estensione di quest'ordine d'idee viene ottenuta coll'uscire dal campo delle similitudini.

[1] Una risoluzione elementare del problema si è vista nell'art. XIX.

[2] Cfr. p. es. F. Severi, *Sui problemi determinati risolubili colla riga e col compasso.* Circolo Matematico di Palermo, 1904. Sussiste anche un teorema analogo per la determinazione delle intersezioni di una conica con rette e cerchi; esso fu enunciato da Descartes e dimostrato da Smith, *Mémoire sur quelques problèmes cubiques et biquadratiques.* « Annali di Matematica », t. 3, 1869, (pag. 112-218).

Le trasformazioni più semplici, che nascono dalla estensione delle elementari, sono in generale quelle che si ottengono con *proiezioni* ripetute del piano (PONCELET).

Queste trasformazioni proiettive possono effettuarsi entro un piano dato, senza uscirne, stante la proprietà di conservare le rette, che le caratterizza, e per la quale esse prendono il nome di *omografie* (MÖBIUS).

Quando sono dati tre punti ABC sopra una retta, la costruzione del punto (*quarto armonico*) D per cui

$$\frac{AD}{BD} = -\frac{AC}{BC},$$

non riesce subito visibile. Una proiezione ce la rende manifesta quando si abbia presente l'invarianza proiettiva del birapporto, dalla quale si deduce appunto la nota proprietà del quadrangolo (art. XV, § 5).

La convenienza di sostituire le proiezioni colle costruzioni dell'omografia, entro il piano, si presenta quando devesi operare sulla figura in relazione alla sua trasformata. Così appunto abbiamo già accennato come il problema d'intersecare una conica con una retta si riconduca alla determinazione delle intersezioni di una retta e d'un cerchio, mediante un'omografia che può supporsi omologica.

Affinchè una conica C si trasformi omograficamente in un cerchio, basta infatti prendere come retta limite (a cui corrisponda la retta all'infinito) una retta a esterna a C, e fare in modo che l'involuzione dei punti coniugati subordinata su a da C si muti nell'involuzione assoluta; ciò si effettua per es. con un'omologia, il cui centro sia comune ai cerchi che hanno per diametri i segmenti compresi fra i punti coniugati dell'involuzione.

Ora appare che la trasformazione indicata permette ancora di ridurre la ricerca delle intersezioni di due coniche, a quella delle intersezioni di una conica (che a volontà può supporsi ellisse, iperbole o parabola) con un cerchio. Si può anche ottenere un resultato più espressivo. Si abbiano due coniche C_1, C_2, definite ma non tracciate; e si abbia d'altra parte una parabola K_1 completamente tracciata. Si può determinare una retta p tangente alla conica C_1, che sia esterna

a C_2; allora si può porre nel piano un'omografia la quale abbia per retta limite p, e muti la conica C_1 in K_1, e l'involuzione dei punti coniugati rispetto a C_2 — data su p — nella involuzione assoluta; quindi la trasformata di C_2 in questa omografia sarà un cerchio K_2. In questo modo il problema di determinare le intersezioni di C_1 e C_2 si riduce a quello d'intersecare la parabola K_1 (fissata a priori) con un cerchio K_2.

Risulta dunque qui che i *problemi* (di 4° grado o riducibili a successivi problemi di 4° grado) *risolubili mediante coniche, si possono risolvere col compasso ed una parabola fissa* (1).

Questo resultato equivale d'altronde a quello stabilito, per altra via, nell'art. XIX, giacchè i problemi di 4° grado si riducono a problemi di 2° e 3° grado in virtù della nota risoluzione dell'equazione di 4° grado.

Fra le omografie notevoli citeremo le *affinità* (di MÖBIUS), cioè le omografie che lasciano ferma la retta all'infinito, le quali si applicano con vantaggio ai problemi ove è questione di *aree*, stante la loro proprietà caratteristica di mutare le aree in un rapporto costante (2).

Si tratti per es. di « iscrivere in un'ellisse un parallelogramma di area data, del quale può anche essere assegnato un vertice ». Il problema si lascia ridurre a quello di « iscrivere in un cerchio un rettangolo di area data », mercè una trasformazione omografica affine dell'ellisse nel cerchio, la quale viene data semplicemente da un'omologia col centro all'infinito. L'ultimo problema si risolve facilmente, dipendendo dalle equazioni

$$xy = a^2, \quad x^2 + y^2 = 4r^2$$

(ove a^2 è l'area data, r il raggio del cerchio); si trova quindi

$$x + y = \pm 2\sqrt{r^2 + \frac{a^2}{2}}$$

$$x - y = \pm 2\sqrt{r^2 - \frac{a^2}{2}},$$

dove x e y sono i lati del rettangolo che deve essere costruito.

(1) Pel teorema di DESCARTES-SMITH enunciato innanzi, basta dare un arco della parabola.

(2) Cfr. per es. ENRIQUES, *Lezioni di Geometria proiettiva*, § 50.

§ 14. **Equivalenza di mezzi costruttivi.** — Le trasformazioni non porgono solo un aiuto per la risoluzione effettiva di problemi proposti, ma illuminano anche la questione della risolubilità dei problemi stessi, mediante istrumenti assegnati.

Si abbia un istrumento a, il quale permetta di effettuare certe costruzioni fondamentali $A_1 A_2 \ldots$; queste definiranno un corpo (A) di problemi, risolubili per mezzo di a (cfr. § 8).

Si effettui ora una trasformazione, la quale muti $A_1 A_2 \ldots$ in certe nuove costruzioni $A_1' A_2' \ldots$. Il valore di un istrumento a', capace di effettuare le operazioni fondamentali $A_1' A_2' \ldots$, si potrà senz'altro misurare, in base alla supposta conoscenza del valore di a; infatti il corpo dei problemi risolubili con a', sarà il corpo (A') trasformato di (A).

In particolare *se il corpo* (A') *contiene le operazioni* $A_1 A_2 \ldots$, esso conterrà l'intiero corpo (A), e perciò *l'istrumento* a' *sarà capace di surrogare* a.

Si perviene appunto a questa conclusione, *quando l'istrumento* a' *permette di effettuare la trasformazione indicata*, poichè allora esso c'insegna a ridurre le costruzioni $A_1 A_2 \ldots$, alle $A_1' A_2' \ldots$. La trasformazione porge così un criterio per giudicare dell'*equivalenza di dati mezzi costruttivi*.

Un semplice esempio in proposito si è visto nell'art. XIV; poichè una trasformazione per raggi vettori reciproci è effettuabile col solo compasso, e poichè essa trasforma la figura costituita da un cerchio e dalle rette d'un piano in un insieme di cerchi, si deduce che il compasso è capace da solo di effettuare quelle costruzioni che si ottengono colla riga e con un cerchio fisso, cioè (secondo il risultato di PONCELET-STEINER, art. XV) tutte quelle effettuabili colla riga e col compasso.

Similmente la figura costituita da una parabola fissa e dai cerchi del piano pel suo vertice, si trasforma — con un'inversione — in quella costituita da una cubica razionale e dalle rette; e, poichè la trasformazione si può eseguire colla sola riga, dati gli enti metrici del piano (per es. mediante un quadrato), si conclude che i problemi di 3° grado, i quali sono risolubili mediante le intersezioni di una parabola coi cerchi pel suo vertice, possono anche risolversi colla sola riga, quando è data nel piano una cubica razionale fissa ed un quadrato, oppure una cissoide ed il centro del suo cerchio

generatore, potendosi in tal caso costruire un quadrato (cfr. art. XIX, § 19).

Un altro esempio istruttivo, di un genere un pò diverso, è il seguente.

Si consideri, nel piano, la polarità rispetto ad un cerchio, la quale porge una trasformazione di punti in rette e di rette in punti. Mediante questa polarità, che si costruisce linearmente, l'operazione del « segare il cerchio con una retta » si trasforma in quella di « condurre per un punto le tangenti al cerchio ». E poichè la prima operazione, insieme a quelle di « segnare un punto » e « tracciare una retta » vale a risolvere tutti i problemi di 2° grado, ed in particolare quello di condurre per un punto le tangenti ad un cerchio, se ne dedurrà che gli stessi problemi sono risolubili colla seconda operazione, la quale può essere effettuata con una riga a due orli (1). Questo resultato è stato stabilito in altro modo nell'ast. XV.

§ 15. **Risoluzione di problemi mediante gli elementi uniti d'una corrispondenza.** — Le trasformazioni o corrispondenze fra i punti di un piano o di una retta, trovano anche una particolare applicazione nella risoluzione di problemi, ove i punti incogniti si presentano come *punti uniti di una corrispondenza.*

Il più semplice esempio di ciò è stato offerto nell'art. XV sotto il nome di *metodo dei tentativi.* Nei problemi ivi considerati, i punti incogniti si presentavano come uniti per una proiettività sopra la retta, la quale veniva individuata da tre tentativi non riusciti.

In generale quando dei punti incogniti (sopra una retta o nel piano) si presentano come uniti per una corrispondenza, della quale sia nota la costruzione, si ha almeno il modo di avvicinarsi alle soluzioni per via di approssimazioni successive, ripetendo la costruzione della corrispondenza stessa (2).

(1) Cfr. ENRIQUES, *Lezioni di Geometria proiettiva*, § 74.

La possibilità di eseguire praticamente l'operazione con una *riga a due orli di lunghezza finita* discende da ciò che si è detto nel § 12. (Cfr. SEVERI, l. c.).

(2) Da questo procedimento di approssimazione, pei punti uniti di una proiettività sulla retta, scaturisce il noto sviluppo di un irrazionale

Ecco ora un esempio di applicazione del metodo, ove interviene una corrispondenza superiore alla proiettività.

Si tratti di inserire fra due rette date a, b un segmento di lunghezza data, il cui prolungamento debba passare per un punto O (art. XIX).

I tentativi di risolvere il problema, con riga e compasso, conducono come è manifesto ad una corrispondenza [2, 2] in cui ad ogni punto di a ne corrispondono due di b e viceversa. Proiettando da O la retta b sulla a, si ottiene su questa una corrispondenza [2, 2], che ha 4 punti uniti, i quali risolvono il problema.

Faremo un'altra applicazione del metodo stesso alla costruzione delle radici di un'equazione cubica

$$f_3(x) = 0,$$

costruzione di cui già si è trattato nell'art. XIX.

Una semplice costruzione geometrica del GRASSMANN (generalizzazione della teoria dei quarti armonici [1]) permette di riguardare i tre punti di una retta che hanno per ascisse le radici suddette, come punti uniti di una corrispondenza [1, 2] (*polarità* rispetto alla terna), la quale scaturisce dal riferire proiettivamente i punti della retta alle *coppie* di un'involuzione I (o ai raggi d'un fascio che sono tangenti, in un punto base, ai cerchi, per due punti fissi, seganti sulla retta le coppie dell'involuzione).

Ora, se si proietta la suddetta corrispondenza sopra una conica (per es. su un cerchio) C, scegliendo il centro di proiezione O sulla curva, l'involuzione verrà segata su C dalle rette di un fascio P, che risulterà proiettivo ad O. I due fasci

quadratico in frazione continua periodica. L'analogo procedimento relativo ai punti uniti di un'omografia piana, corrisponde alla generalizzazione del suddetto algoritmo per gl'irrazionali cubici ecc. (JACOBI, MINKOWSKI).

Poichè n punti della retta rappresentati da un'equazione di grado n, possono riguardarsi come uniti per una corrispondenza $[1, n-1]$, si potrà ottenere una rappresentazione dell'irrazionale di grado n, mercè un procedimento iterativo continuo consistente nella ripetizione di un'operazione razionale di grado $n-1$.

[1] Cfr. CREMONA, *Introduzione ad una teorica geometrica delle curve piane*. Bologna, Gamberini e Parmeggiani, 1862.

proiettivi O e P genereranno una *conica le cui intersezioni col cerchio* C *forniscono le soluzioni dell'equazione cubica data.*

Si supponga invece data, nel piano una cubica C dotata di un punto doppio O. Le tangenti in O a C segheranno la nostra retta in due punti AB. Possiamo operare sulla retta una trasformazione proiettiva in guisa che l'involuzione (trasformata di I) venga a contenere la coppia AB, e che il punto P, corrispondente alla coppia nella corrispondenza data, occupi una posizione arbitraria che ci riserviamo d'indicare.

Ora, si proietti da O sulla cubica C la retta AB; le proiezioni delle coppie di I formeranno su C un'involuzione I', e si dimostra facilmente che le coppie di I' trovansi allineate con un punto fisso P' della cubica. Possiamo ritenere che il punto P' sia la proiezione di P. Allora la corrispondenza [1, 2] data sulla nostra retta, si traduce in una prospettività tra i fasci di raggi O e P'. L'asse di prospettività incontra la curva nei punti uniti.

Si ottiene così una nuova dimostrazione della possibilità di *costruire le radici di un'equazione del 3° grado, mediante le intersezioni di una cubica razionale fissa con una retta* (cfr. art. XIX, § 19).

§ 16. **Conclusione.** — Noi abbiamo messo in luce, sotto molteplici aspetti, i progressi portati dall'Algebra e dalla Geometria moderna, ed abbiamo riconosciuto l'economia che ne risulta nelle costruzioni e nei metodi di risoluzione, per riguardo ai problemi stessi considerati nel loro insieme.

In particolare abbiamo imparato a classificare i problemi, decidendo della loro risolubilità con istrumenti assegnati; si eliminano così i vani tentativi volti a raggiungere uno scopo impossibile, in ordine ai mezzi di cui si dispone.

Ora se i concetti della Scienza moderna ci appaiono più generali e potenti degli antichi, e se perciò siamo tratti a farne valere la superiorità, dobbiamo pure tener presente che essi ci presentano a prima vista come più astratti e quindi più lontani dalla forma immediata in cui sono posti d'ordinario i problemi pratici. Per cogliere in quell'astrattezza il contenuto concreto, ottima via è di rifare la strada che la

mente umana ha percorso per giungervi, ripigliando dunque i metodi ed i principii elementari dei Greci.

Pertanto noi non vogliamo mettere da banda nulla di ciò che i geometri antichi ci hanno insegnato; e domandiamo soltanto ad una più larga ed alta coltura scientifica, di renderci chiari i rapporti di quella Geometria elementare, i cui mirabili particolari meglio rispondono al lume dei generali concetti moderni!