Alma Mater Studiorum · Università di Bologna

facoltà di scienze matematiche, fisiche e naturali
Corso di Laurea Triennale in Matematica

IL TEOREMA DI WEDDERBURN E LO STUDIO DELL'IRRAZIONALITÀ DI CERTI NUMERI

Relatore:
Chiar.mo Prof.
SALVATORE COEN

Presentata da:
ALICE BOLOGNESI

II Sessione
Anno Accademico 2011-2012

Indice

Introduzione

La tesi si propone di studiare alcune proprietà algebriche di interesse generale dandone delle dimostrazioni abbastanza elementari. Con questo intendiamo che le dimostrazioni possono essere facilmente intese da studenti, anche del primo anno universitario, che abbiano seguito un primo corso di Algebra e di Analisi Matematica.

L'elaborato è nettamente distinto in due parti. Nella prima affrontiamo il (piccolo) teorema di Wedderburn, quello che afferma che ogni corpo finito è campo (cioè ha moltiplicazione commutativa). Questo teorema ha avuto svariate dimostrazioni a partire dal 1905 (lo stesso Wedderburn ne ha pubblicate tre). Il teorema ha applicazioni in questioni di geometria desarguesiana, sulle quali però noi non entriamo.

La seconda parte della tesi tratta di problemi di irrazionalità. Precisamente riprendiamo alcuni risultati essenzialmente ottenuti nel diciannovesimo secolo sull'irrazionalità di alcune costanti fondamentali, quali la costante di Eulero, il numero π (la prima dimostrazione del quale però avvenne nel 1768), certe loro potenze e certi valori della funzione arcocoseno reale. Questo risultati hanno varie applicazioni, per esempio gli ultimi citati si sono dimostrati assai utili nella dimostrazione del teorema di Dehn, dovuta a Robin Hartshorne. Anche in questo caso le dimostrazioni sono classiche, ma sono scelte tra quelle più elementari, a nostro avviso accessibili a studenti all'inizio dei loro corsi di Analisi Matematica o Algebra.

La tesi è completata dal testo della dimostrazione al teorema di Wedderburn che egli stesso propose nel 1905 e di quella sull'irrazionalià di π di Niven nel 1947.

Capitolo 1

Il teorema di Wedderburn

In questo capitolo dimostreremo che se R è un corpo finito, allora la moltiplicazione su di esso è commutativa.
Cominciamo dando due definizioni fondamentali per la comprensione del teorema:

Definizione: Sia R un anello. Se R ha un elemento neutro 1 per la moltiplicazione ed ogni suo elemento diverso da 0 ha inverso moltiplicativo, allora R è chiamato *corpo*.

Definizione: Sia R un corpo. Se in R l'operazione di moltiplicazione è commutativa, allora R si dice *campo*.

Il seguente teorema venne dimostrato per la prima volta nel 1905 ad opera di MacLagan Wedderburn. In realtà Leonard E. Dickson dimostrò il teorema nello stesso anno, ma a fugare i dubbi sui problemi di attribuzione lo stesso Dickson scrisse: "For this proof I am indebted to Mr. J. H. MacLagan Wedderburn" [1]. (Vedere appendice a fine capitolo.)
Alla fine del capitolo possiamo osservare la dimostrazione che diede Wedderburn

[1] *On finite algebras*, Nachrichten der Akad. Wissenschaften Gottingen Math. - Phis. Klasse.

del teorema in questione.

Teorema: Ogni corpo finito R è commutativo.

Dimostrazione:

I parte: **Cardinalità n_s dei centralizzatori B_s di R**
Consideriamo un elemento arbitrario $s \in R$ e definiamo $B_s = \{x \in R : xs = sx\}$. B_s è l'insieme degli elementi che commutano con s e viene chiamato *centralizzatore* di s.
B_s contiene 0 e 1. Inoltre è sottocorpo di R; infatti $\forall x, y \in B_s$ abbiamo che:

- $xy \in B_s$, infatti $xys = x(ys) = x(sy) = (xs)y = sxy$;
- $x^{-1} \in B_s$, infatti $xs = sx \Rightarrow s = x^{-1}sx \Rightarrow sx^{-1} = x^{-1}s$.

Prendiamo in considerazione il centro, cioè l'insieme degli elementi che commutano con tutti gli elementi di R; chiamiamo questo insieme C. Notiamo che C è l'intersezione degli insiemi B_s $\forall s \in R$. In particolare:

- tutti gli elementi di C commutano;
- $0, 1 \in C$.

Quindi possiamo affermare che C è un campo finito.
Indichiamo ora con $|C|$ il numero di elementi q di cui è composto C. Per questo, se pensiamo R e B_s come spazi vettoriali sul campo C, essi saranno rispettivamente isomorfi ai campi C^n e C^{n_s} con n, n_s le dimensione dei rispettivi spazi vettoriali su C.
In generale, se consideriamo spazi vettoriali su un campo di dimensione finita, allora il numero degli elementi dei suddetti spazi è una potenza della dimensione

del campo.
Quindi utilizzando la notazione precedente otteniamo che $|R| = q^n$ e allo stesso modo $|B_s| = q^{n_s}$ per opportuni interi $n_s \geq 1$.

II parte: **La relazione di equivalenza $\sim$**

Supponiamo ora per assurdo che R non sia un campo, cioè che non sia un anello commutativo. Possiamo tradurre questa affermazione dicendo che esistono alcuni $s \in R$ per cui B_s non coincide con R.
Definiamo ora la relazione $\sim$ sull'insieme $R^* = R \setminus \{0\}$ tale che

$$a' \sim a \iff a' = x^{-1}ax \text{ per alcuni } x \in R^*.$$

Per questa relazione valgono le proprietà:

- riflessiva: infatti vale $a \sim a$;
- simmetrica: infatti se $a \sim a'$ abbiamo che $a' = x^{-1}ax$, e quindi $a = xa'x^{-1}$, che implica che $a' \sim a$;
- transitiva: infatti $a \sim b \iff b = x^{-1}ax$, $b \sim c \iff c = y^{-1}by$ quindi otteniamo che $c = y^{-1}by = y^{-1}x^{-1}axy = (xy)^{-1}axy$ e siccome $xy \in R^*$ allora $a \sim c$.

Possiamo perciò affermare che $\sim$ è una relazione di equivalenza.
Sia ora $A_s = \{x^{-1}sx : x \in R^*\}$ la classe di equivalenza contenente s.
Osserviamo che se $s \in C$ allora $|A_s| = 1$, cioè $A_s = \{s\}$, e questo si verifica solo in questo caso; infatti in C gli elementi commutano tutti tra loro, e per questo abbiamo che $x = x^{-1}sx$.
Deduciamo che esistono classi A_s con $|A_s| \geq 2$.

III parte: **Calcolo del numero di elementi delle classi di equivalenza**

Ora consideriamo per $s \in R^*$ l'applicazione:

$$f_s : R^* \longrightarrow A_s$$

$$x \longmapsto x^{-1}sx$$

Osserviamo che vale:

$$x^{-1}sx = y^{-1}sy \Leftrightarrow (yx^{-1})s = s(yx^{-1}) \Leftrightarrow yx^{-1} \in B_s^* \Leftrightarrow y \in B_s^*x$$

con $B_s^* = B_s \setminus \{0\}$, dove $B_s^*x = \{zx : z \in B_s^*\}$ ha la stessa dimensione di B_s^*; infatti se $zx = z'x$ allora $z = z'$ con z, z' elementi di B_s^* e per questo l'affermazione precedente è vera.
Dunque ogni elemento $x^{-1}sx$ è l'immagine precisamente di $|B_s^*| = q^{n_s} - 1$ elementi in $|R^*|$ secondo la mappa f_s. Da questo fatto deduciamo che $|R^*| = |A_s||B_s^*|$. Infatti, per ottenere il numeri di elementi di R^*, si deve moltiplicare il numero di elementi contenuti in B_s^* per la quantità di elementi contenuti in ogni classe di equivalenza A_s^* attribuita all'elemento s. In particolare notiamo che

$$\frac{|R^*|}{|B_s^*|} = \frac{q^n - 1}{q^{n_s} - 1} = |A_s|.$$

Abbiamo scritto che $|R^*| = q^n - 1$ perchè il numero di elementi di R è q^n e in R^* tolgo da R l'elemento zero.
Siccome $|A_s|$ è un intero per ogni s, allora lo sarà anche $\frac{q^n-1}{q^{n_s}-1}$.

IV parte: **Gli n_s dividono n**

Sappiamo che le classi di equivalenza individuano una partizione su R^*. Raggruppiamo quindi le classi di equivalenza a seconda del loro numero di elementi: troviamo quindi gli elementi centrali C^* (classi di equivalenza con un solo elemento) e denotiamo con $A_1, ..., A_t$ le classi di equivalenza contenenti più di un

elemento. Dalla nostra supposizione precedente sappiamo che $t \geq 1$.
Dalla partizione di R^* in classi di equivalenza deduciamo che $|R^*| = |C^*| + \sum_{k=1}^{t} |A_k|$. Per questo otteniamo la seguente formula

$$q^n - 1 = q - 1 + \sum_{k=1}^{t} \frac{q^n - 1}{q^{n_k} - 1} \tag{1.1}$$

dove abbiamo che $1 < \frac{q^n-1}{q^{n_k}-1} \in \mathbb{N}\ \forall k$.

Dimostriamo ora la seguente affermazione, che ci sarà utile per concludere la dimostrazione del teorema: $(q^{n_k} - 1) \,|\, (q^n - 1)$ implica che $n_k \,|\, n$.
Infatti:
scriviamo $n = an_k + r$ con $0 \leq r < n_k$, quindi $(q^{n_k} - 1) \,|\, (q^{an_k+r} - 1)$ implica

$$(q^{n_k} - 1) \,|\, [(q^{an_k+r} - 1) - (q^{n_k} - 1)] = q^{n_k}(q^{(a-1)n_k+r} - 1)$$

e pertanto $(q^{n_k} - 1) \,|\, [q^{(a-1)n_k+r} - 1]$, poichè q^{n_k} e $q^{n_k} - 1$ sono primi fra loro. Continuando in questo modo troviamo che $(q^{n_k} - 1) | \, (q^r - 1)$ con $0 \leq r < n_k$, che è possibile solo per $r = 0$ [2], ovvero $n = an_k$, ovvero $n_k \,|\, n$.
Come si voleva, abbiamo dimostrato che

$$n_k \,|\, n\ \forall k. \tag{1.2}$$

V parte: **La nozione di ordine di radici n-esime dell'unità**

Entriamo ora nel campo dei numeri complessi $\mathbb{C}$ e consideriamo il polinomio $x^n - 1$. Come ben noto, le radici di questo polinomio sono chiamate *radici n-esime dell'unità*.

[2] Infatti r deve essere minore di n_k. Per $r = 0$ abbiamo che $(q^{n_k} - 1) \,|\, 0$, il che è vero.

Denotiamo con λ le radici. Siccome $\lambda^n = 1$ possiamo affermare che $|\lambda| = 1$ e che quindi ogni radice giace sul cerchio unitario nel piano complesso.
Abbiamo che

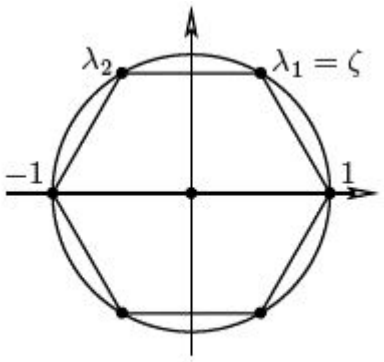
$$1^{\frac{1}{n}} = e^{\frac{1}{n}ln1} = \{e^{\frac{1}{n}2k\pi i} | k \in \mathbb{Z}\} = \{\lambda_0, ..., \lambda_{n-1}\}.$$

Le radici risultano essere esattamente n perchè la radice i-esima coincide con quella (i+n)-esima.
Le n-esime radici λ_k possono essere rappresentate nel seguente modo:

$$\lambda_k = e^{\frac{2k\pi i}{n}} = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} \,\text{con}\, 0 \leq k \leq n-1,$$

Così per ogni k

$$\lambda_k^n = (e^{\frac{2k\pi i}{n}})^{\frac{1}{n}} = e^{2k\pi i} = \cos(2k\pi) + i\sin(2k\pi) = 1.$$



Le radici dell'unità per $n = 6$

Osserviamo che esistono radici il cui ordine non è n, bensì può essere un numero minore. Infatti alcune λ soddisfano l'equazione $\lambda^d = 1$ per $d < n$; per esempio,

nel caso in cui la radice sia $\lambda = 1$ possiamo considerare $d = 2$ ($\lambda^2 = 1$).
Questo discorso è generalizzato considerando n non primo: le radici λ_k hanno ordine minore di n se k è pari nel caso n sia pari, se k è dispari nel caso che n sia dispari. [3]
Per una radice λ fissata, sia d il più piccolo esponente positivo con $\lambda^d = 1$, ovvero d è l'*ordine* di λ nel gruppo delle radici dell'unità.
Ricordiamo il Teorema di Lagrange; esso afferma che l'ordine di ogni elemento di un gruppo divide l'ordine del gruppo stesso. Così diciamo che $d \,|\, n$.
Notiamo comunque che ci sono radici di ordine n, come $\lambda_1 = e^{\frac{2\pi i}{n}} = e^{\frac{1}{n}(2\pi i)}$.

***VI parte:* Il polinomio $\Phi_d(x)$**
Definiamo ora il nuovo polinomio:

$$\Phi_d(x) \;=\; \prod_{\lambda \, di \, ordine \, d} (x - \lambda),$$

ove λ sono le radici n-esime dell'unità.
Ogni radice ha un certo ordine d, e quindi viene inclusa in uno dei polinomi $\Phi_d(x)$ una e una sola volta. Per questo il prodotto di tutti questi polinomi restituirà il polinomio iniziale $x^n - 1$. Possiamo quindi scrivere

$$x^n - 1 \;=\; \prod_{d|n} \Phi_d(x), \tag{1.3}$$

la quale formula ci viene assicurata dal Teorema di Lagrange sopra citato.
Consideriamo ora il polinomio $\Phi_n(x)$; abbiamo visto che esso esiste perchè esistono radici di ordine n. Dimostriamo per induzione che i coefficienti del polinomio $\Phi_n(x)$ sono interi (ovvero $\Phi_n(x) \in \mathbb{Z}[x] \,\forall n$) e che il coefficiente costante

[3] Consideriamo il caso in cui n e k siano pari; possiamo quindi scriverli come $n = 2n'$ e $k = 2k'$. Così possiamo riscrivere λ_k nel seguente modo:

$$\lambda_k \;=\; \cos\frac{4k'\pi}{2n'} + i\sin\frac{4k'\pi}{2n'} \;=\; \cos\frac{2k'\pi}{n'} + i\sin\frac{2k'\pi}{n'}$$

che è radice del polinomio $x^{n'} - 1 = 0$ con $n' < n$.
L'ordine d sarà il valore minimo per cui kd è multiplo di n.

è 1 o -1.

Per n=1 abbiamo che 1 è l'unica radice, e così $\Phi_1(x) = x - 1$.

Assumiamo ora che i coefficienti di $\Phi_d(x)$ siano interi e che i loro coefficienti costanti siano 1 ovvero -1. Scriviamo quindi il polinomio di partenza nel seguente modo:

$$x^n - 1 = p(x)\Phi_n(x) \tag{1.4}$$

$p(x)$ è il polinomio prodotto di tutti i polinomi $\Phi_d(x)$ con $d < n$, ovvero $p(x) = \Phi_1(x)...\Phi_{n-1}(x)$.[4]

A questo punto possiamo scrivere i due polinomi nel seguente modo: $p(x) = \sum_{j=0}^{l} p_j x^j$ e $\Phi_n(x) = \sum_{k=0}^{n-l} a_k x^k$. Inoltre dall'ipotesi induttiva abbiamo che $p_0 = 1$ o $p_0 = -1$ (infatti abbiamo detto che i coefficienti costanti di $\Phi_d(x)$ sono interi $\forall d < n$).

Il coefficiente costante di $p(x)\Phi_n(x)$ è $p_0 a_0$. Siccome $-1 = p_0 a_0$, vediamo che $a_0 \in \{1, -1\}$.

Dimostriamo tramite induzione che i coefficienti di $\Phi_n(x)$ sono interi. Abbiamo appena visto che a_0 è intero. Supponiamo quindi di sapere che $a_1, ..., a_{k-1} \in \mathbb{Z}$. Considerando il coefficiente di x^k calcolato in entrambe le parti di (1.4) otteniamo che

$$\sum_{j=0}^{k} p_j a_{k-j} = \sum_{j=1}^{k} p_j a_{k-j} - p_0 a_k \in \mathbb{Z}$$

Abbiamo appena visto che $a_0, a_1, ..., a_{k-1}$ stanno in $\mathbb{Z}$ per ipotesi induttiva. Allo stesso modo, anche tutti i p_j sono interi. Così anche $p_0 a_k$ deve essere intero, e di conseguenza lo è a_k, poichè p_0 è 1 o -1.

VII parte: **Conclusione**

Per quanto dimostrato finora giungiamo alla conclusione.

Sia n_k tale che $n_k | n$, cioè uno dei numeri che appaiono in (1.1). Scriviamo il

[4] Così abbiamo che $x^n - 1 = \Phi_1(x)\Phi_2(x)...\Phi_{n-1}(x)\Phi_n(x)$

polinomio $x^n - 1$ come prodotto di $\Phi_d(x)$ mettendo in evidenza $\Phi_n(x)$ e il polinomio $x^{n_k} - 1$. Otteniamo:

$$x^n - 1 \,=\, \prod_{d|n} \Phi_d(x) \,=\, (x^{n_k} - 1)\Phi_n(x) \prod_{d|n\,,\, d\nmid n_k\,,\, d\neq n} \Phi_d(x).$$

Consideriamo ora il caso in cui $x = q$. Andando a sostituire nella formula precedente abbiamo

$$q^n - 1 \,=\, (q^{n_k} - 1)\Phi_n(q) \prod_{d|n\,,\, d\nmid n_k\,,\, d\neq n} \Phi_d(q). \tag{1.5}$$

Da questa formula osserviamo subito che

$$\Phi_n(q) \,|\, (q^n - 1). \tag{1.6}$$

Inoltre lavorando sulla formula (1.5) ricaviamo

$$\frac{q^n - 1}{q^{n_k} - 1} \,=\, \Phi_n(q) \prod_{d|n\,,\, d\nmid n_k\,,\, d\neq n} \Phi_d(x)$$

e da questo segue che

$$\Phi_n(q) | \frac{q^n - 1}{q^{n_k} - 1} \tag{1.7}$$

con $\frac{q^n-1}{q^{n_k}-1}$ intero come visto in precedenza.
Poichè le formule (1.6) e (1.7) valgono per ogni k, deduciamo da (1.1) che

$$\Phi_n(q) \,|\, (q - 1),$$

ma questo non può essere vero.
Infatti, come da definizione dei polinomi $\Phi_d(x)$, sappiamo che $\Phi_n(x) = \prod_{\lambda\, di\, ordine\, n}(x-$

λ). Sia $\tilde{\lambda} = a+ib$ una delle radici che si trovano nel polinomio $\Phi_n(x)$. Avevamo supposto $R \neq C$, e quindi possiamo dire che $n > 1$. Abbiamo perciò che $\tilde{\lambda} \neq 1$, che implica che la parte reale a è minore di 1. Se infatti fosse $a = 1$ avrei $\tilde{\lambda} = 1$ che ha ordine n solo nel caso in cui $n = 1$.
Ora $|\tilde{\lambda}|^2 = a^2 + b^2 = 1$ e quindi

$$|q - \tilde{\lambda}|^2 = |q - a - ib|^2 = (q-a)^2 + b^2$$
$$= q^2 - 2aq + a^2 + b^2 = q^2 - 2aq + 1$$
$$> q^2 - 2q + 1 (\text{perchè } a < 1)$$
$$= (q-1)^2$$

e così $|q - \tilde{\lambda}| > q - 1$ vale per tutte le radici di ordine n. Prendendo $x = q$, questo fatto implica che

$$|\Phi_n(q)| = \prod_{\lambda} |q - \lambda| > q - 1$$

che significa che $\Phi_n(q)$ non può essere divisore di $q - 1$, e qui giungiamo alla contraddizione e alla fine della dimostrazione.

□

Piccola appendice sulla storia del teorema

Come detto in precedenza, la dimostrazione originaria del teorema in questione venne data per la prima volta nel 1905 ad opera di MacLagan Wedderburn[5]. Nello stesso anno anche Leonard E. Dickson, collega di Wedderburn, sviluppò

[5] *Transactions of the American Mathematical Society*, vol. 6, n. 2

una dimostrazione del teorema ma riconobbe a quest'ultimo la priorità della scoperta.

Nel 1983 Karen Parshall ha creduto di trovare un errore di omissione nella prima dimostrazione, errore che però non compare nella dimostrazione di Dickson. In seguito questa imprecisione venne corretta. Le due successive dimostrazioni che diede Wedderburn furono provate dopo che quest'ultimo lesse la dimostrazione di Dickson, che era corretta.

Per la sua dimostrazione, Dickson si basò sul teorema di Zsigmondy[6].

[6]Il teorema di Zsigmondy afferma che se $a > b > 0$ sono interi coprimi, allora per ogni $n > 1$ c'è un numero primo p che divide $a^n - b^n$ e che non divide $a^k - b^k$ per ogni intero positivo $k < n$, con le seguenti eccezioni:

- se $a = 2$, $b = 1$ e $n = 6$; oppure
- se $a + b$ è una potenza di 2 e $n = 2$.

1.1 Un teorema sulle algebre finite

di J. H. MacLagan - Wedderburn

Transactions of the American Mathematical Society (1905)

Frobenius e C. S. Pierce hanno mostrato che, nel dominio dei numeri reali, le uniche algebre lineari e associative nelle quali ogni numero, eccetto lo zero, possiede un inverso, sono i quaternioni e le loro sottoalgebre. Inoltre nel dominio complesso nessuna algebra ha questa proprietà. Qui di seguito dimostreremo che il campo di Galois è l'unica algebra di questo tipo che possiede un numero finito di elementi.

Parte 1:

Dato che l'addizione è commutativa in un'algebra lineare associativa, può essere dimostrato, come nella teoria del campo di Galois, che per ogni numero x dell'agebra esiste un primo intero p per cui p volte x è zero e inoltre che p è lo stesso per ogni x. Ne segue che, nel gruppo formato da numeri di un'algebra additiva, ogni elemento è di periodo p e inoltre l'ordine del gruppo è p^n dove n è un intero positivo. I numeri $\neq 0$ dell'algebra formano un gruppo F, di ordine $p^n - 1$, con l'operazione di moltiplicazione. Gli elementi autoconiugati di F, insieme all'elemento zero, formano il campo di Galois.

Se y_1 e y_2 sono elementi autoconiugati di F e x è un elemento qualsiasi,

$$(y_1 + y_2)x \;=\; y_1x + y_2x \;=\; xy_1 + xy_2 \;=\; x(y_1 + y_2)$$

cioè gli elementi autoconiugati sono chiusi rispetto all'addizione, come rispetto alla moltiplicazione, e quindi con 0 formano un campo di Galois. Poichè l'identità è un elemento autoconiugato di F, questo campo di Galois esiste sempre. Se il suo ordine è p^m, l'ordine del sottogruppo di F, composto dai suoi elementi autoconiugati, è di ordine $p^m - 1$. Il sottogruppo verrà denotato con G e il corrispondente campo di Galois con $GF[p^m]$.

Sia x_1 un elemento $\neq 0$ dell'algebra; allora ci sono esattamente p^m numeri distinti della forma $\xi_1 x_1$, dove ξ_1 è un elemento di $GF[p^m]$. Se x_2 è un altro elemento non incluso in questo insieme, ci sono p^{2m} numeri distinti della forma $\xi_1 x_1 + \xi_2 x_2$. Allo stesso modo, se x_3 è un numero non della forma $\xi_1 x_1 + \xi_2 x_2$, ci sono p^{3m} numeri della forma $\xi_1 x_1 + \xi_2 x_2 + \xi_3 x_3$ e così via.
Evidentemente possiamo numerare in questo modo tutti i numeri dell'algebra e quindi possiamo trovare s numeri x_α $(\alpha = 1, 2, ..., s)$ in maniera che ogni numero x possa essere espresso univocamente nella forma

$$x = \sum_{\alpha=1}^{s} \xi_\alpha x_\alpha$$

dove ξ_α $(\alpha = 1, 2, ..., s)$ sono elementi di $GF[p^m]$. L'ordine di F è $p^{ms} - 1$.

Parte 2:
Sia x_α un numero dell'algebra che non giace in $GF[p^m]$. Allora, se y_1 e y_2 sono due numeri commutativi con x_α, anche $y_1 + y_2$ e $y_1 y_2$ commutano con x_α e quindi l'insieme di tutti i numeri che commutano con x_α formano una sottoalgebra. Il gruppo, formato dai numeri di questa algebra con l'operazione di moltiplicazione, sarà denotato con F_{x_α}. Esso contiene G, è di ordine $p^{ms_\alpha} - 1$, dove s_α è un intero positivo.
Quindi, dividendo gli elementi di F in classi coniugate, otteniamo

$$p^n - 1 = p^m - 1 + \sum_{\alpha=1}^{t} k_\alpha \frac{p^n - 1}{p^{ms_\alpha} - 1}. \tag{1.8}$$

Questo mostra che, se il minimo comune multiplo di s_α $(\alpha = 1, 2, ..., s)$ è s', $p^m - 1$ è divisibile da $(p^n - 1)/(p^{ms'} - 1)$. Quindi

$$(p^m - 1)(p^{ms'} - 1) = l(p^n - 1).$$

Riducendo questo modulo p^m vediamo che l deve essere della forma $kp^m - 1$

($k > 0$). Siccome $ms' \leq n$, abbiamo che $k = 1$ e $ms' = n = ms$.

Parte 3:

Dalla teoria dei numeri ipercomplessi segue che c'è un'equazione di grado più basso,

$$f(x) \; = \; x^r + a_1 x^{r-1} + a_2 x^{r-2} + ... + a_{r-1} \; = \; 0, \tag{1.9}$$

con coefficienti in $GF[p^m]$, che è soddisfatta identicamente da ogni numero x dell'algebra, a prescindere da ogni speciale relazione tra le coordinate di x, ad eccezione della condizione che esse giacciano in $GF[p^m]$. Inoltre, c'è come minimo un elemento dell'algebra che non soddisfa nessuna equazione simile di grado minore.

Infatti (1.9) stabilisce che $x^{r-1}, x^{r-2}, ..., x^0$ sono linearmente indipendenti all'interno di $GF[p^m]$ e la condizione di indipendenza può evidentemente essere riproposta in una forma che afferma che certi determinanti, i quali elementi sono funzioni razionali integrali nelle coordinate di x, non svaniscono identicamente. Quindi ci devono essere degli insiemi di valori delle coordinate per cui $x^{r-1}, x^{r-2}, ..., x^0$ sono indipendenti e quindi la particolare x così ottenuta non soddisfa alcuna equazione di grado minore di r. (1.9) è chiamata *equazione caratteristica*, mentre l'equazione di grado minore soddisfatta da una x è chiamata *equazione ridotta*.

$f(x)$ è irriducibile in $GF[p^m]$; se fosse riducibile nessun fattore possiederebbe un inverso, contrariamente alle nostre ipotesi. In maniera simile, l'equazione ridotta in un numero dato è irriducibile.

Per ogni x dato tutte le radici della sue equazione caratteristica $f(x) = 0$ sono radici della sua equazione ridotta $\Phi(x) = 0$, entrambe ritenute equazioni ordinarie in $GF[p^m]$, e quindi, poichè $\Phi(x)$ è irriducibile, $f(x)$ è potenza di $\Phi(x)$ e il grado dell'equazione ridotta è un divisore di r.

Ora assumiamo che F_{x_α} sia abeliano per ogni x_α che non giace in $GF[p^m]$. Sotto

queste ipotesi F_{x_α} è un gruppo moltiplicativo di un campo di Galois e quindi è ciclico. Se x_α è scelto come generatore di F_{x_α} e se s_α è il grado dell'equazione ridotta di x_α, ci sono esattamente $p^{ms_\alpha} - 1$ diverse funzioni razionali in x con coefficienti in $GF[p^m]$; quindi l'ordine di F_{x_α} è $p^{ms\alpha} - 1$.
Ora, è stato dimostrato in precedenza che per alcuni x_α, $s_\alpha = r$ e inoltre ogni s_α è un fattore di r. Perciò r è il minimo comune multiplo di $s_1, s_2, ...$ e quindi $r = s$. Ma $ms = n$. Allora F_{x_α} è identificato con F, ovvero l'algebra è un campo di Galois.
Supponiamo ora che F non sia abeliano. Allora per alcune x non appartenenti a G, F_x non è abeliano. In maniera simile ci saranno alcuni elementi di F_x che non sono autoconiugati in F_x e tali che il gruppo di questi elementi di F_x che sono commutativi con esso non è abeliano; e così via. Allora possiamo dedurre una serie di gruppi di ordine decrescente, nella qual serie nessun membro è abeliano. Ciò è comunque impossibile poichè ogni gruppo contiene G e l'ordine di F è finito. Quindi F deve essere abeliano.

Parte 4:
Lo stesso risultato può essere dedotto senza l'aiuto della teoria delle equazioni caratteristiche. Abbiamo dimostrato che, se F non è un campo, i suoi elementi possono essere raccolti in sottogruppi, e l'ordine di tali gruppi moltiplicativi sono della forma p^{ms_α}. Il Teorema di Sylows afferma che ogni divisore primo di $p^n - 1$ è anche divisore di alcuni $p^{ms_\alpha} - 1$ $(ms_\alpha < n)$. Questo comunque è possibile soltanto in due casi:

- $p = 2$, $n = 6$;
- $p = 2^k - 1$, $n = 2$.

Nel primo caso abbiamo $m = 1$ poichè gli unici divisore di n sono 2 e 3, che sono relativamente primi, quindi da (6) otteniamo

$$2^6 - 1 = 1 + x_1 \frac{2^6 - 1}{2^3 - 1} + x_2 \frac{2^6 - 1}{2^2 - 1}$$

dove x_1, x_2 sono interi entrambi diversi da zero. Questo ci da $62 = 9x_1 + 21x_2$, un'equazione che non può essere soddisfatta da interi. perciò questo caso non può verificarsi.
Il secondo caso è inammissibile poichè $n = 2$ è primo.

Parte 5:

La seguente dimostrazione è più diretta. Se tutti gli elementi dell'algebra sono moltiplicati successivamente per un qualche elemento ad eccezione dello 0 è facile vedere dalla proprietà distributiva che vengono permutati tra loro in modo da non modificare le loro relazioni additive, ovvero ogni operazione del genere da un isomorfismo del gruppo additivo in sè. segue che nel gruppo degli isomorfisci del gruppo additivo ci sono due sottogruppi semplicemente isomorfi con il gruppo moltiplicativo; cioè, uno ottenuto con la moltiplicazione a sinistra, l'altro con quella a destra.
Ogni operazione di uno di questi sottogruppi è commutativa con le operazioni degli altri, e si può vedere che il più grande sottogruppo comune corrisponde all'insieme degli elementi autoconiugati di F e quindi è di ordine $p^m - 1$.
Questi due sottogruppi egenerano un sottogruppo di ordine $(p^n - 1)^2/(p^m - 1)$ del gruppo degli isomorfismi. Poichè il gruppo additivo è un gruppo abeliano del tipo (1,1,...,1), il suo gruppo di isomorfismi è il gruppo omogeneo lineare $GLH(n, p)$ di ordine $(p^n - 1)(p^n - p)...(p^n - p^{n-1})$, un'espressione che è divisibile per $(p^n - 1)^2/(p^m - 1)$ soltanto in due casi speciali spiegati sopra, tranne $m = n$. Escludendo questi due casi, deve essere $m = n$.
Allora F è abeliano.

Capitolo 2

Lo studio di alcuni numeri irrazionali

In questo capitolo dimostreremo l'irrazionalità di π, di e, di alcune delle loro potenze e di altri numeri.
Il problema dell'irrazionalità di questi numeri ha radici profondissime:

- π è definito come

$$\pi = \frac{l(C)}{2r},$$

  con $l(C)$ che indica la lunghezza della circonferenza e r il raggio corrispondente.
  Il suo simbolo venne introdotto solo nel 1706 dal matematico William Jones [1].
  La sua irrazionalità venne dimostrata per la prima volta da Johann Heinrich Lambert nel 1768. Qui è riportata invece la dimostrazione di Ivan Niven del 1947.

- e, chiamato numero di Eulero (o talvolta, in Italia, numero di Nepero), venne introdotto per la prima volta nel 1618 in un lavoro sui logaritmi di John Napier, ma la lettera e per la costante venne usata a partire dal 1727

[1] In *A new introduction to mathematics.*

da Leonhard Euler [2]. Il primo a dimostrare la sua irrazionalità fu Charles Hermite nel 1873, che inoltre stabilì che e è trascendente (ovvero che e non è zero di un polinomio a coefficienti razionali). Il lavoro di Hermite ispirò poi Niven per la dimostrazione dell'irrazionalità di π.

Cominceremo trattando di e e delle sue potenze, e vedremo che anch'esse sono irrazionali dato esponente razionale diverso da 0.

Teorema: e è un numero irrazionale.

Dimostrazione:
Ricordiamo la definizione di e, $e = \sum_{k\geq 0} \frac{1}{k!}$.
Sviluppando la sommatoria otteniamo

$$e := 1 + \frac{1}{1} + \frac{1}{2} + \frac{1}{6} + \frac{1}{24}... = 2,718281828...$$

Supponiamo per assurdo che esistano due interi $a, b > 0$ con $e = \frac{a}{b}$, allora moltiplicando per $n!$ avremmo che

$$n!be = n!a \tag{2.1}$$

per ogni $n \geq 0$. Possiamo scrivere e come

$$e = (1 + \frac{1}{1!} + \frac{1}{2!} + ... + \frac{1}{n!}) + (\frac{1}{(n+1)!} + \frac{1}{(n+2)!} + \frac{1}{(n+3)!} + ...)$$

e studiamo la formula (2.1). A destra abbiamo $n!a$ che è un numero intero.[3] Il termine di sinistra, $n!be$, si decompone invece in due parti. La prima è l'addendo intero

$$bn!(1 + \frac{1}{1!} + \frac{1}{2!} + ... + \frac{1}{n!}) = b(n! + n! + n(n+1)...3 + ... + n + 1)$$

[2] Il primo uso di e in una pubblicazione compare nella *Mechanica* di Eulero del 1736
[3] Infatti sia a che $n!$ sono interi, quindi il loro prodotto $n!a$ è un intero.

mentre la seconda è rappresentata dall'addendo

$$b(\frac{1}{n+1} + \frac{1}{(n+1)(n+2)} + \frac{1}{(n+1)(n+2)(n+3)} + ...) \tag{2.2}$$

Studiamo l'equazione (2.2). Osserviamo che per n grande essa non può essere intera; infatti essa è maggiore di $\frac{b}{n+1}$ e minore di $\frac{b}{n}$. Per verificarlo scrivo

$$\frac{1}{n+1} < \frac{1}{n+1} + \frac{1}{(n+1)(n+2)} + \frac{1}{(n+1)(n+2)(n+3)} + ...$$

$$< \frac{1}{n+1} + \frac{1}{(n+1)^2} + \frac{1}{(n+1)^3} + ...$$

$$= \sum_{k\geq 0} \frac{1}{(n+1)^k} - 1 = \frac{1}{1-\frac{1}{n+1}} - 1 = 1 + \frac{1}{n} - 1 = \frac{1}{n}.$$

Moltiplicando per b otteniamo la disuguaglianza citata sopra. [4] La formula (2.2) quindi non può rapprensentare un intero, e qui si giunge alla contraddizione.

□

[4] Questo fatto può essere anche dimostrato nel seguente modo:
Sia data la serie geometrica infinita

$$P = \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + ...$$

Per $p > 1$ otteniamo

$$pP = 1 + \frac{1}{p} + \frac{1}{p^2} + ... = 1 + P,$$

e quindi

$$P = \frac{1}{p-1}.$$

Ora andremo a dimostrare l'irrazionalità di e^2. Nel teorema precedente abbiamo dimostrato che e è irrazionale; da questo teorema però non possiamo dedurre l'irrazionalità di e^2. Infatti non è certo detto che se α è irrazionale anche α^2 lo sia.
John Cosgrave studiò due procedimenti per dimostrare che e^2 è irrazionale, e considerandoli insieme arrivò anche a provare che e^4 è irrazionale. Il primo metodo deriva da una pubblicazione di Liouville del 1840, mentre il secondo è un'aggiunta di due pagine che Liouville presentò nella stessa rivista.

Per dimostrare il seguente teorema è necessario ricordare la formula

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!} = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + ... \tag{2.3}$$

Teorema: e^2 è irrazionale.

Dimostrazione:
Supponiamo per assurdo che $e^2 = \frac{a}{b}$, con $a, b > 0$ interi. La riscriviamo come

$$be = ae^{-1}.$$

Ricaviamo le seguenti formule sostituendo rispettivamente $x = 1$ e $x = -1$ nella (2.3). Otteniamo

$$e = 1 + \frac{1}{1} + \frac{1}{2} + \frac{1}{6} + \frac{1}{24} + \frac{1}{120} + ...$$

rispettivamente

$$e^{-1} = 1 - \frac{1}{1} + \frac{1}{2} - \frac{1}{6} + \frac{1}{24} - \frac{1}{120} \pm ...$$

e poi moltiplichiamo per $n!$ ottenendo $n!be = n!ae^{-1}$. Studiamo ora $n!be$; esso è la somma di due addendi. Il primo è

$$n!b(1 + \frac{1}{1} + \frac{1}{2} + \frac{1}{6} + ... + \frac{1}{n!})$$

$$= b(n! + n! + n(n-1)(n-2)...3 + ... + 1)$$

che è un intero, e il secondo addendo è

$$n!b(\frac{1}{(n+1)!} + \frac{1}{(n+2)!} + ...) = b(\frac{1}{n+1} + \frac{1}{(n+1)(n+2)} + ...)$$

è approssimativamente $\frac{b}{n}$. Come visto nella dimostrazione precedente, questo valore è maggiore di $\frac{b}{n+1}$ ma minore di $\frac{b}{n}$. Chiamiamo r il secondo addendo; per n sufficientemente grande possiamo affermare per esempio che $r < \frac{1}{3}$.[5]
Ora concentriamoci su $n!ae^{-1} = n!a(1+\frac{1}{1}+\frac{1}{2!}+...+\frac{1}{n!}+\frac{1}{(n+1)!}+...)$; noteremo che anch'esso è vicino ad un intero. Questo valore è composto da due addendi; il primo è

$$(-1)^{n+1}a(n! + n! + n(n-1)...3 + ... + 1)$$

mentre il secondo è

$$(-1)^{n+1}n!a(\frac{1}{(n+1)!} - \frac{1}{(n+2)!} + \frac{1}{(n+3)!} \mp ...),$$

che è approssimativamente $(-1)^{n+1}\frac{a}{n}$. Più precisamente: per ogni n il resto è

[5] Infatti per n che tende all'infinito avremo che r tende a 0; quindi lo possiamo porre minore di $\frac{1}{3}$.

maggiore di $-\frac{a}{n}$, ma minore di

$$-a(\frac{1}{n+1} - \frac{1}{(n+1)^2} - \frac{1}{(n+1)^3} - ...) = -\frac{a}{n+1}(1 - \frac{1}{n}) < 0,$$

[6]

infatti esso è negativo perchè $1 - \frac{1}{n} > 0$ in quanto n è scelto sufficientemente grande e $a > 0$ per ipotesi.
Pongo $-\sigma_n = -\frac{a}{n+1}(1 - \frac{1}{n})$ e sia $r = n!b(\frac{1}{(n+1)!} + \frac{1}{(n+2)!} + ...)$ come visto in precedenza. Notiamo che per n alto e pari abbiamo che $|-\sigma_n| < \frac{1}{3}$.
Se davvero valesse $n!be = n!ae^{-1}$ allora avrei un'uguaglianza del tipo

$$A + r = B - |\sigma_n|$$

dove A e B rappresentano gli addendi interi dei due membri dell'uguaglianza. Lavorando su questa formula otteniamo

$$B - A = r + |\sigma_n|$$

e nella somma $r + |\sigma_n|$ abbiamo entrambi gli addendi positivi e $< \frac{1}{3}$. Qui giungiamo a una contraddizione e dunque $n!be = n!ae^{-1}$ non può valere.

□

[6] Questo fatto si dimostra nel seguente modo:
riscrivo

$$\frac{1}{(n+1)^2} + \frac{1}{(n+1)^3} + ... = \sum_{k \leq 2} \frac{1}{(n+1)^k}$$
$$= \frac{1}{1 - \frac{1}{n+1}} - 1 - \frac{1}{n+1} = \frac{n+1}{n} - 1 - \frac{1}{n+1} = \frac{1}{n(n+1)}.$$

Otteniamo quindi

$$-a(\frac{1}{n+1} - \frac{1}{(n+1)^2} - \frac{1}{(n+1)^3} - ...) = -a(\frac{1}{n+1} - \frac{1}{n(n+1)})$$
$$= -a(\frac{n-1}{n(n+1)} = -\frac{a}{n+1}(\frac{n-1}{n}) = -\frac{a}{n+1}(1 - \frac{1}{n})$$

Affrontiamo l'irrazionalità di e^4. Proviamo a seguire una dimostrazione sulla linea delle precedenti. Supponiamo quindi per assurdo che $e^4 = \frac{a}{b}$ e scriviamo

$$be^2 = ae^{-2}$$

Come in precedenza moltiplichiamo entrambi i membri per $n!$ con n grande e studiamo gli addendi non interi. Otteremo a sinistra un valore che sarà approssimativamente $b\frac{2^{n+1}}{n}$ [7] mentre a sinistra avremmo $(-1)^{n+1}a\frac{2^{n+1}}{n}$; entrambi i valori saranno molto grandi con il crescere di n, e quindi non riusciremmo a giungere a una conclusione.
Quindi dobbiamo seguire una strada alternativa.
Durante la dimostrazione ci serviremo di un piccolo lemma, che è un caso speciale del Teorema di Lagrange.

Lemma: Per ogni $n \geq 1$ l'intero $n!$ contiene il fattore primo 2 al più $n-1$ volte, e l'uguaglianza vale se e solo se n è potenza di 2, ovvero $n = 2^m$.

La dimostrazione del lemma deriva dal fatto che $[\frac{n}{2}]$ fattori sono pari, $[\frac{n}{4}]$ di essi sono divisibili per 4, e così via. Quindi se 2^k è la più grande potenza di 2 che soddisfa $2^k \leq n$, allora $n!$ contiene il fattore primo 2 esattamente

$$[\frac{n}{2}] + [\frac{n}{4}] + ... + [\frac{n}{2^k}] \leq \frac{n}{2} + \frac{n}{4} + ... + \frac{n}{2^k} = n(1 - \frac{1}{2^k}) \leq n - 1$$

volte, con l'uguaglianza che vale in entrambe le disequazioni esattamente se $n = 2^k$ [8].

[7] Infatti l'addendo non intero sarebbe

$$n!b(\frac{2^{n+1}}{(n+1)!} + \frac{2^{n+2}}{(n+2)!} + ...) = b(\frac{2^{n+1}}{n+1} + \frac{2^{n+2}}{(n+1)(n+2)} + ...) = 2^{n+1}b(\frac{1}{n+1} + \frac{2}{(n+1)(n+2)} + ...)$$

[8] Infatti se $n = 2^k$ otteniamo

$$n(1 - \frac{1}{2^k}) = n(1 - \frac{1}{n}) = n - 1.$$

Dimostriamo ora il

Teorema: e^4 è irrazionale.

Dimostrazione:
Supponiamo per assurdo che $e^4 = \frac{a}{b}$ con $a, b > 0$ interi e scriviamo

$$be^2 = ae^{-2}.$$

Ora non scegliamo solo n sufficientemente grande come in precedenza, ma prendiamo n come una potenza grande di 2, $n = 2^m$. In seguito, non moltiplichiamo per $n!$, bensì per $\frac{n!}{2^{n-1}}$. Otteniamo quindi

$$b\frac{n!}{2^{n-1}}e^2 = a\frac{n!}{2^{n-1}}e^{-2}. \tag{2.4}$$

Calcoliamo e^2 e e^{-2} sostituendo nella formula (2.3) $x = 2$, rispettivamente $x = -2$. Abbiamo

$$e^2 = \sum_{n=0}^{\infty} \frac{2^n}{n!} = 1 + \frac{2}{1} + \frac{4}{2} + ... + \frac{2^r}{r!} + ...$$

e

$$e^{-2} = \sum_{n=0}^{\infty} \frac{(-2)^n}{n!} = 1 - \frac{2}{1} + \frac{4}{2} + ... + (-1)^r\frac{2^r}{r!} + ...$$

Studiamo ora gli addendi della formula (2.4), suddividendoli in due gruppi: quelli in cui $r \leq n$ e in cui $r \geq n + 1$.
Fissiamo un qualsiasi r tale che $r \leq n$. Studiamo quindi gli addendi che corrispondono a questo r in entrambi i membri della formula (2.4). A sinistra

otterremo

$$b\frac{n!}{2^{n-1}}\frac{2^r}{r!}$$

mentre a destra

$$(-1)^r a\frac{n!}{2^{n-1}}\frac{2^r}{r!}.$$

Per il lemma precedente abbiamo che per $r > 0$ il valore $r!$ contiene il fattore primo 2 al massimo $r-1$ volte, mentre $n!$ lo contiene esattamente $n-1$ volte. Allora posso scrivere $r! = 2^t r_1$ con $t \leq r-1$, e r_1 dispari, e $n! = 2^{n-1}n_1$ con n_1 dispari. Sostituendo queste scritture negli addendi precedenti notiamo che per $0 < r \leq n$ gli addendi sono pari. [9]

Ora concentriamoci sugli addendi r-esimi con $r \geq n+1$. Siccome n è pari (abbiamo supposto $n = 2^m$), le serie che otteniamo sono

$$\sum_{r\geq n+1} b\frac{2^{r-n+1}}{r(r-1)...(n+1)} = b(\frac{2^2}{n+1}+\frac{2^3}{(n+1)(n+2)}+...) = 2b(\frac{2}{n+1}+\frac{4}{(n+1)(n+2)}+...)$$

e

[9] Se $r! = 2^t r_1$ con $t \leq r-1$, e r_1 dispari, e $n! = 2^{n-1}n_1$ con n_1 dispari i due addendi per r fissato diventano

$$b\frac{n!}{2^{n-1}}\frac{2^r}{r!} = b\frac{2^{n-1}n_1}{2^{n-1}}\frac{2^r}{2^t r_1} = b\frac{n_1}{r_1}2^{r-t}.$$

Ora, r_1 divide n_1; infatti questi due valori sono della forma

$$n_1 = 1\cdot 3\cdot 5\cdot 3\cdot 7\cdot 3^2\cdot ...$$

e

$$r_1 = 1\cdot 3\cdot 5\cdot 3\cdot 7\cdot 3^2\cdot ...$$

con r_1 che ha un numero di fattori al più uguale al numero di fattori di n_1 (infatti abbiamo raccolto ogni fattore primo 2 presente nei valori $n!$ e $r!$.
Allora $b\frac{n_1}{r_1}2^{r-t}$ è un intero, e per di più è pari.
Lo stesso discorso vale per $(-1)^r a\frac{n!}{2^{n-1}}\frac{2^r}{r!}$.

$$\sum_{r\geq n+1}(-1)^r a\frac{2^{r-n+1}}{r(r-1)...(n+1)} = a(-\frac{2^2}{n+1}+\frac{2^3}{(n+1)(n+2)}-...) = 2a(-\frac{2}{n+1}+\frac{4}{(n+1)(n+2)}-...).^{10}$$

Siccome n è pari (abbiamo supposto $n = 2^m$), le serie che otteniamo per $r \geq n+1$ sono

$$2b(\frac{2}{n+1}+\frac{4}{(n+1)(n+2)}+\frac{8}{(n+1)(n+2)(n+3)}+...)$$

rispettivamente

$$2a(-\frac{2}{n+1}+\frac{4}{(n+1)(n+2)}-\frac{8}{(n+1)(n+2)(n+3)}\pm..).$$

Queste serie per n grande saranno approssimativamente $\frac{4b}{n}$, rispettivamente $-\frac{4a}{n}$, come si può notare comparandole con le serie geometriche. Per $n = 2^m$ grande otteniamo che il membro a sinistra di (2.4) è di poco maggiore di un intero, mentre quello di destra è di poco minore (si può verificare questo discorso in maniera praticamente analoga alla dimostrazione precedente). Qui si giunge a una contraddizione.

□

[10] Per ottenere queste sommatorie abbiamo osservato che, siccome $r \geq n+1$, abbiamo

$$b\frac{n!}{2^{n-1}}\frac{2^r}{r!} = b\frac{2^{r-n+1}}{r(r-1)...(n+1)}$$

e

$$(-1)^r a\frac{n!}{2^{n-1}}\frac{2^r}{r!} = (-1)^r a\frac{2^{r-n+1}}{r(r-1)...(n+1)}.$$

Abbiamo appena dimostrato che e^4 è irrazionale. Per mostrare che e^3, e^5 ecc. sono anch'essi irrazionali, ci serviremo di un metodo che risale a Charles Hermite [11] che si basa sul seguente lemma e in particolare sulla definizione di una funzione fondamentale.

La funzione introdotta nel seguente lemma è fondamentale per la dimostrazione dei teoremi centrali di questo capitolo. Lavorando su di essa infatti riusciamo a studiare l'irrazionalità di e^r con $r \in \mathbb{Q} \setminus \{0\}$, di π^2 e di un caso particolare nell'arcocoseno.
Infine, con una piccola variante di $f(x)$, affronteremo l'irrazionalità di π.

Lemma: Per qualche $n \geq 1$ fissato, consideriamo la funzione $f : \mathbb{R} \to \mathbb{R}$ con

$$f(x) \;=\; \frac{x^n(1-x)^n}{n!} \quad [12]$$

- $f(x)$ è una funzione polinomiale di grado $2n$ i cui coefficienti sono nulli fino al grado $(n-1)$-esimo; inoltre i coefficienti di $n!f(x)$ sono interi.
- Per $0 < x < 1$ abbiamo $0 < f(x) < \frac{1}{n!}$.
- Le derivate $f^{(k)}(0)$ e $f^{(k)}(1)$ sono intere per ogni $k \geq 0$.

[11] *Sul la fonction exponentielle*, Comptes rends de l'Academie des Sciences (Paris), 1873

[12] Ricordiamo che il binomio di Newton esprime lo sviluppo della potenza n-esima di un binomio qualsiasi con la formula seguente:

$$(a+b)^n \;=\; \sum_{k=0}^{n} a^{n-k}b^k.$$

In $f(x)$ troviamo il fattore $(1-x)^n$, che possiamo quindi riscrivere come

$$(1-x)^n \;=\; \sum_{k=0}^{n} \binom{n}{k} 1^{n-k}(-x)^k \;=\; \sum_{k=0}^{n} \binom{n}{k} 1^{n-k}(-x)^k.$$

Dimostrazione:

Indico $f(x)$ con $f(x) = \frac{1}{n!}\sum_{i=1}^{2n} c_i x^i$. Dimostriamo che questa scrittura rappresenta effettivamente $f(x)$ e che i coefficienti c_i sono interi per ogni $i = 1...2n$. Sviluppiamo $f(x)$ nel modo seguente:

$$f(x) = \frac{1}{n!}x^n(1-x)^n = \frac{1}{n!}x^n\sum_{k=0}^{n}\binom{n}{k}(-x)^k$$

$$= \frac{1}{n!}(\binom{n}{0}x^n - \binom{n}{1}x^{n+1} + \binom{n}{2}x^{n+2} - ... + (-1)^n\binom{n}{n}x^{2n})$$

$$= \frac{1}{n!}\sum_{i=1}^{2n} c_i x^i$$

dove i coefficienti c_i sono tali che $c_i = (-1)^i\binom{n}{i}$. Essi sono interi perchè i coefficienti binomiali sono numeri sempre interi.

Per dimostrare il secondo punto, consideriamo per ipotesi x tale che $0 < x < 1$. Notiamo subito che $0 < x^n < 1$ e che $0 < (1-x)^n < 1$, quindi anche il loro prodotto sarà minore di 1. Se lo dividiamo per $n!$ avrò che $0 < f(x) < \frac{1}{n!}$.

Dimostriamo ora il terzo punto. La k-esima derivata di $f(x)$ è

$$f^{(k)}(x) = \frac{1}{n!}[\binom{n}{0}n(n-1)...(n-k+1)x^{n-k} - \binom{n}{1}(n+1)n...(n-k+2)x^{n-k+1} +$$

$$... + (-1)^n\binom{n}{n}2n(2n-1)...(2n-k+1)x^{2n-k}]$$

Notiamo che per k tale che $1 \leq k \leq (n-1)$ la k-esima derivata di $f(x)$ si annulla in $x = 0$.

Invece se consideriamo k con $n \leq k \leq 2n$ in $x = 0$ questa derivata non si annulla, anzi otteniamo che

$$f^{(k)}(0) = \frac{k!}{n!}(-1)^k\binom{n}{k} = \frac{k!}{n!}c_k$$

che è un intero perchè $n! \mid k!$.
Osserviamo che $f(x) = f(1-x)$; perciò abbiamo che $f^{(k)}(x) = (-1)^k f^{(k)}(1-x)$, e quindi $f^{(k)}(1) = (-1)^k f^{(k)}(0)$, che è un intero.

□

2.1 Irrazionalità di e^r per r razionale e diverso da 0

Teorema 1: e^r è irrazionale per ogni $r \in \mathbb{Q} \setminus \{0\}$.

Dimostrazione:

È sufficiente dimostrare che e^s non può essere razionale per un intero positivo s (se $e^{\frac{s}{t}}$ fosse razionale, allora $(e^{\frac{s}{t}})^t = e^s$ sarebbe anch'esso razionale). Assumiamo che $e^s = \frac{a}{b}$ per a, b interi, $a, b > 0$, e sia n tale che $n! > as^{2n+1}$. Poniamo

$$F(x) := s^{2n}f(x) - s^{2n-1}f'(x) + s^{2n-2}f''(x) + ... + f^{(2n)}(x),$$

dove $f(x)$ è la funzione del lemma.
$F(x)$ può essere anche scritta come la somma infinita

$$F(x) := s^{2n}f(x) - s^{2n-1}f'(x) + s^{2n-2}f''(x) \mp ...$$

poichè le derivate più alte $f^{(k)}(x)$, per $k > 2n$, si annullano. Da questo vediamo che il polinomio $F(x)$ soddisfa l'identità

$$F'(x) = -sF(x) + s^{2n+1}f(x).$$

Infatti:

$$-sF(x) = -s^{2n+1}f(x) + s^{2n}f'(x) - s^{2n-1}f''(x) \pm ...$$

e sommando questa formula con $s^{2n+1}f(x)$ otteniamo proprio

$$F'(x) = s^{2n}f'(x) - s^{2n-1}f''(x) + s^{2n-2}f^{(3)}(x) \mp ...$$

Moltiplichiamo $F(x)$ per e^{sx} e differenziando abbiamo che

$$\frac{d}{dx}[e^{sx}F(x)] = se^{sx}F(x) + e^{sx}F'(x)$$

$$= se^{sx} + e^{sx}(-sF(x) + s^{2n+1}f(x)) = s^{2n+1}e^{sx}f(x).$$

Poniamo ora $N := b\int_0^1 s^{2n+1}e^{sx}f(x)dx$ e calcoliamo il suo valore:

$$N := b\int_0^1 s^{2n+1}e^{sx}f(x)dx = b[e^{sx}F(x)]_0^1$$

$$= b[e^sF(1) - F(0)] = b\cdot\frac{a}{b}F(1) - bF(0) = aF(1) - bF(0).$$

Il numero $aF(1) - bF(0)$ è un intero, poichè la terza parte del lemma implica che $F(0)$ e $F(1)$ sono interi.
Al contrario la seconda parte del lemma dà una stima di N dal basso e dall'alto,

$$N = b\int_0^1 s^{2n+1}e^{sx}f(x)dx < bs^{2n+1}e^s\frac{1}{n!} = bs^{2n+1}\frac{a}{b}\frac{1}{n!} = \frac{as^{2n+1}}{n!} < 1$$

che mostra che N non può essere un intero. Da qui nasce la contraddizione.

□

2.2 Irrazionalità di π^2

Teorema 2: π^2 è irrazionale.

Dimostrazione:

Assumiamo per assurdo che $\pi^2 = \frac{a}{b}$ per due interi $a, b > 0$. Ora definiamo il polinomio

$$F(x) := b^n(\pi^{2n}f(x) - \pi^{2n-2}f^{(2)}(x) + \pi^{2n-4}f^{(4)}(x) \mp ...);$$

questo soddisfa

$$F''(x) = -\pi^2 F(x) + b^n\pi^{2n+2}f(x).$$

Infatti

$$-\pi^2 F(x) = -b^n(\pi^{2n+2}f(x) - \pi^{2n}f^{(2)} + \pi^{2n-2}f^{(4)} \mp ...)$$

e sommando esso con $b^n\pi^{2n+2}f(x)$ otteniamo

$$F''(x) = b^n(\pi^{2n}f^{(2)}(x) - \pi^{2n-2}f^{(4)}(x) + \pi^{2n-4}f^{(6)}(x) \mp ...)$$

e così è dimostrata la formula precedente.

Ora, le regole elementari della differenziabilità implicano che

$$\frac{d}{dx}[F'(x)\sin\pi x - \pi F(x)\cos\pi x] = F''(x)\sin\pi x + \pi F'(x)\cos\pi x - \pi F'(x)\cos\pi x + \pi^2 F(x)\sin\pi x$$
$$= (F''(x) + \pi^2 F(x))\sin\pi x = (-\pi^2 F(x) + b^n\pi^{2n+2}f(x) + \pi^2 F(x))\sin\pi x$$
$$= b^n\pi^{2n+2}f(x)sin\pi x = b^n\frac{a^n}{b^n}\pi^2 f(x)\sin\pi x$$
$$= \pi^2 a^n f(x)sin\pi x.$$

Adesso definiamo $N := \pi \int_0^1 a^n f(x) \sin \pi x dx$. Calcolando il suo valore otteniamo

$$\begin{aligned} N &= \pi \int_0^1 a^n f(x) \sin \pi x dx = [\frac{1}{\pi} F'(x) \sin \pi x - F(x) \cos \pi x]_0^1 \\ &= \frac{1}{\pi} F'(1) \sin \pi - F(1) \cos \pi - \frac{1}{\pi} F'(0) \sin 0 + F(0) \cos 0 \\ &= F(0) + F(1) \end{aligned}$$

che è un intero per il terzo punto del lemma visto in precedenza. Inoltre N è positivo poichè è definito come integrale di una funzione continua che è positiva. Comunque, se scegliamo n abbastanza grande tale che $\frac{\pi a^n}{n!} < 1$, allora dalla seconda parte del lemma otteniamo

$$0 < N = \pi \int_0^1 a^n f(x) \sin \pi x dx < \frac{\pi a^n}{n!} < 1,$$

che è una contraddizione.

□

2.3 Irrazionalità dell'arcocoseno di certi numeri

Teorema 3: per ogni intero dispari $n \geq 3$, il numero

$$A(n) \;=\; \frac{1}{\pi}\arccos\left(\frac{1}{\sqrt{n}}\right)$$

è irrazionale.

Osservazione: calcoliamo il valore di $A(n)$ per $n = 2$ e $n = 4$.
$A(2) \;=\; \frac{1}{\pi}\arccos\left(\frac{1}{\sqrt{2}}\right) \;=\; \frac{1}{\pi}\cdot\frac{\pi}{4} \;=\; \frac{1}{4}$;
$A(4) \;=\; \frac{1}{\pi}\arccos\left(\frac{1}{2}\right) \;=\; \frac{1}{\pi}\cdot\frac{\pi}{3} \;=\; \frac{1}{3}$.
Entrambi i numeri sono razionali. Quindi la restrizione di n agli interi dispari è essenziale.

Dimostrazione:
Usiamo il teorema:

$$\cos\alpha + \cos\beta \;=\; 2\cos\frac{\alpha+\beta}{2}\cos\frac{\alpha-\beta}{2}$$

dalla trigonometria elementare, che per $\alpha = (k+1)\varphi$ e $\beta = (k-1)\varphi$ implica:

$$\cos(k+1)\varphi + \cos(k-1)\varphi \;=\; 2\cos\frac{(k+1)\varphi+(k-1)\varphi}{2}\cos\frac{(k+1)\varphi-(k-1)\varphi}{2}.$$

Quindi otteniamo

$$\cos(k+1)\varphi \;=\; 2\cos\varphi\cos k\varphi - \cos(k-1)\varphi. \tag{2.5}$$

Prendiamo in considerazione l'angolo $\varphi_n = \arccos\left(\frac{1}{\sqrt{n}}\right)$, che è definito da $\cos\varphi_n = \frac{1}{\sqrt{n}}$ e $0 \leq \varphi_n \leq \pi$. Osserviamo che otteniamo una rappresentazione della forma

$$\cos k\varphi_n = \frac{A_k}{\sqrt{n}^k},$$

dove A_k è un intero non divisibile per n, per ogni $k \geq 0$. Verifichiamo questo fatto per induzione.
Per $k = 0, 1$ abbiamo una rappresentazione di tal tipo con $A_0 = A_1 = 1$. Infatti:

- per $k = 0$ abbiamo $\cos 0 = \frac{A_0}{1} \Rightarrow 1 = \frac{A_0}{1} \Rightarrow A_0 = 1$;
- per $k = 1$ abbiamo $\cos \varphi_n = \frac{A_1}{\sqrt{n}} \Rightarrow \frac{1}{\sqrt{n}} = \frac{A_1}{\sqrt{n}} \Rightarrow A_1 = 1$.

Consideriamo ora $k \geq 1$. Per induzione su k usando (2.5) otteniamo

$$\begin{aligned}
\frac{A_{k+1}}{\sqrt{n}^{k+1}} &= \cos(k+1)\varphi_n \\
&= 2\cos\varphi_n \cos k\varphi_n - \cos(k-1)\varphi_n \\
&= 2\frac{1}{\sqrt{n}}\frac{A_k}{\sqrt{n}^k} - \frac{A_{k-1}}{\sqrt{n}^{k-1}} \\
&= \frac{2A_k - nA_{k-1}}{\sqrt{n}^{k+1}}.
\end{aligned}$$

Quindi abbiamo $A_{k+1} = 2A_k - nA_{k-1}$. Se $n \geq 3$ è dispari e A_k, A_{k-1} non sono divisibili per n, allora troviamo che anche A_{k+1} non può essere divisibile per n. Ora assumiamo che $A(n) = \frac{1}{\pi}\varphi_n = \frac{k}{l}$ sia razionale (con $k, l > 0$ interi). Allora $l\varphi_n = k\pi$ implica

$$\cos l\varphi_n = \cos \pi k \Longrightarrow \frac{A_l}{\sqrt{n}^l} = \cos \pi k$$

e quindi

$$\pm 1 = \cos \pi k = \frac{A_l}{\sqrt{n}^l}.$$

Perciò $\sqrt{n}^l = \pm A_l$ è un intero, con $l \geq 2$, e quindi $n|\sqrt{n}^l$. Con $\sqrt{n}^l | A_l$ abbiamo che n divide A_l, che è una contraddizione.

□

2.4 Irrazionalità di π

Concludiamo riportando con alcune precisazioni la dimostrazione *"Una semplice prova che π è irrazionale"* di Ivan Niven [13].
In fondo a questo sottocapitolo riportiamo anche il documento originale della dimostrazione.

Teorema 4: π è irrazionale.

Dimostrazione:
Sia $\pi = \frac{a}{b}$ il quoziente di interi positivi. Definiamo i polinomi

$$f(x) \;=\; \frac{x^n(a-bx)^n}{n!},$$

$$F(x) \;:=\; f(x) - f^{(2)}(x) + f^{(4)}(x) - ... + (-1)^n f^{(2n)}(x).$$

Poichè $n!f(x)$ ha coefficienti interi e termini in x di grado non minore di n, $f(x)$ e le sue derivate $f^{(j)}(x)$ hanno un valore intero per $x = 0$; anche per $x = \pi = \frac{a}{b}$, poichè $f(x) = f(\frac{a}{b} - x)$. da un elementare calcolo otteniamo

$$\frac{d}{dx}[F'(x)\sin x - F(x)\cos x] \;=\; F''(x)\sin x + F'(x)\cos x - F'(x)\cos x + F(x)\sin x$$

$$=\; F''(x)\sin x + F(x)\sin x \;=\; \sin x[F''(x) + F(x)].$$

Ora calcoliamo le derivate prima e seconda di $F(x)$:

$$F'(x) \;=\; f'(x) - f^{(3)}(x) + f^{(5)}(x) - ... + (-1)^n f^{(2n+1)}(x)$$

[13] Bullettin Ameri. Math. Soc. (1947)

$$F''(x) \;=\; f^{(2)}(x) - f^{(4)}(x) + f^{(6)}(x) - ... + (-1)f^{(2n+2)}(x).$$

Allora, tornando al calcolo del differenziale

$$\sin x[F''(x) + F(x)] \;=\; \sin x f(x).$$

Calcolando l'integrale di questo ultimo risultato otteniamo

$$\int_0^{\pi} f(x)\sin x dx \;=\; [F'(x)\sin x - F(x)\cos x]_0^{\pi}$$

$$=\; F'(\pi)\sin\pi - F(\pi)\cos\pi - F'(0)\sin 0 + F(0)\cos 0 \;=\; F(\pi) + F(0).$$

Ora, $F(\pi) + F(0)$ è un intero, poichè $f^{(j)}(\pi)$ e $f^{(j)}(0)$ sono interi. Ma per $0 < x < \pi$

$$0 \;<\; f(x)\sin x \;<\; \frac{\pi^n a^n}{n!},$$

così l'integrale precedente è positivo, ma arbitrariamente piccolo per n sufficientemente alto. Allora l'integrale è falso, e quindi π non è razionale.

□

A SIMPLE PROOF THAT π IS IRRATIONAL

IVAN NIVEN

Let $\pi = a/b$, the quotient of positive integers. We define the polynomials

$$f(x) = \frac{x^n(a - bx)^n}{n!},$$

$$F(x) = f(x) - f^{(2)}(x) + f^{(4)}(x) - \cdots + (-1)^n f^{(2n)}(x),$$

the positive integer n being specified later. Since $n!f(x)$ has integral coefficients and terms in x of degree not less than n, $f(x)$ and its derivatives $f^{(j)}(x)$ have integral values for $x = 0$; also for $x = \pi = a/b$, since $f(x) = f(a/b - x)$. By elementary calculus we have

$$\frac{d}{dx}\{F'(x)\sin x - F(x)\cos x\} = F''(x)\sin x + F(x)\sin x = f(x)\sin x$$

and

$$(1) \qquad \int_0^\pi f(x)\sin x\,dx = [F'(x)\sin x - F(x)\cos x]_0^\pi = F(\pi) + F(0).$$

Now $F(\pi) + F(0)$ is an *integer*, since $f^{(j)}(\pi)$ and $f^{(j)}(0)$ are integers. But for $0 < x < \pi$,

$$0 < f(x)\sin x < \frac{\pi^n a^n}{n!},$$

so that the integral in (1) is *positive, but arbitrarily small* for n sufficiently large. Thus (1) is false, and so is our assumption that π is rational.

PURDUE UNIVERSITY

Received by the editors November 26, 1946, and, in revised form, December 20, 1946.

Bibliografia

[1] Aigner M. - Ziegler G., *Proofs from THE BOOK*, pp. 23-34 (1998)

[2] Hermite C., *Sur la fonction exponentielle*, Comptes rendus de l'Academie des Sciences, pp. 18-24 (1873)

[3] Liouville, *Sur l'irrationalitè du nombre* $e = 2,718...$, Journal de Mathèmatiques Pures et Appl., pp. 193-194 (1840)

[4] Niven I. *A simple proof that* π *is irrational*, Bulletin Amer. Math. Soc., p.509 (1947)

[5] Wedderburn J., *A theorem of finite algebras*, Trans. Amer. Math. Soc., pp. 349-352 (1905)