SULLA POTENZA DELLE BASI DI GRUPPI E CORPI.

Memoria di **U. Morin** (Padova).

Adunanza del 9 dicembre 1934 - XIII.

L'osservazione (§ 1) che la totalità dei sottoinsiemi finiti di un insieme infinito ha la stessa potenza dell'insieme stesso, si applica (§ 2) allo studio degli isomorfismi tra gruppi abeliani, rilevando in particolare che la potenza della base HAMELIANA è quella del continuo.

Dalla stessa osservazione segue (§ 3) che il grado di trascendenza (non finito) di un corpo è uguale al numero cardinale del corpo, proprietà che contiene come corollario un noto teorema dello STEINITZ.

§ 1.

Sulla potenza della totalità dei sottoinsiemi finiti di un insieme.

1. Supponiamo noti i principali concetti della *teoria degli insiemi,* come quelli di *potenza* di un insieme e di relativo *numero cardinale.* Così ricordiamo che, essendo $\mathfrak{m}$, $\mathfrak{n}$, $\mathfrak{p}$, ... i numeri cardinali degli insiemi M, N, P, ... (in numero finito o infinito), si indica con $\mathfrak{m} + \mathfrak{n} + \mathfrak{p} + \cdots$ quello della loro somma, con $\mathfrak{m}\mathfrak{n}\mathfrak{p} \ldots$ quello del loro *prodotto,* e con $\mathfrak{m}^{\mathfrak{n}}$ quello dell'insieme di tutte le applicazioni di un insieme N sull'insieme M.

2. Ammetteremo in tutte le nostre considerazioni l'*assioma della scelta* (Auswahlpostulat) di ZERMELO, da cui si deduce che ogni insieme può essere considerato *bene ordinato* (Wohlordnungssatz). In base a questo assioma, due numeri cardinali possono essere posti in relazione da un determinato dei tre simboli $>$, $=$, $<$ *(trichotomie)* e per questi numeri valgono le seguenti formole fondamentali [1])

$$(1) \qquad \mathfrak{m} + \mathfrak{m} + \mathfrak{m} + \cdots = \aleph_0 \mathfrak{m} = \mathfrak{m} \qquad (\mathfrak{m} \geq \aleph_0)$$

$$(2) \qquad \mathfrak{m} + \mathfrak{n} = \mathfrak{m}\mathfrak{n} = \mathfrak{n} \qquad (\mathfrak{m} \leq \mathfrak{n},\ \mathfrak{n} \geq \aleph_0)$$

$$(3) \qquad \mathfrak{m}^n = \mathfrak{m} \qquad (\mathfrak{m} \geq \aleph_0,\ n = 1, 2, 3, \ldots).$$

[1]) W. SIERPINSKI, *Leçons sur les nombres transfinis.* [Gauthier-Villars, Paris (1928)], pag. 233.

3. È noto che l'insieme di tutti i sottoinsiemi *infiniti* di un insieme di potenza $\mathfrak{m}$ ($\geq \aleph_0$) ha la potenza $\mathfrak{m}^{\mathfrak{m}} = 2^{\mathfrak{m}} > \mathfrak{m}$. Invece l'insieme di tutti i sottoinsiemi *finiti* di un insieme numerabile è ancora numerabile [2]).

Questa ultima proprietà si estende agevolmente agli insiemi non numerabili, cioè: *L'insieme di tutti i sottoinsiemi finiti e ordinati di un insieme infinito M ha la stessa potenza dell'insieme stesso.*

Il teorema è manifestamente espresso dalla seguente formola

$$(4) \qquad \sum \mathfrak{m}^n = \mathfrak{m} \qquad (\mathfrak{m} \geq \aleph_0,\ n = 1, 2, 3, \ldots)$$

che si verifica combinando le (3) con la (1).

La (4) si può anche scrivere

$$\sum \mathfrak{m}\,\mathfrak{m}^{n-1} = \mathfrak{m},$$

da cui, sopprimendo in base alla (2) il primo termine della sommatoria

$$\sum \mathfrak{m}\,\mathfrak{m}^n = \mathfrak{m}$$

e quindi, i numeri cardinali $\mathfrak{p}_n$ non essendo tutti nulli

$$(5) \qquad \sum \mathfrak{p}_n \mathfrak{m}^n = \mathfrak{m} \qquad (\mathfrak{m} \geq \aleph_0,\ \mathfrak{p}_n \leq \mathfrak{m},\ n = 1, 2, 3, \ldots)$$

che si può così interpretare: *Se ad ogni sottoinsieme finito di un insieme infinito di potenza* $\mathfrak{m}$, *facciamo corrispondere un insieme non vuoto di elementi di potenza non superiore ad* $\mathfrak{m}$, *la somma di tutti questi insiemi ha ancora la potenza* $\mathfrak{m}$.

§ 2.

Isomorfismi tra gruppi dotati di operatori scalari.

4. Abbiasi un gruppo abeliano A di elementi a, b, c, ... dotato di operatori scalari λ, μ, ν, ... che appartengano al corpo k dei numeri razionali, l'elemento unità di k essendo operatore unità nel gruppo [3]).

Se per la legge di composizione del gruppo si adotta la scrittura additiva, si abbia (per definizione)

$$(6) \qquad \lambda(a + b) = \lambda a + \lambda b$$

---

[2]) W. SIERPINSKI, loc. cit. [1]), pp. 223 e 61.

[3]) B. L. VAN DER WAERDEN, *Moderne Algebra*, I Teil. [Julius Springer, Berlin (1930)], pag. 132.

e se invece si adotta quella moltiplicativa, sia

$$(7) \qquad (ab)^{\lambda} = a^{\lambda} b^{\lambda}$$

5. Se A' è un altro gruppo abeliano con operatori scalari dello stesso corpo k, si dice che tra A ed A' intercede un *isomorfismo operatoriale,* se tra i loro elementi intercede una corrispondenza biunivoca che alla somma (o prodotto) di due elementi di A fa corrispondere la somma (o il prodotto) dei corrispondenti elementi di A'; ed inoltre ad un elemento λa (o a^{λ}) corrisponde $\lambda a'$ (o a'^{λ}).

L'isomorfismo operatoriale tra A ed A' è rappresentato da un'equazione $y = f(x)$, in cui la $f(x)$ soddisfa, a seconda che A si interpreti come un gruppo additivo (modulo) M, oppure come un gruppo moltiplicativo G, e così A' come uno M' oppure un G'; alle seguenti equazioni funzionali:

$$(8) \qquad (M, M') \qquad \begin{cases} f(x+y) = f(x) + f(y) \\ f(\lambda x) = \lambda f(x) \end{cases}$$

$$(9) \qquad (G, G') \qquad \begin{cases} f(xy) = f(x) f(y) \\ f(x^{\lambda}) = f(x)^{\lambda} \end{cases}$$

$$(10) \qquad (M, G') \qquad \begin{cases} f(x+y) = f(x) f(y) \\ f(\lambda x) = f(x)^{\lambda} \end{cases}$$

$$(11) \qquad (G, M') \qquad \begin{cases} f(xy) = f(x) + f(y) \\ f(x^{\lambda}) = \lambda f(x). \end{cases}$$

Verifichiamo che in ciascuna di queste coppie di equazioni, la seconda equazione è soddisfatta in conseguenza della prima. Occupiamoci del caso (M, M'). La prima equazione dà per ogni n intero $f(na) = nf(a)$, da cui $nf\left(\frac{1}{n}a\right) = f(a)$, cioè $f\left(\frac{1}{n}a\right) = \frac{1}{n}f(a)$; e quindi $f\left(\frac{m}{n}a\right) = \frac{m}{n}f(a)$.

Questa verifica si estende agli altri casi con un puro cambiamento di scrittura. Dunque: *Un isomorfismo tra due gruppi abeliani con operatori del corpo razionale k è necessariamente un isomorfismo operatoriale.*

In seguito, parlando di gruppi, ammetteremo senz'altro che siano dotati di operatori scalari del corpo k; di modo che i relativi isomorfismi saranno isomorfismi operatoriali.

6. Un gruppo abeliano si dice *finito* rispetto al corpo k degli operatori, se i suoi

elementi si possono rappresentare nella forma

$$\lambda_1 u_1 + \lambda_2 u_2 + \cdots + \lambda_n u_n \tag{12}$$

ove si tratti di un modulo M, oppure nella forma

$$u_1^{\lambda_1} u_2^{\lambda_2} \ldots u_n^{\lambda_n} \tag{13}$$

ove si tratti di un gruppo G. Si può limitare il numero degli elementi u_i in modo che $\lambda_1 u_1 + \lambda_2 u_2 + \cdots + \lambda_n u_n = 0$ oppure $u_1^{\lambda_1} u_2^{\lambda_2} \ldots u_n^{\lambda_n} = 1$ comporti che siano nulle tutte le λ_i. Si dice allora che $(u_1, u_2, \ldots, u_n)$ è una *base* per il gruppo. Segue che il numero n degli elementi della base è determinato per un gruppo; e che è pure determinata la rappresentazione di un elemento del gruppo nella forma (12) [oppure (13)] [4]).

7. Estendiamo queste nozioni a gruppi non finiti.

Dico che per ogni gruppo abeliano non finito, supposto bene ordinato, si può determinare un insieme di elementi

$$U = \{u_1, u_2, \ldots, u_\nu, \ldots\} \tag{14}$$

(ν in generale indice transfinito) tale che ogni elemento del gruppo possa essere messo sotto la forma

$$u = \lambda_1 u_1 + \lambda_2 u_2 + \cdots + \lambda_\nu u_\nu + \cdots \tag{15}$$

ove si tratti di un modulo M, oppure

$$u = u_1^{\lambda_1} u_2^{\lambda_2} \ldots u_\nu^{\lambda_\nu} \ldots \tag{16}$$

trattandosi di un gruppo moltiplicativo G, e dove soltanto un numero *finito* di numeri λ_i sia diverso da zero; mentrecchè una tale rappresentazione non sia possibile per alcun elemento u_ν dell'insieme U rispetto all'insieme $U - u_\nu$. Un insieme U che goda di questa ultima proprietà sarà detto *irriducibile;* ed è immediato che per questo fatto la rappresentazione di un elemento u sotto la forma (15) [oppure (16)] è determinata.

Veniamo alla costruzione di U. Sia u un elemento qualunque del gruppo. Ove esso si esprima nella forma (15) [o (16)] mediante un numero finito qualunque di elementi della sezione $S(u)$, diremo che u *dipende* da $S(u)$. Orbene, un elemento u faccia parte della base U se non dipende dalla sezione $S(u)$.

L'insieme U così determinato è irriducibile. Infatti se un elemento di U dipendesse da altri elementi di U, ciascuno di questi dipenderebbe dai rimanenti, e quindi l'ultimo di essi non potrebbe fare parte di U.

Ciascun elemento del gruppo dipende da U. Se ciò non fosse, sia u il primo

---

[4]) B. L. VAN DER WAERDEN, loc. cit. [3]), pag. 95 e II Teil, pag. 86.

elemento che non dipende da U. Poichè u non appartiene ad U, dipenderà dalla sezione $S(u)$ di cui ciascun elemento, in quanto precedente u, dipende da U. E quindi anche u verrebbe dipendere da U, contro il supposto.

8. *Due gruppi abeliani A e A', le cui basi U e U' abbiano ugual potenza, sono sempre isomorfi.*

Infatti, posta tra le due basi una qualunque corrispondenza biunivoca π, ed assunto come ordinatamento di U' quello che si deduce dall'ordinatamento di U mediante π, cioè $u_\nu \rightarrowtail u'_\nu$; si faccia corrispondere ad ogni elemento di A che si esprime nella forma (15) [rispettivamente (16)] con gli operatori non nulli $(\lambda_{\nu_1}, \lambda_{\nu_2}, \ldots, \lambda_{\nu_n})$, l'elemento di A' che si esprime rispetto alla base U' con gli stessi operatori non nulli.

Che la corrispondenza così ottenuta sia effettivamente un isomorfismo risulta dal fatto che la rappresentazione di un elemento dei gruppi nella forma (15) [rispettivamente (16)] è determinata.

9. Come immediata applicazione della (5) possiamo dimostrare che:

Un gruppo non finito e la sua base hanno la medesima potenza.

Infatti se la potenza della base è $\mathfrak{m} \geqq \aleph_0$, la potenza del gruppo sarà al più

$$\sum \aleph_0 \mathfrak{m}^n \qquad (n = 1, 2, 3, \ldots) \tag{17}$$

cioè, per la (5), ancora $\mathfrak{m}$.

Come corollari:

I) Due gruppi non finiti di ugual potenza (con operatori scalari del corpo razionale k) sono sempre isomorfi.

II) Questi isomorfismi forniscono la più generale soluzione, entro ai due gruppi, dell'equazione funzionale rispettivamente (8), (9), (10) o (11); ove si ponga inoltre la condizione che la $f(x)$ sia univocamente invertibile tra i due gruppi.

III) Due basi di un medesimo gruppo hanno ugual potenza.

IV) Si ottengono tutti gli automorfismi di un gruppo, ponendo una qualunque corrispondenza biunivoca tra due sue basi qualunque.

V) La potenza dell'insieme di tutti gli automorfismi di un gruppo di potenza $\mathfrak{m} \geqq \aleph_0$ è dunque almeno uguale alla potenza di tutte le corrispondenze biunivoche di U con se medesima, cioè $2^{\mathfrak{m}}$; e quindi effettivamente uguale a $2^{\mathfrak{m}}$, poichè questa è la potenza dell'insieme di tutte le corrispondenze del gruppo con sè medesimo.

10. Se il modulo M è il corpo reale (interpretato come un modulo rispetto all'ordinaria operazione di somma), la rispettiva base (14) dicesi *base hameliana* [5]), ed è intervenuta nella costruzione delle soluzioni, nel campo reale, dell'equazione funzionale (8).

---

5) G. HAMEL, *Eine Basis aller Zahlen und die unstetigen Lösungen der Funktionalgleichung* $f(x+y) = f(x) + f(y)$ [Mathematische Annalen, Bd. 60 (1905), pag. 459-463].

Il contributo portato in questo campo dai risultati del n° 9, è la costruzione della più generale soluzione discontinua ed univocamente invertibile (nel campo reale) dell'equazione funzionale (8); e l'aver precisato che *la potenza della base hameliana è quella del continuo.*

11. Prendiamo l'insieme dei numeri reali positivi (zero escluso) ed interpretiamolo come un gruppo moltiplicativo G (rispetto all'ordinaria operazione di moltiplicazione). La base (14) che possiamo determinare per questo gruppo avrà ancora la potenza del continuo (n° 9).

È quindi possibile stabilire una corrispondenza biunivoca tra questa base e la base hameliana (n° 10); ottenendo così un isomorfismo (n° 8) tra il gruppo G dei numeri positivi ed il modulo M dei numeri reali. Questo isomorfismo è espresso da un'equazione $y = f(x)$, in cui $f(x)$ soddisfa all'equazione funzionale (11), o inversamente alla (10).

Risulta dunque che le equazioni funzionali (10) o (11) ammettono come soluzioni oltre, come noto, funzioni esponenziali e logaritmiche, anche funzioni discontinue.

La soluzione discontinua da noi costruita è la più generale. Che essa sia discontinua, anzi nel senso più ampio che si può attribuire a questa parola, si può vedere nel seguente modo. Presi [nel caso della (10)] due elementi a, b di M e i due corrispondenti a', b' di G', purchè tali che

$$\begin{vmatrix} a & b \\ \log a' & \log b' \end{vmatrix} \neq 0,$$

manifestamente possibile per l'arbitrarietà della corrispondenza tra le due basi, il sistema di equazioni

$$\lambda a + \mu b = P$$
$$a'^{\lambda} b'^{\mu} = Q$$

dove P e Q sono due numeri arbitrari rispettivamente di M e G', ammetterà soluzioni reali λ_1 e μ_1. Scelti allora due numeri razionali λ e μ sufficientemente vicini a λ_1 e μ_1, ad un numero di M che differisce da P per meno di ε, corrisponderà un numero di G' che differisce da Q per meno di ε.

§ 3.

Sul grado di trascendenza di un corpo.

12. Sia C un corpo ed R il suo sottocorpo fondamentale. Come noto R è un corpo isomorfo o al corpo dei numeri razionali o al corpo delle classi mod p.

Si dice *base algebrica* del corpo un insieme di elementi di C

$$V = \{a_1, a_2, \ldots, a_\nu, \ldots\} \tag{18}$$

tale che ogni elemento di C dipenda algebricamente in R da V (cioè sia radice di un'equazione algebrica coi coefficienti funzioni razionali in R di elementi di V); mentre ciò non accada per alcun elemento a_ν di V rispetto all'insieme $V - a_\nu$. L'esistenza per ogni corpo di una base algebrica si dimostra ricorrendo al Wohlordnungssatz. Basta perciò attribuire a V ogni elemento a di C che non dipende algebricamente dalla sezione $S(a)$ [6]).

13. Vale il seguente teorema: Due basi algebriche di un medesimo corpo hanno ugual potenza.

La dimostrazione di questo teorema per basi non finite, sia quella originaria dello STEINITZ [7]) che una successiva della Sig.ª NOETHER, riferita da HAUPT [8]), sono notevolmente complesse. Ora con la formola (5) possiamo dimostrare un teorema più completo, del quale il precedente, sempre per basi non finite, è un immediato corollario, cioè:

La potenza di una base algebrica non finita di un corpo è uguale alla potenza del corpo stesso.

Infatti, sia $\mathfrak{m}$ la potenza della base V. Calcoliamo dapprima la potenza del campo d'integrità $R[V]$, cioè dell'insieme di elementi che si ottengono come funzioni razionali intere, in R, di elementi di V.

Un elemento qualunque del campo d'integrità $R[V]$ si ottiene come somma di un numero finito di termini, ciascuno dei quali è il prodotto di un elemento di R per un numero finito di elementi di V; cioè con un'espressione del tipo (15), dove gli elementi u_i siano i diversi elementi u che si ricavano dalla (16) sostituendo agli u_i gli elementi della V: e in ambedue i casi gli elementi λ_i appartengano ad R e solo un numero finito di essi sia diverso da zero. Ora l'insieme degli elementi dati dalla (16) ha ancora la potenza $\mathfrak{m}$ (n° 9), e questa essendo dunque la potenza dell'insieme degli elementi u_i con cui attualmente si costruiscono le (15), la potenza dell'insieme degli elementi u da essa rappresentati, cioè del campo d'integrità $R[V]$, sarà ancora $\mathfrak{m}$.

L'insieme di tutti i polinomi in una variabile coi coefficienti in $R[V]$, ha la stessa potenza dell'insieme di tutti i sottoinsiemi finiti del campo $R[V]$; e poichè un'equa-

---

[6]) E. STEINITZ, *Algebraische Theorie der Körper* [Journal für die reine und angewandte Mathematik, Bd. 137 (1909), pag. 167-309], pag. 288 e segg.

[7]) Loc. cit. [6]).

[8]) O. HAUPT, *Einführung in die Algebra.* [Akademische Verlaggesellschaft, Leipzig (1929)], Bd. II, Kap. 26, 6.

zione algebrica di grado n ha nel corpo C al più n radici [9]), la potenza del corpo C sarà data dalla (5), cioè sarà ancora $\mathfrak{m}$.

La potenza della base algebrica di un corpo si dice anche grado di trascendenza del corpo. Possiamo quindi dire: *Il grado di trascendenza non finito di un corpo è uguale al numero cardinale del corpo.*

Padova, dicembre 1934-XIII.

U. MORIN.

9) O. HAUPT, loc. cit. [8]), Bd. I, pag. 257.