Estratto dall'Annuario del R. Istituto Tecnico di Piacenza, vol. VII (1932)

NOTERELLE DI MATEMATICA

I.

Divisibilità e Numeri primi.

Un'osservazione didattica.

La teoria elementare della divisibilità e dei numeri primi si presenta con grandissima sèmplicità se si ammette una o l'altra delle due proposizioni seguenti:

I) *Se un numero primo divide un prodotto, divide almeno uno dei suoi fattori.*

II) *Un numero non primo si scompone in un* unico *prodotto di fattori primi.* [1].

Può essere conveniente mettere in rilievo che si può dimostrare la proposizione I) *senza premettere la teoria del M. C. D.* come si fa nella generalità dei libri di testo; osservazione questa che avvalora teoricamente e didatticamente il procedimento su accennato.

Per dimostrare la prop. I) basterà considerare un prodotto di due soli fattori, essendo immediata la estensione da n ad $n+1$.

---

[1] Vedi ad esempio: A. SAINTE-LANGUË, *Introd. au cours de Mathêm. élémentaires,* Paris 1913, pag. 21 e seg.; F. MORRA, *Matematica per la Maturità scientifica,* Ed. Porta, Milano-Piacenza, pag. 94 e seg. Il primo autore ammette la proposizione I) mentre il secondo ammette la II).

Si procede per assurdo. Il numero primo p divida il prodotto ab, senza dividere nè a, nè b. Distingueremo i due casi:

1) $a < p$. Considero tutti i prodotti di due fattori di cui il 1° sia $\leqq a$ e il 2° é b, e cioè $1b, 2b, 3b, \ldots\ldots ab$; e tra essi sia $a'b$ *il più piccolo che è divisibile per* p; sarà

$$1 < a' < p;$$

dividendo p per a', sia q il quoziente ed r il resto; avremo

$$p = a' \cdot q + r, \qquad 0 < r < a',$$

e quindi

$$pb = a'b \cdot q + rb, \qquad 0 < rb < a'b;$$

segue che p, dividendo pb e $a'b \cdot q$, dividerebbe rb, *assurdo.*

2) $a > p$. Dividendo a per p, sia q' il quoziente ed r' il resto; avremo

$$a = p \cdot q' + r', \qquad 0 < r' < p,$$

e quindi

$$ab = pb \cdot q' + r'b, \qquad 0 < r'b < pb;$$

segue che p, dividendo ab e $pb \cdot q'$, dividerebbe $r'b$, ciò che è assurdo pel caso 1) essendo $r' < p$. -

Dalla proposizione I) si deduce facilmente la II); e poscia la condizione generale di divisibilità e le regole del M. C. D. e del m. c. m., riferite alla scomposizione dei numeri nel prodotto dei loro fattori primi.

Osserviamo in fine che il cosidetto Teorema fondamentale della divisibilità, cioè

III) *Se un numero divide un prodotto di due fattori, ed è primo con uno di questi, divide l'altro fattore,*

il quale generalmente serve per la dimostrazione delle proposizioni I) e II), risulta invece, con questo ordinamento, come una conseguenza immediata della II).

Invero, se n divide il prodotto ab, ed è primo con a, si avrà

$$ab = nq,$$

ed i fattori primi di n dovranno essere contenuti tutti in b, non comparendo in a; cioè n deve dividere b.

II.

Ancora sul principio d'identità dei polinomi nell'Algebra elementare.

Il principio d'identità di due polinomi interi in x equivale al principio (da cui si deduce) del polimonio identicamente nullo. Per semplicità mi riferirò qui a quest'ultimo principio, che ha due enunciati, dei quali il primo con l'ipotesi sovrabbondante e il secondo con l'ipotesi strettamente necessaria; e cioè:

I) Se un polinomio intero in x (scritto in forma ridotta) è nullo per ogni valore di x, esso ha tutti i suoi coefficienti eguali a 0.

II) Se un polinomio intero e di grado n in x è nullo per più di n valori di x, esso ha tutti i suoi coefficienti eguali a 0.

(A questi enunciati si suole anche dare la forma contronominale equivalente.)

Manifestamente la proposizione I è una conseguenza della II, ma può anche dimostrarsi direttamente.

Nei vecchi trattati la prop. I era omessa, o accettata senza dimostrazione, e la II veniva dimostrata (più o meno completamente) come conseguenza della regola della divisione dei polinomi.

Successiva preoccupazione di rigore fece premettere da alcuni trattatisti la dimostrazione della prop. I, che può ottenersi mostrando che un polinomio in x, con coefficienti non tutti nulli, ha il segno del suo termine di grado minimo o massimo secondochè si dànno ad x valori positivi abbastanza piccoli o abbastanza grandi (ARZELÀ, CATANIA, ecc. [1]). Con un procedimento fondato sul principio di induzione, il compianto G. SANNIA [2] diede della proposizione I una nuova dimostrazione che si trova riprodotta in vari testi (MARTINI, LEONCINI, CIPOLLA [3]).

La dimostrazione, diremo così, classica della prop. II, a cui abbiamo accennato, procede nel seguente modo:

Dalla regola di divisione dei polinomi interi si ricava la formula (gli indici delle lettere A, B, C ed R indicano i gradi in x dei polinomi)

(1) $$A_n(x) = B_m(x) \cdot C_{n-m}(x) + R_{m-1}(x), \text{ ove } n \geqq m,$$

dalla quale, facendo $B_m(x) = x - a$, si ottiene

(2) $$A_n(x) = (x-a) \cdot C_{n-1}(x) + R_0\,;$$

e in questa facendo $x = a$, si ha $A_n(a) = R_0$, e quindi

(3) $$A_n(x) = (x-a) \cdot C_{n-1}(x) + A_n(a)\,;$$

sicchè sarà

(4) $$A_n(x) = (x-a) \cdot C_{n-1}(x) \quad \text{per} \quad A_n(a) = 0.$$

La deduzione successiva della proposizione II non presenta alcuna difficoltà. Se $A_n(x)$, non avente tutti i suoi coefficienti eguali a 0, si annulla per n valori di x: $a_1, a_2, \ldots a_n$, esso è divisibile per $(x-a_1)(x-a_2)\ldots(x-a_n)$, e si ha

$$A_n(x) = (x-a_1)(x-a_2)\ldots(x-a_n) \cdot C_0\,,$$

ove C_0 è indipendente da x e diverso da 0. Segue che $A_n(x)$ non può annullarsi per altri valori di x.

Ora, sulla deduzione delle formule (1), (2), (3), (4), scritte sopra, si avanzarono le seguenti critiche:

(1) C. ARZELÀ, *Algebra elementare* (ho sott'occhio la 3ª ed. del 1905); C. CATANIA, *Algebra elementare*, 1906 (fino alla 3ª ed. del 1910). Cfr. NICOLETTI E SANSONE, *Aritmetica ed Algebra*, vol. 1°, 1924, 2ª ed. 1932.

(2) Supplemento al Periodico di Matematica, Marzo 1902.

(3) A. MARTINI-ZUCCAGNI, *Algebra elementare* (ho sott'occhio la 4ª ed. del 1914); M. LEONCINI, *Aritmetica e Algebra*, 1916; CIPOLLA E MIGNOSI, *Analisi matem. elementare*, 1924; CIPOLLA E AMATO, *Algebra elementare*, 1926.

a) Nelle (1) e (2) i polinomi C ed R non rimangono individuati se non si premette la prop. II, che si vuol dimostrare, o almeno la prop. I.

b) Nella formula (2) non si può porre $x = a$, giacchè allora il divisore diviene $a - a = 0$, e non può essere considerata una divisione col divisore nullo, sicchè non è legittima la deduzione delle formule (3) e (4).

Queste critiche, generalmente accolte, fecero cercare delle nuove dimostrazioni elementari della prop. II; non essendo escluso tuttavia che le nuove dimostrazioni siano state date per ragione di preferenza, e non per condanna della dimostrazione antica. Segnaliamo la dimostrazione esposta dal prof. PINCHERLE nella sua Algebra elementare [1], e quelle più recenti date dal prof. A. LA BARBERA [2].

Da altre parti si credette invece di introdurre delle varianti o dei complementi alla dimostrazione classica della prop. II: o premettendo la dimostrazione della prop. I, come già fu detto, o anche, dimostrando la (3) e la (4) indipendentemente della divisione dei polinomi (ARZELÀ, MARTINI, ENRIQUES [3]).

Nel mio insegnamento non credetti abbandonare la dimostrazione classica, perchè la trovavo sostanzialmente corretta, e didatticamente conveniente; e mi compiacqui pertanto quando da varie parti (PREDELLA, CIAMBERLINI, FAZZARI, CATANIA,..... [4]) furono fatte, in modo più o meno esplicito, le difese di quella dimostrazione, la quale appare rigorosa, senza necessità di varianti, per le seguenti ragioni:

(1) S. PINCHERLE, *Aritmetica generale e Algebra elementare*, 1911.

(2) Periodico di Matematica, Maggio 1926.

(3) ARZELÀ, MARTINI-ZUCCAGNI, loc. cit.; F. ENRIQUES, Periodico di Matem., Maggio 1930. Il procedimento dell'ARZELÀ si fonda sulla divisibilità di $x^n - a^n$ per $x - a$, ed è comunemente seguito. La dimostrazione dell'ENRIQUES è semplice ed elegante; cfr. AMALDI ED ENRIQUES, *Algebra elemetare*, vol. 1°, 1931.

(4) P. PREDELLA, *Algebra ed Aritmetica*, 1915; C. CIAMBERLINI, Suppl. al Periodico di Matem., fasc. I del 1916; G. FAZZARI è citato dal CATANIA nella 5ª ed. (1917) della sua *Algebra elementare*, ove segue la dimostrazione classica, rigorosamente esposta (n. 24 e 28).

a) Scrivendo le formule (1) e (2) s'intende che C ed R sono i polinomi, perfettamente individuati, che derivano dall'algoritmo della divisione dei polinomi interi A e B (senza che sia necessario premettere la prop. I).

b) L'algoritmo stesso, come viene svolto, è indipendente dai valori che si possono dare alla lettera x, e non è affatto escluso che sia $B = 0$.

Sono perciò sempre valide le formule (1), (2), (3), (4).

La convenienza didattica della dimostrazione classica è, secondo il mio parere, in questo, che essa risulta dal semplice collegamento di proposizioni elementari comuni, senza che sia necessario aggiungere alcun particolare procedimento dimostrativo.

Col mio articoletto pubblicato nel 1924 nel Periodico di Matematiche [1], senza pretesa di dir cose nuove e col pensiero di fare cosa utile alla Scuola, desiderai esporre pubblicamente la mia opinione, mettendo nello stesso tempo in rilievo che in un insegnamento elementare si può fare a meno dell'univocità di forma delle espressioni letterali e contentarsi dei risultati determinati che si ottengono.

Mi piace terminare la presente noticina, dirò così, critico-retrospettiva coll'esprimere un' opinione non condivisa generalmente dai nostri scrittori di trattati scolastici, che quasi tutti aspirano all'originalità — la quale è, invece, l'attributo essenziale della ricerca scientifica — e cioè:

La tradizione, anche nell'insegnamento, è una grande forza, e non deve essere abbandonata se non per raggiungere un reale, importante progresso.

EUGENIO MACCAFERRI

---

[1] Periodico di Matem., serie 4ª, vol. IX, n. 3, Maggio 1924; cfr. vol. VI di questo Annuario (1931).

Stampa

Chiar.mo Prof. Giuseppe Peano

Via Barbaroux, 4

Torino

R. ISTITUTO TECNICO "G. D. ROMAGNOSI" ~ PIACENZA ~