Bollettino
Unione Matematica Italiana

Francesco Cecioni

Alcune osservazioni sulla teoria della divisibilità.

Bollettino dell'Unione Matematica Italiana, Serie 3, Vol. **10** (1955), n.3, p. 382–400.

Zanichelli

<http://www.bdim.eu/item?id=BUMI_1955_3_10_3_382_0>

SEZIONE STORICO-DIDATTICA

Alcune osservazioni sulla teoria della divisibilità.

Nota di FRANCESCO CECIONI (a Pisa)

Sunto. - *È contenuto nel n. 1.*

Premesse.

1. La teoria della divisibilità dei polinomi in più variabili viene trattata usando fin da principio il concetto di polinomio irriducibile, in modo quindi che dipende dal campo sul quale i polinomi vogliono considerarsi. Ed anche le condizioni generali di validità della teoria ordinaria della divisibilità vengono sintetizzate nel fatto che il campo d'integrità sia a fattorizzazione unica, ponendo quindi in primo piano il concetto di elemento primo (indecomponibile).

Le osservazioni che qui mi permetto di esporre sono sorte dal proposito di trattare, invece, in modo indipendente dal concetto di elemento primo tutte quelle proprietà di divisibilità che nel fatto non ne dipendono, dividendo così la teoria in due parti: la prima parte che contiene le proprietà che non dipendono dal concetto di elemento primo; la seconda che contiene quelle che ne dipendono essenzialmente.

Questa trattazione sembra più opportuna anche perchè, come sarà visto, esistono campi di integrità nei quali vale la prima parte della teoria, ma non la seconda.

Lo scopo viene raggiunto mediante la semplice osservazione del n. 5 *a*), e, per quanto riguarda i polinomi, con lo studio di questi su un campo di integrità, basato sul noto teorema di GAUSS, la dimostrazione del quale viene opportunamente modificata conformemente allo scopo.

Mi permetto notare che le presenti osservazioni sono state da me esposte da vari anni nei Corsi di *Matematiche Complementari*

all'Università di Pisa; anzi, eccetto quelle dei nn. 20, 21, 22, esse si trovano in miei Corsi litografati degli anni 1938-39 e 1942-43, Corsi citati dall'amico G. Ascoli, che ringrazio cordialmente (*).

2. È opportuno, considerato lo scopo sostanzialmente didattico di questo articolo (e ciò spiega qualche lungaggine che vi compare), richiamare sommariamente i concetti di *campo* (*field*) e di *campo di integrità*. Essi saranno richiamati, per comodità, in modo logicamente sovrabbondante: in qualsiasi testo, che tratti di algebra moderna, possono trovarsi questi concetti definiti mediante le loro proprietà logicamente indipendenti.

Un **campo** è un insieme di elementi tali che:

1. - È definita una relazione che ha per soggetto due elementi qualisivogliono del campo, e che, per due elementi determinati, può essere verificata o no; essa è riflessiva, simmetrica, transitiva. Questa relazione è chiamata *eguaglianza*. Esistono nel campo almeno due elementi diseguali.

2. - Sono definite due operazioni univoche, dette rispettivamente *addizione* e *moltiplicazione*, ciascuna delle quali applicata ad un insieme qualunque (finito) di elementi del campo dà un elemento del campo, detto rispettivamente *somma* e *prodotto*. Somme (prodotti) di elementi rispettivamente eguali sono eguali. Le due operazioni godono delle solite proprietà formali: ciascuna è associativa e commutativa; la moltiplicazione è distributiva rispetto all'addizione.

3. - Esistono, univocamente determinati, due elementi, *zero* ed *uno*, con le solite proprietà:

$x + 0 = x$, $x \cdot 1 = x$, $x \cdot 0 = 0$ per ogni x del campo;
da $ax = 0$, $a \neq 0$, segue $x = 0$.

4. - Esiste ed è unica la *differenza* $a - b$, essendo a e b due elementi qualunque del campo. Definito $-a = 0 - a$, ne risulta $-a = (-1) \cdot a$, e si hanno tutti gli usi formali del segno $-$, pur potendo non esservi una distinzione di elementi positivi e negativi.

5. - Esiste ed è unico il *quoziente* $\frac{a}{b}$, essendo a e b due elementi qualunqe del campo, e $b \neq 0$.

Un **campo di integrità** è un insieme di elementi che soddisfa alle condizioni 1, 2, 3, 4 come sopra, ma invece della 5 è soddisfatta l'altra:

(*) Cfr. le pregevolissime *Lezioni di Matematiche Complementari* di G. Ascoli Fasc. II (Ed. Gheroni, Torino, 1954).

5_1. - *Non* per tutte le coppie di elementi a, b $(b \neq 0)$ esiste il quoziente $\frac{a}{b}$; quando esiste è però unico.

Invece di « campo di integrità » si suole anche dire, « dominio d'integrità ». È da notare però che si suol dare a questo concetto un contenuto diverso: la condizione 5 viene senz'altro soppressa, e non sostituita con la sua negazione 5_1; si lascia cioè indecisa la esistenza del quoziente. Con ciò i campi di integrità possono essere anche campi. Ma perchè la teoria della divisibilità abbia significato, occorre che non si tratti di campi. Perciò adotterò una nomenclatura proposta, verbalmente, dallo ZAPPA: dare il nome di **dominio di integrità** (come si fa comunemente) ad un insieme che soddisfi alle condizioni 1, 2, 3, 4 di sopra, lasciando indecisa l'esistenza del quoziente; e chiamare **campo di integrità** un dominio d'integrità nel quale valga la 5_1, cioè nel quale il quoziente non sempre esista, come appunto è stato detto sopra. Con ciò i domini di integrità si ripartiscono in due tipi: campi, e campi d'integrità. In questo articolo saranno sempre considerati campi di integrità, nel senso ora dichiarato.

È ben noto che un dominio d'integrità finito è un campo. Infatti, se $a_0 = 0, a_1, a_2, \ldots, a_n$ sono i suoi elementi, i prodotti $a_i a_0, a_i a_1, \ldots, a_i a_n$ $(i \neq 0)$ sono tutti distinti (propr. 3); essi sono perciò eguali rispettivamente (anche se non ordinatamente) agli elementi $a_0, a_1, \ldots, a_n$; esistono quindi tutti i quozienti $\frac{a_r}{a_i}$ $(r = 0, 1, \ldots, n)$. Dunque:

Un campo d'integrità (nel senso detto) *contiene infiniti elementi.*

È noto anche che *ogni campo di integrità I è contenuto in* (almeno) *un campo C,* nel senso che esiste in C un sottoinsieme isomorfo aritmeticamente ad I (1). *È anzi univocamente determinato, a meno di un isomorfismo aritmetico, il minimo campo che contiene I.* Esso si ottiene considerando le coppie (a, b), con $b \neq 0$, degli elementi di I, e definendo per esse una relazione (di eguaglianza) ed un calcolo, nel medesimo modo col quale dagli ordinari numeri interi si passa alle frazioni, col metodo appunto delle coppie.

Si noti infine che la condizione della esistenza della differenza (cond. 4ª di sopra) *non sarà adoperata nelle considerazioni generali sulla teoria della divisibilità.* Essa occorrerà solo nelle considerazioni riguardanti i polinomi.

(1) Si suole dire comunemente come è scritto sopra. Non mi sembra però che vi sia contraddizione logica a pensare gli elementi del detto sottinsieme addirittura identici agli elementi di I. Non ritengo, comunque, anche perchè irrilevante allo scopo, insistere su ciò.

La teoria della divisibilità ordinaria.

3. La teoria della divisibilità per i numeri interi (razionali) si svolge partendo dal processo di EUCLIDE per la ricerca del m.c.d.. Da esso segue che il m.c.d. di due numeri a, b, che sarà indicato con $D(a, b)$, è diviso da tutti i divisori comuni di a e b, e che è, per qualunque intero k, $D(ka, kb) = kD(a, b)$. Nel seguito della teoria il processo di EUCLIDE non è più adoperato [2].

Ora la seconda delle proprietà enunciate è conseguenza della prima (n. 5 *a*); non è perciò necessario dedurla dal processo di EUCLIDE. E la prima si assume, come è noto, come definizione del m.c.d., quando si opera in un campo di integrità qualsiasi. Appare perciò opportuno, tenendo presenti anche le osservazioni fatte al n. 1, prospettare le condizioni necessarie e sufficienti sotto le quali in un campo di integrità vale la ordinaria teoria della divisibilità, ed organizzare tale teoria, nel modo appunto che ora sarà esposto, senza presupporre dunque, in particolare, la validità del procedimento di EUCLIDE, nè di alcun procedimento analogo.

Tale modo rende possibile, ad es., una trattazione particolarmente semplice, almeno dal punto di vista logico, della teoria della divisibilità dei polinomi in più variabili, come sarà visto dopo.

4. Consideriamo un qualsiasi *campo di integrità;* i suoi elementi (a, b, ..., m, ...) potremo anche chiamarli numeri (o numeri interi). Non essendo possibile sempre la divisione (anche se il divisore è diverso da zero), nasce il problema della *divisibilità*. Le *proprietà formali della divisibilità* (se m divide a e b, divide $a \pm b$; se m divide a, divide ab; ecc.) sono conseguenze delle proprietà formali delle operazioni, e *valgono perciò in ogni campo di integrità.*

Si noti anche che se $km (\neq 0)$ divide kn, m divide n. Si ha infatti $kn = kmq$, e, per le propr. 3 e 4 dei campi di integrità (n. 2) e per le proprietà formali, $k(n - mq) = 0$, $n = mq$. Viceversa, se m divide n, km divide kn $(k \neq 0)$.

È noto che l'*unità* può avere, nel campo, divisori diversi da essa (ad es., -1 nel campo degli ordinari numeri interi relativi); *i divisori dell'unità* (diversi da essa) si chiamano le *unità secondarie* del campo. Sono ben note, e si dimostrano subito, le seguenti

[2] Esso può adoperarsi per dimostrare che, se è $D(a, b) = \delta$, l'equazione $ax + by = \delta$ è risolubile in numeri interi. Ma questo teorema è da riguardarsi appartenente all'analisi indeterminata piuttosto che alla teoria della divisibilità; esso infatti non vale ad es. (n. 18) per i polinomi in più variabili, pei quali valgono però tutti i teoremi della ordinaria teoria della divisibilità.

proprietà; il numero inverso di una unità è pure una unità; il prodotto e il quoziente di due unità sono ancora unità.

Due elementi del campo si dicono *associati* quando differiscono per un fattore unità. È noto, e si dimostra subito, che condizione necessaria e sufficiente perchè due elementi siano associati è che essi siano l'uno divisibile per l'altro. Si ha pure che: se a è divisibile per b, ogni associato ad a è divisibile per ogni associato a b. Ed anche: se è $m = abc\ldots$, e si sostituisce ad ogni fattore un associato, il nuovo prodotto è associato ad m.

Insomma *nel fatto della divisibilità e nella scomposizione in fattori, due numeri associati non vanno considerati come essenzialmente distinti, cioè ogni numero va considerato a meno di un fattore unità* (arbitrario o opportuno).

5. Def. – *Chiamasi* **massimo comune divisore** *di due, o più, elementi di un campo di integrità un elemento del campo che divide tutti gli elementi considerati ed è diviso da tutti i loro divisori comuni.*

Il m.c.d. di più elementi, ove esista, è unico (a meno di un fattore unità). Se infatti δ_1 e δ_2 sono due tali m.c.d., δ_1 divide δ_2 e δ_2 divide δ_1 (per la def. di sopra), e quindi δ_1 e δ_2 sono associati.

Quando in un campo d'integrità accade che *due elementi qualunque* del campo, non ambedue nulli, ammettono il m.c.d., diremo brevemente che *nel campo esiste il m.c.d.*.

Teorema I. – *Condizione necessaria e sufficiente perchè in un campo di integrità valga tutte la prima parte della teoria della divisibilità ordinaria* (cioè tutta la parte indipendente dal concetto di elemento primo), *è che esista nel campo il m.c.d.*

Sarà precisato maggiormente che cosa va inteso con « prima parte della teoria della divisibilità ordinaria ».

La condizione è intanto, manifestamente, necessaria. Dimostriamone la sufficienza. Dimostriamo perciò che dalla ipotesi della esistenza del m.c.d. di due elementi qualunque seguono successivamente le proprietà appresso indicate.

a) Si ha (con $a \neq 0$, $b \neq 0$, $k \neq 0$, del resto qualunquesiano)

$$D(ka,\ kb) = kD(a,\ b). \tag{1}$$

Il m.c.d. di ka e kb è divisibile per k (per la def.); poniamo allora

$$D(ka,\ kb) = kd' \quad \text{e} \quad D(a,\ b) = d. \tag{2}$$

Ora, kd' divide ka e kb; quindi d' divide a e b (n. 4), e quindi, per la def. di m.c.d., d' divide d.

D'altra parte d divide a e b; quindi kd divide ka e kb (n. 4), e perciò divide anche kd'; allora d divide d'.

Dunque d e d' si dividono mutuamente, e perciò (n. 4) differiscono per un fattore unità; dalle (2) segue allora la (1).

Da questa segue poi che se h è un divisore comune di a e b, si ha

$$D\left(\frac{a}{h}, \frac{b}{h}\right) = \frac{D(a, b)}{h}.$$

b) *Se* m *divide il prodotto* ab, *ed è* D(m, a) = 1, m *divide* b.

Vale la ben nota dimostrazione: $D(mb, ab) = b$; m divide mb ed ab; quindi divide b. È questo, come è noto, il teorema base della ordinaria divisibilità.

c) *Se un numero* m *è primo con ciascun fattore di un prodotto* abc ..., *è primo col prodotto. E viceversa.*

1° - Se fosse $D(m, abc\ldots) = \delta \neq 1$, δ, dividendo m, dovrebbe essere primo con a, con b, con c, ... per l'ipotesi; allora, per b), δ dovrebbe dividere $bc\ldots$, e quindi dovrebbe dividere $c\ldots$. E così di seguito; si cade in contraddizione.

2° - Se m non fosse primo, ad es., con a, i divisori (diversi dell'unità) comuni ad m e ad a dividerebbero m ed $abc\ldots$

d) *Se ogni* $a_i (i = 1, 2 \ldots r)$ *è primo con ogni* $b_j (j = 1, 2 \ldots s)$, *il prodotto* $a_1 a_2 \ldots a_r$ *è primo con* $b_1 b_2 \ldots b_s$. *E viceversa.* La prima parte si ottiene applicando ripetutamente *c*); la seconda si ottiene come la seconda parte di sopra.

e) *Se è* $D(a, b) = 1$, *è anche* $D(a^r, b^s) = 1$.

f) *Se* N *è divisibile per ciascun* $a_i (i = 1, 2 \ldots r)$, *e questi sono primi tra loro due a due,* N *è divisibile per* $a_1 a_2 \ldots a_r$.

Infatti: $N = a_1 q$; a_2, per b), divide q; $N = a_1 a_2 q' = (a_1 a_2) q'$; e così di seguito.

Def. - *Chiamasi* **minimo comune multiplo** (*m. c. m*) *di due o più elementi* a, b, c ... *(non nulli) di un campo di integrità un elemento del campo che è multiplo di tutti questi elementi, e del quale è multiplo ogni multiplo comune degli elementi stessi.* Sarà indicato con $M(a, b, c\ldots)$, e sarà sottinteso che nessuno dei numeri $a, b, c\ldots$ sia zero. $M(a, b, c\ldots)$, ove esista, è unico (a meno di un fattore unità); ciò si dimostra come per il m.c.d.. L'esistenza e le proprietà seguono delle proprietà di sopra, come ora vediamo.

g) *Esiste* M(a, b), *ed è dato da* $\frac{ab}{D(a, b)}$. Vale la ben nota dimostrazione qui riassunta. Sia m un multiplo comune qualsiasi di a e b, e poniamo $\delta = D(a, b)$. Si ha $m = aq_1$, $m = bq_2$, $a = \delta a_1$,

$b = \delta a_2$, $D(a_1, a_2) = 1$; quindi $m = \delta a_1 q_1 = \delta a_2 q_2$, $a_1 q_1 = a_2 q_2$, e (per b) $q_1 = a_2 q$, onde $m = \delta a_1 q_1 = \delta a_1 a_2 q$, cioè m multiplo di $\delta a_1 a_2$. Ma è $\delta a_1 a_2 = \frac{ab}{\delta} = a\frac{b}{\delta} = b\frac{a}{\delta}$, cioè $\delta a_1 a_2$ è multiplo comune di a e b. Ne segue l'asserto.

E si hanno le proprietà

$$M(ka, kb) = kM(a, b) \quad , \quad M\left(\frac{a}{h}, \frac{b}{h}\right) = \frac{M(a, b)}{h}.$$

h) Esistenza e proprietà del m.c.d. e del m.c.m. di più di due elementi. Dimostrazione nel modo noto.

Così il TEOR. I è dimostrato. La « prima parte della teoria della divisibilità », cioè la parte indipendente dal concetto di « numero primo » (ossia indecomponibile), è costituita dal complesso delle proprietà elencate (e, naturalmente, da quelle che seguono da esse e dalle proprietà generali dei campi di integrità).

6. Diremo che *un campo d'integrità è a scomposizione limitata* quando ogni elemento (non nullo) del campo è scomponibile nel prodotto di un numero finito di fattori primi, cioè indecomponibili nel campo. S'intende (v. n. 4) che gli eventuali fattori unità non vanno contati nel numero dei fattori; così se p è primo, ed è $p = ab$, uno dei due fattori a o b sarà un'unità, e l'altro sarà associato a p.

TEOREMA II. – *Condizione necessaria e sufficiente perchè in un campo di integrità, nel quale esiste il m.c.d., valga anche la seconda parte della teoria della divisibilità ordinaria* (cioè la parte dipendente essenzialmente dal concetto di elemento primo), *è che il campo sia a scomposizione limitata.*

La necessità è chiara. Per la sufficienza si noti che due elementi primi diversi (e cioè non associati) sono primi tra loro; allora dal n. 5 *b*) segue immediatamente *l'unicità della scomposizione* di un elemento qualunque in un prodotto di elementi primi; tale unicità, s'intende (v. n. 4), sussiste a meno della sostituzione dei fattori con fattori associati, e della introduzione di fattori unità. Dall'unicità della scomposizione segue immediatamente il criterio generale di divisibilità di un numero per un altro, dedotto dalla scomposizione in fattori primi; e quindi la formazione del m.c.d. e del m.c.m. mediante la scomposizione in fattori primi; ecc.. E questa è appunto la seconda parte della teoria della divisibilità ordinaria.

7. Segue da quanto sopra che la condizione necessaria e sufficiente perchè in un campo di integrità valga *tutta* la teoria della divisibilità ordinaria è che in esso valgano insieme le due proprietà:

1ª *Esistenza del m. c. d.*

2ª *Scomponibilità limitata.*

È immediatamente chiaro che queste due condizioni possono sintetizzarsi, come spesso viene fatto, nell'unica:

Il campo sia a scomposizione (o fattorizzazione) *unica.*

Questo enunciato sintetico non permette però di analizzare la portata separata delle condizioni 1ª e 2ª di sopra (cfr. n. 1 e n. 20).

8. È opportuno anche ricordare quanto segue. La validità del procedimento di EUCLIDE (o di un procedimento analogo) per la ricerca del m. c. d. non è dunque (come è ben noto) condizione necessaria perchè valga la teoria della divisibilità. È pure ben noto che quando in un campo di integrità I un tale procedimento vale, allora è risolubile nel campo I l'equazione di analisi indeterminata (n. 3, nota (1))

$$ax + by = D(a, b), \tag{1}$$

qualunque siano a e b in I.

Si consideri ora un campo d'integrità I e un altro campo d'integrità I_1 più ampio, che contenga I. Se a e b sono elementi di I, ed è $\delta = \mathrm{D(a, b)}$ *in* I, *ciò non sarà vero in generale in* $\mathrm{I_1}$; può darsi anche che in I_1 il $D(a, b)$ non esista (3). Ma se in I esistono due elementi x, y che verificano la (1), allora è $\delta = D(a, b)$ anche in I_1 (v. l. c.); infatti ogni divisore comune ad a e b in I_1 divide δ, per la (1).

Insomma il m. c. d. di due elementi a, b non è, in generale, invariante rispetto al campo di integrità nel quale i due elementi possono essere considerati. Ma se in un campo d'integrità I esiste il m. c. d., ed inoltre l'equazione (1) è sempre risolubile (in particolare, dunque, se vale un procedimento di EUCLIDE), allora il m. c. d. di due elementi qualunque di I rimane lo stesso (a meno dei fattori unità) in qualunque campo d'integrità I_1 che contenga I.

Polinomi in una indeterminata su un campo di integrità.

9. - Consideriamo dapprima un *campo*.

La classe dei polinomi in una indeterminata costruiti su un

(3) A. A. ALBERT, *Modern higher Algebra*, Cambridge, University presse, 1938, p. 31.

campo (cioè aventi i coefficienti in tale campo) *costituisce un campo d'integrità.*

La cosa è ben nota, e di immediata dimostrazione. Va ricordato però che *se il campo è finito* (cioè costituito da un numero finito di elementi), *i polinomi su esso vanno considerati esclusivamente secondo il concetto formale*; *se invece il campo è infinito, possono essere considerati indifferentemente sia secondo il concetto formale che secondo quello funzionale.*

Questa avvertenza si riferisce non solo all'enunciato di sopra, ma a tutta la teoria dei polinomi. La ragione della distinzione indicata tra il caso del campo finito e quello del campo infinito risiede nel *principio di identità*, che domina tutta la teoria dei polinomi, e dal quale dipende anche il fatto sopra enunciato.

Secondo il concetto formale, il principio di identità è vero per definizione.

Secondo il concetto funzionale, occorre distinguere: Se il campo è infinito, il principio di identità dei polinomi è un teorema che si dimostra, per qualunque campo, nel modo solito, ad es. mediante il teorema di KRAMER. Ma se il campo è finito, il teorema di identità dei polinomi è falso; ad es., se n è il numero degli elementi del campo, ogni elemento soddisfa all'equazione $x^n - x \equiv 0$. Ed è falso pure il fatto sopra enunciato; non vale, ad es., il teorema di annullamento del prodotto dei polinomi: $x(x^{n-1} - 1) \equiv 0$.

Le unità del campo di integrità, costituito dai polinomi (in una indeterminata) su un campo C, sono, come si vede subito, gli elementi di C pensati come polinomi di grado *zero*.

10. *Nel campo di integrità, costituito dai polinomi in una indeterminata su un campo, vale tutta la teoria della divisibilità ordinaria;* vale anzi il procedimento di EUCLIDE. La cosa è ben nota.

I polinomi su un campo C sono anche polinomi su qualunque altro campo C_1 che contenga il primo. Si noti al riguardo quanto segue. Valendo il procedimento di EUCLIDE, il m. c. d. di più polinomi si determina razionalmente mediante i coefficienti dei polinomi stessi; esso può essere poi moltiplicato per un elemento arbitrario, rispettivamente di C o di C_1, cioè per una unità del corrispondente campo di polinomi; e non vi è alcuna altra indeterminazione che questa. Ma il m. c. d. va considerato appunto a meno di un tale moltiplicatore; dunque il m. c. d. di più polinomi non dipende dal campo nel quale i polinomi possono essere considerati; e con esso non ne dipende il fatto che più polinomi siano o non siano primi tra loro, e non ne dipende l'applicazione

della prima parte della teoria della divisibilità. Ne dipende invece l'applicazione della seconda parte.

11. Dobbiamo ora considerare *la classe dei polinomi in una indeterminata costruiti su un campo d'integrità* (anzichè su un campo).

Sia I un campo di integrità; chiamiamo R il *campo minimo* che contiene 1 (n. 2). Consideriamo la classe dei polinomi (in una indeterminata) su I, che chiameremo P_I; e consideriamo insieme la classe dei polinomi (in una indeterminata) su R, che chiameremo P_R; la classe P_I è contenuta in P_R; i P_I sono i P_R « coi coefficienti interi ». Nella classe dei polinomi P_R vale il teorema di identità dei polinomi, perchè R (come I; v. n. 2) è infinito (v. n. 9); perciò tale teorema vale anche per i polinomi P_I. Dunque (n. 9) tanto i polinomi di P_I come quelli di P_R possono essere considerati indifferentemente secondo il concetto formale o secondo quello funzionale; diremo perciò indifferentemente « indeterminata » o « variabile ». È ben noto, e si vede subito (cfr. n. 9), che

I polinomi in una variabile su un campo d'integrità (cioè i polinomi P_I) *costituiscono un campo d'integrità.*

Dobbiamo studiare la teoria della divisibilità in tale campo P_I; essa è legata, come è chiaro, alla divisibilità nel campo I. *Le unità* del campo d'integrità P_I sono, come si vede subito, *le unità di* I, pensate come polinomi di grado *zero*.

12. *Ammettiamo che nel campo* I *esista il m. c. d.* (non occorre, dunque, che valga la seconda parte della teoria della divisibilità).

Consideriamo un polinomio $f(x)$ su I, cioè della classe P_I; si chiama *divisore* del polinomio $f(x)$ il m. c. d. dei suoi coefficienti. Un polinomio su I si dice *primitivo* quando ha il divisore 1.

Un polinomio f(x) *di* P_I che abbia il divisore φ può dunque mettersi nella forma

$$f(x) = \varphi f_1(x),$$

con φ numero di I e $f_1(x)$ polinomio di P_I primitivo.

Un polinomio f(x) *di* P_R può mettersi nella forma

$$f(x) = \frac{\alpha}{\beta} f_1(x)$$

con α e β numeri di I e $f_1(x)$ polinomio di P_I primitivo. Basta ridurre i coefficienti di $f(x)$ ad un comune denominatore, portare questo in evidenza, e applicare poi l'osservazione precedente. È chiaro che α e β possono supporsi primi tra loro.

Dimostriamo ora i tre noti teoremi di GAUSS, che qui vengono dimostrati sotto la sola ipotesi della esistenza del m. c. d. in I.

13. TEOREMA I (*di* GAUSS). - *Se in un campo d'integrità* I *esiste il m. c. d., il prodotto di due polinomi su* I *primitivi è pure primitivo.*

Siano

$$f(x) = a_0 + a_1x + \ldots + a_nx^n \quad , \quad g(x) = b_0 + b_1x + \ldots + b_mx^m$$

i due polinomi, e poniamo

$$f(x)g(x) = c_0 + c_1x + \ldots + c_{m+n}x^{m+n}.$$

Sarà

$$\begin{aligned}
c_0 &= a_0b_0 \\
c_1 &= a_0b_1 + a_1b_0 \\
c_2 &= a_0b_2 + a_1b_1 + a_2b_0 \\
c_3 &= a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0 \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
c_m &= a_0b_m + a_1b_{m-1} + a_2b_{m-2} + a_3b_{m-3} + \ldots \\
c_{m+1} &= a_1b_m + a_2b_{m-1} + a_3b_{m-2} + \ldots \\
c_{m+2} &= a_2b_m + a_3b_{m-1} + \ldots \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

È chiara la legge di formazione delle successive colonne. Dimostriamo il teorema per assurdo. c_0, c_1 ... c_{m+n} abbiano un m. c. d. diverso da 1. Consideriamo i numeri c_0, c_1, ..., c_{m+n}. a_0: può darsi che anch'essi abbiano un m. c. d. diverso da 1; consideriamo allora c_0, c_1, ..., c_{m+n}, a_0, a_1: può darsi che anch'essi abbiano un m. c. d. diverso da 1; ma ciò non potrà accadere fino all'insieme c_0, c_1, ..., c_{m+n}, a_0. ..., a_n, perchè $f(x)$ è primitivo. Dovrà dunque accadere che sia, ad es., per fissare le idee:

$$D(c_0.\ c_1, \ldots, c_{m+n}, a_0, a_1) = \delta \neq 1 \tag{1}$$

$D(c_0, c_1, \ldots, c_{m+n}, a_0, a_1, a_2) = 1$; e quindi

$$D(\delta, a_2) = 1. \tag{2}$$

Guardiamo allora, nel quadro di sopra, la 3ª colonna dei termini dei secondi membri; cominciamo dal 1° termine a_2b_0 di questa colonna; dalla 3ª riga del quadro, per (1), risulta che δ divide a_2b_0; quindi, per (2), δ *divide* b_0. Ma allora, passando alla successiva riga (la 4ª), risulta che δ divide a_2b_1, e. per (2), δ *divide* b_1. Così continuando, risulta che δ divide tutti i coefficienti b_0, b_1, ..., b_m, il che è contro l'ipotesi.

COROLLARIO. - *Se in un campo d'integrità* I *esiste il m. c. d., il divisore del prodotto di due polinomi su* I *è il prodotto dei divisori dei fattori.*

Vale la dim. ordinaria. Sia $f(x)g(x) = l(x)$; con le notazioni ed osservazioni del n. 12, poniamo $f(x) = \varphi f_1(x)$, $g(x) = \gamma g_1(x)$, $l(x) = \lambda l_1(x)$; avremo

$$\varphi\gamma[f_1(x)g_1(x)] = \lambda l_1(x).$$

Poichè il prodotto $f_1(x)g_1(x)$ è primitivo (TEOR. I), risulta $\varphi\gamma$ divisore del primo membro, λ divisore del secondo, e quindi, per il principio di identità, $\lambda = \varphi\gamma$, c. d. d.

14. TEOREMA II (di GAUSS). - *Supposto che in un campo d'integrità* I *esista il m. c. d., se un polinomio* f(x) *su* I *è scomponibile in fattori in* P_R, *è scomponibile anche in* P_I.

Vale la dim. ordinaria. Sia $f(x) = g(x)q(x)$, g e q in P_R; poniamo (n. 12)

$$f(x) = \varphi f_1(x) \quad , \quad g(x) = \frac{\alpha}{\beta} g_1(x) \quad , \quad q(x) = \frac{\gamma}{\delta} q_1(x);$$

avremo

$$\varphi f_1(x) = \frac{\alpha\gamma}{\beta\delta} g_1(x)q_1(x) \quad , \quad \beta\delta\varphi f_1(x) = \alpha\gamma g_1(x)q_1(x),$$

$$\beta\delta\varphi = \alpha\gamma \quad , \quad \frac{\alpha\gamma}{\beta\delta} = \varphi \quad , \quad f(x) = \varphi f_1(x) = \varphi g_1(x)q_1(x),$$

che dimostra l'asserto.

15. TEOREMA III (*di* GAUSS). - *Supposto che in un campo d'integrità* I *esista il m. c. d., se un polinomio* f(x) *su* I *è divisibile, in* P_R, *per un polinomio* g(x) *su* I *primitivo, allora* f(x) *è divisibile per* g(x) *anche in* P_I (cioè il quoziente ha necessariamente i coefficienti interi).

In breve: *Per i polinomi di* P_I *la divisibilità in* P_R *porta la divisibilità in* P_I *se il divisore è primitivo* (altrimenti è chiaro che la cosa può non valere: nel caso elementare $x - 1$ è divisibile per $2x - 2$ in P_R, non in P_I).

Vale la dim. ordinaria, analoga, del resto, alla precedente.

16. Ciò premesso, si risolve facilmente il problema della divisibilità in P_I. Si ha il

TEOREMA. - *Se in un campo d'integrità* I *esiste il m. c. d., questo esiste anche nel campo d'integrità* P_I *costituito dai polinomi in una indeterminata coi coefficienti in* I. *E se inoltre* I *è a scomposizione limitata, tale è anche* P_I.

In altre parole: Se in I vale la prima parte della teoria della divisibilità, essa vale anche in P_I; e se in I vale anche la seconda parte, altrettanto accade in P_I.

PRIMA PARTE. - Valgono intanto in P_I i teoremi di GAUSS; se ne deducono le conseguenze che seguono.

a) Condizione necessaria e sufficiente affinchè, essendo $f(x)$ e $g(x)$ due polinomi di P_I, sia $f(x)$ divisibile per $g(x)$ in P_I, è che, posto, secondo il n. 12, $f(x) = \varphi f_1(x)$, $g(x) = \gamma g_1(x)$, sia insieme φ divisibile per γ (in I) e $f_1(x)$ per $g_1(x)$. La sufficienza è chiara. Per la necessità si osservi che se è $f(x) = g(x)q(x)$ e si pone, secondo il n. 12, $q(x) = \lambda q_1(x)$, si ha $\varphi f_1(x) = \gamma\lambda g_1(x)q_1(x)$, onde (come varie volte sopra) $\varphi = \gamma\lambda$ e $f_1(x) = g_1(x)q_1(x)$, c. d. d.

b) *m. c. d. di due polinomi primitivi.* Siano $f_1(x)$, $g_1(x)$ due polinomi primitivi di P_I. Poniamo (n. 10)

$$D[f_1(x),\ g_1(x)] = d(x) \quad \text{in} \quad P_R;$$

sarà (n. 12) $d(x) = \frac{\alpha}{\beta} d_1(x)$, essendo $d_1(x)$ polinomio in P_I, primitivo. Poichè $\frac{\alpha}{\beta}$ è una unità del campo d'integrità P_R (n. 9), si ha anche

$$D[f_1(x),\ g_1(x)] = d_1(x) \quad \text{in} \quad P_R. \tag{1}$$

Dico che *questa eguaglianza è vera anche in* P_1.

Infatti intanto $d_1(x)$ divide $f_1(x)$ e $g_1(x)$ in P_R; ma $d_1(x)$ è primitivo; dunque (TEOR. III di GAUSS) $d_1(x)$ divide $f_1(x)$ e $g_1(x)$ anche in P_I.

Inoltre: sia $l(x)$ un polinomio di P_I che divide $f_1(x)$ e $g_1(x)$ in P_I; essendo $f_1(x)$ e $g_1(x)$ primitivi (basterebbe fosse tale uno di essi), anche $l(x)$ è primitivo, pel COR. del n. 13. Ora $l(x)$ divide $f_1(x)$ e $g_1(x)$ anche in P_R; perciò, per la (1), $l(x)$ divide $d_1(x)$ in P_R; ma $l(x)$ è primitivo; quindi (TEOR. III di GAUSS) $l(x)$ divide $d_1(x)$ anche in P_I. L'asserto è così dimostrato; si ha dunque

$$D[f_1(x),\ g_1(x)] = d_1(x) \quad \text{anche in} \quad P_I;$$

e quanto sopra dà la regola per trovare questo m. c. d.

c) *m. c. d. di due polinomi qualunque.* Siano $f(x)$, $g(x)$ due qualunque polinomi di P_I; poniamo, col solito significato,

$$f(x) = \varphi f_1(x) \quad , \quad g(x) = \gamma g_1(x);$$

segue subito, da *a*), che è in P_I

$$D[f(x),\ g(x)] = D(\varphi,\ \gamma) \cdot D[f_1(x),\ g_1(x)],$$

dove, naturalmente, $D(\varphi, \gamma)$ è un numero di I, e $D[f_1(x), g_1(x)]$ il polinomio di P_I, primitivo, determinato in *b*). La prima parte del teorema è dimostrata.

SECONDA PARTE. - Consideriamo un polinomio qualunque di P_I, $f(x) = \varphi f_1(x)$. I numeri primi di I, pensati come polinomi di P_I di grado zero, sono pure primi in P_I. Per l'ipotesi che I sia a scomposizione limitata, φ è allora scomponibile in un numero finito di fattori primi (di grado zero) in P_I.

Se $f_1(x)$ non è primo in P_I, è scomponibile in un prodotto di fattori che sono primitivi (n. 13, COR.); quindi i « fattori numerici » non subiscono variazioni per la scomposizione di $f_1(x)$; e tale scomposizione è limitata perchè i gradi dei polinomi fattori sono minori del grado del prodotto.

OSSERVAZIONE. - Il teorema è così dimostrato; e la 1ª parte della dim. dà anche un procedimento da seguire per la determinazione del m. c. d. di due polinomi. Non può però qui ripetersi l'osservazione del n. 10 riguardo alla indipendenza del m. c. d. dal campo, che qui è invece un campo *di integrità* I. Infatti nel procedimento indicato compaiono ricerche di m. c. d. in I, e non essendo stata fatta su I alcuna particolare ipotesi, oltre quella dell'esistenza del m. c. d., non è assicurata la invarianza del m. c. d. rispetto al variare del campo I (v. n. 8).

La divisibilità pei polinomi in più indeterminate.

17. *La classe dei polinomi in più indeterminate costruiti su un* **campo** *costituisce un campo di integrità.*

OSSERVAZIONE - Anche qui, come al n. 9, se il campo è finito, i polinomi vanno considerati esclusivamente dal punto di vista formale; se il campo è infinito, possono esser considerati sia formalmente che funzionalmente.

Considerando i polinomi dal punto di vista formale, la dimostrazione dell'enunciato è immediata, come per i polinomi in una indeterminata, e si vale del principio di identità dei polinomi (v. n. 9). Se i polinomi vogliono considerarsi secondo il concetto funzionale, ed il campo è infinito, si dimostra subito in modo noto, per induzione rispetto al numero delle variabili, il teorema di identità, dopo di che la dimostrazione va come sopra. Se il campo è finito, il teorema non vale se si considerano i polinomi dal punto di vista funzionale, perchè già non vale per il caso di una sola indeterminata.

Le unità del campo di integrità costituito dai polinomi in più indeterminate su un campo C sono i numeri di C pensati come polinomi di grado zero.

18. TEOREMA. - *Nel campo di integrità, costituito dai polinomi in più indeterminate su un campo, vale tutta la teoria della divisibilità ordinaria.*

Il teorema è vero per il caso di una indeterminata (n. 10); dimostriamolo allora per induzione, ammettendolo vero per $n-1$ indeterminate.

Sia C il campo sul quale i polinomi considerati sono costruiti; chiamiamo $P_C(x_1, x_2, \ldots, x_n)$ il campo d'integrità costituito dai polinomi su C nelle indeterminate $x_1, x_2, \ldots, x_n$. Ogni tale polinomio può ordinarsi rispetto, ad es., a x_n, ed allora i polinomi di $P_C(x_1, x_2, \ldots, x_n)$ si presentano come polinomi nella sola indeterminata x_n costruiti sul campo d'integrità $I \equiv P_C(x_1, x_2, \ldots, x_{n-1})$; viceversa, ogni tale polinomio è un polinomio di $P_C(x_1, x_2, \ldots, x_n)$. Ora in I vale, per la ipotesi fatta, tutta la teoria della divisibilità ordinaria; quindi (n. 16) essa vale anche in $P_C(x_1, x_2, \ldots, x_n)$, c. d d.

Come si vede, la dimostrazione è contenuta nel teorema generale del n. 16.

La dimostrazione del n. 16 dà anche il modo di trovare il m. c. d. di due polinomi $f(x_1, x_2, \ldots, x_n)$, $g(x_1, x_2, \ldots, x_n)$ in più indeterminate; esso si trova mediante un certo numero di procedimenti di EUCLIDE e di altre operazioni razionali; perciò i coefficienti del m. c. d. di f e g si esprimono razionalmente mediante i coefficienti di f e g stessi. Perciò il m. c. d. di più polinomi non dipende dal campo nel quale i polinomi detti possono essere considerati, ecc., come è stato osservato al n. 10 pei polinomi in una indeterminata.

Il m. c. d. di due polinomi in più indeterminate *non può però trovarsi* (almeno in generale) *mediante un solo procedimento di* EUCLIDE, (o procedimento analogo). Si considerino infatti i due polinomi x^2+y^2, x^2-y^2 primi tra loro; se il loro m. c. d., che è una costante $c \neq 0$, si potesse trovare mediante un solo procedimento di EUCLIDE (o analogo ad esso), esisterebbero due polinomi $X(x, y)$, $Y(x, y)$ pei quali si avrebbe identicamente (cfr. nota (2) al n. 3)

$$(x^2+y^2)X(x, y)+(x^2+y^2)Y(x, y) \equiv c,$$

e ciò è assurdo (basta fare, ad es., $y=0$).

19. Consideriamo ora (cfr. n. 11) *la classe dei polinomi in più indeterminate costruiti su un campo di integrità* (anzichè su un

campo). Per le ragioni dette al n. 11, e ricordando anche il n. 17, tali polinomi possono essere considerati indifferentemente dal punto di vista formale e da quello funzionale; e si vede subito (ed è ben noto) che

I polinomi in più indeterminate su un campo di integrità costituiscono un campo di integrità.

Le *unità* di tale campo sono quelle indicate al n. 11.

Si estende subito il teorema del n. 16:

TEOREMA. - *Se in un campo d'integrità* I *esiste il m. c. d., questo esiste anche nel campo d'integrità* $P_I(x_1, x_2, \ldots, x_n)$ *costituito dai polinomi in* n *indeterminate coi coefficienti in* I. *E se inoltre* I *è a scomposizione limitata, tale è anche* $P_I(x_1, x_2, \ldots, x_n)$.

Basta procedere per induzione ragionando come nella dim. del n. 18, prima per la prima parte, e poi per la seconda.

Vale anche qui, naturalmente, l'osservazione finale del n. 16.

Esempi di validità parziale della teoria.

20. Sia τ un numero trascendente reale. Consideriamo *l'insieme* I *dei numeri del tipo*

$$x_1\tau^{\xi_1} + x_2\tau^{\xi_2} + \ldots + x_h\tau^{\xi_h} \tag{1}$$

dove i coefficienti x_i sono, ad es., numeri razionali relativi qualunque, gli esponenti ξ_i numeri razionali *assoluti* qualunque (che possono essere supposti distinti), e il numero dei termini k è arbitrario (non fisso, dunque). Vediamo subito che l'insieme I è *un campo d'integrità.*

Gli elementi dell'insieme I sono numeri reali; intendiamo che l'eguaglianza, la addizione e la moltiplicazione in I siano rispettivamente l'eguaglianza, la addizione e la moltiplicazione dei numeri reali. Le proprietà 1, 2, 3, 4 della definizione di campo d'integrità (n. 2) sono allora senz'altro verificate; occorre dunque solo esaminare la proprietà 5_1 (n. 2).

Osserviamo perciò che l'espressione (1) di ogni numero di I, quando si suppongano (come supporremo) gli esponenti distinti due a due, è univocamente determinata (a meno, s'intende, dell'ordine dei termini); in altre parole dall'essere

$$x_1\tau^{\xi_1} + x_2\tau^{\xi_2} + \ldots + x_h\tau^{\xi_h} = 0, \tag{2}$$

nell'ipotesi fatta per gli esponenti, si deduce $x_1 = x_2 = \ldots = x_h = 0$.

Infatti, se riduciamo gli esponenti ad un medesimo denominatore n, e poniamo $\xi_i = \frac{n_i}{n}$, $\omega = \tau^{\frac{1}{n}}$, avremo da (2)

$$x_1\omega^{n_1} + x_2\omega^{n_2} + \ldots + x_k\omega^{n_k} = 0;$$

e di qui, essendo anche ω trascendente come τ, si deduce appunto $x_1 = x_2 = \ldots = x_n = 0$.

Chiamiamo allora *grado* di un numero di I il massimo degli esponenti di τ che figurano effettivamente nella espressione (1) (come per i polinomi). Dalla proprietà sopra notata risulta che il grado del prodotto di due numeri di I è la somma dei gradi dei fattori; perciò nessun numero di I può essere divisibile per un altro numero di I di grado maggiore.

La proprietà 5_1 del n. 2 è così dimostrata, ed I è dunque un *campo d'integrità* (4).

Dimostriamo ora che *nel campo d'integrità I esiste il m. c. d.* Siano

$$\alpha = \sum_1^k a_i\tau^{\alpha_i} \qquad \beta = \sum_1^h b_j\tau^{\beta_j}$$

due numeri qualunque di I. Riduciamo tutti gli esponenti ad un medesimo denominatore n (per fissare le idee, il minimo), poniamo

$$\alpha_i = \frac{n_i}{n}, \quad \beta_j = \frac{m_j}{n}, \qquad (i = 1, 2 \ldots k;\ j = 1, 2 \ldots h),$$

e consideriamo i polinomi

$$f(x) = \sum_1^k a_i x^{n_i} \quad , \quad g(x) = \sum_1^h b_j x^{m_j};$$

avremo con ciò

$$\alpha = f(\tau^{\frac{1}{n}}) \quad , \quad \beta = g(\tau^{\frac{1}{n}}). \tag{3}$$

Determiniamo il m. c. d. dei polinomi $f(x)$, $g(x)$ col procedimento di Euclide; se, ed es., il grado di $f(x)$ è non minore di quello di $g(x)$, otterremo

$$\begin{aligned} f(x) &\equiv g(x)q(x) + r(x) \\ g(x) &\equiv r(x)q_1(x) + r_1(x) \\ &\cdots\cdots\cdots \\ r_{s-1}(x) &\equiv r_s(x)q_{s+1}(x). \end{aligned}$$

(4) Se τ fosse un numero algebrico, I sarebbe invece un campo.

Poniamo in queste identità $x = \tau^{\frac{1}{n}}$; tutti questi polinomi $q(x)$, $r(x)$, $q_1(x)$ ... assumono valori che sono numeri di I; indicandoli con λ, ρ, λ_1, ... avremo, guardando le (3),

$$\begin{aligned} \alpha &= \beta\lambda + \rho \\ \beta &= \rho\lambda_1 + \rho_1 \\ &\cdots\cdots \\ \rho_{s-1} &= \rho_s\lambda_{s+1} ; \end{aligned}$$

e di qui, col solito ragionamento, si vede che ρ_s divide α e β ed è diviso da tutti i loro divisori comuni; onde è $\rho_s = D(\alpha, \beta)$ c. d. d.

Nel campo I *non vale però una scomponibilità limitata.* Ad es.:

$$\tau = \tau^{\frac{1}{2}}\tau^{\frac{1}{2}} = \tau^{\frac{1}{3}}\tau^{\frac{1}{3}}\tau^{\frac{1}{3}} = \dots ;$$

od anche

$$\begin{aligned} \tau^2 + \tau + 1 &= (\tau - \tau^{\frac{1}{2}} + 1)(\tau + \tau^{\frac{1}{2}} + 1) \\ &= (\tau - \tau^{\frac{1}{2}} + 1)(\tau^{\frac{1}{2}} - \tau^{\frac{1}{4}} + 1)(\tau^{\frac{1}{2}} + \tau^{\frac{1}{4}} + 1) \\ &= (\tau - \tau^{\frac{1}{2}} + 1)(\tau^{\frac{1}{2}} - \tau^{\frac{1}{4}} + 1)(\tau^{\frac{1}{4}} - \tau^{\frac{1}{8}} + 1)(\tau^{\frac{1}{4}} + \tau^{\frac{1}{8}} + 1) \\ &= \dots\dots \end{aligned}$$

Dunque: *Nel campo di integrità* I *sopra definito vale la prima parte della teoria della divisibilità, ma non la seconda.*

21. L'esempio precedente può anche prospettarsi, dal punto di vista logico, nel modo seguente. Al posto del numero τ consideriamo una *indeterminata* x, e consideriamo le espressioni (polinomi con esponenti razionali assoluti) $\sum_1^k x_i x^{\xi_i}$, con gli ξ_i distinti due a due, e gli x_i variabili in un campo qualunque C. Possiamo considerare addirittura questi polinomi dal punto di vista formale. È immediato che l'insieme di questi « polinomi » costituisce un campo di integrità; e gli stessi ragionamenti di sopra provano, anche nell'attuale significato, le stesse conseguenze di sopra.

22. Si vede subito (la cosa è stata osservata verbalmente dal dott. GABRIELE DARBO, e forse anche da altri) che le funzioni intere (polinomi e trascendenti intere) costituiscono un campo d'integrità, nel quale vale sostanzialmente tutta la teoria della divisibilità.

Tale campo infatti è a fattorizzazione unica, però infinita. Ciò discende subito dal teorema di WEIERSTRASS sulla fattorizzazione delle trascendenti intere. Le unità del campo sono le trascendenti intere che non hanno zeri ($e^{g(z)} \cdot e^{-g(z)} = 1$), in particolare le costanti; perciò i fattori esponenziali, che compaiono nello sviluppo di WEIERSTRASS, sono aritmeticamente irrilevanti. Gli elementi primi del campo sono le funzioni lineari (come nel campo dei polinomi), se noi consideriamo le funzioni intere sul campo complesso. (Potrebbero essere studiate le funzioni intere su un campo qualsiasi).

Essendo il campo delle funzioni intere a fattorizzazione unica (sebbene infinita), valgono in esso tutte le solite proprietà della teoria della divisibilità (nn. 6 e 7).

Si noti che la scomponibilità illimitata che vale in questo campo delle funzioni intere è di natura sostanzialmente diversa da quella che vale nel campo I, considerato al n. 20. Infatti nel campo delle funzioni intere esiste la classe degli elementi primi, ed ogni altro elemento del campo è scomponibile in un prodotto (finito o infinito) di tali elementi primi; invece nel campo I accade, ad es., che l'elemento τ, o una sua potenza qualunque, è scomponibile (v. n. 20), ma la scomposizione non conduce mai ad elementi primi. Sarebbe interessante studiare in generale i tipi diversi di scomponibilità illimitata che possono presentarsi in un campo d'integrità.