RENDICONTI
*del*
SEMINARIO MATEMATICO
*della*
UNIVERSITÀ DI PADOVA

D. BOCCIONI

# Alcune osservazioni sugli anelli pseudo-bezoutiani e fattoriali

*Rendiconti del Seminario Matematico della Università di Padova*, tome 37 (1967), p. 273-288

<http://www.numdam.org/item?id=RSMUP_1967__37__273_0>

# ALCUNE OSSERVAZIONI SUGLI ANELLI PSEUDO-BEZOUTIANI E FATTORIALI

*di* D. BOCCIONI (*a Padova*) *)

Questo lavoro contiene un risultato nuovo (il criterio di fattorialità, qui sotto enunciato, dato dal teor. 2 del n. 7) e nuove dimostrazioni di alcuni risultati classici.

Fra queste ultime vi è la dimostrazione (sostanzialmente semplificata: v. n. 3, penult. capoverso) del *lemma di Gauss* (affermante che il prodotto di due polinomi primitivi è primitivo) per i domini d'integrità commutativi con 1 nei quali ogni coppia di elementi possiede un massimo comun divisore, cioè (usando la terminologia di Bourbaki [5] [1])) *per gli anelli pseudo-bezoutiani.*

Questo « lemma di Gauss generalizzato » (teor. 1, n. 3) è alla base di un teorema di Prüfer (cfr. n. 3), secondo il quale l'anello dei polinomi $A[X]$ è pseudo-bezoutiano se tale è l'anello $A$.

D'altra parte il suddetto criterio di fattorialità (in virtù del quale *un anello è fattoriale se, e solo se, in esso ogni famiglia $F$ di elementi ha un massimo comun divisore, coincidente con un massimo comun divisore di una sottofamiglia finita di $F$*) si presta bene a fornire una nuova dimostrazione (n. 10) del *teorema di Gauss* ($A[X]$ è fattoriale se lo è $A$) strettamente e naturalmente collegata con quella del predetto teorema di Prüfer (cfr. n. 9).

Il suddetto criterio di fattorialità si presta pure, in modo particolarmente naturale, a fornire una nuova dimostrazione della *fattorialità di un anello principale* (n. 8).

---

*) Lavoro eseguito nell'ambito dei Gruppi di ricerca del Comitato Nazionale per la matematica del C.N.R.

Indirizzo dell'A.: Seminario Matematico, Università, Padova.

[1]) I numeri fra parentesi quadre rimandano alla bibliografia alla fine della nota.

Da segnalare infine le nuove dimostrazioni, particolarmente semplici, di altre due classiche proprietà degli anelli pseudo-bezoutiani (v. n. 6).

**1.** – Nel seguito *anello* significherà sempre dominio d'integrità ([9], p. 53) commutativo con una identità $1 \neq 0$.

Se $A$ è un anello, denoteremo nel seguito con $U$ l'insieme degli elementi invertibili (cioè delle unità) di $A$, con $K$ il corpo delle frazioni di $A$, e con i simboli $A^*$, $K^*$ risp. l'insieme degli elementi non nulli di $A$ e l'insieme degli elementi non nulli di $K$. (Cfr. [2], pp. 6-7.)

Se $a$ e $b$ sono elementi qualsiasi di un anello $A$, diremo che $a$ è (in $A$) un divisore di $b$ (oppure che $a$ divide $b$, oppure che $b$ è un multiplo di $a$), e scriveremo $a \mid b$, se esiste un $c \in A$ tale che $b = ac$. (Cfr. [2], p. 6, Remarque 2.)

Questa ben nota relazione di divisibilità $a \mid b$ nell'anello $A$ è una relazione di preordine (cioè è riflessiva e transitiva); essa coincide con la relazione indotta su $A$ dalla relazione di preordine nel corpo $K$ nota come la relazione di divisibilità $x \mid y$ in tale corpo (rispetto ad $A$), ([2], p. 6, Remarque 2).

Se $x, y \in K$, la relazione

$$x \sim y$$

($x$ associato ad $y$), cioè $x \mid y$ e $y \mid x$, è notoriamente (cfr. [2], p. 3) una relazione di equivalenza in $K$, e l'insieme quoziente

$$K/\sim$$

(costituito dalle relative classi di equivalenza) è un insieme (parzialmente) ordinato dalla relazione così definita:

$$\overline{x} \leqslant \overline{y} \Leftrightarrow x \mid y\,, \qquad (x, y \in K), \tag{1}$$

$\overline{z}$ denotando (la classe di equivalenza contenente $z \in K$ cioè) l'insieme degli elementi di $K$ associati a $z$.

L'insieme degli ideali principali frazionari ([2], p. 7) del corpo $K$ (rispetto all'anello $A$), che denoteremo con

$$P(K)\,,$$

è un insieme ordinato dalla relazione insiemistica $\supseteq$, e risulta

$$(x) \supseteq (y) \Leftrightarrow x \mid y\,, \qquad (x, y \in K), \tag{2}$$

cosicchè l'applicazione

$$\omega_0 : \overline{z} \to (z) \qquad (z \in K) \tag{3}$$

è un isomorfismo ordinale ([1], p. 20) di $K/\sim$ su $P(K)$, muniti risp. delle relazioni di ordine $\leqslant$ e $\geq$ (cfr. [2], p. 8).

Nel seguito denoteremo con

$$P(A)$$

l'insieme ordinato, dalla relazione di inclusione $\subseteq$, degli ideali principali (interi) dell'anello $A$.

**2.** – Sia $\{a_i\}$ una famiglia di elementi $a_i$ di un anello $A$, l'insieme $I$ degli indici $i$ della quale sia qualsiasi (finito o infinito). Se, in particolare, $I = \{1, 2, ..., n\}$, il simbolo $\{a_i\}$ potrà essere sostituito dall'equivalente $\{a_1, a_2, ..., a_n\}$.

Un elemento $d$ di $A$ tale che

$$a \mid d \Leftrightarrow a \mid a_i \quad \text{per ogni } i \in I \qquad (a \in A) \tag{4}$$

verrà detto un *massimo comun divisore* (*MCD*) (degli elementi $a_i$) della famiglia $\{a_i\}$ e denotato col simbolo MCD $\{a_i\}$. L'eguaglianza

$$d = \text{MCD}\,\{a_i\} \tag{4'}$$

verrà usata convenzionalmente (analoga convenzione per le altre eguaglianze del seguito contenenti il simbolo MCD) in luogo della equivalenza

$$d \sim \text{MCD}\,\{a_i\}\,, \tag{4''}$$

la quale esprime che MCD $\{a_i\}$ (se esiste) è univocamente determinato da $\{a_i\}$ a meno di fattori invertibili in $A$ [2]). È chiaro che

$$d = \text{MCD}\,\{a_i\} \Leftrightarrow (d) = \sup\{(a_i)\} \tag{5}$$

(l'esistenza del MCD $\{a_i\}$ equivalendo dunque a quella del sup $\{(a_i)\}$),

---

[2]) Si osservi che se, in particolare, $I = \emptyset$, allora MCD $\{a_i\} = 0$.

dove il simbolo

$$\sup\{(a_i)\}$$

denota il supremum ([1], p. 16, e [2], p. 10) *in* $P(A)$ (dell'insieme degli elementi) della famiglia $\{(a_i)\}$ di ideali principali $(a_i)$ di $A$.

Se $H$ è un qualsiasi insieme (parzialmente) ordinato, diremo che $H$ è un *sup-semireticolo* (risp. un *inf-semireticolo*) se in $H$ esiste $\sup\{u, v\}$ (risp. $\inf\{u, v\}$) per ogni coppia $u$, $v$ di elementi di $H$. Diremo che $H$ è un *sup-semireticolo completo* (risp. un *inf-semireticolo completo*) se in $H$ esiste $\sup\{u_i\}$ (risp. $\inf\{u_i\}$) per ogni famiglia non vuota $\{u_i\}$ di elementi $u_i$ di $H$. (Cfr. [8], pp. 20 e 33.)

Se $A$ è un anello, porremo (n. 1):

$$P^*(K) = P(K) - \{(0)\}, \qquad P^*(A) = P(A) - \{(0)\}$$

(cfr. [2], p. 7). Evidentemente (rispetto alla relazione di inclusione $\subseteq$):

I) $P(A)$ è un sup-semireticolo se, e solo se, $P^*(A)$ è un sup-semireticolo;

II) $P(A)$ è un sup-semireticolo completo se, e solo se, $P^*(A)$ è un sup-semireticolo completo.

Se denotiamo con $\omega$ la restrizione dell'applicazione $\omega_0$ (v. (3)) all'insieme degli elementi di $K/\sim$ diversi da $\bar{0}$, questa $\omega$ è un isomorfismo ([2], p. 2) del gruppo ordinato ([2], pp. 1 e 4):

$$K^*/\sim \;=\; K^*/U$$

sul gruppo ordinato $P^*(K)$ ([2], pp. 7-8), quest'ultimo munito della moltiplicazione $(x)(y) = (xy)$ $(x,\ y \in K^*)$ e della relazione d'ordine $\supseteq$. L'isomorfismo $\omega$ applica quindi il sotto-semigruppo $A^*/\sim$ degli elementi interi (cioè $\geqslant \bar{1} = U$) di $K^*/U$ sul sotto-semigruppo $P^*(A)$ degli elementi interi (cioè $\subseteq (1) = A$) di $P^*(K)$. Inoltre $K^*/U$ è il gruppo delle frazioni di $A^*/\sim$, e $P^*(K)$ è il gruppo delle frazioni di $P^*(A)$.

Ne segue che *il gruppo ordinato* $K^*/U$ *è reticolato* ([2], dépliant I) *se e solo se* $A^*/\sim$ è un inf-semireticolo rispetto all'ordine $\leqslant$ in esso definito dalla (1) (per la Proposition 8 di [2], p. 13), cioè se e solo se $P^*(A)$ è un sup-semireticolo rispetto all'inclusione $\subseteq$ (per le proprietà ordinali dell'isomorfismo $\omega$: cfr. [1], p. 21), cioè se e solo se $P(A)$ è un sup-semireticolo (per la I)), ossia se e solo se *ogni coppia di elementi dell'anello* $A$ *ha un MCD in* $A$ (per la (5)).

Il gruppo ordinato $K^*/U$ è filtrante ([2], p. 5), poichè (come sopra si è osservato) ogni suo elemento è il quoziente di due elementi interi, (per la Proposition 4 di [2], p. 5).

Ne segue che *il gruppo ordinato $K^*/U$ è completamente reticolato* ([2], p. 28 [3])) *se e solo se* $A^*/\sim$ è un inf-semireticolo completo (per l'exerc. 29-*a* di [2], p. 28 [4])) cioè se e solo se $P(A)$ è un sup-semireticolo completo (per le proprietà ordinali di $\omega$ e per la II)), ossia se e solo se *ogni famiglia non vuota* (e non necessariamente finita) *di elementi dell'anello $A$ ha un MCD in $A$* (per la (5)).

Secondo Bourbaki ([5], p. 86), un anello $A$ dicesi pseudo-bezoutiano (risp. pseudo-principale) se il gruppo ordinato $K^*/U$ è reticolato (risp. completamente reticolato). In virtù delle due osservazioni fatte qui sopra (e della precedente osservazione [2])), tali definizioni sono dunque equivalenti alle due seguenti.

Un anello $A$ dicesi *pseudo-bezoutiano* (risp. *pseudo-principale*) se ogni coppia (risp. ogni famiglia) di elementi di $A$ ha un massimo comun divisore in $A$.

**3.** – In base alla Proposition 2 di [5], p. 34, un anello è *fattoriale* ([5], p. 32) se, e solo se, esso è gaussiano ([9], p. 115).

Se $A$ è un anello, denoteremo nel seguito con $X$ una indeterminata (cioè un elemento trascendente) sopra $A$ e con

$$A[X]$$

l'anello dei polinomi in $X$ coi coefficienti in $A$.

È ben noto il seguente *teorema di Gauss*: *Se $A$ è un anello fattoriale, $A[X]$ è fattoriale.*

La prova classica di tale teorema ([15], p. 81) è essenzialmente basata sul seguente *lemma di Gauss* [5]: Se $A$ è un anello fattoriale, il prodotto

---

[3]) In tale definizione di gruppo completamente reticolato $G$, a p. 28 di [2], si deve leggere *réticulé* invece di *ordonné* (v. feuille d'errata n. 10, p. 8), ed inoltre evidentemente *partie non vide* invece di *partie*, altrimenti il sup $\emptyset$ sarebbe il minimo di $G$ ([3], p. 13), il quale $G$ sarebbe allora un inf-semireticolo completo ([8], p. 40) e conterrebbe quindi un solo elemento ([1], p. 229).

[4]) In tale esercizio 29-a si deve evidentemente leggere *partie non vide* invece di *partie*, altrimenti l'insieme $P$ degli elementi positivi di $G$ dovrebbe avere un massimo, uguale all'infimum in $P$ di $\emptyset$ ([3], p. 13).

[5]) Disquisitiones Arithmeticae, Art. 42, Werke, Bd. 1, p. 34 (cfr. [6], p. 28-29).

in $A[X]$ di due polinomi primitivi è primitivo, (un polinomio $\sum a_r X^r$ dicesi primitivo se MCD $\{a_r\} = 1$ [6]).

Nel lemma di Gauss, la considerazione del MCD di elementi di $A$ è lecita poichè, com'è noto (cfr. [5], p. 35 e p. 86, exerc. 21), un anello fattoriale è pseudo-bezoutiano, anzi è pseudo-principale, (cfr. pure n. 7, teor. 2).

D'altra parte si conoscono esempi di anelli pseudo-bezoutiani non pseudo-principali, e di anelli pseudo-principali non fattoriali (cfr. [5], p. 87, exerc. 22-b) [7]). Il seguente teorema è quindi una generalizzazione naturale del teorema di Gauss:

*Teorema di Prüfer* [8]: *Se $A$ è un anello pseudo-bezoutiano (risp. pseudo-principale), $A[X]$ è pseudo-bezoutiano (risp. pseudo-principale).*

Sia le prove originali [8]), sia quelle più recenti di questo teorema di Prüfer ([11], n. 45, [10], p. 100, [5], p. 87) sono basate essenzialmente sul seguente

TEOREMA 1 (*lemma di Gauss generalizzato*): *Se $A$ è un anello pseudo-bezoutiano, il prodotto in $A[X]$ di due polinomi primitivi è primitivo.*

Però, nelle prove suddette del teor. di Prüfer, questo teor. 1 (o una proposizione ad esso equivalente) non è mai ottenuto con una dimostrazione diretta (analoga a quella classica del lemma di Gauss), ma è ricavato invece o da un teorema generale della teoria dei sistemi di ideali (il cosiddetto lemma di Dedekind-Mertens: [11], n. 46) la cui prova è notevolmente laboriosa (cfr. [14], p. 24), oppure è ricavato dal fatto che ogni anello pseudo-bezoutiano è integralmente chiuso ([4], p. 15, cfr. [5], p. 86, exerc. 21) e da un teorema di Kronecker [9]) (enunciato ad es. in [5], p. 83, exerc. 12-a, cfr. [11], n. 45) la cui prova moderna [10])

---

[6]) Si noti che il MCD $\{a_r\}$ (con $r$ descrivente l'insieme dei numeri interi $\geqslant 0$) coincide col MCD della sottofamiglia finita di $\{a_r\}$ avente come elementi i coefficienti non nulli del polinomio (cfr. [2])).

[7]) Un classico esempio, dovuto a Dedekind ([7], pp. 100-101), di un anello pseudo-bezoutiano (anzi bezoutiano: [5], p. 85) che non è un corpo, e che non contiene alcun elemento irriducibile ([9], p. 115) e quindi alcun elemento primo (non invertibile), è l'anello di tutti i numeri (complessi) algebrici interi ([9], p. 181).

[8]) [14], p. 26 (la parte fra parentesi è provata in [5], p. 87, exerc. 23).

[9]) Werke, Bd. 2, p. 419: questo teorema di Kronecker, che è la generalizzazione naturale del lemma di Gauss al caso di un anello A integralmente chiuso, fu in seguito ritrovato indipendentemente da Dedekind ([6], p. 28-38) e da Hurwitz (cfr. [11], n. 45).

[10]) Le altre prove originali, citate in [9]), sono vincolate al particolare ambiente numerico (complesso) degli interi algebrici.

comporta il ricorso o al suddetto lemma di Dedekind-Mertens oppure ad uno dei teoremi fondamentali della teoria delle valutazioni ([11], n. 40, cfr. n. 45).

Uno degli scopi del presente lavoro è appunto quello di presentare una semplice dimostrazione diretta del teorema 1. Ciò verrà fatto (dopo le necessarie premesse del n. 4) nel successivo n. 5.

**4.** – Ricordiamo anzitutto che, come si verifica facilmente in base alla definizione di MCD (cfr. [9], p. 119, lemmi 1 e 3, l'implicazione (7) $\Rightarrow$ (8) deducendosi immediatamente dalla (6)):

III) Se $A$ è un anello pseudo-bezoutiano, ogni famiglia finita di elementi $a_i$ (non necessariamente diversi da 0) di $A$ ha un MCD in $A$, e risulta (qualunque sia $b \in A$):

$$\text{MCD}\,\{ba_1, ba_2, \ldots, ba_n\} = b\,\text{MCD}\,\{a_1, a_2, \ldots, a_n\}\,; \tag{6}$$

inoltre, da

$$\text{MCD}\,\{a_1, a_2, \ldots, a_n\} = d \neq 0\,, \qquad a_i = dq_i \;\; (i = 1, 2, \ldots, n) \tag{7}$$

(con $d,\ q_1, q_2, \ldots, q_n \in A$) segue

$$\text{MCD}\,\{q_1, q_2, \ldots, q_n\} = 1\,. \tag{8}$$

Ricordiamo poi la seguente proposizione:

IV) Se $a_1$, $a_2$, $b$ sono elementi qualsiasi di un anello pseudo-bezoutiano $A$, e se

$$b \neq 0\,, \qquad b \mid a_1 a_2\,, \tag{9}$$

allora esistono $b_1,\ b_2 \in A$ tali che:

$$b = b_1 b_2\,, \qquad b_1 \mid a_1\,, \qquad b_2 \mid a_2\,. \tag{10}$$

Esponiamo qui, per comodità del lettore, la semplice deduzione della IV) dalla III) (con $n = 2$) che figura a p. 3 di [14]. [11])

---

[11]) La IV) si può anche ottenere immediatamente (in base alle considerazioni dei nn. 1 e 2) dal corollario del « teorema di decomposizione » per i gruppi reticolati a p. 14 di [2] (applicato al gruppo reticolato $P^*(K)$).

Poichè $b \neq 0$, allora $b_1 = \text{MCD}\{a_1, b\} \neq 0$, $(b_1 \in A)$. Da $a_1 = b_1 q$, $b = b_1 b_2$ (con $q$, $b_2 \in A$) segue perciò (per le (7), (8)): $\text{MCD}\{q, b_2\} = 1$, e quindi (per la (6)): $\text{MCD}\{a_2 q, a_2 b_2\} = a_2$. Da questa, poichè la $(9)_2$ (cioè $a_1 a_2 = bc$, con $c \in A$, cioè $b_1 q a_2 = b_1 b_2 c$) implica $b_2 \mid a_2 q$, e poichè $b_2 \mid a_2 b_2$, risulta $b_2 \mid a_2$. Dunque valgono appunto le (10).

**5.** – Ciò premesso, dimostriamo il teorema 1 (n. 3). Proviamo anzitutto la proposizione seguente.

V) *Sia $A$ un anello pseudo-bezoutiano, e siano $f$ e $g$ due elementi non nulli di $A[X]$:*

$$f = a_0 + a_1 X + \ldots + a_m X^m \qquad (a_m \neq 0), \tag{11}$$

$$g = b_0 + b_1 X + \ldots + b_n X^n \qquad (b_n \neq 0). \tag{12}$$

*Se $d$ è un elemento* (non nullo e) *non invertibile di $A$ che divide tutti i coefficienti del prodotto $fg$ e che non divide tutti i coefficienti di $f$ nè tutti quelli di $g$, se inoltre $a_r$ $(0 \leqslant r \leqslant m)$ è il primo dei coefficienti $a_0, a_1, \ldots, a_m$ di $f$ che non sia un multiplo di $d$, allora esiste in $A$ un elemento* (non nullo e) *non invertibile $d_r$, non associato a $d$, che divide $d$ ed $a_r$.*

Se $b_s$ $(0 \leqslant s \leqslant n)$ è il primo dei coefficienti $b_0, b_1, \ldots, b_n$ di $g$ che non sia un multiplo di $d$, consideriamo il coefficiente di $X^{r+s}$ nel prodotto $fg$, uguale alla somma

$$a_r b_s + a_{r+1} b_{s-1} + a_{r+2} b_{s-2} + \ldots + a_{r+s} b_0$$
$$+ a_{r-1} b_{s+1} + a_{r-2} b_{s+2} + \ldots + a_0 b_{s+r}\,.$$

Questa somma e tutti i suoi addendi diversi dal primo sono multipli di $d$, quindi $d \mid a_r b_s$ e perciò, per la IV), esistono $d_r$, $e_s \in A$ tali che

$$d = d_r e_s, \qquad d_r \mid a_r, \qquad e_s \mid b_s\,. \tag{13}$$

Poichè (per ipotesi) $d$ non divide $b_s$, dalla $(13)_3$ segue che $d$ non è associato ad $e_s$ [12]), e quindi dalla $(13)_1$ segue che $d_r$ non è invertibile. Analogamente, dalla $(13)_2$ risulta che $d_r$ non è associato a $d$. Perciò la V) è dimostrata.

---

[12]) Si ricordi che, se $a$, $b$, $a'$, $b'$ sono elementi qualsiasi di un anello e se $a \sim a'$, $b \sim b'$, allora $a \mid b \Leftrightarrow a' \mid b'$.

VI) Sia $A$ un anello pseudo-bezoutiano, e siano $f$ e $g$ (v. (11) e (12)) due elementi non nulli di $A[X]$. Se $g$ è primitivo e se il prodotto $fg$ non è primitivo, allora $f$ non è primitivo.

Infatti, nelle ipotesi della VI):

1°) in $A$ esiste un elemento (non nullo e) non invertibile $d_0$, che divide tutti i coefficienti del prodotto $fg$, e che divide il coefficiente $a_0$;

2°) se esiste in $A$ un elemento (non nullo e) non invertibile $d_{r-1}$, che divide tutti i coefficienti del prodotto $fg$, e che divide ciascuno dei coefficienti

$$a_0, a_1, \ldots, a_{r-1}, \qquad (1 \leqslant r \leqslant m),$$

allora in $A$ esiste pure un elemento (non nullo e) non invertibile $d_r$, che divide tutti i coefficienti del prodotto $fg$, e che divide ciascuno dei coefficienti

$$a_0, a_1, \ldots, a_{r-1}, a_r .$$

E invero, 1°): Poichè $fg$ non è primitivo, esiste in $A$ un elemento (non nullo e) non invertibile $d_{-1}$ che divide tutti i coefficienti di $fg$. Se $d_{-1} \mid a_0$, allora $d_0 = d_{-1}$. Se invece $a_0$ non è un multiplo di $d_{-1}$, l'esistenza di $d_0$ è assicurata dalla V) (ove si legga $d_{-1}$ invece di $d$, e si ponga $r = 0$), poichè $d_{-1}$ non divide tutti i coefficienti di $g$ (che è primitivo per ipotesi). Inoltre, 2°): Se $d_{r-1} \mid a_r$, allora $d_r = d_{r-1}$. Se invece $a_r$ non è un multiplo di $d_{r-1}$, l'esistenza di $d_r$ è assicurata dalla V) (ove si legga $d_{r-1}$ invece di $d$).

In base a 1°) e 2°), rimane dunque provata l'esistenza in $A$ di un elemento (non nullo e) non invertibile $d_m$, che divide tutti i coefficienti del prodotto $fg$, e che divide ciascuno dei coefficienti $a_0, a_1, \ldots, a_m$ del polinomio $f$, il quale perciò non è primitivo.

La VI) è dunque dimostrata e, con essa, è evidentemente dimostrato il teorema 1.

OSSERVAZIONE 1: Se valgono le ipotesi della V), l'elemento $d$ non può essere irriducibile (perchè $d_r$ ne è un divisore proprio: [9], p. 115).

OSSERVAZIONE 2: Degli elementi $d_{-1}$, $d_0$, $d_1, \ldots, d_m$, considerati nella dimostrazione della VI), ciascuno (tranne il primo) è uguale al precedente, oppure ne è un divisore proprio. Perciò, se in particolare $d_{-1}$ è irriducibile, risulta $d_{-1} = d_0 = d_1 = \ldots = d_m$, e quindi $d_{-1}$ divide tutti i coefficienti del polinomio $f$.

OSSERVAZIONE 3: Se esistesse sempre un $d_{-1}$ irriducibile (come accadrebbe, ad es., nel caso di un $A$ fattoriale), la VI) sarebbe una immediata conseguenza della V) (in virtù dell'osservazione 1).

**6.** – Incidentalmente osserveremo che dalla IV) del n. 4 (che è stata usata nella precedente dimostrazione del teor. 1) si ottiene subito la seguente ben nota proposizione (cfr. [9], pp. 119-120, [2], p. 21, Proposition 14, [13], p. 153, [12], pp. 73-74):

VII) *In un anello pseudo-bezoutiano, ogni elemento irriducibile è primo.*

Infatti, se l'elemento (non nullo e) irriducibile $b$ divide il prodotto $a_1a_2$ e non divide $a_1$, allora $b = b_1b_2$ (v. $(10)_1$) non è associato a $b_1$ (per la $(10)_2$), e quindi (poichè è irriducibile) deve essere associato a $b_2$. Ma allora $b \mid a_2$ (per la $(10)_3$), cioè appunto $b$ è primo.

Un'altra conseguenza diretta della IV) del n. 4 è il seguente ben noto «*lemma di Euclide*» (cfr. [2], p. 18):

VIII) *Se $a_1, a_2, b$ sono elementi qualsiasi di un anello pseudo-bezoutiano, da $b \mid a_1a_2$ e $MCD\{b, a_1\} = 1$ segue $b \mid a_2$.*

Infatti, se $b \neq 0$, poichè $b_1$ (v. $(10)_1$ e $(10)_2$) divide $b$ ed $a_1$, esso divide pure MCD $\{b, a_1\}$, e quindi è invertibile. Ma allora $b$ è associato a $b_2$ (per la $(10)_1$), e quindi divide appunto $a_2$ (per la $(10)_3$). Se poi $b = 0$, la validità della VIII) è manifesta.

Le precedenti dimostrazioni delle due notevoli proprietà VII) e VIII) degli anelli pseudo-bezoutiani possono avere interesse per la loro particolare semplicità.

**7.** – Il seguente teorema 2 (che dimostreremo in questo n.) fornisce un nuovo criterio di fattorialità, l'uso del quale si rivelerà molto semplice e naturale (almeno nelle applicazioni dei successivi nn. 8 e 10).

TEOREMA 2 [13]: *Un anello* (n. 1) *$A$ è fattoriale* (n. 3) *se, e soltanto se, valgono le due seguenti condizioni*:

$\alpha$) *$A$ è pseudo-principale* (n. 2);

$\beta$) *di ogni famiglia non vuota $\{a_i\}$ $(i \in I \neq \emptyset)$ di elementi $a_i$ di $A$, esiste una sottofamiglia finita e non vuota $\{a_t\}$ $(t \in T$ finito non vuoto $\subseteq I)$ tale che*

$$\text{MCD}\{a_i\} = \text{MCD}\{a_t\}. \tag{14}$$

---

[13]) Si osservi che questo teor. 2 è equivalente al criterio di fattorialità enunciato nell'introduzione del presente lavoro. Ciò risulta immediatamente dalla [2]) e dal fatto che, se $I \neq \emptyset$: $a_i = 0$ per ogni $i \in I \Leftrightarrow$ MCD $\{a_i\} = 0$, ($a_i \in A$, anello qualsiasi).

Dedurremo questo teor. 2 dal seguente altro ben noto criterio di fattorialità IX) (la cui prova usuale sfrutta la VII) del n. 6), e dalla seguente nota proprietà X) dei semireticoli (la cui prova è molto semplice).

IX) (Cfr. [9], p. 115-121, [13], pp. 151-152, [12], p. 75.) Un anello $A$ è fattoriale se, e soltanto se, valgono le due seguenti condizioni:

$\gamma$) $A$ è pseudo-bezoutiano (n. 2);

$\delta$) l'insieme ordinato $P(A)$ degli ideali principali di $A$ (n. 1) soddisfa la c.c.a. (= condizione catenaria ascendente: v. ad es. [8], p. 12).

X) (Cfr. [8], p. 33.) Se un sup-semireticolo (n. 2) $H$ soddisfa la c.c.a., allora valgono le due seguenti condizioni:

$\lambda$) $H$ è un sup-semireticolo completo (n. 2);

$\mu$) di ogni famiglia non vuota $\{u_i\}$ $(i \in I \neq \emptyset)$ di elementi $u_i$ di $H$, esiste una sottofamiglia finita e non vuota $\{u_t\}$ $(t \in T$ finito non vuoto $\subseteq I)$ tale che

$$\sup \{u_i\} = \sup \{u_t\} . \tag{15}$$

Ricordiamo che (n. 2):

XI) Le precedenti condizioni $\alpha$) e $\gamma$) sono rispettivamente equivalenti alle seguenti $\alpha'$) e $\gamma'$):

$\alpha'$) $P(A)$ è un sup-semireticolo completo;
$\gamma'$) $P(A)$ è un sup-semireticolo.

*Prova del teor.* 2. Supponiamo che $A$ sia fattoriale. Allora, come è noto (cfr. n. 3), vale la $\alpha$), la quale si riottiene comunque, assieme alla $\beta$), nel modo seguente. Per le IX) e XI), valgono $\gamma'$) e $\delta$). Per la X), ove si legga $P(A)$ invece di $H$, valgono quindi $\lambda$) e $\mu$), cioè $\alpha'$) e $\mu$), quindi (per la XI)) vale appunto intanto la $\alpha$). D'altra parte la $\mu$) (con $P(A)$ invece di $H$) implica appunto la $\beta$) in virtù della (5) del n. 2.

Viceversa, supponiamo che valgano $\alpha$) e $\beta$). La $\alpha$) implica evidentemente la $\gamma$) e (per la XI)) la $\alpha'$). Consideriamo allora una qualunque sequenza $\{(a_n)\}$ $(n = 1, 2, 3, \ldots)$ di elementi $(a_n)$ di $P(A)$, $(a_n \in A)$, ciascuno contenuto nel successivo:

$$(a_1) \subseteq (a_2) \subseteq \ldots \subseteq (a_n) \subseteq \ldots . \tag{16}$$

Per la $\alpha'$), esiste in $P(A)$ il sup $\{(a_n)\}$. Inoltre, per la $\beta$) e per la (5) del

n. 2, esiste un insieme finito e non vuoto $T$ di numeri interi $> 0$, tale che $(t \in T)$:

$$\sup\{(a_n)\} = \sup\{(a_t)\}\,. \tag{17}$$

Ma, per la (16), $\sup\{(a_t)\} = (a_m)$, $m$ denotando il massimo intero appartenente a $T$, e quindi pure (per la (17)):

$$\sup\{(a_n)\} = (a_m)\,. \tag{18}$$

La (18) implica che tutti i termini della (16) con indice $> m$ sono uguali ad $(a_m)$:

$$(a_m) = (a_{m+1}) = \ldots,$$

ossia vale la $\delta$). Ma $\gamma$) e $\delta$) implicano appunto (per la IX)) che $A$ è fattoriale. Perciò il teor. 2 è dimostrato.

È chiaro che, col medesimo ragionamento fatto nel precedente capoverso, si dimostra anche che un qualsiasi sup-semireticolo completo $H$ (invece di $P(A)$) soddisfacente la condizione $\mu$) (invece di $\beta$)) soddisfa pure la c.c.a.; dunque per la X):

XII) *Un sup-semireticolo completo $H$ soddisfa la c.c.a. se, e soltanto se, esso soddisfa la condizione $\mu$).*

**8.** – Come primo esempio di applicazione del precedente teor. 2, mostriamo adesso come esso permetta di riottenere, in modo particolarmente naturale, il seguente ben noto risultato (cfr. ad es. [9], p. 122, [12], p. 78):

XIII) *Ogni anello principale* ([2], p. 50) *è fattoriale.*

Infatti, sia $A$ un anello principale, e sia $\{a_i\}$ $(i \in I)$ una qualsiasi famiglia non vuota di elementi $a_i$ di $A$. Tutte le somme finite e non vuote, ogni addendo delle quali è il prodotto di un qualsiasi elemento di $A$ per un qualsiasi elemento di $\{a_i\}$, costituiscono l'ideale $(\{a_i\})$, generato dagli elementi di $\{a_i\}$. Questo ideale $(\{a_i\})$ deve essere principale, cioè deve esistere un $d \in A$ tale che

$$(\{a_i\}) = (d)\,, \tag{19}$$

e quindi $d$ deve essere una delle somme suddette:

$$d = \sum_{t \in T} r_t a_t\,, \tag{20}$$

dove $T$ è un certo sottinsieme finito e non vuoto di $I$, ed $r_t \in A$ (per ogni $t \in T$). Dalla (19) segue che $(a_i) \subseteq (d)$, cioè che

$$d \mid a_i \tag{21}$$

per ogni $i \in I$. È chiaro che dalle (20) e (21) risulta

$$d = \text{MCD}\,\{a_i\} = \text{MCD}\,\{a_t\}\,,$$

cioè, simultaneamente, la validità delle $\alpha$) e $\beta$) del n. 7. Per il teor. 2, la XIII) è dunque dimostrata.

Questa proposizione XIII) verrà sfruttata nel successivo n. 10.

**9.** – Come secondo esempio di applicazione del teor. 2 del n. 7, esporremo, nel successivo n. 10, una nuova dimostrazione del teorema di Gauss (n. 3).

La necessaria parte preliminare (v. n. 10) di questa dimostrazione del teor. di Gauss è costituita da alcune semplici considerazioni che figurano in una nota prova (cfr. [5], p. 87, exerc. 23-a-b, e [10], p. 100) del teor. di Prüfer (n. 3) a partire dal lemma di Gauss generalizzato (n. 3), prova che perciò è naturale riesporre qui esplicitamente nelle sue linee essenziali.

Ne risulterà così una *dimostrazione simultanea dei due teoremi di Prüfer e di Gauss* (n. 3) basata (oltre che sul teor. 2) sul lemma di Gauss generalizzato (e quindi sulla nuova semplice prova di tale lemma esposta nel n. 5).

Premettiamo la seguente osservazione, di immediata verifica:

XIV) Siano $\{a_i\}$ $(i \in I)$ una famiglia di elementi $a_i$ di un anello $A$, ed $\{a_r\}$ $(r \in R \subseteq I)$ una sottofamiglia di $\{a_i\}$. Supponiamo che in $A$ esistano MCD $\{a_r\}$ e MCD $\{a_i\}$, e che sia

$$\text{MCD}\,\{a_r\} = \text{MCD}\,\{a_i\}\,.$$

Allora, se $J$ è un qualsiasi insieme di indici tale che

$$R \subseteq J \subseteq I\,,$$

in $A$ esiste pure MCD $\{a_j\}$ $(j \in J)$ e risulta

$$\text{MCD}\,\{a_r\} = \text{MCD}\,\{a_j\} = \text{MCD}\,\{a_i\}\,.$$

**10.** – Se $A$ è un anello pseudo-bezoutiano, e se $f$ è un qualsiasi polinomio $\in A[X]$, denoteremo con

$$c(f) \tag{22}$$

il *contenuto* di $f$, cioè il MCD ($\in A$) dei coefficienti di $f$ (la convenzione (4') del n. 2 valendo, naturalmente, anche per il simbolo (22)). In base alle (7)-(8) del n. 4, è chiaro che in $A[X]$ risulta

$$f = c(f)f_1 \qquad (c(f_1) = 1) \tag{23}$$

(cioè con $f_1$ polinomio primitivo $\in A[X]$). Inoltre, se, in $A[X]$:

$$f = df' \qquad (d \in A,\ f' \in A[X],\ c(f') = 1), \tag{24}$$

allora (per la (6) del n. 4):

$$c(f) = d\,. \tag{25}$$

In virtù delle (23) e (24)-(25), dal lemma di Gauss generalizzato (n. 3) segue immediatamente la proposizione seguente (evidentemente equivalente a tale lemma):

XV) *In un anello pseudo-bezoutiano* $A$:

$$c(fg) = c(f)c(g)\,,$$

*qualunque siano i polinomi* $f,\ g \in A[X]$.

Dalla XV) segue poi facilmente il lemma seguente (cfr. [5], p. 87, exerc. 23-a):

XVI) Sia $A$ un anello pseudo-bezoutiano, e sia $K$ il corpo delle frazioni di $A$. Se $f,\ g \in A[X]$, allora

$$f \mid g \quad \text{in} \quad A[X]$$

se, e soltanto se, sono soddisfatte le due condizioni seguenti:

$$c(f) \mid c(g) \quad \text{in } A\,, \qquad f \mid g \quad \text{in } K[X]\,.$$

Da questo lemma XVI) si ottiene subito il teorema di Prüfer (n. 3), (cfr. [10], p. 100, e [5], p. 87, exerc. 23-b):

Infatti, se $A$ è un anello pseudo-bezoutiano (risp. pseudo-principale),

e se $\{f_i\}$ $(i \in I)$ è una famiglia finita (risp. qualsiasi), non vuota, di polinomi non tutti nulli $f_i \in A[X]$, poniamo $(0 \neq d \in A)$:

$$d = \text{MCD}\,\{c(f_i)\} \text{ in } A\,. \tag{26}$$

L'anello $K[X]$ ($K$ corpo delle frazioni di $A$) è notoriamente principale, quindi (v. XIII)) fattoriale, quindi (v. teor, 2) pseudo-principale. Esiste perciò un $\varphi \in K[X]$ $(\varphi \neq 0)$ tale che

$$\varphi = \text{MCD}\,\{f_i\} \text{ in } K[X]\,. \tag{27}$$

In $K[X]$ si può scrivere (cfr. [15], p. 82):

$$\varphi = \frac{a}{b} f' \tag{28}$$

con $a$, $b$ (non nulli) $\in A$ ed $f'$ primitivo $\in A[X]$ $(c(f') = 1)$. Posto allora (v. (26)):

$$f = df' \tag{29}$$

$(f \in A[X])$, dalle (26)-(29), mediante il lemma XVI), risulta evidentemente (osservando anzitutto che, per le (28), (29), $c(f) = d$, $f \sim \varphi$ in $K[X]$, e quindi che, per le (26), (27), $c(f) = \text{MCD}\,\{c(f_i)\}$ in $A$, $f = \text{MCD}\,\{f_i\}$ in $K[X]$):

$$f = \text{MCD}\,\{f_i\} \quad \text{in} \quad A[X]\,, \tag{30}$$

cioè risulta appunto che $A[X]$ è pseudo-bezoutiano (risp. pseudo-principale).

*Prova del teorema di Gauss* (n. 3):

Mantenendo tutte le notazioni usate nella precedente prova del teor. di Prüfer, supponiamo ora che $A$ sia fattoriale. Allora (per il teor. 2) $A$ soddisfa entrambe le condiz. $\alpha$) e $\beta$). Poichè anche l'anello fattoriale $K[X]$ soddisfa entrambe le condiz. $\alpha$) e $\beta$), se la famiglia $\{f_i\}$ $(i \in I)$, qui sopra considerata, è qualsiasi, devono esistere due sottinsiemi finiti e non vuoti $R$, $S$ di $I$ tali che risulti (cfr. (26) e (27)):

$$d = \text{MCD}\,\{c(f_i)\} = \text{MCD}\,\{c(f_r)\} \quad \text{in} \quad A \qquad (r \in R), \tag{31}$$

$$\varphi = \text{MCD}\,\{f_i\} = \text{MCD}\,\{f_s\} \quad \text{in} \quad K[X] \qquad (s \in S). \tag{32}$$

Per l'osservazione XIV) del n. preced., posto

$$T = R \cup S ,$$

dalle (31) e (32) risulta dunque ($t \in T$):

$$d = \mathrm{MCD}\,\{c(f_t)\} = \mathrm{MCD}\,\{c(f_t)\} \quad \text{in} \quad A , \tag{33}$$

$$\varphi = \mathrm{MCD}\,\{f_i\} = \mathrm{MCD}\,\{f_t\} \quad \text{in} \quad K[X] . \tag{34}$$

Da queste (33), (34) e dalle (28), (29), mediante il lemma XVI), risulta allora evidentemente (con un ragionamento identico a quello che ha già permesso di ottenere la (30)):

$$f = \mathrm{MCD}\,\{f_i\} = \mathrm{MCD}\,\{f_t\} \quad \text{in} \quad A[X]$$

($i \in I$, $t \in T$ finito non vuoto $\subseteq I$), cioè risulta che $A[X]$ soddisfa entrambe le condiz. $\alpha$) e $\beta$). Dunque (per il teor. 2) $A[X]$ è appunto fattoriale.

## BIBLIOGRAFIA


[1] Birkhoff G.: *Lattice Theory*, Amer. Math. Soc. (1948).
[2] Bourbaki N.: *Algèbre, Chap. VI-VII*, Hermann (1952).
[3] Bourbaki N.: *Théorie des ensembles, Chap. III*, Hermann (1956).
[4] Bourbaki N.: *Algèbre commutative, Chap.* 5-6, Hermann (1964).
[5] Bourbaki N.: *Algèbre commutative, Chap.* 7, Hermann (1965).
[6] Dedekind R.: *Gesammelte mathematische Werke, Bd. II*, Vieweg (1931).
[7] Dedekind R.: *Gesammelte mathematische Werke, Bd. III*, Vieweg (1932).
[8] Dubreil-Jacotin M. L.; Lesieur L.; Croisot R.: *Leçons sur la théorie des treillis, des structures algébriques ordonnées et des treillis géométriques*, Gauthier-Villars (1953).
[9] Jacobson N.: *Lectures in abstract algebra, Vol. I*, Van Nostrand (1951).
[10] Jaffard P.: *Les systèmes d'idéaux*, Dunod (1960).
[11] Krull W.: *Idealtheorie*, Springer (1935).
[12] Kurosh A. G.: *Lectures on general algebra*, Chelsea (1963).
[13] Morin U.: *Algebra astratta*, Cedam (1955).
[14] Prüfer H.: *Untersuchungen über Teilbarkeitseigenschaften in Körpern*, Journal reine angew. Math., Bd. 168, pp. 1-36 (1932).
[15] van der Waerden B. L.: *Moderne Algebra, I*, Springer (1950).


Manoscritto pervenuto in redazione il 10 giugno 1966.