Osservazioni supplementari sui domini di Dedekind

1. A proposito della fattorizzazione degli ideali

Siano *I, J* due ideali di un dominio di Dedekind *A*. Si può definire, per analogia con la corrispondente nozione per le coppie di elementi di *A*, ***massimo comune divisore* di *I* e *J*** ogni ideale *L* di *A* tale che

a) $L \supset I, L \supset J$ (ossia *L* è divisore comune di *I* e *J*);
b) per ogni ideale *H* di *A* tale che $H \supset I, H \supset J$ si abbia $H \supset L$ (ossia ogni divisore comune di *I* e *J* divide *L*).

In altri termini, *L* è minimale, per inclusione, tra gli ideali che contengono *I* e *J*. È, dunque, l'ideale generato da $I \cup J$, ossia è l'ideale ***I* + *J*** (e, più precisamente, è minimale in quanto minimo). Lo indicheremo con $\mathrm{MCD}(I, J)$.

In modo del tutto simile, si può definire ***minimo comune multiplo* di *I* e *J*** il massimo ideale di *A* contenuto in *I* e *J*, cioè ***I*∩*J***. Lo denoteremo con $\mathrm{mcm}(I, J)$.

Rileggiamo queste due nozioni alla luce delle fattorizzazioni degli ideali di *A*. Supponiamo che *I* e *J* siano ideali propri e non nulli di *A*, dotati delle seguenti fattorizzazioni (scritte in modo da far comparire, eventualmente con esponente nullo, tutti gli ideali primi che siano fattori di uno o dell'altro):

$$I = P_1^{n_1} \cdots P_s^{n_s},$$
$$J = P_1^{m_1} \cdots P_s^{m_s},$$

ove a indici distinti corrispondono ideali primi distinti e gli esponenti sono numeri naturali.

Proviamo che, in maniera identica a quanto avviene per le coppie di elementi di un UFD, valgono le seguenti identità:

i) $\mathrm{MCD}(I, J) = I + J = P_1^{\min(n_1, m_1)} \cdots P_s^{\min(n_s, m_s)}$
ii) $\mathrm{mcm}(I, J) = I \cap J = P_1^{\max(n_1, m_1)} \cdots P_s^{\max(n_s, m_s)}$

Prima di procedere con la dimostrazione del punto i), premettiamo un risultato:

Due ideali di un dominio di Dedekind sono coprimi se e solo se non hanno divisori primi comuni.

Dimostrazione: Siano *U* e *V* ideali del dominio di Dedekind *A*. Se sono coprimi, ossia se $U + V = A$, allora non esiste alcun ideale primo *P* che contenga $U + V$, ossia che contenga *U* e *V*, ossia che li divida entrambi. Viceversa, se *U* e *V* non sono coprimi, allora l'ideale $U + V$ è proprio, e quindi è contenuto in un ideale massimale. Questo è un ideale primo che divide *U* e *V*.

Proviamo ora i). Si ha

$$I+J=P_1^{\min(n_1,m_1)}\cdots P_s^{\min(n_s,m_s)}(\underbrace{P_1^{u_1}\cdots P_s^{u_s}}_{U}+\underbrace{P_1^{v_1}\cdots P_s^{v_s}}_{V}),$$

ove, per ogni $i=1,...,s,\ u_i=n_i-\min(n_i,m_i), v_i=m_i-\min(n_i,m_i),$ ed uno tra u_i e v_i è nullo. Ne consegue che i due ideali U e V sono coprimi, in quanto privi di fattori primi comuni, dunque $U+V=A,$ da cui l'uguaglianza voluta.
L'enunciato ii) si può facilmente provare sulla base della definizione di minimo comune multiplo, alla luce dell'unicità della fattorizzazione. Con lo stesso metodo si può, in realtà, fornire anche una dimostrazione di i), alternativa a quella "aritmetica" qui proposta.

Si noti che da i) e ii) si deduce la seguente formula, valida per ogni coppia di ideali I e J propri non nulli di A, e contenente tutte le operazioni tra ideali finora definite:

$$I\cap J=IJ(I+J)^{-1}.$$

2. Generatori degli ideali di un dominio di Dedekind

Proveremo che ogni ideale di un dominio di Dedekind è generato da uno o due elementi. Precisamente, vale il seguente enunciato.

Teorema Sia I un ideale non nullo di un dominio di Dedekind A. Allora, per ogni $a\in I$ non nullo, esiste $b\in I$ tale che $I=(a,b)$.

Dimostrazione: La tesi è ovvia se I è principale: basterà prendere come elemento b un generatore di I. Supponiamo allora che I non sia principale. Poiché $I\supset(a),$ esiste un ideale J di A tale che $IJ=(a).$ Allora J, oltre che non nullo, è anche proprio, giacché I non può coincidere con $(a).$ Sia (con le convenzioni notazionali di sopra) $J=P_1^{m_1}\cdots P_s^{m_s}$ una sua fattorizzazione (ove gli esponenti sono tutti positivi). Poniamo quindi

$$\tilde{J}=P_1\cdots P_s,$$

e, per ogni $i=1,...,s,$

$$Q_i=P_1\cdots\hat{P}_i\cdots P_s.$$

Dall'unicità della fattorizzazione segue che, per ogni $i=1,...,s,\ I\tilde{J}\subsetneq IQ_i.$ Sia dunque, per ogni $i=1,...,s,\ b_i\in IQ_i\setminus I\tilde{J},$ ed inoltre

$$b=\sum_{i=1}^{s}b_i.$$

Allora $b\in I.$ Invece, per ogni $i=1,...,s,\ b_i\notin IP_i,$ dato che altrimenti si avrebbe che

$$b_i\in IQ_i\cap IP_i=IP_iQ_i=I\tilde{J}.$$

La prima uguaglianza segue dal fatto che $IQ_i\cap IP_i=\mathrm{mcm}(IQ_i,IP_i).$ Ora, fissato un indice i, scriviamo

$$b = b_i + \sum_{j \neq i} b_j .$$

Per ogni indice $j \neq i$, si ha $b_j \in IQ_j \subset IP_i$, in quanto P_i è uno dei fattori di Q_j. Pertanto $b \notin IP_i$, ossia IP_i non divide l'ideale (b). D'altra parte, però, essendo $b \in I$, l'ideale I divide l'ideale (b), esiste cioè un ideale J' tale che $IJ' = (b)$. Ma, per ogni $i = 1,...,s$, P_i non divide J', ossia J, J' sono coprimi. Ma allora

$$(a) + (b) = IJ + IJ' = I(J + J') = IA = I.$$

Ciò prova la nostra tesi.