Fattorizzazione — versione preliminare

GIOVANNI CUTOLO

1. FATTORIZZAZIONE

1.1. Qualche richiamo. Ricordiamo un pò di terminologia, notazioni e risultati elementari, le cui dimostrazioni saranno omesse. Fissiamo un monoide commutativo $(M, \cdot, 1_M)$. Se $a, b \in M$, si dice che a divide b (in M) se e solo se esiste $c \in M$ tale che $b = ac$; in simboli: $a|_M b$ o, più brevemente, $a|b$. Inoltre, a e b sono *associati* in M (e scriviamo $a \sim_M b$) se e solo se $a|_M b$ e $b|_M a$. Per ogni $a \in M$, con $\text{Div}_M(a)$ intendiamo l'insieme $\{x \in M \mid x|a\}$ dei divisori di a in M , mentre l'insieme $\{ax \mid x \in M\}$ dei multipli di a in M è indicato con aM . Con queste notazioni:

Lemma 1.1.1. *Per ogni $a, b \in M$ sono equivalenti:*

(i) $a \sim_M b$; (ii) $\text{Div}_M(a) = \text{Div}_M(b)$; (iii) $aM = bM$.

*Inoltre, se a è cancellabile in M , queste condizioni sono equivalenti a $(\exists u \in \mathcal{U}(M))(b = au)$.*¹

La relazione $\sim_M$ è di equivalenza in M , come si verifica direttamente dalla definizione o dalle caratterizzazioni nel lemma precedente. Inoltre essa è compatibile con la moltiplicazione in M (se $a, b, c \in M$ e $a \sim_M b$ allora $ac \sim_M bc$), dando così luogo al monoide quoziente $M/\sim_M$, che indichiamo con $\tilde{M}$. Per brevità, scriveremo spesso $\tilde{a}$ per la classe $[a]_{\sim_M}$ degli elementi associati di un elemento a di M .

Per ogni $a \in M$, tra i divisori di a ci sono i cosiddetti divisori banali: gli elementi invertibili di M e quelli associati ad a . Se $a \notin \mathcal{U}(M)$ e $\text{Div}_M(a) = \mathcal{U}(M) \cup [a]_{\sim_M}$ (vale a dire: i soli divisori di a in M sono quelli banali), allora si dice che a è *irriducibile* in M . Si dice invece che a è *primo* se e solo se $a \notin \mathcal{U}(M)$ e ogni volta che a divide un prodotto in M allora a divide almeno uno dei fattori: $(\forall b, c \in M)(a|bc \Rightarrow (a|b \text{ o } a|c))$. È facile provare che *ogni elemento primo di M è irriducibile*; il viceversa è in generale falso (si veda l'esempio presentato nell'[Esercizio A.3](#)). È altrettanto facile verificare che ciascuna delle proprietà di essere invertibile, irriducibile, primo è invariante per il passaggio ad associati, nel senso che se $a, b \in M$, allora a verifica la proprietà in questione se e solo se b verifica la stessa proprietà. Meglio ancora: a verifica la proprietà nel monoide M se e solo se $\tilde{a}$ verifica la stessa proprietà in $\tilde{M}$.

Se M è un monoide commutativo cancellativo (in cui, cioè, ogni elemento è cancellabile), si dice che M è *fattoriale* se e solo se è verificata una delle seguenti tre proprietà, tra loro equivalenti:

F₁): ogni elemento non invertibile di M è prodotto di primi.

F₂): ogni elemento non invertibile di M è prodotto di irriducibili, ed ogni irriducibile è primo.

F₃): ogni elemento non invertibile di M è prodotto di irriducibili, in modo essenzialmente unico.

Chiariamo il significato dell'ultima espressione. Se un elemento a è espresso come prodotto di elementi di M in due modi: $x_1 x_2 \cdots x_r = a = y_1 y_2 \cdots y_s$, diciamo che queste due fattorizzazioni sono 'essenzialmente uguali' se e solo se $r = s$ ed esiste una permutazione $\sigma \in \mathbb{S}_r$ tale che $x_i \sim_M y_{i\sigma}$ per ogni $i \in \{1, 2, \dots, r\}$. In altri termini: il numero dei fattori nelle due fattorizzazioni è lo stesso ed è possibile riordinare i fattori y_i in modo che ciascuno degli x_i sia associato in M al corrispondente fattore y_i . Dire che a ha essenzialmente una unica fattorizzazione in irriducibili vuol dire che due qualsiasi fattorizzazioni di a come prodotto di irriducibili devono risultare essenzialmente uguali.

Conseguenza immediata della definizione è che in un monoide fattoriale le proprietà di essere irriducibile e quella di essere primo sono equivalenti.

Esercizi ed Esempi.

A.1. Verificare in dettaglio tutte le affermazioni fatte in questa sezione.

A.2. Verificare che se $M \simeq (\mathbb{Z}, \cdot, 1)$ allora $\tilde{M} \simeq (\mathbb{N}, \cdot, 1)$.

A.3. Sia P il sottomonoido di $(\mathbb{N}^+, \cdot)$ costituito da 1 e dai numeri pari. Descrivere gli elementi irriducibili di P , e verificare che in P non esistono elementi primi. Dedurre che P è un monoide commutativo cancellativo in cui ogni elemento non invertibile (cioè diverso da 1) è prodotto di

¹ $\mathcal{U}(M)$ denota il gruppo degli invertibili di M .

irriducibili, ma non è un monoide fattoriale. Trovare qualche elemento che abbia in P fattorizzazioni in irriducibili che non sono essenzialmente uguali.

A.4. Sia M un monoide commutativo cancellativo, e sia a un elemento cancellabile di M . Allora:

- i) ogni divisore di a è cancellabile;
- ii) due qualsiasi fattorizzazioni di a come prodotto di primi in M sono essenzialmente uguali.

1.2. Una caratterizzazione dei monoidi fattoriali in termini di ordinamenti. Un *preordinamento* in un insieme S è una relazione binaria in S che sia riflessiva e transitiva. Se σ è un preordinamento in S , si può definire in S una relazione binaria ρ ponendo, per ogni $a, b \in \sigma$, $a \rho b$ se e solo se $a \sigma b$ e $b \sigma a$. È facile verificare che ρ è una relazione di equivalenza (che si dice associata a σ) e che σ induce una relazione d'ordine (largo) σ^* nel quoziente S/ρ definita ponendo, per ogni $a, b \in S$, $[a]_\rho \sigma^* [b]_\rho$ se e solo se $a \sigma b$.

Un esempio di questa costruzione l'abbiamo già per le mani: la relazione di divisibilità in un (arbitrario) monoide commutativo M è un preordinamento e la relazione di equivalenza associata a questa è, evidentemente, la relazione $\sim_M$ 'essere elementi associati'. La relazione d'ordine indotta nel quoziente $M/\sim_M = \tilde{M}$ dalla divisibilità in M non è altro che la relazione di divisibilità in $\tilde{M}$, che è così un ordinamento, in accordo col fatto che $\tilde{M}$ ha un unico elemento invertibile, il suo elemento neutro $\tilde{1}$ (a questo proposito può essere utile esaminare l'Osservazione B.2).

Siano $a, b \in M$. Un elemento $d \in M$ divide a (in M) se e solo se $\tilde{d}$ divide $\tilde{a}$ in $\tilde{M}$. Da ciò e dall'analogia osservazione per b al posto di a segue facilmente che d è un massimo comun divisore (MCD) tra a e b in M se e solo se $\tilde{d}$ è un MCD tra $\tilde{a}$ e $\tilde{b}$ in $\tilde{M}$. Poiché la divisibilità è una relazione d'ordine in $\tilde{M}$ quest'ultima affermazione equivale a dire che $\tilde{d}$ è l'estremo inferiore di $\{\tilde{a}, \tilde{b}\}$ nell'insieme ordinato $(\tilde{M}, |)$. Ciò suggerisce di usare la notazione consueta in teoria dei reticoli e scrivere $\tilde{d} = \tilde{a} \wedge \tilde{b}$ per indicare che d è un MCD tra a e b . In modo del tutto analogo, per ogni $m \in M$ abbiamo che m è un minimo comune multiplo (mcm) tra a e b se e solo se $\tilde{m}$ è un mcm tra $\tilde{a}$ e $\tilde{b}$, ovvero $\tilde{m} = \tilde{a} \vee \tilde{b}$ è l'estremo superiore di $\{\tilde{a}, \tilde{b}\}$ in $(\tilde{M}, |)$.

Un richiamo sembra opportuno: l'insieme dei MCD tra due elementi è, in generale, una classe di elementi associati, quindi se d è un MCD tra a e b allora $\tilde{d}$ è l'insieme di tutti i MCD tra a e b in M . Nel passaggio a $\tilde{M}$ si guadagna in definizione: le classi di elementi associati sono singleton, quindi, sempre nel caso in cui d sia un MCD tra a e b , $\tilde{d}$ sarà l'unico MCD tra $\tilde{a}$ e $\tilde{b}$ in $\tilde{M}$. Analogo discorso vale per i mcm.

Ci occupiamo ora del problema dell'esistenza o meno di un MCD o di un mcm per due elementi di un monoide commutativo M . Come ben noto l'esistenza di questi non è generalmente garantita neanche nel caso in cui M sia cancellativo, ma lo è nel caso dei monoidi fattoriali. Infatti, se M è fattoriale e $a, b \in M$, esistono $n \in \mathbb{N}$, elementi irriducibili $p_1, p_2, \dots, p_n$ di M a due a due non associati tra loro ed interi $\alpha_1, \alpha_2, \dots, \alpha_n, \beta_1, \beta_2, \dots, \beta_n \in \mathbb{N}$ tali che $a = \prod_1^n p_i^{\alpha_i}$ e $b \sim_M \prod_1^n p_i^{\beta_i}$. In questo caso, posto $\delta_i = \min\{\alpha_i, \beta_i\}$ e $\mu_i = \max\{\alpha_i, \beta_i\}$ per ogni $i \in \{1, 2, \dots, n\}$, si ha che $\prod_1^n p_i^{\delta_i}$ e $\prod_1^n p_i^{\mu_i}$ sono rispettivamente un MCD ed un mcm tra a e b . Questo ovviamente prova che se M è un monoide fattoriale allora $\tilde{M}$, ordinato per divisibilità, è un reticolo. Dimosteremo che questa proprietà quasi caratterizza i monoidi fattoriali.

L'esistenza di MCD e l'esistenza di mcm in un monoide fattoriale non sono affatto condizioni indipendenti tra loro, come stiamo per verificare. Introduciamo una notazione che utilizzeremo nelle prossime dimostrazioni. Se a e b sono elementi di un monoide commutativo M in cui a sia cancellabile e $a|b$, allora esiste un unico $c \in M$ tale che $b = ac$. In queste condizioni (ma solo in queste) indicheremo tale c con $\left[\frac{b}{a}\right]$. Dunque, se a è cancellabile, $b = a\left[\frac{b}{a}\right]$ equivale a $a|b$.

Proposizione 1.2.1. *Sia M un monoide cancellativo.*

- (i) *Per ogni $a, b \in M$, se esiste un mcm m tra a e b , allora esiste un MCD d tra a e b , e si ha $ab \sim_M dm$.*
- (ii) *Se per ogni $a, b \in M$ esiste un MCD tra a e b , allora per ogni $a, b \in M$ esiste un mcm tra a e b .*

Dimostrazione. Siano $a, b \in M$, ed esista $m \in M$ tale che $\tilde{m} = \tilde{a} \vee \tilde{b}$. Poiché m divide ab , possiamo porre $d = \left[\frac{ab}{m}\right]$, dunque $md = ab$. Da quest'ultima uguaglianza seguono $b = \left[\frac{m}{a}\right]d$ e $a = \left[\frac{m}{b}\right]d$, dunque d divide sia a che b . Sia e un arbitrario divisore comune ad a e b . Posto $n := a\left[\frac{b}{e}\right]$ abbiamo $ne = ab = b\left[\frac{a}{e}\right]e$, quindi, per la regolarità di M , $n = b\left[\frac{a}{e}\right]$. Dunque n è un multiplo comune ad a e b , quindi $m|n$. Da

$ne = ab = md$ segue $\left[\frac{n}{m}\right]e = d$, quindi $e|d$. È così provato che d è un MCD tra a e b ; la dimostrazione di (i) è completa.

Proviamo ora (ii). Nell'ipotesi di (ii), siano $a, b \in M$ e $\tilde{d} = \tilde{a} \wedge \tilde{b}$. Abbiamo $a\left[\frac{b}{\tilde{d}}\right] = b\left[\frac{a}{\tilde{d}}\right]$, perché moltiplicando per d ciascuno dei due membri si ottiene ab . Chiamando questo elemento m , abbiamo così $ab = md$. Chiaramente $a|m$ e $b|m$; proveremo che $\tilde{m} = \tilde{a} \vee \tilde{b}$. Sia n un multiplo comune ad a e b . Per ipotesi, n ed m hanno in M un MCD, chiamiamolo n_1 . Chiaramente, a e b dividono n_1 che a sua volta divide m . Allora $n_1\left[\frac{m}{n_1}\right]d = ab = n_1\left[\frac{a}{n_1}\right]b$, da cui $\left[\frac{m}{n_1}\right]d = \left[\frac{a}{n_1}\right]b$. Quindi $e := \left[\frac{m}{n_1}\right]d|b$; allo stesso modo $e|a$ e quindi, poiché $\tilde{d} = \tilde{a} \wedge \tilde{b}$, abbiamo $e|d$. Pertanto $e \sim_M d$ e così $\left[\frac{m}{n_1}\right] = \left[\frac{e}{d}\right]$ è invertibile. Di conseguenza $m \sim_M n_1$ e quindi $m|n$. Concludiamo che $\tilde{m} = \tilde{a} \vee \tilde{b}$; la dimostrazione è ora completa. $\square$

Può sorprendere la mancanza di simmetria tra le due parti dell'enunciato della [Proposizione 1.2.1](#): l'esistenza di un mcm per una coppia di elementi di M comporta l'esistenza del corrispondente MCD; per ottenere l'implicazione inversa abbiamo richiesto che *tutte* le coppie di elementi di M abbiano un mcm. L'esempio costruito nell'[Esercizio B.4](#) mostra che questa asimmetria è inevitabile: è possibile che, in un monoide commutativo cancellativo, due elementi abbiano un MCD ma non un mcm.

Abbiamo comunque dimostrato che le condizioni di esistenza di MCD e mcm, considerate globalmente, sono equivalenti. Abbiamo così:

Corollario 1.2.2. *Se M è un monoide commutativo cancellativo, sono equivalenti le proprietà:*

- (i) $\tilde{M}$, ordinato per divisibilità, è un reticolo.
- (ii) Per ogni $a, b \in M$, esiste un MCD tra a e b in M (vale a dire: $\tilde{M}$ è un inf-semireticolo).
- (iii) Per ogni $a, b \in M$, esiste un mcm tra a e b in M (vale a dire: $\tilde{M}$ è un sup-semireticolo).

Assumendo che M sia cancellativo, l'ipotesi che $\tilde{M}$ sia un reticolo, ovvero che in M ogni coppia di elementi abbia un MCD, implica che ogni irriducibile in M è primo. Il primo passo per la dimostrazione è questo lemma:

Lemma 1.2.3. *Siano a, b, c elementi di un monoide commutativo cancellativo M . Sia d un MCD tra a e b in M . Supponiamo che anche ac e bc abbiano un MCD e in M . Allora $e \sim_M cd$.*

Dimostrazione. Ovviamente dc è un divisore comune ad ac e bc , quindi $dc|e$. Da $e = dc\left[\frac{de}{e}\right]|ac$ segue, cancellando c , $d\left[\frac{dc}{e}\right]|a$. Allo stesso modo si ottiene $d\left[\frac{dc}{e}\right]|b$. Di conseguenza $d\left[\frac{dc}{e}\right]$ divide il MCD d tra a e b ; quindi $\left[\frac{dc}{e}\right]$ è invertibile ed $e \sim_M cd$. $\square$

Il precedente enunciato sembra del tutto ovvio (lo è ad esempio, nell'ipotesi che M sia fattoriale), e potrebbe sorgere il dubbio che l'ipotesi che esista un MCD tra ac e bc sia superflua. Non è così, l'esistenza di un MCD tra a e b non garantisce quella di un MCD tra ac e bc ; un esempio è dato nell'[Esercizio B.5](#).

Lemma 1.2.4. *Sia M un monoide cancellativo e supponiamo che $\tilde{M}$, ordinato per divisibilità sia un reticolo. Allora, in M , ogni irriducibile è primo.*

Dimostrazione. Assunta l'ipotesi, sia p un irriducibile in M . Allora $p \notin \mathcal{U}(M)$. Per ogni $a, b \in M$, se $p|ab$ e $p \nmid a$ abbiamo ovviamente $\tilde{1} = \tilde{a} \wedge \tilde{p}$, dunque $\tilde{b} = \tilde{a}\tilde{b} \wedge \tilde{p}\tilde{b}$, per il [Lemma 1.2.3](#). Ma p divide sia ab che $p\tilde{b}$, quindi $p|b$. È così provato che p è primo. $\square$

Lemma 1.2.5. *Sia M un monoide cancellativo e supponiamo che $\tilde{M}$, ordinato per divisibilità verifichi la condizione minimale. Allora, in M , ogni elemento non invertibile è prodotto di irriducibili.*

Dimostrazione. Supposta la tesi falsa, esiste in $\tilde{M}$ un elemento $\tilde{a}$ minimale (rispetto a $|\cdot|$) per la proprietà che a non sia invertibile né prodotto di irriducibili. Allora a non è irriducibile, quindi esistono $b, c \in M \setminus \mathcal{U}(M)$ tali che $a = bc$. La minimalità di $\tilde{a}$ garantisce che sia b che c sono prodotti di irriducibili in M , quindi lo stesso vale per a . Questa è una contraddizione. $\square$

Mettendo assieme i risultati ottenuti negli ultimi due lemmi arriviamo al risultato principale di questa sezione.

Teorema 1.2.6. *Sia M un monoide commutativo cancellativo. Allora M è fattoriale se e solo se $\tilde{M}$, ordinato per divisibilità, è un reticolo a condizione minimale.*

Dimostrazione. Se $\tilde{M}$ è un reticolo a condizione minimale, allora i due lemmi precedenti mostrano che ogni elemento non invertibile di M è prodotto di irriducibili e tutti gli irriducibili di M sono primi; dunque M è fattoriale. Viceversa, supponiamo che M sia fattoriale. Abbiamo già osservato che in questo caso ogni coppia di elementi di M ha MCD, quindi $(\tilde{M}, |)$ è un reticolo. Allora ad ogni $a \in M$ possiamo univocamente associare un intero $\tau(a)$ in modo che a sia il prodotto di $\tau(a)$ irriducibili in M (intendendo $\tau(a) = 0$ se a è invertibile). Sia $(\tilde{a}_n)_{n \in \mathbb{N}}$ una successione strettamente decrescente in $(\tilde{M}, |)$. Allora, per ogni $n \in \mathbb{N}$, a_{n+1} è un divisore proprio di a_n in M , e quindi $\tau(a_{n+1}) < \tau(a_n)$. La successione $(\tau(a_n))_{n \in \mathbb{N}}$ è così una successione strettamente decrescente di numeri naturali; questa è una contraddizione. Concludiamo che non esiste alcuna successione strettamente decrescente in $(\tilde{M}, |)$, vale a dire: $(\tilde{M}, |)$ verifica la condizione minimale. A questo punto la dimostrazione è completa. $\square$

Corollario 1.2.7. *Sia M un monoide commutativo cancellativo. Allora M è fattoriale se e solo se $\tilde{M}$, è fattoriale.*

Dimostrazione. Posto $M_1 = \tilde{M}$, abbiamo ovviamente $\tilde{M}_1 \simeq \tilde{M}$. Dunque, per il [Teorema 1.2.6](#), $\tilde{M}$ è fattoriale se e solo se $\tilde{M}$, ordinato per divisibilità, è un reticolo a condizione minimale, ma, per lo stesso teorema, questo equivale all'essere M fattoriale. $\square$

Infine, richiamiamo un pò di terminologia utile. Se M è fattoriale, i suoi elementi irriducibili sono gli a tali che $\tilde{a}$ sia un *atomo* nel reticolo, cioè un elemento minimale tra quelli diversi dal minimo $\tilde{1}$. Dualmente, in un reticolo con massimo si chiamano *coatomi* gli elementi massimali nel reticolo tra quelli diversi dal massimo.

Esercizi, Esempi, Osservazioni.

B.1. Verificare in dettaglio tutte le affermazioni fatte e non dimostrate in questa sezione.

B.2. Se M è un monoide commutativo, la relazione di divisibilità non è, in generale, d'ordine; lo è se e solo se $\sim_M$ è l'uguaglianza. In questo caso, l'unità è l'unico elemento invertibile di M . Se M è cancellativo questa condizione si inverte: la divisibilità in M è una relazione d'ordine se e solo se $\mathcal{U}(M) = \{1_M\}$. Nel caso generale questa equivalenza non vale; chi è interessato può verificarlo con l'esempio fornito al prossimo esercizio.

B.3. Si definisca sull'insieme $S = \mathbb{N} \times \mathbb{N}$ un'operazione binaria $*$ ponendo, per ogni $u, v, s, t \in \mathbb{N}$, $(u, v) * (s, t) = (u + s, r)$, dove r è $v + t$ se $u = s = 0$, il resto di $v + t$ modulo 2, altrimenti. Si verifichi che $(S, *, (0, 0))$ è un monoide commutativo e che in S esiste un solo elemento invertibile (quello neutro), ma gli elementi $a = (1, 0)$ e $b = (1, 1)$ sono associati. In questo monoide, dunque, la relazione di divisibilità non è d'ordine.

B.4. In questo esercizio viene costruito un monoide commutativo cancellativo M , generato da elementi a, b, c, d con la proprietà che a e c siano coprimi, ed abbiano quindi un MCD, ma non abbiano un mcm.

Sia F il gruppo abeliano libero sulla base $\{a_0, b_0, c_0, d_0\}$. Siano poi H is sottogruppo di F generato da $a_0 b_0 c_0^{-1} d_0^{-1}$ e $P = \{a_0^\alpha b_0^\beta c_0^\gamma d_0^\delta \mid \alpha, \beta, \gamma, \delta \in \mathbb{N}\}$ (P è un monoide commutativo libero sulla base $\{a_0, b_0, c_0, d_0\}$). È chiaro che $M := PH/H$ è un monoide commutativo cancellativo (perché immerso nel gruppo F/H) generato da $a := a_0 H$, $b := b_0 H$, $c := c_0 H$, $d := d_0 H$, in cui vale l'uguaglianza $ab = cd$. Si provi che ciascuno di a, b, c, d è irriducibile, quindi 1 è un MCD tra a e c , ma non esistono mcm tra a e c .

Suggerimento: si può osservare che se, per $i \in \{1, 2\}$, poniamo $x_i = a^{\alpha_i} b^{\beta_i} c^{\gamma_i} d^{\delta_i}$, dove gli esponenti sono interi arbitrari, abbiamo $x_1 = x_2$ se e solo se $\alpha_1 - \alpha_2 = \beta_1 - \beta_2 = \gamma_2 - \gamma_1 = \delta_2 - \delta_1$. Da ciò si può dedurre che un elemento $x = a^\alpha b^\beta c^\gamma d^\delta$ di F/H è in M se e solo se esiste $\lambda \in \mathbb{Z}$ tale che $\alpha + \lambda, \beta + \lambda, \gamma - \lambda$ and $\delta - \lambda$ siano tutti non negativi, ovvero: $\min\{\alpha, \beta\} \geq \max\{-\gamma, -\delta\}$. Visto ciò, diventa facile stabilire se due assegnati elementi di M si dividano o meno (e 1 è l'unico elemento invertibile di M), ed arrivare alle conclusioni desiderate.

B.5. In questo esercizio viene costruito un monoide commutativo cancellativo M , con elementi a, b, c in cui esiste un MCD tra a e b ma non esiste un MCD tra ac e bc . La costruzione è simile a quella in [Esercizio B.4](#), ma un pò più elaborata.

Sia F il gruppo abeliano libero di rango 7, sulla base $\{x_1, x_2, \dots, x_7\}$. Siano poi H il sottogruppo di F generato da $x_1 x_3 x_4 x_5^{-1} x_6^{-1}$ e $x_2 x_3 x_4 x_5^{-1} x_7^{-1}$. Sia poi $P = \{\prod_{i=1}^7 x_i^{\alpha_i} \mid (\forall i \in \{1, 2, \dots, 7\})(\alpha_i \in \mathbb{N})\}$, il monoide (libero) generato in F da $x_1, \dots, x_7$, e sia $M = PH/H$. Allora M è un monoide

commutativo cancellativo. Ponendo $a = x_1x_4H$, $b = x_2x_4H$, $c = x_3H$, si verifichi che $d := x_4H$ è un MCD in M tra a e b , ma ac e bc non hanno un MCD in M .

Suggerimento: si osservi che ogni elemento di F/H può essere rappresentato (unicamente) come xH , dove $x = \prod_{i=1}^5 x_i^{\alpha_i}$ per opportuni interi $\alpha_1, \dots, \alpha_5$. Si verifichi che questo elemento è in M se e solo se si ha: $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \geq 0$ e $\alpha_1 + \alpha_2, \alpha_3, \alpha_4 \geq -\alpha_5$. A questo punto è facile verificare che l'unità H di M e d sono gli unici divisori comuni ad a e b . Inoltre x_5H divide ac e bc ma non cd , quindi cd non è un MCD tra ac e bc .

1.3. Applicazioni agli anelli. Sia R un anello commutativo unitario non nullo; indichiamo con $\mathfrak{P}(R)$ l'insieme degli ideali principali di R , ordinato per inclusione. Consideriamo l'applicazione $\varphi: a \in R \mapsto aR \in \mathfrak{P}(R)$. Chiaramente φ è suriettiva. Inoltre, se a e b sono in R , si ha $aR = bR$ se e solo se $a \sim_R b$, cioè se e solo se a e b sono associati nel monoide moltiplicativo di R . In altri termini, il nucleo di equivalenza di φ è la relazione $\sim_R$, dunque φ induce un'applicazione biettiva $\tilde{\varphi}: \tilde{R} \mapsto \mathfrak{P}(R)$, dove abbiamo posto (come faremo d'ora in poi) $\tilde{R} = R/\sim_R$. È anche chiaro che $\tilde{\varphi}$ è (strettamente) decrescente, quindi un anti-isomorfismo da $\tilde{R}$ (che è ordinato per divisibilità) a $\mathfrak{P}(R)$.

Questo anti-isomorfismo permette di stabilire una connessione tra proprietà di ideali (principali) in anelli commutativi unitari e proprietà relative alla divisibilità nei corrispondenti monoide moltiplicativi. Ad esempio, con le notazioni fissate nel paragrafo precedente, un elemento $a \in R$ è irriducibile se e solo se $\tilde{a}$ è minimale tra gli elementi diversi da $\tilde{1}$ in $\tilde{R}$, quindi se e solo se $(\tilde{a})^{\tilde{\varphi}}$, ovvero aR , è massimale tra gli ideali principali diversi da $(\tilde{1})^{\tilde{\varphi}} = R$. Dunque, per ogni $a \in R$,

$$a \text{ è irriducibile in } R \iff aR \text{ è massimale tra gli ideali principali propri di } R$$

A titolo di comparazione, è ovvio che, se $a \neq 0$,

$$a \text{ è primo in } R \iff aR \text{ è un ideale primo di } R.$$

Una applicazione piuttosto elegante dell'anti-isomorfismo φ e dei risultati nella sezione precedente permette di ricavare immediatamente alcuni risultati elementari sugli anelli principali, vediamo come.

Se R è un dominio di integrità unitario, $R^* = R \setminus 0$ è un sottomonoido moltiplicativo di R ed è cancellativo, e $\tilde{R}^*$ risulta anti-isomorfo, come insieme ordinato, all'insieme $\mathfrak{P}^*(R)$ degli ideali principali non nulli di R . Se R è anche principale, $\mathfrak{P}^*(R)$ è l'insieme degli ideali non nulli di R , che è un sottoreticolo del reticolo degli ideali (l'intersezione tra due ideali non nulli è certamente non nulla). Quindi, dal momento che R è noetheriano, $\mathfrak{P}^*(R)$ è un reticolo a condizione massimale; di conseguenza $\tilde{R}^*$ (anti-isomorfo a $\mathfrak{P}^*(R)$) è un reticolo a condizione minimale. Per il [Teorema 1.2.6](#), allora R^* è un monoide fattoriale; il che, ricordiamo, significa che R è un anello fattoriale. Dunque, otteniamo una rapida dimostrazione del fatto che *ogni anello principale è fattoriale*. Inoltre, dal fatto che per elementi non nulli di R le proprietà di essere primo e di essere irriducibile sono equivalenti, osservazioni fatte [poco sopra](#) garantiscono che gli ideali primi non nulli in un anello fattoriale sono necessariamente massimali (vale a dire: *gli anelli principali hanno dimensione di Krull al più 1*).

Anche il teorema di Bézout e le sue varianti possono essere ottenuti in modo simile. Siano a e b elementi di un anello commutativo unitario R . Poiché gli anti-isomorfismi tra insiemi ordinati mandano eventuali estremi inferiori in estremi superiori (e viceversa), per ogni $d \in R$ si ha $\tilde{d} = \tilde{a} \wedge \tilde{b}$ se e solo se dR è estremo superiore di aR e bR in $\mathfrak{P}(R)$, vale a dire: il minimo (rispetto all'inclusione) tra gli ideali principali di R contenenti aR e bR , cioè contenenti $aR + bR$. Dualmente, un $m \in R$ sarà un mcm tra a e b se e solo se mR è il massimo ideale principale contenuto in $aR \cap bR$. In particolare, per ogni $a, b \in R$:

$$\text{se } aR + bR \text{ è principale, allora i suoi generatori sono tutti e soli i MCD tra } a \text{ e } b \text{ in } R; \quad (B)$$

$$\text{se } aR \cap bR \text{ è principale, allora i suoi generatori sono tutti e soli i mcm tra } a \text{ e } b \text{ in } R; \quad (\hat{B})$$

Il primo enunciato, (B) è una delle tante versioni del *Teorema di Bézout*. Questo ed il suo duale ($\hat{B}$) si possono senz'altro applicare nel caso in cui R sia un anello principale, perché in questo caso l'ipotesi che l'ideale $aR + bR$ o $aR \cap bR$ è banalmente verificata. Per quanto riguarda (B), lo stesso vale nel caso in cui ogni ideale finitamente generato di R sia principale. I domini di integrità unitari con questa proprietà di chiamano *anelli di Bézout*. Ovviamente gli anelli principali sono anelli di Bézout; Il sottoanello di $\mathbb{Q}[x]$ costituito dai polinomi con termine noto intero è un esempio di anello di Bézout non principale (lo si può verificare per esercizio).