Corollario 6.8

Dato un anello commutativo unitario A, siano $a, b \in A$. Proviamo che sono equivalenti le seguenti condizioni:

i) a, b sono associati;
ii) a, b hanno gli stessi divisori;
iii) a, b hanno gli stessi multipli.

<u>Dimostrazione:</u> Supponiamo dapprima che a, b siano associati. Allora, se $d \in A$ è tale che $d|\ a$, essendo per ipotesi $a|b$, per transitività si deduce che $d|b$. Ciò prova che ogni divisore di a è divisore di b. Potendo invertire, nel ragionamento precedente, i ruoli di a e b, si prova allo stesso modo che ogni divisore di b è divisore di a. Dunque, in conclusione, coincidono l'insieme dei divisori di a e l'insieme dei divisori di b. Abbiamo così provato che i) $\Longrightarrow$ ii). La dimostrazione dell'implicazione i) $\Longrightarrow$ iii) è del tutto analoga, basta invertire, nella dimostrazione precedente, i termini nelle relazioni di divisibilità: supponendo che a, b siano associati, si consideri $m \in A$ tale che $a|\ m$; essendo per ipotesi $b|a$, per transitività si deduce che $b|m$. Ciò prova che ogni multiplo di a è multiplo di b. Potendo invertire, nel ragionamento precedente, i ruoli di a e b, si prova allo stesso modo che ogni multiplo di b è multiplo di a. Dunque, in conclusione, coincidono l'insieme dei multipli di a e l'insieme dei multipli di b.

Ora, supponiamo che a, b abbiamo gli stessi divisori. Poiché $a|a$, dovrà allora essere $a|b$. Poiché $b|b$, sarà dunque anche $b|a$. Quindi a, b sono associati. Ciò prova che ii) $\Longrightarrow$ i). In maniera analoga si prova iii) $\Longrightarrow$ i), leggendo le relazioni di divisibilità in termini di multipli anziché di divisori.

In sintesi, abbiamo provato che ii) e iii) sono individualmente equivalenti a i). Di conseguenza sono tra loro equivalenti, e quindi equivalenti alla loro congiunzione.