Sam Lloyd: 994940

MAST20022, Group Theory and Linear Algebra, Assignment 1

Q1:

(1) $a|b$, i.e. $a = qb$ for some $q \in \mathbb{Z}$

(2) $\gcd(a,b) = a$, i.e. $a|a \wedge a|b$,
$\langle c|a \wedge c|b \rangle \Rightarrow c|a$, for $\forall c \in \mathbb{Z}$

(1) $\Rightarrow$ (2)

Proof:

$a|b$, let $q=1$ in the definition

$a|a$, trivially $a = 1 \times a$

$\therefore a|b \wedge a|a$

let $c \in \mathbb{Z}$ such that $c|a \wedge c|b$

$\Rightarrow c|a$

$\therefore \langle c|a \wedge c|b \rangle \Rightarrow c|a$ □

(2) $\Rightarrow$ (1)

Proof:

$\gcd(a,b) = a \Rightarrow a|a \wedge a|b$

$\Rightarrow a|b$ □

Therefore (1) $\Leftrightarrow$ (2)

i.e. $a|b \Leftrightarrow \gcd(a,b) = a$