

Work in a fixed commutative monoid M with cancelation.

You may quote, without proof, any result proved in class.

1. Prove that if $[a, b]$ exists then for all c ,
 - (i) $[ac, bc] = [a, b]c$.
 - (ii) (a, b) exists, and $(ac, bc) = (a, b)c$.
2. Prove that $[a, b]$ exists $\iff (ac, bc)$ exists for all c .
3. Prove: if a is prime and a doesn't divide b then $[a^n, b] = a^n b$ for all n
4. Suppose a is a unit or a product of primes. Prove:
 - (i) (a, b) and $[a, b]$ exist for all b .
 - (ii) If (b, c) exists then $(ab, ac) = a(b, c)$.
5. Assume that (x, y) exists for all $x, y \in M$.
 - (i) Prove that if $(a, b) = 1$ then $(a^i, b^j) = 1$ for all (i, j) .
 - (ii) Without assuming $(a, b) = 1$, deduce from (i) that $(a, b)^n = (a^n, b^n)$ for all n .
 - (iii) Prove that if $(a, b) = 1$ and $ab = c^n$ then $a \sim (a, c)^n$ and $b \sim (b, c)^n$.
6. Assuming all the gcd's and lcm's that appear exist, prove the "distributivity laws":
 - (i) $[a, (b, c)] = ([a, b], [a, c])$, and
 - (ii) $(a, [b, c]) = [(a, b), (a, c)]$.

Hint. In (i), the hard part is to show that $([a, b], [a, c])$ divides $[a, (b, c)]$. For this, divide everything in sight by (a, b, c) —which exists (why?)—to reduce to where $(a, b, c) = 1$, in which case $[a, (b, c)] = (ab, ac)$.

Remarks. In a UFM, this problem is easily dealt with by means of prime-power factorizations.

To see all this in an even more abstract setting, look at Thm. 3 on p. 135 (or the note on p. 133) in Garrett Birkhoff's book *Lattice Theory*.