LATTICES OF SETS OF DIVISORS

Let n be a natural number and let D_n be the set of (natural) divisors of n. It can be proved the following result:

Theorem 1. *The ordered set $(D_n, \mid\,)$ (where $\mid$ denotes the divisibility relation) is a lattice that is **distributive** and **bounded**. The minimum is 1 and the maximum is n.*

Notice that, **in general**, not all the elements of D_n have complement. Therefore, $(D_n, \mid\,)$ is not always a Boolean lattice. We will see this in the following example.

Example 1. Consider the set D_{360} with the divisibility relation. The decomposition of 360 as a product of prime numbers is:

$$360 = 2^3 \cdot 3^2 \cdot 5 = 2^3 \cdot 3^2 \cdot 5^1.$$

Then, the number of divisors of 360 is $(3+1)(2+1)(1+1) = 24$. In fact:

$$D_{360} = \{1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 18, 20, 24, 30, 36, 40, 45, 60, 72, 90, 120, 180, 360\}.$$

Since D_{360} is a lattice, we have the operations:

$$a + b = \sup(\{a, b\}) = \mathrm{lcm}(a, b)$$

$$a \cdot b = \inf(\{a, b\}) = \gcd(a, b)$$

Notice that 360 has 6 prime factors (2,2,2,3,3 and 5) distributed into 3 blocks:

- Block of 2's (or red block): $2 \cdot 2 \cdot 2 = 2^3$
- Block of 3's (or blue block): $3 \cdot 3 = 3^2$
- Block of 5's (or green block): 5

There are two types of elements in D_{360}:

- Type 1: Those divisors whose decompositions as a products of prime factors **have only complete blocks of prime factors**. For example:

$$1 \;\; \text{(no block)}$$

$$2^3 = 8 \;\; \text{(red block)}$$

$$3^2 = 9 \;\; \text{(blue block)}$$

$$5 \;\; \text{(green block)}$$

$$2^3 \cdot 3^2 = 72 \;\; \text{(red block and blue block)}$$

$$2^3 \cdot 5 = 40 \;\; \text{(red and green blocks)}$$

$$3^2 \cdot 5 = 45 \;\; \text{(blue and green blocks)}$$

$$2^3 \cdot 3^2 \cdot 5 = 360 \;\; \text{(red, blue and green blocks)}$$

- Type 2: Those divisors which are not of type 1. For example:

$$2^2 = 4 \text{ (the red block is not complete)}$$

$$2^3 \cdot 3 = 24 \text{ (the blue block is not complete)}$$

$$2 \cdot 5 = 10 \text{ (the red block is not complete)}$$

$$2^2 \cdot 3 = 12 \text{ (red and blue blocks are not complete)}$$

It is very easy to deduce that the divisors of Type 1 have complement. For example:

- The complement of $8 = 2^3$ is $45 = 3^2 \cdot 5$ because:

$$8 + 45 = \text{lcm}(8, 45) = 360 \quad \text{and} \quad 8 \cdot 45 = \gcd(8, 45) = 1.$$

  (Notice that the operations $+$ and $\cdot$ are those previously defined!!!)

- The complement of $72 = 2^3 \cdot 3^2$ is 5 because:

$$72 + 5 = \text{lcm}(72, 5) = 360 \quad \text{and} \quad 72 \cdot 5 = \gcd(72, 5) = 1.$$

However, **the divisors of Type 2 have not complement!!** For example, let's prove that $2 \cdot 5 = 10$ has not complement reasoning **by contradiction**. So, assume that it has a complement $\overline{10}$ and let us deduce a contradiction:

Since $\overline{10}$ is the complement of 10, the following conditions must be satisfied: $\gcd(10, \overline{10}) = 1$ and $\text{lcm}(10, \overline{10}) = 360$. But $\gcd(10, \overline{10}) = 1$ means that 10 and $\overline{10}$ **have not common prime factors**. In particular, **2 is not a prime factor of** $\overline{10}$ (because 2 is a prime factor of 10). Therefore $\text{lcm}(10, \overline{10}) \neq 360$, which is **a contradiction!!** (notice that the least common multiple is the product of all prime factors appearing either in 10 or $\overline{10}$ with the maximum exponent; and the maximum exponent of 2 is 1 because 2 is not a prime factor of $\overline{10}$).

It is easy to deduce that a similar reasoning can be applied to any divisor of Type 2. Therefore these divisors have not complement in D_{360}.

This example shows a general behavior:

Theorem 2. *The elements of lattice D_n that have complement are those whose decompositions into primes involve "complete blocks" of prime factors of n.*

Then, if all the prime numbers in the decomposition of n have exponent 1, it is evident that every element of D_n has complement (for example, when $n = 2 \cdot 3 \cdot 5 \cdot 7$). Therefore we have the following consequence (that characterizes when D_n is a Boolean lattice):

Corollary 1. *$(D_n, |\,)$ is a Boolean lattice if and only if all the prime numbers in the decomposition of n have exponent 1.*