1.3. **Dirichlet product and Möbius inversion.** Dirichlet product will be a handy tool for establishing Möbius inversion.

Definition 1.22. Let $f, g : \mathbb{Z}^+ \to \mathbb{C}$ be two arithmetic functions. The *Dirichlet product* (or *Dirichlet convolution*) of f and g is the arithmetic function $f * g$ defined by the formula

$$(f * g)(n) = \sum_{d_1 d_2 = n} f(d_1) g(d_2)$$

where the sum runs over all pairs (d_1, d_2) of positive integers such that $d_1 d_2 = n$.

Remark 1.23. Another equivalent way of writing the formula is

$$(f * g)(n) = \sum_{d \mid n} f(d) g(\frac{n}{d}),$$

where the sum is over all positive divisors d of n. We will use both formulas in the following discussion.

The Dirichlet product has many nice properties. In particular, it is commutative and associative, as we expect for any "product".

Lemma 1.24. *Let $f, g, h : \mathbb{Z}^+ \to \mathbb{C}$ be arithmetic functions, then*

$$f * g = g * f$$
$$(f * g) * h = f * (g * h).$$

Proof. Commutativity is immediate. Indeed, for any $n \in \mathbb{Z}^+$, we have

$$(f * g)(n) = \sum_{d_1 d_2 = n} f(d_1) g(d_2) = \sum_{d_2 d_1 = n} g(d_2) f(d_1) = (g * f)(n).$$

Associativity requires some more manipulations. For any $n \in \mathbb{Z}^+$, we show that both expressions $((f * g) * h)(n)$ and $(f * (g * h))(n)$ can be transformed into the summation $\sum_{d_1 d_2 d_3 = n} f(d_1) g(d_2) h(d_3)$, where the sum runs over all 3-tuples (d_1, d_2, d_3) of positive integers such that $d_1 d_2 d_3 = n$.

For the left-hand side, we have

$$\begin{aligned} ((f * g) * h)(n) &= \sum_{d_0 d_3 = n} (f * g)(d_0) h(d_3) \\ &= \sum_{d_0 d_3 = n} \left(\sum_{d_1 d_2 = d_0} f(d_1) g(d_2) \right) h(d_3) \\ &= \sum_{d_1 d_2 d_3 = n} f(d_1) g(d_2) h(d_3). \end{aligned}$$

The computation for the right-hand side is similar and gives the same expression. So we are done. $\square$

Example 1.25. Here are some simple examples of Dirichlet products:

(1) Let $\mathbb{I}$ be the function defined in Example 1.17 and f an arbitrary arithmetic function, then
$$\mathbb{I} * f = f * \mathbb{I} = f;$$

(2) Let I be the function with constant value 1 and f an arbitrary arithmetic function, then for every $n \in \mathbb{Z}^+$, we have
$$(f * I)(n) = \sum_{d \mid n} f(d);$$

(3) In particular, let f be the μ-function defined in Definition 1.20, then by Proposition 1.21 we have
$$\mu * I = I * \mu = \mathbb{I}.$$

We are ready to prove the following theorem:

Theorem 1.26 (Möbius Inversion Theorem)**.** *Let $f : \mathbb{Z}^+ \to \mathbb{C}$ be an arithmetic function. If we define the arithmetic function $F : \mathbb{Z}^+ \to \mathbb{C}$ by*
$$F(n) = \sum_{d \mid n} f(d),$$
then we have
$$f(n) = \sum_{d \mid n} \mu(d) F(\frac{n}{d}).$$

Proof. We use the full power of Lemma 1.24 and Example 1.25. The definition of F shows $F = f * I$. Then we have
$$f = f * \mathbb{I} = f * (I * \mu) = (f * I) * \mu = F * \mu = \mu * F,$$
which is what we want by Remark 1.23. $\square$

As an immediate application of the theorem, we use it to obtain a formula for yet another important arithmetic function: the Euler ϕ-function.

Definition 1.27. The Euler ϕ-function is defined to be the following arithmetic function: for any $n \in \mathbb{Z}^+$, $\phi(n)$ is the number of integers m with $1 \leqslant m \leqslant n$ and $\mathrm{hcf}(m, n) = 1$.

We first prove the following simple property of the ϕ-function.

Proposition 1.28. *For any $n \in \mathbb{Z}^+$, the Euler ϕ-function satisfies the identity*
$$\sum_{d \mid n} \phi(d) = n.$$

Proof. Consider the n rational numbers

$$\frac{1}{n}, \frac{2}{n}, \cdots, \frac{n-1}{n}, \frac{n}{n}.$$

Reduce each to lowest terms; i.e. perform cancellations to express each number as a quotient of relatively prime integers. The denominators will all be divisors of n. If $d \mid n$, there are exactly $\phi(d)$ of our numbers whose denominators are equal to d after reducing to lowest terms. Thus they sum up to n, as desired. □

We can obtain a formula for the ϕ-function by Möbius inversion theorem.

Proposition 1.29. *Let $n = p_1^{a_1} p_2^{a_2} \cdots p_l^{a_l}$ be the factorisation of $n \in \mathbb{Z}^+$ where $p_1, p_2, \cdots, p_l$ are distinct primes, then*

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_l}\right).$$

Proof. By Theorem 1.26 and Proposition 1.28, we have that

$$\begin{aligned}
\phi(n) &= \sum_{d \mid n} \mu(d) \frac{n}{d} \\
&= n - \sum_i \frac{n}{p_i} + \sum_{i<j} \frac{n}{p_i p_j} - \sum_{i<j<k} \frac{n}{p_i p_j p_k} + \cdots \\
&= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_l}\right),
\end{aligned}$$

as desired. □

Remark 1.30. Using the same factorisation of n, we can also write the formula for Euler ϕ-function in a slightly different form:

$$\phi(n) = p_1^{a_1-1} p_2^{a_2-1} \cdots p_l^{a_l-1} (p_1 - 1)(p_2 - 1) \cdots (p_l - 1).$$

Indeed, we can substitute n by its prime factorisation in the previous formula and cancel all denominators with the corresponding prime factors in n to get this formula. Caution: it does not imply that each p_i is still a prime factor of $\phi(n)$ because the exponent $a_i - 1$ could be zero.