Abstract Algebra

Trong

January 17, 2019

Contents

1 Möbius Function **1**

2 Semigroup **2**

1 Möbius Function

Proposition 1. *For every natural number n define the Möbius function*

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 & (I) \\ 0 & \text{if } p^2 | n \text{ for some prime } p & (II) \\ (-1)^k & \text{if } n = p_1 \cdots p_k \text{ for distinct primes } p_i. & (III) \end{cases}$$

Then μ is multiplicative, i.e. for $(m, n) = 1$,

$$\mu(mn) = \mu(m)\mu(n).$$

Furthermore,

$$\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}. \tag{IV}$$

Proof. Multiplicativity is easy to check if either m or n satisfies (I) or (II). Therefore suppose $m = p_1 \cdots p_k$ and $n = q_1 \cdots q_l$ are each a product of distinct primes. Since $(m, n) = 1$, $p_1, \ldots, p_k, q_1, \ldots, q_l$ are in fact all distinct primes. Then

$$\mu(mn) = (-1)^{k+l} = (-1)^k(-1)^l = \mu(m)\mu(n).$$

To show (IV), recall the formula

$$\begin{aligned}\varphi(n) &= n\Big(1-\frac{1}{p_1}\Big)\cdots\Big(1-\frac{1}{p_k}\Big)\\ &= n - \frac{n}{p_1} - \cdots + \frac{n}{p_1p_2} + \cdots + (-1)^k\frac{n}{p_1\cdots p_k},\end{aligned} \tag{V}$$

where p_i are all the distinct primes of n. Note that every term in this expansion has the form

$$(-1)^j\frac{n}{q_1\cdots q_j} = \mu(d)\frac{n}{d}$$

where the q_i are some subset of $p_1, \dots, p_k$. This accounts for the divisors d of n of the form (I) and (III). We can ignore divisors of the form (II) in (IV) since in those cases $\mu(d) = 0$. Therefore the terms in (V) are precisely the same ones in (IV). ■

2 Semigroup

Definition 2. *A semigroup is a set S with a product which associates to each ordered pair $a, b \in S$ a product ab s.t. associativity holds: $(ab)c = a(bc)$ for any $a, b, c \in S$. In other words, a semigroup is like a group without existence of an identity or inverses.*

Example 3. The set of all mappings of a set X to itself forms a semigroup in which the product is composition of mappings. The set of all one-to-one mappings of a set X to itself forms a group under composition.

Proof. Composition of mappings is associative. One-to-one mappings furnish the identity map and inverses. ■

Proposition 4. *Suppose S is a semigroup with a finite number of elements that obey the Cancellation Laws: if either $ab = ac$ or $ba = ca$, then $b = c$. Then S is a group.*

Proof. For simplicity let $S = \{a, b, c, d, e\}$ consist of 5 elements, where 5 is arbitrary. First we want to show that S contains an identity element. Consider the elements

$$a, aa, aaa, 4a, 5a, 6a.$$

Since S is finite, by Pigeonhole two of these must be the same, say

$$2a = 5a.$$

By Cancellation,

$$a = 4a,$$

so $3a$ is our tentative identity, at least as far as a is concerned. Now to show that it works for b as well:

$$\begin{aligned} 2a &= 5a \\ 2ab &= 5ab \\ b &= 3ab, \end{aligned}$$

IOW, $3a$ is an identity for b too. Arguing similarly for the other elements, we see that $3a$ is an identity for S. Similar arguments will show that every element of S has an inverse, and hence S is a group. ∎