FACTORIAL MONOIDS

A ring $(A, +, \cdot)$ has the following properties
1) $(A, +)$ is an abelian group
2) $(A^*, \cdot)$ is a monoid
3) The binary operations $\cdot$ and $+$ satisfy distributive properties

Note that a multiplicative identity exists because $(A, \cdot)$ is a monoid.

Examples: $(\mathbb{Z}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ are rings.

For a monoid M, the set of elements in M which are invertible is denoted by $M^\times$. Note that $M^\times$ is a group. Remark: If $(A^*, \cdot)$ is a monoid then $(A, +, \cdot)$ is an ~~cane~~ integral domain. Also, $(A^*, \cdot)$ is also a cancellatory monoid.

Example: For the monoid $(\mathbb{Z}, \cdot)$, $(\mathbb{Z}, \cdot)^\times = \{\pm 1\}$.

Let M be a commutative and cancellatory monoid. On M define a relation $\sim$: $a \sim b \overset{\text{def}}{\iff} b = ua$ for some $u \in M^\times$. Such pairs of a and b are called associates. Verify that $\sim$ is an equivalence relation. Let the quotient set generated by $\sim$ be denoted as $M/\sim = \bar{M}$.

Let $\bar{a}, \bar{b} \in \bar{M}$. We can define a binary operation ~~on~~ in the quotient set $\bar{M}$: $\bar{a} \cdot \bar{b} = \overline{ab}$.

Verify that this operation is well-defined.

By this operation the set of equivalence classes $\bar{M}$ becomes a monoid. Show that $(\bar{M})^\times = \{\bar{e}\}$.

Definition: $a \in M$ is called irreducible if $a \notin M^\times$ and the only divisor of a are units and associates of a.

$p \in \mathbb{N}^*$ is irreducible if $p > 1$ and the only divisors of p are 1 and p.

$p \in M$ is called prime if $p \notin M^\times$, and whenever $p \mid ab$ for any $a, b \in M$, then either $p \mid a$ or $p \mid b$.

4.1 Lemma: If $p \in M$, is prime, then P is irreducible.

Remark: The converse holds for $(\mathbb{N}^*, \cdot)$.

Proof: Let p be prime $\Rightarrow p \notin M^\times$.

To show that if $a \mid p$, then $a \in M^\times$ or $a = up$, $u \in M^\times$

$a \mid p \Rightarrow p = ab$ for some $b \in M$. Since p is prime either $p \mid a$ or $p \mid b$. $\Rightarrow$ Either $a = up$ or $b = vp$, $u, v \in M$.

Consider the case $b = vp$. Then $p = avp$.

If M is cancellatory, $1 = av \Rightarrow a \in M^\times$ (a is a unit)

Consider the case $a = up$. The $p = upb$.

If M is commutative and cancellatory, $e = ub$.

$\Rightarrow b \in M^\times$. Therefore $p = ab$ implies p and a are associates.

Therefore, prime numbers are ireducibles.

Illustrative Examples: $M = \{2^\nu \mid \nu \neq 1, \nu \in \mathbb{N}\}$

$4 \mid 8 \cdot 8$. but $4 \nmid 8$. Therefore, 4 is not prime.

Example: Fix prime $p \in \mathbb{N}$. $M = \mathbb{N}^* - \{p\}$

M is a multiplicative monoid, and p^2, p^3 are irreducible.

$p^2 \mid p^2 \cdot p^2 \cdot p^2 \Rightarrow p^2 \mid p^6$. However $p^6 = p^3 \cdot p^3$

But $p^2 \nmid p^3$. Therefore, p^2 is irreducible but not prime. As a result, M is not a factorial.

4.1 Theorem (Gauss): Fundamental theorem of Arithmetic

Let $n \in \mathbb{N}^*$, then (1) n is a product of irreducible elements, (2) the product representation of n is unique.

Proof: By induction. Theorem is true for $n=1$.
Assume the hypothesis for $n<m$, with the representation $m = q_1 q_2 q_3 \cdots q_s = p_1 p_2 \cdots p_r$

Let $m' = p_1 p_2 \cdots p_r - p_1 q_2 \cdots q_s$ (assume $p_1 < q_1$)

$$m' = (p_1 - q_1) q_2 \cdots q_s$$

Also $$m' = p_1 (p_2 \cdots p_r - q_2 \cdots q_s)$$

Since p_1 divides m', and $m' < n$, it must occur in the representation of m' at least. $\Rightarrow bp_1 = b(p_1 - q_1)$

$\Rightarrow q_1 = (1+b) p_1$. which is a contradiction $\Rightarrow p_1 \nmid q_1$.

Consider the case $q_1 < p_1$. By arriving at a similar contradiction, we will conclude $p_1 = q_1$. Factoring out p_1 from m, $\frac{m}{p_1}$ must have a unique representation

Therefore, theorem is proved.

4.2 Theorem: Let M be a monoid. Then the following are equivalent.

(1) Every $a \notin M^\times$ is a product of irreducible elements and this product is unique upto associates and its permutation. i.e, $a = p_1 p_2 \cdots p_r = q_1 \cdot q_2 \cdots q_s$, then $r = s$, & $\exists\ \sigma \in S(r)$ such that $q_i = u_i p_{\sigma(i)}$ $u_i \in M^\times$.

Such a monoid is called a <u>factorial</u>. Ex: $\mathbb{N}^*$.

(2) Every $a \notin M^\times$ is a product of irreducible elements and every irreducible element is a prime.

(3) Every $a \notin M^\times$ is a product of primes in M.

It is not necessary that every element of a monoid is a product of irreducible elements. For example, consider a infinite set X, The monoid is $(\wp(X), \cup)$ where $\wp(X)$ is the power set of X and $\cup$ is the union operation. $A|B \Rightarrow A \subseteq B$. The irreducible elements are singletons.