FUNDAMENTAL THEOREM OF ARITHMETIC

L 3/1

A $(M, \cdot)$ is a monoid. A element $a \in M$ is called irreducible if $a \notin M^{\times}$ and the only divisors of a are e and a.

~~3.1 lemma~~: Remark: An empty product $\prod_{i \in \phi} a_i = e$

$$\left(\prod_{i=1}^{n} a_i\right) a_{n+1} = \prod_{i=1}^{n+1} a_i$$

$$\left(\prod_{i \in I} a_i\right)\left(\prod_{j \in J} a_j\right) = \prod_{k \in I \cup J} a_k$$ where I, J are finite, $I \cap J = \phi$

Let $I = \phi$, $J = \{1\}$, $x = \prod_{i \in \phi} a_i$

$$\Rightarrow x \cdot a = a \Rightarrow x \overset{*}{=} e \Rightarrow \prod_{i \in \phi} a_i = e$$

3.1 Lemma: Every $n \in \mathbb{N}^*$ is a product of irreducible elements

proof: (proof by induction)

Order: On $\mathbb{N}$, there is a relation $\leq$ which is defined by $a, b \in \mathbb{N}$, $a \leq b$, or ~~$b \leq a$~~ $b \geq a$ ~~which~~ having the following properties. (a) reflexive $\leq$, $a \leq a$ $\forall a \in \mathbb{N}$,
(b) transitive $\leq$, if $a \leq b$, $b \leq c$ $\Rightarrow$ then $a \leq c$
(c) antisymmetry if $a \leq b$, $b \leq a$, then $a = b$.
(d) Total order: for $\forall a, b \in \mathbb{N}$ either $(a \leq b)$ or $(b \leq a)$.
Remark: Any set X having a relation satisfying the properties (a), (b) and (c), is called an ordered set.

Well-ordered property: A ordered set is well-ordered if every non-empty ~~set has~~ subset has a smallest element.
Example: $\mathbb{N}$ is well ordered, but not $\mathbb{Z}, \mathbb{R}, \mathbb{Q}$.
Symmetry of order: $a \leq b \Rightarrow$ ~~$b \leq a$~~ $b \geq a$. Let $a \leq b$, $c \neq 0$,
Monotonicity of $\leq$ with $+$ and $\cdot$ $\Rightarrow$ (i) $a + c \leq b + c$, (ii) $ac \leq bc$

3.2 Theorem: (Fundamental Theorem of Arithmetic)

Every $m \in \mathbb{N}^*$ is a product of irreducible elements which is unique upto a permutation.

Proof: Let $m \in \mathbb{N}^*$ be represented as $m = p_1 p_2 \cdots p_r$ and $q_1 q_2 \cdots q_s = m$, where $p_1, p_2 \cdots p_r, q_1, q_2 \cdots q_s$ are irreducibles. To be proved, $r = s$, and there exists a $\sigma \in \mathfrak{S}(\{1, \ldots r\})$ such that $p_i = q_{\sigma(i)}$

We may assume (WMA) $p_1 \leq p_2 \leq \cdots \leq p_r$ & $q_1 \leq q_2 \leq \cdots q_s$. Therefore, we have to prove (a) $r = s$, (b) $p_i = q_i \ \forall i$.

Proof by induction on r. If $r = 0$, then $m = 1 \Rightarrow s = 0 \Rightarrow r = s$. If $r = 1$ and $s \geq 2$ then $p_1 = q_1 q_2 \cdots q_s$ which implies p_1 is not irreducible which is a contradiction. Therefore $r = s = 1$ and $p_1 = q_1$. Let the hypothesis be true for $n \in \mathbb{N}^*$, $n < m$. ~~Put~~ We may assume $p_1 < q_1$. Put $n = m - p_1 q_2 q_3 \cdots q_s \Rightarrow n = (q_1 - p_1) q_2 q_3 \cdots q_s$

Also $n = p_1 (p_2 p_3 \cdots p_r - q_2 q_3 \cdots q_s) \Rightarrow$

$$p_1 (p_2 p_3 \cdots p_r - q_2 q_3 \cdots q_s) = (q_1 - p_1) q_2 q_3 \cdots q_s$$

Note that $n < m$, therefore, n must have a unique representation by the assumed hypothesis. Since p_1 occurs in the representation (as a factor) of n on the L.H.S. Therefore, p_1 must occur on the R.H.S of representation at least once. This is because ~~it~~ by the hypothesis $n < m$ ~~is~~ must have a unique representation as a product of irreducibles. Now, p_1 cannot occur in any one of the $q_2, q_3 \cdots q_s$ because $p_1 < q_1 \leq q_2 \leq \cdots q_s$. Therefore, p_1 must occur in the representation of $q_1 - p_1$. i.e, $p_1 = b(q_1 - p_1) \Rightarrow p_1(1+b) = q_1$. This is a contradiction because ~~p~~ q_1 is a irreducible. Therefore, $p_1 \geq q_1$. Using the same line of argument, we can arrive at a similar contradiction. Finally, $p_1 = q_1$. Proceeding similarly, the theorem can be proved.

Example: $M = \{4n+1 \mid n \in \mathbb{N}\} \subseteq \mathbb{N}$

$(M, \cdot)$ is a submonoid of $(\mathbb{N}^*, \cdot)$

$(21)\cdot(21) = 441 = 9 \cdot 49$. Here $21, 9, 49$ are all irreducible, but the representation of 441 as a product of irreducibles elements is not unique.

Example: $M = \{2^{\nu} \mid \underset{\nu \neq 1}{\nu \in \mathbb{N}}\} = \{1, 2, 2^3, \ldots\}$

$4 \cdot 4 \cdot 4 = 64 = 8 \cdot 8$ Here again 4 and 8 are irreducible, but 64 does not have a unique representation.

Definition: A monoid $(M, \cdot)$ is called a factorial if (1) every element of M is a product of irreducible elements

(2) ~~A~~ Every representation of a element as a product of irreducibles is unique upto a unit.

Example: ~~per~~ $(\mathbb{Z}^*, \cdot)$ is a factorial. Units are $\{\pm 1\}$.

Note that every monoid need not obey the condition (1) of the above definition.

Example: $\{P(X), \cup\}$, where X is a infinite set, $P(X)$ is the power set of X, and $\cup$ is the union operation (binary operation of the monoid).

Note that the irreducible elements of this monoid are the singletons.

similarly, the theorem can be proved.

Example: $M = \{4n+1 \mid n \in \mathbb{N}\} \subseteq \mathbb{N}$

$(M, \cdot)$ is a submonoid of $(\mathbb{N}^*, \cdot)$

$(21)\cdot(21) = 441 = 9 \cdot 49$. Here $21, 9, 49$ are all irreducible, but the representation of 441 as a product of irreducibles elements is not unique.

Example: $M = \{2^r \mid r \in \mathbb{N}, r \neq 1\} = \{1, 2, 2^3, \ldots\}$

$4 \cdot 4 \cdot 4 = 64 = 8 \cdot 8$ Here again 4 and 8 are irreducible, but 64 does not have a unique representation.

Definition: A monoid $(M, \cdot)$ is called a factorial if (1) every element of M is a product of irreducible elements

(2) ~~A~~ Every representation of a element as a product of irreducibles is unique upto a unit.

Example: ~~per~~ $(\mathbb{Z}^*, \cdot)$ is a factorial. Units are $\{\pm 1\}$.

Note that every monoid need not obey the condition (1) of the above definition.

Example: $\{P(X), \cup\}$, where X is a infinite set, $P(X)$ is the power set of X, and $\cup$ is the union operation (binary operation of the monoid).

Note that the irreducible elements of this monoid are the singletons.