Properties Of P-exponents

5.1 Theorem (Gauss): $(\mathbb{N}^*, \cdot)$ is a factorial monoid.

Corollary: $(\mathbb{Z}^*, \cdot)$ is also a factorial.

Every $n \in \mathbb{Z}^*$, can be expressed as

$$n = (-1)^{\varepsilon} p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}, \quad \varepsilon \in \{0,1\}$$

$p_1, p_2, \ldots p_n$ are distinct primes, $\alpha_1, \alpha_2 \ldots \alpha_n \in \mathbb{N}^*$. This form is called the normalized prime factorization of n. Let $\mathbb{P}$ denote the set of primes $\in \mathbb{N}$. We define a function $v_p : \mathbb{Z}^* \longrightarrow \mathbb{N}$ as

$$n \longmapsto v_p(n) = \begin{cases} \alpha_i & \text{if } p = p_i \\ 0 & \text{otherwise.} \end{cases}$$

The normalized prime factorization can be written as

$$n = (-1)^{\varepsilon} \prod_{p \in \mathbb{P}} p^{v_p(n)}$$

v_p is also called the p-adic valuation of $\mathbb{Z}$.

The properties of v_p are given below:

(1) $v_p(n) = 0$ for almost all $p \in \mathbb{P}$.

(2) $v_p(mn) = v_p(m) + v_p(n), \forall p \in \mathbb{P}$.

(3) $v_p(m+n) \geq \min\{v_p(m), v_p(n)\}$, $\forall p \in \mathbb{P}$ & $m+n \neq 0$

(4) $v_p(n) = 0 \ \forall p \in \mathbb{P} \iff$ ~~n = ±1~~ $n = \pm 1$

(5) $m | n$ (or n is a multiple of m) $\iff v_p(m) \leq v_p(n) \ \forall p \in \mathbb{P}$.

(6) $m = \pm n \iff v_p(m) = v_p(n) \ \forall p \in \mathbb{P}$ (m & n are associates)

In order to define $v_p(0)$, we define ∞ with the following properties: (i) $\forall \alpha \in \mathbb{Z}, \alpha < \infty$ ~~(ii) $\infty + \infty = \infty$~~, (iii) $\alpha + \infty = \infty$, (iv) $\infty + \alpha = \infty \quad \forall \alpha < \infty$

This element (∞) included in Z, ~~are~~ and the ~~set Z~~ extended set Z is denoted as $\overline{Z}$.

By introducing '∞', we can define $v_p(0) = \infty$. Note that with this definition of $v_p(0)$, the properties 1 to 6 of v_p continue to hold.

The definition of ν_p can be extended to $\mathbb{Q}$ as follows: Every $x \in \mathbb{Q}$ can be represented as $x = \frac{a}{b}$ $a, b \in \mathbb{Z}$, $b \neq 0$. Now, define ν_p as

$$\nu_p : \mathbb{Q} \longrightarrow \overline{\mathbb{Z}}$$

$$x = \frac{a}{b} \longmapsto \nu_p(a) - \nu_p(b)$$

Verify the following

(i) ν_p is well defined

(ii) If $x \in \mathbb{Q}^*$, then $x = (-1)^{\varepsilon(x)} \prod_{p \in \mathbb{P}} p^{\nu_p(x)}$

(iii) If $x \in \mathbb{Q}^*$ and $x \in \mathbb{Z} \iff \nu_p(x) \in \mathbb{N}, \ \forall p \in \mathbb{P}$

(iv) If $x \in \mathbb{Z}^*$, then x is the n^{th} power in $\mathbb{Q} \iff n \mid \nu_p(x)$ $\forall p \in \mathbb{P}$

5.2 Theorem (Gauss): If $y \in \mathbb{Q}$ satisfies

$$y^n + a_1 y^{n-1} + a_2 y^{n-2} \dots a_n = 0$$

where $a_1, a_2, a_3 \dots a_n \in \mathbb{Z}$, & $n \geq 1$, then $y \in \mathbb{Z}$

Proof: We will check $\nu_p(y) \geq 0 \ \forall p \in \mathbb{P}$

Let $\alpha = \nu_p(y)$.

$$\begin{aligned} n\alpha = n\nu_p(y) &= \nu_p(y^n). \\ &= \nu_p(-(a_1 y^{n-1} + a_2 y^{n-2} \dots a_n)) \\ &\geq \min\{\nu_p(-a_1 y^{n-1}), \nu_p(-a_2 y^{n-2}) \dots \nu_p(a_n)\} \end{aligned}$$

$\Longrightarrow$ $\cancel{n\alpha \geq \min\{(n-1)\nu_p(a_1)\alpha, (n-2)\nu_p(a_2)\alpha \dots \nu_p(a_n)\nu_p(1)\}}$

Using $\nu_p(ab) = \nu_p(a) + \nu_p(b)$

$$\Longrightarrow n\alpha \geq \min\{(n-1)\alpha, (n-2)\alpha, \dots 0\}$$

$$\Longrightarrow \alpha \geq 0 \quad \forall p \in \mathbb{P}.$$

Corollary: Given $n \in \mathbb{N}^*$, $\sqrt{n} \in \mathbb{Q} \Longrightarrow \nu_p(n)$ is even $\forall p \in \mathbb{P}$.

Greatest Common Divisor (GCD): Let M be a monoid, $a, b \in M$. An element $d \in M$ is called gcd

(a) If $d|a$ & $d|b$

(b) If $c|a$ & $c|b \Rightarrow c|d$

The existence of gcd can be easily shown by the fundamental theorem of arithmetic. If gcd exists it is unique upto a unit in M.

5.3 Theorem: Let M be a cancellative & commutative monoid. Then the following are equivalent:

(a) M is a factorial.

(b) Every $a \notin M^{\times}$ is a product of irreducible elements and gcd of any two ~~numbers~~ elements exists.

(Proof is given later)

Properties of GCD:

(1) $\gcd(a, a) = a$

(2) $a|b \Longleftrightarrow \gcd(a, b) = a$

(3) $\gcd(\gcd(a,b), c) = \gcd(a, \gcd(bc))$ (associative)

(4) $\gcd(ca, cb) = c \gcd(a, b)$ (distributive)

(5) $\gcd(ab, c) = \gcd(\gcd(a,c)b, c)$ (Product formula)

Elements $a, b \in M$ are relatively prime if $\gcd(a, b) = 1$.

In what follows we assume the existence of gcd.

5.1 Lemma: Let $a, b \in M$, then

$$\gcd(a,b) = 1 \text{ and } a|bc \Rightarrow a|c.$$

Proof: $a = \gcd(a, bc) = \gcd(bc, a)$

$= \gcd(\gcd(a,b)c, a) = \gcd(c, a)$

because $\gcd(a,b) = 1$

$a = \gcd(c, a) \Rightarrow a|c.$

Corollary: If $\gcd(a,b)$ exists $\forall\, a,b \in M$, then every irreducible element is prime

Proof: Let p be an irreducible element $\notin M^\times$.

To prove $p \mid bc \implies p \mid b$ or $p \mid c$.

$p = \gcd(bc, p) \implies \gcd(b,p) = p$ or $\gcd(c,p) = p$.

because: If $\gcd(b,p) = 1$ i.e $p \nmid b$, then by Lemma 5.1 $p \mid c$.

Proof of Theorem 5.3: Since existence of gcd implies that every irreducible element is a prime, M becomes a factorial monoid.

Division Algorithm, & Euclidean Algorithm

L 6/1

Divison algorithm for finding gcd: Let $a, b \in \mathbb{Z}$, then there exists unique integers q, r such that $a = qb + r$ with $0 \leq r < |b|$

Proof: We may assume $b > 0$, $a \geq 0$. We prove the existence by induction on a

if $a = 0$, $q = r = 0$

If hypothesis is true for ~~$a < b$~~, $a < n$,

then ~~to~~ when ~~$a \geq b$~~ $a = n$, $a - b < n$.

Therefore, ~~a~~ from hypothesis $a - b = \tilde{q} b + \tilde{r}$ $\tilde{q} \in \mathbb{Z}$, $0 \leq \tilde{r} < b$

$$a - b = \tilde{q} b + \tilde{r} \implies a = (\tilde{q}+1) b + \tilde{r}. \quad (\tilde{q}+1) \in \mathbb{Z}$$

To prove uniqueness, let $a = qb + r = q'b + r'$

$$\implies 0 = (q - q')b + (r - r')$$

$$\implies (q - q')b = (r' - r)$$

But $r' - r < |b|$ $\implies q = q'$ and $r = r'$.

$\implies r' - r = 0$