Unique Factorization in $\mathbb{Z}$

(Lemma)

Every positive integer can be written as a product of prime numbers.

(Proof)

Suppose the lemma is not true

Let $A = \{ n \in \mathbb{N} \mid n$ is not a prime product $\}$
(product of primes)

By well-ordering principle,

let $m = \min_{n \in A} n$

Clearly, m is not a prime

$\Rightarrow \exists\ r, s$ such that $1 < r, s < m$ and
$m = rs$

By minimality of m, r and s can be expressed as a prime product

$\Rightarrow$ m can also be expressed as a product of primes $(\Rightarrow \Leftarrow)$

$\Rightarrow$ A is an empty set

* Let p be prime and $n \in \mathbb{Z}$. Then

$\mathrm{ord}_p n = \max \{ a : p^a \mid n \}$

Theorem

Let $n \in \mathbb{Z} \setminus \{0\}$. Then n can be written as

$$n = (-1)^{\epsilon(n)} \prod_{p \mid n} p^{a(p)}$$

where the product runs over all prime numbers and all but finitely many $a(p)$ are zero, where $\epsilon(n) = \begin{cases} 0 & \text{if } n > 0 \\ 1 & \text{if } n < 0 \end{cases}$

Moreover $a(p)$ are uniquely determined, $a(p) = \mathrm{ord}_p n$

Lemma

Let $a, b \in \mathbb{Z}$, $b > 0$ then there exists $q, r \in \mathbb{Z}$, with $0 \leq r < b$ such that $a = qb + r$

(Proof)

Let $R = \{a - xb \mid x \in \mathbb{Z}\}$

Let r be the smallest non-negative element of R.

We claim that $0 \leq r < b$

If not, then $r \geq b$

$\Rightarrow a - xb - r \geq 0$

$\Rightarrow a - (x+1)b \geq 0$ ($\Rightarrow\Leftarrow$ minimality)

Lemma

If $a, b \in \mathbb{Z}$, then $(a, b) = (d)$ where $d = \gcd(a, b)$

Proof

Let $h = \gcd(a, b)$. We show that $(h) = (d) = (a, b)$

- $h \mid a$, $h \mid b \Rightarrow h \mid la + mb$ (Let $la + mb = d$ since $d \in (a, b)$)

  $\Rightarrow h \mid d \Rightarrow (d) \subseteq (h)$

- Since ~~ea~~ $a, b \in (d)$ $\Rightarrow d \mid a$ and $d \mid b$

  $\Rightarrow d \mid h \Rightarrow (h) \subseteq (d)$

Proposition

If $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$

(Proof)

By above lemma, $\exists\, x, y \in \mathbb{Z}$ such that

$ax + by = 1$

$\Rightarrow acx + bcy = 1 \cdot c$

$\Rightarrow a \mid c$ (since $a \mid acx + bcy$)

Corollary

Let p be a prime number.

$p \mid ab \Rightarrow p \mid a$ (or) $p \mid b$

(Proof)

If $p \mid a$, then we are done

Otherwise $\gcd(p, a) = 1 \Rightarrow p \mid b$

Corollary (Exercise!)

If $a, b \in \mathbb{Z}$, then $\operatorname{ord}_p ab = \operatorname{ord}_p a + \operatorname{ord}_p b$

(Theorem proof)

$$n = (-1)^{\epsilon(n)} \prod p^{a(p)}$$

Fix a prime q

$$\operatorname{ord}_q n = \sum a(p) \operatorname{ord}_q p$$

$$= a(q)$$

(Hence proved!)

$\mathbb{Z}$		$K[x]$
$\{\pm 1\}$	$\longleftrightarrow$	$K \setminus \{0\}$
positive integers	$\longleftrightarrow$	monic polynomials
prime numbers	$\longleftrightarrow$	monic irreducible polynomials
$\lvert n \rvert$	$\longleftrightarrow$	degree of polynomial

Unique factorization in $K[x]$

Lemma

Every monic polynomial can be written as product of monic irreducible polynomials.

(Theorem)

Let $f(x) \in K[x] \setminus \{0\}$, then f can be written as

$$f = c \prod_{\substack{p(x) \text{ is} \\ \text{monic irreducible}}} (p(x))^{a(p)}$$

where product runs over all monic irreducible polynomials and all but finitely many $a(p)$ are zero. Moreover $a(p)$, c are uniquely determined.

Let p be monic irreducible polynomial and $f(x) \in K[x]$

$$\operatorname{ord}_p f = \max\{a : p^a \mid f\}$$

(Proof!) $\rightarrow$ Exercise, very similar to $\mathbb{Z}$

Definition

Let R be an integral domain.

R is said to be an Euclidean domain, if there exists $\lambda : R \to \mathbb{N} \cup \{0\}$ such that for every $a, b \in R$ with $b \neq 0$ there exist $q, r \in R$ such that

$a = bq + r$ where either $r = 0$

or $0 \leq \lambda(r) < \lambda(b)$

(Theorem)

An Euclidean domain is a PID

(Proof)

b is an element of I with smallest λ value

For any $a \in I$

$a = qb + r$ either $r = 0$

$\Rightarrow r = 0$ or $0 \leq \lambda(r) < \lambda(q)$

$\Rightarrow I = (b)$