GCD, UFD, and More

Atrajit Sarkar

March 31, 2026

1 Introduction

For a standard reference on these definitions, see the bibliography below.

Notations:

- We have any ring $(R, +, .) := R$.
- Irreducible element: i
- Prime element: p
- Unique factorisation domain: **UFD**
- Greatest Common Divisor Domain: **GCD**
- greates common divisor of a, b : $gcd(a, b)$

Definitions:

1. **Irreducible element:** In R, a non zero, non unit element i is called irreducible element iff $i = ab \Rightarrow$ either a or b is an unit for any $a, b \in R$. Just think it similar to that in $\mathbb{Z}$. In $\mathbb{Z}$ only unit element are ± 1. So the above is traslated to definition of prime.

2. **Prime Element:** In R, a non zero non unit element p is called prime iff $p|ab \Rightarrow p|a$ or $p|b$ for any $a, b \in R$.

   > **Note:** Prime elements are irreducible elements in Integral Domains but converse is not true. See [69504] for the proof.

3. **UFD:** A commutative ring with identity and with no zero divisors (basicalyl an Integral domain) where every element a can be written uniquely as follows:

$$a = \prod_{i=1}^{n} p_i^{k_i} \quad ; k_i \in \mathbb{N}, p_i \text{ is prime element}$$

Note: In UFD, prime and irreducible elements are same. See [257955]

4. **GCD:** A GCD domain is an integral domain where any two elements a, b has a greatest common divisor(gcd). See [PMGCD] for more details and definitions.

5. **Associates:** In R, a, b are called associates iff $a = bu$ for some u is an unit.

2 UFD $\Rightarrow$ GCD

In this section we will prove that in a UFD, any two elements have a gcd.

The proof is same as we can do in $\mathbb{Z}$. Because note in $\mathbb{Z}$ the fundamental theorem of arithmatic is same as the requirement of $\mathbb{Z}$ being a UFD.

proof: So, we take two elements $a, b \in R$ and R being a UFD there is unique primes/irreducibles such that:

$$a = \prod_i p_i^{k_i} u_a, \quad b = \prod_j q_j^{r_j} u_b$$

u_a and u_b are units in R. Now, form an element $d \in R$ as follows,

$$d = \prod_{i,j} \mathrm{COM}(p_i, q_j)^{min\{k_i, r_j\}}$$

Here, $\mathrm{COM}(p_i, q_j) = 1$ if $p_i \neq uq_j$ or $\mathrm{COM}(p_i, q_j) = p_i = uq_j$ if $p_i = uq_j$.

Now, let $c \in R$ be a common divisor of a, b. So, there is $a_1, b_1 \in R$ such that $ca_1 = a$ and $cb_1 = b$. Also

$$c = \prod_t s_t^{m_t}$$

Now, comparing irreducible elements we get according to UFD property,

all s_t has to be an associate of some p_i as well as q_j and this only possible when $p_i = uq_j$ for that specific i, j. Then we have c is of the following form only,

$$c = \prod_{i,j} \mathrm{COM}(p_i, q_j)^{k_{i,j}}$$

where $k_{i,j} \leq min\{k_i, r_j\}$

Hence, $c|d$. Hence $d = gcd(a, b)$.

References

[257955] emmett (https://math.stackexchange.com/users/52451/emmett). *Irreducibles are prime in a UFD*. Mathematics Stack Exchange. URL:https://math.stackexchange.co (version: 2017-03-17). eprint: https://math.stackexchange.com/q/257955. URL: https://math.stackexchange.com/q/257955.

[69504] Hassan Muhammad (https://math.stackexchange.com/users/16942/hassan muhammad). *Is any prime element irreducible?* Mathematics Stack Exchange. URL:https://math.stackexchange.com/q/69504 (version: 2023-03-10). eprint: https://math.stackexchange.com/q/69504. URL: https://math.stackexchange.com/q/69504.

[PMGCD] PlanetMath. *GCD domains*. Wikipedia. URL:https://math.ubbcluj.ro/ calu/GCD.pdf (version: 2020-03-12). 2020. eprint: https://math.ubbcluj.ro/~calu/GCD.pdf. URL: https://math.ubbcluj.ro/~calu/GCD.pdf.